UNIVERSIDAD DE GRANADA

Facultad de Ciencias

Doble Grado en Física y Matemáticas

Trabajo Fin de Grado

ESTRUCTURAS ALGEBRAICAS EN COMPUTACIÓN CUÁNTICA: DISEÑO DE ALGORITMOS CLÁSICOS DE SIMULACIÓN DE CIRCUITOS CUÁNTICOS

Presentado por:
D./D[a]. José Alberto Azorín Puche

Curso Académico 2020-2021

Declaración de originalidad

D. José Alberto Azorín Puche

Declaro explícitamente que el trabajo presentado como Trabajo de Fin de Grado (TFG), correspondiente al curso académico 2020-2021, es original, entendida esta, en el sentido de que no ha utilizado para la elaboración del trabajo fuentes sin citarlas debidamente.

En Granada a 5 de mayo de 2021

Fdo: José Alberto Azorín Puche

Summary

Aquí va un resumen amplio en inglés del trabajo realizado (se recomienda entre 800 y 1500 palabras). En el caso de que la memoria se presente en inglés, este resumen debe ser en español.

Índice

1 Introducción

2 Fundamentos matemáticos

2.1 Teoría de grupos

2.2 Espacios de Hilbert

2.3 Análisis simpléctico

En este breve apartado se introduce una herramienta nueva, ahora desconocida para nosotros, pero que cada vez se utiliza más en diversos ámbitos de la Física y la Computación. Se trata de las **matrices simplécticas**:

Definición 1. *Definida la matriz* $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in \mathbb{R}^{2n\times 2n}$, *decimos que una matriz* $M \in \mathbb{R}^{2n\times 2n}$ *es simpléctica si se verifican las siguientes igualdades:*

$$M^T J M = M J M^T = J \tag{2.1}$$

Notaremos el conjunto de todas las matrices simplécticas de dimensión $2n$ *por* $Sp(2n, \mathbb{R})$.

Como $J^T = J^{-1} = -J$, si M es simpléctica también lo será su matriz inversa S^{-1}:

$$(M^{-1})^T J M^{-1} = -(M^{-1})^T J^{-1} M^{-1} = -(M^T)^{-1} J^{-1} M^{-1} = -(M J M^T)^{-1} = -J^{-1} = J$$
$$M^{-1} J (M^{-1})^T = -M^{-1} J^{-1} (M^{-1})^T = -M^{-1} J^{-1} (M^T)^{-1} = -(M^T J M)^{-1} = -J^{-1} = J$$

Además, es trivial reconocer que el producto de matrices simplécticas es, a su vez, una matriz simpléctica. Así, se tiene que $\mathrm{Sp}(2n, \mathbb{R})$ es un grupo, aquel llamado **grupo simpléctico**.

Se puede comprobar que la definición presentada anteriormente es redundante, puesto que las igualdades 2.1 son, de hecho, equivalentes:

$$M^T J M = J \quad \Leftrightarrow \quad (M^T J M)^{-1} = J^{-1} \quad \Leftrightarrow \quad -M^{-1} J (M^T)^{-1} = -J \quad \Leftrightarrow \quad J = M J M^T$$

Así, bastará con que se verifique una de las dos para que automáticamente se cumpla la otra, simplificándose la definición 1.

Pasamos a definir otra utilidad que necesitaremos para comprender en 4 cómo funciona el algoritmo: el **producto simpléctico**.

Definición 2. *Diremos que una forma bilineal es una forma simpléctica si es antisimétrica y no degenerada. Un caso especial es el conocido como producto simpléctico (o forma simpléctica estándar)* $\sigma : \mathbb{R}^{2n} \times \mathbb{R}^{2n} \longrightarrow \mathbb{R}$, *definido por*

$$\sigma(z, z') = p \cdot x' - p' \cdot x \tag{2.2}$$

donde $z = (x, p)$ *y* $z' = (x', p')$, *con* $x, x', p, p' \in \mathbb{R}^n$ *y "$\cdot$" denota el producto escalar en* $\mathbb{R}^n$.

En efecto, se verifica que $\sigma(z, z') = -\sigma(z, z')$ (antisimetría) y esto implica que todos los vectores z son *isótropos*, esto es, $\sigma(z, z) = 0$.

2.4 Producto tensorial

Proposición 1. *La traza del producto tensorial es el producto de las respectivas trazas*

*** Poner el enunciado bonito y probar el caso que nos interesa (matrices 2x2)

3 Introducción a la Computación Cuántica

Este apartado nos dotará de todo conocimiento necesario para poder abordar nuestro objetivo de comprender el algoritmo [2] y mejorar su eficiencia:

3.1 Postulados de la Mecánica Cuántica

Todo el formalismo de la Mecánica Cuántica puede describirse a partir de unos pocos postulados que resultan de la experimentación. Su validez se comprueba, además, empíricamente: toda la teoría que se ha derivado a partir de ellos funciona sorprendentemente bien con lo que ocurre en la Naturaleza.
Estos postulados [5] nos darán una base sobre la que construir el formalismo matemático necesario para comprender el tratamiento de la información que vamos a hacer:

Postulado 1 Estado de un sistema

Un sistema físico está asociado a un espacio de Hilbert complejo y separable, y un estado puro del sistema (en el instante t) viene descrito por un vector unitario, representado por un ket $|\psi(t)\rangle$ de dicho espacio. [1]

Postulado 2 Observables y operadores

Todo observable de un sistema físico (posición, momento, potencial, etc.) se representa por un operador lineal autoadjunto actuando en el espacio de Hilbert asociado, cuyos vectores propios forman una base completa del mismo.

Postulado 3 Medida de los observables

La medida de un observable A (sobre un cierto estado $|\psi(t)\rangle$) se representa por la acción del operador asociado sobre el correspondiente vector unitario. Por tanto, los únicos valores posibles son los valores propios $\{a_n\}$ (que son reales) del operador. Si el resultado de la observación es a_k, el estado colapsa inmediatamente, proyectándose sobre el subespacio propio asociado a a_k, generado por los vectores propios $\left\{\left|a_k^{(i)}\right\rangle\right\}$:

$$A\,|\psi(t)\rangle = a_k \left|a_k^{(i)}\right\rangle \quad \Rightarrow \quad |\psi(t')\rangle = \frac{P_{A,a_k}\,|\psi(t)\rangle}{\| P_{A,a_k}\,|\psi(t)\rangle \|} \tag{3.1}$$

donde $P_{A,a_k} = \sum_i \left|a_k^{(i)}\right\rangle \left\langle a_k^{(i)}\right|$, siendo discreto el espectro de A.

Postulado 4 Resultado probabilístico de la medida

Si el observable A tiene un espectro discreto, la probabilidad al medirlo de obtener el autovalor a_k (posiblemente degenerado) viene dado por

$$p(a_k) = \frac{\sum_i \left|\left\langle a_k^{(i)}\middle|\psi\right\rangle\right|^2}{\langle\psi|\psi\rangle} \tag{3.2}$$

[1] Se deduce el **Principio de Superposición**: cualquier superposición de estados puros es, a su vez, un estado puro del sistema, entendiéndose superposición como una combinación lineal $\sum_n a_n|\psi_n(t)\rangle$ con coeficientes complejos tales que $\sum_n |a_n|^2 = 1$.

Postulado 5 Evolución temporal de un sistema

La evolución temporal de un estado $|\psi(t)\rangle$ está regida por la ecuación de Schrödinger independiente del tiempo:

$$i\hbar\frac{\partial|\psi(t)\rangle}{\partial t} = \mathcal{H}|\psi(t)\rangle \ , \tag{3.3}$$

donde $\mathcal{H}$ es el operador hamiltoniano, que describe la energía total del sistema.

3.1.1 El operador densidad

El formalismo de la Mecánica Cuántica, tal y como lo hemos presentado, deriva predicciones estadísticas sobre un conjunto (una colección) de sistemas físicos idénticamente preparados, todos ellos caracterizados por un mismo estado $|\psi\rangle$. Por ejemplo, imaginemos un haz de átomos de plata, todos con el mismo estado de espín, como el que resulta del experimento de Stern-Gerlach. En este caso, el haz está polarizado; sin embargo, sabemos que previo al experimento, la orientación de los espines no está polarizada, tenemos un conjunto completamente aleatorio de estados.

¿Cómo tratar, pues, la situación en que haya distintos estados para los sistemas de la preparación? En tal caso, se definen los **estados mezcla** como una colección de sistemas dentro de la cual, una fracción de los elementos presentan un estado $|\psi_1\rangle$ y la fracción restante presenta otro, $|\psi_2\rangle$. Matemáticamente, el estado mezcla se describe por medio de la conocida como **matriz de paridad**[2] :

$$\rho = \omega_1|\psi_1\rangle\langle\psi_1| + \omega_2|\psi_2\rangle\langle\psi_2| \qquad \text{donde } \ \omega_1+\omega_2 = 1. \tag{3.4}$$

Los pesos ω_1 y ω_2 serían las proporciones (expresadas en tanto por uno) de cada uno de los estados presentes en la mezcla. Obsérve que en caso de que sólo hubiera un estado, el operador densidad $\rho = |\psi_1\rangle\langle\psi_1|$ estaría refieriéndose a un estado puro. Este operador es autoadjunto y cumple la condición de normalización $\mathrm{Tr}(\rho) = 1$.

