



UNIVERSIDAD DE SEVILLA

---

FACULTAD DE FÍSICA

DEPARTAMENTO DE FÍSICA ATÓMICA, MOLECULAR Y  
NUCLEAR

**ESTADOS GRAFO: ENTRELAZAMIENTO E  
IMPOSIBILIDAD DE ELEMENTOS DE  
REALIDAD LOCALES**

*Memoria presentada por*

**María del Pilar Moreno Martín**

*para optar al grado de Doctora en Física*

*Sevilla, 19 de abril de 2011*



DEPARTAMENTO DE FÍSICA ATÓMICA, MOLECULAR Y NUCLEAR  
Facultad de Física  
Universidad de Sevilla

**ESTADOS GRAFO: ENTRELAZAMIENTO E  
IMPOSIBILIDAD DE ELEMENTOS DE  
REALIDAD LOCALES**

*Memoria presentada al Departamento de Física Atómica, Molecular y Nuclear, y a la  
Comisión de Doctorado de la Universidad de Sevilla en cumplimiento parcial de los  
requisitos para optar al grado de Doctora en Física*

**El Director:**

**La Tutora:**

CU Adán Cabello Quintero

Dra. Clara Eugenia Alonso Alonso

**La Doctoranda:**

María del Pilar Moreno Martín

19 de abril de 2011



# Agradecimientos

Quiero expresar mi gratitud a mi director de tesis, el catedrático Adán Cabello Quintero, con quien he tenido la ocasión de trabajar; me gustaría agradecerle no sólo su implicación en el desarrollo de las investigaciones realizadas, sino también la confianza que depositó en mí al brindarme en su día la oportunidad de permitirme formar parte del grupo de Información Cuántica de la Universidad de Sevilla, y al luchar por conseguirme una beca de investigación. También quiero agradecerle el haber asumido la dirección de mi trabajo, así como su implicación en mi formación complementaria facilitando mi participación en congresos, en la impartición de clases y en la realización de una estancia en el extranjero.

He de agradecer a Luis Boza su ayuda con el programa que acompaña el artículo “*All-versus-nothing proofs with  $n$  qubits distributed between  $m$  parties*”; y a Antonio José López Tarrida, José Ramón Portillo y David Rodríguez sus inestimables aportaciones como coautores de algunos de los artículos publicados que, posteriormente, he podido desarrollar como capítulos en esta tesis.

A Terry Rudolph, quien con paciencia, dedicación y profesionalidad me transmitió valiosos conocimientos durante mi estancia en el Imperial College, que me enriquecieron como estudiante, sirviéndome todo ello de gran ayuda en el desarrollo de mi trabajo.

A Clara Eugenia Alonso, por el papel desempeñado como tutora en los trámites legales de esta tesis; y José Miguel Arias, Álvaro Domínguez y Paco Moreno, por haber accedido a formar parte del tribunal en la defensa de mi trabajo de investigación.

A los profesores, personal administrativo y técnico del departamento de Física Aplicada II de la Escuela Técnica Superior de Arquitectura, por propiciar un estupendo ambiente de trabajo. A Francisco Gascón y Pilar Gentil, que siempre fueron conmigo cercanos y encantadores. A Sara Girón, por su simpatía, su optimismo y sus ánimos. A Paco Nieves, por ser un excelente compañero de trabajo. A Aureliano Gómez, infalible en la búsqueda de soluciones a problemas técnicos. A Guillermo Manjón, por su nobleza, sencillez y cordialidad, por haberme ofrecido docencia y concedido permiso para que ocupara un hueco en el despacho de becarios. A Jesús Martel, por su amistad, por su apoyo y paciencia, y por su ayuda en el uso del dichoso LaTeX. A Rafael Morente, por orientar y agilizar cuantas gestiones me han sido necesarias. A Teófilo Zamarreño, que mientras era director del departamento hizo un gran esfuerzo al permitirme compartir despacho durante casi un año, también quisiera agradecerle su paciencia, ayuda y

orientación prestadas. No puedo dejar de mencionar a José Pablo Baltanás, Diego Frustaglia, Rafael García-Tenorio, Juan Mantero, Juan Lucas Retamar e Ignacio Vioque.

A los profesores del departamento de Física Aplicada II de la Escuela Técnica Superior de Ingeniería de Edificación, Adán Cabello, Manuel Jesús Espín, Miguel Galindo, Leoncio García, Antonio José López y Martín Muñoz, por haberme acogido como a uno más. He de agradecer especialmente a Agustín Fernández y a Helena Moreno su cordialidad y ayuda en solventar cuestiones de docencia, y a Francisco Pontiga su amabilidad y mediación en la búsqueda de soluciones a problemas técnicos de todo tipo.

A mis compañeras mexicanas del despacho de becarios, Marusia Rentería, Grisel Méndez y Mayra Luna, por su amistad y agradable compañía. Y a los también compañeros durante mi estancia en el Imperial College, Javi Cerrillo, Eduardo Martín, Álvaro Feito, Adolfo del Campo, Miguel Navascués, Alexander Plato y Fernando Brandão, por sus valiosas aportaciones y por haber compartido momentos muy divertidos.

En el plano personal quisiera dar las gracias a mis tíos Pascasio y Victoria, por su afecto y preocupación. A amigos y compañeros de carrera: José Torres, Inma Martínez, Chane, Rafa el tuno, Rafa el de Cádiz, Javi el mago, Diego Ridaó, Jacinto Díaz y tantos otros, por esos ratos de ocio y sueños compartidos, aunque ya estemos lejos unos de otros siempre nos tenemos en mente. A mi amiga Enry Molina por su amistad, ayuda y por el entusiasmo tan contagioso que muestra en todos sus proyectos. A mis amigos de Escacena del Campo, de quienes conservo unos dulces e inolvidables recuerdos. Por último quisiera mencionar a Rosario Cristina Veloz y Sonia Cano, por haber alimentado nuestros lazos de amistad a pesar de la distancia; y mi familia de acogida en Londres, los Behrens, por su hospitalidad y simpatía.

A todos ellos muchas gracias.

# Dedicatoria

Quisiera dedicar este trabajo a quienes han sido un pilar fundamental para que esta tesis llegue a buen fin: a mis padres, Evaristo y Carmen, por los esfuerzos realizados en todos los niveles durante mis estudios, así como por su apoyo incondicional y cariño, que han sido indispensables para no desistir en mis aspiraciones académicas; a mi abuela Carmen Bohórquez, que en paz descansas, el abuelo Paulino y tú habéis llenado nuestros corazones de tantas alegrías que no podría explicar con palabras y que, entre otras muchas cosas, me han aportado valores que me ayudan a crecer como persona; a la memoria de mis abuelos, Evaristo y Dolores, a quienes no tuve la suerte de conocer; a Mari Carmen, Evaristo, Victoria, Virginia y Miguel (hermanos, cuñada y sobrinito), por acompañarme en esta lucha con sus constantes actos y palabras de ánimo.

A todos ellos les dedico con todo mi cariño este trabajo.





# Índice general

<b>Agradecimientos</b>	<b>5</b>
<b>Dedicatoria</b>	<b>7</b>
<b>Resumen</b>	<b>13</b>
<b>Summary</b>	<b>15</b>
<b>Introducción</b>	<b>17</b>
<b>1. Estados grafo</b>	<b>21</b>
1.1. Introducción . . . . .	21
1.2. Definiciones de estados grafo . . . . .	21
1.3. Estado grafo y modelo de Ising . . . . .	22
1.3.1. Preparación de un estado grafo empleando puertas controlled-Z . . . . .	23
1.4. Estado grafo y formalismo estabilizador . . . . .	26
1.4.1. Propiedades del grupo estabilizador . . . . .	27
1.4.2. Estado grafo y estado estabilizador . . . . .	28
1.4.3. Estabilizador de un estado grafo . . . . .	29
1.5. Estudio de la evolución de un estado grafo a través de su estabilizador . . . . .	30
1.5.1. Medidas de Pauli . . . . .	30
1.5.2. Grupo de Clifford . . . . .	32
1.5.3. Grupo local de Clifford . . . . .	33
1.5.4. Definición de grupo de Clifford . . . . .	34
1.6. Preparación de estados grafo . . . . .	35
<b>2. Corrección cuántica de errores</b>	<b>37</b>
2.1. Introducción . . . . .	37
2.2. Corrección clásica de errores . . . . .	37
2.2.1. Código de repetición para corregir el error bit-flip . . . . .	38
2.3. Corrección cuántica de errores . . . . .	39
2.3.1. El código cuántico de tres qubits para el error bit-flip . . . . .	40
2.3.2. Código cuántico de tres qubits para el error phase-flip . . . . .	43
2.3.3. El código de 9 qubits de Shor . . . . .	43

2.4.	Discretización de errores . . . . .	44
2.5.	Códigos estabilizadores de corrección cuántica de errores . . . . .	45
<b>3.</b>	<b>Computación cuántica basada en medidas</b>	<b>49</b>
3.1.	Introducción . . . . .	49
3.2.	Modelos de computación cuántica . . . . .	50
3.3.	Simulación de la CCMC empleando CCBM . . . . .	53
3.3.1.	Formalismo estabilizador y computación cuántica basada en medidas . . . . .	54
3.3.2.	Implementación de una puerta lógica en computación cuántica basada en medidas . . . . .	55
3.4.	Implementación de más de una puerta lógica en computación cuántica basada en medidas . . . . .	59
3.5.	Ordenación temporal de las medidas . . . . .	60
<b>4.</b>	<b>Entrelazamiento</b>	<b>63</b>
4.1.	Introducción . . . . .	63
4.2.	Estados separables y estados entrelazados . . . . .	64
4.2.1.	Entrelazamiento en estados puros . . . . .	64
4.2.2.	Entrelazamiento en estados mezcla . . . . .	65
4.3.	Criterios de separabilidad . . . . .	66
4.3.1.	Entropía de von Neumann . . . . .	67
4.3.2.	Criterio PPT . . . . .	67
4.3.3.	Criterio de reducción . . . . .	68
4.3.4.	Descomposición de Schmidt . . . . .	68
4.3.5.	Desigualdades de Bell . . . . .	70
4.3.6.	Testigos de entrelazamiento . . . . .	70
4.4.	Operaciones locales sobre estados cuánticos . . . . .	71
4.5.	Cuantificación del entrelazamiento . . . . .	73
4.5.1.	Propiedades generales de las medidas de entrelazamiento . . . . .	73
4.6.	Clases de entrelazamiento para estados puros de hasta 4 qubits . . . . .	74
4.6.1.	Teorema de Nielsen . . . . .	74
4.6.2.	Equivalencia entre estados bajo SLOCC . . . . .	75
4.6.3.	Clasificación de los estados puros bajo SLOCC . . . . .	75
<b>5.</b>	<b>Entrelazamiento en estados grafo de ocho qubits</b>	<b>79</b>
5.1.	Introducción . . . . .	79
5.2.	Estados grafo y clases de equivalencia . . . . .	80
5.3.	Complementación local . . . . .	80
5.4.	Criterios de clasificación . . . . .	83
5.4.1.	Mínimo número de puertas controlled- $Z$ necesarias para la preparación . . . . .	83
5.4.2.	Medidas de Schmidt $E_S$ . . . . .	83
5.5.	Procedimientos y resultados . . . . .	86
5.5.1.	Órbitas bajo complementación local . . . . .	86
5.5.2.	Límites de la medida de Schmidt . . . . .	87

<b>6. Conjunto compacto de invariantes...</b>	<b>95</b>
6.1. Introducción . . . . .	95
6.2. Invariantes de Van den Nest, Dehaene y De Moor . . . . .	96
6.3. Resultados . . . . .	99
<b>7. El teorema de Bell</b>	<b>105</b>
7.1. Introducción . . . . .	105
7.2. El argumento de EPR de incompletitud de la Mecánica Cuántica . . . . .	105
7.2.1. Precisiones sobre el criterio EPR de elementos de realidad . . . . .	106
7.3. La versión de Bohm del experimento EPR . . . . .	107
7.4. Teorema de Bell . . . . .	109
7.4.1. Primera desigualdad de Bell . . . . .	110
7.4.2. Desigualdad CHSH . . . . .	113
7.5. Demostraciones “all-versus-nothing” del teorema de Bell . . . . .	116
7.5.1. Demostración GHZ del teorema de Bell . . . . .	116
7.5.2. Demostración AVN del teorema de Bell usando qubits y dos observadores	120
7.5.3. Demostraciones AVN del teorema de Bell con dos observadores empleando medidas en un solo qubit . . . . .	125
<b>8. Demostraciones “all-versus-nothing” bipartitas...</b>	<b>129</b>
8.1. Introducción . . . . .	129
8.2. Requisitos para una demostración BAVN. Estados grafo . . . . .	130
8.3. Correlaciones perfectas que contradicen los elementos de realidad EPR . . . . .	131
8.4. Estados grafo y distribuciones de qubits. . . . .	132
<b>9. Demostraciones “all-versus-nothing” <math>m</math>-partitas...</b>	<b>139</b>
9.1. Introducción . . . . .	139
9.2. Demostraciones AVN $m$ -partitas con $n$ qubits . . . . .	140
9.2.1. Demostraciones AVN $m$ -partitas específicas . . . . .	140
9.2.2. ¿Cuándo una distribución permite una demostración AVN específica? . .	143
9.2.3. Ejemplos prácticos . . . . .	144
9.3. Demostraciones AVN con un mínimo número $m$ de partes . . . . .	147
9.3.1. Posibles distribuciones entre un mínimo número $m$ de partes . . . . .	148
9.3.2. Demostraciones AVN con un mínimo número de partes para cualquier estado grafo . . . . .	150
<b>Conclusiones</b>	<b>159</b>
<b>Conclusions</b>	<b>163</b>
<b>Apéndice</b>	<b>167</b>
<b>Anexo</b>	<b>171</b>
Artículos publicados . . . . .	171
Aportaciones a congresos . . . . .	171

Bibliografía

227

# Resumen

Este trabajo trata de un tipo particular de estados puros de  $n$  qubits, los estados grafo. En el capítulo 1 se presentan tres definiciones de estados grafo (en base a su representación geométrica, al modelo de interacción y en términos del formalismo estabilizador) que posteriormente relacionaremos entre sí. A partir de estas definiciones introduciremos el formalismo estabilizador y obtendremos el estabilizador correspondiente a un estado grafo. Esta es una representación compacta de los estados grafo que nos permitirá describir cómodamente su evolución bajo la acción de las medidas de Pauli y los operadores del grupo de Clifford. Además, explicaremos cómo preparar estados grafo a partir de puertas controlled- $Z$ , y mostraremos algunas referencias donde se exponen detalladamente la preparación experimental de los estados grafo empleando varios métodos y recursos físicos.

Los estados grafo son fundamentales en muchas aplicaciones de la Información Cuántica. En los capítulos 2 y 3 se explica su importancia para la corrección cuántica de errores y la computación cuántica basada en medidas, respectivamente.

Los resultados novedosos se refieren a la clasificación de los estados grafo de hasta  $n = 8$  qubits (capítulo 5), a la identificación de las clases de equivalencia a las que pertenecen los estados grafo de hasta  $n = 8$  qubits (capítulo 6), y a la utilidad de los estados grafo para demostraciones del teorema de Bell de tipo Greenberger-Horne-Zeilinger (también llamadas demostraciones “all-versus-nothing” o, abreviadamente, AVN). Este tipo de demostraciones se abordan atendiendo a su complejidad, de forma que el caso bipartito se trata en el capítulo 8 y el caso  $m$ -partito en el capítulo 9. El capítulo 4 es una introducción al problema de la clasificación de estados entrelazados. En él se anticipan algunos conocimientos básicos para definir y estudiar el entrelazamiento en los estados cuánticos, se introduce brevemente la clasificación de los estados puros entrelazados de hasta  $n = 4$  qubits, y se explica cuáles son las operaciones locales que permiten obtener las clases de equivalencia de los estados grafo. El capítulo 7 es una introducción de los capítulos 8 y 9, en él hemos incluido: el teorema de Bell; dos tipos de desigualdades de Bell, EPR (Einstein-Podolsky-Rosen) y CHSH (Clauser-Horne-Shimony-Holt), atendiendo a si se desenvuelven o no en el escenario EPR original, así como las demostraciones AVN; también hemos discutido cuáles son las desigualdades de Bell que precisan de una menor eficiencia para su comprobación experimental; y la importancia de emplear los estados hiperentrelazados para la comprobación experimental de las demostraciones del teorema de Bell.

En el último capítulo mostramos las conclusiones de los capítulos 5, 6, 8 y 9 que son los que contienen los resultados originales de este trabajo.



# Summary

This work deals with particular types of pure states of  $n$ -qubits: the graph states. In the first chapter, three definitions of graph states (based on their geometric representation, on the subjacent interaction model, and in terms of the stabilizer formalism) are presented, and later interrelated. From these definitions, the stabilizer formalism is introduced and the stabilizer corresponding to a graph state is obtained. This is a compact representation of graph states which allows their evolution to be conveniently described under Pauli local measurements and Clifford operators. Furthermore, the technique for the preparation of graph states from controlled-Z gates is explained, and some references are provided where experimental preparation of graph states is depicted in detail by means of various methods and physical resources.

Graph states are essential in a wide range of applications in Quantum Information. In Chapters 2 and 3, their importance in quantum error correction, and in measurement-base quantum computation, respectively, is explained.

Our innovate results refer to the classification of graph states of up to  $n = 8$  qubits, (Chapter 5), to the identification of the classes of equivalences to which graph states of up to  $n = 8$  qubits belong, (Chapter 6), and to the usefulness of graph states in the proofs of Bell's Theorem of the type Greenberger-Horne-Zeilinger (also known as "all-versus-nothing" (AVN) demonstrations). These sort of demonstrations are addressed in accordance with their complexity, in such way that the bipartite case is dealt in Chapter 8, and the  $m$ -partite case in Chapter 9. Chapter 4 is an introduction to the problem of classification of entangled states where some basic knowledge is given for the definition and study of the entanglement in quantum states, where the classification of the pure entangled states of up to  $n = 4$  qubits are briefly introduced, and where it is explained which local operations allow the equivalence classes of graph states to be obtained. Chapter 7 is an introduction Chapters 8 and 9, and contains: Bell's theorem; two types of Bell's inequalities, EPR (Einstein-Podolsky-Rosen) and CHSH (Clauser-Horne-Shimony-Holt), while taking into account whether they are developed in the original EPR scenario; the AVN demonstrations; a discussion on which Bell inequalities need lower efficiency for their experimental testing; and the importance of using hyperentangled states in the experimental testing of the proofs of Bell's theorem.

In the final chapter, conclusions are drawn on Chapters 5, 6, 8, and 9 which contain the innovate results of this work.





# Introducción

Los estados grafo [1, 2] constituyen una importante subclase de estados estabilizadores. Desempeñan un papel fundamental en aplicaciones y protocolos del procesamiento de la información cuántica. En particular suponen un recurso esencial en la corrección cuántica de errores [3, 4, 5], computación cuántica basada en medidas [6, 7, 8, 9, 10, 11]. Los estados grafo violan máximamente ciertas desigualdades de Bell [12, 13, 14, 15], son robustos contra la decoherencia [16] y se pueden emplear para la obtención demostraciones “all-versus-nothing” del teorema de Bell [17, 18, 19, 20]. También desempeñan un papel fundamental en el estudio del entrelazamiento [1, 2, 21, 22].

Debido a su importancia los estados grafo se han preparado en muchos experimentos. Por ejemplo, están los experimentos de preparación de estados grafo de  $n$  qubits y  $n$  fotones hasta  $n = 6$  [23, 24, 25, 26, 27], los experimentos de preparación de estados grafo de 6 qubits y 4 fotones [28], de 8 qubits y 4 fotones [29], y de 10 qubits y 5 fotones [29]. En particular, los estados grafo de 8 qubits y 4 fotones son especialmente útiles por la alta visibilidad que exhiben.

La posibilidad de representar de forma compacta a los estados grafo a través de su estabilizador [5, 30, 31, 32] ha sido una de las propiedades fundamentales que ha convertido a estos estados en útiles herramientas para tantos propósitos. Por ejemplo, esta forma de representación facilita el estudio de la evolución de los estados grafo bajo la acción de los operadores del grupo de Pauli o los operadores del grupo local Clifford. A través de estos operadores un estado grafo que pertenece a una determinada clase de equivalencia se transforma en otro que pertenece a esa misma clase. La acción de los operadores del grupo local de Clifford se puede representar gráficamente a través de las reglas de complementación local. Dos grafos son equivalentes bajo LC (equivalentes bajo complementación local), o LC equivalentes (equivalentes bajo operaciones locales del grupo de Clifford), si a través de alguna operación local del grupo de Clifford (u operaciones de complementación local) uno cualquiera de ellos se transforma en el otro y viceversa. Las clases de equivalencia de los estados puros se pueden obtener aplicando operaciones SLOCC (operaciones locales estocásticas asistidas por comunicación clásica), de este modo sólo hay una clase de equivalencia para los estados entrelazados de dos qubits, y puede representarse por el estado singlete  $|\Psi^-\rangle$ ; 5 clases de equivalencia para los estados puros entrelazados de tres qubits [33, 34, 35] (entre ellas se encuentran las clases a las que pertenecen los estados  $|GHZ\rangle = \frac{(|000\rangle+|111\rangle)}{\sqrt{2}}$  y  $|W\rangle = \frac{(|100\rangle+|010\rangle+|001\rangle)}{\sqrt{3}}$ , que exhiben auténtico entrelazamiento tripartito); y una familia genérica de un número infinito de elementos, que contiene 9 subfamilias cada una de ellas con una forma diferente de entrelazamiento, asociada a los estados puros de 4 qubits [36]. Los estados grafo son estados puros que también se pueden clasificar a través de operacio-

nes SLOCC, pero para ellos se satisface la equivalencia  $\text{SLOCC} \Leftrightarrow \text{LU}$ , es decir, el problema de decidir si dos estados grafo son equivalentes SLOCC, se reduce al problema de decidir si son equivalentes bajo LU (transformaciones unitarias locales arbitrarias). El problema del estudio y clasificación del entrelazamiento de los estados grafo se puede simplificar aún más gracias a la conjetura  $\text{LU} \Leftrightarrow \text{LC}$ , que aunque es falsa en general, se cumple para estados grafo de hasta  $n = 27$  qubits [37, 38, 39]. En la Ref. [40] se muestra las distintas clases de equivalencia de los estados grafo de hasta  $n = 12$  qubits, donde los elementos de una misma clase son equivalentes bajo complementación local. La clasificación de los estados grafo de  $n$  qubits se realizó hasta  $n = 7$  en [1, 2], pero los invariantes empleados para etiquetar las clases u ordenarlas no distinguían entre algunas de ellas. En las Refs. [21, 22] realizamos la clasificación de los estados grafo de hasta  $n = 8$  qubits con invariantes que distinguen, sin ambigüedad, las distintas clases de equivalencia.

El estabilizador de un estado grafo permite estudiar las correlaciones cuánticas entre los resultados de medidas individuales realizadas sobre sus qubits. El estudio de tales correlaciones puede emplearse para la obtención de demostraciones “all-versus-nothing” (AVN) del teorema de Bell. El teorema de Bell y su demostración [41] condujeron a la invalidez del argumento EPR (Einstein, Podolsky y Rosen) [42] acerca de la incompletitud de la Mecánica Cuántica (MC), y supusieron una de las claves en el desarrollo de nuevas teorías como la Información y Computación Cuánticas. La demostración original del teorema de Bell está basada en correlaciones perfectas, lo que suponía un obstáculo para su comprobación experimental con la tecnología de entonces, esto dio pie al desarrollo de nuevas demostraciones del teorema de Bell. En este trabajo mostraremos dos tipos diferentes de desigualdades de Bell: aquellas que se basan en una predicción perfecta de los valores de los observables y en la hipótesis de localidad, estas son las desigualdades EPR pues se enmarcan en el argumento original EPR (i.e., desigualdades de Bell basadas en correlaciones perfectas); y aquellas en las que las condiciones de realismo y localidad se aplican sobre las probabilidades de los resultados de las medidas realizadas, no sobre los resultados de las medidas, éstas son las desigualdades CHSH (Clauser-Horne-Shimony-Holt) (i.e., desigualdades de Bell que no se basan en correlaciones perfectas).

Las demostraciones AVN son demostraciones del teorema de Bell que no emplean desigualdades. Estas demostraciones consisten en una contradicción algebraica y se sitúan en el marco original EPR [42]. Se han empleado en la construcción de nuevas desigualdades del teorema de Bell [14], que han contribuido a avanzar en el estudio de la eficiencia de detección de los fotodetectores, en la realización de experimentos sin escapatorias (loophole-free) del teorema de Bell, y en el estudio de la decoherencia. La primera demostración AVN del teorema de Bell fue propuesta por Heywood y Redhead [43]. Esencialmente mostraba la conexión entre los teoremas de Kochen-Specker y Bell. Pero la demostración AVN más conocida es la de Greenberger, Horne y Zeilinger (GHZ) [44, 45, 46]. En una demostración GHZ se requiere de un mínimo de tres observadores, a diferencia de los dos observadores de la demostración original del teorema de Bell. Hardy [47] proporcionó la primera demostración AVN bipartita, que aunque era válida para estados entrelazados no se satisfacía para estados máximamente entrelazados. Las verificaciones experimentales para los estados máximamente entrelazados conducían a evidencias que entraban en contradicción con el argumento EPR en el 100 % de las repeticiones de un mismo experimento. De este modo, la búsqueda de las demostraciones AVN evolucionó a fin de extender su validez a estados máximamente entrelazados de dos partículas. La primera demostración AVN

bipartita usando qubits y medidas de un solo qubit está en las Refs. [17, 18]. Esta demostración tenía un argumento similar al de Hardy, y requería únicamente de dos observadores y de un estado máximamente entrelazado. El interés de las medidas de un solo qubit está motivado por la dificultad práctica que conlleva hacer medidas generales de  $n$  qubits ( $n \geq 2$ ) cuando los qubits están codificados en diferentes grados de libertad dentro de la misma partícula. Esta demostración fue comprobada experimentalmente en [48]. Las violaciones de las desigualdades de Bell que presentan mayor contraste con las predicciones clásicas requieren una menor eficiencia para su comprobación experimental, por ejemplo, la demostración experimental de [48] requiere una eficiencia de detección más baja que la comprobación de la demostración GHZ [44, 45].

El empleo de estados hiperentrelazados supone una disminución considerable de los problemas de decoherencia, pues en su preparación se requiere un menor número de partículas. También simplifica la tarea de realizar la separación espacial entre las medidas (condición necesaria para evitar que las medidas sobre unos sistemas puedan influir sobre los resultados de las medidas realizadas sobre los otros), y disminuye la eficiencia de detección [18]. Para aquellos estados hiperentrelazados donde la dimensión  $d$  de cada subsistema sea  $d > 2$ , existen observables locales compatibles que se pueden considerar como elementos de realidad simultáneos [43]. Lo que implica que los observables que aparecen en cada sumando de una desigualdad de Bell de tipo EPR puedan ser compatibles. Estas desigualdades son fundamentales para estudiar el crecimiento de la no localidad de los estados hiperentrelazados [49, 50]. Con todas las ventajas que supone el trabajar con estados hiperentrelazados y los recientes avances que se han producido en la preparación de estos estados [51, 52, 28, 29], es lógico preguntarse por cuáles son las posibles distribuciones bipartitas que permiten demostraciones AVN usando medidas de un solo qubit. Este problema está relacionado con el de decidir qué estados de  $n$  qubits y qué distribuciones permiten desigualdades de Bell de tipo EPR [50, 53] y con nuevos problemas de complejidad de comunicación bipartitas, concretamente con nuevos esquemas de pseudotelepatía cuántica.

La solución a este problema [19] condujo a la búsqueda de demostraciones AVN multipartitas [20]. Los estados empleados para este tipo de demostraciones debían exhibir correlaciones perfectas que permitieran definir elementos de realidad EPR bipartitos, y correlaciones perfectas que contradijeran la existencia de esos elementos de realidad. De este modo los observables que satisfacen la condición EPR de elemento de realidad no pueden llegar a poseer valores predefinidos, porque es imposible asignarles valores que satisfagan las correlaciones perfectas predichas por la MC. Estos estados deben ser autoestados de un número suficientemente grande de operadores del grupo de Pauli. Los estados que encajan con esta descripción son los estados estabilizadores o estados grafo (cualquier estado estabilizador es equivalente bajo transformaciones locales de Clifford a algún estado grafo [32]). Los estados grafo son estados puros máximamente entrelazados, y muchos de ellos se pueden preparar como estados hiperentrelazados [51, 52, 28, 29]. En las Refs. [1, 2, 21, 22] se han obtenido las clases de equivalencia de los estados grafo de hasta  $n = 8$  qubits y fueron los que empleamos en estas demostraciones. No todos los estados grafo de  $n$  qubits, ni todas las distribuciones de sus qubits, permiten demostraciones AVN  $m$ -partitas del teorema de Bell para un determinado  $m$ , donde  $m$  es el número de partículas o partes. Existe una condición necesaria y suficiente para las demostraciones BAVN [19], y una condición necesaria para las demostraciones AVN  $m$ -partitas ( $m > 2$ ) [20]. Si un estado no admite una demostración BAVN (demostración AVN bipartita), entonces permitirá una demostración  $m$ -partita para

algún  $m$  mínimo con  $m > 2$ . Dado un estado grafo, si una distribución permite una demostración  $m$ -partita AVN para algún  $m$  dado, entonces esa misma distribución permitirá demostraciones  $m$ -partitas para cualquier estado grafo que pertenezca a su misma clase de equivalencia LC.

A partir de una demostración  $m$ -partita con  $m$  mínimo, se puede obtener otra con un número  $m$  arbitrario de partes. En las Refs. [19, 20] aportamos las *demostraciones específicas* AVN  $m$ -partitas con  $m$  mínimo ( $m \geq 2$ ) para estados grafo de hasta  $n = 8$  qubits (aunque el método empleado se puede aplicar para estados grafo de  $n > 8$ ). Estas demostraciones son válidas exclusivamente para cada estado grafo. Recientemente se han preparado en el laboratorio estados grafo de 6 qubits [25, 54], pero ninguno de ellos permitía demostraciones BAVN.

En los laboratorios, las correlaciones obtenidas no son perfectas, y lo más conveniente es derivar una desigualdad de Bell para la comprobación de la demostración AVN. La desigualdad de Bell debe violarse con un margen lo suficientemente amplio como para que las imperfecciones reales no puedan afectar a la validez de los resultados [50, 55]. En la Ref. [14], se obtienen las desigualdades de Bell EPR óptimas para los estados grafo de hasta  $n = 6$  qubits que están basadas en las demostraciones BAVN [19].

# Capítulo 1

## Estados grafo

### 1.1. Introducción

Los estados grafo [1, 2] representan un papel principal en Información y Computación Cuánticas. En particular, suponen un recurso esencial en las áreas de corrección cuántica de errores [3, 4, 5], de computación cuántica basada en medidas [6, 7, 8, 9, 10, 11] y clasificación del entrelazamiento [21, 22, 56, 57, 58].

Este primer capítulo se desarrollará en torno al concepto de estado grafo y su representación en términos del formalismo estabilizador. En la sección 1.2 se define el concepto de estado grafo desde tres perspectivas distintas. En las dos secciones siguientes situaremos las dos últimas definiciones en los contextos apropiados y se establecerán los puentes de conexión entre ellas. Concretamente, en la sección 1.3 se estudia la definición de estado grafo dada en función del modelo de interacción, y en la sección 1.4 se profundiza en la definición de estado grafo en términos del formalismo estabilizador; además a lo largo de estas secciones se caracterizará al grupo estabilizador, se verá cómo se preparan los estados grafo empleando controlled-Z, se mostrará la relación entre estado grafo y estado estabilizador, y se expondrá un ejemplo de cómo se obtienen los estabilizadores asociados a los estados grafo. En este capítulo emplearemos conceptos que en su mayoría están definidos en el apéndice.

En la sección 1.5 presentaremos el estabilizador de un estado grafo como instrumento para estudiar su evolución bajo la acción de las medidas de Pauli y de los operadores del grupo de Clifford. El contenido de esta sección se empleará en los capítulos 2, 4, 5 y 6. Finalizaremos con la sección 1.6 donde se recopilarán y comentarán brevemente algunas de las referencias respecto a la preparación de estados grafo. En este capítulo, muchas de los conceptos que se emplean aparecen definidos en el apéndice.

### 1.2. Definiciones de estados grafo

Dependiendo del contexto, se pueden utilizar diversas definiciones de estado grafo. A continuación, presentaremos tres definiciones dadas desde tres enfoques distintos. La primera está basada en la correspondencia biunívoca entre grafo y estado grafo, la segunda en el modelo de in-

teracción subyacente en los estados grafo, y la tercera en términos del formalismo estabilizador:

*Definición 1.* Un estado grafo  $|G\rangle$  de  $n$  qubits es un estado puro asociado a un grafo  $G(V, E)$  que contiene un conjunto de  $n$  vértices  $V = \{1, \dots, n\}$ , que representan qubits, y un conjunto de aristas  $E$  que conectan a pares de vértices,  $E \subset V \times V$ , y que representan relaciones de entrelazamiento entre los qubits correspondientes.

*Definición 2.* Un estado grafo  $|G\rangle$  es un estado puro de  $n$  qubits que se construye atendiendo al esquema de interacción dado por el grafo  $G(V, E)$  que lo representa. Cada arista  $\{a, b\}$  representa una interacción tipo Ising entre los qubits  $a$  y  $b$ . El procedimiento de preparación de un estado grafo a partir de un grafo consiste en partir de un número  $n = |V|$  de qubits en el estado inicial  $|+\rangle$ , y aplicar posteriormente  $C_Z$  entre los pares de qubits adyacentes<sup>1</sup> en  $G$  hasta obtener el estado  $|G\rangle = \prod_{\{a,b\} \in E} C_{Z_{ab}} |+\rangle^V$ .

*Definición 3.* Sea  $G(V, E)$  un grafo. Un estado grafo de  $n$  qubits es el único autovector de autovalor  $+1$  de un conjunto de  $n = |V|$  observables independientes que conmutan que son operadores del grupo de Pauli  $P_n$  (ver apéndice). Esos observables son los operadores generadores que generan el estabilizador  $S$  (ver apartado 1.4.1) asociado al estado grafo.

El concepto de estado grafo (y el de estado estabilizador) también puede extenderse a qudits<sup>2</sup> [2, 59, 60].

Estas tres definiciones están a su vez relacionadas entre sí, veamos cómo. La definición 1 está implícita en la 2 y la 3, pues un estado grafo  $|G\rangle$  dado viene representado por un único grafo  $G$ , el cual contiene en su estructura una receta, que por un lado, permite preparar experimentalmente  $|G\rangle$  (ver apartado 1.3.1), y por otro, obtener los  $n$  generadores estabilizadores que determinan  $|G\rangle$  de forma única (ver apartado 1.4.3). La conexión entre las definiciones 2 y 3 no se establece de forma tan inmediata. En las dos próximas secciones desarrollaremos los contextos en que se enmarcan estas definiciones y estableceremos la relación entre ellas.

### 1.3. Estado grafo y modelo de Ising

La interacción entre un par de qubits aislados del exterior se corresponde con una transformación unitaria dada por la expresión:

$$U_{ab} = e^{-i\varphi_{ab}H_{ab}}, \quad (1.1)$$

donde  $H_{ab}$  es el hamiltoniano de interacción entre el par de qubits  $a$  y  $b$ , y  $\varphi_{ab}$  es el término de evolución temporal. Aquí nos centraremos en un tipo particular de interacciones que se pueden representar mediante grafos simples. Estas interacciones se describen tomando como base al

---

<sup>1</sup>Dos qubits/vértices de un grafo son adyacentes si están unidos por una arista. Dos aristas son adyacentes si tienen un vértice en común.

<sup>2</sup>Los qudits son estados de  $d$  niveles.

modelo de Ising, que se aplicará a un conjunto de espines. Su expresión para dos qubits es

$$H = J\sigma_z^a\sigma_z^b + B(\sigma_z^a + \sigma_z^b). \quad (1.2)$$

Donde  $\sigma_z$  es la componente  $Z$  del espín de cada qubit,  $J$  es la constante de acoplamiento o de interacción<sup>3</sup> y  $B$  es la constante de interacción debida a la acción de un campo magnético global externo. El efecto que produce el campo magnético es el de rotar los qubits  $a$  y  $b$  alrededor del eje  $z$ ; tales rotaciones se pueden llevar a cabo antes o después de que los qubits interactúen, porque no interfieren en este proceso<sup>4</sup>. Por esta razón pueden ser obviadas, y considerarse únicamente el primer sumando

$$H_{ab} = \sigma_z^a\sigma_z^b. \quad (1.3)$$

Esta expresión es conocida como interacción de Ising pura [1]. La constante  $J$  se ha omitido porque puede incluirse en el factor de fase  $\varphi_{ab}$ .

Como veremos en el siguiente apartado, la interacción Ising contribuye a la generación del entrelazamiento multipartito entre los qubits de los estados grafo simples, y posibilita la aplicación de  $C_Z$  en la preparación experimental de estos estados.

### 1.3.1. Preparación de un estado grafo empleando puertas controlled-Z

Las propiedades de las transformaciones unitarias  $U_{ab}$  correspondientes a una interacción de Ising pura son:

1. El orden en que actúan es irrelevante, por lo tanto, son compatibles entre sí

$$[U_{ab}, U_{bc}] = 0, \forall a, b, c \in V. \quad (1.4)$$

2. Los operadores  $U_{ab}$  son simétricos

$$U_{ab} = U_{ba}. \quad (1.5)$$

Estas dos propiedades hacen posible que las interacciones entre los qubits se representen a través de grafos simples, donde cada arista simboliza una interacción de Ising.

Si el estado en que se encuentra cada qubit antes de interactuar es  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ , el estado resultante tras la interacción será máximamente entrelazado<sup>5</sup> y podrá describirse eficientemente en función de su estabilizador.

Por comodidad, en lugar de emplear la interacción de Ising pura, se suele utilizar la controlled phase cuyo hamiltoniano se denotará como  $H_{ab}^{cp}$ . Esta interacción también se ajusta al modelo de Ising, de hecho están relacionadas, puesto que

$$H_{ab}^{cp} = |1\rangle\langle 1|_a \otimes |1\rangle\langle 1|_b, \quad (1.6)$$

<sup>3</sup>Si la interacción es uniforme, entonces todos los vecinos de una partícula dada se encuentran a una misma distancia de ella; en el modelo Ising las interacciones a larga distancia son despreciables.

<sup>4</sup>La orientación del espín de cada qubit está condicionada por la de los qubits vecinos y las fluctuaciones térmicas

<sup>5</sup>El estado vector  $|\psi\rangle_{ab} = U_{ab}|+\rangle|+\rangle$  es máximamente entrelazado si y sólo si el estado reducido de un qubit es máximamente mezcla:  $\text{tr}_a|\psi\rangle_{ab}\langle\psi| = \frac{1}{2}I_b$ .

y sustituyendo cada proyector, obtenemos

$$H_{ab}^{cp} = \left( \frac{I - \sigma_z^a}{2} \right) \otimes \left( \frac{I - \sigma_z^b}{2} \right) = \frac{1}{4} (I \otimes I - \sigma_z^a \otimes I - I \otimes \sigma_z^b + \sigma_z^a \otimes \sigma_z^b). \quad (1.7)$$

Salvo factor de fase, el último sumando se corresponde con una interacción de Ising pura.

Exponenciando la expresión (1.7) y de acuerdo con (1.1), resulta

$$U_{ab}^{cp}(\varrho_{a,b}) = e^{-i\frac{\varrho_{ab}}{4}} e^{-i\frac{\varrho_{ab}}{4}\sigma_z^a} e^{-i\frac{\varrho_{ab}}{4}\sigma_z^b} U_{ab}\left(\frac{\varrho_{a,b}}{4}\right), \quad (1.8)$$

es decir, para una fase de  $\varphi_{ab} = \Pi$ , las transformaciones unitarias correspondientes a las interacciones Ising y la controlled phase, se diferencian en rotaciones adicionales de ángulo  $\frac{\Pi}{4}$  alrededor del eje  $z$ . La fase adicional de ángulo  $-\Pi/4$  se puede ignorar porque afecta a todo el estado. Trabajar con la exponencial de la controlled phase (i.e., controlled phase gate) tiene la ventaja de que su expresión es mucho más fácil de manejar.

La forma matricial de la controlled phase gate es

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi_{ab}} \end{pmatrix}. \quad (1.9)$$

En el caso particular de  $\varphi_{ab} = \Pi/4$ , lo que se obtiene es la puerta controlled-Z,  $C_Z$ , cuya forma matricial es

$$U_{ab} = C_Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \quad (1.10)$$

Y su expresión en función de los proyectores es

$$\begin{aligned} C_Z &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \\ &= |0\rangle\langle 0|_1 (|0\rangle\langle 0| + |1\rangle\langle 1|)_2 + |1\rangle\langle 1|_1 (|0\rangle\langle 0| - |1\rangle\langle 1|)_2 \\ &= \left( \frac{1 + Z_1}{2} \right) \otimes I_2 + \left( \frac{1 - Z_1}{2} \right) \otimes Z_2 \\ &= \frac{1}{2} (I + Z_1 \otimes I_2 + I_1 \otimes Z_2 - Z_1 \otimes Z_2). \end{aligned} \quad (1.11)$$

Los subíndices en esta expresión se refieren a los qubits sobre los que actúan los proyectores.

En resumen, si se aplica una  $C_Z$  sobre un par de qubits, que se encuentren inicialmente en el estado  $|\psi_0\rangle = |+\rangle_a |+\rangle_b = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ , se obtiene el estado máximamente entrelazado  $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$ . Esta operación equivale a crear una arista entre los qubits  $a$  y  $b$ , no conectados inicialmente. Por ser  $U_{ab}$  hermítico, al actuar sobre el estado  $|\psi\rangle$ , el par  $(a, b)$  se desentrelaza y pasa de nuevo al estado  $|\psi_0\rangle$ ; o equivalentemente, se crea una arista y posteriormente se destruye.



De acuerdo con la definición 2 de estado grafo, para preparar un estado grafo  $|G\rangle$  de  $n$  qubits se parte de un número  $n = |V|$  de qubits, cada uno de ellos en el estado inicial  $|+\rangle$  ( $|\psi_0\rangle = \bigotimes_{i \in V} |+\rangle_i$ , o de forma más reducida  $|\psi_0\rangle = |+\rangle^V$ ), que se representa por un grafo vacío o sin aristas. Posteriormente, se aplica una  $C_Z$  entre cada par de qubits  $(a, b)$  adyacentes en  $G$  hasta obtener el estado  $|G\rangle = \prod_{\{a,b\} \in E} C_{Z_{ab}} |+\rangle^V$ . Ver Fig. 1.1.

$$|\psi_0\rangle = |+\rangle \otimes \cdots \otimes |+\rangle \mapsto |G\rangle = \prod_{(a,b) \in E} C_{Z_{ab}} |+\rangle^V. \quad (1.12)$$

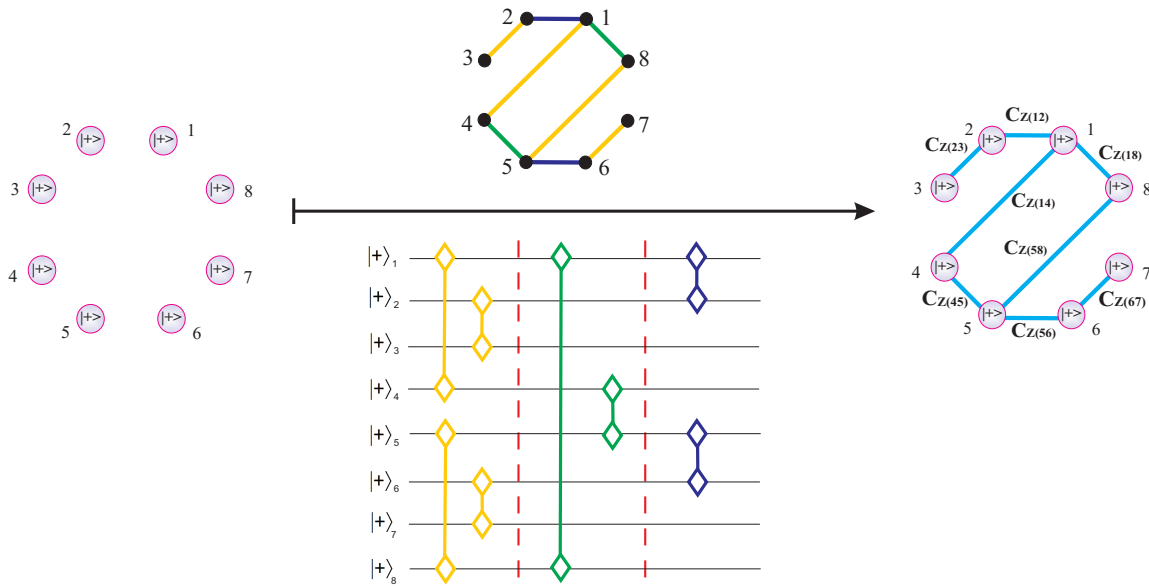


Figura 1.1: Esquema de preparación de un estado grafo  $|G\rangle$  a partir del grafo  $G(V, E)$  que lo representa. Los qubits se encuentran inicialmente en el estado  $|\psi_0\rangle = |+\rangle^V$  que se corresponde con un grafo vacío, y posteriormente, siguiendo el patrón de construcción dado por el grafo, se aplican las  $C_{Z_{ij}}$  necesarias hasta obtener el estado grafo  $|G\rangle$  deseado. La secuencia de aplicación de  $C_Z$  en la que se invierte menos tiempo viene indicada en el circuito.

Teniendo en cuenta que ninguno de los qubits del par que participa en una  $C_Z$  puede emplearse simultáneamente en más de una de estas operaciones, este método de preparación de estados grafo se puede llevar a cabo en un tiempo mínimo que depende del grado del grafo (o máximo grado de todos sus vértices) que represente al estado. Por ejemplo, en la Fig. 1.1 se puede observar el circuito que corresponde a la preparación de un estado grafo; las operaciones  $C_Z$  que se encuentran a un mismo lado de cada línea roja se realizan simultáneamente, y, de acuerdo con el grado del grafo, se invierten tres pasos de tiempo en preparar el estado.

Otro método de preparación de estados grafo es aquel que consiste en elaborar un cluster, que es una estructura como la de la Fig. 3.6, e ir eliminando qubits aplicando las medidas de proyección adecuadas hasta conseguir el estado grafo deseado (capítulo 3). El problema que

surge con este método es que se consume más tiempo (y como consecuencia, el sistema queda expuesto durante más tiempo a las indeseadas interacciones con el entorno) que cuando se emplea el procedimiento basado en  $C_Z$ , pues es preciso construir en primer lugar el cluster y posteriormente eliminar los qubits sobrantes.

En la última década se han desarrollado técnicas basadas en la aplicación de  $C_Z$  para preparar estados grafo de  $n$  qubits y  $m$  partículas (para  $n > m$ ), por ejemplo estados de 6 qubits y 2 partículas [51, 52], de 6 qubits y 4 partículas [28], de 8 qubits y 4 partículas [29], y de 10 qubits y 5 partículas [29].

La definición 1 de estado grafo se fundamenta en la propiedad de que dos estados grafos diferentes,  $|G(V, E)\rangle$  y  $|G'(V, E')\rangle$ , no pueden venir representados por el mismo grafo<sup>6</sup>. Demostrar esta propiedad es inmediato a través del siguiente argumento:

Supongamos que se desea desentrelazar dos estados grafo distintos,  $|G\rangle$  y  $|G'\rangle$ , para obtener el estado vacío  $|+\rangle^V$ . Como las operaciones de entrelazamiento  $C_Z$  son unitarias, habrá que aplicar tantas  $C_Z$  sobre dichos estados como aristas haya. Si los dos estados grafo distintos vienen representados por el mismo grafo  $G$ , entonces se deberá aplicar las mismas  $C_Z$  sobre estos estados para deshacer las mismas aristas, con lo cual

$$\begin{aligned} |+\rangle^V &= \prod_{\{a,b\} \in E} C_{Z_{ab}} |G\rangle = \prod_{\{a,b\} \in E} C_{Z_{ab}} |G'\rangle \\ &= \prod_{\{a,b\} \in E} C_{Z_{ab}} \prod_{\{a,b\} \in E'} C_{Z_{ab}} |+\rangle^V. \end{aligned} \tag{1.13}$$

Esta igualdad será posible si y sólo si los estados grafo son iguales. Luego dos estados vendrán representados por el mismo grafo si y sólo si son iguales.

## 1.4. Estado grafo y formalismo estabilizador

La forma tradicional de representar un estado cuántico es mediante su vector estado. Sin embargo, esta representación no siempre es la más adecuada, pues uno de sus inconvenientes es que el número de vectores base se incrementa de forma exponencial con el número de qubits. El formalismo estabilizador proporciona una representación para los estados grafo basada únicamente en ciertos operadores. Gracias a esta propiedad los estados grafo se pueden emplear en la corrección cuántica de errores [61, 3, 4, 5], a través de códigos estabilizadores; como recurso en computación cuántica basada en medidas [7, 8, 9, 11], y como laboratorio teórico para el estudio del entrelazamiento [56, 57, 58, 21, 22].

---

<sup>6</sup>Los estados grafos  $|G(V, E)\rangle$  y  $|G'(V, E')\rangle$  vendrán representados por estabilizadores distintos,  $S$  y  $S'$ , (ver sección 1.4.3), y precisarán de un número diferente de puertas  $C_Z$  para su preparación (ver sección 1.3.1). Es en este sentido en el que dichos estados no pueden estar representados por un mismo grafo. Si dichos estados poseyeran un entrelazamiento entre sus qubits tal que pertenecieran a la misma clase de equivalencia, sí podrían ser representados por un mismo grafo pero sólo en el marco del estudio del problema de la clasificación del entrelazamiento.

Comenzaremos exponiendo las propiedades del grupo estabilizador.

### 1.4.1. Propiedades del grupo estabilizador

Un *estabilizador*  $S$  de  $n$  qubits se define como cualquier subgrupo abeliano del grupo de Pauli  $P_n$ , que no contenga  $-I^{\otimes n}$  (si este operador estuviera incluido en el estabilizador  $S$ , entonces estabilizaría a su estado asociado  $|\psi\rangle$ ,  $-I^{\otimes n}|\psi\rangle = |\psi\rangle = -|\psi\rangle$ , de donde se deduce que  $|\psi\rangle = 0$ ). Los elementos de  $S$  se denominan *operadores estabilizadores*. El grupo estabilizador se caracteriza por unas propiedades elementales que citaremos a continuación y que se pueden encontrar con más detalle en la bibliografía [62, 1, 2]:

1. Si un estado es autoestado de autovalor  $+1$  de un operador  $A$ ,  $A|\psi\rangle = |\psi\rangle$ , entonces se dice que  $|\psi\rangle$  es *estabilizado* por dicho operador, el cual recibe el nombre de *operador estabilizador*. Por ejemplo, supongamos que el operador de Pauli  $\sigma_X$ , que denotaremos por  $X$ , actúa sobre los estados  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  y  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$X|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad (1.14a)$$

$$X|-\rangle = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (1.14b)$$

A la vista de estos resultados, el operador  $X$  estabiliza sólo al estado  $|+\rangle$ . Además, es el único operador capaz de estabilizar a dicho estado. Se podría realizar un estudio equivalente para el autovalor  $-1$ . En tal caso el estado estabilizado por  $X$  sería el  $|-\rangle$ .

2. La expresión general de los operadores estabilizadores es:  $g = \pm g_1 \otimes \dots \otimes g_n$ , con  $g_i \in P_1$ , siendo  $P_1 = \{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$ . Estos operadores son hermíticos y las matrices que los representan son de dimensión  $2^n \times 2^n$ .

3. Si  $g \in S$ , entonces  $-g \notin S$ .

4. La traza de un operador estabilizador diferente de la identidad es nula.

5. Si dos operadores estabilizadores,  $g$  y  $h$ , estabilizan un estado estabilizador  $|S\rangle$ , su producto  $g \cdot h$  estabilizará el mismo estado.

6.  $S$  como subgrupo de  $P_n$ , posee  $k$  operadores independientes que reciben el nombre de *operadores estabilizadores generadores* u *operadores generadores* de  $S$ . Posee  $2^k$  operadores en total, y lo conforman los  $k$  operadores generadores, todos los posibles productos entre ellos y el operador identidad. Todos ellos conmutan a su vez con la identidad  $I$ . Por estas características  $S$  tiene estructura de grupo, y se denomina *grupo estabilizador* o abreviadamente *estabilizador*. Por ser todos sus elementos compatibles entre sí, el grupo estabilizador es abeliano por construcción. El rango de  $S$  coincide con el cardinal del conjunto de operadores generadores<sup>7</sup>, y, en general,

<sup>7</sup>Los operadores del grupo de Pauli de orden  $n$  se pueden expresar como vectores en notación binaria, lo que permite, entre otras muchas aplicaciones, calcular el rango de un estabilizador  $S$  asociado a un estado grafo  $|G\rangle$ .

en un sistema de  $n$  qubits se satisface que:

$$\text{rang}(S) \leq n. \quad (1.15)$$

7. Sea  $H_S$  el subespacio vectorial común estabilizado por todos los elementos de  $S$ . El número de estados linealmente independientes (l.i.) contenidos en  $H_S$  (o equivalentemente, la dimensión del subespacio  $H_S$ ) se determina mediante la traza del proyector sobre dicho subespacio. El proyector se construye a través de los proyectores  $P_{g_k}$  de los generadores  $g_k$  del estabilizador,  $P_{g_k} = \frac{1}{2}(I + g_k)$ , cuyas trazas valen

$$\text{tr} \left( \frac{I + g_k}{2} \right) = \frac{2^n}{2} = 2^{n-1}. \quad (1.16)$$

La lectura que acompaña a este resultado es que cada operador  $g_k$  estabiliza  $2^{n-1}$  estados l.i.. Extendiendo este razonamiento al conjunto de todos los generadores se construye el proyector sobre el subespacio  $H_S$ , y se obtiene su dimensión a través de la traza

$$\text{tr} \left( \frac{I + g_1}{2} \cdot \frac{I + g_2}{2} \cdots \frac{I + g_k}{2} \right) = \frac{2^n}{2^k} = 2^{n-k}. \quad (1.17)$$

La dimensión del subespacio estabilizado  $H_S$  es  $2^{n-k}$ , donde  $n$  es el número de qubits del sistema y  $k$  el número de operadores generadores. Cada elemento del estabilizador  $S$  estabiliza el mismo subespacio  $H_S$  que es el subespacio más extenso que satisface:  $SH_S = H_S$ . Obsérvese que cada proyector en (1.17) reduce a la mitad la dimensión del estado estabilizado por los proyectores anteriores.

En el apartado siguiente relacionaremos los conceptos de estado estabilizador y estado grafo.

### 1.4.2. Estado grafo y estado estabilizador

Cualquier estabilizador  $S$  donde  $\text{rang}(S) = n$  (i.e., que sea de rango completo) estabiliza, de acuerdo con la expresión (1.17), a un único estado puro denominado *estado estabilizador*  $|S\rangle$ . Luego el estado estabilizador  $|S\rangle$  es el único estado puro que es autoestado de autovalor +1 de todos los elementos de  $S$

$$S|S\rangle = |S\rangle. \quad (1.18)$$

Un estado estabilizador está completamente determinado por su estabilizador.

Un estado grafo es un estado estabilizador (capítulo 5 sección 5.2). Luego a cada estado grafo le corresponde un estabilizador que satisface

$$S|G\rangle = |G\rangle. \quad (1.19)$$

La forma más compacta de expresar un estado grafo de  $n$  qubits en términos de su estabilizador es

$$|G\rangle\langle G| = \prod_{k=1}^n \left( \frac{g_k + I}{2} \right), \quad (1.20)$$

donde los  $g_k$  son los operadores generadores. Si se desarrollara esta expresión, el numerador estaría ocupado por los  $2^n$  operadores de  $S$  asociados al estado grafo, y el denominador por el cardinal de este conjunto de operadores. Un ejemplo práctico donde se utiliza la expresión (1.20) es en la obtención de testigos de entrelazamiento basados en operadores estabilizadores [63, 64, 65], que esencialmente consiste en construir operadores que detectan el auténtico entrelazamiento multipartito en ciertos estados grafo.

### 1.4.3. Estabilizador de un estado grafo

A continuación describiremos cómo se obtienen los elementos del estabilizador  $S$  que caracterizan a un estado grafo  $|G\rangle$  dado, a partir de su grafo  $G$ .

Cada arista del grafo representa una interacción Ising (ver sección 1.3) entre el par de qubits  $(a, b)$  situado en sus extremos. A cada qubit  $i$  se le asigna un operador generador  $g_i$  que se construye a partir del producto tensorial entre la componente  $X$  de espín para el qubit  $i$ , la componente  $Z$  para los qubits  $j \in N_i$  (donde  $N_i$  es la vecindad<sup>8</sup> del qubit  $i$ ), y la identidad  $I$  para aquellos qubits  $k \notin N_i$ , de modo que

$$g_i = X_i \bigotimes_{j \in N_i} Z_j; \quad i = 1, \dots, n. \quad (1.21)$$

Por simplificar no hemos incluido en esta expresión la identidad. Cada uno de los  $g_i$  se puede interpretar como un “patrón de medida” a seguir en cualquier realización experimental con estados estabilizadores, donde cada factor especifica qué componentes de espín medir sobre cada qubit (la identidad equivale a no realizar ninguna medida).

Los posibles resultados de estas medidas son:  $m_x = \pm 1$  y  $m_z = \pm 1$ . Y de acuerdo con la expresión (1.21), han de estar correlacionados de forma que

$$m_{ix} \prod_{j \in N(i)} m_{jz} = 1. \quad (1.22)$$

Los  $2^n$  elementos de  $S$  que estabilizan  $|G\rangle$  proporcionan una colección de correlaciones entre todos los posibles resultados de las medidas de las componentes de espín de cada qubit, que caracterizan unívocamente al estado.

Tomaremos como ejemplo para la construcción de un estabilizador  $S$  el estado grafo  $|LC_3\rangle$ . Este estado es conocido como estado linear cluster de tres qubits, atendiendo al nombre por el que se conoce en Información Cuántica al grafo que lo representa (ver Fig. 1.2). En general, todos los estados grafo basados en grafos de este tipo se denominan estados linear cluster de  $n$  qubits, y se denotan como  $|LC_n\rangle$ .

Los operadores generadores viene dados por las expresiones (1.23a)-(1.23c).

---

<sup>8</sup>Ver definición de vecindad de un vértice de un estado grafo en el apéndice.



Figura 1.2: Grafo que representa al estado grafo  $|LC_3\rangle$ .

$$g_1 = X_1 Z_2 I_3, \quad (1.23a)$$

$$g_2 = Z_1 X_2 Z_3, \quad (1.23b)$$

$$g_3 = I_1 Z_2 X_3. \quad (1.23c)$$

El resto de los elementos del estabilizador  $S$  se obtiene realizando todas las posibles multiplicaciones entre los  $g_i$  sin que se repita ningún resultado

$$g_1 g_2 = Y_1 Y_2 Z_3, \quad (1.24a)$$

$$g_1 g_3 = X_1 I_2 X_3, \quad (1.24b)$$

$$g_2 g_3 = Z_1 Y_2 Y_3, \quad (1.24c)$$

$$g_1 g_2 g_3 = -Y_1 X_2 Y_3. \quad (1.24d)$$

Una forma compacta de expresar el producto de los generadores es ir acumulando todos los índices en un mismo  $g$ , por ejemplo,  $g_1 g_2 \rightarrow g_{12}$ . Para  $n = 3$  hay un total de  $2^3 = 8$  operadores estabilizadores, al incluir la identidad  $I = I_1 \otimes I_2 \otimes I_3$ . Sólo existe un único estado grafo de tres qubits que sea autoestado de estos 8 operadores estabilizadores, y es el  $|LC_3\rangle$ .

A través del estabilizador  $S$  de un estado grafo dado  $|G\rangle$ , se puede analizar cómo evoluciona éste cuando sobre él se realizan medidas proyectivas y transformaciones unitarias. Desarrollaremos este contenido en los siguientes apartados.

## 1.5. Estudio de la evolución de un estado grafo a través de su estabilizador

El estabilizador de un estado grafo resulta de gran utilidad en el estudio de su evolución bajo la acción de ciertas medidas y operadores unitarios. En este apartado estudiaremos cómo evoluciona un estado grafo  $|G\rangle$  tras la aplicación de medidas de Pauli y operadores del grupo de Clifford, empleando su estabilizador  $S$ .

Estas operaciones transforman un estado estabilizador en otro que también es estabilizador, lo cual permite el uso continuado del formalismo estabilizador para describirlos. Este hecho es particularmente útil en corrección cuántica de errores [61, 3, 4, 5] (capítulo 2), en computación cuántica basada en medidas [7, 8, 9, 11] (capítulo 3), y en el estudio del entrelazamiento de los estados grafo [21, 22, 56, 57, 58] (capítulos 5 y 6).

### 1.5.1. Medidas de Pauli

Las *medidas de Pauli* son las medidas proyectivas realizadas con operadores  $O$  pertenecientes al grupo de Pauli  $P_n$ . Al realizar una medida de Pauli sobre un estado estabilizador  $|S\rangle$ , el

resultado es otro estado estabilizador  $|S'\rangle$  autoestado del operador  $O$  empleado en la medida. Un medio para caracterizar el estado output es observar cómo  $O$  actúa sobre el conjunto de los operadores generadores de  $S$  del estado input. Para ello se estudian los siguientes casos:

1. Si  $O$  conmuta con todos los generadores  $g_i$  del estabilizador  $S$ .

Existen dos posibilidades, una de ellas es que  $O$  pertenezca al generador. Tal caso, de acuerdo con la ecuación (1.17), supondría que la dimensión del espacio estabilizado  $H_S$  disminuiría a la mitad. Ahora bien, el espacio estabilizado  $H_S$  está constituido únicamente por el estado estabilizador (o estado grafo)  $|S\rangle$  ( $|G\rangle$ ), por lo que esta opción no es viable. La otra alternativa es que  $O$  coincida con algunos de los elementos de  $S$ , y entonces:  $|S\rangle = |S'\rangle$ .

2. Si  $O$  anticonmuta con uno o más elementos del generador.

En este caso, se debe encontrar el conjunto de generadores que caracterizan el estabilizador del estado output a partir de los del estado input. Si  $O$  anticonmutara con más de un elemento del generador de  $S$  (al que denotaremos como  $\langle g_1, g_2, \dots, g_n \rangle$ ), por ejemplo con  $g_1$  y  $g_2$ , entonces en base en la igualdad  $Og_1g_2 = -g_1Og_2 = g_1g_2O$  (equivalentemente,  $[O, g_1g_2] = 0$ ) se podría reemplazar  $g_2$  por  $g_1g_2$ . De este modo  $O$  anticonmutaría con un único elemento del generador. Por tanto, se podrá suponer, sin pérdida de generalidad, que  $O$  anticonmuta con un único elemento del generador, por ejemplo con  $g_1$ .

$O$  es un operador hermítico que satisface  $O^2 = I$ , luego sus autovalores son  $\pm 1$ . Los proyectores asociados a este operador son  $\left(\frac{I \pm O}{2}\right)$ , y las probabilidades asociadas a sus respectivos resultados vendrán dadas por las expresiones

$$p(+1) = \text{tr}(\langle \psi | \left(\frac{I + O}{2}\right) | \psi \rangle), \quad (1.25a)$$

$$p(-1) = \text{tr}(\langle \psi | \left(\frac{I - O}{2}\right) | \psi \rangle). \quad (1.25b)$$

Empleando que  $g_1|\psi\rangle = |\psi\rangle$  y que  $Og_1 = -g_1O$ , se tiene que

$$\begin{aligned} p(+1) &= \text{tr}(\langle \psi | \left(\frac{I + O}{2}\right) | \psi \rangle) = \text{tr}(\langle \psi | \left(\frac{I + O}{2}\right) g_1 | \psi \rangle) \\ &= \text{tr}(\langle \psi | g_1 \left(\frac{I - O}{2}\right) | \psi \rangle) = \text{tr}(\langle \psi | \left(\frac{I - O}{2}\right) | \psi \rangle), \end{aligned} \quad (1.26)$$

es decir,  $p(+1) = p(-1)$ , y dado que la suma de las probabilidades debe ser igual a 1, cada una de ellas deberá ser igual a 1/2. Luego tras actuar  $O$  sobre  $|\psi\rangle$  habrá un 50% de probabilidades de que el estado resultante sea propio del operador  $O$  con autovalor +1, y en tal caso el conjunto generador del estado vendrá dado por  $\langle O, g_2, g_3, \dots, g_n \rangle$ ; y otro 50% de probabilidades de que el estado resultante sea propio del operador  $O$  con autovalor -1, por lo que el conjunto generador deberá ser en este caso  $\langle -O, g_2, g_3, \dots, g_n \rangle$ .  $O$  debe tener signo negativo para que estabilice al estado  $|S'\rangle$ .

Los realización de sucesivas medidas de Pauli de un mismo operador se puede emplear para hacer un estudio estadístico de sus resultados. Las medidas destinadas a este objetivo son las

*medidas de correlación.*

Las medidas de correlación satisfacen las siguientes propiedades:

1. Las correlaciones sólo tienen sentido entre operadores hermíticos que conmutan entre sí pues sus resultados se pueden obtener en un mismo experimento.

2. El cálculo de la correlación entre  $A$  y  $B$ , se realiza a través del producto  $AB$ ,  $\langle AB \rangle$ . El procedimiento a seguir consiste en primer lugar en medir a la vez  $A$  y  $B$ , a continuación se multiplican los resultados de dichas medidas y se promedia sobre un número determinado de intentos.

3.  $\langle AB \rangle \neq \langle A \rangle \langle B \rangle$ , la igualdad tiene lugar únicamente cuando las medidas de  $A$  y  $B$  son independientes, es decir, cuando no están correlacionadas.

Los operadores estabilizadores, son operadores de correlación (ver sección 1.4.3). Si la medida de un operador de correlación sigue el procedimiento que aparece en el punto 2, entonces será una medida de correlación. Las medidas de correlación son útiles en cualquier aplicación donde se trabaje con operadores de correlación, como por ejemplo en las desigualdades de Bell (capítulo 7), pues almacenan los resultados siguiendo un procedimiento estadístico.

### 1.5.2. Grupo de Clifford

El resultado de una transformación unitaria  $U$  sobre un estado estabilizador  $|\psi\rangle$ ,  $U|\psi\rangle$ , no es generalmente otro estado estabilizador. A nivel práctico, sólo nos interesa el conjunto de operaciones unitarias que nos conduzca desde un estado estabilizador a otro. Si los estabilizadores de los estados están constituidos por operadores del grupo de Pauli  $P_n$ , esta condición nos restringe a únicamente a aquellos operadores unitarios  $U$  que transforman el grupo de Pauli en sí mismo bajo conjugación. Es decir, aquellas que satisfacen

$$S' = USU^\dagger, S, S' \in P_n, \quad (1.27)$$

o equivalentemente

$$P_n = UP_nU^\dagger. \quad (1.28)$$

El grupo matemático de operaciones unitarias que encaja con estas características es el *grupo de Clifford*. Los elementos del grupo de Clifford son los *operadores de Clifford*. La acción de sus operaciones se pueden describir en el marco del formalismo estabilizador. Esta propiedad es esencial en el estudio y clasificación de los estados grafo y en la computación cuántica basada en medidas.

Primero estudiaremos el grupo local de Clifford, y después, extenderemos esta definición para obtener la del grupo de Clifford.



### 1.5.3. Grupo local de Clifford

El *grupo local de Clifford* [2] que actúa sobre un conjunto de  $n$  qubits (o simplemente grupo local de Clifford), denotado como  $C_1^n$ , comprende todas aquellas operaciones unitarias que transforman el grupo de Pauli  $P_n$  en sí mismo bajo conjugación

$$C_1^n := \{U \in U(2)^n \text{ tal que } UP_nU^\dagger = P_n\}, \quad (1.29)$$

es decir,  $C_1^n$  *normaliza* el grupo de Pauli, o bien, el grupo de Pauli es *normalizado* por  $C_1^n$ . Los operadores del grupo local de Clifford son el resultado del producto tensorial de  $n$  operadores pertenecientes al grupo de Clifford de un solo qubit [2], denotado como  $C_1$ , que se define como

$$C_1 := \{U \in U(2) \text{ tal que } UP_1U^\dagger = P_1\}. \quad (1.30)$$

Salvo factor de fase, cualquier operación  $U \in C_1$  puede expresarse como el producto de los operadores pertenecientes al conjunto  $\{H, S\}$  [3, 66], donde  $H$  es la matriz de Hadamard y  $S$  la matriz de fase

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \quad (1.31)$$

A modo de ejemplo, mostraremos la acción de los operadores  $H$  y  $S$  sobre los elementos de  $P_1$  y la matriz identidad:

$$HIH^\dagger = I, \quad HXH^\dagger = Z, \quad HYH^\dagger = -Y, \quad HZH^\dagger = X, \quad (1.32a)$$

$$SIS^\dagger = I, \quad SXS^\dagger = Y, \quad SYS^\dagger = -X, \quad SZS^\dagger = Z. \quad (1.32b)$$

La acción de transformar el grupo de Pauli en sí mismo bajo conjugación llevada a cabo por los operadores de  $C_1$  consiste en permutar las matrices de Pauli entre sí, lo que puede producir posibles cambios de signos únicamente en los operadores del grupo de Pauli de orden uno, pues las matrices  $\pm I$  e  $\pm iI$  permanecen intactas. Por otra parte, dado que la conjugación es lineal, basta conocer la acción de  $U \in C_1$  sobre dos matrices de Pauli cualesquiera para determinar el resultado sobre la que resta.

Salvando los factores de fase, el grupo de Clifford  $C_1$  contiene un total de 24 elementos [1, 2], que como alternativa a  $H$  y  $S$ , se pueden descomponer en términos de los operadores de Pauli y rotaciones de ángulo  $\frac{\Pi}{4}$ .

$$\sqrt{\pm\sigma_j} = e^{\pm i\frac{\Pi}{4}\sigma_j}, \quad j = 1, \dots, 3. \quad (1.33)$$

En la tabla 1.1 hemos seleccionado algunas de las 24 operaciones locales de Clifford. En la primera fila aparecen las matrices de Pauli, y en las filas siguientes se muestra los cambios que sobre ellas han originado las operaciones de Clifford de las filas correspondientes y que vienen especificadas en la segunda columna.

Tabla 1.1: Tabla donde se muestra la acción de cinco operadores, elegidos al azar de entre los 24 que salvo factor de fase generan el grupo local de Clifford [1, 2], sobre las matrices de Pauli.

$\sigma_1 \ \sigma_2 \ \sigma_3$	Operación local de Clifford
$\sigma_1 \ \sigma_2 \ \sigma_3$	$\sigma_0$
$-\sigma_1 \ \sigma_2 \ -\sigma_3$	$\sigma_2$
$\sigma_1 \ \sigma_3 \ -\sigma_2$	$\sqrt{-i\sigma_1}$
$\sigma_3 \ -\sigma_2 \ \sigma_1$	$\sigma_3\sqrt{i\sigma_2}$
$-\sigma_3 \ \sigma_1 \ -\sigma_2$	$\sqrt{i\sigma_3}\sqrt{-i\sigma_2}$

Con objeto de entender cómo actúan los operadores locales de Clifford sobre las distintas matrices de Pauli para un único qubit, nos detendremos en mostrar explícitamente algunos de los cálculos que se indican en la tabla 1.1. La operación indicada en la primera fila es trivial, y la comprobación de la segunda es directa pues sólo intervienen en ella las matrices de Pauli

$$\sigma_2\sigma_1\sigma_2^\dagger = -\sigma_1, \quad \sigma_2\sigma_2\sigma_2^\dagger = \sigma_2, \quad \sigma_2\sigma_3\sigma_2^\dagger = -\sigma_3. \quad (1.34)$$

Para obtener los tres últimos resultados indicados en la tabla es más cómodo trabajar con esta otra expresión de los operadores

$$e^{-i\theta\sigma_i} = [1 - \frac{1}{2!}\theta^2 + \dots]I - i[\theta - \frac{1}{3!}\theta^3 + \dots]\sigma_i = \cos(\theta)I - i\sin(\theta)\sigma_i, \quad i=1, \dots, 3. \quad (1.35)$$

#### 1.5.4. Definición de grupo de Clifford

El grupo de Clifford que actúa sobre un conjunto de  $n$  qubits (o simplemente grupo de Clifford) es generado [3, 66] por las operaciones  $H$  y  $S$  junto con una operación unitaria de dos qubits, como la  $C_Z$  o la controlled-NOT (puerta  $C_{NOT}$ ) la cual se define como

$$C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (1.36)$$

Basándonos en esta propiedad se tiene que, salvo factor de fase, cualquier operador del grupo de Clifford puede descomponerse en un producto del orden de  $n^2$  operadores o puertas [3, 62] que se encuentran en el conjunto  $\{H, S, C_Z\}$ .

Por definición, el grupo de Clifford normaliza al grupo de Pauli  $P_n$  (ver ecuaciones (1.32a) y (1.32b)).

Al actuar los operadores del grupo de Clifford,  $U$ , sobre el conjunto de operadores generadores del estabilizador  $S$  asociado a un estado grafo  $|G\rangle$ , el resultado es otro conjunto de operadores generadores  $UgU^\dagger$  que caracterizan al nuevo estado estabilizador asociado al estado  $U|G\rangle$  (ver

capítulo 5, sección 5.2)

$$g|G\rangle = |G\rangle, \quad (1.37a)$$

$$U(g|G\rangle) = U|G\rangle, \quad (1.37b)$$

$$U(gUU^\dagger|G\rangle) = U|G\rangle, \quad (1.37c)$$

$$(UgU^\dagger)U|G\rangle = U|G\rangle, \quad (1.37d)$$

$$g'|G'\rangle = |G'\rangle. \quad (1.37e)$$

## 1.6. Preparación de estados grafo

En esta sección citaremos algunos de los logros experimentales en la obtención de estados grafo o encaminados a este objetivo. Muchos de ellos son planteados teóricamente para una futura implementación, pero también se han conseguido resultados experimentales concretos. Distinguiremos entre dos áreas, la óptica cuántica y confinamiento de partículas.

### Óptica cuántica

En óptica cuántica se ha dedicado mucho esfuerzo en la obtención experimental de recursos cuánticos entrelazados, útiles en tareas de información y computación cuánticas. En las Refs. [67] y [68] por primera vez se implementó experimentalmente una  $C_{NOT}$  entre dos fotones, y se mostró cómo se podían crear eficientemente estados cluster de fotones entrelazados en polarización, respectivamente. Se han creado técnicas basadas en el hiperentrelazamiento [69, 70] que fueron evolucionando hasta llegarse a implantar experimentalmente [48, 53, 71, 72]. Estos resultados dieron paso a la creación de estados hiperentrelazados de 4, 5 y 6 fotones [24, 73, 74, 75, 76, 77, 78]. Recientemente se han preparado estados de  $n$  qubits y  $m$  partículas (para  $n \geq 6$  y  $n > m$ ), por ejemplo estados de 6 qubits y 2 partículas [51, 52], de 6 qubits y 4 partículas [28], de 8 qubits 4 partículas [29], y de 10 qubits y 5 partículas [29]. Avances recientes apuntan hacia la creación de estado grafos empleando qudits [79] y la construcción de estados clusters más resistentes al ruido [80].

### Partículas atrapadas

Los primeros estudios acerca de partículas cuánticas atrapadas [81, 82] han dado lugar a interesantes aplicaciones teóricas y experimentales donde el propósito es crear, manipular y caracterizar estados entrelazados. La utilización de las diferentes técnicas de confinamiento tiene la ventaja de ofrecer una mejor manipulación de las partículas, el tiempo de coherencia de los sistemas es relativamente grande, y los sistemas preparados son de fácil lectura. La mayoría de los estados entrelazados de muchas partículas se basan en las  $C_Z$  de Cirac-Zoller [83], y en el método de Mølmer y Sørensen [84]. Tienen especial interés las propuestas teóricas de entrelazamiento de dos qubits con iones atrapados [85, 86], simulación de una puerta cuántica con iones atrapados [86], simulación de la interacción de Ising entre los espines de un sistema de iones atrapados [87] para generar un cluster, entrelazamiento de iones sin aplicar puertas [88]. Experimentalmente se ha logrado implementar una  $C_{NOT}$  basada en una cadena de iones

atrapados [89], entrelazar sistemas de cuatro átomos [90, 91], y se ha propuesto un método eficiente para entrelazar átomos en un gas de Bose-Einstein condensado [92]. También se han hecho propuestas teóricas de entrelazamiento de nanodieléctricos en una cavidad óptica [93], y de entrelazamiento de un par de electrones [94]; que supondría la base para el diseño de estructuras de mayor dimensión. En la Ref. [95] se propone la preparación experimental de estados clusters de 6 qubits con sistemas de iones atrapados, este resultado se basa en [96] que es una propuesta para la creación del cluster de 4 qubits con iones atrapados. También se han obtenido estados GHZ usando iones [90, 97].

$$E_S = 1, RI_4 = (0, 0, 0, 35), RI_3 = (0, 0, 56), RI_2 = (0, 28), 2-col : \text{yes.} |GHZ\rangle = \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle). \quad (1.38)$$

## Capítulo 2

# Corrección cuántica de errores

### 2.1. Introducción

La aparición del formalismo estabilizador está ligada a la corrección cuántica de los errores que afectan a los qubits que intervienen en tareas de almacenamiento, procesado y comunicación de la información cuántica, donde el correcto funcionamiento está condicionado por la presencia de ruido. La teoría básica de códigos de corrección de errores describe los métodos de protección de un sistema cuántico contra el ruido, así como sus limitaciones. A través de los procesos de decodificación se devuelve el sistema codificado a su forma original, aunque el éxito no está garantizado.

Con objeto de proporcionar una visión más amplia de las aplicaciones de los estados grafo, y por extensión de los estados estabilizadores, desarrollaremos una breve introducción a la teoría cuántica de corrección de errores. Comenzaremos con la corrección de errores clásicos en la sección 2.2, en la que se mostrará como ejemplo el método clásico para la corrección del error bit-flip. En la sección 2.3 se aportan los motivos por los que los sistemas cuánticos no pueden adoptar el modelo clásico de corrección de errores, además se introducirán las técnicas de corrección cuánticas para el error bit-flip, el phase-flip, y el código de nueve qubits de Shor. En estas secciones se emplean operadores estabilizadores en las etapas de detección y recuperación del estado codificado. La sección 2.4 trata del procedimiento de discretización de errores. Por último, en la sección 2.5 destacaremos el papel de los códigos grafo (que son códigos estabilizadores [4, 5]) en la corrección cuántica de errores y aportaremos ejemplos sencillos.

### 2.2. Corrección clásica de errores

El funcionamiento óptimo de los dispositivos electrónicos depende de cuán protegida esté la información que se procesa de las posibles modificaciones no controladas que pudieran sufrir. Las diversas causas de la corrupción de la información se engloban bajo un único término, el ruido. Los métodos de protección contra el ruido consisten básicamente en añadir información redundante al mensaje de forma que si se corrompe, la redundancia aplicada sea suficiente como para absorber la mayor parte del daño, y mediante algún proceso de recodificación se pueda

recuperar el mensaje original.

Un ejemplo que exhibe con claridad la aplicación de la redundancia de la información como medida de protección es el código de corrección del error *bit-flip*.

### 2.2.1. Código de repetición para corregir el error bit-flip

Supongamos que se envía un bit de información desde un lugar a otro a través de un canal de comunicación clásico ruidoso. El efecto del ruido del canal sobre el bit consistirá en conmutar el bit transmitido (de 0 a 1 ó de 1 a 0), con una cierta probabilidad  $p > 0$ , o dejar el bit intacto (sin error) con probabilidad  $1 - p$ . Un canal de este tipo se denomina *canal binario simétrico* y el error que produce es el *bit-flip*.

Un procedimiento simple para proteger al bit de los efectos del ruido durante su paso por el canal simétrico binario, consiste en aportar información redundante sustituyéndolo por tres copias idénticas del mismo

$$0 \mapsto 000, 1 \mapsto 111. \quad (2.1)$$

Se suele emplear la terminología 0 *lógico* y 1 *lógico* para aludir a las cadenas de bits 000 y 111 respectivamente, ya que juegan el papel de los bits 0 y 1.

Si un emisor envía a través del canal alguno de los bits lógicos, el receptor recibirá al otro lado del mismo un output formado por tres bits, donde cabe la posibilidad de que al menos uno de ellos haya sido afectado por el error. El receptor deberá discernir cuál de ellos se ha permutado. Para ello, empleará el método del *voto mayoritario* que consiste en tomar como output el que corresponde al valor binario que aparece más veces. Por ejemplo, si el emisor envía el bit lógico 000 y al receptor le llega el bit lógico corrompido 100, éste interpretará que el primer bit ha sido afectado por el error bit-flip. El voto mayoritario falla si dos o más bits del bit lógico son conmutados por el canal, y acierta en caso contrario. La probabilidad de que resulten conmutados dos o más bits por el canal viene dada por  $p_e = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$ <sup>1</sup>. El código redundante hará que la transmisión de información a través del canal sea más fiable, en comparación con el envío de un único bit, siempre y cuando se cumpla la condición:  $p_e < p$ , con  $p < \frac{1}{2}$ .

El tipo de código que acabamos de describir se denomina *código de repetición*, ya que se codifica el mensaje que deseamos enviar repitiéndolo cierto número de veces. Esta es la idea básica en la que reposan las técnicas de corrección clásicas más sofisticadas. La redundancia que se aplica sobre los bits, está en proporción con la severidad del ruido del canal.

---

<sup>1</sup>Si los errores bit-flip que sucedan en distintos bits son independientes, el primer sumando de la expresión engloba las tres posibles formas de que se produzcan errores en dos de los tres bits, y ninguno en el que queda; y el segundo sumando se refiere al caso en que los tres bits se vean afectados por el error.

## 2.3. Corrección cuántica de errores

Cuando los recursos utilizados son cuánticos, el procedimiento de corrección de errores consiste en codificar la información que se desea proteger en estados cuánticos robustos contra el ruido y fácilmente decodificables. Los códigos cuánticos de corrección de errores realizan esta tarea empleando básicamente la misma estrategia de redundancia que en el caso clásico. Sin embargo, las diferencias entre la Información Clásica y la Información Cuántica revelan ciertos factores de carácter fundamental a tener en cuenta a fin de hacer que tales códigos sean realizables, y se trata de los tres siguientes:

1. El teorema de no clonación<sup>2</sup>. Si se adoptara el método del código de repetición y se aplicara sobre un estado cuántico desconocido, sería necesario realizar múltiples copias del mismo; hecho inviable por entrar en contradicción con el teorema de no clonación.

2. Los errores son continuos. El método clásico está diseñado para corregir errores discretos, como el bit-flip, pero los errores cuánticos podrían consistir en cambios pequeños, del orden de un cierto  $\epsilon$ , que afectarían imperceptiblemente a las amplitudes del estado de un único qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Estos errores podrían irse acumulando en el tiempo; además, dependiendo de su naturaleza podría no existir un modelo clásico análogo (sección 2.3.2) que sirviera de guía para elaborar una solución cuántica. Determinar exactamente qué error es el que ha tenido lugar a fin de corregirlo parece requerir, por tanto, infinita precisión, y por ello infinitos recursos.

3. La medida destruye la información cuántica<sup>3</sup>. En corrección clásica de errores se observa

---

<sup>2</sup>Como resultado del teorema de no clonación formulado por Wootters y Zurek en 1982 [98], no se puede crear el duplicado de un bit cuántico en un estado desconocido sin perturbar por ello de manera descontrolada el estado original. Su demostración se puede hacer considerando el espacio de Hilbert  $H$  del conjunto formado por dos estados originales  $|\psi_1\rangle$  y  $|\psi_2\rangle$ , el estado ancila  $|\psi_0\rangle$  (i.e., aquel que hace la veces de “papel en blanco” sobre el que se “imprimirá” la nueva copia) y el entorno  $|E_0\rangle$  (i.e., es el conjunto formado por máquina encargada de hacer la copia y el medio que rodea); y un superoperador unitario  $F$ . Con estos elementos se intenta hacer dos copias, una de cada estado:

$$H := H_{orig} \otimes H_{copy} \otimes H_{env}. \quad (2.2)$$

$$F|\psi_1\rangle|\psi_0\rangle|E_0\rangle = F|\psi_1\rangle|\psi_1\rangle|E_1\rangle, \quad (2.3a)$$

$$F|\psi_2\rangle|\psi_0\rangle|E_0\rangle = F|\psi_2\rangle|\psi_2\rangle|E_2\rangle. \quad (2.3b)$$

Si multiplicamos las expresiones anteriores, resulta

$$\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2 \langle E_1|E_2\rangle. \quad (2.4)$$

Al ser todas las amplitudes de probabilidad de módulo menor o igual que la unidad, la ecuación (2.4) se satisfará sólo si  $\langle\psi_1|\psi_2\rangle = 0$ , o bien,  $\langle\psi_1|\psi_2\rangle = 1$ . Luego, en general, la máquina no puede copiar dos estados distintos, arbitrarios y no ortogonales.

<sup>3</sup>Aparte de las medidas estándar o fuertes (que son las que destruyen la información cuántica de un sistema y las que hasta ahora se han venido realizando), la MC ofrece una gran variedad de medidas con la única restricción de que exista un equilibrio entre la información ganada y la perturbación que se realiza sobre el estado. Las medidas débiles entran dentro de este grupo y se caracterizan por perturbar muy poco al sistema. La desventaja que ofrece este tipo de medidas es que a cambio sólo se obtiene una pequeña cantidad información, lo cual no ha impedido que se obtengan resultados exitosos en ciertas aplicaciones [99].

el output de un canal comprobando los bits uno por uno, y entonces se decide qué procedimiento de decodificación hay que aplicar para recuperar el estado original. Generalmente, la observación afecta a los sistemas cuánticos transformándolos en otros distintos, y como consecuencia, la información codificada al principio se modifica de forma irreversible. Esto hace que la recuperación de los estados pueda ser imposible.

Estos factores impiden que se puedan aplicar directamente las técnicas clásicas de corrección de errores en los sistemas cuánticos. En algunos casos, cuando los errores cuánticos tienen análogos clásicos, las técnicas clásicas de corrección se pueden adaptar adecuadamente para corregirlos. Los procesos cuánticos de corrección de errores están caracterizados por las etapas de codificación, detección e identificación de errores, y recuperación; y protegen la información cuántica del ruido, bajo ciertas limitaciones.

En el siguiente apartado se expondrá brevemente la adaptación del código clásico de corrección del error bit-flip a un escenario cuántico.

### 2.3.1. El código cuántico de tres qubits para el error bit-flip

Los sistemas cuánticos interactúan con el medio que los rodea que interfieren en sus propiedades, por este motivo los entornos de los sistemas son considerados ruidosos. Un canal cuántico genérico se puede representar en términos de una interacción unitaria entre el sistema cuántico y un entorno ruidoso. De este modo, cuando se dice que un estado se envía a través de un canal ruidoso, quiere decir que el entorno al que se ve expuesto produce sobre él, a través de dicha interacción, un determinado tipo de error.

El canal *bit-flip* es el equivalente cuántico del canal simétrico binario. Si se envía un estado cuántico inicial  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  a través de un canal bit-flip, entonces con una probabilidad  $p$  se intercambiarán los estados  $|0\rangle$  y  $|1\rangle$ . Este canal se representa por el operador unitario de Pauli  $\sigma_x$ , que denotaremos por  $X$ , también conocido como operador bit-flip. La probabilidad de que el estado no resulte afectado tras su paso por el canal es de  $1 - p$ .

La codificación que puede utilizarse para proteger a los qubits del efecto del ruido en este canal, consiste en sustituir los vectores  $|0\rangle$  y  $|1\rangle$ , por sus respectivos representantes lógicos  $|0_L\rangle$  y  $|1_L\rangle$

$$|0\rangle \longrightarrow |0_L\rangle = |000\rangle, \quad (2.5a)$$

$$|1\rangle \longrightarrow |1_L\rangle = |111\rangle. \quad (2.5b)$$

Entonces el estado codificado es

$$|\psi_{cod}\rangle = \alpha|000\rangle + \beta|111\rangle. \quad (2.6)$$

Esta codificación no supone copiar el estado  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  por triplicado, es decir,

$$|\psi_{cod}\rangle = \alpha|000\rangle + \beta|111\rangle \neq (\alpha|0\rangle + \beta|1\rangle)^{\otimes 3}. \quad (2.7)$$



Experimentalmente, el circuito para proteger al estado de un qubit del error bit-flip consta de dos  $C_{NOT}$ , que entrelazan el estado  $|\psi\rangle$  que hace de control, y dos estados  $|0\rangle$  que ejercen de ancilas. Los estados input y output son:  $|\psi_{in}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle = \alpha|000\rangle + \beta|100\rangle$  y  $|\psi_{cod}\rangle = U_{C_{NOT}}^{(13)} U_{C_{NOT}}^{(12)} (\alpha|000\rangle + \beta|100\rangle) = \alpha|000\rangle + \beta|111\rangle$ , respectivamente. El esquema del circuito viene representado en la Fig. 2.1.

Una vez codificado el estado, se hace pasar a través del canal. Supongamos que cada uno de los tres qubits pasa por una copia independiente del canal bit-flip, y que las condiciones de ruido son tales que ocurre algún error sobre a lo sumo un qubit del estado codificado. Los posibles errores, denotados como  $\varepsilon_i$ , que podrían afectar al estado  $|\psi_{cod}\rangle$  (lo que se expresa como  $\varepsilon|\psi_{cod}\rangle$ ) son

$$\varepsilon_0 = I \otimes I \otimes I \rightarrow \text{no hay ningún error,} \quad (2.8a)$$

$$\varepsilon_1 = X \otimes I \otimes I \rightarrow \text{bit-flip en el qubit 1,} \quad (2.8b)$$

$$\varepsilon_2 = I \otimes X \otimes I \rightarrow \text{bit-flip en el qubit 2,} \quad (2.8c)$$

$$\varepsilon_3 = I \otimes I \otimes X \rightarrow \text{bit-flip en el qubit 3.} \quad (2.8d)$$

Llegados a este punto, es preciso detectar qué tipo de error se ha producido y cómo repararlo, es decir, qué qubit ha salido afectado y cómo se puede “recomponer” con vistas a recuperar el estado inicial. Esta parte del proceso se desglosa en dos etapas:

1. *Detección del error o diagnóstico del síndrome.* Las *medidas de síndrome* informan acerca de qué error se ha producido, sin inferir nada de los valores de  $\alpha$  y  $\beta$ . Luego no causan ningún cambio en el estado protegido por el código. Los resultados de las medidas de síndrome se conocen como *síndromes de error*. Para el canal bit-flip hay cuatro medidas de síndrome, dadas operadores proyectores:

$$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \rightarrow \text{si } \varepsilon_0, \quad (2.9a)$$

$$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \rightarrow \text{si } \varepsilon_1, \quad (2.9b)$$

$$P_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \rightarrow \text{si } \varepsilon_2, \quad (2.9c)$$

$$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \rightarrow \text{si } \varepsilon_3. \quad (2.9d)$$

Por ejemplo, supongamos que ocurre un bit-flip en el qubit 2, entonces el estado afectado por el ruido queda como

$$|\psi'_{cod}\rangle = (I \otimes X \otimes I)(\alpha|000\rangle + \beta|111\rangle) = \alpha|010\rangle + \beta|101\rangle. \quad (2.10)$$

En este caso,  $\langle \psi'_{cod} | P_2 | \psi'_{cod} \rangle = 1$ , mientras que el resultado de las medidas de los otros proyectores es cero.

2. *Recuperación del estado original.* En esta última etapa se utiliza el diagnóstico del síndrome de error para inferir qué procedimiento es el adecuado aplicar con vistas a recuperar el estado inicial. Continuando con el ejemplo anterior, bastará con aplicar el operador  $I \otimes X \otimes I$  sobre el estado dado por la expresión (2.10) para restaurar el estado inicial  $\alpha|000\rangle + \beta|111\rangle$ . El código cuántico de

tres qubits para el error bit-flip muestra las mismas limitaciones que su análogo clásico, es decir, el método de corrección funciona perfectamente cuando haya a lo sumo un error bit-flip en uno de los tres qubits, y esto ocurre con una probabilidad  $(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3$ . La probabilidad de que permanezcan errores sin corregir es su expresión complementaria,  $p_e = 3p^2 - 2p^3$ . Para  $p < \frac{1}{2}$ , la codificación y decodificación descritas implican más fiabilidad que la no intervención, en cuanto a la conservación del estado cuántico se refiere<sup>4</sup>.

Hay otra forma de realizar las medidas de síndrome y que conecta con el formalismo estabilizador. Se trata de realizar dos medidas conjuntas sobre dos qubits. Los operadores que se emplean en este caso son:  $Z \otimes Z \otimes I = Z_1 Z_2$  y  $I \otimes Z \otimes Z = Z_2 Z_3$ , donde  $Z_i$  representa el operador  $\sigma_z$  de Pauli actuando sobre el qubit  $i$ . Los autovalores de estos observables se pueden interpretar como medidas comparativas entre los qubits indicados por los subíndices. Sus resultados se emplean para esclarecer si se produjo o no algún error de tipo bit-flip entre los qubits del código. Los diferentes casos que se presentan son:

Si  $Z_1 Z_2 = +1$  y  $Z_2 Z_3 = +1$ , con alta probabilidad no ha tenido lugar bit-flip en ninguno de los tres qubits.

Si  $Z_1 Z_2 = +1$  y  $Z_2 Z_3 = -1$ , con alta probabilidad hubo un bit-flip en el tercer qubit.

Si  $Z_1 Z_2 = -1$  y  $Z_2 Z_3 = +1$ , con alta probabilidad hubo un bit-flip en el primer qubit.

Si  $Z_1 Z_2 = -1$  y  $Z_2 Z_3 = -1$ , con alta probabilidad hubo un bit-flip en el segundo qubit.

La realización de medidas colectivas no proporciona información sobre las amplitudes del estado codificado, de forma que es posible su recuperación en caso de producirse algún error<sup>5</sup>.

