Beszámoló
Kvantumszámítástudomány, Algebrai kvantumalgoritmusok

Csáji Gergely

November 2020

1 Kvantum algoritmusok

A fő motivációim a terület kutatása iránt a tavaly megírt szakdolgozatom során, a kvantummechanika különös és meghökkentő tulajdonságainak megismerése volt, illetve a kíváncsiság, hogy miképpen lehet ezeket a tulajdonságokat és a mögöttük rejlő matematikát kihasználni, például a számítástudományban. A kutatómunkám elején a fő cél a kvantumszámítógépek működésének és az alapvető modellek megértése volt a cél. Az első olvasott irodalom Chris Bernhard: Kvantumszámítástudomány közérthetően című könyve [1] volt, majd ezután pár matematikailag mélyebb, az alapvető algoritmusokat tartalmazó cikk. A későbbiek megértéséhez itt is adok egy rövid bevezetőt a kvantumszámítástudomány alapjaiba.
A kvantumszámítógépeknek több modellje is létezik, pl kvantum- Turing gépekkel, de a legelterjedtebb a kvantum-áramkör modell, ezt ismertetem itt is.
A legfőbb különbség a hagyományos és a kvantumszámítógépek között, hogy a kvantumszámítógép bitek helyett qubiteket használ. Egy qubit lehet bármilyen $a|0\rangle + b|1\rangle$, $a, b \in \mathbb{C}, |a|^2 + |b|^2 = 1$ alakú állapotban. Viszont, mikor ránézünk a qubitre, azaz megmérjük, akkor összeomlik egy klasszikus bitté, méghozzá $|a|^2$ valószínűséggel 0-vá, $|b|^2$ valószínűséggel 1-gyé. Ha n qubitünk van, akkor azok már tetszőleges $\sum_{i=0}^{2^n-1} a_i|i\rangle$, $\sum |a_i|^2 = 1$ alakú állapotban lehetnek, ahol $|i\rangle$ az i 2-es számrendszerbeli alakjának megfelelő bitsorozat. Azaz egy qubit-sorozat lehetséges állapotai, az összes klasszikus bitsorozat, mint bázisvektorok által generált komplex Hilbert-tér bázisvektorai.
A kvantum áramkörös modell a következő: A számítás egy lépéseként alkalmazhatunk egy U unitér mátrixot valamely qubitekre, majd a végén (akár közben is, igazából ez a két modell ekvivalens) alkalmazhatunk méréseket a qubiteken. Amennyiben néhány qubitre mérést alkalmazunk, a maradék összeomlik azon állapotok szuperpozíciójába, amelyek megmért bitek helyén lévő bitjei a kapott értékkel egyeznek meg. Általában legfeljebb 2 qubiten ható mátrixokat engedünk meg egy lépésben, a többit fixen hagyjuk. Ezt precízebben úgy tesszük meg, hogy vesszük az U mátrix és az identitásmátrix tenzorszorzatát a többi

