Úvod do kvantového počítání

5. přednáška

Miroslav Dobšíček

Katedra počítačů, Fakulta elektrotechnická
České vysoké učení technické v Praze

28. dubna 2005

Část I

Přehled z minulé hodiny

Shrnutí

1. Počet bázových stavů roste exponenciálně s počtem qubitů. Pro n=200 dostáváme počet atomů ve vesmíru.
2. Pro uložení čísla 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.

Část II

Dnešní přednáška

Kvantové brány

Kvantová brána

Kvantová brána s n vstupy a n výstupy je specifikována unitárním operátorem $U : H_{2^n} \to H_{2^n}$ a representována unitární maticí stupně 2^n.

Příklady:

Hadamardova rotace

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad H|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x.y} |y\rangle$$

Negace

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad NOT|x\rangle = |\bar{x}\rangle$$

Další často používané brány

Kontrolovaná negace (XOR)

$$CNOT = \begin{pmatrix} \mathbb{I} & 0 \\ 0 & NOT \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$CNOT\,|x,y\rangle = |x, x \oplus y\rangle$$

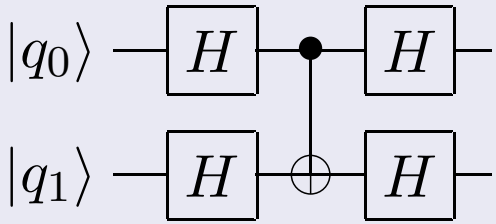
Kontrolovaný CNOT

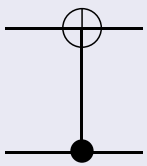
$$CCNOT = \begin{pmatrix} \mathbb{I} & 0 \\ 0 & CNOT \end{pmatrix},$$

$$CCNOT\,|x,y,z\rangle = |x,y,(x \wedge y) \oplus z\rangle$$

Jednoduché obvody

Inversní XOR brána

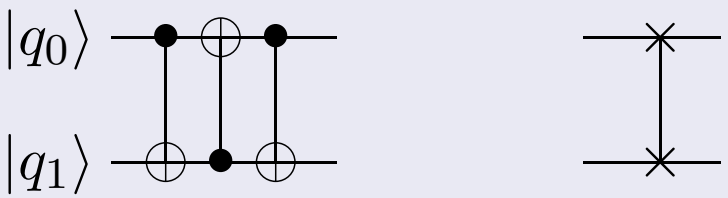




$$
\begin{aligned}
|0,1\rangle &\rightarrow \tfrac{1}{2}(|0,0\rangle + |1,0\rangle - |0,1\rangle - |1,1\rangle \\
&\rightarrow \tfrac{1}{2}(|0,0\rangle + |1,1\rangle - |0,1\rangle - |1,0\rangle \\
&\rightarrow |1,1\rangle
\end{aligned}
$$

Jednoduché obvody

Prohození (swap, flip)



Reversibilita

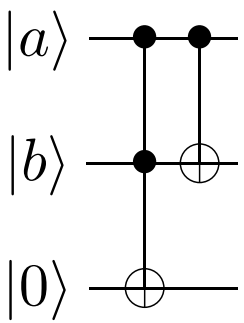
Reversibilní brány

Všechny kvantové brány jsou reprezentovány unitárními maticemi a tudíž jsou reverzibilní. To znamená, že např. AND a NAND nemůžeme implementovat přímo. Potřebujeme pomocné qubity (ancilla qubits), které zajistí jejich reverzibilitu. Jinými slovy akumulují historii výpočtu.
Sčítačka

$$(a, b) \rightarrow (a \oplus b, a \wedge b), \quad \text{není reversibilní.}$$

$$(a, b) \rightarrow (a, a \oplus b, a \wedge b), \quad \text{je reversibilní.}$$

Realizace 2-bitová sčítačky



Problém s akumulací historie

Tři pásky

C. Bennet (1973) dokázal, že pro jakoukoliv funkci f spočitatelnou na jednopáskovém TM, existuje třípáskový reversibilní TM, provádějící mapování

$$f : a \rightarrow (a, j(a), f(a)), \quad \text{kde } j(a) \text{ akumuluje historii.}$$

Omezení růstu historie

Dále nalezl reversibilní způsob jak zastavit nárůst historie.

