Supremacía cuántica con tecnologías cuánticas

Ignacio Fernández Veiga

Trabajo de fin de Grado.

Grado en Física por la Universidad de Sevilla.

Tutor del trabajo: Dr. Lucas Lamata.

Agradecimientos

Quería agradecer en este breve espacio a mi tutor, por haberme ayudado tan atentamente a realizar este trabajo, más aún, dadas las circunstancias de excepción actuales.

Además quería agradecer todos los compañeros y profesores con los que he podido trabajar a lo largo del Grado, porque sin ellos no habría llegado aquí.

Índice general

English Abstract

In this work, we aim to give an introduction to quantum technologies and quantum computation, providing an overview of its foundation. Our main goal is understanding the claim done by Google in which, supossedly, quantum supremacy is achieved experimentally. Quantum supremacy is known as a quantum computation that is much faster than any computation done with current classical computers.

In order to get there, a brief explanation of qubit, logic qubit gates and quantum algorithms is given, in addition to a basic introduction to superconducting circuits with which qubits are built. Finally, a short mathematical approach to ”Quantum speckle”, the algorithm used in the experimental setup of Google and a review of the already named experiment and its consequences is carried out.

1 Introducción

El objetivo de este trabajo es servir como una introducción a la que llamamos "computación cuántica". Esto es, explicar los principios en los que esta se basa, así como hacer un esquema de las diferentes maneras de llevar la teoría de esta, a la realidad (maneras de construir qubits reales, mantener el entrelazamiento y la coherencia, etc.), y de las dificultades que esta tarea implica. Como objetivo final, además, explicaremos el concepto de "supremacía cuántica" y analizaremos cómo ha sido llevada a cabo, de manera que podamos, aunque sea de manera introductoria, comprender en qué consiste y si realmente se ha llegado a superar, como afirma haber realizado Google, a los grandes supercomputadores actuales con una computadora cuántica.

La computación cuántica nace con el objetivo de combinar las propiedades de la física y las ciencias computacionales para solucionar problemas de computación. Este es un campo del que se espera que en los años próximos se consigan resultados nunca antes imaginados. Su importancia reside en que la computación cuántica puede ayudarnos a realizar simulaciones de sistemas cuánticos y resolver problemas que, en simulaciones con computadores clásicos, conllevan un coste exponencialmente mayor. Problemas como la simulación de moléculas, ensayo de medicamentos o incluso en campos de la logística y las finanzas.

Lejos de profundizar en los numerosos campos en los que un trabajo como este está sustentado (véase el álgebra lineal, la mecánica cuántica, teoría sobre circuitos superconductores, teoría de la información, etc.) lo que se pretende es revisar el trabajo realizado por otros en el campo de la computación cuántica y sus últimos avances. Por ello, se requerirán algunas nociones básicas en estos campos para poder entender completamente sobre lo que discutimos y los diferentes conceptos y formalismos que utilizamos.

La manera de proceder que vamos a seguir será dar primero una visión general de los conceptos básicos de la computación cuántica, tales como el qubit, la unidad básica de la computación cuántica, su formalismo, ventajas y formas de manipularlos. Además, explicaremos lo que son las puertas lógicas cuánticas, con su notación y sus requerimientos, y los algoritmos cuánticos, explicando los más básicos y viendo qué utilidad tienen.

Tras ello, haremos una introducción a circuitos superconductores. Estos son una de las muchas formas en las que podemos llevar a realidad los qubits y manipularlos, por lo que son un componente básico en la construcción de computadores cuánticos. Una vez tengamos una idea de ello, expondremos los conceptos básicos de la teoría del "Quantum speckle", algoritmo usado por Google para alcanzar la supremacía cuántica. Este algoritmo plantea una tarea en la cual un computador cuántico puede llegar a límites de cálculo inalcanzables por una máquina clásica (requeriría un tiempo muy elevado y el uso de componentes mucho más eficientes). Y por último, habiendo introducido los campos anteriores, desglosaremos el experimento realizado por Google, llegando a comprender tanto el paso adelante que se ha alcanzado con él y las dificultades que este planteaba, como futuros retos para la comunidad científica.

2 Computación cuántica

2.1 Bit cuántico

2.1.1 Comparación bit-bit cuántico

La noción de bit cuántico (o qubit) es algo fundamental cuando nos aproximamos por primera vez a la teoría de computación cuántica. Para explicarlos, primero debemos tener una idea de lo que son los bits clásicos y cuan importantes son a la hora de construir nuestros ordenadores actuales. La información del capítulo 2 está basada en la información del libro [1], el cual se considera como uno de los mejores libros a la hora de introducirse en el mundo de la computación cuántica. Específicamente del capítulo 1 de este libro.

Un bit es una representación de un dígito, ya sea 0 o 1. Basado en los bits, podemos construir un sistema de numeración binario, con lo cual podemos representar cualquier cifra con combinaciones de 0 y 1. En este concepto se fundamentan todos los aparatos electrónicos actuales. Podemos así implementar algoritmos para realizar operaciones matemáticas (ya sea sumar, multiplicar, etc.) que actúen en función de si el dígito que se observa es uno u otro. Lo que nos bastaría para llevar toda esta idea matemática a la práctica es cualquier sistema físico que se pueda modelar como esta base discreta. Para ello podemos usar el paso o no de la corriente por un cable, por ejemplo. Si en el cable pasa corriente, eso representaría al 1 y, en caso contrario, al 0.

Todo el avance tecnológico desde los años cuarenta hasta hoy se ha concentrado en mejorar las memorias para almacenar más y más 0 y 1 al mismo tiempo (véanse las memorias RAM) y las máquinas encargadas de las tomas de decisiones lógicas basadas en estos dígitos (procesadores). El qubit nos plantea un camino alternativo para la construcción de computadoras debido a su naturaleza cuántica.

El qubit es el análogo cuántico del bit. Son objetos matemáticos que cumplen ciertas propiedades que iremos desglosando a lo largo de la sección. La manera de llevar estos objetos matemáticos a la realidad será discutida en la sección 3. Los qubits tienen también como estados posibles a $|0\rangle$ y $|1\rangle$ (a partir de ahora usaremos la notación de Dirac). La diferencia de

estos con los clásicos reside en que los qubits se pueden encontrar en una combinación lineal de ambos, una superposición. Podemos representar un estado como:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

donde los coeficientes α y β son números complejos, cuyos módulos cuadrados representan la probabilidad de cada estado. Por tanto, se cumple que $|\alpha|^2 + |\beta|^2 = 1$, siendo ψ un vector del espacio complejo bidimensional. Cuando realicemos una medida sobre el sistema, el resultado que obtengamos seguirá siendo 0 o 1, como en el caso clásico, pero no podremos saber, a priori, el resultado que nos dará, sino que sabremos que será 0 con una probabilidad de $|\alpha|^2$ y 1 con una probabilidad de $|\beta|^2$.

Aquí es donde reside la ventaja de la computación cuántica frente a la clásica. Al movernos en un espacio continuo (las infinitas combinaciones de los estados $|0\rangle$ y $|1\rangle$) en lugar de un espacio discreto, uno podría decir que los resultados que obtenemos usando los qubits van contra el sentido común. Nada más lejos de la realidad, los qubits solo obedecen los postulados de la mecánica cuántica. Según uno de estos, el estado del sistema se presenta como una superposición de todos los posibles hasta que se realiza una medida sobre él.

Por tanto, aunque en el momento de realizar la medida, el qubit es similar al bit clásico en el sentido de que el resultado que nos dará será 0 o 1, nos podemos aprovechar de que, hasta el momento de medirlo, la naturaleza cuántica de estos hace que se contemplen todas las posibles combinaciones de ambos. El potencial de esto es enorme, en el sentido de que si conseguimos manejar qubits sin necesidad de medirlos, la cantidad de información que nos ofrecen es exponencialmente mayor que el caso clásico.

2.1.2 Esfera de Bloch

Una forma muy útil de representar el estado de un qubit es la "Esfera de Bloch". Esta es una representación geométrica de la superposición en la que un qubit se encuentra, y es bastante aclaratoria a la hora de explicar operaciones con qubits, como haremos en la sección 2.2. Se basa en que el módulo del estado debe ser 1 (el módulo vendrá representado por la longitud del vector en la esfera). Así, uno puede construir una esfera de radio 1 donde se vea el estado en el que se encuentra el qubit.

Uno puede reescribir la ecuación 2.1 como:

$$|\psi\rangle = e^{i\gamma}[cos(\theta/2)\,|0\rangle + e^{i\phi}sin(\theta/2)\,|1\rangle], \tag{2.2}$$

donde θ, ϕ y γ son números reales. El factor $e^{i\gamma}$, como sabemos de mecánica cuántica, no tiene

ningún efecto observable al ser un factor de fase. Podemos escribir entonces:

$$|\psi\rangle = cos(\theta/2)\,|0\rangle + e^{i\phi} sin(\theta/2)\,|1\rangle\,. \tag{2.3}$$

Los parámetros θ y ϕ definen un punto en la esfera de radio unidad en el espacio tridimensional. Esta esfera es la que definiremos como "Esfera de Bloch". Esta nos será muy útil a la hora de visualizar estados de un único qubit y las operaciones que a este le apliquemos (serán giros en esta representación). El caso de múltiples qubits no tiene análogo.

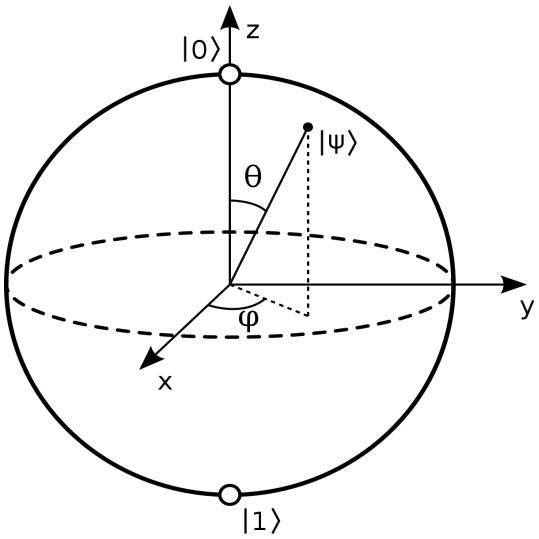


Figura 2.1: Representación de un qubit en la esfera de Bloch. Imagen tomada de [2].

2.1.3 Múltiples qubits

Surge ahora la idea de manipular, en lugar de un solo qubit, varios al mismo tiempo. ¿Qué tipo de ventajas conlleva? De la misma manera que hicimos antes, haremos la analogía con bits clásicos primero. En este caso, si imaginamos que tenemos 2 bits clásicos, la combinación de estos nos dará 4 posibles resultados: 00,01,10 o 11. En el caso de los qubits, los resultados que obtendremos al realizar las correspondientes medidas serán los mismos: $|00\rangle$,$|01\rangle$,$|10\rangle$ o $|11\rangle$. Sin embargo, antes de realizar la medida, estos dos qubits existen en una superposición de los cuatro posibles estados que podemos expresar como:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,, \tag{2.4}$$

donde se sigue cumpliendo la condición de normalización (la suma de las probabilidades es igual a 1). Esta condición se expresa como $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$, donde $\{0,1\}^2$ define las cadenas de longitud 2 compuestas de 0 y 1. La condición de normalización, además, impone que una

vez medimos solo 1 qubit, se produce una renormalización de las probabilidades en la medida del otro.

Generalizando la idea de las cadenas de qubits, si consideramos un sistema de n qubits, construiríamos una base computacional de estados de la forma $\{0,1\}^n$, donde la amplitud del sistema sería 2^n. Si componemos un sistema de, por ejemplo, $n = 100$ qubits, si eso fuera tecnológicamente posible (actualmente el mayor sistema de qubits que se ha podido construir es de $n = 53$ qubits, según el artículo [27]), la amplitud del sistema sería de 2^{100}, amplitud inalcanzable para cualquier computador clásico imaginable. En la capacidad de los computadores cuánticos de manejar esa cantidad de "información oculta" y hacer operaciones con ella reside el poder inigualable de este campo.

2.2 Puertas lógicas cuánticas

Una vez hemos entendido las bases en las que se cimientan los qubits, podemos pasar al siguiente nivel en nuestro objetivo de construir un computador basado en qubits, el cual sería, ¿cómo transportar y manipular qubits? Siguiendo con la analogía que llevamos haciendo todo el trabajo, nuestra problemática ahora sería encontrar elementos similares a los cables (para transportar) y las puertas lógicas (para manipular) que se puedan aplicar a los qubits. Los primeros serán tratados en la sección 3, donde veremos que estos serán circuitos superconductores en el caso que nos atañe, pero podrían haber sido también trampas de iones, sistemas basados en resonancia magnética nuclear, etc. Lo que trataremos aquí serán las puertas lógicas cuánticas (análogas a las clásicas), viendo sus propiedades, restricciones y ventajas.

2.2.1 Puertas lógicas cuánticas para un qubit

Empecemos, por ejemplo, con una puerta lógica clásica muy usada, la puerta NOT. Su funcionamiento se basa en cambiar el resultado del bit al que se la aplicamos. Es decir, si tenemos un bit 0, lo cambiamos a 1 y viceversa. Si buscamos una puerta cuántica análoga, debería cumplirse que, al aplicarla, el qubit $|0\rangle$ pasara a $|1\rangle$ y viceversa. Pero cabe plantearse qué ocurre cuando se lo aplicamos a la superposición de estados. Deberá cumplirse que:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \rightarrow \boxed{\mathrm{X}} \rightarrow |\psi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle\,, \tag{2.5}$$

donde hemos representado la puerta NOT como X, al igual que se suele hacer en la bibliografía.

