Computación cuántica

Introducción para informáticos y matemáticos

Eduardo Sáenz de Cabezón

Índice 1

1. El modelo computacional
   - 1.1 Introdución
   - 1.2 Qubits y estados cuánticos
   - 1.3 Operaciones sobre qubits
   - 1.4 Puertas lógicas y circuitos

2. Algoritmos
   - 2.1 Consulta cuántica
   - 2.2 Deutsch
   - 2.3 Deutsch-Jozsa

Modelo computacional

- El estado de un ordenador cuántico está contenido en un registro cuántico, que se inicializa de una manera predeterminada.
- El estado del ordenador evoluciona siguiendo operaciones específicas, de acuerdo a un algoritmo.
- Al final de la computación, la información del estado del registro cuántico se obtiene mediante una operación especial llamada medida.

Un ordenador cuántico universal es Turing-completo [Deutsch'85].

Notación para qubits

La base estándar para $\mathbb{C}^2$ la denotamos $|0\rangle_1 = \binom{1}{0}$, $|1\rangle_1 = \binom{0}{1}$.
La base para $(\mathbb{C}^2)^{\otimes q}$ tiene 2^q elementos $|0\rangle_q, |1\rangle_q, \ldots, |2^q - 1\rangle_q$.
El estado de q qubits es un vector unitario en
$(\mathbb{C}^2)^{\otimes q} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$:

- El estado de un qubit es $\alpha |0\rangle + \beta |1\rangle$ con $\alpha, \beta \in \mathbb{C}$, $|\alpha^2| + |\beta^2| = 1$
- El estado de q qubits es $\sum_{j=0}^{2^q-1} \alpha_j |j\rangle_q$ con $\alpha_j \in \mathbb{C}$ y $\sum_{j=0}^{2^q-1} |\alpha_j|^2 = 1$

Estados básicos y superposición.

Decimos que q qubits están en estado básico si su estado es tal que $\exists k$ t. q. $|\alpha_k| = 1$ y $\alpha_j = 0 \forall j \neq k$.
En caso contrario diremos que los qubits están en superposición.

Estados producto y entrelazamiento.

Un estado cuántico $|\varphi\rangle \in (\mathbb{C}^2)^{\otimes q}$ es un estado producto si se puede descomponer como producto de q estados de un solo qubit.
En caso contrario diremos que es un estado en entrelazamiento.

Ejemplo

$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$ es un estado producto cuyos factores son dos copias de $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.
$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ es un estado en entrelazamiento (éste en particular se llama par EPR).

Operaciones sobre qubits

Una operación sobre q qubits (llamada puerta) es una matriz unitaria en $\mathbb{C}^{2^q \times 2^q}$. El hecho de ser unitaria es porque debe preservar la norma.

Por tanto las operaciones cuánticas son lineales y reversibles.

Ejemplos

- Bitflip gate, $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, intercambia $|0\rangle$ y $|1\rangle$.
- Phaseflip gate, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ rota π radianes la fase del estado de $|1\rangle$.

Ejemplos

- Transformación de Hadamard, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - $H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  - $H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
  - $H(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) = |0\rangle$ (interferencia)
- Controlled-not, $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ niega el segundo qubit (target) si el primero (control) es 1.
  - $CNOT|0\rangle|b\rangle = |0\rangle|b\rangle$
  - $CNOT|1\rangle|b\rangle = |1\rangle|1-b\rangle$

Un ejemplo de teleportación

Supongamos que Alice quiere enviar un qubit $\alpha_0 |0\rangle + \alpha_1 |1\rangle$ a Bob.
Ambos comparten un par EPR $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
El estado inicial conjunto es

$$(\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$$

$$\frac{1}{\sqrt{2}}\alpha_0 |000\rangle + \frac{1}{\sqrt{2}}\alpha_0 |011\rangle + \frac{1}{\sqrt{2}}\alpha_1 |100\rangle + \frac{1}{\sqrt{2}}\alpha_1 |111\rangle$$