Ahora que contamos con esta nueva herramienta para describir una situación más general que la anterior, es necesaria una reformulación de los postulados 3 y 4 recogidos en la página anterior:

Postulado 3′ Si un sistema físico está en un estado mezcla descrito por una matriz de densidad ρ y medimos un observable A, obteniéndose el valor propio a, el sistema se transforma en un estado mezcla descrito por la matriz de densidad

$$\rho_{A,a} = \frac{P_{A,a}\rho P_{A,a}}{\mathrm{Tr}(\rho P_{A,a})} \tag{3.5}$$

Postulado 4′ Si un sistema físico se encuentra en un estado descrito por una matriz de densidad ρ, entonces la probabilidad de obtener el valor propio a de un observable A es

$$p_a = \mathrm{Tr}(\rho P_{A,a}) \tag{3.6}$$

[2] Para un estado mezcla donde aparecen k estados distintos, definiríamos la matriz de paridad como $\rho = \sum_{i=1}^{k}\omega_i|\psi_i\rangle\langle\psi_i|$, con la ligadura $\sum_{i=1}^{k}\omega_i = 1$.

3.2 Qubits y puertas cuánticas

A continuación, pasamos a describir con detalle los que serán los elementos esenciales de la Computación Cuántica: el qubit y las diferentes puertas cuánticas. Gracias a ellos, es posible realizar una analogía muy clara entre circuitos eléctricos clásicos y los circuitos cuánticos que trataremos de simular.

3.2.1 El qubit: la unidad básica de información

Es conocido que la forma más simple de almacenar información en un ordenador clásico es el **bit**, que toma valores binarios, esto es, que solo puede encontrarse en dos estados (0 y 1). Además, dichos estados son físicamente realizables con componentes muy sencillos (interruptor abierto/cerrado, bombilla encendida/apagada, etc.) y, de ahí que, para observar en qué estado se halla, baste con observar el bit.

La estructura análoga en Computación Cuántica es el **qubit**, o bit cuántico, dado por un sistema cuántico que presenta dos estados básicos $|0\rangle$ y $|1\rangle$ (pensemos, por ejemplo, en un átomo que puede estar en su estado energético fundamental o en un estado excitado), de los que hay que destacar que conforman un sistema ortonormal.

La clave de esto es que, mientras el bit clásico (llamémoslo b) es un elemento $b \in \{0,1\} \cong \mathbb{Z}_2$, el qubit es un vector unitario en un espacio de Hilbert $\mathcal{H}$ complejo y separable, como rezaba el Postulado 1. Así, el qubit puede encontrarse en uno de los estados básicos o una superposición $|\psi\rangle \in \mathcal{H}$ cualquiera de ellos:

$$|\psi\rangle = \alpha_1 |0\rangle + \alpha_2 |1\rangle \quad / \quad |\alpha_1|^2 + |\alpha_2|^2 = 1 \tag{3.7}$$

Nace así, de forma natural, el modelo matemático que nos permitirá trabajar con este nuevo elemento: los vectores $|0\rangle$ y $|1\rangle$ constituyen una base del espacio de Hilbert asociado al sistema, que en nuestro caso será $\mathcal{H} = \mathbb{C}^2$.

A partir de ahora, identificaremos la base $\mathcal{B}_1 = \{|0\rangle, |1\rangle\}$ con la base canónica, $\{(1,0),(0,1)\}$, de manera que podremos escribir los estados en superposición (3.7) en la forma (α_1, α_2).

Conviene, antes de continuar, presentar una segunda base de $\mathbb{C}^2$ que también es relevante y conocida. Se trata de la formada por los llamados "estados equiprobables":

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \overset{\mathcal{B}_1}{=} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad , \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \overset{\mathcal{B}_1}{=} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \tag{3.8}$$

En conclusión, los qubits pueden existir en todo un continuo de estados entre $|0\rangle$ y $|1\rangle$ hasta el instante en que son observados, cuando colapsan, pero nunca podremos conocer (por medio de la observación) las amplitudes que los describen.

3.2.2 Operando sobre los qubits: puertas y medida

Una vez hemos presentado la forma de representar la información, es inevitable preguntarse cómo podemos manipularla: dado que los estados son vectores de $\mathbb{C}^2$, las operaciones que emplearemos con ellos vienen dadas por matrices de $\mathbb{C}^{2\times 2}$. A estas operaciones las llamaremos **puertas cuánticas**, volviendo al paralelismo con la computación clásica y sus puertas lógicas.

Sin embargo, no todas las matrices son válidas: al aplicar una puerta cuántica sobre un qubit, se obtiene un nuevo estado, de forma que la ligadura $|\alpha_1|^2 + |\alpha_2|^2 = 1$ ha de cumplirse antes y después de la aplicación. Como la norma ha de conservarse (los vectores son unitarios), las puertas cuánticas sólo podrán venir dadas por matrices unitarias[3]. Se tiene además el recíproco: toda matriz unitaria puede actuar como una puerta cuántica (en particular, la identidad).

A continuación, se presentan las puertas cuánticas (sobre un qubit) que jugarán algún papel dentro del algoritmo con el que vamos a trabajar:

Matrices de Pauli

Estas tres matrices, muy empleadas en Mecánica Cuántica, suponen los cimientos sobre los que se construye el formalismo estabilizador, que estudiaremos más adelante. Son las siguientes:

$$X \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad , \quad Y \equiv \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad , \quad Z \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.9}$$

Las puertas X y Z son las más relevantes y tienen una interpretación muy sencilla de comprender:

X es el equivalente cuántico de la puerta lógica NOT: convierte $|0\rangle$ en $|1\rangle$ y viceversa. Sus valores propios son +1 y -1, siendo sus autovectores asociados los estados equiprobables, $|+\rangle$ y $|-\rangle$, respectivamente. Resumiendo:

$$X \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_2 \\ \alpha_1 \end{pmatrix} \quad , \quad \begin{matrix} X|+\rangle = +|+\rangle \\ X|-\rangle = -|-\rangle \end{matrix} \tag{3.10}$$

Por su parte, lo que hace Z es invertir el signo de la amplitud asociada al vector $|1\rangle$, dejando invariante la amplitud del otro. Sus vectores propios son los estados básicos, $|0\rangle$ y $|1\rangle$, correspondientes a los valores propios +1 y -1. En definitiva,

$$Z \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ -\alpha_2 \end{pmatrix} \quad , \quad \begin{matrix} Z|0\rangle = +|0\rangle \\ Z|1\rangle = -|1\rangle \end{matrix} \quad . \tag{3.11}$$

Puerta Hadamard

Se trata de una matriz que convierte la base de los estados básicos en la base de los estados equiprobables (3.8). Como H es su propia inversa, resulta que también transforma los estados equiprobables en los estados básicos:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad , \quad \begin{matrix} H|0\rangle = |+\rangle & H|+\rangle = |0\rangle \\ H|1\rangle = |-\rangle & H|-\rangle = |1\rangle \end{matrix} \tag{3.12}$$

Puerta de fase

[3] Si U es una puerta cuántica y $U|\psi\rangle = |\psi'\rangle$, se tiene $1 = \langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle \Rightarrow U^\dagger U = I$.

Se trata de un caso particular de las denominadas puertas de desplazamiento de fase, R_ϕ. Estas puertas dejan invariante el estado base $|0\rangle$, pero añaden una cierta fase a $|1\rangle$. No modifican la probabilidad de medir un estado básico o el otro. La puerta de fase P, aquella que nos interesa, es la que aporta una fase de $\phi = \frac{\pi}{2}$:

$$R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \quad \Rightarrow \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad , \quad \begin{aligned} P|0\rangle &= |0\rangle \\ P|1\rangle &= i|1\rangle \end{aligned} \tag{3.13}$$

Otros ejemplo de puertas de desplazamiento de fase serían la puerta $R_{\frac{\pi}{4}}$ (que llamamos puerta $\frac{\pi}{8}$), o la puerta Z, que resulta ser $Z = R_\pi$) .

Medida del qubit

Después de haber manipulado un qubit, aplicando sobre él las puertas cuánticas convenientes y relacionándolo con otros qubits del circuito, decidimos que queremos medir su estado. Este proceso se representará con una puerta de medida.

Como consecuencia del Postulado 3 y el Postulado 4, cuando observemos un qubit, éste colapsará al estado $|0\rangle$ con probabilidad $|\alpha_1|^2$ o al estado $|1\rangle$ con probabilidad $|\alpha_2|^2$.

La'puerta"que se emplea para transformar el qubit en un estado básico (aquel hacia el que colapsa al ser medido) es el proyector asociado a dicho estado básico. Sin embargo, ésta no podrá ser considerada como puerta cuántica, ya que es singular y no es unitaria.

Acabamos de recordar que los proyectores son, en general, matrices singulares como motivo para ver que no pueden ser puertas cuánticas. ¿Qué problema hay?

