KVANTUM-ALGORITMUSOK ÉS A KVANTUM-SZÁMÍTÓGÉPEK SZÁMÍTÁSI KAPACITÁSA

1 Mi a kvantum-algoritmus?

Def.: (i) A *kvantum-algoritmus* egy fizikai folyamat, amely kvantum-effektusokat használ számítási folyamatok elvégzéséhez.

(ii) Az $C:=(W, \{U_1, \dots U_k\})$ párt *kvantum-áramkör*nek nevezzük, ahol $W \cong \underbrace{V\otimes\dots\otimes V}_{n\text{-szer}}$ ($V \cong \mathbb{C}^2$ *qubit-tér*) egy 2^n dimenziós komplex Hilbert-tér és $\{U_1, \dots U_k\} \in U(2^n)$ unitér operátorok úgy, hogy U_i-k sűrűn generálják $U(2^n)$-et.

Megj.: Fizikai realizálás: pl. n atom gerjesztett-alap állapotai, stb.

(2) Párhuzamos számítás, ill. a lokális operátorok elve

Mitől erős egy ilyen (kvantum-áramkör?

Tfh. $W \cong \underbrace{V \otimes V \otimes V}_{\text{3-qubit tér}}$ és $\big(V, |0\rangle, |1\rangle\big) \cong \mathbb{C}^2$

Klasszikusan ez 3 bitnyi információt tárolhat el, pl.: az
$$\begin{cases} 000 \\ 001 \\ \vdots \\ 111 \end{cases}$$
számok közül egyet.

Viszont kvantumosan létezik az
$$|\psi\rangle = \frac{1}{4}\Big(|0\rangle \otimes |0\rangle \otimes |0\rangle + \ldots + |1\rangle \otimes |1\rangle \otimes |1\rangle\Big) \in W$$
összefonódott állapot, mely mind a 8 számot eltárolja!

Klasszikusan ha a $0, \ldots, 7$ számok mindegyikéhez hozzá akarunk adni egyet, akkor az nyolc lépést igényel. Viszont kvantumosan $\exists$ egyetlen U operátor, mely az összeadást elvégzi a $|\psi\rangle$ állapoton, vagyis egyszerre az összes nyolc számon!

Ez a párhuzamos számítás elve és az alkalmazott U operátor egy lokális operátor.

③ Információ-elméleti megjegyzések

Tehát ha adott egy $O(n)$ (ordó) szabadsági fokú rendszer, akkor ez $O(2^n)$ bit információ tárolására képes. De ez nem effektív: a Shannon-féle információ-elméletben az egy adott kvantum-állapot egyetlen példányán elvégzett (egyetlen) méréssel kinyerhető információ-mennyiség megadható: ez $O(n)$ bit tehát megegyezik a klasszikus rendszer által eltárolt információval. (Holevo 1973, Fuchs–Peres 1996). A ki nem nyerhető extra információ: kvantum-információ.

A természet kvantum-szinten a klasszikushoz képest exponenciális mennyiségű információval operál, de ez klasszikusan elérhetetlen. Tehát úgy tűnik, az egész nem jó semmire.

④ De mégis: orákulumok (Deutsch 1985, 1992, Simon 1994)

Elképzelhető, hogy egy jól elvégzett mérés olyan információval szolgál a rendszerről, ami klasszikusan csak sok lépésben érhető el.

Példa: Az $f: (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ fv-ek globális viselkedésének meghatározása.

<u>Def.</u>: Egy $f: (\mathbb{Z}_2)^n \to \mathbb{Z}_2$ fv.

(i) <u>konstans</u>, ha $f(x) = \begin{cases} 1 & \forall x \\ 0 & \forall x \end{cases}$, vagy

(ii) <u>kiegyensúlyozott</u>, ha $f(x) =$ felerészben 1, felerészben 0.

