Algoritmo de Deutsch–Jozsa

Computación Cuántica: Algorítmica y Software

Joaquín Keller

2026 UCV

Definiciones

$f : \{0,1\}^n \to \{0,1\}$ $\qquad$ 2^{2^n} funciones

f es *constante* ssi $\exists k \in \{0,1\}\ \forall x \in \{0,1\}^n\ f(x) = k$

2 funciones constantes

f es *equilibrada* ssi $|\{x \in \{0,1\}^n | f(x) = 0\}| = |\{x \in \{0,1\}^n | f(x) = 1\}|$

$\frac{2^n!}{2^{n-1}!^2}$ funciones equilibradas

Hay muchas funciones que no son ni constantes ni equilibradas.

El problema

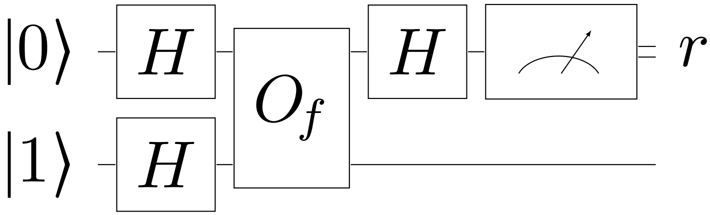
Dada una función $f : \{0,1\}^n \to \{0,1\}$ constante o equilibrada, determinar en cuál categoría está

Complejidad algorítmica: cuantas veces se llama la función f
f es una caja negra, no se considera su complejidad algorítmica

Algoritmo clásico: Evaluar f sobre la mitad de $\{0,1\}^n$ más 1 elemento
Si todos los valores son idénticos, f es constante, si no, f es equilibrada

$2^{n-1}+1$ evaluaciones de $f \Rightarrow$ complejidad algorítmica: $O(2^n)$

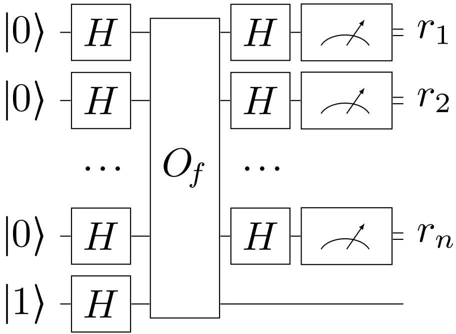
Circuito cuántico para Deutsch–Jozsa, $n = 1$



O_f : Oráculo para f

$$\begin{cases} r = 0 : f \text{ constante} \\ r = 1 : f \text{ equilibrada} \end{cases}$$

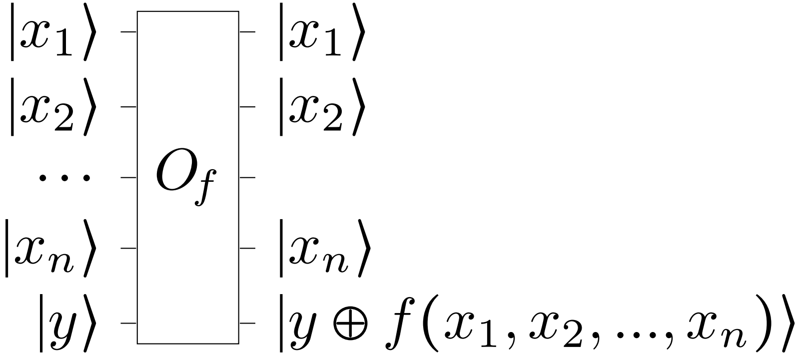
Circuito cuántico para Deutsch–Jozsa, $n \in \mathbb{N}$



O_f : Oráculo para f

$$\begin{cases} \forall i \; r_i = 0 : f \text{ constante} \\ \exists i \; r_i = 1 : f \text{ equilibrada} \end{cases}$$

