Kvantum-bonyolultságelméleti szeparáció relációs osztályokra

Csatári Jakab

2023.05.19.

Referencia

- A Qubit, a Coin, and an Advice String Walk Into a Relational Problem
  Scott Aaronson, Harry Buhrman, William Kretschmer
- https://arxiv.org/pdf/2302.10332.pdf
- 2023. Feb 20.

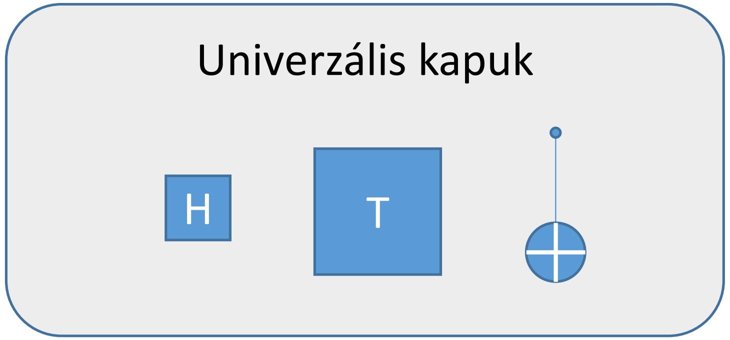
- A cikk első eredménye: FBQP/poly ≠ FBQP/qpoly

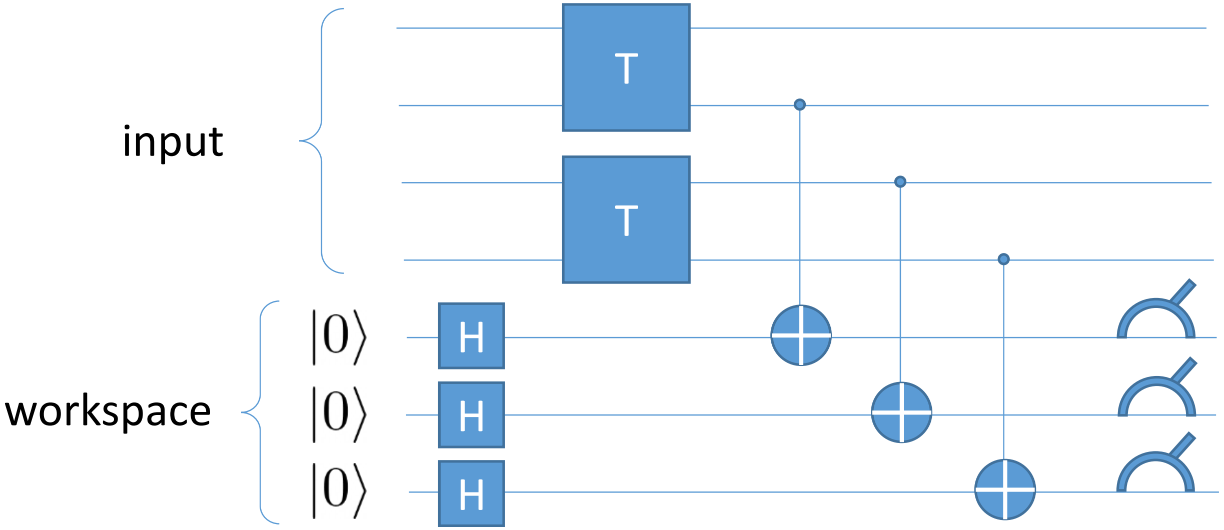
Kvantum-bonyolultságelmélet

- Kvantum analógok klasszikus bonyolultsági osztályokra?

P BPP NP

Kvantum-bonyolultságelmélet





Kvantum-bonyolultságelmélet

- Kvantum analógok klasszikus bonyolultsági osztályokra?

P	BPP	NP
↓	↓	↓
EQP	BQP	QMA

Kvantum-bonyolultságelmélet

- Kvantum analógok klasszikus bonyolultsági osztályokra?

P

↓

EQP

P: klasszikus, determinisztikus, poly(n) időben, mindig jól válaszol

EQP (Exact Quantum Polynomial): kvantum, poly(n) időben, mindig jól válaszol
FÜGG A KAPUKTÓL!

Kvantum-bonyolultságelmélet

- Kvantum analógok klasszikus bonyolultsági osztályokra?