Parece lógico que la representación de las puertas lógicas será mucho más fácil si utilizamos una notación matricial. Si representamos el estado $|\psi\rangle$ matricialmente, tomando la primera

fila como la amplitud de $|0\rangle$ y las segunda como la de $|1\rangle$ nos quedará:

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}. \tag{2.6}$$

De esta imposición, podemos calcular la forma que tendrá la matrix X, quedando su forma como:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.7}$$

La condición que debe cumplirse es que se conserve $|\alpha|^2+|\beta|^2 = 1$. Esto impone una restricción a la hora de construir puertas lógicas cuánticas, la cual es que la matriz que representa a la puerta sea unitaria. De esta manera, se conservará la probabilidad. ¿Qué quiere decir que una matriz sea unitaria? Una matriz unitaria U es una matriz compleja que cumple la condición $UU^\dagger = U^\dagger U = I_n$, donde I_n es la matriz unitaria y $U^\dagger$ es la matriz traspuesta conjugada.

Esta es la única condición que una puerta cuántica debe cumplir. A partir de ella, uno puede construir cualquier tipo de operación, siempre y cuando respete la conservación de la probabilidad. Dos de las puertas más utilizadas, junto con la NOT, son la puerta Z y la puerta de Hadamard (H), que se definen como sigue:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.8}$$

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.9}$$

Es fácil comprobar que ambas son unitarias. La puerta Z actúa dejando $|0\rangle$ invariante y dando la vuelta a $|1\rangle$, haciéndolo $|-1\rangle$, mientras la descripción de cómo actúa H es algo más compleja. H actúa sobre $|0\rangle$ convirtiéndolo a $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$, y sobre $|1\rangle$ convirtiéndolo a $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. A la hora de entender la manera en que H actúa , es útil ver cómo lo hace en la esfera de Bloch sobre un estado cualquiera. Esto se describe en la imagen 2.2

2.2.2 Puertas cuánticas para múltiples qubits

Como sabemos, en computación clásica, existen puertas lógicas que son aplicables a un solo bit (véase la puerta NOT), al igual que existen puertas lógicas aplicables a múltiples bits. Ejemplos de estas serían las puertas AND, OR o XOR, entre muchas otras. Este tipo de puertas lógicas

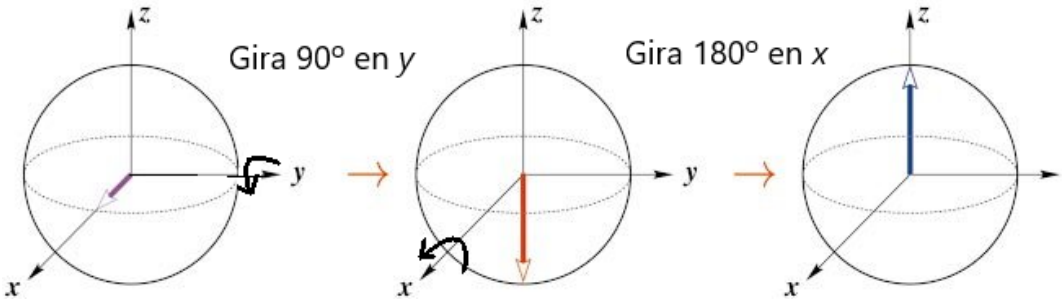
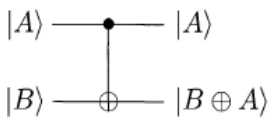


Figura 2.2: Puerta de Hadamard en la esfera de Bloch. Imagen editada. Original de [1].

existen también cuando hablamos de qubits. Este tipo de puertas toman como referencia uno de los qubits y, dependiendo de cual sea su estado, actúan de una manera o de otra sobre el otro qubit. La puerta más útil de todas las existentes es la CNOT. Esta actúa de la siguiente manera: Si el primer qubit, o qubit de control como será llamado a partir de ahora, está fijado en 0, entonces deja invariante el segundo qubit, o qubit objetivo. Si, por el contrario, el qubit de control es un 1, actúa cambiando el qubit objetivo de 0 a 1 o viceversa. Esta operación se puede resumir como $|A, B\rangle \rightarrow |A, A \oplus B\rangle$ siendo $\oplus$ la suma de módulo dos.

Esta puerta es de vital importancia ya que, al igual que en el caso clásico existe un resultado que demuestra que cualquier puerta lógica se puede describir como una composición de puertas NAND, en el caso cuántico existe un resultado similar basado en combinaciones de puertas CNOT y puertas para un solo bit.

Al igual que las puertas de un qubit eran siempre matrices 2x2 debido a las restricciones que existen, las puertas para 2 qubits vendrán representadas por matrices 4x4, que deberán respetar la condición de unitariedad. En general, si estamos trabajando con n qubits, la matriz correspondiente a una puerta para ellos será de tamaño 2^nx2^n.



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Figura 2.3: Representación, tanto esquemática como matricial, de una puerta CNOT. Imagen tomada de [1].

2.3 Algoritmos cuánticos

2.3.1 Circuitos cuánticos

A la hora de describir los circuitos cuánticos, aunque ya hemos descrito algunos de los más básicos, debemos especificar cómo interpretarlos. Las representaciones de ellos se leen de izquierda a derecha y cada línea que vemos es equivalente a un cable. No necesariamente debe ser un cable físico, sino que puede tratarse del paso del tiempo, el movimiento de una partícula, como un fotón, en el espacio, etc.

Existen bastantes restricciones a la hora de comparar los circuitos clásicos con los cuánticos. La primera de ellas es que no se permiten crear "loops", es decir, que una parte del circuito alimente a otra, aunque sí que es posible la creación de híbridos clásico-cuántico, donde exista un feedback en el circuito de una parte a otra. Otra es que no se permite la operación conocida como FANIN (ver ref. [3]), al no ser reversible. Al igual que esta, la operación FANOUT también está restringida. Sin embargo, la propiedad más llamativa que está restringida probablemente sea la de copiar qubits. Este resultado es fundamental en la computación cuántica y afirma que, dado un estado $|\psi\rangle$ desconocido, es imposible crear un estado $|\psi\rangle\,|\psi\rangle$ mediante una operación unitaria. Este resultado es el conocido como *teorema de no clonación* (ver ref. [4] para más detalle).

Dos de las puertas más utilizadas a la hora de hacer circuitos son la puerta controlled-U y la operación de medida (M), ya que no se la puede considear una puerta como tal al no ser unitaria. Controlled-U actúa como una puerta CNOT, pero aplicada a n qubits, teniendo un qubit de control y $n-1$ qubits objetivo sobre los que actúa la puerta unitaria U condicional al qubit de control. Por otra parte, la operación de medida, como su nombre da a entender, convierte un qubit en un estado $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ a un bit clásico M, que será igual a 0 con probabilidad $|\alpha|^2$ e igual a 1 con probabilidad $|\beta|^2$.

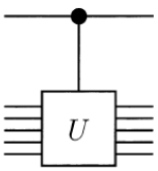


Figura 2.4: Representación de una puerta U. Imagen tomada de [1].

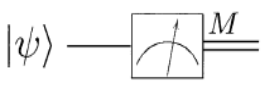


Figura 2.5: Representación de una puerta de medida. Imagen tomada de [1].

Uno de los circuitos más útiles construibles está mostrado en la imagen 2.6, en el que se aplica primero una puerta de Hadamard y una CNOT tras ella a dos qubits. Este circuito permite obtener como estados de salida los "*estados de Bell* ":

$$|\beta_{xy}\rangle = \frac{(|0, y\rangle + (-1)^x |1, \bar{y}\rangle)}{\sqrt{2}}, \tag{2.10}$$

donde x e y pueden ser 0 o 1 e $\bar{y}$ es la negación de y. Estos estados, por su extrañas características físicas, han sido objeto de muchos estudios y nos resultarán útiles en diferentes algoritmos.

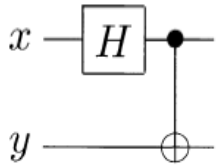


Figura 2.6: Circuito para crear estados de Bell. Imagen tomada de [1]

2.3.2 Paralelismo cuántico

El paralelismo cuántico es una propiedad fundamental de la cual podemos obtener muchísima ventaja a la hora de computar qubits. Es una propiedad intrínseca derivada de los postulados sobre los que se define la mecánica cuántica. Más que la superposición de 0 y 1, el paralelismo (junto con el entrelazamiento) son las propiedades que marcan la diferencia a la hora de tratar con bits clásicos, ya que se presentan como una interacción no local que nos permite expresar diferentes cadenas binarias al mismo tiempo. Esto nos permite aplicarle transformaciones al conjunto de cadenas superpuestas simultáneamente.

Por ejemplo, si consideramos una función $f(x)$ tal que $f(x) : 0, 1 \to 0, 1$, podemos construir un circuito, ilustrado en la imagen 2.7, donde la transformación U_f actúa de manera que $|x, y\rangle \to |x, y \oplus f(x)\rangle$. Podemos evaluar entonces $f(x)$ para dos valores de x al mismo tiempo, aprovechando la propiedad de la superposición del estado preparado. El estado que se introduce en x es fácilmente creado aplicando una puerta de Hadamard a un qubit $|0\rangle$.

$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}. \tag{2.11}$$

Esta propiedad se puede generalizar para n bits, pudiendo evaluarse todos los posibles valores de f simultáneamente en una sola medida. En esto se basarán los algoritmos que serán explicados en la siguiente sección. En general, si preparamos $n + 1$ qubits $|0\rangle^n |0\rangle$, y le aplicamos

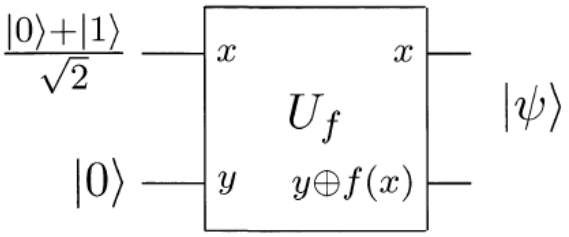


Figura 2.7: Circuito para evaluar $f(x)$ en $|0\rangle$ y $|1\rangle$ (a partir de ahora llamado "caja negra") simultáneamente. Imagen tomada de [1].

puertas de Hadamard a los n primeros, para luego evaluar U_f, obtendremos el estado:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|f(x)\rangle\,. \tag{2.12}$$

2.3.3 Entrelazamiento cuántico

El entrelazamiento cuántico juega un papel fundamental en la computación cuántica. Este fenómeno no tiene equivalente clásico y, durante mucho tiempo, sirvió para poner en entredicho los pilares en los que la teoría cuántica estaba sustentada. Fue predicho en 1935 por Einstein, Podolsky y Rosen (EPR) en su experimento mental, que presentaba una paradoja en la física vigente. Se da cuando un conjunto de partículas no pueden definirse como partículas individuales, para el caso de dos partículas, $\psi(x_1,t)\psi(x_2,t)$. Para describirlas, habría que hacerlo como un sistema con una función de onda única para todo el sistema $\psi(x_1,x_2,t)$.

Esta propiedad, que a primera vista no pareciera nada extraño, tiene implícita en ella una característica que utilizaron para desacreditar la teoría cuántica, y es que si tenemos un sistema de dos partículas, por ejemplo, con espín total 0, separamos las partículas y medimos el espín de una, instantáneamente conoceríamos que el espín de la otra es el contrario. Esto conllevaba que había una comunicación entre las dos partículas que se producía a una velocidad mayor que la de la luz, algo supuestamente imposible, al igual que violaba el realismo local.

Con el tiempo, se demostró que esta propiedad no desacredita la teoría cuántica, sino que es una propiedad sutil de esta. La razón que se esgrimió es que no se puede transmitir información clásica a velocidad superior a la de la luz, ya que solo es posible transmitir información con un conjunto entrelazado por medio de canales de información clásico. Esto es la teleportación cuántica (ver ref. [5]). Sin embargo, la necesidad del canal de información clásico hace que la transmisión de información útil no sea a una velocidad prohibida.

Tras años de estudio, la paradoja EPR fue analizada con más detalle y enfocada por Bell (ver ref.

[6]), el cual explicó que la propiedad matemática que subyace a la propiedad física de entrelazamiento es la llamada no separabilidad (no es posible factorizar la distribución de probabilidad estadística de dos variables estocásticas como producto de distribuciones independientes respectivas)(ver ref. [7]). Este notable científico ideó una serie de experimentos, con una teoría matemática basada en conjunto de probabilidades que daban lugar a las desigualdades de Bell, donde se demostraban todas estas premisas. En ellos se comprobaba que el entrelazamiento cuántico no era ninguna propiedad extraña de la naturaleza cuántica, sino que era una característica inherente a ella, lo que reafirmaban la validez de los postulados de esta, puestos de otra manera en duda debido a las raras consecuencias de esta propiedad, antes no entendida.

Estados que muestran entrelazamiento serían, por ejemplo, los estados de espín 1/2 singlete $|\psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$, o los estados de Bell, ya descritos en 2.10. A la hora de comprobar si un estado es entrelazado o no, uno puede expresar el estado mediante el operador densidad $\rho_\psi(t) \equiv \rho = \sum_j p_j \, |\Psi_j\rangle \langle\Psi_j|$. Todo el formalismo matemático de la mecánica cuántica puede redefinirse en términos de este operador, así como los postulados de esta. La utilidad de esto reside en que, si aplicamos la descomposición de Schmidt a este operador (ver ref. [8]), uno comprueba fácilmente si ese estado es un estado puro o no con tan solo mirar el número de Schmidt. Esto nos simplifica mucho a la hora de generar y comprobar el entrelazamiento de nuestras partículas a partir de su función de onda.

