

Základní kvantové algoritmy

Libor Veis

- 1 Quantum advantage?
- 2 Superhusté kódování
- 3 Deutschův algoritmus
- 4 Úvod do praktických kvantových algoritmů

Quantum advantage?

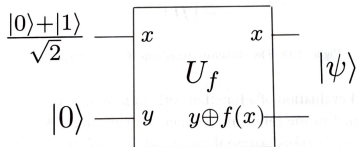
- *Kvantový paralelismus*: linearita operátorů v kvantové mechanice dovoluje kvantovým počítačům spočítat hodnotu funkce $f(x)$ pro různé hodnoty x zároveň.
- Uvažujme pro jednoduchost funkci s jednobitovým definičním oborem a oborem hodnot, $f(x) : \{0, 1\} \rightarrow \{0, 1\}$
- Pro realizaci libovolné funkce však nelze použít pouze jedno-qubitové hradlo, protože by nemuselo být unitární:

$$|i\rangle \xrightarrow{U_f} |f(i)\rangle$$

jak snadno ověříte na příkladu funkce: $f(0) \rightarrow 0$, $f(1) \rightarrow 1$, kdy

$$U_f = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{a} \quad U_f \cdot U_f^\dagger \neq I$$

- "Paralelní" výpočet $f(x)$ lze zrealizovat následujícím kvantovým obvodem



- Zmíněný kvantový obvod generuje

$$|\psi\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}} \quad (1)$$

Úloha 1

Ukažte, že kvantový obvod odpovídající U_f je unitární.

- Tento způsob lze snadno zobecnit na funkce působící na libovolný počet bitů pomocí *Hadamardovy transformace* na n qubitech.
- Kvantový paralelismus však není sám o sobě užitečný - měřením $|\psi\rangle$ v (1) získáme pouze jeden ze dvou možných stavů: $|0, f(0)\rangle$, nebo $|1, f(1)\rangle$.
- Intuitivně by kvantové počítače mohly mít větší výpočetní sílu, nežli jejich klasické protějšky.
- Kvantové počítače, které se fundamentálně liší od klasických počítačů, také přinášejí nové třídy složitosti.

- Klasická teorie složitosti: problém definovaný n -bitovým vstupem. Rozlišujeme:
 - 1 Problémy řešitelné v polynomiálním čase a s polynomiálními prostředky - *řešitelné*
 - 2 Problémy vyžadující exponenciální zdroje - *neřešitelné*
- Třída složitosti P : problémy řešitelné v polynomiálním čase na klasickém počítači.
- Třída složitosti NP : rozhodovací problémy jejichž řešení ("ano") lze v polynomiálním čase na klasickém počítači ověřit.
- NP -úplné problémy: nejsložitější problémy v NP , jejichž řešení v polynomiálním čase by umožnilo řešit všechny NP problémy v polynomiálním čase.
- Např. rozhodovací verze *problému obchodního cestujícího*: Existuje cesta s náklady $\leq k$, která navštíví každé město právě jednou a vrátí se do výchozího bodu?
- Otevřená otázka informatiky:

$$P \stackrel{?}{=} NP, \quad \text{předpoklad } \neq$$

- Třída BPP (*Bounded-error Probabilistic Polynomial*): problémy řešitelné klasickým počítačem v polynomiálním čase s maximální chybovostí $1/3$. Opakováním algoritmu lze chybu exponenciálně snížit.

- Kvantové třídy jsou analogické klasickým pravděpodobnostním třídám.
- *BQP (Bounded-error Quantum Polynomial)*: Kvantový ekvivalent BPP - problémy řešitelné kvantovým obvodem v polynomiálním čase s omezenou chybovostí.
- Protože kvantové počítače dokážou simulovat klasické výpočty, platí vztah:

$$P \subseteq BPP \subseteq BQP$$

- Kvantové výpočty a NP-problémy:
 - ▶ Kvantové počítače umí efektivně faktorizovat celá čísla na součin prvočísel, ale nejsou považovány za dostatečně výkonné k řešení všech NP-problémů.
 - ▶ NP-úplné problémy pravděpodobně nejsou kvantovými počítači řešitelné v polynomiálním čase.
- *Třída QMA (Quantum Merlin-Arthur)*:
 - ▶ Kvantový ekvivalent NP – problémy, které může kvantový počítač v polynomiálním čase ověřit.
 - ▶ Patří sem např. také problém základního stavu obecného dvoučásticového Hamiltoniánu, který je QMA-úplný (velmi obtížný i pro kvantový počítač).

- Alice posílá Bobovi klasickou informaci.
- Při poslání jednoho qubitu Bobovi může ve skutečnosti komunikovat *dva bity klasické informace*!
- Před samotnou komunikací Alice a Bob sdílí Bellův stav (připravený třetí stranou):

$$|\psi\rangle = \frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \quad (2)$$

- Pokud chce Alice poslat jednu ze čtyř možných kombinací dvou bitů, provede na svém příslušnou operaci:

$$00 : I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow |\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \equiv |\Phi^+\rangle$$

$$01 : X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rightarrow |\psi\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \equiv |\Psi^+\rangle$$

$$10 : Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rightarrow |\psi\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \equiv |\Phi^-\rangle$$

$$11 : ZX = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rightarrow |\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \equiv |\Psi^-\rangle$$

Úloha 2

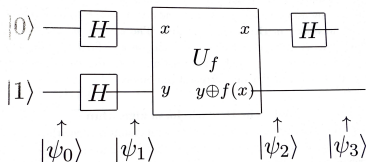
Ukažte, že stavy $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$ tvoří ortonormální bázi.

