Algoritmo de Grover

Introducción e implementación en Qiskit

Federico Fuidio

Facultad de Ingeniería
Universidad de Montevideo
Montevideo

Qiskit Fall Fest FIUBA - 10/11/2025

Índice

Introducción

Descripción del problema

- Dada una función binaria $f : \{0,1\}^n \to \{0,1\}$, queremos encontrar un elemento x tal que $f(x) = 1$.
- Definimos M como la cantidad de entradas tales que $f(x) = 1$ (suponemos, por el momento, que M es conocido).
- Para el caso $M = 1$, clásicamente se necesitan $\mathcal{O}(N) = \mathcal{O}(2^n)$ evaluaciones de la función f para encontrar **el** elemento con $f(x) = 1$.
- En general, la cantidad esperada de evaluaciones necesarias es $\mathcal{O}(N/M)$.

Introducción
Descripción del problema

- Pensamos a las entradas con $f(x) = 1$ como una "entrada marcada" o un "elemento marcado".
- Ejemplo de función $f(x_1, x_2) = x_1\overline{x_2}$ de dos bits que marca a 10.

x	$f(x)$
00	0
01	0
10	1
11	0

Introducción
Problema cuántico

- **Cómo implementamos f en una computadora cuántica, teniendo en cuenta que debemos usar operaciones reversibles?**
- Una forma natural de implementar una función f de n bits es usar $n+1$ qubits.
  - Los primeros n qubits se usan para representar la entrada $x = x_1 x_2 \dots x_n$ de la función.
  - El último qubit se usa para la salida de la función. Si $f(x) = 0$, el qubit queda sin cambiar; y si $f(x) = 1$, aplicamos un `NOT`.

$$O\left|x_1 x_2 \dots x_N\right\rangle \left|y\right\rangle = \left|x_1 x_2 \dots x_N\right\rangle \left|y \oplus f(x)\right\rangle$$

- El operador O es unitario por mapear una base ortonormal a otra base ortonormal.

Introducción
Problema cuántico

x	$f(x)$
00	0
01	0
10	1
11	0

$\|x\rangle\|0\rangle$	$O\|x\rangle\|0\rangle$	$\|x\rangle\|1\rangle$	$O\|x\rangle\|1\rangle$
$\|00\rangle\|0\rangle$	$\|00\rangle\|0\rangle$	$\|00\rangle\|1\rangle$	$\|00\rangle\|1\rangle$
$\|01\rangle\|0\rangle$	$\|01\rangle\|0\rangle$	$\|01\rangle\|1\rangle$	$\|01\rangle\|1\rangle$
$\|10\rangle\|0\rangle$	$\|10\rangle\|1\rangle$	$\|10\rangle\|1\rangle$	$\|10\rangle\|0\rangle$
$\|11\rangle\|0\rangle$	$\|11\rangle\|0\rangle$	$\|11\rangle\|1\rangle$	$\|11\rangle\|1\rangle$

Introducción

Problema cuántico

Estudiamos qué pasa si aplicamos el operador O al estado $|x_1 x_2 \dots x_n\rangle |-\rangle$:

$$O|x_1 x_2 \dots x_n\rangle |-\rangle = O|x_1 x_2 \dots x_n\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \tag{1}$$

$$= |x_1 x_2 \dots x_n\rangle \underbrace{\left(\frac{|f(x)\rangle - \left|\overline{f(x)}\right\rangle}{\sqrt{2}}\right)}_{(-1)^{f(x)}|-\rangle} \tag{2}$$

$$= (-1)^{f(x)} |x_1 x_2 \dots x_n\rangle |-\rangle \tag{3}$$

Descartando el último qubit, que se mantiene en el estado $|-\rangle$, el efecto de O es **cambiar el signo de los elementos marcados**.

