Estructuras algebraicas en Computación Cuántica:

estudio de algoritmos clásicos de simulación de circuitos cuánticos de Clifford

José Alberto Azorín Puche

21 de julio de 2021

Computación... ¿cuántica?

Computación Cuántica e Información Cuántica:[1]
estudio de tareas de procesamiento de la información mediante el uso de sistemas cuánticos (átomos, moléculas, etc.).

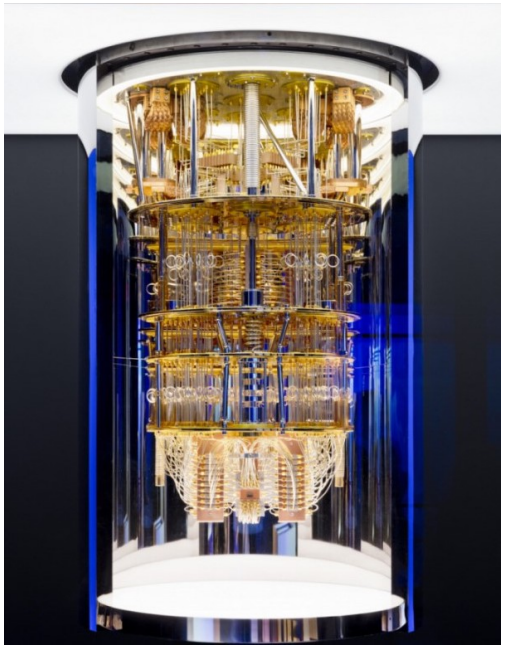


Figura: IBM Q

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

Simulación clásica

Aplicaciones:

- Depuración de ordenadores cuánticos.
- Simulación clásica de sistemas cuánticos.
- Construcción de potentes ordenadores híbridos.
- Importancia de recursos cuánticos en computación cuántica.

Teorema de Gottesman-Knill

Sea un circuito cuántico constituido únicamente por puertas de Clifford y medidas dentro del grupo de Pauli, siendo la preparación uno de los estados básicos del sistema. Dicho circuito puede simularse de forma eficiente en un ordenador clásico.

El qubit: la unidad básica de información

$$\begin{array}{c}\text{Bit clásico}\\ b \in \{0,1\} \cong \mathbb{Z}_2\end{array} \quad \Longrightarrow \quad \begin{array}{c}\text{Bit cuántico (qubit)}\\ |\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \in \mathbb{C}^2\end{array}$$

- Sistema de n qubits:

$$\mathcal{H}^{(n)} = \bigotimes_{i=1}^{n} \mathcal{H}^{(1)} = \left(\mathbb{C}^2\right)^{\otimes n} \qquad \Rightarrow \qquad \mathcal{H}^{(n)} = \mathbb{C}^{2^n}$$

$$\mathcal{B}_n = \left\{ \bigotimes_{i=1}^{n} q_i \mid q_i \in \mathcal{B}_1 \right\} \equiv \{ |x_1 \ldots x_n\rangle \mid x_i = 0,1 \}$$

$$\Downarrow$$

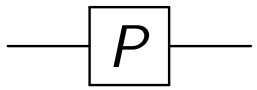
$$|\psi\rangle = \alpha_0 |0\ldots000\rangle + \alpha_1 |0\ldots001\rangle + \alpha_2 |0\ldots010\rangle + \cdots + \alpha_{2^n-2} |1\ldots110\rangle + \alpha_{2^n-1} |1\ldots111\rangle$$

Puertas cuánticas sobre un qubit

Matrices unitarias de dimensión 2.
¡Son operaciones reversibles!