Dado que una puerta viene dada por una matriz unitaria U, su inversa será su matriz adjunta $U^\dagger$; así, cualquier puerta cuántica está representada por una matriz que ha de ser forzosamente reversible. De hecho, esta es una de las grandes ventajas respecto de la Computación Clásica que se introducen con la Computación Cuántica: una vez se ha realizado una operación sobre el qubit, podemos deshacer nuestros pasos sin más que aplicar la operación invertida.

3.2.3 Extensión a sistemas de varios qubits

Comencemos pensando lo que ocurre con bits clásicos. Si tomamos el caso en que sólo tenemos 2 bits (cada uno de ellos con dos estados posibles $\{0, 1\}$), entonces el sistema conjunto podrá adoptar cualquiera de las 4 combinaciones distintas que podemos formar con ellos : 00, 01, 10, 11 (dos interruptores abiertos, uno abierto y otro cerrado, etc.).

Volviendo a los bits cuánticos, el planteamiento es el mismo: un sistema de 2 qubits podrá encontrarse en los estados básicos $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$. Sin embargo, el Principio de Superposición vuelve a abrir una brecha entre bits clásicos y cuánticos: si el sistema puede hallarse en cualquiera de los estados básicos, también puede estar en una superposición de ellos:

$$|\psi\rangle = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle \quad / \quad |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 = 1$$

Generalicemos esto para un sistema de n qubits:

Los posibles estados básicos en los que podemos encontrar el sistema se corresponden con todas las combinaciones de longitud n posibles que podemos crear a partir de valores binarios. En el caso clásico, los estados son elementos de $\{0,1\}^n \equiv \mathbb{Z}^n$.

Para el caso cuántico, la formulación matemática es algo más compleja: cada estado básico del sistema de n qubits vendrá dado por el producto tensorial de los diferentes estados básicos de las componentes que lo conforman. Por ejemplo, tomando $n = 6$, un posible estado básico sería $|001011\rangle = |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle$. Se deduce, por tanto, que los estados básicos de un sistema de n qubits (y por tanto cualquier superposición de ellos) serán elementos del espacio vectorial complejo de dimensión 2^n obtenido como el producto tensorial $\mathbb{C}^2 \otimes \overset{n}{\ldots} \otimes \mathbb{C}^2 \equiv \left(\mathbb{C}^2\right)^{\otimes n}$.

Es importante definir correctamente la base que describirá el espacio que acabamos de conocer para trabajar de forma clara y adecuada. La base vendrá dada por los 2^n estados básicos del sistema, ordenados siguiendo la denominada "ordenación canónica": si empezamos a contar desde 0, cada estado se halla en la posición que se corresponde con su traducción de código binario al sistema decimal.

Lo comprenderemos mejor con un ejemplo. Un sistema de 3 qubits se representa con el espacio 8-dimensional $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Lo describiremos con la siguiente base (ordenada):

$$\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |101\rangle, |111\rangle\}$$

Así, un estado cualquiera de este sistema vendrá expresado como

$$|\psi_3\rangle = \alpha_1 |000\rangle + \alpha_2 |001\rangle + \alpha_3 |010\rangle + \alpha_4 |011\rangle + \alpha_5 |100\rangle + \alpha_6 |101\rangle + \alpha_7 |110\rangle + \alpha_8 |111\rangle ,$$

donde los cuadrados de los módulos de los coeficientes suman 1.

Es aquí donde se puede empezar a atisbar otra de las bondades de la Computación Cuántica frente al modelo clásico: con n bits clásicos podemos representar un sólo estado, mientras que si empleamos n qubits, podemos almacenar 2^n estados diferentes a la vez.

******* CUANDO HAYA INVESTIGADO SOBRE PRODUCTO TENSORIAL, TENDRÉ QUE RETOCAR COSAS CON LAS BASES Y LAS PUERTAS PARA n QUBITS******

Puertas de varios qubits

Al igual que antes, sentimos la necesidad de aprender a manipular los qubits con las distintas puertas cuánticas. Ahora, es normal preguntarse si hay alguna manera de relacionar los qubits que componen el sistema, haciendo que el estado de unos afecten a lo que ocurre con otros.

En Computación Clásica, son conocidas puertas lógicas como AND, OR, XOR, NAND y NOR, que toman dos bits de entrada y devuelven uno de salida aplicando una cierta operación lógica sobre los valores que reciben. El prototipo de puerta cuántica para varios qubits es **CNOT** (o ***controlled*-NOT)**. Ésta se aplica sobre un par de qubits: uno de ellos, a, es el elemento de control, mientras que el otro, b, es el objetivo (o *target*). La puerta cambia el valor lógico de b sólamente cuando el qubit de control se encuentra en el estado básico $|1\rangle$. Por supuesto, esta puerta admite una representación tensorial como cualquier otra:

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad , \qquad \begin{array}{|c|c|c|} \hline \text{a} & \text{b} & \text{CNOT}|ab\rangle = |a\ b \oplus a\rangle \\ \hline 0 & 0 & |00\rangle \\ 0 & 1 & |01\rangle \\ 1 & 0 & |11\rangle \\ 1 & 1 & |10\rangle \\ \hline \end{array} \tag{3.14}$$

Esta puerta no es más que una generalización de la puerta XOR, que aplica la suma exclusiva (o suma modulo 2) de los bits que recibe. Sin embargo, no deja de ser un caso particular de toda una familia de puertas, las ***controlled-U***, que dejan invariante el qubit de control y aplican la puerta unitaria U sobre el *target* cuando el primero se halla en el estado $|1\rangle$:

$$U = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \qquad \Rightarrow \qquad CU \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x_1 & x_2 \\ 0 & 0 & x_3 & x_4 \end{pmatrix} \tag{3.15}$$

¿Y qué ocurre cuando haya que aplicar una **puerta sobre un sólo qubit**? Previamente, presentamos una serie de puertas cuánticas que estaban representadas por matrices de $\mathbb{C}^{2\times 2}$, adecuadas para alterar un solo qubit. Sin embargo, ahora los estados están representados por vectores de dimensión 2^n, de manera que estas matrices dejan de ser válidas. Será necesario recurrir a matrices, todavía unitarias, de $\mathbb{C}^{2^n\times 2^n}$.

Cada vez que queramos aplicar alguna puerta sobre algún qubit, hemos de aplicar el producto tensorial de n puertas, cada una sobre su correpondiente qubit. En caso de que queramos aplicar U sobre uno y solamente uno de los n qubits, digamos el j-ésimo, la operación consistirá en el producto tensorial de $n-1$ matrices identidad por la matriz U (esta última en la posición j). Para operar con más qubits, hacemos lo mismo, colocando matrices identidad en las posiciones correspondientes a los qubits que queramos dejar invariantes. Veamos un ejemplo:

Dado un sistema de $n = 3$ qubits y un estado $|\psi_3\rangle$ como el antes visto, queremos aplicar, a la vez, una puerta X sobre el primer qubit y una Hadamard sobre el tercer qubit. Llamaremos U al operador con el que modificamos el sistema completo (que será una matriz cuadrada de dimensión $2^3 = 8$), y escribiremos cada puerta acompañada de un subíndice denotando el qubit sobre el que actúan. U viene dada, entonces, por

$$U = X_1 \otimes I_2 \otimes H_3 = \left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right] \otimes H_3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\implies \quad U\left|\psi_3\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \\ \alpha_8 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha_4 + \alpha_5 \\ \alpha_4 - \alpha_5 \\ \alpha_7 + \alpha_8 \\ \alpha_7 - \alpha_8 \\ \alpha_1 + \alpha_2 \\ \alpha_1 - \alpha_2 \\ \alpha_3 + \alpha_4 \\ \alpha_3 - \alpha_4 \end{pmatrix}$$

Vemos que lo que hacen estas puertas, aunque no actúen sobre todos los qubits, es modificar las amplitudes (y por tanto las probabilidades) con las que se presentan cada uno de los vectores de la base.

3.3 Circuitos cuánticos

En las páginas que preceden, hemos descubierto los elementos que se emplean en Computación Cuántica con fines diversos (cálculo, simulaciones, etc.). Para utilizarlos, podemos integrarlos en un "circuito cuántico" como el que se representa en la siguiente figura:

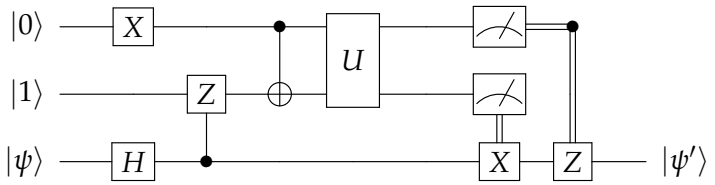


Figura 1: Ejemplo de circuito cuántico

Desgranemos su contenido:

A cada qubit del sistema le hacemos corresponder una línea horizontal, sobre la que se situarán las distintas acciones que pretendemos realizar sobre él. Los circuitos cuánticos se interpretan de izquierda a derecha y, leyendo según este orden, podemos distinguir tres fases diferenciadas:

1. La preparación de estados previa a la ejecución del circuito. A la izquierda de cada una de las líneas mencionadas, se indica el estado inicial del qubit correspondiente. Es habitual partir desde el estado básico $|00...00\rangle$, pero conviene indicarlo siempre.