---

<sup>4</sup>El estado cuántico pertenece a un espacio continuo, por lo que pueden producirse otros errores que corrompan al estado una cantidad infinitesimal. Una forma de comprobar que las correcciones han sido suficientemente efectivas como para que la recuperación del estado se pueda considerar satisfactoria, es empleando la *fidelidad cuántica*, dada por la expresión:  $F(|\psi\rangle, \rho) = \sqrt{\langle \psi | \rho | \psi \rangle}$ . La corrección cuántica de errores se lleva a cabo con objeto de incrementar la fidelidad con que se almacena la información cuántica, hasta una cantidad lo más próxima posible a la unidad. Respecto a la corrección bit-flip, si

$$\rho_1 = (1-p)|\psi\rangle\langle\psi| + pX|\psi\rangle\langle\psi|X, \quad (2.11a)$$

$$\rho_2 = [(1-p)^3 + 3p(1-p)^2]|\psi_{cod}\rangle\langle\psi_{cod}| + \dots, \quad (2.11b)$$

son el estado de un qubit afectado por este error, y el mismo estado corregido (y por tanto codificado en tres qubits) y recuperado (los puntos suspensivos indican que las contribuciones de los errores bit-flip sobre más de un qubit las hemos ignorado), respectivamente. Si comparamos las fidelidades de ambos estados cuánticos, tenemos que la mínima fidelidad para el primer caso es  $F_1 = \sqrt{\langle \psi | \rho_1 | \psi \rangle} = \sqrt{1-p}$ ; mientras que para el segundo es al menos  $F_2 = \sqrt{\langle \psi | \rho_2 | \psi \rangle} = \sqrt{1-3p^2+2p^3}$ . Entonces, si  $p < \frac{1}{2} \rightarrow F_2 > F_1$ , es decir, el código de corrección de tres qubits para el error bit-flip es efectivo.

<sup>5</sup>Nótese que si se hubieran realizado medidas de un sólo qubit sobre  $|\psi_{cod}\rangle$ , por ejemplo  $Z_2$  de resultado  $+1$ , el estado colapsaría a  $|\psi_{cod}\rangle = |000\rangle$ , y entonces no se podría recuperar el estado original.

### 2.3.2. Código cuántico de tres qubits para el error phase-flip

No todos los canales que producen errores sobre los qubits tienen una contrapartida en el terreno clásico. Este es el caso del error *phase-flip*. El canal phase-flip o conmutador de fase de un qubit lo mantiene intacto con una probabilidad  $1 - p$ , y actúa sobre él alterando la fase relativa de los estados  $|0\rangle$  y  $|1\rangle$ , con una probabilidad  $p$ . Este efecto es simulado eficientemente por la acción del operador  $Z$  de Pauli sobre el estado de un qubit, y no posee análogo clásico, pues la fase no es una propiedad de los canales clásicos.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{1-p} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.12a)$$

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \xrightarrow{p} Z|\psi\rangle = Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle. \quad (2.12b)$$

La táctica a emplear para detectar y corregir este tipo de error es similar al caso del error bit-flip, pues estos canales son *unitariamente equivalentes*, es decir, bajo la acción de un operador unitario  $U$  (en este caso el operador de Hadamard) la acción de un canal es la misma que la del otro si el operador que simula el efecto del primer canal va precedido de  $U$  y seguido por  $U^\dagger$ , finalmente estos operadores se incorporan trivialmente al protocolo de corrección.

Para hacer efectiva la equivalencia entre los dos canales, los estados de un qubit se expresan en la base de Hadamard<sup>6</sup>. A partir de la formalización de este cambio de base, es posible simular la acción del canal flip-bit sobre los qubits que se exponen a sus efectos, es decir, si la acción del canal bit-flip consistía en conmutar los estados  $|0\rangle$  y  $|1\rangle$  a través del operador  $X$ ,  $X|0\rangle(|1\rangle) = |1\rangle(|0\rangle)$ , el canal phase-flip conmutará los estados  $|+\rangle$  y  $|-\rangle$  a través del operador  $Z$  de Pauli,  $Z|+\rangle(|-\rangle) = |-\rangle(|+\rangle)$ . En esta nueva base, la codificación que protege el estado de los errores phase-flip vendrá dada por los estados lógicos  $|0_L\rangle = |+++ \rangle$  y  $|1_L\rangle = |-- \rangle$ , de modo que el estado de un qubit codificado es:  $|\psi_{cod}\rangle = \alpha|+++ \rangle + \beta|-- \rangle$ . En la Fig. 2.2 se especifica el circuito que codifica el estado  $|\psi\rangle$ . Se observa que en primer lugar se entrelazan los qubits, y luego actúan las matrices  $H$  sobre los estados  $|\psi\rangle$ ,  $|0\rangle$  y  $|1\rangle$ , con objeto de realizar el cambio de base.

La detección de errores se realiza a través de nuevas medidas proyectivas que se obtienen a partir de las dadas por las ecuaciones (2.9a)-(2.9d) conjugándolas con el operador de Hadamard,  $P_j \mapsto P'_j \equiv H^{\otimes 3} P_j H^{\otimes 3}$ . O bien midiendo los observables  $H^{\otimes 3} (Z_1 Z_2) H^{\otimes 3} = X_1 X_2$  y  $H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$ , y realizando un análisis comparativo entre los signos resultantes (como en la sección 2.3.1). El protocolo de corrección de errores se completa aplicando la operación de recuperación adecuada, y posee la misma probabilidad de éxito que en el error bit-flip.

En el siguiente apartado expondremos el código de corrección de errores de 9 qubits de Shor.

### 2.3.3. El código de 9 qubits de Shor

El código de 9 qubits de Shor consiste en una combinación de los códigos de tres qubits para los errores bit-flip y phase-flip. El proceso de codificación se desarrolla siguiendo una jerarquía

<sup>6</sup>Partiendo de los vectores propios del operador Hadamard,  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  y  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ , expresar el estado general de un qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  en esta base es inmediato.

de niveles que se conoce como *concatenación*. Si  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  es el qubit de partida, la concatenación comienza con la codificación de los estados  $|0\rangle$  y  $|1\rangle$  mediante el código phase-flip ( $|0\rangle \mapsto |+++ \rangle$ ,  $|1\rangle \mapsto |-- \rangle$ ), resultando  $|\psi\rangle = \alpha|+++ \rangle + \beta|-- \rangle$ ; en el siguiente paso se codifica cada qubit de acuerdo con el código bit-flip. El estado resultante tras este proceso es  $|\psi\rangle_{cod} = \alpha|0_L\rangle + \beta|1_L\rangle$ , donde

$$|0_L\rangle = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}, \quad (2.13a)$$

$$|1_L\rangle = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}. \quad (2.13b)$$

El código de Shor es capaz de proteger la información cuántica frente a errores de tipo bit-flip, phase-flip, bit-phase-flip, y, como veremos en el siguiente apartado, también frente a errores de tipo arbitrario. La detección y corrección del error bit-flip se puede realizar aplicando el procedimiento de síndrome y recuperación visto en el apartado 2.3.1. Respecto a los errores de tipo phase-flip, los posibles cambios de signo se podrán observar en los términos entre paréntesis que conforman los bloques de las expresiones (2.13a) y (2.13b); por ejemplo, si el bloque  $(|000\rangle + |111\rangle)$  se transforma en  $(|000\rangle - |111\rangle)$ , entonces se ha producido un phase-flip. Las medidas de síndrome se llevan a cabo con operadores lo suficientemente “grandes” como para captar los cambios de signos entre bloques. Por ejemplo, para comparar los signos entre el primer y el segundo bloque se emplean los operadores  $X_1X_2X_3X_4X_5X_6$  y  $X_4X_5X_6X_7X_8X_9$ . La recuperación del estado se logra sin más que aplicar el operador  $Z_1Z_2Z_3$ . Si ha tenido lugar un error combinado entre los dos anteriores, el problema se afronta por partes, primero resolviendo un tipo de error y luego el otro. La Fig. 2.3 muestra el circuito para codificar el estado de un qubit con este código.

## 2.4. Discretización de errores

En la mayoría de los casos no se conoce exactamente qué ruido está afectando a un sistema cuántico. Lo más práctico sería disponer de códigos,  $C$ , y de operaciones de recuperación de errores,  $R$ , que pudieran emplearse para afrontar cualquier tipo de error (ya sea discreto o continuo) que sea susceptible de producirse.

La *discretización* de errores es el método de corrección de errores cuántico que posee estas características, y se basa en la siguiente estrategia:

Supongamos que un ruido de tipo arbitrario afecta a un sólo qubit y que se puede representar mediante un operador unitario  $\varepsilon$ , que conserve la traza:  $\varepsilon = \sum_i E_i$ , donde  $\sum_i |E_i\rangle\langle E_i| = I$ . Entonces, su efecto sobre el estado de un sólo qubit es:  $\varepsilon(|\psi\rangle\langle\psi|) = \sum_i E_i(|\psi\rangle\langle\psi|)E_i^\dagger$ . Para analizarlo, es mucho más sencillo hacer un seguimiento de uno solo de los operadores  $E_i$ . Como operador de un único qubit se podrá descomponer en suma de la identidad y las tres matrices de Pauli

$$E_i = e_{i0}I + e_{i1}X_1 + e_{i2}Y_1 + e_{i3}Z_1. \quad (2.14)$$

Es decir, un error arbitrario se puede descomponer en una suma discreta de errores bit-flip, bit-phase-flip (representado por el operador de Pauli  $Y_1$ ) y phase-flip. Luego el estado norma-

lizado  $E_i|\psi\rangle$  se puede describir como una superposición de cuatro términos:  $|\psi\rangle$ ,  $X_1|\psi\rangle$ ,  $Z_1|\psi\rangle$  y  $Z_1X_1|\psi\rangle$ . Una medida de síndrome de error lo colapsaría a uno de estos cuatro términos y el estado original se podría recuperar mediante la adecuada operación de inversión. Esto mismo es cierto para todos los términos  $E_i$ , produciéndose la corrección de errores arbitrarios.

Este resultado de la discretización de errores permite afirmar que con el código de Shor se puede corregir cualquier error arbitrario en un qubit.

Si los efectos del ruido afectan a más de un qubit, una aproximación que suele emplearse consiste en suponer que los errores sobre cada qubit se pueden tratar de forma independiente, y si los efectos son lo suficientemente pequeños, es posible expandir la acción total del ruido como suma de términos que involucran, ningún error, error en un qubit, error en dos qubits,...; y tras desechar los de orden mayor que uno, obtener la expresión del error final. También existen soluciones para aquellas situaciones en las que la aproximación de errores independientes no es adecuada, para más detalle consultar las Refs. [62, 100].

En el apartado 2.3.1 se mostró que las medidas de síndrome podían llevarse a cabo a través de la realización de medidas colectivas de ciertos operadores del grupo de Pauli. Este método conecta el formalismo estabilizador con la corrección cuántica de errores. En la siguiente sección, mostraremos que el formalismo estabilizador se puede emplear estratégicamente no sólo en la etapa de síndrome-recuperación de cualquier procedimiento cuántico de corrección de errores, sino también en todo el proceso de corrección.

## 2.5. Códigos estabilizadores de corrección cuántica de errores

Los códigos grafo de corrección de errores son aquellos que se obtienen a partir de estados grafo. De acuerdo con los resultados de Schlingemann [4, 5], todo código grafo es también un código estabilizador, pues existe entre ellos una relación de equivalencia a través de operaciones de Clifford. En este trabajo, por comodidad, hemos elegido introducir los códigos estabilizadores.

Un *código de estabilizador*  $[n, m]$ , también denotado como  $C(S)$ , se define como el espacio vectorial  $V_S$  estabilizado por un subgrupo  $S$  del grupo de Pauli  $P_n$ , tal que  $-I^{\otimes n} \notin S$ .  $S$  posee  $k = n - m$  operadores generadores independientes que conmutan entre sí,  $S = \langle g_1, \dots, g_k \rangle$ . La dimensión del espacio estabilizado por  $S$  es  $\dim V_S = 2^m$ , es decir,  $S$  estabiliza un total de  $2^m$  vectores ortonormales, que conforman el código estabilizador (i.e., los estados que utilizaremos como estados lógicos al codificar un estado de partida).

Si los errores  $E$  que se producen en el canal pertenecen al grupo de Pauli  $P_n$ , entonces actúan sobre el estado codificado de forma similar a como lo hacían las medidas del grupo de Pauli sobre un estado estabilizador dado (capítulo 1, sección 1.5.1). Por lo tanto, emplearemos una disertación similar para estimar el efecto que tienen estas medidas sobre el código estabilizador de un estado. Distinguiremos entre las siguientes situaciones:

1.  $E \in P_n$  y anticonmuta con algún operador del estabilizador  $S$ . La acción de  $E$  sobre el estado codificado repercute indirectamente sobre el estabilizador  $S$  de  $C(S)$ , transformándolo en otro conjunto estabilizador  $S'$  correspondiente a un espacio  $C(S')$  ortogonal al primero. Este error es detectable y admite corrección. Como ejemplo ilustrativo, veamos el siguiente caso:

Supongamos que el código estabilizador viene indicado por el par  $[n, m] = [3, 1]$ , consideremos el estabilizador  $S$  dado por  $S = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}$ <sup>7</sup>. Caracterizaremos el estabilizador. La dimensión del subespacio estabilizado por  $S$  es  $\dim V_S = 2^m = 2^1 = 2$ , y  $S$  es generado por  $k = n - m = 2$  operadores generadores. Veamos:

El operador  $Z_1Z_2$  estabiliza el subespacio generado por los vectores  $\{|000\rangle, |001\rangle, |111\rangle, |110\rangle\}$ .

El operador  $Z_2Z_3$  estabiliza el subespacio generado por los vectores  $\{|000\rangle, |100\rangle, |011\rangle, |111\rangle\}$ .

El operador  $Z_1Z_3$  estabiliza el subespacio generado por los vectores  $\{|010\rangle, |101\rangle, |000\rangle, |111\rangle\}$ .

Luego el subespacio estabilizado por  $S = \langle Z_1Z_2, Z_2Z_3 \rangle$  es  $\{|000\rangle, |111\rangle\}$ , el cual constituye el código estabilizador  $C(S)$ . El estado de un qubit  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  es codificado a través  $C(S)$  en el estado  $|\psi_{cod}\rangle = \alpha|000\rangle + \beta|111\rangle$ .

Supongamos que los errores  $E$  son generados por el conjunto de operadores  $\{Z_1, X_2, Z_3\}$ , entonces, el conjunto total de errores contendrá  $2^3 - 1$  elementos (excluyendo la identidad). De entre los cuales, sólo los errores representados por los operadores  $X_2, Z_1X_2, X_2Z_3$  y  $Z_1X_2Z_3$ , basándonos en las propiedades del grupo de Pauli (ver apéndice), anticonmutarán con algún elemento de  $S$ . Los errores  $X_2$  y  $Z_1X_2Z_3$  son del tipo bit-flip, y al actuar sobre  $|\psi_{cod}\rangle$ , lo transforman en  $|\psi'_{cod}\rangle = \alpha|010\rangle + \beta|101\rangle$ . El diagnóstico del síndrome se realiza haciendo actuar sobre el estado  $|\psi'_{cod}\rangle$  el conjunto generador  $\{Z_1Z_2, Z_2Z_3\}$ , y observando si han tenido lugar cambios de signo (los operadores  $g_k$  tiene la misma función que los operadores de síndrome de medida vistos en secciones anteriores). En este caso, el conjunto generador se transforma en  $\{-Z_1Z_2, -Z_2Z_3\}$ , lo que indica que el error se ha producido en el segundo qubit. La forma de recuperar el estado es aplicando  $X_2$  sobre  $|\psi'_{cod}\rangle$ .

Los operadores  $Z_1X_2$  y  $X_2Z_3$ , transforman el estado  $|\psi_{cod}\rangle$ , en  $|\psi'_{cod}\rangle = \alpha|010\rangle - \beta|101\rangle$  que se caracteriza de nuevo por el conjunto generador  $\{-Z_1Z_2, -Z_2Z_3\}$ . Con esta información es posible corregir el error bit-flip, pero no el phase-flip, por lo que sería conveniente expresar el estado output en la base propia del operador  $X$  (sección 2.2) y verificar los cambios del generador del nuevo estabilizador con el fin de completar la corrección.

2. Si  $E \in P_n$  y  $E \in S$ . Entonces, el estado no se modifica. En el ejemplo anterior, los operadores que poseen esta característica son  $Z_1, Z_3$  y  $Z_1Z_3$ . Desde esta perspectiva, los operadores estabilizadores de cualquier estado grafo constituyen en realidad un conjunto de errores contra los que dichos estados están automáticamente protegidos, y por ello no es necesario intervenir si se dan en algún canal ruidoso.

---

<sup>7</sup>La identidad  $I$  estabiliza a cualquier estado, por lo tanto, a veces la omitiremos en los conjuntos estabilizadores de error.

3. Si  $E \in P_n$ ,  $E \notin S$  y conmuta con todos los elementos de  $S$ . Un error de este tipo transforma el estado original, pero los operadores generadores de  $S$  son incapaces de detectarlo. Por ejemplo, los bit-flip múltiples ( $\varepsilon_1 = X_1X_3$ ,  $\varepsilon_2 = X_1X_2$ ,  $\varepsilon_3 = X_2X_3$ ,  $\varepsilon_4 = X_1X_2X_3$ ) conmutan con todos los operadores estabilizadores de  $S$ , no pertenecen a  $S$ , afectan al estado  $|\psi_{cod}\rangle$ , y no son detectados por los operadores generadores de  $S$ .

Como sabemos, un ejemplo de código estabilizador de corrección de errores cuántico es el código de 9 qubits de Shor. Se trata del código  $[n, m] = [9, 1]$ , con 8 operadores generadores  $g_k$  que estabilizan un espacio de dimensión  $\dim V_S = 2^{(9-8)} = 2$ , constituido por los estados lógicos dados por las ecuaciones (2.13a) y (2.13b). Se añaden 8 qubits para proteger la información del primero.

$$g_k(\text{Shor}) \equiv \begin{cases} g_1 & Z & Z & I & I & I & I & I & I & I \\ g_2 & I & Z & Z & I & I & I & I & I & I \\ g_3 & I & I & I & Z & Z & I & I & I & I \\ g_4 & I & I & I & I & Z & Z & I & I & I \\ g_5 & I & I & I & I & I & I & Z & Z & I \\ g_6 & I & I & I & I & I & I & I & Z & Z \\ g_7 & X & X & X & X & X & X & I & I & I \\ g_8 & X & I & I & I & X & X & X & X & X \end{cases} \quad (2.15)$$

Los errores que son susceptibles de corregirse empleando el código estabilizador de corrección de errores de 9 qubits de Shor, son los que se encuentran en el conjunto  $E = \{I, X_1, Y_1, Z_1; \dots; X_9, Y_9, Z_9\}$ , es decir, cualquier error arbitrario de un qubit.

A grandes trazos, el fundamento de cualquier protocolo de corrección cuántica de errores consiste en codificar los estados cuánticos, mediante alguna operación unitaria  $U_{cod}$ , en un código de corrección de errores. Esta codificación no es más que la extensión del espacio de Hilbert, referido en un principio a un conjunto de  $k$  qubits físicos, a otro que describe a un grupo más numeroso de  $n$  qubits (ver ecuaciones (2.5a), (2.5b), (2.13a) y (2.13b)).

Los  $n - k$  qubits añadidos son los denominados qubits ancila. El estado inicial de los qubits ancilas es  $|00\dots 0\rangle$ . Un código con estas características se denota como código  $[n, k]$ . El subespacio generado por los estados codificados conforma el código  $C$ , el cual podría representarse a través del proyector  $P_C$  sobre dicho subespacio. Por ejemplo, si el código  $C$  fuera generado por los estados  $|000\rangle$  y  $|111\rangle$ , el proyector sobre el subespacio subtendido por ellos será:  $P_C = |000\rangle\langle 000| + |111\rangle\langle 111|$ . Tras la codificación, las medidas de síndrome de error tipificarán y localizarán los errores que se hayan podido producir a causa del ruido. Con esta información es posible revertir los errores y obtener al fin el estado de partida.

En general, el ruido se describe mediante el operador cuántico  $\varepsilon$ , y las etapas de corrección y recuperación se efectúan a la vez a través de un operador cuántico  $R$  que conserva la traza de los estados. El requisito exigido formalmente para que la corrección de errores se pueda considerar como exitosa es:

$$(R \circ \varepsilon)\rho \propto \rho. \quad (2.16)$$

Donde  $\propto$  simboliza la posibilidad de que  $\varepsilon$  no conserve la traza del estado original  $\rho$ .

Para finalizar, existen unas condiciones para la corrección cuántica de errores [62] que se emplean como test para determinar si cierto código cuántico de corrección de errores protege contra un tipo particular de ruido. Si el test lo determina, el conjunto de errores  $\{E_i\}$  constituye un conjunto de errores corregibles.

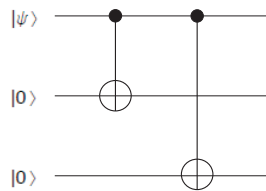


Figura 2.1: Circuito que codifica el estado  $|\psi\rangle$  de un qubit en otro  $|\psi_{cod}\rangle$  de tres qubits para protegerlo contra el error bit-flip.

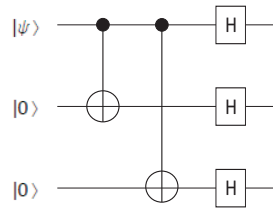


Figura 2.2: Circuito codificador para el código de tres qubits contra el phase-flip.

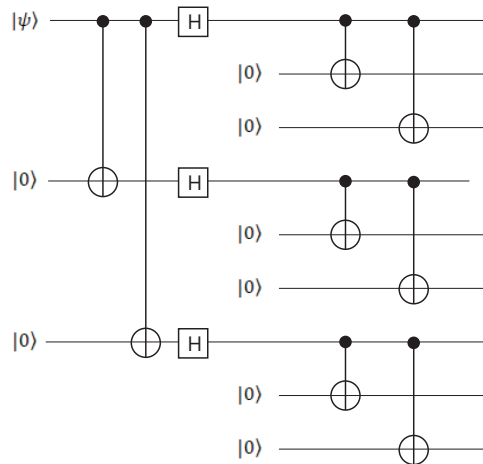


Figura 2.3: Circuito codificador para el código de Shor de nueve qubits. Para destacar la concatenación característica de este código, en la figura aparecen algunas líneas de los estados ancilarios con una sangría.



## Capítulo 3

# Computación cuántica basada en medidas

### 3.1. Introducción

El propósito de este capítulo es mostrar las características esenciales del modelo de computación cuántica basada en medidas (CCBM) [8, 7, 9, 10, 11] también conocido como  $QC_C$ <sup>1</sup>, destacando el papel de los estados grafo [101, 102, 103, 104, 105, 106]. En CCBM, la realización de una tarea de computación se lleva a cabo aplicando una serie de medidas proyectivas sobre estados cluster y otros estados grafo. Este método de computación es diferente del modelo de computación cuántica mediante circuitos de puertas lógicas (*quantum logical network*) o modelo de circuito, al que nos referiremos de forma abreviada como CCMC. Sin embargo, es posible simular CCMC empleando CCBM. De hecho, esta es la forma usual de proceder cuando se introduce la CCBM. El contenido de este capítulo se distribuye como sigue: En la sección 3.2 describiremos las características de estos dos modelos de computación, estableciendo una comparación entre ambos. En la sección 3.3 expondremos la simulación de CCMC a través de CCBM, para ello mostraremos, empleando el formalismo estabilizador, cómo se implementan determinísticamente un conjunto universal de puertas lógicas cuánticas, lo que constituye una prueba de la universalidad del modelo CCBM. En la sección 3.4 veremos cómo se implementan más de una puerta lógica en CCBM. Por último, en la sección 3.5 describiremos brevemente la ordenación temporal de las medidas.

---

<sup>1</sup> $QC_C$  se emplea como abreviación de “one-way quantum computer”, donde el subíndice  $C$  destaca la importancia de los estados cluster en este modelo. Es preciso distinguir entre los conceptos de cluster y estado cluster. El término cluster se emplea como definición de un grupo de qubits equidistantes que pueden disponerse en una red cúbica, una red cuadrada, o en un línea (ver Fig. 3.6). Los estados cluster son estados puros cuánticos de sistemas de dos niveles localizados en un cluster.

### 3.2. Modelos de computación cuántica

En los modelos de computación cuántica se describe cómo realizar operaciones sobre recursos cuánticos<sup>2</sup> de partida, con objeto de implementar algoritmos cuánticos que procesan y extraen la información cuántica contenida para su interpretación final. Por este motivo, tienen una fuerte influencia en el diseño de los experimentos actuales que tratan de realizar ordenadores cuánticos en los laboratorios.

La mayoría de los experimentos y la mayor parte de los algoritmos cuánticos que se conocen, han sido desarrollados siguiendo el CCMC [62, 107, 108]. En este modelo de computación, cualquier circuito clásico puede sustituirse por otro equivalente que contenga únicamente elementos reversibles [62]. En el modelo de circuito, la información cuántica de partida, conocida como *registro cuántico inicial*, se prepara en algún estado input (estado inicial)  $|\psi_{in}\rangle$ , y se procesa hacia algún estado output (estado final)  $|\psi_{out}\rangle$ , aplicando las transformaciones unitarias adecuadas. La Fig. 3.1 muestra la evolución del estado de partida  $|\psi_{in}\rangle$  tras la aplicación ordenada de suce-

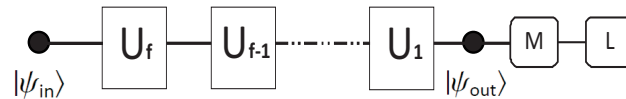


Figura 3.1: Circuito cuántico representativo de la CCMC.  $U_i$  se refiere a las transformaciones unitarias aplicadas en un principio al estado inicial  $|\psi_{in}\rangle$ , y luego a sucesivos estados outputs. M indica la medida sobre el estado final  $|\psi_{out}\rangle$ , y L la lectura de su resultado.

sivas operaciones unitarias  $U_i$ . El procesamiento del registro cuántico inicial finaliza cuando se realizan las medidas oportunas sobre  $|\psi_{out}\rangle$  (representadas por M en la figura) y se procede a su lectura (representada por L en la figura). La interpretación de los resultados aporta la solución del problema que se pretende resolver.

Para el desarrollo óptimo de cualquier computación cuántica se precisa de unos recursos básicos que se pueden clasificar en temporales, espaciales y operacionales. El recurso temporal es la profundidad lógica o mínimo número de pasos en los que las operaciones de computación se pueden realizar paralelamente<sup>3</sup>; es deseable que cualquier procedimiento desarrollado en computación, incluyendo la preparación de un recurso inicial, tenga lugar en el menor tiempo posible pues de esta manera se protege al sistema de los indeseados efectos del ruido a los que se ve expuesto en las situaciones reales. El recurso espacial es el número total de qubits que se va a “consumir” durante el proceso, y el operacional está constituido por el número total de operaciones de la computación. En CCMC estos recursos son:

El recurso temporal. Las operaciones que se implementan en este modelo consisten básicamente en operaciones unitarias realizadas sobre al menos un qubit. Únicamente aquellas operaciones que conmutan entre sí son las que se pueden realizar de forma paralela, contribuyéndose

<sup>2</sup>El concepto de recurso abarca desde el estado más elemental en la información y computación cuántica, un sólo qubit, hasta cualquier sistema cuántico entrelazado de complejidad y composición arbitraria.

<sup>3</sup>Las operaciones que se pueden realizar paralelamente son aquellas que se pueden llevar a cabo de forma simultánea.

a la minimización de la profundidad lógica. El ahorro temporal no sólo constituye una ventaja durante el proceso de cualquier computación, sino también en cualquier otra tarea como por ejemplo en la preparación de un estado entrelazado. En la Fig. 3.2 se muestra un ejemplo sencillo de ahorro temporal en la preparación del estado cluster  $|LC_5\rangle$ . Se entrelazan un total de 5 qubits aplicando puertas controlled-Z ( $C_Z$ ) invirtiendo el menor tiempo posible; las  $C_Z$  que se podrán implementar en el mismo instante o paso de tiempo, son las que involucran pares de qubits distintos.

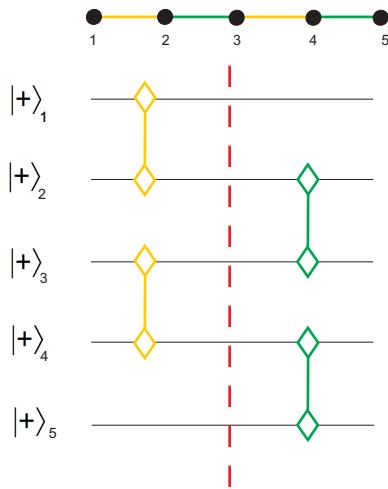


Figura 3.2: Esta figura muestra el procedimiento experimental más corto de entrelazar los qubits del estado  $|LC_5\rangle$ , si la operación de entrelazamiento consiste en la aplicación de puertas  $C_Z$ . Las que se encuentran a un mismo lado de la línea discontinua se implementan simultáneamente y consumen un paso de tiempo. El tiempo total invertido en esta operación es de dos pasos.

El recurso espacial. Por ejemplo, en la construcción de puertas como la  $C_{NOT}$  se emplean dos qubits, mientras que en la implementación de rotaciones sólo se necesita un qubit. Veremos cómo en el modelo de CCBM esto es muy diferente.

El recurso operacional. En la Fig. 3.3 las operaciones unitarias de un solo qubit se representan por  $U$ . Hay un total de dos  $C_{NOT}$  y 6 operaciones  $U$ .

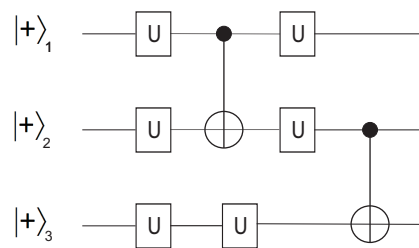


Figura 3.3: Circuito CCMC de tres qubits. Hay un total de 6 operaciones unitarias  $U$  de un sólo qubit, y dos  $C_{NOT}$ .

Resumiendo, el modelo de computación cuántica mediante circuitos de puertas lógicas se basa en una secuencia de puertas lógicas unitarias que procesan qubits [62]. Este modelo de computación es completamente diferente al modelo de computación cuántica basada en medidas

propuesto por Rausendorf y Briegel [8].

Los modelos CCMC y CCBM, aunque son matemáticamente equivalentes, difieren totalmente en carácter físico, pues emplean recursos muy distintos. El modelo CCBM consiste únicamente en la aplicación de sucesivas medidas proyectivas de un solo qubit junto con *retroalimentación*<sup>4</sup> (*feedforward* o *FF*) clásica, necesaria para que la computación sea determinista (ver secciones 3.3.1 y 3.5). El orden y la elección de las medidas determinan el algoritmo de computación. Si se emplea como recurso un estado cluster, el modelo de CCBM es un modelo de computación universal porque puede simular cualquier evolución unitaria (ver apartado 3.3.2).

Los avances experimentales de la última década han ido abriendo paso a la elaboración de ciertos estados grafo [29, 28, 48, 109, 52] sobre los que se han implementado con éxito algoritmos de computación como el de Grover [23, 106] y el de Deusch-Jozsa [104, 105].

La realización de las medidas atiende a una ordenación temporal. En la Fig. 3.4 podemos ver representados por puntos de diferentes colores los qubits que formaban parte de un cluster después de ser medidos. Dentro de cada conjunto de qubits de un mismo color, a los que denotamos genéricamente por  $Q_i$ , las medidas proyectivas se pueden realizar simultáneamente. Las medidas realizadas sobre los qubits de un conjunto condicionan las bases de las medidas para las mediciones sobre los qubits de otro, de manera que los resultados de las medidas de los qubits en  $Q_0$  especifican las bases de medidas de los qubits en  $Q_1$ , y juntos especifican las bases para los qubits en  $Q_2$  que se miden en una tercera ronda, y así sucesivamente. A su vez, este proceso es físicamente irreversible y determinista, pues se destruye el entrelazamiento durante las medidas, y mediante la retroalimentación se seleccionan las bases para futuras proyecciones. El resultado de la computación es la recopilación de los resultados de las medidas de todas las rondas. Organizaremos toda esta información distribuyéndola entre los recursos necesarios para

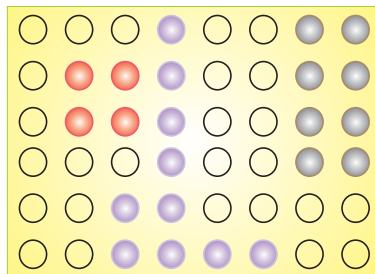


Figura 3.4: Esquema de computación one-way. Los círculos representan qubits. Los diferentes grupos de qubits de un mismo color son los conjuntos  $Q_i$ .

la CCBM:

El recurso temporal. La profundidad lógica depende de la cantidad de medidas especificadas en el patrón de medidas que se pueden realizar simultáneamente. Por ejemplo, las medidas realizadas sobre los qubits de cada  $Q_i$  o los circuitos del grupo de Clifford se pueden realizar en un

<sup>4</sup>Como veremos en la sección 3.5, las operaciones retroalimentación hacen de la computación cuántica un proceso determinista. Se pueden realizar durante el proceso de computación eligiendo la base de medidas dependiendo de los resultados previos, o bien implementando matrices de Pauli de corrección o ajuste sobre el estado output [104].

único paso (ver sección 3.5).

El recurso espacial. Está constituido por estados entrelazados. En comparación con el modelo de CCMC, se requieren más qubits para la misma computación. Por ejemplo, el estado que se necesitaría para realizar el circuito de la Fig. 3.3 sería el representado por la Fig. 3.5.

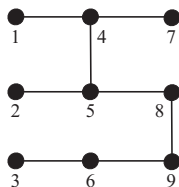


Figura 3.5: Este grafo representa al estado cluster que se usa como recurso en la simulación del circuito de la Fig. 3.3 mediante CCBM. En comparación, este consume tres veces más qubits.

El recurso operacional. Es el número total de medidas de un qubit involucradas en el proceso de computación. De acuerdo con la Fig. 3.5, se necesitarían realizar un total de 6 medidas proyectivas para simular el circuito de la Fig. 3.3 en el que se implementan 8 operaciones.

### 3.3. Simulación de la CCMC empleando CCBM

El modelo de CCMC no es el más apropiado para describir la computación cuántica basada en medidas. Esta afirmación se sostiene con dos argumentos. Por un lado, parte del poder de CCBM deriva del hecho de que las operaciones unitarias se pueden implementar más competentemente que mediante circuitos lógicos de puertas cuánticas. Y por otro, en este modelo se abandona el uso de la mayoría de los términos empleados en CCMC, porque objetos como las puertas cuánticas y conceptos como inputs u outputs, no constituyen elementos con significado propio. No obstante, es el que se suele emplear para explicar el funcionamiento de cualquier computador cuántico, independientemente el modelo de computación subyacente.

A continuación, describiremos brevemente el procedimiento que se usa para simular un circuito cuántico en CCBM, las demostraciones las podremos encontrar en [7].

Comenzaremos distinguiendo entre *qubits cluster* o *qubits físicos*, que son los que constituyen el cluster y se emplean durante la computación; y los *qubits lógicos*, que representan la información que se almacena en los inputs y se procesan durante la computación, pero no existen físicamente. Con esta distinción se pretende hacer notar que se trata de un modelo abstracto de computación. Mostraremos esto estableciendo un paralelismo entre los modelos de computación representados por las figuras 3.3 y 3.5: (1) Cada qubit del circuito cuántico se reemplaza por una línea horizontal de qubits en el cluster. Los diferentes qubits horizontales representan el qubit original en distintos instantes. Las puertas lógicas de un qubit se reemplazan por qubits horizontales adyacentes en el cluster. (2) Las puertas lógicas de dos qubits se simulan usando puentes verticales para conectar los qubits apropiados. Por ejemplo, en la Fig. 3.5, los qubits 1, 4 y 7, representan la evolución unitaria del qubit 1 de la Fig. 3.3 bajo la acción de una operación unitaria de un qubit, de una  $C_{NOT}$  y de otra operación unitaria de un qubit. (3) Sólo para hacer una descripción en términos del modelo CCMC de la CCBM, se seleccionan qubits que simulan

el registro cuántico de los estados inputs,  $I$ , y outputs,  $O$ . El resto de qubits,  $M$ , son los qubits del cuerpo. Estos conjuntos de qubits deben satisfacer que

$$I \cup M \cup O = C, \quad (3.1a)$$

$$I \cap M = M \cap O = I \cap O = \emptyset. \quad (3.1b)$$

Siendo  $C$  el cluster. De este modo, en la Fig. 3.5 los qubits 1, 2 y 3 actuarán como qubits inputs, los qubits 4, 5 y 6 formaran parte del cuerpo  $M$ , y los qubits 7, 8 y 9 serán los qubits outputs. Si se implementan varios algoritmos,  $W_i$ , entonces se seleccionan distintos grupos de qubits dentro del cluster, tales que  $C = C(W_1) \cup C(W_2) \cdots \cup C(W_i)$ . Esta forma de operar es conocida como *método de concatenación de bloques básicos de medidas* [10].

### 3.3.1. Formalismo estabilizador y computación cuántica basada en medidas

El formalismo estabilizador [1, 2] es una herramienta muy útil para caracterizar los estados grafos, así como en el desarrollo de técnicas eficientes de corrección cuántica de errores. Mediante el formalismo estabilizador es posible describir tanto espacios como subespacios de múltiples qubits de una forma compacta, empleándose los operadores estabilizadores de forma análoga a como en la MC se utilizan para descripción de los estados atómicos los números cuánticos.

Empleando el formalismo estabilizador y estados clusters mostraremos cómo se implementan determinísticamente un conjunto universal de puertas en CCBM. Lo cual constituye una prueba de la universalidad de este modelo de computación. La ejecución del patrón de medidas se reduce a manipulaciones del estabilizador  $S$  que caracteriza al estado cuántico  $|\psi\rangle$ . En el siguiente apartado describiremos brevemente en qué consisten tales manipulaciones.

#### Interpretación del patrón de medidas en términos del modelo de circuito empleando computación cuántica basada en medidas

1. A partir de la ecuación de autovalores que satisface el estado cluster inicial  $|\psi\rangle$  se deriva un conjunto de ecuaciones de autovalores que sea compatible con las operaciones  $P_{s_i}$  del patrón de medidas que se ejecutará sobre los qubits  $M$ .

$$P_{s_i} = \frac{1 + (-1)^{s_i} \vec{r}_i \cdot \vec{\sigma}_i}{2}, \quad (3.2)$$

donde  $\vec{r}_i$  es la dirección en la que se proyecta el vector espín  $\vec{\sigma}_i$  del qubit  $i$ , y  $s_i$  define el resultado de la medida sobre el qubit  $j$  anterior al qubit  $i$ . Su valor es 0 si el resultado de la medida es positivo, y 1 si el resultado es negativo.

Dichas ecuaciones de autovalores se emplearán para deducir el conjunto de ecuaciones de autovalores que defina el estado output  $|\phi\rangle$  donde los qubits  $M$  ya han sido medidos.

$$K'|\phi\rangle = |\phi\rangle, \quad (3.3)$$

$K'$  son los operadores de correlación que caracterizan  $|\phi\rangle$ .

2. De acuerdo con el teorema 1 que aparece en la Ref. [7], es posible identificar la operación cuántica que se ha implementado tras la ejecución del patrón de medidas comparando las  $2n$  ecuaciones (3.4a)-(3.4b) con las ecuaciones de autovalores obtenidas (3.3).

$$X^I(UX^{(i)}U^\dagger)^O|\phi\rangle = (-1)^{\lambda_{X,i}}|\phi\rangle, \quad (3.4a)$$

$$Z^I(UZ^{(i)}U^\dagger)^O|\phi\rangle = (-1)^{\lambda_{Z,i}}|\phi\rangle. \quad (3.4b)$$

Donde  $\lambda_{X,i}, \lambda_{Z,i} \in \{0, 1\}$  son los resultados de las medidas realizadas sobre los qubits  $i$  ( $1 \leq i \leq n$ ); sus valores serán igual a cero cuando los resultados de las medidas sean positivos o cuando no se hayan realizado, e igual a 1 cuando los resultados sean negativos; y los superíndices  $I$  y  $O$  se refieren a los qubits inputs y outputs. Tras la comparación se deduce que la realización de las operaciones  $P_{s_i}$  sobre los qubits  $M$  siguiendo algún patrón de medidas dado, equivale a la aplicación de alguna operación unitaria sobre un estado input  $|\psi_{in}\rangle$ . Los estado input y output se relacionan via  $U$

$$|\psi_{out}\rangle = UU_\Sigma|\psi_{in}\rangle. \quad (3.5)$$

El operador  $U_\Sigma$  se conoce como operador *subproducto* (*byproduct*) cuya función es la de hacer de la computación un proceso determinista. Su origen lo trataremos más extensamente en la sección 3.5. El estado que resulta tras realizar las medidas es un producto de los estados de los qubits  $M$  medidos y del estado de la región del cluster que no ha sido medida

$$|\phi\rangle = \bigotimes_{i \in M} |m\rangle \otimes |\phi\rangle_{I \cup O}. \quad (3.6)$$

El segundo factor queda unívocamente determinado por las ecuaciones (3.4a) y (3.4b). Este teorema no implica que todo patrón de medidas implemente una puerta lógica y tampoco impone un orden en la realización de las medidas. En la Ref. [7] este teorema va acompañado de numerosos ejemplos de sus aplicaciones.

### 3.3.2. Implementación de una puerta lógica en computación cuántica basada en medidas

El procedimiento de implementación de cualquier puerta cuántica  $g$  consiste en los siguientes pasos:

1. Preparación de un estado cluster<sup>5</sup> o estado hiperentrelazado.

Supongamos que los qubits se encuentran inicialmente en el estado  $|+\rangle$ <sup>6</sup>, y que se entrelazan

---

<sup>5</sup>Uno de los principales resultados de la Ref. [110] es que el número de medidas que se prevee realizar debería ser el menor posible con el fin de minimizar el tiempo de exposición del sistema a los efectos de la decoherencia, por lo tanto, la eliminación de los qubits redundantes previo paso a al proceso de computación no es una estrategia eficiente. Los nuevos avances experimentales proporcionan la creación de estados que poseen, de partida, el diseño exacto que se precisa para computación pensada, sin necesidad de eliminar ningún qubit.

<sup>6</sup>Si todos los qubits se preparan en el estado  $|+\rangle$  y luego se entrelazan, obtenemos un estado cluster que es un recurso universal donde ningún input posee una información concreta, en este sentido  $QCC$  no tiene un input especificado. Por otro lado, cualquier otro input conocido se puede obtener a partir del estado cuántico estándar  $|+\dots+\rangle$  mediante algún circuito inicial. En otras palabras, si los estados inputs son conocidos y difieren de  $|+\rangle$ , siempre se puede encontrar una transformación unitaria  $U_{in}$  tal que estado  $|\Psi\rangle = U_{in}|+\dots+\rangle$  y cualquier operación unitaria  $U$  que actúe sobre  $|\Psi\rangle$ , se realice en realidad sobre  $U_{in}|+\dots+\rangle$ .

aplicando  $C_Z = \bigotimes_{ab \in C} C_{Z_{ab}}$  (capítulo 1) hasta formar un estado cluster inicial. En la Fig. 3.6 se observan estados cluster de una, dos, y tres dimensiones, respectivamente.

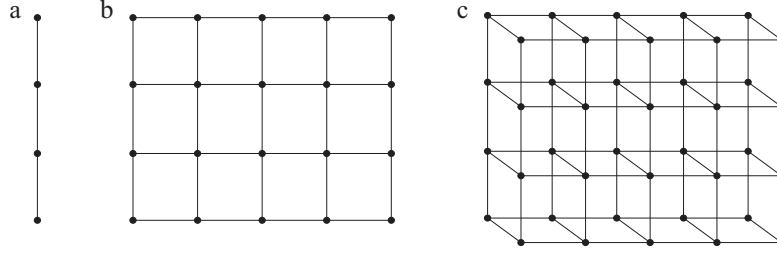


Figura 3.6: (a) Corresponde a un estado cluster de 1D. (b) Corresponde a un estado cluster de 2D. (c) Corresponde a un estado cluster de 3D.

## 2. Eliminación de los qubits redundantes.

Los *qubits redundantes* son aquellos que no intervienen en la tarea de computación. Estos qubits se eliminan aplicando sobre ellos el proyector

$$P_{\sigma_{z_i}} = \frac{1 + (-1)^{s_i} \sigma_z^i}{2}. \quad (3.7)$$

El estado resultante es un estado producto de los qubits medidos  $|s_i\rangle$ , y el resto del estado cluster, denotado como  $|\phi'\rangle_C$ .

$$|\Phi\rangle_C \xrightarrow{P_{\sigma_{z_{C_R}}}} |Z\rangle_{C_R} \otimes |\phi'\rangle_C, \quad (3.8a)$$

$$|Z\rangle_{C_R} \otimes |\phi'\rangle_C = \left( \bigotimes_{i \in C_R} \frac{1 + (-1)^{s_i} \sigma_z^i}{2} \right) |\phi\rangle_C = \left( \bigotimes_{i \in C_R} |s_i\rangle \right) \otimes |\phi'\rangle_C. \quad (3.8b)$$

Con  $C_R$  denotamos a los qubits redundantes del estado cluster y  $|Z\rangle_{C_R}$  los estados los qubits redundantes cuando sobre ellos se aplica  $P_{\sigma_{z_{C_R}}}$ . Los operadores generadores  $K'^a$ , para  $a \in C \setminus C_R$ , de este estado se obtienen de los del estado input,  $K^a$ , eliminando las contribuciones de los qubits redundantes. Su expresión general es

$$K'^a = \sigma_x^a \bigotimes_{\substack{c \in N(a) \\ \cap C \setminus C_R}} \sigma_{z_c}, \quad (3.9)$$

y satisfacen la ecuación de autovalores

$$K'^a |\phi'\rangle_C = (-1)^{k'_a} |\phi'\rangle_C, \quad (3.10a)$$

$$k'_a = (k_a \prod_{\substack{b \in N(a) \\ \cap (C \setminus C_R)}} s_b). \quad (3.10b)$$

Si el estado resultante tuviera autovalores negativos se aplicarían rotaciones locales alrededor del eje  $z$  sobre los oportunos qubits  $b \in N(a)$ . Luego la eliminación de los qubits redundantes



del cluster da como resultado otro estado cluster, en el sentido en que, salvo por las aristas faltantes, su estructura geométrica sigue encajando en la del cluster original.

### 3. Ejecución del patrón de medidas.

La realización de las medidas es equivalente a aplicar el proyector

$$P_{\sigma^i} = \frac{1 + (-1)^{s_i} \vec{r}_i \cdot \vec{\sigma}^i}{2}, \quad (3.11)$$

sobre todos los qubits excepto sobre los qubits seleccionados como outputs. Entre la colección de medidas a realizar están:

#### 3.1. Medidas en la base propia de la componente $\sigma_{x(y)}$ de espín, $P_{\sigma_{x_i(y_i)}}$ .

Llevadas a cabo por el proyector

$$P_{\sigma_{x_i(y_i)}} = \frac{1 + (-1)^{s_i} (i) \cdot \sigma_{x(y)}}{2}, \quad (3.12)$$

su efecto es el de propagar los qubits lógicos a través del cluster. Si comparamos con el modelo CCMC, es como si “viajaran” por los cables o “wires” del circuito, y a su paso por las diferentes operaciones unitarias experimentarían las correspondientes modificaciones en sus estados. También se emplean para la realización de puertas de dos qubits. Este tipo de medidas pertenece al grupo  $Q_0$ , es decir, su aplicación no está condicionada por otras realizadas anteriormente.

#### 3.2. Medidas en la base $B_j$ .

Si los elementos de la base  $B_j$  viene representados por el operador

$$B_j = \frac{|0\rangle + (-1)^{s_j} e^{i\varphi} |1\rangle}{2}, \quad (3.13)$$

las medidas son llevadas a cabo por el proyector

$$\begin{aligned} P_{+\varphi} &= \left( \frac{|0\rangle + e^{i\varphi} |1\rangle}{\sqrt{2}} \right) \times \left( \frac{\langle 0| + e^{-i\varphi} \langle 1|}{\sqrt{2}} \right) \\ &= |0\rangle \langle 0| + |1\rangle \langle 1| + e^{-i\varphi} |0\rangle \langle 1| + e^{i\varphi} |1\rangle \langle 0| \\ &= \frac{I + X \cos(\varphi) - Y \sin(\varphi)}{2} = \frac{I + \vec{r}_{xy} \cdot \vec{\sigma}_{xy}}{2}. \end{aligned} \quad (3.14)$$

El efecto que produce es proyectar el estado de un qubit sobre el plano  $xy$  de la esfera de Bloch. El ángulo  $\varphi$  es la orientación del vector de Bloch respecto al eje de las  $x$  tal y como se muestra en la Fig. 3.7. Se emplean con el fin de realizar rotaciones de ángulo  $\varphi$  sobre los qubits lógicos. Los qubits físicos objetos de estas proyecciones pertenecen a los grupos  $Q_i$  con  $i \neq 0$ , y los resultados de sus medidas influyen en la ordenación temporal del patrón de medidas.

Para el ángulo  $\varphi = 0$  ( $\varphi = \pm \frac{\pi}{2}$ ) en la ecuación 3.14, el proyector se obtiene a partir de los estados propios del operador  $\sigma_x$  ( $\sigma_y$ ) de Pauli. Como ejemplo mostraremos la rotación de ángulo  $\varphi$  alrededor del eje  $z$  de un qubit lógico. De acuerdo con la Fig. 3.8, se parte de un estado  $|LC_2\rangle$ ,

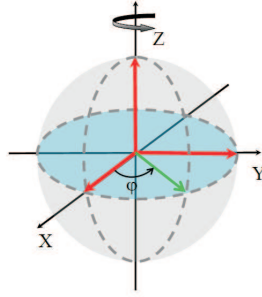


Figura 3.7: Rotación de un qubit lógico en el plano  $xy$  por la aplicación del proyector  $P_\varphi$ .



Figura 3.8: Rotación de un qubit lógico representada por un estado cluster de dos qubits. El primero se encuentra en el estado  $|\psi_{in}\rangle$  y el segundo en el estado  $|+\rangle$ . Para obtener como resultado el giro de un qubit lógico se aplica sobre el primer qubit el operador  $P_\varphi$ .

donde el estado del primer qubit es  $|\psi_{in}\rangle$  y el del segundo  $|+\rangle$ . Aplicando el operador  $P_\varphi$  sobre el qubit 1 obtenemos:

$$|LC_2\rangle = |\psi_{in}+\rangle, \quad (3.15a)$$

$$|\phi\rangle = P_\varphi|\psi_{in}+\rangle = |s_1\rangle \otimes |\psi_{out}\rangle, \quad (3.15b)$$

$$|\psi_{out}\rangle = X^{s_1} H U_Z(\varphi) |\psi_{in}\rangle. \quad (3.15c)$$

La ecuación (3.15a) se refiere al estado cluster  $|LC_2\rangle$  inicial. La ecuación (3.15b) corresponde al estado output después de haber aplicado sobre el primer qubit el operador  $P_\varphi$ . Y la ecuación (3.15c) relaciona los estados de los estados  $|\psi_{in}\rangle$  y  $|\psi_{out}\rangle$ , a través de la rotación lógica de un qubit dada por  $X^{s_1} H U_Z(\varphi)$ , donde  $X$  es la matriz  $\sigma_x$  de Pauli,  $U_Z$  rotación alrededor del eje  $z$ , y  $H$  la matriz de Hadamard.

Cualquier operación lógica cuántica se puede realizar con la elección apropiada de  $B_j(\varphi)$  y un cluster lo suficientemente grande.

#### 4. Medición sobre los qubits del registro output $O$ .

La expresión del estado lógico resultante

$$|\psi_{out}\rangle = U_\Sigma \bigotimes_{i \in O} |O\rangle_i, \quad (3.16)$$

se trata de un estado desentrelazado. Los resultados de las medidas durante la computación son los que informan acerca del proceso de computación y su resultado. Esta información está contenida en las contribuciones de los operadores representados por  $X$  (pues son aquellas que hacen evolucionar al qubit lógico) de  $U_\Sigma$ .

Si se prolongara el proceso de medición hasta los qubits output, no supondría adquirir un conocimiento extra esencial, pues al ser estas las últimas en llevarse a cabo, sus resultados no influirán en la elección futuras operaciones. Sólo en el contexto de la simulación de la computación CCMC a través de CCBM se puede suponer, sin pérdida de generalidad, que los qubits del registro output se miden en la base del operador de Pauli correspondiente a la componente  $z$  de espín para finalizar el procesamiento de la información cuántica.

### 3.4. Implementación de más de una puerta lógica en computación cuántica basada en medidas

Supongamos que se implementan dos puertas lógicas. Entonces se puede optar por los métodos descritos en el siguiente esquema:

*Primer método*

1. Preparamos el estado cluster.
2. Medimos todos los qubits excepto los  $O$ .

*Segundo método*

1. Preparamos el estado cluster para la primera puerta lógica,  $C(g_1)$ , y medimos sobre todos los qubits excepto sobre los  $O_1$ .
2. Implementamos el cluster de la segunda puerta lógica,  $C(g_2)$ , teniendo en cuenta que  $O_1 = I_2$ , medimos sobre todos los qubits salvo sobre los qubits  $O_2$ .

Estos dos métodos son matemáticamente equivalentes. Veamos,  $P_1$  y  $P_2$  son los operadores de proyección que se aplican sobre los conjuntos disjuntos de qubits  $O_1$  y  $O_2$ , por lo tanto conmutan entre sí. El mismo razonamiento se puede aplicar a los operadores  $U_1$  y  $U_2$ , que representan el entrelazamiento entre los qubits en sendos conjuntos. Entonces se satisface que:  $P_1P_2 = P_2P_1$ ,  $U_1U_2 = U_2U_1$ ,  $P_1U_2 = U_2P_1$ ,  $P_2U_2P_1U_1 = P_2P_1U_2U_1 = PS$ .

Como ejemplo veremos la forma de implementar una rotación arbitraria [10]

$$SU(2) = U_Z(\gamma)U_X(\beta)U_Z(\alpha), \tag{3.17}$$

sobre el qubit lógico codificado en el estado  $|\psi_{in}\rangle$ . En (3.17)  $\alpha$ ,  $\beta$ , y  $\gamma$  son los ángulos de Euler. Supongamos que partimos del estado  $|LC_4\rangle$ . Cada par de qubits consecutivo representa una rotación similar a la del protocolo de dos qubits del ejemplo de la Fig. 3.8. Los qubits compartidos por cada par son a su vez input y output. Las operaciones realizadas se muestran en la ecuación (3.18) y se indican en la Fig. 3.9.

$$\begin{aligned} U &= U_3U_2U_1 = X^{s_3}HU_Z(\gamma)X^{s_2}HU_X(\beta)X^{s_1}HU_Z(\alpha) \\ &= X^{s_3}Z^{s_2}X^{s_1}HU_Z((-1)^{s_2}\beta)U_X((-1)^{s_1}\gamma)U_Z(\alpha). \end{aligned} \tag{3.18}$$

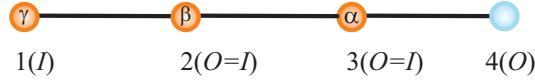


Figura 3.9: Rotación arbitraria de un qubit lógico. El primer qubit es el input y el último el output. Los qubits segundo y tercero hacen las veces de qubits input y output. Los pares de qubits 1-2 y 3-4 se emplean en rotaciones de ángulos  $\gamma$  y  $\alpha$ , respectivamente, alrededor del eje  $z$ . Y aquel formado por los qubits 2-3, en una rotación de ángulo  $\beta$  alrededor del eje  $x$ .

$$|\phi\rangle = |m\rangle \otimes |\psi_{out}\rangle, \quad (3.19a)$$

$$|\psi_{out}\rangle = SU(2)|\psi_{in}\rangle. \quad (3.19b)$$

La ecuación (3.19a) indica el estado final del conjunto de qubits tras las medidas, y la (3.19b) la evolución lógica del estado  $|\Psi_{in}\rangle$  a través de las distintas rotaciones  $SU(2)$  implementadas. Este resultado mejora el de la Ref. [7] donde se utiliza como recurso el estado  $|LC_5\rangle$ . En las Refs. [106, 101] se muestra la forma de implementar rotaciones de un sólo qubit empleando sólo tres qubits en el estado  $|LC_3\rangle$ , y dos ángulos de Euler. En las Refs. [23, 101] podemos ver cómo implementar puertas de dos qubits tales como la  $C_{NOT}$  empleando sólo el estado  $|LC_4\rangle$  dispuesto en forma de C girado  $180^\circ$ . En la Ref. [102] a través del estado  $|LC_6\rangle$ , también dispuesto en forma de C girado  $180^\circ$ , se vuelve a implementar una  $C_{NOT}$ ; pero el resultado es mucho más general porque se establece entre qubits arbitrarios (qubits cuyos estados se especifican en la esfera de Bloch con dos ángulos  $\alpha$  y  $\beta$  cualesquiera).

La implementación de rotaciones arbitrarias y puertas de dos qubits sobre los estados cluster hacen de este recurso un recurso universal de computación, es decir, en el modelo de CCBM se puede llevar a cabo cualquier operación unitaria.

### 3.5. Ordenación temporal de las medidas

En el modelo CCMC la ordenación temporal de las medidas depende del orden en que se aplican las puertas lógicas (ver Fig. 3.1), y sólo se pueden realizar simultáneamente aquellas que conmutan entre sí (ver Fig. 3.2). En CCBM el ordenamiento temporal de las medidas no tiene contrapartida en CCMC, y en muchas ocasiones es posible reducir la profundidad lógica de computación de una forma más efectiva (como ocurre con los circuitos de Clifford). La causa de esta diferencia está en que en CCBM las medidas sobre los qubits tienen resultados aleatorios, pues el operador densidad reducido de cada qubit de un estado máximamente entrelazado, es máximamente mezcla,  $\frac{I}{2}$ . No obstante, la computación cuántica es posible gracias a que estas medidas individuales están correlacionadas entre sí.

Una forma de controlar el resultado de las proyecciones, haciendo de la computación un procedimiento determinista, es mediante el operador subproducto  $U_\Sigma$ . A través de este operador, se recolecta un operador de corrección elevado al exponente  $s_i$ . Por ejemplo, tras la realización de  $P_\varphi$  es necesario aplicar a modo de corrección la matriz de Pauli  $X^{s_i}$  seguida de una puerta

Hadamard  $H$ ; y  $P_{\sigma_z}$  va seguida de la corrección  $Z^{s_i}$ , estos operadores se propagan<sup>7</sup> para ser acumulados en el operador  $U_\Sigma$ . Las acciones de propagación influyen sobre la elección de las bases de futuras medidas, y por lo tanto en la construcción de los conjuntos  $Q_i$  originando, en última instancia, la ordenación temporal de las medidas.

La diversidad de conjuntos  $Q_i$  que caracteriza a CCBM se confecciona de la siguiente manera. Cada conjunto contiene aquellas que se pueden realizar simultáneamente; por ejemplo el conjunto  $Q_0$  de la Fig. 3.4 representa la agrupación de qubits sobre los que se mide en la base propia de los observables  $X$ ,  $Y$  y  $Z$ . Estas medidas se pueden realizar al principio pues el ajuste de sus bases de medida no exige conocer el resultado de las medidas de otros qubits (no se requiere información clásica ganada a través de las medidas sobre otros qubits del cluster). Esto se debe a que los operadores que se simulan empleando estas proyecciones normalizan al grupo de Pauli, por lo que conservan sus propiedades intactas durante la propagación del operador subproducto. Mientras que éste se transforma en general como  $U_g U_\Sigma = (U_g U_\Sigma (U_g)^{-1}) U_g$ . Las puertas lógicas del grupo de Clifford son idóneas para mostrar esta característica, pues transforman el grupo de Pauli en sí mismo bajo conjugación.

Luego los circuitos cuánticos consistentes en realizar únicamente este tipo de puertas se pueden ejecutar en un único paso. Esta afirmación conduce a una extensión del teorema de Gottesman-Knill<sup>8</sup>. Lo que significa que no sólo se pueden eliminar los qubits redundantes de un circuito cuántico, sino también a los que intervienen en la parte de Clifford de cualquier algoritmo, pues su implementación no requiere de recurso cuántico alguno, se pueden simular eficientemente clásicamente. Esta es una de las ventajas de emplear la computación cuántica basada en medidas, frente al modelo CCMC (donde el mejor límite superior viene dado por  $\mathcal{O}(\log n)$  [111]). El lado “oscuro” de decantarse por la eliminación de estos qubits<sup>9</sup> es que el recurso cuántico inicial deja de ser un recurso universal o estado cluster para convertirse en una especie que forma parte de un grupo más amplio, el de los estados grafo, que son herramientas más específicas pensadas para la implementación de tareas concretas.

<sup>7</sup>Ver en Ref. [7] las relaciones de propagación.

<sup>8</sup>En la versión extendida del teorema de Gottesman-Knill toda computación cuántica basada únicamente en estados input cuánticos preparados en la base computacional, en puertas unitarias del grupos de Clifford, y medidas de observables del grupo de Clifford se puede simular eficientemente clásicamente sin necesidad de ningún recurso cuántico.

<sup>9</sup>En la Ref. [1, 2] podemos encontrar las reglas para aplicar las proyecciones en las bases propias de los operadores  $X$ ,  $Y$  y  $Z$  sobre un estado grafo dado.



# Capítulo 4

## Entrelazamiento

### 4.1. Introducción

El entrelazamiento es una propiedad de los sistemas cuánticos que no tiene equivalente en la Física Clásica [41]. En Información Cuántica se ha convertido en un recurso para la realización de tareas imposibles en Física Clásica como la criptografía cuántica [112], la teleportación cuántica [113], y la computación cuántica [6].

Los progresos experimentales en los últimos 20 años están aportando un control cada vez mayor sobre los sistemas cuánticos, lo que ha conducido al desarrollo de la teoría del entrelazamiento y a la creación de muchos experimentos destinados a la generación del entrelazamiento. Pero su estudio es en general complicado, aunque esto no ha impedido que se obtengan resultados satisfactorios en la clasificación del entrelazamiento de ciertos estados puros. Este capítulo es introductorio de los dos siguientes, donde se clasifican los estados grafo de hasta  $n = 8$  qubits, y su contenido se distribuye como sigue: En la sección 4.2 introducimos algunos conceptos básicos, como las definiciones de estados entrelazados y estados separables. En la sección 4.3 introducimos varios criterios empleados en la identificación de estados entrelazados como el criterio PPT (criterio de la traspuesta parcial positiva) de separabilidad, el criterio de reducción, la descomposición de Schmidt, las desigualdades de Bell como test de separabilidad, y los testigos de entrelazamiento. Las operaciones locales más utilizadas para obtener las clases de equivalencia las introducimos en la sección 4.4. En la sección 4.5 definimos las medidas de entrelazamiento y exponemos algunas de sus propiedades. En la sección 4.6 destacamos dos criterios para la obtención de clases de equivalencia, que son el teorema de Nielsen (empleado para determinar la equivalencia entre estados entrelazados bipartitos) y la equivalencia bajo SLOCC (operaciones locales estocásticas asistidas por comunicación clásica), y resumimos la clasificación de los estados puros de hasta  $n = 4$  qubits estableciendo finalmente su relación con la clasificación de los estados grafo.

El escenario en el que trabajaremos será aquel en el que las diferentes partes o subsistemas de un estado entrelazado se encuentran espacialmente separadas unas de otras<sup>1</sup>, pudiendo estar

---

<sup>1</sup>Dos sistemas cuánticos no relativistas están separados si sus funciones espaciales de onda no están solapadas,

comunicadas entre sí mediante un canal clásico. En estas condiciones cualquier protocolo consistente en rondas de operaciones locales sobre los subsistemas (incluyéndose la comunicación clásica de los resultados entre ellos, si se han incluido medidas) puede modificar el sistema transformándolo en otro con las mismas propiedades de entrelazamiento pues el entrelazamiento es un fenómeno no local que no se puede generar, ni alterar mediante operaciones de índole local. Entonces, se dice que pertenecen a la misma clase de equivalencia.

## 4.2. Estados separables y estados entrelazados

En esta sección, atendiendo a cómo se distribuye el entrelazamiento entre las partes de un estado, y distinguiendo entre estado puro y estado mezcla, aportaremos la definición de estado entrelazado. El concepto de estado entrelazado va unido al de estado separable, aquí comenzaremos introduciendo el segundo concepto. Antes de dar estas definiciones partiremos de otras que también necesitaremos.

### 4.2.1. Entrelazamiento en estados puros

*Definición.* Un estado cuántico es puro si está máximamente determinado, es decir, si se puede escribir como

$$\rho = |\psi\rangle\langle\psi|, \quad (4.1)$$

donde el operador densidad de estado  $\rho$  satisface que  $\text{tr}(\rho^2) = 1$ .

*Definición.* Un estado cuántico es bipartito si su espacio de Hilbert se puede descomponer como producto tensorial de dos partes  $A$  y  $B$

$$|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} c_{ij} |a_i\rangle |b_j\rangle \in H_A \otimes H_B, \quad (4.2)$$

donde  $d_A$  y  $d_B$  son las dimensiones de los subespacios  $H_A$  y  $H_B$ , y  $|a_i\rangle$  y  $|b_j\rangle$  las bases para este estado en cada uno de ellos. Los coeficientes  $c_{ij}$  conforman una matriz  $C$  de dimensión  $d_A \times d_B$ . Esta definición se puede extender a estados puros  $m$ -partitos de  $n$  qubits, con  $1 \leq m \leq n$ .

*Definición.* Un estado puro es biseparable si se pueden encontrar dos estados  $|\phi_A\rangle \in H_A$  y  $|\phi_B\rangle \in H_B$  tales que

$$|\psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle. \quad (4.3)$$

Esta definición se puede extender a estados puros  $m$ -separables  $|\psi\rangle = \bigotimes_{i=1}^m |\phi_i\rangle$  donde cada  $|\phi_i\rangle$  es un estado con un número determinado de qubits. El estado será completamente separable si  $m = n$ . Un estado puro que no es completamente separable contiene algún tipo de entrelazamiento.

*Definición.* Un estado puro es entrelazado si no es biseparable.

---

o bien difieren en algunos grados de libertad que permiten su distanciamiento.



Esta definición se basa en la definición de estado biseparable.

Si un estado se puede escribir como (4.3), entonces no está correlacionado, es decir, los subsistemas o partes se pueden preparar independientemente. En estados separables los resultados de las medidas de una parte no dependen de los resultados de las medidas de la otra.

### 4.2.2. Entrelazamiento en estados mezcla

*Definición.* Un estado mezcla es un estado cuántico que no se conoce exactamente, pues viene descrito por un conjunto de estados  $\{|\phi_i\rangle\}$  que llevan asociados una distribución de probabilidad  $\{p_i\}$ , por lo que su operador densidad se puede escribir como una combinación lineal convexa<sup>2</sup> de proyectores de estados puros  $|\phi_i\rangle\langle\phi_i|$

$$\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i| = \sum_i p_i \rho_i, \text{ con } \sum_i p_i = 1 \text{ y } p_i \geq 0. \quad (4.4)$$

La matriz que representa al operador densidad  $\rho$  es semidefinida positiva<sup>3</sup> donde todos los operadores  $|\phi_i\rangle\langle\phi_i|$  son positivos y hermíticos.

*Definición.* Un estado mezcla  $\rho$  es bipartito si su espacio de Hilbert se puede descomponer como producto tensorial de dos partes  $A$  y  $B$

$$\rho = \rho_A \otimes \rho_B, \quad (4.5)$$

donde  $\rho_A$  y  $\rho_B$  son dos estados mezcla definidos en los subespacios  $H_A$  y  $H_B$ , respectivamente. Esta definición se puede extender a estados mezcla  $m$ -partitos de  $n$  qubits, para  $1 \leq m \leq n$ .

*Definición.* Un estado es biseparable [114] si y sólo si su operador densidad  $\rho$  se puede expresar como una combinación lineal convexa de estados puros biseparables  $\rho_i^A \otimes \rho_i^B$

$$\rho = \sum_{i=1}^k p_i \rho_i^A \otimes \rho_i^B, \quad (4.6)$$

donde  $\sum_{i=1}^k p_i = 1$  y  $p_i \geq 0$ .

Esta definición se puede extender a estados  $m$ -partitos como se indica a continuación: Un estado mezcla es  $m$ -separable si se puede escribir como una combinación convexa de estados puros  $m$ -separables, lo cual podría ocurrir para diferentes tipos de particiones. Un estado será completamente separable cuando  $m = n$ , i.e.,  $\rho = \sum_i p_i \rho_i^{(1)} \otimes \cdots \otimes \rho_i^{(n)}$ .

<sup>2</sup>La combinación lineal de los estados  $|\phi_i\rangle\langle\phi_i|$  dada por la expresión (4.4), donde los  $p_i$  satisfacen  $\sum_i p_i = 1$  y  $p_i \geq 0$ , y el estado resultante es de nuevo un estado cuántico, se conoce como combinación lineal convexa.

<sup>3</sup>Un a matriz  $M$  es semidefinida positiva ( $M \geq 0$ ) si y sólo si sus autovalores son no negativos,  $\langle\psi|M|\psi\rangle \geq 0$  para todo  $|\psi\rangle$ .

*Definición.* Un estado es entrelazado si no admite una descomposición como la de (4.6).

Esta definición se obtiene a partir de la de estado biseparable.

*Definición.* Un estado (ya sea puro o mezcla) presenta auténtico entrelazamiento multipartito (o es máximamente entrelazado) cuando no es  $m$ -separable para  $n \geq m > 1$ .

Cuando los sumandos de las definiciones de este apartado sólo poseen un término, estas definiciones se particularizan a estados puros. Ningún término del sumatorio de (4.6) posee correlaciones cuánticas. Un estado separable se puede producir empleando sólo operaciones locales y comunicación clásica (LOCC, sección 4.5), es decir, con estas operaciones se pueden generar estados  $m$ -separables aleatorios con una probabilidad  $p_i$ . Este procedimiento genera únicamente correlaciones clásicas entre los subsistemas.

Aplicar estas definiciones no es trivial pues no existe un algoritmo general para comprobar si la descomposición (4.6) o, por extensión, aquella correspondiente a estados  $m$ -separables, existe para un estado dado. Por ejemplo, en los sistemas  $m$ -partitos no es suficiente con probar que es biseparable respecto a todas las biparticiones posibles para comprobar su separabilidad, pues pueden poseer una estructura de entrelazamiento mucho más rica. Por ejemplo, el estado de 4 qubits de Smolin [115]

$$\rho = \frac{1}{4} \sum_{i=1}^4 |\psi_{AB}^i\rangle\langle\psi_{AB}^i| \otimes |\psi_{CD}^i\rangle\langle\psi_{CD}^i|, \quad (4.7)$$

donde los  $|\psi^i\rangle$  son los cuatro estados de Bell, es separable respecto a cualquier bipartición de dos qubits y es entrelazado respecto a cualquier bipartición de uno y tres qubits. Esta clase de estados se conoce como estado semiseparable o parcialmente separable.

Dada un operador densidad el problema de si es separable o entrelazada se conoce como *problema de la separabilidad*, para el cual existe soluciones particulares que se obtienen a partir de los criterios de separabilidad. Aún se desconoce una solución general al problema de la separabilidad.

Las diferentes clases de entrelazamiento en que se distribuyen los estados entrelazados se obtienen estudiando en cuántas particiones son separables, aunque también se puede abordar el problema atendiendo a cuántas partículas hay entrelazadas.

### 4.3. Criterios de separabilidad

Hay una extensa teoría desarrollada acerca de los diversos criterios de separabilidad, por lo que nos restringiremos a hacer una breve descripción de algunos de ellos.

### 4.3.1. Entropía de von Neumann

La entropía de von Neumann se define como

$$S(\rho) = -\text{tr}(\rho \log_2 \rho) = -\sum_i p_i \log_2(p_i), \quad (4.8)$$

donde  $\rho$  es la matriz densidad de un estado, y los  $p_i$  sus autovalores,  $0 \leq p_i \leq 1$ ,  $\sum_i p_i = 1$ .

La entropía de von Neumann distingue entre estados bipartitos biseparables y estados entrelazados.

La entropía de un sistema bipartito satisface la siguiente desigualdad [116, 117]

$$|S(\rho_A) - S(\rho_B)| \leq S(\rho) \leq S(\rho_A) + S(\rho_B) = S(\rho_A \otimes \rho_B), \quad (4.9)$$

Para estados puros se define la entropía de entrelazamiento  $E_E = S(\rho_A) = S(\rho_B) = I/2$ , donde  $I$  es el *índice de correlación* [118] (*entropía mutua o información mutua de von Neumann*) dado por la expresión:  $I = S(\rho_A) + S(\rho_B) - S(\rho)$ ,  $0 \leq I \leq 2\min[S(\rho_A), S(\rho_B)]$ . Si  $I = 0$  entonces la entropía de entrelazamiento es nula, los dos estados reducidos son puros, y el estado final es factorizable. Si  $I > 0$  entonces la entropía de entrelazamiento es no nula, los dos estados reducidos son estados mezcla y el estado final es entrelazado.

Si el estado total es un estado mezcla bipartito y biseparable el índice de correlación  $I$  es nulo. Pero si  $I > 0$  no es posible distinguir si el estado es o no biseparable. En estos casos el problema se aborda empleando otras entropías [119, 120].

### 4.3.2. Criterio PPT

Dado un estado  $m$ -partito descrito por una matriz densidad  $\rho$ , la traspuesta parcial se define como la trasposición de  $\rho$  respecto a alguno de los subsistemas. Por ejemplo, en un sistema bipartito la traspuesta parcial se podría calcular respecto al subsistema  $A$  ( $B$ ), lo que denotaremos como  $\rho^{T_A}$  ( $\rho^{T_B}$ ). La trasposición parcial satisface que:  $\rho^T = (\rho^{T_A})^{T_B}$  y  $\rho^{T_B} = (\rho^{T_A})^T$ . El espectro de una matriz traspuesta, ya sea parcial o totalmente, no depende de la base. Por otro lado, una matriz densidad  $\rho$  tiene una traspuesta parcial positiva (i.e., la matriz es PPT o positiva bajo trasposición parcial) si su traspuesta parcial no tiene autovalores negativos (i.e., es semidefinida positiva),

$$\rho^{T_A} \geq 0. \quad (4.10)$$

La matriz totalmente traspuesta de un estado entrelazado es positiva. El criterio PPT propuesto por Peres [121], establece que si un estado bipartito es separable, entonces la traspuesta parcial respecto a cualquiera de los subsistemas conserva la positividad del operador densidad de estado. Es decir, si  $\rho$  es separable

$$\rho^{T_A} \geq 0, \quad (4.11)$$

donde  $T_A$  es la traspuesta parcial en el subsistema  $A$ . Según el criterio PPT, si el resultado es negativo, el estado  $\rho$  es entrelazado

$$\rho^{T_A} < 0 \text{ (Condición suficiente de entrelazamiento bipartito según el criterio PPT)}. \quad (4.12)$$

La traspuesta por ser una transformación positiva al actuar sobre un estado desentrelazado, no debe cambiar la positividad. De acuerdo con el criterio PPT, si lo hace es porque ha actuado sólo sobre una parte de estos sistemas y no sobre su totalidad, y por lo tanto es entrelazado.

En la Ref. [122] se prueba que el criterio PPT es una condición necesaria y suficiente de separabilidad para estados bipartitos cuyas dimensiones  $d_A$  y  $d_B$  satisfagan  $d_A d_B \leq 6$  (i.e., sistemas bipartitos del tipo  $2 \otimes 2$  ó  $2 \otimes 3$ ). Para dimensiones mayores esto no es cierto en general<sup>4</sup>. No obstante, la severidad con que se viola el criterio el criterio PPT se puede usar para cuantificar el entrelazamiento a través de un parámetro conocido como negatividad [123, 124].

### 4.3.3. Criterio de reducción

El criterio de reducción [125] establece que si un estado bipartito es separable se cumplen las siguientes desigualdades

$$\rho_A \otimes I_B - \rho_{AB} \geq 0, \quad (4.13a)$$

$$I_A \otimes \rho_B - \rho_{AB} \geq 0. \quad (4.13b)$$

Si las dimensiones  $d_A$  y  $d_B$  satisfacen  $d_A d_B < 6$ , entonces el criterio de reducción es equivalente al PPT. Para dimensiones mayores el criterio de reducción resulta ser más débil.

### 4.3.4. Descomposición de Schmidt

La descomposición de Schmidt o descomposición biortogonal [126, 127, 128, 129] es un recurso muy empleado tanto para caracterizar la separabilidad de los estados puros bipartitos, como para entender las correlaciones entre los dos subsistemas de un estado puro bipartito<sup>5</sup>. De acuerdo con la descomposición de Schmidt, para cualquier estado  $|\psi\rangle_{AB}$  de un sistema compuesto por dos subsistemas  $A$  y  $B$  es posible obtener bases de estados ortonormales,  $|u_i\rangle_A$  y  $|v_i\rangle_B$ , definidas en cada uno de sus correspondientes subespacios de Hilbert,  $H_A$  y  $H_B$ , tales que el estado  $|\psi\rangle_{AB}$  se puede expresar de forma única como

$$|\psi\rangle_{AB} = \sum_i^n \sqrt{\lambda_i} |u_i\rangle_A |v_i\rangle_B, \quad (4.14)$$

donde  $n \leq \min(d_A, d_B)$  y se le conoce como *rango de Schmidt* de  $|\psi\rangle_{AB}$ . En los estados separables el rango de Schmidt es igual a uno. Nótese que a diferencia de (4.2) aquí sólo hay un único índice en el sumatorio. Los  $\sqrt{\lambda_i}$  son los autovalores de los estados reducidos  $\rho_A$  y  $\rho_B$ , se denominan

<sup>4</sup>En las Refs. [130, 131] se encuentran ejemplos de estados no separables que verifican el criterio de la positividad para  $3 \otimes 3$  y  $2 \otimes 4$ . En la Ref. [132] se muestra la siguiente condición necesaria y suficiente de separabilidad, sólo válida para sistemas de dos qubits: Un estado de dos qubits será separable si y sólo si el determinante de la traspuesta parcial de la matriz densidad es no negativo.

<sup>5</sup>En [133] encontramos una explicación extendida de por qué no es extensible a estados multipartitos ni a estados mezcla.

coeficientes de Schmidt, y satisfacen  $\sum_i \lambda_i = 1$

$$\rho_{AB} = |\psi\rangle_{AB}\langle\psi|_{AB}, \quad (4.15a)$$

$$\rho_A = \text{tr}_B[\rho_{AB}] = \sum_i^n \lambda_i |u_i\rangle_A \langle u_i|_A, \quad (4.15b)$$

$$\rho_B = \text{tr}_A[\rho_{AB}] = \sum_i^n \lambda_i |v_i\rangle_B \langle v_i|_B. \quad (4.15c)$$

El cuadrado de cada coeficiente Schmidt  $\sqrt{\lambda_i}$  es el *peso de Schmidt*  $\lambda_i$ . La descomposición de Schmidt siempre existe, pero es única, salvo factor de fase, sólo en el caso en que todos los  $\lambda_i$  sean diferentes [62, 129, 134]. Cuando esto no sucede, el estado  $|\psi\rangle$  se puede descomponer biortogonalmente en un número infinito de bases. La separabilidad de los estados puros bipartitos se caracteriza mediante la descomposición de Schmidt de la siguiente forma:

1. El estado  $|\psi_{AB}\rangle$  es separable o factorizable si y sólo si su descomposición de Schmidt es única y tiene un único coeficiente de Schmidt distinto de cero. Es decir, si se puede escribir como

$$|\psi\rangle = |u\rangle_A |v\rangle_B. \quad (4.16)$$

2. Si hay más de un coeficiente de Schmidt distinto de cero, el estado es entrelazado. Atendiendo a su descomposición biortogonal, los estados entrelazados se pueden clasificar a su vez como:

2.1. Estados de Hardy, que son aquellos estados cuya descomposición biortogonal es única.

2.2. Si los módulos de dos o más coeficientes de Schmidt son iguales, entonces existen infinitas descomposiciones de Schmidt posibles y por tanto existen infinitas correlaciones perfectas entre las partes del sistema. Un estado cuya descomposición biortogonal no es única es un estado máximamente entrelazado. Los estados máximamente entrelazados se caracterizan entonces por poseer un número infinito de bases biortogonales. Un ejemplo de estado máximamente entrelazado es el estado singlete de dos partículas de espín 1/2 o el estado triplete.

En los sistemas  $m$ -partitos, con  $m \geq 3$ , la descomposición  $m$ -ortogonal

$$|\psi\rangle = \sum_i^{\min\{d_{A_1}, \dots, d_{A_m}\}} \sqrt{\lambda_i} |u_i^{(1)}\rangle \otimes |u_i^{(2)}\rangle \otimes \dots \otimes |u_i^{(m)}\rangle, \quad (4.17)$$

no siempre existe, pero cuando existe es única [134]. La descomposición de Schmidt en estos estados se conoce como descomposición de Schmidt generalizada.

Un ejemplo de estados que admiten una descomposición de Schmidt generalizada lo constituyen los estados GHZ

$$|GHZ\rangle_d^{(m)} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} (|i\rangle^{\otimes m}). \quad (4.18)$$

Esta es la expresión generalizada de los estados GHZ. Un ejemplo de estado que no admite una descomposición de Schmidt es el estado  $W = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ . Para los estados mezcla no existe un método numérico que satisfaga el criterio de separabilidad dado por la descomposición de Schmidt.

Por otro lado, la descomposición de Schmidt es útil para el estudio de las correlaciones son dos motivos:

1. Los vectores  $\{|u_i\rangle\}_A$  y  $\{|v_i\rangle\}_B$  permiten definir los operadores hermíticos  $\hat{u}_A = \sum_i u_i |u_i\rangle_A \langle u_i|_A$  y  $\hat{v}_B = \sum_i v_i |v_i\rangle_B \langle v_i|_B$ , respectivamente. Estos operadores representan a los observables  $u$  y  $v$ , de autovalores  $u_i$  y  $v_i$ , que reciben el nombre de *observables de Schmidt*. Las matrices densidad reducida de los componentes de un estado bipartito escritas en la descomposición de Schmidt, son diagonales con el mismo espectro. Cuando se mide  $u$  sobre el subsistema  $A$  y se encuentra el resultado  $u_k$ , entonces cualquier medida de  $v$  sobre  $B$  dará con certeza el resultado  $v_k$ , pues en un estado con descomposición biortogonal los observables de Schmidt están correlacionados.

2. Si las dimensiones de los subsistemas  $H_A$  y  $H_B$  no son iguales, por ejemplo con  $d_A < d_B$ , entonces el subsistema  $A$  no puede entrelazarse con más de  $d_A$  estados ortogonales del subsistema  $B$ . Si el rango de los operadores densidad reducidos fuera cero, entonces todos los coeficientes Schmidt serían nulos y no existiría entrelazamiento entre los subsistemas  $A$  y  $B$  considerados.

Los coeficientes de Schmidt son invariantes algebraicos bajo la acción de transformaciones locales unitarias.

### 4.3.5. Desigualdades de Bell

La mayoría de las desigualdades de Bell [41] se emplean para descartar modelos de variables ocultas locales, pero con ello sólo se excluye la completa separabilidad de los estados. Estas desigualdades de Bell constituyen una condición necesaria pero no suficiente de separabilidad, porque existen estados que las satisfacen, y presentan correlaciones cuánticas [114] que los caracteriza como estados entrelazados. Sin embargo, existen desigualdades de Bell que se pueden usar para probar el auténtico entrelazamiento multipartito, aunque hasta ahora sólo funcionan para unos pocos estados como los GHZ [135, 136, 137, 138], pero no para los estados clusters. Uno de los inconvenientes de estas desigualdades es que requieren de estados preparados con una alta fidelidad<sup>6</sup>, además de precisar una cantidad de medidas que tiende a crecer exponencialmente con el número de qubits.

### 4.3.6. Testigos de entrelazamiento

Los testigos de entrelazamiento [122, 139, 140, 141] son observables que caracterizan los estados separables y constituyen uno de los métodos principales empleados para detectar experimentalmente el entrelazamiento. Un testigo de entrelazamiento se define como:

<sup>6</sup>Ver en la nota 4 del capítulo 2 la definición de fidelidad cuántica.

*Definición.* Un observable  $W$  es un testigo de entrelazamiento (o testigo) si

$$\text{tr}(W\rho) \geq 0, \text{ para todos los estados separables,} \quad (4.19a)$$

$$\text{tr}(W\rho) < 0, \text{ para al menos un estado entrelazado.} \quad (4.19b)$$

Por tanto, si  $\text{tr}(W\rho) < 0$  entonces el estado  $\rho$  es entrelazado, y en tal caso se dice que es detectado por  $W$ . El criterio de entrelazamiento establecido por los testigos es una condición necesaria y suficiente, y se expresa en términos de un operador. Los testigos de entrelazamiento se pueden interpretar geoméricamente, veamos: su valor esperado depende linealmente del estado, por tanto, aquellos estados para los que  $\text{tr}(W\rho) = 0$  se pueden visualizar como un hiperplano que corta el espacio en dos partes. En una parte se satisface que  $\text{tr}(W\rho) > 0$  y contiene el conjunto de todos los estados separables. En la otra, se tiene que  $\text{tr}(W\rho) < 0$  y en ella figuran todos los estados entrelazados.

Para cada estado entrelazado existe un testigo de entrelazamiento que lo detecta [122]. El problema es construir el testigo de entrelazamiento adecuado, tarea que depende en gran medida del criterio de separabilidad que viole dicho estado.

#### 4.4. Operaciones locales sobre estados cuánticos

Un conjunto de estados pertenece a la misma clase de equivalencia de entrelazamiento si poseen el mismo entrelazamiento. Las operaciones más generales que transforman un estado cuántico en otro de la misma clase u órbita son aquellas del tipo:

$$\rho \rightarrow \frac{\Lambda(\rho)}{\text{tr}[\Lambda(\rho)]}, \quad (4.20)$$

donde el numerador es

$$\Lambda(\rho) = \sum_i V_i \rho V_i^\dagger, \quad (4.21)$$

siendo  $\sum_i V_i^\dagger V_i \leq I$  y los  $V_i$  los operadores de Kraus [142, 143].

El denominador de (4.20) satisface  $\text{tr}[\Lambda(\rho)] \leq 1$ , para cualquier estado  $\rho$ , y es la probabilidad asociada a la operación del numerador. Dicha probabilidad es igual a 1 si y sólo si la ecuación (4.21) conserva la traza (i.e.,  $\sum_i V_i^\dagger V_i = I$ ), y cuando esto sucede a  $\Lambda$  se le conoce como *canal cuántico determinista*.

Nos centraremos en aquellas operaciones locales en las que un estado puro  $|\phi\rangle$  se transforma en otro estado puro  $|\psi\rangle$  con una probabilidad no nula, y en las que además el concepto de localidad se aplique a la partición más fina de un estado. Por ejemplo, si se trata de un estado grafo se aplicará sobre cada qubit (vértice del grafo asociado) del mismo. Luego las transformaciones locales sobre un estado  $|\psi\rangle$  que posea  $N$  subsistemas, considerados como las particiones más finas, serán del tipo

$$|\phi\rangle = E_1 \otimes \dots \otimes E_N |\psi\rangle, \quad (4.22)$$

o equivalentemente

$$\varepsilon(\rho) = E_1 \otimes \dots \otimes E_N \rho (E_1)^\dagger \otimes \dots \otimes (E_N)^\dagger, \quad (4.23)$$

si actúan sobre el operador densidad del estado.

Podemos distinguir:

*LU.* Transformaciones unitarias locales arbitrarias donde cada  $E_i \in SU(2)$ <sup>7</sup>. La equivalencia LU ocurre con una probabilidad igual a la unidad.

*LOCC.* Operaciones locales asistidas por comunicación clásica [144]. Cualquier protocolo de comunicación basado en LOCC consiste en realizar operaciones locales sobre los distintos subsistemas de un complejo entrelazado, y en comunicar entre ellos los resultados vía canal clásico. La equivalencia bajo LOCC entre dos estados se establece si y sólo si uno de ellos se puede obtener a partir del otro mediante transformaciones locales unitarias (LU) con una probabilidad igual a la unidad<sup>8</sup> [145, 146],

$$|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle \Leftrightarrow |\psi\rangle \xrightarrow{\text{LU}} |\phi\rangle. \quad (4.24)$$

Generalmente las transformaciones LOCC entre estados puros son irreversibles (i.e., no poseen inversas), por lo que en su conjunto tienen estructura de semigrupo.

*SLOCC.* Operaciones locales estocásticas asistidas por comunicación clásica [145], también conocidas como *operaciones de filtrado local*. Cada operación  $E_i \in SL(2, C)$ <sup>9</sup> es una matriz arbitraria invertible (el entrelazamiento se perdería si no fuera sí [147]). A diferencia de las operaciones de LOCC, no tienen que suceder con una probabilidad igual a la unidad. Las operaciones LU son un caso particular de SLOCC, luego los estados que son equivalentes bajo LU también lo son bajo SLOCC (la inversa no se cumple necesariamente). Por este motivo, la clasificación bajo SLOCC es de “grano grueso” en comparación con la anterior, pues cada clase de equivalencia abarca un espectro más amplio de estados entrelazados incluyéndose importantes características cualitativas del entrelazamiento que con la clasificación anterior no se habrían tenido en cuenta.

$$|\psi\rangle \xrightarrow{\text{LU}} |\phi\rangle \Rightarrow |\psi\rangle \xrightarrow{\text{SLOCC}} |\phi\rangle. \quad (4.25)$$

*LC.* Operaciones locales de Clifford donde cada  $E_i \in C_1$  (capítulo 5). La equivalencia LC ocurre con una probabilidad igual a la unidad.

Dos estados,  $|\phi\rangle$  y  $|\psi\rangle$ , son LU, SLOCC ó LC equivalentes cuando uno de ellos se transforma en el otro bajo la acción de alguna de las operaciones anteriormente citadas.

---

<sup>7</sup>El grupo  $SU(2)$  está formado por matrices unitarias de dimensión  $2 \times 2$  y determinante igual a la unidad. Su forma general es:  $U(\vec{a}) = a_0 - i\vec{a} \cdot \vec{\sigma}$ ,  $|\vec{a}| \leq 1$ ,  $a_0 = \pm\sqrt{1 - \vec{a}^2}$ , donde  $\vec{\sigma}$  son las matrices de Pauli,  $\vec{a}$  las coordenadas de cualquier vector de  $R^3$  y  $a_0$  una variable auxiliar.

<sup>8</sup>Es decir, cuando la traza de (4.20) es igual a la unidad.

<sup>9</sup>El grupo  $SL(2, C)$  consiste en el conjunto de matrices complejas de dimensión  $2 \times 2$  con determinante igual a la unidad.



## 4.5. Cuantificación del entrelazamiento

Las medidas de entrelazamiento cuantifican la cantidad de entrelazamiento en un estado dado. No existen resultados generales que se puedan emplear para cuantificar cualquier tipo de estado entrelazado, pero sí un gran número de resultados parciales, suficientes en muchos casos para las aplicaciones prácticas. En esta sección introduciremos las propiedades que, en general, una medida de entrelazamiento  $E(\rho)$  debería satisfacer [148], aunque no todos los cuantificadores de entrelazamiento lo hacen. No entraremos en discutir los diferentes métodos de cuantificación del entrelazamiento porque trascenderíamos de los objetivos previstos en este trabajo.

### 4.5.1. Propiedades generales de las medidas de entrelazamiento

1. Cualquier medida de entrelazamiento  $E(\rho)$  es nula si el estado es separable.

2. Una medida de entrelazamiento debe ser invariante bajo cambios locales de base, es decir, debe ser invariante bajo transformaciones locales unitarias

$$E(\rho) = E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger). \quad (4.26)$$

Esta propiedad debe satisfacerse por toda medida de entrelazamiento.

3. Dado que el entrelazamiento no puede crearse aplicando operaciones LOCC,  $E(\rho)$  no se incrementa bajo la acción de estas operaciones. Luego si  $\Lambda^{LOCC}$  es una transformación positiva implementada por una LOCC entonces

$$E[\Lambda^{LOCC}(\rho)] \leq E(\rho). \quad (4.27)$$

Esta condición es conocida como monotonicidad bajo LOCC, e implica la invariancia bajo transformaciones locales unitarias. Si una LOCC transforma el estado  $\rho$  en otros estados  $\rho_k$  con probabilidades  $p_k$ , entonces

$$\sum_k p_k E(\rho_k) \leq E(\rho). \quad (4.28)$$

Esta condición es más fuerte que la (4.27), aunque es satisfecha por muchas medidas de entrelazamiento.

4. El entrelazamiento decrece con la mezcla de dos o más estados

$$E\left(\sum_k p_k \rho_k\right) \leq \sum_k p_k E(\rho_k). \quad (4.29)$$

Esta desigualdad se interpreta como sigue: si se parte de un conjunto de estados  $\rho_k$  y se pierde información de uno de ellos, entonces el entrelazamiento decrece. Esta propiedad no la satisfacen todas la medidas de entrelazamiento [149].

5. Si se reparten  $n$  copias del mismo estado  $\rho$  entre  $n$  observadores, entonces se tiene que

$$E(\rho^{\otimes n}) = nE(\rho). \quad (4.30)$$

Esto conlleva que si dos observadores comparten dos estados diferentes,  $\rho_1$  y  $\rho_2$ , entonces

$$E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2). \quad (4.31)$$

Esta propiedad tampoco es satisfecha por todas las medidas de entrelazamiento [150].

## 4.6. Clases de entrelazamiento para estados puros de hasta 4 qubits

Es esta sección, haremos un breve recopilatorio de las clases de entrelazamiento en las que se clasifican todos los estados puros de hasta 4 qubits.

Dado un estado puro  $|\psi\rangle$  de algún sistema compuesto la cuestión es: ¿En qué clases de estados se puede transformar si los observadores entre los que distribuyen sus partes integrantes realizan operaciones locales en sus respectivos subsistemas permitiéndose la comunicación clásica entre ellas?

### 4.6.1. Teorema de Nielsen

De acuerdo con el teorema de Nielsen [151], cualquier estado puro bipartito  $|\psi\rangle_{AB}$  se puede transformar en otro estado puro  $|\phi\rangle_{AB}$  vía LOCC si y sólo si para cada  $k \in 1, \dots, d$  se tiene que

$$\sum_{j=1}^k \lambda_j^{(\psi)\downarrow} \leq \sum_{j=1}^k \lambda_j^{(\phi)\downarrow}. \quad (4.32)$$

En esta igualdad  $\sum_{j=1}^k \lambda_j^{(\psi)}$  es mayorizada<sup>10</sup> por  $\sum_{j=1}^k \lambda_j^{(\phi)\downarrow}$ . Para  $k = d$  se obtiene una igualdad estricta. Los  $\lambda_i$  son los pesos de Schmidt. El vector  $\vec{\lambda}^{\downarrow}(|\psi\rangle_{AB})$ , formado por los pesos de Schmidt de  $|\psi\rangle_{AB}$  ordenados en orden decreciente, es mayorizado por el correspondiente vector  $\vec{\lambda}^{\downarrow}(|\phi\rangle_{AB})$ . La transformación de un estado a otro, en ambos sentidos, puede tener lugar sólo si los coeficientes de Schmidt de ambos estados son iguales.

