Kvantumszámítástudomány beszámoló

Csáji Gergely
Témavezető: Ivanyos Gábor

dec. 06

Bevezetés

- Qubit: $a|0\rangle + b|1\rangle$, $a, b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$
- Klasszikus bitek, mint bázisvektorok által generált komplex Hilbert tér egységvektorai: $|0\rangle = (1, 0)$, $|1\rangle = (0, 1)$
- n darab qubit már tetsz. $\sum_{i=0}^{2^n-1} a_i|i\rangle$, $\sum_{i=0}^{2^n-1} |a_i|^2 = 1$ alakú állapotban lehet
- Mérés hatására $|a_i|^2$ valószínűséggel $|i\rangle$-t mérünk

Kvantum áramkör modell

- Logikai kapuk helyett Unitér mátrixok, melyek a qubiteken hatnak.
- PI Hadamard kapu: $|0\rangle \to (|0\rangle + |1\rangle)$, $|1\rangle \to (|0\rangle - |1\rangle)$
- Mátrixosan: $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- $|x\rangle$-ből minden bitre alkalmazva: $\sum_{y \in \mathbb{Z}_2^n} (-1)^{\langle x,y \rangle} |y\rangle$
- Megengedett kapuk: legfeljebb 2 qubiten ható unitér mátrixok
- Megengedünk még méréseket is a qubiteken $\Rightarrow$ A maradék összeomlik
- PI: $|00\rangle + |10\rangle + |11\rangle$ második qubitjét megmérjük és $1 \Rightarrow$ összeomlik $|11\rangle$-be
- Lépésszám $=$ használt kapuk száma

Simon Algoritmusa

- Feladat: 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 $x = y + s$, találjuk ki s-et
- Adott egy orákulum, aki kiszámlja f-et: $|x\rangle|0^l\rangle \to |x\rangle|f(x)\rangle$

Simon Algoritmusa

- Kiindulunk $|0^n\rangle|0^l\rangle$-ből
- Első n qubitre n darab Hadamard: $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|0^l\rangle$
- Orákulum: $\sum_{x\in\mathbb{Z}_2^n}|x\rangle|f(x)\rangle$
- Második l bitet megmérve: $(|x\rangle+|x+s\rangle)|f(x)\rangle$
- Első n qubitre újabb n darab Hadamard, többi bitet elhagyva:

$$\sum_{y\in\mathbb{Z}_2^n}((-1)^{\langle x,y\rangle}+(-1)^{\langle x+s,y\rangle})|y\rangle$$

- Megmérve: $y:\langle y,s\rangle=0$
- Elég sok ilyenből meghatározható s

Shor Algoritmusa

- Feladat: N nem prímhatvány, nem páros szám prímtényezőkre bontása
- Prímfelbontás helyett rendkeresés $\mathbb{Z}_N^*$-ban
- 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 $x^r \equiv 1(N) \iff (x^{r/2}-1)(x^{r/2}+1) \equiv 0(N) \iff (x^{r/2}-1)(x^{r/2}+1) = kN,\ k \in \mathbb{Z}$
- $lnko(N, x^{r/2}-1)$ és $lnko(N, x^{r/2}+1)$ N két nemtriviális osztója lesz

Rendkereső algoritmus

- Random $x \in \mathbb{Z}_N^*$
- Hadamardokkal: $\sum_{a \in \mathbb{Z}_{2^l}} |a\rangle|0\rangle$
- A többi qubitre kiszámoljuk $f(a) = x^a \ (mod\ N)$-t: $\sum_{a \in \mathbb{Z}_{2^l}} |a\rangle|f(a)\rangle$
- Mérés után: $|y\rangle + |y + r\rangle + |y + 2r\rangle ...$
- Innen a Fourier-transzformáció egy kvantumos változata, majd egy mérés és ügyes utófeldolgozás

Rejtett részcsoport probléma

- G véges csoport, $f : G \to S \subset \{0,1\}^l$, létezik $H \leq G$: $f(x) = f(y) \iff xH = yH$
- Feladat: Megtalálni H-t, egy f-et kiszámitó orákulummal
- Ennek speciális esete pl Shor prímfaktorizációs és Diszkrét logaritmus problémája is
- A Simon problémánál $G = Z_2^n$, $H = \{0, s\}$
- A rendkereső algoritmusnál $G = Z_{\phi(N)}$, $H = \langle r \rangle$, $f : G \to \mathbb{Z}_N^*$: $f(a) = x^a \ (mod\ N)$

Rejtett eltolás probléma

- G véges csoport, $f : G \rtimes \mathbb{Z}_2 \to S$, $\exists s \in G$:, hogy $f(x, 0) = f(xs, 1)$.
- Feladat: Megtalálni s-et egy f-et kiszámító orákulummal.
- G kommutatív $\Rightarrow$ rejtett eltolás G-ben $=$ rejtett részcsoport $G \rtimes \mathbb{Z}_2$-ben, $H = \{(0, 0), (s, 1)\}$

Kvantum Bonyolultságelmélet

- BQP, QMA
- $BQP \subset PP$, $QMA \subset PP$
- $QIP = IP = PSPACE = BQPSPACE$
- $MIP^* = RE$
- Nyitott:
  - $QMA = QCMA$?
  - QMA-ban feltehető-e, hogy Arthur 1 vsz-el elfogad?
  - Klasszikus tételek kvantumosításai