2. El cuerpo del circuito, compuesto por todas las puertas lógicas que actúan sobre los qubits y las diferentes relaciones que se establecen entre ellos. Es en esta parte cuando el estado de los n qubits se ve alterado.

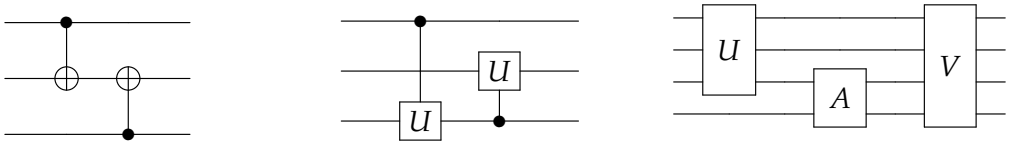
3. La salida que resulta del circuito. Aunque se parte conociendo el estado de n qubits, puede interesarnos un número menor de estados como output. Esto es lo que ocurre en la Figura 1, ya que solo obtenemos el estado final del tercer qubit, habiendo "perdido"los dos restantes.

Sigamos con esta exploración sobre los circuitos cuánticos pasando por las diferentes puertas cuánticas que podemos representar:

(a) Matrices de Pauli (b) Hadamard (c) Fase (d) Medida

Figura 2: Puertas cuánticas sobre un sólo qubit.

La puerta de medida merece especial atención, ya que aparece un elemento nuevo: un "cable clásico". Avanzamos en 3.2.2 que, ante la medida del qubit, éste colapsa sobre uno de los dos estados básicos, $|0\rangle$ o $|1\rangle$, y esta operación es la única irreversible entre todas las que podemos encontrar. Estos hechos fuerzan la necesidad de una forma alternativa de representar el canal por el que comunicamos el estado de dicho qubit. Así, la puerta de medida siempre irá seguida de una doble línea horizontal delatando este nuevo cable.



(a) Puertas CNOT (b) Puertas *controlled-U* (c) Puertas sobre varios qubits

Figura 3: Puertas cuánticas sobre varios qubits

En las puertas controladas se observa que hay una línea vertical uniendo las líneas correspondientes a los qubits que asocia. El punto negro se coloca sobre el cable correspondiente al qubit de control, mientras que el otro extremo es el *target*. La operación realizada por la puerta CNOT se representa por $\oplus$, aunque podríamos poner una puerta X en su lugar.

********** ¿MERECE LA PENA PONER UN EJEMPLO DE CIRCUITO CUÁNTICO CALCULANDO EL ESTADO FINAL? **********

3.4 El formalismo estabilizador

La comunicación de información, codificada en qubits, está sujeta a un ruido que puede alterar el estado de alguno de ellos, provocando que el mensaje de llegada difiera de aquel que envió el emisor. Para tratar de corregir estos posibles errores, existe multitud de códigos de detección y corrección de errores.

Dentro de estos códigos, podemos encontrar un tipo de gran relevancia, que va a suponer el centro en torno al cual gira este trabajo: los códigos estabilizadores. Detrás de ellos, se esconde todo un formalismo que encuentra en la teoría de grupos su principal apoyo.

3.4.1 El grupo estabilizador

Dado un estado puro $|\psi\rangle$, decimos que la matriz unitaria U estabiliza a $|\psi\rangle$ si $|\psi\rangle$ es un vector propio de U con valor propio 1, esto es, $U|\psi\rangle = |\psi\rangle$. Es claro que la matriz

identidad, I, estabiliza cualquier estado puro.

Obsérvese que si dos matrices U y V estabilizan un estado $|\psi\rangle$, también lo harán su producto y sus matrices inversas:

$$\left.\begin{array}{r} U|\psi\rangle = |\psi\rangle \\ V|\psi\rangle = |\psi\rangle \end{array}\right\} \quad \Rightarrow \quad UV|\psi\rangle = U(V|\psi\rangle) = U|\psi\rangle = |\psi\rangle$$

$$U|\psi\rangle = |\psi\rangle \quad \Rightarrow \quad |\psi\rangle = U^{-1}U|\psi\rangle = U^{-1}(U|\psi\rangle) = U^{-1}|\psi\rangle$$

En definitiva, el conjunto de las matrices que estabilizan un cierto estado puro $|\psi\rangle$ constituye un subgrupo dentro del grupo unitario $U_{\mathbb{C}}(2n)$, siendo n el número de qubits que componen el sistema. Lo llamaremos **grupo estabilizador** de $|\psi\rangle$ y lo notaremos $\text{Stab}(|\psi\rangle)$.[4]

La idea fundamental del formalismo estabilizador es abandonar la representación de un estado cuántico $|\psi\rangle$ a partir de un vector de amplitudes (como hemos estado haciendo hasta ahora), para pasar a representarlo a partir de su grupo estabilizador. Esto podría parecer poco práctico, puesto que se pasa de necesitar 2^n coeficientes, en el primer caso, a 2^{2n} para representar todas las matrices en el segundo. Sin embargo, vamos a ver que somos capaces de encontrar una representación mucho más compacta.

Es el momento de recordar las matrices de Pauli que conocimos en 3.9. Es sencillo comprobar que se cumplen las siguientes igualdades

$$\begin{array}{lll} X^2 = +I & Y^2 = +I & Z^2 = +I \\ XY = +iZ & YZ = +iX & ZX = +iY \\ YX = -iZ & ZY = -iX & XZ = -iY \end{array} \tag{3.16}$$

En particular, se tiene que las matrices de Pauli conmutan o anticonmutan dos a dos. A la vista de estas igualdades, resulta evidente que la identidad, junto con las matrices de Pauli, multiplicadas por $\{\pm 1, \pm i\}$, forman un subgrupo de $U_{\mathbb{C}}(2)$ (con el producto de matrices).

En caso de que tratemos con un sistema de n qubits, los operadores que se pueden formar a partir de ellas vienen dados por los diferentes productos tensoriales de n matrices de Pauli (o identidad) posibles. A estos operadores los llamaremos **operadores de Pauli sobre n qubits**. Por las propiedades del producto tensorial, se garantiza que cualquier producto de estos operadores da lugar a otro operador de Pauli. En definitiva, la identidad y los operadores de Pauli sobre n qubits, multiplicados por un factor de $\{\pm 1, \pm i\}$ también forman un grupo:

$$\mathcal{P}_n = \left\{ u \cdot \bigotimes_{i=1}^{n} P_i \;/\; u \in \{\pm 1, \pm i\} \;,\; P_i \in \{I, X, Y, Z\} \;\forall i \in \{1, ..., n\} \right\} \tag{3.17}$$

A este grupo lo llamaremos **Grupo de Pauli** sobre n qubits, que consta, claramente, de $|\mathcal{P}_n| = 4^{n+1}$ elementos. La ley de composición interna con la que se define este grupo no es otra que la composición de operadores, esto es, el producto de matrices unitarias de dimensión 2^n.

[4] Esta idea puede extenderse: dado un grupo de matrices G, se dice que G es el grupo estabilizador de un espacio V_G si todos los vectores de V_G quedan invariantes ante la acción de cualquiera de las matrices que contiene.

Después de estas definiciones, estamos en condiciones de presentar el siguiente teorema que nos aporta el grupo de operadores con el que vamos a trabajar:

Teorema 1. *Dado un estado $|\psi\rangle$ de n qubits, las siguientes afirmaciones son equivalentes:*

(i) *$|\psi\rangle$ se puede obtener a partir del estado $|0\rangle^{\otimes n}$ por medio de únicamente la acción de puertas CNOT, Hadamard y de fase.*

(ii) *$|\psi\rangle$ se puede obtener a partir del estado $|0\rangle^{\otimes n}$ por medio de únicamente la acción de puertas CNOT, Hadamard, de fase y de medida.*

(iii) *$|\psi\rangle$ es estabilizado por exactamente 2^n operadores de Pauli.*

(iv) *$|\psi\rangle$ queda completamente determinado por $S(|\psi\rangle) = Stab(|\psi\rangle) \bigcap \mathcal{P}_n$ (grupo de los operadores de Pauli que estabilizan a $|\psi\rangle$).*

Demostración. ***** POR HACER ***** □

En esto se resume, pues, la representación que tomaremos a partir de ahora: para hablar de un estado de n qubits, usaremos el grupo de 2^n matrices unitarias que lo estabilizan. Como un grupo G cualquiera tiene un sistema generador de tamaño $\log_2 |G|$ (DEMOSTRAR EN LA PARTE DE TEORÍA DE GRUPOS Y AÑADIR REFERENCIA), nos bastará con tener n operadores para describir $S(|\psi\rangle)$ por completo.

Veámoslo con un ejemplo para el caso $n = 3$: Tomando el estado $|011\rangle$, por ejemplo, es sencillo darse cuenta que el grupo que lo estabiliza es

$$S(|011\rangle) = \{I,\ Z_1,\ -Z_2,\ -Z_3,\ -Z_1Z_2,\ -Z_1Z_3,\ Z_2Z_3,\ Z_1Z_2Z_3\}$$

pero basta conocer únicamente tres de sus elementos, ya que el resto se pueden generar a partir de ellos: $S(|011\rangle) = \langle Z_1,\ -Z_2,\ -Z_3\rangle$.