qubiten. Az $|i\rangle$ bázisvektort pedig a koordinátáknak megfelelő 2-dimenziós vektorok tenzorszorzatának tekintjük, ahol $|0\rangle = (1,0)^T$ és $|1\rangle = (0,1)^T$. A lépésszámot ekkor a szükséges kvantumkapuk számának definiáljuk.
Példa egy kvantum kapura a Hadamard kapu, mely a következőt csinálja: $|0\rangle$-hoz hozzárendeli $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$-t, illetve $|1\rangle$-hez $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$-t. Ha egy n hosszú $|i\rangle$ állapotunk van, akkor minden qubitre alkalmazva egy Hadamard kaput könnyen kiszámolható, hogy $\frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_2^n} (-1)^{\langle x,y \rangle} |y\rangle$-t kapunk, ahol a skalárszorzatot *mod* 2 kell érteni.
Ezek alapján már könnyen megérthető az egyik első, a klasszikusnál exponenciálisan hatékonyabb kvantum algoritmus, Simon algoritmusa. Itt a probléma a következő: Adott egy $f : \mathbb{Z}_2^n \to S \subset \{0,1\}^l$ függvény, amire tudjuk, hogy $\exists s \in \mathbb{Z}_2^n$, hogy $f(x) = f(y) \iff x = y$ vagy $x = y + s$. A feladat s megtalálása, feltéve, hogy f polinom időben kiszámolható, vagy létezik orákulum, aki kiszámolja, azaz egy olyan U_f unitér transzformáció, ami $|x\rangle|0^l\rangle$-hoz hozzárendeli $|x\rangle|f(x)\rangle$-t. Az algoritmus a következő:
Kiindulunk $|0^n\rangle|0^l\rangle$-ből, majd az első n qubitre n darab Hadamardot alkalmazva a $\sum_{x \in \mathbb{Z}_2^n} |x\rangle|0^l\rangle$ állapotot kapjuk (a normáló tényezőt az egyszerűség kedvéért szokás elhagyni). Ezt az orákulum a $\sum_{x \in \mathbb{Z}_2^n} |x\rangle|f(x)\rangle$ állapotba viszi. Innen a második l bitet megmérve az állapot összeomlik $(|x\rangle + |x+s\rangle)|f(x)\rangle$-re. Innentől már csak az első n qubitre lesz szükségünk. Újabb n darab Hadamarddal a $\sum_{y \in \mathbb{Z}_2^n} ((-1)^{\langle x,y \rangle} + (-1)^{\langle x+s,y \rangle})|y\rangle$ állapotot kapjuk. Ezt megmérve, egy uniform random olyan y-t kapunk, amely merőleges s-re, mivel csak az ilyen y-ok együtthatója nem 0. Azaz ezt $\mathcal{O}(n)$-szer megcsinálva kapunk $n-1$ lineárisan független ilyen y-t, amiből aztán klasszikus gauss eliminációval polinomidőben meghatározható s.
Ezek után megismerkedtem a legfontosabb és legismertebb kvantum algoritmusokkal. Ezek közül mindenképp érdemes megemlíteni Grover algoritmusát [5], mely egy rendezetlen halmazban tud egy adott tulajdonságú elemet a klasszikusnál négyzetesen gyorsabb időben megtalálni. Mivel a SAT nyelv eldöntése is egy ilyen problémának tekinthető, (keresni egy olyan $x \in \{0,1\}^n$-t, hogy $\varphi(x) = 1$), így Grover algoritmusa a legtöbb NP feladathoz egy négyzetes gyorsítást ígér.
A másik, ami talán a legismertebb és legjelentősebb, Peter Shor algoritmusa [11], mely polinomidőben prímtényezők szorzatára bont egy tetszőleges számot. (Illetve Shor egy másik úttörő algoritmusa a diszkrét logaritmus problémát oldja meg [11]). Shor algoritmusa a következő észrevételekre épül: először is a prímfaktorizáció visszavezethető egy elem rendjének a megtalálására a következőképpen: Feltehetjük, hogy N nem páros és nem prímhatvány. (ha prímhatvány, azt klasszikus módszerekkel is el lehet hatékonyan dönteni, ha páros, akkor addig osztjuk 2-vel, míg páratlan lesz). Ekkor megmutatható, hogy legalább $\frac{1}{2}$ valószínűséggel egy random $x \in \mathbb{Z}_N^*$ r rendje osztható 2-vel, valamint $x^{r/2} - 1$ és $x^{r/2} + 1$ egyike sem többszöröse N-nek. Ekkor $x^r \equiv 1(N) \iff (x^{r/2} - 1)(x^{r/2} + 1) \equiv 0(N) \iff (x^{r/2} - 1)(x^{r/2} + 1) = kN$, $k \in \mathbb{Z}$. Mivel egyik tag sem többszöröse N-nek, így mindkét tag N-el vett legnagyobb közös osztóját kiszámolva N-nek két nemtriviális osztóját kapjuk. A rendkereső algoritmus pedig úgy zajlik, hogy először választunk egy random

x-et, majd a Simon algoritmushoz hasonlóan Hadamardokkal létrehozzuk az uniform szuperpozíciós állapotot ($\sum_{a\in\mathbb{Z}_{2^l}}|a\rangle|0\rangle$), majd a többi qubitre kiszámoljuk $f(a)=x^a\ (mod\ N)$-t, végül megmérjük és tegyük fel, hogy $f(y)$-t kapunk. Ez egy $|y\rangle+|y+r\rangle+|y+2r\rangle...$ alakú állapotot eredményez. Innen a Fourier-transzformáció egy kvantumos változatát alkalmazva, majd egy méréssel és ügyes utófeldolgozással meg tudjuk találni r-t, azaz x rendjét a $\mathbb{Z}_N^*$ csoportban, ami tehát legalább $\frac{1}{2}$ valószínűséggel jó lesz, azaz elvezet minket N egy nemtriviális osztójának megtalálásához.