Alice entonces aplica una puerta CNOT a sus dos qubits:

$$\frac{1}{\sqrt{2}}\alpha_0 |000\rangle + \frac{1}{\sqrt{2}}\alpha_0 |011\rangle + \frac{1}{\sqrt{2}}\alpha_1 |110\rangle + \frac{1}{\sqrt{2}}\alpha_1 |101\rangle$$

Y después una puerta de Hadamard en su primer qubit

$$\frac{1}{2}\alpha_0 |000\rangle + \frac{1}{2}\alpha_0 |100\rangle + \frac{1}{2}\alpha_0 |011\rangle + \frac{1}{2}\alpha_0 |111\rangle + \frac{1}{2}\alpha_1 |010\rangle + \frac{1}{2} - \alpha_1 |110\rangle + \frac{1}{2}\alpha_1 |001\rangle - \frac{1}{2}\alpha_1 |101\rangle$$

Este resultado lo podemos escribir de la siguiente forma

$$\frac{1}{2}|00\rangle(\alpha_0|0\rangle + \alpha_1|1\rangle) + \frac{1}{2}|01\rangle(\alpha_0|1\rangle + \alpha_1|0\rangle) + \frac{1}{2}|10\rangle(\alpha_0|0\rangle - \alpha_1|1\rangle) + \frac{1}{2}|11\rangle(\alpha_0|1\rangle - \alpha_1|0\rangle).$$

Alice entonces mide sus dos qubits y envía el resultado a Bob (dos bits) que (por un protocolo preacordado) sabe que si el segundo bit enviado por Alice es un 1 debe aplicar una puerta X en su qubit, y si el primero es un 1 debe aplicar después una puerta Z.

Por ejemplo, si Alice lee $|10\rangle$ sabemos que Bob tiene $(\alpha_0 |0\rangle - \alpha_1 |1\rangle)$. Con el resultado de Alice, Bob sabe que debe aplicar solamente Z a lo que tiene, obteniendo $(\alpha_0 |0\rangle + \alpha_1 |1\rangle)$, que es el qubit original de Alice.

Puertas lógicas y circuitos

Las puertas elementales

- X, Z, H y CNOT ya vistas
- $R_\phi = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{smallmatrix}\right)$ que rota la fase del estado $|1\rangle$ en un ángulo ϕ: $R_\phi |0\rangle = |0\rangle$, $R_\phi |1\rangle = e^{i\phi} |1\rangle$ (notar que $Z = R_\pi$).
- Puertas de Pauli: $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$ y $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, forman una base de $\mathbb{C}^{2\times 2}$ y cumplen que $XYZ = iI$.
- Puerta de Toffoli, también llamada CCNOT, es una puerta de tres qubits que niega el tercero si los dos primeros están ambos a 1.

Circuitos booleanos clásicos

- Grafo acíclico dirigido finito con puertas AND, OR y NOT
- n nodos de entrada (n bits)
- 1 o más nodos de salida

Circuitos cuánticos

- Grafo acíclico dirigido finito con puertas cuánticas de hasta 2 ó 3 qubits
- n nodos de entrada (n qubits) y algunos nodos más inicializados a $|0\rangle$ (espacio de trabajo)
- Estado final en el que algunos nodos específicos se miden.

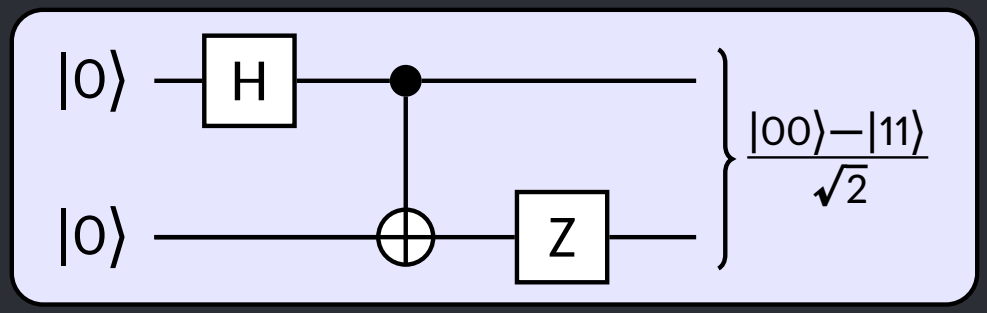


Figura: Un circuito cuántico que produce un estado entrelazado a partir de $|00\rangle$ usando una puerta Hadamard, una CNOT y una Z.