Legyen adott egy „orákulum", v. „fekete doboz", ami előállítja a fentebbi f fv-t. Döntsük el az doboz <u>egyszeri meghívásával</u>, hogy a fv. milyen típusú. (Klasszikusan az orákulumot legalább $(2^{n-1}+1)$-szer meg kell hívni.)

Viszont létezik egy $|\Psi_f\rangle \in (\underbrace{V\otimes\cdots\otimes V}_{n})\otimes V$ kvantum-állapot, amelyen egyetlen mérést végezve a kérdés megválaszolható: Az orákulumot egy $U_f : (\underbrace{V\otimes\cdots\otimes V}_{n})\otimes V \to (\underbrace{V\otimes\cdots\otimes V}_{n})\otimes V$ unitér operátorrá tesszük:

$$\left.\begin{array}{l}\displaystyle\sum_{x\in(\mathbb{Z}_2)^n} |x\rangle \\[2em] |0\rangle\end{array}\right\} \longrightarrow \boxed{U_f} \longrightarrow \sum_{x\in(\mathbb{Z}_2)^n} |x\rangle \otimes |f(x)\rangle$$

$$|\Psi_f\rangle := \sum_{x\in(\mathbb{Z}_2)^n} |x\rangle \otimes |f(x)\rangle$$ a f fv. összes lehetséges értékét tartalmazza! Továbbá $|\Psi_f\rangle$-et az orákulum egyszeri megkérdezésével kaptuk. Nyilván

$$|\Psi_f\rangle = \begin{cases} \sum |x\rangle \otimes |1\rangle, \text{ vagy} \\ \sum |x\rangle \otimes |0\rangle & \text{ha } f \text{ konstans} \end{cases}$$

$$= \sum_{x,y} \left(|x\rangle \otimes |1\rangle + |y\rangle \otimes |0\rangle \right) \quad \text{ha } f \text{ kiegyensúlyozott.}$$

Ezek jól elkülöníthető kvantum-állapotok.

Megjegyzések: (i) az relatív gyorsulás a klasszikus-hoz képest (méghozzá exponenciális!) mert föltettük, hogy a fekete dobozt nem ismerjük.

(ii) Egy klasszikus valószínűségi algoritmus ~~egy~~, mely tetsz. $\varepsilon > 0$ esetén $1-\varepsilon$ valószínűséggel eldönti milyen fv-ről van szó, ugyanolyan gyors (Hf!) Tehát az exp gyorsulás csak $\varepsilon = 0$-nál jelenik meg. Mivel a gyakorlatban $\forall$ algoritmus valószínűségi, ezért ezek az orákulumok elvi jelentőségűek. Az első $\varepsilon > 0$-nál is exp sebességű algoritmusok:

Bernstein–Vazirani 1993, Simon 1994.

(ezekkel nem foglalkozunk).

5) Gyors algoritmus $f: \mathbb{Z}_M \to \mathbb{Z}_N$ fv. periodusának meghatározására

Legyen $f: \mathbb{Z}_M \to \mathbb{Z}_N$ egy periodikus fv, tehát $\exists\ 0 < p \leq M$, hogy

$$f(x+p) = f(x) \quad \forall x \in \mathbb{Z}_M.$$

Nyilván $p \mid M$.

Meghatározzuk p-et $O\left((\log M)^3\right)$ lépésben.

Megint föltesszük, hogy $\exists\ U_f$ unitér orákulum, mely f-et előállítja:

legyen $V_{1,2} := \underbrace{V \otimes \dots \otimes V}_{n}$, hogy $2^n \gg \max(M,N)$ (n-qubites áramkör). Ekkor $U_f : V_1 \otimes V_2 \to V_1 \otimes V_2$

$$\left.\begin{matrix} \sum\limits_{x \in \mathbb{Z}_M} |x\rangle \\ |0\rangle \end{matrix}\right\} \longrightarrow \boxed{\; U_f \;} \longrightarrow \frac{1}{\sqrt{N}} \sum_{x \in \mathbb{Z}_M} |x\rangle \otimes |f(x)\rangle$$

$$|\psi_f\rangle := \frac{1}{\sqrt{M}} \sum_{x \in \mathbb{Z}_M} |x\rangle \otimes |f(x)\rangle \in V_1 \otimes V_2$$

