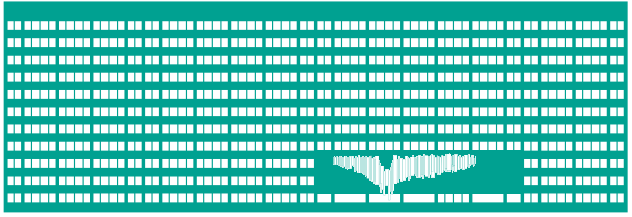
VŠB TECHNICKÁ UNIVERZITA OSTRAVA

VSB TECHNICAL UNIVERSITY OF OSTRAVA



www.vsb.cz

Základy kvantového počítání

Marek Lampart

VŠB – Technická Univerzita Ostrava

marek.lampart@vsb.cz

18. ledna, 2023

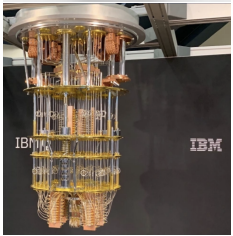
VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA APLIKOVANÉ MATEMATIKY


NCC-1701

Kvantový počítač

- **Kvantový počítač**
  - teoretický model zařízení vykonávající výpočty
  - využívá fenomény kvantové mechaniky: **superpozice**, **interference**
- Kvantové počítání
  - v klasickém počítači data reprezentujeme bity (0, 1)
  - v kvantovém počítači se používáme qubity (kvantové bity), které mohou být nula, jedna, nebo i kombinace obou

Kvantový počítač



- **Kvantový počítač**
  - teoretický model zařízení vykonávající výpočty
  - využívá fenomény kvantové mechaniky: **superpozice**, **interference**
- **Kvantové počítání**
  - v klasickém počítači data reprezentujeme bity (0, 1)
  - v kvantovém počítači se používáme qubity (kvantové bity), které mohou být nula, jedna, nebo i kombinace obou

Trošku historie

- Kvantový počítač byl poprvé navržen v roce 1981 laureátem Nobelovy ceny Richardem Feynmanem.
- Průlomovým algoritmem v kvantovém počítání byla publikace P. Shora z roku 1994 o kvantovém algoritmu pro provádění prvočíselného rozkladu celých čísel v podstatě v polynomiálním čase.
- *Kvantové počítání* (teorie) je průsečíkem matematiky, fyziky a informatiky.

Trošku historie

- Kvantový počítač byl poprvé navržen v roce 1981 laureátem Nobelovy ceny Richardem Feynmanem.
- Průlomovým algoritmem v kvantovém počítání byla publikace P. Shora z roku 1994 o kvantovém algoritmu pro provádění prvočíselného rozkladu celých čísel v podstatě v polynomiálním čase.
- *Kvantové počítání* (teorie) je průsečíkem matematiky, fyziky a informatiky.

Trošku historie

- Kvantový počítač byl poprvé navržen v roce 1981 laureátem Nobelovy ceny Richardem Feynmanem.
- Průlomovým algoritmem v kvantovém počítání byla publikace P. Shora z roku 1994 o kvantovém algoritmu pro provádění prvočíselného rozkladu celých čísel v podstatě v polynomiálním čase.
- *Kvantové počítání* (teorie) je průsečíkem matematiky, fyziky a informatiky.

Trošku historie

- Kvantový počítač byl poprvé navržen v roce 1981 laureátem Nobelovy ceny Richardem Feynmanem.
- Průlomovým algoritmem v kvantovém počítání byla publikace P. Shora z roku 1994 o kvantovém algoritmu pro provádění prvočíselného rozkladu celých čísel v podstatě v polynomiálním čase.
- *Kvantové počítání* (teorie) je průsečíkem matematiky, fyziky a informatiky.

Trošku historie

- Kvantový počítač byl poprvé navržen v roce 1981 laureátem Nobelovy ceny Richardem Feynmanem.
- Průlomovým algoritmem v kvantovém počítání byla publikace P. Shora z roku 1994 o kvantovém algoritmu pro provádění prvočíselného rozkladu celých čísel v podstatě v polynomiálním čase.
- *Kvantové počítání* (teorie) je průsečíkem matematiky, fyziky a informatiky.