- Puerta de fase

$$P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$



- Puerta Hadamard

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

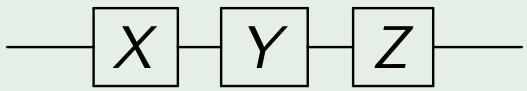
$$H|0\rangle = |+\rangle \qquad H|+\rangle = |0\rangle$$
$$H|1\rangle = |-\rangle \qquad H|-\rangle = |1\rangle$$

Matrices de Pauli

$$X \equiv \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

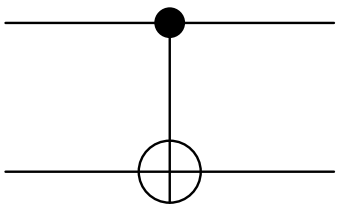
$$Y \equiv \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z \equiv \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$



Más puertas cuánticas

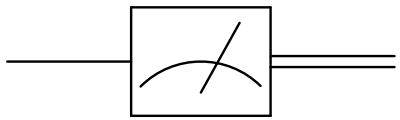
- Puerta cNOT (*controlled-X*):



a	b	cNOT$\|ab\rangle = \|a\ b \oplus a\rangle$
0	0	$\|00\rangle$
0	1	$\|01\rangle$
1	0	$\|11\rangle$
1	1	$\|10\rangle$

- "Puerta" de medida:

$$Z = (+1)\,|0\rangle\langle 0| + (-1)\,|1\rangle\langle 1|$$



El grupo estabilizador

Dados G grupo y X conjunto, llamamos **estabilizador** de $x \in X$ en G a

$$\mathrm{Stab}(x) = \{g \in G \,|\, ac(g, x) = x\}.$$

Grupo de Pauli

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

Grupo estabilizador de un estado $|\psi\rangle$

$$\mathcal{S}\left(|\psi\rangle\right) = \{T \in \mathcal{P}_n \,|\, T\,|\psi\rangle = |\psi\rangle\} \equiv \mathcal{S}$$

2^n elementos $\Rightarrow$ n generadores

Código estabilizador asociado a un grupo G

$$\mathcal{V} := \{|\psi\rangle : \sigma\,|\psi\rangle = |\psi\rangle \;\; \forall \sigma \in G\}$$

Aplicación de puertas cuánticas

$$U|\psi\rangle = UT|\psi\rangle = UTU^\dagger U|\psi\rangle \ , \ \forall T \in \mathcal{S}$$

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	X

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

Puertas de Clifford

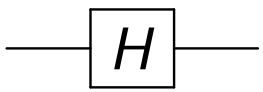
$$\mathcal{S}\left(|\psi\rangle\right) = \mathcal{S} \quad \Longrightarrow \quad U|\psi\rangle = UT|\psi\rangle = UTU^{\dagger}U|\psi\rangle \ , \ \forall T \in \mathcal{S}.$$

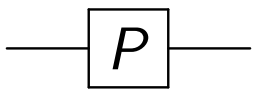
- Dados G grupo y A conjunto, se define el **normalizador de A en G** como

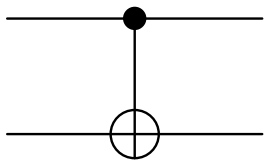
$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

Grupo de Clifford

$$N_{\mathcal{U}_n}(\mathcal{P}_n) = \{U \in \mathcal{U}_n \mid UTU^{-1} \in \mathcal{P}_n \, , \, \forall T \in \mathcal{P}_n\}$$







