Úvod do kvantového počítání

2. přednáška

Miroslav Dobšíček

Katedra počítačů, Fakulta elektrotechnická
České vysoké učení technické v Praze

17. března 2005

Část I

Přehled z minulé hodiny

Alternativní výpočetní modely

Hledání silnějšího výpočetního modelu než Turingův stroj

$\Rightarrow$ poražení Silné Churchovi teze:
Problém je řešitelný v polynomiálním čase, právě tehdy když je v polynomiálním čase řešitelný na TM.

"Známé" modely:

- Kvantové počítače
- DNA počítače

Kvantové počítače

- Založeno na kvantové mechanice
- Aplikace
  - Rychlejší algoritmy
  - Generování náhodných čísel
  - Kvantová distribuce klíčů
- Fyzická realizace
  - NMR
  - Cavity QED
  - Ion trap

DNA počítače

- Založeno na "puzzle" párování nukleotidů T, C, G, A
- Aplikace
  - experimenty s problémem obchodního cestujícího (NPC problém)
- Fyzická realizace
  - Nukleotidová polévka s míchačem a dodávkami cukru

Část II

Dnešní přednáška

Co je to qubit?

Kvantový bit - qubit

Obecný tvar:

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Qubit žije v Hilbertově prostoru H_2.
- $B = \{|0\rangle, |1\rangle\}$ tvoří bázi prostoru.
- Evoluce kvantového systému je unitární.
- Měření způsobuje kolaps qubitu na jeden z bázových vektorů.
- α a β jsou komplexní amplitudy.

Notační zápis podle Diraca

- $|\phi\rangle$ - sloupcový vektor (nazývaný ket), $|\phi\rangle = (x_1, x_2, \dots)^T$
- $\langle\phi|$ - řádkový vektor (nazývaný bra), $\langle\phi| = (|\phi\rangle)^*$
- $\langle\phi|\psi\rangle$ - vnitřní součin
- $|\phi\rangle \otimes |\psi\rangle$ - tensorový součin
- $||\phi||$ - norma

Vektorový prostor V nad tělesem F

Množinu V nazveme vektorovým prostorem nad tělesem F

$\Longleftrightarrow$ máme definované operace $+ : V \times V \to V$ (vektorové sčítání) a $\cdot : F \times V \to V$ (skalární násobení) a platí:

1. $(V, +)$ je komutativní grupa.
2. $\alpha|\phi\rangle = |\phi\rangle\alpha$
3. $\alpha(\beta|\phi\rangle) = (\alpha\beta)|\phi\rangle$
4. $(\alpha + \beta)|\phi\rangle = \alpha|\phi\rangle + \beta|\phi\rangle$
5. $\alpha(|\phi\rangle + |\psi\rangle) = \alpha|\phi\rangle + \alpha|\psi\rangle$

Vnitřní součin $\langle\cdot|\cdot\rangle$

Nechť je V komplexní vektorový prostor.

Funkci $\langle\cdot|\cdot\rangle : V \times V \to C$

nazveme vnitřní součin, právě tehdy když

1. $\langle\phi|\phi\rangle \in R, \quad \langle\phi|\phi\rangle \geq 0, \quad \langle\phi|\phi\rangle = 0 \Leftrightarrow |\phi\rangle = 0$
2. $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$
3. $\langle\phi|(|\psi\rangle + |\lambda\rangle) = \langle\phi|\psi\rangle + \langle\phi|\lambda\rangle$
4. $\langle\phi|\alpha\psi\rangle = \alpha\langle\phi|\psi\rangle$
5. $\langle\alpha\phi|\psi\rangle = \alpha^*\langle\phi|\psi\rangle$

Hilbertův prostor

Hilberův prostor

je úplný komplexní vektorový prostor H s vnitřním součinem $\langle\cdot|\cdot\rangle$ a definovanou normou $||\phi|| = \sqrt{\langle\phi|\phi\rangle}$