Conjuntos universales de puertas lógicas

Decimos que un conjunto de puertas lógicas $\mathscr{U}$ es universal si cualquier transformación unitaria se puede construir a partir de las puertas de $\mathscr{U}$.

- El conjunto de todas las operaciones sobre un qubit junto con CNOT es universal.
- El conjunto $\{CNOT, H, T = R_{\pi/4}\}$ es universal en el sentido de aproximación (cualquier otra tansformación unitaria se puede aproximar con precisión arbitraria).
- El conjunto $\{H, CCNOT(Toffoli)\}$ es universal para matrices unitarias con entradas reales en el sentido de aproximación.

Teorema de Solovay-Kitaev

Dado un conjunto universal de puertas cuánticas $\mathscr{U}$ y una matriz $U \in \mathbb{C}^{2q \times 2q}$ existe una constante c tal que hay una sucesión S de longitud $O(\log^c \frac{1}{\epsilon})$ de puertas de $\mathscr{U}$ que es una ϵ-aproximación de U.

Clases de complejidad

Complejidad Clásica

P: es la clase de los problemas de decisión que pueden ser resueltos por una máquina de Turing determinista en tiempo polinomial.

NP: es la clase de los problemas para los que las instancias en las que la solución es SÍ tienen una prueba verificable en tiempo polinomial.

Clases de complejidad

Complejidad Clásica Probabilística

BPP: es la clase de los problemas de decisión que pueden ser resueltos por una máquina de Turing determinista en tiempo polinomial con un error acotado por 1/3 en todas las instancias.

MA: es la clase de los problemas para los que las instancias en las que la solución es SÍ existe una prueba en tiempo polinomial que puede convencer a un verificador en tiempo polinomial con probabilidad alta. Y si la solución es NO, toda prueba polinomial es rechazada con probabilidad alta.

