Códigos cuánticos

Jesús García-López[1]

Resumen

La Teoría Cuántica de la Información y la Computación Cuántica estudian la representación y el tratamiento de la información en un modelo cuántico. Este modelo tiene algunas propiedades nuevas importantes como, por ejemplo, el paralelismo cuántico que permite realizar cálculos simultáneos sobre una cantidad exponencial de información. Otra aplicación importante de las propiedades del modelo es la implementación de protocolos criptográficos de cuaderno único. Pero, el hecho de que el modelo sea continuo o analógico exige el uso de códigos cuánticos para la corrección de errores. En este artículo analizamos la capacidad de corrección de los códigos cuánticos a partir de una distribución de probabilidad del error.

1 Introducción

En el modelo cuántico de computación [3, 8, 13, 23, 30] la unidad de información básica es el *qubit* o bit cuántico. Un qubit puede estar en dos estados puros distintos que se denotan $|0\rangle$ y $|1\rangle$ respectivamente. Físicamente se representa por un sistema cuántico de dos estados. El sistema cuántico de dos estados más conocido por los profanos en la materia es, sin duda, el spin de un electrón. En este sistema podemos representar el spin $-\frac{1}{2}$ por el estado $|0\rangle$ y el spin $+\frac{1}{2}$ por el estado $|1\rangle$.

Hasta ahora el modelo cuántico no se diferencia del clásico: un bit tiene dos valores posibles y un qubit puede estar en dos estados puros posibles. Sin embargo un qubit puede estar además en estados intermedios, es decir, en estados que son combinación lineal de los dos estados puros. Esta es la primera gran diferencia entre los modelos de computación clásico y cuántico. Por ejemplo, el spin de un electrón puede estar en estado

$$\Psi = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \qquad (1)$$

La primera conclusión importante es que un qubit es un vector de un espacio vectorial generado por los dos estados puros, es decir, es un vector de $\mathcal{V} = L(|0\rangle, |1\rangle)$. Según la mecánica cuántica $\mathcal{V}$ es un espacio de Hilbert complejo en el que $\mathcal{B} = [|0\rangle, |1\rangle]$ es una base ortonormal y los estados son vectores unitarios.

Entonces un qubit puede estar en cualquier estado $\Psi = a|0\rangle + b|1\rangle$ tal que $a, b \in \mathbb{C}$ y $|a|^2 + |b|^2 = 1$. Los coeficientes a y b se llaman amplitudes y cuando uno de ellos es cero el qubit está en un estado puro. Resulta relativamente fácil entender los estados puros pero no sucede lo mismo con los estados intermedios.

Volvamos a retomar el ejemplo del spin de un electrón y analicemos un estado intermedio, por ejemplo el de la fórmula 1. En este caso el qubit Ψ no tiene spin definido. Para convencerse de ello basta recordar que el spin de un electrón es una magnitud física que está cuantificada, es decir, que sólo puede tener los valores $-\frac{1}{2}$ y $+\frac{1}{2}$. Además estos valores corresponden a los estados puros $|0\rangle$ y $|1\rangle$ respectivamente. Por lo tanto el estado intermedio Ψ no tiene spin definido.

Como consecuencia de esta situación surge la segunda gran diferencia entre los modelos de computación clásico y cuántico. Siempre es posible leer el valor de un bit pero generalmente no es posible leer o medir el estado de un qubit. Entonces ¿qué información proporciona la lectura de un qubit?

Para entenderlo sigamos con el ejemplo del spin de un electrón. Vamos a estudiar lo que ocurre al medir el qubit definido en la fórmula 1. Para ello empleamos el dispositivo esquematizado en la figura 1. El proceso de medida consiste en hacer pasar al electrón a través de la rendija del panel 1. Cuando pasa por la rendija el electrón atraviesa un

[1]Dpto. Matemática Aplicada. E.U. Informática. U. Politécnica Madrid. E-mail: jglopez@eui.upm.es

campo magnético que desvía su trayectoria, hacia abajo si su spin es $-\frac{1}{2}$ y hacia arriva si su spin es $+\frac{1}{2}$. Finalmente el electrón atraviesa una de las dos rendijas del panel 2, la inferior si su spin es $-\frac{1}{2}$ y la superior si su spin es $+\frac{1}{2}$.

