Kvantum-bonyolultságelméleti szeparáció relációs osztályokra

Csatári Jakab

Témavezető: Gilyén András

2023

Bevezetés

A félév során egy idei cikk eredményét dolgoztam fel. *A Qubit, a Coin, and an Advice String Walk Into a Relational Problem* egy olyan kvantum-bonyolultságelméleti cikk, melyben a szerzők Scott Aaronson, Harry Buhrman és William Kretschmer arra keresik a választ, hogy különböző súgások hogyan érintenek kvantum bonyolultsági osztályokat. Egy régebbi, 2006-os cikk eredményét felhasználva belátták, hogy $\mathbf{FBQP/poly} \neq \mathbf{FBQP/qpoly}$. A beszámolómban erről írok, egy ezzel kapcsolatos nyitott kédésről, illetve teszek egy meggondolást a relációs kvantumalgoritmusok uniform vs nem-uniform változatáról.

1. Kvantumelméleti előkészületek

Míg a klasszikus számítási modellek alapegysége egy két lehetséges (0 vagy 1) állapotban levő bit, a kvantumszámítás úgynevezett qubitekre épül. Egy qubit e két állapot szuperpozíciója, melyet algebrailag a következő módon tudunk leírni:

Egy qubit állapota $|\psi\rangle := a \cdot |0\rangle + b \cdot |1\rangle$, ahol $a, b \in \mathbb{C}$ és $|a|^2 + |b|^2 = 1$.

A 0 bitnek a $|0\rangle := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ felel meg, míg 1-nek az $|1\rangle := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, a-t és b-t amplitúdóknak hívjuk.

Egy több qubites rendszer összekapcsolt állapotát az állapotok tenzorszorzatával tudjuk leírni, például egy 2 qubites rendszer bázisállapotai:

$$|00\rangle := |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; |01\rangle := |0\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \; |10\rangle := |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; |11\rangle := |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

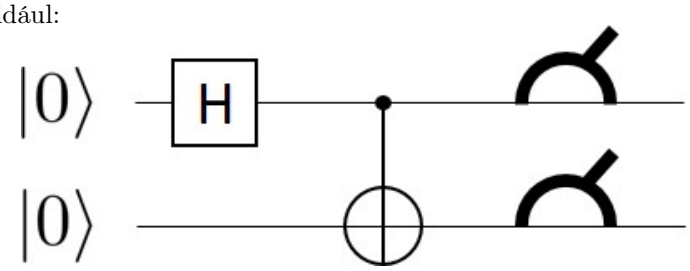
Egy $|\psi\rangle := a \cdot |0\rangle + b \cdot |1\rangle$ szuperpozícióban lévő qubit állapotát nem ismerjük, hogy mondhassunk róla valamit, meg kell mérjük a számítási bázisban, ekkor $|a|^2$ valószínűséggel $|0\rangle$-t mérünk és $|b|^2$ valószínűséggel $|1\rangle$-et. Viszont egy mérés során az állapota is megváltozik, összeomlik a mért állapotra.

Általánosabban, ha egy n qubites állapotot (regisztert) megmérünk:
$|\psi\rangle = a_0|0\rangle + a_1|1\rangle + ... + a_{2^n-1}|2^n - 1\rangle$ (most $\sum_{i=0}^{2^n-1} |a_i|^2 = 1$), akkor $|a_i|^2$ valószínűséggel omlik össze az $|i\rangle$ állapotba.

A $2^n \times 2^n$ dimenziós unitér mátrixok egy n qubites állapotot képeznek le egy másik állapotba, ezeket kvantum kapuknak hívjuk. Néhány ismertebb kapu **I**, **X**, **Z**, Hadamard (**H**), Controlled-NOT (**CNOT**), Toffoli (**T**), ezek közül a beszámolóban csak a Hadamard-ra és a CNOT-ra lesz szükség:

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \; \mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Egy kvantumalgoritmuson valahány qubitre alkalmazott kvantum kapuk sorát, illetve rájuk alkalmazott méréseket értjük - egy algoritmusban tipikusan néhány előre meghatározott kaput használhatunk, melyek konstans sok qubiten hatnak és együtt univerzálisak (azaz bármely kapu leírható a kombinációjukból). Egy kvantumalgoritmus pedig leírható kvantumáramkörrel, melyet konvenció szerint úgy szoktunk ábrázolni, hogy egy qubitnek egy vonalat rajzolunk, majd balról jobbra haladva ábrázoljuk, milyen kaput alkalmazunk rajta, illetve hogy mikor mérjük meg. Például:



Ahol **H** a Hadamard kapu, a középső kapu egy **CNOT** melyben az első qubit a control bit, végül mindkettőt megmérjük.