- Normalizovaný (jednotkový) vektor $|\phi\rangle \Leftrightarrow ||\phi|| = 1$
- Ortonormální systém $B = \{|b_1\rangle, |b_2\rangle, \dots\}$ tvoří bázi prostoru H, právě tehdy když pro všechny vektory $|\phi\rangle$ můžeme psát

$$|\phi\rangle = \sum_i \lambda_i |b_i\rangle$$

- Ortonormální bázové vektory - normalizované bázové vektory

Vlastnosti Hilbertova prostoru

- Hilbertův prostor je H je isomorfní k tělesu C^n.
- Zápis ket a bra vektorů umožňuje vnitřní součin vyjádřit jako běžné násobení matic.
- Pokud H_1 a H_2 jsou Hilbertovy prostory, pak tensorový součin

$$H = H_1 \otimes H_2 = \left\{ \sum_{|i\rangle \in B_1} \sum_{|j\rangle \in B_2} c_{ij} |i,j\rangle : c_{ij} \in C \right\}$$

  je také Hilbertův prostor s bází $B = B_1 \times B_2$.
- $\dim H = \dim H_1 \cdot \dim H_2$

Příklady bází

Standardní báze:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Duální báze:

$$|0'\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |1'\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$|0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Lineární operátory

Nechť je V vektorový prostor.

Funkci (operátor) $A : V \to V$ nazveme lineární

právě tehdy když platí

$$A\left(\lambda|\phi\rangle + \mu|\psi\rangle\right) = \lambda A|\phi\rangle + \mu A|\psi\rangle$$

Operátor A zapisujeme jako čtvercovou matici $n \times n$.

$$A = \begin{pmatrix} a_{0,0} & \cdots & a_{0,n-1} \\ \vdots & & \vdots \\ a_{n-1,0} & \cdots & a_{n-1,n-1} \end{pmatrix}$$

Lineární operátory

Operátor A můžeme také napsat jako

$$A = \sum_{i,j} a_{ij} |i\rangle\langle j|$$

$|i\rangle, |j\rangle$ odpovídají standardním bázovým vektorům. Pro matici 2×2 dostaneme:

$$\begin{pmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{pmatrix} = a_{0,0}|0\rangle\langle 0| + a_{0,1}|0\rangle\langle 1| + a_{1,0}|1\rangle\langle 0| + a_{1,1}|1\rangle\langle 1|$$

Pro prvky matice a_{ij} můžeme psát

$$a_{ij} = \langle i|A|j\rangle$$

Důležité druhy operátorů

Sdružený operátor

Operátor $A^\dagger = \left(A^T\right)^* = \sum_{i,j} a_{ji}^* |i\rangle\langle j|$ nazveme sdruženým operátorem k operátoru A.

Operátor

- samo sdružený (self-adjoint, Hermitián) $\Leftrightarrow A^\dagger = A$
  - vlastní čísla Hermitiánu jsou vždy reálná
- unitární $\Leftrightarrow A^\dagger A = AA^\dagger = I$
  - $\rightarrow A^{-1} = A^\dagger$
  - unitární operátor zachovává vnitřní součin; $\langle A\phi | A\psi\rangle = \langle \phi | \psi \rangle$

Postuláty kvantové mechaniky

1. Kvantový stav

Libovolnému fyzickému systému S může být přiřazen komplexní Hilbertův prostor H, kterému říkáme stavový prostor systému S. Stav systému S je úplně popsán vektorem $|\phi\rangle \in H$ s normou $||\phi|| = 1$, kterému říkáme stavový vektor systému S.

Nejjednoduší netriviální kvantově mechanický systém je kvantový bit - qubit z prostoru H_2. Stav $|\phi\rangle$ může být zapsán jako lineární kombinace (superpozice) dvou bázových vektorů označaných $|0\rangle, |1\rangle$.

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \text{kde} \quad \alpha, \beta \in C \quad \text{a} \quad |\alpha|^2 + |\beta|^2 = 1$$

Postuláty kvantové mechaniky

2. Evoluce

Dočasný vývoj uzavřeného kvantového systému je popsán Schrödingerovou rovnicí

$$i\hbar\frac{\partial}{\partial t}|\phi\rangle = \mathcal{H}|\phi\rangle$$

kde $\hbar$ je Planckova konstanta a $\mathcal{H}$ je Hamiltonián popisující dynamiku v prostoru H.

