Kvantum-bonyolultságelméleti szeparáció relációs osztályokra

Csatári Jakab

2023.06.01.

Referencia

- A Qubit, a Coin, and an Advice String Walk Into a Relational Problem
  Scott Aaronson, Harry Buhrman, William Kretschmer (2023 Feb)

- A cikk első eredménye: FBQP/poly ≠ FBQP/qpoly

- Ezt dolgoztam fel
  + meggondolások uniform – nem-uniform osztályok közt

Relációs probléma

- Döntési problémáknál:

$$x \overset{?}{\in} L \qquad\qquad A : \{0,1\}^* \to \{0,1\}$$

- Relációs problémáknál:

$$R \subseteq \{0,1\}^* \times \{0,1\}^*$$

$$(x,y) \overset{?}{\in} R \qquad\qquad A : \underset{x}{\{0,1\}^*} \to \underset{y}{\{0,1\}^*}$$

Relációs probléma

Példa:

$$R := \{(x, y) \mid x + y \text{ páros}\}$$

FBQP

Function **B**ounded-Error **Q**uantum **P**olynomial

Def: Azon $R \subseteq \{0,1\}^* \times \{0,1\}^*$ relációk osztálya, melyekre $\exists A$ polinomiális kvantum algoritmus, hogy $\forall x \in \{0,1\}^*$:

$$Pr[(x, A(x)) \in R] \geq 1 - \epsilon$$

FBQP/poly

Def: Azon $R \subseteq \{0,1\}^* \times \{0,1\}^*$ relációk osztálya, melyekre $\exists A$ polinomiális kvantum algoritmus és polinomiális méretű (klasszikus) súgás $\{s_n\}_{n \geq 1}$, hogy $\forall x \in \{0,1\}^*$:

$$Pr[(x, A(x|s_{|x|})) \in R] \geq 1 - \epsilon$$

FBQP/rpoly

Def: Azon $R \subseteq \{0,1\}^* \times \{0,1\}^*$ relációk osztálya, melyekre $\exists A$ polinomiális kvantum algoritmus és polinomiális méretű (klasszikus) súgások eloszlása $\{D_n\}_{n\geq 1}$, hogy $\forall x \in \{0,1\}^*$:

$$\underset{r\sim D_n}{Pr}\left[(x, A(x|r)) \in R\right] \geq 1 - \epsilon$$

FBQP/qpoly

Def: Azon $R \subseteq \{0,1\}^* \times \{0,1\}^*$ relációk osztálya, melyekre $\exists A$ polinomiális kvantum algoritmus és polinomiális méretű kvantum súgás $\{|\psi_n\rangle\}_{n\geq 1}$, hogy $\forall x \in \{0,1\}^*$:

$$Pr[(x, A(x||\psi_n\rangle)) \in R] \geq 1 - \epsilon$$

FBQP/qpoly

Def: Azon $R \subseteq \{0,1\}^* \times \{0,1\}^*$ relációk osztálya, melyekre $\exists A$ polinomiális kvantum algoritmus és polinomiális méretű kvantum súgás $\{|\psi_n\rangle\}_{n\geq 1}$, hogy $\forall x \in \{0,1\}^*$:

$$Pr[(x, A(x||\psi_n\rangle)) \in R] \geq 1 - \epsilon$$

$|\psi_n\rangle$: poly(n) qubit szuperpozíciója

FBQP súgásokkal

$$\mathrm{FBQP/poly} \subseteq \mathrm{FBQP/rpoly} \subseteq \mathrm{FBQP/qpoly}$$

FBQP súgásokkal

$$\mathrm{FBQP/poly} \subseteq \mathrm{FBQP/rpoly} \subseteq \mathrm{FBQP/qpoly}$$

$$= \qquad \subsetneq$$

FBQP/rpoly ≠ FBQP/qpoly

- R_F reláció megfogalmazása
- $\forall F : R_F \in$ FBQP/qpoly
- $\exists F : R_F \notin$ FBQP/poly = FBQP/rpoly

R_F reláció

Boole függvény sereg:

$$F = \{f_n\}_{n \geq 1} \qquad f_n : \{0,1\}^n \to \{0,1\}$$

$$R_F := \{(x,(y,b)) \mid f_n(y) \oplus f_n(y \oplus x) = b\}$$

ahol $x, y \in \{0,1\}^n, b \in \{0,1\}$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

0. lépés

Ha $x = |0^n\rangle$ akkor output: $(y, 0)$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

0. lépés

Ha $x = |0^n\rangle$ akkor output: $(y, 0)$

$$f_n(y) \oplus f_n(y \oplus x) = b$$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

0. lépés

Ha $x = |0^n\rangle$ akkor output: $(y, 0)$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

algoritmus $A \in \mathbb{F}_2^{n-1 \times n}$ nulltere: $\{0, x\}$

$$|\psi_n\rangle \to |\psi_n\rangle |Ay\rangle$$

0. lépés

Ha $x = |0^n\rangle$ akkor output: $(y, 0)$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

0. lépés

Ha $x = |0^n\rangle$ akkor output: $(y, 0)$

algoritmus $A \in \mathbb{F}_2^{n-1 \times n}$ nulltere: $\{0, x\}$

$$|\psi_n\rangle \to |\psi_n\rangle |Ay\rangle$$

megmérjük $|Ay\rangle$-t

$$\frac{1}{\sqrt{2}} \left((-1)^{f_n(y)} |y\rangle + (-1)^{f_n(y \oplus x)} |y \oplus x\rangle \right)$$

Kvantum algoritmus $\forall F : R_F \in$ FBQP/qpoly

súgás

$$|\psi_n\rangle := \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{f_n(y)} |y\rangle$$