2. Bonyolultságelméleti előkészületek

A bonyolultságelmélet célja különböző számítási problémák kategorizálása. Az egyik legismertebb problémaosztály **P** például olyan nyelveket tartalmaz, melyekhez létezik az input méretében polinomiális futásidejű ***klasszikus*** algoritmus, ami eldönti az inputról, hogy benne van-e a nyelvben vagy sem.

Kvantumalgoritmusokhoz hasonlóan lehet definiálni bonyolultsági osztályokat, például **P** kvantum analógja: **EQP** (Exact Quantum Polynomial) amibe azon nyelvek tartoznak, melyekhez létezik polinomiális futásidejű ***kvantum*** algoritmus, ami eldönti az input nyelvbeliségét. Az hogy egy osztályba milyen nyelvek tartoznak, függhet az univerzális kapuk halmazától, ez a helyzet például **EQP** esetében is. Viszont vannak "szerencsésebben" definiált osztályok, mint **BQP**, amit a következő részben definiálok - a **BQP**-ben levő nyelvek halmaza mindig ugyanaz függetlenül a megengedett kapuktól.

Kvantumalgoritmus esetén a futásidőt az őt leíró kvantumáramkör kapuinak számával mérjük. Kvantum-bonyolultsági osztályok esetén is beszélhetünk uniform osztályokról. Egy osztály akkor uniform, ha létezik determinisztikus Turing-gép, ami polinomiális időben futva megadja az input hosszához szükséges áramkört.

3. Definíciók

Most néhány definicióval vezetem elő a cikk állítását, miszerint **FBQP/poly** $\neq$ **FBQP/qpoly**.

Definíció (BPP): Azon $L \subseteq \{0,1\}^*$ nyelvek osztálya, melyekre $\exists A$ polinomiális (klasszikus) algoritmus, hogy:

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

Itt $A(x)$ alatt az algoritmus outputját értem x inputra, illetve $L(x) \in \{0,1\}$ azt jelenti, hogy x benne van-e L-ben. Tehát **BPP** esetén megengedünk $\frac{1}{3}$ valószínűséget, hogy hibázzon az algoritmus. Viszont megjegyzem, hogy a " $\geq \frac{2}{3}$" a definícióban önkényes, bármely $0 < \epsilon < \frac{1}{2}$ esetén írhatunk helyette " $\geq 1 - \epsilon$" -t is - belátható, hogy a módosítással is ugyanazok a nyelvek tartoznak az osztályba.

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

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

Döntési problémák esetén $x \in \{0,1\}^*$ inputra $\{0,1\}$ outputot keresünk (1 ha $x \in L$, különben 0). Relációs problémák esetén ezzel szemben több output is megfelelő lehet:

Definíció (Relációs probléma): Egy $R \subseteq \{0,1\}^* \times \{0,1\}^*$ -et relációnak hívunk. Feltesszük, hogy R olyan, hogy $\forall x\ \exists y : (x,y) \in R$. Egy probléma relációs probléma, ha $x \in \{0,1\}^*$ input esetén olyan $y \in \{0,1\}^*$ outputot keresünk, melyre $(x,y) \in R$.

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

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

Egy bonyolultsági osztályt elláthatunk súgással. Ez alatt azt értjük, hogy megengedjük, hogy az algoritmus mellé megadjunk egy $\{s_n\}_{n\geq 1}$ súgás halmazt, és amikor x inputra futtatjuk, akkor az algoritmusunk használhatja az $s_{|x|}$ súgást is a futásához.