2.3.4 Algoritmos cuánticos comunes

Los algoritmos cuánticos surgen de la necesidad de realizar, con tecnologías cuánticas, tareas que podían ser realizadas por computadores clásicos. Dentro de este ámbito, existen multitud de algoritmos diseñados para realizar tareas clásicas con ordenadores cuánticos. Algunos de mayor utilidad que otros, algunos actualmente "fáciles" de llevar a la práctica y otros que no son más que diseños teóricos que, con las tecnologías actuales, no se han podido realizar en el mundo real. En esta sección explicaremos el primer algoritmo cuántico, el algoritmo de Deutsch-Jozsa, formulado en 1992 y cuyo nombre se debe a sus creadores David Deutsch y Richard Jozsa (ver ref. [9]). Este algoritmo no es de mucha utilidad práctica, ya que su meta es determinar si una función es balanceada o no, pero nos sirve de gran ayuda para entender el paralelismo, el entrelazamiento cuántico y la interferencia en un caso práctico, además de ser el primer ejemplo en el que se comprobó la mejora exponencial en la capacidad de cómputo de estas tecnologías. Para explicar el algoritmo, es bastante útil introducir primero el caso del algoritmo de Deutsch, algo más sencillo y bastante aclarativo a la hora de entender su generalización.

Nuestro objetivo es saber si una caja negra U_f actúa devolviendo siempre 0 o si, por el contrario, actúa de diferente manera dependiendo si el qubit de control es $|0\rangle$ o $|1\rangle$. Para ello, si lo pensamos clásicamente, bastaría con probar una vez con un bit 0 y otra con un bit 1. La

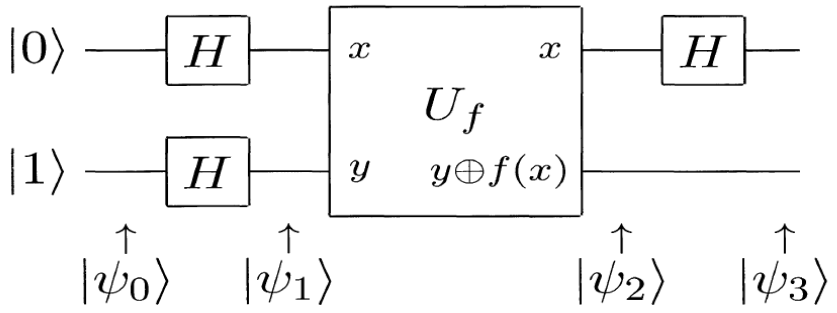


Figura 2.8: Esquema del circuito que realiza el algoritmo de Deutsch. Imagen tomada de [1].

ventaja es que, si pensamos "cuánticamente" podemos solucionar este problema en un solo paso. Consideremos un estado inicial:

$$|\psi_0\rangle = |01\rangle\,. \tag{2.13}$$

Haciendo pasar a cada qubit por una puerta de Hadamard, se crea una superposición que dará como estado:

$$|\psi_1\rangle = \left[\frac{(|0\rangle + |1\rangle)}{\sqrt{2}}\right]\left[\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right]. \tag{2.14}$$

Aplicando ahora U_f al estado resultante, dará:

$$|\psi_2\rangle = \begin{cases} \pm\left[\dfrac{(|0\rangle + |1\rangle)}{\sqrt{2}}\right]\left[\dfrac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right] & \text{si } f(0) = f(1). \\ \pm\left[\dfrac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right]\left[\dfrac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right] & \text{si } f(0) \neq f(1). \end{cases} \tag{2.15}$$

Si pasamos por una puerta de Hadamard al primer qubit queda:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right] & \text{si } f(0) = f(1), \\ \pm|1\rangle\left[\dfrac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right] & \text{si } f(0) \neq f(1), \end{cases} \tag{2.16}$$

que se puede escribir como:

$$|\psi_3\rangle = \pm\,|f(0)\oplus f(1)\rangle \left[\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right]. \tag{2.17}$$

Así que, haciendo solo la medida del primer qubit, uno puede determinar $f(0)\oplus f(1)$, y por tanto obtener una característica global del sistema, midiendo solo un qubit, ya que $f(0)\oplus f(1)$ es 0 si $f(0) = f(1)$ y 1 si $f(0) \neq f(1)$.

Si queremos generalizar, tomando n qubits de control en el estado $|0\rangle$ y un qubit en el estado $|1\rangle$ nuestro estado inicial sería:

$$|\psi_0\rangle = |0\rangle^{\otimes n}\,|1\rangle\,. \tag{2.18}$$

Aplicando la transformada de Hadamard en el registro de control y la puerta de Hadamard al qubit objetivo se tiene el estado como:

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right]. \tag{2.19}$$

Aplicándole a este estos qubits la caja negra U_f, cuya forma de proceder ya hemos descrito, tenemos:

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}\,|x\rangle}{\sqrt{2^n}} \left[\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right]. \tag{2.20}$$

Tras estas operaciones, se aplica la transformada de Hadamard de nuevo a los n qubits de registro. Esta operación no es trivial y, para generalizar el resultado, podemos comprobar como actúa la puerta de Hadamard en un estado $|x\rangle$ primero, para luego escribir el resultado más general.

Para x=0:

$$H\,|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{(-1)^{0\cdot 0}\,|0\rangle}{\sqrt{2}} + \frac{(-1)^{0\cdot 1}\,|1\rangle}{\sqrt{2}} = \sum_z \frac{(-1)^{0\cdot z}\,|z\rangle}{\sqrt{2}} = \sum_z \frac{(-1)^{x\cdot z}\,|z\rangle}{\sqrt{2}}. \tag{2.21}$$

Igualmente para x=1:

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{(-1)^{1\cdot 0}|0\rangle}{\sqrt{2}} + \frac{(-1)^{1\cdot 1}|1\rangle}{\sqrt{2}} = \sum_z \frac{(-1)^{1\cdot z}|z\rangle}{\sqrt{2}} = \sum_z \frac{(-1)^{x\cdot z}|z\rangle}{\sqrt{2}}. \tag{2.22}$$

Así, generalizando el resultado que hemos obtenido para 1 qubit, si consideramos el conjunto de los n qubits de control:

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}, \tag{2.23}$$

siendo $x \cdot z$ el productor interior de módulo 2 de x con z. Llegamos a la conclusión que el estado $|\psi_3\rangle$ puede escribirse como:

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{\sqrt{2^n}} \left[\frac{(|0\rangle - |1\rangle)}{\sqrt{2}}\right]. \tag{2.24}$$

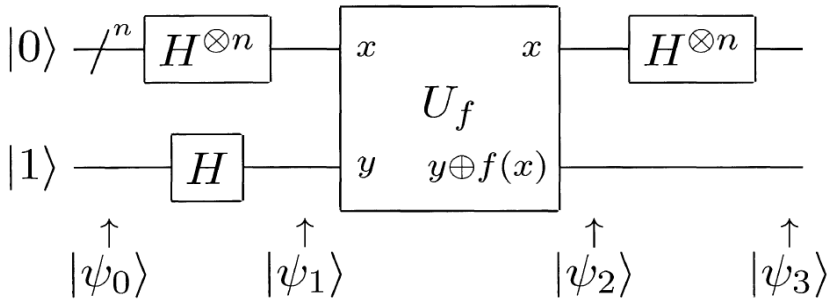


Figura 2.9: Implementación del algoritmo de Deutsch-Jozsa. Imagen tomada de [1].

Sabemos que la amplitud del estado $|0\rangle^{\otimes n}$ es $\sum_x (-1)^{f(x)}/2^n$. Ahora consideremos los casos posibles. En caso de que f sea constante, se puede comprobar que ese sumatorio es +1 ó -1 dependiendo del valor de $f(x)$. Como ya sabemos que el módulo de $|\psi_3\rangle$ debe ser 1, el resto de qubits (en nuestro caso el qubit objetivo) debe resultar en un valor 0, para que la condición del módulo se conserve.

Si, por el contrario, f es balanceada, el sumatorio se anulará por parejas, resultando en una amplitud igual a 0. Debido a la condición del módulo del estado, nuestro qubit restante deberá resultar en un valor de 1. Por tanto, con una sola evaluación del qubit objetivo, podemos discernir si $f(x)$ es balanceada o constante.

Si intentáramos realizar esta operación de manera clásica, se requerirían, al menos, $2^n/2 + 1$ observaciones, y eso sería solo en el caso de que la función fuera balanceada, ya que comprobaríamos la primera mitad de bits y todos saldrían 0 y, si miráramos luego el siguiente y fuera

1, ya comprobaríamos que es balanceada. Si fuera igual a 0, deberíamos seguir mirando el resto de bits para comprobar que todos dan el mismo resultado.

En este drástico cambio del número de medidas necesarias está la gran ventaja del algoritmo. Y, aunque la utilidad de este algoritmo no parece gran cosa, existen algoritmos basados en las propiedades de la mecánica cuántica como este que sí que tendrían una gran utilidad. Hablamos, por ejemplo, del algoritmo de Shor (para ver el formalismo de este algoritmo y saber más ir a ref. [10]) que sirve para descomponer en factores un número N de manera eficiente.

Este algoritmo, cuya implementación no ha sido llevada a cabo para números significativos, aunque sí que lo han hecho para factorizar números simples (como 15= 3 x 5), tiene gran importancia debido a que, si llegamos a conseguirlo, cambiaría las reglas de la criptografía de clave pública, como la RSA[1]. Esto se debe a que, para descifrar mensajes, es necesario descomponer en factores primos grandes números. Esta tarea no puede ser llevada a cabo por computadoras clásicas en un tiempo $O((logN)^k$, de manera que, a medida que aumentamos N, los computadores conocidos se vuelven inútiles. Sin embargo, con el algoritmo de Shor, se puede romper el algoritmo RSA en un tiempo polinómico, lo que bastaría para descifrar toda la criptografía actual. Aunque la manera de realizar esto sea probabilística, esto supondría una nueva era en la criptografía y la ciberseguridad. Pero podemos estar tranquilos, ya que aún se está lejos de implementar este algoritmo para números mayores de 3 cifras y deberán hacerse muchos avances tecnológicos antes de poder traerlo a la realidad de manera eficiente.

Otro de los algoritmos cuánticos conocidos es el algoritmo de Grover [11], cuyo objetivo es el buscar en una secuencia de N datos no ordenada. La mejora de este algoritmo es que lo puede realizar en un tiempo $O(N^{1/2})$ en comparación con los algoritmos clásicos, que realizarían esto en un tiempo $O(N)$, por tanto hay una mejora en el algoritmo del orden de la raíz cuadrada. Al igual que en el caso de Shor, los resultados de este algoritmo son probabilísticos, aunque se puede obtener una probabilidad de error más y más baja a medida que se aumentan las interacciones entre los qubits.

2.4 Información cuántica y dificultades

A la hora de construir un aparato de procesado de información cuántico, toda la teoría vista nos permite comprobar que será mucho más potente que cualquiera clásico. La pregunta que aparece ahora es, ¿qué tipo de dificultades derivan de la construcción de un dispositivo como este? ¿Cuánta información somos capaces de procesar de manera eficiente? ¿Qué limitaciones nos encontramos cuando tratamos con este tipo de dispositivos? Todas estas preguntas intentarán ser respondidas brevemente en esta sección, aunque para tratar todo este tipo de preguntas existe una amplia teoría (teoría de información cuántica), a la que remitimos al lector si está

[1]Sistema criptográfico de clave pública más utilizado.

más interesado en este campo.

El primero de los problemas que aparecen a la hora de tratar con la información de manera cuántica es el del ruido. Gracias al teorema del umbral de ruido, sabemos que, dado un nivel de ruido para un computador cuántico, somos capaces de reducir el nivel de este por debajo de un valor umbral a costa de una complicación relativamente pequeña en la computación.

La dificultad de reducir estos niveles de ruido no solo reside en el nivel tecnológico que se tenga a la hora de construir los qubits, las puertas cuánticas, etc., sino que también existen trabas a la hora de comprimir los mensajes que pretendemos transmitir y la información con la que deseamos trabajar. Los resultados básicos a la hora de considerar estas preguntas serán el *teorema de codificación en un canal sin ruido* y *teorema de codificación en un canal con ruido* de Shannon, donde el primero cuantifica cuantos bits se necesitan para almacenar información emitida por una fuente de información, y el segundo cuantifica como de fiable es la información transmitida a través de un canal con ruido (ver ref. [12]).

En la analogía clásica, podemos definir una fuente de información como un conjunto de probabilidades $p_j, j = 1, 2..., d$. Cada uso de la fuente sería como elegir la letra j con probabilidad p_j. Ahora, si sabemos que algunas letras son más probables que otras, podemos hacer una distribución de probabilidades determinadas para los p_j y así reducir el número de bits utilizados para comprimir esta información. El *teorema de codificación en un canal sin ruido* nos dice que una fuente como la descrita puede ser comprimida de manera que, en promedio, cada uso de esta puede ser representada usando $H(p_j)$ bits de información, siendo $H(p_j) \equiv -\sum_j p_j log(p_j)$ (entropía de Shannon).

Tocaría, ahora, definir un análogo para el caso cuántico. Una fuente de información cuántica será descrita por un conjunto de probabilidades p_j y sus correspondientes estados $|\psi_j\rangle$, donde cada uso de la fuente produciría un estado $|\psi_j\rangle$ con probabilidad p_j. En lo relativo a la compresión de nuestro mensaje, debemos tener en cuenta que ahora existiría un error asociado a la distorsión relacionada a la compresión del mensaje. Para medir esta, se introduce un parámetro de *fidelidad*, que cuantifica cómo de bien se ha comprimido-descomprimido nuestro estado.