Oráculo



$y \in \{0,1\} \qquad x_i \in \{0,1\} \qquad f : \{0,1\}^n \to \{0,1\}$

Notación entera para los vectores de la base

n: Número de qubits $\quad\quad$ $\underline{k}$: Representación binaria de k en n bits

$$k \in \mathbb{N} \quad 0 \leq k < 2^n$$

$$|\underline{k}\rangle = |k_1\rangle \otimes |k_2\rangle \otimes \ldots \otimes |k_n\rangle = \bigotimes_{j=1}^{n} |k_j\rangle = |k_1 k_2 \ldots k_n\rangle$$

$$\begin{aligned}
|\underline{0}\rangle &= |000\ldots000\rangle \\
|\underline{1}\rangle &= |000\ldots001\rangle \\
|\underline{2}\rangle &= |000\ldots010\rangle \\
&\ldots \\
|\underline{2^n-2}\rangle &= |111\ldots110\rangle \\
|\underline{2^n-1}\rangle &= |111\ldots111\rangle
\end{aligned}$$

Oráculo

$$\begin{array}{c} |\underline{x}\rangle \\ |y\rangle \end{array} \; \boxed{O_f} \; \begin{array}{c} |\underline{x}\rangle \\ |y \oplus f(x)\rangle \end{array}$$

$$O_f\left(|\underline{x}\rangle \otimes |y\rangle\right) = |\underline{x}\rangle \otimes |y \oplus f(x)\rangle$$

$$y \in \{0,1\} \qquad x \in \{0,1\}^n \qquad f : \{0,1\}^n \to \{0,1\}$$

$O_f O_f = \mathbb{I}$ (ver demostración con $n = 1$)

$O_f = O_f^{-1}$ O_f es hermitiano (unitario y autoinversa)

Transformación de Hadamard (1)

$$H^{\otimes n} = \overbrace{H \otimes H \otimes \ldots \otimes H}^{n} = \bigotimes_{n} H$$

$$H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \qquad H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \qquad H|b\rangle = \frac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} (-1)^{bx}|x\rangle \qquad b \in \{0,1\}$$

$$H^{\otimes n}|\underline{0}\rangle = (H|0\rangle)^{\otimes n} = \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)^{\otimes n}$$

$$= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} |\underline{l}\rangle$$

Transformación de Hadamard (2)

$$H^{\otimes n}\left|\underline{k}\right\rangle = \left(H\left|\underline{k}\right\rangle\right)^{\otimes n} = \frac{1}{\sqrt{2^n}}\bigotimes_{j=1}^{n}\Big(\left|0\right\rangle + (-1)^{k_j}\left|1\right\rangle\Big)$$

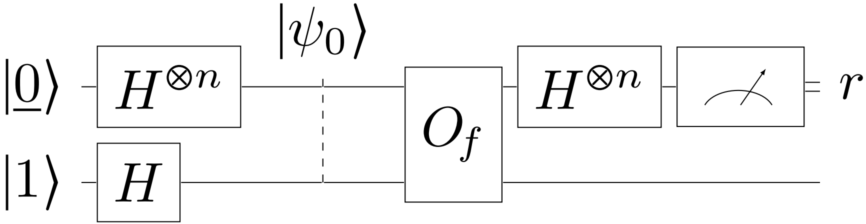
$$= \frac{1}{\sqrt{2^n}}\left(\left|0\right\rangle + (-1)^{k_1}\left|1\right\rangle\right)\otimes\left(\left|0\right\rangle + (-1)^{k_2}\left|1\right\rangle\right)\otimes\ldots\otimes\left(\left|0\right\rangle + (-1)^{k_n}\left|1\right\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}\prod_{j=1}^{n}(-1)^{k_j l_j}\left|\underline{l}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}(-1)^{\sum_{j=1}^{n}k_j l_j}\left|\underline{l}\right\rangle \qquad x^a x^b = x^{a+b}$$

$$= \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}(-1)^{\bigoplus_{j=1}^{n}k_j l_j}\left|\underline{l}\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}(-1)^{k\odot l}\left|\underline{l}\right\rangle$$