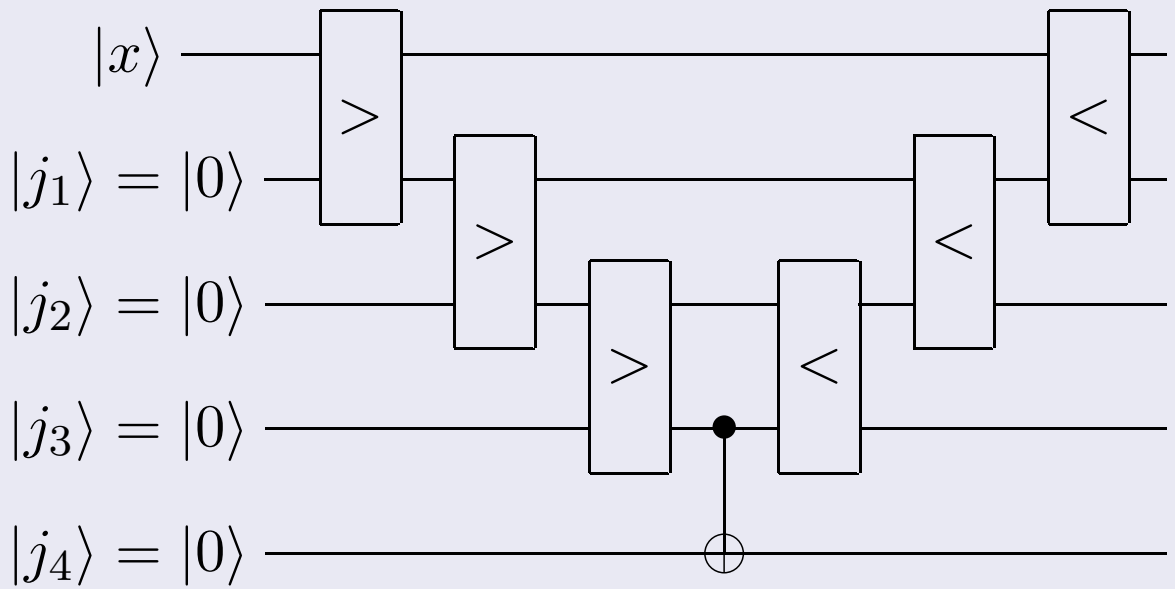
$$\text{Výpočet: } a \rightarrow (a, j(a), f(a))$$

$$\text{Rozvětvení: } (a, j(a), f(a)) \rightarrow (a, j(a), f(a), f(a))$$

$$\text{Výpočet}^{-1}\text{: } (a, j(a), f(a), f(a)) \rightarrow (a, f(a))$$

Omezení růstu historie

Blokové schéma



Hledání globálních vlastností dané funkce

Možné vlastnosti:

- Periodicita
- Konstantnost
- ...

Deutschův problém

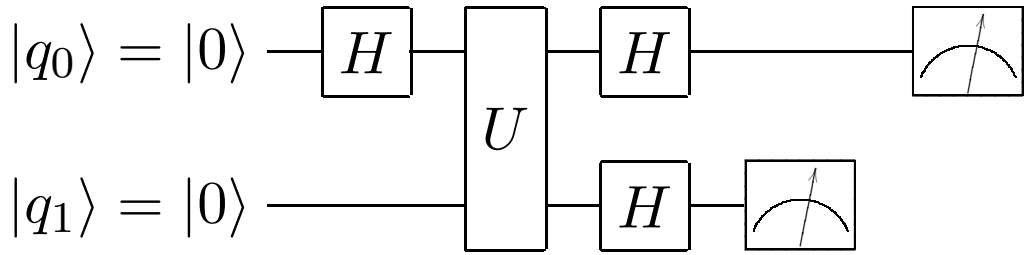
Je dána funkce $f : \{0,1\} \to \{0,1\}$ v podobě černé skříňky.
Zjistěte zda platí
$f(0) = f(1) \Rightarrow$ f je konstatní nebo
$f(0) \neq f(1) \Rightarrow$ f je balancovaná .

Převedení $f(x)$ do unitárního mapování

Mapování U_f

$$U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$$

Nedeterministické řešení



Měření na druhém qubitu

- 0 . . . informace ztracena.
- 1 . . . informace uložena v prvním qubitu.

Měření na prvním qubitu

- 0 . . . f je konstantní.
- 1 . . . f je balancovaná.

Převedení $f(x)$ do fáze

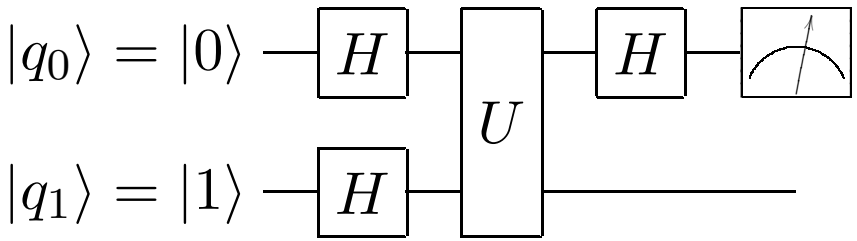
Mapování V_f

$$V_f : |x\rangle \rightarrow (-1)^{f(x)}|x\rangle$$

V_f se dá vyjádřit pomocí U_f:

$$U_f : |x, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\rangle \rightarrow (-1)^{f(x)}|x, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\rangle$$

Deterministické řešení



Měření na prvním qubitu

- 0 . . . f je konstatní.
- 1 . . . f je balancovaná.