Definíció (FBQP/poly): 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 $\forall x \in \{0,1\}^*$:

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

Definíció (FBQP/rpoly): 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 $\forall x \in \{0,1\}^*$:

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

Definíció (FBQP/qpoly): 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 $\forall x \in \{0,1\}^*$:

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

Itt $|\psi_n\rangle$ -nek megengedjük, hogy poly(n) qubit tetszőleges szuperpozíciója legyen.

4. FBQP/poly $\neq$ FBQP/qpoly

Először is jegyezzük meg, hogy triviálisan **FBQP/poly** $\subseteq$ **FBQP/rpoly** $\subseteq$ **FBQP/qpoly**, hiszen egyrészt a determinisztikus súgás speciális esete annak, hogy egy eloszlás szerint választjuk, másrészt poly(n) qubit amplitúdóit megfelelően választva az eloszlást belekódolhatjuk a kvantumsúgásunkba.

A cikkben a Hoeffding egyenlőtlenséget használva belátják, hogy **FBQP/poly** = **FBQP/rpoly**. Tehát itt a randomizáltság a súgásban nem ad többletet a kvantumalgoritmusunknak. Másfelől viszont az is igaz, hogy **FBQP/rpoly** $\subsetneq$ **FBQP/qpoly**, ezt fogjuk belátni.

A szeparáció ötlete a következő: definiálunk egy R_F, F-től függő relációt és belátjuk, hogy

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

Definíció (R_F): Legyen $F := \{f_n\}_{n\geq 1}$, ahol $f_n : \{0,1\}^n \to \{0,1\}$ boolean függvény. Ekkor

$$R_F := \{(x,(y,b)) \mid f_n(y) \oplus f_n(y \oplus x) = b\} \qquad \text{ahol } x \in \{0,1\}^n, y \in \{0,1\}^n, b \in \{0,1\}$$

Mivel f_n-ek lehetnek nagyon specifikusak, természetesen F lehet olyan, hogy $\forall f_n$-et ki tudjunk számolni polinomiális időben tetszőleges inputra. Ha erről van szó, akkor persze R_F benne van **FBQP/poly**-ban is, sőt még szűkebb osztályokban is. A reláció nehézségét az adja, hogy véletlen választott F szinte biztosan eléggé komplex lesz ahhoz, hogy ne ismerjünk gyorsabb algoritmust f_n kiszámolására, mint a triviális n mély döntési fát (ami viszont már exponenciális).

1) Belátjuk, hogy $\forall F$: $R_F \in \mathbf{FBQP/qpoly}$:

Most mutatok egy kvantumalgoritmust, amely tetszőleges F-re megoldja az R_F relációt, kvantum súgás mellett. Legyen $|\psi_n\rangle$ a súgás n hosszú inputhoz:

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

Először is tegyük fel, hogy $x \neq |0^n\rangle$, ezt megtehetjük, ugyanis ha a csupanulla inputot kapjuk, akkor egyszerűen válaszolhatjuk $(y, 0)$ -át tetszőleges $y \in \{0,1\}^n$ -nal, hiszen ekkor $f_n(y) \oplus f_n(y \oplus 0) = f_n(y) \oplus f_n(y) = 0$.

Keressünk $A \in \mathbb{F}_2^{n-1\times n}$ mátrixot, melynek a nulltere pontosan $\{0, x\}$, majd rendeljük hozzá a súgásunkhoz az $n-1$ hosszú $|Ay\rangle$ regisztert:

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

Vegyük észre, hogy ha A nulltere pontosan $\{0, x\}$, akkor

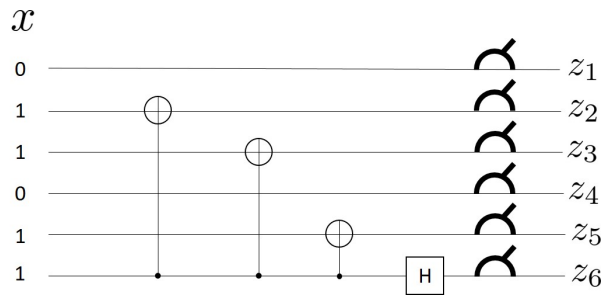
- $\forall y : Ay = 0 \oplus Ay = Ax \oplus Ay = A(x \oplus y)$
- Ha $z \notin \{y, y \oplus x\}$, akkor $Ay \neq Az$. Mert indirekt: $0 = Az \oplus Ay = A(z \oplus y) \neq 0$