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- Kvantová chemie
- Počítačem podporovaný návrh léčiv a generativní chemie
- Optimalizační úlohy

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Aplikace

- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- Optimalizační úlohy

Aplikace

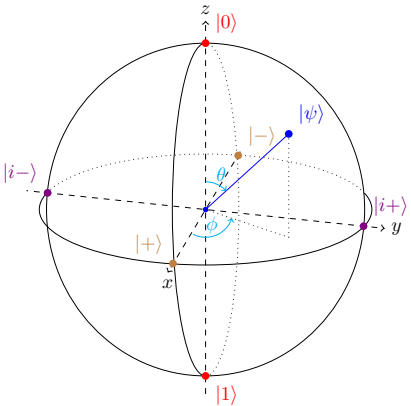
- Kryptografie
- Prohledávání
- Simulace kvantových systémů
- Strojové učení
- Výpočetní biologie
- **Kvantová chemie**
- Počítačem podporovaný návrh léčiv a generativní chemie
- **Optimalizační úlohy**

Kvantový bit (zkráceně *qubit*) je dvoudimenzionální kvantově mechanický systém, který je ve stavu

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

kde α i β jsou komplexní čísla, což jsou *amplitudy* kvantových stavů $|0\rangle$ resp. $|1\rangle$, platí $|\alpha|^2 + |\beta|^2 = 1$.
V této definici se užívá standardní *bra-ketová* notace, tady označuje

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad \text{a} \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$



Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohu být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n bázových vektorů délky 2^n

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

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohu být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n bázových vektorů délky 2^n

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

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantové registry

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohu být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n bázových vektorů délky 2^n

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

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantové registry

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohu být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n bázových vektorů délky 2^n

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

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohu být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n bázových vektorů délky 2^n

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

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

Kvantový registr

- zahrnuje více qubitů najednou,
- kvantový registr je tedy analogie klasického procesorového registru a kvantové počítače provádějí výpočty pomocí manipulací qubitů v rámci daného registru,
- každý qubit $|\psi\rangle$ v registru je superpozicí $\alpha|0\rangle + \beta|1\rangle$ prvků výpočetní báze $|0\rangle$ a $|1\rangle$,
- registr s n qubity je superpozicí všech možných 2^n bitových řetězců, které mohu být reprezentovány n bity,
- stavový prostor n kvantového registru je lineární kombinací n bázových vektorů délky 2^n

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

kde i je celé číslo v desítkové soustavě reprezentující číslo délky n ve dvojkové soustavě.

- Pro (1) platí normalizační podmínka pro jednotlivé amplitudy pravděpodobností:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \tag{2}$$

- Logicky, součet pravděpodobností všech možných stavů musí být 1, protože žádný jiný stav nastat nemůže a zároveň se jednotlivé stavy navzájem vylučují.
- Kvantové registry jsou přímým rozšířením qubitů.

- Pro (1) platí normalizační podmínka pro jednotlivé amplitudy pravděpodobností:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \tag{2}$$

- Logicky, součet pravděpodobností všech možných stavů musí být 1, protože žádný jiný stav nastat nemůže a zároveň se jednotlivé stavy navzájem vylučují.
- Kvantové registry jsou přímým rozšířením qubitů.

- Pro (1) platí normalizační podmínka pro jednotlivé amplitudy pravděpodobností:

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1. \tag{2}$$

- Logicky, součet pravděpodobností všech možných stavů musí být 1, protože žádný jiný stav nastat nemůže a zároveň se jednotlivé stavy navzájem vylučují.
- Kvantové registry jsou přímým rozšířením qubitů.

Kvantové registry

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (0\,0\,1\,0\,0\,0\,0\,0)^{\mathrm{T}}.$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (0\,0\,1\,0\,0\,0\,0\,0)^{\mathrm{T}}.$$

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = (0\,0\,1\,0\,0\,0\,0\,0)^{\mathrm{T}}.$$

