# Algoritmo de Grover

Luis Daniel Benavides Navarro, 2-03-2024

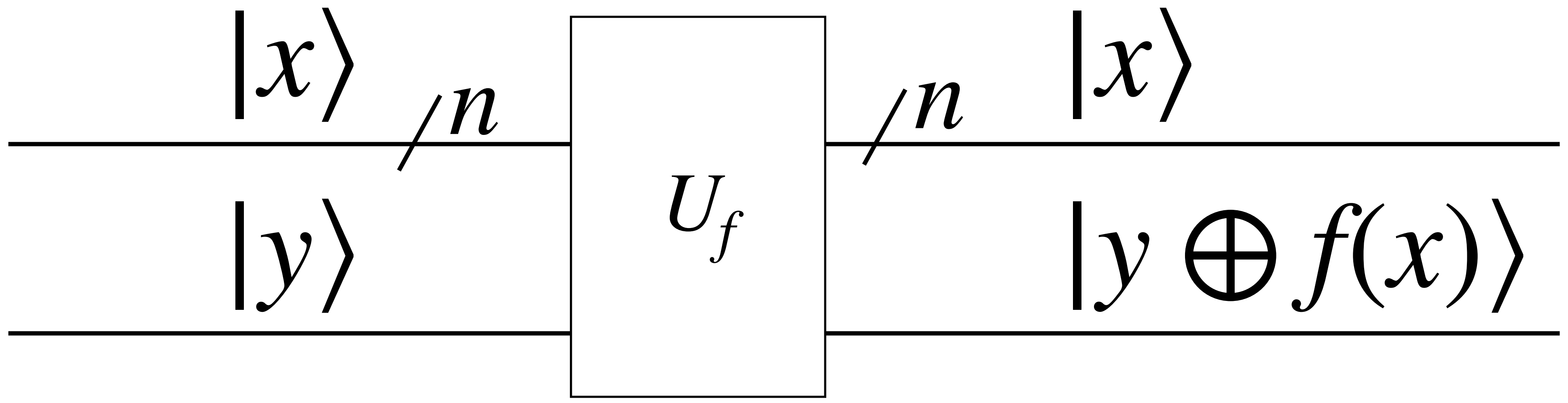
# Estrategia General de los Algoritmos cuánticos

- Iniciar los qubits en un estado clásico.
- Poner los qubits en superposición
- Realizar las operaciones en los qubits.
- Realizar una observación

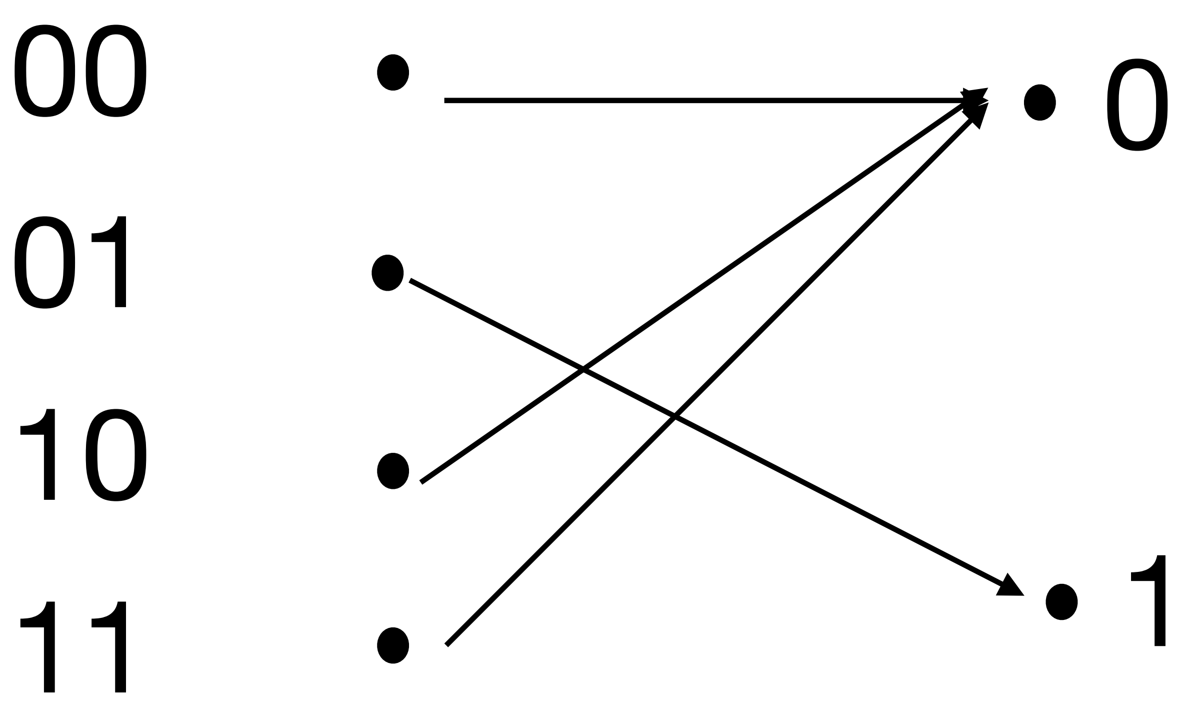
# Problema que deseamos resolver

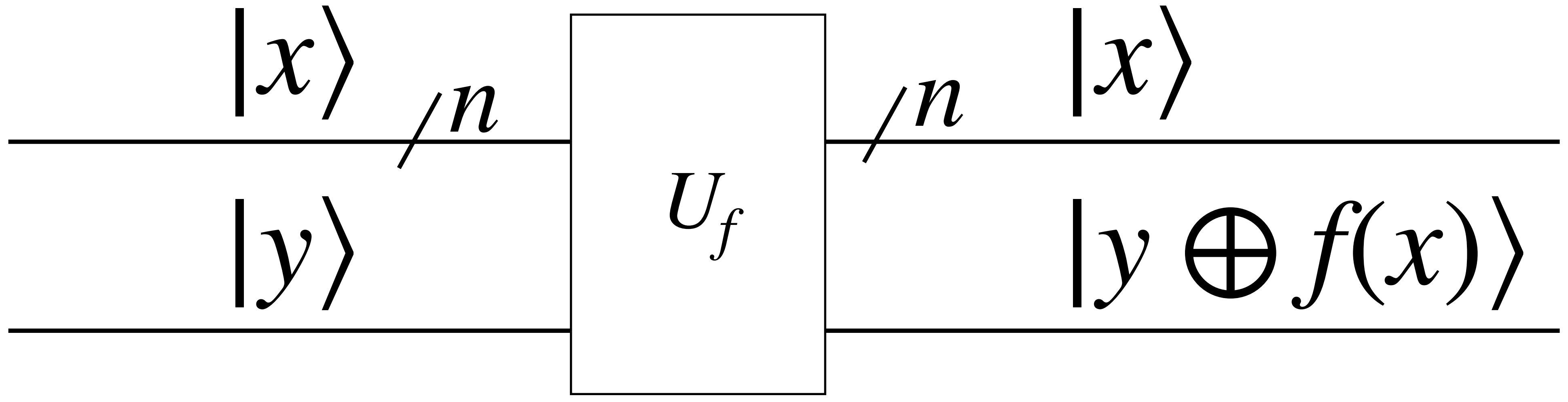
- El problema que resuelve es el de búsqueda algorítmica
- La búsqueda algorítmica es la búsqueda exhaustiva de un número con una condición particular.
- La búsqueda se puede modelar como examinar varias posibilidades para ver cuál satisface una condición:
    - Imagine que nos dan una función $f : \{0,1\}^n \rightarrow \{0,1\}$
    - Y nos aseguran que existe una cadena binaria en particular $x_0$ tal que:
    - $f(x) = \begin{cases} 1, & \text{if } x = x_0 \\ 0, & \text{if } x \neq x_0 \end{cases}$
    - En un computador clásico necesitaríamos evaluar las $2^n$ cadenas en el peor de los casos. En promedio podríamos encontrar el valor en $2^n/2$ pasos.
    - Con el algoritmo de Grover necesitaremos $\sqrt{2^n}$