Végezzünk mérést a V_2 regiszteren, pl. $y_0 = f(x_0)$ az eredmény, ahol $x_0 \in \mathbb{Z}_M$ a legkisebb ilyen tulajdonságú elem. Ekkor:

$$|\psi_f\rangle \xmapsto{\text{mérés } V_2\text{-n}} |\phi\rangle := \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |x_0 + kp\rangle \otimes |y_0\rangle$$

és $pK = M$.

Gond: mivel y_0 véletlen, x_0 is az, így $|\phi\rangle$ egy véletlen periodikus állapot. Megoldás:

Diszkrét Fourier ~~T~~ranszformáció (DFT) a V_1-téren:

$$F : V_1 \longrightarrow V_1 \;, \quad F_{ab} = \frac{1}{\sqrt{M}} \exp\left(\frac{2\pi i\, ab}{M}\right)$$

Ekkor $$F|\phi\rangle = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} e^{\frac{2\pi i\, x_0 j}{p}} \left| j \frac{M}{p} \right\rangle \otimes |y_0\rangle$$

Most ismét mérést végzünk V_1-en, az eredmény: $c_0 = j_0 \cdot \frac{M}{p}$ értéket kapunk.

$$\frac{c_0}{M} = \frac{j_0}{p}$$

Ismert. Ha $(j_0, p) = 1$ (relatív prímek), akkor $\frac{j_0}{p}$-ből p-t is megkapjuk.

KÉSZ.

Szükséges lépések összeszámolása:

(i) annak valószínűsége, hogy $(j_0, p) = 1$ arányos $(\log N)^{-1}$-gyel, mert:

$$\# \{ j_0 \mid (j_0, p) = 1 \} \geq \{ q \text{ prím} \mid q \leq p \} \sim \frac{p}{\log p}$$

(prímszám-tétel). Ezért $O(\log p) \sim O(\log M)$ ~~lép~~ db mérést végezve ~ 1 valószínűséggel p-re relatív prím j_0-t kapunk.

(ii) Kvantum-szituációban a Diszkrét Gyors Fourier trafó (DFFT) egy $M \times M$ méretű ~~mátrixon~~ esetén $O((\log M)^2)$ lépést igényel.

(iii) $|0\rangle \in V_1$, akkor $\sum_{x \in V_1} |x\rangle = \mathcal{F}|0\rangle$, ez is $O((\log M)^2)$ lépés.

Mindent figyelembe véve: $\sim O((\log M)^3)$ lépésben az f fv. r periódusa ~ 1 valószínűséggel meghatározható!

<u>Megj.</u>: Ugyanilyen gyors algoritmus létezik véges Abel-csoportok faktorizálására is.

6 A Shor-algoritmus (Shor, 1994)

Adott $N \in \mathbb{Z}$ páratlan, keresünk $A \in \mathbb{N}$ számot, hogy $A | N$.

Az algoritmus leírása:

A) Adott $N \in \mathbb{N}$, euklideszi algoritmussal egy véletlenül választott $a \leq N$ számnál $O(\text{poly}(\log N))$ lépésben eldöntjük, hogy:

$$(a, N) = \begin{cases} > 1 & \text{kész} \\ = 1 & \Rightarrow \text{B} \end{cases}$$

B) Euler-tétele miatt $\exists\, r \in \mathbb{N}$, hogy ő a legkisebb: $a^r \equiv 1 \pmod N$.

<u>Megj.</u>: pl. $\varphi(N) = N \prod_{\substack{p | N \\ \text{prím}}} \left(1 - \frac{1}{p}\right)$ Euler-f.

jó, de általában nem a legkisebb értéket kapjuk.