Al igual que en el caso clásico, existe un *teorema de codificación en un canal sin ruido* nombrado en honor a su creador (Schumacher), que incluye la restricción de que sea posible recuperar la información con una fidelidad cercana a 1. Lo curioso es que, en el caso de que los estados sean ortogonales, el límite de compresión de la fuente coincide con el límite clásico de Shannon ($H(p_j)$, pero si consideramos el caso más general, donde los estados no son ortogonales necesariamente, el límite ya no es el clásico, sino que podemos llegar a un límite estrictamente menor, la *Entropía de Von Neumann*, permitiéndonos comprimir aún más la información transmitida por la fuente. El concepto de entropía como medida de incertidumbre de una fuente de

información será muy importante a la hora de hablar del algoritmo utilizado por Google en la sección 4.

3 Circuitos superconductores

Aquí pretendemos dar una idea sobre como los circuitos superconductores pueden comportarse como átomos, en el sentido de que experimentan transiciones entre dos niveles de energía, lo que puede ser utilizado para modelarlos como qubits. Esta propiedad introduce una ventaja a la hora de trabajar, la cual es que se pueden comprobar comportamientos cuánticos a escalas macroscópicas en ellos.

La composición de esta sección está fundamentada en el paper [13], tratando de explicar los resultados que muestran, sin profundizar sobremanera en el formalismo matemático ni en la ingeniería detrás de los circuitos superconductores e intentando dar una idea de la modelización de estos a un nivel accesible a estudiantes de Grado.

La meta de construir un computador cuántico conlleva la necesidad de ser capaz de preparar, manipular y leer múltiples qubits al mismo tiempo, además de poder modificarlos de manera individual. En la situación más óptima, todas estas propiedades deberían complementarse con la propiedad de que el sistema sea escalable (aumento de capacidad con el aumento de componentes).

Los circuitos superconductores son una de las maneras de traer a la realidad todas estas características. Grosso modo, los materiales superconductores son materiales que no presentan ninguna resistencia eléctrica al paso de electrones a través de ellos. Los electrones en estos materiales, según la teoría BCS [14], se aparean formando un par de fermiones que se comportan como bosones (par de Cooper) que condensan en un único nivel de energía fundamental, similar al condensado de Bose-Einstein [15]. Además, a menor tamaño, menor acoplamiento con el entorno y mejor coherencia cuántica.

Podemos hacer una analogía entre los circuitos superconductores y los átomos. Por una parte, ambos presentan niveles de energía discretos y oscilaciones cuánticas coherentes entre estos niveles. Estas oscilaciones, las oscilaciones de Rabi [16], son una prueba del acoplamiento entre el átomo y el pulso del campo que le apliquemos. Son, para ser más concretos, el intercambio de energía coherente entre un campo electromagnético cuantizado y cualquier sistema de dos niveles de energía. Este intercambio suele producirse en una cavidad de láser, y ocurre con una

tasa proporcional a ν, es decir, al campo aplicado. Los fotones de diferentes longitudes de onda que se le aplicarían a los átomos para excitar sus electrones, serían para nuestros circuitos corrientes y voltajes aplicados, que harán que cambien sus niveles de energía.

Por otra parte, los circuitos, a diferencia de los átomos, pueden ser diseñados para tener ciertas características que nos beneficien, véanse frecuencias de transición, momentos dipolares, etc. Estos circuitos superconductores se construyen mediante uniones Josephson, que aprovechan el hecho de que se puede transmitir corriente eléctrica a través de dos superconductores separados gracias al efecto túnel. Es necesario hablar de dos escalas de energías que determinarán el comportamiento de estos: La energía de acoplamiento de Josephson, $E_J = I_c\phi_0/2\pi$, siendo I_c la corriente crítica y $\phi_0 = h/2e$, y la energía de carga para un par de Cooper, $E_c = (2e)^2/2C$, donde C es la capacidad de una unión de Josephson. Por último, cabe decir que la fase ϕ de la función de onda de un par de Cooper y el número n de pares de Cooper cumplen la relación de incertidumbre de Heisenberg: $\Delta n \Delta\phi \geq 1$.

3.1 Qubits de carga y de carga-flujo

Este tipo de qubits se construyen sobre una pequeña "isla", llamada "caja de pares de Cooper" [18], que se conecta con el entorno mediante una o dos uniones de Josephson, anteriormente explicadas, y es controlada por una fuente de voltaje a través de una capacitancia de puerta. Su nombre se debe a que sus estados fundamentales son estados de carga, es decir, estados que representan la existencia o exceso de pares de Cooper en la isla.

Cabe considerar aquí la modelización del sistema de pares de Cooper en la caja [17]. El hamiltoniano de este sistema (incluyendo la fuente de voltaje, dado que consideramos un circuito como el de la imagen 3.1) viene dado por:

$$H(n_g) = H_{el} + H_J = E_C(\hat{n} - n_g)^2 - E_J \cos\phi, \tag{3.1}$$

donde E_C y E_J son las energías de carga y de Josephson y ϕ es la diferencia de fase a través de la unión Josephson y es la responsable del tunelado de los pares de Cooper. La fuente de voltaje V_G controla el offset de carga inducido, $n_g = C_g V_g/2e$.

En el régimen de carga solo los dos estados más bajos de cargas son importantes. Estos difieren entre sí en un par de Cooper. Esto se puede ver manipulando un poco el hamiltoniano dado. Para hacer esto, debemos tener en cuenta que el número de pares de Cooper en exceso o en falta se debe modelar como un operador $\hat{n}$, ya que fluctúa de forma cuántica. Sus autoestados serán $|N\rangle_c$, sabiendo además como se relacionan $\hat{n}$ y el operador ϕ: $\exp(\pm i\phi)\,|n\rangle_c = |n \pm 1\rangle_c$.

Podemos reescribir entonces el hamiltoniano en la representación de carga:

$$H(n_g) = \sum_{N\in\mathbb{Z}} = \left[E_C(n-n_g)^2 \left|n\right\rangle_C \left\langle n\right|_C - E_J/2(\left|n\right\rangle_C \left\langle n+1\right|_C + \left|n+1\right\rangle_C \left\langle n\right|_C)\right]. \tag{3.2}$$

Alrededor de $n_g = 1/2$, el sistema puede ser descrito como un sistema físico de dos niveles, con un hamiltoniano reducido:

$$H = E_C(n_g)\sigma_z - 1/2E_J\sigma_x, \tag{3.3}$$

donde las matrices de Pauli son $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ y $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$, definidas en los dos estados de la base, que corresponden a 0 o a 1 par de Cooper en exceso en la caja. Esto hace que la utilización de un aparato de interferencia cuántica conformado por dos uniones haga de E_J una manera de realizar el acoplamiento: $E_J(\phi_{ext}) = 2E_{J0}\cos(\pi\phi_{ext}/\phi_0)$, siendo E_{J0} la energía de acoplamiento Josephson para cada parte de la unión, ϕ_{ext} el flujo magnético externo y ϕ_0 el flujo cuántico.

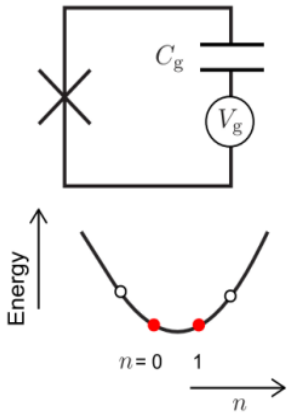


Figura 3.1: Circuito que forma el qubit de carga, junto con la representación de sus estados fundamentales. Imagen tomada de [13].

Se deben considerar dos estados de carga cuando el offset de la caja que induce la fuente V_g es del orden de la carga del electrón, $|0\rangle$ y $|1\rangle$, y dos autoestados de la energía que serían combinación de estos dos, $|\pm\rangle$. A medida que la carga aumenta (el número de pares de Cooper), desde cero, donde los dos estados fundamentales son $|0\rangle$ y $|1\rangle$, gradualmente se comprueba que los niveles fundamentales van cambiando a $|\pm\rangle$, siendo en n_g donde más diferencia se ve, lo que se puede observar en la imagen 3.2.

Se puede aproximar al qubit como un sistema de dos niveles fundamentales de energía. Esto es básicamente lo que se pretende conseguir para construir nuestro computador, tener un sistema

de dos niveles de energía que se comporte de manera cuántica. Esto se puede afirmar, ya que los niveles fundamentales están tan alejados de los niveles superiores que se pueden considerar solo esos dos, en las condiciones óptimas de trabajo. Este gráfico se da para el régimen de carga, donde E_c/E_J es mayor que 1. Estos tipos de qubits están normalmente hechos en materiales superconductores como niobio o aluminio, usando litografía de haces de electrones.

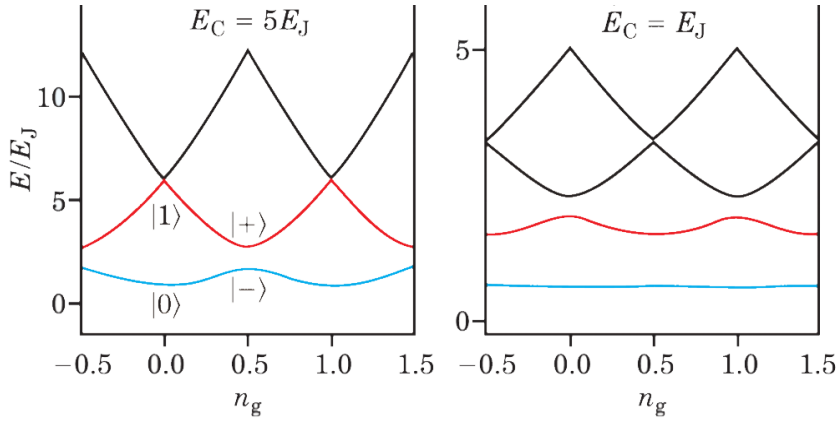


Figura 3.2: Niveles de energía para la caja de pares de Cooper. Imagen tomada de [13], con edición propia.

En el caso de que $E_c/E_J \approx 1$, los grados de libertad de la carga y del flujo juegan un papel similar y los niveles de energía fundamentales no están tan diferenciados de niveles superiores como en el caso del régimen de carga. Cuando el qubit se encuentra en este régimen, se le suele llamar qubit de carga-flujo. Sus dos autoestados más bajos $|\pm\rangle$ son superposición de muchos estados de carga y no solo de $|0\rangle$ y $|1\rangle$, por lo que la única base posible sería $\left[|+\rangle, |-\rangle\right]$.

3.2 Qubits de flujo

Si el grado de libertad de la fase es un valor suficientemente grande, se convierte en el dominante. Esto hace que los qubits pasen a ser de otro tipo, qubits de flujo, los cuales se construyen como se muestra en la figura 3.3. Por lo general, se realiza más de una unión Josephson, a pesar de que la imagen solo muestre una. En ellas la energía de acoplo de Josephson E_J es mucho mayor que la energía de carga para cada unión.

En el proceso de diseño y producción de estos circuitos, los parámetros de unión se diseñan para que una corriente persistente fluya continuamente cuando se aplica un flujo magnético externo. Esto se hace con el propósito de que la supercorriente sea inducida para incrementar o reducir el flujo cerrado, de forma que el fluxoide[1], el cual combina la fase de Josephson ϕ con el flujo magnético total, está cuantizado: $(\phi_0/2\pi)\Phi + \Phi_{ext} + \Phi_{ind} = m\Phi_0$. Estos qubits han sido testados experimentalmente y se observaron oscilaciones cuánticas coherentes en ellos.

[1]El fluxoide en un superconductor es un múltiplo del cuanto de flujo. Coincide con el flujo lejos de su superficie.

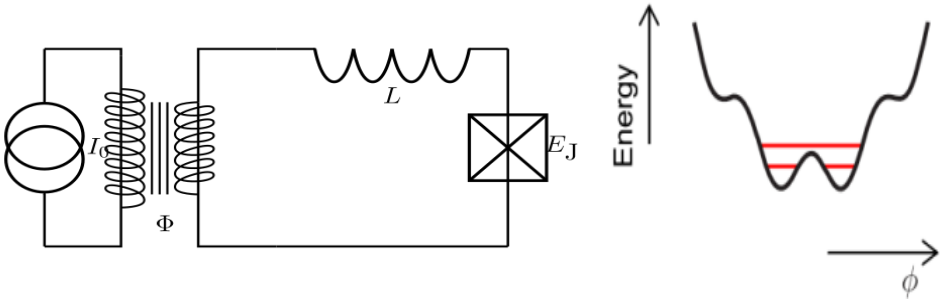


Figura 3.3: Circuito que forma el qubit de flujo, junto con la representación de sus estados fundamentales. Imagen tomada de [13].

La descripción del espectro de energía de este tipo de qubits depende fuertemente del valor de f que consideremos, donde f se define como $f = \Phi_{ext}/\Phi_0$. Como se puede ver, en las proximidades de $f = 0.5$, $|+\rangle$ y $|-\rangle$, que serán los niveles fundamentales, están bien separados de los niveles más altos, y son una superposición de las dos supercorrientes (horaria y antihoraria) $|\uparrow\rangle$ y $|\downarrow\rangle$. A medida que nos alejamos de este valor, $|+\rangle$ y $|-\rangle$ alcanzan a $|\uparrow\rangle$ y $|\downarrow\rangle$, dependiendo de si $f < 0.5$ o $f > 0.5$ se encuentran de una manera o de otra. Por tanto, a la hora de representar el qubit de flujo, es válido tanto el uso de la base $\left[|+\rangle, |-\rangle\right]$ como el de $\left[|\uparrow\rangle, |\downarrow\rangle\right]$. Todo esto se puede ver en la imagen 3.4.