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}.$$

- Každá bitová konfigurace v kvantové superpozici je označena jako tenzorový součin jednotlivých qubitů.
- Například $|010\rangle$, která reprezentuje v bitovém řetězci číslo 2, má tvar:

$$|010\rangle = |0\rangle \otimes |1\rangle \otimes |0\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = (0\,0\,1\,0\,0\,0\,0\,0)^{\mathrm{T}}.$$

$$\begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}.$$

Kvantové registry

- Připomeňme, že $\otimes$ značí operaci *tenzorového součinu* definovaného pro dva vektory $|u\rangle$ a $|v\rangle$ dimenze m resp. n následujícím způsobem

$$|u\rangle\,|v\rangle = |uv\rangle \quad = |u\rangle \otimes |v\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 v \\ u_2 v \\ \vdots \\ u_m v \end{pmatrix} =$$

$$= \begin{pmatrix} u_1 v_1 & u_1 v_2 & \dots & u_1 v_n & u_2 v_1 & u_2 v_2 & \dots & u_2 v_n & \dots & u_m v_1 & u_m v_2 & \dots & u_m v_n \end{pmatrix}^T$$

- Výsledný vektor $|uv\rangle$ je tedy dimenze mn.
- Tenzorový součin je distributivní i asociativní, ale obecně není komutativní.

- Připomeňme, že $\otimes$ značí operaci *tenzorového součinu* definovaného pro dva vektory $|u\rangle$ a $|v\rangle$ dimenze m resp. n následujícím způsobem

$$|u\rangle\,|v\rangle = |uv\rangle \quad = |u\rangle \otimes |v\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 v \\ u_2 v \\ \vdots \\ u_m v \end{pmatrix} =$$

$$= \begin{pmatrix} u_1v_1 & u_1v_2 & \dots & u_1v_n & u_2v_1 & u_2v_2 & \dots & u_2v_n & \dots & u_mv_1 & u_mv_2 & \dots & u_mv_n \end{pmatrix}^T$$

- Výsledný vektor $|uv\rangle$ je tedy dimenze mn.
- Tenzorový součin je distributivní i asociativní, ale obecně není komutativní.

- Připomeňme, že $\otimes$ značí operaci *tenzorového součinu* definovaného pro dva vektory $|u\rangle$ a $|v\rangle$ dimenze m resp. n následujícím způsobem

$$|u\rangle\,|v\rangle = |uv\rangle \quad = |u\rangle \otimes |v\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 v \\ u_2 v \\ \vdots \\ u_m v \end{pmatrix} =$$

$$= \begin{pmatrix} u_1v_1 & u_1v_2 & \dots & u_1v_n & u_2v_1 & u_2v_2 & \dots & u_2v_n & \dots & u_mv_1 & u_mv_2 & \dots & u_mv_n \end{pmatrix}^T$$

- Výsledný vektor $|uv\rangle$ je tedy dimenze mn.
- Tenzorový součin je distributivní i asociativní, ale obecně není komutativní.

- Připomeňme, že $\otimes$ značí operaci *tenzorového součinu* definovaného pro dva vektory $|u\rangle$ a $|v\rangle$ dimenze m resp. n následujícím způsobem

$$|u\rangle\,|v\rangle = |uv\rangle \quad = |u\rangle \otimes |v\rangle = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{pmatrix} \otimes \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 v \\ u_2 v \\ \vdots \\ u_m v \end{pmatrix} =$$

$$= \begin{pmatrix} u_1v_1 & u_1v_2 & \dots & u_1v_n & u_2v_1 & u_2v_2 & \dots & u_2v_n & \dots & u_mv_1 & u_mv_2 & \dots & u_mv_n \end{pmatrix}^T$$

- Výsledný vektor $|uv\rangle$ je tedy dimenze mn.
- Tenzorový součin je distributivní i asociativní, ale obecně není komutativní.

Například tří qubitový registr má tvar

$$|\psi_3\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle \quad (3)$$

Kvantové brány

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*[1].
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

[1] Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^{\dagger}$, kde $U^{\dagger}$ je matice konjugovaná k matici U ($U^{\dagger} = \overline{U}^{T}$). Navíc platí $UU^{\dagger} = U^{\dagger}U = I$.

Kvantové brány

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*[1].
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

[1] Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^{\dagger}$, kde $U^{\dagger}$ je matice konjugovaná k matici U ($U^{\dagger} = \overline{U}^{T}$). Navíc platí $UU^{\dagger} = U^{\dagger}U = I$.

Kvantové brány

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*[1].
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

[1] Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^{\dagger}$, kde $U^{\dagger}$ je matice konjugovaná k matici U ($U^{\dagger} = \overline{U}^{T}$). Navíc platí $UU^{\dagger} = U^{\dagger}U = I$.