# ¿Podemos representar el problema con compuertas y matrices?



# ¿Podemos representar el problema con compuertas y matrices?

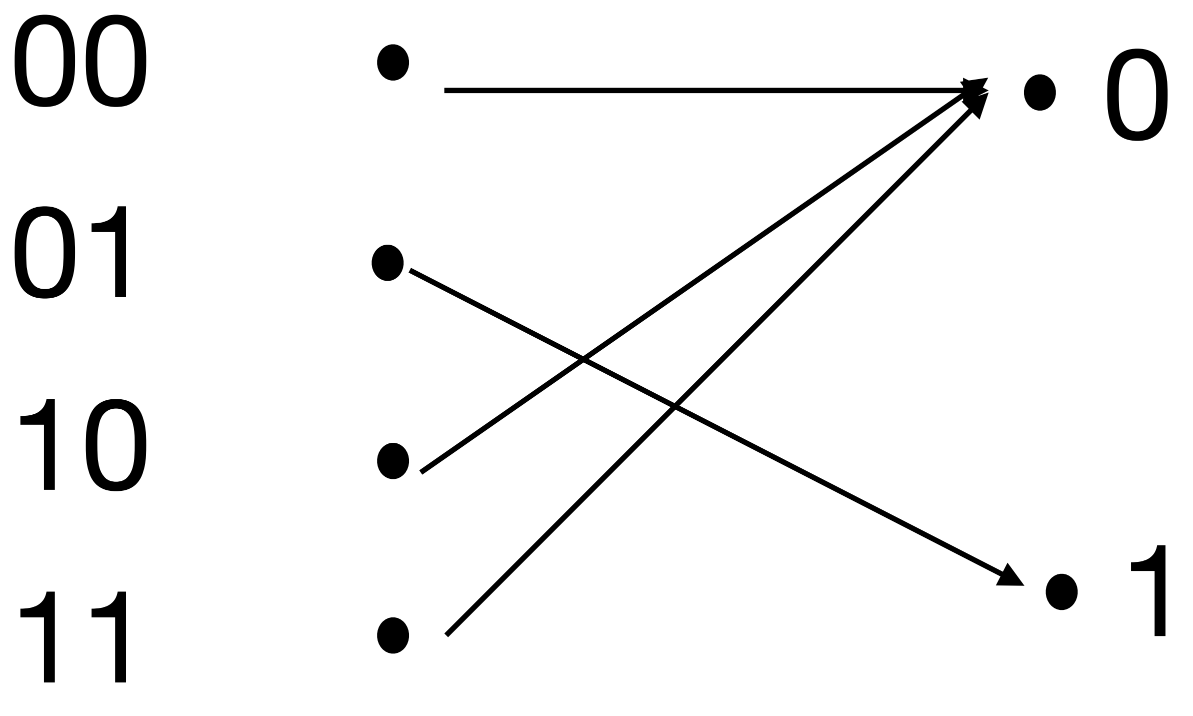


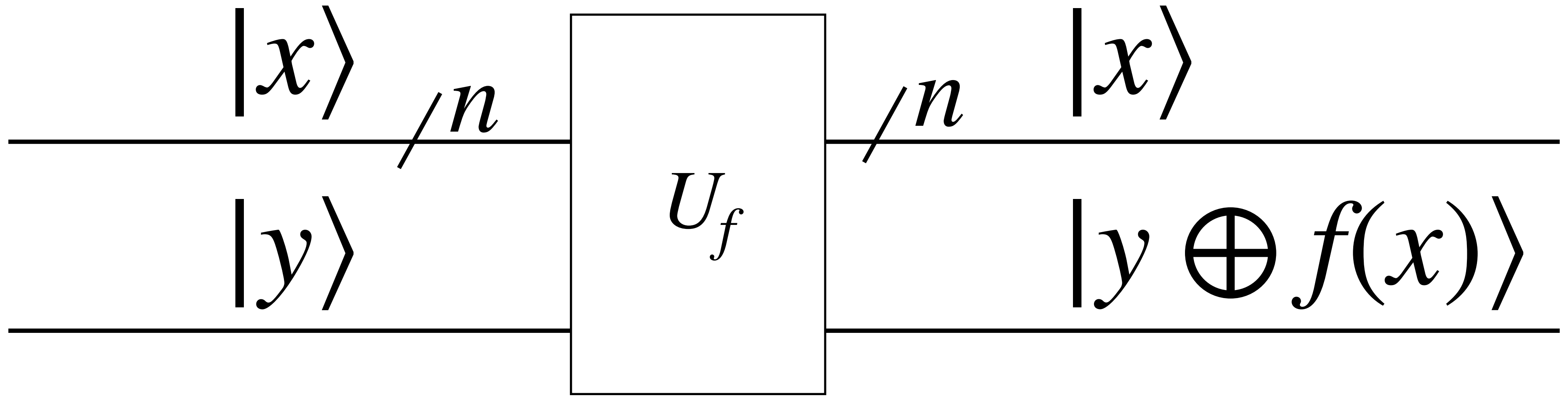




| | **000** | **001** | **010** | **011** | **100** | **101** | **110** | **111** |
|---|---|---|---|---|---|---|---|---|
| **000** | | | | | | | | |
| **001** | | | | | | | | |
| **010** | | | | | | | | |
| **011** | | | | | | | | |
| **100** | | | | | | | | |
| **101** | | | | | | | | |
| **110** | | | | | | | | |
| **111** | | | | | | | | |

**Ejercicio**.
Representar
otras funciones.

# ¿Podemos representar el problema con compuertas y matrices?



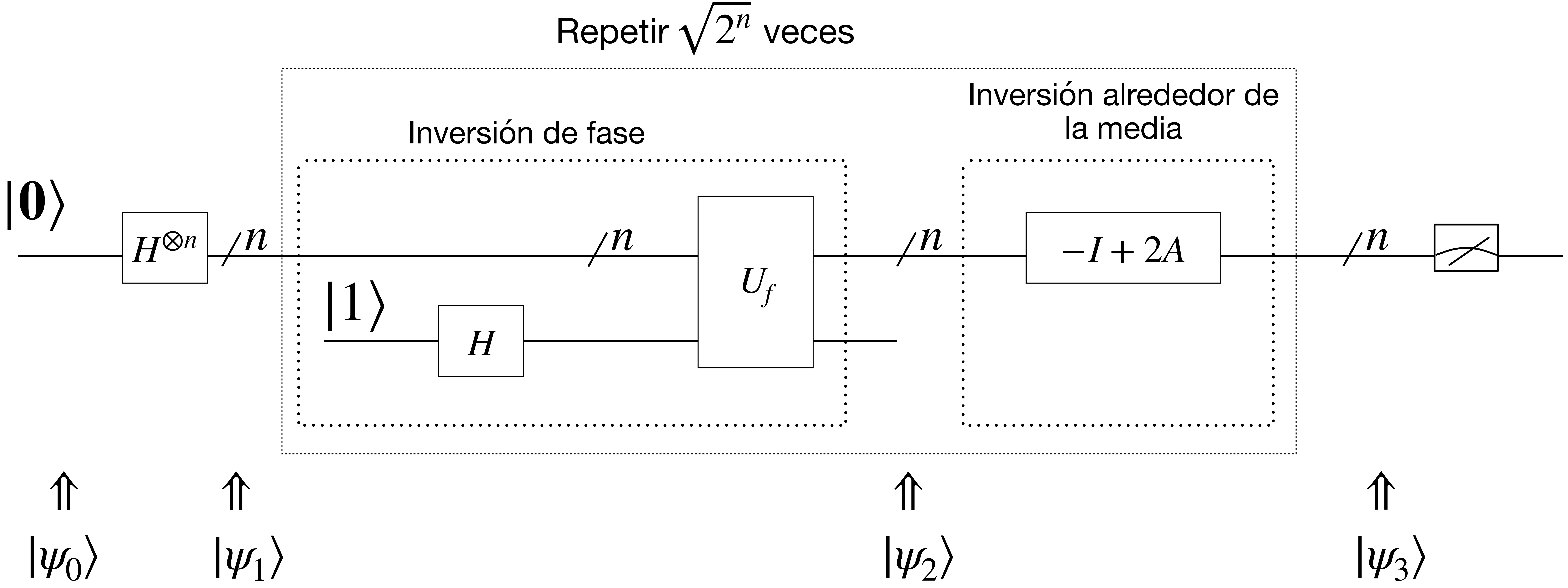




| | **000** | **001** | **010** | **011** | **100** | **101** | **110** | **111** |
|---|---|---|---|---|---|---|---|---|
| **000** | 1 | | | | | | | |
| **001** | | 1 | | | | | | |
| **010** | | | | 1 | | | | |
| **011** | | | 1 | | | | | |
| **100** | | | | | 1 | | | |
| **101** | | | | | | 1 | | |
| **110** | | | | | | | 1 | |
| **111** | | | | | | | | 1 |

**Ejercicio**.
Representar
otras funciones.

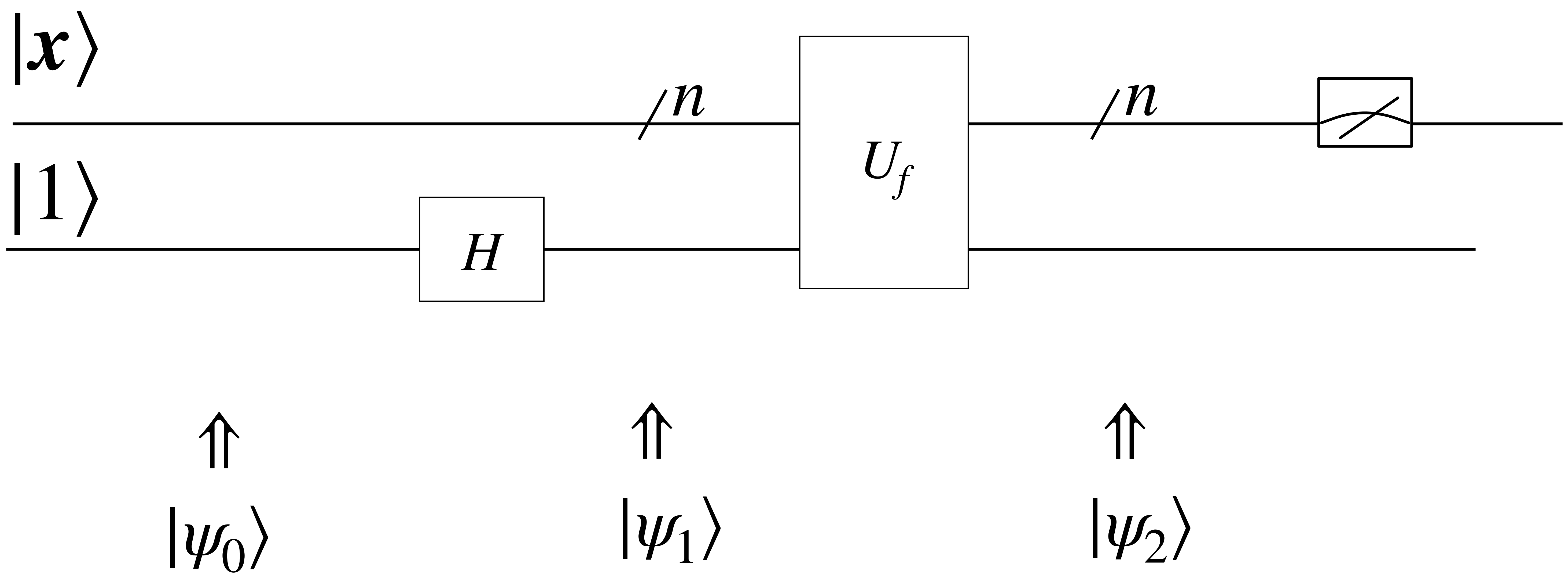
# ¿Podemos hacerlo mejor con un sistema cuántico?