Tehát, ha megmérjük az $|Ay\rangle$ regisztert a számítási bázisban, akkor az $|y\rangle$ regiszter összeomlik a következőre:

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

Ezt követően, ha megmérjük az $|y\rangle$ regiszter állapotát az $\{|y\rangle \pm |y \oplus x\rangle\}$ bázisban, akkor 1-valószínűséggel pontosan akkor mérünk $|y\rangle + |y \oplus x\rangle$-et, ha $f_n(y) = f_n(y \oplus x)$, különben 1-valószínűséggel $|y\rangle - |y \oplus x\rangle$-et mérünk.

A speciális mérést ebben a bázisban a kövekezőképpen csinálhatjuk meg: Az áramkört x függvényében épitjük fel, ahol x helyiértéke 0, ott nem csinálunk semmit, csak a végén megmérjük a számítási bázisban. Ahol pedig 1-es van ott az egyiküket control qubitnek választjuk és a többieket össze **CNOT**-oljuk vele, végül a control qubitünkre elvégzünk egy **H** transzformációt. Ha mindez megvan akkor mérjük meg a qubiteinket a számítási bázisban. Például, ha $x = |011011\rangle$:



Ekkor, ha $z_1z_2z_3z_4z_5z_6$-ot mérünk, azt állítom, hogy $(y, b) := (z_1z_2z_3z_4z_5 0, z_6)$. Ehhez azt kell meggondolni, hogy a **CNOT**-ok úgy változtatják meg az állapotunkat, hogy csak két lehetséges mérésünk legyen, az egyik y, a másik pedig csak annyiban tér el, hogy ott a control qubit 1. Míg a **H** éppen a megfelelőt ejti ki a kettő közül (ez f_n-től függ).

Tehát $\forall F$ esetén ez az algoritmus 1-valószínűséggel jó outputot ad, így $R_F \in \mathbf{FBQP/qpoly}$.

2) Belátjuk, hogy $\exists F$: $R_F \notin \mathbf{FBQP/poly}$=$\mathbf{FBQP/rpoly}$. Ehhez felhasználjuk a hidden matching problémának egy eredményét.

Definíció (Hidden Matching): A HM_N probléma a következő: Alice kap egy $z \in \{0,1\}^N$ inputot, Bob pedig egy $M \in \mathcal{M}_N$ teljes párosítást $\{1, ..., N\}$-en. Alice kommunikálhat Bob-nak (fordítva nem) és Bob-nak olyan (i, j, b) outputot kell adnia, melyre $(i, j) \in M$ és $b = z_i \oplus z_j$ (ahol $i, j \in \{1, ..., N\}$, $b \in \{0, 1\}$).

Ekkor ha $\mathcal{M}_N$-től azt várjuk el, hogy $\mathcal{M}_N = \{M_1, M_2, ..., M_m\}$, ahol ezek a teljes párosítások páronként éldiszjunktak és $m = \Omega(N)$. Akkor a következő 2006-os eredmény igaz:

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

Ez gyakorlatilag azt jelenti, hogy nincs lényegében jobb randomizált algoritmus a triviális-on kívül, miszerint Alice véletlenszerűen küld $O(\sqrt{N})$ darab z_i bitet, Bob pedig ha kapott olyan párt ami eleget tesz $(i,j) \in M$-nek, akkor tud jól válaszolni. A birthday paradoxon szerint ugyanis, ha Alice T bitet küld, akkor

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

Ekkor viszont, ha $T = c \cdot \sqrt{N}$, akkor ez $\frac{c^2}{2}$, tehát már konstans c-re is nagy valószínűséggel kapunk élet.

