Shor kvantum-algoritmusa diszkrét logaritmusra

Ivanyos Gábor
MTA SZTAKI

Debrecen, 2011 január 12.

Tartalom

Kvantum bit

- **Állapot:** a $B = \mathbb{C}^2$ komplex euklideszi tér egy egységvektora:

  az $a|0\rangle + b|1\rangle$ szuperpozíció (lineáris kombináció),

  ahol $|a|^2 + |b|^2 = 1$
- **Kitüntetett bázis:** $|0\rangle, |1\rangle$
- **Mérés után:**
  - 0: $|a|^2$ valószínűséggel,
  - 1: $|b|^2$ valószínűséggel.

n kvantum bites rendszer

- **Állapot:** a $B^{\otimes n} = \mathbb{C}^{2^n}$ komplex euklideszi tér egy egységvektora:

  a $\sum_{s \in S} a_s |s\rangle$ szuperpozíció,

  ahol $S = \{0,1\}^n$ és $\sum_{s \in S} |a_s|^2 = 1$.
- **Kitüntetett bázis:** $|s\rangle$, ahol $s \in S$:

  $|0 \ldots 00\rangle, |0 \ldots 01\rangle, |1 \ldots 11\rangle$.
- **Mérés után:** az s bitsorozat: $|a_s|^2$ valószínűséggel.

Kvantum kapuk

- **d bites kvantum kapu:** egy 2^d dimenziós unitér transzformáció

Példák:

- **Hadamard-kapu:** $H : |0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$,
$$|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
- **Kontrollált fáziseltolás:**
$$|0x\rangle \mapsto |0x\rangle,\ |10\rangle \mapsto |10\rangle,$$
$$|11\rangle \mapsto \omega|11\rangle, \text{ ahol } |\omega| = 1.$$

Kvantum példa-kapuk mátrixa

- **Hadamard-kapu:**

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

- **Kontrollált fáziseltolás:**

$$\begin{pmatrix}1 & & & \\ & 1 & & \\ & & 1 & \\ & & & \omega\end{pmatrix}$$

Kvantum-áramkör: számolás

- n kvantum bites rendszeren
- egy- és kétbites kvantum kapuk sorozata
  - megadva az is, hogy mely kvantum bit(ek)en hatnak ("drótozás", sorrend is számít)
  - formálisan: a megfelelő transzformáció $\otimes$ identitás
- **Művelet:** a kapuknak megfelelő transzformációk szorzata
- **Időigény (lépésszám):** a sorozat hossza
- **Megjegyzés:** konstans $d > 2$-re legfeljebb d bites kapukból álló áramkörök: az 1-2 bitessel polinomiálisan ekvivalens modell.

Kvantum-párhozamosság

- Tfh. $s \in S_1 = \{0,1\}^{n_1}$-re $s \mapsto f(s) \in \{0,1\}^{n_2}$ T időben számolható.
- Ekkor

$$\sum_{s \in S_1} a_s |s\rangle |y\rangle \mapsto \sum_{s \in S_1} a_s |s\rangle |f(s) \mathrm{XOR} y\rangle$$

$O(T)$ lépésben számolható kvantumgéppel

Kvantum-áramkör: mérés/működés

- a kapuk szorzata az input bitsorozatnak megfelelő báziselemre
- végül mérés
- randomizált algoritmushoz hasonló jellegű
- a megfelelő nyelvosztály: BPQ
- **Megjegyzés:** Véges ún. univerzális kapukészlettel – a kapuk közelítése segítségével – szintén polinomiálisan ekvivalens modell kapható.

Részleges mérés

- Kétrészes állapot (két "regiszter"):

$$\sum_{s_1 \in S_1} \sum_{s_2 \in S_2} a_{s_1 s_2} |s1\rangle |s_2\rangle$$

- Tfh. a második regisztert tovább nem használjuk
  Kényelmes "megmérni és eldobni"
- s_2 eredmény valószínűsége

$$\sum_{s_1 \in S_1} |a_{s_1 s_2}|^2$$

- maradék állapot s_2 mérése esetén

$$\frac{1}{\sqrt{\sum_{s_1 \in S_1} |a_{s_1 s_2}|^2}} \sum_{s_1 \in S_1} a_{s_1 s_2} |s_1\rangle$$

- $\sim$ disztributivitás alkalmazása

A Kvantum Fourier-transzformáció

- QFT modulo N: $x \in \{0, \ldots, N-1\}$-re

$$|x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega^{x \cdot y} |y\rangle,$$

  ahol $\omega = \sqrt[N]{1}$.
- Báziscsere a ciklikus léptetés sajátvektoraira
- Hatékonyan (azaz $(\log N)^{O(1)}$ méretű kvantum-áramkörrel) implementálható, ha $N = 2^k$
- Tetszőleges N-re hatékonyan (azaz $(\log N \log \frac{1}{\epsilon})^{O(1)}$ méretű kvantum-áramkörrel) **közelíthető** $\leq \epsilon$ hibával.