QEC. Código de inversión del qubit

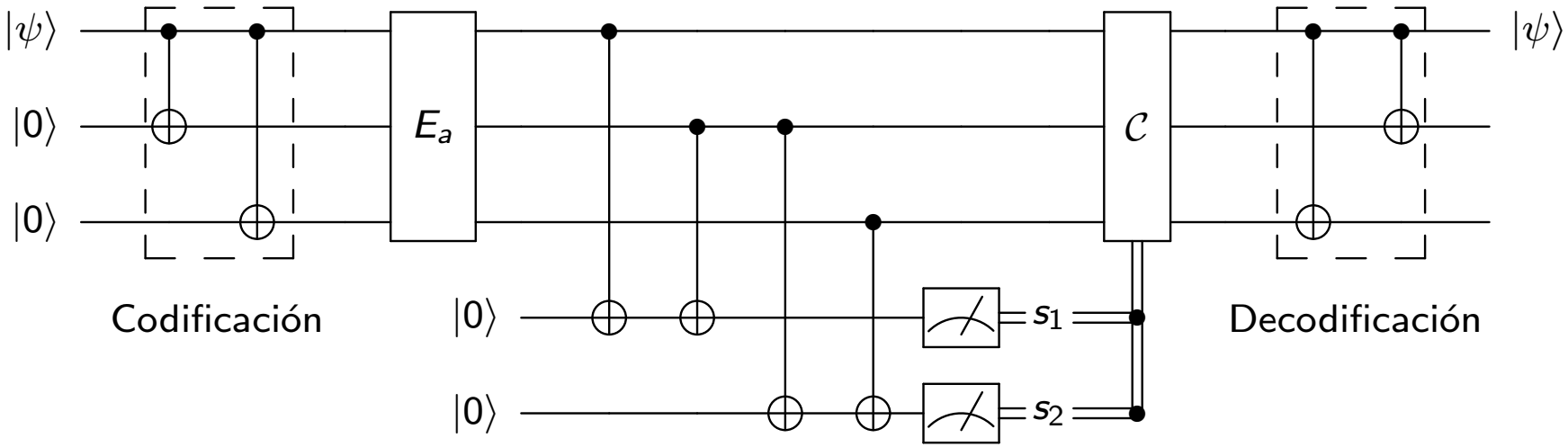
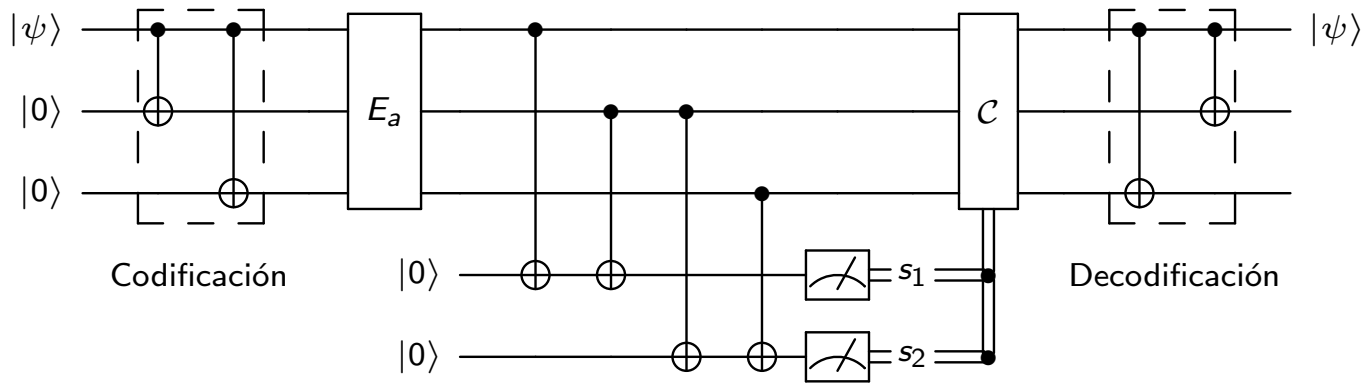


Figura: Circuito de corrección del error "invertir un qubit".