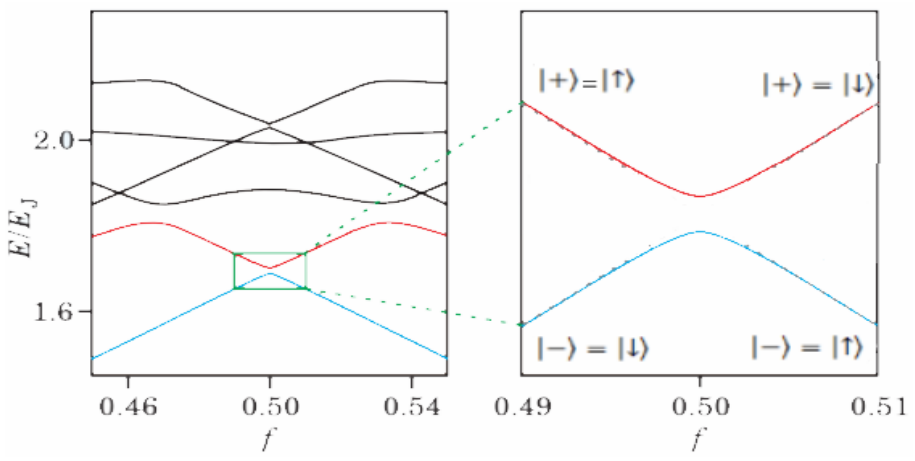


Figura 3.4: Niveles de energía para un qubit de flujo con 3 uniones. Imagen tomada de [13].

3.3 Qubits de fase

Estos qubits utilizan una unión Josephson que posee una unión corriente-bias. La utilización de una señal de bias es fundamental para producir un ladeo al potencial de Josephson de la unión. Bias (o corriente de polarización) es una corriente continua (DC) hecha fluir deliberadamente entre dos puntos con el propósito de controlar el circuito. Este ladeo hace que el el número de estados ligados al pozo de potencial se reduzca. De esta manera, la corriente de polarización

nos sirve para controlar la profundidad del pozo de potencial mostrado en la imagen 3.5, ya que nos ayuda a controlar ϕ, y el potencial de Josephson es proporcional a cos ϕ.

Vemos en el esquema de los niveles de energía que existe un tercer nivel de energía disponible, no muy lejano a los dos niveles básicos. La cercanía del tercer nivel de energía se puede traducir en una ventaja a la hora de determinar la probabilidad de ocupación de los niveles del qubit al poder este estar fuera del pozo de potencial por efecto túnel.

Se puede realizar operaciones lógicas situando el circuito en un campo de microondas de frecuencia $(E_1 - E_0)/h$. Esto sería lo correspondiente a operaciones entre los dos niveles fundamentales. Si se aplica al qubit un pulso de frecuencia $(E_2 - E_1)/h$, produciría transiciones entre los niveles $|1\rangle$ y $|2\rangle$. Se podría entonces saber el estado del qubit midiendo la probabilidad de ocupación de $|2\rangle$. Además, cabe añadir que en estos qubits, E_J/E_C es órdenes de magnitud mayor que en los otros tipos de qubits.

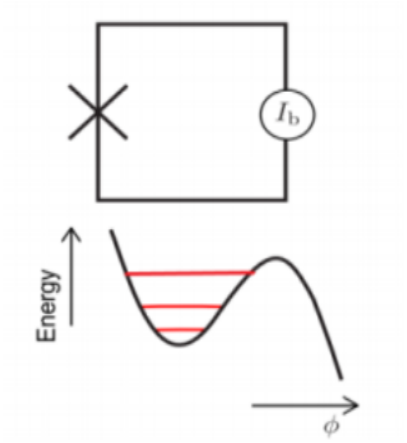


Figura 3.5: Circuito formado por una unión corriente-bias, que forma un qubit de fase. Imagen tomada de [13].

3.4 Electrodinámica cuántica de circuitos, ruido y otras aplicaciones

Para construir computadores cuánticos, necesitamos ser capaces de realizar operaciones de dos qubits y no solo trabajar con qubits individuales. Por tanto, necesitamos alguna manera de acoplar los circuitos explicados durante la sección unos a otros para que actúen de manera conjunta. Para realizar esto, uno puede utilizar condensadores e inducciones.

Controlar el acoplamiento de los condensadores no es una tarea sencilla. Se prefiere tratar generalmente solo con inductancias a la hora de acoplar qubits, ya que producen acoplamientos controlables por flujo magnético cuando trabajan con qubits de carga y pueden llegar a conformar puertas CNOT. Una vez se reproducen las puertas CNOT en circuitos cuánticos, y si se es

capaz de reducir sus errores experimentales, cualquier tipo de puerta lógica sería reproducible, como hemos mencionado en la sección 2.2.2.

También es posible acoplar qubits de flujo. Esto sucede debido a que la energía de acoplamiento de Josephson en los qubits de flujo es mucho mayor que en los qubits de carga, lo que hace que las supercorrientes en los bucles sean mayores, y que con inductancias mucho más pequeñas se produzca un acoplamiento entre qubits mayor. Este acoplo también se puede hacer en qubits de fase. La manera de acoplar qubits experimentalmente está graficada en la figura 3.6, donde están representados diferentes circuitos en los que se acoplan qubits por medio de condensadores, C_m, y/o inductancias, L.

Las oscilaciones de Rabi, por otra parte, ocurren de manera proporcional al acoplamiento sistema-campo. Entre los procesos en los que se observan las oscilaciones de Rabi, el más básico consistiría en la interacción entre un fotón y un sistema de dos niveles. La interacción de estos solo es observable en el régimen de "acoplamiento fuerte", donde el periodo de las oscilaciones de Rabi ($1/\nu$) es mucho más corto que el tiempo de decoherencia del sistema de dos niveles y que el tiempo de vida medio del fotón en la cavidad [2]. El acoplamiento fuerte constituye la base de la llamada electrodinámica cuántica de cavidades.

La coherencia cuántica es una propiedad fundamental a la hora de construir qubits acoplados. Por ello se busca siempre el mayor valor de esta en los circuitos que hemos visto. En ellos, existe también un nivel de ruido que no podemos despreciar. Este ruido se debe tanto al acoplamiento entre los circuitos y el entorno, como a posibles errores que se den en el circuito a la hora de acoplar qubits, aunque estos pueden ser fácilmente corregidos con diferentes códigos como veremos más adelante.

En la gran mayoría de qubits que hemos visto, el término de decoherencia debida al ruido que predomina es un término $1/f$. Si nos centramos en casos concretos, en los qubits de carga, este término es principalmente debido a fluctuaciones de carga. Estas fluctuaciones pueden ser, por ejemplo, cargas atrapadas entre el sustrato y las capas de óxido de las uniones Josephson.

Entender y modelar el problema de la decoherencia sigue siendo un reto para la comunidad científica. Muchos modelos han sido probados para representarla, tales como el modelo de espín-bosón (ver ref. [19]) y el de espín-fluctuador (ver ref. [20]). Sin embargo, se requieren teorías fenomenológicas a escalas microscópicas a la hora de entender los fenómenos que se esconden tras el ruido $1/f$.

Por otra parte, el desarrollo de circuitos superconductores nos da una herramienta muy útil a la hora de comprobar características de la mecánica cuántica a nivel experimental. Así, se pueden utilizar para comprobar las desigualdades de Bell (ver ref. [21]), para producir estados

[2] Un volumen cerrado por paredes conductoras donde se puede extraer o añadir energía.

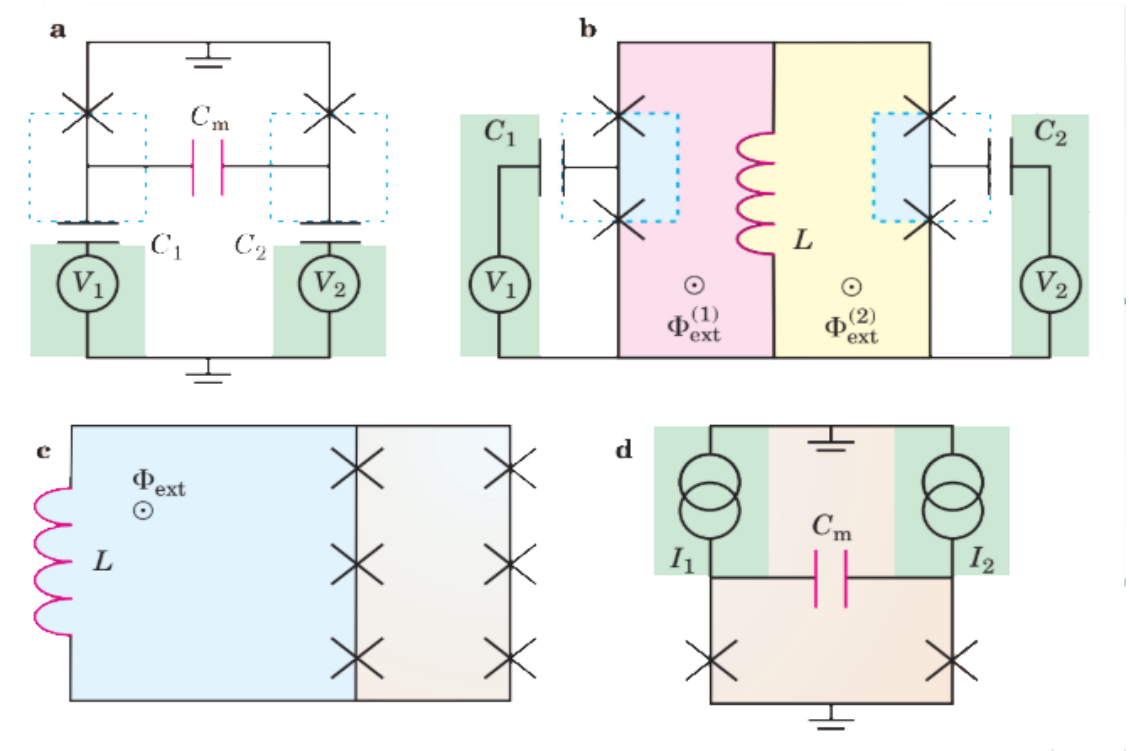


Figura 3.6: Acoplo de qubits. Imagen tomada de [13].

con los que comprobar la hipótesis del gato de Schrödinger, realizar el experimento EPR, observar interferencias Ramsey, etc. Este tipo de aplicaciones hacen del campo de los circuitos superconductores una mina a explotar en el ámbito de la física y jugarán un papel crucial en el desarrollo de futuras tecnologías.

4 Moteado cuántico o "Quantum speckle"

Ya tenemos los conocimientos básicos sobre computación cuántica, así como una idea general del modo de construir qubits en el mundo real y entrelazarlos para aprovechar sus características y hacer puertas cuánticas. El siguiente paso en la búsqueda de la supremacía cuántica sería idear un algoritmo cuántico que pudiera también ser recreado clásicamente, el cual, a medida que aumentemos el número de operaciones, llegue un punto en el que el computador clásico no fuera capaz de hacer tal cantidad de cálculos y que el computador cuántico fuera capaz de resolver con una seguridad razonablemente alta de que no se están cometiendo errores en él.

En el caso del computador cuántico de Google, este algoritmo (de moteado cuántico o "Quantum speckle") fue el que sirvió para alcanzar la supremacía cuántica. Su tarea era la de verificar la salida de un generador cuántico de números aleatorios. Esto se explicará con más detalle en la sección 5 , pero en resumen, debido a la interferencia cuántica, cuando se generan cadenas de bits aleatorias con circuitos cuánticos (10010101111, 1101011101,...), unas cadenas son más probables de obtenerse que otras. El algoritmo comprobaría la "similitud " (matizaremos esto más tarde) de la distribución de probabilidad de las cadenas obtenidas experimentalmente con la distribución de probabilidad uniforme. Esto proporciona una medida para saber si el computador cuántico está trabajando correctamente o si se están produciendo errores. Para ello explicaremos el concepto de referencia de entropía cruzada como medida de fidelidad de los circuitos.

Computar la salida de circuitos cuánticos aleatorios es una tarea complicada para los computadores clásicos, ya que el coste computacional aumenta exponencialmente a medida que se aumenta el número de qubits o la profundidad del circuito. Por ello, se llega al punto donde las simulaciones clásicas requieren un tiempo demasiado grande como para ser realizado. Por tanto se tendrá que extrapolar de la región de experimentos que sí pueden ser llevados a cabo para tener una idea de cuán grande sería el coste computacional del experimento en el régimen de supremacía cuántica. Este punto se conseguiría, según los resultados obtenidos, en una red de 2D de 7 x 7 qubits y con una profundidad de unos 40 ciclos. Todos los resultados que se

resumen en este capítulo se basan en los obtenidos en [22].

4.1 Introducción y objetivo

Este algoritmo y sus resultados, así como gran parte de la teoría en la que se sustenta, tienen su origen en la teoría del caos cuántico, así como en la teoría de la complejidad computacional y la teoría de matrices aleatorias, necesarias para el cálculo de distribuciones de probabilidad en estos casos. Igualmente, hemos comentado el objetivo de este algoritmo, que se basa en la implementación de circuitos cuánticos aleatorios. Esto se conseguirá aplicando una serie de puertas lógicas cuánticas.