C) Tfh. r páros. Ekkor $a^r - 1 \equiv 0 \pmod N$

$$\underbrace{\left(a^{r/2} + 1\right)}_{=\alpha} \underbrace{\left(a^{r/2} - 1\right)}_{=\beta} \equiv 0 \pmod N$$

Ekkor ha $N \nmid \alpha$, $N \nmid \beta$ akkor $(\alpha, N) > 1$ és $(\beta, N) > 1$ euklideszi algoritmussal megkereshetők $\mathcal{O}(\mathrm{poly}(\log N))$ lépésben és ezek megadják N egy szorzat-felbontását.

<u>Megj.</u>: (i) a nagysebességű lépés (B)-ben kell: $a^r \equiv 1 \pmod N \Leftrightarrow \exists f: \mathbb{Z}_M \to \mathbb{Z}_N$ fv, ami r szerint periodikus: $f(x) = a^x$
$\left(f(x+r) = a^{x+r} \equiv a^x = f(x) \right)$.

(ii) <u>Tétel</u> (Deutsch, Jozsa 1998) Ha adott N páratlan, akkor $1 < a \le N$ ~~esetén annak valószínűsége, hogy~~ és $(a, N) = 1$ esetén annak valószínűsége, hogy $(\bullet)$ $a^r \equiv 1$-re r páros és $(\bullet\bullet)$ $\alpha, \beta = a^{r/2} \pm 1 \nmid N$, mindig $\ge \frac{1}{2}$. $\boxtimes$

Lépések összeszámlálása: $(\bullet)$ Euklideszi algoritmusok $\mathcal{O}(\mathrm{poly}(\log N))$; $(\bullet\bullet)$ ~ 1 valószínűséggel $(a, N) = 1$: $\mathcal{O}(\log N)$; $(\bullet\bullet\bullet)$ r megkeresése $\sim \mathcal{O}\left((\log N)^3\right)$
$(\bullet\bullet\bullet\bullet)$ r-re kirótt ~~feltételek~~ feltételek: $\mathcal{O}(1)$

Egy példa: $N := 15$

Ⓐ $a := 7$

Ⓑ $r = 4 \quad (4 \mid 15) = 8)$

Ⓒ $7^4 - 1 = (7^2 - 1)(\cancel{7}^2 + 1) = 48 \cdot 50$

$15 \nmid 50, \quad 15 \nmid 48$

$\underline{\underline{(15, 50) = 5}}, \quad \underline{\underline{(15, 48) = 3}}.$

Érdekes megjegyzések:

(i) melyek a leggyorsabban faktorizálható számok?

Lemma: Legyen N olyan, hogy $\forall\, a \in \mathbb{N}$ $(a, N) = 1$ esetén $a^2 \equiv 1 \pmod N$. Ekkor $24 \mid N$. $\boxtimes$

tehát a 24-gyel osztható számok a leggyorsabban faktorizálhatók!

(ii) Máig nem ismert, hogy $\exists$-e klasszikus exp. sebességű faktorizáló algoritmus.

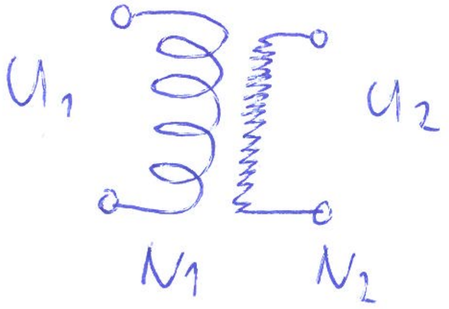
7 Megjegyzések a P/NP problémáról

A P/NP nem támadható kvantum-algoritmusokkal, mert a rendezetlen tárban való keresés Grover-féle $O(\sqrt{N})$ algoritmusa nem javítható tovább.

8 Topologikus kvantum-mező alapú számítógépek (Freedman, Kitaev, ...)

Elv: Egy TQFT-beli várható értékek egyre nehezebben kiszámítható dolgokat realizálnak, ha az elmélet egyre „nem-Abelibb" és „nem-lineárisabb".