# El algoritmo de Grover

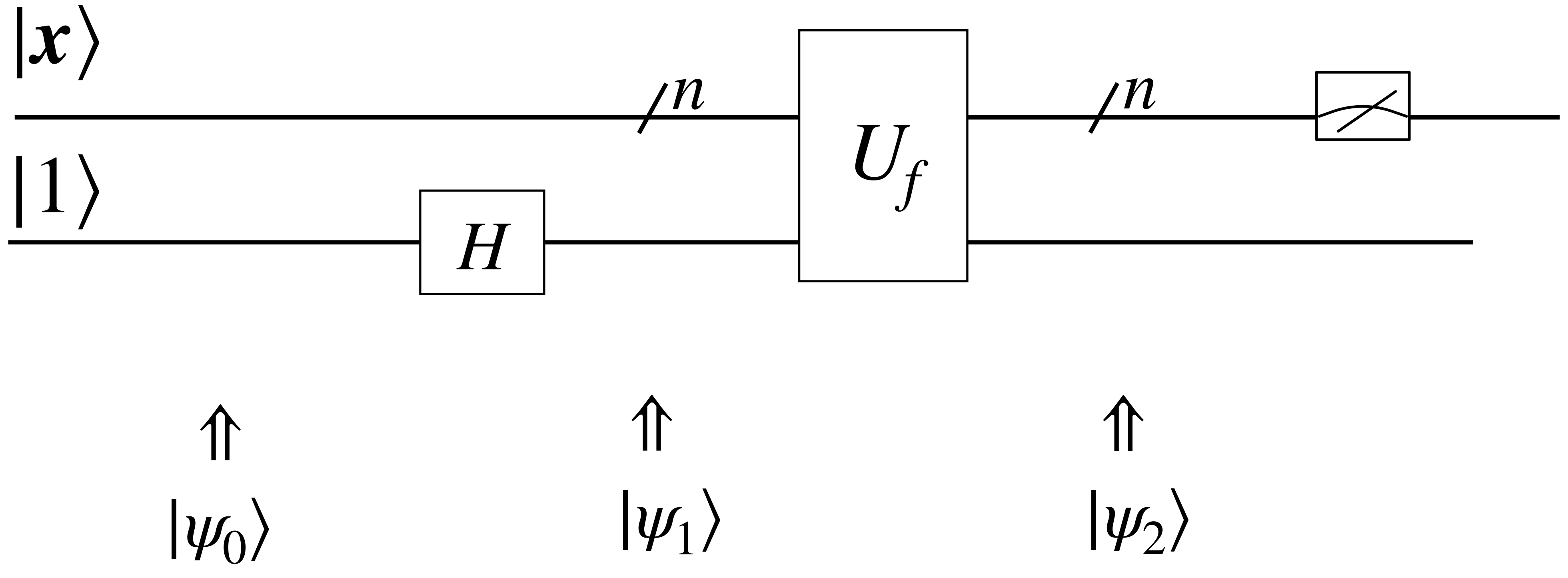


# Inversión de fase

# Inversión de fase

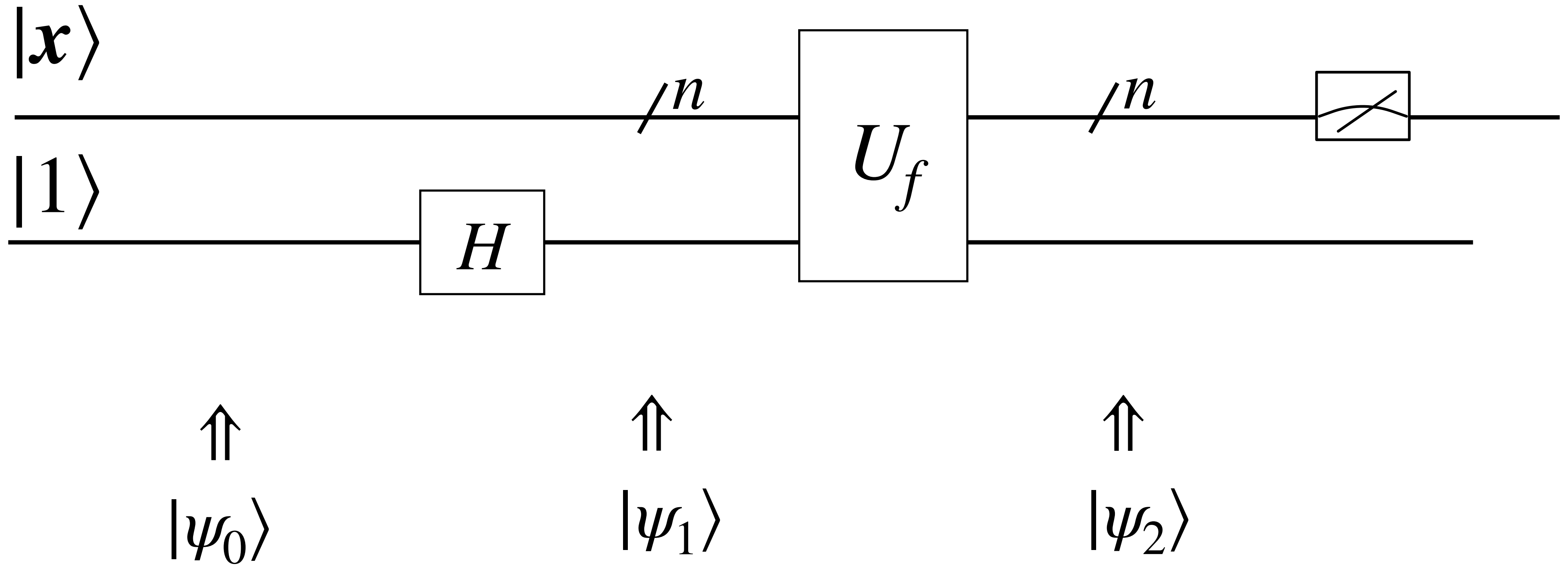


# Inversión de fase




$$|\psi_0\rangle = |\boldsymbol{x}\rangle \otimes |1\rangle = |\boldsymbol{x},1\rangle$$

# Inversión de fase



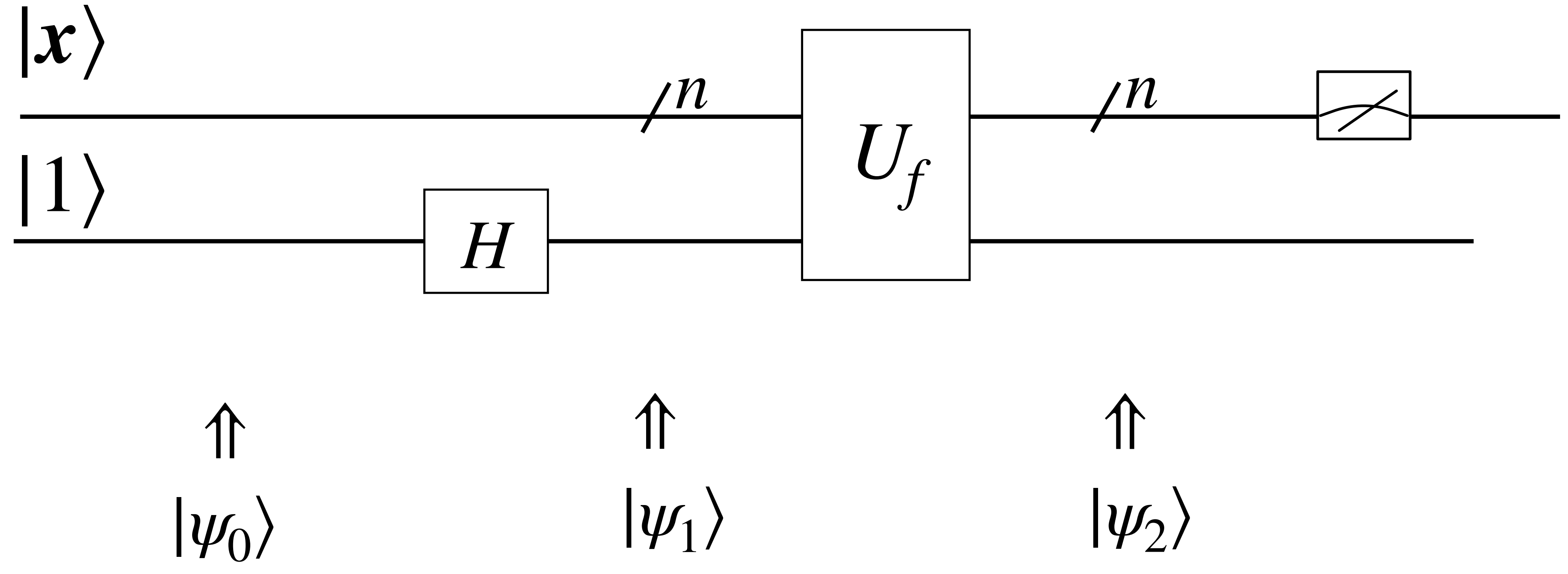

$|\psi_0\rangle = |\mathbf{x}\rangle \otimes |1\rangle = |\mathbf{x},1\rangle$

$$|\psi_1\rangle = (I \otimes H)[|\mathbf{x}\rangle \otimes |1\rangle]$$

$$|\psi_1\rangle = |\mathbf{x}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|\psi_1\rangle = \frac{|\mathbf{x},0\rangle - |\mathbf{x},1\rangle}{\sqrt{2}}$$

# Inversión de fase




$$|\psi_0\rangle = |\boldsymbol{x}\rangle \otimes |1\rangle = |\mathbf{0},1\rangle$$

$$|\psi_1\rangle = \frac{|\boldsymbol{x},0\rangle - |\boldsymbol{x},1\rangle}{\sqrt{2}}$$

$$|\psi_2\rangle = \frac{|\boldsymbol{x}, f(x)\rangle - |\boldsymbol{x}, \neg f(x)\rangle}{\sqrt{2}}$$

$$|\psi_2\rangle = \begin{cases} \dfrac{|\boldsymbol{x},1\rangle - |\boldsymbol{x},0\rangle}{\sqrt{2}} & \text{si } x = x_0 \\ \dfrac{|\boldsymbol{x},0\rangle - |\boldsymbol{x},1\rangle}{\sqrt{2}} & \text{si } x \neq x_0 \end{cases}$$

$$|\psi_2\rangle = (-1)^{f(x)} * \frac{|\boldsymbol{x},0\rangle - |\boldsymbol{x},1\rangle}{\sqrt{2}}$$

$$|\psi_2\rangle = (-1)^{f(x)}|\boldsymbol{x}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