- Alice svůj qubit potom pošle Bobovi a ten měřením v Bellově bázi dokáže čtyři zmíněné možnosti rozlišit.

Úloha 3

Navrhněte kvantový obvod pro převod z Bellovy báze $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$ do výpočetní báze $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

- Deutschův algoritmus využívá podobný kvantový obvod, jaký jsme si představili při kvantově-paralelním výpočtu $f(x)$:



- Dokáže však ze superpozice stavů díky interferenci (dodatečná Hadamardova hradla) získat informaci o součtu funkčních hodnot $f(0) + f(1)$, při *jediné* aplikaci U_f ! $\Rightarrow$ *quantum advantage*
- Analýza kvantového obvodu:

$$\begin{aligned}
 |\psi_1\rangle &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \\
 &= \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle)
 \end{aligned}$$

$$|\psi_2\rangle = \frac{1}{2}(|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(0)\rangle)$$

- Když $f(0) = 0$ and $f(1) = 0$:

$$|\psi_2\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Když $f(0) = 1$ and $f(1) = 1$:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}(|01\rangle - |00\rangle + |11\rangle - |10\rangle) = \frac{1}{2}(|0\rangle \otimes (|1\rangle - |0\rangle) + |1\rangle \otimes (|1\rangle - |0\rangle)) \\ &= -\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

- Takež pokud $f(0) = f(1)$:

$$|\psi_2\rangle = \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

- Stejným postupem lze ukázat, že když $f(0) \neq f(1)$:

$$|\psi_2\rangle = \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

- Aplikací posledního Hadamardova hradla získáme

$$|\psi_3\rangle = \pm |0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad \text{když } f(0) = f(1)$$

$$= \pm |1\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad \text{když } f(0) \neq f(1)$$

$$|\psi_3\rangle = \pm |f(0) \oplus f(1)\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

- Deutschův algoritmus, přestože není příliš praktický, ukazuje, že kvantové počítače dokáží určité úlohy řešit efektivněji.

Úloha 4

Vyzkoušejte si Deutschův algoritmus pro funkci $f(0) \rightarrow 1$, $f(1) \rightarrow 0$ v prostředí OpenQASM:
<http://quantum.ibm.com/composer>.

- Zobecnění Deutschova algoritmu pro n qubitů.
- Dokáže jednou aplikací U_f rozlišit, zda je funkce na definičním oboru n bitů *konstantní*, nebo *balancovaná*.
 - ▶ Konstantní: dává stejnou hodnotu $f(x)$ pro všechny x .
 - ▶ Balancovaná: dává hodnotu $f(x) = 1$ pro polovinu všech možných x a $f(x) = 0$ pro druhou polovinu.
- Přestože se opět jedná spíše o “akademický problém”, kvantové počítače ho dokáží vyřešit *exponenciálně rychleji*, neboť v klasickém případě (v nejhorší situaci), je funkce $f(x)$ potřeba aplikovat minimálně $(2^n/2 + 1)$ –krát.

- Diskrétní Fourierova transformace převádí vektor komplexních čísel $x_0, \dots, x_{N-1}$ na vektor $y_0, \dots, y_{N-1}$ podle

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \quad (3)$$

- Diskrétní Fourierova transformace má nespočet aplikací v nejrůznějších odvětvích vědy a techniky.
- *Kvantová Fourierova transformace* (QFT) je lineární transformace U na n qubitech, která převádí výpočetní bázevý stav $|j\rangle$ na superpozici podle

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \quad (4)$$

- Při aplikaci QFT na superpozici bázevých stavů získáme novou superpozici, kde rozvojové koeficienty odpovídají FT původním koeficientům.

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left(\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \right) |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle \quad (5)$$

- Klasická rychlá Fourierova transformace škáluje jako $N \log N$, kde $N = 2^n$, tedy jako $n2^n$.
- Jak si ukážeme v příští hodině, QFT lze realizovat pomocí n^2 kvantových hradel $\Rightarrow$ *exponenciální zrychlení*!
- QFT se však nedá použít přímočaře, protože polynomiálním množstvím měření nejsme schopni získat informaci o rozvojových koeficientech 2^n stavů v superpozici.
- QFT tvoří základ *Shorova algoritmu* pro faktORIZACI celých čísel na součin prvočísel, či algoritmu odhadu fáze, *Phase Estimation*, který se ve fyzice a chemii používá k řešení vlastního problému Hamiltoniánu.
- Grooverův algoritmus pro hledání v netříděné databázi:
 - ▶ Klasické algoritmy škálují jako $\mathcal{O}(N)$, kde N je počet elementů v databázi.
 - ▶ Grooverův kvantový algoritmus škáluje jako $\mathcal{O}(\sqrt{N})$.
 - ▶ Oproti QFT “pouze” kvadratické zrychlení, nicméně se jedná o široce se vyskytující problém.