

Kvantumalgoritmusok

Kvantum algoritmusok és kvantum komplexitás, Deutsch algoritmus, Deutsch-Józsa áramkör, Deutsch-Józsa algoritmus

Kvantumalgoritmus

Egy *kvantumalgoritmus* egy valószínűségi algoritmus a következő plusz tulajdonságokkal:

1. tartalmaz kvantum áramköröket
2. tartalmaz más kvantumalgoritmust alciklusként

Időkomplexitás

Legyen Q egy kvantum áramkör.

1. Ekkor Q *futási ideje* vagy *időkomplexitása* a mérete, azaz a bement qubitek száma plusz a kapuk száma.
2. Továbbá, Q *térkomplexitása* a bemenet qubitek száma plusz a segéd qubitek száma.

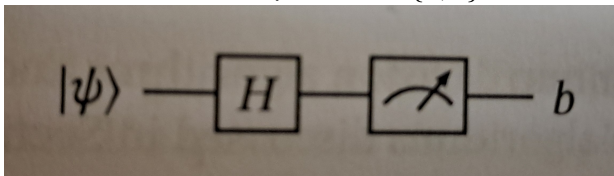
Példa: Kvantum éremdobás

Input: $\emptyset$

Output: 0 or 1

1. éremdobás
2. $|\psi\rangle \leftarrow |0\rangle$
3. $b \leftarrow$ KvantumÉremdobás $|\psi\rangle$
4. return b
5. end

A kvantum éremdobás áramköre, ahol $|\psi\rangle$ egy egy-qiubit-es kvantumállapot és $b \in \{0, 1\}$:



Deutsch algoritmus - Klasszikus verzió

Bevezette: David Deutsch (1985), átdolgozta: Cleve et al. (1998)

Tekintsünk egy $f : \{0, 1\} \rightarrow \{0, 1\}$ függvényt. Az f függvény "fekete doboz" számunkra, azaz nem tudjuk pontosan mit számol. Csak a bemeneteket és kimeneteket tudjuk vizsgálni.

Azt mondjuk, hogy f *konstans*, ha $f(0) = f(1)$, tehát $f(0) \oplus f(1) = 0$, és f *kiegyensúlyozott* ha $f(0) \neq f(1)$, és így $f(0) \oplus f(1) = 1$.

Példák

A következő függvényértékek lehetségesek

$$f(0) = 0, f(1) = 0$$

$$f(0) = 1, f(1) = 0$$

$$f(0) = 0, f(1) = 1$$

$$f(0) = 1, f(1) = 1$$

Az első és negyedik esetben f konstans. A második és harmadik esetben f kiegyensúlyozott.

Deutsch probléma

Ha van hozzáférésünk egy f függvény fekete dobozához, azaz ki tudjuk számolni a függvényértékeket, akkor döntsük el, hogy f konstans-e vagy kiegyensúlyozott-e.

Input: Fekete doboz, mely kiszámolja egy $f : \{0, 1\} \rightarrow \{0, 1\}$ függvényhez tartozó függvényértékeket.

Output: $f(0) \oplus f(1)$

Ez a probléma természetesen egyszerűen megoldható, kettő darab lekérdezéssel: Ha tudjuk $f(0)$ -t, akkor még $f(1)$ -et is kell tudnunk, ahhoz hogy el tudjuk dönteni, az f kiegyensúlyozott-e vagy sem.

A probléma kvantum megfelelőjében pedig elég lesz egy lekérdezés, ahhoz hogy el tudjuk dönteni, az f kiegyensúlyozott-e vagy sem.

