

Úvod do kvantového počítání

Libor Veis

- 1 Kvantové bity
- 2 Kvantová hradla
- 3 Měření
- 4 Kvantové obvody

- Základní jednotkou klasické informace je *bit*, který může nabývat dvou diskrétních hodnot: 0, 1.
- Základní jednotkou kvantové informace je *qubit*, který může být libovolnou lineární kombinací báзовých stavů $|0\rangle$ a $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \quad (1)$$

- $|0\rangle, |1\rangle \dots$ *ortonormální* výpočetní báze
- $|\alpha|^2, |\beta|^2 \dots$ pravděpodobnost měření qubitu ve stavu $|0\rangle, |1\rangle$:

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2)$$

- Homogenní superpozice

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (3)$$

- Z rovnice (2) vyplývá, že stav qubitu lze napsat jako

$$|\psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right) \quad (4)$$

- $e^{i\gamma}$ je *neměřitelná* globální fáze

$$\langle\psi| \dots |\psi\rangle \Rightarrow e^{-i\gamma} e^{i\gamma} \dots \quad (5)$$

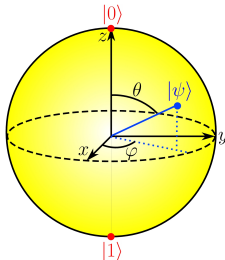
Úloha 1

Ověřte, že rovnice (4) splňuje normalizaci (2).

- Stav jednoho qubitu lze tedy efektivně zapsat jako

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad (6)$$

- Úhly θ a φ určují bod na tří-dimenzionální jednotkové Blochově sféře



Úloha 2

Jaký bod na Blochově sféře odpovídá stavu $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$?

- Výpočetní báze stavy $|0\rangle$ a $|1\rangle$ tvoří dvoudimenzionální vektorový (Hilbertův) prostor.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \text{tedy} \quad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

- Při přechodu k n qubitům pracujeme s 2^n dimenzionálním vektorovým prostorem, např.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

- Obecný dvou-qubitový stav má tvar

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \quad (7)$$

- Vícequbitové stavy mohou být:

Product states

$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- ▶ mohou být zapsány jako tensorový produkt vlnových funkcí sub-systémů

Entangled states

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \dots \text{Bellův stav}$$

- ▶ “spooky action at a distance”
- ▶ klíčové ingelligence kvantového počítání

- Qubity jsou obvykle inicializovány ve stavu $|\text{zero}\rangle = |0\dots 0\rangle$.
- Výpočetní báze stavy mohou kódovat decimální čísla v jejich binární podobě:

$$|4\rangle = |1\ 0\ 0\rangle$$

konvence: *třetí qubit* ← *druhý qubit* → *první qubit*

Úloha 3

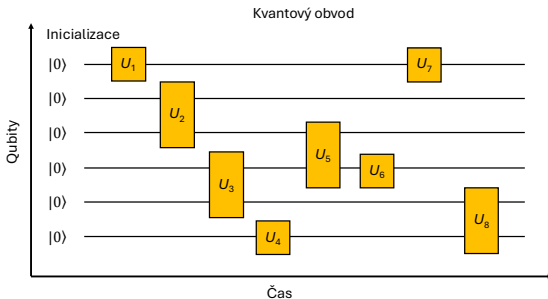
Dokažte, že Bellův stav nelze zapsat jako tensorový produkt stavů jednotlivých qubitů.

- Klasické počítačové obvody se skládají z vodičů a logických hradel.
- Nejpoužívanější výpočetní model kvantových počítačů je založený na kvantových obvodech, které se skládají z kvantových hradel.
- Protože časový vývoj kvantových systémů je unitární:

$$\hat{U}(t) = e^{-i\hat{H}t} \quad (8)$$

⇒ kvantová hradla jsou *unitární operátory*.

- Každou operaci s více qubity lze rozložit na sekvenci pouze jedno- a dvou-qubitových hradel.



- Kvantovou analogií klasického logického hradla NOT je Pauliho matice X :

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

$$\Rightarrow X|0\rangle = |1\rangle, \quad X|1\rangle = |0\rangle$$

$$\text{Obecně: } X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

- Důležité jsou i další Pauliho matice:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Exponenciálním tvarem Pauliho matic jsou vyjádřeny rotační operátory kolem os x , y a z :

$$R_x(\theta) = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} X = \begin{pmatrix} \cos \frac{\theta}{2} & -i \sin \frac{\theta}{2} \\ -i \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \quad (9)$$

$$R_y(\theta) = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Y = \begin{pmatrix} \cos \frac{\theta}{2} & -\sin \frac{\theta}{2} \\ \sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix} \quad (10)$$

$$R_z(\theta) = \cos \frac{\theta}{2} I - i \sin \frac{\theta}{2} Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \quad (11)$$

Úloha 4

Jaká rotace převede stav $|0\rangle$ na stav $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$?

