Kvantumszámítástudomány

Kaczúr Flórián

Témavezető: Friedl Katalin

2021. május

Bevezetés

- qubit: $\alpha\left|0\right\rangle + \beta\left|1\right\rangle$: $\left|0\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\left|1\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1$.

Bevezetés

- qubit: $\alpha |0\rangle + \beta |1\rangle$: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1$.
- regiszter: $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{2^n-1} |2^n - 1\rangle$, $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

Bevezetés

- qubit: $\alpha |0\rangle + \beta |1\rangle$: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1.$
- regiszter: $\alpha_0 |0\rangle + \alpha_1 |1\rangle + \ldots + \alpha_{2^n-1} |2^n - 1\rangle$, $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$
- transzformációk: **unitér**
  - $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  - $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
  - $O_{x,\pm} : |i\rangle \to (-1)^{x_i} |i\rangle$

Bevezetés

- qubit: $\alpha\,|0\rangle + \beta\,|1\rangle$: $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, $|\alpha|^2 + |\beta|^2 = 1.$
- regiszter: $\alpha_0\,|0\rangle + \alpha_1\,|1\rangle + \ldots + \alpha_{2^n-1}\,|2^n-1\rangle$, $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$
- transzformációk: **unitér**
  - $X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
  - $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$
  - $O_{x,\pm} : |i\rangle \to (-1)^{x_i}\,|i\rangle$
- mérés: $|i\rangle$ bázisvektor, $|\alpha_i|^2$ valószínűséggel

Nehézségek

Tétel

Nem létezik $A : |\Phi\rangle\,|0\rangle \to |\Phi\rangle\,|\Phi\rangle$ *unitér transzformáció [1].*

Állítás

A legtöbb $f : \{0,1\}^n \to \{0,1\}$ *függvény kiszámításához exponenciálisan sok transzformációra van szükség [1].*

Deutsch-Józsa

- $x \in \{0,1\}^{2^n}$ konstans vagy kiegyensúlyozott

Deutsch-Józsa

- $x \in \{0, 1\}^{2^n}$ konstans vagy kiegyensúlyozott
- $|0^n\rangle$

Deutsch-Józsa

- $x \in \{0,1\}^{2^n}$ konstans vagy kiegyensúlyozott
- $|0^n\rangle$
- $H^{\otimes n} O_{x,\pm} H^{\otimes n}$

Deutsch-Józsa

- $x \in \{0,1\}^{2^n}$ konstans vagy kiegyensúlyozott
- $|0^n\rangle$
- $H^{\otimes n} O_{x,\pm} H^{\otimes n}$
- $\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \left(\sum_{j \in \{0,1\}^n} (-1)^{i \odot j} |j\rangle \right)$

Deutsch-Józsa

- $x \in \{0,1\}^{2^n}$ konstans vagy kiegyensúlyozott
- $|0^n\rangle$
- $H^{\otimes n} O_{x,\pm} H^{\otimes n}$
- $\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \left(\sum_{j \in \{0,1\}^n} (-1)^{i \odot j} |j\rangle \right)$
- $|0^n\rangle$ együtthatója: $\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i}$

Deutsch-Józsa

- $x \in \{0,1\}^{2^n}$ konstans vagy kiegyensúlyozott
- $|0^n\rangle$
- $H^{\otimes n} O_{x,\pm} H^{\otimes n}$
- $\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i} \left(\sum_{j \in \{0,1\}^n} (-1)^{i \odot j} |j\rangle \right)$
- $|0^n\rangle$ együtthatója: $\frac{1}{2^n} \sum_{i \in \{0,1\}^n} (-1)^{x_i}$
- mérés
  - x konstans $\rightarrow |0^n\rangle$
  - x kiegyensúlyozott $\rightarrow$ más

Kvantum bolyongás

Adott egy X csúcshalmazú gráf P átmenetmátrixszal, egy $v \in M \subseteq X$ jelölt csúcsot keresünk, legyen $\varepsilon = \dfrac{|M|}{|X|}$. A bolyongás egy lépését egy $W(P)$ unitér mátrixszal való szorzás jelenti, emiatt az éleken lépkedünk.

Algoritmus ([2], [3]):

- kezdőállapot: $|\pi\rangle = \sum_{x \in X} \sqrt{\pi_x}\,|x\rangle \cdot \Big(\sum_{y \in X} \sqrt{p_{xy}}\,|y\rangle \Big)$

Kvantum bolyongás

Adott egy X csúcshalmazú gráf P átmenetmátrixszal, egy $v \in M \subseteq X$ jelölt csúcsot keresünk, legyen $\varepsilon = \dfrac{|M|}{|X|}$. A bolyongás egy lépését egy $W(P)$ unitér mátrixszal való szorzás jelenti, emiatt az éleken lépkedünk.

Algoritmus ([2], [3]):

- kezdőállapot: $|\pi\rangle = \sum_{x \in X} \sqrt{\pi_x}\,|x\rangle \cdot \left(\sum_{y \in X} \sqrt{p_{xy}}\,|y\rangle \right)$
- $\dfrac{1}{\sqrt{\varepsilon}}$-szor:
  1. $|x\rangle\,|y\rangle$ bázisvektorok negálása, ha $x \in M$
  2. tükrözés $|\pi\rangle$-re

Kvantum bolyongás

Adott egy X csúcshalmazú gráf P átmenetmátrixszal, egy $v \in M \subseteq X$ jelölt csúcsot keresünk, legyen $\varepsilon = \frac{|M|}{|X|}$. A bolyongás egy lépését egy $W(P)$ unitér mátrixszal való szorzás jelenti, emiatt az éleken lépkedünk.

Algoritmus ([2], [3]):

- kezdőállapot: $|\pi\rangle = \sum_{x \in X} \sqrt{\pi_x}\,|x\rangle \cdot \left(\sum_{y \in X} \sqrt{p_{xy}}\,|y\rangle \right)$
- $\frac{1}{\sqrt{\varepsilon}}$-szor:
  1. $|x\rangle\,|y\rangle$ bázisvektorok negálása, ha $x \in M$
  2. tükrözés $|\pi\rangle$-re
- mérés

Alkalmazások

1. Elemkülönbözőség: $O(n^{2/3})$
2. $A, B, C \in \mathbb{R}^{n \times n}$, $(AB)_{i,j} \neq C_{i,j}$: $O(n^{5/3})$
3. Háromszög keresése: $O(n^{1.3})$

Hivatkozások

- R. de Wolf, *Quantum computing: Lecture Notes* (https://arxiv.org/pdf/1907.09415.pdf)
- M. Santha, *Quantum walk based search algorithms* In Proceedings of 5th TAMC, pages 31–46, 2008. arXiv/0808.0059.
- F. Magniez, A. Nayak, J. Roland, and M. Santha. *Search via quantum walk*. In Proc. of the 39th ACM Symposium on Theory of Computing, pages 575–584, 2007.