<sup>10</sup>La mayorización consiste en lo siguiente: Supongamos que tenemos dos vectores de dimensión  $d$ ,  $\vec{x}^{\downarrow} = (x_1, \dots, x_d)$  e  $\vec{y}^{\downarrow} = (y_1, \dots, y_d)$  (el símbolo  $\downarrow$  indica que las componentes se ordenan en orden decreciente), entonces  $\vec{x}$  es mayorizado por  $\vec{y}$ ,  $\vec{x} \prec \vec{y}$  si para cada  $k \in 1, \dots, d$

$$\sum_{j=1}^k x_j^{\downarrow} \leq \sum_{j=1}^k y_j^{\downarrow}.$$

Donde la desigualdad es una igualdad se mantiene cuando  $k = d$ . La relación de mayorización es de orden parcial en  $R^d$ , es decir, que al menos hay dos componentes  $x$  e  $y$  tales que  $x \prec y$  e  $y \prec x$ , si y sólo si  $x = y$ .

### 4.6.2. Equivalencia entre estados bajo SLOCC

La equivalencia entre estados bajo SLOCC ha sido estudiada [33, 34, 35, 152] con objeto de caracterizar todas las posibles clases de estados puros entrelazados. El objetivo es partir de un determinado sistema  $|\psi\rangle$  y convertirlo en otro  $|\phi\rangle$ , destinado a la realización una determinada tarea cuántica. Para ello, el escenario de trabajo es aquel en que cada subsistema se encuentra lo suficientemente separado espacialmente del resto, de modo que cada parte se puede manipular mediante operaciones locales de forma independiente [153]. Los resultados del conjunto de las acciones locales llevan asociados una determinada probabilidad. Las partes pueden estar comunicadas mediante canales clásicos, que dan lugar a una serie de correlaciones clásicas entre el conjunto comunicado. La ventaja de emplear operaciones locales que permitan pasar de un estado  $|\psi\rangle$  a otro  $|\phi\rangle$  con una probabilidad no nula pero no necesariamente igual a la unidad es que las clases de equivalencia que surgen constituyen una clasificación de grano grueso<sup>11</sup> respecto a la basada en LOCC.

### 4.6.3. Clasificación de los estados puros bajo SLOCC

En esta sección veremos las principales clases de equivalencia bajo SLOCC de estados puros entrelazados.

#### Estados puros de dos qubits

Los estados de dos qubits son equivalentes SLOCC a estados grafo de dos qubits, que pueden presentarse conectados o no [152]. En particular, cualquier estado puro entrelazado de dos qubits se puede convertir en el estado singlete  $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ . Luego sólo hay una clase de equivalencia SLOCC para los estados entrelazados de dos qubits, y puede representarse por el estado singlete  $|\psi^-\rangle$ .

#### Estados puros de tres qubits

Los estados puros entrelazados de tres qubits [33, 34, 35] se clasifican en cinco clases de equivalencia. Tres de ellas están integradas por estados biseparables, que son el resultado del producto entre un par entrelazado de dos qubits cualesquiera y el qubit no entrelazado.

En las otras dos clases de equivalencia el entrelazamiento se caracteriza por ser auténtico entrelazamiento tripartito. Veamos cuáles son. Dado un estado de tres qubits  $|\psi\rangle$ , es posible transformar una copia del mismo en otro estado  $|\phi\rangle$  a través de operaciones SLOCC en el espacio de cada qubit [33]

$$|\phi\rangle = A \otimes B \otimes C|\psi\rangle. \quad (4.33)$$

El estado  $|\phi\rangle$  puede ser el  $|GHZ\rangle = \frac{(|000\rangle + |111\rangle)}{\sqrt{2}}$  (que es equivalente SLOCC a un estado grafo), o el  $|W\rangle = \frac{(|100\rangle + |010\rangle + |001\rangle)}{\sqrt{3}}$  (que no posee equivalente en forma de grafo). Dichos estados  $|GHZ\rangle$  y  $|W\rangle$  no se pueden relacionar por operaciones SLOCC. Estos dos estados son los representantes

<sup>11</sup>Dado el carácter continuo de los parámetros que definen a las distintas clases de equivalencia LOCC, al ampliar el abanico de posibilidades de pertenencia a una clase determinada la clasificación es igual de rigurosa que mediante LOCC con la ventaja de que no se generan subclases dentro de una clase.

de las dos clases de equivalencia a que aludimos antes. Se necesitan 6 parámetros para caracterizar las propiedades no locales de un estado  $|GHZ\rangle$ , mientras que sólo se necesitan 5 para el estado  $|W\rangle$  [154]; por esta razón la clase GHZ es mucho más numerosa que la W. El estado GHZ es un estado de tres qubits máximamente entrelazado, pero con la peculiaridad de que si se desentrelaza uno de sus qubits, por ejemplo el C, el estado  $\rho_{AB} = (\text{tr}_C[|GHZ_3\rangle\langle GHZ_3|])$  queda completamente desentrelazado. Por el contrario, el estado W tiene la propiedad de que si se elimina uno de sus qubits, los dos restantes  $\rho_{AB} = (\text{tr}_C[|W\rangle\langle W|])$  presentan auténtico entrelazamiento bipartito [153, 155].

### Estados puros de $n \geq 4$ qubits

Los estados de 4 qubits [36] se agrupan en una familia genérica de un número infinito de elementos que contiene 9 subfamilias, cada una de ellas con una forma diferente de entrelazamiento. ¿Por qué las clases de entrelazamiento para estados que posean un número  $n$  de qubits  $n \geq 4$  poseen un número infinito de elementos [33]? Sea  $H^{(n)} = C^2 \otimes \dots \otimes C^2$  el espacio de Hilbert de un sistema  $n$ -partito de  $n$  qubits, el número de amplitudes complejas que se necesitan para especificar un estado es  $2^n$ , y si descartamos el parámetro que funciona como fase global compleja resulta ser al final  $2^n - 1$ . Por tanto, el número de parámetros reales independientes o grados de libertad es el doble,  $2(2^n - 1)$ . Por otro lado, las transformaciones del tipo SLOCC se representan por matrices invertibles del grupo  $SL(2, C)$  que por ser de dimensión  $2 \times 2$ , posee 4 componentes complejas que dan lugar a 8 parámetros reales. Aplicando la condición de invertibilidad, esta cantidad se reduce a 6 parámetros reales independientes por cada operación SLOCC. El conjunto de clases de equivalencia bajo SLOCC, denotado por

$$\frac{H^n}{SL_2(C) \times SL_2(C) \times \dots \times SL_2(C)}, \quad (4.34)$$

que posee  $n$  factores en el denominador, dependerá de al menos  $2(2^n - 1) - 6n$  parámetros independientes. Esta cantidad es una cota inferior, que para el caso  $n = 3$  permite que haya un número finito de clases de equivalencia, pero para  $n \geq 4$  aparecen infinitas clases de equivalencia etiquetadas con parámetros continuos. Este comportamiento se debe a que el número de parámetros que se necesita para especificar un estado cuántico es mayor (del orden de  $2^n$ ) que el que se puede manejar a través de operaciones SLOCC (del orden de  $n$ ), y a medida que crece  $n$  esta diferencia se va acrecentando.

En la Ref. [147] se muestra que cualquier estado puro multipartito se puede transformar mediante operaciones SLOCC en otro estado que sea equivalente al primero bajo LU. Por tanto, si dos estados grafo son equivalentes SLOCC también serán equivalentes bajo operaciones locales unitarias, es más, para estados grafo las equivalencias SLOCC y LU son coincidentes [156, 157]. De esta manera, el problema de decidir si dos estados grafo son equivalentes SLOCC, se reduce al problema de decidir si dos estados grafo son equivalentes bajo LU. Luego dos estados grafo  $|G_1\rangle$  y  $|G_2\rangle$  son equivalentes bajo SLOCC si y sólo si son equivalentes bajo LU

$$|G_1\rangle \xrightarrow{\text{SLOCC}} |G_2\rangle \Leftrightarrow |G_1\rangle \xrightarrow{\text{LU}} |G_2\rangle. \quad (4.35)$$

Por otro lado, la conjetura  $LU \Leftrightarrow LC$  (operaciones locales de Clifford) establece que los estados estabilizadores que son equivalentes  $LU$ , deben ser también equivalentes bajo  $LC$ . Realmente, para los estados grafo la equivalencia  $LU \Leftrightarrow LC$  es cierta en los casos más simples [38, 39], apareciendo los primeros contraejemplos para los estados con  $n = 27$  qubits [37]. Esta propiedad, unido al hecho de que  $LC$  tenga una contrapartida gráfica (la complementación local, ver apéndice) permite abordar el estudio de la clasificación de estos estados en clases de equivalencia. Nos detendremos en este punto para retomarlo en el siguiente capítulo dedicado a estudio de la clasificación de los estados grafo de hasta  $n = 8$  qubits.



## Capítulo 5

# Entrelazamiento en estados grafo de ocho qubits

### 5.1. Introducción

Los estados grafo tienen un papel fundamental en la teoría del entrelazamiento. En el capítulo anterior, hicimos un breve recopilatorio de las clases de equivalencia en que se dividen los estados puros entrelazados de hasta  $n = 4$  qubits. Los resultados fueron que la clasificación de tales estados se complicaba cada vez más a medida que aumentaba el número de qubits, de modo que para  $n \geq 4$ , hay una cantidad infinita de diferentes clases de estados puros entrelazados de  $n$  qubits.

Por los diferentes papeles fundamentales que desempeñan los estados grafo en la teoría de la Información Cuántica (los cuales hemos resaltado varias veces a lo largo de este trabajo), se ha dedicado mucho esfuerzo en su obtención experimental. Por una parte, están los experimentos de estados grafo de  $n$  qubits y  $n$  fotones hasta  $n = 6$  [23, 24, 25, 26, 27]. Y por otra, la combinación de dos técnicas, el hiperentrelazamiento (i.e., entrelazamiento en varios grados de libertad, como polarización y momento lineal) [48, 51, 53, 69, 70, 71, 72] y las fuentes de entrelazamiento de 4, 5 y 6 fotones usando *parametric down-conversion* [24, 73, 74, 75, 76, 77, 78], que permiten crear estados grafo de 6 qubits y 4 fotones [28], de 8 qubits y 4 fotones [29], y de 10 qubits y 5 fotones [29]. En particular, los estados grafo de 8 qubits y 4 fotones son especialmente útiles por la alta visibilidad que exhiben.

Hein, Eisert y Briegel (HEB) [1, 2] clasificaron los estados grafo de hasta  $n = 7$  qubits. Esta clasificación se ha empleado para identificar nuevas clases de demostraciones “all-versus-nothing”  $m$ -partitas (capítulos 9 y 8) [19, 20], nuevas desigualdades de Bell [14], así como para la impulsar la preparación de varios estados grafo [29].

El principal objetivo de este capítulo es extender la clasificación realizada por (HEB) [1, 2] hasta los estados grafo de ocho qubits. Atendiendo a los resultados previos, hay 45 clases de estados grafo no equivalentes bajo transformaciones unitarias de un solo qubit. Respecto a los estados grafo de ocho qubits, hay un total de 101 clases de estados no equivalentes, todas ellas

obtenidas por varios investigadores (ver Ref. [40]), que clasificaremos de acuerdo a varias relevantes propiedades físicas en la teoría de la Información Cuántica.

Organizaremos este capítulo de la siguiente manera: En las secciones 5.2 y 5.3 introduciremos las operaciones locales de Clifford y las operaciones de complementación local como herramientas para obtener las clases de equivalencia de los estados grafo de hasta 8 qubits. En la sección 5.4 estableceremos los criterios de clasificación empleados en [1, 2], con vistas a establecer una ordenación entre las clases de equivalencia en la sección 5.5.1. En la sección 5.5 presentaremos nuestros resultados.

## 5.2. Estados grafo y clases de equivalencia

Los estados grafo [158, 159] constituyen una importante subclase de estados estabilizadores. Un destacado resultado que relaciona la teoría de grafos y los estados estabilizadores es que cualquier estado estabilizador  $|S\rangle$  es LC equivalente (equivalente bajo una transformación local de Clifford) a algún estado grafo  $|G\rangle$  [5, 30, 31]. Su demostración la podemos encontrar en [32].

Este enunciado es un caso particular del establecido por Schlingemann [5] quien trabajó con sistemas de  $d$  niveles, y demostró que un código estabilizador es LC equivalente a un código grafo.

Otro resultado que relaciona los estados estabilizadores y los estados grafo es aquel que establece que un único estado estabilizador  $|S\rangle$  puede ser equivalente a varios estados grafo [160]

$$|G_1\rangle = U_1|S\rangle, \quad |G_2\rangle = U_2|S\rangle, \quad (5.1)$$

si y sólo si éstos son equivalentes entre si bajo transformaciones locales de Clifford

$$|G_1\rangle = U_1 U_2^\dagger |G_2\rangle. \quad (5.2)$$

Esta propiedad permite obtener toda una colección de estados grafo equivalentes, bajo transformaciones locales de Clifford, que representan a un mismo estado estabilizador. Estos conjuntos de estados grafo equivalentes se denominan clases de equivalencia u órbitas [1, 2, 21, 22], y serán caracterizadas en este capítulo y en el siguiente.

## 5.3. Complementación local

Las transformaciones locales de Clifford sobre los estados grafo pueden describirse a través de unas reglas gráficas conocidas como complementación local denotadas por  $\tau_a(G)$  [161].

La complementación local  $\tau_a(G)$  sobre un determinado vértice  $a$  perteneciente a un grafo  $G$ , se obtiene complementando el subgrafo de  $G(E, V)$  que viene dado por el vértice  $a$  y su vecindad  $N_a$ , conservándose intacto el resto del grafo (ver apéndice).

La regla de complementación local (regla LC) establece que:



Si  $G(E, V)$  es el grafo que representa al estado grafo  $|G\rangle$ , mediante complementación local sobre un vértice  $a \in V$  se obtiene un nuevo grafo  $G'(E', V)$  que corresponde a otro estado grafo  $|G'\rangle$  equivalente a  $|G\rangle$  bajo la acción de algún operador local de Clifford  $U_a^\tau |G\rangle$

$$|\tau_a(G)\rangle = U_a^\tau |G\rangle = |G'\rangle, \quad (5.3)$$

donde

$$U_a^\tau |G\rangle = e^{-i\frac{\Pi}{4}\sigma_x^{(a)}} \bigotimes_{b \in N_a} e^{i\frac{\Pi}{4}\sigma_z^{(b)}}, \quad (5.4)$$

que de acuerdo con (1.33), la expresión 5.4 puede escribirse también como

$$U_a^\tau = \sqrt{-i\sigma_x^{(a)}} \bigotimes_{b \in N_a} \sqrt{i\sigma_z^{(b)}}. \quad (5.5)$$

Es decir, si aplicamos complementación local sobre un vértice de un grafo, los estados grafo input y output se deben relacionar a través de alguna operación del grupo local de Clifford.

Por consiguiente, diremos que dos estados grafo  $|G\rangle$  y  $|G'\rangle$  son LC equivalentes (equivalentes bajo alguna operación local del grupo de Clifford) si y sólo si los grafos que los representan se relacionan bajo una secuencia de complementaciones locales:  $G' = \tau_{a_1} \circ \dots \circ \tau_{a_n}(G)$ , donde  $a_1, \dots, a_n \in V$ . Incluiremos la demostración de esta propiedad porque a través de ella se puede observar cómo evoluciona un estado grafo bajo la acción de los operadores  $U_a^\tau$ , empleando su estabilizador:

Sean  $|G\rangle$  y  $|G'\rangle$  dos estados grafo tales que los grafos que los representan se relacionan mediante una operación de complementación local sobre el vértice  $a$ ,  $G' = \tau_a(G)$ . Sean  $S$  y  $S'$  los estabilizadores respectivos, y  $g_b$  y  $g'_b$ , sus correspondientes operadores generadores. Los operadores generadores asociados a cualquier qubit representado por un vértice  $c$  que no pertenezca a  $N_a$  no van a modificarse bajo la acción de  $U_a^\tau$ , porque  $g_c$  y  $U_a^\tau$  se refieren a conjuntos de qubits distintos<sup>1</sup>

$$U_a^\tau g_c (U_a^\tau)^\dagger = g_c = g'_c. \quad (5.6)$$

Los operadores generadores asociados a los vértices  $b'$  pertenecientes a  $N_a$  (que denotaremos por

---

<sup>1</sup>Podría ocurrir que  $a$  y  $c$  tuvieran al menos un vecino en común, en tal caso, los operadores  $g_c$  y  $U_a^\tau$  tendrían en común al menos un operador local  $Z$  (que representa a la matriz de Pauli  $\sigma_z$ ). Lo cual significaría que no habría ningún obstáculo para que  $g_c$  y  $U_a^\tau$  siguieran conmutando.

$K_{b'}$ ) no son compatibles con  $U_a^\tau$ , y se transformarán de la siguiente manera

$$\begin{aligned}
U_a^\tau K_b(U_a^\tau)^\dagger &= (e^{-i\frac{\Pi}{4}X_a} \bigotimes_{b \in N_{a-b'}} e^{i\frac{\Pi}{4}Z_b} e^{i\frac{\Pi}{4}Z_{b'}}) \times (X_{b'} \bigotimes_{b \in N_{a-b'}} Z_b \otimes Z_a) \\
&\times (e^{-i\frac{\Pi}{4}Z_{b'}} \bigotimes_{b \in N_{a-b'}} e^{-i\frac{\Pi}{4}Z_b} e^{i\frac{\Pi}{4}X_a}) \\
&= (e^{-i\frac{\Pi}{4}X_a} e^{-i\frac{\Pi}{4}X_a} \bigotimes_{b \in N_{a-b'}} e^{-i\frac{\Pi}{4}Z_b} e^{i\frac{\Pi}{4}Z_b} \otimes e^{i\frac{\Pi}{4}Z_{b'}} e^{i\frac{\Pi}{4}Z_{b'}}) \\
&\times (X_{b'} \bigotimes_{b \in N_{a-b'}} Z_b \otimes Z_a) \\
&= (-iX_a \bigotimes_{b \in N_{a-b'}} I \otimes iZ_{b'}) \times (X_{b'} \bigotimes_{b \in N_{a-b'}} Z_b \otimes Z_a) \\
&= (X_a \bigotimes_{b \in N_a} Z_b) \times (X_{b'} \bigotimes_{b \in N_{b'}+N_a} Z_b) \\
&= g_a g_{b'}.
\end{aligned} \tag{5.7}$$

Con la idea de presentar una visión más compacta, en el desarrollo anterior no hemos empleado la notación  $\sigma_i$  para referirnos a las matrices de Pauli, y tampoco hemos añadido las matrices identidad para adecuar la dimensión de los operadores<sup>2</sup>. Respecto a la identidad de la expresión que se encuentra justo antes del último signo igual, la hemos descompuesto de la siguiente manera:

$$\bigotimes_{b \in N_{a-b'}} I = \left( \bigotimes_{b \in N_{a-b'}} Z_b \right) \left( \bigotimes_{b \in N_{a-b'}} Z_b \right). \tag{5.8}$$

La transformación de los generadores del estado grafo input bajo la acción del operador  $U_a^\tau$  tiene lugar como se describe en el desarrollo (5.7), es decir, multiplicando el operador generador del vértice de  $G$  sobre el que se aplica la complementación local,  $g_a$ , con cada uno de los generadores  $g_{b'}$  asociados a los vértices  $b \in N_a$  del grafo completado localmente  $G'$ . Luego los operadores generadores del nuevo estado serán los  $g_c$ , para  $c \notin N_a$ ,  $g_a$  y los  $g_{b'}$  que coinciden con los generadores del grafo  $G'$  obtenido por complementación local sobre el vértice  $a$ .

Hemos demostrado que tras la aplicación de una operación de complementación local sobre el grafo  $G$  se obtiene un grafo  $G'$  correspondiente a otro estado grafo, que es equivalente bajo LC al estado grafo representado por el primer grafo. Una secuencia de complementaciones locales, vuelve a ser equivalente a la acción un operador del grupo local de Clifford, luego el resultado obtenido es aplicable también cuando se emplea más de una operación de complementación local.

Otra importante propiedad de la complementación local, es que la acción de cualquier operador del grupo de Clifford sobre los estados grafo se puede descomponer en una secuencia de complementaciones locales sobre los grafos vinculados a ellos. Su demostración se puede encontrar en las Refs. [32, 162].

<sup>2</sup>Aunque realmente no era necesario porque se sobrentiende que al trabajar con operadores de correlación de un mismo estado, todos poseen igual dimensión.

## 5.4. Criterios de clasificación

De acuerdo con HEB, los criterios para ordenar las clases son:

1. Número de qubits.
2. Mínimo número de puertas controlled- $Z$  ( $C_Z$ ) necesarias para la preparación,  $|E|$ .
3. Medidas de Schmidt,  $E_S$ .
4. Índices de rango,  $IR$

Por ejemplo, la clase No. 1 es la única que contiene estados grafo de solo dos qubits, la No. 2 es la única que contiene estados grafo de tres qubits [1, 2]. Las clases No. 3 y No. 4 poseen 4 qubits y requieren de  $|E| = 3$  puertas controlled- $Z$ , sin embargo, se diferencian en que la medida de Schmidt  $E_S$  de la clase No. 3 es igual a 1, mientras que para la clase No. 4 es igual a 2.

Veremos en qué consisten cada uno de estos criterios por separado.

### 5.4.1. Mínimo número de puertas controlled- $Z$ necesarias para la preparación

Como vimos en el capítulo 1, para preparar un estado grafo, cada qubit debe encontrarse inicialmente en el estado  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  y, posteriormente, estos se conectan entre sí a través de puertas  $C_Z$ . Normalmente, los diferentes elementos pertenecientes a una misma clase LC requieren distinto número de puertas  $C_Z$  para su preparación. El primer criterio para comenzar con la clasificación de los estados grafo de ocho qubits es que el representante elegido de cada clase de equivalencia se corresponda con aquel que posea un mínimo número de aristas,  $|E|$ .

### 5.4.2. Medidas de Schmidt $E_S$

La medida de Schmidt fue introducida por Eisert y Briegel como una herramienta para cuantificar el genuino entrelazamiento multipartito de los sistemas cuánticos [163, 164] (capítulo 4). De acuerdo con la descomposición de Schmidt (capítulo 4, apartado 4.3.4), cualquier vector estado  $|\psi\rangle \in H^{(1)} \otimes \dots \otimes H^{(N)}$  de un sistema cuántico multipartito de  $N$  componentes se puede representar como

$$|\psi\rangle = \sum_{i=1}^R \xi_i |\psi_i^{(1)}\rangle \otimes \dots \otimes |\psi_i^{(N)}\rangle, \quad (5.9)$$

donde  $\xi_i \in \mathbb{C}$  para  $i = 1, \dots, R$ , y  $|\psi_i^{(j)}\rangle \in H^{(j)}$ , para  $j = 1, \dots, N$  (en comparación con la descomposición de Schmidt del capítulo 4, hemos empleado aquí una notación diferente para adaptarla a la del artículo [21]). La medida de Schmidt asociada a este vector estado, se define como

$$E_S(|\psi\rangle) = \log_2(r), \quad (5.10)$$

donde  $r$  es el mínimo número  $R$  de términos en los que puede descomponerse el estado  $|\psi\rangle$  de acuerdo con (5.9). Para el caso particular de un sistema de dos componentes ( $N = 2$ ),  $r$  viene dado por el rango de Schmidt del estado  $|\psi\rangle$ . Antes de conocer cómo se obtiene el rango de Schmidt, es necesario introducir los siguientes conceptos:

### Partición de un conjunto $V$ de vértices de un grafo $G = (V, E)$

Dado un estado grafo  $G = (V, E)$ , una partición de  $V$  es cualquier tupla  $(A_1, \dots, A_M)$  de subconjuntos disjuntos  $A_i \subset V$  tales que  $\bigcup_{i=1}^M A_i = V$ . Si  $M = 2$ , entonces la partición se denomina *bipartición* y se denota como  $(A, B)$ .

Una partición  $(A_1, \dots, A_N)$  es *más fina* que otra  $(B_1, \dots, B_M)$ , si todo  $A_i$  está contenido en algún  $B_j$ . La notación empleada para indicar que la partición  $(A_1, \dots, A_N)$  es más fina que  $(B_1, \dots, B_M)$  es

$$(A_1, \dots, A_N) \leq (B_1, \dots, B_M). \quad (5.11)$$

Por otro lado  $(B_1, \dots, B_M)$  es con respecto a  $(A_1, \dots, A_N)$  una *partición más gruesa*.

Para un grafo  $G = (V, E)$ , la *partición más fina* es aquella en la que  $|A_i| = 1$ , para todo  $i = 1, \dots, M$ . Si se unen dos de las componentes de una partición, la medida de Schmidt  $E_S$  no se incrementará, pues bajo el aumento del “grosor del grano” de la partición, sólo puede mantenerse o decrecer. Si denotamos a la medida de Schmidt de un estado dado por  $|\psi\rangle$  evaluado respecto a la partición  $(A_1, \dots, A_N)$  como  $E_S^{(A_1, \dots, A_N)}(|\psi\rangle)$ , entonces los espacios de Hilbert del sistema multipartito lo conformarán los granos de la partición. Con esta notación, la propiedad de  $E_S$  de no aumentar con respecto al aumento del grosor del grano se representa como

$$E_S^{(A_1, \dots, A_N)}(|\psi\rangle) \geq E_S^{(B_1, \dots, B_M)}(|\psi\rangle), \quad (5.12)$$

si  $(A_1, \dots, A_N) \leq (B_1, \dots, B_M)$ .

### Rango de Schmidt ( $RS$ )

Sea la bipartición  $(A, B)$ , tal que  $A \cup B = V$  y  $A \cap B = \emptyset$ , dada sobre el conjunto de vértices  $V = \{1, \dots, N\}$  de un grafo  $G = (V, E)$  caracterizado por su matriz de adyacencia  $\Gamma_{ij}$  (ver apéndice). Al tratar con biparticiones resulta muy útil etiquetar los vértices de modo que  $A = \{1, \dots, p\}$ ,  $B = \{p + 1, \dots, N\}$ . Entonces, es posible descomponer la matriz de adyacencia  $\Gamma$ , en las submatrices  $\Gamma_A$  y  $\Gamma_B$ , las cuales representan las conexiones o aristas dentro de los subconjuntos  $A$  y  $B$  respectivamente. La submatriz  $\Gamma_{AB}$  es una matriz que representa las conexiones entre las particiones  $A$  y  $B$ ,

$$\Gamma = \begin{pmatrix} \Gamma_A & \Gamma_{AB} \\ \Gamma_{AB}^T & \Gamma_B \end{pmatrix} \quad (5.13)$$

En estas condiciones, el rango de Schmidt  $RS_A(G)$  de un estado grafo  $|G\rangle$ , representado por el grafo  $G = (V, E)$ , con respecto a la bipartición  $(A, B)$  viene dado por el rango binario (i.e., rango sobre  $F(2)$ )<sup>3</sup> de la submatriz  $\Gamma_{AB}$ ,

$$RS_A(G) = \text{rang}_{F_2}(\Gamma_{AB}). \quad (5.14)$$

<sup>3</sup>Hemos asumido la notación referida al espacio vectorial binario de una sola partícula que se emplea en [2].

Las submatrices  $\Gamma_{AB}$  y  $\Gamma_{AB}^T$  poseen igual rango de Schmidt por ser la una la traspuesta de la otra, lo que denotamos como:  $RS_A(G) = RS_B(G)$ . Por otro lado, hay un total de  $2^{N-1}|^4$  formas distintas de elegir cualesquiera de las agrupaciones de una distribución bipartita ( $A$  ó  $B$ ) de los  $N$  vértices de un grafo  $G$  dado. Fijando una de ellas, se puede obtener la matriz de adyacencia  $\Gamma$ .

### Índices de rango ( $IR$ )

Dado un grafo  $G(V, E)$ , los *índices de rango* (*rank indexes*) se obtienen al calcular el  $RS_A(G)$  para todas las posibles biparticiones que se puedan realizar (para cada grupo de vértices  $A \in V$ ), y acumulando la cantidad de veces que tiene lugar un cierto rango en tuplas ordenadas. Expli- caremos este concepto más claramente con el siguiente ejemplo:

Tomamos al azar uno de los grafos que pertenecen a la clasificación de los estados grafo de ocho qubits de las tablas 5.1, 5.2 y 5.3.

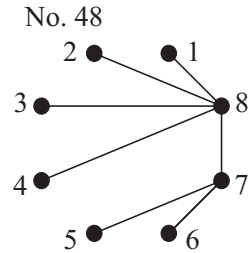


Figura 5.1: Grafo No. 48 de la clasificación de los estados grafo de ocho qubits.

Realizamos una distribución bipartita de los vértices de este grafo, por ejemplo:  $(\{1, 2, 3, 4, 5, 6\}, \{7, 8\}) = \{A, B\}$ . Y a continuación, para obtener una mejor visión de las submatrices  $\Gamma_A$ ,  $\Gamma_B$  y  $\Gamma_{AB}$  que constituirán la matriz de adyacencia  $\Gamma$  del grafo No. 48, reordenamos las filas y columnas de  $\Gamma$  de forma que las numeradas como 7 y 8 se sitúen en primer lugar

$$\begin{pmatrix} (7) & (8) & (1) & (2) & (3) & (4) & (5) & (6) \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & (7) \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & (8) \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & (1) \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & (2) \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & (3) \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & (4) \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & (5) \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & (6) \end{pmatrix} \quad (5.15)$$

<sup>4</sup>Dado el conjunto  $V$  de vértices, se pueden formar en total  $2^N$  distribuciones bipartitas donde cada bipartición  $(A, B)$  es tal que  $|B| = V - |A|$ , pero si eliminamos aquella distribución en la que una de las agrupaciones sea  $V$  y la otra el conjunto vacío (lo que se logra con la operación  $2^N/2$ ) entonces tenemos como resultado  $2^{N-1}$  biparticiones.

Consideremos la submatriz de dimensión  $|A| \times |B|$  (con  $|A|$  y  $|B|$  denotamos los cardinales de los conjuntos  $A$  y  $B$ ) asociada a las aristas que conectan  $A$  y  $B$ .

$$\Gamma_{AB}(G48) = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \quad (5.16)$$

Si deseamos obtener el índice de rango-2 ó  $IR_2$  (índice de rango de orden 2), entonces calculamos el rango binario de la submatriz  $\Gamma_{AB}(G48)$ , es decir,  $RS_A(G48)$ ; y repetimos este mismo procedimiento para todas las distribuciones bipartitas (donde  $A$  englobe sólo dos vértices) que podamos construir para el mismo grafo. Tras el recuento de los resultados obtenidos, el índice de rango-2 se escribe de forma comprimida mediante la tupla  $(D, U)$ , donde  $D$  es el número de veces en que aparece el resultado 2, y  $U$  indica el número de veces que se obtiene el resultado 1.

Los  $IR_3$  y  $IR_4$  se obtienen repitiendo este procedimiento iterativamente para los casos en los que  $A$  posea 3 y 4 vértices, respectivamente. Las tuplas correspondientes serán  $IR_3(G48) = (T, D, U)$  y  $IR_4(G48) = (C, T, D, U)$ , donde  $T$  indica las veces que se ha obtenido  $RS_A(G48) = 3$  y  $C$  las veces que se ha obtenido  $RS_A(G48) = 4$ .

En general, los índices de rango para todas las distribuciones bipartitas donde la parte más pequeña  $A$  contenga  $p$  vértices, vienen dados por la  $p$ -tupla

$$IR_p = (\nu_p^p, \dots, \nu_1^p) = [\nu_j^p]_{j=p}^1, \quad (5.17)$$

donde  $\nu_j^p$  es el número de veces que resulta  $RS_A(G) = j$ , con  $|A| = p$ .

## 5.5. Procedimientos y resultados

Los resultados de nuestro trabajo los mostramos en la Fig. 5.3 y en las tablas 5.1, 5.2 y 5.3. A continuación proporcionaremos los detalles que nos condujeron a estos resultados.

### 5.5.1. Órbitas bajo complementación local

Hemos generado todas las órbitas LC para  $n = 8$  y hemos calculado en número de grafos no isomorfos<sup>5</sup> en cada órbita. Hemos identificado los representantes con el mínimo número de aristas  $|E|$  y de entre ellos hemos elegido a aquel que se caracterizaba por poseer el mínimo grado máximo. La razón de escoger precisamente este tipo de grafos como representante óptimo de un órbita radica en que, de esta manera, el estado grafo asociado requiere del mínimo número de puertas  $C_Z$  para su preparación y, como consecuencia, de una mínima profundidad de preparación<sup>6</sup> [165]. Todos los representantes óptimos de cada una de las 101 clases de equivalencia u

<sup>5</sup>En teoría de grafos, dos grafos dados,  $G$  y  $H$  son isomorfos si existe una biyección  $f, f : V(G) \rightarrow V(H)$  entre los conjuntos de sus vértices que conserva la relación de adyacencia. Es decir, cualquier par de vértices  $u$  y  $v$  de  $G$  son adyacentes si y sólo si lo son sus imágenes,  $f(u)$  y  $f(v)$  en  $H$ .

<sup>6</sup>La profundidad de preparación es el mínimo número de pasos de tiempo que se necesitan para preparar un estado. Cuando la profundidad de preparación, referida a una órbita LC, es mínima, entonces el número de etapas que se invierte en preparar el estado es el más corto de la órbita. Una mínima profundidad de preparación en los estados grafo, provee al estado de una protección contra la decoherencia pues se reduce el tiempo en que va a ver sometido al contacto con el medio exterior.

órbitas están representados en la Fig. 5.3, y en las tablas 5.1, 5.2 y 5.3 están recogidos los datos para  $|LC|$  (i.e., cardinal de la órbita LC) y  $|E|$ .

### 5.5.2. Límites de la medida de Schmidt

La medida de Schmidt  $E_S$  se calcula a partir del mínimo número de términos  $R$  en que se puede descomponer un estado (ver (5.9)). Para un estado general, la dificultad del cálculo de  $E_S$  escala exponencialmente con el número de partes  $N$ , así como con el grado de entrelazamiento que exista entre ellas. HEB solventaron el problema para los estados grafo aportando una forma de obtener los límites superior e inferior de la medida de Schmidt. Estos límites de la medida de Schmidt son fáciles de calcular y en muchos casos coinciden, lo que determina el valor de  $E_S$ . Veamos cuáles son las cotas de  $E_S$ .

#### Persistencia de Pauli y tamaño del recubrimiento de vértices mínimo

Para cualquier estado grafo, los límites superiores de su medida de Schmidt  $E_S(|G\rangle)$  son la *persistencia de Pauli* (*Pauli persistency*)  $PP(G)$  y el tamaño del recubrimiento de vértices mínimo  $RV(G)$ ,

$$E_S(|G\rangle) \leq PP(G) \leq RV(G). \quad (5.18)$$

La persistencia de Pauli es el mínimo número de medidas locales de Pauli que es preciso realizar para desentrelazar un estado grafo determinado. HEB describieron unas reglas de transformación gráfica asociadas que muestran el efecto que tiene sobre el grafo la aplicación de las distintas medidas locales de Pauli [1, 2].

El *recubrimiento de vértices* (*vertex cover*) es un concepto de teoría de grafos, y se refiere a cualquier conjunto de vértices  $V'$  de un grafo  $G$  en el que incidan el conjunto total de las aristas del grafo. El recubrimiento de vértices será mínimo, si se logra con un mínimo número de vértices. En la Fig. 5.2, mostramos dos tipos de recubrimientos para el grafo No. 59 de nuestra clasificación, el de la izquierda es mínimo y el de la derecha no.

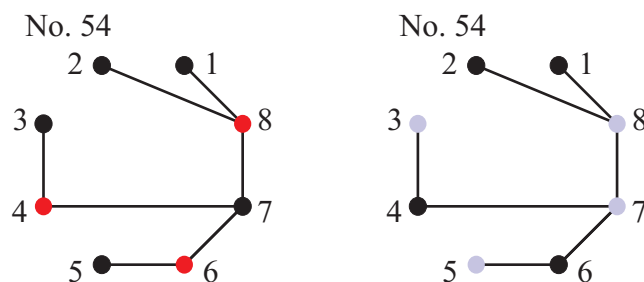


Figura 5.2: Vemos representado dos recubrimientos de vértices distintos para el grafo No. 59 de nuestra clasificación. El conjunto de vértices 4, 6 y 8 de la figura de la izquierda conforma el recubrimiento de vértices mínimo del grafo, mientras que el recubrimiento de la figura de la izquierda dado por los vértices 3, 5, 7 y 8, no es el mínimo.

De acuerdo con las reglas gráficas para las medidas de Pauli, dado que cada medida  $\sigma_z$  elimina todas las aristas incidentes en un vértice,  $VC(G)$  podría coincidir con  $PP(G)$  si nos restringimos a realizar sólo este tipo de medidas. Sin embargo, en grafos con muchas aristas puede que lo más adecuado sea realizar una combinación de medidas  $\sigma_x$ ,  $\sigma_y$  y  $\sigma_z$  que proporcione una secuencia de desentrelazamiento más eficiente, obteniéndose así un mejor límite inferior  $PP(G)$  para la medida de Schmidt.

### Rango de Schmidt maximal $RS_{max}$

Para cualquier estado grafo  $|G\rangle$ , el límite inferior de la medida de Schmidt  $E_S(|G\rangle)$  es el *rango de Schmidt maximal* (*maximal Schmidt rank*),

$$RS_{max}(G) \leq E_S(|G\rangle). \quad (5.19)$$

El rango de Schmidt maximal es el límite inferior de la medida de Schmidt con respecto la partición más fina. Esta información se extrae del máximo rango de Schmidt que resulta tras calcularlo para todas las posibles biparticiones de un grafo dado  $G = (V, E)$ ,

$$RS_{max}(G) := \max_{A \subseteq V} RS_A(G). \quad (5.20)$$

De acuerdo con la definición de rango de Schmidt, el rango de Schmidt maximal para cualquier estado es a lo sumo el mayor entero menor o igual que  $\frac{N}{2}$ .

### Añadir o eliminar aristas y vértices

La complementación local sobre grafos no modifica la medida de Schmidt de los estados grafos asociados. Este hecho facilita enormemente el cálculo de la medida de Schmidt asociada a una determinada órbita pues es posible elegir el grafo más adecuado para su obtención. Sin embargo, no todas las acciones locales que se realizan sobre los grafos dejan invariante la medida de Schmidt, pero en contra de lo que pudiera parecer esto puede convertirse en una situación ventajosa para resolver algunos casos en los que el cálculo de  $E_S$  sea más dificultoso. Tal es el caso de la *regla de los vértices/aristas* [1, 2]. De acuerdo con esta regla, por una parte, mediante la adición o eliminación de una arista  $e$  que conecta a dos vértices del grafo  $G$  la medida de Schmidt del grafo resultante  $G'$  ( $G' = G \pm e$ ) puede a lo sumo crecer o decrecer una unidad. Por otra parte, si un vértice  $v$  (incluyendo sus aristas incidentes) se elimina, la medida de Schmidt del grafo resultante  $G'$  ( $G' = G - v$ ) no puede incrementarse, sino que a lo sumo decrecerá en una unidad. Si  $E_S(|G + e\rangle)$  es la medida de Schmidt del estado grafo correspondiente al grafo  $G + e$ , entonces las reglas anteriores pueden resumirse según las siguientes expresiones

$$E_S(|G + e\rangle) \leq E_S(|G\rangle) + 1, \quad (5.21a)$$

$$E_S(|G - e\rangle) \geq E_S(|G\rangle) - 1, \quad (5.21b)$$

$$E_S(|G - v\rangle) \geq E_S(|G\rangle) - 1. \quad (5.21c)$$

En este trabajo hemos empleado estas reglas de dos formas distintas:



1. En primer lugar, como un test interno para comprobar nuestros cálculos, comparando pares de grafos relacionados mediante una secuencia de eliminaciones de aristas/vértices.

2. Y en segundo lugar, como una útil herramienta para encontrar alguna cota de la medida de Schmidt en algunos grafos problemáticos. La forma de proceder en estos casos es la siguiente: se compara el grafo problemático  $G$  con  $G'$ , que es aquel que resulta de eliminar alguna arista o vértice y que posea una medida de Schmidt conocida.

### Medidas de Schmidt para algunos tipos especiales de grafos

Hay algunos estados grafo para los cuales los límites superior e inferior de las medidas de Schmidt coinciden, proporcionando directamente el valor de  $E_S$ . Dado que el rango de Schmidt maximal para cualquier estado puede ser a lo sumo  $\lfloor \frac{N}{2} \rfloor$ , para aquellos estados en los que los límites superior e inferior de  $E_S$  coinciden se satisface que  $RS_{max}(G) = E_S(|G\rangle) = PP(G) = RV(G) \leq \lfloor \frac{N}{2} \rfloor$ . Entre los estados grafo que satisfacen esta condición están los GHZ, los estados representados por árboles, los anillos con un número par de vértices, y los clusters. En nuestro trabajo hemos usado los siguientes resultados en relación a los estados GHZ y los árboles:

1. La medida de Schmidt para cualquier estado GHZ multipartito es 1.

2. Un árbol  $T$  es un grafo que no tiene ciclos. La medida de Schmidt del estado grafo correspondiente  $|T\rangle$  es el tamaño del recubrimiento de vértices mínimo:  $E_S(|T\rangle) = RV(T)$ .

Hay otra clase interesante de estados grafo para nuestros propósitos, son los llamados *grafos bicoloreables* (*2-colorable graphs*). Un bicoloreado propio es un etiquetado sobre el conjunto de vértices de un grafo  $G = (V, E)$ , dado por la función  $V \rightarrow \{1, 2\}$ , tal que los vértices han de etiquetarse de forma que ningún vértice adyacente comparta la misma etiqueta. Las etiquetas pueden ser identificadas con colores, y dado que hay dos, si el grafo admite el etiquetado que acabamos de describir, entonces es bicoloreable. Otra denominación empleada por los matemáticos para referirse a los grafos bicoloreables es la de grafos bipartitos. Un grafo es *bipartito*, si el conjunto (de la totalidad) de los vértices se pueden distribuir entre dos conjuntos disjuntos  $A$  y  $B$ , tales que ningún vértice esté conectado a otro que se encuentre en el mismo subconjunto al que él pertenece (las aristas conectan a pares de vértices donde uno de ellos pertenece a  $A$  y el otro a  $B$ ).

Para este tipo de grafos, HEB [1, 2] proporcionaron límites superiores e inferiores de la medida de Schmidt dados por la expresión

$$\frac{1}{2} \text{rang}_{F_2} \leq E_S(|G\rangle) \leq \lfloor \frac{|V|}{2} \rfloor, \quad (5.22)$$

donde  $\Gamma$  es la matriz de adyacencia del grafo bicoloreable. Si  $\Gamma$  es invertible, entonces

$$E_S(|G\rangle) = \lfloor \frac{|V|}{2} \rfloor. \quad (5.23)$$

Cualquier grafo  $G$  que no sea bicoloreable, se puede transformar en otro que sea bicoloreable  $G'$  con sólo eliminar los vértices apropiados de los ciclos con longitud impar presentes en  $G$ . La

eliminación de vértices en grafos, se realiza a través del proyector de la matriz de Pauli  $\sigma_z$  y da lugar a nuevos límites superiores de  $E_S(|G\rangle)$ :

$$E_S(|G\rangle) \leq E_S(|G'\rangle) + M \leq \lfloor \frac{|V - M|}{2} \rfloor + M \leq \lfloor \frac{|V| + M}{2} \rfloor, \quad (5.24)$$

donde  $M$  es el número de vértices eliminados. En este trabajo, hemos usado estos nuevos límites en algunos grafos como herramientas para comprobar nuestros cálculos.

Tabla 5.1: Clasificación del entrelazamiento de las 101 clases de estados grafos de 8 qubits. No. es el número de la clase. Las diferentes columnas,  $|E|$ ,  $E_S$ ,  $IR_j$  y  $|LC|$ , las hemos elegido en base a las Refs. [1, 2].  $|E|$  es el número de aristas de aquellos representantes que posean un mínimo número de aristas.  $E_S$  es la medida de Schmidt (o sus límites inferior y superior).  $IR_j$  son los índices de rango, donde  $j$  indica el número de qubits en la parte de menor tamaño de una bipartición (los rangos aparecen en orden decreciente).  $|LC|$  es el número de elementos no isomorfos de la clase. La última columna indica si en la clase LC hay algún grafo bicolorable.

No.	$ LC $	$ E $	$E_S$	$IR_4$	$IR_3$	$IR_2$	bicolorable
46	2	7	1	(0,0,0,35)	(0,0,56)	(0,28)	yes
47	6	7	2	(0,0,20,15)	(0,30,26)	(12,16)	yes
48	6	7	2	(0,0,30,5)	(0,45,11)	(15,13)	yes
49	16	7	2	(0,0,30,5)	(0,45,11)	(17,11)	yes
50	4	7	2	(0,0,34,1)	(0,48,8)	(16,12)	yes
51	16	7	2	(0,0,34,1)	(0,51,5)	(19,9)	yes
52	10	7	3	(0,12,16,7)	(16,28,12)	(20,8)	yes
53	16	7	3	(0,12,22,1)	(16,34,6)	(20,8)	yes
54	44	7	3	(0,12,22,1)	(16,35,5)	(21,7)	yes
55	16	7	3	(0,18,14,3)	(18,33,5)	(21,7)	yes
56	44	7	3	(0,18,14,3)	(22,29,5)	(23,5)	yes
57	10	7	3	(0,18,15,2)	(18,36,2)	(21,7)	yes
58	25	7	3	(0,18,16,1)	(18,36,2)	(22,6)	yes
59	44	7	3	(0,18,16,1)	(22,31,3)	(23,5)	yes
60	44	7	3	(0,24,9,2)	(24,30,2)	(23,5)	yes
61	26	7	3	(0,24,10,1)	(28,25,3)	(23,5)	yes
62	120	7	3	(0,24,10,1)	(28,26,2)	(24,4)	yes
63	66	7	3	(0,26,7,2)	(30,24,2)	(25,3)	yes
64	14	7	4	(8,12,12,3)	(32,18,6)	(24,4)	yes
65	25	7	4	(8,12,14,1)	(32,20,4)	(24,4)	yes
66	120	7	4	(8,14,12,1)	(34,19,3)	(25,3)	yes
67	72	7	4	(8,16,10,1)	(36,17,3)	(25,3)	yes
68	172	7	4	(8,18,8,1)	(38,16,2)	(26,2)	yes
69	10	8	2	(0,0,34,1)	(0,52,4)	(20,8)	yes
70	10	8	2	(0,0,35,0)	(0,54,2)	(21,7)	yes
71	10	8	3	(0,12,22,1)	(16,36,4)	(20,8)	no
72	21	8	3	(0,12,22,1)	(16,36,4)	(22,6)	no
73	10	8	3	(0,18,17,0)	(18,36,2)	(21,7)	no
74	44	8	3	(0,18,17,0)	(22,32,2)	(23,5)	yes
75	66	8	3	(0,18,17,0)	(22,33,1)	(24,4)	no
76	26	8	3	(0,20,14,1)	(24,30,2)	(24,4)	yes
77	26	8	3	(0,24,10,1)	(24,31,1)	(23,5)	yes
78	28	8	3	(0,24,10,1)	(28,27,1)	(23,5)	no
79	44	8	3	(0,24,11,0)	(28,26,2)	(23,5)	no

Tabla 5.2: Clasificación del entrelazamiento de las 101 clases de estados grafos de 8 qubits. No. es el número de la clase. Las diferentes columnas,  $|E|$ ,  $E_S$ ,  $IR_j$  y  $|LC|$ , las hemos elegido en base a las Refs. [1, 2].  $|E|$  es el número de aristas de aquellos representantes que posean un mínimo número de aristas.  $E_S$  es la medida de Schmidt (o sus límites inferior y superior).  $IR_j$  son los índices de rango, donde  $j$  indica el número de qubits en la parte de menor tamaño de una bipartición (los rangos aparecen en orden decreciente).  $|LC|$  es el número de elementos no isomorfos de la clase. La última columna indica si en la clase LC hay algún grafo bicoloreable.

No.	$ LC $	$ E $	$E_S$	$IR_4$	$IR_3$	$IR_2$	bicoloreable
80	132	8	3	(0,24,11,0)	(28,27,1)	(24,4)	no
81	114	8	3	(0,24,11,0)	(30,25,1)	(25,3)	yes
82	72	8	3	(0,26,9,0)	(30,26,0)	(25,3)	no
83	72	8	3	(0,28,6,1)	(32,23,1)	(25,3)	yes
84	198	8	3	(0,28,7,0)	(34,22,0)	(26,2)	yes
85	56	8	$3 < 4$	(0,30,4,1)	(34,21,1)	(25,3)	no
86	28	8	4	(8,16,10,1)	(32,22,2)	(24,4)	no
87	10	8	4	(8,16,10,1)	(32,24,0)	(24,4)	yes
88	56	8	4	(8,16,10,1)	(36,18,2)	(26,2)	no
89	66	8	4	(8,16,11,0)	(36,18,2)	(25,3)	yes
90	72	8	4	(8,18,9,0)	(34,22,0)	(25,3)	no
91	63	8	4	(8,18,9,0)	(36,20,0)	(26,2)	yes
92	66	8	4	(8,18,9,0)	(38,16,2)	(25,3)	no
93	176	8	4	(8,18,9,0)	(38,17,1)	(26,2)	no
94	76	8	4	(8,20,6,1)	(36,19,1)	(25,3)	no
95	194	8	4	(8,20,7,0)	(38,18,0)	(26,2)	yes
96	352	8	4	(8,20,7,0)	(40,15,1)	(26,2)	no
97	154	8	4	(8,22,4,1)	(42,13,1)	(27,1)	no
98	542	8	4	(8,22,5,0)	(42,14,0)	(27,1)	no
99	300	8	4	(12,16,7,0)	(44,11,1)	(27,1)	yes
100	214	8	4	(14,17,4,0)	(48,8,0)	(28,0)	yes
101	14	9	3	(0,20,15,0)	(24,32,0)	(25,3)	no
102	66	9	3	(0,28,7,0)	(32,24,0)	(25,3)	no
103	66	9	3	(0,30,5,0)	(36,20,0)	(26,2)	yes
104	6	9	3	(0,32,0,3)	(32,24,0)	(24,4)	yes
105	57	9	$3 < 4$	(0,30,5,0)	(36,19,1)	(25,3)	no
106	28	9	4	(8,18,9,0)	(38,18,0)	(25,3)	no
107	17	9	4	(8,20,6,1)	(32,24,0)	(24,4)	no
108	72	9	4	(8,20,7,0)	(36,20,0)	(25,3)	no
109	87	9	4	(8,20,7,0)	(40,16,0)	(27,1)	no
110	114	9	4	(8,22,5,0)	(40,16,0)	(26,2)	no
111	372	9	4	(8,22,5,0)	(40,16,0)	(26,2)	no
112	70	9	4	(8,24,2,1)	(40,16,0)	(26,2)	no
113	264	9	4	(8,24,3,0)	(44,12,0)	(27,1)	no
114	542	9	4	(8,24,3,0)	(44,12,0)	(27,1)	no
115	156	9	4	(12,18,5,0)	(46,9,1)	(27,1)	no
116	174	9	4	(12,20,3,0)	(46,10,0)	(27,1)	no

Tabla 5.3: Clasificación del entrelazamiento de las 101 clases de estados grafos de 8 qubits. No. es el número de la clase. Las diferentes columnas,  $|E|$ ,  $E_S$ ,  $IR_j$  y  $|LC|$ , las hemos elegido en base a las Refs. [1, 2].  $|E|$  es el número de aristas de aquellos representantes que posean un mínimo número de aristas.  $E_S$  es la medida de Schmidt (o sus límites inferior y superior).  $IR_j$  son los índices de rango, donde  $j$  indica el número de qubits en la parte de menor tamaño de una bipartición (los rangos aparecen en orden decreciente).  $|LC|$  es el número de elementos no isomorfos de la clase. La última columna indica si en la clase LC hay algún grafo bicolorable.

No.	$ LC $	$ E $	$E_S$	$IR_4$	$IR_3$	$IR_2$	bicolorable
117	542	9	4	(12,20,3,0)	(46,10,0)	(27,1)	no
118	262	9	4	(12,20,3,0)	(48,8,0)	(28,0)	no
119	802	9	4	(14,19,2,0)	(50,6,0)	(28,0)	no
120	117	9	4	(16,16,3,0)	(50,6,0)	(28,0)	yes
121	10	10	3	(0,32,2,1)	(32,24,0)	(24,4)	no
122	37	10	3	(0,32,3,0)	(40,16,0)	(27,1)	yes
123	36	10	4	(8,22,5,0)	(44,12,0)	(26,2)	no
124	7	10	4	(8,24,0,3)	(32,24,0)	(24,4)	no
125	103	10	4	(8,24,3,0)	(42,14,0)	(26,2)	no
126	46	10	4	(8,24,3,0)	(44,12,0)	(27,1)	no
127	170	10	4	(8,26,1,0)	(46,10,0)	(27,1)	no
128	74	10	4	(12,20,3,0)	(46,10,0)	(27,1)	yes
129	340	10	4	(12,22,1,0)	(48,8,0)	(27,1)	no
130	254	10	4	(12,22,1,0)	(50,6,0)	(28,0)	no
131	433	10	4	(14,21,0,0)	(52,4,0)	(28,0)	no
132	476	10	4	(16,18,1,0)	(52,4,0)	(28,0)	no
133	28	10	$4 < 5$	(12,22,0,1)	(48,8,0)	(28,0)	no
134	9	11	$3 < 4$	(0,30,5,0)	(40,15,1)	(25,3)	no
135	39	11	4	(8,26,1,0)	(44,12,0)	(26,2)	no
136	46	11	4	(12,20,3,0)	(50,6,0)	(27,1)	no
137	208	11	$4 < 5$	(16,18,1,0)	(52,4,0)	(28,0)	no
138	298	11	$4 < 5$	(18,17,0,0)	(54,2,0)	(28,0)	no
139	24	11	$4 < 5$	(20,10,5,0)	(50,5,1)	(27,1)	no
140	267	11	$4 < 5$	(20,14,1,0)	(54,2,0)	(28,0)	no
141	4	12	4	(28,0,7,0)	(56,0,0)	(28,0)	no
142	22	12	$4 < 5$	(14,21,0,0)	(56,0,0)	(28,0)	no
143	46	12	$4 < 5$	(20,12,3,0)	(50,6,0)	(27,1)	yes
144	28	13	4	(28,4,3,0)	(56,0,0)	(28,0)	no
145	7	13	$4 < 5$	(16,18,1,0)	(56,0,0)	(28,0)	no
146	51	13	$4 < 5$	(24,10,1,0)	(56,0,0)	(28,0)	no

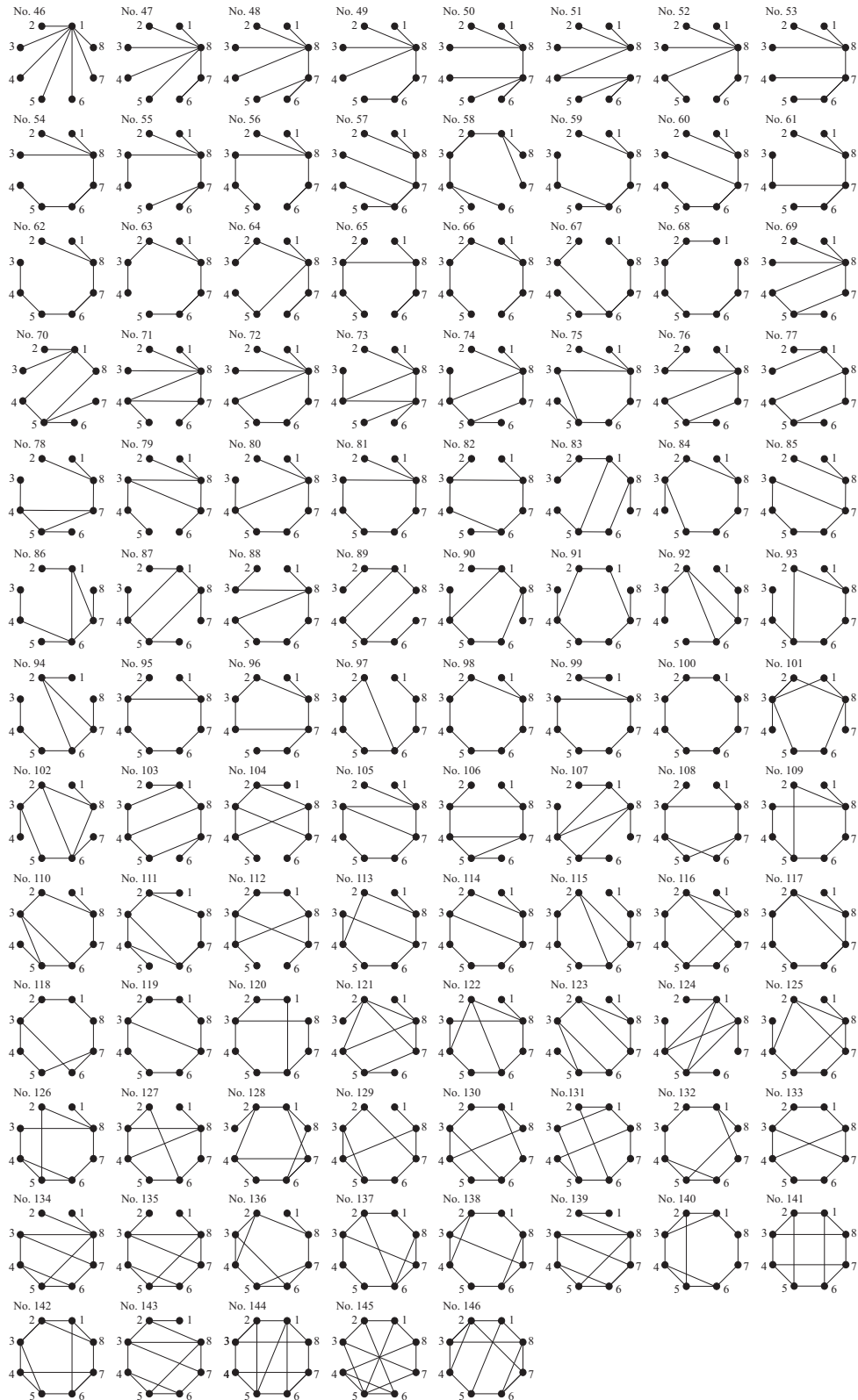


Figura 5.3: Grafos asociados a las 101 clases de estados grafo no equivalentes bajo complementación local e isomorfismo de grafos. Figura tomada de la Ref. [21].

## Capítulo 6

# Conjunto compacto de invariantes que caracterizan los estados grafo de hasta ocho qubits

### 6.1. Introducción

Como vimos en capítulos anteriores, los estados grafo [1, 2] son fundamentales en Información Cuántica, especialmente en corrección cuántica de errores [4, 5, 61] y en computación cuántica basada en medidas [6]. En el capítulo anterior, comprobamos que los estados grafo también juegan un papel fundamental en el estudio del entrelazamiento.

En el capítulo 4, introdujimos la clasificación de los estados entrelazados de hasta  $n = 4$  qubits, como paso previo al estudio de la clasificación de los estados grafo de hasta  $n = 8$  qubits. En total, para  $n = 3$  hay seis clases de estados equivalentes bajo SLOCC (operaciones locales estocásticas asistidas por comunicación clásica) [33] y sólo uno de ellos admiten una representación en forma de grafo. Para  $n \geq 4$  el número de clases equivalentes bajo SLOCC es infinita pues la cantidad de parámetros que las caracterizan crece exponencialmente con el número de qubits.

De entre todos los tipos diferentes de estados entrelazados, nos centraremos concretamente en los estados grafo. Dos estados cuánticos tienen el mismo entrelazamiento si son equivalentes bajo operaciones SLOCC (capítulo 4), y dos estados grafo que son equivalentes bajo SLOCC también lo son bajo operaciones LU (transformaciones locales unitarias). La conjetura  $LU \Leftrightarrow LC$  (operaciones locales de Clifford) establece que los estados estabilizadores que son equivalentes LU, deben ser también equivalentes bajo LC, sin embargo, Ji *et al.* demostraron que tal conjetura es falsa [37]. Realmente, para los estados grafo la equivalencia  $LU \Leftrightarrow LC$  es cierta en los casos más simples [38, 39], apareciendo los primeros contraejemplos para los estados con  $n = 27$  qubits [37].

En este capítulo desarrollaremos principalmente el contenido del artículo citado en la Ref. [22], que constituye una contribución original al dominio de este trabajo. Principalmente, nuestra

tarea consistió en encontrar un conjunto compacto de invariantes que se pudiera emplear para distinguir entre las clases de equivalencia que eran indistinguibles cuando se caracterizaban a través de los invariantes de HEB (Hein, Eisert y Briegel) (capítulo 5). Estos estados grafo son a lo sumo de 8 qubits, por lo que la conjetura  $LU \Leftrightarrow LC$  es válida (a falta de contraejemplos conocidos para  $n < 27$ ).

HEB clasificaron el entrelazamiento de los estados grafo de hasta  $n = 7$  qubits [1, 2], y recientemente su método de clasificación se ha extendido hasta  $n = 8$  qubits [21]. Los criterios para ordenar las clases que se han seguido en las Refs. [1, 2, 21] están basados en varias medidas de entrelazamiento: medida de Schmidt para las distribuciones  $n$ -partitas  $E_S$  (la cual mide el genuino entrelazamiento  $n$ -partito de las clases [163]), y los rangos de Schmidt para todas las distribuciones bipartitas (acumulados en índices de rango,  $IR$  [1, 2]). Además se han añadido otros datos que arrojan información de la órbita y del representante óptimo de la misma, como el número de elementos en una órbita  $|LC|$  y el número de aristas  $|E|$  del representante óptimo (aquel que posee el mínimo número de aristas). Con este método, no es posible distinguir entre las clases 40, 42 y 43, que corresponden a grafos de 7 qubits; y tampoco entre las clases 110 y 111, 113 y 114, y entre las 116 y 117, que son representadas por grafos de 8 qubits (capítulo 5).

Van den Nest, Dehaene y De Moor (VDD) propusieron un conjunto finito de invariantes que caracterizaban todas las clases [166]. Sin embargo, ya para  $n = 7$ , este conjunto poseía más de  $2 \times 10^{36}$  invariantes que no están explícitamente calculados, y por este motivo no resultan útiles para resolver el problema. Por otro lado VDD creen que este conjunto de invariantes puede ser mejorado, si no para todos los estados estabilizadores, al menos para algunas subclases de estados. Es más, ellos establecen que es probable que sólo sean necesarios algunos invariantes para reconocer una clase equivalente bajo LC y que no es improbable que exista una lista completa más pequeña de invariantes que exhiba menos redundancia. En este capítulo mostramos que, si  $n \leq 8$ , entonces es suficiente con cuatro invariantes para reconocer una clase LC determinada de estados grafo.

Este capítulo se organiza de la siguiente manera: En la sección 6.2 introducimos algunos resultados acerca de los invariantes propuestos por VDD, y en la sección 6.3 presentamos nuestros resultados.

## 6.2. Invariantes de Van den Nest, Dehaene y De Moor

Es preciso introducir previamente algunos conceptos que nos permitan entender el argumento principal de esta sección.

*Soportes.* Sea  $|\psi\rangle$  un estado estabilizador y  $S(|\psi\rangle)$  el correspondiente estabilizador. Dado un operador estabilizador  $s_i = \alpha_i M_1^{(i)} \otimes \cdots \otimes M_n^{(i)}$ , donde los  $M_i^{(i)}$  pueden representar matrices de Pauli o la matriz identidad, su soporte,  $\text{supp}(s_i)$ , es el conjunto de todas las etiquetas de los qubits  $j \in \{1, \dots, n\}$ , sin incluir aquellas que indiquen posiciones de las matrices identidad en el operador estabilizador. El soporte se conserva bajo complementación local, porque estas operaciones no tienen el poder de intercambiar los qubits de sus lugares, y por otro lado transforman el grupo local de Pauli en sí mismo, preservando la identidad (capítulo 1). El soporte de un



operador estabilizador se suele denotar como  $\text{supp}(s_i)=\omega$ . El *peso de un soporte* es su cardinal el cual se representa por  $|\omega|$ . Como ejemplo para ilustrar cómo se obtienen los soportes de un estado grafo, tomaremos el estado grafo  $|LC_3\rangle$  representado por la Fig. 6.1.



Figura 6.1: Grafo  $LC_3$  asociado al estado grafo  $|LC_3\rangle$ .

$$s_1 = g_1 = X_1 \otimes Z_2 \otimes I_3, \quad \{1, 2\}, \quad |\{1, 2\}| = 2, \quad (6.1a)$$

$$s_2 = g_2 = Z_1 \otimes X_2 \otimes Z_3, \quad \{1, 2, 3\}, \quad |\{1, 2, 3\}| = 3, \quad (6.1b)$$

$$s_3 = g_3 = I_1 \otimes Z_2 \otimes X_3, \quad \{2, 3\}, \quad |\{2, 3\}| = 2, \quad (6.1c)$$

$$s_4 = g_{11} = I_1 \otimes I_2 \otimes I_3, \quad \{\emptyset\}, \quad |\{\emptyset\}| = 0, \quad (6.1d)$$

$$s_5 = g_{12} = Y_1 \otimes Y_2 \otimes Z_3, \quad \{1, 2, 3\}, \quad |\{1, 2, 3\}| = 3, \quad (6.1e)$$

$$s_6 = g_{13} = X_1 \otimes I_2 \otimes X_3, \quad \{1, 3\}, \quad |\{1, 3\}| = 2, \quad (6.1f)$$

$$s_7 = g_{23} = Z_1 \otimes Y_2 \otimes Y_3, \quad \{1, 2, 3\}, \quad |\{1, 2, 3\}| = 3, \quad (6.1g)$$

$$s_8 = g_{123} = -Y_1 \otimes X_2 \otimes Y_3, \quad \{1, 2, 3\}, \quad |\{1, 2, 3\}| = 3. \quad (6.1h)$$

Hemos expresado cada operador del estabilizador del estado  $|LC_3\rangle$  en función de sus operadores generadores (empleando la notación reducida del capítulo 1 para el producto matricial entre operadores generadores) , y junto a cada uno de ellos hemos agregado el soporte correspondiente y junto con su cardinal.

*Invariantes relacionados con los soportes.* El conjunto de operadores  $\{s_i\}_{i=1}^{2^k}$  de un estabilizador  $S$  se puede clasificar en clases de equivalencia, denotadas por  $[\omega]$ , atendiendo a sus soportes. Dos operadores  $s_i$  y  $s_j$  de un mismo estabilizador pertenecen a la misma clase de equivalencia  $[\omega]$  si tienen el mismo soporte. Denotaremos por  $A_\omega(|\psi\rangle)$  al número de operadores estabilizadores  $s_i \in S(|\psi\rangle)$  con  $\text{supp}(s_i)=\omega$ , luego  $A_\omega(|\psi\rangle)$  es el cardinal de la clase de equivalencia  $[\omega]$  en un estabilizador  $S$ . Cualquier estado grafo  $|G\rangle$  es un estado estabilizador, por lo que todas estas definiciones se le pueden aplicar igualmente. Los soportes no aportan información de los operadores locales que conforman los  $s_i$ , sólo de cuántos lugares ocupados por aquellos son distintos de la identidad. El conjunto complementario de cada uno de los soportes informa acerca de la identidades locales en cada  $s_i \in S$ . El teorema clave que proporcionan VDD en la Ref. [166] aporta un conjunto finito de invariantes que caracterizan las clases de equivalencia LC para los estados estabilizadores. Este será el teorema que presentaremos a continuación, aunque para facilitar su comprensión, no utilizaremos la notación binaria empleada por VDD.

**Teorema.** Sea  $|\psi\rangle$  el estado estabilizador de  $n$  qubits correspondiente al estabilizador  $S_{|\psi\rangle}$ . Sea  $r \in \mathbb{N}_0$  y consideremos los subconjuntos  $\omega_k, \omega_{kl} \subseteq \{1, \dots, n\}$  para todo  $k, l \in \{1, \dots, r\}$  con  $k < l$ . Denotemos por  $\Omega := (\omega_1, \omega_2, \dots, \omega_{12}, \omega_{13}, \dots)$  y sea  $\mathcal{T}_{n,r}^\Omega(|\psi\rangle)$  el conjunto de todas las tuplas  $(s_1, \dots, s_r) \in S_{|\psi\rangle} \times \dots \times S_{|\psi\rangle}$  que satisfacen

$$\text{supp}(s_k) = \omega_k, \quad \text{supp}(s_k s_l) = \omega_{kl}. \quad (6.2)$$

Entonces se tiene que: (i)  $|\mathcal{T}_{n,r}^{\Omega}(|\psi\rangle)|$  es invariante LC, (ii) la clase de equivalencia LC de  $|\psi\rangle$  está completamente determinada por los valores de todos los invariantes  $|\mathcal{T}_{n,n}^{\Omega}(|\psi\rangle)|$ .

En otras palabras, los invariantes que proporcionan VDD a través de este teorema se refieren a los cardinales de los conjuntos  $\mathcal{T}_{n,r}^{\Omega}(|\psi\rangle)$ , que no son más que aquellos conjuntos formados por los operadores estabilizadores  $s_i$ , cuyos soportes cumplen las restricciones 6.2, para cada  $r$ . En el caso particular de  $r = 1$ , los invariantes coinciden con los cardinales  $A_{\omega_k}(|\psi\rangle)$  de cada una de las clases de equivalencia  $[\omega_k]$ ,

$$|\{s \in S_{|\psi}\} | \text{supp}(s) = \omega_k \}|. \quad (6.3)$$

Para  $r = 1$ ,  $\Omega = (\omega_1)$  indica todas las posibles formas de escoger un único soporte. El número de posibles soportes es  $2^n$  para  $r = 1$ , pero no todos los  $A_{\omega_k}(|\psi\rangle)$  tienen por qué ser distintos de cero, eso dependerá del estabilizador asociado al estado de  $n$  qubits, de hecho para los estados grafo, la clase de equivalencia  $[\omega_k]$  en la que  $|\omega_k| = 1$  no es ocupada por ningún operador estabilizador, luego  $A_{\omega_k}(|\psi\rangle) = 0$ . Este resultado se debe a que  $|\omega_k| = 1$  se asocia con aquellos operadores estabilizadores que posean un único operador local distinto de  $I$ , es decir, con estados grafos con vértices aislados, lo cual se contradice con el concepto de estado grafo que hemos manejado hasta ahora al que corresponde un grafo simple conexo.

Dado que ya hemos obtenido los soportes del estabilizador  $S$  del estado  $|LC_3\rangle$  (ver ecuaciones (6.1a)-(6.1h)), emplearemos estos datos para mostrar un ejemplo de cuáles serían los invariantes correspondientes a la clase LC a la que pertenece el estado  $|LC_3\rangle$  si  $r=1$

$$A_{\{1\}}(|LC_3\rangle) = 0, \quad (6.4a)$$

$$A_{\{2\}}(|LC_3\rangle) = 0, \quad (6.4b)$$

$$A_{\{3\}}(|LC_3\rangle) = 0, \quad (6.4c)$$

$$A_{\{1,2\}}(|LC_3\rangle) = 1, \quad (6.4d)$$

$$A_{\{1,3\}}(|LC_3\rangle) = 1, \quad (6.4e)$$

$$A_{\{2,3\}}(|LC_3\rangle) = 1, \quad (6.4f)$$

$$A_{\{1,2,3\}}(|LC_3\rangle) = 4, \quad (6.4g)$$

$$A_{\{\emptyset\}}(|LC_3\rangle) = 1. \quad (6.4h)$$

Los invariantes para la clase LC a la que pertenece  $|LC_3\rangle$  son los  $A_{\omega_i}(|LC_3\rangle)$  dados por (6.4a)-(6.4h). Sólo hay dos estados dentro de esta misma clase, el  $|LC_3\rangle$  y el  $|GHZ_3\rangle$ , y si seguimos el procedimiento anterior para obtener los invariantes del  $|GHZ_3\rangle$ , comprobaremos que alcanza el mismo resultado.

Para  $r = 2$ , se tiene que  $\Omega = (\omega_1, \omega_2; \omega_{12})$ , donde  $\Omega$  denota cada una de las posibles formas diferentes de elegir dos soportes, representados por  $\omega_1$  y  $\omega_2$ , y después un tercer soporte  $\omega_{12}$ . El conjunto  $\mathcal{T}_{n,r}^{\Omega}(|\psi\rangle)$  contiene todas las posibles 2-tuplas de operadores estabilizadores  $(s_1, s_2)$  de  $|LC_3\rangle$  que satisfacen

$$\text{supp}(s_1) = \omega_1, \quad \text{supp}(s_2) = \omega_2, \quad \text{supp}(s_1 s_2) = \omega_{12}. \quad (6.5)$$

De nuevo, muchos de estos conjuntos  $\mathcal{T}_{n,r}^\Omega(|\psi\rangle)$  podrían estar vacíos porque no haya ninguna 2-tupla de operadores estabilizadores que satisfaga las condiciones dadas en (6.5) para una elección de  $\Omega$  dada. Por ejemplo, si escogemos  $\Omega = (\omega_1, \omega_2; \omega_{12})$  tales que

$$\omega_1 = \{1, 2\}, \quad \omega_2 = \{1, 2, 3\}, \quad \omega_{12} = \{1, 2, 3\}, \quad (6.6)$$

de acuerdo con las ecuaciones (6.1a)-(6.1h) hay un único operador con soporte  $\omega_1$ , y es el  $s_1$  y cuatro operadores con soporte  $\omega_2$ :  $s_2, s_5, s_7$  y  $s_8$ . El conjunto de las 2-tuplas que verifica (6.5), es:  $\mathcal{T}_{n,2}^\Omega(|LC_3\rangle) = \{(s_1, s_2), (s_1, s_5), (s_1, s_7), (s_1, s_8)\}$ , luego para  $r = 2$  la cardinalidad del conjunto es  $|\mathcal{T}_{n,2}^\Omega(|LC_3\rangle)| = 4$ .

Si el conjunto de soportes  $\Omega$  es tal que

$$\omega_1 = \{1, 2\}, \quad \omega_2 = \{2, 3\}, \quad \omega_{12} = \{1, 2, 3\}, \quad (6.7)$$

hay un único operador con soporte  $\omega_1$ , el  $s_1$ ; y un único operador con soporte  $\omega_2$ , el  $s_3$ . El conjunto de las 2-tuplas que verifican la ecuación (6.5) es  $\mathcal{T}_{n,2}^\Omega(|LC_3\rangle) = \{0\}$ , puesto que la 2-tupla que tiene de soportes  $\omega_1$  y  $\omega_2$  es  $(s_1, s_3)$ , sin embargo,  $s_1 s_3 = s_6$  cuyo soporte es  $\omega_{12} = \{1, 3\} \neq \{1, 2, 3\}$ .

Sea  $M = 2^n$  la cantidad de posibles soportes, donde  $n$  es el número de qubits. Por una parte hay  $\binom{M}{2}$  combinaciones posibles de dos soportes  $(\omega_1, \omega_2)$ , más  $M$  parejas de la forma  $(\omega_1, \omega_1 = \omega_2)$ . Por otro lado, hay  $M$  posibles formas de elegir  $\omega_{12}$ . Luego, en total hay  $M \left[ M + \binom{M}{2} \right]$  formas diferentes de elegir  $\Omega$ . Para  $n = 3$  este número es 288.

Tras este primer teorema, VDD proporcionan a través de un segundo teorema otra familia de invariantes. Su enunciado es exactamente igual que el del anterior, a excepción de la restricción dada por (6.2) que es sustituida por esta otra

$$\text{supp}(s_k) \subseteq \omega_k, \quad \text{supp}(s_k s_l) \subseteq \omega_{kl}. \quad (6.8)$$

Estos nuevos invariantes LC se corresponden con las dimensiones de los espacios vectoriales dados por operadores estabilizadores que cumplen la restricción (6.8) que se obtienen a partir del cálculo de los rangos de cada uno de ellos. Sin embargo, centraremos nuestra atención únicamente sobre el método propuesto en el primer teorema para  $r = 1$ , porque es suficiente para identificar las 101 clases de equivalencia de los estados grafo de 8 qubits. Aunque esto puede no ser suficiente para estados grafo con  $n > 8$ . Remitimos al lector a la Ref. [166] para la demostración de los teoremas y conocimiento de las siguientes familias de invariantes.

### 6.3. Resultados

El número de invariantes VDD para un estado grafo de  $n$  qubits crece rápidamente con  $n$  y  $r$ . Por ejemplo, para  $n = 3$ , en número de invariantes para  $r = 1$  es 8, y para  $r = 2$  es de 288. Si el estado grafo fuera de 8 qubits, habría 256 invariantes para  $r = 1$ , y 8421376 para  $r = 2$ . Al tratarse de una cantidad de invariantes tan numerosa, calcular los invariantes VDD para los estados grafo de 8 qubits no resulta ser de gran utilidad a la hora de afrontar este

problema<sup>1</sup>. En general, el número total de invariantes VDD para los estados grafo de  $n$  qubits y todos los posibles valores de  $r$  es  $M + \sum_{r=2}^n C'(M, r)C'(M, P)$ , donde  $M = 2^n$ ,  $P = \binom{r}{2}$  y  $C'(M, r)$  denotan las posibles combinaciones con repetición de  $M$  elementos escogidos de  $r$  en  $r$ . Para  $n = 7$ , el resultado es  $2,18 \times 10^{36}$ , y para  $n = 8$  es  $1,88 \times 10^{53}$ .

¿Cuántos de ellos son necesarios para distinguir entre todas las clases de equivalencia LC? VDD establecieron que las clases de equivalencia estaban completamente determinadas por los valores de todos los invariantes  $|\mathcal{T}_{n,r}^\Omega(|\psi\rangle)|$  para  $r = n$ . Sin embargo, esta cantidad sigue siendo demasiado grande. El problema de encontrar los invariantes que se puedan emplear para distinguir entre las clases de equivalencia de los estados entrelazados, resulta más práctico a medida que la cantidad de estos sea más pequeña. Por ello, estamos interesados en el mínimo valor de  $r$  que permita obtener los invariantes que discriminen inequívocamente las clases LC. En la Ref. [166] los autores destacan que hay ejemplos de clases de equivalencia para estados estabilizadores que están caracterizados por invariantes de  $r$  pequeño, como es el caso de los estados GHZ. Además, VDD aclaran que sería posible caracterizar con valores de  $r$  pequeños determinados subconjuntos de estados estabilizadores. Nosotros hemos calculado los invariantes VDD con  $r = 1$ , para las 146 clases de equivalencia LC, que corresponden a los estados grafo desde  $n = 2$ , hasta  $n = 8$  qubits. La consecución de este objetivo ha implicado calcular los cardinales  $A_\omega(|\psi\rangle)$  de las clases de equivalencia  $[\omega]$  ( $2^n$  por cada clase) de los 146 estados grafos representantes del conjunto de clases de equivalencia LC. Todos los resultados suman un total de 30060 invariantes. Nuestros resultados confirman que los invariantes con parámetro  $r = 1$  son suficientes para distinguir entre las 146 clases de equivalencia LC.

Nuestro objetivo no es mostrar esos 30060 invariantes, sino comprimir esta información para construir unos invariantes más simples a partir de ellos. Los nuevas cantidades resultantes deberán ser también invariantes, luego tendrán que satisfacer los siguientes requisitos:

I. La información compacta que se pretende obtener no debe ser ambigua y se debe poder leer fácilmente.

II. La información compacta debe ser invariante bajo LC.

III. La información compacta debe permitir distinguir todas las clases de equivalencia.

VDD consideran que los invariantes  $A_\omega(|\psi\rangle)$  son versiones locales de la distribución de pesos de un estabilizador  $W_{|\psi\rangle}$ , que es un concepto usado frecuentemente en la teoría de codificación cuántica y clásica, y que introduciremos más adelante. Para  $r \geq 2$  la nueva serie de invariantes involucra  $r$ -tuplas de operadores estabilizadores y sus correspondientes soportes, y son una generalización de la distribución de pesos. Denotaremos por

$$A_d(|\psi\rangle) = \sum_{\omega, |\omega|=d} A_\omega(|\psi\rangle), \quad (6.9)$$

<sup>1</sup>Una gran cantidad de invariantes requiere invertir un tiempo de computación importante, y una información harto complicada de almacenar y establecer como referencia comparativa entre clases.

al número de operadores estabilizadores cuyo peso es igual a  $d$ . De acuerdo con esta notación, la distribución de pesos de un estabilizador es el conjunto de todos los  $A_d(|\psi\rangle)$ , para todos los posibles valores del peso, es decir,

$$W_{|\psi\rangle} = \{A_d(|\psi\rangle)\}_{d=0}^n. \quad (6.10)$$

Nosotros hemos calculado los  $W_{|\psi\rangle}$  de las 146 clases de equivalencia LC. Se puede ver fácilmente que si  $A_\omega(|\psi\rangle)$  es invariante LC, entonces  $W_{|\psi\rangle}$  es también un invariante LC que permite expresar de forma compacta los invariantes  $A_\omega(|\psi\rangle)$ . Sin embargo, como se puede ver en la tabla 6.1,  $W_{|\psi\rangle}$  no permite distinguir entre dos clases de equivalencia LC cualesquiera, pues a partir de  $n = 6$  comienzan a aparecer las coincidencias. Concretamente los estados No. 13 y No. 15 de la clasificación HEB [1, 2] son claramente degenerados si empleamos  $W_{|\psi\rangle}$  para expresar los invariantes. Estos problemas de degeneración aumentan para los estados grafo de  $n = 8$  qubits. Por tanto, tuvimos que buscar una forma original de comprimir los invariantes. Comenzamos

Tabla 6.1: Distribución de pesos para los estados grafo de hasta seis qubits.

Estado grafo	$A_0$	$A_1$	$A_2$	$A_3$	$A_4$	$A_5$	$A_6$
1	1	0	3				
2	1	0	3	4			
3	1	0	6	0	9		
4	1	0	2	8	5		
5	1	0	10	0	5	16	
6	1	0	4	6	11	10	
7	1	0	2	8	13	8	
8	1	0	0	10	15	6	
9	1	0	15	0	15	0	33
10	1	0	7	8	7	24	17
11	1	0	6	0	33	0	24
12	1	0	4	8	13	24	14
13	1	0	3	8	15	24	13
14	1	0	2	8	17	24	12
15	1	0	3	8	15	24	13
16	1	0	3	0	39	0	21
17	1	0	1	8	19	24	11
18	1	0	0	8	21	24	10
19	1	0	0	0	45	0	18

por introducir dos definiciones:

*Clases equipotentes.* Independientemente de que  $|\omega_1| \neq |\omega_2|$  o no, dos clases de equivalencia respecto al soporte  $[\omega_1]$  y  $[\omega_2]$  son equipotentes si y sólo si poseen el mismo cardinal:  $A_{\omega_1}(|\psi\rangle) = A_{\omega_2}(|\psi\rangle)$ .

*Multiplicidad de  $A_\omega$  o potencia de  $A_\omega$ .* El número de clases equipotentes para un cardinal dado es invariante bajo LC y se denominará multiplicidad o potencia de  $A_\omega$ , y lo denotaremos por  $M(A_\omega)$ .

Por ejemplo, tomemos la lista de invariantes dada por las ecuaciones (6.4a)-(6.4h) para calcular las multiplicidades. Después de contabilizarlos, el valor 0 aparece 3 veces, es decir, hay tres clases de equivalencia  $[\omega]$  con esa cardinalidad, luego  $M(0) = 3$ . Aplicando este mismo criterio, se tiene que  $M(1) = 4$  y  $M(4) = 1$  para el estado  $|LC_3\rangle$ .

Si tabulamos los valores de  $A_\omega(|\psi\rangle)$  junto con sus correspondientes valores de  $M(A_\omega)$ , obtenemos la información compacta que andábamos buscando relacionada con los invariantes VDD para  $r = 1$ . Estos nuevos invariantes satisfacen los requisitos I, II y III para las 146 clases de equivalencia LC. Los resultados se muestran en las tablas 6.2, 6.3 y 6.4, y tras su observación se puede comprobar que sólo cuatro números son suficientes para distinguir entre todas las clases de equivalencia LC de estados grafo de  $n \leq 8$  qubits: se trata de las multiplicidades de los valores 0, 1, 3 y 4.

Tabla 6.2: Invariantes de los estados grafo de  $n$  qubits, con  $3 \leq n \leq 6$ . Notación: valor<sub>multiplicidad</sub>. La numeración de las clases coincide con la de las Refs. [1, 2].

No.	Invariants
1	$0_2, 1_1, 3_1$
2	$0_3, 1_4, 4_1$
3	$0_8, 1_7, 9_1$
4	$0_8, 1_3, 2_4, 5_1$
5	$0_{15}, 1_{16}, 16_1$
6	$0_{18}, 1_8, 2_3, 4_2, 10_1$
7	$0_{17}, 1_7, 2_6, 5_1, 8_1$
8	$0_{15}, 1_{11}, 3_5, 6_1$
9	$0_{32}, 1_{31}, 33_1$
10	$0_{38}, 1_{15}, 2_8, 8_2, 17_1$
11	$0_{41}, 1_{16}, 4_6, 24_1$
12	$0_{38}, 1_{14}, 2_7, 4_1, 5_2, 8_1, 14_1$
13	$0_{42}, 1_6, 2_8, 4_6, 5_1, 13_1$
14	$0_{37}, 1_{12}, 2_8, 3_4, 6_2, 12_1$
15	$0_{42}, 1_{12}, 4_6, 5_3, 13_1$
16	$0_{44}, 1_4, 2_{12}, 5_3, 21_1$
17	$0_{34}, 1_{18}, 2_6, 3_1, 5_4, 11_1$
18	$0_{33}, 1_{21}, 3_3, 4_6, 10_1$
19	$0_{47}, 1_1, 3_{15}, 18_1$

Tabla 6.3: Invariantes de los estados grafo de 7 qubits. Notación:  $\text{valor}_{\text{multiplicidad}}$ . La numeración de las clases coincide con la de las Refs. [1, 2].

No.	Invariants
20	$0_{63}, 1_{64}, 64_1$
21	$0_{78}, 1_{32}, 2_{15}, 16_2, 34_1$
22	$0_{84}, 1_{32}, 4_8, 8_3, 40_1$
23	$0_{77}, 1_{31}, 2_{15}, 8_3, 17_1, 26_1$
24	$0_{87}, 1_{25}, 4_8, 5_6, 16_1, 25_1$
25	$0_{92}, 1_{12}, 2_8, 4_7, 5_4, 8_4, 20_1$
26	$0_{87}, 1_{16}, 2_{14}, 4_7, 8_1, 10_2, 28_1$
27	$0_{80}, 1_{25}, 2_{11}, 3_3, 4_3, 5_3, 8_1, 14_1, 23_1$
28	$0_{85}, 1_{15}, 2_{16}, 4_3, 6_7, 9_1, 18_1$
29	$0_{87}, 1_{12}, 2_{15}, 4_9, 5_3, 13_1, 22_1$
30	$0_{80}, 1_{21}, 2_{12}, 3_6, 4_1, 5_4, 8_3, 17_1$
31	$0_{86}, 1_{28}, 4_3, 5_4, 8_6, 20_1$
32	$0_{89}, 1_{12}, 2_{16}, 4_4, 5_4, 8_2, 32_1$
33	$0_{72}, 1_{40}, 2_3, 3_4, 4_4, 9_4, 18_1$
34	$0_{85}, 1_{14}, 2_{17}, 4_7, 5_1, 6_2, 13_1, 22_1$
35	$0_{79}, 1_{25}, 2_{12}, 4_2, 5_6, 8_3, 17_1$
36	$0_{86}, 1_{14}, 2_{17}, 4_4, 5_2, 6_2, 8_2, 26_1$
37	$0_{80}, 1_{21}, 2_{12}, 3_8, 4_1, 5_2, 6_2, 12_1, 21_1$
38	$0_{74}, 1_{32}, 2_8, 3_3, 4_5, 7_5, 16_1$
39	$0_{77}, 1_{22}, 2_{16}, 3_5, 4_2, 7_5, 16_1$
40	$0_{70}, 1_{36}, 2_7, 3_7, 6_7, 15_1$
41	$0_{78}, 1_{22}, 2_{14}, 3_5, 4_3, 5_4, 11_1, 20_1$
42	$0_{74}, 1_{26}, 2_{15}, 3_5, 6_7, 15_1$
43	$0_{84}, 1_8, 2_{21}, 3_7, 6_7, 15_1$
44	$0_{78}, 1_{24}, 2_3, 3_{15}, 4_6, 10_1, 19_1$
45	$0_{83}, 1_{22}, 3_{10}, 4_{10}, 6_2, 24_1$

Tabla 6.4: Invariantes de los estados grafo de 8 qubits. Notación: valor<sub>multiplicidad</sub>. La numeración de las clases coincide con la de la Ref. [21].

No.	Invariants	No.	Invariants
46	$0_{128, 1127, 129_1}$	97	$0_{163, 144, 217, 314, 45, 54, 72, 106, 22_1}$
47	$0_{158, 163, 232, 322, 65_1}$	98	$0_{157, 155, 217, 39, 44, 53, 63, 71, 94, 122, 24_1}$
48	$0_{173, 164, 415, 163, 84_1}$	99	$0_{165, 140, 218, 317, 44, 52, 62, 71, 94, 122, 24_1}$
49	$0_{158, 162, 231, 161, 172, 321, 50_1}$	100	$0_{152, 159, 216, 38, 412, 98, 21_1}$
50	$0_{176, 163, 816, 65_1}$	101	$0_{168, 158, 418, 83, 96, 122, 24_1}$
51	$0_{176, 156, 47, 58, 87, 321, 44_1}$	102	$0_{177, 126, 226, 34, 411, 52, 62, 86, 201, 32_1}$
52	$0_{192, 124, 216, 48, 57, 84, 164, 37_1}$	103	$0_{174, 120, 240, 39, 64, 72, 82, 124, 27_1}$
53	$0_{180, 130, 230, 48, 82, 102, 162, 171, 49_1}$	104	$0_{200, 121, 424, 56, 134, 57_1}$
54	$0_{163, 154, 222, 38, 84, 92, 181, 241, 42_1}$	105	$0_{159, 158, 215, 34, 412, 92, 104, 161, 34_1}$
55	$0_{185, 132, 216, 413, 87, 202, 44_1}$	106	$0_{193, 119, 215, 312, 612, 91, 123, 54_1}$
56	$0_{181, 130, 223, 46, 67, 83, 92, 122, 181, 30_1}$	107	$0_{196, 19, 224, 412, 54, 88, 132, 41_1}$
57	$0_{191, 132, 29, 416, 106, 161, 66_1}$	108	$0_{180, 126, 226, 34, 44, 610, 92, 123, 36_1}$
58	$0_{176, 149, 414, 514, 202, 41_1}$	109	$0_{164, 140, 228, 32, 48, 54, 61, 72, 106, 22_1}$
59	$0_{183, 128, 225, 46, 52, 63, 82, 102, 132, 141, 161, 34_1}$	110	$0_{174, 132, 222, 313, 44, 71, 82, 106, 111, 31_1}$
60	$0_{179, 132, 225, 49, 63, 83, 101, 142, 201, 38_1}$	111	$0_{166, 140, 222, 39, 49, 51, 61, 74, 101, 131, 161, 31_1}$
61	$0_{186, 124, 220, 410, 58, 82, 104, 161, 40_1}$	112	$0_{168, 131, 232, 39, 48, 51, 72, 134, 31_1}$
62	$0_{169, 146, 215, 37, 45, 57, 81, 92, 121, 151, 181, 33_1}$	113	$0_{161, 146, 221, 310, 44, 56, 61, 83, 112, 141, 26_1}$
63	$0_{175, 127, 231, 34, 46, 62, 87, 91, 142, 26_1}$	114	$0_{158, 151, 220, 312, 42, 53, 61, 72, 82, 114, 26_1}$
64	$0_{200, 18, 214, 418, 56, 86, 131, 142, 29_1}$	115	$0_{164, 140, 228, 32, 47, 56, 87, 141, 26_1}$
65	$0_{188, 113, 228, 416, 64, 92, 124, 33_1}$	116	$0_{161, 138, 237, 37, 42, 61, 73, 106, 28_1}$
66	$0_{181, 120, 226, 38, 48, 63, 74, 81, 103, 161, 28_1}$	117	$0_{161, 143, 223, 314, 44, 53, 61, 72, 102, 132, 28_1}$
67	$0_{179, 124, 226, 34, 48, 52, 68, 92, 121, 181, 30_1}$	118	$0_{155, 155, 212, 316, 49, 98, 21_1}$
68	$0_{170, 135, 220, 312, 47, 52, 74, 81, 102, 132, 25_1}$	119	$0_{152, 159, 216, 310, 49, 61, 86, 112, 23_1}$
69	$0_{180, 154, 48, 57, 164, 172, 37_1}$	120	$0_{160, 142, 229, 33, 412, 61, 86, 112, 23_1}$
70	$0_{176, 162, 814, 161, 172, 32_1}$	121	$0_{192, 125, 424, 56, 88, 41_1}$
71	$0_{188, 122, 232, 57, 84, 172, 69_1}$	122	$0_{176, 124, 224, 36, 416, 61, 72, 106, 22_1}$
72	$0_{148, 184, 28, 37, 84, 174, 35_1}$	123	$0_{190, 128, 212, 31, 516, 86, 112, 51_1}$
73	$0_{185, 132, 215, 412, 810, 161, 50_1}$	124	$0_{200, 15, 232, 56, 88, 134, 41_1}$
74	$0_{178, 130, 226, 49, 66, 83, 92, 241, 36_1}$	125	$0_{169, 135, 228, 34, 44, 56, 64, 81, 92, 122, 33_1}$
75	$0_{166, 154, 214, 46, 57, 84, 91, 142, 171, 29_1}$	126	$0_{170, 144, 214, 36, 512, 86, 101, 112, 26_1}$
76	$0_{188, 126, 214, 414, 52, 86, 92, 131, 142, 29_1}$	127	$0_{161, 148, 219, 36, 49, 54, 76, 101, 161, 28_1}$
77	$0_{186, 128, 218, 412, 54, 104, 142, 161, 40_1}$	128	$0_{161, 142, 233, 33, 46, 61, 73, 106, 28_1}$
78	$0_{191, 124, 222, 41, 58, 87, 142, 60_1}$	129	$0_{160, 150, 218, 38, 49, 63, 72, 94, 121, 30_1}$
79	$0_{178, 132, 225, 47, 66, 84, 123, 42_1}$	130	$0_{156, 152, 219, 39, 410, 61, 86, 112, 23_1}$
80	$0_{166, 149, 215, 36, 48, 56, 81, 91, 111, 141, 201, 35_1}$	131	$0_{152, 159, 216, 312, 46, 62, 74, 104, 25_1}$
81	$0_{156, 170, 23, 34, 415, 92, 101, 134, 28_1}$	132	$0_{156, 152, 216, 313, 410, 75, 102, 131, 25_1}$
82	$0_{179, 127, 227, 34, 46, 64, 82, 91, 125, 30_1}$	133	$0_{148, 169, 212, 32, 416, 98, 21_1}$
83	$0_{179, 124, 226, 34, 410, 52, 64, 82, 92, 121, 181, 30_1}$	134	$0_{188, 134, 320, 63, 910, 54_1}$
84	$0_{165, 149, 214, 36, 410, 76, 81, 102, 132, 25_1}$	135	$0_{166, 144, 220, 33, 412, 810, 35_1}$
85	$0_{160, 156, 216, 34, 410, 54, 81, 144, 32_1}$	136	$0_{191, 130, 23, 33, 412, 715, 101, 48_1}$
86	$0_{190, 110, 230, 416, 53, 92, 102, 162, 37_1}$	137	$0_{154, 151, 226, 38, 46, 62, 74, 104, 25_1}$
87	$0_{200, 19, 216, 424, 52, 134, 57_1}$	138	$0_{154, 151, 224, 314, 41, 65, 96, 27_1}$
88	$0_{176, 128, 216, 314, 412, 71, 84, 114, 23_1}$	139	$0_{183, 112, 231, 310, 510, 66, 123, 30_1}$
89	$0_{174, 130, 232, 44, 52, 66, 85, 142, 32_1}$	140	$0_{160, 136, 234, 39, 48, 64, 92, 122, 27_1}$
90	$0_{175, 124, 233, 34, 410, 62, 74, 81, 162, 34_1}$	141	$0_{212, 11, 314, 628, 45_1}$
91	$0_{168, 128, 244, 31, 42, 64, 72, 82, 124, 27_1}$	142	$0_{184, 143, 628, 45_1}$
92	$0_{175, 127, 231, 34, 48, 62, 81, 91, 106, 34_1}$	143	$0_{179, 114, 235, 315, 73, 88, 101, 32_1}$
93	$0_{170, 133, 226, 39, 44, 52, 66, 71, 91, 122, 151, 27_1}$	144	$0_{172, 19, 256, 36, 64, 88, 29_1}$
94	$0_{182, 120, 226, 38, 410, 52, 83, 101, 132, 161, 34_1}$	145	$0_{188, 137, 32, 628, 45_1}$
95	$0_{164, 141, 228, 36, 44, 54, 62, 72, 112, 142, 29_1}$	146	$0_{164, 121, 256, 32, 64, 88, 29_1}$
96	$0_{167, 140, 223, 37, 45, 55, 71, 84, 112, 141, 29_1}$		



# Capítulo 7

## El teorema de Bell

### 7.1. Introducción

El teorema de Bell [41] señala que el programa para completar la Mecánica Cuántica (MC) sugerido por Einstein, Podolsky y Rosen [42] es incompatible con la propia MC, y muestra que el entrelazamiento distingue a la MC de cualquier teoría clásica, asentando una de las bases de la Información y Computación Cuánticas.