A Deutsch probléma kvantum verziója

Az f függvényt helyettesítünk egy unitér U operátorral.

$$U_f : \mathbb{H}_2 \rightarrow \mathbb{H}_2$$

$$U_f : |x\rangle |y\rangle \rightarrow |x\rangle |f(x) \oplus y\rangle = |x\rangle X^{f(x)} |y\rangle$$

Input: Egy fekete doboz, mely kiszámolja az egy $f : \{0, 1\} \rightarrow \{0, 1\}$ függvényhez tartozó U_f operátort

Output: $f(0) \oplus f(1)$

A megoldás

Az Input állapot

$$|\psi_0\rangle = |0\rangle |1\rangle$$

Ezután egy Hadamard operátor hat az első qubiten és a második qubiten, mely a következő állapotot eredményez:

$$|\psi_1\rangle = |x_+\rangle |x_-\rangle = \frac{1}{\sqrt{2}}(|0\rangle |x_-\rangle + |1\rangle |x_-\rangle)$$

Ebben a szuperpozícióban a két állapot $|0\rangle |x_-\rangle$ és $|1\rangle |x_-\rangle$ egyenlő súlyú.

Most a fázisvisszahatás trükköt alkalmazzuk. Tudjuk, hogy

$$U_f |0\rangle |x_{-}\rangle = (-1)^{f(0)} |0\rangle |x_{-}\rangle$$

és

$$U_f |1\rangle |x_{-}\rangle = (-1)^{f(1)} |0\rangle |x_{-}\rangle$$

Ezek a kvantumállapotok tartalmazzák a globális fázis tényezőket $(-1)^{f(0)}$ és $(-1)^{f(1)}$. Viszont globális fázis tényezők nem befolyásolják a mérések eredményeit.

Most alkalmazzuk U_f -et a $|\psi_1\rangle$ szuperpozíción. Ennek eredménye

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle) |x_{-}\rangle.$$

Itt $(-1)^{f(0)}$ és $(-1)^{f(1)}$ globális fázis tényező, ezért vissza lehet lökni ezeket a $|0\rangle$ és $|1\rangle$ amplitudójához az első qubitben. Ezáltal információhoz jutunk $f(0)$ és $f(1)$ -ről amikor mérést végzünk $U_f |x_+\rangle |x_-\rangle$ -n.

Itt a kvantumpárhuzamosság szerepel: U_f egy alkalmazása megváltoztatja mindkettő állapot $|0\rangle$ és $|1\rangle$ amplitudóját. Végül

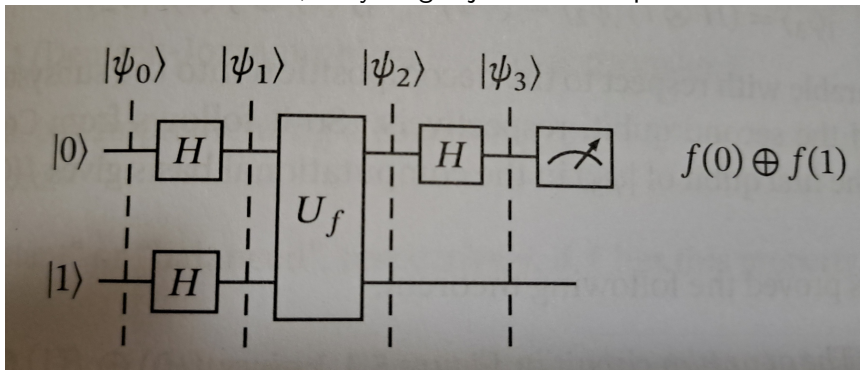
$$|\psi_3\rangle = (H \otimes I) |\psi_2\rangle = (-1)^{f(0)} |f(0) \oplus f(1)\rangle |x_-\rangle.$$

Ez az állapot szeparálható úgy, hogy az első és a második qubit szerepel. Tehát méréskor a $|\psi_3\rangle$ első qubitje megadja $(f(0) \oplus f(1))$ értékét 1 valószínűséggel.