Térjünk vissza R_F-hez, ha adott nekünk f_n, akkor a hozzá tartozó igazságtábla egy $\{0,1\}^{2^n}$ bitsorozat. Míg ha $x \neq 0$, akkor $M_x := (y, y \oplus x)$ minden x-re egy teljes párosítás $N = 2^n$ elemen, minden M_x páronként éldiszjunkt és minden inputhoz különböző M_x tartozik, így a számuk $2^n - 1 = \Omega(2^n)$. Ha Alice ismeri az igazságtáblát, Bob pedig kap egy M_x teljes párosítást, akkor ez egy HM_{2^n} probléma (ahol Alice a súgásunk, Bob pedig az algoritmusunk). Az előző tétel miatt pedig ahhoz, hogy $\geq \frac{7}{8}$ valószínűséggel jól válaszoljon az algoritmus $\Omega(2^{n/2})$ bit súgás szükséges.

Tehát, ha $F' \sim \{F | F = \{f_n\}_{n \geq 1}\}$ egy uniform random eleme az összes lehetséges F-nek, akkor ahhoz hogy $\geq \frac{7}{8}$ valószínűséggel jól fusson fix n-re - exponenciális súgásra van szükség. Tehát

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

Mivel minden n-re ezek a valószínűségek függetlenek:

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

Tehát 1 valószínűséggel létezik F, amire $R_F \notin \mathbf{FBQP/poly}$=$\mathbf{FBQP/rpoly}$.

5. További meggondolások

- A kvantum algoritmusunkban 1 valószínűséggel adunk jó outputot, így azt is látjuk, hogy $\forall F : R_F \in \mathbf{FEQP/qpoly}$.
- $R_F \notin \mathbf{FBQP/poly}$ -nál nem használtuk ki, hogy a poly súgás mögött **FBQP** algoritmus van, gyakorlatilag tetszőleges uniform **C** osztályra igaz, hogy $R_F \notin \mathbf{C/poly}$.
- Jelöljük $\mathbf{C}_U$ -val hogy egy **C** osztály uniform, $\mathbf{C}_{NU}$ -val hogy nem-uniform.

  Ekkor $\mathbf{FBQP}_U\mathbf{/poly} = \mathbf{FBQSIZE}_{NU}\mathbf{(poly(}n\mathbf{))}$ - hiszen polinomiális méretű program áramköre belekódolható a súgásba, másrészt $\mathbf{FBQP}_U\mathbf{/poly} \subseteq \mathbf{FBQP}_{NU}\mathbf{/poly} \subseteq \mathbf{FBQSIZE}_{NU}\mathbf{(poly(}n\mathbf{))}$.
- A tételnek egyúttal az is következménye, hogy $\mathbf{FEQP}_U\mathbf{/qpoly} \not\subset \mathbf{FBQSIZE}_{NU}(o(2^n))$, hiszen a kvantum-súgásos algoritmus 1 valószínűséggel megoldja a HM_{2^n}-et, míg ehhez $\Omega(2^{n/2})$ méretű klasszikus súgásra van szükség így $\mathbf{FEQP}_U\mathbf{/qpoly} \not\subset \mathbf{FBQP}_U\mathbf{/size}(o(2^n)) = \mathbf{FBQSIZE}_{NU}(o(2^n))$ (az "=" az előző ponthoz hasonlóan következik).

Nyitott kérdés: Ha egy relációs problémát n qubites súgással meg lehet oldani, akkor hány klasszikus bites súgásra van szükség ugyanehhez? Létezik-e probléma, ahol $\Omega(2^{n/2})$-nél többre van szükség, vagy ennyi minden esetben elég? Ezzel kapcsolatos eredmények, hogy sampling problémák esetén létezik olyan, amire $\Omega(2^n)$ bitre szükség van. Ezzel szemben döntési és promise problémák esetén $O(2^{n/2})$ minden problémára elég. A cikkben hajlanak arra, hogy valószínűbb, hogy a válasz 2^n-hez közelebb van, mint $2^{n/2}$-hez.

Felhasznált Irodalom

[1] A Qubit, a Coin, and an Advice String Walk Into a Relational Problem - Scott Aaronson, Harry Buhrman, William Kretschmer (2023): https://arxiv.org/abs/2302.10332v1

[2] Exponential Separation of Quantum and Classical One-Way Communication Complexity - Ziv Bar-Yossef, T. S. Jayram, Iordanis Kerenidis (2006): https://epubs.siam.org/doi/abs/10.1137/060651835