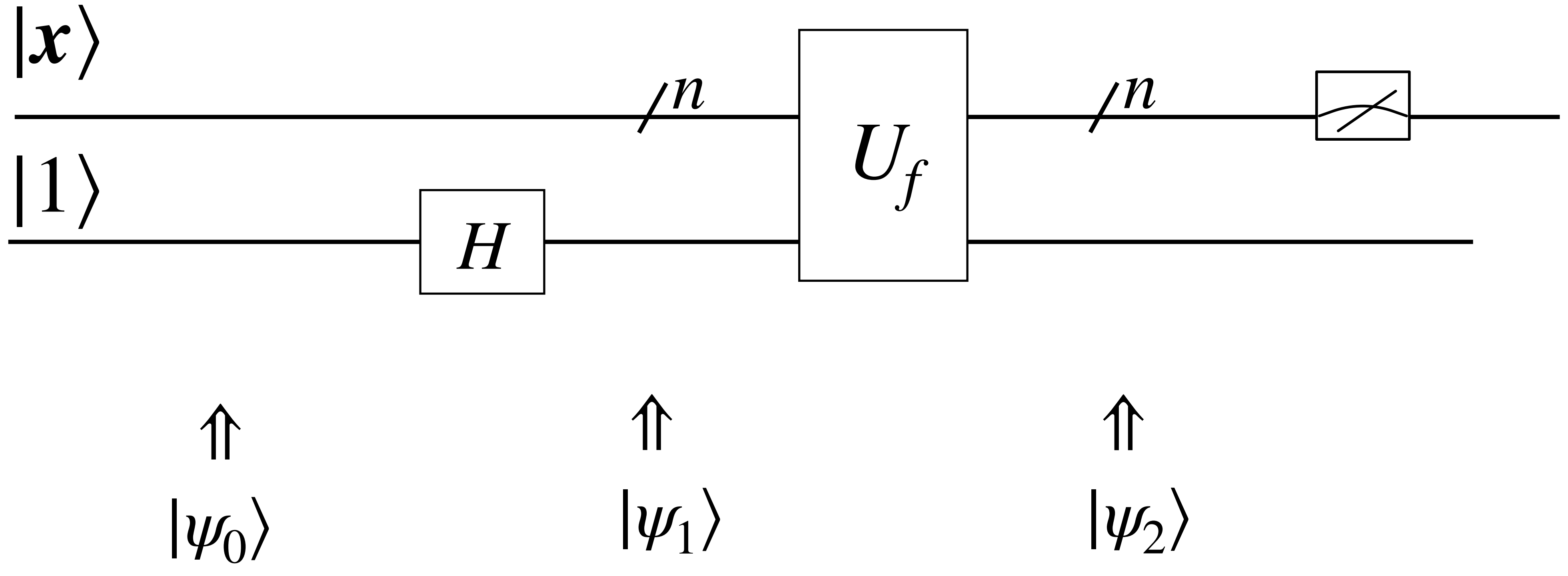
# Inversión de fase

## Ejemplo

$$|\psi_0\rangle = |\boldsymbol{x}\rangle \otimes |1\rangle = |\boldsymbol{0},1\rangle$$

$$|\psi_1\rangle = \frac{|\boldsymbol{x},0\rangle - |\boldsymbol{x},1\rangle}{\sqrt{2}}$$

$$|\psi_2\rangle = (-1)^{f(x)}|\boldsymbol{x}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$




$$x_0 = 100$$

$$|\boldsymbol{x}\rangle = [\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}}]^T$$

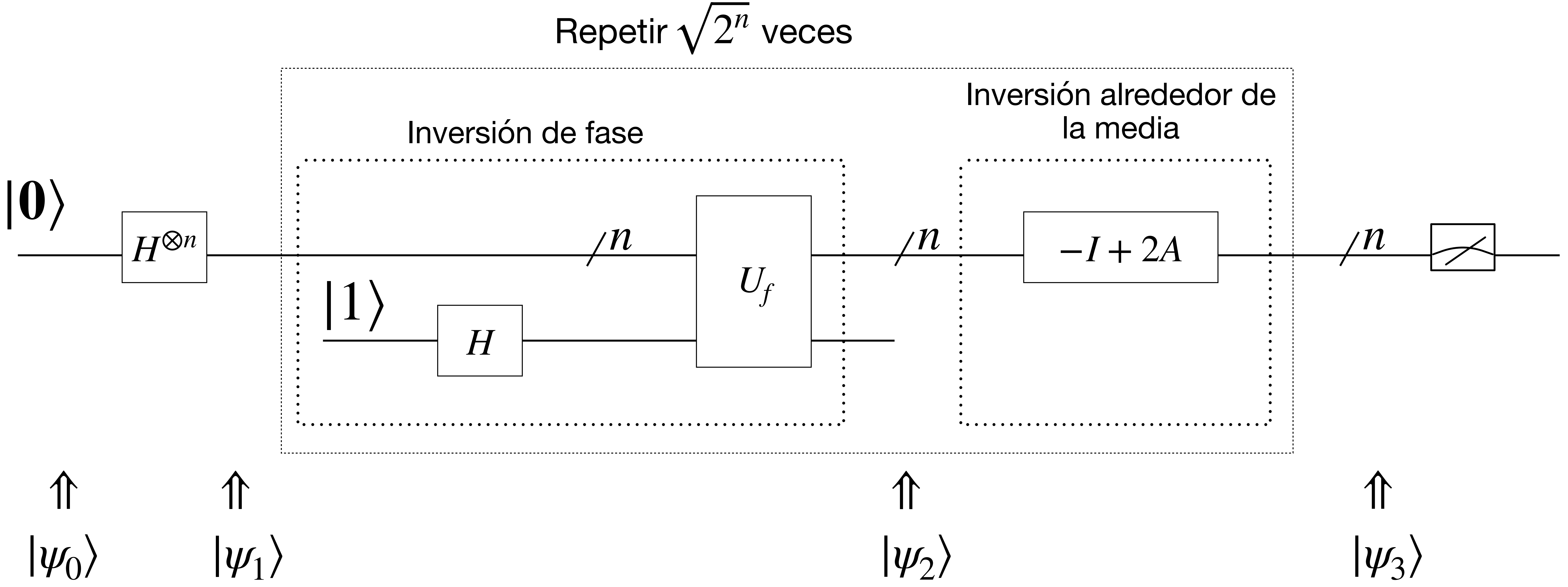
$$|\boldsymbol{x}\rangle = \frac{1}{\sqrt{8}} \sum_{z\in\{0,1\}^3} |z\rangle$$

$$|\psi_2\rangle = (-1)^{f(x)}\frac{1}{\sqrt{8}} \sum_{z\in\{0,1\}^3} |z\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$|\psi_2\rangle = [\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},-\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}},\frac{1}{\sqrt{8}}]^T \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

La inversión de fase marca el valor buscado, pero no lo separa lo suficiente para distinguirlo.

# El algoritmo de Grover

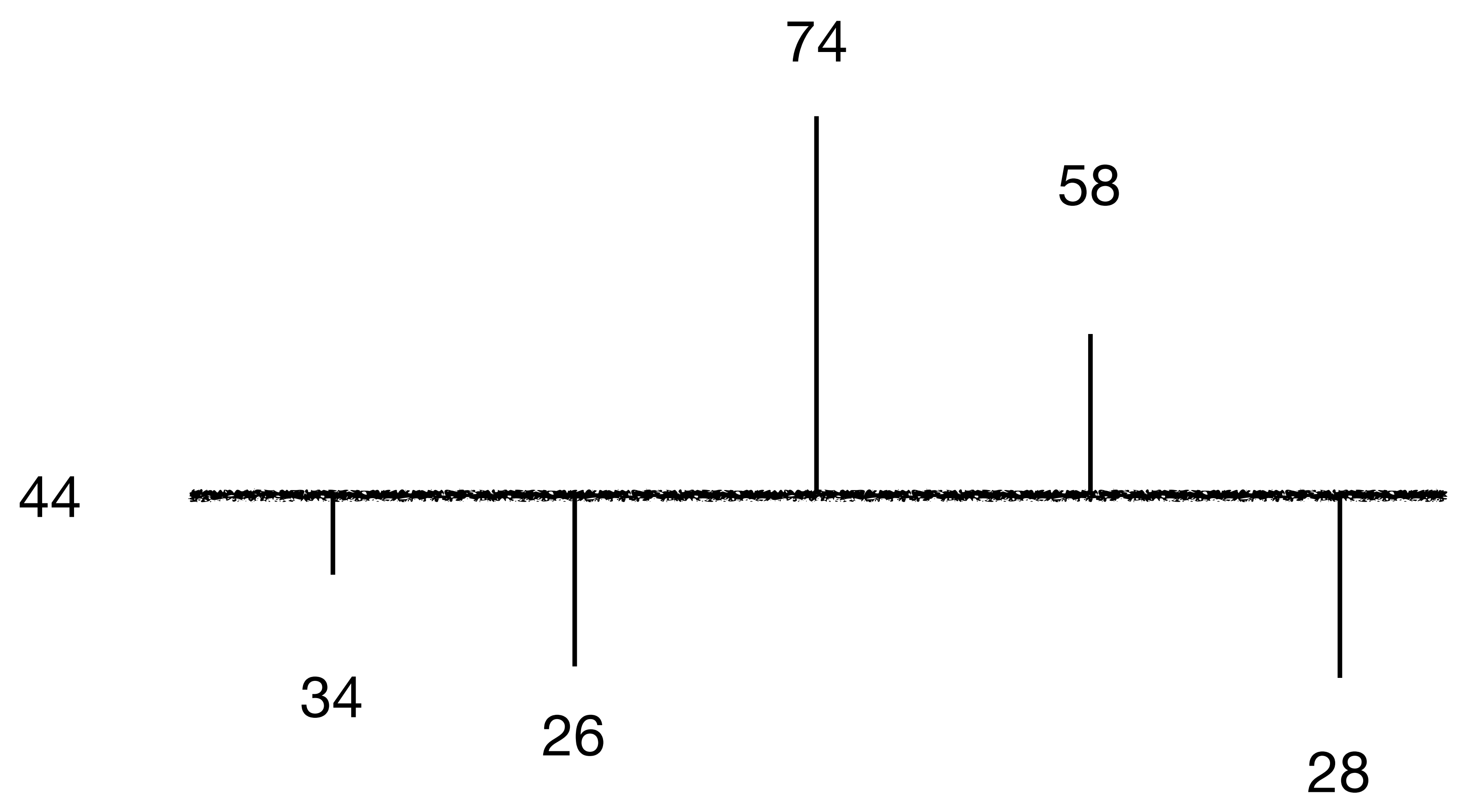


# Inversión alrededor de la media

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$V = [34,26,74,58,28]^T \qquad a = 44$$



