Introducción a la Computación Cuantica
Corrección de errores cuanticos

Sergio Montoya Ramirez
Kenneth Alejandro Rodriguez Peña

Contents

Chapter 1 — Page 2

1.1 Introducción 2
1.2 Ejemplo: Phase Flip 2
1.3 Formalismos 3
1.4 Códigos Importantes 4
Código de Shor — 5
1.5 Códigos CSS 5
1.6 Conclusiones 5

Chapter 2 — **Bibliografía** — Page 6

Chapter 3 — **Annexos** — Page 7

3.1 Temas faltantes 7
3.2 Circuito de phase flip 7
3.3 Deducción de la cota de Hamming 7
3.4 Circuito de Shor 8
3.5 Demostración de que el código de Shor corrige errores arbitrarios 8
3.6 Demostración de equivalencia para códigos CSS 9

Chapter 1

1.1 Introducción

Uno de los puntos más difíciles para convertir la computación cuántica en una realidad es la gran sensibilidad de los qubits físicos. Dada la naturaleza cuántica de estos, mantener un estado y actuar sobre él sin que colapse o sea alterado por variables externas (como la temperatura o los cambios electromagnéticos) hace que la necesidad de manejar errores en la computación cuántica sea de primera categoría. Al mismo tiempo, el teorema de no clonación impide aplicar estrategias clásicas de corrección de errores, como la redundancia de información. Sin embargo, en 1995 (y posteriormente en 1996), Shor y Calderbank encontraron una forma de abordar este problema: distribuir la información en varios qubits y crear un código que permitiera interpretarlos correctamente para recuperar la información original[3].

Este proyecto tiene como objetivo resumir brevemente algunos de los puntos más importantes del campo *quantum error correction* (QEC). Para lograrlo, se abordarán tres aspectos fundamentales. En primer lugar, se presentará un ejemplo de código de corrección que permitirá entender los patrones generales del campo. A continuación, se examinará una teoría general de errores que proporciona los fundamentos matemáticos necesarios para comprender varios aspectos cruciales de QEC. Por último, se analizarán ejemplos de códigos importantes pertenecientes a la familia de códigos estabilizadores, como el código de Shor y la familia de códigos CSS. No obstante, dada la considerable diferencia entre la notación de estabilizadores y las notaciones aprendidas en el curso, se utilizarán principalmente nociones alternativas a la estabilización para explicarlos.

Esta ruta, aunque limitada por el espacio y tiempo disponibles, permitirá obtener una visión estructurada de las bases de este campo.

1.2 Ejemplo: Phase Flip

Este ejemplo sigue de cerca la presentación del código de bit de repetición para phase flips, como se describe en el Capítulo 10 de Nielsen y Chuang [1]. Imagine que tiene un canal con un ruido que, con probabilidad p, produce un *phase flip* en su qubit. Esto significa que, con probabilidad p, transforma $|\psi\rangle$ en $X|\psi\rangle$. Para este caso, podemos crear nuestro primer código cambiando a una base conocida, con elementos

$$|0_L\rangle = |000\rangle\,; \quad |1_L\rangle = |111\rangle\,.$$

Es decir, el estado $|\psi\rangle = a|0\rangle + b|1\rangle$ se convierte en $a|0_L\rangle + b|1_L\rangle$. Puede ver un circuito que implementa esta conversión en 3.2

Ahora bien, también debemos contar con un procedimiento que nos permita determinar en cuál de los qubits ocurrió el cambio. Para ello, vamos a medir sin hacer distinciones entre estados, de modo que no se destruya el qubit, utilizando los siguientes operadores:

$$\begin{aligned} P_0 &\equiv |000\rangle\langle 000| + |111\rangle\langle 111|\,, \\ P_1 &\equiv |100\rangle\langle 100| + |011\rangle\langle 011|\,, \\ P_2 &\equiv |010\rangle\langle 010| + |101\rangle\langle 101|\,, \\ P_3 &\equiv |001\rangle\langle 001| + |110\rangle\langle 110|\,. \end{aligned}$$

De esta manera, podemos identificar en qué qubit ocurrió el error y, por lo tanto, aplicar nuevamente X para regresar al estado original.

Ahora bien, ¿cómo sabemos que este procedimiento funciona mejor que el caso original? Para ello, definamos la fidelidad, de modo que podamos analizar el peor caso en este canal.