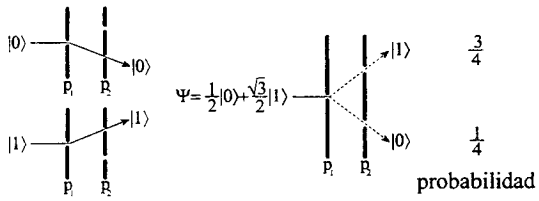

Figura 1: Medida del spin de $\Psi = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$

El qubit Ψ que estamos analizando es un estado intermedio y en consecuencia no tiene spin definido. No es difícil convencerse de que el electrón tiene posibilidad de desviarse tanto hacia abajo como hacia arriba. En primer lugar conviene aclarar que el electrón saldrá por una de las dos rendijas del panel 2. Si pudiese alcanzar posiciones intermedias entre las rendijas del panel 2 el spin del electrón no estaría cuantificado. Una vez asumido este hecho vamos a justificar por qué tiene posibilidad de salir tanto por la rendija inferior como por la rendija superior. Si sólo tuviese posibilidad de salir por una de las rendijas, supongamos que por la superior, significaría que se trata del estado puro $|1\rangle$ pues tendría spin definido.

Pero las sorpresas todavía no han acabado. Si el electrón ha pasado por la rendija inferior su spin, después de la medida, sólo puese ser $-\frac{1}{2}$ y su estado $|0\rangle$. De modo análogo, si el electrón ha pasado por la rendija superior su spin, después de la medida, sólo puese ser $+\frac{1}{2}$ y su estado $|1\rangle$. El proceso de medida, además de dar una información incompleta sobre el qubit, lo modifica. De alguna manera el proceso de medida *obliga al qubit a decidirse por uno de los dos estados puros.*

Una vez hecho el análisis cualitativo de la medida del qubit es conveniente describir cuantitativamente el proceso. Los postulados de la mecánica cuántica establecen que la probabilidad p_0 (p_1) de que el estado final del qubit sea $|0\rangle$ ($|1\rangle$) es igual al cuadrado del módulo de la amplitud de $|0\rangle$ ($|1\rangle$) en la combinación lineal. Para el qubit Ψ del ejemplo el resultado final será $|0\rangle$ con probabilidad $p_0 = \frac{1}{4}$ y $|1\rangle$ con probabilidad $p_1 = \frac{3}{4}$.

En la tabla de la figura 2 se resume el proceso de medida de un qubit. Decimos que el resultado de la medida es 0 (1) si el estado final es $|0\rangle$ ($|1\rangle$).

Estado	M.	Estado final	Probabilidad
$a\|0\rangle + b\|1\rangle$	0	$\frac{a}{\|a\|}\|0\rangle$	$p_0 = \|a\|^2$
$a\|0\rangle + b\|1\rangle$	1	$\frac{b}{\|b\|}\|1\rangle$	$p_1 = \|b\|^2$

Figura 2: Medida de un qubit

Tal como ocurre en computación clásica, en la que se utilizan cadenas de bits, en computación cuántica se trabaja con n qubits. Un $n-$ qubit es un vector unitario del espacio de Hilbert complejo $\mathcal{V}_n = \mathcal{V} \otimes \cdots \otimes \mathcal{V}$ en el que $\mathcal{B}_n = [|0\cdots00\rangle, |0\cdots01\rangle, |0\cdots10\rangle, \ldots, |1\cdots11\rangle]$ es una base ortonormal. Los vectores de la base $\mathcal{B}_n$ están definidos del siguiente modo

$$|x_1 \ldots x_n\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle, \;\; x_1, \ldots, x_n \in \{0, 1\}$$

La cadena de bits $x_1x_2\ldots x_n$ la podemos interpretar como un número natural x representado en el sistema de numeración binario. De este modo los vectores de la base $\mathcal{B}_n$ se identifican con los números naturales x que cumplen $0 \leq x < 2^n$ (números con n dígitos binarios). Y, una vez identificada la cadena de bits $x_1x_2\ldots x_n$ con el número natural x, se puede escribir x en el sistema de numeración decimal. En definitiva podemos escribir $\mathcal{B}_n = [|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n - 1\rangle]$.