Este capítulo es introductorio de los dos siguientes. Su contenido se distribuye como sigue: En las secciones 7.2, 7.3 y 7.4 exponemos el argumento EPR de la incompletitud de la MC, el ejemplo de EPR-Bohm, y el teorema de Bell, respectivamente. En la sección 7.5 introduciremos las demostraciones de tipo Greenberger-Horner-Zeilinger del teorema de Bell (o demostraciones “all-versus-nothing”).

### 7.2. El argumento de EPR de incompletitud de la Mecánica Cuántica

Antes de la aparición de la MC, las teorías físicas se basaban en dos hipótesis ampliamente aceptadas:

1. Las magnitudes físicas tienen valores predefinidos que existen independientemente de la observación. Esta condición es conocida como condición de *realismo*.
2. Los efectos de las acciones locales no pueden transmitirse a una velocidad superior a la de la luz. Esta es la condición de *localidad*.

Cualquier teoría clásica es una teoría *realista local* por poseer estas dos características.

La MC, no satisface la condición de realismo desde una perspectiva realista local. Esto provoca que muchos científicos aún crean que la MC no es una teoría satisfactoria.

En 1935, Einstein, Podolsky y Rosen (EPR) publicaron un artículo [42] en el que argumentan que una teoría física puede considerarse satisfactoria sólo en caso de poder responder afirmativamente a dos preguntas:

1. ¿Es una teoría correcta?
2. ¿Es completa la descripción dada por la teoría?

Para EPR, si los resultados predichos por una teoría están de acuerdo con los resultados experimentales, entonces es una teoría correcta. Y si, además, todo elemento de realidad tiene una contrapartida en la teoría física, entonces es una teoría completa. El criterio que EPR emplean para decidir si una cantidad física es o no un elemento de realidad es el siguiente:

“Si, sin perturbar al sistema, podemos predecir con certeza (i.e., con probabilidad igual a la unidad) el valor de una cantidad física, entonces existe un elemento de realidad correspondiente a esa cantidad física”.

Proponen este criterio como una condición suficiente para decidir si una cantidad física es un elemento de realidad.

Con su artículo, EPR intentan demostrar que la MC es una teoría incompleta. El argumento que emplean se basa fundamentalmente en identificar en un sistema elementos de realidad compatibles<sup>1</sup> entre sí asociados a cantidades físicas que en MC son incompatibles.

EPR no aportan una descripción alternativa que complete la teoría cuántica, pero sugieren que tal descripción es posible.

### 7.2.1. Precisiones sobre el criterio EPR de elementos de realidad

“...without in any way disturbing a system...”

Para asegurar que un sistema no sea perturbado de ninguna manera, no debe existir posibilidad de conexión causal entre el sistema y las posibles fuentes de perturbación. Lo habitual es considerar que la decisión de qué mide Alicia (Bob), y el registro del resultado de la medida de Bob (Alicia) estén separados por un intervalo de género-espacio. Esto es suficiente para garantizar la no perturbación entre ellos (ver [167]). Esta idea se enuncia a veces como *principio de localidad*<sup>2</sup>, que en términos relativistas viene a decir que dos eventos con separación de género-

<sup>1</sup>De acuerdo con A. Peres [186] p. 203, la compatibilidad se define de la siguiente manera: “Si se prepara un sistema físico de modo que el resultado del test A es predecible y repetible, y si entonces se realiza un test B (en lugar del test A) compatible una posterior realización del test A daría el mismo resultado que si el test B no se hubiera realizado”.

<sup>2</sup>Escuetamente, las teorías locales son aquellas que excluyen la posibilidad de acción a distancia, y EPR la asumen implícitamente en su artículo: “...since at time of measurement the two systems no longer interact, no real change can take place in the second system in consequence of anything that may be done on first system. This is, of course, merely a statement of what it is meant by the absence of interaction between the two systems”.

espacio no admiten conexión causal<sup>3</sup>. En estas condiciones, las medidas que se realizan sobre sistemas separados, y en un intervalo temporal donde los eventos no admiten conexión causal. Evitamos así que estén causalmente conectados, es decir, que las influencias físicas no se puedan propagar más rápido que la velocidad de la luz, y por lo tanto no se perturben los sistemas.

“...we can predict with certainty...”

El significado de esta frase es que a partir de las medidas realizadas sobre uno o varios sistemas, es posible predecir con certeza (con probabilidad igual a la unidad) los resultados de las medidas del resto. Los resultados que se pueden predecir con certeza se dice que están perfectamente correlacionados (o perfectamente anticorrelacionados). Formalmente, en un sistema descrito por un estado  $\rho$ , hay  $p$  correlaciones perfectas cuando hay  $p$  observables  $O_i$  diferentes con valores esperados  $+1$  o  $-1$ , tales que  $\langle O_i \rangle_\rho = 1$ .

La versión de Bohm [168] del experimento EPR es más sencilla que la original de EPR, porque usa observables dicotómicos en lugar de observables de espectro continuo. Por este motivo, es el que se suele emplear para exponer el argumento EPR acerca de la incompletitud de la MC.

### 7.3. La versión de Bohm del experimento EPR

En la versión de Bohm [168] del experimento EPR se miden las componentes de espín de dos partículas de espín  $1/2$ . Cualquier componente de espín de una partícula de espín  $1/2$  puede tomar sólo dos valores, luego el problema se reduce a trabajar con observables dicotómicos. Pasemos a describir el experimento de Bohm (ver Fig. 7.1): Una fuente F situada a la misma

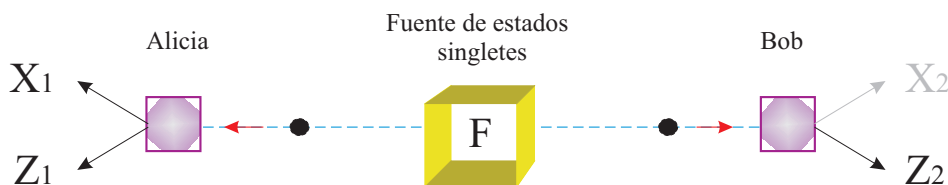


Figura 7.1: La fuente F emite singletes. Las partículas de cada par vuelan hacia los observadores Alicia y Bob, separados espacialmente por un intervalo de género espacio. Alicia y Bob miden con sus Stern-Gerlach las componentes de espín  $X_1$  y  $Z_1$ , y  $Z_2$ , respectivamente.

distancia de dos observadores<sup>4</sup>, tradicionalmente llamados Alicia (A) y Bob (B), produce pares

<sup>3</sup>Dos eventos del espacio-tiempo,  $R_1 = (ct_1, \vec{r}_1)$  y  $R_2 = (ct_2, \vec{r}_2)$ , tienen una separación  $(\Delta S)^2 = c(t_1 - t_2)^2 - (\vec{r}_1 - \vec{r}_2)^2$ . Los eventos con  $(\Delta S)^2 \geq 0$  tienen una separación de género-tiempo, y pueden estar causalmente conectados. Los eventos con  $(\Delta S)^2 < 0$  tienen una separación de género-espacio y, según la Relatividad Especial, no puede haber relación causal entre ellos.

<sup>4</sup>De este modo las partículas llegan al mismo tiempo a sendos aparatos Stern-Gerlach, descartándose la posibilidad de conexión causal entre los resultados de las medidas.

de partículas máximamente entrelazadas, por ejemplo, singletes

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle), \quad (7.1)$$

donde los estados  $|\pm\rangle$  son los estados tales que  $\sigma_z|\pm\rangle = \pm|\pm\rangle$ , siendo  $\sigma_z$  la matriz de Pauli de la componente  $Z$  de espín de una partícula. En un estado singlete, el espín del sistema total está completamente determinado y su valor es  $S = 0$ . Una vez que se crea un singlete, se separan sus componentes y se distribuyen entre los observadores. Estos están separados a una distancia tal que las medidas de Alicia y Bob están separadas por un intervalo de género-espacio.

Cada observador está equipado con un dispositivo de Stern-Gerlach que le permite medir una componente de espín. El de Alicia puede medir las componentes de espín en dos posibles direcciones ortogonales,  $\vec{n}_z$  y  $\vec{n}_x$ , y Bob sólo mide la componente de espín en la dirección  $\vec{n}_z$ .

Supongamos que Alicia realiza una medida de espín sobre la partícula 1 eligiendo la dirección  $\vec{n}_z$  (es decir, mide  $Z_1 = \vec{S}_1 \cdot \vec{n}_z$ ), y el resultado es  $+1$ . Dado que el sistema se encontraba inicialmente entrelazado, y que durante la separación las partículas no han interactuado con ningún otro sistema, el espín  $S$  del conjunto no se habrá alterado. Entonces, es posible predecir con certeza la componente de espín de la segunda partícula,  $Z_2$ , cuyo valor será  $-1$ . Consecuentemente, si Bob mide la componente de espín de la partícula 2, obtendrá con total seguridad  $-1$  sin afectar al sistema. Por lo tanto, de acuerdo con el criterio de elemento de realidad, la cantidad física  $Z_2$  tendrá asociada un elemento de realidad. Una vez que se hayan realizado estas medidas, los estados de las partículas estarán perfectamente definidos. El estado del conjunto será ahora

$$|\Psi\rangle = |+-\rangle_{zz}. \quad (7.2)$$

Mientras que las partículas están en vuelo, nada le impide a Alicia girar su Stern-Gerlach y medir la componente  $X_1$  de la primera partícula. Aplicando un razonamiento análogo al caso anterior, se puede inferir que la cantidad física  $X_2$  tendrá asociada también un elemento de realidad. El estado del sistema tras realizar las medidas será

$$|\Psi\rangle = |+-\rangle_{xx}. \quad (7.3)$$

Esto parece sugerir que ambas componentes de espín están bien definidas en la partícula 2. Como se han obtenido sin perturbarla de modo alguno, deben existir con independencia de la elección de medir los observables,  $Z_1$  ó  $X_1$ . Por este motivo, en una teoría más completa que la MC debería haber magnitudes incompatibles (en MC) que tuvieran valores definidos simultáneamente.

En contraposición, está la interpretación de este experimento desde la MC. De acuerdo con esta teoría, el singlete inicial es un estado bien definido, propio del operador  $S$  cuyo autovalor es igual a 0. Mientras que las partículas individuales poseen un 50% de probabilidad de obtener algunos de los autovalores ( $+1$  ó  $-1$ ) para una proyección arbitraria de la componente de espín. Si después de realizarse las medidas  $Z_1$  y  $Z_2$ , Alicia (Bob) desea medir la componente  $X_1$  ( $X_2$ ) de espín, la componente de espín  $X_2$  ( $X_1$ ) quedará a su vez completamente definida porque las correlaciones entre las partículas se siguen manteniendo a pesar de estar distanciadas. Si el resultado de  $X_1$  es  $+1$ , el estado del sistema vendría dado por la ecuación (7.3). Sin embargo, las componentes  $Z_1$  y  $Z_2$  estarán completamente indeterminadas. Si expresamos uno de los estados

de las partículas de la ecuación (7.3), por ejemplo, de la segunda, en la base de la componente  $Z$  de espín, el estado resultante es

$$|\Psi\rangle = |+\rangle_x \otimes \frac{1}{\sqrt{2}}(|+\rangle_z + |-\rangle_z). \quad (7.4)$$

En (7.4) queda determinada unívocamente la componente  $X$  de espín de la primera partícula, mientras que la componente  $Z$  de la segunda partícula está completamente indeterminada<sup>5</sup>.

Para EPR no es admisible que las medidas sobre la partícula 1 influyan sobre aquellas que se realizaran sobre la partícula 2, y viceversa, pues esto llevaría a la violación de la causalidad relativista. La explicación más coherente con las hipótesis clásicas es que los elementos de realidad físicos asociados a las medidas de espín, no están descritos por el estado cuántico del sistema, y por esta razón la MC no ofrece una descripción completa de los sistemas.

Estas expectativas sugerían idear una versión completa de la teoría cuántica que reprodujera sus predicciones. La sugerencia era añadir nuevas variables al estado cuántico. Este tipo de teorías se denomina genéricamente de *variables ocultas locales* (LHTV), y en ellas la función de ondas reproduce los mismos resultados que la MC pero tomando el promedio sobre un conjunto de valores de este tipo de variables, como sucedía con las teorías estadísticas de la física clásica<sup>6</sup>.

Hubo que esperar alrededor de 50 años para advertir que la naturaleza no permite una descripción en términos de elementos de realidad de EPR, ni en términos de variables ocultas locales. Este descubrimiento fue obra de Bell [41].

## 7.4. Teorema de Bell

El teorema de Bell [41, 170] establece que:

“Ninguna teoría de variables ocultas locales puede reproducir todas las predicciones de la mecánica cuántica.”

---

<sup>5</sup>Los operadores correspondientes a las componentes de espín de una misma partícula, son conjugados dos a dos, luego si tras medir  $Z_1$ , tratamos de medir la componente  $X_1$ , la componente  $Z$  de la misma partícula no conserva su valor inicial sino que queda completamente determinada. Decimos entonces que su valor ha sido perturbado por la segunda medida. El estado cuántico para la partícula 2 tras realizarse la segunda medida es  $|\Psi\rangle = \frac{1}{2}[|+\rangle_x \otimes (|-\rangle_z - |+\rangle_z) + |-\rangle_x \otimes (|-\rangle_z + |+\rangle_z)]$ . Si el autovalor de  $X_1$  es  $+1$  entonces  $|\Psi\rangle = |+\rangle_x \otimes \frac{1}{\sqrt{2}}(|-\rangle_z - |+\rangle_z)$ .

<sup>6</sup>En 1938 Einstein publicó junto con Infeld un libro [169] en el que defendía la naturaleza estadística de la MC. Emplearon para ello las analogías existentes entre esta teoría y las teorías estadísticas de la física clásica. En ambos tipos de teorías las predicciones no pueden trascender hasta las partículas individuales, sino que únicamente se pueden realizar sobre la media de un elevado número de partículas. Sin embargo, existe una destacada diferencia entre ellas, y es que en la estadística, la leyes que gobiernan el comportamiento de un grupo de partículas proceden del las que rigen el comportamiento individual de éstas, mientras que la física cuántica establece directamente las leyes que gobiernan a un grupo de partículas, sin conexión alguna con aquellas que podrían regir los comportamientos individuales.

Atendiendo a este resultado, los observables de un sistema físico no pueden tener valores predefinidos.

Como demostración, Bell propone una teoría de variables ocultas locales y deriva una desigualdad a partir de las distribuciones de probabilidad que se obtienen de los resultados de las medidas hechas sobre pares de sistemas bajo el supuesto de localidad. Estas distribuciones de probabilidad se conocen como *correlaciones locales*. En las correlaciones locales, la información que compartieron ambos sistemas durante el tiempo que estuvieron interaccionando en el pasado, fijaron los resultados de las medidas de sus respectivos observables en el presente.

La violación de la desigualdad de Bell es un método estándar para identificar la llamada no-localidad cuántica.

#### 7.4.1. Primera desigualdad de Bell

La primera desigualdad de Bell [41] se basa en el experimento de Bohm ideado para mostrar la paradoja EPR. Supongamos que disponemos de un conjunto de pares de partículas preparadas en estados que están completamente especificados por  $\lambda$ ,  $\lambda \in \Lambda$ . El conjunto de variables locales de un estado viene representado por  $\lambda$ . Sin pérdida de generalidad, podemos suponer que sus valores están distribuidos de forma continua en un colectivo  $\Lambda$ , tal que la probabilidad de que la función de distribución  $\rho(\lambda)$  (o estado de un par de partículas) se encuentre en el intervalo  $[\lambda, \lambda + d\lambda]$ , sea  $d\rho = \rho(\lambda)d\lambda$ . La densidad de estados  $\rho$  está normalizada,

$$\int_{\Lambda} \rho(\lambda)d\lambda = \int_{\Lambda} d\rho = 1. \quad (7.5)$$

Promediando el valor de un observable  $X$  sobre el conjunto del total de pares de estados, obtenemos el valor medio  $E(X)$  de  $X$ ,

$$E(X) = \int_{\Lambda} X(\lambda)\rho(\lambda)d\lambda. \quad (7.6)$$

Al promediar sobre todos los pares de partículas preparados, estamos promediando sobre los posibles valores de la variable oculta  $\lambda$  que describe cada par emitido por la fuente. El resultado de la medida dependerá de la orientación de los analizadores y del parámetro  $\lambda$ <sup>7</sup>. Si  $\vec{a}$  es la dirección fija en la que está orientado el aparato de medida de Alicia, y  $\vec{b}$  y  $\vec{b}'$  son las dos direcciones alternativas para el de Bob (ver Fig. 7.2), entonces adoptando el convenio  $\hbar/2 = 1$ , las posibles medidas de Alicia y Bob son

$$A(\vec{a}, \lambda) = \pm 1, \quad B(\vec{b}, \lambda) = \pm 1, \quad B(\vec{b}', \lambda) = \pm 1. \quad (7.7)$$

Con vistas a calcular la correlación  $E(A, B)$  es preciso calcular primero el producto de los observables  $A$  y  $B$ , el cual dependerá del estado del par de partículas y de las orientaciones de sendos aparatos de medida. De acuerdo con cualquier teoría de variables locales, los resultados de

<sup>7</sup>Si se conoce  $\lambda$  una vez que el par haya sido emitido por la fuente, en cualquier teoría realista local existirá alguna regla de evolución para obtener su valor en tiempos posteriores

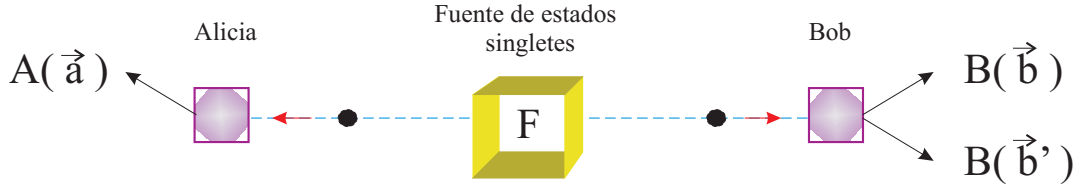


Figura 7.2: La fuente F emite singletes. Las partículas de cada par vuelan por separado hacia los observadores Alicia y Bob, separados por un intervalo de género espacio. Alicia mide el observable  $A$ , y Bob los observables  $B$  y  $B'$ .

las medidas que realice un observador no dependerá de los obtenidos por otro que se encuentre lo suficientemente distanciado de él. En estas condiciones, la dependencia del producto  $AB$  respecto a  $\lambda$  y a las orientaciones de los aparatos de medida es

$$AB = A(\vec{a}, \lambda)B(\vec{b}, \lambda). \quad (7.8)$$

La correlación entre ambas medidas de espín, o lo que es lo mismo, el valor medio del observable  $AB$  es

$$E(\vec{a}, \vec{b}) = \int_{\Lambda} A(\vec{a}, \lambda)B(\vec{b}, \lambda)\rho(\lambda)d\lambda. \quad (7.9)$$

Siguiendo el experimento de EPR-Bohm, si los pares se encuentran en estado singlete  $|\Psi^{-}\rangle$ , las componentes de espín a lo largo de cualquier dirección espacial  $\vec{n}$ , están completamente anticorrelacionadas. Luego su suma a lo largo de la dirección  $\vec{a}$  verificará que

$$A(\vec{a}) + B(\vec{a}) = 0. \quad (7.10)$$

Para estados perfectamente anticorrelacionados, en base de las ecuaciones (7.7) y (7.8), se obtiene que

$$E(\vec{a}, \vec{a}) = -1. \quad (7.11)$$

Lo que equivale a

$$A(\vec{a})B(\vec{a})|\Psi^{-}\rangle = -|\Psi^{-}\rangle. \quad (7.12)$$

Tras haber especificado las correlaciones entre los resultados de las medidas, identificaremos las cantidades físicas representadas por los observables medidos en el sistema con los elementos de realidad EPR.

Supondremos que el aparato de medida de Alicia está orientado en una dirección fija  $\vec{a}$ , y que el de Bob tiene dos direcciones alternativas  $\vec{b}$  y  $\vec{b}'$ . Partiendo de la diferencia  $E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}')$ , y usando las ecuaciones (7.7) y (7.10) se obtiene

$$\begin{aligned} E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}') &= \int_{\Lambda} [A(\vec{a}, \lambda)B(\vec{b}, \lambda) - A(\vec{a}, \lambda)B(\vec{b}', \lambda)] \rho(\lambda)d\lambda = \\ &= - \int_{\Lambda} [A(\vec{a}, \lambda)A(\vec{b}, \lambda) - A(\vec{a}, \lambda)A(\vec{b}', \lambda)] \rho(\lambda)d\lambda = \\ &= \int_{\Lambda} A(\vec{a}, \lambda)A(\vec{b}, \lambda) [1 - A(\vec{b}, \lambda)A(\vec{b}', \lambda)] \rho(\lambda)d\lambda. \end{aligned} \quad (7.13)$$

Los resultados de los productos  $A(\vec{a}, \lambda)B(\vec{b}, \lambda)$  pueden ser  $+1$  ó  $-1$ . Si se aplica la condición de normalización (7.5), se tiene que

$$|E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}')| \leq \int_{\Lambda} [1 - A(\vec{a}, \lambda)A(\vec{b}', \lambda)\rho(\lambda)d\lambda] = 1 + E(\vec{b}, \vec{b}'). \quad (7.14)$$

Reorganizando este resultado, finalmente se alcanza la forma en que se suele presentar la primera desigualdad de Bell:

$$|E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}')| - E(\vec{b}, \vec{b}') \leq 1. \quad (7.15)$$

Esta es la expresión que debería satisfacer cualquier estado singlete que se pueda estudiar empleando una teoría de variables ocultas locales. Según el formalismo cuántico, las correlaciones cuánticas que aparecen en la ecuación anterior, dependen únicamente de la orientación relativa de los analizadores de Alicia y Bob. Veamos, los kets  $|\vec{n}, +\rangle$  y  $|\vec{n}, -\rangle$  indican los posibles resultados de las proyecciones del momento de espín de una partícula de espín  $1/2$  a lo largo de alguna dirección arbitraria  $\vec{n}$ . Si la dirección de proyección es  $\vec{n}_z$ , entonces con los kets  $|+\rangle$  y  $|-\rangle$  especifican las orientaciones up ( $\uparrow$ ) y down ( $\downarrow$ ), respectivamente, a lo largo de la misma. Si reescribimos el estado singlete empleando la notación general de los kets, entonces

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\vec{n}_1, +\rangle_1|\vec{n}_1, -\rangle_2 - |\vec{n}_1, -\rangle_1|\vec{n}_1, +\rangle_2). \quad (7.16)$$

Supongamos que el  $\vec{n}_1$  de la ecuación anterior es la dirección del analizador de Alicia. Si la dirección del analizador de Bob es  $\vec{n}_2$ , entonces las dos direcciones se relacionan a través de las expresiones

$$|\vec{n}_1, +\rangle_2 = \cos\left(\frac{\theta}{2}\right)|\vec{n}_2, +\rangle_2 + \sin\left(\frac{\theta}{2}\right)|\vec{n}_2, -\rangle_2, \quad (7.17a)$$

$$|\vec{n}_1, -\rangle_2 = -\sin\left(\frac{\theta}{2}\right)|\vec{n}_2, +\rangle_2 + \cos\left(\frac{\theta}{2}\right)|\vec{n}_2, -\rangle_2. \quad (7.17b)$$

Sustituyendo estas expresiones en la ecuación (7.16), se obtiene que

$$\begin{aligned} |\Psi\rangle = \frac{1}{\sqrt{2}} & [-\sin\left(\frac{\theta}{2}\right)|\vec{n}_1, +\rangle_1|\vec{n}_2, +\rangle_2 + \cos\left(\frac{\theta}{2}\right)|\vec{n}_1, +\rangle_1|\vec{n}_2, -\rangle_2 \\ & - \cos\left(\frac{\theta}{2}\right)|\vec{n}_1, -\rangle_1|\vec{n}_2, +\rangle_2 - \sin\left(\frac{\theta}{2}\right)|\vec{n}_1, -\rangle_1|\vec{n}_2, -\rangle_2]. \end{aligned} \quad (7.18)$$

La amplitud de probabilidad de que los momentos de espín de las partículas 1 y 2 tengan orientación up a lo largo de las direcciones de sus analizadores es  $P_{++}(\vec{n}_1, \vec{n}_2) = 1/2 \sin^2(\theta/2)$ . El resto de los coeficientes de la ecuación anterior tienen una interpretación análoga. Si multiplicamos cada una de estas probabilidades por sus autovalores asociados, obtenemos el valor esperado del observable  $S_a \otimes S_b$ :  $E(\vec{a}, \vec{b}) = \langle \rho | S_a \otimes S_b | \rho \rangle = -\vec{a} \cdot \vec{b} = -\cos \theta_{ab}$ . Si los aparatos de medida se orientan formando entre sí ángulos de  $60^\circ$  como se indica en la Fig. 7.3, el resultado de las correlaciones es  $E(\vec{a}, \vec{b}) = E(\vec{b}, \vec{b}') = \frac{-1}{2}$  y  $E(\vec{a}, \vec{b}') = \frac{1}{2}$ . Sustituyendo estos valores en la



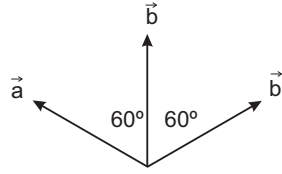


Figura 7.3: Direcciones coplanarias que definen las tres direcciones de medida para las cuales la predicción cuántica viola la desigualdad de Bell.

ecuación (7.15), resulta que esta disposición de los aparatos de medida conduce a una violación de la desigualdad de Bell estimada en  $3/2$ ,

$$|E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}')| - E(\vec{b}, \vec{b}') = \frac{3}{2} > 1. \quad (7.19)$$

Las correlaciones de este tipo son correlaciones perfectas, es decir, sólo son válidas para sistemas donde se esperan dos tipos de resultados,  $+1$  y  $-1$ . Este hecho requiere la detección de una fracción de partículas lo suficientemente alta respecto a la cantidad de pares emitidos, como para que esos resultados puedan ser considerados representativos del total. Además, el conjunto de variables ocultas involucradas está siempre perfectamente anticorrelacionadas cuando los analizadores son paralelos. Los experimentos reales de la época se realizaban bajo condiciones que no cumplían las exigencias teóricas con la precisión necesaria como para que las medidas se pudieran considerar perfectas. Por lo que las correlaciones observadas se alejaban demasiado de las correlaciones perfectas empleadas en el transcurso de esta demostración, y finalmente, esta primera demostración no pudo ser comprobada en los laboratorios.

Las desigualdades de Bell que como ésta desigualdad se basan en una perfecta predicción de los valores de los observables y en la hipótesis de localidad, de acuerdo con el argumento original de EPR, son desigualdades de Bell de tipo EPR. En la siguiente sección veremos cómo los avances teóricos y experimentales actuales permiten estudiar este tipo de correlaciones perfectas y comprobar las desigualdades de tipo EPR.

En 1971, Bell [171] obtuvo una nueva desigualdad considerando la posible no detección de las partículas por el detector, e incluyendo en la teoría de variables ocultas locales el efecto que el estado de los aparatos de medida ejerce sobre las correlaciones. Su nuevo resultado es equivalente a la desigualdad CHSH que veremos a continuación.

#### 7.4.2. Desigualdad CHSH

En 1969, Clauser, Horne, Shimony y Holt [170] obtuvieron una desigualdad conocida como CHSH. Esta desigualdad de Bell es una versión más general de la desigualdad original, pues el modelo de variables ocultas empleado para la obtención de las correlaciones satisface que:

1. Las probabilidades de los resultados de todos los observables locales están predeterminados.
2. Estas probabilidades no se pueden modificar por la realización de medidas sobre sistemas

separados.

Es decir, las condiciones de realismo y localidad anteriores se aplican sobre las probabilidades de los resultados de las medidas realizadas, no sobre los resultados de las medidas, por lo que, no están basadas en los elementos de realidad de EPR. Entonces, no se obtendrán correlaciones perfectas. A estas desigualdades de Bell se les conoce como desigualdades de tipo CHSH. El montaje del experimento para la demostración CHSH del teorema de Bell corresponde a la

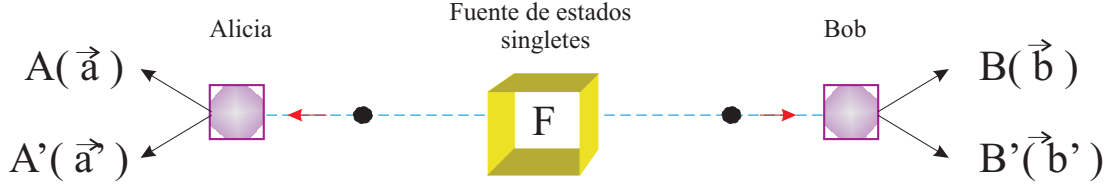


Figura 7.4: La fuente F emite singletes. Las partículas de cada par vuelan por separado hacia los observadores Alicia y Bob, separados por un intervalo de género espacio. Los observables que miden cada observador están indicados en la figura.

Fig. 7.4. Tanto Alicia como Bob pueden elegir dos direcciones alternativas,  $(\vec{a}, \vec{a}')$  y  $(\vec{b}, \vec{b}')$ , en sus respectivos aparatos de medida. Las medidas se realizan simultáneamente para evitar la transferencia de información entre los sistemas.  $E$  es el valor medio de los resultados tras realizar un experimento un número elevado de veces.

La desigualdad que deben satisfacer las correlaciones que caracterizan a los estados preparados es

$$2 \leq E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{b}') + E(\vec{a}', \vec{b}) + E(\vec{a}', \vec{b}') \leq 2. \quad (7.20)$$

Si las variables fueran operadores, podríamos hablar del operador CHSH (en general, a los operadores obtenidos a partir de las desigualdades de Bell se les conoce como *operadores de Bell*) dado por la expresión

$$\hat{\beta}_{\text{CHSH}} = A \otimes (B - B') + A' \otimes (B + B'). \quad (7.21)$$

Este operador podría actuar sobre un estado  $\rho$  que admita un modelo de variables ocultas locales, y de acuerdo con (7.20) debe satisfacer que

$$|\text{tr}(\hat{\beta}_{\text{CHSH}_\rho})| \leq 2. \quad (7.22)$$

Por intuición, la violación máxima se alcanzaría cuando la suma de los términos de la igualdad fuera igual al valor máximo 4, sin embargo, nunca se ha llegado a alcanzar este límite experimentalmente. La máxima violación que predice el formalismo cuántico corresponde a la desigualdad de Tsirelson [172] dada por la expresión

$$|\text{tr}(\hat{\beta}_{\text{CHSH}_\rho})| \leq 2\sqrt{2}. \quad (7.23)$$

$\rho$  es el estado singlete  $\rho = |\Psi^-\rangle\langle\Psi^-|$ .

La dificultad que conlleva el empleo de esta desigualdad estriba en construir el observable de Bell adecuado para cada estado y experimento. Por otro lado, su aplicación directa sobre estados mezcla no ofrece resultados claros. La desigualdad CHSH pudo adaptarse para su comprobación en estados cuánticos arbitrarios de dos qubits [173], aunque hay resultados no menos interesantes que surgieron en estudios posteriores.

En general, para dos sistemas (denotados como 1 y 2, respectivamente) separados por un intervalo de género espacio, cada uno con una dimensión del espacio de Hilbert mayor o igual de dos, cualquier operador de Bell CHSH tiene la siguiente expresión

$$\widehat{\beta}_{\text{CHSH}} = \sum_{i=1}^m \sum_{j=1}^n C(i, j) \langle A_1^{(i)} B_2^{(j)} \rangle. \quad (7.24)$$

Donde  $C(i, j)$  son ciertos coeficientes constantes, e  $i$  y  $j$  son los índices (discretos o continuos) que distinguen entre los posibles experimentos sobre los sistemas 1 y 2, respectivamente.  $\langle A_1^{(i)} B_2^{(j)} \rangle$  es una función de correlación (la medida de los productos de los observables medidos sobre 1 y 2), que en base a las condiciones 1. y 2. deben tener la forma

$$\langle A_1^{(i)} B_2^{(j)} \rangle = \sum_{\lambda} f_1(A_1^{(i)}, \lambda) g_2(B_2^{(j)}, \lambda) p(\lambda). \quad (7.25)$$

Donde  $f_1(A_1^{(i)}, \lambda)$  [ $g_2(B_2^{(j)}, \lambda)$ ] es una función que depende del valor experimental de  $A_1^{(i)}$  ( $B_2^{(j)}$ ), y  $\lambda$  es el parámetro de suma o integración (dependiendo de si toma valores discretos o continuos) que permite que la descripción tenga una probabilidad natural;  $p(\lambda)$  es la distribución de probabilidad del parámetro. Cualquier estado separable satisface una desigualdad CHSH. Sin embargo, hay estados separables que violan la desigualdad de Bell original [174] debido a que dicha desigualdad de Bell se basa en asunciones que no son satisfechas por estos estados separables [175, 176].

Las desigualdades CHSH no son más que un tipo elemental de desigualdades de Bell en el que intervienen únicamente dos observadores, Alicia y Bob, y cada uno de ellos puede realizar medidas sobre observables dicotómicos. Las desigualdades de Bell conforman una infinita familia construida con distintos tipos de medidas de correlación entre sistemas, donde pueden intervenir  $n$  observadores/partes y cada uno de ellos evalúan  $m$  observables de  $l$  autovalores (con  $n, m$  y  $l \geq 2$ ). Hemos visto dos tipos de desigualdades de Bell, las EPR y las CHSH.

De entre las demostraciones del teorema de Bell están aquellas que en lugar de emplear desigualdades se basan en una contradicción algebraica. Se trata de las demostraciones “all-versus-nothing” (AVN) [46]. En el siguiente apartado trataremos este tipo de demostraciones. Veremos además, su importancia en la construcción de nuevas desigualdades de Bell.

## 7.5. Demostraciones “all-versus-nothing” del teorema de Bell

La violación de una desigualdad de Bell tiene el inconveniente de realizarse únicamente a través de procedimientos estadísticos. Existe otra vía para mostrar el conflicto entre los elementos de realidad introducidos por EPR y la MC, en la que las desigualdades son prescindibles y donde las correlaciones perfectas predichas por la MC son las piezas claves.

Una demostración “all-versus-nothing” (el nombre se introdujo en [46]) está basada en un conjunto de  $s$  correlaciones perfectas de un estado cuántico. Si éstas se construyen empleando elementos de realidad EPR, entonces  $s - q$  de esas correlaciones perfectas conducen a un resultado opuesto al predicho por las otras  $q$  correlaciones. Si todas las  $s$  correlaciones son esenciales para obtener una contradicción (i.e., que no se obtendrá ninguna contradicción si se elimina algunas de ellas), entonces se dice que la demostración AVN es *crítica*.

El nombre “all-versus-nothing” refleja una particular característica de estas demostraciones, y es que en caso de no obtenerse ninguna contradicción, el estado de partida admite una descripción LHTV. En caso contrario, no hay lugar para ninguna teoría local poniéndose de manifiesto el carácter no local del estado cuántico.

La primera demostración AVN fue propuesta por Heywood y Redhead [43]. Esencialmente muestra la conexión entre los teoremas de Kochen-Specker<sup>8</sup> y Bell. Del lado del primer teorema, se desprende que cualquier interpretación realista involucra una contradicción algebraica; de parte del segundo, se tiene que el realismo supone la no-localidad. Heywood y Redhead demuestran que cualquier teoría local conduce a una contradicción algebraica que se puede interpretar como una manifestación de la no-localidad.

Pero la demostración AVN más conocida es la de Greenberger, Horne y Zeilinger (GHZ) [44, 45]. GHZ desarrollan su trabajo empleando un sistema de cuatro qubits en el estado

$$|\Psi\rangle = 1/\sqrt{2}(|+\rangle_1|+\rangle_2|-\rangle_3|-\rangle_4 - |-\rangle_1|-\rangle_2|+\rangle_3|+\rangle_4) = 1/\sqrt{2}(|++--\rangle - |--++\rangle). \quad (7.26)$$

Los estados de este tipo son conocidos como estados GHZ<sup>9</sup>, y las demostraciones AVN que se valen de ellos se conocen comúnmente como demostraciones GHZ. Mermin [46] propuso una versión simplificada de la primera demostración GHZ empleando tres partículas de espín 1/2, y será la que escogeremos para exponer en qué consiste este tipo de demostraciones.

### 7.5.1. Demostración GHZ del teorema de Bell

En la versión de Mermin, las partículas se crean en una misma fuente y posteriormente se separan (ver Fig. 7.5). Cada una de ellas se dirige hacia un aparato Stern-Gerlach que se

<sup>8</sup>El teorema de Kochen-Specker demuestra que es imposible asignar valores definidos a un conjunto de observables de un sistema cuántico individual. Utilizan para ello un contraejemplo empleando los estados de espín de una partícula de espín 1. Se valen de un total de 117 observables, correspondientes a los cuadrados de las componentes del momento angular de espín a lo largo de 117 direcciones distintas, para demostrar que no hay forma de asignar valores 0 y 1 a todos esos observables de manera que satisfagan la relación  $v(A) + v(B) + v(C) = 2$  para cualquier conjunto,  $A$ ,  $B$  y  $C$ , de observables asociados que sean mutuamente ortogonales.

<sup>9</sup>Para un sistema de  $n$  qubits, los estados GHZ se pueden escribir como:  $1/\sqrt{2}(|+\rangle^{\otimes n} + |-\rangle^{\otimes n})$ . También es frecuente ver esta expresión general en términos de los kets  $|0\rangle$  y  $|1\rangle$ , los cuales se identifican con los resultados positivos y negativos de los autovalores de un operador actuando sobre su estado propio de un qubit. Esta no es la única forma en que se pueden ver escritos los estados GHZ, pues existen tantas posibilidades como combinaciones de + y - admisibles para los valores de  $m$  de la expresión:  $1/\sqrt{2}(|m_1 m_2 \dots m_n\rangle \pm | - m_1 - m_2 \dots - m_n\rangle)$ .

podrá orientar en dos direcciones cualesquiera ortogonales entre sí, como por ejemplo:  $\vec{n}_x$  ó  $\vec{n}_y$ . El resultado de la medida de la proyección del espín de cada partícula,  $\sigma_i = \vec{\sigma} \cdot \vec{n}_i$ , se etiqueta con  $+1$ , si la componente de espín está orientada en el sentido positivo (orientación up) de alguna de las dos direcciones. El signo  $-1$  indica que la componente de espín se orienta en sentido contrario al establecido como positivo (orientación down). El estado del sistema viene descrito por

$$|\Psi\rangle = 1/\sqrt{2}(|+++ \rangle - |-- \rangle), \quad (7.27)$$

los kets  $|+\rangle$  y  $|-\rangle$  representan los estados de espín up y down; dicho estado es el mismo sea cual sea la dirección de orientación  $\vec{n}$  del aparato, porque los estados de este tipo tienen simetría esférica (i.e., dado un estado, los resultados de la proyección de un autovalor a lo largo de cualquier dirección tiene la misma probabilidad de suceder). Además, es entrelazado y exhibe correlaciones de espín perfectas, es decir, si las componentes de espín de las partículas 1 y 2, son  $+1$  ( $-1$ ), entonces, con total seguridad, la componente de espín de la tercera partícula será también  $+1$  ( $-1$ ). Estas correlaciones equivalen a operadores de correlación de autovalor  $+1$  ( $-1$ ) cuando actúan sobre el estado  $|\Psi\rangle$ , y se obtienen a partir de los operadores de Pauli de espín de cada partícula,  $\sigma_i$ .

El argumento que emplean GHZ consiste en lo siguiente: A partir de los operadores de correlación<sup>10</sup> se construyen unas ecuaciones lineales. Dichas ecuaciones, en principio, deben ser satisfechas por las variables ocultas asociadas a los resultados de las medidas de las componentes de espín, pero tras asignarles los valores  $\pm 1$  nunca llegan a satisfacerse, obteniéndose una contradicción. La interpretación de la contradicción es que no es posible emplear una descripción de variables ocultas que encaje con las correlaciones que predice la mecánica cuántica.

Como ya hemos destacado en varias ocasiones, la introducción de las variables ocultas no es una premisa extra, sino que está justificada porque los resultados de las componentes de espín satisfacen la condición de elemento de realidad EPR (i.e., los resultados de las medidas de las componentes de espín de dos partículas cualesquiera permite predecir con certeza, el resultado de la medida sobre una tercera), y tales valores concretos no están contenidas en el estado cuántico  $\Psi$ . Se trata entonces de unas variables que en la descripción cuántica permanecen “ocultas”.

Los operadores de correlación han de conmutar entre sí para evitar que el estado se modifique al operar sobre él, y así queda siempre bien definido por la misma función de ondas. Las ecuaciones que satisfacen los operadores de correlación son

$$X_1 \otimes Y_2 \otimes Y_3 |\Psi\rangle = |\Psi\rangle, \quad (7.28a)$$

$$Y_1 \otimes X_2 \otimes Y_3 |\Psi\rangle = |\Psi\rangle, \quad (7.28b)$$

$$Y_1 \otimes Y_2 \otimes X_3 |\Psi\rangle = |\Psi\rangle, \quad (7.28c)$$

$$-X_1 \otimes X_2 \otimes X_3 |\Psi\rangle = |\Psi\rangle. \quad (7.28d)$$

Donde  $X_i$ ,  $Y_i$  y  $Z_i$  son las componentes de espín de la partícula  $i$ -ésima. Estos observables cumplen el criterio de elemento de realidad EPR, y por lo tanto, respecto a cualquier teoría

<sup>10</sup>Los operadores de correlación son en definitiva los valores esperados del producto de los resultados  $+1$  ó  $-1$  de las mediciones sobre las partículas individuales.

local, los resultados de sus medidas deben estar predefinidos. Si denotamos los resultados como  $v(k_i)$ , para  $k_i = X_i, Y_i$  ó  $Z_i$ , atendiendo a las ecuaciones (7.28a)-(7.28d), y a su condición de variables ocultas, deben satisfacer

$$v(X_1) \times v(Y_2) \times v(Y_3) = 1, \quad (7.29a)$$

$$v(Y_1) \times v(X_2) \times v(Y_3) = 1, \quad (7.29b)$$

$$v(Y_1) \times v(Y_2) \times v(X_3) = 1, \quad (7.29c)$$

$$v(X_1) \times v(X_2) \times v(X_3) = -1. \quad (7.29d)$$

Si observamos las ecuaciones (7.29a)-(7.29d), cada variable aparece dos veces, y los valores que

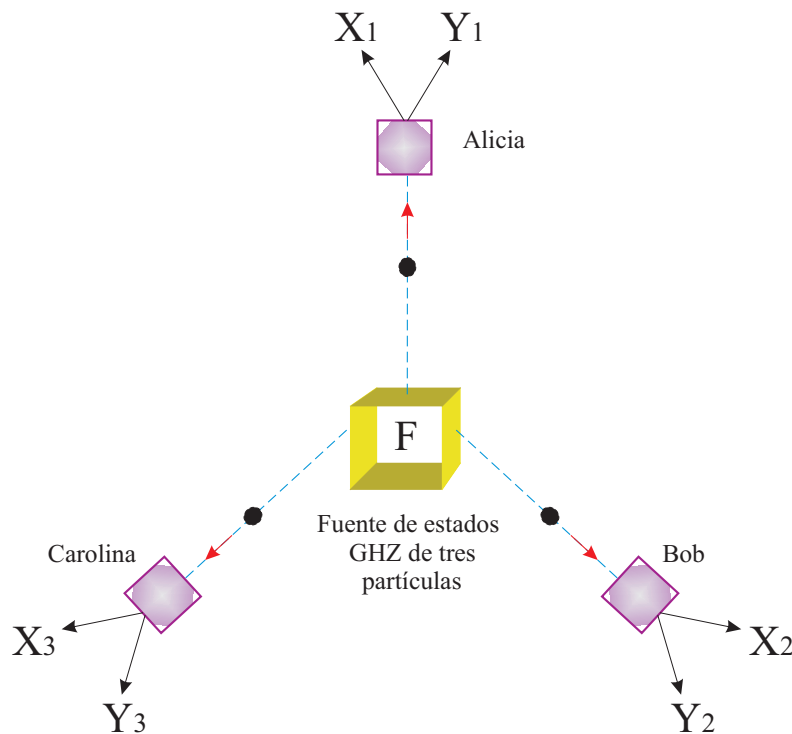


Figura 7.5: La fuente F emite estados GHZ de tres partículas. Cada una de ellas se dirige hacia un observador distinto, separados por un intervalo de género espacio, y realizarán las medidas indicadas en los operadores de correlación.

pueden tomar oscilan entre  $+1$  y  $-1$ . Si se realiza el producto entre todos los términos situados a la derecha de la igualdad el resultado será  $-1$ , mientras que para los términos de la izquierda será  $+1$ . Estos dos resultados deben relacionarse a través de una igualdad,  $1 = -1$ , alcanzándose así la contradicción predicha por GHZ.

La demostración de GHZ original [44] empleaba un sistema de cuatro partículas de espín  $1/2$ , distribuidas entre cuatro observadores separados por sendos intervalos de género espacio.

Con la demostración GHZ [46] se logra poner de manifiesto la imposibilidad de elementos de realidad locales en MC. Por emplear correlaciones perfectas esta demostración se sitúa en el marco original EPR [42]. No obstante, requiere de un mínimo de tres observadores<sup>11</sup>, y no dos como en la demostración original del teorema de Bell.

Anteriormente, Heywood y Readhead [43] obtuvieron una demostración del teorema de Bell sin desigualdades que requería únicamente dos observadores y dos partículas de espín 1; pero precisaba de un espacio de Hilbert de dimensión 9, mientras que la demostración original del teorema de Bell tiene lugar en un espacio de Hilbert de dimensión 4 [41]. Esta demostración fue simplificada por Brown y Svetlichny [177] empleando un argumento similar al que usaron Kochen-Specker para demostrar que los elementos de realidad que se correspondían con las medidas realizadas sobre espacios separables debían ser contextuales<sup>12</sup>. Poco después, Hardy [47] proporciona una demostración del teorema de Bell para un estado de dos partículas que sólo requiere de un espacio de Hilbert de dimensión 4, y no emplea desigualdades. Sin embargo, esta demostración es válida únicamente para un tipo particular de estado entrelazado, aunque posteriormente [178] demostró que su resultado es válido para cualquier tipo de estados entrelazados, exceptuando a los estados máximamente entrelazados. Pero en la desigualdad original del teorema de Bell la máxima discrepancia con los modelos locales se alcanza con estados máximamente entrelazados [179], también conocidos como estados de Bell [180].

Experimentalmente, para la demostración de Hardy, sólo en el 9 % de las repeticiones o rondas de un mismo experimento se encontraban contradicciones con el argumento EPR, mientras que en las verificaciones experimentales de la demostración GHZ se encontraban evidencias de tales contradicciones en el 100 % de los casos.

Todos estos resultados condujeron a la búsqueda de demostraciones AVN a través de estados máximamente entrelazados de dos partículas, en pro de la evolución del problema de encontrar demostraciones AVN. En la Ref. [181] Cabello introduce una demostración AVN empleando un argumento similar al de Hardy, y que funcionaba en el 100 % de los experimentos. Requiere únicamente dos observadores y dos estados máximamente entrelazados de dos qubits. Posteriormente, publica una versión más simplificada de esta demostración [182] que será la que introduciremos en el siguiente apartado.

---

<sup>11</sup>La razón de precisar tres observadores está en que si se reparten tres partículas entre solo dos observadores, los observables involucrados no satisfacen el criterio EPR de elemento de realidad. La forma de comprobarlo, es muy directa, pues aquel que posea una sola partícula, tras las mediciones, únicamente puede aportar un dato para predecir los resultados de las mediciones sobre los otros dos, lo cual atendiendo a las expresiones de las ecuaciones (7.29a)-(7.29d) resulta insuficiente. Respecto al observador que posea las otras dos, a pesar de ser capaz de aportar un número de datos suficiente para hacer las predicciones sobre el resultado de la tercera partícula del otro observador, atendiendo al argumento EPR esos resultados no son válidos, pues las partículas que se encuentran en un mismo observador no están separadas por intervalos de género-espacio (no satisfacen la condición de localidad).

<sup>12</sup>La contextualidad es una propiedad fundamental de los sistemas cuánticos. Un sistema cuántico exhibe contextualidad cuando el resultado de las medidas dependa de qué observables compatibles fueron medidos previamente. Un sistema cuántico de dos qubits que pudiera enmarcarse dentro de un modelo contextual, se caracterizaría porque independientemente del estado en que se encontrara inicialmente, una determinada secuencia de medidas de un conjunto finito de observables dicotómicos y compatibles entre sí, conduciría a una contradicción que es independiente del estado input.

### 7.5.2. Demostración AVN del teorema de Bell usando qubits y dos observadores

Cabello [181, 182] introduce una demostración AVN del teorema de Bell que conserva la estructura lógica de la demostración de Hardy [47, 178]. Emplea para ello un estado entrelazado formado por dos copias de estados máximamente entrelazados, en lugar de una única copia como en la demostración de Hardy. La demostración de Cabello está inspirada en la versión teorema de Kochen-Specker de Peres [183] y Mermin [184] (ver también [185, 186, 187]).

El experimento teórico que acompaña a la demostración consiste en una fuente que produce dos pares de singletes de qubits, que se separan de forma que los qubits 1 y 2 vuelan hacia Alicia, y los qubits 3 y 4 hacia Bob (ver Fig. 7.6). La separación entre Alicia y Bob es de tipo género espacio, asumiendo la condición de localidad. Si la expresión de un singlete es

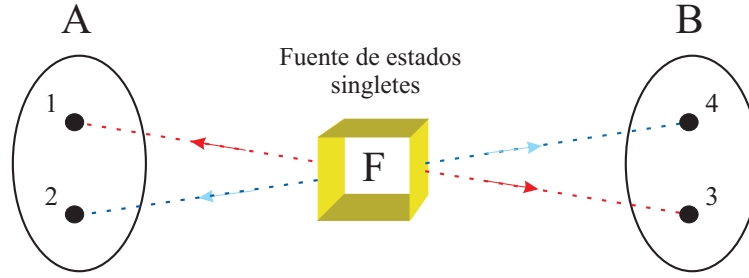


Figura 7.6: La fuente F emite un par de singletes. Las partículas de cada par se reparten entre los observadores A (Alicia) y B (Bob), separadas espacialmente por un intervalo de género espacio. Las líneas discontinuas representan el cese de la interacción entre las partículas de cada par.

$$|\Psi^-\rangle_{ij} = \frac{1}{\sqrt{2}}(|01\rangle_{ij} - |10\rangle_{ij}), \quad (7.30)$$

donde  $|01\rangle_{ij} = |0\rangle_i \otimes |1\rangle_j$ , siendo  $\sigma_z|0\rangle = |0\rangle$  y  $\sigma_z|1\rangle = -|1\rangle$ , con  $\sigma_z$  hemos denotado a la matriz de Pauli de la componente Z de espín; entonces la expresión del estado inicial emitido por la fuente del experimento vendrá dada por

$$\begin{aligned} |\Psi\rangle_{1324} &= |\Psi^-\rangle_{13} \otimes |\Psi^-\rangle_{24} \\ &= \frac{1}{2}(|0101\rangle - |0110\rangle - |1001\rangle + |1010\rangle), \end{aligned} \quad (7.31)$$

los cuatro qubits involucrados se etiquetan como 1, 3, 2 y 4. Si en (7.31) intercambiamos las partículas 2 y 3, el estado será finalmente

$$|\Psi\rangle_{1234} = \frac{1}{2}(|0011\rangle - |0110\rangle - |1001\rangle + |1100\rangle). \quad (7.32)$$

Cada uno de ellos dispone de un aparato Stern-Gerlach de modo que Alicia (Bob) puede orientarlo a lo largo de las dos direcciones ortogonales  $\vec{n}_x$  y  $\vec{n}_z$ . Los resultados de las medidas pueden



ser  $+1$  y  $-1$ . El estado (7.32) satisface las siguientes correlaciones perfectas:

$$Z_1 \cdot Z_3 |\Psi\rangle = -|\Psi\rangle, \quad (7.33a)$$

$$Z_2 \cdot Z_4 |\Psi\rangle = -|\Psi\rangle, \quad (7.33b)$$

$$X_1 \cdot X_3 |\Psi\rangle = -|\Psi\rangle, \quad (7.33c)$$

$$X_2 \cdot X_4 |\Psi\rangle = -|\Psi\rangle, \quad (7.33d)$$

$$Z_1 Z_2 \cdot Z_3 \cdot Z_4 |\Psi\rangle = |\Psi\rangle, \quad (7.33e)$$

$$X_1 X_2 \cdot X_3 \cdot X_4 |\Psi\rangle = |\Psi\rangle, \quad (7.33f)$$

$$Z_1 \cdot X_2 \cdot Z_3 X_4 |\Psi\rangle = |\Psi\rangle, \quad (7.33g)$$

$$X_1 \cdot Z_2 \cdot X_3 Z_4 |\Psi\rangle = |\Psi\rangle, \quad (7.33h)$$

$$Z_1 Z_2 \cdot X_1 X_2 \cdot Z_3 X_4 \cdot X_3 Z_4 |\Psi\rangle = -|\Psi\rangle. \quad (7.33i)$$

Con  $(\cdot)$  hemos separado los operadores. A partir de las ecuaciones (7.33a)-(7.33d) se establece que, en base al criterio EPR de elementos de realidad, los resultados de las medidas de los observables  $X_1, X_2, X_3, X_4, Z_1, Z_2, Z_3$  y  $Z_4$  se pueden considerar elementos de realidad. Luego sus valores estaban ya presentes antes de que Alicia (Bob) realizaran sus medidas, y por lo tanto, no dependen de los experimentos que deseen realizar.

Respecto a las ecuaciones (7.33e)-(7.33h), observar que es necesario realizar mediciones sobre partículas que pertenecen a un mismo observador para poder predecir con certeza los resultados de las medidas del otro observador. Al no estar las partículas de un mismo observador separadas por un intervalo de género espacio, las mediciones que se realicen sobre una cualquiera de ellas podría interferir sobre los resultados de las medidas de las demás. Pero no es esto lo que sucede. Veamos, las ecuaciones (7.33a)-(7.33d) revelan que uno de los observadores trabaja siempre con operadores que anteriormente fueron considerados como elementos de realidad ( $X_1, X_2, X_3, X_4, Z_1, Z_2, Z_3$  y  $Z_4$ ), por lo tanto sus valores ya están establecidos. Esto significa que las medidas de los operadores correspondientes no interfieren entre sí. Además, a partir de estos resultados se puede predecir con certeza los observables  $X_1 X_2, Z_1 Z_2, X_3 X_4$  y  $Z_3 Z_4$ , luego éstos también satisfacen las condiciones necesarias para ser considerados elementos de realidad. Las mismas conclusiones se pueden inferir para los observables de (7.33i).

En resumen, existe un elemento de realidad asociado a cada cantidad física que representa a cada uno de estos observables, y como tales existen antes incluso de ser medidos, por lo que sus valores no dependen de la elección del experimento que Alicia (Bob) decida realizar. Escribiremos las ecuaciones (7.33a)-(7.33i) en términos de los valores de los elementos de realidad

correspondientes al resultado de las medidas de los observables que ahí aparecen

$$v(Z_1)v(Z_3) = -1, \quad (7.34a)$$

$$v(Z_2)v(Z_4) = -1, \quad (7.34b)$$

$$v(X_1)v(X_3) = -1, \quad (7.34c)$$

$$v(X_2)v(X_4) = -1, \quad (7.34d)$$

$$v(Z_1Z_2)v(Z_3)v(Z_4) = 1, \quad (7.34e)$$

$$v(X_1X_2)v(X_3)v(X_4) = 1, \quad (7.34f)$$

$$v(Z_1)v(X_2)v(Z_3X_4) = 1, \quad (7.34g)$$

$$v(X_1)v(Z_2)v(X_3Z_4) = 1, \quad (7.34h)$$

$$v(Z_1Z_2)v(X_1X_2)v(Z_3X_4)v(X_3Z_4) = -1. \quad (7.34i)$$

Como en la versión de Mermin de la demostración GHZ, de nuevo es imposible que se satisfagan estas ecuaciones sustituyendo los valores de la variables (+1 ó -1). La forma más directa de mostrar esta contradicción, es multiplicando los miembros que se encuentran a la izquierda de las ecuaciones (7.34a)-(7.34i) e igualando este resultado con el de los productos de los términos de la derecha. El resultado del producto de la parte izquierda va a ser igual a +1 porque todas las variables se repiten un número par de veces, mientras que el de la derecha será igual a -1. Al igualar estos resultados, +1 = -1, resulta la contradicción predicha por GHZ.

Desde un punto de vista teórico, la comprobación experimental de esta demostración AVN consiste en comprobar cada una de las ecuaciones de autovalores. Para obtener unos resultados que muestren claramente que las correlaciones son lo suficientemente fuertes como para respaldar la existencia de los elementos de realidad, en una situación ideal sería necesario repetir muchas veces cada experimento. La comprobación de (7.34i) se podría llevar a cabo a partir de los productos de las ocho primeras, y este resultado debería estar de acuerdo con los resultados de cualquier experimento destinado a su comprobación.

Al trasladar estas situaciones ideales a los laboratorios reales, surgen una serie de obstáculos originados principalmente por la necesidad de altas eficiencias de los detectores, pues esto da lugar a que las ecuaciones (7.34a)-(7.34i) se alejen de los valores ideales  $\pm 1$ . Los dispositivos experimentales de entonces no permitían una verificación experimental directa de esta demostración AVN. Para resolver este problema, una práctica común es derivar desigualdades de Bell con ciertas funciones de correlación. Los límites de validez de las mismas se establecen mediante condiciones de localidad probabilísticas muy generales, que finalmente son violadas por las predicciones cuánticas. Concretamente, para ésta demostración, Cabello derivó una desigualdad empleando un procedimiento análogo al que ideó Mermin [49] para los estados GHZ de  $n$  qubits. Para ello, en primer lugar, se obtiene un operador  $\hat{O}$  que contiene los nueve operadores de correlación que aparecen en las ecuaciones (7.33a)-(7.33i). El estado  $|\Psi\rangle_{1234}$ , será propio de  $\hat{O}$ . Dado que los detectores no son ideales, los valores esperados de las correlaciones ya no serán  $\pm 1$ , como ocurría con las correlaciones perfectas de los experimentos teóricos. Entonces, para determinar sus valores, se reemplaza cada operador de correlación de  $\hat{O}$  por una función de distribución de probabilidad de las medidas que están especificadas en él. Las funciones de correlación que

describen los resultados de los nueve posibles experimentos realizados sobre el estado  $|\Psi\rangle$  es

$$P_{AB}(a, b) = \int \rho(\lambda)p(a, \lambda)p(b, \lambda)d\lambda, \quad (7.35)$$

donde  $\lambda$  es un conjunto de parámetros común a los cuatro qubits, caracterizado con una función de distribución  $\rho(\lambda)$  que está sujeta sólo a la condición de que los resultados de los experimentos de Alicia (Bob) no repercuten sobre los de Bob (Alicia). Si tal representación existe, entonces el valor medio del producto de los resultados de uno de los operadores medidos por Alicia y de uno de los medidos por Bob será

$$E_{AB} = \int \rho(\lambda)E_A(\lambda)E_B(\lambda)d\lambda, \quad (7.36)$$

donde cada  $E$  de la integral es de la forma

$$E = p(+1, \lambda) - p(-1, \lambda), \quad (7.37)$$

cuyo valor está comprendido entre  $-1$  y  $+1$ . Este operador pasa a ser una función de correlación construida a partir de la modificación de cada operador de correlación de (7.34a)-(7.34i)

$$\begin{aligned} F = \int \rho(\lambda)(-E_{Z_1 \cdot Z_3} - E_{Z_2 \cdot Z_4} - E_{X_1 \cdot X_3} - E_{X_2 \cdot X_4} \\ + E_{Z_1 Z_2 \cdot Z_3 \cdot Z_4} + E_{X_1 X_2 \cdot X_3 \cdot X_4} + E_{Z_1 \cdot X_2 \cdot Z_3 Z_4} + E_{X_1 \cdot Z_2 \cdot X_3 Z_4} - E_{Z_1 Z_2 \cdot X_1 X_2 \cdot Z_3 X_4 \cdot X_3 Z_4}). \end{aligned} \quad (7.38)$$

$F$  posee 12 cantidades distintas, cada una de ellas se encuentra entre  $-1$  y  $+1$ , y, dado que es lineal en  $E$ , alcanzará su valor máximo cuando lo hagan cada una de estas cantidades. De este modo, es fácil comprobar que  $F$  posee un límite clásico

$$F \leq 7, \quad (7.39)$$

mientras que de acuerdo con las predicciones cuánticas,  $F$  viene dado por

$$F_{MC} = \langle \Psi | \hat{O} | \Psi \rangle = 9, \quad (7.40)$$

el cual contradice la predicción clásica dada en (7.39).

Experimentalmente, se podrían realizar sin ningún problema las medidas de los observables que aparecen en las ecuaciones (7.34a)-(7.34h), ya que estas operaciones se realizan sobre qubits distintos. La comprobación de la ecuación (7.34i), resultaría más complicada. Veamos, de acuerdo con su expresión, del lado de Alicia (Bob) de deben medir los observables  $X_1 X_2$  ( $X_3 X_4$ ) y  $Z_1 Z_2$  ( $Z_3 Z_4$ ), que a pesar de ser compatibles, si los observamos detenidamente veríamos que en un mismo experimento se debería poder medir parte de ellos donde los observables son incompatibles, como por ejemplo:  $X_1$  y  $Z_1$ . Por este motivo resulta un proceso muy complicado. Desde el punto de vista teórico, medir estos observables equivale a medir  $Y_1$  ( $Y_3$ ) e  $Y_2$  ( $Y_4$ )<sup>13</sup>, pero

<sup>13</sup>La equivalencia entre los resultados de estas medidas (salvo factor de fase) es:  $Y_1 Y_2$  ( $Y_3 Y_4$ )  $\longleftrightarrow$   $Z_1 Z_2 \cdot X_1 X_2$  ( $Z_3 X_4 \cdot X_3 Z_4$ ).

medir el espín a lo largo de la dirección  $y$ , mientras que las partículas están en vuelo, presenta unas dificultades que no se observan cuando las direcciones elegidas son  $x$  ó  $z$ . Una forma de resolver este problema, consiste en percatarse de que medir  $Z_1 Z_2 \cdot X_1 X_2$  ( $Z_3 X_4 \cdot X_3 Z_4$ ), equivale a medir el operador de Bell sobre las partículas 1 y 2 (3 y 4). Los autovectores del operador de Bell, son los estados de Bell:  $\{|\Phi^\pm\rangle, |\psi^\pm\rangle\}$  ( $\{|\chi^\pm\rangle, |\omega^\pm\rangle\}$ ). La distinción entre los resultados  $+1$  y  $-1$  del operador  $Z_1 Z_2 \cdot X_1 X_2$  ( $Z_3 X_4 \cdot X_3 Z_4$ ), es equivalente a distinguir entre los estados  $\{|\Phi_{12}^+\rangle, |\psi_{12}^-\rangle\}$  ( $\{|\chi_{34}^+\rangle, |\omega_{34}^-\rangle\}$ ) y  $\{|\Phi_{12}^-\rangle, |\psi_{12}^+\rangle\}$  ( $\{|\chi_{34}^-\rangle, |\omega_{34}^+\rangle\}$ ), donde

$$|\Phi_{12}^\pm\rangle = \frac{1}{\sqrt{2}}\{|00\rangle \pm |11\rangle\}, \quad (7.41a)$$

$$|\chi_{34}^\pm\rangle = \frac{1}{\sqrt{2}}\{|0\bar{0}\rangle \pm |1\bar{1}\rangle\}, \quad (7.41b)$$

$$|\psi_{12}^\pm\rangle = \frac{1}{\sqrt{2}}\{|01\rangle \pm |10\rangle\}, \quad (7.41c)$$

$$|\omega_{34}^\pm\rangle = \frac{1}{\sqrt{2}}\{|1\bar{0}\rangle \pm |0\bar{1}\rangle\}; \quad (7.41d)$$

con  $x|\bar{0}\rangle = |\bar{0}\rangle$  y  $x|\bar{1}\rangle = -|\bar{1}\rangle$ .

Con la medida de los operadores  $Z_1 Z_2$ ,  $X_1 X_2$  ( $Z_3 X_4$ ,  $X_3 Z_4$ ) se distinguiría entre dos de los cuatro estados de Bell  $\{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$  ( $\{|\chi^\pm\rangle, |\omega^\pm\rangle\}$ ). Los qubits 3 y 4 (1 y 2) conforman, junto con los qubits 1 y 2 (3 y 4), sendos estados singletes; así que una vez que se realicen estas medidas, sus estados pasan a ser los mismos que los estados de los qubits medidos. Entonces, para poder demostrar la ecuación (7.34i), habría que partir de un estado que permitiera distinguir entre dos de los cuatro estados de Bell.

Cualquier estado propio del conjunto de operadores  $Z_1 Z_2$ ,  $X_1 X_2$ ,  $Z_3 X_4$ , y  $X_3 Z_4$ , podría emplearse para obtener una demostración del teorema de Bell como la que hemos visto en este apartado. Este hecho se podría enfocar para obtener nuevas demostraciones independientes del estado del teorema de Kochen-Specker de la imposibilidad de asignar variables ocultas locales no contextuales<sup>14</sup> en la MC [188]. Mermin derivó demostraciones dependientes del estado a partir versión de Peres de la demostración del teorema de Kochen-Specker [189], y de su propia simplificación [190, 191] de la demostración GHZ [49, 192]. En la Ref. [182] hay una demostración independiente del teorema de Kochen-Specker basada en la demostración AVN introducida en este apartado y que puede transformarse en una demostración del teorema de Bell<sup>15</sup>.

Resumiendo, la demostración presentada en este apartado, es del tipo de las demostraciones de Hardy, y puede ser reorganizada como una demostración GHZ con sólo dos observadores. Esta demostración es válida para estados máximamente entrelazados. Permite, por un lado, derivar una desigualdad de Bell comprobable experimentalmente, y por otro, conduce a una demostración del teorema de Kochen-Specker dependiente del estado. De este modo es posible mostrar una perspectiva más amplia entre las relaciones de los teoremas de Kochen-Specker y Bell.

<sup>14</sup>Las variables ocultas no contextuales son aquellas que asignan valores predefinidos a observables físicos, asumiendo que tales valores no dependen de los observables físicos compatibles junto con los que se midan.

<sup>15</sup>Es precisamente esta característica lo que la diferencia de la demostración de Mermin de la Ref. [189], pues al contener únicamente operadores no locales, no puede transformarse en una demostración del teorema de Bell.

Esta demostración pudo ser comprobada experimentalmente en el año 2005 [71, 72]. En la Ref. [71] se emplean estados de pares de fotones entrelazados en polarización y momento lineal. Las funciones de correlación de este experimento reproducen con una alta fidelidad las correlaciones perfectas predichas por la MC (7.34a)-(7.34i), pues sólo el 4% de los eventos detectados admiten una interpretación realista local. Como se trata de un porcentaje tan bajo, su presencia se puede justificar por imprecisiones experimentales. El valor de la función de correlación total es:  $F = 8,5694 \pm 0,00533$ . El resultado de la Ref. [72] para  $F$  es del mismo orden,  $F = 8,114 \pm 0,001$ .

En la línea del desarrollo de nuevas demostraciones del teorema de Bell, surge la cuestión de si son posibles demostraciones AVN con dos observadores realizando medidas de un solo qubit. En el próximo apartado veremos el recurso cuántico que se empleó para este tipo de demostraciones.

### 7.5.3. Demostraciones AVN del teorema de Bell con dos observadores empleando medidas en un solo qubit

La demostración AVN de dos observadores anterior [181, 182] posee dos desventajas frente a la demostración GHZ [45]:

- 1) Es más compleja en el sentido en que requiere un mayor número de predicciones cuánticas.
- 2) Proporciona menos evidencia contra el realismo local.

Estas dos desventajas están relacionadas, pues en la demostración AVN de dos observadores, 8 de las 9 correlaciones perfectas (es decir, el 89% del total) pueden explicarse mediante alguna teoría realista local; mientras que en la demostración GHZ, sólo 3 de las 4 correlaciones perfectas (es decir, el 75%) se puede explicar mediante una teoría realista local. Con lo cual, la eficiencia de detección necesaria para la demostración AVN bipartita anterior será más alta que para una demostración GHZ de tres observadores.

En la nueva demostración AVN del teorema de Bell con dos observadores [17, 18], únicamente son necesarias 4 correlaciones perfectas. El recurso que se emplea para obtenerla es un estado  $|LC_4\rangle$  de cuatro qubits y dos fotones. Cada fotón posee dos qubits. Un estado de este tipo, se puede obtener entrelazando dos grados de libertad, polarización y momento lineal, en cada fotón [48]. Los estados que se obtienen codificando diferentes grados de libertad en una misma partícula se denominan estados *hiperentrelazados*. La ecuación correspondiente al estado  $|LC_4\rangle$  obtenido es (7.42).

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}(|Hu\rangle_1|Hu\rangle_2 + |Hd\rangle_1|Hd\rangle_2 + |Vu\rangle_1|Vu\rangle_2 - |Vd\rangle_1|Vd\rangle_2) \\ &= \frac{1}{2}(|HuHu\rangle + |HdHd\rangle + |VuVu\rangle - |VdVd\rangle). \end{aligned} \quad (7.42)$$

$|H\rangle_j$  y  $|V\rangle_j$  representan la polarización horizontal y vertical respectivamente;  $|u\rangle_j$  y  $|d\rangle_j$  son dos posibles caminos (i.e., dirección de los momentos lineales de las partículas) ortogonales, up y

down, para el fotón  $j$ .

De acuerdo con los grados de libertad de polarización del fotón  $j$ , los observables locales son los siguientes

$$X_j = |H\rangle_j\langle V| + |V\rangle_j\langle H|, \quad (7.43a)$$

$$Y_j = i(|V\rangle_j\langle H| - |H\rangle_j\langle V|), \quad (7.43b)$$

$$Z_j = |H\rangle_j\langle H| - |V\rangle_j\langle V|. \quad (7.43c)$$

Análogamente, para los tres grados de libertad del momento los observables son

$$x_j = |u\rangle_j\langle d| + |d\rangle_j\langle u|, \quad (7.44a)$$

$$y_j = i(|d\rangle_j\langle u| - |u\rangle_j\langle d|), \quad (7.44b)$$

$$z_j = |u\rangle_j\langle u| - |d\rangle_j\langle d|. \quad (7.44c)$$

Hay un total de dos fotones, y los cuatro qubits se distribuyen como aparece en la Fig. 7.7. Cada

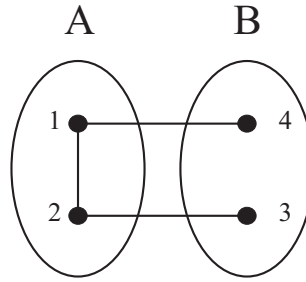


Figura 7.7: Estado  $|LC_4\rangle$  que representa a un sistema de dos fotones entrelazados en polarización y momento. Los qubits vienen representados por puntos, y los fotones (observadores/partes) por óvalos. Cada fotón posee dos qubits, uno de polarización y otro de momento. Los fotones están separados por un intervalo de género espacio.

observable puede tener sólo dos posibles valores:  $+1$  y  $-1$ . El estado  $|\Psi\rangle$  satisface las siguientes ecuaciones

$$X_1 z_1 X_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45a)$$

$$Y_1 z_1 Y_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45b)$$

$$Z_1 y_1 y_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45c)$$

$$z_1 z_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45d)$$

$$X_1 X_2 z_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45e)$$

$$Y_1 Y_2 z_2 |\Psi\rangle = -|\Psi\rangle, \quad (7.45f)$$

$$x_1 Z_2 x_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45g)$$

$$X_1 x_1 Y_2 y_2 |\Psi\rangle = |\Psi\rangle, \quad (7.45h)$$

$$Y_1 x_1 X_2 y_2 |\Psi\rangle = -|\Psi\rangle. \quad (7.45i)$$

Las cantidades físicas que representan los observables que aquí aparecen satisfacen el criterio de elemento de realidad de EPR. Veamos, las ecuaciones (7.45e), (7.45f) y (7.45g), permiten predecir los valores  $v(X_1)$ ,  $v(Y_1)$  y  $v(x_1)$ , que corresponden a los qubits de Alicia, a partir de las respectivas medidas de los pares de observables  $X_2, z_2$ ;  $Y_2, z_2$ ; y  $x_2, Z_2$ , sobre los qubits de Bob. Estas medidas no afectan a las predicciones sobre Alicia, porque Alicia y Bob están separados por un intervalo de género espacio. En las ecuaciones (7.45a), (7.45b), (7.45c), y (7.45d) se puede aplicar este mismo razonamiento para los valores  $v(X_2)$ ,  $v(Y_2)$ ,  $v(y_2)$  y  $v(z_2)$ . Las medidas de los observables compatibles de un mismo fotón son independientes, en el sentido en que la medida de uno de ellos no cambia el valor de la del otro. Por ejemplo, si medimos  $z_2$ , esto no va a cambiar el valor de  $X_2$ , porque  $X_2$  se puede predecir con certeza a partir de las medidas de  $X_1$  y  $z_1$  (ver (7.45a)) realizadas por otro observador espacialmente separado. Luego todos los resultados satisfacen todos los requisitos para ser considerados elementos de realidad, y como tales, no dependen del orden elegido para realizar las medidas pues sus valores existen incluso antes de ser medidos.

Del conjunto de ecuaciones (7.45a)-(7.45i) se puede extraer otro que encierre la contradicción característica de las demostraciones tipo AVN. Esas ecuaciones son: (7.45a), (7.45b), (7.45d) y (7.45e). Si las reescribimos en términos de los valores de las medidas

$$v(X_1) = v(X_2)v(z_2), \quad (7.46a)$$

$$v(Y_1) = -v(Y_2)v(z_2), \quad (7.46b)$$

$$v(X_1)v(x_1) = v(Y_2)v(y_2), \quad (7.46c)$$

$$v(Y_1)v(x_1) = v(X_2)v(y_2). \quad (7.46d)$$

Las variables sólo pueden sustituirse por  $+1$  ó  $-1$ . Al multiplicar los términos de la derecha de las ecuaciones (7.46a)-(7.46d) e igualarlos con el resultado del producto de los términos de la izquierda, se obtiene la contradicción,  $1 = -1$ , como demostración del teorema de Bell.

Las demostraciones de tipo AVN se siguen directamente de las correlaciones perfectas predichas por la mecánica cuántica. Su verificación experimental en un laboratorio ideal, requeriría repetir un elevado número de veces el experimento destinado a la comprobación de cada una de las ecuaciones (7.46a), (7.46b) y (7.46c). Para la última ecuación, se procede de la misma manera, y, cuando se obtienen los resultados de los experimentos, se comparan con el del producto de los resultados de los experimentos de las ecuaciones anteriores. En los laboratorios no ideales, las correlaciones obtenidas no son perfectas, y, al igual que en la sección anterior, es conveniente derivar una desigualdad de Bell para la comprobación de la demostración AVN. Dicha desigualdad de Bell debe violarse con un margen lo suficientemente amplio como para que las imperfecciones reales no puedan afectar a la validez de los resultados.

Si el operador  $\hat{O}$  es  $\hat{O} = X_1X_2z_2 - Y_1 - Y_2z_2 + X_1x_1Y_2y_2 + Y_1x_1X_2y_2$ , las predicciones por parte de cualquier teoría LHTV establecen que  $\langle \hat{O} \rangle \leq 2$ . Mientras que las predicciones cuánticas conducen a  $\langle \hat{O} \rangle = 4$ , que es el mismo límite que obtuvo Mermin en la demostración GHZ [45], pero a diferencia de éste, sólo son necesarios dos observadores, como en la desigualdad de Bell original.

El empleo del estado hiperentrelazado (7.42) ofrece una clara ventaja sobre aquel que se

construía a base de dos productos de estados de Bell [181, 182], y es que sólo se precisa de cuatro operadores de correlación, frente a los nueve de la descripción anterior. Esto equivale a que la realización de experimentos con estados hiperentrelazados requiere de una eficiencia de fotodetección más baja para lograr un resultado aceptable, pues se necesita menos evidencia para su comprobación.

Esta violación fue comprobada experimentalmente en el año 2007 [48]. El recurso utilizado fue un estado de cuatro qubits y dos fotones, construido mediante una técnica de óptica lineal que consiste en entrelazar los grados de libertad de polarización y momento lineal de dos fotones. Primero se comprobó que los observables locales eran elementos de realidad EPR, y posteriormente se construyó el operador  $\hat{O}$  con un resultado para  $\langle \hat{O} \rangle$  de  $3,4145 \pm 0,0095$ .



## Capítulo 8

# Demostraciones “all-versus-nothing” bipartitas del teorema de Bell usando qubits

### 8.1. Introducción

El teorema de Bell [41] y las posteriores versiones de su demostración, pusieron de manifiesto que la MC no puede ser reformulada a través de una teoría de variables ocultas locales. Las implicaciones de las demostraciones del teorema de Bell derivaron en el nacimiento de nuevas teorías como la Información y Computación Cuánticas, cuyas aportaciones favorecen el desarrollo de las nuevas tecnologías.

La demostración GHZ [44, 46] del teorema de Bell es considerada como el caso más fuerte contra el realismo local desde el teorema de Bell. No contiene desigualdades y forma parte del grupo de demostraciones “all-versus-nothing” (AVN) del teorema de Bell [46]. A diferencia del teorema original de Bell, la versión GHZ requiere de tres observadores en lugar de dos, debido a que únicamente con tres observadores se satisface el criterio EPR de elemento de realidad. Si recuperamos este criterio y lo aplicamos al caso bipartito de una demostración AVN, entonces, dados dos observadores, Alicia y Bob, separados espacialmente será posible predecir con certeza los resultados de las medidas realizadas por Alicia (Bob) a partir de los resultados de las medidas realizadas por Bob (Alicia).

En el capítulo 7 hicimos un estudio de las primeras demostraciones de tipo AVN insistiendo en las primeras demostraciones bipartitas usando qubits [181, 182] (adaptadas posteriormente para dos fotones [193]). En su verificación experimental [71, 72] esta demostración presentaba la dificultad de realizar medidas conjuntas de dos qubits. Posteriormente, se publicó una demostración [17, 18] en la que únicamente se empleaban medidas de un solo qubit. El recurso empleado para su verificación experimental, fue un estado hiperentrelazado de dos fotones y 4 qubits entrelazados en polarización y momento lineal [48]. Cada observador podía acceder a un fotón y a sus dos qubits.

La posibilidad de preparar estados hiperentrelazados de  $n$  qubits y  $m$  partículas, como los

estados de 6 qubits y 2 partículas [51, 52], los de 6 qubits 4 partículas [28], los de 8 qubits y 4 partículas [29], y los de 10 qubits 5 partículas [29]; condujeron de forma natural al siguiente problema:

Si  $n$  qubits fueran distribuidos entre dos partes, ¿cuáles son los estados puros cuánticos y las posibles distribuciones que permiten demostraciones AVN empleando medidas de un solo qubit?

Este problema está relacionado con el de decidir qué estados de  $n$ -qubits y qué distribuciones permiten desigualdades de Bell de tipo EPR [50, 53], y con nuevos problemas de complejidad de comunicación bipartitas, concretamente con nuevos esquemas de pseudotelepatía cuántica.

El contenido de este capítulo se distribuye como sigue: En las secciones 8.2 y 8.3 mostraremos la condición necesaria y suficiente para la existencia de demostraciones AVN bipartitas (BAVN), usando únicamente medidas de un solo qubit para estados hiperentrelazados de cualquier número de qubits. En la sección 8.4 proporcionaremos explícitamente todas las demostraciones BAVN distintas empleando estados grafo de hasta  $n = 7$  qubits.

## 8.2. Requisitos para una demostración BAVN. Estados grafo

Dado un estado cuántico de  $n$  qubits para obtener una demostración de tipo BAVN, las medidas de un solo qubit deben satisfacer los siguientes requisitos:

(a) Correlaciones perfectas para definir elementos de realidad EPR bipartitos. Todo observable de un solo qubit involucrado en la demostración debe satisfacer el criterio EPR de elementos de realidad.

(b) Correlaciones perfectas que contradigan los elementos de realidad EPR. Los observables que satisfagan la condición EPR no pueden tener resultados predefinidos, pues debe ser imposible asignarles valores que satisfagan todas las correlaciones perfectas predichas por la MC.

Las correlaciones perfectas son necesarias para establecer los elementos de realidad y probar que son incompatibles con la MC. Por este motivo, estamos interesados en estados que sean simultáneamente autoestados de un número suficientemente alto de operadores que se puedan expresar como  $n$  productos tensoriales de operadores de un solo qubit. El máximo número de operadores de un solo qubit que anticonmutan es tres. Sin pérdida de generalidad, podremos restringir nuestra atención al un conjunto de operadores de un solo qubit formado por las matrices de Pauli:  $X = \sigma_x$ ,  $Y = \sigma_y$  y  $Z = \sigma_z$ . Esto nos conduce al concepto de estado estabilizador. Un estado estabilizador (capítulo 1) es un estado que es simultáneamente autoestado de un conjunto de  $n$  elementos independientes del grupo de Pauli  $P_n$  que conmutan entre sí y de autovalor  $+1$ . Los  $n$  elementos independientes (los conocidos como operadores generadores estabilizadores), lo son en el sentido en que ninguno de ellos se puede escribir como producto de los otros, y generan un subgrupo máximamente abeliano llamado grupo estabilizador del estado. Como sabemos, un grupo estabilizador de estas características contiene  $2^n$  operadores estabilizadores,

que conformarán las correlaciones perfectas que necesitamos para las demostraciones.

Dado que cualquier estado estabilizador es equivalente a un estado grafo bajo transformaciones locales del grupo de Clifford [5, 30, 31], podremos restringir nuestra atención en los estados grafo [1, 2]. Actualmente, los estados grafo están omnipresentes en la teoría de la información cuántica por su papel en la corrección cuántica de errores [4, 61], en la computación cuántica basada en medidas [6, 9], o en su uso para el estudio de la clasificación del entrelazamiento [1, 2, 21, 22]. Los primeros estados grafo de  $n$  qubits con  $n > 2$  fueron los estados GHZ, y aparecieron en el contexto de las demostraciones AVN. No es entonces sorprendente que en la obtención de demostraciones BAVN, se recurra a los estados grafo. Por otro lado, ya se vislumbraba que este recurso cuántico podría ser adecuado cuando DiVincenzo y Peres mostraron que el requisito (b) no sólo era satisfecho por los estados GHZ sino también por cualquier código de palabras empleado en la corrección cuántica de errores [194], así mismo Scarni *et al.* mostraron que (b) también se satisfacía para estados cluster construidos a partir de estructuras clusters de cualquier dimensión [13] (ver Fig. 3.6). Por último, el hecho de que los estados grafo conexos de hasta 7 qubits hubieran sido exhaustivamente clasificados [1, 2], unido a la capacidad experimental actual de preparación de muchos de ellos, favoreció el empleo de los estados grafo como recurso en la obtención de demostraciones BAVN. Por lo tanto, el problema planteado inicialmente se reduce al siguiente:

Si  $n$  qubits fueran distribuidos entre 2 partes/observadores, ¿cuáles son los estados grafo de  $n$  qubits y las posibles distribuciones de qubits que permiten una demostración AVN bipartita usando únicamente observables de un solo qubit?

### 8.3. Correlaciones perfectas que contradicen los elementos de realidad EPR

Demostraremos que el requisito (b) del apartado 8.2 es satisfecho por cualquier estado grafo.

Lema 1. Cualquier estado grafo asociado con un grafo conexo de tres o más vértices conduce a una contradicción algebraica con el concepto de elemento de realidad.

Este resultado fue anticipado en [2, 13, 194]. El interés de la demostración del lema 1 está en proporcionar métodos para obtener ejemplos explícitos de conjuntos de correlaciones perfectas que satisfagan (b).

Demostración. Si el qubit  $i$  está conectado con el qubit  $j$ , y el  $j$  está conectado con el qubit  $k$ , hay dos posibilidades. Una es que  $i$  no esté conectado a  $k$ . Entonces, no existe ninguna teoría que asigne valores predefinidos,  $-1$  ó  $1$ , a  $Y_i, Z_i, X_j, Y_j, Y_k$  y  $Z_k$ , simultáneamente satisfaciendo las cuatro ecuaciones

$$g_i g_j |G\rangle = |G\rangle, \quad Y_i Y_j Z_k |G\rangle = |G\rangle, \quad (8.1a)$$

$$g_j |G\rangle = |G\rangle, \quad Z_i X_j Z_k |G\rangle = |G\rangle, \quad (8.1b)$$

$$g_j g_k |G\rangle = |G\rangle, \quad Z_i Y_j Y_k |G\rangle = |G\rangle, \quad (8.1c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad Y_i X_j Y_k |G\rangle = -|G\rangle, \quad (8.1d)$$

dado que  $g_i g_j \cdot g_j \cdot g_j g_k$  (donde con  $\cdot$  indicamos el producto entre los operadores) no es igual que  $g_i g_j g_k$  (como se espera en cualquier teoría de valores predefinidos), sino que es igual que  $-g_i g_j g_k$ . Hemos empleado la notación usual,  $g_\alpha$ , para representar los operadores generadores.

La otra posibilidad es que el qubit  $i$  esté también conectado al qubit  $k$ . Entonces, no existe una teoría que asigne los valores predefinidos  $-1$  ó  $1$ , a  $X_i, Z_i, X_j, Z_j, X_k$  y  $Z_k$ , simultáneamente satisfaciendo las cuatro ecuaciones.

$$g_i |G\rangle = |G\rangle, \quad X_i Z_j Z_k |G\rangle = |G\rangle, \quad (8.2a)$$

$$g_j |G\rangle = |G\rangle, \quad Z_i X_j Z_k |G\rangle = |G\rangle, \quad (8.2b)$$

$$g_k |G\rangle = |G\rangle, \quad Z_i Z_j X_k |G\rangle = |G\rangle, \quad (8.2c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad X_i X_j X_k |G\rangle = -|G\rangle, \quad (8.2d)$$

dado que  $g_i g_j g_k$  es igual a  $-g_i g_j g_k$ . Cualquier conjunto de ecuaciones asociadas a operadores estabilizadores que contengan un subconjunto que satisfaga (b) también satisfará (b). Por lo tanto, dado un estado grafo asociado a un grafo conexo de  $n > 3$  vértices, habrá cientos de posibles subconjuntos distintos satisfaciendo (b). La mayor parte de ellos involucra las tres matrices de Pauli, pero otros no. Sin embargo, en nuestras demostraciones BAVN es importante que las tres matrices de Pauli de todos y cada uno de los qubits de Alicia (Bob) puedan ser considerados como elementos de realidad, porque estamos interesados en nuevas demostraciones BAVN que impliquen a las nuevas clases de estados grafo, y no en aquellas que son meras consecuencias de los estados grafo de pocos qubits considerados anteriormente.

Por tanto, el problema que tenemos que resolver es averiguar para qué estados grafo y distribuciones, las tres matrices de Pauli son elementos de realidad de un solo qubit en un escenario bipartito.

## 8.4. Estados grafo y distribuciones de qubits que permiten demostraciones BAVN

Una distribución de  $n$  qubits entre Alicia y Bob se dice que permite *elementos de realidad bipartitos* cuando, para todos y cada uno de los qubits, los resultados de las medidas de dos matrices de Pauli sobre el qubit  $j$  de Alicia (Bob) pueden ser predichos con certeza únicamente a partir de los resultados de las medidas sobre los qubits de Bob (Alicia).

Definimos el *estabilizador reducido* de los qubits de Alicia (Bob) como aquel que se obtiene eliminando las contribuciones de los qubits de Bob (Alicia). Una condición necesaria y suficiente para la existencia de elementos de realidad bipartitos es la siguiente:

**Lema 2.** Una distribución de  $n$  qubits entre Alicia (a quien se le da  $n_A$  qubits) y Bob (a quien se le da  $n_B = n - n_A$  qubits) permite elementos de realidad bipartitos si y sólo si  $n_A = n_B$ , y el estabilizador reducido de los qubits de Alicia (Bob) contiene todas las posibles variaciones con repetición  $I, X, Y$  y  $Z$ , tomadas de  $n_A$  ( $n_B$ ) en  $n_A$  ( $n_B$ ), sin que se repita ninguna.

**Demostración.** Supongamos que dos matrices de Pauli de los qubits de Alicia, por ejemplo,  $X_1$  e  $Y_1$ , son elementos de realidad. Entonces, se deben poder predecir con certeza a partir de

las medidas de Bob. Luego el estabilizador reducido de los qubits de Alicia debe contener

$$X_1 \otimes I_2 \otimes \dots \otimes I_{n_A}, \quad (8.3a)$$

$$Y_1 \otimes I_2 \otimes \dots \otimes I_{n_A}. \quad (8.3b)$$

Por lo tanto, dado que la tercera matriz de Pauli del qubit 1 de Alicia se obtiene a partir del producto de las ecuaciones (8.3a) y (8.3b), ésta también debe ser un elemento de realidad y pertenecer al estabilizador reducido de los qubits de Alicia

$$Z_1 \otimes I_2 \otimes \dots \otimes I_{n_A}. \quad (8.4)$$

Lo mismo debe ocurrir con las tres matrices de Pauli del resto de qubits de Alicia,  $2, \dots, n_A$ . Por lo tanto, el estabilizador reducido de los qubits de Alicia deben contener también

$$I_1 \otimes X_2 \otimes I_3 \otimes \dots \otimes I_{n_A}, \quad (8.5a)$$

$$I_1 \otimes Y_2 \otimes I_3 \otimes \dots \otimes I_{n_A}, \quad (8.5b)$$

$$I_1 \otimes Z_2 \otimes I_3 \otimes \dots \otimes I_{n_A}, \dots, \quad (8.5c)$$

$$I_1 \otimes \dots \otimes I_{n_A-1} \otimes Z_{n_A}. \quad (8.5d)$$

Además, el estabilizador reducido de los qubits de Alicia deben contener todos los posibles productos de las ecuaciones (8.3a), (8.3b), (8.4), (8.5a)-(8.5d); es decir, todas las variaciones con repetición de  $I, X, Y$ , y  $Z$ , escogidos de  $n_A$  en  $n_A$ , lo que equivale a  $4^{n_A} = 2^{2n_A}$  (que debe coincidir con  $2^n$ , pues a través de las variaciones con repetición hemos obtenido la cantidad total de operadores estabilizadores que es posible obtener). Un razonamiento análogo se puede aplicar sobre las tres matrices de Pauli de todos y cada uno de los qubits de Bob, de modo que su estabilizador reducido contiene también todos los posibles productos de

$$X_{n_A+1} \otimes I_{n_A+2} \otimes \dots \otimes I_{n_B}, \dots, \quad (8.6a)$$

$$I_{n_A+1} \otimes \dots \otimes I_{n_B-1} \otimes Z_{n_B}. \quad (8.6b)$$

Pero el estabilizador total contiene sólo  $2^{n_A+n_B} = 2^n$  términos, que tal y como acabamos de deducir, debe ser a su vez igual a  $2^{2n_A}$  ( $2^{2n_B}$ ). Luego, la única posibilidad es que  $n_A = n_B$ . Obsérvese que la opción de que se generen variaciones con repetición repetidas no es viable porque nunca interviene los mismos operadores en los distintos productos. Basándonos en este resultado, sólo los estados grafo con un número par de qubits satisfacen el lema 2, y dado que es una condición necesaria y suficiente, al aplicarse sobre todas las posibles distribuciones de qubits de todos los estados grafo posibles, obtenemos una completa clasificación de todas las posibles demostraciones BAVN.