Mind Shor, mind a legtöbb, a klasszikusnál exponenciális gyorsabban megoldható probléma egy algebrai feladat, a rejtett részcsoport probléma speciális esetei. Ezek után tehát ezirányban folytattam a kutatást. A rejtett részcsoport problémában adott egy G véges csoport, egy $S\subset\{0,1\}^l$ halmaz és egy $f: G\to S$ függvény, amiről tudjuk, hogy $f(x)=f(y)$, akkor és csak akkor, ha x és y ugyanabban a baloldali mellékosztályában van H-nak, valamilyen $H\leq G$ részcsoportra. Ekkor azt mondjuk, hogy f elrejti H-t. Feltesszük továbbá, hogy adott egy orákulum, mely kiszámolja f-et a fenti módon. A feladat a H részcsoport megtalálása.
Például a Simon problémánál $G=Z_2^n$, $H=\{0,s\}$. A rendkereső algoritmusnál $G=Z_{\phi(N)}$, (ahol $\phi(N)$, az N-nél kisebb, $N-$hez relatív prím egészek száma), $f(a)=x^a\ (mod\ N)$, és $H=\langle r\rangle$ (ahol r az x rendje).
Ha G Abel csoport, akkor létezik általános, polinomiális futásidejű algoritmus, ami megoldja a rejtett részcsoport problémát. Ez főképp azon múlik, hogy Abel csoportokra hatékonyan kivitelezhető a kvantum-Fourier-transzformáció. Az algoritmus meglepően egyszerű, mindössze egy kis reprezentációelmélet szükséges hozzá. A nemkommutatív eset már jóval bonyolultabb. Itt még csak bizonyos csoportokra ismertek hatékonyabb algoritmusok, azonban ezek is legjobb esetben szubexponenciális idejűek. Ezek közül tanulmányoztam Ettinger és Hoyer algoritmusát [2], mely a diédercsoportra ad egy olyan módszert, mely csak polinom sokszor kérdez a kvantumos orákulumtól, viszont a kapott adatokhoz még további exponenciális idejű klasszikus utófeldolgozás szükséges H megállapításához.
Fontos eredménye még a cikknek, hogy a Diéder csoport ($\mathbb{Z}_N\rtimes\mathbb{Z}_2$) rejtett részcsoport problémája polinomiálisan visszavezethető arra az esetre, amikor H $\{(0,0),(s,1)\}$ alakú. Egy másik fontos algoritmus a diéder csoport rejtett részcsoportproblémájára Kuperberg algoritmusa [8]. Ez szubexponenciális ($2^{\mathcal{O}(\sqrt{log|G|})}$) futásidejű. Ráadásul általánosítható tetszőleges $G\rtimes\mathbb{Z}_2$ alakú csoportra, ahol G Abel. A tárigény ugyan szintén szubexponenciális, de Regev [10] csinált egy módosítást, amivel apró futásidőbeli növeléssel polinomiális tárigényűvé tehető.
Ezután témavezetőm, Ivanyos Gábor útmutatásával, Kuperberg algoritmusának néhány ötletét felhasználva kidolgoztam egy algoritmust, mely n-ben polinomiális és t-ben exponenciális időben oldja meg a rejtett részcsoport problémát $\mathbb{Z}_{2^t}^n\rtimes\mathbb{Z}_2$-ben. Ez egyben egy másik fontos probléma, a rejtett eltolás egy speciális esete $\mathbb{Z}_{2^t}^n$-ben. Itt adott egy G véges csoport, egy $S\subset\{0,1\}^l$ halmaz, és egy $f: G\rtimes\mathbb{Z}_2\to S$ leképezés, melyre igaz, hogy $\exists s\in G\ f(x,0)=f(xs,1)$. Ennek a legspeciálisabb esete volt a Simon probléma (ahol $G=\mathbb{Z}_2^n$).