Kvantové brány

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*[1].
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

[1] Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^{\dagger}$, kde $U^{\dagger}$ je matice konjugovaná k matici U ($U^{\dagger} = \overline{U}^{T}$). Navíc platí $UU^{\dagger} = U^{\dagger}U = I$.

Kvantové brány

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*[1].
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

[1] Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^{\dagger}$, kde $U^{\dagger}$ je matice konjugovaná k matici U ($U^{\dagger} = \overline{U}^{T}$). Navíc platí $UU^{\dagger} = U^{\dagger}U = I$.

Kvantové brány

- Klasické logické brány jsou matematicky popsány pomocí Booleovské algebry. Kvantové logické brány fungují na podobném principu.
- Kvantové logické brány aplikované na kvantové registry zobrazují kvantovou superpozici na jinou a společně umožňují vývoj systému do nějakého požadovaného konečného stavu, správné odpovědi.
- Kvantové logické brány jsou matematicky reprezentovány pomocí transformací matic (lineárních operací) aplikovaných na kvantový registr tenzorováním transformačních matic maticí reprezentující daný registr.
- Všechny matice odpovídající kvantové logické bráně jsou *unitární*[1].
- Unitární transformace prováděné na jednom qubitu mohou být efektivně vizualizovány na Blochově sféře.
- Tak jako v případě klasických logických bran je i v případě kvantových logických bran zavedena standardní množina používaných bran.

[1] Komplexní matice U je *unitární* právě tehdy, když $U^{-1} = U^{\dagger}$, kde $U^{\dagger}$ je matice konjugovaná k matici U ($U^{\dagger} = \overline{U}^{T}$). Navíc platí $UU^{\dagger} = U^{\dagger}U = I$.

- *Pauliho brány* X, Y a Z odpovídají rotaci o úhel π kolem osy x, y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$-\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- *Pauliho brány* X, Y a Z odpovídají rotaci o úhel π kolem osy x, y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$-\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- *Pauliho brány* X, Y a Z odpovídají rotaci o úhel π kolem osy x, y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$-\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- *Pauliho brány* X, Y a Z odpovídají rotaci o úhel π kolem osy x, y či z respektive.
- Pauliho brána X přehodí amplitudy $|0\rangle$ a $|1\rangle$

$$-\boxed{X}- = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- $$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

- $$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

- Nejdůležitější a taky nejpoužívanější binární kvantovou branou je CNOT

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

- Nejdůležitější a taky nejpoužívanější binární kvantovou branou je CNOT

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

- Nejdůležitější a taky nejpoužívanější binární kvantovou branou je CNOT

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

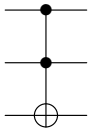
-

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

Nejdůležitější a taky nejpoužívanější ternární kvantovou branou je Toffoliho brána (CCNOT)

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

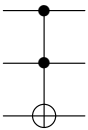
Nejdůležitější a taky nejpoužívanější ternární kvantovou branou je Toffoliho brána (CCNOT)



$$=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$$

Kvantové brány

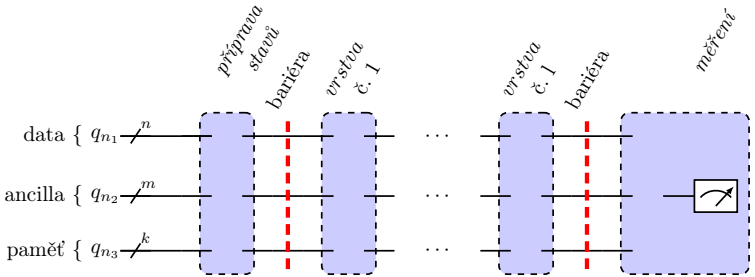
Brána	značení	vstup	výstup
Pauli-X		$\|0\rangle$	$\|1\rangle$
		$\|1\rangle$	$\|0\rangle$
CNOT		$\|00\rangle$	$\|00\rangle$
		$\|01\rangle$	$\|01\rangle$
		$\|10\rangle$	$\|11\rangle$
		$\|11\rangle$	$\|10\rangle$