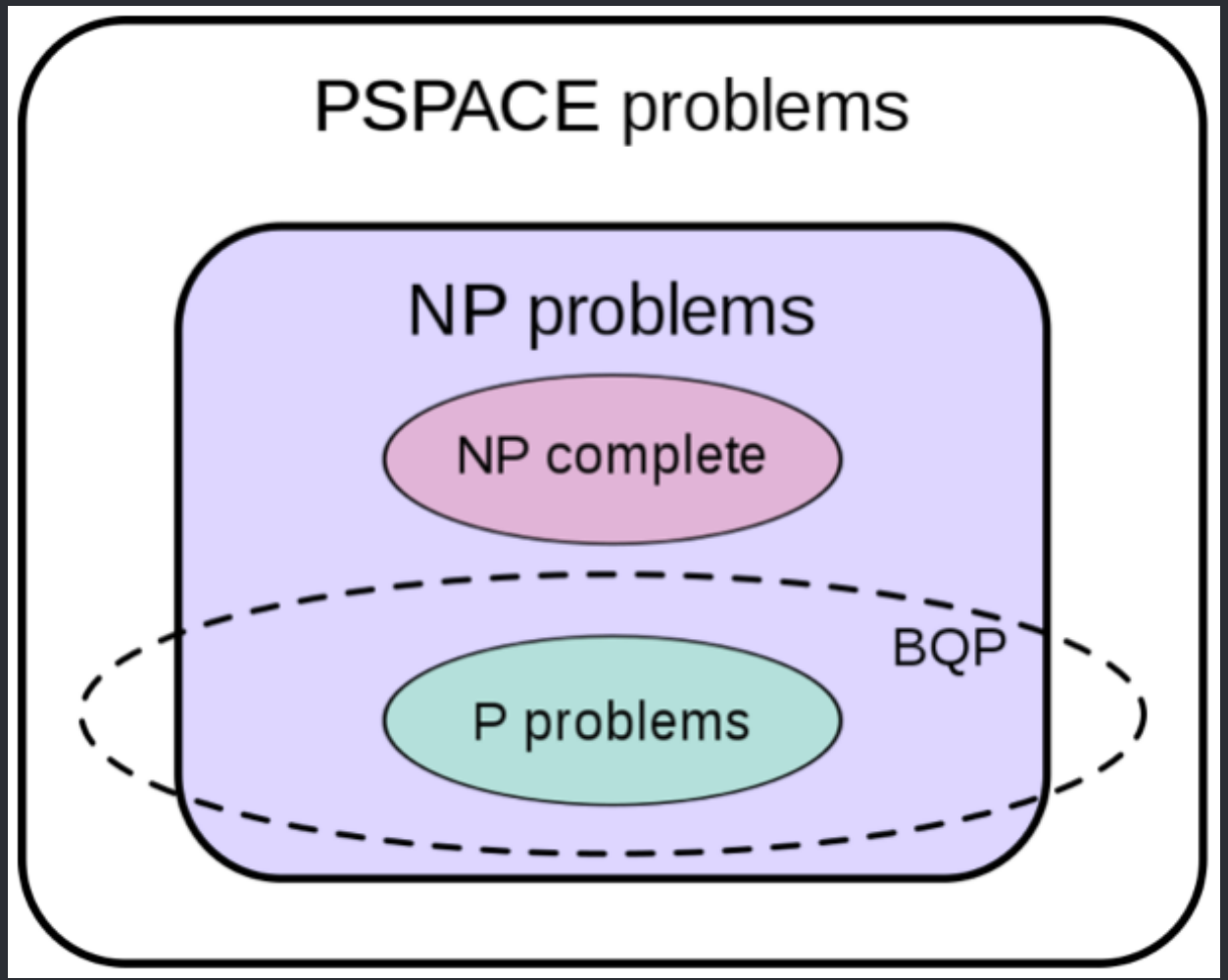
Clases de complejidad

Complejidad Cuántica

BQP: es la clase de los problemas de decisión que pueden ser resueltos por una ordenador cuántico en tiempo polinomial con un error acotado por 1/3 en todas las instancias.

QMA: es la clase de los problemas para los que las instancias en las que la solución es SÍ existe una prueba cuántica en tiempo polinomial que puede convencer a un verificador cuántico en tiempo polinomial con probabilidad alta. Y si la solución es NO, toda prueba polinomial cuántica es rechazada con probabilidad alta.

Clases de complejidad



Índice 2

1. El modelo computacional
    1.1 Introdución
    1.2 Qubits y estados cuánticos
    1.3 Operaciones sobre qubits
    1.4 Puertas lógicas y circuitos

2. Algoritmos
    2.1 Consulta cuántica
    2.2 Deutsch
    2.3 Deutsch-Jozsa

Consulta cuántica

Un tipo de puerta cuántica muy usada en los algoritmos es la consulta cuántica 'quantum query'.
Sea $N = 2^n$ y $x = (x_1, \ldots, x_n) \in \{0,1\}^N$ un input de tamaño N.
Consideramos la operación $O_x : |i, 0\rangle \mapsto |i, x_i\rangle$, que dado un input i de n qubits (adress bits) devuelve el qubit x_i, al último qubit del input lo llamamos target bit. La puerta cuántica correspondiente es

$$O_x |i, b\rangle \longrightarrow |i, b \oplus x_i\rangle$$

En notación matricial es una matriz de permutación, y por tanto es unitaria.

