Úvod do kvantového počítání

4. přednáška

Miroslav Dobšíček

Katedra počítačů, Fakulta elektrotechnická
České vysoké učení technické v Praze

20. dubna 2005

Část I

Přehled z minulé hodiny

Kvantové stavy

Stav 1 qubitu:

- Čistý
  - Možné zobrazit na Blochově kouli.

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

- Mixovaný
  - Pro práci v reálných podmínkách.
  - Diracova notace

$$[\phi\rangle = \bigoplus(p_i, |\phi_i\rangle)$$

  - Densitní matice (operátory)

$$\rho_{[\phi\rangle} = \sum p_i |\phi_i\rangle\langle\phi_i|$$

Tensorový součin

Tensorový součin vektorů:

$$|x\rangle = (x_1, x_2)^T, \quad |y\rangle = (y_1, y_2)^T$$

$$|x\rangle \otimes |y\rangle = |x, y\rangle = |xy\rangle = (x_1 y, x_2 y)^T = (x_1 y_1, x_1 y_2, x_2 y_1, x_2 y_2)^T$$

Tensorový součin matic

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & & \vdots \\ a_{n,1}B & \cdots & a_{n,n}B \end{pmatrix}$$

2-qubitový registr

$|q_1\rangle \otimes |q_2\rangle$ bez operátoru

$|q_1\rangle$ ——

$|q_2\rangle$ ——

- registr je ve stavu $|\phi\rangle = |q_1\rangle \otimes |q_2\rangle$

$|q_1\rangle \otimes |q_2\rangle$ s operátorem

$|q_1\rangle$ ———

$|q_2\rangle$ —[H]—

- registr je ve stavu $|\phi\rangle = |q_1\rangle \otimes |q_2\rangle$
- působící operátor je $I \otimes H$

Část II

Dnešní přednáška

Separovatelné a entanglované stavy

Separovatelné – Registr lze rozepsat na tenzorový součin jednotlivých qubitů.

$$\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$$

Entanglované – Registr nelze rozepsat na tenzorový součin jednotlivých qubitů.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \ldots \text{nelze rozepsat.}$$

Porušení principu lokality

Kvantová propletenost stavů je vlastnost neklesající s fyzickou vzdáleností qubitů $\Rightarrow$ porušení principu lokality.

Měření na 2-qubitovém systému

Měření můžeme provést na libovolném počtu qubitů z registru.

Na dvou qubitech

Stav $|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$ zkolabuje na stav $|01\rangle$ nebo na stav $|11\rangle$.

Na jednom qubitu

Stav $|\phi\rangle = \frac{1}{4}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ při měření na

- 1. qubitu s výsledkem 0 resp. 1 zkolabuje na stav $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ resp. $\frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$.
- 2. qubitu s výsledkem 0 resp. 1 zkolabuje na stav $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ resp. $\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$.

Neklonovací teorém

Neklonovací teorém

Neznámý kvantový stav nelze kopírovat. Jinými slovy, pro libovolný jedno-qubitový stav $|\phi\rangle$ neexistuje unitární transformace U pro kterou platí

$$U|\phi, 0\rangle = |\phi, \phi\rangle.$$

Důkaz

Předpokládejme, že taková transformace U existuje a pro ortogonální stavy α, β platí $U|\alpha, 0\rangle = |\alpha, \alpha\rangle, U|\beta, 0\rangle = |\beta, \beta\rangle$.
Nechť $|\gamma\rangle = \frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)$.
Potom $U|\gamma, 0\rangle = \frac{1}{\sqrt{2}}(|\alpha, \alpha\rangle + |\beta, \beta\rangle) \neq |\gamma, \gamma\rangle =$
$\frac{1}{2}(|\alpha, \alpha\rangle + |\alpha, \beta\rangle + |\beta, \alpha\rangle + |\beta, \beta\rangle$.

n-qubitový registr

Pojmenování bází v binární soustavě:

$$|\phi\rangle = \sum_{i \in \{0,1\}^n} \alpha_i |i\rangle$$

Pojmenování bází v desítkové soustavě:

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

kde $\alpha_i \in C$ a $\sum \alpha_i = 1$.

Počet stavů systému

Je vidět, že počet stavů kvantového systému roste exponenciálně s fyzickou velikostí (tj. počtem použitých qubitů).

Kvantový paralelismus

... důsledek linearity

Unitární operace se aplikuje na všechny báze paralelně:

$$\mathsf{U}|\phi\rangle = \mathsf{U}\sum_{i=0}^{2^n-1}\alpha_i|i\rangle = \sum_i \alpha_i \mathsf{U}|i\rangle$$

- V prostoru H_{2^n} se používají matice o velikosti $2^n \times 2^n$.
- Zpravidla se v jednom kroku aplikuje pouze jedno-dvou qubitový operátor na jeden-dva qubity; na zbytek se působí identitou.

Aplikace operátoru U na i-tý qubit:

$$U_n = \bigotimes_{k=0}^{i-1} I \otimes U \otimes \bigotimes_{k=i+1}^{n} I.$$

Poznámky ke kvantovým registrům

1. Počet bázových stavů roste exponenciálně s počtem qubitů. Pro n=200 dostáváme počet atomů ve vesmíru.
2. Pro uložení čisla N potřebujeme $\lceil \lg (N+1) \rceil$ qubitů.
3. Přechod z bázového stavu do jiného je v lineárním čase; je potřeba nejvíce n NOT operací na jednotlivé qubity.
4. Registr neuchovává exponenciálně mnoho vytěžitelné informace. Spolehlivě lze získat pouze n bitů informace z n-qubitového registru.
5. Vývoj n-qubitového systému je dán maticí $2^n \times 2^n$. Pro simulaci na klasickém počítači je potřeba $2^n(2.2^n - 1)$ operací.