Introducción
Problema cuántico

Planteo cuántico

- Tenemos un **oráculo** O_f tal que, en la base computacional, actúa cambiando el signo de los elementos marcados por f:

$$O_f |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} |x\rangle & \text{si } f(x) = 0 \\ -|x\rangle & \text{si } f(x) = 1 \end{cases}$$

- El oráculo O_f se puede implementar de forma directa o aplicando la operación O al estado $|x\rangle |-\rangle$.
- Veamos cómo podemos encontrar el elemento marcado usando el oráculo O_f con $\mathcal{O}(\sqrt{N/M})$ aplicaciones del oráculo.

Algoritmo

Motivación

Estudiemos qué pasa si aplicamos la operación O_f a una superposición uniforme de todos los estados de la base computacional, es decir, al estado $H|0\rangle = |+\rangle^{\otimes n}$:

$$O_f |+\rangle^{\otimes n} = O_f \left[\frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i\rangle \right] \tag{4}$$

$$= \frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} (-1)^{f(i)} |i\rangle \tag{5}$$

Algoritmo

Motivación

Aplicamos un operador de difusión $A = H(2\left|0\right\rangle\left\langle 0\right| - \mathbb{I})H = 2\left|+\right\rangle^{\otimes n}\left\langle +\right|^{\otimes n} - \mathbb{I}$, que tiene el efecto de invertir cada amplitud α_i sobre la media, $\overline{\alpha}$:

Algoritmo

Motivación

Aplicamos un operador de difusión $A = H(2\left|0\right\rangle\left\langle 0\right| - \mathbb{I})H = 2\left|+\right\rangle^{\otimes n}\left\langle +\right|^{\otimes n} - \mathbb{I}$, que tiene el efecto de invertir cada amplitud α_i sobre la media, $\overline{\alpha}$:

$$A\left|\psi\right\rangle = \left(2\left|+\right\rangle^{\otimes n}\left\langle +\right|^{\otimes n} - \mathbb{I}\right)\sum_{i\in\{0,1\}^n}\alpha_i\left|i\right\rangle \tag{6}$$

Algoritmo

Motivación

Aplicamos un operador de difusión $A = H(2\left|0\right\rangle\left\langle 0\right| - \mathbb{I})H = 2\left|+\right\rangle^{\otimes n}\left\langle +\right|^{\otimes n} - \mathbb{I}$, que tiene el efecto de invertir cada amplitud α_i sobre la media, $\overline{\alpha}$:

$$A\left|\psi\right\rangle = \left(\sum_{i\in\{0,1\}^n} \alpha_i \overbrace{\left(\left\langle +\right|^{\otimes n}\left|i\right\rangle\right)}^{\frac{1}{\sqrt{N}}} 2 \overbrace{\left|+\right\rangle^{\otimes n}}^{\frac{1}{\sqrt{N}}\sum_j \left|j\right\rangle}\right) - \left(\sum_{i\in\{0,1\}^n} \alpha_i \left|i\right\rangle\right) \tag{6}$$

Algoritmo
Motivación

Aplicamos un operador de difusión $A = H(2\left|0\right\rangle\left\langle 0\right| - \mathbb{I})H = 2\left|+\right\rangle^{\otimes n}\left\langle +\right|^{\otimes n} - \mathbb{I}$, que tiene el efecto de invertir cada amplitud α_i sobre la media, $\overline{\alpha}$:

$$A\left|\psi\right\rangle = \left(\sum_{i\in\{0,1\}^n} \alpha_i \frac{1}{\sqrt{N}} 2 \frac{1}{\sqrt{N}} \sum_{j\in\{0,1\}^n} \left|j\right\rangle\right) - \left(\sum_{i\in\{0,1\}^n} \alpha_i \left|i\right\rangle\right) \tag{6}$$

$$= \left(\sum_{j\in\{0,1\}^n} 2\left[\sum_{i\in\{0,1\}^n} \frac{1}{N}\alpha_i\right]\left|j\right\rangle\right) - \left(\sum_{j\in\{0,1\}^n} \alpha_j \left|j\right\rangle\right) \tag{7}$$

$$= \sum_{j\in\{0,1\}^n} \left(2\overline{\alpha} - \alpha_j\right)\left|j\right\rangle \tag{8}$$