Antes de comenzar, conviene definir algunos conceptos que aún no conocemos y que serán esenciales a la hora de entender el logro conseguido. El primero de ellos es el de profundidad de un circuito cuántico, la cual ya ha sido nombrada. La profundidad de un circuito se define como la longitud del camino más largo desde la entrada a la salida, moviéndose hacia delante en el tiempo, a través de los "qubits cables" [1]. En este camino, se considera una unidad de tiempo cada puerta que vayamos tomando. Podemos esclarecer esta definición con un ejemplo. Fijémonos en la figura 4.1:

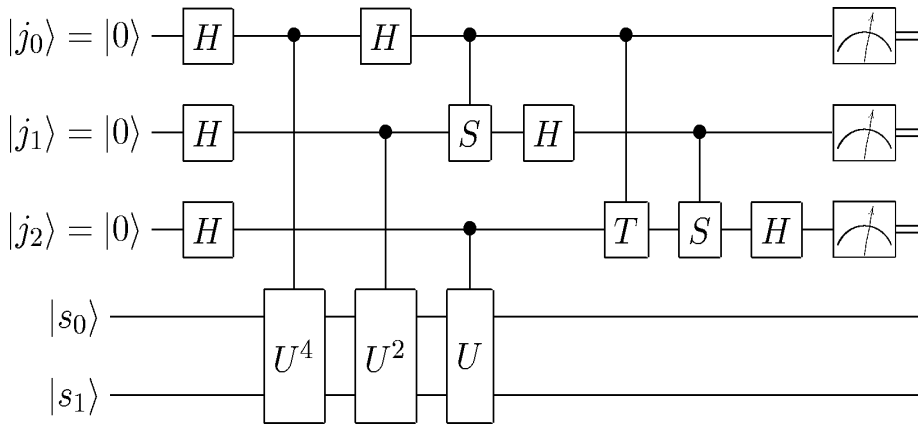


Figura 4.1: Ejemplo de un circuito cuántico. Imagen tomada de [23].

Para calcular la profundidad, tendríamos que ir sumando una unidad por cada puerta que pasáramos en el camino más largo que haya para llegar a un qubit determinado. En este caso, habría dos caminos por los cuales obtendríamos la profundidad del circuito. Uno sería el que recorre desde $|j_0\rangle$ por H, U^4, H, S, H, S, H y la medida, el cual nos da la medida de 8 unidades de tiempo, y el otro sería haber seguido el cable del primer qubit después de S y haber tomado T, siguiendo esa línea luego, lo que nos conduciría al mismo resultado.

Otro de los conceptos que debemos conocer es la distribución de Porter-Thomas. Esta, es característica del caos cuántico, y nuestro estudio se centrará en la convergencia a ella de la

[1] Los qubits que iremos pasando por el camino de la entrada a la salida.

distribución de probabilidad de las salidas de nuestros circuitos. El estudio de la distribución de Porter-Thomas está fuera de los objetivos debido a la dificultad de la teoría en la que se sustenta. Podemos, al menos, dar su forma, y remitimos al lector a la lectura de [24], donde puede tomar una idea más extensa si está interesado en estos conocimientos, aunque hay numerosos documentos en los que se habla sobre esta.

Si se consideran estados generados por un circuito cuántico pseudo-aleatorio, es posible aproximarlos a una distribución uniforme en el espacio de Hilbert, para profundidades suficientemente grandes. Como consecuencia, las probabilidades de las cadenas generadas por un circuito pseudo-aleatorio $\{p = p_u(x)\}$ se aproximan a la función de Porter Thomas, que tiene la forma Ne^{-pN}, con media $1/N$. Así, estudiaremos la convergencia a la entropía de la función de Porter-Thomas: $-\sum_j p_u(x_j) \log p_u(x_j) \rightarrow \log N - 1 + \delta$, siendo δ la constante de Euler, y $p_u(x_j)^k \rightarrow k!/N^{k-1}$ para $k > 10$.

Mencionamos con frecuencia el concepto de circuitos cuánticos aleatorios. Es lógico preguntarse, ¿cómo exactamente se contruyen estos para que la salida de los qubits sea aleatoria? La respuesta sería, primero, con una secuencia de puertas de Hadamard, para rotar el eje x. Tras esto, solo se trabaja con puertas controlled-Z (CZ gates), para operaciones de entrelazado de dos qubits, junto con un conjunto de puertas de 1 bit $\{X^{1/2}, Y^{1/2}, T\}$. Básicamente, en los d ciclos realizados, se van alternando diferentes configuraciones de CZ-gates como se muestra en la figura 4.2. De la misma manera, en los lugares en los que no se aplica una CZ-gate en un ciclo, se coloca una de las 3 puertas de 1-qubit, siguiendo la norma de que, después de aplicar la puerta de Hadamard, se aplica una T-gate, la cual es representada por la matriz diagonal $\{1, e^{i\pi/4}\}$, si a esta no le ha tocado la CZ-gate. En los siguientes ciclos, se usan puertas de 1 qubit, $\{X^{1/2}, Y^{1/2}\}$ con la misma probabilidad de escoger entre ambas, solo después de que el mismo qubit haya visto una CZ en el ciclo anterior y si ya ha pasado por una T-gate. $\{X^{1/2}, Y^{1/2}\}$ representan asimismo rotaciones de $\pi/2$ alrededor del eje x o y, respectivamente, en la esfera de Bloch. A nuestro propósito, parece bastar con una cantidad de d ciclos igual a 20 en una red de 7x6 qubits.

4.2 Entropía cruzada como medida de fidelidad

A continuación, explicaremos el fundamento matemático del concepto de entropía cruzada, y veremos cómo valernos de este para saber cómo de bien está trabajando el sistema de qubits. Consideraremos $S = \{x_1, ..., x_m\}$, como una muestra de cadenas de bits x_j, en la base computacional. Además, $p_u(x)$ será la distribución de probabilidad de estas, la cual es aproximadamente independiente e idéntica a la distribución de Porter-Thomas. De la misma manera, y con el objetivo de no tener que especificarlo más tarde, $S_{unc} = \{x_1^{unc}, ..., x_m^{unc}\}$ será una muestra que no esta correlacionada con la muestra anterior, con su correspondiente función de distribución

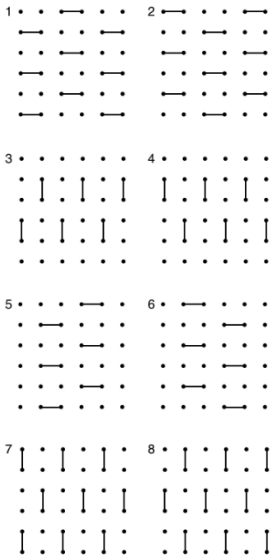


Figura 4.2: Conjunto de 6x6 qubits, donde se grafican las CZ-gates con líneas que entrelazan qubits. Procedemos secuencialmente de 1 a 8. No se pueden aplicar CZ-gates a dos qubits vecinos al mismo tiempo. Imagen tomada de [22].

$p_{UNC}(x_j)$. Según el teorema del límite central: $\log Pr_U(S) = -m(\log N - 1 + \delta) + O(m^{1/2})$.

Uno se plantea ahora cuál es la probabilidad $Pr_U(S_{UNC})$ de obtener S_{unc} de la salida $|\psi_d\rangle$ del circuito U . Este resultado viene dado también por el teorema del límite central, que nos dice que: $\log Pr_U(S_{UNC}) = -mH(p_{UNC}, p_U) + O(m^{1/2})$, siendo H la entropía cruzada entre p_{UNC} y p_U, $H(p_{UNC}, p_U) \equiv -\sum_{j=1}^{N} p_{UNC}(x_j) \log p_U(x_j)$. Esta magnitud será crucial a la hora de entender el resultado que proclama la supremacía cuántica. Se puede promediar en el circuito obteniendo: $\mathbb{E}_U[H(p_{UNC}, p_U)] = -\sum_{j=1}^{N} \mathbb{E}_U[H(p_{UNC}(x_j))]\mathbb{E}_U[H(p_U(x_j))]$. De aquí, se puede ver muy fácilmente que, una m-muestra S obtenida de un circuito aleatorio, representa una característica única de este. Definiendo: $H_0 \equiv -\mathbb{E}_U[\log p_U(x_j)] = \log N + \delta$, lo que daría la entropía de una distribución que da la misma probabilidad a todos los valores de p_U, entonces se obtiene: $\mathbb{E}_U[\log Pr_U(S) - \log Pr_U(S_{UNC})] = m$.

Llegamos aquí al quid de la cuestión. Podemos usar la diferencia entre la entropía cruzada y H_0 como medidor de calidad de un algoritmo A a la hora de verificar las cadenas de bits correspondientes a p_U. Definiremos entonces $\Delta H(p_A) \equiv H_0 - H(p_A, p_U)$. Esta será llamada diferencia de entropía, y su valor es igual a la unidad para circuitos aleatorios ideales y 0 para distribuciones no correlacionadas en cadenas de bits cuando promediamos en U. La diferencia de entropía cruzada es $\alpha \equiv \mathbb{E}_U[\Delta H(p_{exp})]$. Esta medida es la que dictará, en la práctica, si se ha conseguido llegar al régimen de supremacía cuántica que buscamos. Ya que, a mayor α, mejor es la caracterización que hace el algoritmo de las cadenas de bit aleatorias. Por tanto, el objetivo estará cumplido si se consigue que $1 \geq \alpha > C$, donde $C = \mathbb{E}_U[\Delta H(p^*)]$ está dada por

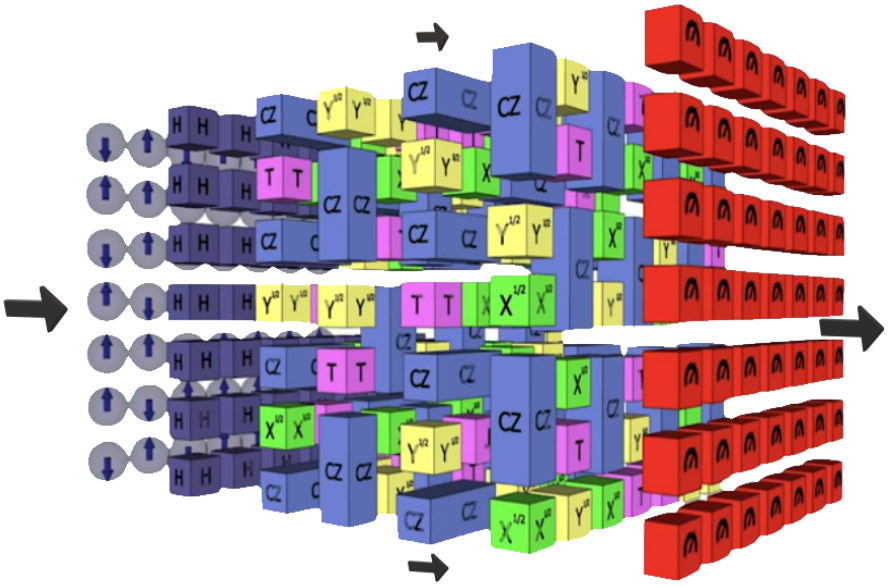


Figura 4.3: Representación tridimensional del algoritmo, donde las flechas señalan el avance temporal y cada capa el conjunto de puertas aplicadas en un paso. Las flechas azules iniciales representan el qubit en la esfera de Bloch. Imagen tomada de [25].

el mejor resultado obtenido por un algoritmo clásico A^*, con distribución de salida p^*.

Esto se estima que ocurre para circuitos de 7x7 qubits y una profundidad de aproximadamente 40 ciclos. Podemos hacernos una idea de la cantidad de memoria que necesitamos para almacenar los resultados en una memoria clásica. Tenemos en cuenta que los bytes necesarios para almacenar una función de onda de n qubits son 2^nx2x4 bytes. Para 48 qubits, esto requeriría una memoria de, al menos, 2.25 petabytes, que es el máximo que se puede realizar en una supercomputadora clásica del momento. Para circuitos con menos qubits, las simulaciones nos proporcionan una $C = 1$ y la supremacía cuántica resulta imposible, ya que no se puede mejorar el resultado de las simulaciones clásicas.

Obtener la diferencia de entropía cruzada α a partir de una cadena de bits experimental S_{exp} obtenida de la salida de un circuito después de m realizaciones de este no es una tarea trivial, y debemos hacer ciertas aproximaciones así como tener una idea del fundamento matemático en el que se basa. Para una muestra S_{exp}, aplicando el teorema del límite central obtenemos que, $\alpha \simeq H_0 + 1/m \sum_{j=1}^{m} \log p_U(x_j^{exp})$, con error estadístico $\kappa/\sqrt{m}$ y $\kappa \simeq 1$. Esto nos muestra que si conseguimos computar $\log p_U(x_{exp})$ por medio de un computador clásico, seremos capaces de obtener α. Si nos centramos en modelos de error teórico para esta medida que luego podamos comparar con la realidad, debemos hablar de la magnitud ρ, la cual es la salida que se obtiene del circuito. Esta se define como, $\rho = \alpha_f U |\psi_0\rangle \langle\psi_0| U^\dagger + (1 - \alpha_f)\sigma_U$, donde α_f es la fidelidad del circuito. Esta fidelidad se puede relacionar, mediante relaciones y resultados matemáticos que, como hemos dicho, son demasiado extensos como para explicar explícitamente en este

trabajo, con el valor α, de manera que $\alpha \approx \alpha_f$.

Esta nueva magnitud será la cota de entropía cruzada. En el modelo seguido en teoría, obtenemos, $\alpha \approx exp(-r_1 g_1 - r_2 g_2 - r_{init} n - r_{res} n)$, donde $g_1, g_2 >> 1$ son el número de puertas de 1 y 2 qubits y $r_1, r_2 << 1$ son las llamadas tasas de error de Pauli (ver ref.[26]) para puertas de 1 y 2 qubits. Estas tasas de error representan el error por puerta lógica de 1 qubit, que es 1 menos la fidelidad de la puerta si el error es mucho menor que 1. El valor de estos para puertas de 1 qubit suele ser del 1 por mil (0.001). Mientras que los errores en puertas de dos qubits suelen ser un orden de magnitud mayor, del 1 por cien (0.01).