La identificación de los vectores de la base $\mathcal{V}_n$ con cadenas de n bits es importante para codificar información en un $n-$ qubit, mientras que identificarlos con números naturales tiene que ver con nuestra predilección por el sistema de numeración decimal. Con esta notación un $n-$ qubit se puede escribir del siguiente modo

$$\Psi = \sum_{x=0}^{2^n-1} a_x|x\rangle \quad \text{tal que} \quad \sum_{x=0}^{2^n-1} |a_x|^2 = 1 \qquad (2)$$

Conviene resaltar que la dimensión de $\mathcal{V}_n$ es exponencial, concretamente es 2^n. Esta es la propiedad clave para conseguir el paralelismo cuántico. Por el momento sólo podemos apreciar la enorme capacidad de un $n-$ qubit para almacenar información. Por ejemplo, el par de números

$(131, 211)$ se puede codificar en una cadena de 16 bits, 8 para cada número, que se puede representar mediante el $16-$qubit $\Psi_1 = |1000001111010011\rangle = |27641\rangle$. Sin embargo en un $16-$qubit se puede codificar mucha más información. Así el estado

$$\Psi_2 = \frac{1}{256} \sum_{x=0}^{65535} |x\rangle \qquad (3)$$

es una combinación lineal de todos los pares de números de 8 dígitos binarios desde el $(0,0)$ hasta el $(255,255)$, ambos incluidos. En el ejemplo anterior los ocho primeros qubits codifican el primer número del par, mientras los ocho qubits restantes codifican el segundo número.

En un $n-$qubit podemos medir cualquiera de los qubits, por ejemplo el $k-$ésimo. El proceso es análogo al que ya hemos descrito para un qubit y está descrito en la tabla de la figura 3. Consiste en proyectar ortogonalmente sobre uno de los dos subespacios en los que el qubit está en estado definido y renormalizar la proyección. El cuadrado de la norma de la proyección sobre un subespacio indica la probabilidad de que la proyección se produzca sobre dicho subespacio.

Estado final	Probabilidad
$\Psi_0 = \frac{1}{\sqrt{p_0}} \sum_{\substack{0 \le x < 2^n \\ x_k = 0}} a_x \lvert x\rangle$	$p_0 = \sum_{\substack{0 \le x < 2^n \\ x_k = 0}} \lvert a_x\rvert^2$
$\Psi_1 = \frac{1}{\sqrt{p_1}} \sum_{\substack{0 \le x < 2^n \\ x_k = 1}} a_x \lvert x\rangle$	$p_1 = \sum_{\substack{0 \le x < 2^n \\ x_k = 1}} \lvert a_x\rvert^2$

Figura 3: Medida del $k-$ésimo qubit

En general una medida cuántica tiene asociada una suma ortogonal del espacio de Hilbert $\mathcal{V} = S_0 \perp S_1 \perp \cdots \perp S_k$ y el resultado de la medida de un estado $\Psi = \Psi_0 + \Psi_1 + \cdots + \Psi_k$, en el que $\Psi_i \in S_i$ para todo $0 \le i \le k$, es

$$\frac{\Psi_i}{\|\Psi_i\|} \quad \text{con probabilidad} \quad \|\Psi_i\|^2 \qquad (4)$$

Para construir algoritmos cuánticos es necesario describir cómo se puede modificar el estado de un $n-$qubit, es decir describir las puertas cuánticas. Puesto que se trata de transformar un vector en otro vector parece lógico suponer que las puertas cuánticas van a ser aplicaciones lineales. Como además los vectores deben ser siempre unitarios sólo puede tratarse de transformaciones unitarias. En efecto así es, como se desprende de los postulados de la mecánica cuántica.

Por tanto un algoritmo cuántico es una secuencia de puertas y medidas cuánticas que actúan sobre un $n-$qubit que inicialmente es el primer vector de la base, es decir $|0\rangle$. Es evidente que un ordenador cuántico no puede aplicar una puerta cuántica arbitraria. Por este motivo las puertas cuánticas deben descomponerse en puertas cuánticas elementales de uno o dos qubits.