Algoritmo

Motivación

Si aplicamos el operador AO_f al estado $|+\rangle^{\otimes n}$, tiene el efecto de cambiar las amplitudes $1/\sqrt{N}$ de $|+\rangle^{\otimes n}$ como:

$$\frac{1}{\sqrt{N}} \rightarrow \left[2\frac{1}{N} \overbrace{\frac{1}{\sqrt{N}}(N-2M)}^{\text{Suma de amplitudes de } O_f|+\rangle^{\otimes n}} - \overbrace{\frac{1}{\sqrt{N}}(-1)^{f(i)}}^{\text{Amplitud de } |i\rangle \text{ en } O_f|+\rangle^{\otimes n}} \right] \tag{9}$$

Algoritmo

Motivación

Si aplicamos el operador AO_f al estado $|+\rangle^{\otimes n}$, tiene el efecto de cambiar las amplitudes $1/\sqrt{N}$ de $|+\rangle^{\otimes n}$ como:

$$\frac{1}{\sqrt{N}} \to \frac{1}{\sqrt{N}}\left[2 - \frac{4M}{N} - (-1)^{f(i)}\right] = \frac{1}{\sqrt{N}} \begin{cases} 3 - \frac{4M}{N} & \text{Si } f(i) = 1 \\ 1 - \frac{4M}{N} & \text{Si } f(i) = 0 \end{cases} \tag{9}$$

Notemos que, si $3 - 4M/N > 1 \Rightarrow M < N/2$ la amplitud de los estados marcados va a aumentar.

- **Aumenta la probabilidad de medir un elemento marcado**

Algoritmo
Motivación

Ejemplo: función $f(x) = x_1\overline{x_2}$ ($n = 2$, $N = 4$, $M = 1$)

- Comenzamos con una superposición uniforme de los cuatro estados de la base computacional:

$$|+\rangle^{\otimes n} = \frac{1}{2}\left(|00\rangle + |01\rangle + \overbrace{|10\rangle}^{\text{Estado marcado}} + |11\rangle\right)$$

- Después de implementar la operación AO_f, las amplitudes pasan a ser:

$$\frac{1}{\sqrt{N}} \to \frac{1}{\sqrt{N}}\begin{cases} 3 - \frac{4M}{N} & \text{Si } f(i) = 1 \\ 1 - \frac{4M}{N} & \text{Si } f(i) = 0 \end{cases} \Rightarrow AO_f\,|+\rangle^{\otimes n} = |10\rangle$$

Algoritmo
Descripción

- **Qué pasa si seguimos aplicando AO_f?**
- **Se puede seguir aumentando la amplitud de los estados marcados?**

Definimos los estados $|\alpha\rangle$ (combinación uniforme de estados **NO** marcados) y $|\beta\rangle$ (combinación uniforme de estados marcados).

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{i \in f^{-1}(0)} |i\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_{i \in f^{-1}(1)} |i\rangle$$

Algoritmo
Descripción

Una propiedad interesante es que en todo el proceso nos mantenemos en el plano generado por los vectores $|\alpha\rangle$ y $|\beta\rangle$, por ejemplo:

$$|+\rangle^{\otimes n} = \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle$$

$$O_f|+\rangle^{\otimes n} = \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle - \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle$$

$$AO_f|+\rangle^{\otimes n} = \frac{\sqrt{N-M}}{\sqrt{N}}\left(1-\frac{4M}{N}\right)|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}\left(3-\frac{4M}{N}\right)|\beta\rangle$$

Algoritmo
Descripción

Veamos el efecto de AO_f en el subespacio generado por $|\alpha\rangle$ y $|\beta\rangle$.

