Kvantum-számítógépek, univerzalitás és véges csoportok

Ivanyos Gábor
MTA SZTAKI

BME Matematikai Modellalkotás szeminárium,
2013 szeptember 24.

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 $s \in S$:

  $|0 \ldots 00\rangle, |0 \ldots 01\rangle, |1 \ldots 11\rangle$.
- **Jelölések:**
  $|01101\rangle := |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle = |0\rangle|1\rangle|1\rangle|0\rangle|1\rangle = |01\rangle|101\rangle$

- **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:**
  $|0x\rangle \mapsto |0x\rangle$, $|10\rangle \mapsto |10\rangle$,
  $|11\rangle \mapsto \omega|11\rangle$, 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
- **Általánosabban:** konstans $d > 2$-re legfeljebb d bites kapukból álló áramkörök: az 1-2 bitessel polinomiálisan ekvivalens modell.
- **Példa:** n bites Hadamard-transzf.

$$H^{\otimes n} : |x\rangle \mapsto 2^{-n/2} \sum_{z \in \{0,1\}^n} (-1)^{x \cdot z} |z\rangle$$

$(x \cdot z := \sum x_i z_i \mod 2)$

Kvantum-párhuzamosság

- $f : S_1 = \{0,1\}^{n_1} \to \{0,1\}^{n_2}$
- Tfh. hogy f Boole-áramkörrel (azaz "klasszikusan") T időben számolható.
- Ekkor

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

  $O(T)$ lépésben megvalósítható kvantumgéppel
  $(+ = XOR)$

- lényeg:

$$\sum_{s \in S_1} a_s |s\rangle |0\rangle \mapsto \sum_{s \in S_1} a_s |s\rangle |f(s)\rangle$$

Kvantum-áramkör: mérés/működés

- a kapuk szorzata az input bitsorozatnak megfelelő báziselemre
- végül mérés
- a randomizált algoritmusokhoz hasonló jellegű
- a polinomidőben "felismerhető" nyelvek osztálya: **BQP**
- Véges **univerzális** kapukészlettel – a kapuk közelítése segítségével – szintén polinomiálisan ekvivalens modell kapható (Solovay-Kitaev).

Példa - a Simon-féle feladat

- Feladat:
  - "adott" $f : \{0,1\}^n \longrightarrow \{0,1\}^n$
  - tulajdonság: van olyan $v \in \{0,1\}^n \setminus \{\underline{0}\}$, hogy $f(x) = f(y) \Longleftrightarrow x = y + v$
    $(+ = XOR)$
  - Keressük meg v-t!
- Klasszikus bonyolultság: $2^{\Omega(n/2)}$ lekérdezés kell
- Kvantum: $O(n)$ lekérdezés, poly(n) idő

Simon algoritmusa

$2n$ kvantum biten (2 db. n bites "regiszter") kiindulás:

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

$$\downarrow \quad H^{\otimes n}$$

$$2^{-n/2} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle$$

$$\downarrow \quad f \text{ kiértékelése (kv-párh.)}$$

$$2^{-n/2} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$

$$=$$

$$2^{-n/2-1} \sum_{x\in\{0,1\}^n} (|x\rangle + |x+v\rangle)|f(x)\rangle$$

Simon algoritmusa II

$$2^{-n/2-1} \sum_{x\in\{0,1\}^n} (|x\rangle + |x+v\rangle)|f(x)\rangle$$

$$\downarrow \qquad H^{\otimes n}$$

$$2^{-n-1} \sum_{x\in\{0,1\}^n} \sum_{z\in\{0,1\}^n} ((-1)^{x\cdot z} + (-1)^{(x+v)\cdot z})|z\rangle|f(x)\rangle$$

$$= \qquad \text{"interferencia":}$$

együttható 0 lesz, ha $v \cdot z \neq 0$

$$2^{-n} \sum_{x\in\{0,1\}^n} \sum_{z\in v^\perp} ((-1)^{x\cdot z})|z\rangle|f(x)\rangle$$

mérés

$$(z, F) \text{ valószínűsége} = \begin{cases} 2^{2-2n} & \text{ha } z \in v^\perp \\ 0 & \text{ha } z \notin v^\perp \end{cases}$$

Simon algoritmusa III

$$(z, F) \text{ valószínűsége} = \begin{cases} 2^{2-2n} & \text{ha } z \in v^{\perp} \\ 0 & \text{ha } z \notin v^{\perp} \end{cases}$$

z-re szorítkozva egyenletes eloszlás $v^{\perp}$-en

$O(n)$ ismétléssel $v^{\perp}$ bázisát kapjuk (jó eséllyel)