2 Códigos cuánticos

El modelo cuántico de computación es un modelo continuo o analógico y, por esta razón, va a necesitar un sistema de corrección de errores ([1-34] excepto [3, 8, 13, 23, 30]). El mecanismo clásicamente conocido para ello consiste en codificar la información mediante un código corrector. Tanto clásicamente como cuánticamente la clave para la corrección de errores es introducir redundancia al codificar la información.

En el modelo cuántico los errores pueden ser arbitrariamente pequeños. A primera vista esto puede parecer un obstáculo insalvable. Sin embargo las propiedades de las medidas cuánticas permiten corregir errores continuos. Sea $\mathcal{C}$ un código cuántico que codifica un $m-$qubit en un $n-$qubit. Se trata formalmente de una aplicación lineal inyectiva que conserva el producto escalar cuya imagen se denomina espacio código.

$$\mathcal{C} : \mathcal{V}_m \to \mathcal{V}_n, \quad \text{Esp. código: } S_0 = \mathcal{C}(\mathcal{V}_m) \qquad (5)$$

Para determinar el conjunto de errores que se van a corregir se eligen $d'' = 2^{n-m}$ operadores unitarios de error E_0, E_1, $\ldots$, $E_{d''-1}$. Entre ellos debe estar el operador indentidad que supondremos que es el primero, es decir $E_0 = I$. Para que este proceso, que se denomina proceso de discretización de errores, permita corregir cualquier combinación lineal de estos errores es preciso que los subespacios $S_h = E_h(S_0)$ para todo $0 \le h < d''$ cumplan lo siguiente

$$\mathcal{V}_n = S_0 \perp S_1 \cdots \perp S_{d''-1} \qquad (6)$$

Supongamos que un estado codificado Ψ_0 sufre una perturbación convirtiéndose en el estado Ψ. El estado inicial es un estado código, es decir $\Psi_0 \in S_0$, mientras que el estado perturbado en general no lo es, es decir $\Psi \notin S_0$. Si el estado perturbado es de la forma

$$\Psi = \alpha_0 E_0 \Psi_0 + \alpha_1 E_1 \Psi_0 + \cdots + \alpha_{d''-1} E_{d''-1} \Psi_0 \quad (7)$$

con $|\alpha_0|^2 + \cdots + |\alpha_{d''-1}|^2 = 1$, se puede recuperar el estado inicial Ψ_0. En efecto medimos respecto de la descomposición ortogonal de la fórmula 6. El resultado será $\frac{\alpha_h}{|\alpha_h|} E_h \Psi_0$ para un valor de h entre 0 y $d'' - 1$. Aplicando a continuación la puerta cuántica E_h^{-1} se obtiene $\frac{\alpha_h}{|\alpha_h|}\Psi_0$. Este estado no es exactamente Ψ_0 pero, al diferir solamente en factor de fase (número complejo unitario), ambos estados son indistinguibles desde el punto de vista de la mecánica cuántica.

Los operadores unitarios de error se pueden elegir de forma que, por ejemplo, se corrijan todos los errores que afectan a un único qubit. El mejor código con estas características que codificar 1 qubit es un código de 5 qubits [6, 21]. Este código es óptimo en el sentido de que ningún código de menos de 5 qubits puede corregir todos los errores de un solo qubit.

3 Distribución de probabilidad del error

Como se ha visto el estado Ψ de un $n-$qubit es un vector unitario de un espacio de Hilbert complejo $\mathcal{V}_n$. En este espacio vectorial de dimensión $d = 2^n$ se considera la base ortonormal $\mathcal{B}_n = [|0\rangle, |1\rangle, \ldots |d-1\rangle]$, respecto de la cual el estado Ψ se puede representar como

$$\Psi = \sum_{k=0}^{d-1} \alpha_k |k\rangle \quad \text{tal que} \quad \sum_{k=0}^{d-1} |\alpha_k|^2 = 1 \quad (8)$$