Para nuestros propósitos, disponíamos de los estados grafo de la clasificación de Hein *et al.* [1, 2], donde figuran los representantes óptimos de cada clase de equivalencia de todos los estados grafo con menos de 8 qubits. Los grafos pertenecientes a una misma clase de equivalencia son aquellos equivalentes bajo complementación local.

Si un estado grafo con sus qubits distribuidos de una forma determinada satisface el lema 2, entonces todos aquellos estados grafo que pertenezcan a su misma clase de equivalencia satisfarán este mismo lema para dicha distribución, y permitirán una demostración BAVN. Esto

es porque la clase de equivalencia de un estado grafo dado se obtiene aplicando operaciones de complementación local, que como sabemos, constituyen la descripción gráfica de las operaciones del grupo local de Clifford las cuales se caracterizan por transformar el grupo de Pauli  $P_n$  en sí mismo bajo conjugación, manteniendo intacta la matriz identidad (capítulo 5). Por lo tanto, una distribución bipartita de los qubits de un estado grafo que permita elementos de realidad, lo seguirá haciendo después de que se aplique cualquier operación de complementación. Por ejemplo, tomemos la distribución de qubits representada por el esquema 4a de la Fig. 8.2. Los elementos de realidad para los qubits de Alicia y Bob son:

Qubits de Alicia:

$$X_1 I_2 = Z_3 X_4, \quad I_1 X_2 = X_3 Z_4, \quad (8.7a)$$

$$Y_1 I_2 = Y_3 X_4, \quad I_1 Y_2 = X_3 Y_4, \quad (8.7b)$$

$$Z_1 I_2 = X_3 I_4, \quad I_1 Z_2 = I_3 X_4. \quad (8.7c)$$

Qubits de Bob:

$$X_3 I_4 = Z_1 I_2, \quad I_3 X_4 = I_1 Z_2, \quad (8.8a)$$

$$Y_3 I_4 = Y_1 Z_2, \quad I_3 Y_4 = Z_1 Y_2, \quad (8.8b)$$

$$Z_3 I_4 = X_1 I_2, \quad I_3 Z_4 = I_1 X_2. \quad (8.8c)$$

Si aplicamos una operación de complementación local sobre el vértice 1 (ver Fig. 8.1), entonces las expresiones (8.7a)-(8.7c) y (8.8a)-(8.8c) se transformarán (salvo factor de fase) en

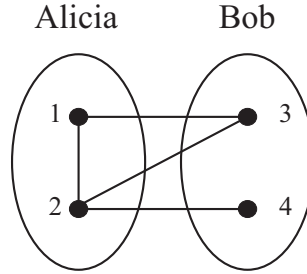


Figura 8.1: Estado grafo equivalente bajo complementación local sobre el qubit 1 al estado No. 4a de la Fig. 8.2. Esta distribución permite elementos de realidad bipartitos y demostraciones BAVN.

Qubits de Alicia:

$$X_1 I_2 = Z_3 X_4, \quad I_1 Y_2 = Y_3 Z_4, \quad (8.9a)$$

$$Z_1 I_2 = X_3 X_4, \quad I_1 X_2 = Y_3 Y_4, \quad (8.9b)$$

$$Y_1 I_2 = Y_3 I_4, \quad I_1 Z_2 = I_3 X_4. \quad (8.9c)$$

Qubits de Bob:

$$Y_3 I_4 = Y_1 I_2, \quad I_3 X_4 = I_1 Z_2, \quad (8.10a)$$

$$X_3 I_4 = Z_1 Z_2, \quad I_3 Y_4 = Y_1 X_2, \quad (8.10b)$$

$$Z_3 I_4 = X_1 I_2, \quad I_3 Z_4 = I_1 Y_2. \quad (8.10c)$$

Que siguen siendo elementos de realidad.

Hay sólo un estado grafo de 4 qubits

$$|\psi_{4a}\rangle = \frac{1}{2}(|00\rangle|\overline{00}\rangle + |01\rangle|\overline{01}\rangle + |10\rangle|\overline{10}\rangle - |11\rangle|\overline{11}\rangle), \quad (8.11)$$

donde  $|00\rangle|\overline{00}\rangle = |\sigma_z = 0\rangle_1 \otimes |\sigma_z = 0\rangle_2 \otimes |\sigma_x = 0\rangle_3 \otimes |\sigma_x = 0\rangle_4$ . La distribución de los qubits entre los observadores es tal que los qubits 1 y 2 pertenecen a Alicia, y los qubits 3 y 4 a Bob. El estado  $|\psi_{4a}\rangle$  corresponde al grafo No. 4 de acuerdo con la clasificación de Hein *et al.* [1, 2], y

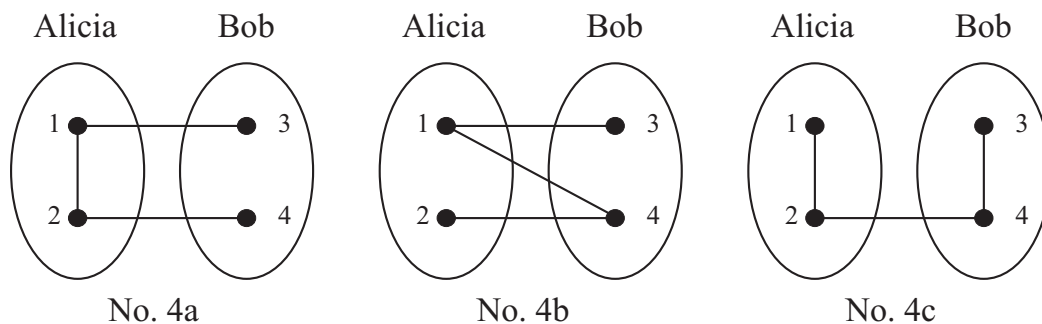


Figura 8.2: Distribuciones bipartitas del estado  $|LC_4\rangle$  (estado grafo No. 4 de la clasificación de Hein *et al.* [1, 2]). La distribución 4a permite elementos de realidad bipartitos y demostraciones BAVN. La distribución 4b es equivalente bajo LC a la 4a. La distribución 4c no es equivalente a ninguna de ellas y no permite elementos de realidad bipartitos.

con el 4a de la Fig. 8.2. Cualquier otra distribución no equivalente de qubits, no permite una demostración BAVN, como por ejemplo, la representación 4c de la Fig. 8.2. Esta demostración fue introducida en [17] y es la única (sin tener en cuenta las posibles representaciones equivalentes) con 4 qubits empleando medidas de un solo qubit. Entre los estados grafos No. 5 y No. 17 de la misma clasificación, hay sólo 6 estados cuyas distribuciones conducen a demostraciones BAVN. Todos ellos son estados grafos de 6 qubits, donde cada parte posee tres qubits. Sus correspondientes grafos se muestran en la Fig. 8.3. Las expresiones explícitas de cada estado grafo  $|G\rangle$  pueden venir dadas por los estabilizadores  $S$  correspondientes que se pueden obtener a partir de los grafos que los representan (capítulo 1).

Recientemente se han preparado en el laboratorio estados grafo de 6 qubits [25, 54], pero ninguno de ellos permitía demostraciones BAVN.

Las demostraciones BAVN del teorema de Bell consisten en una contradicción algebraica donde cada observable involucrado es un elemento de realidad bipartito. Su comprobación experimental consiste en repetir muchas veces cada experimento destinado a verificar cada igualdad que intervenga en la contradicción (capítulo 7 apartado 7.5.3). Estas demostraciones se emplearon para obtener desigualdades de Bell [14] tipo Mermin [184] para los estados grafo de hasta  $n = 6$  qubits distribuidos como en la sección 8.4. Tales distribuciones permiten los elementos de realidad bipartitos necesarios para su obtención. Dichas desigualdades presentan la más alta violación del realismo local (i.e., el más alto grado de no localidad<sup>1</sup>) de entre aquellas desigualdades obtenidas sólo con operadores estabilizadores.

Los avances experimentales de la última década en tecnología cuántica, permiten preparar estados de dos partículas con correlaciones casi perfectas, lo cual da pie al desarrollo de nuevas pruebas experimentales de desigualdades de Bell bipartitas de tipo EPR. Normalmente, para la comprobación experimental de este tipo de desigualdades se siguen dos estrategias [50]:

1. Relajar el criterio EPR y definir a los elementos de realidad como aquellos observables cuyos autovalores se pueden predecir con casi perfecta certeza [55]. Esta definición extendería automáticamente la validez de las desigualdad de Bell a todos los pares preparados.

2. La segunda estrategia, es válida sólo si se preparan pares tales que, una muy alta fracción de ellos permita una perfecta predecibilidad. Entonces, se puede asumir el criterio EPR original. En este caso, la desigualdad EPR es legítima sólo para una fracción de pares. Sin embargo, se pueden obtener resultados experimentales concluyentes realizando pruebas para todos los pares, y estimando cómo la fracción de pares para los cuales la desigualdad no es válida puede afectar a los resultados experimentales.

---

<sup>1</sup>El *grado de no-localidad* es una medida de la no-localidad de un estado. De acuerdo con el resultado de Mermin [49], la no-localidad de un sistema es mayor a medida que crece su tamaño (entendiendo por crecimiento de un sistema tanto si en éste aumenta su número inicial de partículas, como si se incrementa el número de grados de libertad por partícula como ocurre con los estados hiperentrelazados). Mermin obtuvo su resultado empleando desigualdades de Bell  $n$ -partitas obtenidas a partir de estados GHZ de  $n$  qubits, pero su comprobación experimental es complicada por la sensibilidad a la decoherencia que presentan estos estados y por la dificultad que conlleva realizar medidas sobre  $n$  sistemas espacialmente separados. Una posible solución a estos problemas es trabajar con estados hiperentrelazados. Las desigualdades de Bell de tipo EPR constituyen un medio fundamental para estudiar el crecimiento de la no-localidad de los estados hiperentrelazados. Mientras mayor sea el grado de no-localidad, mayor será el contraste entre el valor clásico esperado de un operador de Bell  $\beta$  de acuerdo con una teoría local de tipo EPR y las predicciones de la MC. El grado de no-localidad se puede emplear para el estudio de las eficiencias de los fotodetectores requeridas para para realizar experimentos libres del loophole asociado con la posibilidad de asignar elementos de realidad locales para satisfacer alguna desigualdad de Bell (mientras mayor sea el grado de no localidad menor será la eficiencia de detección requerida para verificar dichas desigualdades); por otro lado, el grado de no-localidad está también relacionado con la robustez que frente a la decoherencia presentan las violaciones de las desigualdades de Bell asociadas a ciertos estados.



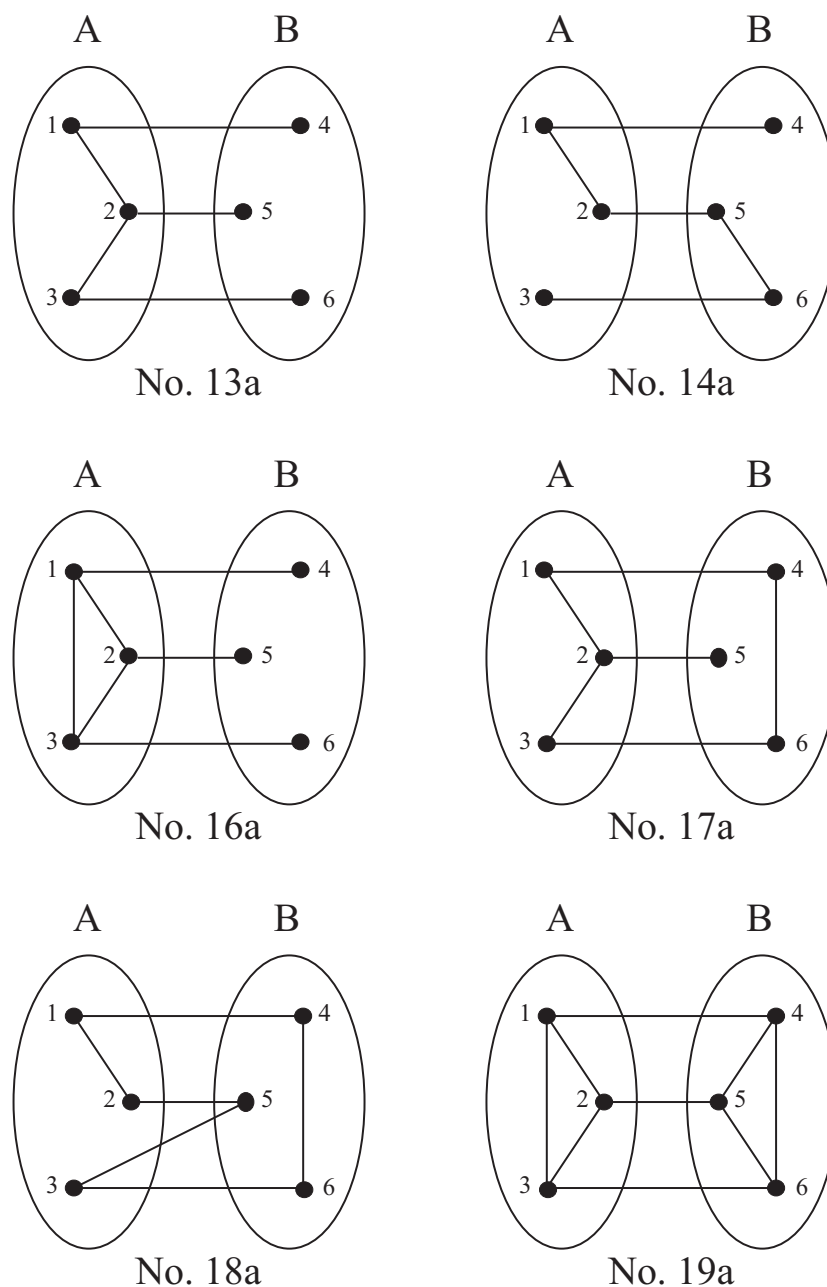


Figura 8.3: Distribuciones bipartitas de los estados grafo de 6 qubits que permiten elementos de realidad bipartitos y demostraciones BAVN. La nomenclatura de los grafos es la de la clasificación de Hein *et al.* [1, 2], pero las etiquetas de los qubits es distinta: Los qubits 1, 2 y 3 pertenecen a Alicia (A) y los etiquetados por 4, 5 y 6 a Bob (B).



## Capítulo 9

# Demostraciones “all-versus-nothing” $m$ -partitas del teorema de Bell usando qubits

### 9.1. Introducción

Las demostraciones AVN [46] del teorema de Bell [41] son consideradas como la vía para poner de manifiesto de la forma más directa el conflicto entre los elementos de realidad EPR y la Mecánica Cuántica. La primera demostración AVN fue obtenida por Heywood y Readhead [43]. Sin embargo, la demostración AVN más famosa es la de Greenberger, Horne, y Zeilinger (GHZ) [44, 45, 46]. La primera demostración AVN bipartita usando qubits y medidas de un solo qubit aparece en [17, 18]. El interés de restringirnos a las medidas de un solo qubit está motivado por la dificultad práctica que conlleva hacer medidas generales sobre  $N$  qubits ( $N \geq 2$ ) cuando los qubits están codificados en diferentes grados de libertad dentro de la misma partícula.

En los capítulos 7 y 8 hemos hecho una recopilación de algunas de las aportaciones más destacadas al desarrollo de este tipo de demostraciones. En el capítulo 8 mostramos una condición necesaria y suficiente para la existencia de demostraciones AVN bipartitas (BAVN), usando estados grafo de cualquier número de qubits [19], y obtuvimos las distribuciones de qubits que permiten este tipo de demostraciones para los estados grafo de la clasificación de Hein *et al.* [1, 2].

Recientemente, se han preparado experimentalmente estados de  $n$  qubits y  $m$  partículas ( $n > m$ ) que exhiben correlaciones perfectas. Por ejemplo, estados grafo de 6 qubits y 2 partículas [51, 52], de 6 qubits y 4 partículas [28], de 8 qubits y 4 partículas [29], y de 10 qubits y 5 partículas [29]. Para estos estados surge de forma natural el siguiente problema:

Consideremos  $m$  partes distantes; la parte  $i$  puede realizar medidas de un solo qubit sobre la partícula  $i$ , y la partícula  $i$  contiene  $n_i \geq 1$  qubits ( $\sum_{i=1}^m n_i = n$ ). ¿Cuáles son los estados de  $n$  qubits y  $m$  partículas que permiten demostraciones AVN  $m$ -partitas?

Este problema se resolvió para el caso de  $m = 2$  partículas/partes [19] (capítulo 8). En este

capítulo daremos la solución para un número arbitrario  $m$  de partículas/partes, y lo organizaremos como sigue:

Una demostración AVN  $m$ -partita es específica para un estado grafo de  $n$  qubits y  $m$  partículas cuando no hay un estado grafo con menos qubits que satisfaga las mismas correlaciones. En la sección 9.2.1 discutiremos los requisitos para que una demostración AVN  $m$ -partita sea específica de un estado grafo de  $n$  qubits y  $m$  partículas, y describiremos un método para decidir si un estado grafo de  $n$  qubits y  $m$  partículas permite una demostración AVN  $m$ -partita específica. Aplicaremos este método para decidir si algunos estados grafo de  $n$  qubits y  $m$  partículas preparados recientemente en los laboratorios permiten demostraciones AVN  $m$ -partitas. Como material suplementario [195], proporcionamos un programa escrito en Mathematica que se puede emplear para saber si un estado grafo dado de  $n$  qubits y  $m$  partículas permite una demostración  $m$ -partita específica.

En la sección 9.2.2 resolveremos el siguiente problema: Dado un estado grafo de  $n$  qubits, ¿cuál es el mínimo número  $m$  de partes que permite una demostración AVN  $m$ -partita específica? Se puede emplear el mismo programa [195] para obtener todas las distribuciones de un estado grafo de  $n$  qubits entre un número arbitrario  $m$  partes y todas las distribuciones entre un mínimo número de partes que permiten demostraciones AVN.

Con la solución de este problema se pueden obtener todas las distribuciones no equivalentes que permiten demostraciones AVN, pues cualquier distribución obtenida a partir de una que permita una demostración AVN específica, distribuyendo los qubits que originalmente pertenecían a una misma parte entre nuevas partes, también permitirá una demostración AVN. Como material suplementario, proporcionamos todas las distribuciones no equivalentes entre un mínimo número  $m$  de partes que permiten una demostración AVN  $m$ -partita específica para todos los estados grafo con  $n \leq 8$  qubits.

Los estados grafo de  $n$  qubits y  $m$  partículas que emplearemos para nuestros propósitos son los representantes óptimos de la clasificación de Hein *et al.* [1, 2] y los de la clasificación de Cabello *et al.* [21, 22].

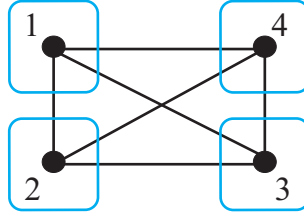
## 9.2. Demostraciones AVN $m$ -partitas con $n$ qubits

### 9.2.1. Demostraciones AVN $m$ -partitas específicas

Se dice que una demostración AVN  $m$ -partita es específica de un estado grafo dado de  $n$  qubits y  $m$  partículas cuando no haya ningún estado grafo con menos qubits que satisfaga las mismas correlaciones.

Las correlaciones perfectas de cualquier estado grafo asociado a un grafo conexo de tres o más vértices conducen a contradicciones con el concepto de elemento de realidad cuando cada qubit se asigna a un observador (parte) distinto [14, 18, 19, 181, 194]. El problema está en averiguar si esas contradicciones son específicas para una determinada distribución de un estado grafo o de lo contrario se pueden obtener a partir de un estado grafo de menos qubits.

Por ejemplo, supongamos que tomamos la demostración AVN tetrapartita basada en las siguientes correlaciones perfectas correspondientes a la distribución del estado grafo  $|FC_4\rangle$  (que pertenece la clase de equivalencia bajo LC del estado  $|GHZ_4\rangle$ ) en la que cada qubit pertenece a un observador distinto, tal y como se muestra en la Fig. 9.1


 Figura 9.1: Distribución del estado grafo  $|FC_4\rangle$  entre 4 partes distintas.

$$X_1 Z_2 Z_3 Z_4 = 1, \quad g_1 = 1, \quad (9.1a)$$

$$Z_1 X_2 Z_3 Z_4 = 1, \quad g_2 = 1, \quad (9.1b)$$

$$Z_1 Z_2 X_3 Z_4 = 1, \quad g_3 = 1, \quad (9.1c)$$

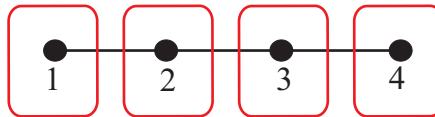
$$-X_1 X_2 X_3 Z_4 = 1, \quad g_1 g_2 g_3 = 1. \quad (9.1d)$$

Este es un ejemplo de una demostración AVN que no es específica del estado  $|FC_4\rangle$ . Si observamos las anteriores ecuaciones (donde los operadores generadores  $g_i$  están igualados a sus autovalores), es fácil percatarse de que se satisfacen independientemente del valor de  $Z_4$ , es decir, si prescindimos de  $Z_4$  obtendremos un sistema equivalente de ecuaciones que no se pueden satisfacer simultáneamente:

$$X_1 Z_2 Z_3 = Z_1 X_2 Z_3 = Z_1 Z_2 X_3 = -X_1 X_2 X_3. \quad (9.2)$$

La demostración anterior no es específica del estado  $|FC_4\rangle$  porque no se requiere de la partícula que contiene el cuarto qubit, ni para alcanzar la contradicción ni en la definición de los elementos de realidad involucrados en esta contradicción. Esta partícula sólo se ha empleado para medir  $Z_4$  y para transmitir el resultado. El único papel que ha desempeñado el resultado de  $Z_4$  ha sido garantizar que  $X_1$ ,  $Z_1$ ,  $X_2$ ,  $Z_2$ ,  $X_3$  y  $Z_3$  sean elementos de realidad en un escenario tetrapartito, luego su valor es irrelevante. Esta misma contradicción se obtiene a través de las correlaciones perfectas del estado  $|FC_3\rangle$  distribuido entre tres observadores.

El siguiente ejemplo es una muestra de cómo la especificidad de una demostración AVN puede depender de la forma en que se distribuyan los qubits entre las partes. Consideremos una demostración AVN basada en las siguientes correlaciones perfectas del estado  $|LC_4\rangle$ , cuyo grafo mostramos en la Fig. 9.2:


 Figura 9.2: Distribución del estado grafo  $|LC_4\rangle$  entre 4 partes distintas. Esta distribución no permite una demostración AVN específica para este estado.

$$Y_1 Y_2 Z_3 = 1, \quad g_1 g_2 = 1, \quad (9.3a)$$

$$Z_1 X_2 Z_3 = 1, \quad g_2 = 1, \quad (9.3b)$$

$$Z_1 Y_2 Y_3 Z_4 = 1, \quad g_2 g_3 = 1, \quad (9.3c)$$

$$-Y_1 X_2 Y_3 Z_4 = 1, \quad g_1 g_2 g_3 = 1. \quad (9.3d)$$

Si los qubits están distribuidos de forma que a cada parte le corresponda un qubit distinto (ver Fig. 9.2), la demostración no es específica porque la parte que posee el cuarto qubit no interviene, ni en la contradicción, ni en la definición de los elementos de realidad. Luego si eliminamos su contribución de las ecuaciones (9.3a)-(9.3d), obtendremos un sistema de ecuaciones que no se pueden satisfacer simultáneamente,

$$Y_1 Y_2 Z_3 = Z_1 X_2 Z_3 = Z_1 Y_2 Y_3 = -Y_1 X_2 Y_3. \quad (9.4)$$

Esta contradicción puede obtenerse igualmente a partir de las correlaciones perfectas del estado  $|LC_3\rangle$ . Sin embargo, si la distribución de qubits del  $|LC_4\rangle$  es tal que los qubits 1 y 4 pertenecen a Alicia, y los qubits 2 y 3 a Bob (ver Fig. 9.3), entonces la única forma de garantizar que, por ejemplo,  $X_2$  sea un elemento de realidad es introduciendo la correlación perfecta

$$Z_1 X_2 X_4 = 1, \quad (9.5)$$

que se obtiene a partir del estabilizador  $S$  del estado  $|LC_4\rangle$ . Obsérvese que la parte que posee el qubit 4 debe elegir entre al menos dos medidas. Por tanto, podemos concluir que una demostra-

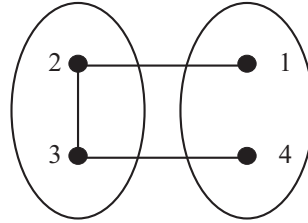


Figura 9.3: Distribución del estado grafo  $|LC_4\rangle$  entre 2 partes distintas. Esta distribución permite una demostración AVN específica para este estado.

ción AVN es específica para una distribución de un estado grafo dado de  $n$  qubits y  $m$  partículas si en ella aparecen al menos dos observables de cada qubit.

Dado que las correlaciones necesarias para definir los elementos de realidad pueden (junto con aquellas que ya se emplearon para la contradicción) conllevar contradicciones adicionales, es apropiado que los observables necesarios para garantizar que otros observables sean elementos de realidad (como  $X_4$  y  $Z_4$  en el ejemplo anterior), sean a su vez elementos de realidad. Por tanto, de ahora en adelante nos centraremos en las demostraciones AVN en las que al menos dos observables de cada qubit sean elementos de realidad. Si se trata de dos observables de Pauli, por ejemplo,  $X_i$  e  $Y_i$ , entonces el tercer observable de Pauli  $Z_i$  es también un elemento de realidad. En consecuencia nos centraremos sólo en aquellas distribuciones de estados grafo en las que los tres observables de Pauli de todos y cada uno de los qubits sean elementos de realidad.

### 9.2.2. ¿Cuándo una distribución permite una demostración AVN específica?

El siguiente problema es: Dada una distribución de un estado grafo de  $n$  qubits entre  $m$  partes, cómo decidir si es una de aquellas en las que todos los observables de Pauli de un solo qubit son elementos de realidad. Para dar una respuesta a esta cuestión, clasificaremos los  $2^n$  elementos del estabilizador de un estado grafo de  $n$  qubits cualquiera en cuatro clases:

1. Hay  $2^{n-2}$  operadores estabilizadores (esto es un cuarto de los elementos del estabilizador  $S$ ) que permiten predecir  $X_i$  a partir de los resultados de las medidas sobre otros qubits: aquellos que son producto del generador estabilizador  $g_i$ , un número par (desde ahora en adelante, el término “par” incluirá también el cero) de  $g_j$  con  $j \in N(i)$ , y un número arbitrario (en “número arbitrario” incluiremos también el cero) de  $g_k$ , con  $k \neq i$  y  $k \notin N(i)$ .

2. Hay un total de  $2^{n-2}$  operadores estabilizadores que permiten predecir  $Y_i$  a partir de los resultados de las medidas de otros qubits: aquellos que son producto de  $g_i$ , un número impar de  $g_j$  con  $j \in N(i)$  y un número arbitrario de  $g_k$ , con  $k \neq i$  y  $k \notin N(i)$ .

3. Hay un total de  $2^{n-2}$  operadores estabilizadores que permiten predecir  $Z_i$  a partir de los resultados de las medidas de otros qubits: aquellos que son producto de un número impar de  $g_j$  con  $j \in N(i)$  y un número arbitrario de  $g_k$ , con  $k \neq i$  y  $k \notin N(i)$ .

4. Hay un total de  $2^{n-2}$  operadores estabilizadores que contienen  $I_i$ : aquellos que son producto de un número par de  $g_j$  con  $j \in N(i)$  y un número arbitrario de  $g_k$ , con  $k \neq i$  y  $k \notin N(i)$ .

Cada partícula puede incluir más de un qubit, por lo que es conveniente denotar como  $P(i)$  al conjunto de qubits que están en la misma partícula que el qubit  $i$ . La clasificación de operadores estabilizadores que acabamos de introducir resulta de utilidad para lo siguiente:

Dada una distribución de un estado grafo de  $n$  qubits entre  $m$  partes,  $X_i$  es un elemento de realidad si y sólo si existe un operador estabilizador del estado grafo que satisface los dos requisitos siguientes:

- (1) No contiene  $g_j$  para todo  $j \in P(i)$  pero contiene un número par de  $g_k$  con  $k \in N(j)$ .
- (2) Contiene  $g_i$  y un número par de  $g_l$  con  $l \in N(i)$ .

Por ejemplo, consideremos el estado  $|LC_4\rangle$  distribuido de tal forma que Alicia posee los qubits 1 y 4, y Bob los qubits 2 y 3 (ver Fig. 9.3). Preguntemos entonces: ¿Es  $X_1$  un elemento de realidad? Esta pregunta es equivalente a ésta otra: ¿Hay un operador estabilizador tal que no contenga  $g_4$  [dado que  $P(1) = \{4\}$ ], pero contenga un número par (en este caso ha de ser necesariamente cero) de  $g_3$  [dado que  $N(4) = \{3\}$ ], contenga también a  $g_1$ , y a un número par (necesariamente cero) de  $g_2$  [dado que  $N(1) = \{2\}$ ]? La respuesta es sí; el único operador estabilizador con estas propiedades es  $g_1 = X_1 Z_2$ .

Del mismo modo,  $Y_i$  será un elemento de realidad si y sólo si hay al menos un operador estabilizador que satisfaga (1) y la siguiente condición:

- (3) Contiene  $g_i$  y un número impar de  $g_l$  con  $l \in N(i)$ .

Por último  $Z_i$  es un elemento de realidad si y sólo si hay un operador estabilizador que satisfaga (1) y la siguiente condición:

- (4) No contiene  $g_i$  pero contiene un número impar de  $g_l$  con  $l \in N(i)$ .

Conociendo estas reglas, el procedimiento a seguir para decidir si una distribución concreta permite una demostración AVN específica consiste en lo siguiente: Primero comprobamos para el qubit  $i$  si  $X_i$  e  $Y_i$  son elementos de realidad. Si alguno de ellos no lo es, entonces la distribución no permite una demostración AVN específica. Si, por el contrario, ambos son elementos de realidad entonces pasamos al qubit  $j$ , y comprobamos si  $X_j$  e  $Y_j$  son elementos de realidad, y así con todos los qubits. Si todos los  $X_i$  e  $Y_i$  son elementos de realidad, entonces la distribución permite una demostración AVN específica.

Hay casos simples en los que es fácil ver que una distribución no permite una demostración AVN. Por ejemplo, si alguna partícula engloba más de  $n/2$  qubits, entonces o bien (1) es incompatible con (2), o bien (1) es incompatible con (3) y (4). En la siguiente sección aportaremos una demostración alternativa. Si en una distribución el qubit  $i$  está conectado únicamente con qubits que pertenecen a la misma partícula, el requisito (1) es incompatible con el (3) y el (4). Como material suplementario, proporcionamos un programa en Mathematica [195] para decidir si un estado grafo de  $n$  qubits y  $m$  partículas permite una demostración AVN  $m$ -partita específica.

### 9.2.3. Ejemplos prácticos

Como ejemplo de aplicación de estas reglas, sería interesante discutir si algunos de los estados preparados en experimentos recientes permiten o no una distribución AVN específica asumiendo el escenario natural en que cada parte tiene una partícula (cada observador puede realizar medidas sobre los qubits de la partícula que le pertenece).

Precisamente se han preparado recientemente posibles distribuciones de estados de seis qubits y dos/cuatro partículas [52, 28]. En la Fig. 9.4 aparecen varias distribuciones del estado  $|LC_6\rangle$ , cada una de las cuales representa una forma diferente de preparación experimental del mismo estado. La Fig. 9.4(a) representa al estado  $|LC_6\rangle$  de 4 fotones preparados en la Ref. [28]. Esta distribución no permite una demostración AVN específica dado que el qubit 1 está conectado únicamente al qubit 2, siendo este su único vecino que además está englobado en la misma partícula; el qubit 6 se encuentra en una situación similar a la del qubit 1. La Fig. 9.4(b) representa al estado  $|LC_6\rangle$  de dos fotones preparado en la Ref. [52]. Esta distribución satisface todos los requisitos para permitir una demostración AVN específica. Además, es la única distribución bipartita de este estado que permite una demostración AVN específica [19]. Algunas distribuciones del estado  $|LC_6\rangle$  de 4 partículas que permiten demostraciones AVN se pueden obtener trivialmente a partir de la distribución de la Fig. 9.4(b) con solo separar qubits que



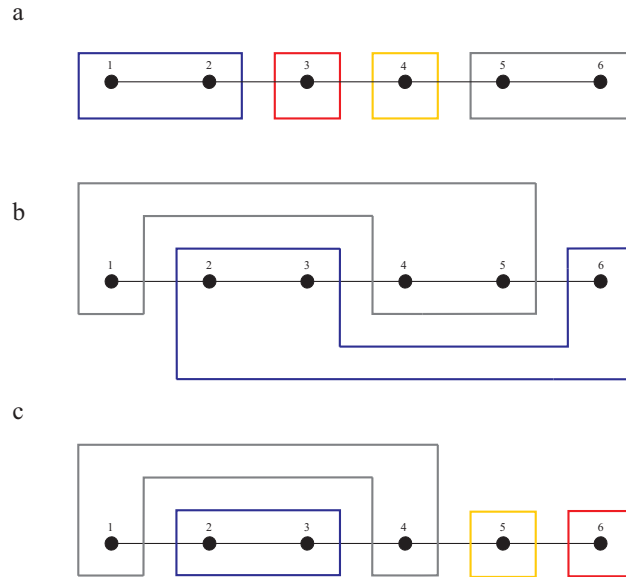


Figura 9.4: Diferentes distribuciones del estado grafo  $|LC_6\rangle$  entre dos y cuatro partículas. Cada recinto cuadrado representa a una partícula. (a) corresponde a un estado de 4 fotones preparado en la Ref. [28]. (b) corresponde a un estado de dos fotones preparado en la Ref. [52]. En (a) no todos los observables de Pauli de un solo qubit son elementos de realidad EPR, y por lo tanto la distribución no da lugar a una demostración AVN. Las distribuciones (b), (c) y (d) sí permiten demostraciones AVN.

pertenecen a la misma partícula en varias partículas. Por ejemplo, en la Fig. 9.4(c) se observa una distribución que permite una demostración AVN específica. No hay ninguna distribución en 4 partículas que permita una demostración AVN específica que no se pueda obtener de la distribución de la Fig. 9.4(b). Este estado fue construido con objeto de estudiar el grado de no-localidad<sup>1,2,3</sup>. Sólo aquellas distribuciones que permiten demostraciones AVN garantizan la existencia de elementos de realidad EPR para todos los observables de Pauli de un solo qubit de cualquier teoría local. Para estas distribuciones es posible construir demostraciones de tipo AVN

<sup>1</sup>Ver nota 1 del capítulo 8.

<sup>2</sup>El estado de la Fig. 9.4(b) posee la única distribución de seis qubits entre dos partículas cuyas correlaciones perfectas exhiben el mismo grado de no-localidad que el estado  $|GHZ_6\rangle$  [14], pero es más robusto contra la decoherencia. Este resultado muestra que las desigualdades de Bell para estados grafo podrían ser muy ventajosas a la hora de observar violaciones macroscópicas de las desigualdades de Bell. Además en lugar de requerir seis observadores separados, sólo se necesitan dos [19], y su grado de no-localidad es  $D = 1,7545 \pm 0,00700$ . La violación de su desigualdad de Bell representa el primer test experimental de no-localidad de un estado grafo de seis qubits. Por otro lado, al ser su grado de no-localidad más elevado que el de otros sistemas más simples, se pone de manifiesto que la no-localidad se incrementa con la complejidad de los sistemas.

<sup>3</sup>Sea  $\varrho$  el estado del sistema que no está afectado por ruido, y sea  $\varrho' = p\varrho + (1-p)I/2$  el mismo estado afectado por ruido. Si el ruido actúa sobre cada qubit por separado, entonces el valor de la desigualdad de Mermin decrece como  $p^6$  dado que está basada en correlaciones perfectas. En las nuevas desigualdades de Bell la mitad de los términos posee la identidad como operador de un solo qubit, lo que contribuye a un decaimiento dado por  $p^5$ , y el total de la violación decrece como  $(p^6 - p^5)/2$ .

y desigualdades óptimas de Bell [14] tipo Mermin [46]. El grado de no-localidad que exhibe este tipo de desigualdades es el más alto, pues dichas desigualdades presentan la más alta violación del realismo local de entre aquellas desigualdades obtenidas sólo con operadores estabilizadores.

Para la distribución de la Fig. 9.4(a) no tiene sentido obtener desigualdades de Bell tipo Mermin, porque no todos los observables locales son elementos de realidad.

La Fig. 9.5 contiene posibles distribuciones del estado grafo  $|Y_6\rangle$ . La Fig. 9.5(a) representa el estado de cuatro fotones preparado en la Ref. [28]: esta distribución no permite demostraciones AVN específicas dado que el qubit 1 está sólo conectado al qubit 2, y el qubit 5 está conectado sólo al qubit 4. Las Figs. 9.5(b)-(d) representan distribuciones del estado  $|Y_6\rangle$  entre cuatro partículas, y permiten demostraciones específicas AVN.

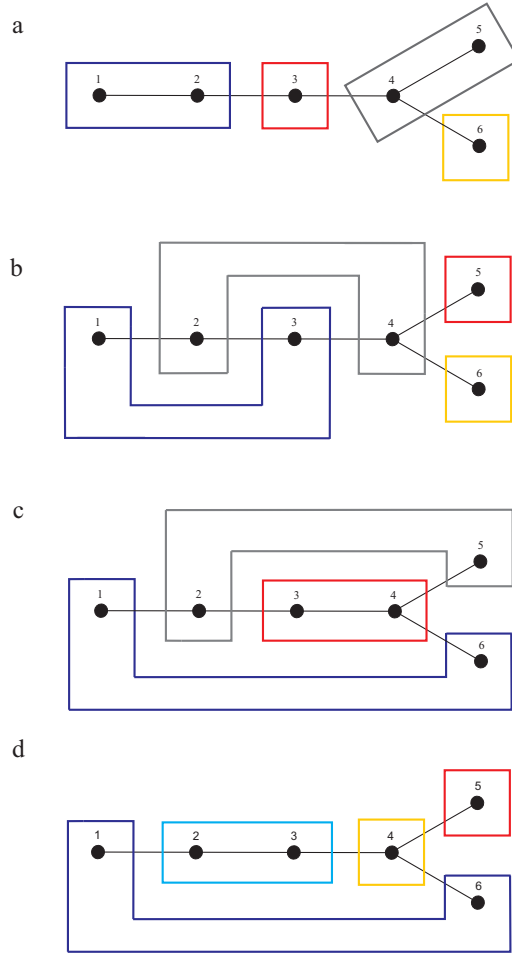


Figura 9.5: Diferentes distribuciones del estado grafo  $|Y_6\rangle$  entre cuatro partículas. (a) corresponde a un estado de cuatro fotones preparado en la Ref. [28] y no permite una demostración AVN específica. (b)-(d) permiten demostraciones AVN específicas.

Por tanto la aplicación de las reglas anteriores sobre los estados grafo nos permite determinar si una distribución admite o no demostraciones de tipo AVN. Además son determinantes para la construcción de aquellos estados grafo con los que obtener desigualdades de Bell óptimas tipo Mermin, con las que es posible avanzar en el estudio de la relación entre el crecimiento de la violación del realismo local y la decoherencia.

### 9.3. Demostraciones AVN con un mínimo número $m$ de partes

En la sección anterior, acabamos de ver que el estado  $|Y_6\rangle$  admite demostraciones AVN específicas cuando sus qubits se distribuyen adecuadamente entre cuatro partículas. Ahora la

cuestión es si  $|Y_6\rangle$  admite demostraciones AVN específicas cuando se distribuyen entre tres o menos partículas, o formulado de manera más general: Dado un estado grafo de  $n$  qubits, ¿cuál es el mínimo número de partes  $m$  que permite una demostración AVN  $m$ -partita específica para este estado?

### 9.3.1. Posibles distribuciones entre un mínimo número $m$ de partes

Introduciremos una condición necesaria para la existencia de elementos de realidad  $m$ -partitos.

La siguiente definición será útil para su demostración. Definimos el estabilizador reducido de los qubits de la partícula  $A$  como aquel obtenido a partir del estabilizador del estado original reemplazando los observables de los qubits de las otras partículas con matrices identidad.

Lema. Una distribución de  $n = n_{max} + n_B + \dots + n_m$  qubits entre  $m$  partes tal que  $n_{max} \geq n_B \geq \dots \geq n_m$  permite elementos de realidad  $m$ -partitos si y sólo si  $n_{max} \leq n_B + \dots + n_m$ .

Demostración. Supongamos que la partícula  $m_i$  engloba los qubits  $1, \dots, n_{max}$ , donde  $n_{max}$  es el máximo número de qubits correspondientes a cualquier partícula, y que la partícula  $m_j$  incluye los qubits  $n_{max} + 1, \dots, n_{max} + n_j$ . Si  $X_1, Y_1, Z_1, X_2, \dots, Z_{n_{max}}$  son elementos de realidad, entonces el estabilizador reducido de los qubits de  $m_i$  debe contener los elementos de realidad

$$X_1 \otimes I_2 \otimes \dots \otimes I_{n_{max}}, \quad (9.6a)$$

$$Y_1 \otimes I_2 \otimes \dots \otimes I_{n_{max}}, \quad (9.6b)$$

$$Z_1 \otimes I_2 \otimes \dots \otimes I_{n_{max}}, \quad (9.6c)$$

$$I_1 \otimes X_2 \otimes \dots \otimes I_{n_{max}}, \dots, \quad (9.6d)$$

$$I_1 \otimes I_2 \otimes \dots \otimes Z_{n_{max}}. \quad (9.6e)$$

Además, el estabilizador reducido de los qubits de  $m_i$  debe contener todos los posibles productos de las ecuaciones (9.6a)-(9.6e), esto es, todas las posibles variaciones con repetición de  $I, X, Y$  y  $Z$  escogidos de  $n_i$  en  $n_i$ , que hacen un total de  $4^{n_{max}} = 2^{2n_{max}}$ . Aplicamos un razonamiento similar sobre las tres matrices de Pauli de todos y cada uno de los qubits de  $m_j$ . Por lo tanto, el estabilizador reducido de los qubits de  $m_j$  debe contener también todos los posibles productos de

$$X_{n_{max}+1} \otimes I_{n_{max}+2} \otimes \dots \otimes I_{n_{max}+n_j}, \dots, \quad (9.7a)$$

$$I_{n_{max}+1} \otimes I_{n_{max}+2} \otimes \dots \otimes Z_{n_{max}+n_j}, \quad (9.7b)$$

que hacen un total de  $4^{n_j} = 2^{2n_j}$ . Sin embargo, el estabilizador reducido de la suma de las partes  $m_i$  y  $m_j$  tiene sólo  $2^{n_{max}+n_j}$  términos. Por lo tanto, la única posibilidad es que  $n_{max} = n_j$ , lo que prueba el lema.

Dado un estado grafo de  $n$  qubits,  $n_{max}$  restringe el mínimo número posible de partículas y los posibles números de qubits por partícula. Dado  $n$ , la tabla 9.1 muestra los posibles mínimos números de partículas y las correspondientes distribuciones posibles de los  $n$  qubits. En la tabla

9.1 también se incluyen otras posibles distribuciones, pero se corresponden con aquellos casos donde el número de partículas no es mínimo.

Tabla 9.1: Posibles tipos de distribuciones de un estado grafo de  $n$  qubits entre un mínimo número  $m$  de partículas. Por ejemplo,  $(2,2,1)$  denota la distribución de  $n = 5$  qubits entre  $m = 3$  partículas, tales que las partículas 1 y 2 engloban dos qubits cada una, y la 3 un solo qubit.

$n$	$m$	Distribuciones
2	2	(1,1)
3	3	(1,1,1)
4	2	(2,2)
	4	(1,1,1,1)
5	3	(2,2,1)
	5	(1,1,1,1,1)
6	2	(3,3)
	3	(2,2,2)
	4	(2,2,1,1)
	6	(1,1,1,1,1,1)
7	3	(3,3,1), (3,2,2)
	4	(2,2,2,1)
	5	(2,2,1,1,1)
	7	(1,1,1,1,1,1,1)
8	2	(4,4)
	3	(3,3,2)
	4	(3,3,1,1), (3,2,2,1), (2,2,2,2)
	5	(2,2,2,1,1)
	6	(2,2,1,1,1,1)
	8	(1,1,1,1,1,1,1,1)

Un corolario del lema que acabamos de demostrar es que no hay distribuciones que permitan demostraciones AVN específicas en las cuales una partícula involucre más de  $n/2$  qubits. Este resultado ya se empleó en la sección anterior.

Esta demostración nos indica, además, que para poder predecir con certeza los elementos de realidad de los qubits pertenecientes a una parte  $m_i$  se necesita de un número de qubits que coincida con el cardinal de  $m_i$ , qubits que pueden pertenecer o bien a una única parte  $m_j$ , o bien estar distribuidos entre varias. Si pertenecen a una única parte y  $m$  es el mínimo número de partes que permite una demostración AVN, entonces los cardinales de  $m_i$  y  $m_j$  serán coincidentes. Una distribución AVN  $m$ -partita donde  $m$  sea mínimo posee al menos dos partes que satisfacen esta característica. A modo de ejemplo, véanse las distribuciones de la tabla 9.1.

### 9.3.2. Demostraciones AVN con un mínimo número de partes para cualquier estado grafo

Contamos con todas las herramientas necesarias para obtener todas las posibles distribuciones con un mínimo número de partículas que permiten demostraciones AVN específicas para cualquier estado grafo. Para este propósito hemos usado la clasificación de estados grafo de hasta  $n = 7$  qubits de la Ref. [1, 2], y la clasificación de los estados grafo de ocho qubits de la Refs. [21, 22]. Dado un estado grafo de  $n$  qubits, para obtener todas las posibles distribuciones entre un mínimo número  $m$  de partes que permiten demostraciones específicas AVN usaremos la tabla 9.1 de la siguiente manera: Supongamos que  $n = 6$ . Entonces debemos probar primero si es posible obtener demostraciones AVN para las distribuciones con un número mínimo de partes, que en este caso es  $m = 2$ , con tres qubits en cada parte, (3,3). Si no fuera posible, pasamos al siguiente tipo de distribución, que es para  $m = 3$  con dos qubits en cada parte, (2,2,2). Si ninguna de las distribuciones de los  $n$  qubits del estado grafo elegido permite una demostración AVN tripartita del tipo (2,2,2), volvemos a hacer uso de la tabla y probamos con la siguiente distribución, la (2,2,1,1), y así sucesivamente. Sólo hay un tipo de estado grafo para el cual la única distribución que permite una demostración AVN  $m$ -partita específica es aquella en la que a cada parte le corresponde un único qubit, y es el estado GHZ de un número  $n$  arbitrario de qubits.

Aplicando este método, hemos obtenido todas las distribuciones no equivalentes entre un mínimo número  $m$  de partes para todos los estados grafo de hasta  $n = 8$  qubits. A continuación, mostramos todas las posibles distribuciones entre un mínimo número de partículas para las 19 clases LC de estados grafo de 6 qubits (ver Fig. 9.6 y tabla 9.2), las 26 clases LC de estados grafo de 7 qubits (ver Fig. 9.7, y tablas 9.3 y 9.4), y las 101 clases LC de estados grafo de 8 qubits (ver Fig. 5.3, y tablas 9.5, 9.6 y 9.7). Además, proporcionamos como material suplementario un programa para obtener, dado un estado grafo de  $n$  qubits, todas las posibles distribuciones entre un número arbitrario de partes y todas las posibles distribuciones entre un mínimo número de partes que permiten demostraciones AVN.

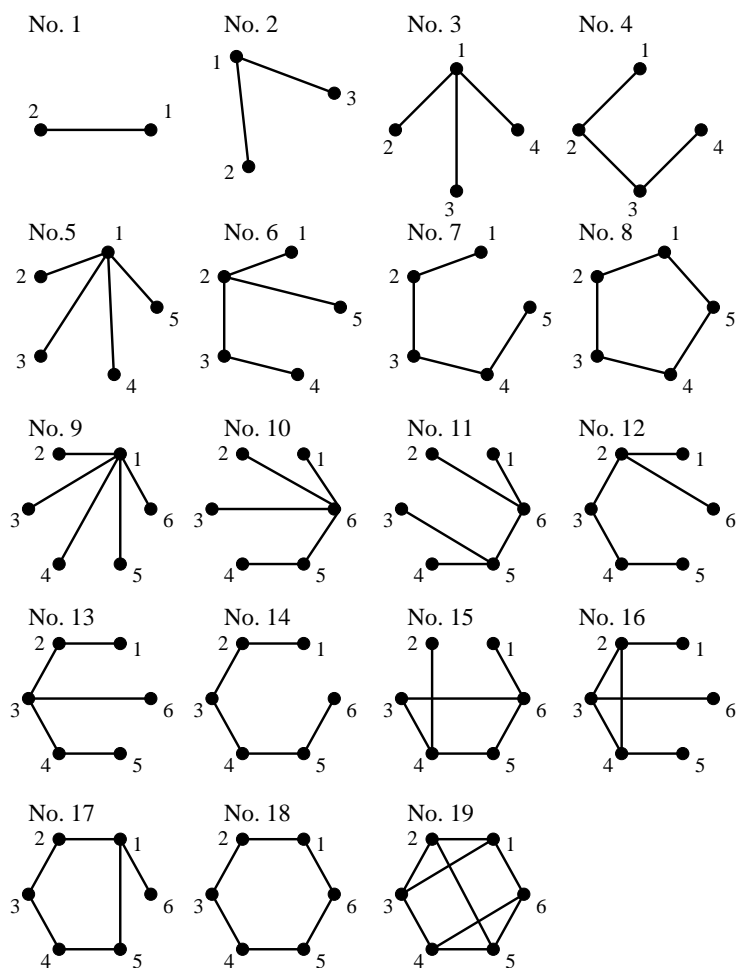


Figura 9.6: Grafos asociados a las 19 clases de estados grafo de hasta 6 qubits no equivalentes bajo complementación local e isomorfismo de grafos. Figura tomada de la Refs. [1, 2] con permiso de los autores.

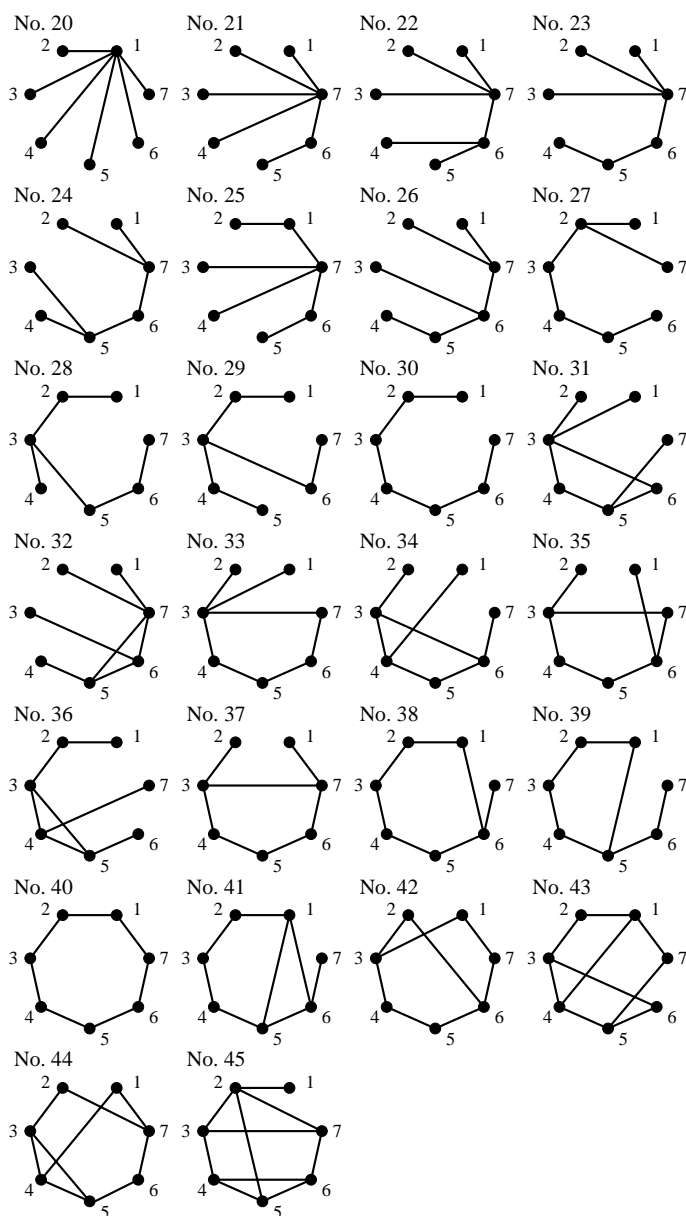


Figura 9.7: Grafos asociados a las 26 clases de estados grafo de 7 qubits no equivalentes bajo complementación local e isomorfismo de grafos. Figura tomada de la Refs. [1, 2] con permiso de los autores.



Tabla 9.2: Distribuciones de qubits de un estado grafo (numerado como en la Fig. 9.6) entre un mínimo número  $m$  de partículas  $A, B, \dots, F$ , que permiten demostraciones AVN específicas. La tabla contiene todas las distribuciones no equivalentes de todos los estados grafo de hasta 6 qubits.

Estado grafo No.	$m$	$A$	$B$	$C$	$D$	$E$	$F$
1	2	1	2				
2 ( $GHZ_3$ )	3	1	2	3			
3 ( $GHZ_4$ )	4	1	2	3	4		
4 ( $LC_4$ )	2	1,4	2,3				
5 ( $GHZ_5$ )	5	1	2	3	4	5	
6	3	1	2,4	3,5			
7 ( $LC_5$ )	3	1,5	2,4	3			
8 ( $RC_5$ )	3	1	2,5	3,4			
9 ( $GHZ_6$ )	6	1	2	3	4	5	6
10	4	1	2,4	5,6	3		
11	3	1,5	2,3	4,6			
12	3	1,5	2,4	3,6			
13	2	1,5,6	2,3,4				
14 ( $LC_6$ )	2	1,4,5	2,3,6				
15	3	1,4	2,6	3,5			
16	2	2,3,4	1,5,6				
17	2	1,2,5	3,4,6				
18 ( $RC_6$ )	2	1,2,4	3,5,6				
19	2	1,2,3	4,5,6				

Tabla 9.3: Distribuciones de qubits de un estado grafo (numerado como en la Fig. 9.7) entre un mínimo número  $m$  de partículas  $A, B, \dots, G$ , que permiten demostraciones AVN específicas. La tabla contiene todas las distribuciones no equivalentes de todos los estados grafo de 7 qubits correspondientes al intervalo de clases de equivalencia LC 20-42.

Estado grafo No.	$m$	$A$	$B$	$C$	$D$	$E$	$F$	$G$
20 ( $GHZ_7$ )	7	1	2	3	4	5	6	7
21	5	1, 6	5, 7	2	3	4		
22	4	1, 4	6, 7	2, 5	3			
23	4	1, 4	6, 7	2, 5	3			
24	4	1, 4	5, 7	3, 6	2			
25	3	1, 4, 6	2, 5, 7	3				
	3	1, 4, 6	5, 7	2, 3				
26	3	1, 4, 6	5, 7	2, 3				
	3	1, 3, 5	4, 6, 7	2				
27	3	1, 4, 5	2, 3, 6	7				
	3	1, 4, 5	2, 3	6, 7				
28	3	1, 3, 6	2, 5, 7	4				
	3	1, 3, 7	2, 4	5, 6				
29	3	1, 3, 4	2, 6, 5	7				
	3	1, 3, 4	2, 6	5, 7				
30 ( $LC_7$ )	3	1, 5, 7	2, 6	3, 4				
	3	1, 3, 5	2, 4, 6	7				
31	4	1, 4	2, 6	3, 5	7			
32	3	1, 6, 5	2, 3, 4	7				
	3	1, 5, 6	2, 3	4, 7				
33	3	1, 4, 7	2, 5, 6	3				
	3	1, 5, 6	3, 4	2, 7				
34	3	1, 2, 5	3, 4, 6	7				
	3	1, 2, 6	3, 4	5, 7				
35	3	1, 3, 4	5, 6, 7	2				
	3	1, 5, 7	2, 6	3, 4				
36	3	1, 6, 7	3, 4, 5	2				
	3	1, 6, 7	2, 5	3, 4				
37	3	1, 4, 5	3, 6, 7	2				
	3	1, 3, 6	2, 7	4, 5				
38	3	1, 2, 4	3, 5, 6	7				
	3	1, 2, 4	3, 6	5, 7				
39	3	1, 4, 5	2, 3, 6	7				
	3	1, 4, 5	2, 7	3, 6				
40 ( $RC_7$ )	3	1, 4, 7	2, 3, 6	5				
	3	1, 4, 7	2, 6	3, 5				
41	3	1, 4, 6	2, 3, 5	7				
	3	1, 4, 6	2, 7	3, 5				
42	3	1, 5, 7	3, 4, 6	2				
	3	1, 5, 7	3, 6	2, 4				

Tabla 9.4: Distribuciones de qubits de un estado grafo (numerado como en la Fig. 9.7) entre un mínimo número  $m$  de partículas  $A, B, \dots, G$ , que permiten demostraciones AVN específicas. La tabla contiene todas las distribuciones no equivalentes de todos los estados grafo de 7 qubits para las clases LC números 43, 44 y 45.

Estado grafo No.	$m$	$A$	$B$	$C$	$D$	$E$	$F$	$G$
43	3	1, 2, 7	3, 4, 5	6				
	3	1, 2, 7	3, 4	5, 6				
44	3	1, 3, 7	4, 5, 6	2				
	3	1, 3, 7	5, 6	2, 4				
45	3	1, 6, 7	2, 3, 4	5				
	3	1, 6, 7	2, 5	3, 4				

Tabla 9.5: Distribuciones de qubits de un estado grafo (numerado como en la Fig. 5.3) entre un mínimo número  $m$  de partículas  $A, B, \dots, H$ , que permiten demostraciones AVN específicas. La tabla contiene todas las distribuciones no equivalentes de los estados grafo de 8 qubits correspondientes al intervalo de clases de equivalencia LC 46-74.

Estado grafo No.	$m$	$A$	$B$	$C$	$D$	$E$	$F$	$G$	$H$
46 ( $GHZ_8$ )	8	1	2	3	4	5	6	7	8
47	6	1,6	2,7	3	4	5	8		
48	5	1,5	2,6	3,7	4	8			
49	5	1,7	3,5	4,6	2	8			
50	4	1,6	2,7	3,5	4,8				
51	4	1,7	2,5	3,4	6,8				
52	4	1,5	2,4	3,6	7,8				
	4	1,5,6	3,4,7	2	8				
	4	1,5,7	3,6	4,8	2				
53	4	1,5	2,6	3,4	7,8				
	4	1,4,6	2,5	3,7	8				
	4	1,4,6	5,7,8	2	3				
54	4	1,7	2,6	3,5	4,8				
	4	1,4,7	2,6	3,5	8				
	4	1,5,6	4,7,8	2	3				
55	3	1,4,6	2,3,5	7,8					
56	3	1,4,6	2,3,7	5,8					
57	3	1,3,4	2,5,7	6,8					
58	3	1,3,6	2,4,7	5,8					
59	3	1,3,6	4,7,8	2,5					
60	3	1,5,7	2,3,6	4,8					
61	3	1,6,4	2,3,5	7,8					
62	3	1,5,7	2,3,6	8,4					
63	3	1,2,5	3,6,8	4,7					
64	2	1,2,4,7	3,5,6,8						
65	2	1,2,4,7	3,5,6,8						
66	2	1,2,4,7	3,5,6,8						
67	2	1,3,5,7	2,4,6,8						
68 ( $LC_8$ )	2	1,4,5,8	2,3,6,7						
69	4	1,5	2,6	3,7	4,8				
70	4	1,4	2,7	3,6	5,8				
71	4	1,5,6	2,4	8,7	3				
	4	1,5,6	4,7,8	3	2				
	4	1,5	2,4	3,6	7,8				
72	4	1,5,7	2,6	4,8	3				
	4	1,4,6	5,7,8	2	3				
	4	1,5	2,6	3,7	4,8				
73	3	1,4,5	2,3,6	7,8					
74	3	1,5,7	3,6,8	2,4					

Tabla 9.6: Distribuciones de qubits de un estado grafo (numerado como en la Fig. 5.3) entre un mínimo número  $m$  de partículas  $A, B, \dots, H$ , que permiten demostraciones AVN específicas. La tabla contiene todas las distribuciones no equivalentes de los estados grafo de 8 qubits correspondientes al intervalo de clases de equivalencia LC 75-108.

Estado grafo No.	$m$	$A$	$B$	$C$	$D$	$E$	$F$	$G$	$H$
75	3	1, 5, 7	2, 4, 6	3, 8					
76	3	1, 2, 4	3, 6, 8	5, 7					
77	3	1, 4, 6	2, 3, 5	7, 8					
78	3	1, 6, 7	2, 5, 4	3, 8					
79	3	1, 3, 6	2, 4, 7	5, 8					
80	3	1, 3, 6	2, 5, 7	4, 8					
81	3	1, 4, 5	2, 3, 6	7, 8					
82	3	1, 3, 7	2, 5, 8	4, 6					
83	3	1, 4, 6	2, 5, 7	3, 8					
84	3	1, 3, 5	4, 6, 8	2, 7					
85	3	1, 5, 7	3, 4, 8	2, 6					
86	2	1, 3, 6, 7	2, 4, 5, 8						
87	2	1, 4, 6, 7	2, 3, 5, 8						
88	2	1, 2, 4, 7	3, 5, 6, 8						
89	2	1, 3, 6, 8	2, 4, 5, 7						
90	2	1, 4, 6, 8	2, 3, 5, 7						
91	2	1, 3, 6, 7	2, 4, 5, 8						
92	2	1, 3, 5, 7	2, 4, 6, 8						
93	2	1, 2, 4, 6	3, 5, 7, 8						
94	2	1, 3, 5, 8	2, 4, 6, 7						
95	2	1, 3, 4, 7	2, 5, 6, 8						
96	2	1, 3, 5, 7	2, 4, 6, 8						
97	2	1, 3, 5, 7	2, 4, 6, 8						
98	2	1, 3, 5, 6	2, 4, 7, 8						
99	2	1, 4, 5, 8	2, 3, 6, 7						
100 ( $RC_8$ )	2	1, 3, 6, 8	2, 4, 5, 7						
101	3	1, 6, 8	2, 3, 5	4, 7					
102	3	1, 3, 7	2, 4, 5	6, 8					
103	3	1, 7, 8	2, 3, 5	4, 6					
104	3	1, 3, 7	5, 6, 8	2, 4					
105	3	1, 3, 6	2, 4, 5	7, 8					
106	2	1, 3, 4, 6	2, 5, 7, 8						
107	2	1, 4, 6, 7	2, 3, 5, 8						
108	2	1, 4, 6, 8	2, 3, 5, 7						

Tabla 9.7: Distribuciones de qubits de un estado grafo (numerado como en la Fig. 5.3) entre un mínimo número  $m$  de partículas  $A, B, \dots, H$ , que permiten demostraciones AVN específicas. La tabla contiene todas las distribuciones no equivalentes de los estados grafo de 8 qubits correspondientes al intervalo de clases de equivalencia LC 109-146.

Estado grafo No.	$m$	$A$	$B$	$C$	$D$	$E$	$F$	$G$	$H$
109	2	1, 2, 3, 6	4, 5, 7, 8						
110	2	1, 2, 5, 6	3, 4, 7, 8						
111	2	1, 2, 5, 7	3, 4, 6, 8						
112	2	1, 3, 4, 6	2, 5, 7, 8						
113	2	1, 4, 5, 6	2, 3, 7, 8						
114	2	1, 3, 5, 6	2, 4, 7, 8						
115	2	1, 3, 4, 6	2, 5, 7, 8						
116	2	1, 2, 3, 5	4, 6, 7, 8						
117	2	1, 4, 5, 7	2, 3, 6, 8						
118	2	1, 5, 8, 6	2, 3, 4, 7						
119	2	1, 3, 6, 8	2, 4, 5, 7						
120	2	1, 2, 4, 8	3, 5, 6, 7						
121	3	1, 4, 5	2, 7, 8	3, 6					
122	3	1, 5, 7	2, 7, 8	3, 4					
123	2	1, 3, 5, 6	2, 4, 7, 8						
124	2	1, 4, 6, 7	2, 3, 5, 8						
125	2	1, 4, 5, 7	2, 3, 6, 8						
126	2	1, 2, 4, 6	3, 5, 7, 8						
127	2	1, 3, 4, 6	2, 5, 7, 8						
128	2	1, 3, 6, 7	2, 4, 5, 8						
129	2	1, 3, 5, 6	2, 4, 7, 8						
130	2	1, 2, 5, 8	3, 4, 6, 8						
131	2	1, 3, 6, 7	2, 4, 5, 8						
132	2	1, 4, 5, 6	2, 3, 7, 8						
133	2	1, 6, 7, 8	2, 3, 4, 5						
134	3	1, 4, 6	3, 7, 8	2, 5					
135	2	1, 3, 4, 7	2, 5, 6, 8						
136	2	1, 3, 4, 5	2, 6, 7, 8						
137	2	1, 2, 3, 4	5, 6, 7, 8						
138	2	1, 3, 4, 6	2, 5, 7, 8						
139	2	1, 6, 7, 8	2, 3, 4, 5						
140	2	1, 4, 5, 6	2, 3, 7, 8						
141	2	1, 6, 7, 8	2, 3, 4, 5						
142	2	1, 3, 7, 8	2, 4, 5, 6						
143	2	1, 3, 4, 7	2, 5, 6, 8						
144	2	1, 2, 5, 6	3, 5, 7, 8						
145	2	1, 4, 5, 8	2, 3, 6, 7						
146	2	1, 2, 4, 5	3, 6, 7, 8						

# Conclusiones

## Capítulo 5

En resumen, hemos extendido la clasificación del entrelazamiento en estados grafo propuesta en [1, 2] hasta  $n = 8$  qubits, donde hay un total de 101 clases de equivalencia u órbitas. Para cada una de estas clases hemos obtenido un representante que se caracteriza por precisar un mínimo número de puertas controlled-Z para su preparación (ver Fig. 5.3), y calculamos la medida de Schmidt para las distribuciones octopartitas (los cuales miden el genuino entrelazamiento octopartitos de las clases), y los rangos de Schmidt para todas las distribuciones bipartitas (ver tablas 5.1, 5.2 y 5.3).

Esta nueva clasificación nos ayudará a obtener nuevas demostraciones “all-versus-nothing” del teorema de Bell [19, 20] (capítulos 8 y 9) y nuevas desigualdades de Bell [14, 196]. Más generalmente, nos ayudará a investigar la no-localidad (i.e., la no simulabilidad de las predicciones de la mecánica cuántica mediante un modelos de variables ocultas locales) de los estados grafo [14].

La extensión de la clasificación en HEB, nos ha conducido a conocer algunas de las limitaciones de este método de clasificación. De hecho, ya para algunas de las clases de equivalencia de los estados grafo de  $n = 7$  qubits no era capaz de arrojar información suficiente para distinguirlas entre sí. Por ejemplo, como podemos ver en la tabla 9.8, los representantes de las clases No. 40, No. 42 y No. 43 en [1, 2] poseen el mismo número de qubits, requieren el mismo número de  $C_Z$  para su preparación, tienen la misma medida de Schmidt e índices de rango. Como se muestra

Tabla 9.8: Estados grafo de siete qubits de la clasificación de HEB [1, 2] que no son distinguibles.

No.	LC	V	E	$RS_{max}$	PP	$IR_3$	$IR_2$	bicoloreable
40	92	7	7	3	4	(28,7,0)	(21,0)	no
42	33	7	8	3	4	(28,7,0)	(21,0)	no
43	9	7	9	3	3	(28,7,0)	(21,0)	yes

en la tabla 9.9, este mismo problema se repite entre las clases No. 110 y No. 111, entre las No. 113 y No. 114, y entre las clases No. 116 y No. 117 de nuestra clasificación. Basándonos en [1, 2], hemos situado aquellos estados con |LC| más bajo en primer lugar. Sin embargo, esta solución no es satisfactoria porque el número de elementos que pertenecen a una misma clase de equivalencia

Tabla 9.9: Estados grafo de ocho qubits de la clasificación de HEB [1, 2] que no son distinguibles.

No.	LC	E	E <sub>S</sub>	IR <sub>4</sub>	IR <sub>3</sub>	IR <sub>2</sub>	bicoloreable
110	114	9	4	(8,22,5,0)	(40, 16,0)	(26,2)	no
111	372	9	4	(8,22,5,0)	(40, 16,0)	(26,2)	no
113	264	9	4	(8,24,3,0)	(44, 12,0)	(27,1)	no
114	542	9	4	(8,24,3,0)	(44, 12,0)	(27,1)	no
116	174	9	4	(12,20,3,0)	(46, 10,0)	(27,1)	no
117	542	9	4	(12,20,3,0)	(46, 10,0)	(27,1)	no

no está relacionado con las propiedades del entrelazamiento que caracteriza a un determinada clase. Por otro lado, Van den Nest, Dehaene, and De Moor propusieron un conjunto finito de invariantes que caracterizaban todas las clases [166], sin embargo, este conjunto de invariantes posee más de  $2 \times 10^{36}$  elementos para  $n = 7$ . El problema de obtener un mínimo conjunto de invariantes capaz de distinguir todas las clases con  $n \leq 8$  qubits está en la Ref. [22] y será el contenido que desarrollaremos en el siguiente capítulo.

Otro punto débil de este método es que el valor preciso de  $|E_S|$  es todavía desconocido en algunas clases. Este problema se podría haber resuelto para la mayoría de ellos, si conociéramos el valor exacto de éste parámetro para el estado ring cluster de 5 qubits, pero precisamente este es el primer caso de la clasificación de HEB en que no se tiene un valor preciso de  $E_S$ , y, desafortunadamente, nosotros tampoco hemos hecho ningún progreso al respecto.

Las tablas 5.1, 5.2 y 5.3 muestran que no hay estados grafo de ocho qubits con todos sus índices de rango  $IR_p = [\nu_j^p]_{j=p}^1$ , donde  $\nu_j^p \neq 0$  si  $j = p$  y  $\nu_j^p = 0$  si  $j < p$ , es decir, no hay estados grafos de ocho qubits que exhiban un rango maximal con respecto a todas las posibles biparticiones, ni tampoco donde el entrelazamiento esté simétricamente distribuido entre todas las partes. Estos estados se caracterizan por ser más robustos contra el descentralazamiento cuando se realizan sobre ellos un reducido número de medidas. Tampoco se dan estos casos para los estados grafo de 7 qubits, no obstante, hemos localizados dos casos para estados grafos de menos 6 qubits, y son el ring cluster de 5 qubits y el No. 19 que es un estado de grafo de 6 qubits. En la Ref. [197] encontramos la información necesaria para trabajar con los grafos. Los grafos vienen especificados mediante un código conocido como código nauty. Dado un grafo conexo, hay asociado un código que lo identifica y a través de él se puede obtener su matriz de adyacencia.

## Capítulo 6

Hemos mostrados que para distinguir entre las clases de equivalencia de los estados grafo de hasta  $n = 8$  qubits, son suficientes sólo cuatro cantidades, las cuales son invariantes bajo LC.



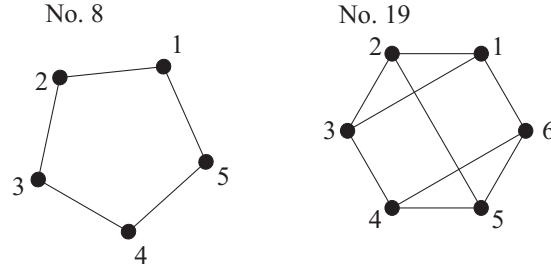


Figura 9.8: En esta figura hemos reunido a dos grafos, el  $RC_5$  y el No. 19, que representan a los únicos los estados grafos con menos de 8 qubits, tales que poseen rango de Schmidt maximal para todas las posibles biparticiones, y donde el entrelazamiento está simétricamente distribuido entre toda las partes. Los datos que corroboran estas conclusiones son:  $IR_2(|G(19)\rangle) = (10, 0)$ ,  $IR_3(|G(19)\rangle) = (10, 0, 0)$ ,  $IR_2(|G(19)\rangle) = (15, 0)$ .

Este resultado resuelve el problema de la clasificación de los estado de hasta  $n = 8$  qubits desarrollados en las Refs. [1, 2, 21].

También hemos mostrado que la conjetura [198] de que la lista de invariantes LC dada por la ecuación (6.8) es suficiente para caracterizar las clases LC equivalentes de todos los estados estabilizadores, la cual no es cierta en general, sí lo es para los estados grafo de hasta  $n = 8$  qubits. Hemos mostrado además que la lista de invariantes LC dada por la ecuación (6.3) es suficiente para distinguir entre clases las de equivalencia. Esto resuelve el problema sugerido en [166], de considerar la posibilidad de caracterizar una subclase especial de estados estabilizadores a través de familias de invariantes.

## Capítulo 8

En este capítulo, hemos aportado una condición necesaria y suficiente para la existencia de demostraciones BAVN, usando qubits para estados grafo de cualquier número de qubits.

Los requerimientos para obtener una demostración AVN son: a) Correlaciones perfectas necesarias para definir los elementos de realidad EPR bipartitos. Hemos empleado los estados grafo representantes óptimos de la clasificación de Hein *et al.* [1, 2] en estas demostraciones. b) Correlaciones perfectas que contradigan los elementos de realidad EPR. A través del lema 1, hemos comprobado que todos estados grafo conexos de más de tres qubits conducen a una contradicción algebraica con el concepto de elemento de realidad.

La mayoría de los estados grafo no se pueden emplear en una demostración BAVN. Sólo unos pocos estados grafo satisfacen al mismo tiempo el lema y los requisitos a) y b). Además, dado que el lema 2 es una condición necesaria y suficiente, cuando se aplican a todas las posibles distribuciones de qubits y a todos los posibles estados grafo se obtiene una clasificación completa de todas las posibles demostraciones BAVN. Las distribuciones de qubits de cada representante óptimo que satisfagan el lema 2, serán válidas para todos los estados grafo que pertenezcan a la

misma clase de equivalencia.

Los únicos estados de menos de 8 qubits y distribuciones de qubits que, salvo transformación unitaria, permiten demostraciones BAVN son el estado  $|\psi_{4a}\rangle$  corresponde al grafo No. 4 de acuerdo con la clasificación de Hein *et al.* [1, 2], y con el 4a de la Fig. 8.2 [17] y es la única (sin tener en cuenta las posibles representaciones equivalentes) con 4 qubits empleando medidas de un sólo qubit. Entre los estados grafos No. 5 y 7 de la misma clasificación, hay sólo 6 estados cuyas distribuciones conducen a demostraciones BAVN. Todos ellos son estados grafos de 6 qubits, donde cada parte posee tres qubits. Sus correspondientes grafos se muestran en la Fig. 8.3. Las expresiones explícitas de cada estado se pueden obtener a partir de sus grafos usando su estabilizador.

Dos estados grafo de 6 qubits se han preparado recientemente en el laboratorio [25, 54] pero ninguno de ellos permite demostraciones BAVN.

## Capítulo 9

Hemos desarrollado las herramientas para decidir si una distribución de  $n$  qubits entre  $m$  partes permite una demostración AVN específica  $m$ -partita. Como resultado hemos obtenido todas las demostraciones AVN  $m$  partitas usando estados cuánticos de  $n$  qubits y  $m$  partículas, para  $n < 9$  qubits y un mínimo número  $m$  de partes. Esto nos permite obtener todas las demostraciones AVN  $m$ -partitas, usando estados cuánticos de  $n$  qubits y  $m$  partículas, con un número arbitrario de partes.

La motivación de este trabajo, fue responder a algunas preguntas que surgieron tras el desarrollo de avances experimentales que permitieron la preparación en el laboratorio de estados grafo de varias partículas conteniendo varios qubits. Los resultados presentados en este artículo, proporcionan a los experimentalistas las herramientas necesarias para diseñar nuevas demostraciones AVN y nuevas desigualdades de Bell basadas en ellas [14, 17, 46], similares a aquellas de las Refs. [48, 52] para estados específicos, pero explotando la posibilidad de preparar experimentalmente nuevas clases de estados grafo.

# Conclusions

Conclusions are drawn for those chapters which correspond to the innovative results of our work.

## Chapter 5

The classification of the entanglement of graph state proposed in [1] for  $n < 8$  qubits has now been extended to 8 qubits. Notice that for  $n = 8$  there are 101 classes, while for  $n < 8$  there are only 45 classes. For each of these classes a representative is obtained which requires the minimum number controlled-Z gates for its preparation (see Fig. 5.3), and the Schmidt measure is calculated for the 8-partite splits (which measure the genuine 8-partite entanglement of the class), and the Schmidt ranks are computed for all bipartite splits (see Tables 5.1, 5.2, and 5.3). This classification will help us to obtain new “all-versus-nothing” proofs of Bell’s theorem [19, 20] (see Chapters 8 and 9) and new Bell inequalities. More generally, it will help towards research into the non-locality (i.e., the non-simulability of the predictions of quantum mechanics by means of non-local hidden variable models) of graph states [14].

Extending the HEB classification a further step sheds some light on the limitations of this method of classification. Indeed, this method fails to distinguish all classes in  $n = 7$ . For instance, classes No. 40, No. 42, and No. 43 in [1, 2] have the same number of qubits, require the same minimum number of controlled-Z gates for the preparation, and have the same Schmidt measure and rank indexes (see Table 9.10). The same problem occurs between classes No. 110

Table 9.10: Indistinguishable 7 qubits graph states of the HEB classification [1, 2].

No.	LC	V	E	$SR_{max}$	PP	$RI_3$	$RI_2$	2-col
40	92	7	7	3	4	(28,7,0)	(21,0)	no
42	33	7	8	3	4	(28,7,0)	(21,0)	no
43	9	7	9	3	3	(28,7,0)	(21,0)	yes

and No. 111, between classes No. 113 and No. 114, and between classes No. 116 and No. 117 in our classification (see Table 9.11). Following [1, 2], we have placed those classes with lowest |LC| in the first place. However, this solution is not satisfactory, since |LC| is not related to the entanglement properties of the class. On the other hand, Van den Nest, Dehaene, and De

Tabla 9.11: Indistinguishable 8-qubits graph states of the HEB classification [1, 2].

No.	LC	E	$E_S$	$IR_4$	$IR_3$	$IR_2$	2-col
110	114	9	4	(8,22,5,0)	(40, 16,0)	(26,2)	no
111	372	9	4	(8,22,5,0)	(40, 16,0)	(26,2)	no
113	264	9	4	(8,24,3,0)	(44, 12,0)	(27,1)	no
114	542	9	4	(8,24,3,0)	(44, 12,0)	(27,1)	no
116	174	9	4	(12,20,3,0)	(46, 10,0)	(27,1)	no
117	542	9	4	(12,20,3,0)	(46, 10,0)	(27,1)	no

Moor proposed a finite set of invariants that characterize all classes [166]. However, this set has more than  $2 \times 10^{36}$  invariants for  $n = 7$ . The problem of obtaining a minimum set of invariants capable of distinguishing all classes with  $n \leq 8$  qubits will be addressed elsewhere [22], and is developed in the following chapter.

Another weak point in the method is that the precise value of  $|E_S|$  is still unknown for some classes. This problem could have been solved, for most of these classes if the value for the 5-qubit ring cluster state were known, but it is precisely this first graph state in the HEB classification for which the value of  $E_S$  remains unknown. Unfortunately, no progress in calculating  $E_S$  for the 5-qubit ring cluster state has yet been made.

Tables 5.1, 5.2, and 5.3 show that there are no 8-qubit graph states whose rank indexes are  $RI_p = [\nu_j^p]_{j=p}^1$  with  $\nu_j^p \neq 0$  if  $j = p$ , and  $\nu_j^p = 0$  if  $j < p$ , i.e., there are no 8-qubit graph states which exhibit maximal rank with respect to all possible bipartite splits, nor where entanglement is symmetrically distributed between all parties. These states are robust against disentanglement when only a few measurements are carried out. Neither are there 7-qubit graph states with this property. However, we have encountered two cases with this property (see Fig. 9.9): a single 5-qubit graph state (class No. 8 in [1, 2]) and a single 6-qubit graph state (class No. 19 in [1, 2]).

Reference [197] provides the information necessary in order to work with graphs. The graphs are specified by means of a code known as the Nauty code. Given a related graph, there is an associated code that identifies it, and through this code its adjacency matrix can be obtained.

## Chapter 6

We have shown that, in order to distinguish between the equivalence classes of the graph states of up to  $n = 8$  qubits, it is sufficient to calculate four quantities. These four LC invariants characterize any LC class of  $n = 8$  qubits.

This result solves the problem raised in the classification of graph states of  $n = 8$  qubits developed in Refs. [1, 2, 21].

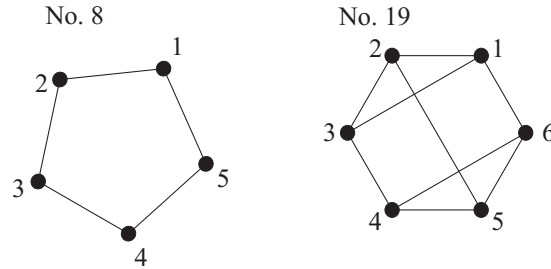


Figura 9.9: This figure shows two graphs,  $RC_5$  and No. 19, which represent the only two graph-states with fewer than 8 qubits, in such a way that they possess a maximal Schmidt rank for all possible bipartitions and where the entanglement is distributed symmetrically between all parties. The data which justifies these conclusions are:  $RI_2(|RC_5\rangle) = (10, 0)$ ,  $RI_3(|G(19)\rangle) = (10, 0, 0)$ ,  $RI_2(|G(19)\rangle) = (15, 0)$ .

The conjecture [198] that the list of LC invariants given in Eq. (6.8) is sufficient to characterize the LC equivalence classes of all stabilizer states, is not true in general [2], but we have shown that it is indeed true for graph states of up to  $n = 8$  qubits. Moreover, we have shown that, for graph states of  $n = 8$  qubits, the list of LC invariants given in Eq. (6.3), is sufficient in order to distinguish between all inequivalent classes of graph states. This solves a problem suggested in [166], regarding the possibility of characterizing special subclass of stabilizer states through the use of families of invariants.

## Chapter 8

In this chapter we show a necessary and sufficient condition for the existence of bipartite AVN proofs using only single-qubit measurements (BAVN) for graph states of any number of qubits. We then proceed to explicitly provide all physically distinct BAVN proofs with up to 7 qubits.

The single-qubit measurements necessary in a BAVN proof must satisfy two requirements: (a) Perfect correlations to define bipartite EPR's elements of reality. Every observable single-qubit involved in the proof must satisfy EPR's criterion of elements of reality. (b) Perfect correlations that contradict EPR's elements of reality. The observables that satisfy EPR's condition cannot have predefined results, since it must be impossible to assign them values that satisfy all the perfect correlations predicted by quantum mechanics. Lemma 1 shows any graph state associated to a connected graph of three or more vertices leads to algebraic contradictions with the concept of elements of reality (when each qubit is distributed to a different party).

The majority of graph states cannot be used in BAVN proofs. The remarkable point is that there are a few graph states and distributions of qubits that satisfy the requirements of Lemma 2, and therefore simultaneously fulfill (a) and (b). Moreover, since Lemma 2 is a necessary and

sufficient condition, when it is applied to every possible distribution of qubits of all possible graph states then a complete classification of all possible BAVN proofs is obtained.

The distributions of qubits of each optimum representative that satisfy Lemma 2 are valid for all those graph states which belong to the same equivalence class.

The only states, and distributions of qubits that, with the exception of unitary transformations, allow BAVN proofs are the following: the 4-qubit graph state  $|\psi_{4a}\rangle$  corresponding to the graph state No. 4 according to [1, 2] and graph 4a in the Fig. 8.2 [17]. This is the only distribution of a 4-qubits graph state with single qubit measurements which allows a BAVN. Between 5 and 7 qubits, there are only 6 possible states and distributions leading to BAVN proofs. All of these are 6-qubit states in which each party has 3 qubits. Their corresponding graphs are summarized in Fig. 8.3. The explicit expressions of each state can be obtained from its graph by means of the corresponding stabilizer. Two 6-qubit graph states have recently been prepared in the laboratory [25, 54], although neither allows BAVN proofs.

## Chapter 9

We have developed tools with which to decide whether a distribution of  $n$  qubits between  $m$  parties allows an  $m$ -partite AVN proof specific to this distribution (i.e., a proof which cannot be obtained using a state with fewer qubits). As a result, we have obtained all inequivalent  $m$ -partite AVN proofs using  $n$ -qubit  $m$ -particle quantum states with  $n < 9$  qubits and a minimum number  $m$  of parties. This enables us to obtain all inequivalent  $m$ -partite AVN proofs using  $n$ -qubit  $m$ -particle quantum states with  $n < 9$  qubits with an arbitrary number of parties.

The motivation of this work was to answer several natural questions raised by recent experimental developments which enabled laboratory preparation of graph states of several particles, each of which carries several qubits. The results presented in this article provide tools to help experimentalists to design new AVN proofs and to determine new Bell inequalities based on these AVN proofs [14, 17, 46], similar to those given in Refs. [48, 52] for specific states, but exploiting the possibility of experimentally preparing new classes of graph states.

# Apéndice

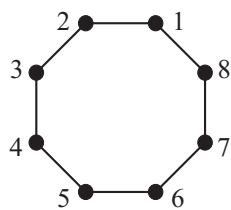
## Apéndice del capítulo 1

### Definiciones de teoría de grafos

La teoría de grafos es una disciplina matemática que trata del estudio de las propiedades y aplicaciones matemático-interdisciplinarias de los grafos.

*Grafo.* Un grafo [199] es un conjunto de  $n$  vértices, donde  $V = \{1, \dots, n\}$ , y un conjunto de aristas  $E$  que conectan pares de vértices tales que  $E \subset V \times V$ .

*Matriz de adyacencia de un grafo.* Cualquier grafo  $G$  puede ser descrito por su matriz de adyacencia  $\Gamma(G)$ ; que es una matriz cuadrada y simétrica, de dimensión  $V \times V$ , y sus elementos toman los valores  $\Gamma_{ij} = 1$  cuando el vértice  $i$  está conectado al vértice  $j$ , y  $\Gamma_{ij} = 0$  en caso contrario.



$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Figura 9.10: Grafo y la matriz de adyacencia correspondiente.

*Grado de un vértice.* Es el número de aristas que inciden en él.

*Grado de un grafo.* Es el máximo grado de todos sus vértices.

*Vecindad del vértice  $i$ ,* denotada como  $N(i)$  ó  $N_i$ . Es el conjunto de vértices adyacentes al vértice  $i$ .

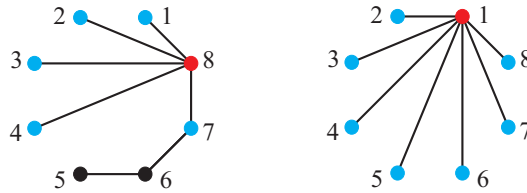


Figura 9.11: En azul hemos indicado la vecindad del vértice 8 del grafo de la izquierda y la del vértice 1 del de la derecha.

*Complementación de un vértice o complementación local.* La complementación local sobre un vértice  $a$  perteneciente a un grafo  $G(V, E)$ , se denota como  $\tau_a(G)$ , y se obtiene eliminando las aristas que existan entre los vértices de su vecindad  $N(a)$  y completando las aristas faltantes entre ellos. Las adyacencias del resto de vértices del grafo permanecen intactas.

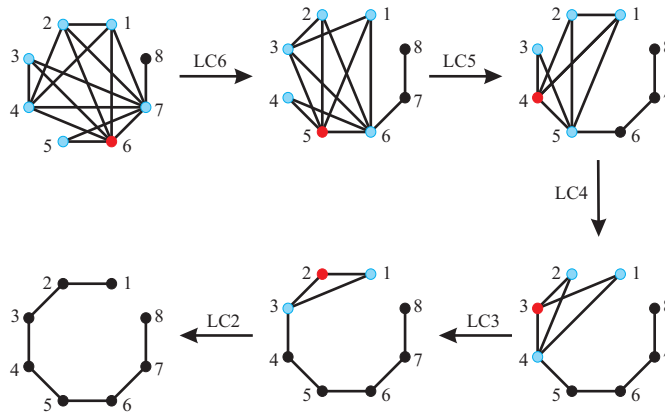


Figura 9.12: Secuencia de complementaciones locales sobre los vértices destacados en color rojo. Los vértices azules representan las respectivas vecindades de aquellos. Las operaciones de complementación local, que se han indicado como  $LC_i$  siendo  $i$  los vértices de los grafos sobre los que actúan, se han ido aplicando hasta obtener el grafo con menos aristas.

## Grupo de Pauli

El grupo de Pauli, constituye la base en la que se fundamenta y desarrolla el formalismo estabilizador. En esta sección, aportaremos su definición, describiremos cómo se generan sus elementos y cuáles son sus propiedades.

El grupo de Pauli  $P_n$  es un grupo multiplicativo constituido por un total de  $4 \times 4^n$  operadores unitarios que son el resultado del producto tensorial entre  $n$  matrices pertenecientes al conjunto  $\{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$ , donde cada una de ellas va acompañada de uno de los factores de fase del conjunto  $\{\pm 1, \pm i\}$ . En particular, para  $n = 1$  el grupo de Pauli posee 16 elementos representados en forma compacta por  $P = (\{\pm 1, \pm i\} \cdot \{\sigma_0, \sigma_x, \sigma_y, \sigma_z\})$ . Estas matrices son la identidad y el conjunto de las matrices de Pauli; se caracterizan por ser hermíticas, unitarias, y, exceptuando



la matriz identidad, son de traza nula.

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (9.8)$$

Los elementos del grupo de  $P_n$  se pueden expresar de forma general como:  $g = \alpha_1 \sigma_1 \otimes \alpha_2 \sigma_2 \otimes \alpha_3 \sigma_3 \otimes \cdots \otimes \alpha_m \sigma_m$ , donde los subíndices indican los qubits sobre los que actúan los operadores locales de Pauli, y los  $\alpha_i$  los factores de fase que se podrán multiplicar entre sí para dar lugar a un factor de fase global en cada operador.

De entre las propiedades que satisface el grupo de Pauli destacaremos las siguientes:

1. El grupo de Pauli de orden  $n$  posee al menos un subconjunto de operadores conocidos como *operadores generadores*,  $g_1, g_2, \dots, g_n$ , que generan el grupo, es decir, cualquier otro operador del grupo se puede escribir como producto de ellos. Los operadores generadores son *operadores independientes*, en el sentido en que ninguno de ellos se puede expresar como producto de otros elementos del grupo. Al conjunto de estos operadores se le conoce como *generador*.

2. Si  $A$  y  $B \in P_n$ , entonces conmutan o anticonmutan [200]. Especificaremos bajo qué condiciones los elementos de  $P_n$  satisfacen esta propiedad. Denotaremos mediante  $A_i$  y  $B_i$  a los operadores de  $P_1$  tales que bajo producto tensorial dan lugar a los elementos  $A$  y  $B$  de  $P_n$ .

Para expresar de una forma más sencilla el producto escalar entre  $A$  y  $B$ , consideraremos previamente la función  $f(i)$  dada por la expresión

$$f(i) = \begin{cases} 0, & \text{si } A_i \text{ y } B_i \text{ conmutan;} \\ 1, & \text{si } A_i \text{ y } B_i \text{ anticonmutan,} \end{cases} \quad (9.9)$$

tal que  $A_i B_i = (-1)^{f(i)} B_i A_i$  conserva el orden de los factores en la multiplicación. A continuación, realizamos las operaciones que nos conducirán a comprobar esta propiedad:

$$[A, B] = AB - BA = BA((-1)^{\sum_{i=1}^n f(i)} - 1), \quad (9.10a)$$

$$\{A, B\} = AB + BA = BA((-1)^{\sum_{i=1}^n f(i)} + 1). \quad (9.10b)$$

Analizando estos resultados se tiene que dos operadores distintos,  $A$  y  $B$ , conmutarán (anticonmutarán) si y solo si  $\sum_{i=1}^n f(i)$  es par (impar), incluyendo el cero. Luego los operadores de  $P(n)$  conmutarán (anticonmutarán) si contienen un número par (impar) de elementos de  $P(1)$  que anticonmutan.

Con objeto de entender más claramente esta propiedad proponemos los siguientes ejemplos:

a)  $n = 1$ . Es el caso trivial pues los operadores  $A$  y  $B \in \{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$ . Luego conmutarán si y sólo si  $A = B$  o si algunos de ellos es la identidad. Basándonos en esta propiedad del grupo de Pauli, una lectura paralela y equivalente para este caso particular es que los operadores de  $P_1$  sólo conmutarán cuando haya una cantidad par, en este caso nula, de operadores que anticonmuten.

b)  $n \geq 2$ . Este caso da lugar a tres posibilidades distintas que expondremos a modo de ejemplos sólo para  $n = 2$ , pues se trata de un prototipo que ilustra de forma sencilla el contenido de la propiedad:

b.1) Hay un número par de operadores que anticonmutan:

$$g_1 = X_1 \otimes Y_2, \quad (9.11a)$$

$$g_2 = Y_1 \otimes X_2, \quad (9.11b)$$

$$[g_1, g_2] = g_1 g_2 - g_2 g_1 = Z_1 \otimes Z_2 - Z_1 \otimes Z_2 = 0. \quad (9.11c)$$

Si se hace un recuento de los conjuntos de operadores de  $P_1$  que anticonmutan, hay un total de dos, y son:  $X_1$  e  $Y_1$  y  $X_2$  e  $Y_2$ . Al tratarse de un número par,  $g_1$  y  $g_2$  conmutarán como se indica en (9.11c).

b.2) En el siguiente ejemplo, siguiendo el razonamiento anterior, tras el recuento hay una cantidad nula de operadores que anticonmutan

$$g_1 = I_1 \otimes Y_2, \quad (9.12a)$$

$$g_2 = Y_1 \otimes Y_2, \quad (9.12b)$$

$$[g_1, g_2] = g_1 g_2 - g_2 g_1 = Y_1 \otimes I_2 - Y_1 \otimes I_2 = 0. \quad (9.12c)$$

Por tanto,  $g_1$  y  $g_2$  serán compatibles como se indica en (9.12c).

c) Finalmente, si el número de operadores que anticonmuta es impar:

$$g_1 = X_1 \otimes Y_2, \quad (9.13a)$$

$$g_2 = X_1 \otimes X_2, \quad (9.13b)$$

$$[g_1, g_2] = g_1 g_2 - g_2 g_1 = I_1 \otimes iZ_2 + I_1 \otimes iZ_2 = -2iI \otimes Z_2 \neq 0. \quad (9.13c)$$

Hay un solo conjunto de operadores que anticonmutan:  $Y_2$  y  $X_2$ . Luego,  $g_1$  y  $g_2$  anticonmutarán como se indica en (9.13c).

