Bases de corrección cuantica de errores

Sergio Montoya Ramirez [1] Kenneth Alejandro Rodriguez Peña [1]

[1]Univerisad de los Andes

Introducción

La computación cuántica enfrenta un reto fundamental con los qubits físicos, pues son extremadamente sensibles al ruido y al entorno (por su naturaleza cuántica), lo que genera errores incluso antes de realizar operaciones lógicas. Así mismo, el teorema de no clonación impide aplicar estrategias clásicas de correción de errores sobre los qubits. Es de esta manera, que Shor (1995) y Calderbank–Shor–Steane (1996) introdujeron los primeros códigos de corrección cuántica, basados en distribuir la información de un qubit en varios qubits físicos y detectar qué error ocurrió sin medir directamente el estado lógico.

En este trabajo se resumirán los elementos básicos de la corrección cuántica: ejemplos simples, fundamentos matemáticos y códigos estabilizadores como los de Shor y CSS.

Ejemplo: Phase Flip

El canal de *phase flip* consiste en invertir la fase del qubit con una probabilidad p de que ocurra. Para corregirlo, se propone un código de tres qubits con estados lógicos

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

Si un error ocurre en uno de los tres qubits, medimos operadores que identifican cuál fue afectado sin destruir la información lógica. Esto permite aplicar X en el qubit correcto para recuperar el estado original, lo cual se consigue con operadores estabilizadores:

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

Formalismos

Codigo

Sea $\mathcal{L}$ un espacio de tamaño fijo, decimos que $\mathcal{M}$ un subespacio de algun espacio 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.

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

$$\forall p \in C : (\mathcal{R} \circ \mathcal{E})(p) \propto p \tag{1}$$

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.

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

$$PE_i^\dagger E_j P = \alpha_{ij} P \tag{2}$$

para alguna matriz hermitica α de numeros complejos.

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]

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

Estabilizadores

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].

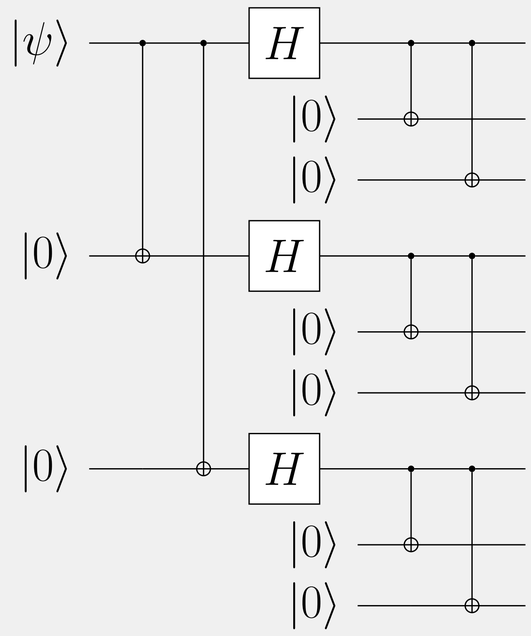
Una de las caracteristicas mas importantes es que al definir de esta manera un estado estamos construyendo grupos y por tanto podemos usar teoria de grupos para realizar las interpretaciones de los diversos codigos. Esto es parte de lo que hace tan increiblemente fuerte el formalismo de estabilizadores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

Codigo 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 la figura, 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.



¿Por que puede corregir 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:

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

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.

Codigos 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.

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].

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.

References

[1] A. R. Calderbank and Peter W. Shor.
Good quantum error-correcting codes exist.
Physical Review A, 54(2):1098–1105, 1996.

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

[3] Michael A. Nielsen and Isaac L. Chuang.
Quantum Computation and Quantum Information.
Cambridge University Press, 10 edition, 2010.

[4] Peter W. Shor.
Scheme for reducing decoherence in quantum computer memory.
Physical Review A, 52(4):R2493–R2496, 1995.