$$O_f(x\,|\alpha\rangle + y\,|\beta\rangle) = x\,|\alpha\rangle - y\,|\beta\rangle$$

$$A\,|\alpha\rangle = \left(\frac{2}{N}\frac{N-M}{\sqrt{N-M}} - \frac{1}{\sqrt{N-M}}\right)\sqrt{N-M}\,|\alpha\rangle + \frac{2}{N}\frac{N-M}{\sqrt{N-M}}\sqrt{M}\,|\beta\rangle$$

$$A\,|\beta\rangle = \frac{2}{N}\frac{M}{\sqrt{M}}\sqrt{N-M}\,|\alpha\rangle + \left(\frac{2}{N}\frac{M}{\sqrt{M}} - \frac{1}{\sqrt{M}}\right)\sqrt{M}\,|\beta\rangle$$

Algoritmo
Descripción

Por tanto, AO_f se puede escribir matricialmente en la base $\mathcal{B} = \{|\alpha\rangle, |\beta\rangle\}$ como:

$$ {}_{\mathcal{B}}[AO_f]_{\mathcal{B}} = \begin{bmatrix} -\frac{2}{N}M + 1 & -\frac{2}{N}\sqrt{M}\sqrt{N-M} \\ \frac{2}{N}\sqrt{M}\sqrt{N-M} & -\frac{2}{N}M + 1 \end{bmatrix} $$

Notemos que ${}_{\mathcal{B}}[AO_f]_{\mathcal{B}}$ es unitaria. No solo eso, sino que tiene la forma de una matriz de rotación:

$$ {}_{\mathcal{B}}[AO_f]_{\mathcal{B}} = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} $$

Con $\theta = 2\arcsin\left(\sqrt{M}/\sqrt{N}\right) = 2\arccos\left(\sqrt{N-M}/\sqrt{N}\right)$.

Algoritmo
Descripción

Podemos, por tanto, encontrar la descomposición espectral de $_{\mathcal{B}}[AO_f]_{\mathcal{B}}$:

$$
{}_{\mathcal{B}}[AO_f]_{\mathcal{B}} = \begin{bmatrix} i/\sqrt{2} & -i/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{bmatrix} \begin{bmatrix} -i/\sqrt{2} & 1/\sqrt{2} \\ i/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}
$$

$$
{}_{\mathcal{B}}[AO_f]^r_{\mathcal{B}} = \begin{bmatrix} i/\sqrt{2} & -i/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} e^{ir\theta} & 0 \\ 0 & e^{-ir\theta} \end{bmatrix} \begin{bmatrix} -i/\sqrt{2} & 1/\sqrt{2} \\ i/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}
$$

Algoritmo
Descripción

La componente de $|\beta\rangle$ después de aplicar r veces la operación ${}_{\mathcal{B}}[AO_f]_{\mathcal{B}}$ es:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}^{\dagger} {}_{\mathcal{B}}[AO_f]^r_{\mathcal{B}} \begin{bmatrix} \sqrt{N-M}/\sqrt{N} \\ \sqrt{M}/\sqrt{N} \end{bmatrix} = \cos(r\theta)\frac{\sqrt{M}}{\sqrt{N}} + \sin(r\theta)\frac{\sqrt{N-M}}{\sqrt{N}} \tag{10}$$

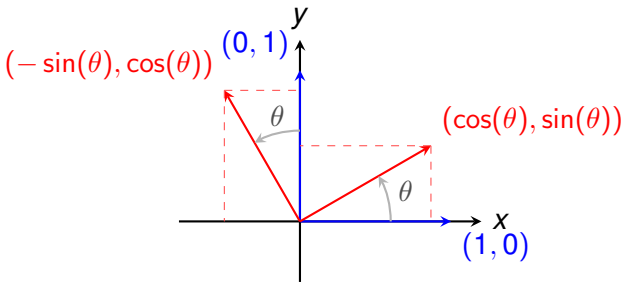
$$= \cos(r\theta)\sin(\theta/2) + \sin(r\theta)\cos(\theta/2) \tag{11}$$

$$= \sin\left(r\theta + \frac{\theta}{2}\right) \tag{12}$$

Para maximizar la componente en $|\beta\rangle$ queremos que $r\theta + \theta/2 \approx \pi/2$