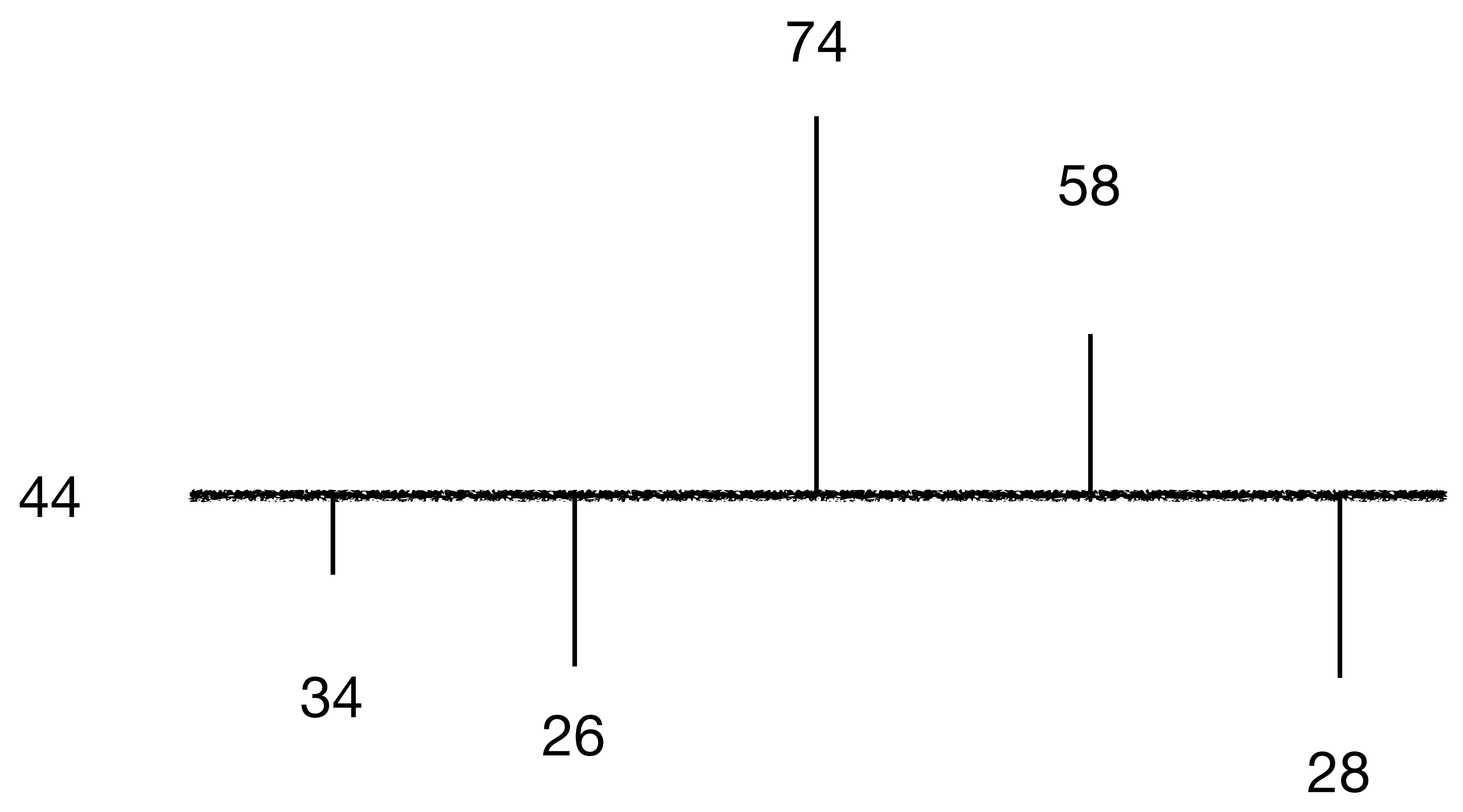

Ahora vamos a invertir cada número alrededor de la media.

- Esto no altera la media
- Solo pasa los que están arriba de la media abajo de la media, y los que están abajo de la media pasan arriba de la media.

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$V = [34,26,74,58,28]^T \qquad a = 44$$




Ahora vamos a invertir cada número alrededor de la media.

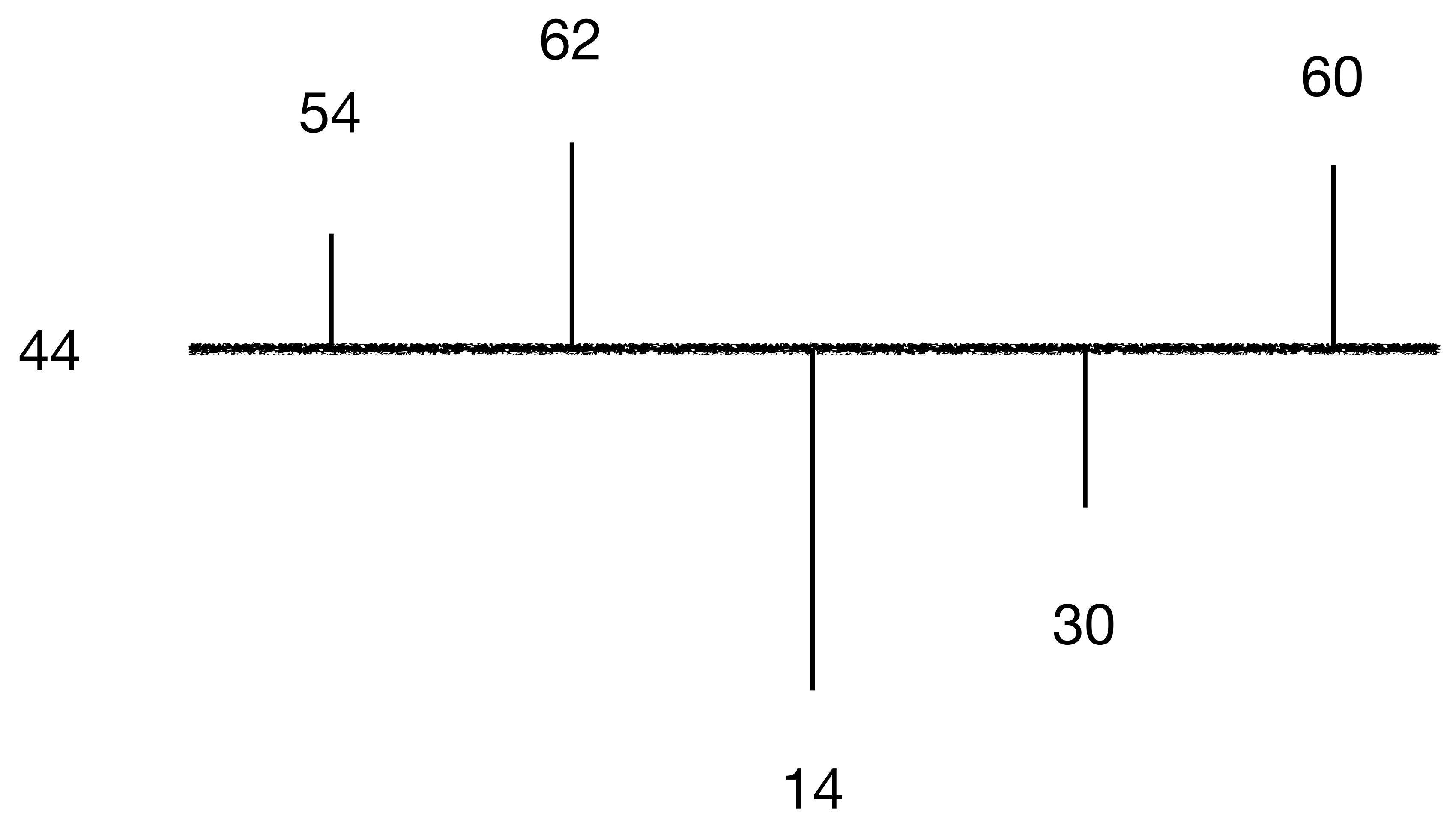
- Esto no altera la media

- Solo pasa los que están arriba de la media abajo de la media, y los que están abajo de la media pasan arriba de la media.

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$V = [54,62,14,30,60]^T \qquad a = 44$$




Ahora vamos a invertir cada número alrededor de la media.

- Esto no altera la media

- Solo pasa los que están arriba de la media abajo de la media, y los que están abajo de la media pasan arriba de la media.

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$V = [34{,}26{,}74{,}58{,}28]^T \qquad a = 44$$

$$v_r = a - (v_i - a)$$

$$v_r = 44 - (34 - 44) = 54$$

$$v_r = 44 - (26 - 44) = 62$$

$$v_r = 44 - (74 - 44) = 14$$

$$v_r = 44 - (58 - 44) = 30$$

$$v_r = 44 - (28 - 44) = 60$$

$$V_r = [54{,}62{,}14{,}30{,}60]^T$$

Ahora vamos a invertir cada número alrededor de la media.

- Esto no altera la media
- Solo pasa los que están arriba de la media abajo de la media, y los que están abajo de la media pasan arriba de la media.

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$V = [34,26,74,58,28]^T$$

$$a = 44$$

$$V_r = [54,62,14,30,60]^T$$

$$v_r = a - (v_i - a)$$

$$v_r = -v_i + 2a$$

¿Podemos escribir esto en términos de matrices?

Ahora vamos a invertir cada número alrededor de la media.

- Esto no altera la media

- Solo pasa los que están arriba de la media abajo de la media, y los que están abajo de la media pasan arriba de la media.

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$V = [34,26,74,58,28]^T \qquad a = 44$$

$$V_r = [54,62,14,30,60]^T$$

$$v_r = a - (v_i - a)$$

$$v_r = -v_i + 2a$$

$$A = \begin{bmatrix} \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \\ \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} & \frac{1}{5} \end{bmatrix}$$

$$A * V = [44,44,44,44,44]^T$$

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$V = [34, 26, 74, 58, 28]^T$  $a = 44$

$V_r = [54, 62, 14, 30, 60]^T$

$v_r = a - (v_i - a)$

$v_r = -v_i + 2a$

$$A = \begin{bmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \end{bmatrix}$$

# Inversión alrededor de la media

## Iniciemos con un ejemplo

$$v_r = a - (v_i - a)$$

$$A[i,j] = \frac{1}{2^n}$$

$$v_r = -v_i + 2a$$

$$V_r = -V_i + 2AV_i$$

$$V_r = (-I + 2A)V_i$$

$$(-I + 2A) = \begin{bmatrix} -1 + \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & -1 + \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & -1 + \frac{1}{2^n} \end{bmatrix}$$

Usted puede probar que $(-I + 2A)$ es una matriz unitaria.