P $\Downarrow$ EQP

BPP $\Downarrow$ BQP

BPP: klasszikus, randomizált, poly(n) időben, korlátos hibával (< 1/3)

BQP: kvantum, poly(n) időben, korlátos hibával (Nem függ a kapuktól)

Kvantum-bonyolultságe

- Kvantum analógok klasszikus bo

P	BPP	NP
↓	↓	↓
EQP	BQP	QMA

NP: klasszikus, nem-determinisztikus, poly(n) időben ($\forall x \exists y$ poly(n) méretű tanú: $A(x, y) = 1$)

QMA (Quantum Merlin-Arthur): kvantum, $\forall x \exists y$ kv. állapot: $A(x, y) = 1$ korlátos hibával

BPP

Def: Azon $L \subseteq \{0,1\}^*$ nyelvek osztálya, melyekre $\exists A$ polinomiális randomizált algoritmus, hogy:

$$Pr[A(x) = L(x)] \geq \frac{2}{3}$$

BPP

Def: Azon $L \subseteq \{0,1\}^*$ nyelvek osztálya, melyekre $\exists A$ polinomiális randomizált algoritmus, hogy:

$$Pr[A(x) = L(x)] \geq \cancel{\frac{2}{3}} \; \boxed{1 - \epsilon}$$

$$0 < \epsilon < \frac{1}{2}$$

BQP

Def: Azon $L \subseteq \{0,1\}^*$ nyelvek osztálya, melyekre $\exists A$ polinomiális kvantum algoritmus, hogy:

$$Pr[A(x) = L(x)] \geq 1 - \epsilon$$

Relációs probléma

- Döntési problémáknál:

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

- Relációs problémáknál:

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

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

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:

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

FBQP

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

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

$poly(|x| + 1/\epsilon)$

$(x, A(x|0^{1/\epsilon}))$

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

Súgás

- Input hosszától függő additional input: $\{s_n\}_{n \geq 1}$
- Ha $|x| = n$: $A(x|s_n) = y$
- Súgás mérete?
  Randomizált vagy determinisztikus?
  Klasszikus vagy kvantum?

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:

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

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:

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

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:

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

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:

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

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

FBQP súgásokkal

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

FBQP súgásokkal

$$\begin{array}{ccccc} \text{FBQP/poly} & \subseteq & \text{FBQP/rpoly} & \subseteq & \text{FBQP/qpoly} \\ & = & & \subsetneq & \end{array}$$

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

R_F reláció

Miért nem triviális? $$f_n(y) \oplus f_n(y \oplus x) = b$$

- Megkapjuk x -et
- Kiszámoljuk $f_n(y)$ és $f_n(y \oplus x)$ értékeket, tetszőleges y-ra
- b = a mod 2 összegük

R_F reláció

Miért nem triviális? $$f_n(y) \oplus f_n(y \oplus x) = b$$

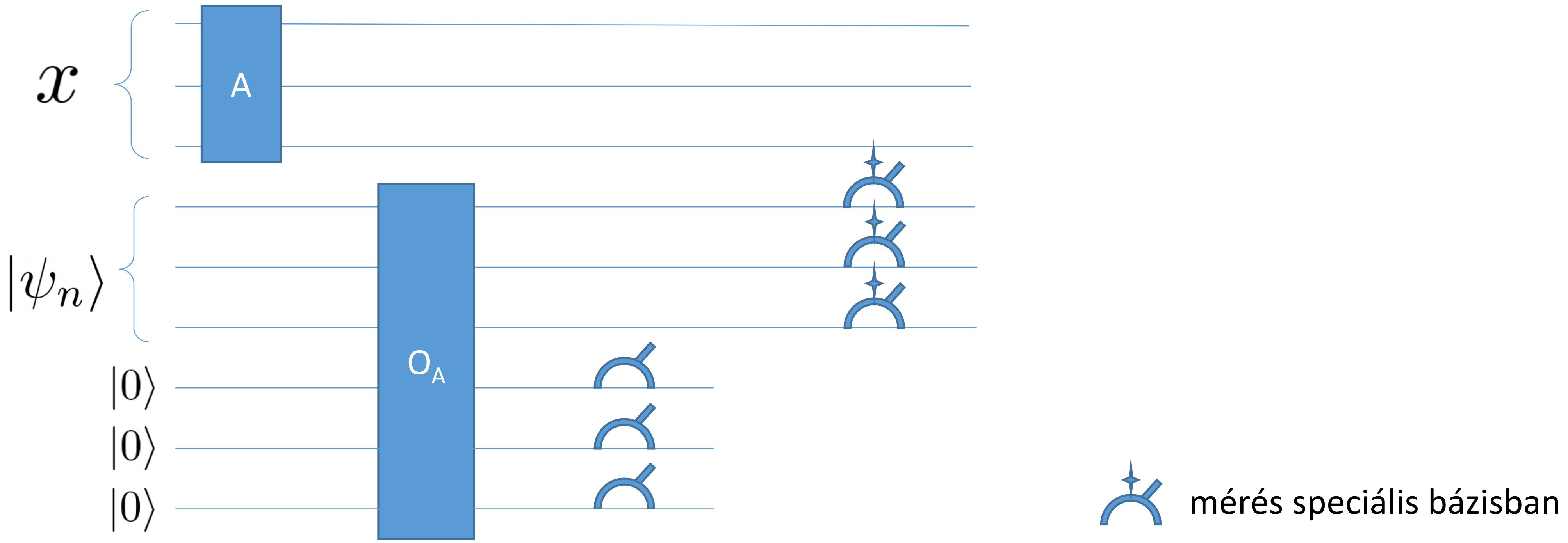
f_n : Ha a legjobb módszerünk kiszámolni a hozzá tartozó igazságtáblát, az exponenciális méret $O(2^n)$