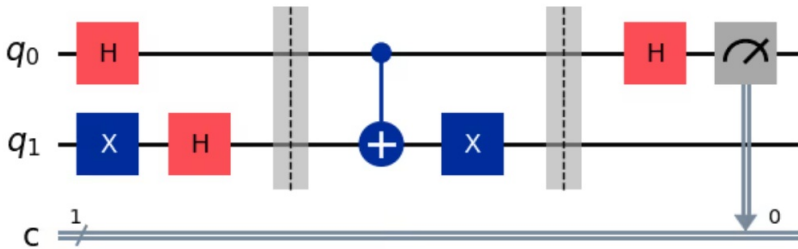
A következő kvantumáramkör megadja $(f(0) \oplus f(1))$ értékét 1 valószínűséggel. Ebben szerepel egy fekete doboz U_f egyszeri alkalmazása, és a Hadamard kapu alkalmazása háromszor.

Klasszikus verzió vs Kvantum verzió: Két lekérdezés/számolás helyett csak egy számolásra van szükség.

A kvantumáramkör, mely megoldja a Deutsch problémát:



Deutsch probléma megoldása Qiskit-ben:



Megjegyzés

A Deutsch algoritmusnak nincs nagy gyakorlati haszna, viszont ez volt történelmileg az első kvantumalgoritmus, mely gyorsabban old meg egy problémát mint a klasszikus megoldások.

Deutsch-Jozsa probléma

1992-ben Deutsch és Jozsa általánosította a Deutsch problémát, és adott meg egy kvantumáramkört ennek megoldására.

Input: Fekete doboz, mely kiszámolja egy $f : \{0, 1\}^n \rightarrow \{0, 1\}$ függvényhez tartozó függvényértékeket.

Output: $f(0) \oplus f(1)$

A Deutsch-Jozsa probléma kvantum verziója

Az f függvényt helyettesítünk egy unitér U operátorral.

$$U_f : \mathbb{H}_n \otimes \mathbb{H}_1 \rightarrow \mathbb{H}_1 \otimes \mathbb{H}_n$$

$$U_f : |\vec{x}\rangle |y\rangle \mapsto |\vec{x}\rangle |f(\vec{x}) \oplus y\rangle = |\vec{x}\rangle X^{f(\vec{x})} |y\rangle$$

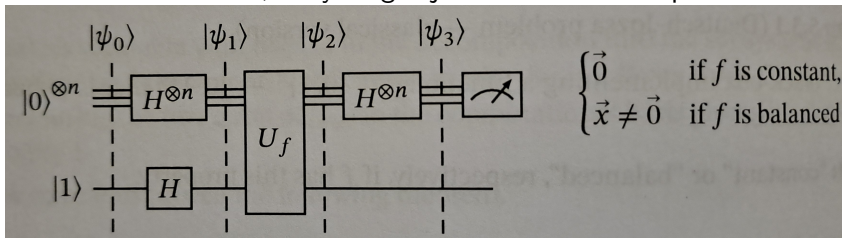
Input: Egy n pozitív szám. Egy fekete doboz, mely kiszámolja az egy $f : \{0, 1\} \rightarrow \{0, 1\}$ függvényhez tartozó U_f operátort

Output: *konstans vagy kiegyensúlyozott*

Tétel

Legyen $n \in \mathbb{N}$ és $f : \{0, 1\}^n \rightarrow \{0, 1\}$ egy konstans vagy kiegyensúlyozott függvény, és U_f unitér operátor ahogy korábban definiált. Ekkor a következő kvantumáramkör kimenete $\vec{0}$ ha f konstans és $\vec{x} \in \{0, 1\}^n$, $\vec{x} \neq \vec{0}$, ha f kiegyensúlyozott. Ebben szerepel egy fekete doboz U_f egyszeri alkalmazása, és a Hadamard kapu alkalmazása $2n + 1$ -szer.