Tartalom

Diszkrét log

- **A feladat:** A (kommutatív) csoport, $a, b \in A$, keresendő a legkisebb $z \geq 0$ egész, amelyre $a^z = b$.
- **Egyszerűsítő feltevés:** a és b rendje ismert p prímszám. Ekkor $0 < z < p$.
- **Eszköz:** $f : \mathbb{Z}_p \times \mathbb{Z}_p \to A$

$$f(z_1, z_2) = a^{-z_1} b^{z_2}$$

$f(z_1, z_2)$ gyors hatványozással hatékonyan számolható

- **Fontos tulajdonság:**

$$f(z_1, z_2) = a^{-z_1} b^{z_2} = a^{z_2 z - z_1} a^{-z_2 z} b^{z_2} = a^{z_2 z - z_1}$$

Diszkrét log algoritmus -első lépések

$$|0\rangle|0\rangle|0\rangle$$

$$\downarrow \text{ QFT mod } p \text{ az első két regiszterre}$$

$$\frac{1}{p}\sum_{z_1\in\mathbb{Z}_p}\sum_{z_2\in\mathbb{Z}_p}|z_1\rangle|z_2\rangle|0\rangle$$

$$\downarrow f \text{ számítása}$$

$$\frac{1}{p}\sum_{z_1\in\mathbb{Z}_p}\sum_{z_2\in\mathbb{Z}_p}|z_1\rangle|z_2\rangle|a^{-z_1}b^{z_2}\rangle =$$

$$f \text{ tulajdonsága}$$

$$= \frac{1}{p}\sum_{z_1\in\mathbb{Z}_p}\sum_{z_2\in\mathbb{Z}_p}|z_1\rangle|z_2\rangle|a^{z_2z-z_1}\rangle =$$

$$z_1 \leftrightarrow z_2z+u, \text{ ahol } u=z_1-z_2z$$

$$= \frac{1}{p}\sum_{u\in\mathbb{Z}_p}\sum_{z_2\in\mathbb{Z}_p}|z_2z+u\rangle|z_2\rangle|a^{-u}\rangle$$

Diszkrét log algoritmus -második lépések

$$\frac{1}{p}\sum_{u\in\mathbb{Z}_p}\sum_{z_2\in\mathbb{Z}_p}|z_2 z+u\rangle|z_2\rangle|a^{-u}\rangle$$

$\downarrow$ harmadik regiszter mérése és eldobása

$$\frac{1}{\sqrt{p}}\sum_{z_2\in\mathbb{Z}_p}|z_2 z+u\rangle|z_2\rangle$$

valamely véletlen $u\in\mathbb{Z}_p$-re

egyenletes valószínűséggel

Az $(z,1)$-gyel történő ciklikus léptetésre invariáns vektor

A léptetések közös sajátaltereit érdemes nézni (QFT)

Diszkrét log algoritmus - QFT

$$\frac{1}{\sqrt{p}} \sum_{z_2 \in \mathbb{Z}_p} |z_2 z + u\rangle |z_2\rangle$$

$$\downarrow \text{ QFT mod } p \text{ a két regiszterre}$$

$$\frac{1}{p^{3/2}} \sum_{y_1} \in \mathbb{Z}_p \sum_{y_2 \in \mathbb{Z}_p} \sum_{z_2 \in \mathbb{Z}_p} \omega^{(z_2 z+u) y_1} \omega^{z_2 y_2} |y_1\rangle |y_2\rangle$$

$|y_1\rangle|y_2\rangle$ együtthatója:

$$\frac{1}{p^{3/2}} \sum_{z_2 \in \mathbb{Z}_p} \omega^{(z_2 z+u) y_1 + z_2 y_2} = \frac{\omega^{u y_1}}{p^{3/2}} \sum_{z_2 \in \mathbb{Z}_p} \left(\omega^{z y_1 + y_2}\right)^{z_2}.$$

Diszkrét log algoritmus - befejező mérés

Együtthatók: $|y_1\rangle|y_2\rangle$ együtthatója:

$$\frac{\omega^{uy_1}}{p^{3/2}} \sum_{z_2 \in \mathbb{Z}_p} \left(\omega^{zy_1+y_2}\right)^{z_2} = \begin{cases} \frac{\omega^{uy_1}}{p^{1/2}} & \text{ha } zy_1 + y_2 = 0 \\ 0 & \text{egyébként} \end{cases}$$

Mérés eredménye: olyan $(y_1, y_2) \in \mathbb{Z}_p^2$, hogy

$$zy_1 + y_2 = 0,$$

ezek egyforma $(\frac{1}{p})$ valószínűséggel.

Siker: $1 - \frac{1}{p}$ valószínűséggel $y_1 \neq 0$ és ekkor $z = -y_2 y_1^{-1}$.