Antes de continuar, prestemos atención a la notación que vamos a emplear a partir de ahora: se omitirán los símbolos de producto tensorial, $\otimes$ y se indicará a qué qubit está afectando la puerta que se escriba. Además, en caso de que sea la identidad la que está actuando sobre un qubit, también será omitida. Veamos algunos ejemplos para comparar y comprender mejor esta novedad:

$$Z_1 \equiv Z_1 \otimes I_2 \otimes I_3 \quad , \quad -Z_1Z_3 \equiv Z_1 \otimes I_2 \otimes (-Z_3) \quad , \quad I \equiv I_1 \otimes I_2 \otimes I_3$$

Como consecuencia del Teorema 1, llamamos **circuito estabilizador** a cualquier circuito compuesto por puertas CNOT, Hadamard, de fase y de medida. Llamaremos **estado estabilizador** a cualquier estado obtenido desde $|0\rangle^{\otimes n}$ por medio de un circuito estabilizador.

3.4.2 Puertas unitarias en el formalismo estabilizador

En el apartado anterior se develó una nueva forma de representar los sistemas formados por un cierto número n de qubits. El problema que se plantea con ello es la necesidad de adaptar todo lo que habíamos aprendido hasta ahora, ya que tanto la medida como las puertas cuánticas se habían diseñado para trabajar según las amplitudes que presentara cada uno de los vectores de la base.

Supongamos que se aplica una puerta unitaria U sobre el estado $|\psi\rangle$ que, recordemos, estará descrito por el grupo de matrices $S(|\psi\rangle) \equiv S$. Entonces, para cualquier elemento $g \in S$, se tiene

$$U|\psi\rangle = Ug|\psi\rangle = UgU^\dagger U|\psi\rangle \ , \tag{3.18}$$

de manera que el vector $U|\psi\rangle$ es estabilizado por la matriz $UgU^\dagger$, de donde se deduce que el grupo $USU^\dagger = \{UgU^\dagger / g \in S\}$ estabiliza el estado $U|\psi\rangle$. Es más, si $S = \langle g_1, g_2, ..., g_l\rangle$, se tiene que $Ug_1U^\dagger, ..., Ug_lU^\dagger$ generan $USU^\dagger$. Así, para conocer cómo afectan las puertas sobre el estabilizador, será suficiente averiguar cómo modifican a los generadores del estabilizador.

Veamos algunos ejemplos de las puertas unitarias que actúan sobre un sólo qubit. Por ejemplo, la puerta de Hadamard afecta a cada una de las matrices de Pauli como se muestra a continuación:

$$HXH^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = Z \tag{3.19}$$

$$HYH^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & 2i \\ -2i & 0 \end{pmatrix} = -Y \tag{3.20}$$

$$HZH^\dagger = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = X \tag{3.21}$$

Para ver el efecto de las puertas de fase, el procedimiento sería muy similar y para las puertas de Pauli, podemos utilizar las igualdades 3.16 simplificando los cálculos enormemente. Resumimos todos los resultados en la tabla 1.

Estos resultados son directamente aplicables al caso en que nuestro sistema esté formado por n qubits. Por ejemplo, el estado $|0\rangle^{\otimes n}$ tiene al grupo $\langle Z_1, ..., Z_n\rangle$ por estabilizador y si hacemos pasar cada uno de los qubits por una puerta Hadamard, el grupo estabilizador del sistema pasaría a ser $\langle X_1, ..., X_n\rangle$.

Avanzando hacia al caso en que la puerta unitaria U relaciona más de un qubit (digamos k), hemos de entender que la operación a realizar es $UAU^\dagger = B$, donde tanto A como B son matrices de dimensión 2^k resultado del producto vectorial de k matrices de Pauli. El ejemplo más obvio es el de la puerta *controlled*-NOT (que representaremos simplemente por U):

$$\begin{aligned} UX_1U^\dagger &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X_1 \otimes X_2 \end{aligned} \tag{3.22}$$

De igual manera, podríamos proceder con cualquiera de las matrices de Pauli o con cualquiera de las puertas unitarias sobre varios qubits que quisiéramos utilizar. En cualquier caso, por el Teorema 1, sabemos que dentro de este tipo sólo vamos a necesitar las puertas CNOT. De nuevo, el resto de resultados a considerar se encuentran recogidos en las tablas que presentamos a continuación:

Puerta	Entrada	Salida
X	X	X
	Y	$-Y$
	Z	$-Z$
Y	X	$-X$
	Y	Y
	Z	$-Z$
Z	X	$-X$
	Y	$-Y$
	Z	Z
H	X	Z
	Y	$-Y$
	Z	Z

Puerta	Entrada	Salida
P	X	Y
	Y	$-X$
	Z	Z
CNOT	X_1	X_1X_2
	X_2	X_2
	X_1X_2	X_1
	Y_1	Y_1X_2
	Y_2	Z_1Y_2
	Y_1Y_2	$-X_1Z_2$
	Z_1	Z_1
	Z_2	Z_1Z_2
	Z_1Z_2	Z_2

Tabla 1: Acción de puertas unitarias sobre las matrices de Pauli

******* CONVIENE QUE DEJE LAS PUERTAS X,Y,Z O LAS QUITO (DADO QUE NO SON PUERTAS DE LAS QUE VAMOS A UTILIZAR)??????? *********

Obsérvese que, en la tabla expuesta, hay información redundante: debido a las relaciones entre las matrices de Pauli (3.16), conociendo lo que ocurre con dos de ellas se puede calcular lo que ocurre con la tercera a partir de ello. En nuestro algoritmo, se empleará sólamente la información referente a las puertas X y Z sin que esto suponga pérdida alguna de información.

* REESCRIBIR COSAS EN TÉRMINOS DE NORMALIZADOR Y CENTRALIZADOR

3.4.3 La medida en el formalismo estabilizador

La última pieza del formalismo estabilizador que hemos de descubrir es la medida de un qubit, que también puede realizarse fácilmente. Pretendemos medir un operador $g \in \mathcal{P}_n$, suponiendo, sin pérdida de generalidad, que no va acompañado de factor multiplicativo $u \in \{-1, \pm i\}$. Como el sistema está en un estado $|\psi\rangle$ estabilizado por $S(|\psi\rangle) = \langle g_1, ...g_l\rangle$, pueden ocurrir dos cosas:

a. g conmuta con todos los generadores del estabilizador:

Como $g_j g |\psi\rangle = g g_j |\psi\rangle = g |\psi\rangle \ \forall j = 1, ..., n$, $g |\psi\rangle$ está también estabilizado por $S(|\psi\rangle)$ y es, por tanto, un múltiplo de $|\psi\rangle$. Como $g^2 = I$, forzosamente $g |\psi\rangle = \pm |\psi\rangle$, de modo que g o $-g$ es un elemento del estabilizador.

Si $g \in S(|\psi\rangle)$, se tiene que $g |\psi\rangle = |\psi\rangle$ y de ahí que al medir g se vaya a obtener el valor $+1$ con probabilidad 1. Además, como $|\psi\rangle$ ya se encuentra en el subespacio que proyecta g, la medida no alterará el estado del sistema, dejando el grupo estabilizador

invariante. Lo mismo ocurriría si fuera $-g$ el que está en el estabilizador, obteniéndose en este caso el valor -1.

En definitiva, si g conmuta con todos los generadores del estabilizador, su medida será un procedimiento determinista que no altera al grupo estabilizador.

b. g anticonmuta con uno o más generadores del estabilizador y conmuta con el resto:

Antes de nada, veamos que todo se reduce al caso en que g anticonmuta con sólo uno de los generadores del estabilizador: si g anticonmuta con dos generadores g_1 y g_2, por ejemplo, resulta que g conmuta con su producto $g_1 g_2$. Así, podemos sustituir uno de los dos generadores por el producto (que también es un elemento del grupo estabilizador), dejando sólo un generador que anticonmute con g. Podríamos repetir este paso las veces que hiciera falta según cuántos generadores anticonmutasen con g.

g tiene dos valores posibles que pueden resultar de su medida, ± 1, cuyos proyectores son $\frac{I \pm g}{2} |\psi\rangle\langle\psi|$, respectivamente. Por tanto, las probabilidades de medir cada uno de estos valores propios viene dada por:

$$p_{+1} = \mathrm{Tr}\left(\frac{I+g}{2} |\psi\rangle\langle\psi|\right) \qquad p_{-1} = \mathrm{Tr}\left(\frac{I-g}{2} |\psi\rangle\langle\psi|\right) \tag{3.23}$$

Y usando que $g_1 |\psi\rangle = |\psi\rangle$ y $g g_1 = -g_1 g$ llegamos a que

$$p_{+1} = \mathrm{Tr}\left(\frac{I+g}{2} g_1 |\psi\rangle\langle\psi|\right) = \mathrm{Tr}\left(g_1 \frac{I-g}{2} |\psi\rangle\langle\psi|\right) \tag{3.24}$$