Az algoritmussal a kari TDK-n is indultam. Az alapötlete a következő: Hadamard és kvantum Fourier transzformációkkal tudunk létrehozni olyan $(u, \varphi_u\rangle)$ párokat, ahol $|\varphi_u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\frac{2\pi i\langle u,s\rangle}{N}}|1\rangle)$, ahol $N = 2^t$ és a skalárszorzatot $mod\ N$ kell érteni. Továbbá az u-k a $\mathbb{Z}_{2^t}^n$ csoport uniform random elemei, melyek ismertek számunkra. Két ilyen $|\varphi_u\rangle$, $|\varphi_v\rangle$-ből, egy egyszerű módszerrel kaphatunk egy $|\varphi_{u+v}\rangle$ vagy egy $|\varphi_{u-v}\rangle$ állapotot $\frac{1}{2} - \frac{1}{2}$ valószínűséggel. Majd kihasználva, hogy $\mathbb{Z}_2^n$ felett bármely $n+1$ vektor lineárisan összefüggő, így találhatunk olyan $a_i \in \{0,1\}$ együtthatókat, amire $\sum a_i u_i \equiv 0\ (mod\ 2)$. Belátható, hogy megfelelően választva az a_i-ket $\mathbb{Z}_{2^{t-1}}^n$ egy véletlen elemének dupláját kapjuk. Ennek megfelelően összeadjuk a $|\varphi\rangle$-ket is, és mivel $u + v \equiv u - v\ (mod\ 2)$, így mindegy, hogy a fenti módszerrel mit kapunk. Ezt iterálva a végén egy olyan $|\phi_u\rangle$-t kapunk, aminek a koordinátái oszthatók 2^{t-1}-el, így $\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\sum_{i\in\mathcal{I}} s_i}|1\rangle)$ alakú, ahol $\mathcal{I}$ azon koordinátákból áll, ahol u nem 0. Erre a Hadamard inverzét alkalmazva (ami önmaga), majd megmérve a qubitet kapunk egy egyenletet s bizonyos koordinátáinak összegének paritására, majd kellően sok ilyen mintából meghatározhatjuk az s $(mod\ 2)$ vektort. Ennek ismeretében pedig a feladat visszavezethető $\mathbb{Z}_{2^{t-1}}^n$ rejtett eltolás problémájára, s így ezt iterálva végül meghatározhatjuk s-et.
Tanulmányoztam egy cikket Friedl Katalin, Ivanyos Gábor és másoktól [4], mely egy hasonló hatékonyságú algoritmust ad, ráadásul feloldható csoportokra is alkalmazható. Ennek hátránya, hogy rendkívül bonyolult, és exponenciálisan sok összefonódott qubitet használ, míg a mi algoritmusunk egyszerű, és a tárigénye mindössze kvadratikus. (sőt qubitekből elég lineáris mennyiségű). Ez már csak azért is egy fontos szempont, mert a kvantumszámítógépeknél sokkal nagyobb jelentőségű a tárigény, mivel rendkívül nehéz elérni, hogy a qubitek megfelelően viselkedjenek és ne fonódjanak össze egymással vagy ne lépjenek kapcsolatba a környezettel. Éppen ezért napjaink legjobb kvantumszámítógépe is mindössze 54 qubittel operál.
Az algoritmus általánosítása prímhatvány és összetett alapokra sajnos nem sikerült, ugyanis a használt módszerek túlságosan ráépültek az alap kettőhatványságára. Például a fent leírt módon a $|\varphi_u\rangle$-kat megfelelően összeadni az általános esetben már csak exponenciálisan kis valószínűséggel lehet, ráadásul mivel a qubiteket nem lehet lemásolni, így még csak nem is tudjuk többször megpróbálni.

2 Kvantum bonyolultságelmélet

A félév végén a kvantumszámítástudomány egy másik fontos területével, a kvantum bonyolultságelmélettel kezdtem el foglalkozni. Ez olyan nyelvosztályokkal foglalkozik, mint a BQP, mely a kvantumszámítógéppel polinom időben eldönthető nyelvek osztálya, illetve klasszikus nyelvosztályok kvantumos általánosításaival. Ilyen például a QIP, mely az IP (azon nyelvek, melyekre létezik interaktív protokoll, ahol egy mindentudó Merlin be tudja bizonyítani úgy Arthurnak polinom sok lépésben, hogy $x \in L$, hogy Arthur exp nagy valószínűséggel elfogad, ellenkező esetben pedig Merlin minden bizonyítását Arthur csak exponenciálisan