Úloha 5

Pokud je x reálné číslo a pro matici A platí $A^2 = I$, ukažte že

$$\exp(iAx) = \cos(x)I + i\sin(x)A$$

- Důležitým jedno-qubitovým hradlem je Hadamardovo hradlo:

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

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

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

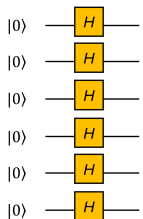
- Často se toto hradlo značí jen jako H , neplést s Hamiltoniánem!

Úloha 6: circuit identities

Je užitečné být schopen zjednodušovat obvody pohledem, s využitím dobře známých identit. Dokažte následující:

$$HXH = Z, \quad HYH = -Y, \quad HZH = X$$

- Aplikací Hadamardova hradla na n qubitů ve stavu $|0\rangle$ získáme homogenní superpozici všech možných 2^n stavů:


$$\begin{aligned} &= (H|0\rangle) \otimes (H|0\rangle) \otimes (H|0\rangle) \otimes \dots \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \dots \\ &= \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle \end{aligned}$$

- Libovolné jedno-qubitové hradlo, U , lze složit z rotací podél dvou neparalelních vektorů, např. os z a y :

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta) \quad (12)$$

- Pro univerzalitu jsou potřeba *entanglující* dvou-qubitová hradla, tzn. ne ve tvaru $U_1 \otimes U_2$
- Nejčastěji používaným je controlled NOT, CNOT:


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{l} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \rightarrow \begin{array}{l} |00\rangle \\ |01\rangle \\ |11\rangle \\ |10\rangle \end{array}$$

Úloha 7

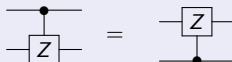
Na příkladu stavu $|+\rangle \otimes |0\rangle$ ověřte, že CNOT je entanglující dvou-qubitové hradlo, tzn. že vytvoří entanglovaný stav.

- Alternativou může být controlled-Z:

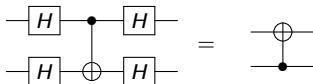
$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Úloha 8

Ověřte, že platí následující rovnost:

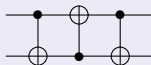


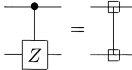
- Z úlohy 8 vyplývá, že role “control” a “target” je v případě kvantových počítačů libovolná.
- Na základě úlohy 6 není těžké ověřit, že platí také následující rovnost



Úloha 8

Ověřte, že prohození dvou qubitů (SWAP gate) se dá realizovat sekvencí 3 CNOT hradel:

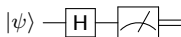


Hadamard		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	controlled-NOT		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Pauli-X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	swap		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Pauli-Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	controlled-Z		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	controlled-phase		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$			
$\pi/8$		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$			

- Zdroj: M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press 2000.

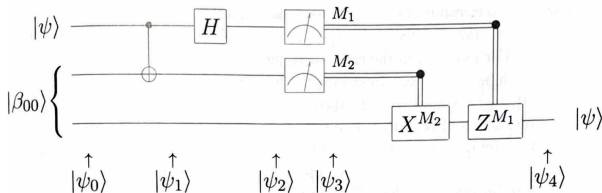
- Posledním krokem kvantových obvodů je obvykle měření.
- Měření má *destruktivní charakter* - kolaps vlnové funkce.
- Pozorovatelné veličiny O jsou reprezentovány Hermitovskými maticemi, můžeme měřit jejich střední hodnotu, tzn. $\langle O \rangle = \langle \psi | O | \psi \rangle$, průměrováním přes mnoho měření.
- Měření ve *výpočetní bázi* $i^{\text{tého}}$ qubitů: $\langle \psi | Z_i | \psi \rangle$.
- Stringy fermionických operátorů mohou být reprezentovány pomocí stringů Pauliho matic (uvidíme později) - potřebujeme měřit také v bázi vlastních vektorů matic X a $Y \Rightarrow$ báze transformace, např.

Měření v X bázi:



$$\begin{aligned} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned}$$

- Neznámý kvantový stav nelze zkopírovat - *No cloning theorem* (viz. později)!
- Kvantová teleportace spočívá v přenosu stavu z jednoho qubitu (který je změřen - zaniká!) na druhý. Neporušuje tedy *no cloning theorem*. Byla několikrát realizována experimentálně.
- Realizace probíhá prostřednictvím sdíleného *entanglovaného* stavu dvou qubitů.
- Protože se musí komunikovat klasickou cestou výsledek měření z jedné strany na druhou, není v rozporu se speciální teorií relativity (rychlost teleportace nemůže být vyšší než rychlost světla!).



$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (13)$$

- Analýza kvantového obvodu:

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

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]$$

$$|\psi_2\rangle = \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$$

$$|\psi_2\rangle = \frac{1}{2} [|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

Úloha 9

Naimplementujte a vyzkoušejte si kvantovou teleportaci v prostředí OpenQASM:
<http://quantum.ibm.com/composer>.