4.3 Complejidad computacional y supremacía cuántica

Si nos fijamos ahora en la dificultad de realizar las simulaciones de las que hemos hablado en una computadora clásica, sucede, al igual que antes, que uno debería tener una idea base sobre teoría de complejidad computacional, así como del modelo de Ising. Sabemos que la implementación del algoritmo en un computador clásico, para casos asintóticos de n, requiere del uso de la teoría de complejidad computacional, ya que este problema aumenta la necesidad de recursos de manera exponencial a medida que se aumenta n. Además, se requiere de corrección de errores a la hora de comprobar cómo de bien se está ejecutando.

En el algoritmo de Google, la función $pU(x) = |\langle x|\psi_d\rangle|^2$ da una muestra directa de la función de partición del modelo aleatorio complejo de Ising, $\langle x|\psi_d\rangle = \lambda \sum_s exp(i\frac{\pi}{4} H_x(s))$, con $H_x(s) = h_x \cdot s + s^\dagger \cdot \hat{J} \cdot s$, como la energía clásica, siendo s el vector de espín ± 1, h_x un vector del campo local y $\hat{J}$ la matriz de acoplamiento. Esto puede ser usado para aproximar el mapeo de la función con los algoritmos. Es decir, si sabemos que el resultado (simulado) de la salida del circuito debe adecuarse con la función de Ising, podemos usar eso como forma de medir la calidad de la simulación.

La clave en los resultados obtenidos reside en que esta tarea de simular circuitos cuánticos con métodos clásicos se vuelve exponencialmente más exigente en lo que a almacenamiento respecta. Por ello, como hemos comentado, los supercomputadores actuales fallan para una cantidad mayor de 48 qubits y una profundidad de unos 40 ciclos. Ahí es donde los ordenadores cuánticos dan un paso adelante para postularse como única solución a problemas tan complejos.

Este método, es solo uno más de los diferentes métodos existentes para evaluación de errores. Este, nos da una manera novedosa de caracterizar y validar modelos de error para sistemas cuánticos abiertos. Además, la aplicación no está solo centrada en esto, sino que tiene otros campos de aplicación como la evolución de hamiltonianos caóticos. Una buena implementación del método requeriría unos errores de alrededor del 0.5 % para puertas de 2 qubits y de

0.05 % para puertas de 1 qubit. Como veremos en las siguientes secciones, esto se ha conseguido experimentalmente, y por ello se puede afirmar que se ha alcanzado la supremacía cuántica con una veracidad suficiente.

5 Prueba experimental de la supremacía cuántica

Conocemos ya en qué consiste la supremacía cuántica, cómo llevarla a cabo, en qué teoría se sustenta, etc. En esta sección describiremos el resultado de Google, en el que afirma haber alcanzado la tan mencionada supremacía cuántica, analizando los datos y especificaciones que nos dan en su trabajo realizado y publicado en Octubre de 2019 [27]. En él, se afirma haber realizado una tarea (la explicada en la sección anterior) con un procesador de 53 qubits (eran 54 pero uno no funcionó) para la cual un ordenador clásico hubiera requerido de unos 10.000 años, según afirman ellos. Este procesador, llamado Sycamore, está constituido de 53 qubits superconductores, cuyo espacio computacional generado equivaldría a un espacio de dimensión 2^{53}. Este realizó la tarea encomendada en unos 200 segundos, usando el proceso de cota de entropía cruzada, que hemos descrito ya en el capítulo 4, pero con alguna variante que ahora explicaremos.

Figura 5.1: Procesador Sycamore utilizado por Google para alcanzar la supremacía cuántica. Imagen tomada de [28].

La tarea de este procesador era la que ya hemos descrito, verificar la salida de circuitos aleatorios que, debido a la interferencia cuántica, tienen una distribución de probabilidad determinada. No tienen, por tanto, todas las combinaciones las mismas probabilidades de salir, y eso es lo que comprueba el computador, que la distribución de probabilidades no es homogénea. Para ello, se diseñó una serie de puertas de 1 y 2 qubits con el objetivo de entrelazarlos y hacer

que trabajen en conjunto.

El método para comprobar que el procesador trabaja correctamente será la cota de entropía cruzada, que compara con qué frecuencia obtenemos cierta cadena de bits experimentalmente, con la correspondiente modelización teórica obtenida por un simulador clásico. El proceso para esto será almacenar cada cadena de bits $\{x_i\}$, y calcular la media de las probabilidades simuladas para las cadenas medida, es decir, la fidelidad de entropía cruzada: $\mathcal{F}_{XEB} = 2^n \langle P(x_i) \rangle_i - 1$. Esta medida es análoga a α, con la que hemos venido trabajando. Representa una correlación con la frecuencia con la que se obtienen cadenas que tienen mucha probabilidad de salir. En su fórmula, n es el número de qubits, $P(x_i)$ es la probabilidad de que la cadena x_i sea computada para el circuito cuántico ideal, y el promedio que aparece se hace sobre las cadenas observadas. Al igual que con α, $\mathcal{F}_{XEB} = 1$ si no hay erores en el circuito. Si, sin embargo, verificamos la salida de una distribución uniforme, donde $\langle P(x_i) \rangle_i = 1/2^n$, el resultado será 0.

El objetivo que se plantean en este trabajo, es el de conseguir $\mathcal{F}_{XEB}$ con un valor alto para circuitos que no puedan ser tratados por un computador clásico. La obtención de $\mathcal{F}_{XEB}$, llegado el punto, se hace intratable para computadores clásicos. Sin embargo, bajo ciertas simplificaciones que mostraremos, podemos obtener resultados que muestran una fidelidad considerable.

5.1 Montaje experimental del procesador

El procesador consistía en una red bidimensional de 54 qubits, donde cada uno estaba acoplado a los cuatro vecinos más cercanos, como se muestra en la figura 5.2. Uno de ellos, como hemos comentado, falló a la hora de realizar el experimento, y por ello los datos obtenidos son los correspodientes a 53 qubits y 86 acoplos. Se utilizaron qubits que podían ser modelados como resonadores superconductores a $5-7$ GHz con el objetivo de reducir errores. Cada qubit tenía dos controles, una guía de microondas para excitar el qubit, y un controlador de flujo magnético para controlar la frecuencia. Cada qubit estaba conectado, además, a un resonador lineal, que servía para medir el estado de este.

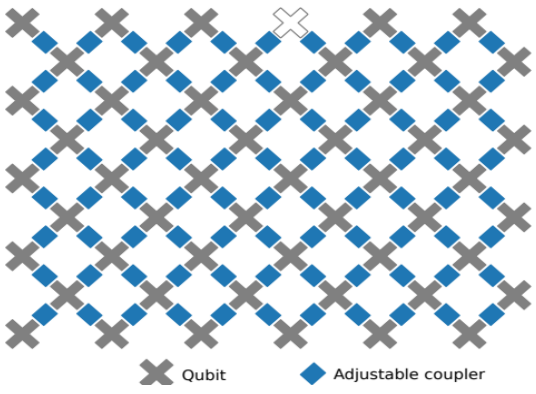


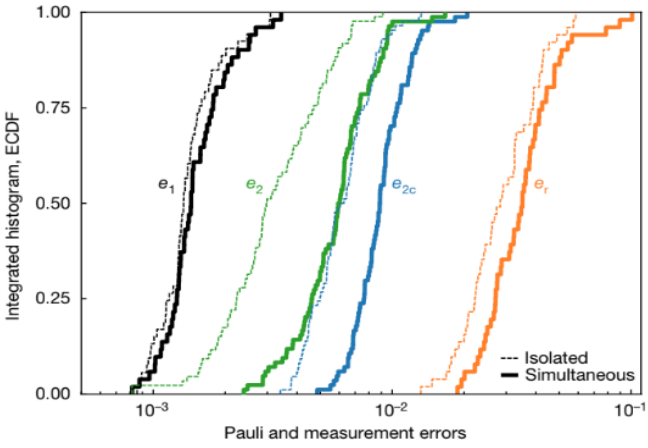
Figura 5.2: Representación de la red que conforma al procesador. Imagen tomada de [27].

El chip estaba conectado a una placa de circuito superconductor, como se ve en la foto, y enfriado por debajo de 20 mK para reducir la energía térmica debida al ambiente, que podría influir en los niveles de energía de los qubits. A partir de aquí, los resultados y datos que mostraremos son los reflejados en la ref. [27], y remitimos al lector a esta si quiere una mayor profundización en ellos. Nosotros solo los mostraremos como aclaración del control de errores en puertas cuánticas que llevaron a cabo.

Los qubits podían ser leídos simultáneamente usando una técnica de multiplexación por división de frecuencia (ver ref. [29]). Las puertas de un solo qubit se realizaban aplicando pulsos de microondas de 25 ns. resonantes con la frecuencia del qubit, mientras el acoplo entre qubits estaba apagado. Para las puertas de 1 solo qubit, se hace este proceso para $n = 1$, así la probabilidad de error durante una operación solitaria es medida. En cada qubit aplicamos un número variable m de puertas seleccionadas y se mide $\mathcal{F}_{XEB}$ varias veces. Se observa una reducción de $\mathcal{F}_{XEB}$ a medida que aumenta m. Esto es modelado por: $[1 - e_1/(1 - 1/D^2)]^m$, siendo e_1 la probabilidad de error de Pauli para puertas de 1 qubit ya explicadas. Esta manera de proceder nos permite separar el error correspondiente a a coherencia del error de control de coherencia. Repitiendo esto con todos los qubits simultáneamente, se observa que la probabilidad de error solo se incrementa una cantidad pequeña, lo que nos viene a decir que el dispositivo tiene poca diafonía, lo que es favorable. La diafonía, en resumen, es un fenómeno entre circuitos por el cual parte de las señales de uno (perturbador) aparece en el otro (perturbado) y se mide como una atenuación.

En el caso de las puertas de dos qubits, se acoplan poniendo dos qubits vecinos en resonancia, aplicando una puerta CZ sobre ambos. Esta puerta está representada de forma matricial por la matriz diagonal con todo 1 menos el último elemento que es -1, y básicamente cambia la orientación de la componente Z en la esfera de Bloch. Las frecuencias de estas puertas se establecen de manera que se mitiguen los mismos mecanismos de error que los corespondientes a puertas de 1 qubit. Se procede, al igual que antes, realizando m ciclos, donde cada uno está conformado por una puerta de 1 qubit aleatoriamente escogida para el qubit, y tras estas, una puerta de 2 qubits. Esto resulta en un error medio e_2 de 0.36 %. Tras esto, se vuelve a correr el circuito de la misma manera pero haciendo que el conjunto entero experimente el proceso simultáneamente. En este caso se pbtiene un error e_2 de aproximadamente 0.62 %.

Una vez obtenidos los errores de las puertas individuales, así como los correspondientes a la lectura de los qubits, se puede modelar la fidelidad de un circuito cuántico como el producto de probabilidades de error teórico y el error correspondiente a las medidas. Se predice entonces un valor de fidelidad total de alrededor de 0.2 %, lo que podría ser solucionado con unas pocas de millones de medidas, ya que la incertidumbre de $\mathcal{F}_{XEB}$ va como $1/\sqrt{N_s}$ siendo N_s el número de muestras. Se asume que hacer sistemas más y más grandes no introduce errores adicionales más allá de los errores medidos a nivel de 1 y 2 qubits. Esta asunción se comprobará más



Average error	Isolated	Simultaneous
Single-qubit (e_1)	0.15%	0.16%
Two-qubit (e_2)	0.36%	0.62%
Two-qubit, cycle (e_{2c})	0.65%	0.93%
Readout (e_r)	3.1%	3.8%

Figura 5.3: Histograma de los errores de Pauli del circuito, así como los correspondientes a las medidas, tanto los realizados en aislamiento como los simultáneos. Imagen tomada de [27].

adelante. El sistema más grande que construyeron en los laboratorios de Google constaba de 53 qubits como hemos dicho, 1113 puertas de un qubit y 430 puertas de 2 qubits. Todos los resultados correspondientes a los errores se ven de una manera más gráfica en la figura 5.3.

5.2 Alcance de la supremacía cuántica

Como ya comentamos, la secuencia que se siguió a la hora de producir circuitos aleatorios consistía en una serie de puertas cuánticas aplicadas de forma que se hiciera aleatoria la cadena producida. Esta secuencia consistía en la aplicación de puertas de un solo qubit $\{X^{1/2}, Y^{1/2}, W^{1/2}\}$ a todos los qubits, eligiéndolas de manera aleatoria, seguida de puertas de 2 qubits aplicadas por pares. Esto está mostrado en la figura 4.3. Como es lógico, en el régimen de supremacía cuántica, no es posible computar $\mathcal{F}_{XEB}$, ya que se necesita su simulación clásica. Sin embargo, son posibles ciertas simplificaciones para obtener un resultado aproximado de este:

- Parchear el circuito: Consiste en dividir el circuito en dos partes, correr cada parte por separado, obtener la fidelidad de ambos y calcular la total como producto de ambas.
- Elidir el circuito: Consiste en quitar algunas puertas de 2 qubits, con el objetivo de hacer más fácil el computar la fidelidad total. Este procedimiento mantiene un carácter más cuántico que el anterior, ya que el anterior no permite el entrelazamiento entre los dos bloques, mientras que este sí lo permite.
- Correr circuitos de verificación: Este último consiste en correr el circuito con el mismo número de puertas cuánticas que "el circuito de supremacía", pero con una secuencia de puertas que haga más fácil el cálculo de la fidelidad del circuito de manera clásica.

