

**Technická Univerzita v Kosiciach  
Fakulta elektrotechniky a informatiky**

# **Meranie a interakcia kvantových obvodov**

**Diplomová práca**

**2020**

**Marián Sabat**

**Technická Univerzita v Kosiciach  
Fakulta elektrotechniky a informatiky**

# **Meranie a interakcia kvantových obvodov**

**Diplomová práca**

Študijný program: Informatika

Študijný odbor: 9.2.1 Informatika

Školiace pracovisko: Katedra počítačov a informatiky (KPI)

Školiteľ: prof. Ing. Ján Kollár, CSc.

Konzultant:

**Košice 2020**

**Marián Sabat**

Názov práce: Meranie a interakcia kvantových obvodov

Pracovisko: Katedra počítačov a informatiky, Technická Univerzita v Ko-  
siciach

Autor: Marián Sabat

Školiteľ: prof. Ing. Ján Kollár, CSc.

Konzultant:

Dátum: 1. 1. 2020

Kľúčové slová: Kvantové počítanie a iné kľúčové slova

Abstrakt: ABSTRAKT

Thesis title: Measurement and interaction of quantum circuits

Department: Department of Computers and Informatics, Technical University of Kosice

Author: Marián Sabat

Supervisor: prof. Ing. Ján Kollár, CSc.

Tutor:

Date: 1. 1. 2020

Keywords: Quantum computers and other key words

Abstract: ABSTRAKT

Tu vložte zadávací list pomocí příkazu  
`\thesispec{cesta/k/suboru/so/zadavacim.listom}`  
v preambule dokumentu.

### **Čestné vyhlásenie**

Vyhlasujem, ze vsetko som pisal sam ...

Košice, 1.1.2020

.....

*Vlastnoručný podpis*

**Podakovanie**

# Obsah

---

Úvod	1
1 Ciele prace (Formulacia ulohy)	2
2 Matematické základy kvantových systémov	3
2.1 Matice	3
2.1.1 Násobenie matice skalárom	3
2.1.2 Násobenie matíc	4
2.1.3 Transpozícia matice	4
2.1.4 Tenzorový súčin matíc	4
2.2 Komplexné čísla	4
2.2.1 Operácie na množine komplexných čísel	5
2.2.2 Základné charakteristiky komplexných čísel	6
2.3 Vektory	6
2.4 Pojmi a definície	7
3 Teoretické základy kvantových systémov	9
3.1 Základné definície	9
3.2 Systém s jedným kvantovým bitom	11
3.3 System s viacerými kvantovými bitmi	11
3.4 Princíp merania	11
4 Kvantový systém	12
4.1 IBM QX	12
4.1.1 Stavy a ich zapis	12
4.1.2 Operácie kvantových hradiel	12



---

<b>5</b>	<b>Pravdepodobnostná analýza kvantových obvodov</b>	<b>13</b>
5.1	Analýza nepreviazaných stavov . . . . .	13
5.2	Analýza previazaných stavov . . . . .	14
<b>6</b>	<b>Meranie kvantových obvodov</b>	<b>16</b>
6.1	Princíp merania kvantových obvodov . . . . .	16
6.2	Fiktívne meranie . . . . .	16
6.2.1	Experiment 1 . . . . .	16
6.2.2	Experiment 2 . . . . .	16
6.2.3	Experiment 3 . . . . .	16
<b>7</b>	<b>Pravdepodobnostný model kvantového výpočtu - návrh a realizácia</b>	<b>17</b>
7.1	Definícia vstupu . . . . .	17
7.2	Pravdepodobnostný model . . . . .	18
<b>8</b>	<b>Kvantová teleportácia</b>	<b>21</b>
<b>9</b>	<b>Celkové vyhodnotenie</b>	<b>22</b>
<b>10</b>	<b>Záver</b>	<b>23</b>
	<b>Literatúra</b>	<b>24</b>

# Zoznam obrázkov

---

2.1	Zobrazenie komplexného čísla $z$ : $x$ - reálna os, $y$ - imaginárna os . .	5
5.1	Jednoduchý kvantový obvod (namodelovaný v IBM Quantum Experience) . . . . .	13
7.1	Konceptuálny návrh programu . . . . .	17
7.2	Kvantový obvod s previazanými kvantovými bitmi. . . . .	18
7.3	Strom stavov (StateTree) po vykonaní kvantového obvodu. . . . .	19

# Úvod

---

Často sa hovorí o konci platnosti Moorovho zákona. Je možné, že v blízkej budúcnosti svet bude nútený zmentiť klasické počítače od základu. Jedným často spomínaným vývojovým schodom v tejto oblasti je kvantový počítač. Pokusy využiť kvantovú fyziku v odbore počítačovej vedy možno nájsť už v minulosti, no až v horizonte niekoľkých rokov nastal prelom a kvantové počítače vznikajú po celom svete.

