Kvantumalgoritmusok
Bernstein-Vazirani algoritmus

Története

- A Bernstein-Vazirani algoritmus egy speciális esete a Deutsch-Jozsa problémának.

Története

- A Bernstein-Vazirani algoritmus egy speciális esete a Deutsch-Jozsa problémának.
- Ethan Bernstein és Umesh Vazirani 1997

Története

- A Bernstein-Vazirani algoritmus egy speciális esete a Deutsch-Jozsa problémának.
- Ethan Bernstein és Umesh Vazirani 1997
- Célja az volt, hogy a BPP (Bounded-error probabilistic polynomial time) és a BQP (Bounded-error quantum polynomial time) időkomplexítási osztályt különböztesse.

Probléma

Adott egy fekete doboz, mely kiszámol egy függvényt

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

Probléma

Adott egy fekete doboz, mely kiszámol egy függvényt

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

ahol

$$f(x) = x \cdot s = x_1 s_1 \oplus x_2 s_2 \oplus \ldots \oplus x_n s_n,$$

valamilyen $s \in \{0,1\}^n$ titkos bináris sztringre.

Klasszikus verzió

Klasszikusan, a leghatékonyabb módszer az, amikor n-szer kiszámítjuk a függvényt úgy hogy $x = 2^i$ minden $i\{0, 1, \ldots, n-1\}$.

Klasszikus verzió

Klasszikusan, a leghatékonyabb módszer az, amikor n-szer kiszámítjuk a függvényt úgy hogy $x = 2^i$ minden $i\{0, 1, \ldots, n-1\}$.

$$f(1000\ldots0) = s_1$$

$$f(0100\ldots0) = s_2$$

$$f(0010\ldots0) = s_3$$

$$\vdots$$

$$f(0000\ldots1) = s_n$$

Klasszikus verzió

Klasszikusan, a leghatékonyabb módszer az, amikor n-szer kiszámítjuk a függvényt úgy hogy $x = 2^i$ minden $i\{0, 1, \ldots, n-1\}$.

$$f(1000\ldots0) = s_1$$

$$f(0100\ldots0) = s_2$$

$$f(0010\ldots0) = s_3$$

$$\vdots$$

$$f(0000\ldots1) = s_n$$

A klasszikus verzióban n darab számolásra van szükség s megtalálásához.

Kvantum verzió

1. A $|0\rangle^{\otimes n}$ qubit állapotra alkalmazzunk egy Hadamard transzformációt. Így

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

Kvantum verzió

1. A $|0\rangle^{\otimes n}$ qubit állapotra alkalmazzunk egy Hadamard transzformációt. Így

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

2. Aztán alkalmazzuk az U_f (fekete doboz) operátort:

$$|x\rangle \mapsto (-1)^{f(x)} |x\rangle$$

Kvantum verzió

1. A $|0\rangle^{\otimes n}$ qubit állapotra alkalmazzunk egy Hadamard transzformációt. Így

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

2. Aztán alkalmazzuk az U_f (fekete doboz) operátort:

$$|x\rangle \mapsto (-1)^{f(x)} |x\rangle$$

3. Így

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

4. Még egy Hadamard transzformációt alkalmazzuk minden qubiten. Ezért ahol $s_i = 1$ változik az állapot $|-\rangle \mapsto |1\rangle$ és ahol $s_i = 0$, ott az állapot $|+\rangle \mapsto |0\rangle$.