Tfh. poly sok input eredményét beleprogramozzuk (pl. $f_n(y)$-t is)

Tetsz. x-re valószínű, hogy nem tudjuk $f_n(y \oplus x)$-et

Kvantum algoritmus

Szeretnénk algoritmust, ami $|\psi_n\rangle$ súgás mellett megoldja R_F-et
Ekkor $\forall F : R_F \in$ FBPQ/qpoly



Kvantum algoritmus

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

- 0. lépés: Ha $x = |0^n\rangle$, akkor tetszőleges y-ra return($(y, 0)$)

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

Kvantum algoritmus

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

- 1. lépés: Keressünk $A \in \mathbb{F}_2^{n-1\times n}$ mátrixot, aminek a nulltere pontosan $\{0, x\}$

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

Kvantum algoritmus

- 1. lépés: Keressünk $A \in \mathbb{F}_2^{n-1 \times n}$ mátrixot, aminek a nulltere pontosan $\{0, x\}$

Például $n = 3 \quad x = 001$

$$001 \to 00$$

Kvantum algoritmus

- 1. lépés: Keressünk $A \in \mathbb{F}_2^{n-1 \times n}$ mátrixot, aminek a nulltere pontosan $\{0, x\}$

Például $n = 3 \quad x = 001$

$$001 \to 00$$
$$010 \to 10$$
$$100 \to 01$$

Kvantum algoritmus

- 1. lépés: Keressünk $A \in \mathbb{F}_2^{n-1 \times n}$ mátrixot, aminek a nulltere pontosan $\{0, x\}$

Például $n = 3 \quad x = 001$

$$\begin{aligned} 001 &\to 00 \\ 010 &\to 10 \\ 100 &\to 01 \end{aligned}$$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Kvantum algoritmus

Például $n = 3 \quad x = 001$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{array}{ll} 000 \to 00 & 100 \to 01 \\ 001 \to 00 & 101 \to 01 \\ 010 \to 10 & 110 \to 11 \\ 011 \to 10 & 111 \to 11 \end{array}$$

Kvantum algoritmus

Például $n = 3 \quad x = 001$

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{aligned} 000 &\to 00 \qquad & 100 &\to 01 \\ 001 &\to 00 & 101 &\to 01 \\ 010 &\to 10 & 110 &\to 11 \\ 011 &\to 10 & 111 &\to 11 \end{aligned}$$

$$Ay = A(x+y)$$

Kvantum algoritmus

Vagy, ha például $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Kvantum algoritmus

Vagy, ha például $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{array}{ll} 000 \rightarrow 00 & 100 \rightarrow 11 \\ 001 \rightarrow 11 & 101 \rightarrow 00 \\ 010 \rightarrow 01 & 110 \rightarrow 10 \\ 011 \rightarrow 10 & 111 \rightarrow 01 \end{array}$$