Consulta cuántica

Podemos aplicar O_x a una superposición de varios i. Cada aplicación de O_x se llama una consulta, y el número de consultas necesarias es una medida importante en la aplicación de algoritmos cuánticos.
En concreto podemos construir consultas de la forma $|i\rangle \mapsto (-1)^{x_i} |i\rangle$ si ponemos el target bit a $|-\rangle$, donde $|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
Esta transformación suele denotarse $O_{x,\pm}$.

$$O_{x,\pm} = O_x(|i\rangle |-\rangle) = |i\rangle \frac{1}{\sqrt{2}}(|x_i\rangle - |1 - x_i\rangle) = (-1)^{x_i} |i\rangle |-\rangle$$

El algoritmo de Deustsch

El problema

Dada una función $f : \{0, 1\} \to \{0, 1\}$ queremos saber si f es constante o equilibrada, es decir, si $f(0) = f(1)$ ó $f(0) \neq f(1)$.

Algoritmo clásico:

```
return (ev(f,0)==ev(f,1))
```

Necesita dos evaluaciones de f pero realmente sólo buscamos un bit de información: $f(0) \oplus f(1)$.

El algoritmo de Deutsch

Algortimo cuántico:

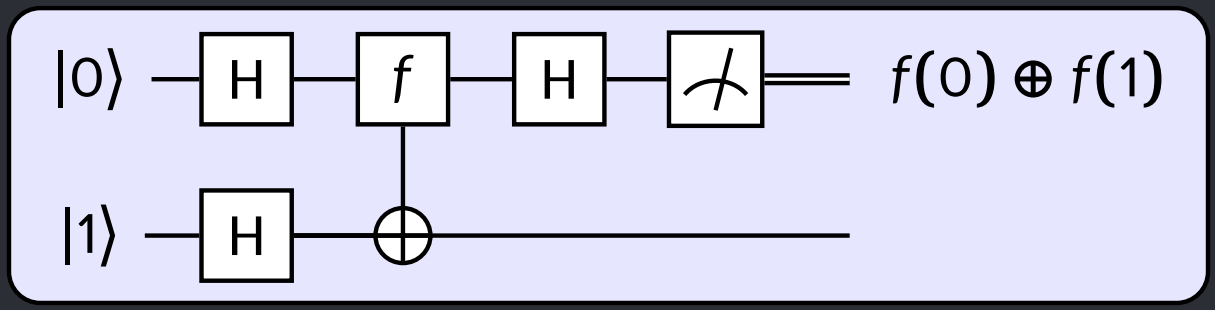


Figura: Circuito cuántico del algoritmo de Deutsch.

El algoritmo hace un único uso de la evaluación cuántica de f que es una consulta $O_{f(x)}$ o equivalntmente una puerta denotada por U_f y dada por una matriz unitaria (para cualquier f) cuyo comportamiento es $|xy\rangle \rightarrow |x\rangle\,|y \oplus f(x)\rangle$ con $y \in \{0, 1\}$.

El algoritmo de Deutsch

Notación: Base $|\pm\rangle$:

$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Demostración del algoritmo:

Primera puerta:

$$|01\rangle \xrightarrow{H\otimes H} \frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$$

El algoritmo de Deutsch

Segunda puerta:

$$\frac{1}{\sqrt{2}}|0\rangle|-\rangle+\frac{1}{\sqrt{2}}|1\rangle|-\rangle \xrightarrow{U_f} \left(\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\right)\right)|-\rangle$$

El algoritmo de Deutsch

Tercera puerta:

$$\left(\frac{1}{\sqrt{2}} \left((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) \right) |-\rangle \longrightarrow |f(0) \oplus f(1)\rangle \, |1\rangle$$

Con una sola evaluación cuántica de f obtenemos el bit de información buscado, que leemos al medir el estado del primer qubit tras la ejecución del algoritmo.