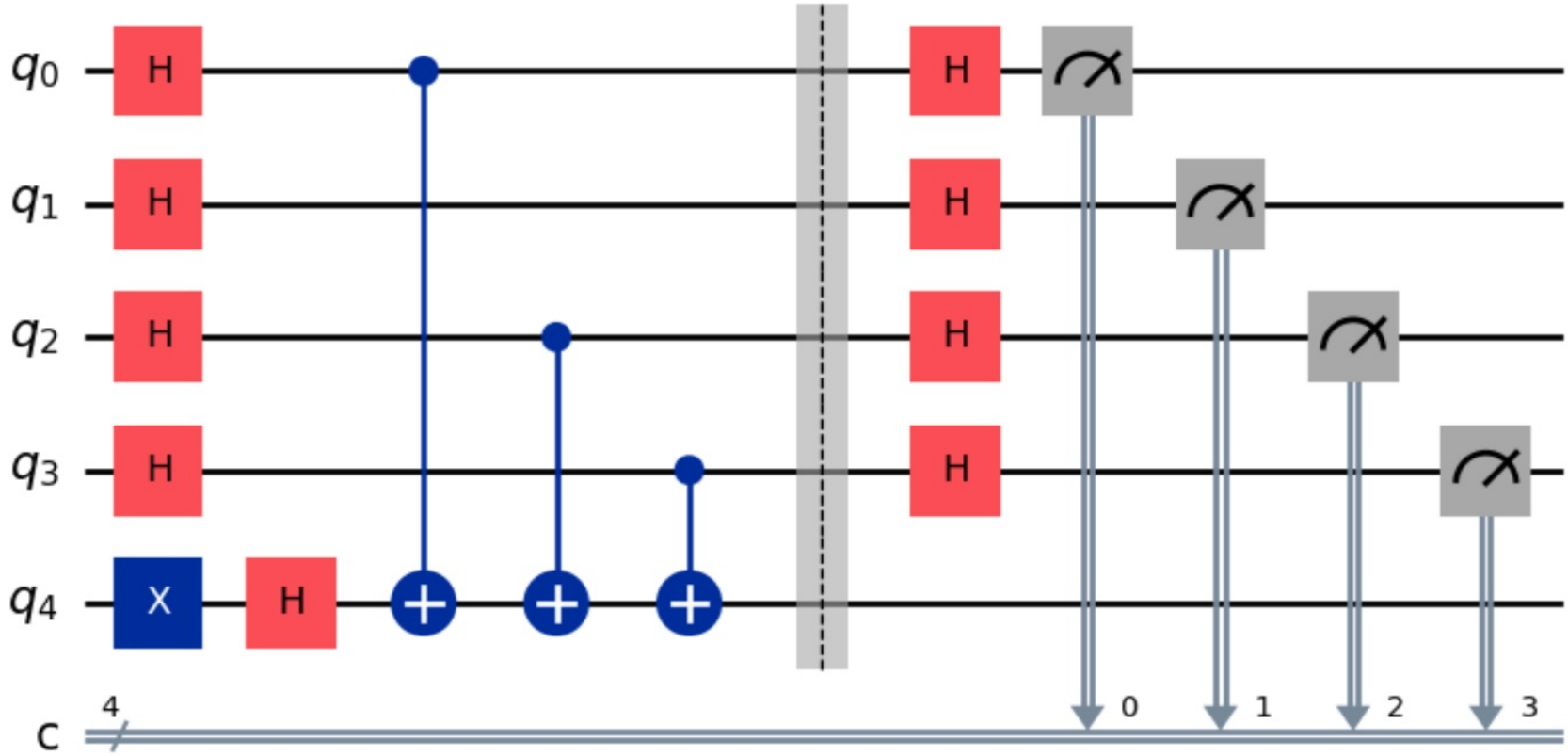
4. Még egy Hadamard transzformációt alkalmazzuk minden qubiten. Ezért ahol $s_i = 1$ változik az állapot $|-\rangle \mapsto |1\rangle$ és ahol $s_i = 0$, ott az állapot $|+\rangle \mapsto |0\rangle$.

5. Mérést végzünk a $\{|0\rangle, |1\rangle\}$ bázisban. Így megkapjuk s-t.

4. Még egy Hadamard transzformációt alkalmazzuk minden qubiten. Ezért ahol $s_i = 1$ változik az állapot $|-\rangle \mapsto |1\rangle$ és ahol $s_i = 0$, ott az állapot $|+\rangle \mapsto |0\rangle$.

5. Mérést végzünk a $\{|0\rangle, |1\rangle\}$ bázisban. Így megkapjuk s-t.

A kvantum verzióban egy számolás elegendő s meghatározására.


q_0
q_1
q_2
q_3
q_4
c
4
H
X
0
1
2
3