Si representamos los coeficientes en forma binómica, es decir $\alpha_k = x_{2k} + i\, x_{2k+1}$ para todo $0 \le k \le d-1$, el estado Ψ queda parametrizado por los puntos de una esfera unitaria de dimensión $2d-1$ que denotaremos $\mathcal{S}_{2d-1}$:

$$R_\Psi = (x_0, \ldots, x_{2d-1}) \text{ con } \sum_{j=0}^{2d-1} x_j^2 = 1 \quad (9)$$

Utilizaremos esta parametrización para introducir la distribución de probabilidad del error. Sin embargo no utilizaremos coordenadas cartesianas sino coordenadas esféricas.

$$T_\Psi = (\theta_0, \ldots, \theta_{2d-2}) \begin{cases} 0 \le \theta_0, \ldots, \theta_{2d-3} \le \pi \\ 0 \le \theta_{2d-2} \le 2\pi \end{cases}$$

$$x_j = \sin(\theta_0) \cdots \sin(\theta_{j-1}) \cos(\theta_j), \quad 0 \le j \le 2d-2$$

$$x_{2d-1} = \sin(\theta_0) \cdots \sin(\theta_{2d-2})$$

Sea Ψ el resultado de una perturbación de un estado Ψ_0 causada, por ejemplo, por la influencia del entorno sobre el $n-$qubit (decoherencia). Supondremos que la probabilidad de que el resultado de la perturbación sea Ψ depende exclusivamente de $\|\Psi_0 - \Psi\|$. Supondremos sin pérdida de generalidad que $\Psi_0 = |0\rangle$ y, como consecuencia, que $R_{\Psi_0} = (1, 0, \ldots, 0)$ y que $T_{\Psi_0} = (0, \ldots, 0)$. Entonces

$$\Psi = \sum_{k=0}^{d-1} \alpha_k |k\rangle \implies \|\Psi_0 - \Psi\|^2 = 2 - 2\cos(\theta_0) \quad (10)$$

Esto quiere decir que la función de densidad de la distribución de probabilidad del error sólo depende del ángulo θ_0. Por lo tanto, es una función constante en las intersecciones de la esfera con hiperplanos ortogonales al primer eje coordenado, es decir en los *paralelos*.

Definición 1 *Llamamos distribución $Q(d, \sigma)$ a toda distribución de probabilidad de un $n-$qubit con la siguiente función de densidad, parametrizada sobre la esfera $\mathcal{S}_{2d-1}$,*

$$f_d(\sigma, \theta_0) = \frac{(2d-2)!!}{(2\pi)^d} \frac{(1-\sigma^2)}{(1+\sigma^2-2\sigma\cos(\theta_0))^d} \quad (11)$$

donde $d = 2^n$ y el parámetro σ pertenece al intervalo $(-1, 1)$.

Cuando σ se aproxima a 1 la probabilidad se concentra en el punto R_{Ψ_0}, anulándose el error. En sentido contrario, si σ se aproxima a -1 la probabilidad se concentra en el punto diametralmente opuesto de R_{Ψ_0}, maximizándose el error. En cambio si el parámetro σ es igual a 0 la distribución es uniforme, es decir, después de la perturbación todos los estados son igualmente probables. En la figura 4 se puede ver cómo cambia la distribución en función del parámetro.

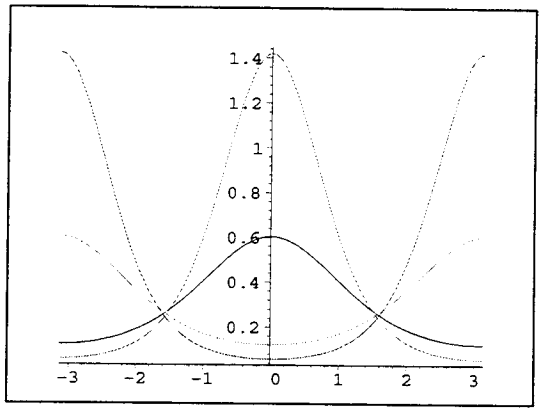

Figura 4: $Q(8,\sigma)$, $\sigma = -0.1$, -0.05, 0, 0.05 y 0.1

Definición 2 *Llamamos varianza de un $n-$ qubit Ψ con distribución $Q(d,\sigma)$, $Var(\Psi)$, al valor esperado de la variable aleatoria $\|\Psi_0 - \Psi\|^2$ es decir a $E[2-2\cos(\theta_0)]$.*