Definition 1.2.1: Fidelidad

Sea ρ la acción de un canal; entonces, la fidelidad se define como

$$F = \sqrt{\langle\psi|\,\rho\,|\psi\rangle}, \tag{1.1}$$

donde $|\psi\rangle$ es el estado de interés (normalmente, el estado inicial).

Note que este canal se comporta como

$$\rho = (1-p)\,|\psi\rangle\,\langle\psi| + pX\,|\psi\rangle\,\langle\psi|\,X.$$

Por lo tanto, tiene una fidelidad de:

$$F = \sqrt{(1-p) + p\,\langle\psi|\,X\,|\psi\rangle\,\langle\psi|\,X\,|\psi\rangle}.$$

Observe que $\langle\psi|\,X\,|\psi\rangle \geqslant 0$, por lo que, en general para este canal, la fidelidad mínima estará definida por la amplitud de probabilidad del estado de interés. En nuestro caso original, $F = \sqrt{1-p}$. Por otro lado, para el caso de nuestro código, nos interesan únicamente los procesos en los que haya ocurrido un error o menos, ya que nuestro código solo corrige en ese caso. La probabilidad de que esto ocurra es la probabilidad de que no ocurra ningún error, es decir, $(1-p)^3$, más tres veces la probabilidad de que ocurra un solo error, es decir, $3p(1-p)^2$. Así, la probabilidad total es

$$(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3,$$

y, en consecuencia, la fidelidad mínima sería $F = \sqrt{1-3p^2+2p^3}$, que es mayor que la original siempre y cuando $p < \frac{1}{2}$.

Este ejemplo nos proporciona algunas de las bases necesarias para comprender el tema de la corrección cuántica de errores. En particular, muestra el funcionamiento general de estos mecanismos, que consiste en codificar la información, distribuirla en más qubits de los estrictamente necesarios y desarrollar un procedimiento que revierta los efectos de los errores. Sin embargo, aún necesitamos mayor formalidad en lo que estamos tratando.

1.3 Formalismos

En el caso anterior vimos un ejemplo muy concreto de un codigo que mejoraba la fiabilidad en un canal con un ruido concreto. Sin embargo, este ejemplo particular se aprovechaba de las caracteristicas del ruido para representar la corrección del error y el aumento en la fiabilidad. Ahora nos interesa construir una teoria mas general de los errores.

Para comenzar es importante definir lo que es un codigo

Definition 1.3.1: Codigo

Sea $\mathcal{L}$ un espacio de tamaño fijo, decimos que $\mathcal{M}$ un subespacio de algun espacio $\mathcal{B}^n$ es un codigo que codifica $\mathcal{L}$ si existe una operación $\mathcal{V} : \mathcal{L} \to \mathcal{M}$ que se le conoce como codificador[2].

Esto es similar a lo que vimos arriba, es un subespcio de n qubits que pueden codificar la información de algun conjunto. Ahora bien, esto es una definición general, estos mismos codigos podrian tomarse simplemente como maneras de dar significado a un subespacio.

Definition 1.3.2: Codigo que Corrige errores

Sea C un codigo y $\mathcal{E}$ un procedimiento que define un error. Decimos que C corrige $\mathcal{E}$ si existe un procedimiento $\mathcal{R}$ tal que[1]

$$\forall p \in C : (\mathcal{R} \circ \mathcal{E})(p) \propto p \tag{1.2}$$

Una nota importante que ver es que el $\propto$ nos representa que realmente la operación de recuperación no nos devuelve exactamente al qubit original. Sin embargo, si nos debe devolver a un qubit que codifique la misma información que el anterior.

Theorem 1.3.1 Condiciones para que un Codigo Corriga un error

Sea C un codigo y P el proyector a C. Suponga que $\mathcal{E}$ es una operación cuantica con elementos $\{E_i\}$. Una condición necesaria y suficiente para que exista una operación $\mathcal{R}$ que corrija $\mathcal{E}$ en C es

$$PE_i^\dagger E_j P = \alpha_{ij} P \tag{1.3}$$

para alguna matriz hermitica α de numeros complejos[1].
Nota: Este teorema lo puede encontrar como el teorema 10.1 en el libro de Nielsen y Chuang acompañado de su respectiva demostración. La demostración no se tendra aqui pues requiere el uso de muchos otros teoremas que salen del alcance de este texto.