# Anexo

Aquí incluimos el listado de los artículos publicados durante el período predoctoral, y el de las contribuciones a los distintos congresos donde hemos presentado nuestro trabajo, ambos ordenados cronológicamente. También hemos incorporado dichos artículos y las contribuciones que teníamos a nuestra disposición.

## Artículos publicados

1. A. Cabello y P. Moreno, “Bipartite all-versus-nothing proofs of Bell’s theorem with single-qubit measurements”, *Phys. Rev. Lett.* **99**, 220402 (2007).
2. A. Cabello, O. Gühne, P. Moreno, y D. Rodríguez, “Nonlocality for graph states”, *Laser Phys.* **18**, 3 (2008).
3. A. Cabello, A. J. López-Tarrida, P. Moreno y J. R. Portillo, “Compact set of invariants characterizing graph states of up to eight qubits”, *Phys. Rev. A* **80**, 012102 (2009).
4. A. Cabello, A. J. López-Tarrida, P. Moreno y J. R. Portillo, “Entanglement in eight-qubit graph states”, *Phys. Lett. A* **373**, 2219 (2009), *ibid* 374, 3991 (2010).
5. A. Cabello y P. Moreno, “All-versus-nothing proofs with  $n$  qubits distributed between  $m$  parties”, *Phys. Rev. A* **81**, 042110 (2010).

## Aportaciones a congresos

1. A. Cabello y P. Moreno, “Demostraciones bipartitas ‘todo o nada’ del teorema de Bell usando qubits”, *XXXI Reunión Bienal de la Real Sociedad Española de Física* (Granada, 10-14 de septiembre, 2007). M. C. Carrión Pérez, J. A. García García, J. F. Gómez Lopera, e I. Sánchez García (XXXI Reunión Bienal de la Real Sociedad Española de Física, Real Sociedad Española de Física, Madrid, 2007), vol. 31, p. 292.
2. A. Cabello, J. R. Portillo, A. J. López-Tarrida y P. Moreno, “Entrelazamiento en estados grafo de 8 qubits”, *Avances en Matemática Discreta en Andalucía y en El Algarve, I Workshop Matemática Discreta Algarve Andalucía y VI Encuentros Andaluces de Matemática Discreta* (Instituto Superior de Engenharia da Universidade Do Algarve, Galaroz, Huelva, España, 2009), p. 71.

3. A. Cabello y P. Moreno, "Demostraciones 'todo o nada'  $m$ -partitas del teorema de Bell con qubits", *XXXII Reunión Bienal de la Real Sociedad Española de Física* (Ciudad Real, 7-11 de septiembre de 2009). M. A. López de la Torre, J. A. de Toro y J. González (XXXII Bienal de la Real Sociedad Española de Física, Real Sociedad Española de Física, Madrid, 2009), p. 537-538.
4. A. Cabello, A. J. López-Tarrida, P. Moreno y J. R. Portillo, "Conjunto compacto de invariantes que permiten caracterizar estados grafo de hasta ocho qubits", *XXXII Reunión Bienal de la Real Sociedad Española de Física* (Ciudad Real, 7-11 de septiembre de 2009). M. A. López de la Torre, J. A. de Toro y J. González (XXXII Bienal de la Real Sociedad Española de Física, Real Sociedad Española de Física, Madrid, 2009), p. 540-541.
5. A. Cabello, A. J. López-Tarrida, P. Moreno y J. R. Portillo, "Compact set of invariants characterizing graph states up to eight qubits", *QIPC 2009. International Conference on Quantum Information Processing and Communication* (September 21-25, 2009, Rome, Italy). Book of abstracts, p. 39.
6. A. Cabello, J. R. Portillo, A. J. López-Tarrida y P. Moreno, "Classification of the entanglement properties of eight qubit graph states", *JCCGG 2009. The 7th Japan Conference on Computational Geometry and Graphs (Kanazawa, Japón, 11-13 de noviembre de 2009)*. Book of abstracts, Japan Advanced Institute of Science and Technology, Kanazawa, 2009, pp. 105-106.
7. A. Cabello y P. Moreno, "All-versus-nothing proofs of Bell's theorem with  $n$ -qubit distributed between  $m$  parties", *QIPC 2009. International Conference on Quantum Information Processing and Communication* (September 21-25, 2009, Rome, Italy). Book of abstracts, p. 45.
8. A. Cabello y P. Moreno, "All-versus-nothing proofs of Bell's theorem with  $n$ -qubit distributed between  $m$  parties", *International Conference on Quantum Information and Computation* (Estocolmo, 4-8 de octubre de 2010). I. Bengtsson, G. Björk y M. Bourennane (eds.) International Conference on Quantum Information and Computation. Stockholm, 4-8 October, 2010. Book of abstracts, p. P2.20.

## Bipartite All-Versus-Nothing Proofs of Bell's Theorem with Single-Qubit Measurements

Adán Cabello\* and Pilar Moreno

*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

(Received 17 May 2007; published 27 November 2007)

If  $n$  qubits were distributed between 2 parties, which quantum pure states and distributions of qubits would allow all-versus-nothing (or Greenberger-Horne-Zeilinger-like) proofs of Bell's theorem using only single-qubit measurements? We show a necessary and sufficient condition for the existence of these proofs for *any* number of qubits, and provide *all* distinct proofs up to  $n = 7$  qubits. Remarkably, there is only one distribution of a state of  $n = 4$  qubits, and six distributions, each for a different state of  $n = 6$  qubits, which allow these proofs.

DOI: [10.1103/PhysRevLett.99.220402](https://doi.org/10.1103/PhysRevLett.99.220402)

PACS numbers: 03.65.Ud, 03.65.Ta, 03.67.Mn, 42.50.Xa

The Greenberger-Horne-Zeilinger (GHZ) proof [1,2] of Bell's theorem [3] not only “opened a new chapter on the hidden variables problem” [4] and made “the strongest case against local realism since Bell's work” [5], it also inspired the quantum protocols for reducing communication complexity [6] and for secret sharing [7], and motivated the study of multipartite entanglement [8]. The GHZ proof provides a direct contradiction, using qubits and without requiring inequalities, between the Einstein-Podolsky-Rosen (EPR) criterion of elements of reality [9] and perfect correlations predicted by quantum mechanics. Mermin coined the name “all-versus-nothing” (AVN) for proofs like GHZ's, based on  $m$  perfect correlations such that, if we assume elements of reality,  $m - 1$  of them lead us to the conclusion that it is the *opposite* of the one given by the  $m$ th correlation [10].

However, while the original proof of Bell's theorem required only 2 separated parties, the GHZ proof required 3 because, when the qubits are distributed between 2 parties, there is no physical reason supporting the assumption that all single-qubit observables appearing in the proof have predefined results, since some of them do *not* satisfy EPR's criterion of elements of reality. EPR's criterion states that: “if, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity” [9]. Applied to the bipartite case, this means that it must be possible to predict with certainty the results of measuring all observables appearing in the proof on Alice's (Bob's) side from the results of spacelike separated measurements on Bob's (Alice's) side.

The first 2-party AVN proof with qubits was introduced in [11,12], then adapted for 2 photons [13], and finally tested in the laboratory [14,15]. One of the difficulties of experimentally implementing this 2-party AVN proof was that it required 2-qubit local measurements [16]. The first 2-party AVN proof requiring only single-qubit measurements was introduced in [17,18] and has been recently demonstrated in the laboratory [19]. These bipartite AVN

proofs required 4-qubit states with 2 qubits each on Alice's and Bob's sides.

The possibilities brought forth by recent developments like 2-photon hyperentangled states (i.e., entangled in several degrees of freedom) encoding 3 or more qubits in each photon [20], and 6-photon 6-qubit states [21,22], naturally lead to the following problem: If  $n$  qubits were distributed between 2 parties, which are the quantum pure states and possible distributions of qubits that allow a 2-party AVN proof using only single-qubit measurements?

This problem is also related to the one of finding genuinely new bipartite communication complexity problems with a quantum advantage (specifically, new schemes of quantum pseudotelepathy [23]), and to the problem of deciding which  $n$ -qubit states and distributions of qubits allow bipartite EPR-Bell inequalities [24,25].

In this Letter we show a necessary and sufficient condition for the existence of bipartite AVN proofs using only single-qubit measurements (BAVN hereafter) for *any* number of qubits. We then proceed to explicitly provide *all* physically distinct BAVN proofs with up to 7 qubits.

A BAVN proof consists of an  $n$ -qubit quantum state and a set of single-qubit measurements that satisfy two requirements: (a) *Perfect correlations to define bipartite EPR's elements of reality.* Every single-qubit observable involved in the proof must satisfy EPR's criterion of elements of reality. (b) *Perfect correlations that contradict EPR's elements of reality.* The observables that satisfy EPR's condition *cannot* have predefined results, because it must be impossible to assign them values that satisfy all the perfect correlations predicted by quantum mechanics.

Perfect correlations are necessary to establish elements of reality and to prove that they are incompatible with quantum mechanics. Therefore, the states we are interested in must be simultaneous eigenstates of a sufficient number of commuting  $n$ -fold tensor products of single-qubit operators. Suppose that  $A$  and  $B$  are single-qubit operators on the same qubit. If they are different, they cannot be commuting operators. The only way to make the  $n$ -fold tensor products be commuting operators is to choose  $A$  and  $B$  to

be *anticommuting* operators. Therefore, in an AVN proof, all the local operators corresponding to the same qubit must be anticommuting operators. The maximum number of anticommuting single-qubit operators is 3. Therefore, without loss of generality, we can restrict our attention to a specific set of 3 single-qubit anticommuting operators on each qubit, e.g., the Pauli matrices  $X = \sigma_x$ ,  $Y = \sigma_y$ , and  $Z = \sigma_z$ . This leads us to the notion of stabilizer states. An  $n$ -qubit *stabilizer state* is defined as the simultaneous eigenstate with eigenvalue 1 of a set of  $n$  independent (in the sense that none of them can be written as a product of the others) commuting elements of the Pauli group, defined as the group, under matrix multiplication, of all  $n$ -fold tensor products of  $X$ ,  $Y$ ,  $Z$ , and the identity  $\mathbb{1}$ . The  $n$  independent elements are called *stabilizer generators* and generate a maximally Abelian subgroup called the *stabilizer group* of the state [26]. The  $2^n$  elements of the stabilizer group are called *stabilizing operators* and provide all the perfect correlations of the stabilizer state.

Moreover, since any stabilizer state is local Clifford equivalent (i.e., equivalent under the local unitary operations that map the Pauli group to itself under conjugation) to a graph state [27], then we can restrict our attention to graph states. A *graph state* [28] is a stabilizer state whose generators can be written with the help of a graph.  $|G\rangle$  is the  $n$ -qubit state associated with the graph  $G$ , which gives a recipe both for preparing  $|G\rangle$  and for obtaining  $n$  stabilizer generators that uniquely determine  $|G\rangle$ . On one hand,  $G$  is a set of  $n$  vertices (each of them representing a qubit) connected by edges (each of them representing an Ising interaction between the connected qubits). On the other hand, the stabilizer generator  $g_i$  is obtained by looking at the vertex  $i$  of  $G$  and the set  $N(i)$  of vertices that are connected to  $i$ , and is defined by

$$g_i = X_i \bigotimes_{j \in N(i)} Z_j, \quad (1)$$

where  $X_i$ ,  $Y_i$ , and  $Z_i$  denote the Pauli matrices acting on the  $i$ th qubit.  $|G\rangle$  is the unique  $n$ -qubit state that fulfills

$$g_i |G\rangle = |G\rangle, \quad \text{for } i = 1, \dots, n. \quad (2)$$

Therefore, the stabilizer group is

$$S(|G\rangle) = \{s_j, j = 1, \dots, 2^n\}; \quad s_j = \prod_{i \in I_j(G)} g_i \quad (3)$$

where  $I_j(G)$  denotes a subset of  $\{g_i\}_{i=1}^n$ . The stabilizing operators of  $|G\rangle$  satisfy

$$s_j |G\rangle = |G\rangle. \quad (4)$$

Equations like (4) are the ones that can be used to establish elements of reality and prove their incompatibility with quantum mechanics.

Although graph states are now ubiquitous in quantum information theory due to their role as code words of quantum error correcting codes [26], or in measurement-

based quantum computation [29], or due to their use in the classification of entanglement [30], the first  $n > 2$ -qubit graph states were the GHZ states and appeared in the context of AVN proofs. It is then not that surprising that, when we want to obtain BAVN proofs, we go back to graph states. Indeed, DiVincenzo and Peres already showed that the requirement (b) does not only occur for GHZ states, but is also inherent to all standard code words of quantum error correcting codes [31]. More recently, Scarani *et al.* have shown that (b) holds for cluster states constructed on square lattices of any dimension [32]. Furthermore, a positive by-product of focusing on graph states is that graph states associated with connected graphs have been exhaustively classified. There is only one 2-qubit graph state (equivalent to a Bell state), only one 3-qubit graph state (the GHZ state), two 4-qubit graph states (the GHZ and the cluster state), four 5-qubit graph states, eleven 6-qubit graph states, and twenty-six 7-qubit graph states [28].

Therefore, our problem reduces to the following: If  $n$  qubits were distributed between 2 parties, which  $n$ -qubit graph states and possible distributions of qubits allow a bipartite AVN proof using only single-qubit observables?

Note that, even considering only up to 7 qubits, there are hundreds of states and possible distributions that could potentially lead to a BAVN proof. Remarkably, this is not the case.

Our starting point is the observation that requirement (b) is satisfied by *any* graph state.

*Lemma 1.*—Any graph state associated with a connected graph of 3 or more vertices leads to algebraic contradictions with the concept of elements of reality (when each qubit is distributed to a different party).

This result was anticipated in [30–32]. The interest of the following proof is that it provides methods for obtaining explicit examples of sets of perfect correlations satisfying (b).

*Proof.*—If qubit  $i$  is connected to qubit  $j$ , and  $j$  is connected to  $k$ , there are two possibilities. One is that  $i$  is not connected to  $k$ . Then, no theory exists that assigns predefined values  $-1$  or  $1$  to  $Y_i$ ,  $Z_i$ ,  $X_j$ ,  $Y_j$ ,  $Y_k$ , and  $Z_k$ , simultaneously satisfying the four equations

$$g_i g_j |G\rangle = |G\rangle, \quad (5a)$$

$$g_j |G\rangle = |G\rangle, \quad (5b)$$

$$g_j g_k |G\rangle = |G\rangle, \quad (5c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad (5d)$$

since  $g_i g_j \cdot g_j \cdot g_j g_k$  (where “ $\cdot$ ” means matrix multiplication) is equal, not to  $g_i g_j g_k$  (as expected in any theory with predefined values), but to  $-g_i g_j g_k$ .

The other possibility is that qubit  $i$  is also connected to  $k$ . Then, no theory exists that assigns predefined values  $-1$  or  $1$  to  $X_i$ ,  $Z_i$ ,  $X_j$ ,  $Z_j$ ,  $X_k$ , and  $Z_k$ , simultaneously satisfying the four equations

$$g_i|G\rangle = |G\rangle, \quad (6a)$$

$$g_j|G\rangle = |G\rangle, \quad (6b)$$

$$g_k|G\rangle = |G\rangle, \quad (6c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad (6d)$$

since  $g_i g_j g_k$  is equal to  $-g_i g_j g_k$ . ■

Any set of equations associated with the stabilizing operators containing a subset satisfying (b) also satisfies (b). Therefore, given a graph state associated with a connected graph of  $n > 3$  vertices, there are *thousands* of possible different subsets of equations satisfying (b). Most of them involve the three Pauli matrices of all the qubits, but some of them do not. However, in our BAVN proofs it is relevant that the three Pauli matrices of *each and every one* of Alice's (Bob's) qubits can be regarded as EPR elements of reality, because we are interested in new BAVN proofs involving new classes of graph states, not those which are mere consequences of previously considered graph states of fewer qubits.

Therefore, the problem we have to solve is that of finding out for which graph states and distributions are all the three Pauli matrices for all the single-qubit elements of reality in a bipartite scenario. A distribution of  $n$  qubits between Alice and Bob is said to permit *bipartite elements of reality* when, for each and every qubit, the results of measuring two Pauli matrices on Alice's (Bob's) qubit  $j$  can be predicted with certainty from the results of measurements on Bob's (Alice's) qubits only.

Let us define the *reduced stabilizer* of Alice's (Bob's) qubits as the one obtained by tracing out Bob's (Alice's) qubits. A necessary and sufficient condition for bipartite elements of reality is the following.

**Lemma 2.**—A distribution of  $n$  qubits between Alice (who is given  $n_A$  qubits) and Bob (who is given  $n_B = n - n_A$  qubits) permits bipartite elements of reality if and only if  $n_A = n_B$ , and the reduced stabilizer of Alice's (Bob's) qubits contains *all* possible variations with repetition of the four elements,  $\mathbb{1}$ ,  $X$ ,  $Y$ , and  $Z$ , which choose  $n_A$  ( $n_B$ ), without repeating any of them.

**Proof.**—Suppose that two Pauli matrices of Alice's qubit 1, e.g.,  $X_1$  and  $Y_1$ , are elements of reality. Then each of them must be predicted with certainty from Bob's measurements. That is, the reduced stabilizer of Alice's qubits

must contain

$$X_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (7a)$$

$$Y_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}. \quad (7b)$$

Therefore, the third Pauli matrix of Alice's qubit 1 must also be an element of reality, since the product of (7a) and (7b), which must belong to the reduced stabilizer of Alice's qubits, is

$$Z_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}. \quad (8)$$

The same must happen with the three Pauli matrices of Alice's qubits 2,  $\dots$ ,  $n_A$ . Therefore, the reduced stabilizer of Alice's qubits must also contain

$$\mathbb{1}_1 \otimes X_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (9a)$$

$$\mathbb{1}_1 \otimes Y_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (9b)$$

$$\mathbb{1}_1 \otimes Z_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \dots, \quad (9c)$$

$$\mathbb{1}_1 \otimes \dots \otimes \mathbb{1}_{n_A-1} \otimes Z_{n_A}. \quad (9d)$$

Moreover, the reduced stabilizer of Alice's qubits must contain all the possible products of Eqs. (7a), (7b), (8), and (9a)–(9d); that is, all possible variations with repetition of the four elements,  $\mathbb{1}$ ,  $X$ ,  $Y$ , and  $Z$ , choose  $n_A$ , which are  $4^{n_A} = 2^{2n_A}$ . Furthermore, a similar reasoning applies to the three Pauli matrices of each and every one of Bob's qubits. Therefore, the reduced stabilizer of Bob's qubits must also contain all the possible products of

$$X_{n_A+1} \otimes \mathbb{1}_{n_A+2} \otimes \dots \otimes \mathbb{1}_{n_B}, \dots, \quad (10a)$$

$$\mathbb{1}_{n_A+1} \otimes \dots \otimes \mathbb{1}_{n_B-1} \otimes Z_{n_B}. \quad (10b)$$

But the total stabilizer has only  $2^{n_A+n_B}$  terms; therefore the only possibility is that  $n_A = n_B$ . In addition, note that there is no space for any of the variations with repetition to be repeated. ■

Most of the graph states *cannot* be used in BAVN proofs. The remarkable point is that there are a few graph states and distributions of qubits that satisfy the requirements of Lemma 2, and therefore simultaneously fulfill (a) and (b). Moreover, since Lemma 2 is a necessary and sufficient condition, when we apply it to every possible distribution of qubits of all possible graph states, we obtain a *complete* classification of all possible BAVN proofs.

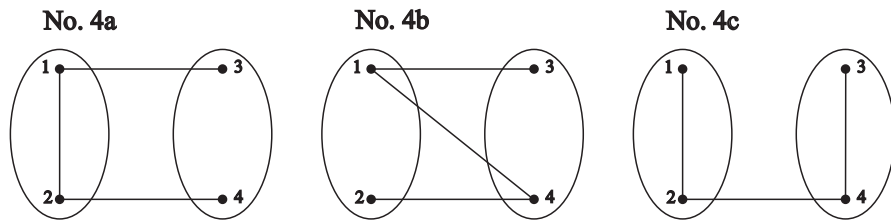


FIG. 1. Bipartite distributions of the 4-qubit cluster state (graph state no. 4 according to Hein *et al.* [28]). Distribution 4a permits bipartite elements of reality and BAVN proofs. Distribution 4b is physically equivalent (it is just relabeling the basis). Distribution 4c is not equivalent to the other two, and does not permit bipartite elements of reality.

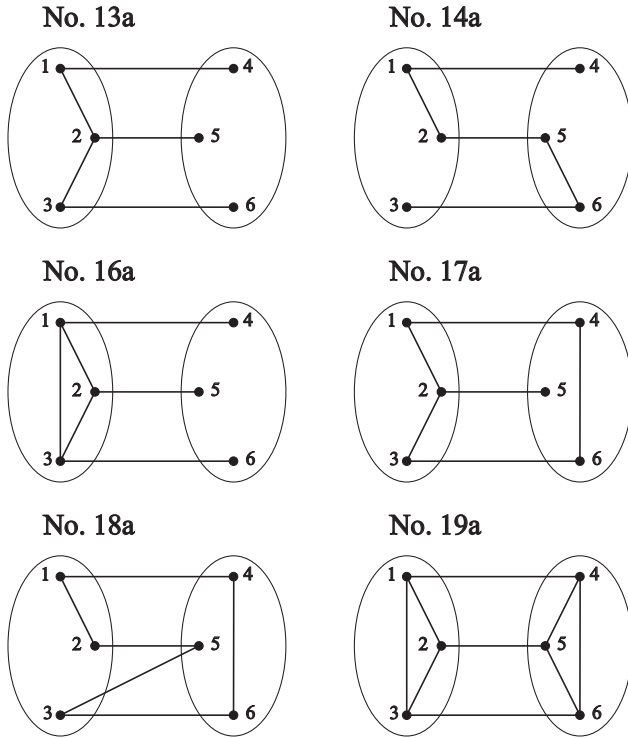


FIG. 2. Bipartite distributions of the 6-qubit graph states that permit bipartite elements of reality and BAVN proofs. The graphs' nomenclature follows Hein *et al.* [28], but the labeling of the qubits is different: Qubits 1, 2, and 3 belong to Alice, and qubits 4, 5, and 6 belong to Bob.

With  $n < 8$  qubits, and modulo single-qubit unitary transformations, the only states and distributions of qubits that allow BAVN proofs are the following. There is only one graph state with 4 qubits:

$$|\psi_{4a}\rangle = \frac{1}{\sqrt{2}}(|00\rangle|\bar{0}\bar{0}\rangle + |01\rangle|\bar{0}\bar{1}\rangle + |10\rangle|\bar{1}\bar{0}\rangle - |11\rangle|\bar{1}\bar{1}\rangle), \quad (11)$$

where  $|00\rangle|\bar{0}\bar{0}\rangle = |\sigma_z = 0\rangle_1 \otimes |\sigma_z = 0\rangle_2 \otimes |\sigma_x = 0\rangle_3 \otimes |\sigma_x = 0\rangle_4$ , with qubits 1 and 2 in Alice's side, and qubits 3 and 4 in Bob's. The state  $|\psi_{4a}\rangle$  corresponds to the graph state no. 4 according to Hein *et al.* [28], with its qubits distributed as in Fig. 1, distribution 4a. Note that any other nonequivalent distribution of qubits does not allow BAVN proofs (see Fig. 1). This BAVN proof is precisely the one introduced in [17]. The new result is that the proof in [17] is *the only one* with 4 qubits and single-qubit measurements.

Between 5 and 7 qubits, there are only 6 possible states and distributions leading to BAVN proofs. All of them are 6-qubit states in which each party has 3 qubits. Their corresponding graphs are summarized in Fig. 2. The explicit expressions of each state can be obtained from its graph using (1) and (2). Two 6-qubit graph states have been recently prepared in the laboratory [21,22], but none of

them allows BAVN proofs. A 6-qubit BAVN proof constitutes an interesting experimental challenge for the near future.

This work was sparked by questions made by F. Verstraete and M. Żukowski. The authors thank H. Briegel, W. Dür, O. Gühne, A. J. López-Tarrida, and M. van den Nest for their useful comments, and acknowledge support by the Spanish MEC Project No. FIS2005-07689 and the Junta de Andalucía Excellence Project No. P06-FQM-2243.

\*adan@us.es

- [1] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, Holland, 1989), p. 69.
- [2] N. D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
- [3] J. S. Bell, *Physics* (Long Island City, N.Y.) **1**, 195 (1964).
- [4] M. Żukowski, *Phys. Lett. A* **157**, 198 (1991).
- [5] R. K. Clifton, M. L. G. Redhead, and J. N. Butterfield, *Found. Phys.* **21**, 149 (1991).
- [6] R. Cleve and H. Buhrman, *Phys. Rev. A* **56**, 1201 (1997).
- [7] M. Żukowski *et al.*, *Acta Phys. Pol. A* **93**, 187 (1998).
- [8] W. Dür, G. Vidal, and J. I. Cirac, *Phys. Rev. A* **62**, 062314 (2000).
- [9] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [10] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [11] A. Cabello, *Phys. Rev. Lett.* **86**, 1911 (2001).
- [12] A. Cabello, *Phys. Rev. Lett.* **87**, 010403 (2001).
- [13] Z.-B. Chen *et al.*, *Phys. Rev. Lett.* **90**, 160408 (2003).
- [14] C. Cinelli *et al.*, *Phys. Rev. Lett.* **95**, 240405 (2005).
- [15] T. Yang *et al.*, *Phys. Rev. Lett.* **95**, 240406 (2005).
- [16] A. I. Lvovsky, *Phys. Rev. Lett.* **88**, 098901 (2002).
- [17] A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).
- [18] A. Cabello, *Phys. Rev. A* **72**, 050101(R) (2005).
- [19] G. Vallone *et al.*, *Phys. Rev. Lett.* **98**, 180502 (2007).
- [20] J. T. Barreiro *et al.*, *Phys. Rev. Lett.* **95**, 260501 (2005).
- [21] Q. Zhang *et al.*, *Nature Phys.* **2**, 678 (2006).
- [22] C.-Y. Lu *et al.*, *Nature Phys.* **3**, 91 (2007).
- [23] A. Cabello, *Phys. Rev. A* **73**, 022302 (2006).
- [24] A. Cabello, *Phys. Rev. Lett.* **97**, 140406 (2006).
- [25] M. Barbieri *et al.*, *Phys. Rev. Lett.* **97**, 140407 (2006).
- [26] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
- [27] M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **69**, 022316 (2004).
- [28] M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [29] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [30] M. Hein *et al.*, in *Quantum Computers, Algorithms and Chaos*, edited by G. Casati *et al.* (IOS Press, Amsterdam, 2006).
- [31] D. P. DiVincenzo and A. Peres, *Phys. Rev. A* **55**, 4089 (1997).
- [32] V. Scarani *et al.*, *Phys. Rev. A* **71**, 042325 (2005).



# Nonlocality for Graph States

A. Cabello<sup>a,\*</sup>, O. Gühne<sup>b,c</sup>, P. Moreno<sup>a</sup>, and D. Rodríguez<sup>d</sup>

<sup>a</sup> *Departamento de Física Aplicada II, Universidad de Sevilla, Sevilla, E-41012 Spain*

<sup>b</sup> *Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Technikerstraße 21A, Innsbruck, A-6020 Austria*

<sup>c</sup> *Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020 Austria*

<sup>d</sup> *Departamento de Física Aplicada III, Universidad de Sevilla, Sevilla, E-41092 Spain*

\*e-mail: adan@us.es

Received October 18, 2007

**Abstract**—The possibility of preparing two-photon entangled states encoding three or more qubits in each photon leads to the following problem: If  $n$  qubits were distributed between two parties, which quantum pure states and qubit distributions would allow all-versus-nothing (or Greenberger–Horne–Zeinger-like) proofs of Bell’s theorem using only single-qubit measurements? We show a necessary and sufficient condition for the existence of these proofs and provide all existing proofs up to  $n = 7$  qubits. On the other hand, the possibility of preparing  $n$ -photon  $n$ -qubit graph states leads to the following problem: If  $n$  qubits were distributed between  $n$  parties, which would be the optimal Bell inequalities? We show all optimal  $n$ -party Bell inequalities for the perfect correlations of any graph state of  $n < 6$  qubits. Optimal means that the ratio between the quantum violation and the bound for local hidden-variable theories is the maximum over all possible combinations of perfect correlations. This implies that the required detection efficiencies for loophole-free Bell tests are minimal.

PACS numbers: 03.65.Ud, 03.67.Pp, 03.67.-a, 42.50.-p

DOI: 10.1134/S1054660X08030249

## 1. “ALL-VERSUS-NOTHING” PROOFS OF BELL’S THEOREM

The Greenberger–Horne–Zeinger (GHZ) proof [1, 2] of Bell’s theorem [3] not only “opened a new chapter on the hidden-variables problem” [4] and made “the strongest case against local realism since Bell’s work” [5], it also inspired the quantum protocols for reducing communication complexity [6] and for secret sharing [7], and motivated the study of multipartite entanglement [8]. The GHZ proof provides a direct contradiction, using qubits and without requiring inequalities, between Einstein, Podolsky, and Rosen’s (EPR’s) criterion of elements of reality [9] and perfect correlations predicted by quantum mechanics. Mermin coined the name “all-versus-nothing” (AVN) for proofs like GHZ’s, based on  $m$  perfect correlations such that, if we assume elements of reality,  $m - 1$  of them lead us to the conclusion that it is the *opposite* of the one given by the  $m$ th correlation [10].

However, while the original proof of Bell’s theorem required only two separated parties, the GHZ proof required three, because, when the qubits are distributed between two parties, there is no physical reason supporting the assumption that all single-qubit observables appearing in the proof have predefined results, since some of them do *not* satisfy EPR’s criterion of elements of reality. EPR’s criterion states that: “If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity” [9].

Applied to the bipartite case, this means that it must be possible to predict with certainty the results of measuring all observables appearing in the proof on Alice’s (Bob’s) side from the results of space-like separated measurements on Bob’s (Alice’s) side.

The first two-party AVN proof with qubits was introduced in [11, 12], then adapted for two photons [13], and finally tested in the laboratory [14, 15]. One of the difficulties of experimentally implementing this two-party AVN proof was that it required two-qubit local measurements [16]. The first two-party AVN proof requiring only single-qubit measurements was introduced in [17, 18] and has been recently demonstrated in the laboratory [19]. These bipartite AVN proofs required four-qubit states with two qubits each on Alice’s and Bob’s sides.

The possibilities brought forth by recent developments like two-photon hyper-entangled states (i.e., entangled in several degrees of freedom) encoding three or more qubits in each photon [20], and six-photon six-qubit states [21, 22], naturally lead to the following problem: If  $n$  qubits were distributed between two parties, which are the quantum pure states and possible distributions of qubits that allow a two-party AVN proof using only single-qubit measurements?

This problem is also related to the one of finding genuinely new bipartite communication complexity problems with a quantum advantage (specifically, new schemes of quantum pseudotelepathy [23]), and to the problem of deciding which  $n$ -qubit states and distribu-

tions of qubits allow bipartite EPR–Bell inequalities [24, 25].

In Section 3, we show a necessary and sufficient condition for the existence of bipartite AVN proofs using only single-qubit measurements (BAVN hereafter) for *any* number of qubits. We, then, proceed to explicitly provide *all* physically distinct BAVN proofs with up to seven qubits.

## 2. BELL INEQUALITIES FOR PERFECT CORRELATIONS AND EXPONENTIALLY GROWING-WITH-SIZE NONLOCALITY

Einstein–Podolsky–Rosen’s (EPR’s) argument of the incompleteness of quantum mechanics is based on the perfect correlations of a specific state [9]. Conversely, the violation of the original Bell inequality, which shows that quantum mechanics predicts values beyond those of EPR’s local realism, makes use of non-perfect correlations [3]. Greenberger, Horne, and Zeilinger showed that, for some  $n$ -qubit states (henceforth called GHZ states), Bell’s theorem can be proved in quite an elegant way by invoking only perfect correlations [1]. Finally, Mermin [2] realized that the perfect correlations of GHZ states lead to genuinely new  $n$ -party Bell inequalities, where the degree of nonlocality, defined as the ratio  $\mathcal{D}$  between the quantum violation and the bound for local hidden-variable theories (LHVTs), increases *exponentially* with  $n$ .

This discovery is important for two reasons: On the one hand, it suggests that nonlocality is not a purely microscopic effect, but may instead increase with the size of the system. On the other hand, it is potentially useful for the design of a loophole-free Bell experiment, since the minimum detection efficiency  $\eta$  required for a  $n$ -party Bell experiment without the detection loophole [26] satisfies

$$\mathcal{D} = [1 - (1 - \eta)^n] \eta^{-n}, \quad (1)$$

showing that the required  $\eta$  decreases significantly if  $\mathcal{D}$  increases [24].

Unfortunately, it is difficult to perform an exponentially growing-with- $n$  nonlocality experiment or a loophole-free Bell experiment using GHZ states. This is because the GHZ state’s sensitivity to decoherence also increases with  $n$  [27], so that the advantage of a higher  $\mathcal{D}$  or a lower  $\eta$  vanishes. Indeed, actual experiments with  $n \geq 4$  GHZ states have low visibilities [28]. A fundamental limitation seemingly exists to observe macroscopic  $n$ -party nonlocality with GHZ correlations. At this point, a natural question arises: Does this limitation also hold for other types of  $n$ -qubit states? Specifically, does it hold for  $n$ -qubit *graph* states? Graph states [29, 30] are particularly interesting for several reasons. Firstly, graph states are a natural extension of GHZ states, in the sense that they are a larger class of states with perfect correlations. Secondly, the effect of decoherence in various graph states has already been studied

and it has been shown that, for a fixed  $n$ , some graph states are much more robust against decoherence than GHZ states [27]. Finally, graph states play an eminent role in many applications of quantum information like quantum error-correction [31] and measurement-based quantum computation [32].

The nonlocal properties of graph states have been studied recently from several perspectives [17, 33–37]. In [34, 35], it has been shown that for all graph states there is a Bell inequality involving only perfect correlations. These inequalities show that nonlocality increases exponentially with  $n$  for some specific classes of graph states like GHZ states [2], linear cluster states, and other regular graph states [34, 35]. However, these inequalities are *not* optimal: there are Bell inequalities with higher  $\mathcal{D}$  and requiring a lower  $\eta$ . This means that the scaling of  $\mathcal{D}$  with  $n$  for graph states is unknown; we have only lower bounds.

In Section 4, we provide *all* optimal Bell inequalities for the perfect correlations of *all* graph states up to  $n = 5$  qubits. With this aim, for a given graph state, we consider all possible Bell operators  $\beta$ , which are sums of the stabilizing operators. For each  $\beta$ , we compute the maximum attainable value for LHVTs, which can be accomplished by considering the finite set of deterministic LHVTs [34]. Then, we compute the corresponding  $\mathcal{D}$  and determine the  $\beta$  which leads to the highest violation. The exhaustive study for  $n \geq 6$  becomes computationally difficult since the number of possible Bell operators to explore is  $2^{2^n}$ , and the number of inequivalent graph states increases rapidly with  $n$ .

## 3. BIPARTITE ALL-VERSUS-NOTHING PROOFS OF BELL’S THEOREM WITH SINGLE-QUBIT MEASUREMENTS

### 3.1. Requirements for an AVN Proof

A BAVN proof consists of a  $n$ -qubit quantum state and a set of single-qubit measurements which satisfy two requirements:

(a) *Perfect correlations to define bipartite EPR’s elements of reality.* Every single-qubit observable involved in the proof must satisfy EPR’s criterion of elements of reality.

(b) *Perfect correlations that contradict EPR’s elements of reality.* The observables which satisfy EPR’s condition cannot have predefined results, because it must be impossible to assign them values which satisfy all of the perfect correlations predicted by quantum mechanics.

Perfect correlations are necessary to establish elements of reality and to prove that they are incompatible with quantum mechanics. Therefore, the states we are interested in must be simultaneous eigenstates of a sufficient number of commuting  $n$ -fold tensor products of single-qubit operators. Suppose that  $A$  and  $B$  are single-qubit operators on the same qubit. If they are different,

they cannot be commuting operators. The only way to make the  $n$ -fold tensor products be commuting operators is to choose  $A$  and  $B$  to be *anticommuting* operators. Therefore, in an AVN proof, all of the local operators corresponding to the same qubit must be anticommuting operators. The maximum number of anticommuting single-qubit operators is three. Therefore, without a loss of generality, we can restrict our attention to a specific set of three single-qubit anticommuting operators on each qubit, e.g., the Pauli matrices  $X = \sigma_x$ ,  $Y = \sigma_y$ , and  $Z = \sigma_z$ . This leads us to the notion of stabilizer states.

### 3.2. Stabilizer States and Stabilizing Operators

A  $n$ -qubit *stabilizer state* is defined as the simultaneous eigenstate with eigenvalue 1 of a set of  $n$  independent (in the sense that none of them can be written as a product of the others) commuting elements of the Pauli group, defined as the group, under matrix multiplication, of all  $n$ -fold tensor products of  $X$ ,  $Y$ , and  $Z$ , and the identity  $\mathbb{1}$ . The  $n$  independent elements are called *stabilizer generators* and generate a maximally abelian subgroup called the *stabilizer group* of the state [31]. The  $2^n$  elements of the stabilizer group are called *stabilizing operators*, and provide all of the perfect correlations of the stabilizer state.

Moreover, since any stabilizer state is a local Clifford equivalent (i.e., equivalent under the local unitary operations that map the Pauli group to itself under conjugation) to a graph state [38], then we can restrict our attention to graph states.

### 3.3. Graph States

A *graph state* [29, 30] is a stabilizer state whose generators can be written with the help of a graph.  $|G\rangle$  is the  $n$ -qubit state associated with the graph  $G$ , which gives both a recipe for preparing  $|G\rangle$  and for obtaining  $n$  stabilizer generators which uniquely determine  $|G\rangle$ . On one hand,  $G$  is a set of  $n$  vertices (each of them representing a qubit) connected by edges (each of them representing an Ising interaction between the connected qubits). On the other hand, the stabilizer generator  $g_i$  is obtained by looking at the vertex  $i$  of  $G$  and the set  $N(i)$  of vertices which are connected to  $i$ , and is defined by

$$g_i = X_i \bigotimes_{j \in N(i)} Z_j, \quad (2)$$

where  $X_i$ ,  $Y_i$ , and  $Z_i$  denote the Pauli matrices acting on the  $i$ th qubit.  $|G\rangle$  is the unique  $n$ -qubit state which fulfils

$$g_i |G\rangle = |G\rangle, \quad \text{for } i = 1, \dots, n. \quad (3)$$

Therefore, the stabilizer group is

$$S(|G\rangle) = \{s_j, j = 1, \dots, 2^n\}; \quad s_j = \prod_{i \in I_j(G)} g_i, \quad (4)$$

where  $I_j(G)$  denotes a subset of  $\{g_i\}_{i=1}^N$ . The stabilizing operators of  $|G\rangle$  satisfy

$$s_j |G\rangle = |G\rangle. \quad (5)$$

Equations like (5) are the ones that can be used to establish the elements of reality and prove their incompatibility with quantum mechanics.

Although graph states are now ubiquitous in quantum information theory due to their role as code words for quantum error-correcting codes [31], or in measurement-based quantum computation [32], or due to their use in the classification of entanglement [29, 30], the first  $n > 2$ -qubit graph states were the GHZ states and appeared in the context of AVN proofs. It is, then, not that surprising that, when we want to obtain BAVN proofs, we go back to the graph states. Indeed, DiVincenzo and Peres already showed that the requirement (b) does not only occur for GHZ states, but is also inherent to all standard code words for quantum error-correcting codes [36]. More recently, Scarani et al. have shown that (b) holds for cluster states constructed on square lattices of any dimension [37]. Furthermore, a positive byproduct of focusing on graph states is that graph states associated with connected graphs have been exhaustively classified. There are only one two-qubit graph state (equivalent to a Bell state), only one three-qubit graph state (the GHZ state), two four-qubit graph states (the GHZ and the cluster state), four five-qubit graph states, 11 six-qubit graph states, and 26 seven-qubit graph states [29, 30].

### 3.4. Bipartite AVN Proofs with Single-Qubit Measurements for Graph States

Therefore, our problem reduces to the following: If  $n$  qubits were distributed between two parties, which  $n$ -qubit graph states and possible distributions of qubits allow a bipartite AVN proof using only single-qubit observables?

Note that, even considering only up to seven qubits, there are hundreds of states and possible distributions which could potentially lead to a BAVN proof. Remarkably, this is not the case.

Our starting point is the observation that requirement (b) is satisfied by *any* graph state.

#### 3.4.1. Necessary and sufficient conditions.

**Lemma 1:** Any graph state associated with a connected graph of three or more vertices leads to algebraic contradictions with the concept of elements of reality (when each qubit is distributed to a different party).

This result was anticipated in [30, 36, 37]. The interest of the following proof is that it provides methods for

obtaining explicit examples of sets of perfect correlations satisfying (b).

*Proof:* If qubit  $i$  is connected to qubit  $j$ , and  $j$  is connected to  $k$ , there are two possibilities. One is that  $i$  is not connected to  $k$ . Then, no theory exists which assigns predefined values  $-1$  or  $1$  to  $Y_i, Z_i, X_j, Y_j, Y_k$ , and  $Z_k$  simultaneously satisfying the four equations

$$g_i g_j |G\rangle = |G\rangle, \quad (6a)$$

$$g_j |G\rangle = |G\rangle, \quad (6b)$$

$$g_j g_k |G\rangle = |G\rangle, \quad (6c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad (6d)$$

since  $g_i g_j \cdot g_j \cdot g_j g_k$  (where “ $\cdot$ ” means matrix multiplication) is equal, not to  $g_i g_j g_k$  (as expected in any theory with predefined values), but to  $-g_i g_j g_k$ .

The other possibility is that qubit  $i$  is also connected to  $k$ . Then, no theory exists which assigns predefined values  $-1$  or  $1$  to  $X_i, Z_i, X_j, Z_j, X_k$ , and  $Z_k$  simultaneously satisfying the four equations

$$g_i |G\rangle = |G\rangle, \quad (7a)$$

$$g_j |G\rangle = |G\rangle, \quad (7b)$$

$$g_k |G\rangle = |G\rangle, \quad (7c)$$

$$g_i g_j g_k |G\rangle = |G\rangle, \quad (7d)$$

since  $g_i \cdot g_j \cdot g_k$  is equal to  $-g_i g_j g_k$ .

Any set of equations associated with the stabilizing operators containing a subset satisfying (b) also satisfies (b). Therefore, given a graph state associated with a connected graph of  $n > 3$  vertices, there are *thousands* of possible different subsets of equations satisfying (b). Most of them involve the three Pauli matrices of all the qubits, but some of them do not. However, in our BAVN proofs, it is relevant that the three Pauli matrices of *each and every one* of Alice’s (Bob’s) qubits can be regarded as EPR elements of reality. One reason to consider all the qubits is that we are interested in new BAVN proofs involving new kinds of graph states and not mere consequences of previously considered graph states with fewer qubits.

Therefore, the problem we have to solve is that of finding out for which graph states and distributions are all three Pauli matrices for all single-qubits elements of reality in a bipartite scenario. A distribution of  $n$  qubits between Alice and Bob is said to permit *bipartite elements of reality* when, for each and every qubit, the results of measuring two Pauli matrices on Alice’s (Bob’s) qubit  $j$  can be predicted with certainty from the results of measurements on Bob’s (Alices’s) qubits only. Note that when two Pauli matrices can be predicted, the third one can also be predicted.

Let us define the *reduced stabilizer* of Alice’s (Bob’s) qubits as the one obtained by tracing out Bob’s

(Alice’s) qubits. A necessary and sufficient condition for bipartite elements of reality is the following.

*Lemma 2:* A distribution of  $n$  qubits between Alice (who is given  $n_A$  qubits) and Bob (who is given  $n_B = n - n_A$  qubits) permits bipartite elements of reality if and only if  $n_A = n_B$ , and the reduced stabilizer of Alice’s (Bob’s) qubits contains *all* possible variations with repetition of the four elements,  $\mathbb{1}, X, Y$ , and  $Z$ , choose  $n_A$  ( $n_B$ ), without repeating any of them.

*Proof:* Suppose that two Pauli matrices of Alice’s qubit 1, e.g.,  $X_1$  and  $Y_1$ , are elements of reality. Then, each of them must be predicted with certainty from Bob’s measurements. That is, the reduced stabilizer of Alice’s qubits must contain

$$X_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (8a)$$

$$Y_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}. \quad (8b)$$

Therefore, the third Pauli matrix of Alice’s qubit 1 must also be an element of reality, since the product of (8a) and (8b), which must belong to the reduced stabilizer of Alice’s qubits, is

$$Z_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_A}. \quad (9)$$

The same must happen with the three Pauli matrices of Alice’s qubits 2, ...,  $n_A$ . Therefore, the reduced stabilizer of Alice’s qubits must also contain

$$\mathbb{1}_1 \otimes X_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (10a)$$

$$\mathbb{1}_1 \otimes Y_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (10b)$$

$$\mathbb{1}_1 \otimes Z_2 \otimes \mathbb{1}_3 \otimes \dots \otimes \mathbb{1}_{n_A}, \quad (10c)$$

...

$$\mathbb{1}_1 \otimes \dots \otimes \mathbb{1}_{n_A-1} \otimes Z_{n_A}. \quad (10d)$$

Moreover, the reduced stabilizer of Alice’s qubits must contain all possible products of the Eqs. (8a)–(10d); that is, all possible variations with repetition of the four elements,  $\mathbb{1}, X, Y$ , and  $Z$ , choose  $n_A$ , which are  $4^{n_A} = 2^{2n_A}$ . Furthermore, a similar reasoning applies to the three Pauli matrices of each and every one of Bob’s qubits. Therefore, the reduced stabilizer of Bob’s qubits must also contain all possible products of

$$X_{n_A+1} \otimes \mathbb{1}_{n_A+2} \otimes \dots \otimes \mathbb{1}_{n_B}, \quad (11a)$$

...

$$\mathbb{1}_{n_A+1} \otimes \dots \otimes \mathbb{1}_{n_B-1} \otimes Z_{n_B}. \quad (11b)$$

But, the total stabilizer only has  $2^{n_A+n_B}$  terms; therefore, the only possibility is that  $n_A = n_B$ . In addition, note that there is no space for any of the variations with repetition to be repeated.

**3.4.2. Classification.** Most of the graph states *cannot* be used in BAVN proofs. The remarkable point is that there are a few graph states and distributions of qubits which satisfy the requirements of Lemma 2, and, therefore, simultaneously fulfill (a) and (b). Moreover, since Lemma 2 is a necessary and sufficient condition, when we apply it to every possible distribution of qubits of all possible graph states, we obtain a *complete* classification of all possible BAVN proofs.

With  $n < 8$  qubits, and modulo single-qubit unitary transformations, the only states and distributions of qubits which allow BAVN proofs are the following. There is only one graph state with four qubits:

$$|\psi_{4a}\rangle = \frac{1}{2}(|00\rangle|\bar{0}\bar{0}\rangle + |01\rangle|\bar{0}\bar{1}\rangle + |10\rangle|\bar{1}\bar{0}\rangle - |11\rangle|\bar{1}\bar{1}\rangle), \quad (12)$$

where  $|00\rangle|\bar{0}\bar{0}\rangle = |\sigma_z = 0\rangle_1 \otimes |\sigma_z = 0\rangle_2 \otimes |\sigma_x = 0\rangle_3 \otimes |\sigma_x = 0\rangle_4$ , with qubits 1 and 2 in Alice's side, and qubits 3 and 4 in Bob's. The state  $|\psi_{4a}\rangle$  corresponds to graph state no. 4 according to Hein et al. [29, 30], with its qubits distributed as in Fig. 2, distribution 4a. Note that any other inequivalent distribution of qubits does not allow BAVN proofs (see Fig. 2). This BAVN proof is precisely the one introduced in [17]. The new result is that the proof in [17] is *the only one* with four qubits and single-qubit measurements.

Between five and seven qubits, there are only six possible states and distributions leading to BAVN proofs. All of them are six-qubit states in which each party has three qubits. Their corresponding graphs are summarized in Fig. 3. The explicit expressions of each state can be obtained from its graph using (2) and (3). Two six-qubit graph states have been recently prepared in the laboratory [21, 22], but none of them allows BAVN proofs. A six-qubit BAVN proof constitutes an interesting experimental challenge for the near future.

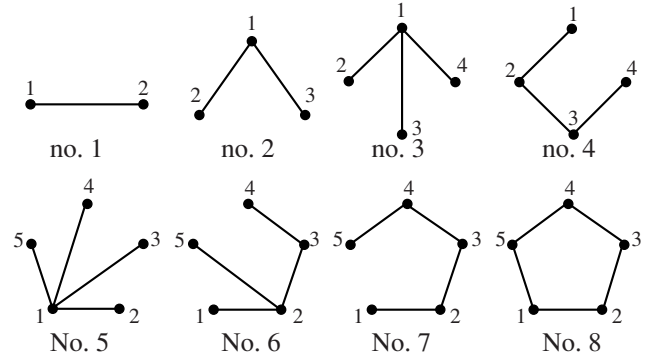
#### 4. OPTIMAL BELL INEQUALITIES FOR THE PERFECT CORRELATIONS OF ALL GRAPH STATES UP TO FIVE QUBITS

##### 4.1. Graph State No. 1 or Bell State

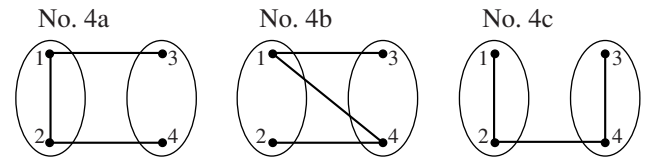
The only two-qubit graph state is, up to local unitaries, the two-qubit singlet state. The perfect correlations of this state do not permit a proof of nonlocality (of any hidden-variable theory trying to reproduce quantum mechanics), only a proof of contextuality [2, 39]. The perfect correlations of all other graph states, however, lead to Bell inequalities.

##### 4.2. Graph State No. 2, Three-Qubit GHZ, Star Graph, or Fully Connected Graph State

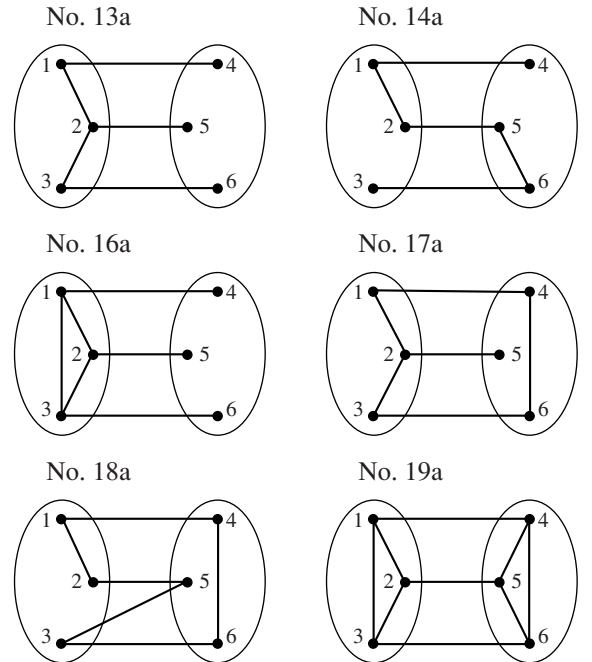
For three qubits, there is also only one graph state, coming from the star graph no. 2 (see Fig. 1). This state is, up to local unitaries, the three-qubit GHZ state. Fol-



**Fig. 1.** Graphs associated with all graph states of up to five qubits which are inequivalent under local transformations and graph isomorphism. The classification and notation stems from [29, 30].



**Fig. 2.** Bipartite distributions of the four-qubit cluster state (graph state no. 4 according to Hein et al. [29, 30]). Distribution 4a permits bipartite elements of reality and BAVN proofs. Distribution 4b is physically equivalent (it is just relabeling the basis). Distribution 4c is not equivalent to the other two, and does not permit bipartite elements of reality.



**Fig. 3.** Bipartite distributions of the six-qubit graph states that permit bipartite elements of reality and BAVN proofs. The graph's nomenclature follows Hein et al. [29, 30], but the labeling of the qubits is different: Qubits 1, 2, and 3 belong to Alice, and qubits 4, 5, and 6 belong to Bob.

lowing the method described above, we obtain that the optimal Bell inequality for the perfect correlations of graph state no. 2 is

$$-2 \leq \langle \beta_2 \rangle_{\text{LHV}} \leq 2, \quad (13)$$

where  $\langle \dots \rangle_{\text{LHV}}$  denotes the expectation value for LHVTs, and  $\beta_2$  turns out to be unique and completely symmetric,

$$\beta_2 = g_1(1 + g_2)(1 + g_3), \quad (14)$$

where  $g_i$  is the  $i$ th generator of graph state no. 2 using the labeling from Fig. 1. The quantum expected value of  $\beta_2$  is four. Clearly, it is equal to the number of terms in  $\beta_2$ . Therefore, the degree of nonlocality is  $\mathcal{D}(\beta_2) = 2$ .

Bell inequality (13) is the Mermin inequality for the three-qubit GHZ state [2]. Taking into account the definition of the generators described above, it can be written as

$$\beta_2 = X_1 Z_2 Z_3 + Y_1 Y_2 Z_3 + Y_1 Z_2 Y_3 - X_1 Y_2 Y_3. \quad (15)$$

In the following, however, we will write the Bell operators only in terms of the generators  $g_i$  of the corresponding state. This reveals their algebraic structure and leads to a compact notation.

#### 4.3. Graph State No. 3, Four-Qubit GHZ, Star Graph, or Fully Connected Graph State

For the case of four qubits, there are two inequivalent graph states. The first is the four-qubit GHZ state, corresponding to the star graph no. 3, and the second is the cluster state, corresponding to the linear cluster graph no. 4 (see Fig. 1). Both states have been prepared in various experiments [40, 41].

The optimal Bell inequality for the four-qubit GHZ state is

$$-2 \leq \langle \beta_3^{(i)} \rangle_{\text{LHV}} \leq 2, \quad (16)$$

where there are eight different Bell operators  $\beta_3^{(i)}$  giving the maximum degree of nonlocality. Two of them are completely symmetric,

$$\beta_3^{(1)} = g_1(1 + g_2 g_3 + g_2 g_4 + g_3 g_4), \quad (17a)$$

$$\beta_3^{(2)} = g_1(g_2 + g_3 + g_4 + g_2 g_3 g_4), \quad (17b)$$

where qubit 1 is the one connected to the other three (see Fig. 1). The other six are

$$\beta_3^{(3-5)} = g_1(1 + g_i)(1 + g_j), \quad (18a)$$

$$\beta_3^{(6-8)} = g_1 g_i(1 + g_j)(1 + g_k), \quad (18b)$$

where  $i, j, k \in \{2, 3, 4\}$  are pairwise different. For graph state no. 3, the quantum expected value of any  $\beta_3^{(i)}$  is four, so the degree of nonlocality is  $\mathcal{D}(\beta_3^{(i)}) = 2$ .

Interestingly, the Bell operator of the original Mermin inequality [2] is *not* among these Bell operators. It is, in fact, a sum of two optimal Bell operators; in our notation, it reads  $\langle \beta_3^{(1)} + \beta_3^{(2)} \rangle_{\text{LHV}} \leq 4$ . On the other hand, there are Bell inequalities which give a degree of nonlocality of  $2\sqrt{2}$  for the four-qubit GHZ state, but they require eight terms and involve nonperfect correlations [42].

#### 4.4. Graph State No. 4 or Four-Qubit Cluster State

Concerning the four-qubit cluster state, the optimal Bell inequality is

$$-2 \leq \langle \beta_4^{(i)} \rangle_{\text{LHV}} \leq 2, \quad (19)$$

where there are eight different Bell operators  $\beta_4^{(i)}$  giving the maximum degree of nonlocality,

$$\beta_4^{(1)} = (1 + g_1)g_2(1 + g_3), \quad (20a)$$

$$\beta_4^{(2)} = \beta_4^{(1)} g_4, \quad (20b)$$

$$\beta_4^{(3)} = (1 + g_1)g_2(1 + g_3 g_4), \quad (20c)$$

$$\beta_4^{(4)} = \beta_4^{(3)} g_4, \quad (20d)$$

and the other four Bell operators are obtained from the previous ones by making the permutations  $1 \longleftrightarrow 4$  and  $2 \longleftrightarrow 3$  of the qubits. For the cluster state, the quantum expected value of any  $\beta_4^{(i)}$  is four, so the degree of nonlocality is  $\mathcal{D}(\beta_4^{(i)}) = 2$ . Note that these inequalities contain those introduced in [17, 37] and have been recently tested in the laboratory [41]. The  $\beta_4^{(i)}$  are 2-2-2-1-setting Bell operators (i.e., one qubit does not require alternative measurements). Therefore, none of them is completely symmetric.

#### 4.5. Graph State No. 5, Five-Qubit GHZ, Star Graph, or Fully Connected Graph State

For the case of five qubits, there are four different graph states. First, we have the five-qubit GHZ state, corresponding to the five-qubit star graph (graph no. 5 in Fig. 1), and the five-qubit Y state (graph no. 6). Then, we have the five-qubit linear cluster state (graph no. 7) and finally, the five-qubit ring cluster state (graph no. 8), a state important for quantum error-correction codes [31].

The optimal Bell inequality for the five-qubit GHZ state is given by

$$-4 \leq \langle \beta_5 \rangle_{\text{LHV}} \leq 4, \quad (21)$$

where  $\beta_5$  is unique and completely symmetric,

$$\beta_5 = g_1(1 + g_2)(1 + g_3)(1 + g_4)(1 + g_5). \quad (22)$$

For graph state no. 5, the quantum expected value of  $\beta_5$  is 16, so the degree of nonlocality is  $\mathcal{D}(\beta_5) = 4$ . This is the Mermin inequality for the five-qubit GHZ state [2].

#### 4.6. Graph State No. 6 or Five-Qubit Y State

Let us now consider the five-qubit Y state (graph no. 6). For this state, we have a larger set of optimal inequalities. All take the form

$$-7 \leq \langle \beta_6^{(i)} \rangle_{\text{LHV}} \leq 7, \quad (23)$$

where there are 36 possible optimal Bell operators  $\beta_6^{(i)}$ . Half of them are related to the other half by  $\beta_6^{(i+18)} = g_4 \beta_6^{(i)}$ , where  $i = 1, \dots, 18$ . Out of the first 18, only two of them are completely symmetric (i.e., invariant after permuting  $g_1$  and  $g_5$ ; see Fig. 1). They are

$$\beta_6^{(1)} = (g_1 + g_5)g_3(1 + g_4) + A, \quad (24a)$$

$$\beta_6^{(2)} = (1 + g_1g_5)g_3(1 + g_4) + A, \quad (24b)$$

where

$$A = g_2[(1 + g_1 + g_5)(1 + g_3 + g_3g_4) + (1 + g_1g_5)g_4]. \quad (25)$$

The other 16 are

$$\beta_6^{(3)} = (1 + g_1)g_3(1 + g_4) + A, \quad (26a)$$

$$\beta_6^{(4)} = (1 + g_1)g_3(1 + g_4)g_5 + A, \quad (26b)$$

$$\beta_6^{(5)} = (g_1 + g_5)g_3(1 + g_4) + B, \quad (26c)$$

$$\beta_6^{(6)} = (1 + g_1g_5)g_3(1 + g_4) + B, \quad (26d)$$

$$\beta_6^{(7)} = (1 + g_1)g_3(1 + g_4) + B, \quad (26e)$$

$$\beta_6^{(8)} = (1 + g_1)g_3(1 + g_4)g_5 + B, \quad (26f)$$

$$\beta_6^{(9)} = g_3(1 + g_4)(1 + g_5) + B, \quad (26g)$$

$$\beta_6^{(10)} = g_1g_3(1 + g_4)(1 + g_5) + B, \quad (26h)$$

where

$$B = g_2[(1 + g_1 + g_5)(g_1 + g_3 + g_3g_4) + g_4(1 + g_5)], \quad (27)$$

and  $\beta_6^{(j)}$  with  $j = 11, \dots, 18$  are obtained, respectively, from  $\beta_6^{(k)}$  with  $j = 3, \dots, 10$  by permuting  $g_1$  and  $g_5$ .

$\beta_6^{(1)}$  is a 3-3-3-3-2-setting Bell operator ( $Z_2$  is missing), also  $\beta_6^{(3)}$  ( $X_5$  is missing),  $\beta_6^{(5)}$  ( $Z_2$  is missing),  $\beta_6^{(7)}$  ( $X_5$  is missing), and  $\beta_6^{(9)}$  ( $X_1$  is missing).  $\beta_6^{(2)}$ ,  $\beta_6^{(4)}$ ,

$\beta_6^{(6)}$ ,  $\beta_6^{(8)}$ , and  $\beta_6^{(10)}$  are 3-3-3-3-3-setting Bell operators. Therefore,  $\beta_6^{(i)}$  are 3-3-3-3-2-setting Bell operators if  $i$  is odd, and 3-3-3-3-3-setting Bell operators if  $i$  is even. For graph state no. 6, the quantum expected value of any  $\beta_6^{(i)}$  is 15. Therefore, the degree of nonlocality is  $\mathcal{D}(\beta_6^{(i)}) = 15/7 \approx 2.14$ .

#### 4.7. Graph State No. 7 or Five-Qubit Linear-Cluster State

For the five-qubit linear-cluster state (graph no. 7), the optimal Bell inequality is given by

$$-8 \leq \langle \beta_7 \rangle_{\text{LHV}} \leq 8, \quad (28)$$

where the Bell operator is unique and completely symmetric,

$$\beta_7 = (1 + g_1)[(1 + g_2)g_3(1 + g_4) + g_2g_4](1 + g_5). \quad (29)$$

For graph state no. 7, the quantum expected value of  $\beta_7$  is 20. Therefore, the degree of nonlocality is  $\mathcal{D}(\beta_7) = 5/2 = 2.5$ .

#### 4.8. Graph State No. 8 or Five-Qubit Ring-Cluster State

Let us finally deal with the five-qubit ring-cluster state (graph state no. 8). There are 111 optimal Bell inequalities: six of them are of the type

$$-7 \leq \langle \beta_8^{(i)} \rangle_{\text{LHV}} \leq 9, \quad (30)$$

where there are six possible Bell operators. One of them is completely symmetric,

$$\beta_8^{(1)} = \gamma + \sum_{i=1}^5 g_i g_{i+1}, \quad (31)$$

where the summation indices are taken modulo 5, and

$$\gamma = \frac{1}{2} \left[ \prod_{i=1}^5 (1 + g_i) - \prod_{i=1}^5 (1 - g_i) \right] \quad (32)$$

is the sum of all stabilizing operators which are products of an odd number of generators. The other five Bell operators are

$$\begin{aligned} \beta_8^{(j+1)} &= \gamma + g_j g_{j+1} + g_j g_{j+2} + g_{j-1} g_{j+1} \\ &+ g_{j-2} g_j g_{j+1} g_{j+2} + g_{j-2} g_{j-1} g_j g_{j+1}, \end{aligned} \quad (33)$$

where  $j = 1, \dots, 5$ . In addition, there are 105 optimal Bell inequalities of the type  $-11 \leq \langle \beta_8^{(i)} \rangle_{\text{LHV}} \leq 9$ , where the Bell operators also have 21 terms. For graph state no. 8, the quantum expected value of any  $\beta_8^{(i)}$  is 21.

All optimal Bell inequalities for the correlations of all inequivalent graph states up to five qubits.  $\mathcal{D}$  is the degree of nonlocality.  $\mathcal{O}$  is the minimum number of observers required for a Bell experiment to discard the EPR elements of reality using only the perfect correlations (i.e., the stabilizers) of the corresponding graph state

Graph state no.	$\mathcal{D}$	$\mathcal{O}$	Terms	Settings	(Completely symmetric) inequalities
2 (GHZ <sub>3</sub> , LC <sub>3</sub> , RC <sub>3</sub> , ST <sub>3</sub> , FC <sub>3</sub> )	2	3	4	2-2-2	(1) 1
3 (GHZ <sub>4</sub> , ST <sub>4</sub> , FC <sub>4</sub> )	2	4	4	2-2-2-2	(2) 8
4 (LC <sub>4</sub> , RC <sub>4</sub> )	2	2	4	2-2-2-1	(0) 8
5 (GHZ <sub>5</sub> , ST <sub>5</sub> , FC <sub>5</sub> )	4	5	16	2-2-2-2-2	(1) 1
6 (Y <sub>5</sub> )	15/7 ≈ 2.14	3	15	3-3-3-3-2/3-3-3-3-3	2 (18)/2 (18)
7 (LC <sub>5</sub> )	5/2 = 2.5	3	20	3-3-3-3-3	(1) 1
8 (RC <sub>5</sub> )	7/3 ≈ 2.33	3	21	3-3-3-3-3	(1 + ?) 6 + 105

Therefore, the degree of nonlocality is  $\mathcal{D}(\beta_8^{(i)}) = 21/9 \approx 2.33$ .

## 5. CONCLUSIONS

In Section 3, we have presented a necessary and sufficient condition for the existence of bipartite all-versus-nothing proofs of Bell's theorem with single-qubit measurements, and provided all states, up to  $n = 7$  qubits, and distributions of qubits which allow these proofs. Remarkably, there is only one distribution of a state of  $n = 4$  qubits, and six distributions, each for a different state of  $n = 6$  qubits, which allow these proofs.

In Section 4, we have obtained the optimal Bell inequalities for the perfect correlations of all graph states of less than six qubits. The results are summarized in the table. Our Bell inequalities are useful tools for: (a) the experimental analysis of states which are particularly relevant in many applications of quantum information like quantum error-correction and measurement-based quantum computation, (b) all-versus-nothing refutations of local realism, (c) designing loophole-free Bell experiments, and (d) measuring the degree of nonlocality of different graph states, and, therefore, addressing problems like how nonlocality scales with  $n$  within a family of graph states, or which graph states have more interesting nonlocality vs. decoherence bounds.

## ACKNOWLEDGMENTS

The authors thank H. Briegel for useful discussions. A.C. acknowledges support from the Spanish MEC Project no. FIS2005-07689, and the Junta de Andalucía Excellence Project no. P06-FQM-02243. O.G. acknowledges support from the FWF and the EU (OLAQUI, SCALA, and QICS).

## REFERENCES

1. D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, Ed. by M. Kafatos (Kluwer, Dordrecht, 1989).
2. N. D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
3. J. S. Bell, *Physics* (Long Island City, N.Y.) **1**, 195 (1964).
4. M. Żukowski, *Phys. Lett. A* **157**, 198 (1991).
5. R. K. Clifton, M. L. G. Redhead, and J. N. Butterfield, *Found. Phys.* **21**, 149 (1991).
6. R. Cleve and H. Buhrman, *Phys. Rev. A* **56**, 1201 (1997).
7. M. Żukowski et al., *Acta Phys. Pol. A* **93**, 187 (1998).
8. W. Dür, G. Vidal, and J. I. Cirac, *Phys. Rev. A* **62**, 062314 (2000).
9. A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
10. N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
11. A. Cabello, *Phys. Rev. Lett.* **86**, 1911 (2001).
12. A. Cabello, *Phys. Rev. Lett.* **87**, 010403 (2001).
13. Z.-B. Chen et al., *Phys. Rev. Lett.* **90**, 160408 (2003).
14. C. Cinelli et al., *Phys. Rev. Lett.* **95**, 240405 (2005).
15. T. Yang et al., *Phys. Rev. Lett.* **95**, 240406 (2005).
16. A. I. Lvovsky, *Phys. Rev. Lett.* **88**, 098901 (2002).
17. A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).
18. A. Cabello, *Phys. Rev. A* **72**, 050101 (R) (2005).
19. G. Vallone et al., *Phys. Rev. Lett.* **98**, 180502 (2007).
20. J. T. Barreiro et al., *Phys. Rev. Lett.* **95**, 260501 (2005).
21. Q. Zhang et al., *Nature Phys.* **2**, 678 (2006).
22. C.-Y. Lu et al., *Nature Phys.* **3**, 91 (2007).
23. A. Cabello, *Phys. Rev. A* **73**, 022302 (2006).
24. A. Cabello, *Phys. Rev. Lett.* **97**, 140406 (2006).
25. M. Barbieri et al., *Phys. Rev. Lett.* **97**, 140407 (2006).
26. P. M. Pearle, *Phys. Rev. D* **2**, 1418 (1970).
27. W. Dür and H.J. Briegel, *Phys. Rev. Lett.* **92**, 180403 (2004); C. Simon and J. Kempe, *Phys. Rev. A* **65**, 052327 (2002).
28. Z. Zhao et al., *Nature* (London) **430**, 54 (2004); D. Leibfried et al., *Nature* (London) **438**, 639 (2005); C.-Y. Lu et al., *Nature Phys.* **3**, 91 (2007).



29. M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
30. M. Hein et al., *Quantum Computers, Algorithms, and Chaos*, Ed. by G. Casati et al. (IOS, Amsterdam, 2006).
31. D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
32. R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
33. L.-Y. Hsu, *Phys. Rev. A* **73**, 042308 (2006); J. Barrett et al., *Phys. Rev. A* **75**, 012103 (2007); C. Wu et al., *Phys. Rev. A* **75**, 032332 (2007).
34. O. Gühne et al., *Phys. Rev. Lett.* **95**, 120405 (2005).
35. G. Tóth, O. Gühne, and H.J. Briegel, *Phys. Rev. A* **73**, 022303 (2006).
36. D. P. DiVincenzo and A. Peres, *Phys. Rev. A* **55**, 4089 (1997).
37. V. Scarani et al., *Phys. Rev. A* **71**, 042325 (2005).
38. M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **69**, 022316 (2004).
39. A. Peres, *Phys. Lett. A* **151**, 107 (1990).
40. C. A. Sackett et al., *Nature (London)* **404**, 256 (2000); Z. Zhao et al., *Phys. Rev. Lett.* **91**, 180401 (2003); P. Walther et al., *Nature (London)* **434**, 169 (2005); K. Chen et al., *Phys. Rev. Lett.* **99**, 120503 (2007).
41. N. Kiesel et al., *Phys. Rev. Lett.* **95**, 210502 (2005); P. Walther et al., *Phys. Rev. Lett.* **95**, 020403 (2005); G. Vallone et al., *Phys. Rev. Lett.* **98**, 180502 (2007).
42. M. Ardehali, *Phys. Rev. A* **46**, 5375 (1992).



## Entanglement in eight-qubit graph states

Adán Cabello<sup>a,\*</sup>, Antonio J. López-Tarrida<sup>a</sup>, Pilar Moreno<sup>a</sup>, José R. Portillo<sup>b</sup>

<sup>a</sup> Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain

<sup>b</sup> Departamento de Matemática Aplicada I, Universidad de Sevilla, E-41012 Sevilla, Spain

### ARTICLE INFO

#### Article history:

Received 11 March 2009

Received in revised form 24 April 2009

Accepted 27 April 2009

Available online 6 May 2009

Communicated by P.R. Holland

#### PACS:

03.65.Ud

03.65.Ta

03.67.Mn

42.50.Xa

### ABSTRACT

Any 8-qubit graph state belongs to one of the 101 equivalence classes under local unitary operations within the Clifford group. For each of these classes we obtain a representative which requires the minimum number of controlled-Z gates for its preparation, and calculate the Schmidt measure for the 8-partite split, and the Schmidt ranks for all bipartite splits. This results into an extension to 8 qubits of the classification of graph states proposed by Hein, Eisert, and Briegel [M. Hein, J. Eisert, H.J. Briegel, Phys. Rev. A 69 (2004) 062311].

© 2009 Elsevier B.V. All rights reserved.

### 1. Introduction

Graph states [1,2] are a type of  $n$ -qubit pure states that play several fundamental roles in quantum information theory. In quantum error-correction, the stabilizer codes which protect quantum systems from errors [3] can be realized as graph codes [4,5]. In measurement-based (or one-way) quantum computation [6], graph states are the initial resources consumed during the computation. Moreover, some graph states are universal resources for quantum computation [7]. In quantum simulation, graph states allow us to demonstrate fractional braiding statistics of anyons in an exactly solvable spin model [8]. Graph states have been used in multipartite purification schemes [9]. The Clifford group has been used for entanglement distillation protocols [10]. Graph states naturally lead to Greenberger–Horne–Zeilinger (GHZ) or all-versus-nothing proofs of Bell's theorem [11–16], which can be converted into Bell inequalities which are maximally violated by graph states [17–22]. Some specific graph states are essential for several quantum communication protocols, including entanglement-based quantum key distribution [23], teleportation [24], reduction of communication complexity [25], and secret sharing [26,27].

In addition to all these applications, graph states also play a fundamental role in the theory of entanglement. For  $n \geq 4$  qubits, there is an infinite amount of different, inequivalent classes of  $n$ -qubit pure entangled states. The graph state formalism is a use-

ful abstraction which permits a detailed (although not exhaustive) classification of  $n$ -qubit entanglement of  $n \geq 4$  qubits.

For all these reasons, a significant experimental effort is devoted to the creation and testing of graph states of an increasing number of qubits. On one hand, there are experiments of  $n$ -qubit  $n$ -photon graph states up to  $n = 6$  [28–32]. On the other hand, the combination of two techniques, hyper-entanglement (i.e., entanglement in several degrees of freedom, like polarization and linear momentum) [33–39] and the sources of 4, 5, and 6-photon entanglement using parametric down-conversion [29,40–45] allows us to create 6-qubit 4-photon graph states [46,47], 8-qubit 4-photon graph states [46], and even 10-qubit 5-photon graph states [46]. The use of 4-photon sources for preparing 8-qubit graph states is particularly suitable due to the high visibility of the resulting states.

The classification and study of the entanglement properties of graph states have been achieved, up to 7 qubits, by Hein, Eisert, and Briegel (HEB) in [1] (see also [2]). This classification has been useful to identify new two-observer all-versus-nothing proofs [16], new Bell inequalities [21,22], and has stimulated the preparation of several graph states [46]. The main purpose of this Letter is to extend the classification in [1,2] to 8-qubit graph states.

Up to 7 qubits, there are 45 classes of graph states that are not equivalent under one-qubit unitary transformations. With 8 qubits, there are 101 new classes. All these classes have been obtained by various researchers (see, e.g., [48]). The purpose here is to classify them according to several relevant physical properties for quantum information theory.

The Letter is organized as follows. In Section 2 we define qubit graph states and local complementation, which is the main clas-

\* Corresponding author.

E-mail address: adan@us.es (A. Cabello).

sifying tool. To establish an order between the equivalence classes we will use the criteria proposed in [1,2]. These criteria are introduced in Section 3. In Section 4 we present our results. In Section 5 we present the conclusions and point out some pending problems.

## 2. Basic concepts

### 2.1. Graph state

A  $n$ -qubit graph state  $|G\rangle$  is a pure state associated to a graph  $G = (V, E)$  consisting of a set  $V$  of  $n$  vertices and a set  $E$  of edges connecting some of the vertices. Each vertex represents a qubit. The graph  $G$  provides both a recipe for preparing  $|G\rangle$  and a mathematical characterization of  $|G\rangle$ .

The recipe for preparing the state is the following. First, prepare each qubit in the state  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ . Then, for each edge connecting two qubits,  $i$  and  $j$ , apply the controlled- $Z$  gate between qubits  $i$  and  $j$ , i.e., the unitary transformation  $C_Z = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$ .

The mathematical characterization of  $|G\rangle$  is the following. The graph state  $|G\rangle$  associated to the graph  $G$  is the only  $n$ -qubit state which fulfills

$$g_i |G\rangle = |G\rangle, \quad \text{for } i = 1, \dots, n, \quad (1)$$

where  $g_i$  are the generators of the stabilizer group of the state, defined as the set  $\{s_j\}_{j=1}^n$  of all products of the generators. Specifically,  $g_i$  is the generator operator associated to the vertex  $i$ , defined by

$$g_i := X^{(i)} \bigotimes_{j \in \mathcal{N}(i)} Z^{(j)}, \quad (2)$$

where  $\mathcal{N}(i)$  is the neighborhood of the vertex  $i$ , i.e., those vertices which are connected to  $i$ , and  $X^{(i)}$  ( $Z^{(i)}$ ) denotes the Pauli matrix  $\sigma_x$  ( $\sigma_z$ ) acting on the  $i$ th qubit.

### 2.2. Local complementation

For our purposes, the key point is that *local complementation* (LC) is a simple transformation which leaves the entanglement properties invariant.

Two  $n$ -qubit states,  $|\phi\rangle$  and  $|\psi\rangle$  have the same  $n$ -partite entanglement if and only if there are  $n$  one-qubit unitary transformations  $U_i$ , such that  $|\phi\rangle = \bigotimes_{i=1}^n U_i |\psi\rangle$ . If these one-qubit unitary transformations belong to the Clifford group, then both states are said to be local Clifford equivalent. The one-qubit Clifford group is generated by the Hadamard gate  $H = (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)/\sqrt{2}$  and the phase gate  $P = |0\rangle\langle 0| + i|1\rangle\langle 1|$ .

Van den Nest, Dehaene, and De Moor found that the successive application of a transformation with a simple graphical description is sufficient to generate the complete equivalence class of graph states under local unitary operations within the Clifford group (hereafter simply referred as class or orbit) [49]. This simple transformation is LC.

On the stabilizer, LC on the qubit  $i$  induces the map  $Y^{(i)} \mapsto Z^{(i)}$ ,  $Z^{(i)} \mapsto -Y^{(i)}$  on the qubit  $i$ , and the map  $X^{(j)} \mapsto -Y^{(j)}$ ,  $Y^{(j)} \mapsto X^{(j)}$  on the qubits  $j \in \mathcal{N}(i)$  [2]. On the generators, LC on the qubit  $i$  maps the generators  $g_j^{\text{old}}$  with  $j \in \mathcal{N}(i)$  to  $g_j^{\text{new}} g_i^{\text{new}}$ .

Graphically, LC on the qubit  $i$  acts as follows: One picks out the vertex  $i$  and inverts the neighborhood  $\mathcal{N}(i)$  of  $i$ ; i.e., vertices in the neighborhood which were connected become disconnected and vice versa.

It has been shown by Van den Nest, Dehaene, and De Moor that for a particular class of qubit graph states local unitary equivalence implies local Clifford equivalence [50]. Moreover, numerical results show that local Clifford equivalence coincides with local unitary equivalence for qubit graph states associated with connected

graphs up to  $n = 7$  vertices [1,2]. It should be noted, however, that not all local unitary transformations between graph states can be represented as successive LCs. A counterexample with  $n = 27$  is described in [51].

Using LC, one can generate the orbits of all LC-inequivalent  $n$ -qubit graph states. For a small  $n$ , the number of orbits has been well known for a long time (see, e.g., [48]). Specifically, for  $n = 8$ , there are 101 LC-inequivalent classes.

## 3. Criteria for the classification

Following HEB, the criteria for ordering the classes are: (a) number of qubits, (b) minimum number of controlled- $Z$  gates needed for the preparation, (c) the Schmidt measure, and (d) the rank indexes. For instance, class No. 1 is the only one containing two-qubit graph states, class No. 2 is the only one containing three-qubit graph states [1,2]. Classes No. 3 and No. 4 both have  $n = 4$  qubits and require a minimum of  $|E| = 3$  controlled- $Z$  gates. However, class No. 3 has Schmidt measure  $E_S = 1$ , while class No. 4 has  $E_S = 2$ .

### 3.1. Minimum number of controlled- $Z$ gates for the preparation

Different members of the same LC class require a different number of controlled- $Z$  gates for their preparation starting from the state  $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$  for each qubit. The first criterion for our classification is the minimum number of controlled- $Z$  gates required for preparing one graph state *within the LC class*. This corresponds to the number of edges of the graph with the minimum number of edges within the LC class,  $|E|$ . We will provide a representative with the minimum number of edges for each LC class.

### 3.2. Schmidt measure

The *Schmidt measure* was introduced by Eisert and Briegel as a tool for quantifying the genuine multipartite entanglement of quantum systems [52] (see also [53]). Any state vector  $|\psi\rangle \in \mathcal{H}^{(1)} \otimes \dots \otimes \mathcal{H}^{(N)}$  of a composite quantum system with  $N$  components can be represented as

$$|\psi\rangle = \sum_{i=1}^R \xi_i |\psi_i^{(1)}\rangle \otimes \dots \otimes |\psi_i^{(N)}\rangle, \quad (3)$$

where  $\xi_i \in \mathbb{C}$  for  $i = 1, \dots, R$ , and  $|\psi_i^{(j)}\rangle \in \mathcal{H}^{(j)}$ , for  $j = 1, \dots, N$ . The Schmidt measure associated with a state vector  $|\psi\rangle$  is then defined as

$$E_S(|\psi\rangle) = \log_2(r), \quad (4)$$

where  $r$  is the minimal number  $R$  of terms in the sum of Eq. (3) over all linear decompositions into product states. In case of a two-component system ( $N = 2$ ), the minimal number of product terms  $r$  is given by the *Schmidt rank* of the state  $|\psi\rangle$ . Hence, the Schmidt measure could be considered a generalization of the Schmidt rank to multipartite quantum systems [see Eq. (9) below]. The Schmidt measure can be extended to mixed states by means of a convex roof extension. In this Letter, however, we will deal only with pure states.

Given a graph  $G = (V, E)$ , a *partition* of  $V$  is any tuple  $(A_1, \dots, A_M)$  of disjoint subsets  $A_i \subset V$ , with  $\bigcup_{i=1}^M A_i = V$ . In case  $M = 2$ , we refer to the partition as a *bipartition*, and denote it  $(A, B)$ . We will write

$$(A_1, \dots, A_N) \leq (B_1, \dots, B_M), \quad (5)$$

if  $(A_1, \dots, A_N)$  is a *finer partition* than  $(B_1, \dots, B_M)$ , which means that every  $A_i$  is contained in some  $B_j$ . The latter is then a *coarser*

partition than the former. For any graph  $G = (V, E)$ , the partitioning where  $(A_1, \dots, A_M) = V$  such that  $|A_i| = 1$ , for every  $i = 1, \dots, M$ , is referred to as the *finest partition*.

We must point out that  $E_S$  is nonincreasing under a coarse graining of the partitioning: If two components are merged in order to form a new component, then the Schmidt measure can only decrease. If we denote the Schmidt measure of a state vector  $|\psi\rangle$  evaluated with respect to a partitioning  $(A_1, \dots, A_N)$  as  $E_S^{(A_1, \dots, A_N)}(|\psi\rangle)$ , meaning that the respective Hilbert spaces are those of the grains of the partitioning, then the nonincreasing property of  $E_S$  can be expressed as

$$E_S^{(A_1, \dots, A_N)}(|\psi\rangle) \geq E_S^{(B_1, \dots, B_M)}(|\psi\rangle), \quad (6)$$

if  $(A_1, \dots, A_N) \leq (B_1, \dots, B_M)$ .

Let  $(A, B)$  be a bipartition (i.e.,  $A \cup B = V$ ;  $A \cap B = \emptyset$ ) of a graph  $G = (V, E)$ , with  $V = \{1, \dots, N\}$ , and let us denote the adjacency matrix of the graph by  $\Gamma$ , i.e., the symmetric matrix with elements

$$\Gamma_{ij} = \begin{cases} 1, & \text{if } (i, j) \in E, \\ 0, & \text{otherwise.} \end{cases} \quad (7)$$

When we are dealing with a bipartition, it is useful to label the vertices of the graph so that  $A = \{1, \dots, p\}$ ,  $B = \{p + 1, \dots, N\}$ . Then, we can decompose the adjacency matrix  $\Gamma$  into submatrices  $\Gamma_A$ ,  $\Gamma_B$  (that represent edges within  $A$  and edges within  $B$ ), and  $\Gamma_{AB}$  (the  $|A| \times |B|$  off-diagonal submatrix of the adjacency matrix  $\Gamma$  that represents those edges between  $A$  and  $B$ ),

$$\begin{pmatrix} \Gamma_A & \Gamma_{AB} \\ \Gamma_{AB}^T & \Gamma_B \end{pmatrix} = \Gamma. \quad (8)$$

The Schmidt rank  $SR_A(G)$  of a graph state  $|G\rangle$  represented by the graph  $G = (V, E)$ , with respect to the bipartition  $(A, B)$ , is given by the binary rank [i.e., the rank over  $GF(2)$ ] of the submatrix  $\Gamma_{AB}$ ,

$$SR_A(G) = \text{rank}_{\mathcal{F}_2}(\Gamma_{AB}). \quad (9)$$

It follows straightforwardly from the definition that  $SR_A(G) = SR_B(G)$ , because the different bipartitions are fixed by choosing the smaller part, say  $A$ , of the bipartition  $(A, B)$ , which gives  $2^{N-1}$  bipartitions.

### 3.3. Rank indexes

While calculating the Schmidt rank with respect to all possible bipartitions of a given graph, let us count how many times a certain rank occurs in all the bipartite splits, and then classify this information according to the number of vertices in  $A$ , the smaller part of the split under consideration. There is a compact way to express this information, the so-called *rank indexes* [1,2]. The rank index for all the bipartite splits with  $p$  vertices in the smaller part  $A$  is given by the  $p$ -tuple

$$RI_p = (v_p^p, \dots, v_1^p) = [v_j^p]_{j=p}^1, \quad (10)$$

where  $v_j^p$  is the number of times in which  $SR_A(G) = j$ , with  $|A| = p$ , occurs.

## 4. Procedures and results

The main results of the Letter are summarized in Fig. 2 and Table 1. In the following, we provide details on the calculations leading to these results.

### 4.1. Orbits under local complementation

We have generated all LC orbits for  $n = 8$  and calculated the number of non-isomorphic graphs in each LC orbit, denoted by  $|LC|$ . These numbers are counted up to isomorphism.

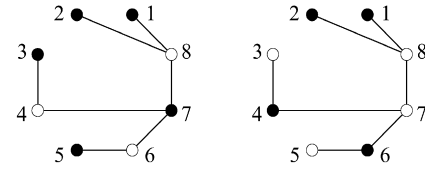


Fig. 1. The set of vertices 4, 6, and 8 is the minimal vertex cover of the graph (left). The set of vertices 3, 5, 7, and 8, is a vertex cover of the graph, but is not minimal, it has size 4 (right).

In addition, for each orbit, we have calculated a representative with the minimum number of edges  $|E|$ . As representative, we have chosen the one (or one of those) with the minimum number of edges and the minimum maximum degree (i.e., number of edges incident with a vertex). This means that the graph state associated to this graph requires the minimum number of controlled-Z gates for its preparation, and the minimum preparation depth (i.e., its preparation requires a minimum number of steps) [54]. All the representatives of each of the 101 orbits are illustrated in Fig. 2.  $|LC|$  and  $|E|$  are in Table 1.

### 4.2. Bounds to the Schmidt measure

It is a well-known fact that for any measure of multiparticle entanglement proposed so far, including the Schmidt measure  $E_S$ , the computation is exceedingly difficult for general states. In order to determine  $E_S$ , one has to show that a given decomposition in Eq. (3) with  $R$  terms is minimal. For a general state, the minimization problem involved can be a very difficult problem of numerical analysis, which scales exponentially in the number of parties  $N$  as well as in the degree of entanglement of the state itself. Nevertheless, this task becomes feasible if we restrict our attention to graph states. HEB established several upper and lower bounds for the Schmidt measure in graph theoretical terms [1,2]. These bounds make possible to determine the Schmidt measure for a large number of graphs of practical importance, because in many cases the bounds proposed are easily computable and, remarkably, the upper and lower bounds frequently coincide.

#### 4.2.1. Pauli persistency and size of the minimal vertex cover

For any graph state  $|G\rangle$ , upper bounds for its Schmidt measure  $E_S(|G\rangle)$  are the *Pauli persistency*  $PP(G)$  and the *size of the minimal vertex cover*  $VC(G)$ ,

$$E_S(|G\rangle) \leq PP(G) \leq VC(G). \quad (11)$$

The Pauli persistency is the minimal number of local Pauli measurements necessary to disentangle a graph state. Concerning this question, HEB described graphical transformation rules when local Pauli measurements are applied [1,2].

A vertex cover is a concept from graph theory: It is any subset  $V' \subseteq V$  of vertices in a graph  $G$  to which any edge of  $G$  is incident (see Fig. 1). Therefore, the minimal vertex cover of a graph is the smallest one, whose size is denoted by  $VC(G)$ . According to the graphical rules for the Pauli measurements, since each  $\sigma_z$  measurement simply deletes all edges incident to a vertex, the size of the minimal vertex cover would equal the Pauli persistency, provided that we restrict the Pauli measurements to  $\sigma_z$  measurements. Nevertheless, in graphs with many edges, i.e., very connected, a proper combination of  $\sigma_x$ ,  $\sigma_y$ , and  $\sigma_z$  measurements could provide a more efficient disentangling sequence, giving a better upper bound  $PP(G)$  for the Schmidt measure. See [1,2] for details.

#### 4.2.2. Maximal Schmidt rank

For any graph state  $|G\rangle$ , a lower bound for the Schmidt measure  $E_S(|G\rangle)$  is the *maximal Schmidt rank*,

$$SR_{\max}(G) \leq E_S(|G\rangle). \quad (12)$$

While calculating the Schmidt rank with respect to all possible bipartitions of a given graph  $G = (V, E)$ , if one maximizes the Schmidt rank over all bipartitions  $(A, B)$  of the graph, and takes into account the nonincreasing property of  $E_S(|G\rangle)$  [see Eq. (6)], then one obtains a lower bound for the Schmidt measure with respect to the finest partitioning. This lower bound is the maximal Schmidt rank,

$$SR_{\max}(G) := \max_{A \subseteq V} SR_A(G). \quad (13)$$

According to the definition of Schmidt rank, the maximal Schmidt rank for any state is, at most,  $\lfloor \frac{N}{2} \rfloor$ , i.e., the largest integer less than or equal to  $\frac{N}{2}$ .

#### 4.2.3. Addition and deletion of edges and vertices

As we mentioned in Section 2.2, applying the LC-rule does not change the Schmidt measure  $E_S$ . It is interesting to remark that other local changes to the graph, such as the deletion of edges or vertices, have only a limited effect on  $E_S$ . This fact is established by HEB [1] in what they call the *edge/vertex rule*: On one hand, by deleting (or adding) an edge  $e$  between two vertices of a graph  $G$  the Schmidt measure of the resulting graph  $G' = G \pm e$  can at most decrease (or increase) by 1. On the other hand, if a vertex  $v$  (including all its incident edges) is deleted, the Schmidt measure of the resulting graph  $G' = G - v$  cannot increase, and will at most decrease by one. If  $E_S(|G + e\rangle)$  denotes the Schmidt measure of the graph state corresponding to the graph  $G + e$ , then the previous rules can be summarized as

$$E_S(|G + e\rangle) \leq E_S(|G\rangle) + 1, \quad (14a)$$

$$E_S(|G - e\rangle) \geq E_S(|G\rangle) - 1, \quad (14b)$$

$$E_S(|G - v\rangle) \geq E_S(|G\rangle) - 1. \quad (14c)$$

We have used these rules in two ways: Firstly, as an internal test to check our calculations, comparing pairs of graphs connected by a sequence of addition or deletion of edges/vertices; and secondly, as a useful tool that, in some graphs, has enabled us to go from a bounded to a determined value for the Schmidt measure, once again by comparison between a problematic graph  $G$  and a resulting graph  $G'$  (typically obtained by edge or vertex deletion) of a known Schmidt measure.

#### 4.2.4. Schmidt measure in some special types of graphs

There are some special types of graph states in which lower and upper bounds for the Schmidt measure coincide (see [1]), giving directly a determined value for  $E_S$ . Since the maximal Schmidt rank for any state can be at most  $\lfloor \frac{N}{2} \rfloor$ , and restricting ourselves to states with coincident upper and lower bounds to  $E_S$ , it is true that  $SR_{\max}(G) = E_S(|G\rangle) = PP(G) = VC(G) \leq \lfloor \frac{N}{2} \rfloor$ . This is the case for GHZ states, and states represented by trees, rings with an even number of vertices, and clusters. In our work we have used the following results concerning GHZ states and trees:

- (a) The Schmidt measure for any multipartite GHZ state is 1.
- (b) A *tree*  $T$  is a graph that has no cycles. The Schmidt measure of the corresponding graph state  $|T\rangle$  is the size of its minimal vertex cover:  $E_S(|T\rangle) = VC(T)$ .

There is another interesting kind of graphs for our purposes, the so-called *2-colorable graphs*. A graph is said to be 2-colorable when it is possible to perform a *proper 2-coloring* on it: This is a labeling  $V \rightarrow \{1, 2\}$ , such that all connected vertices are associated with a different element from  $\{1, 2\}$ , which can be identified with two colors. It is a well-known fact in graph theory that a necessary and sufficient criterion for a graph to be 2-colorable is that it does not contain any cycles of odd length. Mathematicians call these graphs

*bipartite graphs* due to the fact that the whole set of vertices can be distributed into two disjoint subsets  $A$  and  $B$ , such that no two vertices within the same subset are connected, and therefore every edge connects a vertex in  $A$  with a vertex in  $B$ .

HEB [1] provided lower and upper bounds for the Schmidt measure that could be applied to graph states represented by 2-colorable graphs:

$$\frac{1}{2} \text{rank}_{\mathcal{F}_2}(\Gamma) \leq E_S(|G\rangle) \leq \left\lfloor \frac{|V|}{2} \right\rfloor, \quad (15)$$

where  $\Gamma$  is the adjacency matrix of the 2-colorable graph. If  $\Gamma$  is invertible, then

$$E_S(|G\rangle) = \left\lfloor \frac{|V|}{2} \right\rfloor. \quad (16)$$

Besides, HEB pointed out that any graph  $G$  which is not 2-colorable can be turned into a 2-colorable one  $G'$  by simply deleting the appropriate vertices on cycles with odd length present in  $G$ . The identification of this graphical action with the effect of a  $\sigma_z$  measurement on qubits corresponding to such vertices yields new upper bounds for  $E_S(|G\rangle)$ :

$$E_S(|G\rangle) \leq E_S(|G'\rangle) + M \leq \left\lfloor \frac{|V - M|}{2} \right\rfloor + M \leq \left\lfloor \frac{|V| + M}{2} \right\rfloor, \quad (17)$$

where  $M$  is the number of removed vertices. We have used these new bounds in some graphs as a tool to check our calculations.