Teorema 3 *La varianza de un $n-$ qubit Ψ con distribución $Q(d,\sigma)$ es*

$$Var(\Psi) = 2(1-\sigma) \tag{12}$$

El teorema 3 demuestra que, como ya se mencionó anteriormente, cuando σ se aproxima a 1 (-1) la probabilidad se concentra en Ψ_0 $(-\Psi_0)$. En efecto, el límite cuando σ tiende a 1 (-1) de $\mathrm{E}\left[\|\Psi_0 - \Psi\|^2\right]$ es 0 (4) y por lo tanto la probabilidad se concentra en Ψ_0 $(-\Psi_0)$.

4 Análisis del error

Sea Ψ_{in} un $m-$ qubit y $\mathcal{C}$ un código cuántico que codifica Ψ_{in} mediante el $n-$ qubit Ψ_0, es decir, $\Psi_0 = \mathcal{C}\Psi_{in}$. Supongamos que este estado sufre una perturbación, convirtiéndose en un estado Ψ que sigue una distribución de probabilidad $Q(d,\sigma)$.

El código cuántico $\mathcal{C}$ tiene asociado un subespacio de dimensión $d' = 2^m$, denominado espacio código, que se define como $S_0 = \mathcal{C}(\mathcal{V}_m)$ y que contiene a Ψ_0. El subespacion S_0 es uno de los $d'' = 2^{n-m}$ subespacios de dimensión d' asociados al código que determinan una descomposición ortogonal del espacio $\mathcal{V}_n$. A su vez, cada subespacio S_h $(0 \le h \le d''-1)$ tiene asociado un operador unitario E_h que cumple $S_h = E_h(S_0)$.

$$\mathcal{V}_n = S_0 \perp S_1 \perp \cdots \perp S_{d''-1} \tag{13}$$

Se puede suponer, sin pérdida de generalidad, que $\Psi_0 = |0\rangle$, $S_0 = L(\,|0\rangle, \ldots, |d'-1\rangle\,)$ y que para todo $0 \le h \le d''-1$ y todo $0 \le k \le d-1$ se cumple $E_h|k\rangle = |(hd'+k) \bmod d\rangle$. Entonces se verifica $S_h = E_h(S_0) = L(\,|hd'\rangle, |hd'+1\rangle, \ldots, |hd'+d'-1\rangle\,)$ y $E_h\Psi_0 = |hd'\rangle$ para todo $0 \le h \le d''-1$.

Podemos aplicar el código $\mathcal{C}$ para corregir el estado Ψ. Para ello medimos el estado Ψ, obteniendo como resultado la proyección $\Pi_h\Psi$ (convenientemente normalizada) en uno de los subespacios S_h $(0 \le h \le d''-1)$. Finalmente se corrige el error correspondiente calculando $\tilde{\Psi}_0 = E_h^{-1}\Pi_h\Psi$.

Para determinar la capacidad de corrección del código $\mathcal{C}$ vamos a calcular la varianza del error después de la corrección, es decir, $\mathrm{E}\left[\|\Psi_0 - \tilde{\Psi}_0\|^2\right]$. Pero antes vamos a determinar la probabilidad P_h de que la proyección se produzca sobre el subespacio S_h $(0 \le h \le d''-1)$. Usando la simetría de la distribución de probabilidad se deduce que $\mathrm{E}\left[|\alpha_k|^2\right] = \mathrm{E}\left[|\alpha_{k'}|^2\right]$ para todo $0 < k, k' < d$. El mismo argumento permite probar que $P_h = P_{h'}$ para todo $0 < h, h' < d''$. Entonces

$$P_0 = \mathrm{E}\left[|\alpha_0|^2\right] + (d'-1)\mathrm{E}\left[|\alpha_1|^2\right] \tag{14}$$

$$P_h = d'\mathrm{E}\left[|\alpha_1|^2\right] \quad 0 < h < d' \tag{15}$$

Teorema 4 *La probabilidad de que la proyección se produzca sobre el subespacio S_h para $0 \le h \le d''-1$ es*

$$P_0 = 1 - \frac{d''-1}{d''}(1-\sigma^2) \tag{16}$$

$$P_h = \frac{1-\sigma^2}{d''} \quad \textit{para todo} \quad 0 < h < d'' \tag{17}$$