Sin embargo, esta es solo una manera de saber que un codigo corrige un error. Algo importante es poder encontrar el mejor codigo para cierto error. Para esto podemos usar la cota de Hamming que nos dice el limite teorico de eficiencia de un codigo que corrija un error.

Theorem 1.3.2 Cota de Hamming

Sea C un codigo que codifica k qubits en n qubits y que puede corregir cualquier subconjunto de t errores. Particularmente, asuma sin perdida de generalidad que corrige $j \leq t$ errores. Entonces se cumple la cota [1]

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leq 2^n \tag{1.4}$$

Nota: La deducción de este cota la puede encontrar en **??**.

Como ultima nota importante antes de pasar a los codigos que vamos a explicar es el formalismo de estabilizadores. Este es importante pues muchos de los codigos mas importantes en QEC son basados en este mismo formalismo.

Las bases del formalismo de estabilizadores consiste en mirar un estado no desde sus caracteristicas si no desde los operadores que lo estabilizan. Un operador se dice que estabiliza a un estado si el estado es un eigenvector con eigenvalue +1. Es decir, S estabiliza $|\psi\rangle$ si $s|\psi\rangle = |\psi\rangle$[1].

Example 1.3.1 (Ejemplo de Estabilizador)

En nuestro primer ejemplo para el qubit

$$|\psi\rangle = a|000\rangle + b|111\rangle$$

Los operadores definidos P_i eran estabilizadores de este. Puesto que al aplicarlo nos devolvian el mismo qubit sin cambios.

Una de las caracteristicas mas importantes es que al definir de esta manera un estado estamos construyendo grupos y por tanto podemos usar teoria de grupos para realizar las interpretaciones de los diversos codigos. Esto es parte de lo que hace tan increiblemente fuerte el formalismo de estabilizadores y lo que nos va a permitir hablar de los siguientes codigos que usan este formalismo.

1.4 Códigos Importantes

A continuación, veremos ejemplos de códigos de corrección de errores importantes en el campo. Todos estos códigos son estabilizadores. Mencionaremos las operaciones que estabilizan estos códigos para ejemplificar su funcionamiento. Sin embargo, debido a la extensión de los temas y a lo novedoso de la notación de estabilizadores, utilizaremos principalmente explicaciones que no dependan de ellos.

1.4.1 Código de Shor

Este fue uno de los primeros códigos de corrección de errores, diseñado por Shor en 1995 en el artículo *Scheme for reducing decoherence in quantum computer memory*. Este código permite corregir errores arbitrarios en un solo qubit.

El código se define mediante el circuito que puede verse en el anexo 3.4, transformando $|0\rangle \to |+++\rangle$ y $|1\rangle \to |---\rangle$. La operación de recuperación se divide en dos partes:

1. Determinar el qubit afectado. Aquí resulta crucial que este código sea estabilizador, ya que utilizamos sus operadores para identificar el qubit donde ocurrió el error.

2. Una vez identificado el qubit erróneo, se procede a corregirlo. La corrección es un término genérico, ya que este código corrige errores arbitrarios. Puede consultarse el anexo 3.5 para más detalles.

1.5 Códigos CSS

Los códigos CSS (Calderbank-Shor-Steane) son un subconjunto de los códigos estabilizadores. Informalmente, permiten construir códigos que corrigen los mismos errores a partir de dos códigos existentes, utilizando menos qubits para la codificación.

Definition 1.5.1: Códigos CSS

Sean C_1 y C_2 códigos lineales $[n, k_1]$ y $[n, k_2]$ (cerrados bajo suma módulo 2) tales que:

- $C_2 \subset C_1$,
- C_1 y $C_2^{\perp}$ corrigen t errores.

Definimos el código CSS de C_1 sobre C_2 como el código $[n, k_1 - k_2]$ denotado por $CSS(C_1, C_2)$ mediante el siguiente procedimiento. Sea $x \in C_1$, entonces definimos el estado:

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

donde $+$ denota suma módulo 2. Nótese que si $x' \in C_1$ y $x - x' \in C_2$, entonces $|x + C_2\rangle = |x' + C_2\rangle$. El código $CSS(C_1, C_2)$ corresponde al espacio generado por los estados $|x + C_2\rangle$, los cuales forman un conjunto ortonormal[1].
Nota: Para más detalles sobre la igualdad $|x + C_2\rangle = |x' + C_2\rangle$, consúltese el anexo 3.6.