Kvantum algoritmus

Vagy, ha például $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{array}{ll} 000 \to 00 & 100 \to 11 \\ 001 \to 11 & 101 \to 00 \\ 010 \to 01 & 110 \to 10 \\ 011 \to 10 & 111 \to 01 \end{array}$$

$$Ay = A(x+y)$$

Kvantum algoritmus

$$A0 = Ax = 0$$

$$A(x + y) = Ax + Ay = Ay$$

Kvantum algoritmus

Vagy, ha például $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\begin{array}{ll} 000 \to 00 & 100 \to 11 \\ 001 \to 11 & 101 \to 00 \\ 010 \to 01 & 110 \to 10 \\ 011 \to 10 & 111 \to 01 \end{array}$$

$$Ay = A(x + y)$$

Kvantum algoritmus

Indirekt: $z \notin \{y, y + x\}$

$$Ay = Az$$

De ekkor:

$$0 = Ay - Az = A(y - z)$$

Kvantum algoritmus

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

- 2. lépés: Mérjük meg az $|Ay\rangle$ regisztert a számítási bázisban
  Így az $|y\rangle$ regiszter összeomlik:

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

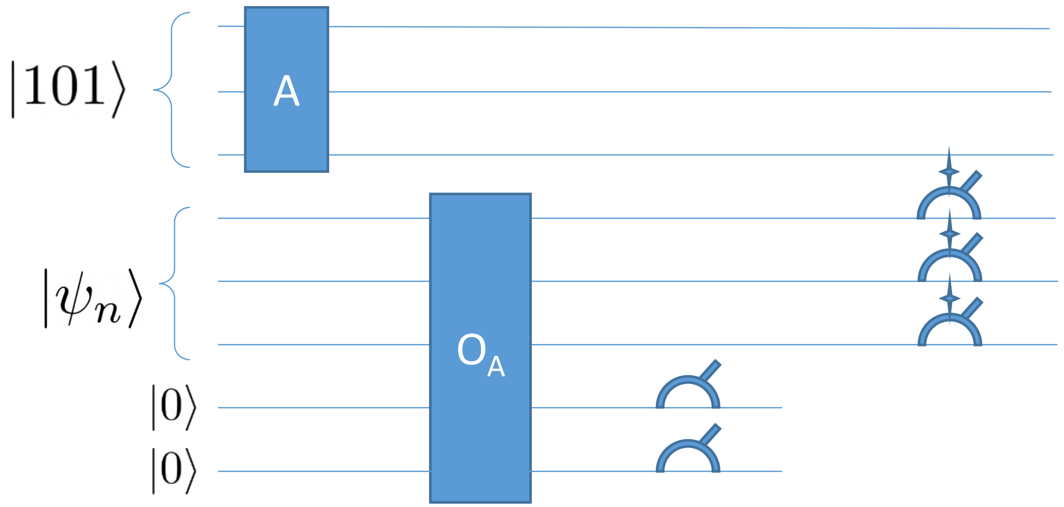
Kvantum algoritmus

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

- 3. lépés: Mérjük meg az $\{|y\rangle \pm |y \oplus x\rangle\}$ bázisban

Mérés (1 val)	$\lvert y\rangle + \lvert y \oplus x\rangle$	$\lvert y\rangle - \lvert y \oplus x\rangle$	$\lvert y\rangle - \lvert y \oplus x\rangle$	$\lvert y\rangle + \lvert y \oplus x\rangle$
$f_n(y)$	0	0	1	1
$f_n(y \oplus x)$	0	1	0	1