Por último vamos a calcular $\mathrm{E}\left[\|\Psi_0 - \tilde{\Psi}_0\|^2\right]$, con el objetivo de determinar la capacidad de corrección del código. Este valor esperado mide la varianza del estado que resulta después de la corrección y se obtiene de la siguiente forma:

$$\mathrm{E}\left[\sum_{h=0}^{d''-1}\sum_{k=hd'}^{(h+1)d'-1} |\alpha_k|^2\|\Psi_0 - E_h^{-1}\Pi_h\Psi\|^2\right] = \sum_{h=0}^{d''-1}\mathrm{E}\left[\sum_{k=hd'}^{(h+1)d'-1} |\alpha_k|^2\|E_h\Psi_0 - \Pi_h\Psi\|^2\right]$$

En la última igualdad hemos usado que E_h es una transformación unitaria y, por tanto, conserva la norma y que $E_0\Psi_0 = \Psi_0$. Además, por la simetría de la distribución del error, el valor esperado es igual para todo $0 < h < d''$. Utilizando estos resultados la expresión anterior queda del siguiente modo:

$$\mathrm{E}\left[\sum_{k=0}^{\lceil d'-1} |\alpha_k|^2 \|\Psi_0 - \Pi_0\Psi\|^2\right] + (d''-1)\ \mathrm{E}\left[\sum_{k=d'}^{\lceil 2d'-1} |\alpha_k|^2 \|E_1\Psi_0 - \Pi_1\Psi\|^2\right]$$

Teorema 5 *Los primeros términos del desarrollo en serie de potencias de σ de la varianza del error después de la aplicación del código corrector son*

$$Var(\tilde{\Psi}_0) \approx 2\left(1 - 2^{d+d'}\frac{d!}{d'!}\frac{(2d'+1)!!}{(2d+1)!!}\sigma\right) \qquad (18)$$

Referencias

[1] D. Aharonov and M. Ben-Or. *Fault-tolerant quantum computation with constant error rate.* SIAM J. Comp., to appear. Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9906129.

[2] A. Ashikhmin and S. Lytsin. *Upper bounds on the size of quantum codes.* IEEE Trans. Inf. Theory, **45** (4), 1206–1215. (1999).

[3] D. Aharonov. *Quantum Computation.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9812037. (1998).

[4] A. Ashikhmin. *Remarks on bounds for quantum codes.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9705037. (1997).

[5] A. Barenco, T. A. Brun, R. Schak and T. P. Spiller. *Effects of noise on quantum error correction algorithms.* Phys. Rev. A, 56, 1177–1188, (1997).

[6] C. H. Bennet, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters. *Mixed state entanglement and quantum error correction.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9909058, (1999).

[7] D. Bacon, J. Kempe, D. A. Lidar and K. B. Whaley. *Universal fault-tolerant computation on decoherence free subspaces.* Phys. Rev. A, 54, 3824, (1996). Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9604024.

[8] A. Cabello. *Bibliographic guide to the foundations of quantum mechanics and quantum information.* Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/0012089, (2001).

[9] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. Sloane. *Quantum error correction and orthogonal geometry.* Phys. Rev. Lett., 78, 405–408, (1997).

[10] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. Sloane. *Quantum error correction via codes over GF(4).* IEEE Trans. Inf. Theory, 44 (4), 1369–1387, (1998).

[11] A. R. Calderbank and P. W. Shor. *Good quantum error-correcting codes exist.* Phys. Rev. A, 54, 1098–1105, (1996). Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9512032.

[12] A. Ekert and C. Macchiavelo. *Error correction in quantum communication.* Phys. Rev. Lett., 77, 2585, (1996). Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9602022.