Brána	značení	vstup	výstup
Toffoli		$\|000\rangle$	$\|000\rangle$
		$\|001\rangle$	$\|001\rangle$
		$\|010\rangle$	$\|010\rangle$
		$\|100\rangle$	$\|100\rangle$
		$\|011\rangle$	$\|011\rangle$
		$\|101\rangle$	$\|101\rangle$
		$\|110\rangle$	$\|111\rangle$
		$\|111\rangle$	$\|110\rangle$

Kvantový obvod - obecně

Tři základní vrstvy:

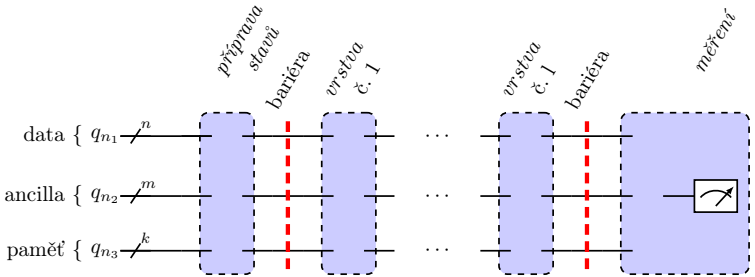
1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



Kvantový obvod - obecně

Tři základní vrstvy:

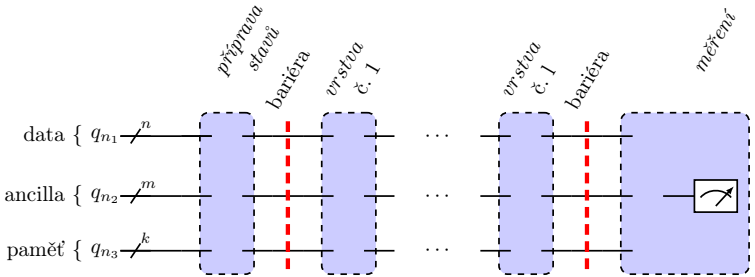
1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



Kvantový obvod - obecně

Tři základní vrstvy:

1. kódování dat, která mohou být klasická nebo kvantová, do stavu sady vstupních qubitů,
2. posloupnost kvantových bran aplikovaných na tuto sadu vstupních qubitů,
3. měření jednoho nebo více qubitů na konci pro získání klasicky interpretovatelného výsledku.



Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

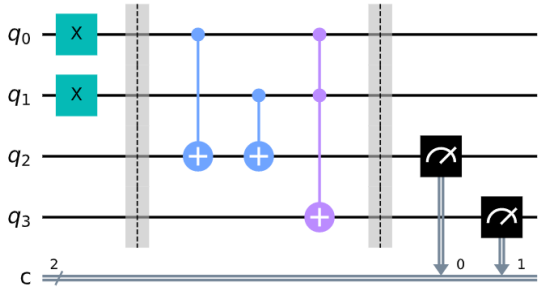
4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Měření

1. jediný způsob, jak extrahovat informace z n qubitů v daném stavu,
2. proces měření provádí hardware s digitálním displejem, tzv. n-qubitová měřicí brána,
3. n-qubitová měřicí brána je schematicky znázorněna symbolem

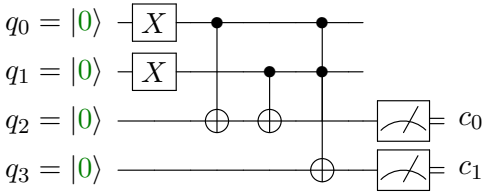
4. na rozdíl od unitárních bran, které mají jedinečný výstupní stav pro každý vstupní stav, je stav qubitů vycházejících z měřicí brány statisticky určen pouze stavem vstupních qubitů,
5. akci měření nelze vrátit zpět: ke konečnému stavu neexistuje způsob, jak rekonstruovat počáteční stav,
6. měření je nevratné,
7. měření není v žádném smyslu lineární,
8. říkáme, že stav před měřením se v důsledku měření redukuje/kolabuje na stav po měření,
9. stav n qubitů není nic jiného než abstraktní symbol, používaný prostřednictvím Bornova pravidla k výpočtu pravděpodobností výsledků měření.