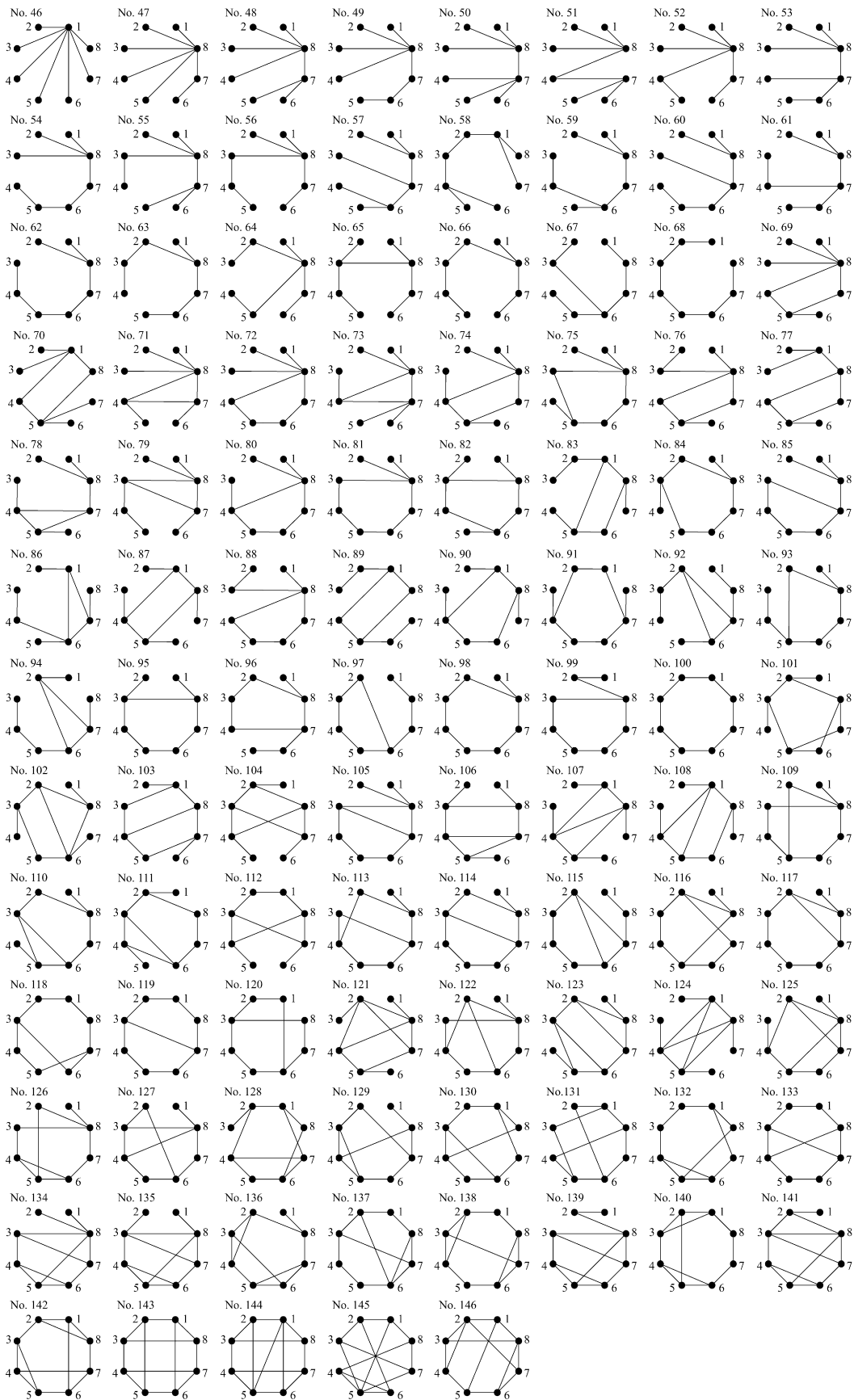
## 5. Conclusions, open problems, and future developments

To sum it all up, we have extended to 8 qubits the classification of the entanglement of graph states proposed in [1] for  $n < 8$  qubits. Notice that for  $n = 8$  we have 101 classes, while for  $n < 8$  there are only 45 classes. For each of these classes we obtain a representative which requires the minimum controlled-Z gates for its preparation (see Fig. 2), and calculate the Schmidt measure for the 8-partite split (which measures the genuine 8-party entanglement of the class), and the Schmidt ranks for all bipartite splits (see Table 1).

This classification will help us to obtain new all-versus-nothing proofs of Bell's theorem [16] and new Bell inequalities. Specifically, any 8-qubit graph state belonging to a class with a representative with 7 edges (i.e., a tree) has a specific type of Bell inequality [22]. More generally, it will help us to investigate the nonlocality (i.e., the non-simulability of the predictions of quantum mechanics by means of non-local hidden variable models) of graph states [21].

Extending the classification in [1] a further step sheds some light on the limitations of the method of classification. The criteria used in [1] to order the classes (see Section 3) already failed to distinguish all classes in  $n = 7$ . For instance, classes No. 40, No. 42, and No. 43 in [1,2] have the same number of qubits, require the same minimum number of controlled-Z gates for the preparation, and have the same Schmidt measure and rank indexes. The same problem occurs between classes No. 110 and No. 111, between classes No. 113 and No. 114, and between classes No. 116 and No. 117 in our classification (see Table 1). Following [1,2], we have placed the class with lower  $|LC|$  in the first place. However, this solution is not satisfactory, since  $|LC|$  is not related to the entanglement properties of the class. On the other hand, Van den Nest, Dehaene, and De Moor have proposed a finite set of invariants that characterizes all classes [55]. However, this set has more than  $2 \times 10^{36}$  invariants already for  $n = 7$ . The problem of obtaining a minimum set of invariants capable of distinguishing all classes with  $n \leq 8$  qubits will be addressed elsewhere [56].

Another weak point in the method is that the precise value of  $E_S$  is still unknown for some classes. The good news is that, for most of these classes, the value might be fixed if we knew the



**Fig. 2.** Graphs associated to the 101 classes on 8-qubit graph states inequivalent under local complementation and graph isomorphism. We have chosen as representative of the class the one (or one of those) with minimum number of edges and minimum maximum degree (i.e., number of edges incident with a vertex), which means that it requires the minimum number of controlled-Z gates in the preparation and minimum preparation depth.

**Table 1**  
Entanglement of the 101 classes of 8-qubit graph states. No. is the number of the class; it is assigned attending to  $|E|$ ,  $E_S$ , and  $RI_j$ ; the numbering starts at the point in which the one in Refs. [1,2] ends.  $|LC|$  is the number of nonisomorphic elements of the class.  $|E|$  is the number of edges of those representatives with the minimum number of edges.  $E_S$  is the Schmidt measure (or its lower and upper bounds).  $RI_j$  is the rank index with  $j$  qubits in the smaller bipartition (i.e., the number of bipartite splits in which a certain rank occurs; ranks appear in decreasing order from left to right). 2-col indicates whether or not a 2-colorable representative exists.

No.	$ LC $	$ E $	$E_S$	$RI_4$	$RI_3$	$RI_2$	2-col	No.	$ LC $	$ E $	$E_S$	$RI_4$	$RI_3$	$RI_2$	2-col
46	2	7	1	(0,0,0,35)	(0,0,56)	(0,28)	yes	97	154	8	4	(8,22,4,1)	(42,13,1)	(27,1)	no
47	6	7	2	(0,0,20,15)	(0,30,26)	(12,16)	yes	98	542	8	4	(8,22,5,0)	(42,14,0)	(27,1)	no
48	6	7	2	(0,0,30,5)	(0,45,11)	(15,13)	yes	99	300	8	4	(12,16,7,0)	(44,11,1)	(27,1)	yes
49	16	7	2	(0,0,30,5)	(0,45,11)	(17,11)	yes	100	214	8	4	(14,17,4,0)	(48,8,0)	(28,0)	yes
50	4	7	2	(0,0,34,1)	(0,48,8)	(16,12)	yes	101	14	9	3	(0,20,15,0)	(24,32,0)	(25,3)	no
51	16	7	2	(0,0,34,1)	(0,51,5)	(19,9)	yes	102	66	9	3	(0,28,7,0)	(32,24,0)	(25,3)	no
52	10	7	3	(0,12,16,7)	(16,28,12)	(20,8)	yes	103	66	9	3	(0,30,5,0)	(36,20,0)	(26,2)	yes
53	16	7	3	(0,12,22,1)	(16,34,6)	(20,8)	yes	104	6	9	3	(0,32,0,3)	(32,24,0)	(24,4)	yes
54	44	7	3	(0,12,22,1)	(16,35,5)	(21,7)	yes	105	57	9	3 < 4	(0,30,5,0)	(36,19,1)	(25,3)	no
55	16	7	3	(0,18,14,3)	(18,33,5)	(21,7)	yes	106	28	9	4	(8,18,9,0)	(38,18,0)	(25,3)	no
56	44	7	3	(0,18,14,3)	(22,29,5)	(23,5)	yes	107	17	9	4	(8,20,6,1)	(32,24,0)	(24,4)	no
57	10	7	3	(0,18,15,2)	(18,36,2)	(21,7)	yes	108	72	9	4	(8,20,7,0)	(36,20,0)	(25,3)	no
58	25	7	3	(0,18,16,1)	(18,36,2)	(22,6)	yes	109	87	9	4	(8,20,7,0)	(40,16,0)	(27,1)	no
59	44	7	3	(0,18,16,1)	(22,31,3)	(23,5)	yes	110	114	9	4	(8,22,5,0)	(40,16,0)	(26,2)	no
60	44	7	3	(0,24,9,2)	(24,30,2)	(23,5)	yes	111	372	9	4	(8,22,5,0)	(40,16,0)	(26,2)	no
61	26	7	3	(0,24,10,1)	(28,25,3)	(23,5)	yes	112	70	9	4	(8,24,2,1)	(40,16,0)	(26,2)	no
62	120	7	3	(0,24,10,1)	(28,26,2)	(24,4)	yes	113	264	9	4	(8,24,3,0)	(44,12,0)	(27,1)	no
63	66	7	3	(0,26,7,2)	(30,24,2)	(25,3)	yes	114	542	9	4	(8,24,3,0)	(44,12,0)	(27,1)	no
64	14	7	4	(8,12,12,3)	(32,18,6)	(24,4)	yes	115	156	9	4	(12,18,5,0)	(46,9,1)	(27,1)	no
65	25	7	4	(8,12,14,1)	(32,20,4)	(24,4)	yes	116	174	9	4	(12,20,3,0)	(46,10,0)	(27,1)	no
66	120	7	4	(8,14,12,1)	(34,19,3)	(25,3)	yes	117	542	9	4	(12,20,3,0)	(46,10,0)	(27,1)	no
67	72	7	4	(8,16,10,1)	(36,17,3)	(25,3)	yes	118	262	9	4	(12,20,3,0)	(48,8,0)	(28,0)	no
68	172	7	4	(8,18,8,1)	(38,16,2)	(26,2)	yes	119	802	9	4	(14,19,2,0)	(50,6,0)	(28,0)	no
69	10	8	2	(0,0,34,1)	(0,52,4)	(20,8)	yes	120	117	9	4	(16,16,3,0)	(50,6,0)	(28,0)	yes
70	10	8	2	(0,0,35,0)	(0,54,2)	(21,7)	yes	121	10	10	3	(0,32,2,1)	(32,24,0)	(24,4)	no
71	10	8	3	(0,12,22,1)	(16,36,4)	(20,8)	no	122	37	10	3	(0,32,3,0)	(40,16,0)	(27,1)	yes
72	21	8	3	(0,12,22,1)	(16,36,4)	(22,6)	no	123	36	10	4	(8,22,5,0)	(44,12,0)	(26,2)	no
73	10	8	3	(0,18,17,0)	(18,36,2)	(21,7)	no	124	7	10	4	(8,24,0,3)	(32,24,0)	(24,4)	no
74	44	8	3	(0,18,17,0)	(22,32,2)	(23,5)	yes	125	103	10	4	(8,24,3,0)	(42,14,0)	(26,2)	no
75	66	8	3	(0,18,17,0)	(22,33,1)	(24,4)	no	126	46	10	4	(8,24,3,0)	(44,12,0)	(27,1)	no
76	26	8	3	(0,20,14,1)	(24,30,2)	(24,4)	yes	127	170	10	4	(8,26,1,0)	(46,10,0)	(27,1)	no
77	26	8	3	(0,24,10,1)	(24,31,1)	(23,5)	yes	128	74	10	4	(12,20,3,0)	(46,10,0)	(27,1)	yes
78	28	8	3	(0,24,10,1)	(28,27,1)	(23,5)	no	129	340	10	4	(12,22,1,0)	(48,8,0)	(27,1)	no
79	44	8	3	(0,24,11,0)	(28,26,2)	(23,5)	no	130	254	10	4	(12,22,1,0)	(50,6,0)	(28,0)	no
80	132	8	3	(0,24,11,0)	(28,27,1)	(24,4)	no	131	433	10	4	(14,21,0,0)	(52,4,0)	(28,0)	no
81	114	8	3	(0,24,11,0)	(30,25,1)	(25,3)	yes	132	476	10	4	(16,18,1,0)	(52,4,0)	(28,0)	no
82	72	8	3	(0,26,9,0)	(30,26,0)	(25,3)	no	133	28	10	4 < 5	(12,22,0,1)	(48,8,0)	(28,0)	no
83	72	8	3	(0,28,6,1)	(32,23,1)	(25,3)	yes	134	9	11	3 < 4	(0,30,5,0)	(40,15,1)	(25,3)	no
84	198	8	3	(0,28,7,0)	(34,22,0)	(26,2)	yes	135	39	11	4	(8,26,1,0)	(44,12,0)	(26,2)	no
85	56	8	3 < 4	(0,30,4,1)	(34,21,1)	(25,3)	no	136	46	11	4	(12,20,3,0)	(50,6,0)	(27,1)	no
86	28	8	4	(8,16,10,1)	(32,22,2)	(24,4)	no	137	208	11	4 < 5	(16,18,1,0)	(52,4,0)	(28,0)	no
87	10	8	4	(8,16,10,1)	(32,24,0)	(24,4)	yes	138	298	11	4 < 5	(18,17,0,0)	(54,2,0)	(28,0)	no
88	56	8	4	(8,16,10,1)	(36,18,2)	(26,2)	no	139	24	11	4 < 5	(20,10,5,0)	(50,5,1)	(27,1)	no
89	66	8	4	(8,16,11,0)	(36,18,2)	(25,3)	yes	140	267	11	4 < 5	(20,14,1,0)	(54,2,0)	(28,0)	no
90	72	8	4	(8,18,9,0)	(34,22,0)	(25,3)	no	141	4	12	4	(28,0,7,0)	(56,0,0)	(28,0)	no
91	63	8	4	(8,18,9,0)	(36,20,0)	(26,2)	yes	142	22	12	4 < 5	(14,21,0,0)	(56,0,0)	(28,0)	no
92	66	8	4	(8,18,9,0)	(38,16,2)	(25,3)	no	143	46	12	4	(20,12,3,0)	(50,6,0)	(27,1)	yes
93	176	8	4	(8,18,9,0)	(38,17,1)	(26,2)	no	144	28	13	4	(28,4,3,0)	(56,0,0)	(28,0)	no
94	76	8	4	(8,20,6,1)	(36,19,1)	(25,3)	no	145	7	13	4 < 5	(16,18,1,0)	(56,0,0)	(28,0)	no
95	194	8	4	(8,20,7,0)	(38,18,0)	(26,2)	yes	146	51	13	4 < 5	(24,10,1,0)	(56,0,0)	(28,0)	no
96	352	8	4	(8,20,7,0)	(40,15,1)	(26,2)	no								

value for the 5-qubit ring cluster state, which is the first graph state in the classification for which the value of  $E_S$  is unknown [1,2]. Unfortunately, we have not made any progress in calculating  $E_S$  for the 5-qubit ring cluster state.

Table 1 shows that there are no 8-qubit graph states with rank indexes  $RI_p = [v_j^p]_{j=p}^1$  with  $v_j^p \neq 0$  if  $j = p$ , and  $v_j^p = 0$  if  $j < p$ , i.e., with maximal rank with respect to all bipartite splits, i.e., such that entanglement is symmetrically distributed between all parties. These states are robust against disentanglement by a few measurements. Neither there are 7-qubit graph states with this property [1,2]. This makes more interesting the fact that there is a single 5-qubit and a single 6-qubit graph state with this property [1,2].

**Acknowledgements**

The authors thank H.J. Briegel, O. Gühne, M. Grassl, M. Hein, C. Santana, and M. Van den Nest, for their help. This work has

benefited from the use of the program *nauty* [57] for computing automorphism groups of graphs. A.C., A.J.L., and P.M. acknowledge support from projects No. P06-FQM-02243, No. FIS2008-05596, and No. PAI-FQM-0239. J.R.P. acknowledges support from projects No. P06-FQM-01649, No. MTM2008-05866-C03-01, and No. PAI-FQM-0164.

**References**

- [1] M. Hein, J. Eisert, H.J. Briegel, Phys. Rev. A 69 (2004) 062311.
- [2] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, H.J. Briegel, in: G. Casati, D.L. Shepelyansky, P. Zoller, G. Benenti (Eds.), Quantum Computers, Algorithms and Chaos, IOS Press, Amsterdam, 2006.
- [3] D. Gottesman, Phys. Rev. A 54 (1996) 1862.
- [4] D. Schlingemann, R.F. Werner, Phys. Rev. A 65 (2002) 012308.
- [5] D. Schlingemann, Quantum Inf. Comput. 2 (2002) 307.
- [6] R. Raussendorf, H.J. Briegel, Phys. Rev. Lett. 86 (2001) 5188.
- [7] M. van den Nest, A. Miyake, W. Dür, H.J. Briegel, Phys. Rev. Lett. 97 (2006) 150504.

- [8] Y.-J. Han, R. Raussendorf, L.-M. Duan, Phys. Rev. Lett. 98 (2007) 150404.
- [9] W. Dür, H. Aschauer, H.-J. Briegel, Phys. Rev. Lett. 91 (2003) 107903.
- [10] J. Dehaene, M. Van den Nest, B. De Moor, F. Verstraete, Phys. Rev. A 67 (2003) 022310.
- [11] D.M. Greenberger, M.A. Horne, A. Zeilinger, in: M. Kafatos (Ed.), Bell's Theorem, Quantum Theory, and Conceptions of the Universe, Kluwer Academic, Dordrecht, 1989, p. 69.
- [12] D.P. DiVincenzo, A. Peres, Phys. Rev. A 55 (1997) 4089.
- [13] V. Scarani, A. Acín, E. Schenck, M. Aspelmeyer, Phys. Rev. A 71 (2005) 042325.
- [14] O. Gühne, G. Tóth, P. Hyllus, H.J. Briegel, Phys. Rev. Lett. 95 (2005) 120405.
- [15] A. Cabello, Phys. Rev. Lett. 95 (2005) 210401.
- [16] A. Cabello, P. Moreno, Phys. Rev. Lett. 99 (2007) 220402.
- [17] N.D. Mermin, Phys. Rev. Lett. 65 (1990) 1838.
- [18] M. Ardehali, Phys. Rev. A 46 (1992) 5375.
- [19] G. Tóth, O. Gühne, H.J. Briegel, Phys. Rev. A 73 (2006) 022303.
- [20] L.-Y. Hsu, Phys. Rev. A 73 (2006) 042308.
- [21] A. Cabello, O. Gühne, D. Rodríguez, Phys. Rev. A 77 (2008) 062106.
- [22] O. Gühne, A. Cabello, Phys. Rev. A 77 (2008) 032108.
- [23] A.K. Ekert, Phys. Rev. Lett. 67 (1991) 661.
- [24] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Phys. Rev. Lett. 70 (1993) 1895.
- [25] R. Cleve, H. Buhrman, Phys. Rev. A 56 (1997) 1201.
- [26] M. Żukowski, A. Zeilinger, M.A. Horne, H. Weinfurter, Acta Phys. Pol. A 93 (1998) 187.
- [27] D. Markham, B.C. Sanders, Phys. Rev. A 78 (2008) 042309.
- [28] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, A. Zeilinger, Nature (London) 434 (2005) 169.
- [29] N. Kiesel, C. Schmid, U. Weber, O. Gühne, G. Tóth, R. Ursin, H. Weinfurter, Phys. Rev. Lett. 95 (2005) 210502.
- [30] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, J.-W. Pan, Nat. Phys. 3 (2007) 91.
- [31] C.-Y. Lu, W.-B. Gao, O. Gühne, X.-Q. Zhou, Z.-B. Chen, J.-W. Pan, Phys. Rev. Lett. 102 (2009) 030502.
- [32] J.K. Pachos, W. Wieczorek, C. Schmid, N. Kiesel, R. Pohlner, H. Weinfurter, arXiv:0710.0895 [quant-ph].
- [33] P.G. Kwiat, J. Mod. Opt. 44 (1997) 2173.
- [34] P.G. Kwiat, H. Weinfurter, Phys. Rev. A 58 (1998) R2623.
- [35] C. Cinelli, M. Barbieri, R. Perris, P. Mataloni, F. De Martini, Phys. Rev. Lett. 95 (2005) 240405.
- [36] T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Żukowski, Z.-B. Chen, J.-W. Pan, Phys. Rev. Lett. 95 (2005) 240406.
- [37] J.T. Barreiro, N.K. Langford, N.A. Peters, P.G. Kwiat, Phys. Rev. Lett. 95 (2005) 260501.
- [38] M. Barbieri, F. De Martini, P. Mataloni, G. Vallone, A. Cabello, Phys. Rev. Lett. 97 (2006) 140407.
- [39] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini, V. Berardi, Phys. Rev. Lett. 98 (2007) 180502.
- [40] H. Weinfurter, M. Żukowski, Phys. Rev. A 64 (2001) 010102(R).
- [41] M. Eibl, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Żukowski, H. Weinfurter, Phys. Rev. Lett. 90 (2003) 200403.
- [42] S. Gaertner, M. Bourennane, M. Eibl, C. Kurtsiefer, H. Weinfurter, Appl. Phys. B 77 (2003) 803.
- [43] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, H. Weinfurter, Phys. Rev. Lett. 92 (2004) 107901.
- [44] P. Walther, M. Aspelmeyer, K.J. Resch, A. Zeilinger, Phys. Rev. Lett. 95 (2005) 020403.
- [45] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, H. Weinfurter, Phys. Rev. Lett. 100 (2008) 070504.
- [46] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, J.-W. Pan, arXiv:0809.4277 [quant-ph].
- [47] W.-B. Gao, X.-C. Yao, P. Xu, O. Gühne, A. Cabello, C.-Y. Lu, Z.-B. Chen, J.-W. Pan, unpublished.
- [48] L.E. Danielsen, Database of Self-Dual Quantum Codes, <http://www.iu.uib.no/~larsed/vncorbits/>. Note that in this Letter we are only interested in graph states associated to connected graphs. In quantum codes, connected graphs correspond to indecomposable quantum codes (i.e., those that cannot be expressed as the direct sum of two smaller codes).
- [49] M. Van den Nest, J. Dehaene, B. De Moor, Phys. Rev. A 69 (2004) 022316.
- [50] M. Van den Nest, J. Dehaene, B. De Moor, Phys. Rev. A 71 (2005) 062323.
- [51] Z. Ji, J. Chen, Z. Wei, M. Ying, arXiv:0709.1266 [quant-ph].
- [52] J. Eisert, H.J. Briegel, Phys. Rev. A 64 (2001) 022306.
- [53] S. Severini, Phys. Lett. A 356 (2006) 99.
- [54] M. Mhalla, S. Perdrix, in: 8th Workshop on Quantum Information Processing (QIP'05), Boston, January 2005, arXiv:quant-ph/0412071.
- [55] M. van den Nest, Dehaene, B. De Moor, Phys. Rev. A 72 (2005) 014307.
- [56] A. Cabello, A.J. López-Tarrida, P. Moreno, J.R. Portillo, arXiv:0904.3551 [quant-ph].
- [57] B.D. McKay, nauty User's Guide (Version 2.4) Department of Computer Science, Australian National University, Canberra, Australia, 2007.





## Erratum

## Erratum to “Entanglement in eight-qubit graph states” [Phys. Lett. A 373 (2009) 2219]

Adán Cabello<sup>a,\*</sup>, Antonio J. López-Tarrida<sup>a</sup>, Pilar Moreno<sup>a</sup>, José R. Portillo<sup>b</sup>

<sup>a</sup> Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain

<sup>b</sup> Departamento de Matemática Aplicada I, Universidad de Sevilla, E-41012 Sevilla, Spain

## ARTICLE INFO

## Article history:

Received 23 July 2010

Available online 11 August 2010

## ABSTRACT

Some errors are corrected.

© 2009 Elsevier B.V. All rights reserved.

Four out of the 101 graphs in Fig. 2 in [1] are incorrect. The correct ones are in Fig. 1.

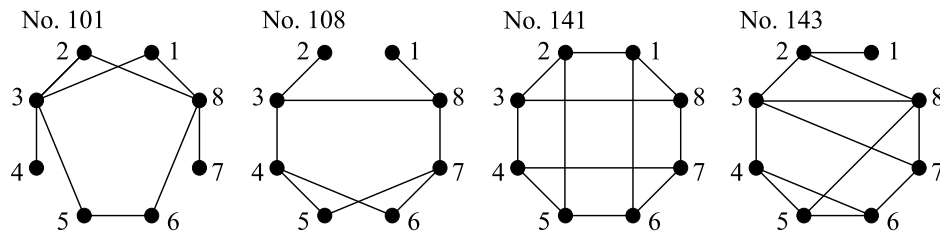


Fig. 1. Corrected graphs.

In addition, in Table 1 in [1], the value of  $E_S$  for the state No. 143 is incorrect. The correct one is  $4 < 5$ . We thank L.E. Danielsen for bringing this error to our attention.

## References

- [1] A. Cabello, A.J. López-Tarrida, P. Moreno, J.R. Portillo, Phys. Lett. A 373 (2009) 2219.

DOI of original article: 10.1016/j.physleta.2009.04.055.

\* Corresponding author.

E-mail address: adan@us.es (A. Cabello).

**Compact set of invariants characterizing graph states of up to eight qubits**Adán Cabello,<sup>1,\*</sup> Antonio J. López-Tarrida,<sup>1</sup> Pilar Moreno,<sup>1</sup> and José R. Portillo<sup>2</sup><sup>1</sup>*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*<sup>2</sup>*Departamento de Matemática Aplicada I, Universidad de Sevilla, E-41012 Sevilla, Spain*

(Received 21 February 2009; published 1 July 2009)

The set of entanglement measures proposed by Hein, Eisert, and Briegel for  $n$ -qubit graph states [Phys. Rev. A **69**, 062311 (2004)] fails to distinguish between inequivalent classes under local Clifford operations if  $n \geq 7$ . On the other hand, the set of invariants proposed by van den Nest, Dehaene, and De Moor (VDD) [Phys. Rev. A **72**, 014307 (2005)] distinguishes between inequivalent classes, but contains too many invariants (more than  $2 \times 10^{36}$  for  $n=7$ ) to be practical. Here we solve the problem of deciding which entanglement class a graph state of  $n \leq 8$  qubits belongs to by calculating some of the state's intrinsic properties. We show that four invariants related to those proposed by VDD are enough for distinguishing between all inequivalent classes with  $n \leq 8$  qubits.

DOI: [10.1103/PhysRevA.80.012102](https://doi.org/10.1103/PhysRevA.80.012102)

PACS number(s): 03.65.Ud, 03.65.Ta, 03.67.Mn, 42.50.Xa

**I. INTRODUCTION**

Graph states [1,2] are fundamental in quantum information, especially in quantum error correction [3–5] and measurement-based quantum computation [6]. Graph states also play a fundamental role in the study of entanglement. Two quantum states have the same entanglement if they are equivalent under stochastic local operations and classical communication (SLOCC). For  $n=3$ , there are six classes under SLOCC [7]. For  $n \geq 4$  the number of classes under SLOCC is infinite and is specified by an exponentially increasing number of parameters. However, if we focus on graph states of  $n < 27$  qubits, then the discussion becomes simpler. On one hand, every two graph states which are SLOCC equivalent are also equivalent under local unitary (LU) operations [8]. On the other hand, previous results suggest that, for graph states of  $n < 27$  qubits, the notion of LU equivalence and local Clifford equivalence (LC equivalence) coincide. The “LU $\Leftrightarrow$ LC conjecture” states that “every two LU-equivalent stabilizer states must also be LC equivalent.” Ji *et al.* proved that the LU $\Leftrightarrow$ LC conjecture is false [9]. However, the LU $\Leftrightarrow$ LC is true for several classes of  $n$  qubit graph states [10,11] and the simplest counterexamples to the conjecture are graph states of  $n=27$  qubits [9]. Indeed, Ji *et al.* “believe that 27 is the smallest possible size of counterexamples of LU $\Leftrightarrow$ LC.” In this paper we assume that deciding whether or not two graph states of  $n < 27$  qubits have the same entanglement is equivalent to deciding whether or not they are LC equivalent.

The aim of this paper is to solve the following problem. Given an  $n$ -qubit graph state with  $n < 9$  qubits, decide which entanglement class it belongs to just by examining some of the state's intrinsic properties (i.e., without generating the whole LC class). The solution to this problem is of practical importance. If one needs to prepare a graph state  $|G\rangle$  and knows that it belongs to one specific class, then one can prepare  $|G\rangle$  by preparing the LC-equivalent state  $|G'\rangle$  requiring the minimum number of entangling gates and the mini-

mum preparation depth of that class (see [1,2,12]) and then transform  $|G'\rangle$  into  $|G\rangle$  by means of simple one-qubit unitary operations. The problem is that, so far, we do not know a simple set of invariants which distinguishes between all classes of entanglement, even for graph states with  $n \leq 7$  qubits.

The classification of graph states' entanglement has been achieved, up to  $n=7$  qubits, by Hein, Eisert, and Briegel (HEB) [1] (see also [2]) and has recently been extended to  $n=8$  qubits [12]. The criteria for ordering the classes in [1,2,12] are based on several entanglement measures: the minimum number of two-qubit gates required for the preparation of a member of the class, the Schmidt measure for the  $n$ -partite split (which measures the genuine  $n$ -party entanglement of the class [13]), and the Schmidt ranks for all bipartite splits (or rank indexes [1,2]). The problem is that this set of entanglement measures fails to distinguish between inequivalent classes (i.e., between different types of entanglement). There is already an example of this problem in  $n=7$ : none of these entanglement measures allows us to distinguish between the classes 40, 42, and 43 in [1,2]. A similar problem occurs in  $n=8$ : none of these entanglement measures allows us to distinguish between classes 110 and 111, between classes 113 and 114, and between classes 116 and 117 in [12]. Therefore, we cannot use these invariants for deciding which entanglement class a given state belongs to. Reciprocally, if we have such a set of invariants, then we can use it to unambiguously label each of the classes.

Van den Nest, Dehaene, and De Moor (VDD) proposed a finite set of invariants that characterizes all classes [14]. However, already for  $n=7$ , this set has more than  $2 \times 10^{36}$  invariants which are not explicitly calculated anywhere, so this set is not useful for classifying a given graph state. Indeed, VDD “believe that [their set of invariants] can be improved—if not for all stabilizer states then at least for some interesting subclasses of states” [14]. Moreover, they state that “it is likely that only [some] invariants need to be considered in order to recognize LC equivalence” [14] and that “it is not unlikely that there exist smaller complete lists of invariants which exhibit less redundancies” [14]. In this paper we show that, if  $n \leq 8$ , then four invariants are enough to recognize the type of entanglement.

\*adan@us.es

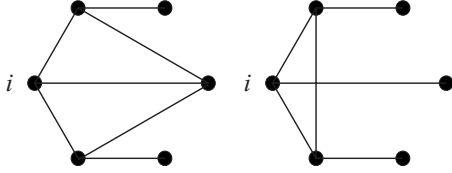


FIG. 1. Graphical effect of local complementation on qubit  $i$ . Local complementation on qubit  $i$  on the graph on the left (right) leads to the graph on the right (left).

The paper is organized as follows. In Sec. II we introduce some basic concepts of the graph state formalism and review some of the results about the invariants proposed by VDD that will be useful in our discussion. In Sec. III we present our results and in Sec. IV our conclusions.

## II. BASIC CONCEPTS

### A. Stabilizer

The Pauli group  $\mathcal{G}_n$  on  $n$  qubits consists of all  $4 \times 4^n$ -fold tensor products of the form  $M = \alpha_M M_1 \otimes \dots \otimes M_n$ , where  $\alpha_M \in \{\pm 1, \pm i\}$  is an overall phase factor and  $M_i$  is either the  $2 \times 2$  identity matrix  $\sigma_0 = \mathbb{1}$  or one of the Pauli matrices  $X = \sigma_x$ ,  $Y = \sigma_y$ , and  $Z = \sigma_z$ .

An  $n$ -qubit stabilizer  $\mathcal{S}$  in the Pauli group is defined as an Abelian subgroup of  $\mathcal{G}_n$  which does not contain the operator  $-\mathbb{1}$  [15]. A stabilizer consists of  $2^k$  Hermitian (therefore, they must have real overall phase factors  $\pm 1$ )  $n$ -qubit Pauli operators  $s_i = \alpha_i M_1^{(i)} \otimes \dots \otimes M_n^{(i)} \in \mathcal{G}_n, i = 1, \dots, 2^k$  for some  $k \leq n$ . We will call the operators  $s_i$  stabilizing operators.

In group theory, a set of elements  $\{g_1, \dots, g_l\}$  in a group  $G$  is said to generate the group  $G$  if every element of  $G$  can be written as a product of elements from  $\{g_1, \dots, g_l\}$ . The notation  $G = \langle g_1, \dots, g_l \rangle$  is commonly used to describe this fact, and the set  $\{g_1, \dots, g_l\}$  is called the generator of  $G$ . The generator of an  $n$ -qubit stabilizer  $\mathcal{S}$  is a subset (not necessarily unique)  $\gamma_{\mathcal{S}} = \{g_1, \dots, g_k\}$ , consisting of  $k \leq n$  independent stabilizing operators, such that  $\mathcal{S} = \langle \gamma_{\mathcal{S}} \rangle$ . In this context, independent means that no product of the form  $g_1^{a_1} \dots g_k^{a_k}$ , where  $a_i \in \{0, 1\}$  yields the identity except when all  $a_i = 0$ . As a consequence, removing any operator  $g_i$  from the generator makes the generated group smaller.

By definition, given a stabilizer  $\mathcal{S}$ , the stabilizing operators  $s_i$  commute, so that they can be diagonalized simulta-

TABLE I. Stabilizer and supports for the  $|\text{LC}_3\rangle$ .

Stabilizing operators		Support	Weight
XZ1	$s_1 = g_1$	{1,2}	2
ZXZ	$s_2 = g_2$	{1,2,3}	3
lZX	$s_3 = g_3$	{2,3}	2
lll	$s_4 = g_1 g_1$	$\{\emptyset\}$	0
YYZ	$s_5 = g_1 g_2$	{1,2,3}	3
XlX	$s_6 = g_1 g_3$	{1,3}	2
ZYY	$s_7 = g_2 g_3$	{1,2,3}	3
-YXY	$s_8 = g_1 g_2 g_3$	{1,2,3}	3

TABLE II. Weight distribution for graph states up to six qubits.

Graph state	$A_0$	$A_1$	$A_2$	$A_3$	$A_4$	$A_5$	$A_6$
1	1	0	3				
2	1	0	3	4			
3	1	0	6	0	9		
4	1	0	2	8	5		
5	1	0	10	0	5	16	
6	1	0	4	6	11	10	
7	1	0	2	8	13	8	
8	1	0	0	10	15	6	
9	1	0	15	0	15	0	33
10	1	0	7	8	7	24	17
11	1	0	6	0	33	0	24
12	1	0	4	8	13	24	14
13	1	0	3	8	15	24	13
14	1	0	2	8	17	24	12
15	1	0	3	8	15	24	13
16	1	0	3	0	39	0	21
17	1	0	1	8	19	24	11
18	1	0	0	8	21	24	10
19	1	0	0	0	45	0	18

neously and, therefore, share a common set of eigenvectors that constitute a basis of the so-called vector space  $V_{\mathcal{S}}$  stabilized by  $\mathcal{S}$ . The vector space  $V_{\mathcal{S}}$  is of dimension  $2^q$  when  $|\gamma_{\mathcal{S}}| = n - q$ . Remarkably, if  $|\mathcal{S}| = 2^n$ , then there exists a unique common eigenstate  $|\psi\rangle$  on  $n$  qubits with eigenvalue 1, such that  $s_i |\psi\rangle = |\psi\rangle$  for every stabilizing operator  $s_i \in \mathcal{S}$ . Such a state  $|\psi\rangle$  is called a stabilizer state because it is the only state that is fixed (stabilized) by every operator of the stabilizer  $\mathcal{S}$ .

Graph states are a special kind of stabilizer states (with  $k = n$ ) associated with graphs. It has been demonstrated that every stabilizer state is equivalent under local complementation (defined below) to some (generally non unique) graph state [5].

### B. Graph state

A  $n$ -qubit graph state  $|G\rangle$  is a pure state associated to a graph  $G(V, E)$  consisting of a set of  $n$  vertices  $V = \{1, \dots, n\}$  and a set of edges  $E$  connecting pairs of vertices,  $E \subset V \times V$ . Each vertex represents a qubit. The graph  $G$  provides a mathematical characterization of  $|G\rangle$ . The graph state  $|G\rangle$  associated to the graph  $G$  is the unique  $n$ -qubit state fulfilling

$$g_i |G\rangle = |G\rangle, \quad \text{for } i = 1, \dots, n, \quad (1)$$

where  $g_i$  are the generators of the state's stabilizer group, defined as the set  $\{s_j\}_{j=1}^{2^n}$  of all products of the generators.  $g_i$  is the generator operator associated to the vertex  $i$ , defined by

$$g_i := X^{(i)} \otimes_{(i,j) \in E} Z^{(j)}, \quad (2)$$

where the product is extended to those vertices  $j$  which are connected with  $i$  and  $X^{(i)}(Z^{(i)})$  denotes the Pauli matrix  $\sigma_x(\sigma_z)$  acting on the  $i$ th qubit.

TABLE III. Invariants for the  $n$ -qubit graph states with  $3 \leq n \leq 6$ . Notation: value<sub>multiplicity</sub>. The numeration of the classes is the one in [1,2].

No.	Invariants
1	$0_2, 1_1, 3_1$
2	$0_3, 1_4, 4_1$
3	$0_8, 1_7, 9_1$
4	$0_8, 1_3, 2_4, 5_1$
5	$0_{15}, 1_{16}, 16_1$
6	$0_{18}, 1_8, 2_3, 4_2, 10_1$
7	$0_{17}, 1_7, 2_6, 5_1, 8_1$
8	$0_{15}, 1_{11}, 3_5, 6_1$
9	$0_{32}, 1_{31}, 33_1$
10	$0_{38}, 1_{15}, 2_8, 8_2, 17_1$
11	$0_{41}, 1_{16}, 4_6, 24_1$
12	$0_{38}, 1_{14}, 2_7, 4_1, 5_2, 8_1, 14_1$
13	$0_{42}, 1_6, 2_8, 4_6, 5_1, 13_1$
14	$0_{37}, 1_{12}, 2_8, 3_4, 6_2, 12_1$
15	$0_{42}, 1_{12}, 4_6, 5_3, 13_1$
16	$0_{44}, 1_4, 2_{12}, 5_3, 21_1$
17	$0_{34}, 1_{18}, 2_6, 3_1, 5_4, 11_1$
18	$0_{33}, 1_{21}, 3_3, 4_6, 10_1$
19	$0_{47}, 1_1, 3_{15}, 18_1$

**C. Local complementation**

Two  $n$ -qubit states,  $|\phi\rangle$  and  $|\psi\rangle$ , have the same  $n$ -partite entanglement if and only if there are  $n$  one-qubit unitary transformations  $U_i$ , such that  $|\phi\rangle = \otimes_{i=1}^n U_i |\psi\rangle$ . If these one-qubit unitary transformations belong to the Clifford group, then the two states are said to be LC equivalent. VDD found that the successive application of a transformation with a simple graphical description is enough to generate the complete equivalence class of graph states under local unitary operations within the Clifford group (hereafter simply referred to as class or orbit) [16]. This simple transformation is local complementation.

On the stabilizer, local complementation on the qubit  $i$  induces the map  $Y^{(i)} \mapsto Z^{(i)}, Z^{(i)} \mapsto -Y^{(i)}$  on the qubit  $i$  and the map  $X^{(j)} \mapsto -Y^{(j)}, Y^{(j)} \mapsto X^{(j)}$  on the qubits  $j$  connected with  $i$  [2]. On the generators, local complementation on the qubit  $i$  maps the generators  $g_j^{\text{old}}$ , with  $j$  connected with  $i$ , to  $g_j^{\text{new}} g_i^{\text{new}}$ .

Graphically, local complementation on qubit  $i$  acts as follows. Those vertices connected with  $i$  which were connected from each other become disconnected from each other and vice versa. An example is in Fig. 1.

Using local complementation, one can generate the orbits of all LC-inequivalent  $n$ -qubit graph states. There are 45 orbits for  $n \leq 7$  [1,2] and 101 orbits for  $n=8$  [12].

**D. Supports and LC invariants related to supports**

Let  $|\psi\rangle$  be a stabilizer state and  $\mathcal{S}(|\psi\rangle)$  the corresponding stabilizer. Given a stabilizing operator  $s_i = \alpha_i M_1^{(i)} \otimes \dots \otimes M_n^{(i)}$ , its support  $\text{supp}(s_i)$  is the set of all  $j \in \{1, \dots, n\}$  such that

TABLE IV. Invariants for the seven-qubit graph states. Notation: value<sub>multiplicity</sub>. The numeration of the classes is the one in [1,2].

No.	Invariants
20	$0_{63}, 1_{64}, 64_1$
21	$0_{78}, 1_{32}, 2_{15}, 16_2, 34_1$
22	$0_{84}, 1_{32}, 4_8, 8_3, 40_1$
23	$0_{77}, 1_{31}, 2_{15}, 8_3, 17_1, 26_1$
24	$0_{87}, 1_{25}, 4_8, 5_6, 16_1, 25_1$
25	$0_{92}, 1_{12}, 2_8, 4_7, 5_4, 8_4, 20_1$
26	$0_{87}, 1_{16}, 2_{14}, 4_7, 8_1, 10_2, 28_1$
27	$0_{80}, 1_{25}, 2_{11}, 3_3, 4_3, 5_3, 8_1, 14_1, 23_1$
28	$0_{85}, 1_{15}, 2_{16}, 4_3, 6_7, 9_1, 18_1$
29	$0_{87}, 1_{12}, 2_{15}, 4_9, 5_3, 13_1, 22_1$
30	$0_{80}, 1_{21}, 2_{12}, 3_6, 4_1, 5_4, 8_3, 17_1$
31	$0_{86}, 1_{28}, 4_3, 5_4, 8_6, 20_1$
32	$0_{89}, 1_{12}, 2_{16}, 4_4, 5_4, 8_2, 32_1$
33	$0_{72}, 1_{40}, 2_3, 3_4, 4_4, 9_4, 18_1$
34	$0_{85}, 1_{14}, 2_{17}, 4_7, 5_1, 6_2, 13_1, 22_1$
35	$0_{79}, 1_{25}, 2_{12}, 4_2, 5_6, 8_3, 17_1$
36	$0_{86}, 1_{14}, 2_{17}, 4_4, 5_2, 6_2, 8_2, 26_1$
37	$0_{80}, 1_{21}, 2_{12}, 3_8, 4_1, 5_2, 6_2, 12_1, 21_1$
38	$0_{74}, 1_{32}, 2_8, 3_3, 4_5, 7_5, 16_1$
39	$0_{77}, 1_{22}, 2_{16}, 3_5, 4_2, 7_5, 16_1$
40	$0_{70}, 1_{36}, 2_7, 3_7, 6_7, 15_1$
41	$0_{78}, 1_{22}, 2_{14}, 3_5, 4_3, 5_4, 11_1, 20_1$
42	$0_{74}, 1_{26}, 2_{15}, 3_5, 6_7, 15_1$
43	$0_{84}, 1_8, 2_{21}, 3_7, 6_7, 15_1$
44	$0_{78}, 1_{24}, 2_3, 3_{15}, 4_6, 10_1, 19_1$
45	$0_{83}, 1_{22}, 3_{10}, 4_{10}, 6_2, 24_1$

$M_j^{(i)}$  differs from the identity. Therefore, the support of  $s_i$  is the set of the labels of the qubits on which the action of the Pauli matrices is nontrivial (i.e., there is a  $X, Y$ , or  $Z$  Pauli matrix acting on the qubit). Notice that the support is preserved under the maps induced on the stabilizer by local complementation (see Sec. II C).

Let  $\omega \subseteq \{1, \dots, n\}$  be the support of a stabilizing operator  $s_i$ ,  $\text{supp}(s_i) = \omega$ . The weight of the operator  $s_i$  is the cardinality of its support,  $|\omega|$ . The identity operator  $\mathbb{1} \otimes \dots \otimes \mathbb{1}$ , which is always present in a stabilizer due to the underlying group structure, fulfills  $\omega = \{\emptyset\}$  and, therefore, is of weight zero.

The set of operators  $\{s_i\}_{i=1}^{2^k}$  of a stabilizer  $\mathcal{S}$  can be classified into equivalence classes according to their supports, defining a partition in the stabilizer. We will say that two stabilizing operators  $s_i$  and  $s_j$  of  $\mathcal{S}$  belong to the same equivalence class  $[\omega]$  if they have the same support  $\omega$ , i.e.,  $\text{supp}(s_i) = \text{supp}(s_j) = \omega$ . We denote by  $A_\omega(|\psi\rangle)$  the number of elements (stabilizing operators)  $s_i \in \mathcal{S}(|\psi\rangle)$  with  $\text{supp}(s_i) = \omega$ . In other words,  $A_\omega(|\psi\rangle)$  is the cardinality of the equivalence class  $[\omega]$ . Since any graph state  $|G\rangle$  is a special type of stabilizer state, these definitions can also be applied to them.

TABLE V. Invariants for the eight-qubit graph states. Notation: value<sub>multiplicity</sub>. The numeration of the classes is the one in [12].

No.	Invariants	No.	Invariants
46	0 <sub>128</sub> , 1 <sub>127</sub> , 129 <sub>1</sub>	97	0 <sub>163</sub> , 1 <sub>44</sub> , 2 <sub>17</sub> , 3 <sub>14</sub> , 4 <sub>5</sub> , 5 <sub>4</sub> , 7 <sub>2</sub> , 10 <sub>6</sub> , 22 <sub>1</sub>
47	0 <sub>158</sub> , 1 <sub>63</sub> , 2 <sub>32</sub> , 32 <sub>2</sub> , 65 <sub>1</sub>	98	0 <sub>157</sub> , 1 <sub>55</sub> , 2 <sub>17</sub> , 3 <sub>9</sub> , 4 <sub>4</sub> , 5 <sub>3</sub> , 6 <sub>3</sub> , 7 <sub>1</sub> , 9 <sub>4</sub> , 12 <sub>2</sub> , 24 <sub>1</sub>
48	0 <sub>173</sub> , 1 <sub>64</sub> , 4 <sub>15</sub> , 16 <sub>3</sub> , 84 <sub>1</sub>	99	0 <sub>165</sub> , 1 <sub>40</sub> , 2 <sub>18</sub> , 3 <sub>17</sub> , 4 <sub>4</sub> , 5 <sub>2</sub> , 6 <sub>2</sub> , 7 <sub>1</sub> , 9 <sub>4</sub> , 12 <sub>2</sub> , 24 <sub>1</sub>
49	0 <sub>158</sub> , 1 <sub>62</sub> , 2 <sub>31</sub> , 16 <sub>1</sub> , 17 <sub>2</sub> , 32 <sub>1</sub> , 50 <sub>1</sub>	100	0 <sub>152</sub> , 1 <sub>59</sub> , 2 <sub>16</sub> , 3 <sub>8</sub> , 4 <sub>12</sub> , 9 <sub>8</sub> , 21 <sub>1</sub>
50	0 <sub>176</sub> , 1 <sub>63</sub> , 8 <sub>16</sub> , 65 <sub>1</sub>	101	0 <sub>168</sub> , 1 <sub>58</sub> , 4 <sub>18</sub> , 8 <sub>3</sub> , 9 <sub>6</sub> , 12 <sub>2</sub> , 24 <sub>1</sub>
51	0 <sub>176</sub> , 1 <sub>56</sub> , 4 <sub>7</sub> , 5 <sub>8</sub> , 8 <sub>7</sub> , 32 <sub>1</sub> , 44 <sub>1</sub>	102	0 <sub>177</sub> , 1 <sub>26</sub> , 2 <sub>26</sub> , 3 <sub>4</sub> , 4 <sub>11</sub> , 5 <sub>2</sub> , 6 <sub>2</sub> , 8 <sub>6</sub> , 20 <sub>1</sub> , 32 <sub>1</sub>
52	0 <sub>192</sub> , 1 <sub>24</sub> , 2 <sub>16</sub> , 4 <sub>8</sub> , 5 <sub>7</sub> , 8 <sub>4</sub> , 16 <sub>4</sub> , 37 <sub>1</sub>	103	0 <sub>174</sub> , 1 <sub>20</sub> , 2 <sub>40</sub> , 3 <sub>9</sub> , 6 <sub>4</sub> , 7 <sub>2</sub> , 8 <sub>2</sub> , 12 <sub>4</sub> , 27 <sub>1</sub>
53	0 <sub>180</sub> , 1 <sub>30</sub> , 2 <sub>30</sub> , 4 <sub>8</sub> , 8 <sub>2</sub> , 10 <sub>2</sub> , 16 <sub>2</sub> , 17 <sub>1</sub> , 49 <sub>1</sub>	104	0 <sub>200</sub> , 1 <sub>21</sub> , 4 <sub>24</sub> , 5 <sub>6</sub> , 13 <sub>4</sub> , 57 <sub>1</sub>
54	0 <sub>163</sub> , 1 <sub>54</sub> , 2 <sub>22</sub> , 3 <sub>8</sub> , 8 <sub>4</sub> , 9 <sub>2</sub> , 18 <sub>1</sub> , 24 <sub>1</sub> , 42 <sub>1</sub>	105	0 <sub>159</sub> , 1 <sub>58</sub> , 2 <sub>15</sub> , 3 <sub>4</sub> , 4 <sub>12</sub> , 9 <sub>2</sub> , 10 <sub>4</sub> , 16 <sub>1</sub> , 34 <sub>1</sub>
55	0 <sub>185</sub> , 1 <sub>32</sub> , 2 <sub>16</sub> , 4 <sub>13</sub> , 8 <sub>7</sub> , 20 <sub>2</sub> , 44 <sub>1</sub>	106	0 <sub>193</sub> , 1 <sub>19</sub> , 2 <sub>15</sub> , 3 <sub>12</sub> , 6 <sub>12</sub> , 9 <sub>1</sub> , 12 <sub>3</sub> , 54 <sub>1</sub>
56	0 <sub>181</sub> , 1 <sub>30</sub> , 2 <sub>23</sub> , 4 <sub>6</sub> , 6 <sub>7</sub> , 8 <sub>3</sub> , 9 <sub>2</sub> , 12 <sub>2</sub> , 18 <sub>1</sub> , 30 <sub>1</sub>	107	0 <sub>196</sub> , 1 <sub>9</sub> , 2 <sub>24</sub> , 4 <sub>12</sub> , 5 <sub>4</sub> , 8 <sub>8</sub> , 13 <sub>2</sub> , 41 <sub>1</sub>
57	0 <sub>191</sub> , 1 <sub>32</sub> , 2 <sub>9</sub> , 4 <sub>16</sub> , 10 <sub>6</sub> , 16 <sub>1</sub> , 66 <sub>1</sub>	108	0 <sub>180</sub> , 1 <sub>26</sub> , 2 <sub>26</sub> , 3 <sub>4</sub> , 4 <sub>4</sub> , 6 <sub>10</sub> , 9 <sub>2</sub> , 12 <sub>3</sub> , 36 <sub>1</sub>
58	0 <sub>176</sub> , 1 <sub>49</sub> , 4 <sub>14</sub> , 5 <sub>14</sub> , 20 <sub>2</sub> , 41 <sub>1</sub>	109	0 <sub>164</sub> , 1 <sub>40</sub> , 2 <sub>28</sub> , 3 <sub>2</sub> , 4 <sub>8</sub> , 5 <sub>4</sub> , 6 <sub>1</sub> , 7 <sub>2</sub> , 10 <sub>6</sub> , 22 <sub>1</sub>
59	0 <sub>183</sub> , 1 <sub>28</sub> , 2 <sub>25</sub> , 4 <sub>6</sub> , 5 <sub>2</sub> , 6 <sub>3</sub> , 8 <sub>2</sub> , 10 <sub>2</sub> , 13 <sub>2</sub> , 14 <sub>1</sub> , 16 <sub>1</sub> , 34 <sub>1</sub>	110	0 <sub>174</sub> , 1 <sub>32</sub> , 2 <sub>22</sub> , 3 <sub>13</sub> , 4 <sub>4</sub> , 7 <sub>1</sub> , 8 <sub>2</sub> , 10 <sub>6</sub> , 11 <sub>1</sub> , 31 <sub>1</sub>
60	0 <sub>179</sub> , 1 <sub>32</sub> , 2 <sub>25</sub> , 4 <sub>9</sub> , 6 <sub>3</sub> , 8 <sub>3</sub> , 10 <sub>1</sub> , 14 <sub>2</sub> , 20 <sub>1</sub> , 38 <sub>1</sub>	111	0 <sub>166</sub> , 1 <sub>40</sub> , 2 <sub>22</sub> , 3 <sub>9</sub> , 4 <sub>9</sub> , 5 <sub>1</sub> , 6 <sub>1</sub> , 7 <sub>4</sub> , 10 <sub>1</sub> , 13 <sub>1</sub> , 16 <sub>1</sub> , 31 <sub>1</sub>
61	0 <sub>186</sub> , 1 <sub>24</sub> , 2 <sub>20</sub> , 4 <sub>10</sub> , 5 <sub>8</sub> , 8 <sub>2</sub> , 10 <sub>4</sub> , 16 <sub>1</sub> , 40 <sub>1</sub>	112	0 <sub>168</sub> , 1 <sub>31</sub> , 2 <sub>32</sub> , 3 <sub>9</sub> , 4 <sub>8</sub> , 5 <sub>1</sub> , 7 <sub>2</sub> , 13 <sub>4</sub> , 31 <sub>1</sub>
62	0 <sub>169</sub> , 1 <sub>46</sub> , 2 <sub>15</sub> , 3 <sub>7</sub> , 4 <sub>5</sub> , 5 <sub>7</sub> , 8 <sub>1</sub> , 9 <sub>2</sub> , 12 <sub>1</sub> , 15 <sub>1</sub> , 18 <sub>1</sub> , 33 <sub>1</sub>	113	0 <sub>161</sub> , 1 <sub>46</sub> , 2 <sub>21</sub> , 3 <sub>10</sub> , 4 <sub>4</sub> , 5 <sub>6</sub> , 6 <sub>1</sub> , 8 <sub>3</sub> , 11 <sub>2</sub> , 14 <sub>1</sub> , 26 <sub>1</sub>
63	0 <sub>175</sub> , 1 <sub>27</sub> , 2 <sub>31</sub> , 3 <sub>4</sub> , 4 <sub>6</sub> , 6 <sub>2</sub> , 8 <sub>7</sub> , 9 <sub>1</sub> , 14 <sub>2</sub> , 26 <sub>1</sub>	114	0 <sub>158</sub> , 1 <sub>51</sub> , 2 <sub>20</sub> , 3 <sub>12</sub> , 4 <sub>2</sub> , 5 <sub>3</sub> , 6 <sub>1</sub> , 7 <sub>2</sub> , 8 <sub>2</sub> , 11 <sub>4</sub> , 26 <sub>1</sub>
64	0 <sub>200</sub> , 1 <sub>8</sub> , 2 <sub>14</sub> , 4 <sub>18</sub> , 5 <sub>6</sub> , 8 <sub>6</sub> , 13 <sub>1</sub> , 14 <sub>2</sub> , 29 <sub>1</sub>	115	0 <sub>164</sub> , 1 <sub>40</sub> , 2 <sub>28</sub> , 3 <sub>2</sub> , 4 <sub>7</sub> , 5 <sub>6</sub> , 8 <sub>7</sub> , 14 <sub>1</sub> , 26 <sub>1</sub>
65	0 <sub>188</sub> , 2 <sub>28</sub> , 4 <sub>16</sub> , 6 <sub>4</sub> , 9 <sub>2</sub> , 12 <sub>4</sub> , 33 <sub>1</sub>	116	0 <sub>161</sub> , 1 <sub>38</sub> , 2 <sub>37</sub> , 3 <sub>7</sub> , 4 <sub>2</sub> , 6 <sub>1</sub> , 7 <sub>3</sub> , 10 <sub>6</sub> , 28 <sub>1</sub>
66	0 <sub>181</sub> , 1 <sub>20</sub> , 2 <sub>26</sub> , 3 <sub>8</sub> , 4 <sub>8</sub> , 6 <sub>3</sub> , 7 <sub>4</sub> , 8 <sub>1</sub> , 10 <sub>3</sub> , 16 <sub>1</sub> , 28 <sub>1</sub>	117	0 <sub>161</sub> , 1 <sub>43</sub> , 2 <sub>23</sub> , 3 <sub>14</sub> , 4 <sub>4</sub> , 5 <sub>3</sub> , 6 <sub>1</sub> , 7 <sub>2</sub> , 10 <sub>2</sub> , 13 <sub>2</sub> , 28 <sub>1</sub>
67	0 <sub>179</sub> , 1 <sub>24</sub> , 2 <sub>26</sub> , 3 <sub>4</sub> , 4 <sub>8</sub> , 5 <sub>2</sub> , 6 <sub>8</sub> , 9 <sub>2</sub> , 12 <sub>1</sub> , 18 <sub>1</sub> , 30 <sub>1</sub>	118	0 <sub>155</sub> , 1 <sub>55</sub> , 2 <sub>12</sub> , 3 <sub>16</sub> , 4 <sub>9</sub> , 9 <sub>8</sub> , 21 <sub>1</sub>
68	0 <sub>170</sub> , 1 <sub>35</sub> , 2 <sub>20</sub> , 3 <sub>12</sub> , 4 <sub>7</sub> , 5 <sub>2</sub> , 7 <sub>4</sub> , 8 <sub>1</sub> , 10 <sub>2</sub> , 13 <sub>2</sub> , 25 <sub>1</sub>	119	0 <sub>152</sub> , 1 <sub>59</sub> , 2 <sub>16</sub> , 3 <sub>10</sub> , 4 <sub>9</sub> , 6 <sub>1</sub> , 8 <sub>6</sub> , 11 <sub>2</sub> , 23 <sub>1</sub>
69	0 <sub>180</sub> , 1 <sub>54</sub> , 4 <sub>8</sub> , 5 <sub>7</sub> , 16 <sub>4</sub> , 17 <sub>2</sub> , 37 <sub>1</sub>	120	0 <sub>160</sub> , 1 <sub>42</sub> , 2 <sub>29</sub> , 3 <sub>3</sub> , 4 <sub>12</sub> , 6 <sub>1</sub> , 8 <sub>6</sub> , 11 <sub>2</sub> , 23 <sub>1</sub>
70	0 <sub>176</sub> , 1 <sub>62</sub> , 8 <sub>14</sub> , 16 <sub>1</sub> , 17 <sub>2</sub> , 32 <sub>1</sub>	121	0 <sub>192</sub> , 1 <sub>25</sub> , 4 <sub>24</sub> , 5 <sub>6</sub> , 8 <sub>8</sub> , 41 <sub>1</sub>
71	0 <sub>188</sub> , 1 <sub>22</sub> , 2 <sub>32</sub> , 5 <sub>7</sub> , 8 <sub>4</sub> , 17 <sub>2</sub> , 69 <sub>1</sub>	122	0 <sub>176</sub> , 1 <sub>24</sub> , 2 <sub>24</sub> , 3 <sub>6</sub> , 4 <sub>16</sub> , 6 <sub>1</sub> , 7 <sub>2</sub> , 10 <sub>6</sub> , 22 <sub>1</sub>
72	0 <sub>148</sub> , 1 <sub>84</sub> , 2 <sub>8</sub> , 3 <sub>7</sub> , 8 <sub>4</sub> , 17 <sub>4</sub> , 35 <sub>1</sub>	123	0 <sub>190</sub> , 1 <sub>28</sub> , 2 <sub>12</sub> , 3 <sub>1</sub> , 5 <sub>16</sub> , 8 <sub>6</sub> , 11 <sub>2</sub> , 51 <sub>1</sub>
73	0 <sub>185</sub> , 1 <sub>32</sub> , 2 <sub>15</sub> , 4 <sub>12</sub> , 8 <sub>10</sub> , 16 <sub>1</sub> , 50 <sub>1</sub>	124	0 <sub>200</sub> , 1 <sub>5</sub> , 2 <sub>32</sub> , 5 <sub>6</sub> , 8 <sub>8</sub> , 13 <sub>4</sub> , 41 <sub>1</sub>
74	0 <sub>178</sub> , 1 <sub>30</sub> , 2 <sub>26</sub> , 4 <sub>9</sub> , 6 <sub>6</sub> , 8 <sub>3</sub> , 9 <sub>2</sub> , 24 <sub>1</sub> , 36 <sub>1</sub>	125	0 <sub>169</sub> , 1 <sub>35</sub> , 2 <sub>28</sub> , 3 <sub>4</sub> , 4 <sub>4</sub> , 5 <sub>6</sub> , 6 <sub>4</sub> , 8 <sub>1</sub> , 9 <sub>2</sub> , 12 <sub>2</sub> , 33 <sub>1</sub>
75	0 <sub>166</sub> , 1 <sub>54</sub> , 2 <sub>14</sub> , 4 <sub>6</sub> , 5 <sub>7</sub> , 8 <sub>4</sub> , 9 <sub>1</sub> , 14 <sub>2</sub> , 17 <sub>1</sub> , 29 <sub>1</sub>	126	0 <sub>170</sub> , 1 <sub>44</sub> , 2 <sub>14</sub> , 3 <sub>6</sub> , 5 <sub>12</sub> , 8 <sub>6</sub> , 10 <sub>1</sub> , 11 <sub>2</sub> , 26 <sub>1</sub>
76	0 <sub>188</sub> , 1 <sub>26</sub> , 2 <sub>14</sub> , 4 <sub>14</sub> , 5 <sub>2</sub> , 8 <sub>6</sub> , 9 <sub>2</sub> , 13 <sub>1</sub> , 14 <sub>2</sub> , 29 <sub>1</sub>	127	0 <sub>161</sub> , 1 <sub>48</sub> , 2 <sub>19</sub> , 3 <sub>6</sub> , 4 <sub>9</sub> , 5 <sub>4</sub> , 7 <sub>6</sub> , 10 <sub>1</sub> , 16 <sub>1</sub> , 28 <sub>1</sub>
77	0 <sub>186</sub> , 1 <sub>28</sub> , 2 <sub>18</sub> , 4 <sub>12</sub> , 5 <sub>4</sub> , 10 <sub>4</sub> , 14 <sub>2</sub> , 16 <sub>1</sub> , 40 <sub>1</sub>	128	0 <sub>161</sub> , 1 <sub>42</sub> , 2 <sub>33</sub> , 3 <sub>3</sub> , 4 <sub>6</sub> , 6 <sub>1</sub> , 7 <sub>3</sub> , 10 <sub>6</sub> , 28 <sub>1</sub>
78	0 <sub>191</sub> , 1 <sub>24</sub> , 2 <sub>22</sub> , 4 <sub>1</sub> , 5 <sub>8</sub> , 8 <sub>7</sub> , 14 <sub>2</sub> , 60 <sub>1</sub>	129	0 <sub>160</sub> , 1 <sub>50</sub> , 2 <sub>18</sub> , 3 <sub>8</sub> , 4 <sub>9</sub> , 6 <sub>3</sub> , 7 <sub>2</sub> , 9 <sub>4</sub> , 12 <sub>1</sub> , 30 <sub>1</sub>
79	0 <sub>178</sub> , 1 <sub>32</sub> , 2 <sub>25</sub> , 4 <sub>7</sub> , 6 <sub>6</sub> , 8 <sub>4</sub> , 12 <sub>3</sub> , 42 <sub>1</sub>	130	0 <sub>156</sub> , 1 <sub>52</sub> , 2 <sub>19</sub> , 3 <sub>9</sub> , 4 <sub>10</sub> , 6 <sub>1</sub> , 8 <sub>6</sub> , 11 <sub>2</sub> , 23 <sub>1</sub>
80	0 <sub>166</sub> , 1 <sub>49</sub> , 2 <sub>15</sub> , 3 <sub>6</sub> , 4 <sub>8</sub> , 5 <sub>6</sub> , 8 <sub>1</sub> , 9 <sub>1</sub> , 11 <sub>1</sub> , 14 <sub>1</sub> , 20 <sub>1</sub> , 35 <sub>1</sub>	131	0 <sub>152</sub> , 1 <sub>59</sub> , 2 <sub>16</sub> , 3 <sub>12</sub> , 4 <sub>6</sub> , 6 <sub>2</sub> , 7 <sub>4</sub> , 10 <sub>4</sub> , 25 <sub>1</sub>
81	0 <sub>156</sub> , 1 <sub>70</sub> , 2 <sub>3</sub> , 3 <sub>4</sub> , 4 <sub>15</sub> , 9 <sub>2</sub> , 10 <sub>1</sub> , 13 <sub>4</sub> , 28 <sub>1</sub>	132	0 <sub>156</sub> , 1 <sub>52</sub> , 2 <sub>16</sub> , 3 <sub>13</sub> , 4 <sub>10</sub> , 7 <sub>5</sub> , 10 <sub>2</sub> , 13 <sub>1</sub> , 25 <sub>1</sub>
82	0 <sub>179</sub> , 1 <sub>27</sub> , 2 <sub>27</sub> , 3 <sub>4</sub> , 4 <sub>6</sub> , 6 <sub>4</sub> , 8 <sub>2</sub> , 9 <sub>1</sub> , 12 <sub>5</sub> , 30 <sub>1</sub>	133	0 <sub>148</sub> , 1 <sub>69</sub> , 2 <sub>12</sub> , 3 <sub>2</sub> , 4 <sub>16</sub> , 9 <sub>8</sub> , 21 <sub>1</sub>
83	0 <sub>179</sub> , 1 <sub>24</sub> , 2 <sub>26</sub> , 3 <sub>4</sub> , 4 <sub>10</sub> , 5 <sub>2</sub> , 6 <sub>4</sub> , 8 <sub>2</sub> , 9 <sub>2</sub> , 12 <sub>1</sub> , 18 <sub>1</sub> , 30 <sub>1</sub>	134	0 <sub>188</sub> , 1 <sub>34</sub> , 3 <sub>20</sub> , 6 <sub>3</sub> , 9 <sub>10</sub> , 54 <sub>1</sub>
84	0 <sub>165</sub> , 1 <sub>49</sub> , 2 <sub>14</sub> , 3 <sub>6</sub> , 4 <sub>10</sub> , 7 <sub>6</sub> , 8 <sub>1</sub> , 10 <sub>2</sub> , 13 <sub>2</sub> , 25 <sub>1</sub>	135	0 <sub>166</sub> , 1 <sub>44</sub> , 2 <sub>20</sub> , 3 <sub>3</sub> , 4 <sub>12</sub> , 8 <sub>10</sub> , 35 <sub>1</sub>
85	0 <sub>160</sub> , 1 <sub>56</sub> , 2 <sub>16</sub> , 3 <sub>4</sub> , 4 <sub>10</sub> , 5 <sub>4</sub> , 8 <sub>1</sub> , 14 <sub>4</sub> , 32 <sub>1</sub>	136	0 <sub>191</sub> , 1 <sub>30</sub> , 2 <sub>3</sub> , 3 <sub>3</sub> , 4 <sub>12</sub> , 7 <sub>15</sub> , 10 <sub>1</sub> , 48 <sub>1</sub>
86	0 <sub>190</sub> , 1 <sub>10</sub> , 2 <sub>30</sub> , 4 <sub>16</sub> , 5 <sub>3</sub> , 9 <sub>2</sub> , 10 <sub>2</sub> , 16 <sub>2</sub> , 37 <sub>1</sub>	137	0 <sub>154</sub> , 1 <sub>51</sub> , 2 <sub>26</sub> , 3 <sub>8</sub> , 4 <sub>6</sub> , 6 <sub>2</sub> , 7 <sub>4</sub> , 10 <sub>4</sub> , 25 <sub>1</sub>
87	0 <sub>200</sub> , 1 <sub>9</sub> , 2 <sub>16</sub> , 4 <sub>24</sub> , 5 <sub>2</sub> , 13 <sub>4</sub> , 57 <sub>1</sub>	138	0 <sub>154</sub> , 1 <sub>51</sub> , 2 <sub>24</sub> , 3 <sub>14</sub> , 4 <sub>1</sub> , 6 <sub>5</sub> , 9 <sub>6</sub> , 27 <sub>1</sub>
88	0 <sub>176</sub> , 1 <sub>28</sub> , 2 <sub>16</sub> , 3 <sub>14</sub> , 4 <sub>12</sub> , 7 <sub>1</sub> , 8 <sub>4</sub> , 11 <sub>4</sub> , 23 <sub>1</sub>	139	0 <sub>183</sub> , 1 <sub>12</sub> , 2 <sub>31</sub> , 3 <sub>10</sub> , 5 <sub>10</sub> , 6 <sub>6</sub> , 12 <sub>3</sub> , 30 <sub>1</sub>
89	0 <sub>174</sub> , 1 <sub>30</sub> , 2 <sub>32</sub> , 4 <sub>4</sub> , 5 <sub>2</sub> , 6 <sub>6</sub> , 8 <sub>5</sub> , 14 <sub>2</sub> , 32 <sub>1</sub>	140	0 <sub>160</sub> , 1 <sub>36</sub> , 2 <sub>34</sub> , 3 <sub>9</sub> , 4 <sub>8</sub> , 6 <sub>4</sub> , 9 <sub>2</sub> , 12 <sub>2</sub> , 27 <sub>1</sub>
90	0 <sub>175</sub> , 1 <sub>24</sub> , 2 <sub>33</sub> , 3 <sub>4</sub> , 4 <sub>10</sub> , 6 <sub>2</sub> , 7 <sub>4</sub> , 8 <sub>1</sub> , 16 <sub>2</sub> , 34 <sub>1</sub>	141	0 <sub>212</sub> , 1 <sub>1</sub> , 3 <sub>14</sub> , 6 <sub>28</sub> , 45 <sub>1</sub>
91	0 <sub>168</sub> , 1 <sub>28</sub> , 2 <sub>44</sub> , 3 <sub>1</sub> , 4 <sub>2</sub> , 6 <sub>4</sub> , 7 <sub>2</sub> , 8 <sub>2</sub> , 12 <sub>4</sub> , 27 <sub>1</sub>	142	0 <sub>184</sub> , 1 <sub>43</sub> , 6 <sub>28</sub> , 45 <sub>1</sub>
92	0 <sub>175</sub> , 1 <sub>27</sub> , 2 <sub>31</sub> , 3 <sub>4</sub> , 4 <sub>8</sub> , 6 <sub>2</sub> , 8 <sub>1</sub> , 9 <sub>1</sub> , 10 <sub>6</sub> , 34 <sub>1</sub>	143	0 <sub>179</sub> , 1 <sub>14</sub> , 2 <sub>35</sub> , 3 <sub>15</sub> , 7 <sub>3</sub> , 8 <sub>8</sub> , 10 <sub>1</sub> , 32 <sub>1</sub>
93	0 <sub>170</sub> , 1 <sub>33</sub> , 2 <sub>26</sub> , 3 <sub>9</sub> , 4 <sub>4</sub> , 5 <sub>2</sub> , 6 <sub>6</sub> , 7 <sub>1</sub> , 9 <sub>1</sub> , 12 <sub>2</sub> , 15 <sub>1</sub> , 27 <sub>1</sub>	144	0 <sub>172</sub> , 1 <sub>9</sub> , 2 <sub>56</sub> , 3 <sub>6</sub> , 6 <sub>4</sub> , 8 <sub>8</sub> , 29 <sub>1</sub>
94	0 <sub>182</sub> , 1 <sub>20</sub> , 2 <sub>26</sub> , 3 <sub>8</sub> , 4 <sub>10</sub> , 5 <sub>2</sub> , 8 <sub>3</sub> , 10 <sub>1</sub> , 13 <sub>2</sub> , 16 <sub>1</sub> , 34 <sub>1</sub>	145	0 <sub>188</sub> , 1 <sub>37</sub> , 3 <sub>2</sub> , 6 <sub>28</sub> , 45 <sub>1</sub>
95	0 <sub>164</sub> , 1 <sub>41</sub> , 2 <sub>28</sub> , 3 <sub>6</sub> , 4 <sub>4</sub> , 5 <sub>4</sub> , 6 <sub>2</sub> , 7 <sub>2</sub> , 11 <sub>2</sub> , 14 <sub>2</sub> , 29 <sub>1</sub>	146	0 <sub>164</sub> , 1 <sub>21</sub> , 2 <sub>56</sub> , 3 <sub>2</sub> , 6 <sub>4</sub> , 8 <sub>8</sub> , 29 <sub>1</sub>
96	0 <sub>167</sub> , 1 <sub>40</sub> , 2 <sub>23</sub> , 3 <sub>7</sub> , 4 <sub>5</sub> , 5 <sub>5</sub> , 7 <sub>1</sub> , 8 <sub>4</sub> , 11 <sub>2</sub> , 14 <sub>1</sub> , 29 <sub>1</sub>		

### E. Invariants of Van den Nest, Dehaene, and De Moor

The following theorem is a key result obtained by VDD in [14] that presents a finite set of invariants which characterizes the LC equivalence class of any stabilizer state (i.e., functions that remain invariant under the action of all local Clifford transformations). We have chosen an adapted formulation of the theorem to group multiplication involving Pauli operators [see Eq. (3)], slightly different from VDD's original notation, which is based on the well-known equivalent formulation of the stabilizer formalism in terms of algebra over the field  $\mathbb{F}_2 = \text{GF}(2)$ , where arithmetic is performed modulo 2 and each stabilizing operator is identified with a  $2n$ -dimensional binary index operator.

*Theorem 1.* Let  $|\psi\rangle$  be a stabilizer state on  $n$  qubits corresponding to a stabilizer  $\mathcal{S}_{|\psi\rangle}$ . Let  $r \in \mathbb{N}_0$  and consider subsets  $\omega_k, \omega_{kl} \subseteq \{1, \dots, n\}$  for every  $k, l \in \{1, \dots, r\}$ , with  $k < l$ . Denote  $\Omega := (\omega_1, \omega_2, \dots, \omega_{12}, \omega_{13}, \dots)$  and let  $\mathcal{T}_{n,r}^\Omega(|\psi\rangle)$  be the set consisting of all tuples  $(s_1, \dots, s_r) \in \mathcal{S}_{|\psi\rangle} \cdots \mathcal{S}_{|\psi\rangle}$  satisfying

$$\text{supp}(s_k) = \omega_k, \quad \text{supp}(s_k s_l) = \omega_{kl}. \quad (3)$$

Then, (i)  $|\mathcal{T}_{n,r}^\Omega(|\psi\rangle)|$  is LC invariant and (ii) the LC equivalence class of  $|\psi\rangle$  is completely determined by the values of all invariants  $|\mathcal{T}_{n,r}^\Omega(|\psi\rangle)|$  (i.e., where  $r=n$ ).

VDD provide another family of support-related invariants, based on a second theorem with the same formulation than the one above, except for the substitution of conditions (3) by new constraints

$$\text{supp}(s_k) \subseteq \omega_k, \quad \text{supp}(s_k s_l) \subseteq \omega_{kl}. \quad (4)$$

These new LC invariants are the dimensions of certain vector spaces and, in principle, are more manageable from a computational point of view because they involve the generator matrix of the stabilizer and rank calculation. Nevertheless, we will focus our attention on the first family of invariants, since they suffice to solve the problem we address in this paper with no extra computational effort. To resort to the second family would be justified in case we had to use invariants with a high  $r$  value to achieve LC discrimination among graph states up to eight qubits. We refer the reader to Ref. [14] for a proof of Theorem 1 and the extension to the second family of LC invariants.

The invariants of Theorem 1 are the cardinalities of certain subsets  $\mathcal{T}_{n,r}^\Omega(|\psi\rangle)$  of  $\mathcal{S}_{|\psi\rangle} \cdots \mathcal{S}_{|\psi\rangle}$ , which are defined in terms of simple constraints (3) on the supports of the stabilizing operators. VDD pointed out that, for  $r=1$ , these invariants count the number of operators in the stabilizer with a prescribed support. Therefore, fixing  $r=1$ , for every possible support  $\omega_k \subseteq \{1, \dots, n\}$ , there is an invariant

$$|\{s \in \mathcal{S}_{|\psi\rangle} | \text{supp}(s) = \omega_k\}|. \quad (5)$$

That is, the invariants for  $r=1$  are the  $A_{\omega_k}(|\psi\rangle)$ , i.e., the cardinalities of the equivalence classes  $[\omega_k]$  of the stabilizer. The number of possible supports in a stabilizer of an  $n$ -qubit state is equal to  $2^n$  and, therefore, there are  $2^n$  VDD's invariants for  $r=1$ . Many of them could be equal to zero. In fact, when dealing specifically with graph states, it can be easily seen that  $A_{\omega_k}(|\psi\rangle) = 0$  when referred to supports fulfilling  $|\omega_k| = 1$  because stabilizing operators of weight 1 are not

present in the stabilizer of a graph state due to the inherent connectivity of the graphs associated to the states that rules out isolated vertices.

On the other hand, VDD consider the invariants  $A_{\omega_k}(|\psi\rangle)$  as "local versions" of the so-called weight distribution of a stabilizer, a concept frequently used in classical and quantum coding theory. For  $r \geq 2$ , the new series of invariants involve  $r$ -tuples of stabilizing operators and their corresponding supports and constitute a generalization of the weight distribution. Let us denote

$$A_d(|\psi\rangle) = \sum_{\omega, |\omega|=d} A_\omega(|\psi\rangle), \quad (6)$$

the number of stabilizing operators with weight equal to  $d$ . According to this notation, the weight distribution of a stabilizer is the  $(n+1)$ -tuple

$$W_{|\psi\rangle} = \{A_d(|\psi\rangle)\}_{d=0}^n. \quad (7)$$

In principle,  $W_{|\psi\rangle}$  could be a compact way to present the whole information about the invariants  $A_\omega(|\psi\rangle)$ , i.e., VDD's invariants with  $r=1$ . This question will be addressed later.

In order to clarify the content of VDD's theorem, let us briefly discuss the way it works when applied to a particular graph state. We have chosen the three-qubit linear cluster state,  $|\text{LC}_3\rangle$ , because of its simplicity, combined with a sufficient richness in the stabilizer structure. Table I shows the stabilizer of  $|\text{LC}_3\rangle$  with its eight stabilizing operators,  $\{s_1, \dots, s_8\}$ . Three of them ( $s_1 = g_1, s_2 = g_2$ , and  $s_3 = g_3$ ) constitute a generator.  $|\text{LC}_3\rangle$  is a three-qubit graph state, so there are  $2^3 = 8$  possible supports (8 being the number of subsets in the set  $\{1, 2, 3\}$ ):

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}. \quad (8)$$

VDD's invariants for  $r=1$ . In this case,  $\Omega = (\omega_1)$ . By  $\Omega$ , we denote each of all the possible ways to choose a single support  $\omega_1$ , so there are eight choices for  $\Omega$ , which are those listed in Eq. (8). Given a particular choice of  $\Omega = (\omega_1)$ , the set  $\mathcal{T}_{n,1}^\Omega(|\text{LC}_3\rangle)$  contains all stabilizing operators  $s_1$  for the  $|\text{LC}_3\rangle$  fulfilling

$$\text{supp}(s_1) = \omega_1, \quad (9)$$

so, as a matter of fact,  $\mathcal{T}_{n,1}^\Omega(|\text{LC}_3\rangle)$  is the equivalence class  $[\omega_1]$  associated to the support  $\omega_1$ . Only five out of the eight possible supports are in fact present in the stabilizer of the  $|\text{LC}_3\rangle$  (see the column "Support" in Table I) and, therefore, we can distinguish between five nonempty equivalence classes  $[\omega]$ . According to VDD's theorem, the LC invariants for  $r=1$ ,  $|\mathcal{T}_{n,1}^\Omega(|\text{LC}_3\rangle)|$ , are the cardinalities  $A_\omega(|\text{LC}_3\rangle)$  of such equivalence classes  $[\omega]$ , namely,

$$A_{\{\emptyset\}}(|\text{LC}_3\rangle) = 1, \quad (10a)$$

$$A_{\{1\}}(|\text{LC}_3\rangle) = 0, \quad (10b)$$

$$A_{\{2\}}(|\text{LC}_3\rangle) = 0, \quad (10c)$$

$$A_{\{3\}}(|\text{LC}_3\rangle) = 0, \quad (10d)$$

$$A_{\{1,2\}}(|LC_3\rangle) = 1, \tag{10e}$$

$$A_{\{1,3\}}(|LC_3\rangle) = 1, \tag{10f}$$

$$A_{\{2,3\}}(|LC_3\rangle) = 1, \tag{10g}$$

$$A_{\{1,2,3\}}(|LC_3\rangle) = 4. \tag{10h}$$

VDD’s invariants for  $r=2$ . In this case,  $\Omega=(\omega_1, \omega_2; \omega_{12})$ . By  $\Omega$  we denote each of all the possible different ways to choose two supports  $\omega_1, \omega_2$ , and then a third support  $\omega_{12}$ . Let  $M=2^n$  be the number of possible supports and  $n$  being the number of qubits. On one hand, there are  $\binom{M}{2}$  different combinations of two supports  $(\omega_1, \omega_2)$ , plus  $M$  couples of the form  $(\omega_1, \omega_2 = \omega_1)$ . On the other hand, there are  $M$  possible choices for  $\omega_{12}$ . As a consequence, there are  $M[M + \binom{M}{2}]$  ways to choose  $\Omega$ . For  $n=3$ , this number is 288. Given a particular choice of  $\Omega=(\omega_1, \omega_2; \omega_{12})$ , the set  $\mathcal{T}_{n,2}^\Omega(|LC_3\rangle)$  contains all the two-tuples of the stabilizing operators  $(s_1, s_2)$  of the  $|LC_3\rangle$  fulfilling

$$\text{supp}(s_1) = \omega_1, \quad \text{supp}(s_2) = \omega_2, \quad \text{supp}(s_1 s_2) = \omega_{12}. \tag{11}$$

Many of these sets  $\mathcal{T}_{n,2}^\Omega(|LC_3\rangle)$  could be empty because the stabilizer fails to fulfill any of the conditions (11). The cardinalities of the 288 sets,  $|\mathcal{T}_{n,2}^\Omega(|LC_3\rangle)|$ , are the VDD’s invariants that we are interested in. For instance, if we choose  $\Omega=(\omega_1, \omega_2; \omega_{12})$  such that

$$\omega_1 = \{1, 2\}, \quad \omega_2 = \{1, 2, 3\}, \quad \omega_{12} = \{1, 2, 3\}, \tag{12}$$

then, according to the information in Table I, there is only one operator with support  $\omega_1$ , namely,  $s_1$ , and four operators with support  $\omega_2$ :  $s_2, s_5, s_7$ , and  $s_8$ . We obtain  $\mathcal{T}_{n,2}^\Omega(|LC_3\rangle) = \{(s_1, s_2), (s_1, s_5), (s_1, s_7), (s_1, s_8)\}$  because these four two-tuples verify conditions (11) and the value of the corresponding VDD’s invariant is the cardinality of the set,  $|\mathcal{T}_{n,2}^\Omega(|LC_3\rangle)| = 4$ .

Another example. If we choose  $\Omega$  such that  $\omega_1 = \{1, 2\}$ ,  $\omega_2 = \{2, 3\}$ , and  $\omega_{12} = \{1, 2, 3\}$ , then the VDD’s invariant is  $|\mathcal{T}_{n,2}^\Omega(|LC_3\rangle)| = 0$  because the two-tuple  $(s_1, s_3)$  defined by the supports  $\omega_1$  and  $\omega_2$  fulfills  $s_1 s_3 = s_6$  and  $s_6$  does not match with support  $\omega_{12}$ .

### III. RESULTS

The number of VDD’s invariants for an  $n$ -qubit graph state grows very rapidly with  $r$  (and, of course, with  $n$ ). If  $n=3$ , there are eight invariants for  $r=1$  and 288 invariants for  $r=2$ . For an eight-qubit graph state, there are 256 invariants for  $r=1$  and 8 421 376 for  $r=2$ . Obviously, the problem of calculating all the VDD’s invariants for graph states up to eight qubits becomes completely unfeasible if there are no restrictions on  $r$ . The total number of VDD’s invariants for a given  $n$ -qubit graph state, and all possible values of  $r$ , is  $M + \sum_{r=2}^n C'(M, r) C'(M, P)$ , where  $M=2^n$ ,  $P = \binom{M}{2}$ , and  $C'(M, r)$  denotes the combinations with repetition of  $M$  elements choose  $r$ . For  $n=7$ , this formula gives  $2.18 \times 10^{36}$ ; for  $n=8$ , it gives  $1.88 \times 10^{53}$ .

How many of them are needed to distinguish between all LC equivalence classes? VDD stated that “the LC equivalence class of  $|\psi\rangle$  is completely determined by the values of all invariants  $|\mathcal{T}_{n,n}^\Omega(|\psi\rangle)|$  (i.e., where  $r=n$ )” [14]. However, this number [i.e.,  $C'(M, r) C'(M, P)$  with  $r=n$ ] is still too large to be practical. For  $n=7$  is  $2.18 \times 10^{36}$  and for  $n=8$  is  $1.88 \times 10^{53}$  (i.e., most of the invariants correspond to the case  $r=n$ ). We are interested in the minimum value of  $r$  that yields a series of invariants sufficient to distinguish between all the 146 LC equivalence classes of graph states up to  $n=8$  qubits. In Ref. [14], the authors point out that there are examples of equivalence classes in stabilizer states which are characterized by invariants of small  $r$ ; for instance, those equivalent to GHZ states. In addition, they remark that a characterization based on small  $r$  values could be feasible, at least for some interesting subclasses or subsets of stabilizer states. We have calculated the VDD’s invariants for  $r=1$  for the 146 LC equivalence classes of graph states with up to  $n=8$  qubits. This implies calculating the cardinalities  $A_\omega(|\psi\rangle)$  of the corresponding equivalence classes  $[\omega]$  of the 146 representatives of the LC-equivalence classes, 30 060 invariants in total (since there are 1, 1, 2, 4, 11, 26, and 101 classes of two-, three-, four-, five-, six-, seven-, and eight-qubit graph states, respectively, and the number of VDD’s invariants with  $r=1$  is  $2^n$  for each class). Our results confirm the conjecture that invariants with  $r=1$  are enough for distinguishing between the 146 LC equivalence classes for graph states up to eight qubits. It is therefore unnecessary to resort to families of VDD’s invariants  $|\mathcal{T}_{n,r}^\Omega(|\psi\rangle)|$  with  $r \geq 2$ .

Our goal is not to show the values of these 30 060 invariants but to compress all this information and construct simple invariants from it. However, in order to do it properly, some requirements should be fulfilled. (I) The compacted information must be unambiguous and easily readable. (II) The compacted information must be LC invariant. (III) The compacted information concerning different LC equivalence classes must still distinguish between any of them.

Following the comments of VDD in Ref. [14] about considering the invariants  $A_\omega(|\psi\rangle)$  as “local versions” of the weight distribution  $W_{|\psi\rangle}$  of a stabilizer, we have calculated  $W_{|\psi\rangle}$  for the 146 LC classes of equivalence, according to definition (7). It can easily be seen that, if  $A_\omega(|\psi\rangle)$  is LC invariant, then  $W_{|\psi\rangle}$  is also LC invariant and permits a compact way to compress the information of the invariants  $A_\omega(|\psi\rangle)$ . Unfortunately,  $W_{|\psi\rangle}$  is not able to distinguish between any two LC classes of equivalence. Table II shows that the weight distribution fails to distinguish between LC classes starting from  $n=6$ . Graph states with labels 13 and 15 in Refs. [1,2] have the same weight distribution and this degeneration increases as the number of qubits grows, as we have checked out calculating  $W_{|\psi\rangle}$  for all graph states up to eight qubits.

Therefore, we must look for a way to compress the information about the invariants  $A_\omega(|\psi\rangle)$ , which satisfies (I)–(III). The fact that the stabilizing operators of a stabilizer can be classified into equivalence classes according to their supports (equivalence classes  $[\omega]$ ), and that the cardinalities of such classes  $[\omega]$  are the invariants  $A_\omega(|\psi\rangle)$ , leads us to introduce two definitions. Two classes  $[\omega_1]$  and  $[\omega_2]$  are equipotent if and only if both have the same cardinality, i.e.,  $A_{\omega_1}(|\psi\rangle)$

$=A_{\omega_2}(|\psi\rangle)$ , regardless of whether their stabilizing operators have different weights  $|\omega_1| \neq |\omega_2|$  or not. It is clear that the number of equipotent equivalence classes  $[\omega]$  for a given cardinality  $A_{\omega}(|\psi\rangle)$  is LC invariant. We will call it the  $A_{\omega}$  multiplicity (or  $A_{\omega}$  potency) and denote it by  $M(A_{\omega})$ . For instance, if we take a look at the list of invariants  $A_{\omega}(|\text{LC}_3\rangle)$  [see Eqs. (10a)–(10h)] we find that the value 0 appears three times (so there are three equivalence classes  $[\omega]$  with that cardinality) and then  $M(0)=3$ . Using this criterion,  $M(1)=4$  and  $M(4)=1$  for the  $|\text{LC}_3\rangle$ .

If we tabulate the values of  $A_{\omega}(|\psi\rangle)$  together with the corresponding values of  $M(A_{\omega})$ , we obtain a two-index compact information, which is LC invariant and, more importantly, LC discriminant, as required. The results are shown in Tables III–V.

In Table V we can see that four numbers are enough to distinguish between all classes of graph states with  $n=8$  qubits: the multiplicities of the values 0, 1, 3, and 4. Indeed, in Tables III and IV we see that these four numbers are enough to distinguish between all classes of graph states with  $n \leq 8$  qubits.

#### IV. CONCLUSIONS

We have shown that, to decide which entanglement class a graph state of  $n \leq 8$  qubits belongs to, it is enough to cal-

culate four quantities. These four LC invariants characterize any LC class of  $n \leq 8$  qubits.

This result solves a problem raised in the classification of graph states of  $n \leq 8$  qubits developed in Refs. [1,2,12]. A compact set of invariants that characterize all inequivalent classes of graph states with a higher number of qubits can be obtained by applying the same strategy. This can be done numerically up to  $n=12$ , a number of qubits beyond the present experimental capability in the preparation of graph states [17].

We have also shown that the conjecture [18] that the list of LC invariants given in Eq. (4) is sufficient to characterize the LC equivalence classes of all stabilizer states, which is not true in general [1], is indeed true for graph states of  $n \leq 8$  qubits. Moreover, we have shown that, for graph states of  $n \leq 8$  qubits, the list of LC invariants given in Eq. (5), which is more restrictive than the list given in Eq. (4), is enough. This solves a problem suggested in [14], regarding the possibility of characterizing special subclasses of stabilizer states using subfamilies of invariants.

#### ACKNOWLEDGMENTS

The authors thank H. J. Briegel, O. Gühne, M. Hein, and M. Van den Nest for their help. A.C., A.J.L., and P.M. acknowledge support from Projects No. P06-FQM-02243, No. FIS2008-05596, and No. PAI-FQM-0239. J.R.P. acknowledges support from Projects No. P06-FQM-01649, No. MTM2008-05866-C03-01, and No. PAI-FQM-0164.

- 
- [1] M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [2] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, in *Quantum Computers, Algorithms and Chaos*, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS Press, Amsterdam, 2006).
- [3] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
- [4] D. Schlingemann and R. F. Werner, *Phys. Rev. A* **65**, 012308 (2001).
- [5] D. Schlingemann, *Quantum Inf. Comput.* **2**, 307 (2002).
- [6] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [7] W. Dür, G. Vidal, and J. I. Cirac, *Phys. Rev. A* **62**, 062314 (2000).
- [8] M. Van den Nest, J. Dehaene, and B. De Moor, Proceedings of the 16th International Symposium on Mathematical Theory of Networks and Systems, Katholieke Universiteit Leuven, Belgium, 2004.
- [9] Z. Ji, J. Chen, Z. Wei, and M. Ying, e-print arXiv:0709.1266.
- [10] M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **71**, 062323 (2005).
- [11] B. Zeng, H. Chung, A. W. Cross, and I. L. Chuang, *Phys. Rev. A* **75**, 032325 (2007).
- [12] A. Cabello, A. J. López-Tarrida, P. Moreno, and J. R. Portillo, *Phys. Lett. A* **373**, 2219 (2009).
- [13] J. Eisert and H. J. Briegel, *Phys. Rev. A* **64**, 022306 (2001).
- [14] M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **72**, 014307 (2005).
- [15] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
- [16] M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **69**, 022316 (2004).
- [17] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, e-print arXiv:0809.4277.
- [18] A. Bouchet, *Discrete Math.* **114**, 75 (1993).



**All-versus-nothing proofs with  $n$  qubits distributed between  $m$  parties**

Adán Cabello\* and Pilar Moreno†

*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

(Received 30 September 2009; revised manuscript received 28 February 2010; published 27 April 2010)

All-versus-nothing (AVN) proofs show the conflict between Einstein, Podolsky, and Rosen's elements of reality and the perfect correlations of some quantum states. Given an  $n$ -qubit state distributed between  $m$  parties, we provide a method with which to decide whether this distribution allows an  $m$ -partite AVN proof specific for this state using only single-qubit measurements. We apply this method to some recently obtained  $n$ -qubit  $m$ -particle states. In addition, we provide all inequivalent AVN proofs with less than nine qubits and a minimum number of parties.

DOI: [10.1103/PhysRevA.81.042110](https://doi.org/10.1103/PhysRevA.81.042110)

PACS number(s): 03.65.Ud, 03.67.Mn, 42.50.Xa

**I. INTRODUCTION**

Einstein, Podolsky, and Rosen (EPR) showed that quantum mechanics is incomplete in the sense that not every element of reality has a counterpart inside the theory [1]. EPR proposed the following criterion to identify an element of reality: "If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity" [1]. In practice, nondisturbance can be guaranteed when the measurements are performed on distant systems. Predictions with certainty are possible for states having perfect correlations. A quantum state  $\rho$  has  $p$  perfect correlations when there are  $p$  different observables  $O_i$  such that  $\langle O_i \rangle_\rho = 1$ .