El algoritmo de Deustsch-Jozsa

El problema

Tenemos una función $f : \{0,1\}^n \to \{0,1\}$ que es de uno de estos dos tipos:

- Constante:

$$f(x) = 0 \, \forall x \in \{0,1\}^n \text{ o bien } f(x) = 1 \, \forall x \in \{0,1\}^n$$

- Equilibrada:

$$|\{x \in \{0,1\}^n \text{ t.q. } f(x) = 0\}| = |\{x \in \{0,1\}^n \text{ t.q. } f(x) = 1\}| = 2^{n-1}$$

queremos saber si f es constante o equilibrada.

El algoritmo de Deustsch-Jozsa

Algoritmos clásicos:

- Un algoritmo clásico determinista necesita $2^{n-1} + 1$ evaluaciones de f en el peor caso
- Un algoritmo clásico probabilístico puede obtener con k evaluaciones una respuesta correcta siempre si f es constante y con probabilidad $1 - \frac{1}{2^k}$ si f es equilibrada.

Algoritmo cuántico:

El algoritmo de Deutsch-Jozsa utiliza una sola evaluación cuántica de f y n medidas para un resultado correcto siempre.

El algoritmo de Deutsch-Jozsa

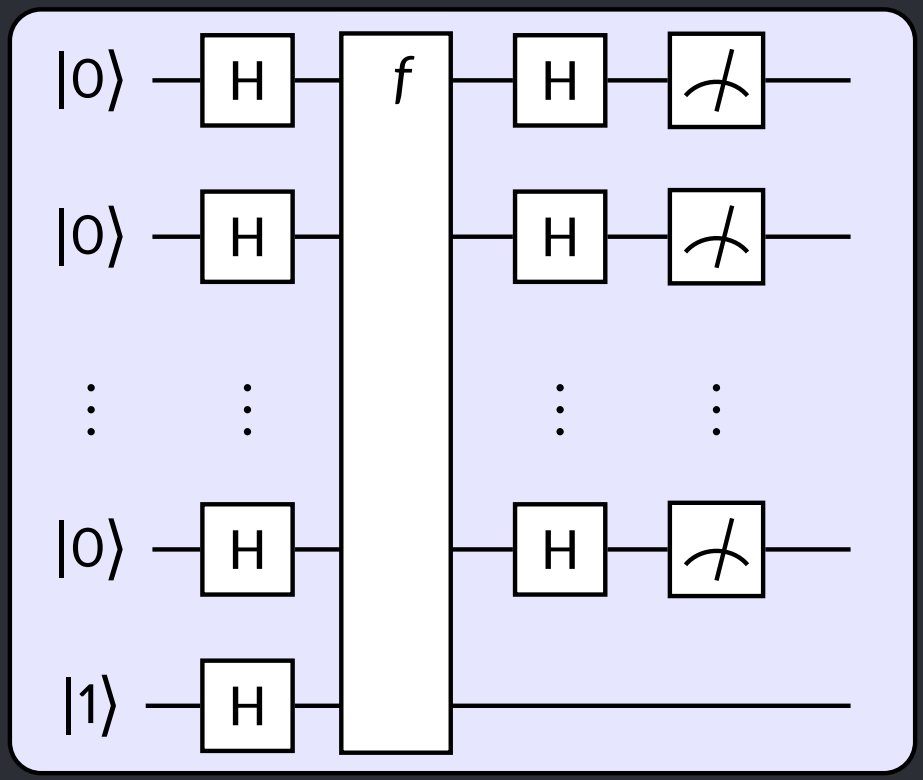


Figura: Circuito cuántico del algoritmo de Deutsch-Jozsa.

El algoritmo es una generalización del algoritmo de Deutsch.

- El algoritmo de Deutsch-Jozsa supone una mejora exponencial sobre cualquier algoritmo clásico determinista
- El algoritmo de Bernstein-Vazirani (variante de Deutsch-Jozsa) supone una mejora polinomial sobre cualquier algoritmo clásico probabilístico con probabilidad de error $< 1/3$
- El algoritmo de Simon supone una mejora exponencial sobre algoritmos clásicos probabilísticos con error acotado