A kvantumáramkör, mely megoldja a Deutsch-Jozsa problémát:



Simon algoritmus

Daniel R. Simon (1994)

Klasszikus verzió

Input: Egy fekete doboz, mely kiszámolja egy $f := \{0, 1\}^n \rightarrow \{0, 1\}^n$ függvényhez tartozó függvényértékeket úgy, hogy van egy $\vec{s} \in \{0, 1\}^n$, nem tiszta 0 sztring, úgyhogy $f(\vec{x}) = f(\vec{y})$ akkor és csak akkor ha $\vec{x} = \vec{y}$ vagy $\vec{x} = \vec{y} \oplus \vec{s}$

Output: $\vec{s}$

Megjegyzés: A továbbiakban s jelölést használunk $\vec{s}$ helyett.

Esetek

1. $s = 0$: Ekkor $f(x) = f(y) \Leftrightarrow x = y$. Ebben az esetben f egy bijektív függvény (one-to-one)
2. $s \neq 0$: Ekkor $f(x) = f(x \oplus s)$. Ebben az esetben f egy olyan függvény, melynek párokhoz tartozó függvényértékei különböznek.

Példa

x	$f(x)$
000	10011
001	00101
010	00101
011	10011
100	11010
101	00001
110	00001
111	11010

Legyen $s = 001$, ekkor

$$f(000) = f(011) = 10011$$

$$f(001) = f(010) = 00101$$

$$f(100) = f(111) = 11010$$

$$f(101) = f(110) = 00001$$

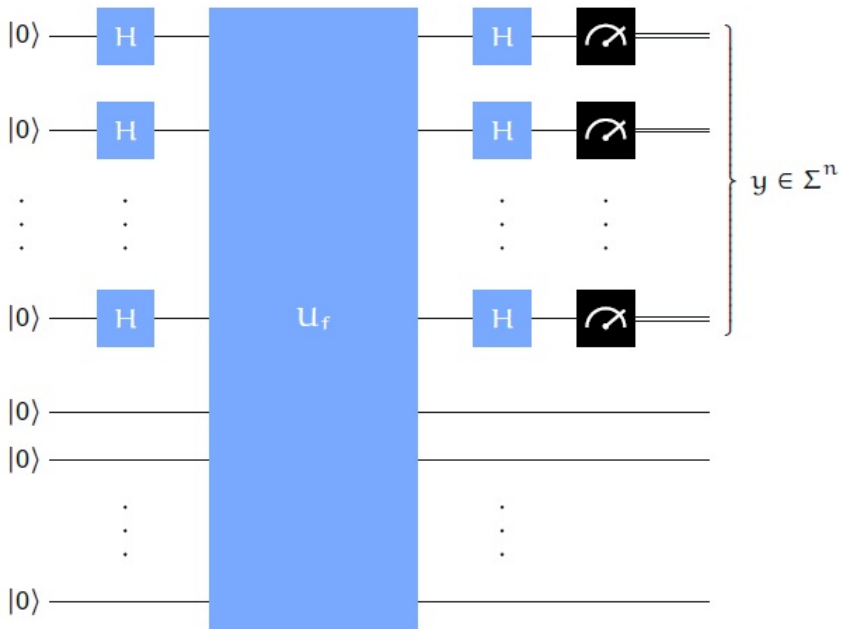
Kvantum verzió

f helyett U_f operátor

$$U_f : \mathbb{H}_n \rightarrow \mathbb{H}_n \quad U_f : |x\rangle |y\rangle \mapsto |x\rangle |f(x) \oplus y\rangle$$

Input: Egy fekete doboz, mely kiszámolja U_f operátor és egy $f := \{0, 1\}^n \rightarrow \{0, 1\}^n$ függvényhez tartozó függvényértékeket úgy, hogy van egy $\vec{s} \in \{0, 1\}^n$, nem tiszta 0 sztring, úgyhogy $f(\vec{x}) = f(\vec{y})$ akkor és csak akkor ha $\vec{x} = \vec{y}$ vagy $\vec{x} = \vec{y} \oplus \vec{s}$

Output: $\vec{s}$



Időigény

A klasszikus megoldás időigénye **exponenciális**, ezzel szemben a Simon algoritmus időigénye **lineáris**.