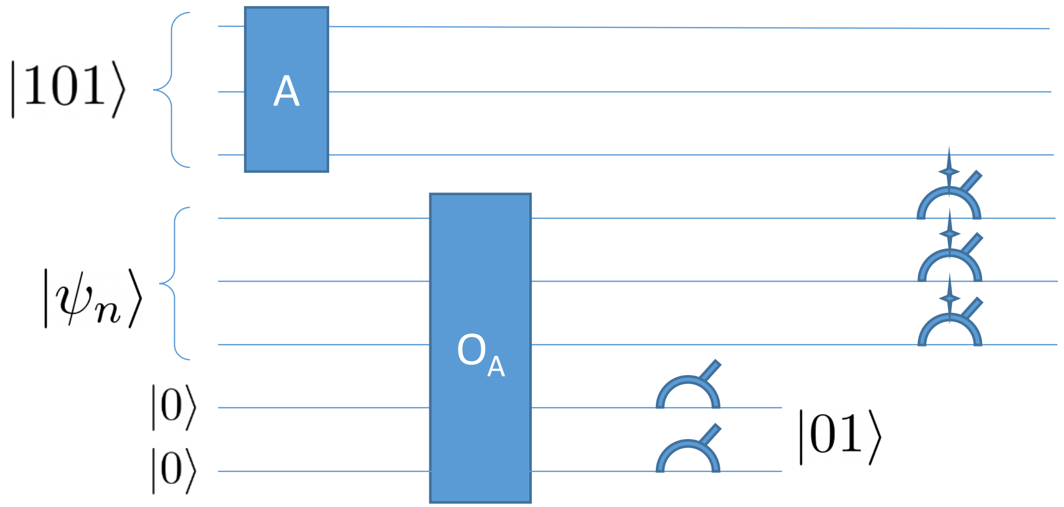
Kvantum algoritmus példa



1. $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Kvantum algoritmus példa



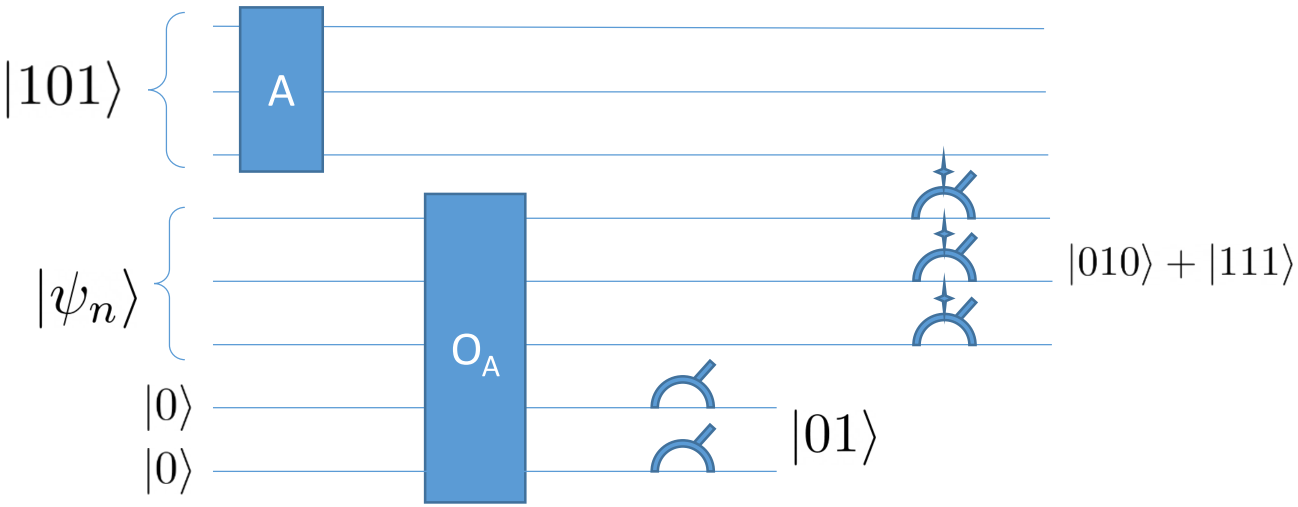
1. $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