No napriek tomu stále chýba množstvo nástrojov, ktoré by sprístupnili vývoj širšej verejnosti. Existujú voľne dostupné simulátory na generovanie kvantových obvodov, ale od plne funkčných programov máme ešte ďaleko. Tento odbor je veľmi náročný a každý pokus zaberá množstvo času.

Touto prácou sa pokúsime vylepšiť súčasnú situáciu. A to vytvorením nástroja, ktorý by zlepšil porozumenie pri vykonávaní programov. I keď nepôjde o dokonale sofistikovaný simulátor kvantového počítača, napriek tomu porozumenie, zrýchlenie a spríjemnenie vývoja programov pre tento druh počítačov môže priniesť nové pokroky v odvetví.

Bude v našom úmysle, čo najjednoduchšie vysvetliť princípy, ktoré sa skrývajú za fungovaním kvantových počítačov. Naša práca ponúka teoretické minimum nutné na porozumenie praktických experimentov a využíva ho pri priblížení základných kvantových javov, ako napríklad zvjazanie kvantových bitov, ktoré tvoria podstatu kvantových výpočtov ale aj pri zložitejších úkonoch ako kvantová teleportácia.

Čo je najdôležitejšie, pokúsime sa jasne a zrozumiteľne vysvetliť princíp merania zmien stavov kvantových bitov. Poskytneme pohľad do matematického aparátu, ktorý umožňuje simuláciu kvantových programov na klasických strojoch. Priblížime vývoj pravdepodobnostného modelu vytvoreného vo funkcionálnom jazkyu Haskell. A poskytneme komplexný návod na jeho použitie.

# 1 Ciele prace (Formulacia ulohy)

---

Prvou z častí, ktoré je nutné splniť je analýza princípov merania pri vykonávaní kvantových programov. Je nutné poskytnúť teoretické informácie o spôsobe fungovania kvantových počítačov a vysvetliť matematické úkony, doplnené o praktické príklady, nutné pri meraní zmeny stavov kvantových bitov.

Hlavným grom práce bude tvoriť návrh a implementácia zjednodušeného kvantového systému. Tento program bude schopný merať stav kvantového systému bez kolabovania bitov. Funkcionalita bude postavená na princípoch získaných z analýzy.

Podstatnou funkcionalitou výsledného programu bude grafické zobrazenie vypočítaných pravdepodobností stavov kvantových bitov a prehľad ako sa dané bity menia počas behu programu.

## 2 Matematické základy kvantových systémov

---

Na pochopenie problematiky kvantových počítačov je nutná znalosť aspoň základnej lineárnej algebry. V tejto kapitole je opísaný matematický aparát využívaný ako teoretický základ celej práce.

### 2.1 Matice

Maticou typu  $m \times n$  je nazývaná sústava prvkov zapísaných do schémy s  $m$  riadkami a  $n$  stĺpcami, kde  $n, m \in \mathbb{N}$  [1]. Teda:

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & & & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

#### 2.1.1 Násobenie matice skalárom

Toto násobenie je vykonané násobením každého prvku matice danou skalárnou hodnotou [1]. Majme maticu  $A$  typu  $2 \times 2$  a skalárnu hodnotu  $k$ , potom platí

$$kA = k \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} ka_{11} & ka_{12} \\ ka_{21} & ka_{22} \end{bmatrix}$$

Operácia násobenia matice skalárnou hodnotou je komutatívna, čiže na poradí operandov nezáleží. Nech  $B$  je matica a  $\alpha, \beta$  sú skalárne hodnoty, potom

$$(\alpha + \beta)B = \alpha B + \beta B,$$

$$(\alpha\beta)B = \alpha(\beta B)$$

### 2.1.2 Násobenie matíc

Nech je daná matica  $A$  typu  $m \times n$  a matica  $B$  typu  $n \times p$ , potom výsledná matica  $C = AB$  je typu  $m \times p$  a pre jej prvky platí

$$c_{ij} = \sum_{k=1}^n A_{ik} B_{kj} = A_{i1} B_{1j} + \dots + A_{in} B_{nj},$$

kde  $i = 1, \dots, m$ , a  $j = 1, \dots, p$  [1]. Pre túto operáciu neplatí komutatívnosť.