Pl.: U(1) elektrodinamikában: a transzformátorban:



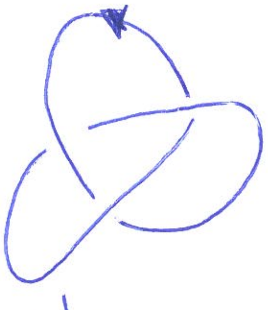
$$\frac{U_1}{U_2} \sim \frac{N_1}{N_2}$$

Tehát a mért feszültségek az L_1, L_2 hurkok hurkolódási együtthatóját számolják (Gauß, kölcsönös indukciós együttható):

$$L(L_1,L_2) = \frac{1}{4\pi}\oint_{L_1}\oint_{L_2} \frac{\underline{r}_1-\underline{r}_2}{|\underline{r}_1-\underline{r}_2|^3}\cdot(d\underline{r}_1\times d\underline{r}_2) \sim \frac{N_1}{N_2}.$$

Ez a csomók egy algoritmikusan jól számolható invariánsa. De mi lenne, ha a transzformátorban $U(1)$ helyett $SU(2)$ áramok folynának?

Legyen $K: S^1 \to M^3$ csomó, ahol M^3 egy kompakt 3-sokaság.



Példa csomóra

Létezik egy $t\in\mathbb{C}$ változóval felírható „polinom", mely K-nak erős invariánsa: Jones-polinom

Defi: (i) $J_{\bigcirc}(t) := 1$ (trivi csomóra legyen 1)

(ii) $t^{-1} J_{L_+}(t) - t\, J_{L_-}(t) = \left(\sqrt{t} - \frac{1}{\sqrt{t}}\right) J_{L_0}(t)$

(bogozási reláció)

Pl. a fentebbi 3-levelű csomóra: $J_K(t) = -t^4 + t^3 + t$

Általában nagyon nehezen számolható!

Tek. az Chern–Simons–Witten 3dim topologikus kvantum-mező elméletet (TQFT)

$$S_k(\nabla) = \frac{k}{4\pi}\int_{M^3} tr\left(A\wedge dA + \frac{2}{3}A\wedge A\wedge A\right)$$

ahol $k\in\mathbb{Z}$, $\nabla = d+A$ egy $SU(2)$ konnexió a M^3 feletti $E\simeq M^3\times\mathbb{C}^2$ trivializált $SU(2)$ nyalábon. Legyen $K: S^1\to M^3$ egy csomó, egy ehhez tartozó megfigyelőt definiálunk a Chern–Simons–Witten TQFT-ben: (Wilson-hurok)

$$Wilson(K) := tr\left(P\exp\left(\int_K A\right)\right)$$

(vagyis a ∇ holonómiája K mentén), akkor ennek várható értéke:

$$Witten_k(K) := \int_{\mathcal{B}} e^{iS_k(\nabla)}\, Wilson(K)\, D[\nabla]$$

<u>Tétel</u> (Witten, 1990 Fields-érem)

$$J_K\left(e^{-\frac{2\pi i}{k+2}}\right) = Witten_k(K)$$

(i) Legyen $\#K$ a K csomó egy 2 dim. diagramjában a kereszteződések száma. Ekkor ha $k = 0, 1, \ldots \sigma(\#K)$-ra ~~...~~ előállítjuk a $\mathrm{Witten}_k(K) = J_K(\xi_k)$ értékeket, akkor $J_K(t)$ már $\sigma(\#K)$ lépésben reprodukálható!!!

(ii) Adott K-ra $J_K(t)$ kiszámítása a $\sigma(\exp(\#K))$ lépést igényel. $J_K(t)$ kiszámítása NP-teljes?

(iii) Az $J_k(D)$ elméletek a kvantum-Hall effektus k-adik szintjén realizálhatók?