# Inversión alrededor de la media

## Que pasa si la entrada está en superposición

$V_r = (-I + 2A)V_i$

$v_r = -v_i + 2a$

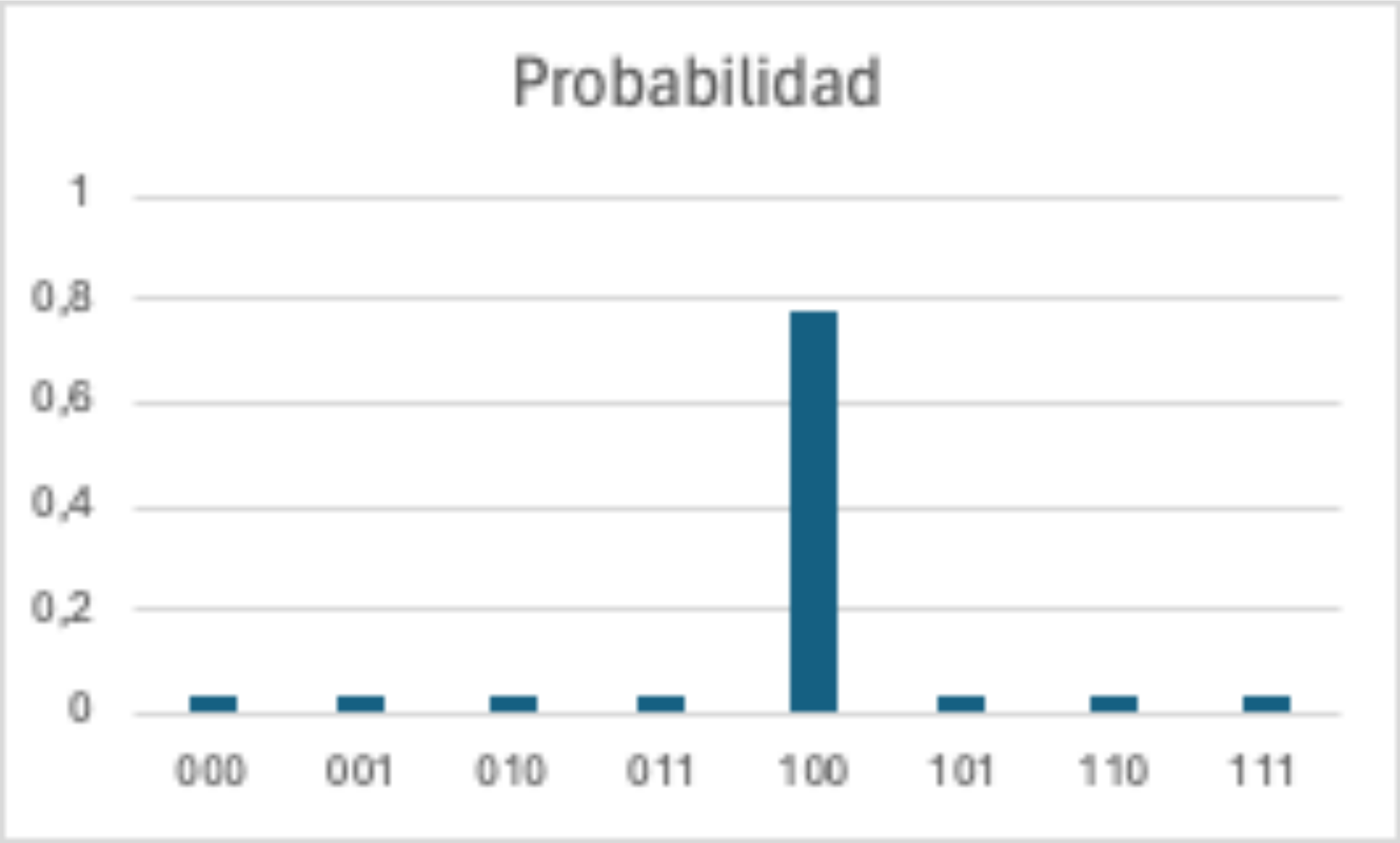
$$|\psi\rangle = [\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, -\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}]^T$$

$$a = \frac{1}{8}(\frac{7}{\sqrt{8}} - \frac{1}{\sqrt{8}}) = \frac{1}{8}\frac{6}{\sqrt{8}} = \frac{3\sqrt{2}}{16}$$

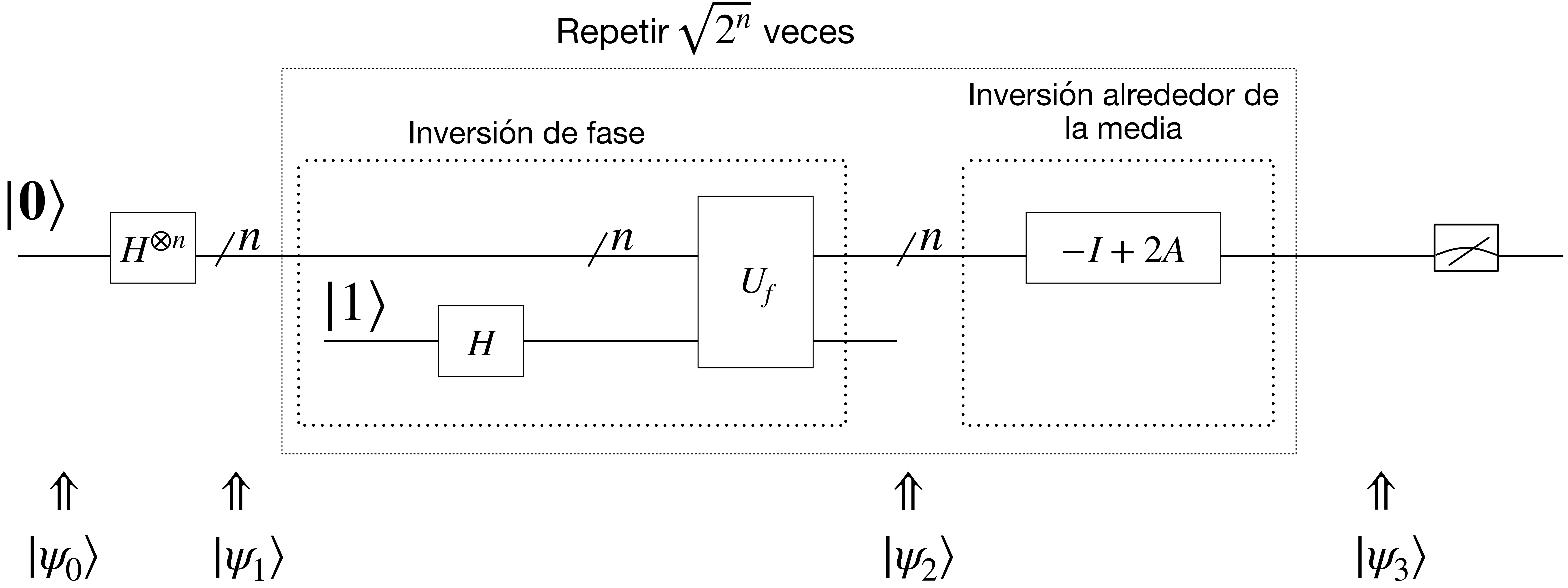
$$v_r = -\frac{1}{\sqrt{8}} + 2 * \frac{3\sqrt{2}}{16} = \frac{\sqrt{2}}{8}$$

$$v_r = \frac{1}{\sqrt{8}} + 2 * \frac{3\sqrt{2}}{16} = \frac{5\sqrt{2}}{8}$$

$$|\psi\rangle_r = [\frac{\sqrt{2}}{8}, \frac{\sqrt{2}}{8}, \frac{\sqrt{2}}{8}, \frac{\sqrt{2}}{8}, \frac{5\sqrt{2}}{8}, \frac{\sqrt{2}}{8}, \frac{\sqrt{2}}{8}, \frac{\sqrt{2}}{8}]^T$$