kicsi valószínűséggel fogadja el), vagy a QMA,mely MA (azon nyelvek osztálya, melyekhez létezik olyan interaktív protokoll, ami csak egy fordulós, azaz Merlin küld egy bizonyítást, majd Arthur valamilyen véletlen bitsorozatot választ és ezek függvényében eldönti, hogy elfogad-e) általánosítása. Az általánosítás többnyire abban ál, hogy megengedjük, hogy az üzenetek (akár összefonódott) kvantumbitek legyenek, illetve Arthurnak már egy kvantumszámítógépe van. Itt rengeteg érdekes cikket és eredményt találtam. Mivel egy kvantunszámítógép egy qubitre Hadamardot alkalmazva, majd megmérve a qubitet tud egy véletlen pénzfeldobást szimulálni, így a $BPP \subset BQP$ tartalmazás triviális. A[3] cikk például úgynevezett gapP függvények segítségével (ezek olyan függvények, amikre létezik olyan nemdeterminisztikus Turing gép, hogy $f(x)$ megadja, hogy mennyi T elfogadó lépéssorazatinak $-$ T elutasító lépéssorozatainak száma x inputon) megmutatja, hogy $BQP \subset PP$. Egy másik cikk [9] ennél erősebbet is belátott, hasonló módszerekkel, mégpedig, hogy $QMA \subset PP$ is fennál. Érdekes eredménye szintén ennek a cikknek, hogy míg klasszikus esetben minden konstans sok fordulós Arthur-merlin játék összeomlik AM-re, addig a kvantumos esetben csak $QMAM$-re omlik össze, ráadásul itt az is teljesül, hogy $QMAM = QIP = IP = PSPACE$ [6], azaz a kétfordulós kvantum Atrhur Merlin játékok már ugyanolyan erősek, mint tetszőleges klasszikus/kvantum interaktív protokoll. A valós esetben egy ilyen eredmény többek közt PH összeomlását eredményezné, tehát valószínűtlen. Még meghökkentőbb eredmény, melyet egy 200 oldalas cikkben idén publikáltak, hogy a több bizonyítós esetben a kvantumos változat sokkalta erősebb, mint a klasszikus, méghozzá míg $MIP = NEXP$, addig $MIP^* = QMIP = RE$ [7], ahol RE a rekurzív felsorolható nyelvek osztálya. Tehát kvantumos esetben még klasszikusan eldönthetetlen nyelvekre is léteznek több Merlines interaktív bizonyítások, azaz például a híres leállási problémára is. Ezt a többletet elsősorban az adja, hogy két kvantum Merlin, még a protokoll előtt elő tud készíteni egy összefonódott qubit párt, melynek egyik qubitjét az egyikuk, másik qubitjét a másikuk őrzi meg.
Számtalan érdekes nyitott kérdés található ezen a területen. Például igaz-e, hogy $QCMA$, ahol Merlin csak klasszikus biteket küldhet Arthurnak, egyenlő QMA-val? Jelenleg a klasszikus PH mintájára BQP-ből és QMA-ból alkotott, 3 különböző kvantum-polinomiális hierarchia tulajdonságait vizsgálom, illetve a modellek közti összefüggéseket.

References

[1] Chris Bernhardt. *Quantum Computing for Everyone*. The MIT Press, 2019. ISBN: 0262039257.

[2] Mark Ettinger and Peter Høyer. "On Quantum Algorithms for Noncommutative Hidden Subgroups". In: *Adv. Appl. Math.* 25.3 (2000), pp. 239–251. DOI: 10.1006/aama.2000.0699. URL: https://doi.org/10.1006/aama.2000.0699.

[3] Lance Fortnow and John Rogers. "Complexity Limitations on Quantum Computation". In: vol. 59(2). July 1998, pp. 202–209. ISBN: 0-8186-8395-3. DOI: 10.1109/CCC.1998.694606.

[4] Katalin Friedl et al. "Hidden Translation and Translating Coset in Quantum Computing". In: *SIAM J. Comput.* 43.1 (2014), pp. 1–24. DOI: 10.1137/130907203. URL: https://doi.org/10.1137/130907203.

[5] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866. URL: https://doi.org/10.1145/237814.237866.

[6] Rahul Jain et al. *QIP = PSPACE*. 2009. arXiv: 0907.4737 [quant-ph].

[7] Zhengfeng Ji et al. *MIP*=RE*. 2020. arXiv: 2001.04383 [quant-ph].

[8] Greg Kuperberg. "A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem". In: *SIAM J. Comput.* 35.1 (2005), pp. 170–188. DOI: 10.1137/S0097539703436345. URL: https://doi.org/10.1137/S0097539703436345.

[9] C. Marriott and J. Watrous. "Quantum Arthur-Merlin games". In: *Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004.* 2004, pp. 275–285. DOI: 10.1109/CCC.2004.1313850.

[10] Oded Regev. "A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space". In: (July 2004).

[11] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM J. Comput.* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/S0097539795293172. URL: https://doi.org/10.1137/S0097539795293172.