Jednoduchý kvantový obvod

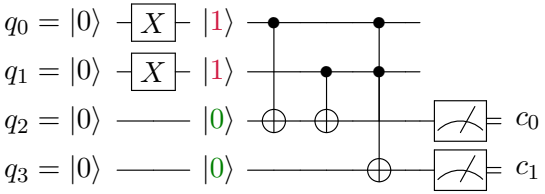


Vstup	Výstup
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|10\rangle$

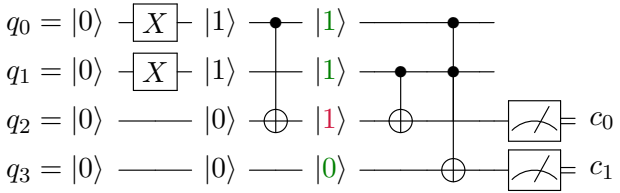
Jednoduchý kvantový obvod



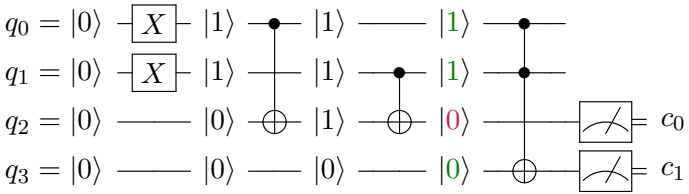
Jednoduchý kvantový obvod



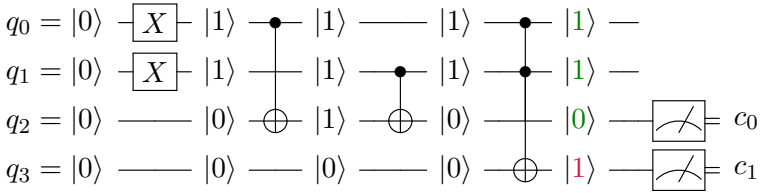
Jednoduchý kvantový obvod



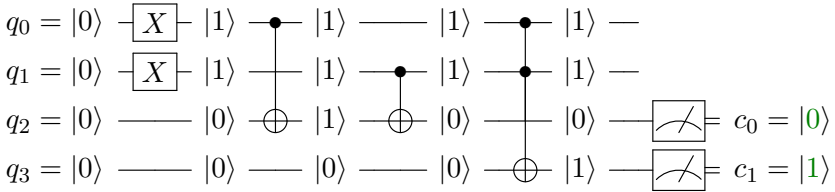
Jednoduchý kvantový obvod



Jednoduchý kvantový obvod



Jednoduchý kvantový obvod



... ale to podstatné zatím nezaznělo

Kvantová superpozice stavů

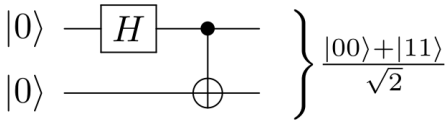
- základní princip kvantové mechaniky
- každé dva (a více) kvantové stavy lze kombinovat (superponovat)
- vzniká nový kvantový stav

Brána	značení	vstup	výstup
Hadamard		$\|0\rangle$ $\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$

50% pravděpodobnost, že na výstupu bude naměřena hodnota $|0\rangle$
50% pravděpodobnost, že na výstupu bude naměřena hodnota $|1\rangle$

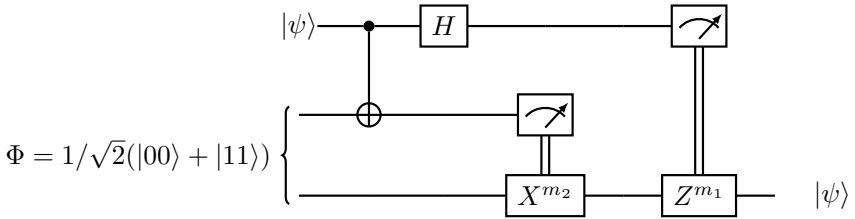
Ještě jeden příklad

Jednoduchý kvantový obvod, který vytváří *provázanost* dvou qubitů



výstup tohoto obvodu nelze rozdělit na jednotlivé základní stavy $|0\rangle$ a $|1\rangle$

Kvantový obvod reprezentující teleportaci kvantového stavu



Děkujeme za pozornost

Marek Lampart

VŠB – Technická Univerzita Ostrava

marek.lampart@vsb.cz

18. ledna, 2023

VŠB TECHNICKÁ UNIVERZITA OSTRAVA | FAKULTA ELEKTROTECHNIKY A INFORMATIKY | KATEDRA APLIKOVANÉ MATEMATIKY