# El algoritmo de Grover



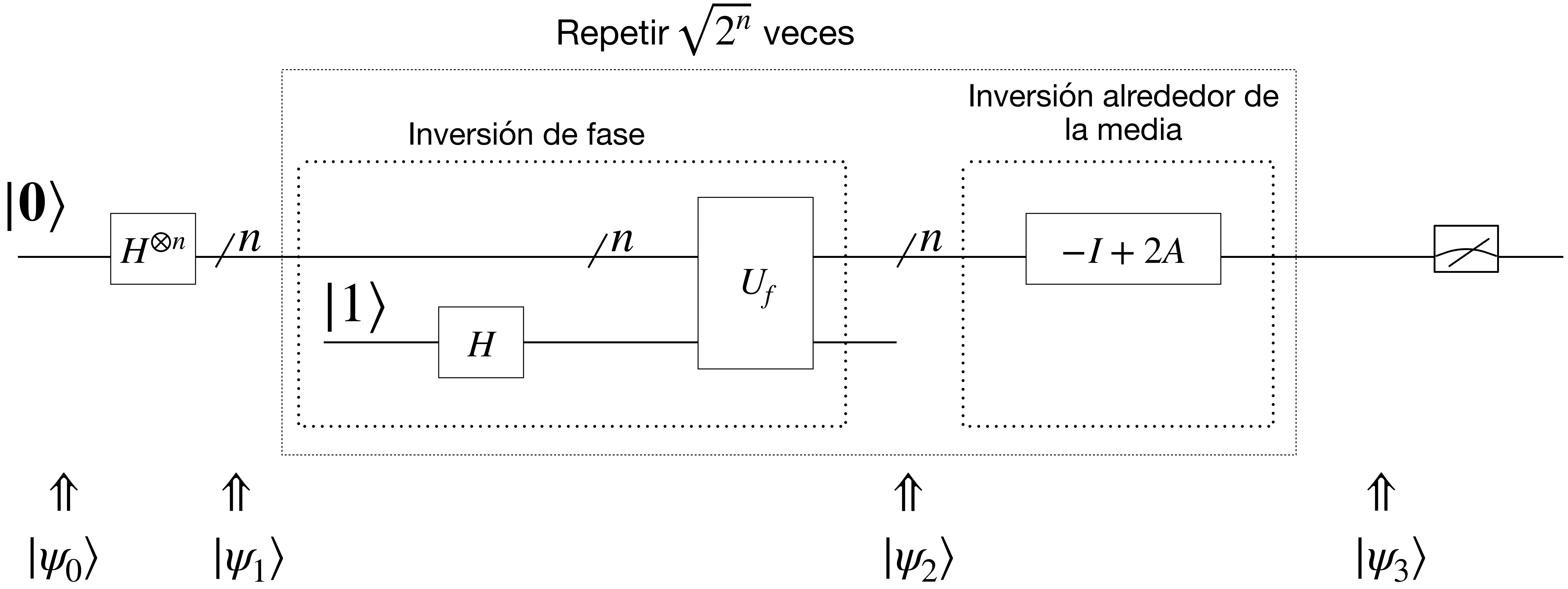
# Implementación

# El algoritmo de Grover

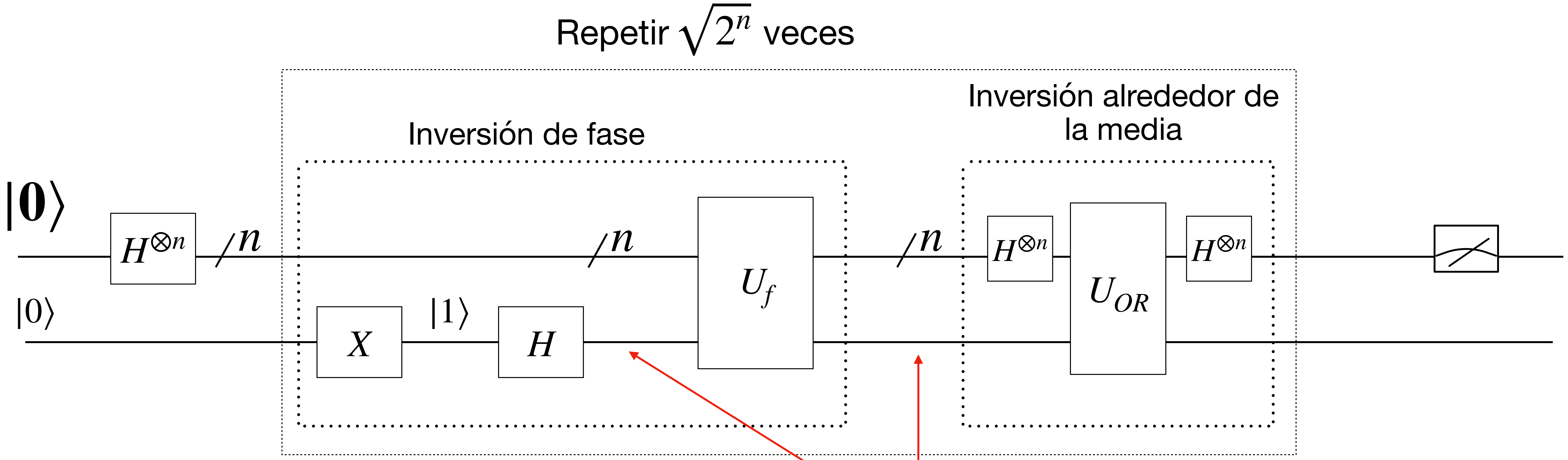
## Notas sobre implementación

- El paper original: https://arxiv.org/pdf/quant-ph/9605043.pdf
- Notas en los límites del algoritmo: https://arxiv.org/pdf/quant-ph/9605034.pdf
    - Ojo cuando el n=2, la búsqueda se hace en una iteración
    - También si hay t soluciones y $2^n/t = 4$, se pueden encontrar con una iteración.
- Notas sobre implementación en le computador de IBM:
    - https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms/grovers-algorithm

# El algoritmo de Grover

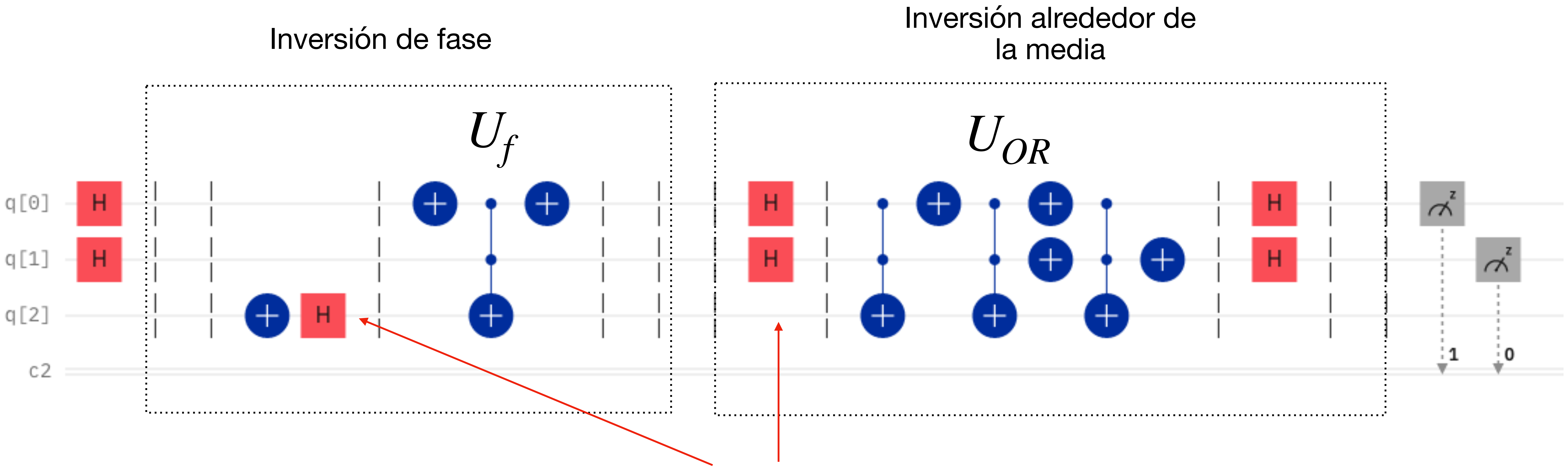


# El algoritmo de Grover




Nota: Reutilizo el valor de $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ que no cambia. Si no lo pudiera utilizar debería usar un qubit auxiliar independiente para la inversión alrededor de la media.

# Implementación con n=2



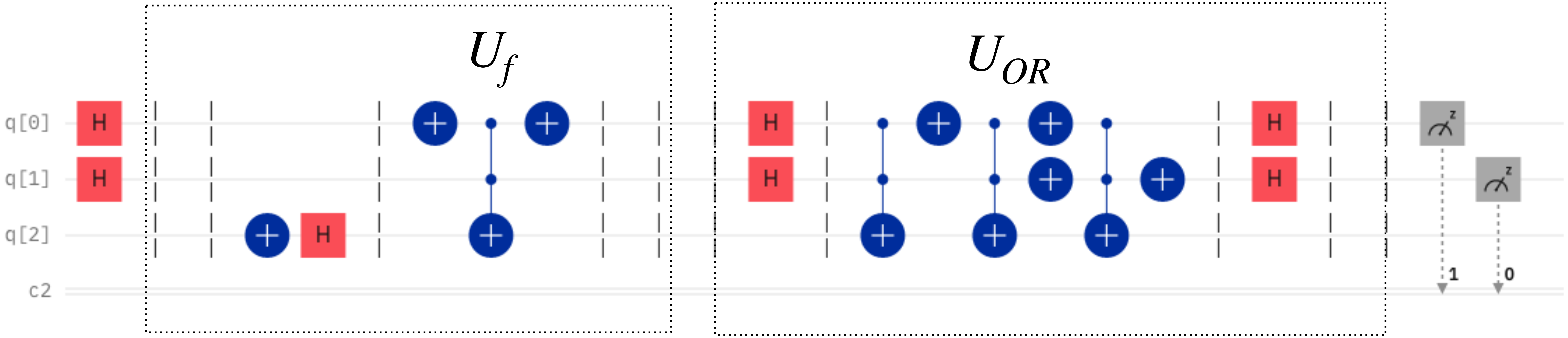

Nota: Reutilizo el valor de $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ que no cambia.

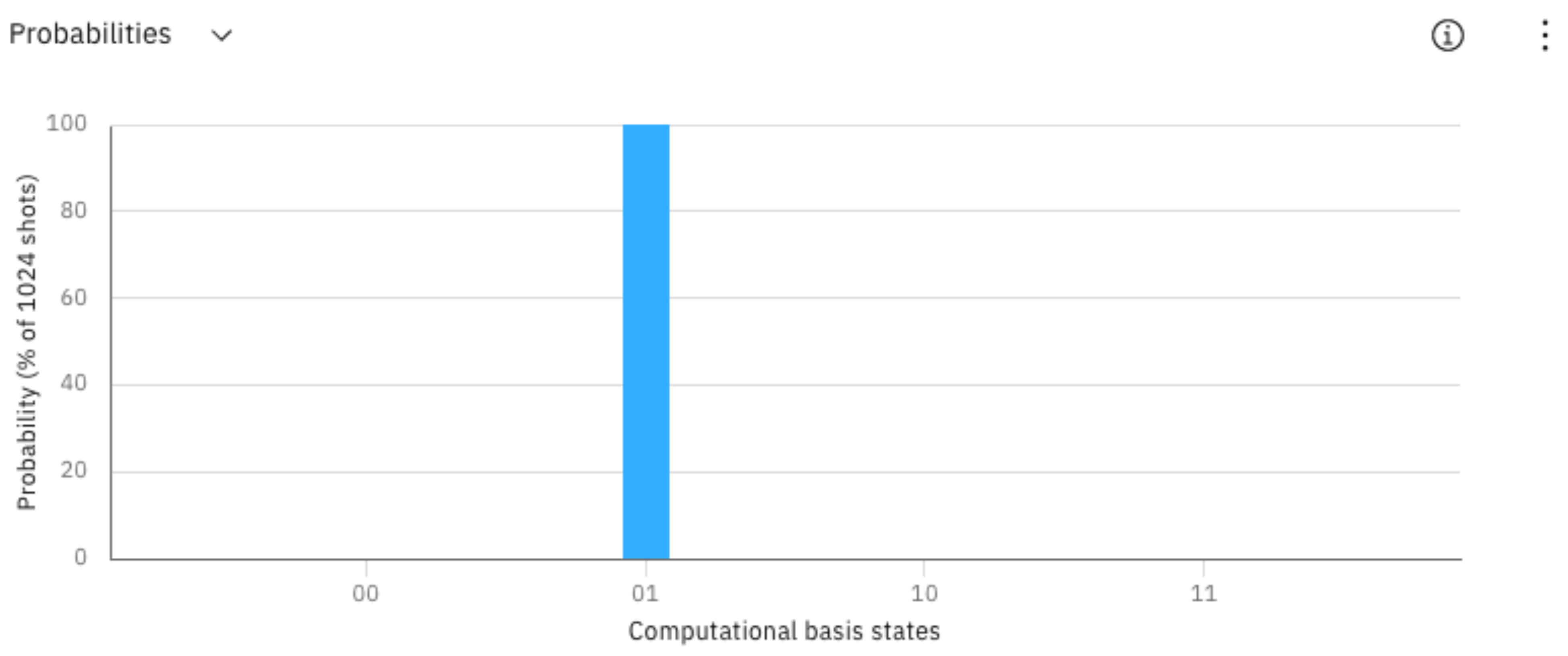
Si no lo pudiera utilizar debería usar un qubit auxiliar independiente para la inversión alrededor de la media.