Por último, empleamos que $\mathrm{Tr}(ABC) = \mathrm{Tr}(BCA)$ para llevar g_1 a la derecha de la expresión y absorberlo con $\langle\psi|$ (puesto que $g_1 = g_1^\dagger$). Con ello, deducimos que

$$p_{+1} = \mathrm{Tr}\left(\frac{I-g}{2} |\psi\rangle\langle\psi|\right) = p_{-1} \qquad \Rightarrow \qquad p_{+1} = p_{-1} = \frac{1}{2} \tag{3.25}$$

Concluimos, por tanto, que en este caso el resultado de la medida será aleatorio y que, una vez medido g obteniéndose ± 1, el estado colapsará convirtiéndose en $|\psi^\pm\rangle = \frac{I \pm g}{\sqrt{2}} |\psi\rangle$. Su grupo estabilizador pasará a ser $\langle \pm g, g_2, ..., g_n \rangle$

********** VOY A TENER QUE HABLAR TAMBIÉN SOBRE PUERTAS DE CLIFFORD Y LA FUNCIÓN DE WIGNER **********

4 Presentación del algoritmo

En esta sección, trataremos de explicar el algoritmo desarrollado por Gottesman y Aaronson [2] de forma detallada. Comenzaremos viendo que toda la representación del sistema gira en torno a una matriz simpléctica para tratar después el reto de actualizarla después de la acción de las distintas puertas cuánticas.

4.1 La matriz estabilizadora

Con el fin de que la matriz mencionada se comprenda de forma casi inmediata, hemos de pasar primero por una reformulación del grupo de Pauli, basada en un recurso al que llamaremos *etiquetas* [3].

Recordemos que un sistema de n qubits estaba asociado al espacio de Hilbert $\left(\mathbb{C}^2\right)^{\otimes n}$. Este espacio está asociado, de forma natural, al grupo $G = \mathbb{Z}_2^n$ (del que obtenemos los estados básicos), de dimensión $\mathfrak{g} = 2^n$, por medio de la relación:

$$|g\rangle = |g(1)\rangle \otimes ... \otimes |g(n)\rangle \qquad g \in G \tag{4.1}$$

donde $g = (g(1), ..., g(n))$ es un elemento del grupo. Teniendo esto en mente, podemos escribir las matrices de Pauli X y Z como los siguiente operadores que actúan sobre elementos de $\left(\mathbb{C}^2\right)^{\otimes n}$:

$$X(g) := \sum_{h \in G} |h + g\rangle\langle h| \qquad , \qquad Z(g) := \sum_{h \in G} \chi_g(h)\, |h\rangle\langle h| \tag{4.2}$$

donde $g \in G$ y $\chi_g : G \longrightarrow \{-1, +1\}$ es un homomorfismo definido por

$$\chi_g(h) = \exp\left(2\pi i \sum_{i=1}^{n} \frac{g(i)h(i)}{2}\right). \tag{4.3}$$

Con esta notación, las componentes $g(i) = 1$ se traducirán en que la puerta X o Z actúa sobre el qubit i, mientras que $g(j) = 0$ quiere decir que no se aplican, esto es, se halla la matriz identidad en su lugar. Tomemos, por ejemplo, el elemento $g = (0, 1) \in \mathbb{Z}_2^2$ para ver esta nomeclatura en acción:

$$\begin{aligned} X(0,1) &= |00+01\rangle\langle 00| + |01+01\rangle\langle 01| + |10+01\rangle\langle 10| + |11+01\rangle\langle 11| \\ &= |01\rangle\langle 00| + |00\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\ &= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I_1 \otimes X_2 \end{aligned}$$

$$\begin{aligned} Z(0,1) &= e^{i\pi\cdot 0}\,|00\rangle\langle 00| + e^{i\pi\cdot 1}\,|01\rangle\langle 01| + e^{i\pi\cdot 0}\,|10\rangle\langle 10| + e^{i\pi\cdot 1}\,|11\rangle\langle 11| \\ &= +\,|00\rangle\langle 00| - |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = I_1 \otimes Z_2 \end{aligned}$$

De esto, se deduce que cualquier operador de Pauli podrá reescribirse de la siguiente forma

$$T_a = i^{-a_x \cdot a_z} X(a_x) Z(a_z) \ , \qquad a_x, a_z \in \mathbb{Z}_2^n \tag{4.4}$$

o lo que es lo mismo:

$$T_a = i^{-a_x \cdot a_z} \left(X_1^{a_{x_1}} \otimes ... \otimes X_n^{a_{x_n}} \right) \left(Z_1^{a_{z_1}} \otimes ... \otimes Z_n^{a_{Z_n}} \right) \ , \qquad a_x, a_z \in \mathbb{Z}_2^n \tag{4.5}$$

Notaremos $a \equiv (a_x, a_z) \in \mathbb{Z}_2^{2n}$ al vector de etiquetas que determina de forma única al correspondiente operador de Pauli.

Una vez hemos asimilado esta escritura de los operadores de Pauli por medio de etiquetas, podemos presentar el ente matemático con el que vamos a representar el sistema de n qubits y que haremos evolucionar a conveniencia. Ante la falta de convenio en la bibliografía para apodarlo (*check matrix* en [1] o *tableau* en [2]), el nombre **matriz estabilizadora** será suficientemente representativo.

La idea es utilizar dicha matriz para representar los distintos generadores del grupo $S(|\psi\rangle)$. Para el caso en que tengamos n qubits, ya sabemos que es suficiente con n generadores para que el grupo quede completamente representado. Consideraremos también otros n generadores del "destabilizador", esto es, operadores que no forman parte del estabilizador pero que, junto con él, generan el grupo de Pauli completo. Así, tenemos $2n$ generadores, $R_i = \pm P_1 ... P_n$ (******** ¿LO SELECCIONAMOS NOSOTROS CON ESA FORMA O LA i DESAPARECE POR ALGÚN MOTIVO?*********), cada uno de los cuales se corresponderá con una de las filas de nuestra matriz estabilizadora.

El algoritmo representa un estado por la matriz de variables binarias x_{ij}, z_{ij}, r_{ij} para cada $i, j \in \{1, ..., 2n\}$:

$$\begin{array}{ccc}
R_1 & \to & \left(\begin{array}{ccc|ccc|c}
x_{11} & \dots & x_{1n} & z_{11} & \dots & z_{1n} & r_1 \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{n1} & \dots & x_{nn} & z_{n1} & \dots & z_{nn} & r_n \\
\hline
x_{(n+1)1} & \dots & x_{(n+1)n} & z_{(n+1)1} & \dots & z_{(n+1)n} & r_{n+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
x_{(2n)1} & \dots & x_{(2n)n} & z_{(2n)1} & \dots & z_{(2n)n} & r_{2n}
\end{array}\right) \\
\vdots & & \\
R_n & \to & \\
R_{n+1} & \to & \\
\vdots & & \\
R_{2n} & \to &
\end{array} \tag{4.6}$$

Los elementos destabilizadores están representados por las filas $\{1, ..., n\}$ mientras que los generadores del grupo estabilizador se corresponderán con las filas $\{n+1, ..., 2n\}$. Las $2n$ primeras entradas en cada fila serán la etiqueta del operador de Pauli correspondiente, mientras que r_i denota la fase que lo acompaña: $r_i = 0$ para fases positivas y $r_i = 1$ para fases negativas.

4.2 Algoritmo de simulación

Antes de hablar sobre el algoritmo, necesitamos ver cómo implementaremos la operación dentro del grupo de Pauli que, recordemos, es la composición de operadores (o producto de matrices de dimensión 2^n). La denotaremos por el símbolo $+$, para evitar confusiones. A continuación, se define la subrutina encargada de computar la recién mencionada operación:

rowsum(h,i) Esta subrutina toma las filas h e i de la matriz estabilizadora (generadores R_h y R_i) y reescribe sobre la fila h, transformándola en el generador $R_i + R_h$.

Lo primero que hace es ver qué ocurre con la fase del nuevo generador. Para ello, definimos la función $g : \mathbb{Z}_2^4 \longrightarrow \{-1, 0, +1\}$, que acepta como parámetros las etiquetas (x_1, z_1, x_2, z_2) correspondiente a dos matrices de Pauli y devuelve un coeficiente r tal que i^r es la fase resultante cuando dichas matrices han sido multiplicadas. Es sencillo comprobar que la forma explícita de esta función será:

$$g(x_1, z_1, x_2, z_2) = \begin{cases} 0 & \text{si } (x_1, z_1) = (0,0) \\ x_2(1 - 2z_2) & \text{si } (x_1, z_1) = (0,1) \\ z_2(2x_2 - 1) & \text{si } (x_1, z_1) = (1,0) \\ z_2 - x_2 & \text{si } (x_1, z_1) = (1,1) \end{cases} \tag{4.7}$$

Gracias a ella, seremos ahora capaces de establecer cuál es el nuevo valor para r_h. Nos fijamos en el valor de la siguiente expresión, en la que se reúnen las aportaciones de las fases de cada uno de los generadores y las que ofrecen los n productos de matrices de Pauli que se van a llevar a cabo:

$$d = 2r_h + 2r_i + \sum_{j=1}^{n} g(x_{ij}, z_{ij}, x_{hj}, z_{hj})$$

Entonces, asignaremos $r_h := 0$ si $d \equiv 0 \pmod 4$ y $r_h := 1$ cuando $d \equiv 2 \pmod 4$ (nunca se dará el caso en que d sea congruente a 1 o 3).