Protože unitární operátor U lze vyjádřit jako $U = e^{-i\mathcal{H}}$, můžeme druhý postulát přeformulovat do tvaru:

$$|\phi_{t_2}\rangle = U|\phi_{t_1}\rangle, \quad \text{pro čas} \quad t_1 \leq t_2$$

Příklad evoluce

Hadamardova rotace

Jeden z nejdůležitějších jedno-qubitových operátorů je Hadamardova rotace.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

! Odpovídá diskrétní Fourierově transformaci v Z_2. !

Hadamardova rotace

Příklady:

1. $$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$
2. $$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$
3. Obecně:
$$H_n|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x.y}|y\rangle$$
$$\text{kde } x.y = \oplus_{i=1}^{n} x_i y_i \, .$$

Postuláty kvantové mechaniky

3. Měření

Měření je popsáno self-adjoint operátorem A (observable) se spektrální dekompozicí

$$A = \sum_{i=0}^{k} a_i P_i = \sum_{i=0}^{k} a_i |p_i\rangle\langle p_i|,$$

kde a_i jsou unikátní vlastní hodnoty (eigenvalues) a P_i projekce do podprostoru určeného vlastními vektory (eigenvectors) $|p_i\rangle$.

Vlastní hodnoty odpovídají možným výsledkům získaných pomocí měření.

Výsledky měření

Měřením stavu $|\phi\rangle$ získáme výsledek a_i s pravděpodobností

$$\Pr(a_i) = ||P_i|\phi\rangle||^2 = \langle\phi|P_i|\phi\rangle\,.$$

Destruktivní důsledek měření

Stav $|\phi\rangle$ po měření kolabuje na stav

$$|\phi'\rangle = \frac{P_i|\phi\rangle}{\sqrt{\langle\phi|P_i|\phi\rangle}}\,.$$

$\Rightarrow$ pokud není $|\phi\rangle$ shodný s vlastním vektorem, který určuje projekční prostor, je původní superpozice stavu $|\phi\rangle$ nenávratně zničena.

Průměrná hodnota vlastních čísel

Při měření operátorem A se můžeme ptát, jaká bude průměrná naměřená hodnota. Víme, že

$$Pr(a_i) = ||P_i|\phi\rangle||^2 = \langle\phi|P_i|\phi\rangle,$$

$$A = \sum_{i=0}^{k} a_i P_i \,.$$

Potom

$$EA = \sum_{i=0}^{k} \Pr(a_i) a_i = \sum_{i=0}^{k} \langle\phi|a_i P_i|\phi\rangle = \langle\phi|A|\phi\rangle \,.$$

Výpočet vlastních vektorů a čísel

Vlastní čísla a vektory splňují rovnici

$$A|v\rangle = a|v\rangle$$

Úpravy:

$$A|v\rangle = a.\mathrm{I}.|v\rangle$$

$$(A - a.\mathrm{I})|v\rangle = 0$$

- pro $\det(A - a.\mathrm{I}) \neq 0 \Rightarrow |v\rangle = 0$
- pro $\det(A - a.\mathrm{I}) = 0 \Rightarrow |v\rangle \neq 0$

Výpočet vlastních vektorů a čísel

Pro operátor $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ vypočteme vlastní čísla:

$$\begin{vmatrix} 0-a & 1 \\ 1 & 0-a \end{vmatrix} = a^2 - 1 = 0 \quad \Rightarrow \quad a_{1,2} = \pm 1$$

Výpočet vlastního vektoru pro $a_1 = 1$:

$$\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \Rightarrow \quad v_1 = v_2 \quad \Rightarrow \quad |p_1\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Výpočet vlastního vektoru pro $a_2 = -1$:

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \Rightarrow \quad v_1 = -v_2 \quad \Rightarrow \quad |p_2\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

Duální báze

Po normalizaci dostaneme

$$|p_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ a } |p_2\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} .$$

Duální báze

Výše uvedené vektory tvoří tzv. duální bázi označovanou $\{|0'\rangle, |1'\rangle\}$. Platí

- $|0'\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$
- $|1'\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$