# Implementación con n=2

Inversión de fase

Inversión alrededor de la media

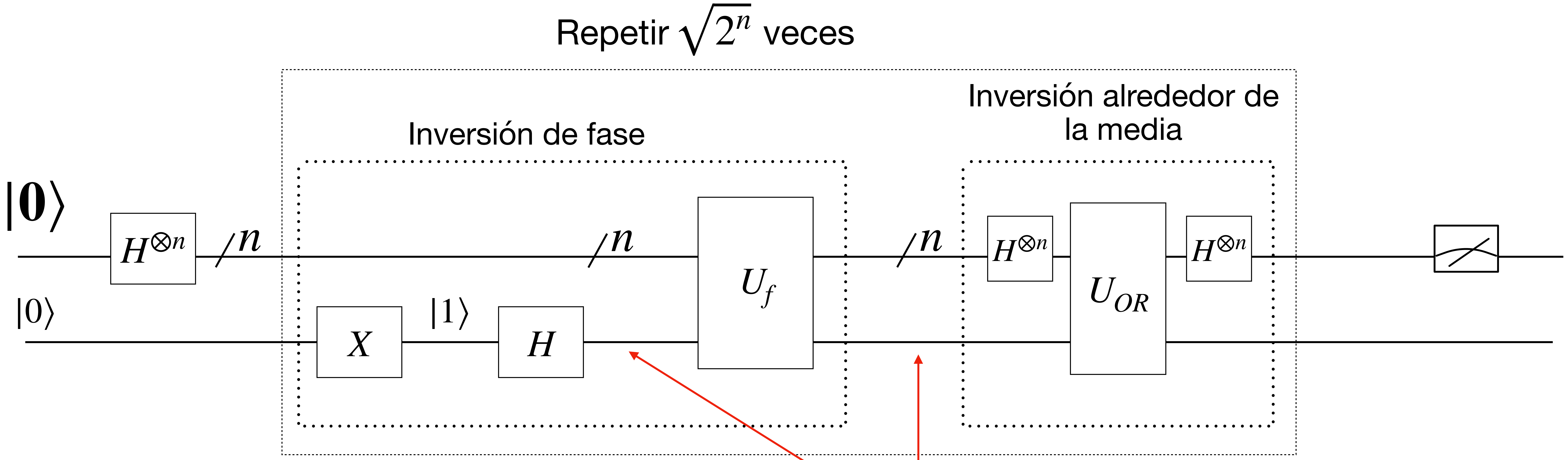



$$f(x) = \begin{cases} 1, & \text{if } x = 01 \\ 0, & \text{if } x \neq 01 \end{cases}$$

Aunque $\sqrt{2^2} = 4$, este es un caso especial del Algoritmo de Grover y está demostrado que llega con 100% de probabilidad a la respuesta correcta en una iteración.

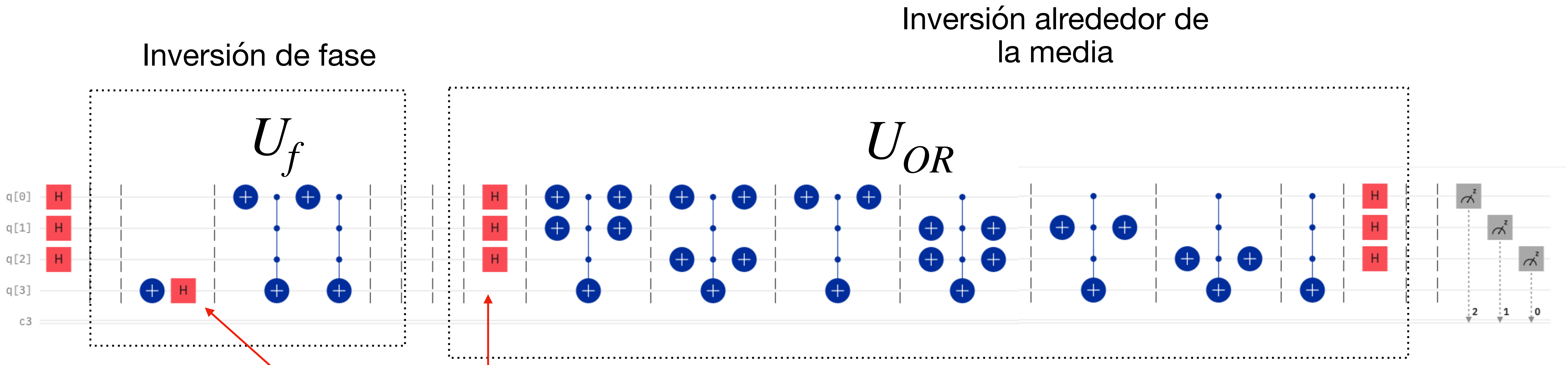
# El algoritmo de Grover con n=3 y 2 soluciones




Nota: Reutilizo el valor de $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ que no cambia.

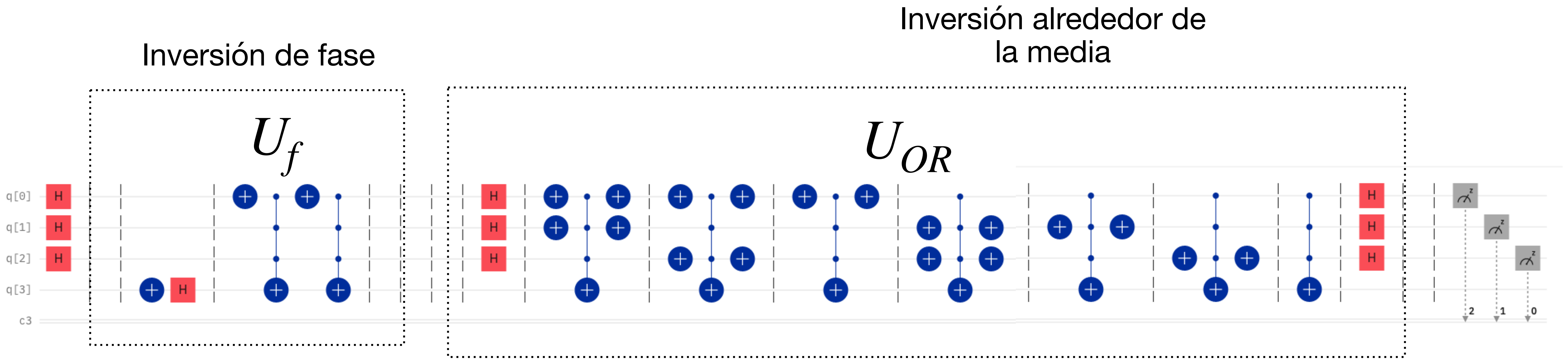
Si no lo pudiera utilizar debería usar un qubit auxiliar independiente para la inversión alrededor de la media.

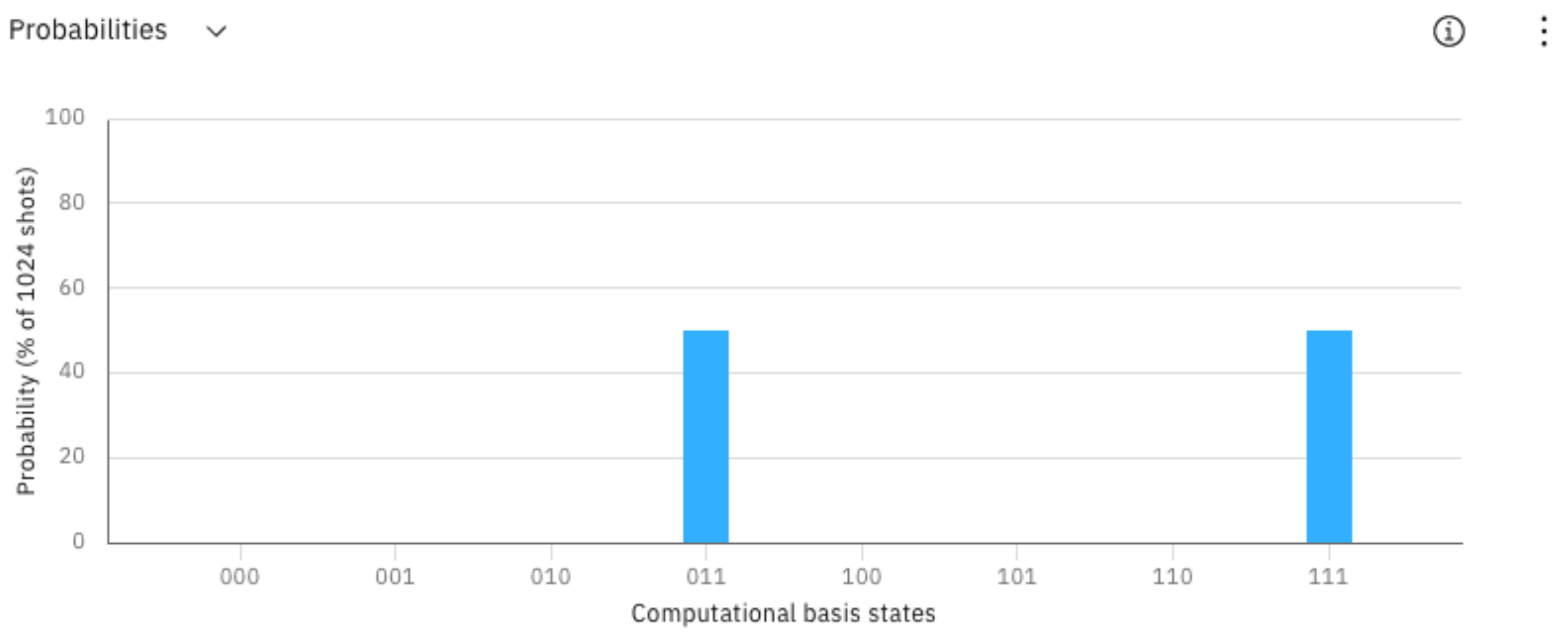
# Implementación con n=3 y 2 soluciones




Nota: Reutilizo el valor de $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ que no cambia. Si no lo pudiera utilizar debería usar un qubit auxiliar independiente para la inversión alrededor de la media.

# Implementación con n=3 y 2 soluciones




$$f(x) = \begin{cases} 1, & \text{if } x = 011 \\ 1, & \text{if } x = 111 \\ 0, & \text{if } x \neq 011 \wedge x \neq 111 \end{cases}$$

Aunque $floor(\sqrt{2^3}) = 2$, este es un caso especial del Algoritmo de Grover y está demostrado que llega con 100% de probabilidad a la respuesta correcta en una iteración. En general si $2^n/soluciones = 4$ el algoritmo necesita una sola iteración.

# ¿Preguntas?