Ahora que ya tenemos la fase, podemos modificar las etiquetas que denotan al generador R_h. Esta etapa es más sencilla, simplemente tenemos que ejecutar $x_{hj} := x_{ij} \oplus x_{hj}$ $z_{hj} := z_{ij} \oplus z_{hj}$ para cada columna $j \in \{1, ..., n\}$, donde la operación $\oplus$ no es más que la suma módulo 2.

4.2.1 Representación de estados puro

Llegamos al tan esperado algoritmo para simular circuitos cuánticos. Comenzamos ilustrando el caso en que lo que hacemos evolucionar es un estado puro, para generalizarlo posteriormente al caso de estados mezcla.

El estado de partida será $|0\rangle^{\otimes n}$, de manera que $S\left(|0\rangle^{\otimes n}\right) = \langle Z_1, ..., Z_n \rangle$. Por tanto, añadiendo una fila auxiliar R_{2n+1} a la matriz (su utilidad se verá más tarde), su configuración inicial vendrá dada por $r_i = 0$ para todo $i \in \{1, .., 2n+1\}$ y $x_{ij} = \delta_{ij}$, $z_{ij} = \delta_{(i-n)j}$, $\forall i \in \{1, ..., 2n+1\}$ $\forall j \in \{1, ..., n\}$. Por ejemplo, si $n = 2$ la matriz estabilizadora en el instante inicial adoptará la forma

$$\left(\begin{array}{cc|cc|c} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Durante la simulación, modificaremos el estado del sistema por medio de puertas cuánticas. ¿Cómo interpretará el algoritmo la acción de cada una de ellas?

- **CNOT sobre b controlado por a:** Para cada fila $i \in \{1,...,2n\}$, se tienen $r_i := r_i \oplus x_{ia}z_{ib}(x_{ib} \oplus z_{ia} \oplus 1)$ y $x_{ib} := x_{ib} \oplus x_{ia}$, $z_{ia} := z_{ia} \oplus z_{ib}$.
- **Hadamard sobre el qubit a:** Para todo $i \in \{1,...,2n\}$, asignamos $r_i := r_i \oplus x_{ia}z_{ia}$ e intercambiamos x_{ia} y z_{ia}.
- **Puerta de fase sobre el qubit a:** Cambiaremos $r_i := r_i \oplus x_{ia}z_{ia}$ y $z_{ia} := z_{ia} \oplus x_{ia}$ para todas las filas $i \in \{1,...,2n\}$.

Representando las distintas situaciones con los operadores correspondientes, es sencillo comprobar que estas acciones se corresponden a la perfección con lo que recogimos en la tabla 1.

Lo que tiene más enjundia de este algoritmo es el proceso de medida, cuya esencia son las consideraciones que expusimos en 3.4.3. Comentaremos primero lo que hace el algoritmo y, seguido de ello, daremos la justificación teórica:

Medida del qubit a en la base canónica: Comprobamos si hay algún índice $p \in \{n+1,...,2n\}$ tal que $x_{pa} = 1$. Se abre la puerta a dos posibilidades distintas:

Caso 1 : tal p existe. En caso de haber más de uno, tomaremos el mínimo de ellos.

La medida será aleatoria, así que el estado requiere ser actualizado. Para tal fin, llamamos a rowsum(i,p) para todas las filas $i \in \{1,...,2n\}$ tales que $i \neq p$ y $x_{ia} = 1$. Tras ello, guardamos la fila R_p en la R_{p-n} y llenamos R_p de ceros, excepto r_p (que tomará los valores 0 o 1 con igual probabilidad) y $z_{pa} = 1$. Por último, devolvemos el valor r_p como resultado de la medida.

Caso 2 : no existe tal p.

Ahora la salida será determinista, así que la medida no alterará el estado. Sólo tenemos que ver si se observa 0 o 1. Para ello, rellenamos de ceros la fila R_{n+1} completa y sobre ella, sumamos con rowsum$(2n+1, i+n)$ todas las filas R_{i+n} con $i \in \{1,...,n\}$ tales que $x_{ia} = 1$. Finalizamos devolviendo r_{2n+1} como salida de la medida.

Todo lo anterior parece muy abstracto, pero vamos a ver cómo todo cobra sentido después de varias apreciaciones:

1. Empezamos por definir el producto simpléctico pertinente para trabajar en estas situaciones. Recordando la definición 2, se entiende que, considerando dos filas de la matriz como $R_i \equiv (x_i, z_i) \in \mathbb{Z}_2^{2n}$, el producto simpléctico de generadores se define como

$$(R_h|R_i) = z_h \cdot x_i - z_i \cdot x_h \pmod 2 = \bigoplus_{j=1}^{n} (x_{ij}z_{hj} \oplus x_{hj}z_{ij}) \tag{4.8}$$

De esta definición se deduce un resultado importante:

Lema 1. *Sean R_h y R_i dos generadores de la matriz estabilizadora. Entonces R_h conmuta con R_i si $(R_h|R_i) = 0$, y anticonmuta con él si $(R_h|R_i) = 1$.*

Demostración. Sean dos operadores de Pauli $P = i^k P_1...P_n$ y $Q = i^l Q_1...Q_n$ (donde P_i y Q_i son matrices de Pauli). Es claro que $[P,Q] = 0$ si y solo si el número de índices tales que

$\{P_j, Q_j\} = 0$ es par. De forma análoga, $\{P, Q\} = 0$ si y solo si dicho número de índices es impar.

Por otro lado, con una tabla en la que se consideren todas las posibles combinaciones (********* HE HECHO LA TABLA PARA COMPROBARLO, ¿LO PONGO AQUÍ O EN UN ANEXO?**********), es sencillo demostrar que para un índice arbitrario $j \in \{1, ..., n\}$, $[P_j, Q_j] = 0$ si y solo $x_{qj}z_{pj} \oplus x_{pj}z_{qj} = 0$, y $\{P_j, Q_j\} = 0$ si y solo si $x_{qj}z_{pj} \oplus x_{pj}z_{qj} = 1$.

Supongamos que $(R_h|R_i) = 0$, esto es, $\bigoplus_{j=1}^{n}(x_{hj}z_{ij} \oplus x_{ij}z_{hj}) = 0$. Tenemos entonces que el número de sumandos $(x_{hj}z_{ij} \oplus x_{ij}z_{hj})$ que no se anulan es par (ya que reduciendo módulo 2 se anula). Por lo visto en el párrafo anterior, esto equivale a que el número de parejas $\left((R_h)_j, (R_i)_j\right)$ que anticonmutan es par. Por lo mencionado al comienzo de la demostración, esto equivale, a su vez, a la primera afirmación del lema.

Supongamos ahora que $(R_h|R_i) = 1$ y, de forma análoga a lo anterior, deducimos que el número de sumandos $(x_{hj}z_{ij} \oplus x_{ij}z_{hj})$ que resultan 1 ha de ser impar (para que no se anule reduciendo módulo 2). Por tanto, el número de parejas $\left((R_h)_j, (R_i)_j\right)$ que anticonmutan es impar, lo que equivale a que R_h y R_i anticonmuten. □

2. Recogemos las relaciones enre los distintos generadores de la matriz en la siguiente

Proposición 2. *Las siguientes afirmaciones sobre la matriz estabilizadora se cumplen siempre:*

(i) $R_{n+1}, ..., R_{2n}$ *generan* $S(|\psi\rangle)$, *y* $R_1, ..., R_{2n}$ *generan* $\mathcal{P}_n$.

(ii) Los generadores $R_1, ..., R_n$ *conmutan entre ellos.*

(iii) $\forall h \in \{1, ..., n\}$, R_h *anticonmuta con* R_{h+n}.

(iv) Para todos $i, h \in \{1, ..., n\}$ *tales que* $i \neq h$, R_i *conmuta con* R_{h+n}.

Demostración. *** POR HACER *** □

3. Medir el qubit a en la base canónica equivale a medir la puerta Z_a:

Volvamos a la notación 4.2. Denotando $e_i \in \mathbb{Z}_2^n$ al elemento de G que tiene un 0 en todas sus coordenadas salvo en la posición i, $Z(e_i)$ sería el operador que deja invariantes todos los qubits, salvo el i-ésimo, sobre el que se aplica la puerta Z. La matriz Z tiene dos valores propios diferentes, cada uno de ellos asociado a un proyector $|x\rangle\langle x|$, $x \in \mathbb{Z}_2$, de rango 1. Se sigue entonces que la medida de $Z(e_i) \equiv Z_i$ corresponde a la medida del i-ésimo qubit en la base canónica.