2. $|01\rangle$ -et mérünk

$$\frac{1}{\sqrt{2}}((-1)^{f_n(010)}|010\rangle + (-1)^{f_n(111)}|111\rangle)$$

Kvantum algoritmus példa



1. $x = 101$

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

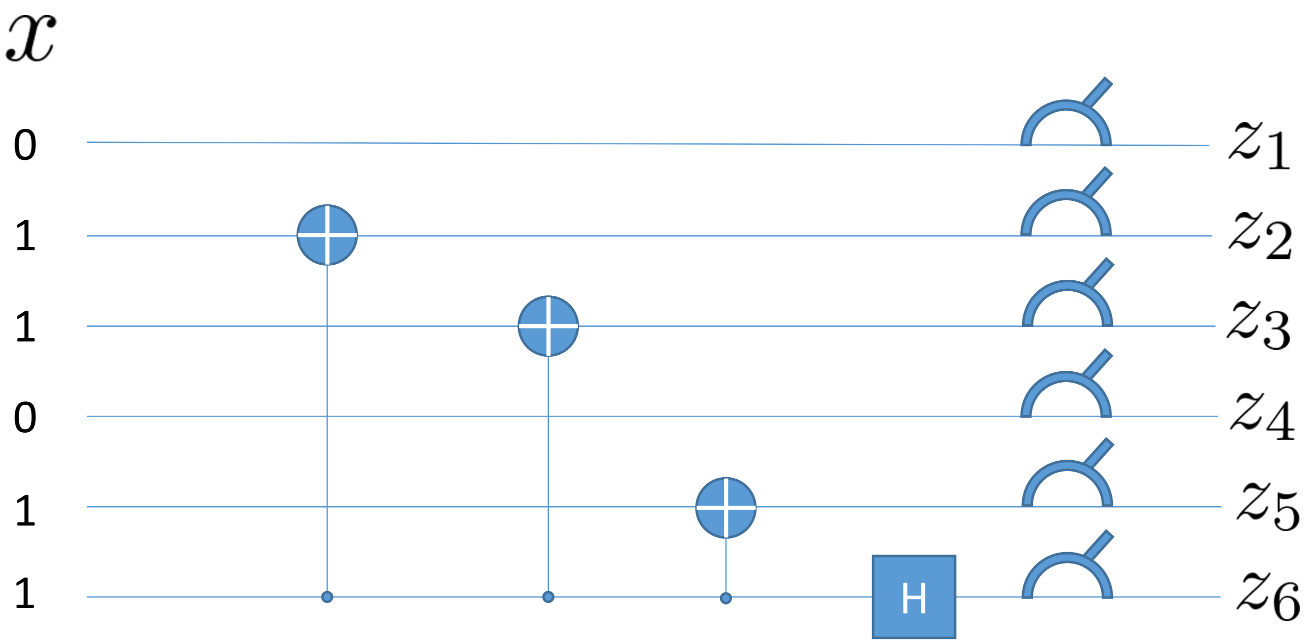
2. $|01\rangle$ -et mérünk

$$\frac{1}{\sqrt{2}}\left((-1)^{f_n(010)}|010\rangle + (-1)^{f_n(111)}|111\rangle\right)$$

3. $f_n(010) = 1 \quad f_n(111) = 1$

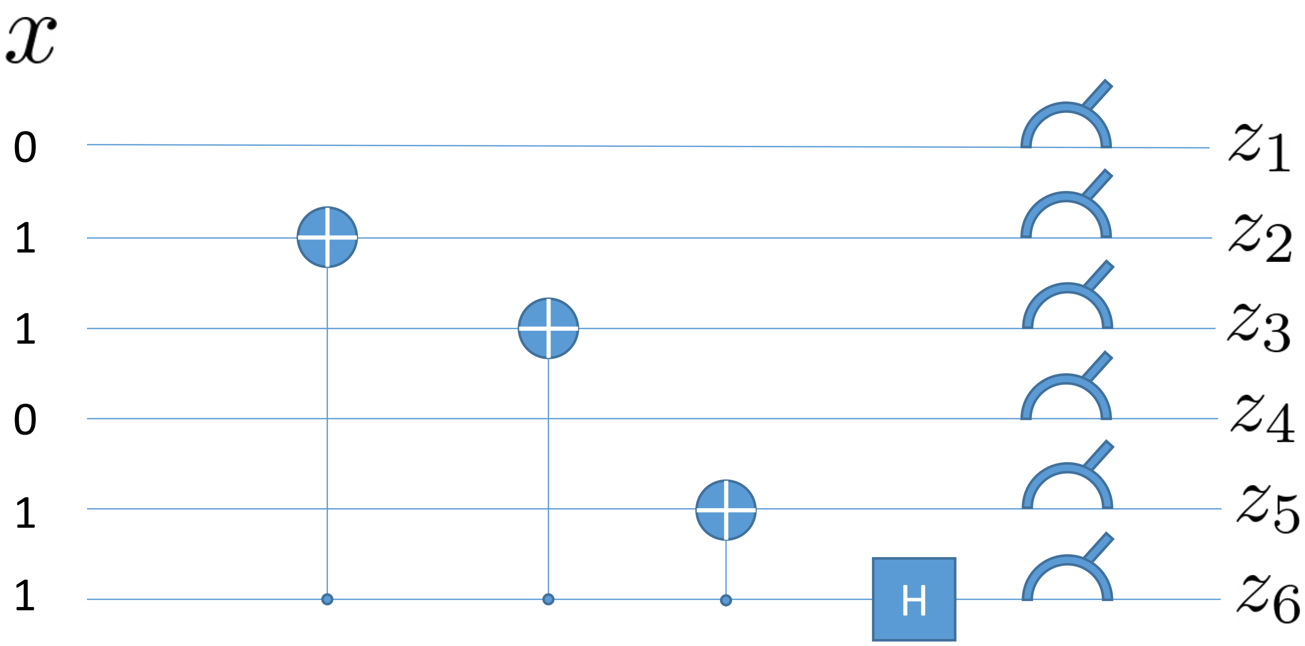
$$\frac{1}{\sqrt{2}}(-|010\rangle - |111\rangle) \longrightarrow |010\rangle + |111\rangle$$