La ventaja de esta construcción es evidente: si encontramos un subcódigo que corrija los mismos t errores, podemos reducir considerablemente el tamaño del código original. Un ejemplo notable de código CSS es el código de Shor.

1.6 Conclusiones

En este trabajo se estudiaron y explicaron los conceptos básicos de la corrección de errores cuánticos. Con ello, se comprendió que un código cuántico permite distribuir la información en múltiples qubits, lo cual ofrece ventajas significativas para manejar los errores característicos de la computación cuántica. Además, se presentaron las bases teóricas de la corrección de errores y se enunciaron algunos de sus teoremas más importantes, que permiten determinar si un código corrige un error determinado. Finalmente, se analizaron de manera general dos casos relevantes: el código de Shor y la familia de códigos CSS. Si bien esta es una introducción incompleta al tema, resulta suficiente para obtener una visión general de los patrones que sigue.

Chapter 2

Bibliografía

Este texto está basado principalmente en el libro *Quantum Computation and Quantum Information* de Michael A. Nielsen e Isaac L. Chuang. La mayor parte de la información aquí presentada proviene de ejemplos y desarrollos incluidos en esa obra. No obstante, también se consultaron otras referencias, que se listan a continuación, junto con una breve explicación sobre su uso.

1. Nielsen, Michael A. e Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10.ª ed. Cambridge University Press, 2010.

   Esta obra constituye la bibliografía principal. Todos los temas tratados en el presente texto son abordados con mayor detalle en el capítulo 10 de dicho libro.

2. Kitaev, Aleksei Yu., Alexander Shen y Mihail N. Vyalyi. *Classical and Quantum Computation*. Graduate Studies in Mathematics 47. American Mathematical Society, 2002.

   Este libro permitió profundizar en algunos detalles matemáticos, en particular para la definición de códigos. La definición utilizada aquí es una versión simplificada, ya que no era posible incluir el nivel de detalle que ofrece esta referencia.

3. Calderbank, A. R. y Peter W. Shor. "Good Quantum Error-Correcting Codes Exist". *Physical Review A* 54, n.° 2 (1996): 1098-1105. https://doi.org/10.1103/PhysRevA.54.1098.

   Este fue uno de los primeros artículos sobre códigos cuánticos de corrección de errores. Se utilizó especialmente para la introducción y algunas definiciones, dado que, al ser un trabajo fundacional, presenta una sección introductoria y de definiciones particularmente útil.

4. Shor, Peter W. "Scheme for Reducing Decoherence in Quantum Computer Memory." Physical Review A 52, no. 4 (1995): R2493–96. https://doi.org/10.1103/PhysRevA.52.R2493.

   Este es uno de los primeros artículos en computación cuantica y la presentación del codigo de 9 qubits de Shor. Se utilizo para la definición de este codigo en el texto.

Chapter 3

Annexos

3.1 Temas faltantes

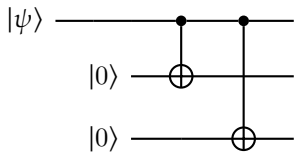
El QEC (Quantum Error Correction) es un campo inmenso y muy activo en la investigación actual. Por lo tanto, en un texto de estas características resultaba imposible cubrirlo todo. Aun con esta limitación, que entendemos el lector comprende, existían aspectos importantes relacionados con el contenido de este texto que no se cubrieron por falta de espacio. Así, esta sección no pretende mencionar temas omitidos por el nivel de complejidad, sino detalles relevantes que no alcanzaron a ser tratados.

1. **Códigos degenerados:** Este tema es crucial para el campo del QEC, pues representa una de las diferencias clave entre la corrección de errores clásica y la cuántica. No se cubrió porque, aunque era relevante para partes de este trabajo (como la cota de Hamming), resultaba particularmente extenso y sus implicaciones no eran imprescindibles (por ejemplo, no se conoce un código degenerado que esté por debajo de la cota de Hamming [1]).

2. **Códigos lineales:** Durante la explicación de los códigos CSS se menciona que C_1 y C_2 son lineales, y se aclara qué significa ser lineal en el contexto de la demostración particular (se hará uso de esto en el anexo 3.6). Sin embargo, no se define explícitamente en qué consisten. Esto se debe a que es un concepto heredado de la computación clásica y, aunque relevante para QEC, su definición y funcionamiento quedaban fuera del alcance de este texto.