Con el objetivo de saber qué proceso de simplificado mostraba mejor las características de los circuitos en la realidad, se realizaron $N_s = 5\text{x}10^6$ muestras, en 10 circuitos que diferían en la elección de las puertas de 1 qubit. Así, se dictó que las fidelidades que más se adecuaban a los resultados experimentales eran los correspondientes a los circuitos en los que se habían elidido parte de ellos. Por ello, estos fueron los elegidos para obtener la fidelidad de los circuitos más complejos.

De esta manera, procediendo con los circuitos elididos, realizaron $N_s = 30\text{x}10^6$ muestras para 10 circuitos de 53 qubits haciendo 20 ciclos, con reordenaciones de las puertas entre ellos, igual que habían hecho anteriormente. Así, se obtuvo una fidelidad de $\mathcal{F}_{XEB} = (2.24 \pm 0.21)\text{x}10^{-3}$. Se tiene pues, que la fidelidad de correr estos circuitos en el procesador cuántico es mayor que 0.1 %.

Simular los circuitos generados cuánticamente nos sirve, por una parte, para verificar los errores que se producen en el procesador experimental con el que tratamos, ya que la cota de entropía cruzada requiere de las probabilidades simuladas para su cálculo, como para tener una idea de la cuantía de tiempo que necesitaría el realizar la tarea propuesta en ordenadores clásicos. Esto nos permite comprobar cuándo la tarea se rige en un régimen de supremacía cuántica, dado que comprobamos que se llega a un límite donde el tiempo requerido es de miles de años.

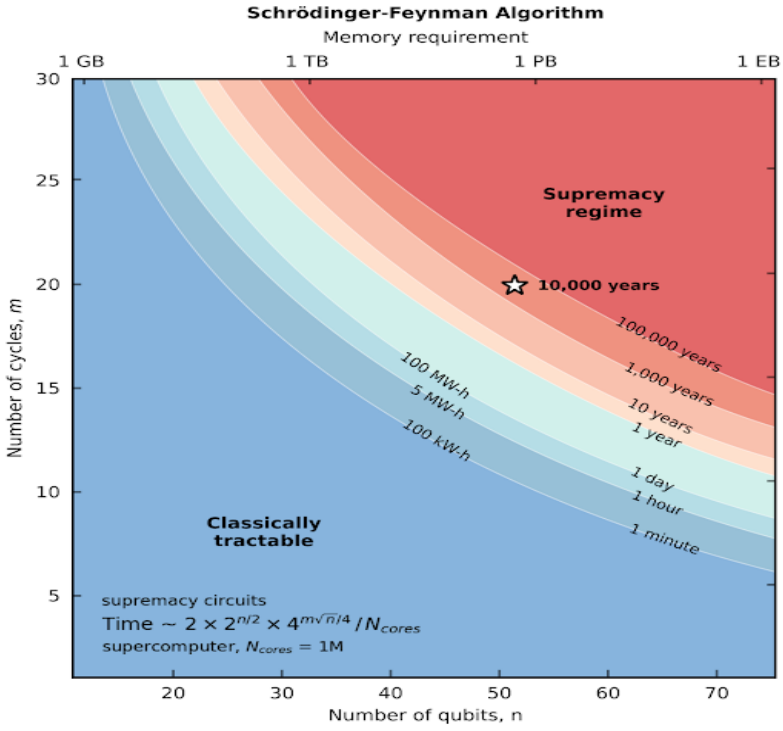


Figura 5.4: Comparativa del tiempo y la potencia requeridas para la simulación de los circuitos cuánticos, dependiendo del número de ciclos y de qubits de estos . Imagen tomada de [30].

Se calcula que el coste de computar clásicamente un circuito como el utilizado por Google una cantidad de veces $m = 14$ con una fidelidad del 1 % tardaría, aproximadamente, 1 año en la

tarea de computar 3 millones de cadenas de bits. Para dar una idea un poco más extendida de cual es el coste computacional de este tipo de circuitos, para $m = 20$ y una fidelidad del 0.1 %, en los servidores de Google costaría unos 50 trillones de horas, mientras que el procesador cuántico Sycamore tardó unos 600 segundos. Para extrapolaciones así, uno puede fijarse en el gráfico 5.4.

Ahora que hemos llegado a la supremacía cuántica, uno puede plantearse si las aproximaciones que hechas por el camino son válidas. Para que nuestras asunciones fueran ciertas y consistentes, el sistema debería mostrar valores bajos para errores correlacionados. Ya que, en el proceso de construcción del experimento, se optimizan los controles para minimizar los errores sistemáticos, diseñando puertas que trabajan mucho más rápido que las fuente de ruido, eligiendo circuitos que aleatorizan errores, etc., estas suposiciones serán acertadas.

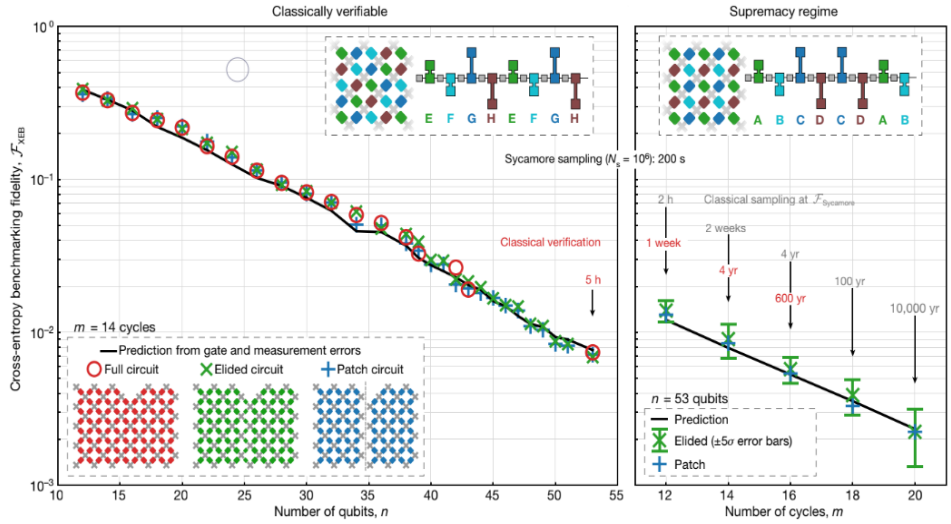


Figura 5.5: Datos experimentales de las cotas de verificación de errores, tanto para el régimen clásico como para el régimen de supremacía cuántica. Imagen tomada de [27].

6 Conclusiones

Todos los resultados expuestos en este trabajo tratan de mostrar el increíble logro realizado por los equipos de Google. Hacer que una computadora cuántica realice cálculos de otra manera inaccesibles es un logro que la humanidad lleva décadas persiguiendo, desde que se planteara este tipo de computadoras como un ideal utópico. Además, su importancia reside en que marca un punto de partida, desde el que se espera que se produzcan mejoras en cuanto a hardware se refiere, siguiendo una ley equivalente a la ley de Moore para procesadores de este tipo, doblando periódicamente su volumen computacional cada cierto número de años. Para que se cumplan estos pronósticos, deben hacerse cuantiosos avances, tanto teóricos como a nivel tecnológico, en el campo de la corrección de errores, los modelos que para ello utilizamos.

Hemos tratado de explicar de forma accesible conceptos y resultados que requieren de nociones en muchos campos para ser completamente aprehendidos. Las explicaciones que hemos dado son, en gran medida, ideas de los pioneros en todos los campos que hemos tocado. Las hemos intentado explicar de forma clara pero, inevitablemente, requieren de una mayor inmersión para una compresión más completa.

Se espera que los resultados e ideas que se trataron de explicar durante el trabajo hayan sido adquiridos por el lector o, al menos, hayan despertado la curiosidad de este para profundizar aún más en un campo que es tan amplio como heterogéneo. Este campo, en el cual se está volcando mucha atención debido a los posibles avances a conseguir en el futuro cercano, está destinado a cambiar la manera en que concebimos la informática, las computadoras y el mundo de las comunicaciones como tal.

Bibliografía

[1] Nielsen, M. A. and Chuang, I. L. (2000). *Quantum Computation and Quantum Information.* Cambridge, Reino Unido. 1ª edición. Editorial Cambridge University press.

[2] Wikipedia, la enciclopedia libre. *Bloch sphere* (2008). `https://en.wikipedia.org/wiki/Bloch_sphere#/media/File:Bloch_sphere.svg`

[3] Singh, P., Quora. *What is fan in and fan out in logic circuits?* (2017). `https://www.quora.com/What-is-fan-in-and-fan-out-in-logic-circuits`

[4] Wootters, W., Zurek, W. (1982). "A single quantum cannot be cloned". *Nature*, **5886**, 802–803

[5] Bashar,M. A., Chowdhury, M. A., Islam, R., Rahman,M. S., Das, S. K. (2009). "A Review and Prospects of Quantum Teleportation ". *Journal of Basic and Applied Sciences*, **1**, No. 2, 296

[6] Bell, J. S., (1964) "On the Einstein Podolsky Rosen paradox". *Physics Publishing Company.* **1**, No. 3, 195-290.

[7] Ismael, J. and Schaffer, J. (2016). "Quantum Holism: Nonseparability as Common Ground". *Synthese*, Springer.

[8] Aniello, P. and Lupo, C. (2008)"On the relation between Schmidt coefficients and entanglement". *arXiv.org* arXiv:0812.4167 [quant-ph].

[9] Nagata, K. et al. (2017). "Quantum Cryptography Based on the Deutsch-Jozsa Algorithm". *International Journal of Theoretical Physics*, **56**, 9.

[10] Shor, P. W. (1996)"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". *SIAM Journal of Scientific Computing 26*, 1484.

[11] Grover, L. K. (1996)"A fast quantum mechanical algorithm for database search". *arXiv.org* arXiv:quant-ph/9605043.

[12] Shannon, C. E. (1948)"A Mathematical Theory of Communication". *The Bell System Technical Journal.* **27**, No. 3, 379.

[13] You,J. Q. and Nori, F. (2005). "Superconducting Circuits and Quantum Information". *Physics Today*. **58**, 42.

[14] Bardeen, J., Cooper, L.N. and Schrieffer, J.R. (1957). "Microscopic Theory of Superconductivity". *Physical Review Journal* **106**, 162.

[15] Yukalov, V. I. (2011). "Basics of Bose-Einstein Condensation". *Physics of Particles and Nuclei* **42**, 460-513.

[16] Dudin, Y. O., Li, L., Bariani, F. and Kuzmich, A. (2012). "Observation of coherent many-body Rabi oscillations". *arXiv.org*, arXiv:1205.7061 [physics.atom-ph].

[17] Vion, D. (2019). *Josephson Quantum bits based on a Cooper Pair Box*. CEA-Saclay, Orme des merisiers, Gif sur Yvette Cedex , Francia. `http://iramis.cea.fr/drecam/spec/Pres/Quantro/Qsite/publi/articles/fichiers/reviews/REVvion.pdf`.

[18] Hekking, F. W. J., Buisson , O., Balestro, F., Vergniory, M. G., (2002). "Cooper Pair Box Coupled to a Current-Biased Josephson Junction" *arXiv.org*, arXiv:cond-mat/0201284 [cond-mat.supr-con].

[19] Cipolla, M. and Landi, G., (2018). "Processing quantum coherence using the spin-boson model." `https://www.groundai.com/project/processing-quantum-coherence-using-the-spin-boson-model/2`

[20] Wang, J. et al. (2013). "Spin Fluctuation and Coherence in Concentrated systems" *American Physical Society*, **58**, 1.

[21] Kofman, A. G., Korotkov, A. N. (2008). "Analysis of Bell inequality violation in superconducting qubits". *Physical Review B* **77**, 104502.

[22] Boixo, S. et al. (2018). "Characterizing quantum supremacy in near-term devices". *Nature Physics*. **14**, 595-600.

[23] Stack Exchange. Quantum Computing. (2019) *How to calculate circuit depth properly?*. `https://quantumcomputing.stackexchange.com/questions/5769/how-to-calculate-circuit-depth-properly`.

[24] Bogomolny, E. (2016). "Modification of the Porter-Thomas distribution by rank-one interaction". *Physical Review Letters*. **118**, 022501.

[25] Google AI Blog *QuantumCasts: Sergio Boixo explaining Quantum Supremacy* (2019). `https://research.google/teams/applied-science/quantum/`.

[26] Kern,O., Alber, G. and Shepelyansky, D. L. (2004). "Quantum error correction of coherent errors by randomization". *The European Physical Journal D - Atomic, Molecular, Optical*

and Plasma Physics **32**, 153–156.

[27] Arute, F. et al. (2019). "Quantum supremacy using a programmable superconducting processor". *Nature*. **574**, 505–510.

[28] Corbella, J., La vanguardia. *Google demuestra la supremacía cuántica* (2019). https://www.lavanguardia.com/ciencia/20191023/471156519790/ordenador-cuantico-google-supremacia-computacion-cuantica.html.

[29] Wei, D., Guangwei, D., Ping, T. G. and Han, T. Y. (2016). "Multiplexing Read-Out of Charge Qubits by a Superconducting Resonator". *Chinese Physics Letters*. **33**, 4.

[30] Google AI Blog *Quantum Supremacy Using a Programmable Superconducting Processor* (2019). https://ai.googleblog.com/2019/10/quantum-supremacy-using-programmable.html.