4. Supongamos que la medida del qubit a da lugar a una salida determinista. Esto es lo que ocurría en el caso en que el operador medido conmutaba con todos los generadores del estabilizador y, por tanto, pertenecía a él. Existe entonces una elección (única) de coeficientes $c_1, ..., c_n \in \{0, 1\}$ tales que

$$\sum_{h=1}^{n} c_h R_{h+n} = \pm Z_a. \tag{4.9}$$

Nos proponemos averiguar el valor de los coeficientes, ya que sumando los R_{h+n} adecuados, podremos saber si la fase del output es positiva o negativa. Obsérvese que, para todo $i \in \{1, ..., n\}$,

$$c_i \overset{\underset{P2}{L1}}{=} \sum_{h=1}^{n} c_h(R_i|R_{h+n}) = \left(R_i \middle| \sum_{h=1}^{n} c_h R_{h+n}\right) = (R_i|Z_a) \tag{4.10}$$

Así, comprobando si R_i anticonmuta con Z_a (cosa que ocurrirá si y solo si $x_{ia} = 1$, puesto que esto denotará que R_i tiene una matriz X o Y en la posición a), podemos saber si $c_i = 1$ y, por tanto, si rowsum$(2n+1, i+n)$ ha de ser llamada.

Ya disponemos de todos los ingredientes necesarios para comprender lo que hacemos al medir el qubit a, es decir, al medir el operador Z_a:

Caso 1. Al tomar un $p \in \{n+1, ..., 2n\}$ tal que $x_{pa} = 1$, estamos seleccionando un generador del estabilizador, R_p, que anticonmuta con Z_a. Al sumar este generador con el resto de estabilizadores que también anticonmutan con Z_a (los que cumplen $x_{ia} = 1$), estamos convirtiéndolos en generadores que sí conmuten con Z_a. Llevamos, finalmente, el generador R_p, que anticonmuta, al destabilizador (posición $p - n$) y registramos Z_a como el generador R_p del estabilizador. En el estabilizador quedan, por tanto, n generadores que conmutan todos entre sí.

Caso 2. Al no tener ningún $x_{pa} = 0$, Z_a conmuta con todos los generadores del estabilizador y, de ahí, $+Z_a$ o $-Z_a$ pertenece a él (aunque no tiene por qué ser necesariamente unos de los generadores). Tras ello, sumamos aquellos generadores del estabilizadores correspondientes a los generadores del destabilizador que anticonmutan con Z_a. Con ello, estamos computando la suma 4.9 de aquellos términos con $c_h = 1$, de manera que sabiendo el signo de la fase en el primer miembro de la igualdad, seremos conocedores del signo que aparece en el segundo miembro: un signo $+$ significará que la salida es el estado $|0\rangle$ y $-$ dará a entender que el output es $|1\rangle$.

4.2.2 Representación de estados mezcla

Si recordamos lo visto en 3.1.1, la matriz densidad supone una generalización de los estados puros. En este apartado, buscamos adaptar el algoritmo para un cierto tipo de estados mezcla: los **estados mezcla estabilizadores**, es decir, estados concebidos como una distribución uniforme sobre todos los estados que se encuentran en un subespacio estabilizado por un grupo descrito a partir de $r < n$ generadores.

Será necesario conocer la forma en que se escribe la matriz densidad de un estado mezcla en términos de su estabilizador. Si M es un operador de Pauli, $\frac{I+M}{2}$ resulta ser el proyector sobre el espacio propio de M asociado al autovalor $+1$. Por tanto, la matriz densidad que representa a un estado mezcla estabilizador (estando su estabilizador generado por lo operadores $M_1, ..., M_r$) vendrá dada por [5]

$$\rho = \frac{1}{2^r} \bigotimes_{i=1}^{r} (I + M_i) \tag{4.11}$$

Para llevar a cabo nuestra simulación, situamos los r generadores del estabilizador en las filas $n+1, ..., n+r$ y sus correspondientes generadores destabilizadores como las filas $1, ..., r$. Las $2(n-r)$ filas restante se rellenan con una colección de operadores $\overline{X_i}$ y $\overline{Z_i}$, que conmutan tanto con el estabilizador como con el destabilizador. Elegimos

[5] Conocido el resultado de la proposición 1, es sencillo ver que se cumple que $\mathrm{Tr}(\rho) = 1$. Además, ρ es un operador autoadjunto por serlo las matrices de Pauli, y de ahí, cada $I + M_i$.

estos operadores de forma que cumplan las siguientes relaciones de conmutatividad: $[\overline{X_i}, \overline{X_j}] = [\overline{Z_i}, \overline{Z_j}] = [\overline{X_i}, \overline{Z_j}] = 0$ si $i \neq j$, y $\{\overline{X_i}, \overline{Z_i}\} = 0$. Colocaremos $\overline{X_i}$ en las filas $r+i$ y $\overline{Z_i}$ en las fils $n+r+i$, para todo $i \in \{1, ..., n-r\}$.

Se empezará la simulación desde el estado mezcla inicial $|0...0\rangle\langle 0...0| \otimes I$ (0 en los $n-r$ primeros qubits y el estado completamente mezclado en los últimos r qubits). En tal caso, se eligen los operadores $\overline{X_i} = X_{i+r}$ y $\overline{Z_i} = Z_{i+r}$. Notaremos $\bar{i} = i - n$ si $i \geq n+1$ e $\bar{i} = i + n$ si $i \leq n$. En tal caso, la proposición 2 se traducirá en que las filas R_i y R_j conmutarán a no ser que $i = \bar{j}$, en cuyo caso anticonmutarán.

Pasemos a estudiar el algoritmo en esta situación algo más compleja. Con respecto a la acción de puertas unitarias, podemos decir que se mantiene todo lo dicho anteriormente para los estados puros. Lo que sí cambia es la *medida* de un qubit a, que resulta algo más difícil, apareciendo ahora tres casos distintos:

Caso I: $x_{pa} = 1$ para algún $p \in \{n+1, ..., n+r\}$.

Lo que ocurre es que Z_a anticonmuta con (al menos) un elemento del estabilizador, de forma que la medida es aleatoria. Actualizamos el estado de igual forma que en el Caso I de estados puros.

Caso II: $x_p a = 0$ en todas las filas $p > r$.

Ahora Z_a conmuta con todo el estabilizador y es, de hecho, un elemento suyo. El output de la medida tendrá un resultado determinista, que averiguamos como hicimos en el Caso II para estados puros, sumando todas las filas que anticonmutan con Z_a.

Caso III: $x_{pa} = 0$ para todo $p \in \{n+1, ..., n+r\}$, pero $x_{ma} = 1$ para algún $m \in \{n+r+1, ..., 2n\}$.

Ahora Z_a conmuta con todos los generadores del estabilizador, pero no forma parte de él. La medida da lugar a un resultado aleatorio, pero la forma de actulizar el estado del sistema difiera respecto a lo que hacemos en el Caso I:

R_m anticonmuta con Z_a y por ello, tomará el papel de R_p en el Caso I: guardamos la fila R_m en la fila $R_{\overline{m}}$ y asignamos a la fila m las etiquetas correspondientes a Z_a, dejando el valor de la fase r_m en manos del azar. Una vez hemos hecho esto, intercambiamos las filas R_{n+r+1} y R_m, y también las filas R_{r+1} y R_m. Por último, incrementamos el número r a $r+1$: el estabilizador ha ganado un nuevo generador, $R_{n+r+1} \equiv Z_a$, y el correspondiente destabilizador R_{r+1} (el antiguo R_m) anticonmuta con él.

Es evidente que el número de medidas que podemos hacer está limitado, ya que a partir de la $(n-r)$-ésima medida, el estabilizador ya tendría los n generadores que le permitimos tener como máximo.

* QUIERO EXPLICAR EL STATE UPDATE EN TÉRMINOS DEL CENTRALIZADOR

Estudiando el algoritmo, nos damos cuenta de que está diseñado para que se verifiquen continuamente las condiciones que da la proposición 2, ya que es esto lo que garantiza que el tanto el grupo estabilizador como el grupo de Pauli estén correctamente generados por las correspondiente filas de la matriz.

5 Mejoras de eficiencia en el algoritmo

6 Interpretación de resultados. Implicaciones en Computación Cuántica

7 Conclusiones

8 Agradecimientos

Referencias

[1] N. Nielsen, I.L. Chuang,
Quantum Computation and Quantum Information, Cambridge U. P., Cambridge, 2010

[2] S. Aaronson, D. Gottesman,
Improved Simulation of Stabilizer Circuits, Phys. Rev. A 70, 052328 (2004),
quant-ph/0406196

[3] J. Bermejo-Vega, M. Van der Nest,
Classical simulations of Abelian-group normalizer circuits with intermediate measurements, Quantum Information & Computation, Volume 14 Issue 3-4,
March 2014, 1210.3637

[4] M.A. de Gosson,
Symplectic methods in Harmonic Analysis and in Mathematical Physics.
26 Birkhauser, Basel 2011.

[5] N. Zettili,
Quantum Mechanics: Concepts and Applications (2nd Revised ed.), Wiley, 2009

[6] J. Sakurai, J. Napolitano,
Modern quantum mechanics (2nd ed.). Addison Wesley, 2011