Visualización

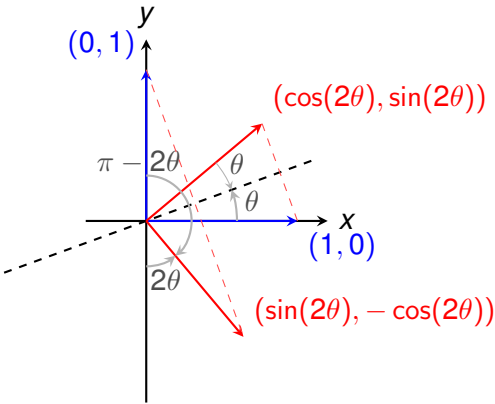
Matrices de rotación y reflexión



$$R_{\text{rot}}(\theta) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$$

Visualización

Matrices de rotación y reflexión



$$R_{\text{ref}}(\theta) = \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix}$$

También podemos escribir:

$$R_{\text{ref}}(\theta) = 2\,\mathbf{v}\mathbf{v}^{\dagger} - \mathbb{I},$$

con:

$$\mathbf{v} = \begin{bmatrix} \cos(\theta) \\ \sin(\theta) \end{bmatrix}$$

Visualización

Matrices de rotación y reflexión

Notemos que una reflexión sobre el eje x (es decir, una reflexión con ángulo $\theta = 0$) seguida por una reflexión de un ángulo θ corresponde a una rotación de 2θ:

$$R_{\text{ref}}(\theta)R_{\text{ref}}(0) = \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{13}$$

$$= \begin{bmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{bmatrix} \tag{14}$$

$$= R_{\text{rot}}(2\theta) \tag{15}$$

Visualización

Acción del operador de Grover en el plano

En el plano definido por $|\alpha\rangle$ y $|\beta\rangle$, el operador O_f actúa como una reflexión sobre el eje x (la componente de $|\alpha\rangle$), mientras que el operador A se puede escribir como:

$$A = 2\,|+\rangle^{\otimes n}\,\langle +|^{\otimes n} - \mathbb{I} \tag{16}$$

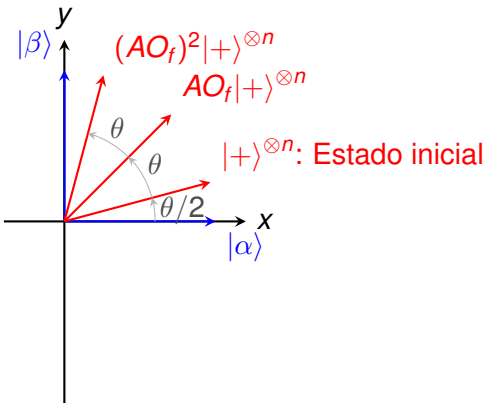
$$= 2\left(\frac{\sqrt{N-M}}{\sqrt{N}}\,|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}\,|\beta\rangle\right)\left(\frac{\sqrt{N-M}}{\sqrt{N}}\,\langle\alpha| + \frac{\sqrt{M}}{\sqrt{N}}\,\langle\beta|\right) - \mathbb{I} \tag{17}$$

El ángulo $\theta/2$ entre $|\alpha\rangle$ y $|+\rangle^{\otimes n}$ en el plano es:

$$\frac{\theta}{2} = \arcsin\left(\frac{\sqrt{M}}{\sqrt{N}}\right)$$

Visualización

Acción del operador de Grover en el plano



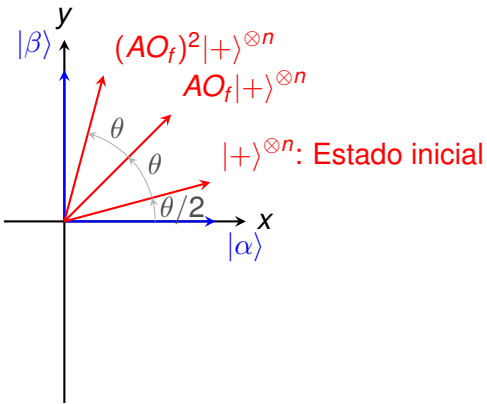
Después de r iteraciones, el ángulo de $(AO_f)^r\,|+\rangle^{\otimes n}$ en el plano es de $r\theta + \theta/2$. Queremos elegir r para que:

$$r\theta + \frac{\theta}{2} \approx \frac{\pi}{2}$$

$$\Rightarrow r\theta \approx \frac{\pi}{2} - \frac{\theta}{2}$$

Visualización

Acción del operador de Grover en el plano



$$r\theta \approx \pi/2 - \theta/2 = \arccos\left(\sqrt{M}/\sqrt{N}\right)$$

$$\Rightarrow r_{\text{ideal}} = \frac{\arccos\left(\sqrt{M}/\sqrt{N}\right)}{\theta}$$

En general, r_{ideal} no es un entero, por lo que debemos aplicar R iteraciones, siendo $R := [r_{\text{ideal}}]$ el entero más cercano a r_{ideal}.

Visualización

Visualización geométrica

Buscamos ahora una cota superior para R. Recordemos que:

$$R = [r_{\text{ideal}}] \leq \lceil r_{\text{ideal}} \rceil = \left\lceil \frac{\pi - \theta}{2\theta} \right\rceil = \left\lceil \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil \leq \left\lceil \frac{\pi}{2\theta} \right\rceil.$$

Como la función $\lceil x \rceil$ es monótona creciente, basta con acotar θ para obtener una cota sobre R. Sabemos que:

$$\frac{\theta}{2} \geq \sin\left(\frac{\theta}{2}\right) = \frac{\sqrt{M}}{\sqrt{N}}.$$

Por tanto:

$$R \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil \Rightarrow R = \mathcal{O}\left(\sqrt{\frac{N}{M}}\right).$$

Comentarios finales

Probabilidad de éxito

En la cantidad ótpima de iteraciones, el ángulo γ entre el eje y y $(AO_f)^r \left|+\right\rangle^{\otimes n}$ es a lo sumo $\theta/2$:

$$|r_{\text{ideal}} - R| \leq 0.5 \Rightarrow \left|\frac{\pi/2 - \theta/2}{\theta} - R\right| \leq 0.5 \Rightarrow \left|\overbrace{\pi/2 - (\theta/2 + R\theta)}^{\gamma}\right| \leq 0.5\theta$$

Por tanto, la probabilidad de éxito P_{E} es:

$$P_{\text{E}} = \sin^2(R\theta + \theta/2) = \cos^2(|\gamma|) \geq \cos^2(\theta/2) = \sqrt{\frac{N-M}{N}}^2 = \frac{N-M}{N}$$

La probabilidad de éxito es mayor o igual $1/2$ siempre que $M \leq N/2$.

Comentarios finales

Qué pasa si $M > N/2$?

Si sabemos de antemano que $M > N/2$, basta preparar el estado $|+\rangle^{\otimes n}$ y medir. La probabilidad de éxito inicial ya es $P_{\mathrm{E}} = M/N \geq 1/2$, por lo que no es necesario aplicar el operador AO_f.

Qué pasa si no conocemos el valor de M?

- Podemos usar **Quantum Counting**, que permite estimar el valor de M (y por tanto el número de iteraciones óptimo R) mediante *Quantum Phase Estimation*.
- También podemos repetir el algoritmo tomando la cantidad de iteraciones óptima para $M_t = N/2^t$ entradas marcadas, con $t = 0, 1, \ldots$

Gracias!

Federico Fuidio

Facultad de Ingeniería
Universidad de Montevideo
Montevideo

Qiskit Fall Fest FIUBA - 10/11/2025