Mérés a speciális bázisban



$$(y, b) = (z_1 z_2 z_3 z_4 z_5 0, z_6)$$

Mérés a speciális bázisban



$$(y, b) = (z_1 z_2 z_3 z_4 z_5 0, z_6)$$

$$\frac{1}{\sqrt{2}}(-\underbrace{|010101\rangle}^{y} + \underbrace{|001110\rangle}^{y \oplus x})$$

$$\Big\downarrow \text{CNOT}$$

$$\frac{1}{\sqrt{2}}(-|001111\rangle + |001110\rangle)$$

$$\Big\downarrow \text{H}$$

$$\frac{1}{2}(-|001111\rangle + |001110\rangle$$
$$-|001111\rangle - |001110\rangle)$$

A Hadamard miatt megtudjuk a relatív állapotukat

Tehát $R_F \in$ FBQP/qpoly

Ha A az előbbi kvantum algoritmus

$$Pr[(x, A(x||\psi_n\rangle)) \in R_F] = 1 > 1 - \epsilon$$

Kvantum kommunikációs bonyolultság

Egyirányú kommunikációs probléma:

(x) Alice inputja, (y) Bob inputja T: (x,y) -> * feladat

Alice kommunikálhat Bob-nak, de Bob-nak kell megoldani

D(T): min (determinisztikusan) küldött bitek száma, hogy tetsz (x,y)-ra meg tudja oldani Bob

Kvantum kommunikációs bonyolultság

D(T): (determinisztikusan) küldött bitek száma

R(T): (hiba korlátos) randomizált protokollal küldött – shared randomness

Q(T): (hiba korlátos) kvatum protokollal küldött

$D(T) \geq R(T) \geq Q(T)$

Hidden Matching Probléma

- Exponential Separation of Quantum and Classical One-Way Communication Complexity
  Ziv Bar-Yossef, T. S. Jayram, Iordanis Kerenidis (2006)
- https://www.irif.fr/~jkeren/jkeren/CV_Pubs_files/BJK04.pdf

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

Kérdés: mennyit kell Alice-nak (randomizáltan) kommunikálnia?

Kell:
- $(i, j) \in M$ ← wlog. feltehető, hogy teljesül
- $b = z_i \oplus z_j$

Kérdés milyen hiba korlátot szeretnénk?
1/2 val. jó output triviális

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

$x \neq 0^n$

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

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

Alice kommunikációja megfelel a súgásnak:
Tehát */rpoly $\Leftrightarrow$ randomizált egyirányú kommunikáció

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

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

Kapcsolat R_F -fel

Előző Tétel miatt:

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

Ha $F' \sim \{F \,|F = \{f_n\}_{n\geq 1}\}$, 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: $\exists F : R_F \notin$ FBQP/poly = FBQP/rpoly

Meg lehet gondolni

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

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

- $R_F \in$ FEQP/qpoly

Meg lehet gondolni

- $FBQP_U/poly = FBQSIZE_{NU}(poly(n))$
  - „$\supseteq$": $FBQSIZE_{NU}(poly(n))$ programja belekódolható a súgásba
  - „$\subseteq$": $FBQP_U/poly \subseteq FBQP_{NU}/poly \subseteq FBQSIZE_{NU}(poly(n))$

$$FBQP_U/qpoly \supsetneq FBQSIZE_{NU}(poly(n)),$$

sőt $FBQP_U/qpoly \supsetneq FBQSIZE_{NU}(2^{O(n)})$

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 többre is szükség van?
Milyen erős a szeparáció $\Omega(2^{n/2})$ és $\Omega(2^n)$ között?

Köszönöm a figyelmet!