$v^{\perp}$-ből v lin. egyenletrendszer

Áramkör: $H^{\otimes n}$; f kiért.; $H^{\otimes n}$; (majd mérés)

Shor faktorizáló és diszkrét log algoritmusai hasonló elven

Teljesség, univerzalitás: fogalmak

- **Elnevezések:** teljes, K-univerzális (ad hoc), univerzális
- n **bites kvantum kapu** (fix "drótozás"): $u \in U_{2^n}$
- n **bites kvantum-áramkör** (fix "drótozás"): $u_1, \ldots, u_\ell$

  u_i a $\Gamma \subseteq U_{2^n}$ kapukészletből
  megvalósított művelet: $u_1 \cdots u_\ell$
- **teljesség:** minden $u \in U_{2^n}$

  tetszőleges pontossággal
  közelíthető Γ-beli kapukból felépített áramkörrel
  más szóval: Γ az U_{2^n} egy sűrű részcsoportját generálja.
  pontosabban, modulo a skalármátrixok
  (állapotok skalárszorosai egyenértékűek)
- Solovay-Kitaev: $\exists\ f(n, \mathit{hiba})$ hosszú közelítő sorozat

n-bites kapuk n-nél több biten

drótozás: $K > n$,

$$\mu : [n] = \{1, \ldots n\} \to [K] = \{1, \ldots, K\} \quad \text{beágy.}$$

u_μ hatása

- u a $\mu(1), \ldots, \mu(n)$ biteken
- a maradékon identitás
  formálisan: $u_\mu = u \otimes I$

Univerzalitás

- K-**univerzalitás:** $\{u_\mu | u \in \Gamma, \mu : [n] \to [K]$ beágy.$\}$ teljessége
- monoton tul.: ha $K \geq 2$, K-univerzalitás $\Rightarrow$ $K+1$-univerzalitás

  (felhasznált tény: a 2-bites kapuk halmaza K-univerzális minden K-ra)

  Megj.: az 1-bites kapuk nem 2-univerzálisak (sem 3-,stb...)!
- **univerzalitás:** $\exists K \geq \max\{n, 2\}$, amelyre Γ is K-univerzális

Kapcsolatos algoritmikus problémák

- **teljesség** - több számítási modellben eldönthető
  - **Derksen-Koiran-Jeandel 2003, 2005**
    "szimbolikus" testek felett
    eszköz: csoportok *Zariski*-lezártjának a kiszám.
    Tény: Kompakt valós lineáris csoportok
    polinom-egyenletrendszerekkel definiálhatók
    SU_{2^n}-beli "metrikus" sűrűség $\Leftrightarrow$ $SL_{2^n}(\mathbb{C})$-beli Zariski-sűrűség.
    Zariski-lezárt: ugyanazokat a polinomegyenleteket teljesíti
  - **Jeandel 2004:** algebrai számtestek felett (polinomidőben!)
- K-**univerzalitás** $\Leftrightarrow$ megfelelő nagyobb kapukészlet teljessége

Kapcsolatos algoritmikus problémák II

- K-**univerzalitás** $\Leftrightarrow$ megfelelő nagyobb kapukészlet teljessége
- **univerzalitás** - nem nyilvánvaló, hogy eldönthető
  - hiányzik: felső korlát a legkisebb K-ra

    amelyre egy univerzális kapukészlet K-univerzális
  - Nagy W. Attila: $\exists$ 2 bites készlet, amely 3-univ, de nem 2-univ.
  - Jeandel példája: $K > 2n - 6$ végtelen sok n-re

Az eredmények

- a K-univerzalitás eldönthető egy $2^{8K}(|\Gamma|+2)$ homogén lineáris egyenletből álló 2^{8K} változós egyenletrendszerrel.
- Ha $n \geq 2$, egy n bites univerzális kapukészlet K_0-univerzális valamely

$$K_0 \leq 256n\text{-}re.$$

Megj.: A $256n$-univerzalitást eldöntő egyenletrendszer mérete polinomiális a bemenet méretében (az $|\Gamma| \cdot 2^{2n}$ számból áll).

A bizonyítás 1. (könnyű) lépése

Γ is K-**univerzális**

$\Updownarrow$

(12), $(12\ldots K)$ (vagy az S_K tetsz. gen. rendszere),

a Γ-beli, az első n bitre drótozott kapuival együtt **teljes**.