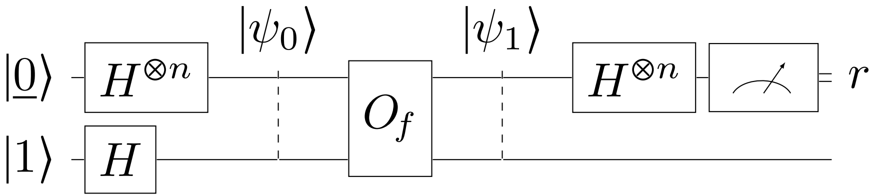
$$k\odot l = \bigoplus_{j=1}^{n}k_j l_j = k_1 l_1 \oplus k_2 l_2 \oplus \ldots \oplus k_n l_n$$

Circuito cuántico para Deutsch–Jozsa



$$|\psi_0\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} |\underline{l}\rangle\right) \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} \left(|\underline{l}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} |\underline{l}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

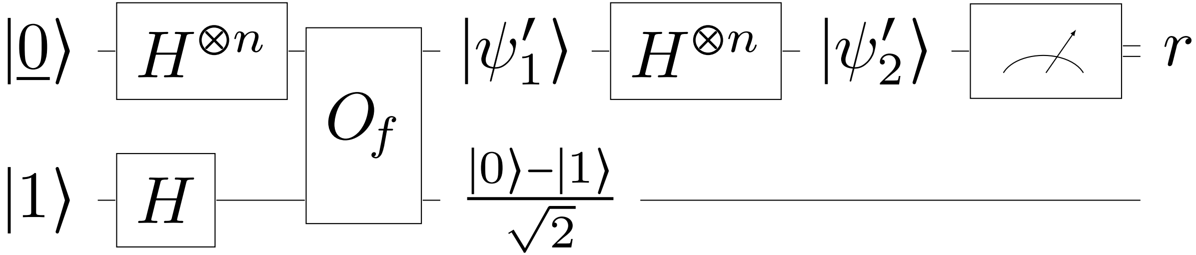


$$|\psi_1\rangle = O_f\,|\psi 0\rangle = O_f\left(\frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}|l\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1} O_f\left(|l\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}|l\rangle \otimes \frac{|0\oplus f(l)\rangle-|1\oplus f(l)\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}(-1)^{f(l)}\,|l\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \left(\frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1}(-1)^{f(l)}\,|l\rangle\right) \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$|0 \oplus f(l)\rangle - |1 \oplus f(l)\rangle = (-1)^{f(l)}(|0\rangle - |1\rangle)$$



$$|\psi_1'\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} (-1)^{f(l)} |\underline{l}\rangle \qquad |\psi_2'\rangle = H^{\otimes n} |\psi_1'\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} (-1)^{f(l)} H^{\otimes n} |\underline{l}\rangle$$

$$|\psi_2'\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} (-1)^{f(l)} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} (-1)^{k \odot l} |\underline{k}\rangle$$

$$= \frac{1}{2^n} \sum_{l=0}^{2^n-1} \sum_{k=0}^{2^n-1} (-1)^{f(l)+k\odot l} |\underline{k}\rangle = \frac{1}{2^n} \sum_{k=0}^{2^n-1} |\underline{k}\rangle \sum_{l=0}^{2^n-1} (-1)^{f(l)+k\odot l}$$

$$|\psi_2'\rangle = \frac{1}{2^n}\sum_{k=0}^{2^n-1}|\underline{k}\rangle \sum_{l=0}^{2^n-1}(-1)^{f(l)+k\odot l} \qquad r = \mathcal{M}(|\psi_2'\rangle) \in [0,1]^{2^n}$$

La amplitud de probabilidad de $|\underline{0}\rangle$ es

$$\alpha = \frac{1}{2^n}\sum_{l=0}^{2^n-1}(-1)^{f(l)+0\odot l} = \frac{1}{2^n}\sum_{l=0}^{2^n-1}(-1)^{f(l)}$$

Si f es constante $\alpha = \pm 1$ y la probabilidad $P(r = \underline{0}) = |\alpha|^2 = 1$

Si f es equilibrada, $\alpha = 0$ y la probabilidad $P(r = \underline{0}) = |\alpha|^2 = 0$

$$2^n\alpha = \sum_{\{f(l)=0\}}(-1)^0 + \sum_{\{f(l)=1\}}(-1)^1 = |\{f(l) = 0\}| - |\{f(l) = 1\}| = 0$$