QEC. Código de inversión del qubit

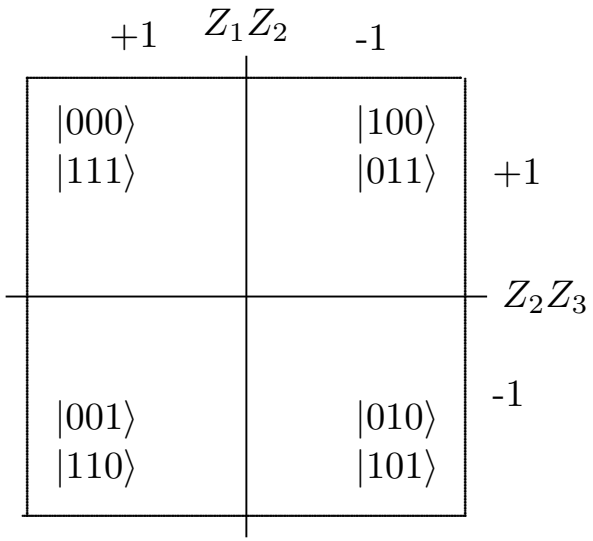


Codificación

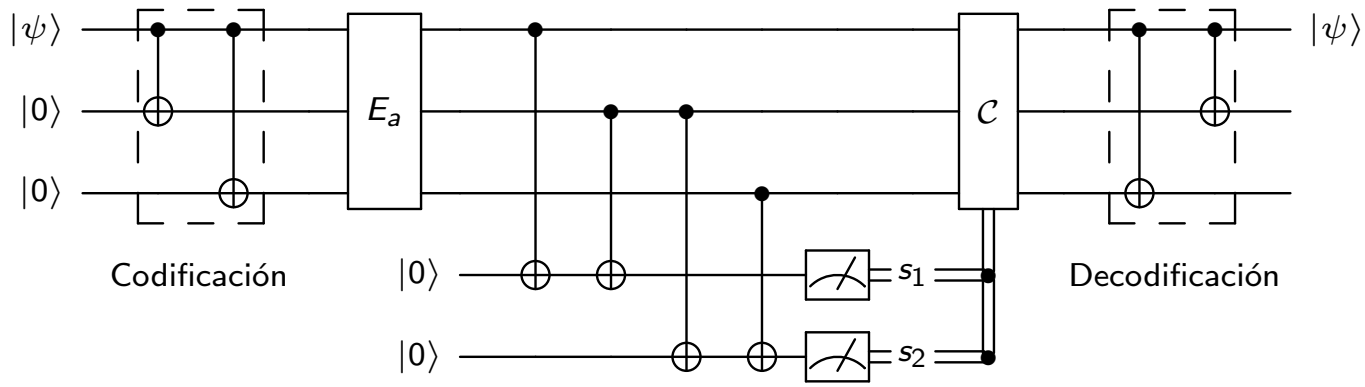
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$|\psi\rangle_c = \alpha\,|000\rangle + \beta\,|111\rangle$$

$$\mathcal{S} = \langle Z_1Z_2, Z_2Z_3\rangle$$



QEC. Código de inversión del qubit

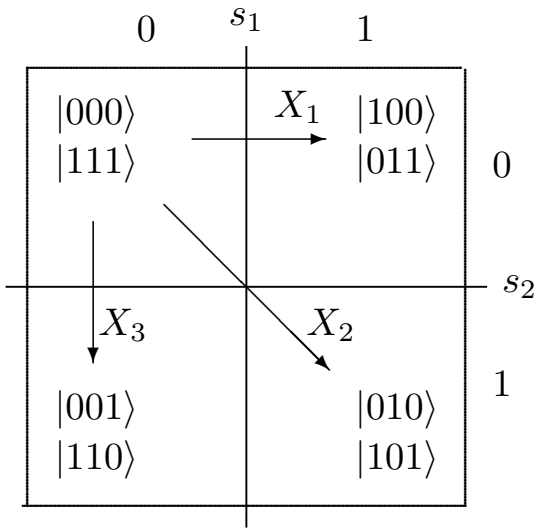


Codificación

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

$$|\psi\rangle_c = \alpha\,|000\rangle + \beta\,|111\rangle$$

$$\mathcal{S} = \langle Z_1Z_2, Z_2Z_3\rangle$$



La matriz estabilizadora

- Las matrices de Pauli conmutan/anticonmutan

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

- **Etiquetas:** vectores $(x_a, z_a) \in \mathbb{Z}_2^{2n}$ tales que

$$T_a = i^{-x_a \cdot z_a} \left(X_1^{x_{a1}} \otimes \ldots \otimes X_n^{x_{an}}\right)\left(Z_1^{z_{a1}} \otimes \ldots \otimes Z_n^{z_{an}}\right) \ , \quad x_a, z_a \in \mathbb{Z}_2^n$$

$$\begin{array}{ccc} T_1 & \rightarrow & \left(\begin{array}{ccc|ccc} x_{11} & \ldots & x_{1n} & z_{11} & \ldots & z_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ x_{n1} & \ldots & x_{nn} & z_{n1} & \ldots & z_{nn} \end{array}\right) \\ \vdots & & \\ T_n & \rightarrow & \end{array}$$