A bizonyítás 2. (nehéz) lépése: kritérium teljességre

- $\Gamma' \subset U_{2^K}$ teljes (K biten)
  $\Updownarrow$
- A következő $2^{8K} \times 2^{8K}$ méretű mátrixok közös fixpontja egy 24 dimenziós alteret alkotnak:

$$\gamma \otimes \gamma \otimes \gamma \otimes \gamma \otimes \overline{\gamma} \otimes \overline{\gamma} \otimes \overline{\gamma} \otimes \overline{\gamma} \quad (\gamma \in \Gamma')$$

- (Ez Γ' hatása a $V^{\otimes 4} \otimes (V^{\otimes 4})^*$ téren, ahol $V = \mathbb{C}^{2^K}$)
- (Megj.: 24 az egész GL_{2^K} csoport hasonló hatásának a fixpontjainak a dimenziója.)
- Guralnick és Tiep 2005-ös mély eredményéből
  Amin múlik: a véges egyszerű csoportok osztályozása.

Jeandel kritériuma és a Larsen-alternatíva

- $\Gamma' \subset U_{2^\kappa}$ teljes K biten

  $\Updownarrow$

- A következő 2 feltétel:
  (1) Γ' közös fixpontjai a $V^{\otimes 2} \otimes (V^{\otimes 2})^*$ téren 2-dimenziós altér
  (2) $\langle \Gamma' \rangle$ végtelen
- Biz.: legyen G a $\langle \Gamma \rangle$ komplex Zariski-lezártja
  (1) $\Leftrightarrow$ $s\ell_{2^\kappa}$ is irreducibilis G konjugálási hatására nézve.
  Ekkor vagy $G_0 = \{1\}$ vagy $G_0 = SL_{2^\kappa}$.

  G_0 = G-nek az 1-et tart. komponense
- Hátrány: (2) nem egyenletekkel adott.
- (Ugyanakkor néhány input modellben jól használható.
  Pl. racionális mátrixokra Babai-Beals-Rokcmore.)

A bizonyítás 3. lépése: szerencse

- S_K jelenléte $\Rightarrow$ tenzoralgebra $\rightarrow$ polinomgyűrű
- Kapcsolható polinomideál: I
- I homogén ideál 2^{8n} változóban
- $\Gamma \cup S_K$ fixpontjai $\sim$ I K-dimenziós részének komplementere
- $H_I(K) = \Gamma \cup S_K$ fixpontjainak dim. (H_I az I Hilbert-függvénye.)
- Ha Γ univerzális, $H_I(K) = 24$ elég nagy K-re.
- a legkisebb ilyen $K{=}H_I$ regularitása
- Lazard regularitási korlátja nulldimenziós ideálra

Jobb korlátok?

- Univerzalitás- korlátok: alsó $2n$ (bizonyos n-ekre) - felső $256n$
- Korlátok kis n-ekre, (pl. $n = 2$-re ismert alsó korlát 3)
- Tenzor-felbontás kihasználható-e:
  - $W = B^{\otimes 4} \otimes (B^{\otimes 4})^*$, $W^{\otimes n}$ örökli ezt a felbontást
  - Pl. $W \cong M_{16}(\mathbb{C})$, $W^{\otimes n}$. Fixpontok: részalgebra.
- Univerzalitás eldönthetősége CFSG nélkül????
- $W^{\otimes n}$ alterei és a lin. csoportok közötti Galois-kapcsolat kihasználása?
  - Schrijver: fixpontok a teljes tenzor-algebrában leírhatók
  - Van-e ennek következménye kis tenzorhatványokra
  - Véges csoportok fixpontjai???

További univerzalitás-fogalmak?

- Pl. "ideiglenes tár" használata
  - Az $U \otimes I_{2^L}$ alakú transzformációk közelítendők
  - **csak** a $\cdots \otimes |0\rangle^{\otimes L}$ alakú állapotok alterén
  - a teljes $\mathbb{C}^{\otimes 2^K} \otimes \mathbb{C}^{\otimes 2^L}$ teret kihasználó kapukkal
- Egyéb modellek (pl. "globális" hatású kapuk?)

(nehéz a kvantum biteket megcélozni)

Numerikus/közelítő input?

- ϵ-közelség **nem-univerzális** kapukészlethez eldönthető (csak elvileg). Polinom-egyenlőtlenségrendszer megoldásán alapuló módszer.
- Van-e hatékonyabb????
- Kapcsolódó kérdés: Milyen feltételek mellett igaz, hogy ha $\Gamma \subset GL(W)$-nek a $v \in W^{\otimes n}$ ($|v| = 1$) "közel"-fixpontja, akkor Γ közel van egy olyan rendszerhez, aminek v tényleges fixpontja?
- Egyéb, értelmes numerikus stabilitási szempontok????