3. **Teoría de grupos para estabilizadores:** En el texto se mencionó que parte de la fortaleza del formalismo de estabilizadores proviene de su uso de la teoría de grupos. Sin embargo, no se explicó cómo los estabilizadores generan un grupo ni por qué esto tiene un efecto tan relevante. La razón para omitirlo fue el espacio y el alcance del texto, ya que habría requerido definir qué es un grupo, álgebras entre grupos, entre otros conceptos que no era posible incluir en estas circunstancias.

3.2 Circuito de phase flip



3.3 Deducción de la cota de Hamming

Esta deducción seguirá el enfoque de Nielsen y Chuang [1].

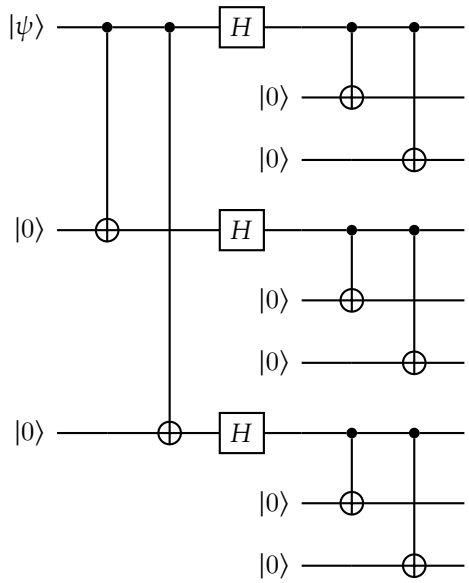
Sea C un código que codifica k qubits en n qubits y es capaz de corregir cualquier subconjunto de hasta t errores. En particular, sin pérdida de generalidad, asumamos que corrige $j \leqslant t$ errores. Existen $\binom{n}{j}$ posiciones

posibles para estos j errores. Nótese que, para $j \leqslant t$, en el código final debemos considerar la suma de todos los valores posibles de j.

Además, dado que cualquier error puede representarse como una combinación de los operadores X, Y y Z, hay 3^j posibilidades de error. Por último, si se desea que el código sea no degenerado (algo no siempre necesario), se requeriría un espacio de dimensión 2^k. Todos estos elementos deben cumplir que la dimensión total sea menor o igual al número de estados disponibles en el espacio de Hilbert de n qubits, lo que resulta en:

$$\sum_{j=0}^{t} \binom{n}{j} 3^j 2^k \leqslant 2^n$$

3.4 Circuito de Shor



3.5 Demostración de que el código de Shor corrige errores arbitrarios

Supongamos que tenemos un error $\mathcal{E}$ con elementos $\{E_i\}$, de modo que para el estado $|\psi\rangle = a\,|0_L\rangle + b\,|1_L\rangle$ se cumple:

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \sum_i E_i\,|\psi\rangle\langle\psi|\,E_i^\dagger.$$

Ahora bien, sabemos que cualquier E_i puede escribirse como una combinación lineal de la forma:

$$E_i = e_{i0}I + e_{i1}X_j + e_{i2}Z_j + e_{i3}X_jZ_j,$$

donde j es el número del qubit en el que ocurre el error. Esto nos proporciona el elemento invertible necesario para corregir un error arbitrario. Cabe aclarar que este resultado supone que los errores actúan de manera independiente entre qubits, lo cual es una aproximación razonable, aunque existen condiciones en las que esta suposición no se cumple. En tales casos, es preferible utilizar un código que corrija errores en más de un qubit, como, por ejemplo, algunos códigos de la familia CSS.

3.6 Demostración de equivalencia para códigos CSS

Debemos demostrar que si $x - x' \in C_2$, entonces $|x + C_2\rangle = |x' + C_2\rangle$. Para ello, sea $z = x - x'$. Así,

$$\begin{aligned} |x' + C_2\rangle &= \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x' + y\rangle \\ &= \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + z + y\rangle \\ &= \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + (z + y)\rangle \,. \end{aligned}$$

Nótese que, como + denota la suma módulo 2 y estamos trabajando con códigos lineales (que son cerrados bajo esta operación), si $z \in C_2$, entonces $z + y$ recorre todo C_2 cuando y lo hace. Por lo tanto, podemos redefinir $y' = z + y$ y obtener:

$$\begin{aligned} |x' + C_2\rangle &= \frac{1}{\sqrt{|C_2|}} \sum_{y' \in C_2} |x + y'\rangle \\ &= |x + C_2\rangle \,, \end{aligned}$$

lo cual completa la demostración. □