Puertas cuánticas en el algoritmo

$$U|\psi\rangle = UT|\psi\rangle = UTU^{\dagger}U|\psi\rangle \ , \ \forall T \in \mathcal{S}$$

Puerta	Entrada	Salida
H	X	Z
	Z	X
P	X	Y
	Z	Z
cNOT	X_1	X_1X_2
	X_2	X_2
	X_1X_2	X_1
	Z_1	Z_1
	Z_2	Z_1Z_2
	Z_1Z_2	Z_2

La medida en el formalismo estabilizador

Sea G un grupo y $A \subset G$. Definimos el **centralizador** de A en G como

$$\mathcal{C}_G(A) = \{g \in G \mid g * a = a * g \ \forall a \in A\}.$$

$$Z = (+1)\,|0\rangle\langle 0| + (-1)\,|1\rangle\langle 1| \qquad \mathcal{S} = \langle T_1, ..., T_n \rangle$$

- **Caso I:** Z_a anticonmuta con, al menos, un generador de $\mathcal{S}$.

$$|\psi'\rangle = \frac{I \pm Z_a}{\sqrt{2}}\,|\psi\rangle \quad \text{y} \quad \mathcal{S}' = \langle \pm Z_a, \mathcal{C}_{\mathcal{S}}(Z_a) \rangle\,.$$

- **Caso II:** Z_a conmuta con todos los generadores de $\mathcal{S}$.

$$|\psi'\rangle = |\psi\rangle \quad \text{y} \quad \mathcal{S}' = \mathcal{C}_{\mathcal{S}}(Z_a) = \mathcal{S}.$$

Eficiencia del algoritmo

Problema a resolver: pertenencia a un grupo.

- Caso I: $O(n^2)$.
  Productos de operadores que anticonmutan con Z_a.

- Caso II: $O(n^3)$.
  Resolución de sistema de ecuaciones.

$$\pm Z_a = T_1^{c_1} \cdot \ldots \cdot T_n^{c_n} \ , \qquad (c_1, \ldots, c_n) \in \mathbb{Z}_2^n$$

Nueva matriz estabilizadora

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

- Se define una subrutina **rowsum(h,i)** que suma las filas R_h y R_i: ejecuta la composición de los generadores correspondientes.

Ideas del algoritmo

- Aplicación de puertas cuánticas:
  Fórmulas explícitas para actualizar la matriz estabilizadora.

- Medida de un qubit:

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

  - **Caso I:** $\exists p \in \{n+1, ..., 2n\}$ tal que $x_{pa} = 1$.
  - **Caso II:** No existe tal $p \Rightarrow \sum_{h=1}^{n} c_h R_{h+n} = \pm Z_a$.

Eficiencia del algoritmo

Producto simpléctico $\Rightarrow$ ~~resolución de sistemas de ecuaciones~~.

$\uparrow$ rowsum $\Longrightarrow$ $\uparrow$ coste

Complejidad: $O(n^2)$

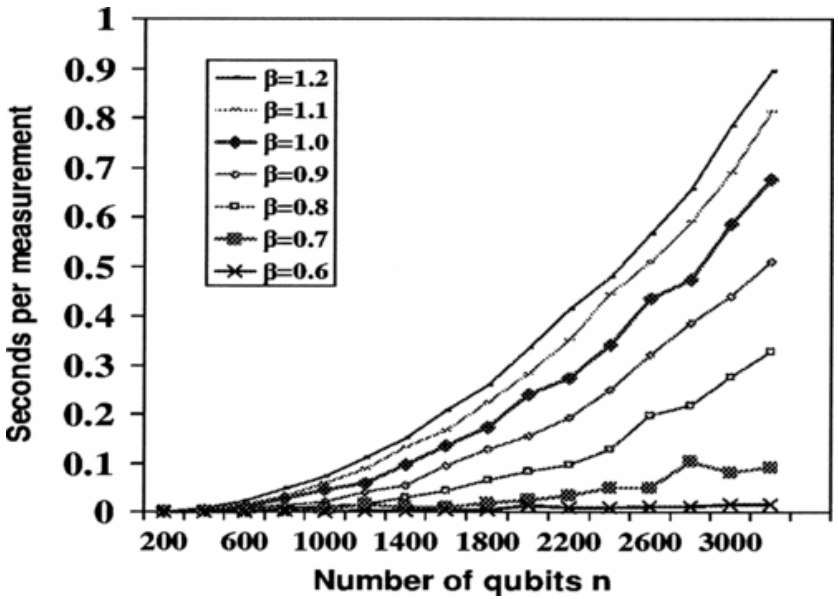


Figura: Experimento test del algoritmo de Aaronson-Gottesman[2].