0. lépés

Ha $x = |0^n\rangle$ akkor output: $(y, 0)$

algoritmus $A \in \mathbb{F}_2^{n-1 \times n}$ nulltere: $\{0, x\}$

$$|\psi_n\rangle \to |\psi_n\rangle |Ay\rangle$$

↓ megmérjük $|Ay\rangle$-t

$$\frac{1}{\sqrt{2}} \left((-1)^{f_n(y)} |y\rangle + (-1)^{f_n(y \oplus x)} |y \oplus x\rangle \right)$$

↓ megmérjük $\{|y\rangle \pm |y \oplus x\rangle\}$ bázisban

$$= \begin{cases} |y\rangle + |y \oplus x\rangle & \text{ha } f_n(y) = f_n(y \oplus x) \\ |y\rangle - |y \oplus x\rangle & \text{ha } f_n(y) \neq f_n(y \oplus x) \end{cases}$$

Hidden Matching Probléma

Def (HM_N):

Legyen $z \in \{0,1\}^N$ Alice inputja, $M \in \mathcal{M}_N$ teljes párosítás Bob inputja, ekkor Bob célja:

Output: (i, j, b) , ahol

- $(i, j) \in M$
- $b = z_i \oplus z_j$

$i, j \in \{1, ..., N\}$ $b \in \{0, 1\}$

$\mathcal{M}_N = \{M_1, M_2, ..., M_m\}$ páronként éldiszjunkt teljes párosítások, ahol $m = \Omega(N)$

Hidden Matching Probléma

A birthday paradox argument:

Alice rand választ $c \cdot \sqrt{N}$ indexet, megfelelő biteket átküldi

$$E[\text{Élek száma } T \text{ db random index közt}] = \binom{T}{2} \frac{1}{N-1} \approx \frac{T^2}{2N}$$

$$\frac{T^2}{2N} \to \frac{c^2 N}{2N} = \frac{c^2}{2}$$

$T \geq 2\sqrt{N}$ -re pl. már elég valószínű

Hidden Matching Probléma

Tétel (Yossef-Jayram-Kerenidis):

Bármely egyirányú randomizált protokollhoz, mely megoldja HM_N -et $\leq \frac{1}{8}$ hibával, szükség van $\Omega(\sqrt{N})$ bit kommunikációra.

Láttuk, hogy $\Theta(\sqrt{N})$-ről van szó igazából.

Kapcsolat R_F -fel

$$x \neq 0^n$$

$$M_x := \{(y, y \oplus x) | y = 1, ..., 2^n\} \qquad \mathcal{M}_n := \{M_1, M_2, ..., M_{2^n - 1}\}$$

Alice ismeri f_n igazságtábláját ($\{0,1\}^{2^n}$), Bob ismeri x-et, így M_x-et is

Alice kommunikációja megfelel a súgásnak

És most $N = 2^n$

Kapcsolat R_F -fel

Előző Tétel miatt:

Alice-nak $\Omega(2^{n/2})$ bitet kell küldeni, hogy $\frac{7}{8}$ val. jól válaszoljon

Kapcsolat R_F -fel

Előző Tétel miatt:

Alice-nak $\Omega(2^{n/2})$ bitet kell küldeni, hogy $\frac{7}{8}$ val. jól válaszoljon

Ha $F' \sim \{F \mid F = \{f_n\}_{n\geq 1}\}$, akkor

$$Pr[poly(n) \text{ méretű } s_n \text{ súgás mellett } x \in \{0,1\}^n \text{ inputra } (x, A(x|s_n)) \in R_{F'}] \leq \frac{7}{8}$$

Kapcsolat R_F -fel

Előző Tétel miatt:

Alice-nak $\Omega(2^{n/2})$ bitet kell küldeni, hogy $\frac{7}{8}$ val. jól válaszoljon

Ha $F' \sim \{F \mid F = \{f_n\}_{n\geq 1}\}$, akkor

$$Pr[poly(n) \text{ méretű } s_n \text{ súgás mellett } x \in \{0,1\}^n \text{ inputra } (x, A(x|s_n)) \in R_{F'}] \leq \frac{7}{8}$$

De ez minden n-re független, így

$$Pr[poly(|x|) \text{ méretű } \{s_n\}_{n\geq 1} \text{ súgások mellett } x \in \{0,1\}^* \text{ inputra } (x, A(x|s_n)) \in R_{F'}] \leq \prod_{n=1}^{\infty} \frac{7}{8} = 0$$

Kapcsolat R_F -fel

Tehát 1 valószínűséggel: $\exists F : R_F \notin$ FBQP/poly = FBQP/rpoly

További meggondolások

- $R_F \notin$ FBQP/poly -nál nem használtuk ki, hogy FBQP az algoritmus

  Ha C uniform: $R_F \notin$ C/poly

- $R_F \in$ FEQP/qpoly

További meggondolások

- $FBQP_U/poly = FBQSIZE_{NU}(poly(n))$

  ” $\supseteq$ ”: $FBQSIZE_{NU}(poly(n))$ programja belekódolható a súgásba

  ” $\subseteq$ ”: $FBQP_U/poly \subseteq FBQP_{NU}/poly \subseteq FBQSIZE_{NU}(poly(n))$

- $FEQP_U/qpoly \not\subset FBQSIZE_{NU}(o(2^{n/2}))$

Nyitott kérdés

Hány klasszikus bitre van szükség randomizált súgás esetén, olyan problémára, amire elég n qubit?

Láttuk, hogy R_F esetén $\Omega(2^{n/2})$ -re szükség van.

Van-e relációs probléma, melyre belátható, hogy többre is szükség van?

Köszönöm a figyelmet!