[13] A. Galindo and M. A. Martín-Delgado. *Information and Computation: Classical and Quantum Aspects.* Reviews of Modern Physics (to appear). Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/0112105, (2001).

[14] D. Gottesman. *Class of quantum error-correcting codes saturating the quantum Hamming bound.* Phys. Rev. A, 54, 1862, (1996).

[15] D. Gottesman. *Stabilizer Codes and Quantum Error Correction.* Ph.D. thesis, Californa Institute of Technology, Pasadena, CA, 1997.

[16] A. Yu Kitaev. *Quantum error correction with imperfect gates.* Quantum Communication, Computing and Measurement, (eds.) Hirota,

Holevo and Caves, 181–188, Plenum Press, New York, 1997.

[17] E. Knill and R. Laflamme. *A theory of quantum-correcting codes.* Phys. Rev. A, 55, 900, 1997. Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/-quant-ph/9604034.

[18] E. Knill, R. Laflamme and L. Viola *Theory of quantum error correction for general noise.* Los Alamos Physics Preprint Archive http://-xxx.lanl.gov/abs/quant-ph/9908066, (1999).

[19] D. A. Lidar, D. A. Bacon and K. B. Whaley. *Concatenating decoherence free subspaces with quantum error correcting codes.* Phys. Rev. Lett., 82 (22), 4556–4559, (1999).

[20] D. A. Lidar, I. L. Chuang and K. B. Whaley. *Decoherence-free subspaces for quantum computation.* Phys. Rev. Lett., 81 (12), 2594–2597, (1998).

[21] R. Laflamme, C. Miquel, J.-P. Paz and W. H. Zurek. *Perfect quantum error correction codes.* Phys. Rev. Lett., 77, 198, (1996). Los Alamos Physics Preprint Archive http://xxx.lanl.-gov/abs/quant-ph/9602019.

[22] D. W. Leung, M. A. Nielsen, I. L. Chuang and Y. Yamamoto. *Approximate quantum error correction can lead to better codes.* Phys. Rev. A, 56, 2567–2573, (1997). Los Alamos Physics Preprint Archive http://xxx.lanl.-gov/abs/quant-ph/9704002.

[23] M. A. Nielsen and L. I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press. 2000.

[24] E. M. Rains. *Quantum weight enumerators.* IEEE Trans. Inf. Theory, 44 (4), 1388–1394, (1998). Los Alamos Physics Preprint Archive http://xxx.lanl.gov/abs/quant-ph/9704002.

[25] E. M. Rains. *Monotonicity of the quantum linear programming bound.* IEEE Trans. Inf. Theory, 45 (7), 2489–2492, (1999).

[26] E. M. Rains. *Nonbinary quantum codes.* IEEE Trans. Inf. Theory, 45 (6), 1827–1832, (1999).

[27] E. M. Rains. *Quantum shadow enumerators.* IEEE Trans. Inf. Theory, 45 (7), 2361–2366, (1999).

[28] E. M. Rains, R. H. Hardin, P. W. Shor and N. J. A. Sloane. *Nonadditive quantum code.* Phys. Rev. Lett., 79 (5), 953–954, (1997).

[29] P. W. Shor. *Scheme for reducing decoherence in quantum computer memory.* Phys. Rev. A, 52, 2493–2496, (1995).

[30] A. Steane. *Quantum computing.* Los Alamos Physics Preprint Archive http://xxx.lanl.-gov/abs/quant-ph/9708022. (1997).

[31] A. M. Steane. *Error correcting codes in quantum theory.* Phys. Rev. Lett., 77, 793–797, (1996).

[32] A. M. Steane. *Multiple particle interference and quantum error correction.* Proc. R. Soc. London A, 452, 2551–2576, (1996).

[33] P. Zanardi. *Stabilizing quantum information.* Los Alamos Physics Preprint Archive http://-xxx.lanl.gov/abs/quant-ph/9910016. (1999).

[34] P. Zanardi and M. Raseti. *Noisless quantum codes.* Phys. Rev. Lett., 79 (17), 3306–3309. (1998).