[2] S. Aaronson, D. Gottesman, *Improved Simulation of Stabilizer Circuits*, Phys. Rev. A 70, 052328 (2004).

Conclusions

- Quantum Computation needs classical simulations.
- Clifford circuits are essential for classical simulations.
- Gottesman-Knill theorem $\Longrightarrow$ they are efficiently simulable.
- Mathematical tools: theory group, symplectic product.
- Gottesman-Knill algorithm $\Longrightarrow O(n^3)$.
- Aaronson-Gottesman algorithm $\Longrightarrow O(n^2)$.

Thank you for your attention!

Puertas cuánticas en el algoritmo de Aaronson-Gottesman

Para cada fila $i \in \{1, ..., 2n\}$:

- **Hadamard sobre el qubit a:**
  $r_i := r_i \oplus x_{ia} z_{ia}$.
  Intercambiamos x_{ia} y z_{ia}.
- **Puerta de fase sobre a:**
  $r_i := r_i \oplus x_{ia} z_{ia}$.
  $z_{ia} := z_{ia} \oplus x_{ia}$.
- **cNOT $a \to b$:**
  $r_i := r_i \oplus x_{ia} z_{ib} (x_{ib} \oplus z_{ia} \oplus 1)$.
  $x_{ib} := x_{ib} \oplus x_{ia}$, $z_{ia} := z_{ia} \oplus z_{ib}$.

Puerta	Entrada	Salida
H	X	Z
	Z	X
P	X	Y
	Z	Z
cNOT	X_1	$X_1 X_2$
	X_2	X_2
	$X_1 X_2$	X_1
	Z_1	Z_1
	Z_2	$Z_1 Z_2$
	$Z_1 Z_2$	Z_2

La medida en el algoritmo de Aaronson-Gottesman

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

- **Caso I:** $\exists p \in \{n+1, ..., 2n\}$ tal que $x_{pa} = 1$.
  - rowsum(i, p) para todo $i \neq p$ tal que $x_{ia} = 1$.
  - $R_p \to R_{p-n}$ y $Z_a \to R_p$ (fase r_p aleatoria).

- **Caso II:** No existe tal $p \Rightarrow \sum_{h=1}^{n} c_h R_{h+n} = \pm Z_a$.

$$c_i = \sum_{h=1}^{n} c_h (R_i|R_{h+n}) = \left(R_i \middle| \sum_{h=1}^{n} c_h R_{h+n} \right) = (R_i|Z_a) \quad i \in \{1, ..., n\}$$

  - rowsum$(2n+1, i+n)$ para todo $i \in \{1, ..., n\}$ tal que $x_{ia} = 1$.