Thirty years after EPR's paper, Bell proved that there is an irresolvable conflict between EPR's elements of reality and quantum mechanics [2]. All-versus-nothing (AVN) proofs are the most direct way to reveal this conflict. An AVN proof is based on a set of  $s$  perfect correlations of a specific quantum state. The name "all-versus-nothing" [3] reflects one particular feature of these proofs: If one assumes EPR elements of reality, then  $s - q$  of these perfect correlations lead to a conclusion that is the opposite of the one obtained from a subset of the other  $q$  perfect correlations. If all  $s$  correlations are essential to obtain a contradiction (i.e., if the contradiction vanishes when we remove one of them), then the AVN proof is said to be critical.

The first AVN proof was obtained by Heywood and Redhead [4]. However, the most famous AVN proof is Greenberger, Horne, and Zeilinger's (GHZ) [5–7]. The first bipartite AVN proof with qubits is in Refs. [8,9]. The first bipartite AVN proof with qubits and using only single-qubit measurements is in Refs. [10,11]. The interest of the case in which the parties are restricted to perform single-qubit measurements is motivated by the practical difficulty of making general  $N$ -qubit measurements ( $N \geq 2$ ) when the qubits are encoded in different degrees of freedom of the same particle.

Recently, several  $n$ -qubit  $m$ -particle states ( $n > m$ ) having perfect correlations have been experimentally prepared, for instance, 4-qubit two-photon [12], 6-qubit two-photon [13,14], 6-qubit four-photon [15], 8-qubit four-photon [16], and 10-qubit five-photon graph states [16].

For these  $n$ -qubit  $m$ -particle states, a natural problem is the following: Consider  $m$  distant parties; party  $i$  can perform single-qubit measurements on particle  $i$ , and particle  $i$  contains  $n_i \geq 1$  qubits ( $\sum_{i=1}^m n_i = n$ ); which  $n$ -qubit  $m$ -particle states allow  $m$ -partite AVN proofs? This problem has been solved for the case of  $m = 2$  particles or parties [17]. In this article, we address the problem for an arbitrary number  $m$  of particles or parties.

The article is organized as follows: In Sec. II, we show that there is an equivalence between pure states allowing AVN proofs and graph states. This will simplify the task of finding all inequivalent  $n$ -qubit  $m$ -partite AVN proofs.

An  $m$ -partite AVN proof is specific for an  $n$ -qubit  $m$ -particle graph state when there is no graph state with fewer qubits satisfying the same correlations. In Sec. III, we discuss the requirements of an  $m$ -partite AVN proof to be specific for an  $n$ -qubit  $m$ -particle graph state and describe a method to decide whether a given  $n$ -qubit  $m$ -particle graph state allows a specific  $m$ -partite AVN proof. We apply this method to decide whether some  $n$ -qubit  $m$ -particle graph states recently prepared in the laboratory allow  $m$ -partite AVN proofs. As supplementary material [18], we provide a computer program to decide whether a given  $n$ -qubit  $m$ -particle graph state allows a specific  $m$ -partite AVN proof.

In Sec. IV we solve the following problem: Given an  $n$ -qubit graph state, what is the minimum number  $m$  of parties that allows a specific  $m$ -partite AVN proof. As supplementary material [18], we provide a computer program to obtain, given an  $n$ -qubit graph state, all distributions between  $m$  parties and all distributions between a minimum number of parties which allow AVN proofs.

The solution of the previous problem allows us to obtain all inequivalent distributions allowing AVN proofs since any distribution obtained from one allowing a specific AVN proof by giving qubits that originally belong to the same party to new parties will also allow an AVN proof. As supplementary material, we provide all inequivalent distributions between a minimum number  $m$  of parties allowing specific  $m$ -partite AVN proofs for all  $n$ -qubit graph states of  $n \leq 8$  qubits [19].

\*adan@us.es

†mpmoreno@us.es

## II. AVN PROOFS AND GRAPH STATES

### A. AVN proofs and stabilizer states

An AVN proof requires an  $n$ -qubit quantum state distributed between  $m$  parties. This state has a set of perfect correlations between the results of single-qubit measurements. These correlations must satisfy two requirements. First, they must allow us to define  $m$ -partite EPR's elements of reality. This means that every single-qubit observable involved in the AVN proof must satisfy EPR's criterion of elements of reality (i.e., its value can be predicted with certainty using only the results of single-qubit measurements on distant particles). Second, they must lead to a contradiction when EPR's criterion of elements of reality is assumed. Therefore the conclusion of an AVN proof is that if the quantum predictions are correct, observables which satisfy EPR's condition cannot have predefined results since it is impossible to assign them values which simultaneously satisfy the perfect correlations predicted by quantum mechanics.

Perfect correlations are necessary to establish elements of reality and to prove that they are incompatible with quantum mechanics. Therefore the states which allow AVN proofs must be simultaneous eigenstates of a sufficient number of commuting  $n$ -fold tensor products of single-qubit operators. Indeed, the following observations lead us to the conclusion that without loss of generality, we can restrict our attention to a particular family of states.

Two different single-qubit operators  $A$  and  $B$  on the same qubit cannot commute. A necessary condition to make  $n$ -fold tensor products be commuting operators is to choose  $A$  and  $B$  to be anticommuting operators. Therefore, in an AVN proof, all single-qubit operators corresponding to the same qubit must be anticommuting operators. The maximum number of anticommuting single-qubit operators is three. Therefore, without loss of generality, we can restrict our attention to a specific set of three single-qubit anticommuting operators on each qubit, for example, the Pauli matrices  $X = \sigma_x$ ,  $Y = \sigma_y$ , and  $Z = \sigma_z$ . This leads us to the concept of stabilizer state. An  $n$ -qubit stabilizer state is the simultaneous eigenstate with eigenvalue 1 of a set of  $n$  independent commuting elements of the Pauli group (i.e., the group, under matrix multiplication, of all  $n$ -fold tensor products of  $X$ ,  $Y$ ,  $Z$  and the identity  $\mathbb{1}$ ). The  $n$  independent elements are called stabilizer generators and generate a maximally Abelian subgroup, the stabilizer group of the state [20]. The  $2^n$  elements of the stabilizer group are the stabilizing operators and provide all the perfect correlations of the stabilizer state.

A further simplification is possible since any stabilizer state is local Clifford equivalent (i.e., equivalent under the local unitary operations that map the Pauli group to itself under conjugation) to a graph state [21]. Therefore the problem of which  $n$ -qubit pure states and distributions of qubits between the parties allow  $m$ -partite AVN proofs is reduced to the problem of which  $n$ -qubit graph states and distributions allow  $m$ -partite AVN proofs.

### B. Graph states

A graph state [22] is a stabilizer state whose generators can be written with the help of a graph.  $|G\rangle$  is the  $n$ -qubit

state associated with the graph  $G$ , which gives a recipe both for preparing  $|G\rangle$  and for obtaining  $n$  stabilizer generators that uniquely determine  $|G\rangle$ . On one hand,  $G$  is a set of  $n$  vertices (each representing a qubit) connected by edges (each representing an Ising interaction between the connected qubits). On the other hand, the stabilizer generator  $g_i$  is obtained by looking at the vertex  $i$  of  $G$  and the set  $N(i)$  of vertices which are connected to  $i$  and is defined by

$$g_i = X_i \otimes_{j \in N(i)} Z_j, \quad (1)$$

where  $X_i$ ,  $Y_i$ , and  $Z_i$  denote the Pauli matrices acting on the  $i$ th qubit.  $|G\rangle$  is the only  $n$ -qubit state that fulfills

$$g_i |G\rangle = |G\rangle \quad \text{for } i = 1, \dots, n. \quad (2)$$

Therefore the stabilizer group is

$$S(|G\rangle) = \{s_j, j = 1, \dots, 2^n\}, \quad s_j = \prod_{i \in I_j(G)} g_i, \quad (3)$$

where  $I_j(G)$  denotes a subset of  $\{g_i\}_{i=1}^N$ . The stabilizing operators provide all the perfect correlations of  $|G\rangle$ :

$$\langle G | s_j | G \rangle = 1. \quad (4)$$

Graph states associated with connected graphs have been exhaustively classified. There is only 1 two-qubit graph state (equivalent to a Bell state), only 1 three-qubit graph state (equivalent to a GHZ state), and 2 four-qubit graph states (equivalent to a GHZ and a cluster state), 4 five-qubit graph states, 11 six-qubit graph states, 26 seven-qubit graph states [22], and 101 eight-qubit graph states [23].

## III. $n$ -QUBIT $m$ -PARTITE AVN PROOFS

### A. Specific $m$ -partite AVN proofs

The perfect correlations of any graph state associated with a connected graph of three or more vertices lead to contradictions with the concept of elements of reality when each qubit is distributed to a different party [17,24–26]. However, the first problem consists of finding whether these contradictions are specific to a given distribution of a graph state or, on the contrary, they can be obtained with a graph state of fewer qubits.

For example, take the four-party AVN proof based on the following four perfect correlations of the distribution of the four-qubit fully connected graph state  $|FC_4\rangle$  (a four-qubit GHZ state) in which each qubit belongs to a different party:

$$X_1 Z_2 Z_3 Z_4 = 1, \quad (5a)$$

$$Z_1 X_2 Z_3 Z_4 = 1, \quad (5b)$$

$$Z_1 Z_2 X_3 Z_4 = 1, \quad (5c)$$

$$-X_1 X_2 X_3 Z_4 = 1. \quad (5d)$$

This is an example of an AVN proof which is nonspecific for the state  $|FC_4\rangle$ , the reason being that neither the contradiction nor the definition of the elements of reality involved in this contradiction requires any choice from the party which has the fourth qubit. This party only has to measure  $Z_4$  and broadcast the result. The only role of the result of  $Z_4$  is to guarantee that  $X_1$ ,  $Z_1$ ,  $X_2$ ,  $Z_2$ ,  $X_3$ , and  $Z_3$  are elements of reality in a four-party scenario. However, the contradiction occurs for any

result of  $Z_4$ . It occurs because the following equations cannot be simultaneously satisfied:

$$X_1 Z_2 Z_3 = Z_1 X_2 Z_3 = Z_1 Z_2 X_3 = -X_1 X_2 X_3. \quad (6)$$

The particular value of  $Z_4$  is irrelevant. The same contradiction can be obtained using the perfect correlations of a three-qubit fully connected graph state  $|FC_3\rangle$  (a three-qubit GHZ state) distributed between three parties.

The next example illustrates that whether an AVN proof is specific can depend on the way in which the qubits are distributed between the parties. Consider the AVN proof based on the following four correlations of the four-qubit linear cluster state  $|LC_4\rangle$  associated with the graph where qubit 1 is connected to qubit 2, which is connected to qubit 3, which is connected to qubit 4:

$$Y_1 Y_2 Z_3 = 1, \quad (7a)$$

$$Z_1 X_2 Z_3 = 1, \quad (7b)$$

$$Z_1 Y_2 Y_3 Z_4 = 1, \quad (7c)$$

$$-Y_1 X_2 Y_3 Z_4 = 1. \quad (7d)$$

If the qubits are distributed so that each qubit goes to a different party, then the AVN proof is not specific since the party who has the fourth qubit does not need to make any choice, neither for the contradiction nor for the definition of the elements of reality. The contradiction

$$Y_1 Y_2 Z_3 = Z_1 X_2 Z_3 = Z_1 Y_2 Y_3 = -Y_1 X_2 Y_3 \quad (8)$$

can be obtained from the perfect correlations of a three-qubit linear cluster state  $|LC_3\rangle$  associated with the graph where qubit 1 is connected to qubit 2, which is connected to qubit 3.

However, if qubits 1 and 4 belong to Alice, and qubits 2 and 3 belong to Bob, then the only way to guarantee that, for example,  $X_2$  is an element of reality in this scenario (i.e., that its result can be predicted using only the results of measurements on Alice's side) is by using the following perfect correlation of the  $|LC_4\rangle$ :

$$Z_1 X_2 X_4 = 1. \quad (9)$$

Therefore the party who has qubit 4 must choose between at least two measurements. To sum up, an AVN proof is specific for a given distribution of a graph state when at least two observables of all the qubits are involved.

Since the additional correlations needed to define the elements of reality can (together with those already used for the contradiction) involve additional contradictions, it is appropriate that the observables needed to guarantee that other observables are elements of reality (like  $X_4$  and  $Z_4$  in the previous example) are themselves elements of reality. Therefore hereinafter we will focus on AVN proofs in which at least two of the observables of all the qubits are elements of reality. It can be easily seen that when two Pauli observables, for example,  $X_i$  and  $Y_i$ , are elements of reality, then the third Pauli observable,  $Z_i$ , is also an element of reality. Therefore we shall focus only on those graph states and distributions in which the three Pauli observables of each and every one of the qubits are elements of reality.

## B. When does a distribution allow a specific AVN proof ?

The next problem is, given a distribution of an  $n$ -qubit graph state between  $m$  parties, how to decide whether it is one in which all single-qubit Pauli observables are elements of reality. For that purpose, it is useful to note that the  $2^n$  perfect correlations (i.e., stabilizing operators) of an  $n$ -qubit graph state can be classified in four classes:

1. There are  $2^{n-2}$  stabilizing operators (i.e., a quarter of the stabilizing operators of the graph state) that allow us to predict  $X_i$  from the results of measurements on other qubits: those that are products of the stabilizer generator  $g_i$  [defined in Eq. (1)], an even number (hereinafter "even" includes zero) of  $g_j$  with  $j \in N(i)$ , and an arbitrary number (hereinafter "arbitrary number" includes zero) of  $g_k$  with  $k \neq i$  and  $k \notin N(i)$ .

2. There are  $2^{n-2}$  stabilizing operators that allow us to predict  $Y_i$  from the results of measurements on other qubits: those that are products of  $g_i$ , an odd number of  $g_j$  with  $j \in N(i)$ , and an arbitrary number of  $g_k$  with  $k \neq i$  and  $k \notin N(i)$ .

3. There are  $2^{n-2}$  stabilizing operators that allow us to predict  $Z_i$  from the results of measurements on other qubits: those that are products of an odd number of  $g_j$  with  $j \in N(i)$  and an arbitrary number of  $g_k$  with  $k \neq i$  and  $k \notin N(i)$ .

4. There are  $2^{n-2}$  stabilizing operators that contain  $\mathbb{1}_i$ : those that are products of an even number of  $g_j$  with  $j \in N(i)$  and an arbitrary number of  $g_k$  with  $k \neq i$  and  $k \notin N(i)$ .

Each particle can carry more than one qubit. It is therefore convenient to denote as  $P(i)$  the set of qubits which are in the same particle as qubit  $i$ . The previous classification of the stabilizing operators is useful in the following sense: Given the distribution of an  $n$ -qubit graph state between  $m$  parties,  $X_i$  is an element of reality if and only if there exists a stabilizing operator of the graph state which satisfies the following two requirements: (1) It does not contain  $g_j$  for all  $j \in P(i)$  but contains an even number of  $g_k$  with  $k \in N(j)$  and (2) it contains  $g_i$  and an even number of  $g_l$  with  $l \in N(i)$ . For instance, consider the four-qubit linear cluster state  $|LC_4\rangle$  associated with the graph where qubit 1 is connected to qubit 2, which is connected to qubit 3, which is connected to qubit 4, distributed such that Alice has qubits 1 and 4 and Bob has qubits 2 and 3. The question is, is  $X_1$  an element of reality? This is equivalent to the question, is there a stabilizing operator such that it does not contain  $g_4$  [since  $P(1) = \{4\}$ ] but contains an even number (necessarily zero) of  $g_3$  [since  $N(4) = \{3\}$ ] and  $g_1$  and an even number (necessarily zero) of  $g_2$  [since  $N(1) = \{2\}$ ]? The answer is yes; the only stabilizing operator with these properties is  $g_1 = X_1 Z_2$ .

Similarly,  $Y_i$  is an element of reality if and only if there is a stabilizing operator satisfying (1) and the following condition: (3) It contains  $g_i$  and an odd number of  $g_l$  with  $l \in N(i)$ .

Finally,  $Z_i$  is an element of reality if and only if there is a stabilizing operator satisfying (1) and the following condition: (4) It does not contain  $g_i$  but contains an odd number of  $g_l$  with  $l \in N(i)$ .

To decide whether a specific distribution allows a specific AVN proof, we first focus on qubit  $i$  and test whether  $X_i$  and  $Y_i$  are elements of reality. If either is not an element of reality, then the distribution does not allow a specific AVN proof. If both are elements of reality, then we test whether  $X_j$  and  $Y_j$  of qubit  $j$  are elements of reality, and so on for all the qubits.

If all  $X_i$  and  $Y_i$  are elements of reality, then the distribution allows a specific AVN proof.

Indeed, there are simple cases where it can easily be seen that a distribution does not allow an AVN proof. For example, if more than  $n/2$  qubits are carried by the same particle, for qubits of the particle with more than  $n/2$  qubits, either requirement (1) is incompatible with (2), or (1) is incompatible with (3) and (4). An alternative proof will be provided in Sec. IV. If there is a qubit  $i$  such that  $N(i) \in P(i)$  (i.e., if in the graph representing the state, qubit  $i$  is connected only to qubits of the same particle), requirement (1) is incompatible with requirements (3) and (4). As supplementary material [18], we provide a computer program to decide whether a given  $n$ -qubit  $m$ -particle graph state allows a specific  $m$ -partite AVN proof.

### C. Examples

As an example of the application of these rules, it is interesting to discuss whether some recently prepared 6-qubit two- and four-particle states allow specific AVN proofs, assuming the natural scenario in which each party has one particle.

Figure 1 contains several possible distributions of a six-qubit linear cluster state  $|LC_6\rangle$ . Figure 1(a) represents the four-photon  $|LC_6\rangle$  prepared in Ref. [15]. This distribution does not allow a specific AVN proof since qubit 1 is connected only to qubit 2 and qubit 6 is connected only to qubit 5.

Figure 1(b) represents the two-photon  $|LC_6\rangle$  prepared in Ref. [14]. This distribution satisfies all the requirements and thus allows a specific AVN proof. Indeed, Fig. 1(b)

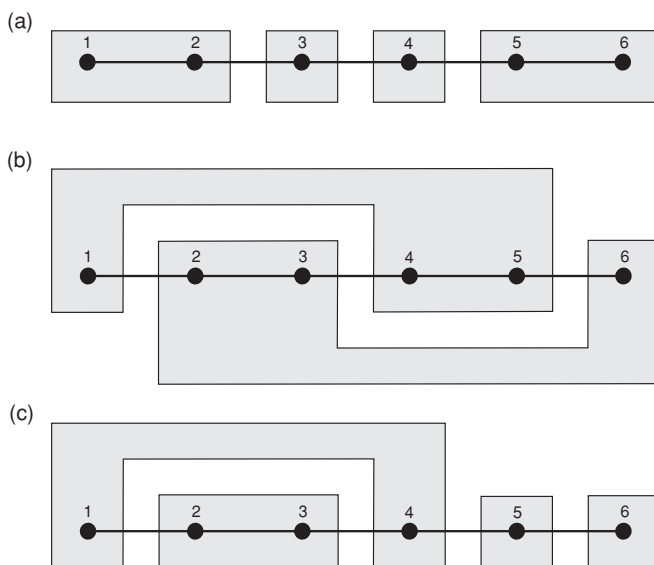


FIG. 1. Different distributions of a six-qubit linear cluster state  $|LC_6\rangle$  between two and four particles. Each gray area represents a particle. (a) Corresponds to the four-photon state prepared in Ref. [15]. (b) Corresponds to the two-photon state prepared in Ref. [14]. In (a), not all single-qubit Pauli observables are EPR elements of reality, and therefore no AVN proof is possible. (b) and (c) Allow AVN proofs.

represents the only bipartite distribution of the six-qubit linear cluster state which allows a specific AVN proof [17]. Some distributions of  $|LC_6\rangle$  in four particles allowing AVN proofs can be trivially obtained from Fig. 1(b) by splitting qubits that belong to the same particle into several particles. For instance, a distribution allowing a specific AVN proof is illustrated in Fig. 1(c). It can be easily seen that there is no distribution in four particles which allows a specific AVN proof which cannot be obtained from the distribution in Fig. 1(b).

Figure 2 contains several possible distributions of a six-qubit  $Y$ -graph state  $|Y_6\rangle$ . Figure 2(a) represents the four-photon  $|Y_6\rangle$  prepared in Ref. [15]. This distribution does not allow a specific AVN proof since qubit 1 is connected only to qubit 2 and qubit 5 is connected only to qubit 4. Figures 2(b)–2(d) represent distributions of  $|Y_6\rangle$  between four particles allowing specific AVN proofs.

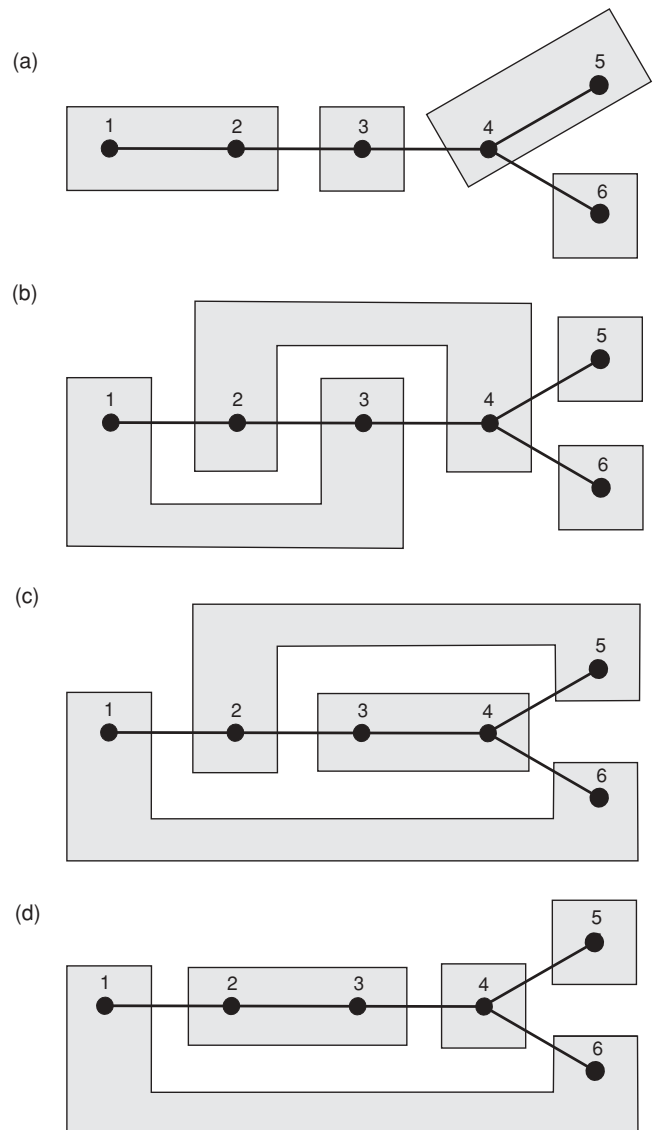


FIG. 2. Different distributions of the six-qubit  $Y$ -graph state between four particles. (a) Corresponds to the state prepared in Ref. [15] and does not allow a specific AVN proof. (b)–(d) Allow specific AVN proofs.

**IV. AVN PROOFS WITH A MINIMUM NUMBER  $m$  OF PARTIES**

**A. Possible distributions between a minimum number of parties**

In the previous section, we have seen that  $|Y_6\rangle$  admits specific AVN proofs when their qubits are suitably distributed between four particles. The question is whether  $|Y_6\rangle$  admits specific AVN proofs when it is distributed between three particles or less, or more generally speaking, the question is, given an  $n$ -qubit graph state, what is the minimum number of parties  $m$  which allows  $m$ -partite AVN proofs specific for this state?

The following definition will be useful for solving this problem. Let us define the reduced stabilizer of particle  $A$ 's qubits as the one obtained from the stabilizer of the original state by replacing the observables on all other particles' qubits with identity matrices.

*Lemma:* A distribution of  $n = n_{\max} + n_B + \dots + n_m$  qubits between  $m$  parties such that  $n_{\max} \geq n_B \geq \dots \geq n_m$  allows  $m$ -partite elements of reality if and only if  $n_{\max} \leq n_B + \dots + n_m$ .

*Proof:* Suppose that particle  $m_i$  carries qubits  $1, \dots, n_{\max}$ , where  $n_{\max}$  is the maximum number of qubits carried by any particle, and that particle  $m_j$  carries qubits  $n_{\max} + 1, \dots, n_{\max} + n_j$ . If  $X_1, Y_1, Z_1, X_2, \dots, Z_{n_{\max}}$  are elements of reality, then the reduced stabilizer of  $m_i$ 's qubits must contain

$$X_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_{\max}}, \tag{10a}$$

$$Y_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_{\max}}, \tag{10b}$$

$$Z_1 \otimes \mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_{n_{\max}}, \tag{10c}$$

$$\mathbb{1}_1 \otimes X_2 \otimes \dots \otimes \mathbb{1}_{n_{\max}}, \dots, \tag{10d}$$

$$\mathbb{1}_1 \otimes \mathbb{1}_2 \otimes \dots \otimes Z_{n_{\max}}. \tag{10e}$$

Moreover, the reduced stabilizer of  $m_i$ 's qubits must contain all possible products of Eqs. (10a)–(10e), that is, all possible variations with repetition of the four elements  $\mathbb{1}, X, Y,$  and  $Z$ , choosing  $n_i$ , which are  $4^{n_{\max}} = 2^{2n_{\max}}$ . A similar reasoning applies to the three Pauli matrices of each and every one of  $m_j$ 's qubits. Therefore the reduced stabilizer of  $m_j$ 's qubits must also contain all possible products of

$$X_{n_{\max}+1} \otimes \mathbb{1}_{n_{\max}+2} \otimes \dots \otimes \mathbb{1}_{n_{\max}+n_j}, \dots, \tag{11a}$$

$$\mathbb{1}_{n_{\max}+1} \otimes \mathbb{1}_{n_{\max}+2} \otimes \dots \otimes Z_{n_i+n_j}, \tag{11b}$$

which are  $4^{n_j} = 2^{2n_j}$ . However, the reduced stabilizer of the sum of the parties  $m_i$  and  $m_j$  has only  $2^{n_{\max}+n_j}$  terms; therefore the only possibility is that  $n_{\max} = n_j$ . ■

Given an  $n$ -qubit graph state,  $n_{\max}$  restricts the possible minimum numbers of particles and the possible numbers of qubits per particle. Given  $n$ , Table I presents the possible minimum numbers of particles and the corresponding possible distributions. Other possible distributions are already contained between those in Table I, but in those cases, the number of particles is not the minimum.

A corollary of the lemma is that there are no specific AVN proofs in which one particle has more than  $n/2$  qubits (this result was used in Sec. III).

TABLE I. Possible distributions of an  $n$ -qubit graph state between a minimum number  $m$  of particles. For instance, (2,2,1) denotes a distribution of  $n = 5$  qubits between  $m = 3$  particles such that particles 1 and 2 have two qubits each and particle 3 has one qubit.

$n$	$m$	Distribution
2	2	(1,1)
3	3	(1,1,1)
4	2	(2,2)
	4	(1,1,1,1)
5	3	(2,2,1)
	5	(1,1,1,1,1)
6	2	(3,3)
	3	(2,2,2)
	4	(2,2,1,1)
	6	(1,1,1,1,1,1)
7	3	(3,3,1), (3,2,2)
	4	(2,2,2,1)
	5	(2,2,1,1,1)
	7	(1,1,1,1,1,1,1)
8	2	(4,4)
	3	(3,3,2)
	4	(3,3,1,1), (3,2,2,1), (2,2,2,2)
	5	(2,2,2,1,1)
	6	(2,2,1,1,1,1)
	8	(1,1,1,1,1,1,1,1)

**B. AVN proofs with a minimum number of parties for any graph state**

Equipped with these tools, we can obtain all possible distributions with a minimum number of particles allowing specific AVN proofs for any graph state. We have obtained all which are inequivalent under single-qubit unitary operations for all graph states up to  $n = 8$  qubits. For this purpose, we used the classification of graph states up to  $n = 7$  qubits proposed in Ref. [22] and the classification of eight-qubit graph states proposed in Ref. [23]. Given an  $n$ -qubit graph state, to obtain all the distributions between a minimum number of parties allowing specific AVN proofs, we can use Table I in the following way. Suppose that  $n = 6$ . We first test whether AVN proofs are possible for the simplest distributions permitted by Table I, that is,  $m = 2$  parties with three qubits each. If no AVN proof is possible, then we test whether there are AVN proofs for the next possible distributions permitted by Table I, that is,  $m = 3$  parties with two qubits each, and so on.

Applying this method, we have obtained all inequivalent distributions between a minimum number of particles for all graph states with up to eight qubits. In the supplementary material [19], we show all distributions between a minimum number of particles for the 19 classes of graph states with up to six qubits, the 26 classes of graph states with seven qubits, and the 101 classes of graph states with eight qubits. In addition, we provide as supplementary material [18] a computer program to obtain, given an  $n$ -qubit graph state, all distributions between  $m$  parties and all distributions between a minimum number of parties which allow AVN proofs.

## V. CONCLUSIONS

We have developed tools with which to decide whether a distribution of  $n$  qubits between  $m$  parties allows an  $m$ -partite AVN proof specific for this distribution (i.e., which cannot be obtained using a state with fewer qubits). As a result, we have obtained all inequivalent  $m$ -partite AVN proofs using  $n$ -qubit  $m$ -particle quantum states with  $n < 9$  qubits and a minimum number  $m$  of parties. This enables us to obtain all inequivalent  $m$ -partite AVN proofs using  $n$ -qubit  $m$ -particle quantum states with  $n < 9$  qubits with an arbitrary number of parties.

The motivation of this work was to answer some natural questions raised by recent experimental developments allowing the preparation in the laboratory of graph states of several particles, each carrying several qubits. The results presented

in this article provide tools to help experimentalists to design tests of new AVN proofs and new Bell inequalities based on these AVN proofs [7,10,27], similar to those reported in Refs. [12,14] for specific states but exploiting the possibility of experimentally preparing new classes of graph states.

## ACKNOWLEDGMENTS

The authors thank W.-B. Gao, O. Gühne, and A. J. López Tarrida for their useful comments and M. Hein, J. Eisert, and H. J. Briegel for their permission for reproducing two figures of Ref. [20] in the supplementary material to this article. The authors acknowledge support from Project Nos. P06-FQM-02243 and FIS2008-05596.

- 
- [1] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
  - [2] J. S. Bell, *Physics* (Long Island City, NY) **1**, 195 (1964).
  - [3] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
  - [4] P. Heywood and M. L. G. Redhead, *Found. Phys.* **13**, 481 (1983).
  - [5] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), p. 69.
  - [6] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).
  - [7] N. D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
  - [8] A. Cabello, *Phys. Rev. Lett.* **86**, 1911 (2001).
  - [9] A. Cabello, *Phys. Rev. Lett.* **87**, 010403 (2001).
  - [10] A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).
  - [11] A. Cabello, *Phys. Rev. A* **72**, 050101(R) (2005).
  - [12] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini, and V. Berardi, *Phys. Rev. Lett.* **98**, 180502 (2007).
  - [13] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, *Phys. Rev. Lett.* **95**, 260501 (2005).
  - [14] R. Ceccarelli, G. Vallone, F. De Martini, P. Mataloni, and A. Cabello, *Phys. Rev. Lett.* **103**, 160401 (2009).
  - [15] W.-B. Gao, X.-C. Yao, P. Xu, O. Gühne, A. Cabello, C.-Y. Lu, C.-Z. Peng, T. Yang, Z.-B. Chen, and J.-W. Pan, e-print [arXiv:0906.3390](https://arxiv.org/abs/0906.3390) (2009).
  - [16] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, *Nat. Phys.* doi:10.1038/nphys1603 (2010).
  - [17] A. Cabello and P. Moreno, *Phys. Rev. Lett.* **99**, 220402 (2007).
  - [18] See supplementary material at <http://link.aps.org/supplemental/10.1103/PhysRevA.81.042110> for a computer program in MATHEMATICA.
  - [19] See supplementary material at <http://link.aps.org/supplemental/10.1103/PhysRevA.81.042110> for all inequivalent distributions between a minimum number  $m$  of parties allowing specific  $m$ -partite AVN proofs for all  $n$ -qubit graph states of  $n \leq 8$  qubits.
  - [20] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
  - [21] M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **69**, 022316 (2004).
  - [22] M. Hein, J. Eisert, and H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
  - [23] A. Cabello, A. J. López Tarrida, P. Moreno, and J. R. Portillo, *Phys. Lett. A* **373**, 2219 (2009).
  - [24] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H. J. Briegel, in *Quantum Computers, Algorithms and Chaos*, edited by G. Casati, D. L. Shepelyansky, P. Zoller, and G. Benenti (IOS Press, Amsterdam, 2006).
  - [25] D. P. DiVincenzo and A. Peres, *Phys. Rev. A* **55**, 4089 (1997).
  - [26] V. Scarani, A. Acín, E. Schenck, and M. Aspelmeyer, *Phys. Rev. A* **71**, 042325 (2005).
  - [27] A. Cabello, O. Gühne, and D. Rodríguez, *Phys. Rev. A* **77**, 062106 (2008).

# DEMOSTRACIONES BIPARTITAS “TODO O NADA” DEL TEOREMA DE BELL USANDO QUBITS

Adán Cabello y Pilar Moreno

Departamento de Física Aplicada II. Universidad de Sevilla. Avenida de Reina Mercedes s/n 41012 Sevilla (Spain)

adan@us.es

**Resumen:** Si distribuimos  $n$  qubits entre dos observadores, ¿qué estados puros y qué formas de distribuir los qubits permiten hacer demostraciones “todo o nada” (o de tipo Greenberger-Horne-Zeilinger) del teorema de Bell, usando sólo medidas sobre qubits individuales? Mostramos una condición necesaria y suficiente para que tales demostraciones sean posibles, y la aplicamos para obtener todas las demostraciones con menos de ocho qubits. Curiosamente, salvo transformaciones unitarias de un solo qubit, sólo existen un estado de cuatro qubits (distribuidos de una determinada manera) y seis estados de seis qubits (con una determinada distribución de qubits para cada estado) que permiten estas demostraciones.

## 1. Introducción

La demostración de Greenberger, Horne, y Zeilinger (GHZ) [1] es la primera demostración del teorema de Bell basada en las correlaciones perfectas que predice la Mecánica Cuántica para estados de  $n$  qubits. Estas demostraciones reciben el nombre de demostraciones “todo o nada” (TON) [2]. Sin embargo, mientras que la demostración de Bell necesitaba sólo dos observadores, la de GHZ necesita tres. La razón por la que un estado de GHZ de tres qubits no permite una demostración TON bipartita es que, si repartimos los tres qubits entre dos observadores, no existe ninguna razón física que justifique que los observables involucrados en la demostración de GHZ deban tener valores  $-1$  ó  $1$  en una teoría de variables ocultas locales, ya que dichos observables no satisfacen la *condición de elemento de realidad* de Einstein, Podolsky, y Rosen (EPR) [3] (i.e., su resultado no se puede predecir con certeza a partir de medidas hechas por el observador que no posee dicho qubit).

La primera demostración TON bipartita fue introducida en [4] y necesitaba cuatro qubits. Los cuatro qubits pueden codificarse en la polarización y el momento lineal de dos fotones [5]. De esta manera se ha verificado experimentalmente [6,7]. Una de las dificultades experimentales de la demostración [4] es que requiere medidas colectivas sobre dos qubits [8]. La primera demostración TON bipartita usando sólo medidas sobre qubits individuales fue introducida en [9] y ha sido recientemente verificada en el laboratorio usando la polarización y el momento lineal de dos fotones [10].

La posibilidad de codificar tres qubits en dos fotones [11] y la posibilidad de preparar estados de seis fotones entrelazados en polarización [12,13] lleva, de forma natural, al siguiente problema: Si distribuimos  $n$  qubits entre dos observadores ( $n_A$  para Alicia y  $n_B = n - n_A$  para Bob), ¿qué estados puros y qué formas de distribuir los qubits permiten hacer demostraciones TON bipartitas usando sólo medidas sobre qubits individuales?

## 2. Resultados

Cualquier demostración TON bipartita usando sólo medidas sobre qubits individuales necesita cumplir dos requisitos:

(a) Tienen que existir correlaciones perfectas que permitan predecir con certeza el resultado de las medidas de las tres matrices de Pauli de Alicia (Bob), a partir de medidas sobre los qubits de Bob (Alicia) [3].

(b) Tienen que existir correlaciones perfectas que no puedan satisfacerse si se supone que los observables de un qubit tienen valores definidos -1 o 1.

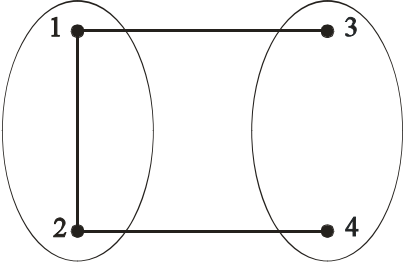
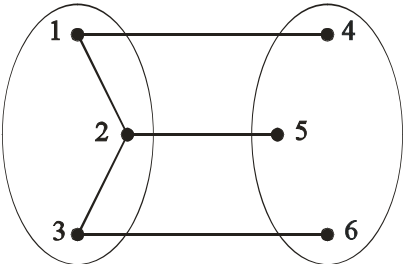
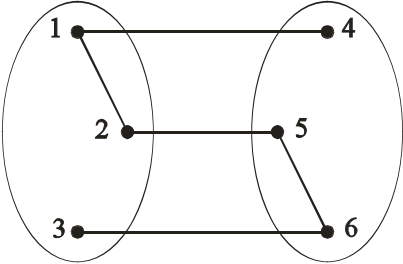
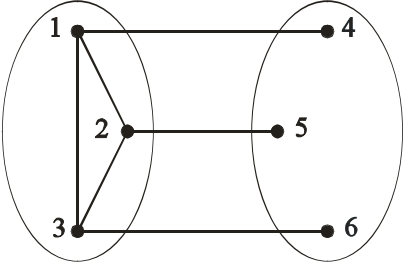
Por tanto, buscamos estados que sean autoestados de un número suficiente de operadores que sean producto tensorial de operadores de un solo qubit. Si nos restringimos al conjunto de operadores de un solo qubit formado por la identidad y las tres matrices de Pauli, entonces los estados que nos interesan son los *estados estabilizadores* [14]. Como cualquier estado estabilizador es equivalente bajo transformaciones Clifford locales a un estado grafo [15] (los *estados grafo* son un tipo particular de estados estabilizador cuyo generador se obtiene con ayuda de un grafo [16,17]), nuestro problema se reduce al de encontrar qué estados grafo de  $n$  qubits y qué formas de distribuir los qubits permiten hacer demostraciones TON bipartitas usando sólo medidas sobre qubits individuales.

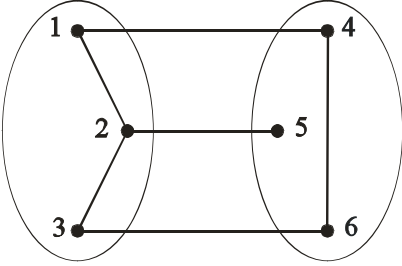
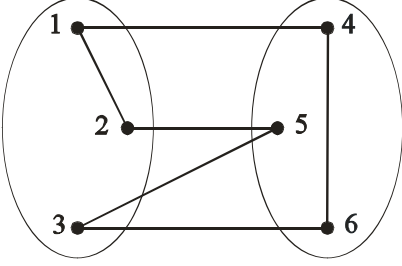
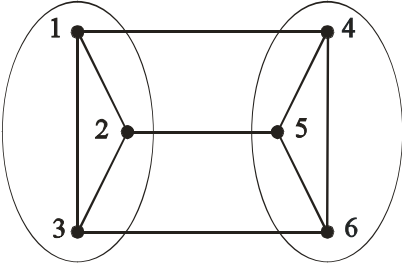
En principio es un problema complicado, puesto que existen 45 clases distintas de estados grafo asociados a grafos conexos de menos de 8 qubits [16,17], y centenares de posibles distribuciones de los qubits entre Alicia y Bob. Además, todos los estados grafo de tres o más qubits satisfacen (b), puesto que cualquiera de ellos contiene subgrafos conexos de tres vértices que representan estados GHZ de tres qubits [17]. Por lo tanto, el problema es averiguar para qué estados y distribuciones de qubits se satisface (a).

Nuestro principal resultado (que no demostraremos aquí) es que (a) se satisface si y sólo si  $n_A = n_B$  y el grupo estabilizador de los qubits de Alicia (Bob) contiene todas las variaciones con repetición de la identidad y las tres matrices de Pauli tomados de  $n_A$  en  $n_A$  (de  $n_B$  en  $n_B$ ), y ninguna de ellas repetida.

Aplicando este resultado hemos obtenido que, con menos de ocho qubits, sólo existen un estado grafo de cuatro qubits (distribuidos de una determinada manera) y seis estados grafo de seis qubits (con una determinada distribución de qubits para cada estado) que permiten demostraciones TON bipartitas. La demostración con cuatro qubits era ya conocida [9], las otras seis son nuevas. En la tabla se presentan los grafos asociados a los estados grafo y las distribuciones de qubits que permiten demostraciones TON bipartitas. Además, se indican las correlaciones perfectas que hacen que se satisfaga el requisito (a).



Grafo y distribución de qubits	Elementos de realidad de Alicia	Elementos de realidad de Bob
<p data-bbox="284 286 400 320"><b>No. 4a</b></p> 	$X_1 = Z_3 X_4$ $Y_1 = Y_3 X_4$ $Z_1 = X_3$ $X_2 = X_3 Z_4$ $Y_2 = X_3 Y_4$ $Z_2 = X_4$	$X_3 = Z_1$ $Y_3 = Y_1 Z_2$ $Z_3 = X_1 Z_2$ $X_4 = Z_2$ $Y_4 = Z_1 Y_2$ $Z_4 = Z_1 X_2$
<p data-bbox="284 656 421 689"><b>No. 13a</b></p> 	$X_1 = Z_4 X_5$ $Y_1 = Y_4 X_5$ $Z_1 = X_4$ $X_2 = X_4 Z_5 X_6$ $Y_2 = X_4 Y_5 X_6$ $Z_2 = X_5$ $X_3 = X_5 Z_6$ $Y_3 = X_5 Y_6$ $Z_3 = X_6$	$X_4 = Z_1$ $Y_4 = Y_1 Z_2$ $Z_4 = X_1 Z_2$ $X_5 = Z_2$ $Y_5 = Z_1 Y_2 Z_3$ $Z_5 = Z_1 X_2 Z_3$ $X_6 = Z_3$ $Y_6 = Z_2 Y_3$ $Z_6 = Z_2 X_3$
<p data-bbox="284 1043 421 1077"><b>No. 14a</b></p> 	$X_1 = Z_4 X_5 Z_6$ $Y_1 = Y_4 X_5 Z_6$ $Z_1 = X_4$ $X_2 = X_4 Z_5$ $Y_2 = X_4 Y_5 Z_6$ $Z_2 = X_5 Z_6$ $X_3 = Z_6$ $Y_3 = Z_5 Y_6$ $Z_3 = X_6$	$X_4 = Z_1$ $Y_4 = Y_1 Z_2$ $Z_4 = X_1 Z_2$ $X_5 = Z_2 X_3$ $Y_5 = Z_1 Y_2 X_3$ $Z_5 = Z_1 X_2$ $X_6 = Z_1 X_2 Z_3$ $Y_6 = Z_1 X_2 Y_3$ $Z_6 = X_3$
<p data-bbox="284 1424 421 1458"><b>No. 16a</b></p> 	$X_1 = Z_4 X_5 X_6$ $Y_1 = Y_4 X_5 X_6$ $Z_1 = X_4$ $X_2 = X_4 Z_5 X_6$ $Y_2 = X_4 Y_5 X_6$ $Z_2 = X_5$ $X_3 = X_4 X_5 Z_6$ $Y_3 = X_4 X_5 Y_6$ $Z_3 = X_6$	$X_4 = Z_1$ $Y_4 = Y_1 Z_2 Z_3$ $Z_4 = X_1 Z_2 Z_3$ $X_5 = Z_2$ $Y_5 = Z_1 Y_2 Z_3$ $Z_5 = Z_1 X_2 Z_3$ $X_6 = Z_3$ $Y_6 = Z_1 Z_2 Y_3$ $Z_6 = Z_1 Z_2 X_3$

<p>No. 17a</p> 	$\begin{aligned} X_1 &= Z_4 X_5 \\ Y_1 &= Y_4 X_5 Z_6 \\ Z_1 &= X_4 Z_6 \\ \\ X_2 &= Y_4 Z_5 Y_6 \\ Y_2 &= Y_4 Y_5 Y_6 \\ Z_2 &= X_5 \\ \\ X_3 &= X_5 Z_6 \\ Y_3 &= Z_4 X_5 Y_6 \\ Z_3 &= Z_4 X_6 \end{aligned}$	$\begin{aligned} X_4 &= Z_1 Z_2 X_3 \\ Y_4 &= Y_1 X_3 \\ Z_4 &= X_1 Z_2 \\ \\ X_5 &= Z_2 \\ Y_5 &= Z_1 Y_2 Z_3 \\ Z_5 &= Z_1 X_2 Z_3 \\ \\ X_6 &= X_1 Z_2 Z_3 \\ Y_6 &= X_1 Y_3 \\ Z_6 &= Z_2 X_3 \end{aligned}$
<p>No. 18a</p> 	$\begin{aligned} X_1 &= X_5 X_6 \\ Y_1 &= -X_4 X_5 Y_6 \\ Z_1 &= X_4 Z_6 \\ \\ X_2 &= X_4 Z_5 Z_6 \\ Y_2 &= Y_4 Y_5 Y_6 \\ Z_2 &= Z_4 X_5 X_6 \\ \\ X_3 &= Z_5 Z_6 \\ Y_3 &= Z_4 Z_5 Y_6 \\ Z_3 &= Z_4 X_6 \end{aligned}$	$\begin{aligned} X_4 &= X_2 X_3 \\ Y_4 &= -X_1 Y_2 X_3 \\ Z_4 &= X_1 Z_2 \\ \\ X_5 &= Z_2 Z_3 \\ Y_5 &= Z_1 Y_2 Z_3 \\ Z_5 &= Z_1 X_2 \\ \\ X_6 &= X_1 Z_2 Z_3 \\ Y_6 &= Y_1 Y_2 Y_3 \\ Z_6 &= Z_1 X_2 X_3 \end{aligned}$
<p>No. 19a</p> 	$\begin{aligned} X_1 &= Z_4 Y_5 Y_6 \\ Y_1 &= -Y_4 X_5 X_6 \\ Z_1 &= X_4 Z_5 Z_6 \\ \\ X_2 &= Y_4 Z_5 Y_6 \\ Y_2 &= -X_4 Y_5 X_6 \\ Z_2 &= Z_4 X_5 Z_6 \\ \\ X_3 &= Y_4 Y_5 Z_6 \\ Y_3 &= -X_4 X_5 Y_6 \\ Z_3 &= Z_4 Z_5 X_6 \end{aligned}$	$\begin{aligned} X_4 &= Z_1 Y_2 Y_3 \\ Y_4 &= -Y_1 X_2 X_3 \\ Z_4 &= X_1 Z_2 Z_3 \\ \\ X_5 &= Y_1 Z_2 Y_3 \\ Y_5 &= -X_1 Y_2 X_3 \\ Z_5 &= Z_1 X_2 Z_3 \\ \\ X_6 &= Y_1 Y_2 Z_3 \\ Y_6 &= -X_1 X_2 Y_3 \\ Z_6 &= Z_1 Z_2 X_3 \end{aligned}$

**Tabla 1.** Grafos asociados a los estados grafo y distribuciones de qubits que permiten demostraciones TON bipartitas. Para cada uno de estos estados grafo se indican las correlaciones perfectas que hacen que se satisfaga el requisito (a). La nomenclatura de los grafos es la de [16,17].

## Bibliografía

- [1] D. M. Greenberger, M. A. Horne, y A. Zeilinger, en M. Kafatos (ed.), *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, Kluwer Academic, Dordrecht, 1989, p. 69.
- [2] N. D. Mermin. Phys. Rev. Lett. **65**, 1838 (1990).
- [3] A. Einstein, B. Podolsky, y N. Rosen. Phys. Rev. **47**, 777 (1935).
- [4] A. Cabello. Phys. Rev. Lett. **87**, 010403 (2001).
- [5] Z.-B. Chen, J.-W. Pan, Y.-D. Zhang, C. Brukner, y A. Zeilinger. Phys. Rev. Lett. **90**, 160408 (2003).
- [6] C. Cinelli, M. Barbieri, R. Perris, P. Mataloni, y F. De Martini. Phys. Rev. Lett. **95**, 240405 (2005).
- [7] T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Zukowski, Z.-B. Chen, y J.-W. Pan. Phys. Rev. Lett. **95**, 240406 (2005).
- [8] A. I. Lvovsky. Phys. Rev. Lett. **88**, 098901 (2002).

- [9] A. Cabello. Phys. Rev. Lett. **95**, 210401 (2005).
- [10] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini, y V. Berardi, quant-ph/0703191.
- [11] J. T. Barreiro, N. K. Langford, N. A. Peters, y P. G. Kwiat. Phys. Rev. Lett. **95**, 260501 (2005).
- [12] Q. Zhang, A. Goebel, C. Wagenknecht, Y.-A. Chen, B. Zhao, T. Yang, A. Mair, J. Schmiedmayer, y J.-W. Pan. Nature Physics **2**, 678 (2006).
- [13] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, y J.-W. Pan. Nature Physics **3**, 91 (2007).
- [14] D. Gottesman, Ph. D. thesis, Caltech, 1997; quant-ph/9705052.
- [15] M. Van den Nest, J. Dehaene, y B. De Moor. Phys. Rev. A **69**, 022316 (2004).
- [16] M. Hein, J. Eisert, y H. J. Briegel. Phys. Rev. A **69**, 062311 (2004).
- [17] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, y H. J. Briegel, en *Proceedings of the International School of Physics “Enrico Fermi” on “Quantum Computers, Algorithms and Chaos”*, Varenna, Italy, July, 2005; quant-ph/0602096.

## Demostraciones “todo o nada” $m$ -partitas del teorema de Bell con qubits

Adán Cabello y Pilar Moreno

Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Sevilla, adan@us.es, mpmoreno@us.es.

El criterio de elementos de realidad de Einstein, Podolsky, y Rosen (EPR) dice: “Si, sin perturbar un sistema, podemos predecir con certeza (i.e., con probabilidad igual a uno) el valor de una cantidad física, entonces existe un elemento de realidad asociado a esa cantidad física” [1]. La condición de “sin perturbar” se cumple si las medidas necesarias para las predicciones se hacen sobre sistemas distantes. Las predicciones “con certeza” son posibles en estados que tengan correlaciones perfectas.

Las demostraciones “todo o nada” (TON) del teorema de Bell muestran la imposibilidad de reproducir las correlaciones perfectas en un estado cuántico utilizando el concepto de elementos de realidad de EPR. El nombre “todo o nada” [2] refleja una característica particular de estas demostraciones: si se asume la existencia de elementos de realidad, entonces  $p-1$  de las correlaciones perfectas conducen a la predicción opuesta a la de la correlación  $p$ -ésima.

La primera demostración TON se debe a Heywood y Redhead [3]. La demostración más famosa de este tipo es la de Greenberger, Horne, y Zeilinger [4-6]. La primera demostración TON bipartita con qubits está en [7, 8], y la primera que usa sólo medidas sobre qubits individuales está en [9, 10]. El interés de usar sólo medidas sobre qubits individuales está relacionado con los recientes avances en los que se codifican distintos qubits en diferentes grados de libertad de una misma partícula: si nos restringimos a las medidas sobre qubits individuales, entonces no son necesarias medidas de observables que involucren distintos grados de libertad.

Se han obtenido experimentalmente varios estados de  $m$  partículas y  $n$  qubits (con  $m < n$ ) con correlaciones perfectas: estados de 4-qubits en 2-fotones [11], 6-qubits en 2-fotones [12, 13], 6-qubits en 4-fotones [14], 8-qubits en 4-fotones [15], y 10 qubits en 5 fotones [15]. Se esperan obtener más estados en el futuro.

Esto nos lleva de forma natural al problema de qué estados de  $m$  partículas y  $n$  qubits permiten demostraciones TON  $m$ -partitas usando sólo medidas sobre qubits individuales.

Recientemente, el problema se ha resuelto para  $m = 2$  observadores [16]. Aquí lo resolvemos para un número arbitrario de observadores. Primero enunciamos un criterio para decidir si un estado de  $n$ -qubits distribuido entre  $m$  observadores permite demostraciones TON usando sólo medidas sobre qubits individuales. A continuación, caracterizamos todas las demostraciones TON, no equivalentes bajo operaciones unitarias de un solo qubit, y con un número mínimo de observadores, para  $n \leq 8$ .

### Referencias

- [1] A. Einstein, B. Podolsky, y N. Rosen, *Phys. Rev.* 47, 777 (1935).
- [2] N.D. Mermin, *Phys. Rev. Lett.* 65, 1838 (1990).
- [3] P. Heywood y M. L. G. Redhead, *Found. Phys.* 13, 481 (1983).
- [4] D.M. Greenberger, M.A. Horne, y A. Zeilinger, en *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, editado por M. Kafatos (Kluwer Academic, Dordrecht, Holland, 1989), p. 69.
- [5] D.M. Greenberger, M.A. Horne, A. Shimony, y A. Zeilinger, *Am. J. Phys.* 58, 1131 (1990).
- [6] N.D. Mermin, *Phys. Rev. Lett.* 65, 3373 (1990).
- [7] A. Cabello, *Phys. Rev. Lett.* 86, 1911 (2001).

- [8] A. Cabello, Phys. Rev. Lett. 87, 010403 (2001).
- [9] A. Cabello, Phys. Rev. Lett. 95, 210401 (2005).
- [10] A. Cabello, Phys. Rev. A 72, 050101(R) (2005).
- [11] G. Vallone et al., Phys. Rev. Lett. 98, 180502 (2007).
- [12] J.T. Barreiro et al., Phys. Rev. Lett. 95, 260501 (2005).
- [13] R. Ceccarelli et al. (no publicado).
- [14] W.-B. Gao et al. (no publicado).
- [15] W.-B. Gao et al., arXiv:0809.4277 [quant-ph].
- [16] A. Cabello y P. Moreno, Phys. Rev. Lett. 99, 220402 (2007).

## Conjunto compacto de invariantes que permiten caracterizar estados grafo de hasta ocho qubits

A. Cabello<sup>1</sup>, A. J. López-Tarrida<sup>1</sup>, P. Moreno<sup>1</sup> y J. R. Portillo<sup>2</sup>

<sup>1</sup> Departamento de Física Aplicada II, Universidad de Sevilla, 41012 Sevilla; tarrida@us.es

<sup>2</sup> Departamento de Matemática Aplicada I, Universidad de Sevilla, 41012 Sevilla

Los estados grafo [1, 2] son fundamentales en información cuántica, especialmente en corrección cuántica de errores [3-5] y computación cuántica basada en medidas [6]. Los estados grafo también juegan un papel fundamental en el estudio del entrelazamiento. Dos estados cuánticos tienen el mismo entrelazamiento si y sólo si son equivalentes bajo operaciones locales unitarias (LU). Para un número de qubits  $n \geq 4$  hay una cantidad infinita de clases de entrelazamiento diferentes (i. e., no equivalentes LU). No obstante, si nos centramos en estados grafo, entonces la discusión se hace más simple. Resultados previos sugieren que para estados grafo de  $n < 27$  qubits las nociones de equivalencia LU y equivalencia LC son coincidentes [7].

El propósito de nuestro trabajo es resolver el siguiente problema: dado un estado grafo de  $n$  qubits con  $n < 9$ , decidir a qué clase de entrelazamiento pertenece examinando solamente algunas propiedades intrínsecas del estado (i. e., sin tener que generar la clase LC completa). La solución a este problema tiene importancia práctica: si se necesita preparar un estado grafo  $|G\rangle$  y se sabe que éste pertenece a una clase específica, entonces se puede obtener  $|G\rangle$  preparando el estado LC- equivalente  $|G'\rangle$  que requiere el mínimo número de puertas de entrelazamiento y la mínima profundidad de preparación de la clase (v. [1, 2, 8]), y a continuación transformando  $|G'\rangle$  en  $|G\rangle$  mediante operaciones unitarias sencillas de un qubit. El problema es que hasta el momento no se conoce un conjunto sencillo de invariantes que permitan distinguir entre todas las clases de entrelazamiento, incluso si nos restringimos a estados grafo con un número de qubits  $n \leq 7$ .

El conjunto de medidas de entrelazamiento propuesto en [1, 2] no logra distinguir entre clases no equivalentes (i. e., entre diferentes tipos de entrelazamiento). Por tanto, no podemos utilizar esos invariantes para decidir a qué clase de entrelazamiento pertenece un estado dado.

Van den Nest, Dehaene y De Moor (VDD) han propuesto un conjunto finito de invariantes que caracteriza todas las clases [9]. Sin embargo, incluso para  $n = 7$  dicho conjunto consta de  $2 \times 10^{36}$  más de invariantes que además no están calculados explícitamente en ningún sitio, de modo que este conjunto no es útil para clasificar un estado grafo dado. En este trabajo mostramos que si  $n \leq 8$  bastan 4 invariantes relacionados con los de VDD para reconocer el tipo de entrelazamiento.

Aquí introducimos un nuevo tipo de invariante LC que denominamos *multiplicidad*,  $M(A\omega)$ , que cuenta, para las clases de equivalencia ligadas a los soportes de los operadores de estabilización de un estado grafo, cuántas tienen una misma cardinalidad dada. Hemos demostrado que basta con sólo cuatro de estas multiplicidades para decidir a qué clase de entrelazamiento pertenece un estado grafo con un número de qubits  $n \leq 8$ : las multiplicidades de algunos de los invariantes de VDD de valores, 0, 1, 3 y 4. Por consiguiente, estos cuatro invariantes LC caracterizan cualquier clase LC para  $n \leq 8$ . Aplicando la misma estrategia se puede obtener un conjunto compacto de invariantes que caractericen todas las clases no equivalentes de estados grafo para un número de qubits mayor. Esto puede llevarse a cabo numéricamente hasta  $n = 7$ , es decir, más allá de la capacidad experimental actual de preparación de estados grafo [10].

Los autores agradecen la financiación de los proyectos P06-FQM-02243, FIS2008-05596, PAI-FQM-0239, P06-FQM-01649, MTM2008-05866-C03-01 y PAI-FQM-0164.

## Referencias

- [1] M. Hein, J. Eisert, y H. J. Briegel, *Phys. Rev. A* 69, 062311 (2004).
- [2] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, y H. J. Briegel, en *Quantum Computers, Algorithms and Chaos*, editado por G. Casati, D. L. Shepelyansky, P. Zoller, y G. Benenti (IOS Press, Amsterdam, 2006).
- [3] D. Gottesman, *Phys. Rev. A* 54, 1862 (1996).
- [4] D. Schlingemann y R. F. Werner, *Phys. Rev. A* 65, 012308 (2001).
- [5] D. Schlingemann, *Quantum Inf. Comput.* 2, 307 (2002).
- [6] R. Raussendorf y H. J. Briegel, *Phys. Rev. Lett.* 86, 5188 (2001).
- [7] Z. Ji, J. Chen, Z. Wei, y M. Ying, arXiv:0709.1266v2 [quant-ph].
- [8] A. Cabello, A. J. López-Tarrida, P. Moreno, y J. R. Portillo, arXiv:0812.4625 [quant-ph].
- [9] M. Van den Nest, J. Dehaene, y B. De Moor, *Phys. Rev. A* 72, 014307 (2005).
- [10] W.-B. Gao et al., arXiv:0809.4277 [quant-ph].

## All-versus-nothing proofs of Bell's theorem with $n$ -qubit distributed between $m$ parties

Adán Cabello<sup>1</sup>, Pilar Moreno<sup>1</sup>

<sup>1</sup>*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

e-mail: [mpmoreno@us.es](mailto:mpmoreno@us.es)

(Poster, Mo23)

Einstein, Podolsky, and Rosen's (EPR's) criterion of elements of reality states that "if, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity" [1]. Non-disturbance is guaranteed when the measurements required for a prediction with certainty are performed on distant systems. Predictions with certainty are possible for states with perfect correlations.

All-versus-nothing (AVN) proofs of Bell's theorem show the impossibility of reproducing the perfect correlations of a specific quantum state by means of EPR's elements of reality. The name AVN [2] reflects one particular feature of these proofs: If one assumes elements of reality, then  $p - 1$  of the perfect correlations of the state lead to a prediction that is the opposite of the one given by the  $p$ th perfect correlation.

The first AVN proof is due to Heywood and Redhead [3]. However, the most famous AVN proof is due to Greenberger, Horne, and Zeilinger (GHZ) [4, 5, 6]. The first bipartite AVN proof with qubits is in [7, 8]. The first bipartite AVN proof using only single-qubit measurements is in [9, 10]. The interest of using only single-qubit measurements is motivated by recent developments where several qubits are carried by the same particle, encoded in different degrees of freedom. If one is restricted to single-qubit measurements, then measurements that entangle different degrees of freedom are not needed.

Several  $n$ -qubit  $m$ -particle states, with  $m < n$ , have been demonstrated so far: 4-qubit 2-photon [11], 6-qubit 2-photon [12, 13], 6-qubit 4-photon [14], 8-qubit 4-photon [15], and 10-qubit 5-photon graph states [15]. More states are expected in the near future.

These possibilities naturally lead to the problem of which  $n$ -qubit  $m$ -particle states allow  $m$ -party AVN proofs using only single-qubit measurements. Recently, the problem has been solved for  $m = 2$  parties [16]. Here we address the problem for arbitrary  $m$ .

We first provide a criterion to decide whether or not an  $n$ -qubit state distributed between  $m$  parties allows an AVN proof using only single-qubit measurements. We then characterize all AVN proofs using only single-qubit measurements that are non-equivalent under single-qubit unitary operations and have a minimum number of observers for  $n \leq 8$  qubits.

We acknowledge support from the MCI Project No. FIS2008-05596, and the Junta de Andalucía Excellence Project No. P06-FQM-02243.

## References

- [1] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [2] N.D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [3] P. Heywood and M. L. G. Redhead, *Found. Phys.* **13**, 481 (1983).
- [4] D.M. Greenberger, M.A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, Holland, 1989), p. 69.
- [5] D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).
- [6] N.D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
- [7] A. Cabello, *Phys. Rev. Lett.* **86**, 1911 (2001).
- [8] A. Cabello, *Phys. Rev. Lett.* **87**, 010403 (2001).
- [9] A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).
- [10] A. Cabello, *Phys. Rev. A* **72**, 050101(R) (2005).
- [11] G. Vallone *et al.*, *Phys. Rev. Lett.* **98**, 180502 (2007).
- [12] J.T. Barreiro *et al.*, *Phys. Rev. Lett.* **95**, 260501 (2005).
- [13] R. Ceccarelli *et al.* (unpublished).
- [14] W.-B. Gao *et al.* (unpublished).
- [15] W.-B. Gao *et al.*, arXiv:0809.4277 [quant-ph].
- [16] A. Cabello and P. Moreno, *Phys. Rev. Lett.* **99**, 220402 (2007).



## Compact set of invariants characterizing graph states up to eight qubits

Adán Cabello<sup>1</sup>, Antonio J. López-Tarrida<sup>1</sup>, Pilar Moreno<sup>1</sup>, José R. Portillo<sup>2</sup>

<sup>1</sup>*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

<sup>2</sup>*Departamento de Matemática Aplicada I, Universidad de Sevilla, E-41012 Sevilla, Spain*

e-mail: [tarrida@us.es](mailto:tarrida@us.es)

(Poster, Mo17)

Graph states [1, 2] are fundamental in quantum information, specially in quantum error-correction [3, 4, 5] and measurement-based quantum computation [6]. Graph states also play a fundamental role in the study of entanglement. Two quantum states have the same entanglement if and only if they are equivalent under local unitary (LU) operations. For  $n \geq 4$  there is an infinite amount of different entanglement (i.e., LU-inequivalent) classes. However, if we focus on graph states, then the discussion becomes simpler. Previous results suggest that for graph states of  $n < 27$  qubits, the notion of LU-equivalence and LC-equivalence coincide [7].

The aim of our work is to solve the following problem: given an  $n$ -qubit graph state with  $n < 9$  qubits, deciding which entanglement class it belongs to just by examining some of the state's intrinsic properties (i.e., without generating the whole LC-class). The solution to this problem is of practical importance: if one needs to prepare a graph state  $|G\rangle$  and knows that it belongs to one specific class, then one can prepare  $|G\rangle$  by preparing the LC-equivalent state  $|G'\rangle$  requiring the minimum number of entangling gates and the minimum preparation depth of that class (see [1, 2, 8]), and then transform  $|G'\rangle$  into  $|G\rangle$  by means of simple one-qubit unitary operations. The problem is that, so far, no simple set of invariants which distinguishes between all classes of entanglement is known, even for graph states with  $n \leq 7$  qubits.

The set of entanglement measures proposed in [1, 2] fails to distinguish between inequivalent classes (i.e., between different types of entanglement). Therefore, we cannot use these invariants for deciding which entanglement class a given state belongs to.

Van den Nest, Dehaene, and De Moor (VDD) have proposed a finite set of invariants that characterizes *all* classes [9]. However, already for  $n = 7$ , this set has more than  $2 \times 10^{36}$  invariants which are not explicitly calculated anywhere, so this set is not useful for classifying a given graph state. In our work we show that, if  $n \leq 8$ , then 4 invariants related to those of VDD are enough to recognise the type of entanglement.

We introduce a new type of LC-invariant, the multiplicity  $M(A_\omega)$ , that counts the number of support-related classes with the same cardinality. We have shown that only 4 of these multiplicities are enough to decide which entanglement class a graph state of  $n \leq 8$  qubits belongs to: the multiplicities of some of the VDD's invariants of values 0, 1, 3, and 4. Therefore, these 4 LC-invariants characterize any LC-class of  $n \leq 8$  qubits. A compact set of invariants that characterize all inequivalent classes of graph states with a higher number of qubits can be obtained by applying the same strategy. This can be done numerically up to  $n = 12$ , a number of qubits beyond the present experimental capability in the preparation of graph states [10].

The authors acknowledge support from projects P06-FQM-02243, FIS2008-05596, PAI-FQM-0239, P06-FQM-01649, MTM2008-05866-C03-01, and PAI-FQM-0164.

## References

- [1] M. Hein, J. Eisert, and H.J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [2] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.J. Briegel, in *Quantum Computers, Algorithms and Chaos*, edited by G. Casati, D.L. Shepelyansky, P. Zoller, and G. Benenti (IOS Press, Amsterdam, 2006).
- [3] D. Gottesman, *Phys. Rev. A* **54**, 1862 (1996).
- [4] D. Schlingemann and R.F. Werner, *Phys. Rev. A* **65**, 012308 (2001).
- [5] D. Schlingemann, *Quantum Inf. Comput.* **2**, 307 (2002).
- [6] R. Raussendorf and H.J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [7] Z. Ji, J. Chen, Z. Wei, and M. Ying, arXiv:0709.1266v2 [quant-ph].
- [8] A. Cabello, A.J. López-Tarrida, P. Moreno, and J.R. Portillo, arXiv:0812.4625.
- [9] M. Van den Nest, J. Dehaene, and B. De Moor, *Phys. Rev. A* **72**, 014307 (2005).
- [10] W.-B. Gao *et al.* arXiv:0809.4277 [quant-ph].

## All-versus-nothing proofs with $n$ qubits distributed between $m$ parties

Adán Cabello<sup>1,\*</sup> and Pilar Moreno<sup>1,†</sup>

<sup>1</sup>*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*

All-versus-nothing (AVN) proofs [1–6] show the conflict between Einstein, Podolsky, and Rosen’s (EPR) elements of reality [7] and the perfect correlations of some quantum states. The name of “all-versus-nothing” [8] reflects a particular feature of these proofs: If one consider a set of perfect correlations and assumes EPR elements of reality, then a subset of these correlations leads to a conclusion that is opposite of the one obtained from the complementary subset of correlations.

The perfect correlations among single qubit measurements required for AVN proofs are given by the  $2^n$  stabilizer operators of an  $n$ -qubit graph state. The possibility of experimentally preparing new classes of graph states [9–11] naturally leads to the following problem: Does a distribution of an  $n$ -qubit graph state between  $m$  parties allow an AVN proof? This problem has been solved for  $m = 2$  [12]. Here we describe a method to decide whether a given  $n$ -qubit  $m$ -particle graph state allows an  $m$ -partite AVN proof specific for this state (i.e., which cannot be obtained using a graph state with fewer qubits) [13]. This method requires that two observables of each qubit are EPR elements of reality. This forces a series of constraints that are only satisfied by a reduced group of the graph state’s stabilizer operators. We detail these requirements and apply them to decide whether some  $n$ -qubit  $m$ -particle graph states recently prepared in the laboratory [9–11] allow  $m$ -partite AVN proofs.

We also address the following problem: Given an  $n$ -qubit graph state, what is the minimum number  $m$  of parties that allows a specific  $m$ -partite AVN proof? The solution of this problem enables us to obtain all inequivalent distributions allowing AVN proofs with  $n < 9$  qubits and an arbitrary number  $m$  of parties [13].

These results provide the tools to help experimentalists

to design tests of new AVN proofs and new Bell inequalities based on these proofs [14].

We acknowledge support from the Spanish MCI Project FIS2008-05596, and the Junta de Andalucía Excellence Project P06-FQM-02243.

---

\* adan@us.es

† mpmoreno@us.es

- [1] P. Heywood and M. L. G. Redhead, *Found. Phys.* **13**, 481 (1983).
- [2] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bells Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), p. 69.
- [3] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).
- [4] A. Cabello, *Phys. Rev. Lett.* **86**, 1911 (2001).
- [5] A. Cabello, *Phys. Rev. Lett.* **87**, 010403 (2001).
- [6] A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).
- [7] A. Einstein, B. Podolsky, and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [8] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [9] R. Ceccarelli, G. Vallone, F. De Martini, P. Mataloni, and A. Cabello, *Phys. Rev. Lett.* **103**, 160401 (2009).
- [10] W.-B. Gao, X.-C. Yao, P. Xu, O. Gühne, A. Cabello, C.-Y. Lu, C.-Z. Peng, T. Yang, Z.-B. Chen, and J.-W. Pan, *arXiv:0906.3390* (2009).
- [11] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, *Nat. Phys.* **6**, 331 (2010).
- [12] A. Cabello and P. Moreno, *Phys. Rev. Lett.* **99**, 220402 (2007).
- [13] A. Cabello and P. Moreno, *Phys. Rev. A* **81**, 042110 (2010).
- [14] A. Cabello, O. Gühne, and D. Rodríguez, *Phys. Rev. A* **77**, 062106 (2008).

# Bibliografía

- [1] M. Hein, J. Eisert y H. J. Briegel, *Phys. Rev. A* **69**, 062311 (2004).
- [2] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest y H. J. Briegel, en *Quantum Computers, Algorithms and Chaos*, editado por G. Casati, D.L. Shepelyansky, P. Zoller y G. Benenti (IOS Press, Amsterdam, 2006).
- [3] D. Gottesman, *PhD Thesis*, quant-ph/97005052v1 (1997).
- [4] D. Schlingemann y R. F. Werner, *Phys. Rev. A* **65**, 012308 (2001).
- [5] D. Shlingemann, *Quant. Inf. Comp.* **2**, 307 (2002).
- [6] R. Raussendorf y H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [7] R. Raussendorf, D. E. Browne y H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [8] R. Raussendorf y H. J. Briegel, *Quant. Inf. Comp.* **6**, 443 (2002).
- [9] R. Raussendorf y H. J. Briegel, *Quantum Information Processing*, editado por Universität Karlsruhe, Fakultät für Informatik y Universität Erlangen, Institut für Optik, Information und Photonik (Wiley-VCH Verlag GmbH & Co. KGaA, Alemania, 2005). También disponible en quant-ph/0207183v1.
- [10] D. Browne y H. Briegel, quant-ph/0603226v2 (2006).
- [11] R. Raussendorf, D. E. Browne y H. J. Briegel, *J. Mod. Opt.* **49**, 1299 (2002).
- [12] O. Gühne, G. Tóth, P. Hyllus y H. J. Briegel, *Phys. Rev. Lett.* **95**, 120405 (2005).
- [13] V. Scarani, A. Acín, E. Schenck y M. Aspelmeyer, *Phys. Rev. A* **71**, 042325 (2005).
- [14] A. Cabello, O. Gühne y D. Rodríguez, *Phys. Rev. A* **77**, 062106 (2008).
- [15] A. Cabello, O. Gühne, P. Moreno y D. Rodríguez, *Laser Phys.* **18**, 3, 335 (2008).
- [16] W. Dür y H. J. Briegel, *Phys. Rev. Lett.* **92**, 180403 (2004).
- [17] A. Cabello, *Phys. Rev. Lett.* **95**, 210401 (2005).
- [18] A. Cabello, *Phys. Rev. A* **72**, 050101(R) (2005).

- [19] A. Cabello y P. Moreno, *Phys. Rev. Lett.* **99**, 220402 (2007).
- [20] A. Cabello y P. Moreno, *Phys. Rev. A* **81**, 042110 (2010).
- [21] A. Cabello, A. J. López-Tarrida, P. Moreno y J. R. Portillo, *Phys. Lett. A* **373**, 2219 (2009), *ibid* **374**, 3991 (2010).
- [22] A. Cabello, A. J. López-Tarrida, P. Moreno y J. R. Portillo, *Phys. Rev. A* **80**, 012102 (2009).
- [23] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer y A. Zeilinger, *Nature* **434**, 169 (2005).
- [24] N. Kiesel, C. Schmid, U. Weber, O. Gühne, G. Tóth, R. Ursin y H. Weinfurter, *Phys. Rev. Lett.* **95**, 210502 (2005).
- [25] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goedel, T. Yang y J.-W. Pan, *Nat. Phys.* **3**, 91 (2007).
- [26] C.-Y. Lu, W.-B. Gao, O. Gühne, X.-Q. Zhou, Z.-B. Chen y J.-W. Pan, *Phys. Rev. Lett.* **102**, 030502 (2009).
- [27] J. K. Pachos, W. Wieczorek, C. Schmid, N. Kiesel, R. Pohlner y H. Weinfurter, *New J. Phys.* **11**, 083010 (2009).
- [28] W.-B. Gao, X.-C. Yao, P. Xu, O. Gühne, A. Cabello, C.-Y. Lu, T. Yang, Z.-B. Chen y J.-W. Pan, *Phys. Rev. A* **82**, 042334 (2010).
- [29] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen y J.-W. Pan, *Nat. Phys.* **6**, 331 (2010).
- [30] M. Grassl, A. Klappenecker y M. Rötteler, *IEEE International Symposium on Information (Lausanne, Switzerland, 2002)*, p. 45.
- [31] M. Van den Nest, J. Dehaene y B. De Moore, *Phys. Rev. A* **70**, 034302 (2004).
- [32] M. Van den Nest, J. Dehaene y B. De Moore, *Phys. Rev. A* **69**, 022316 (2004).
- [33] W. Dür, G. Vidal y J. I. Cirac, *Phys. Rev. A* **62**, 062314 (2000).
- [34] A. Acín, E. Jane, W. Dür y G. Vidal, *Phys. Rev. Lett.* **85**, 4811 (2000).
- [35] F. Verstaete, J. Dehaene y B. De Moor, *Phys. Rev. A* **65**, 032308 (2002).
- [36] F. Verstaete, J. Dehaene y B. De Moor, H. Verschelde, *Phys. Rev. A* **65**, 052112 (2002).
- [37] Z. Ji, J. Chen, Z. Wei y M. Ying, *Quant. Inf. Comp.* **1&2**, 97 (2010).
- [38] M. Van den Nest, J. Dehaene y B. De Moor, *Phys. Rev. A* **71**, 062323 (2005).
- [39] B. Zeng, H. Chung, A. W. Cross y I. L. Chuang, *Phys. Rev. A* **75**, 032325 (2007).

- [40] L. E. Danielsen, *Database of Self-Dual Quantum Codes*, <http://www.iu.uib.no/~larsed/vncorbits/>. Este trabajo está centrado únicamente en estados grafos asociados a grafos conexos. En códigos cuánticos, los grafos conexos se corresponden a códigos cuánticos indescomponibles (i.e., aquellos que no se pueden expresar en dos códigos más pequeños).
- [41] J. S. Bell, *Physics*, **1**, 195 (1964).
- [42] A. Einstein, B. Podolsky y N. Rosen, *Phys. Rev.* **47**, 777 (1935).
- [43] P. Heywood y M. L. G. Redhead, *Found. Phys.* **13**, 481 (1983).
- [44] D. M. Greenberger, M. A. Horne y A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos (Kluwer Academic, Dordrecht, 1989), p. 69.
- [45] D. M. Greenberger, M. A. Horne, A. Shimony y A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).
- [46] N. D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
- [47] L. Hardy, *Phys. Rev. Lett.* **68**, 2981 (1992).
- [48] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini y V. Berardi, *Phys. Rev. Lett.* **98**, 180502 (2007).
- [49] N. D. Mermin, *Phys. Rev. Lett.* **65**, 1838 (1990).
- [50] A. Cabello, *Phys. Rev. Lett.* **97**, 140406 (2006).
- [51] J. T. Barreiro, N. K. Langford, N. A. Peters y P. G. Kwiat, *Phys. Rev. Lett.* **95**, 260501 (2005).
- [52] R. Ceccarelli, G. Vallone, F. De Martini, P. Mataloni y A. Cabello, *Phys. Rev. Lett.* **103**, 160401 (2009).
- [53] M. Barberi, F. De Martini, P. Mataloni, G. Vallone y A. Cabello, *Phys. Rev. Lett.* **97**, 140407 (2006).
- [54] Q. Zhan, A. Goebel, C. Wagenknecht, Y.-A. Chen, B. Zhao, T. Yang, A. Mair, J. Schmiedmayer y J.-W. Pan, *Nat. Phys.* **2**, 678 (2006).
- [55] P. H. Eberhard y P. Rosset, *Found. Phys.* **25**, 91 (1995).
- [56] M. Van den Nest, A. Miyake, W. Dür y H. J. Briegel, *Phys. Rev. Lett.* **97**, 150504 (2006).
- [57] D. Fattal, T. S. Cubitt, Y. Yamamoto, S. Bravyi y I. L. Chuang, *quant-ph/0406168v1* (2004).
- [58] G. Wang y M. Ying, *Phys. Rev. A* **75**, 052332 (2007).
- [59] A. Ketkar, A. Klappenecker, S. Kumar, P. K. Sarvepalli, *IEEE Trans. Inf. Th.* **52**, 4892 (2005).

- [60] M. Bahrangiri y S. Beigi, quant-ph/0610267 (2006).
- [61] D. Gottesman, Phys. Rev. A **54**, 1862 (1996).
- [62] M. A. Nielsen y I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [63] O. Gühne y G. Tóth, Phys. Rep. **474**, 1 (2009).
- [64] G. Tóth y O. Gühne, Phys. Rev. A **72**, 022340 (2005).
- [65] G. Tóth y O. Gühne, Phys. Rev. Lett. **94**, 0606501 (2005).
- [66] B. Eastin, *PhD Thesis*, quant-ph/0710.2560v1 (2007).
- [67] D. E. Browne y T. Rudolph, Phys. Rev. Lett. **95**, 010501 (2005).
- [68] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph y A. Zeilinger, Phys. Rev. Lett. **93**, 020504 (2004).
- [69] P. G. Kwiat, J. Mod. Opt. **44**, 2173 (1997).
- [70] P. G. Kwiat y H. Weinfurter, Phys. Rev. A **58**, 2623(R) (1998).
- [71] C. Cinelli, M. Barbari, R. Perris, P. Mataloni y F. De Martini, Phys. Rev. Lett. **95**, 240405 (2005).
- [72] T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Żukowski, Z.-B. Chen y J.-W. Pan, Phys. Rev. Lett. **95**, 240406 (2005).
- [73] H. Weinfurter y M. Żukowski, Phys. Rev. A **64**, 010102(R) (2001).
- [74] M. Eibl, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Żukowski y H. Weinfurter, Phys. Rev. Lett. **90**, 200403 (2003).
- [75] S. Gaertner, M. Bourennane, M. Eibl, C. Kurtsiefer y H. Weinfurter, Appl. Phys. B **77**, 803 (2003).
- [76] M. Bourennane, M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello y H. Weinfurter, Phys. Rev. Lett. **92**, 107901 (2004).
- [77] P. Walther, M. Aspelmeyer, K. J. Resch y A. Zeilinger, Phys. Rev. Lett. **95**, 020403 (2005).
- [78] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello y H. Weinfurter, Phys. Rev. Lett. **100**, 070504 (2008).
- [79] N. Spagnolo, C. Vitelli, M. Paternostro, F. De Martini y F. Sciarrino quant-ph/1012.3660v1 (2010).
- [80] K. L. Brown, S. De, V. M. Kendon y W. J. Murno, quant-ph/1011.2984v1 (2010).

- [81] A. Ashkin, Phys. Rev. Lett. **24**, 156 (1970).
- [82] A. Ashkin, *Optical and Manipulation of Neutral Particles Using Lasers*, (World Scientific, Singapur, 2006).
- [83] J. I. Cirac y P. Zoller, Phys. Rev. Lett. **74**, 4091 (1995).
- [84] K. Mølmer y A. Sørensen, Phys. Rev. Lett. **82**, 1835 (1999).
- [85] J. F. Poyatos, J. I. Cirac y P. Zoller, Phys. Rev. Lett. **81**, 1322 (1998).
- [86] J. F. Poyatos, J. I. Cirac y P. Zoller, Phys. Rev. Lett. **78**, 390 (1997).
- [87] D. Porras y J. I. Cirac, Phys. Rev. Lett. **92**, 207901 (2004).
- [88] A. Retzker, J. I. Cirac y B. Reznik, Phys. Rev. Lett. **94**, 050504 (2005).
- [89] F. Schmidt-Kaler, H. Häffner, M. Riebe, S. Gulde, G. P. T. Lancaster, T. Deuschle, C. Becher, C. F. Roos, J. Eschner y R. Blatt, Nature **422**, 6930 (2003).
- [90] C. A. Sackett, D. Kielpinski, B. E. King, C. Langer, V. Meyer, C. J. Myatt, M. Rowe, Q. A. Turchette, W. M. Itano, D. J. Wineland y C. Monroe, Nature **404**, 256 (2000).
- [91] A. Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.-M. Raimond y S. Haroche, Science **288**, 2024 (2002).
- [92] A. Sørensen, L.-M. Duan, J. I. Cirac P. Zoller, Nature **409**, 6816 (2001).
- [93] O. Romero-Isart, A. C. Pflanzer, M. L. Juan, R. Quidant, N. Kiesel, M. Aspelmeyer y J. I. Cirac, quant-ph/1010.3109v1 (2010).
- [94] L. Lamata, D. Porras, J. I. Cirac, J. Goldman y G. Gabrielse, Phys. Rev. A **81**, 022301 (2010).
- [95] S.-Y. Li y F.-L. Yan, quant-ph/1002.1981v1 (2010).
- [96] S.-B. Zheng, Phys. Rev. A **73**, 065802 (2006).
- [97] D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle y D. J. Wineland, Nature **438**, 639 (2005).
- [98] W. K. Wothers y W. H. Zurek, Nature **299**, 802 (1982).
- [99] N. Brunner y C. Simon, Phys. Rev. Lett. **105**, 010405 (2010).
- [100] J. Preskill, *Notes en Quantum Computation*, <http://www.theory.caltech.edu/preskill/ph229>.
- [101] G. Vallone, E. Pomarico, F. De Martini y P. Mataloni, Phys. Rev. Lett. **100**, 160502 (2008).

- [102] W.-B. Gao, P. Xu, X.-C. Yao, O. Gühne, A. Cabello, C.-Y. Lu, C.-Z. Peng, Z.-B. Chen y J.-W. Pan, *Phys. Rev. Lett.* **104**, 020501 (2010).
- [103] K. Chen, C.-M. Li, Q. Zhang, Y.-A. Chen, A. Goebel, S. Chen, A. Mair y J.-W. Pan, *Phys. Rev. Lett.* **99**, 120503 (2007).
- [104] G. Vallone, G. Donati, N. Bruno, A. Chiuri y P. Mataloni, *Phys. Rev. A* **81**, 050302(R) (2010).
- [105] M. S. Tame y M. S. Kim, *Phys. Rev. A* **82**, 030305(R) (2010).
- [106] R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaeck, T. Jennewein y A. Zeilinger, *Nature* **445**, 65 (2007).
- [107] D. Deutsch, *Proc. R. London, Ser. A* **425**, 73 (1990).
- [108] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin y H. Weinfurter, *Phys. Rev. A* **52**, 3457 (1995).
- [109] J. T. Barreiro, N. K. Langford, N. A. Peters y P. G. Kwiat, *Phys. Rev. Lett.* **95**, 260501 (2005).
- [110] M. S. Tame, M. Paternostro, M. S. Kim y V. Vedral, *Int. J. Quant. Info.* **4**, 689 (2006).
- [111] D. Belitz, R. Narayanan, T. R. Kirkpatrick y T. Vojta, *Phys. Rev. Lett.* **85**, 4602 (2000).
- [112] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [113] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres y W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [114] R. F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
- [115] J. A. Smolin, *Phys. Rev. A* **63**, 032306 (2001).
- [116] H. Araki y E. Lieb, *Commun. Math. Phys.* **18**, 160 (1970).
- [117] A. Wehrl, *Rev. Mod. Phys.* **50**, 221 (1978).
- [118] S. Barn y S. J. D. Phoenix, *Phys. Rev. A* **44**, 535 (1991).
- [119] M. Horodecki, P. Horodecki y R. Horodecki, *Phys. Lett. A* **210**, 377 (1996).
- [120] A. Vidiella-Barranco, *Phys. Lett. A* **260**, 335 (1999).
- [121] A. Peres, *Phys. Rev. Lett.* **77**, 1413 (1996).
- [122] M. Horodecki, P. Horodecki y R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).
- [123] K. Zyczkowski, P. Horodecki, A. Sanpera y M. Lewenstein, *Phys. Rev. A* **58**, 883 (1998).
- [124] G. Vidal y R. F. Werner, *Phys. Rev. A* **65**, 032314 (2002).



- [125] M. Horodecki y P. Horodecki, quant-ph/9708015v3 (1998).
- [126] E. Schmidt, Math. Ann. **63**, 433 (1907).
- [127] E. Schmidt, Math. Ann. **64**, 161 (1907).
- [128] L. E. Ballentine, *Quantum Mechanics*, Prentice-Hall (Englewood Cliffs, New Jersey, 1990).
- [129] A. Peres, *Quantum Theory: Concepts and Methods*, (Kluwer Academic Publishers, Dordrecht, 1993).
- [130] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
- [131] D. Bruss y A. Peres, Phys. Rev. A **61**, 30301(R) (2000).
- [132] P. Horodecki, R. Augusiak y M. Demianowicz, Phys. Rev. A **74**, 052323 (2006).
- [133] A. Peres, Phys. Lett. A **202**, 16 (1995).
- [134] A. Elby y J. Bub, Phys. Rev. A **49**, 4213 (1994).
- [135] D. Collins, N. Gisin, S. Popescu, D. Roberts y V. Scarani, Phys. Rev. Lett. **88**, 170405 (2002).
- [136] P. Mitchell, S. Popescu y D. Roberts, Phys. Rev. A **70**, 060101 (2004).
- [137] D. Pérez-García, M. M. Wolf, C. Palazuelos, I. Villanueva y M. Junge, Comm. Math. Phys. **279**, 455 (2008).
- [138] M. Żukowski y D. Kaszlikowski, Phys. Rev. A **56**, 1682(R) (1997).
- [139] D. Bruß, J. I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein y A. Sanpera, J. Mod. Opt. **49**, 1399 (2002).
- [140] M. B. Terhal, Phys. Lett. A **271**, 319 (2000).
- [141] M. Lewenstein, B. Kraus, J. I. Cirac y P. Horodecki, Phys. Rev. A **62**, 052310 (2000).
- [142] K. Kraus, *States, Effects and Operations* (Spring-Verlag, Berlin, 1983).
- [143] J. Preskill, *Information for Physics 219/Computer Science 219, Quantum Computation*, [www.theory.caltech.edu/people/preskill/ph229](http://www.theory.caltech.edu/people/preskill/ph229).
- [144] C. H. Bennett, D. P. DiVicenzo, J. Smolin y W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [145] C. H. Bennet, S. Popescu, D. Rohrlich, J. A. Smolin y A. V. Thapliyal, Phys. Rev. A **63**, 012307 (2000).
- [146] G. Vidal, J. Mod. Opt. **47**, 355 (2000).
- [147] F. Verstaete, J. Dehaene y B. De Moor, Phys. Rev. A **68**, 012103 (2003).

- [148] V. Vedral, M. B. Plenio, M. A. Rippin y P. L. Knight, *Phys. Rev. Lett.* **78**, 2275 (1997).
- [149] M. B. Plenio, *Phys. Rev. Lett.* **95**, 090503 (2005).
- [150] M. B. Plenio y S. Virmani, *Quant. Inf. Comp.* **7**, 1 (2007).
- [151] M. A. Nielsen, *Phys. Rev. Lett.* **83**, 2 (1999).
- [152] H. K. Lo y S. Popescu, *Phys. Rev. A* **63**, 02230 (2001).
- [153] W. Dür y J. I. Cirac, *Phys. Rev. A* **61**, 042314 (2000).
- [154] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre y R. Tarrach, *Phys. Rev. Lett.* **85**, 1560 (2000).
- [155] M. Koashi, V. Bužek y N. Imoto, *Phys. Rev. A* **62**, 050302 (2000).
- [156] M. Van den Nest, J. Dehaene y B. De Moor, *Proceedings of the 16th International Symposium on Mathematical Theory of Network and Systems*, Katholieke Universiteit Leuven, Bélgica (2004).
- [157] M. Van den Nest, J. Dehaene y B. De Moor, *Virtual J. Quant. Inf.*, <http://www.vjquantuminfo.org>, **04** (2004).
- [158] W. Dür, H. Aschauer y H. J. Briegel, *Phys. Rev. Lett.* **91**, 107903 (2003).
- [159] J. Dehaene, M. Van den Nest, B. De Moor y F. Verstraete, *Phys. Rev. A* **67**, 022310 (2003).
- [160] K. M. R. Audemark y M. B. Plenio, *New J. Phys.* **7**, 170 (2005).
- [161] A. Bouchet, *Combinatorica* **11**, 315 (1991); *Discrete Math.* **114**, 75 (1993).
- [162] D. G. Glynn, enviado a *Elect. J. Combinat.*, Preprint: [http://homepage.mac.com/dglynn/quantum files/Personal3.html](http://homepage.mac.com/dglynn/quantum%20files/Personal3.html) (2002).
- [163] J. Eisert y H. J. Briegel, *Phys. Rev. A* **64**, 022306 (2001).
- [164] S. Severini, *Phys. Lett. A* **356**, 99 (2006).
- [165] M. Mhalla y S. Perdrix, *8th Workshop Quantum Information Processing (QIP'05)* (Boston, USA, 2005), quant-ph/0412071v1 (2005).
- [166] M. Van den Nest, Dehaene y B. De Moor, *Phys. Rev. A* **72**, 014307 (2005).
- [167] A. Einstein, *Albert Einstein: Philosopher-Scientist* (Open Court, La Salle, Illinois, 1949), vol. 1, p. 2.
- [168] D. Bohm, *Quantum Theory* (Dover, New York, 1989).
- [169] A. Einstein y L. Infeld, *The Evolution of Physics* (Simon y Schuster, New York, 1938), p. 280.

- [170] J. F. Clauser, M. A. Horne, A. Shimony y R. A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).
- [171] J. S. Bell, *J. Phys. C* **2** 41, (1981).
- [172] S. B. Tsirelson, *Lett. Math. Phys.* **4**, 93 (1980).
- [173] R. Horodecki, P. Horodeki y M. Horodeki, *Phys. Lett. A* **200**, 340 (1995).
- [174] E. R. Loubenets, *Phys. Rev. A* **69**, 042102 (2004).
- [175] C. Simon, *Phys. Rev. A* **71**, 026102 (2005).
- [176] M. Żukowski, *Found. Phys.* **36**, 541 (2006).
- [177] H. R. Brown y G. Svetlichny, *Found. Phys.* **20**, 1379 (1990).
- [178] L. Hardy, *Phys. Rev. Lett.* **71**, 1665 (1993).
- [179] G. Kar, *Phys. Lett. A* **204**, 99 (1995).
- [180] S. L. Braunstein, A. Mann y M. Revzen, *Phys. Rev. Lett.* **68**, 3259 (1992).
- [181] A. Cabello, *Phys. Rev. Lett.* **86**, 1911 (2001).
- [182] A. Cabello, *Phys. Rev. Lett.* **87**, 010403 (2001).
- [183] A. Peres, *Phys. Lett. A* **151**, 107 (1990).
- [184] N. D. Mermin, *Phys. Rev. Lett.* **65**, 3373 (1990).
- [185] A. Peres, *Found. Phys.* **22**, 357 (1992).
- [186] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, 1993), p. 151.
- [187] A. Peres, *Found. Phys.* **26**, 807 (1996).
- [188] S. Kochen y E. P. Specker, *J. Math. Mech.* **17**, 59 (1967).
- [189] A. Peres, *Phys. Lett. A* **151**, 107 (1990).
- [190] N. D. Mermin, *Phys. Today* **43**, 6, 9 (1990).
- [191] N. D. Mermin, *Am. J. Phys.* **58**, 731 (1990).
- [192] N. D. Mermin, *Rev. Mod. Phys.* **65**, 803 (1993).
- [193] Z.-B. Chen, J.-W. Pan, Y.-D. Zhang, Č. Brukner y A. Zeilinger, *Phys. Rev. Lett.* **90**, 160408 (2003).
- [194] D. P. DiVincenzo y A. Peres, *Phys. Rev. A* **55**, 4089 (1997).

- 
- [195] Programa en MATHEMATICA que se puede encontrar en <http://link.aps.org/supplemental/10.1103/PhysRevA.81.042110>.
- [196] O. Gühne y A. Cabello, *Phys. Rev. A* **77**, 032108 (2008).
- [197] B. D. McKay, *nauty User's Guide (Version 2.4)* (Departamento de Ciencias de la Computación, Universidad Nacional Australiana, Canberra, Australia, 2007).
- [198] A. Bouchet, *Discrete Math.* **114**, 75 (1993).
- [199] R. Diestel, *Graph Theory* (Springer-Verlag, Hielberg, 2010), vol. 173.
- [200] M. B. Elliott, *PhD Thesis*, quant-ph/0807.2876v1 (2008).