Teleportación Cuántica

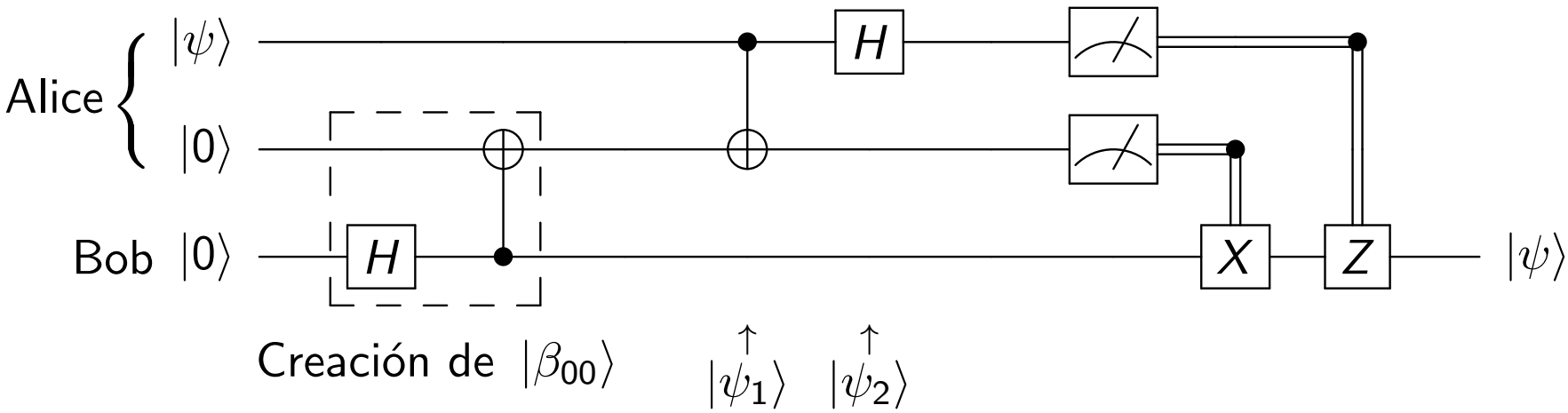


Figura: Circuito para teleportar el estado $|\psi\rangle$.

$$|\psi_0\rangle = |\psi\rangle\,|\beta_{00}\rangle = \left[a\,|0\rangle\,\frac{|00\rangle + |11\rangle}{\sqrt{2}} + b\,|1\rangle\,\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right]$$

Teleportación Cuántica

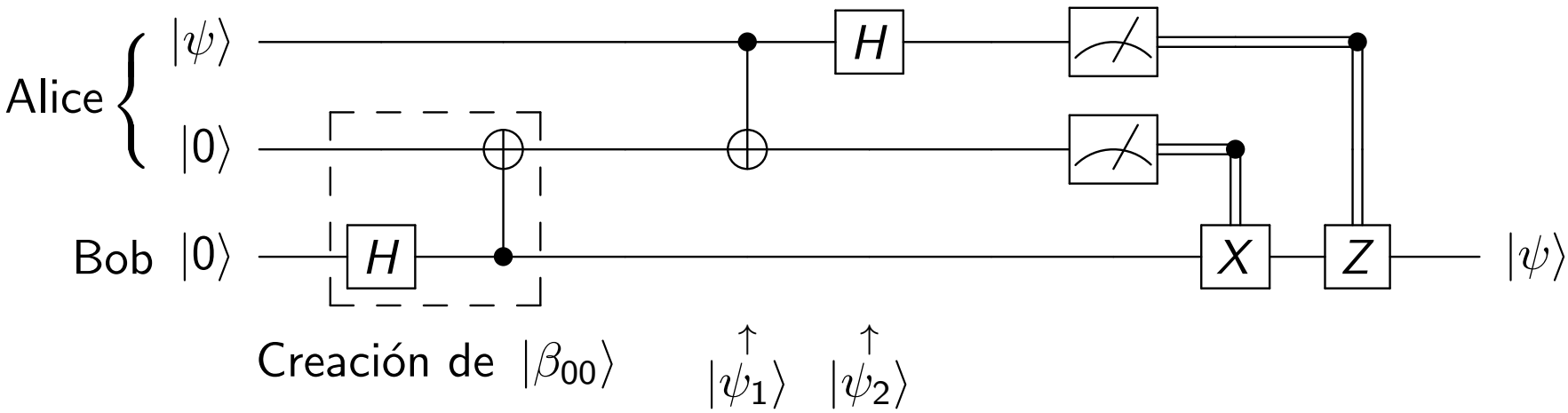


Figura: Circuito para teleportar el estado $|\psi\rangle$.

$$|\psi_2\rangle = \frac{1}{2}\left[\,|00\rangle\,(a\,|0\rangle + b\,|1\rangle) + |01\rangle\,(a\,|1\rangle + b\,|0\rangle)\right.$$
$$\left. + |10\rangle\,(a\,|0\rangle - b\,|1\rangle) + |11\rangle\,(a\,|1\rangle - b\,|0\rangle)\,\right].$$