### 2.1.3 Transpozícia matice

Ak  $A$  je matica typu  $m \times n$ , potom jej transponovaná matica  $A^T$  je typu  $n \times m$  a platí [1]

$$(A^T)_{ij} = A_{ji}$$

### 2.1.4 Tenzorový súčin matíc

Nech  $A$  je matica typu  $m \times n$  a  $B$  je typu  $r \times s$ . Tenzorový súčin alebo Kroneckerov súčin, označený ako  $A \otimes B$  je definovaný ako [2]

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \dots & & & \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}$$

Nakoľko je  $a_{ij}B$  submatica typu  $r \times s$ , je zjavné, že výsledná matica je typu  $mr \times ns$ .

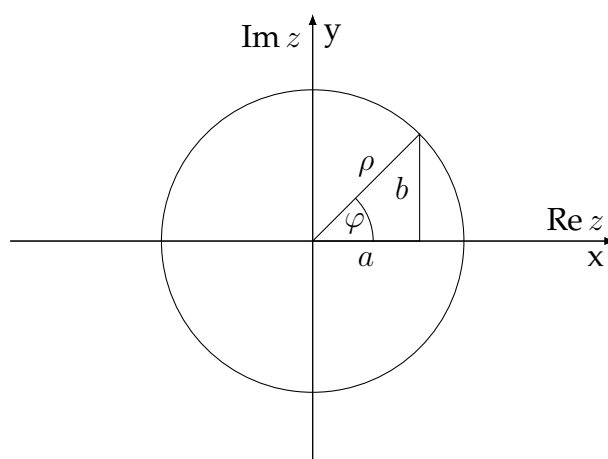
## 2.2 Komplexné čísla

Množinou komplexných čísel  $\mathbb{C}$  je nazývaná množina  $\mathbb{R}^2$  spolu s operáciami sčítania a násobenia. Ľubovoľný prvok  $z = (a, b) \in \mathbb{C}$  je nazývaný komplexné číslo [3]. Komplexné čísla možno reprezentovať nie len ako usporiadanú dvojicu, ale aj pomocou:

1. Algebraickej formy

$$z = a + bi$$

, kde  $a, b \in \mathbb{R}$  a  $i^2 = -1$ ,



Obr. 2.1: Zobrazenie komplexného čísla  $z$ :  $x$  - reálna os,  $y$  - imaginárna os

2. Polárnych súradníc  $\rho$  a  $\varphi$ ,

kde  $\rho, \varphi \in \mathbb{R}$  a  $\rho > 0$ . V geometrickej reprezentácii (Obr. 2.1) je  $\rho$  veľkosť vektora  $\vec{Oz}$ , kde  $O$  je počiatok súradnicovej sústavy, a  $\varphi$  je uhol medzi osou  $x$  a daným vektorom.

Je zrejmé, že pre vyjadrenie pomocou polárnych súradníc platí  $a = \rho \cos \varphi$  a  $b = \rho \sin \varphi$  [3]. Potom je možné zapísať

$$z = \rho e^{i\varphi}$$

,kde  $z \in \mathbb{C}$ ,  $\rho, \varphi \in \mathbb{R}$  a  $\rho > 0$ .  $e^{i\varphi}$  je komplexná jednotka, inak povedané jej absolútna hodnota je rovná 1.

$$|e^{i\varphi}| = 1$$

A z Eulerovho vzťahu platí

$$e^{i\varphi} = \cos \varphi + i \sin \varphi$$

## 2.2.1 Operácie na množine komplexných čísel

### Súčet komplexných čísel

- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $\rho_1 e^{i\varphi_1} + \rho_2 e^{i\varphi_2} = \rho_1 (\cos \varphi_1 + i \sin \varphi_1) + \rho_2 (\cos \varphi_2 + i \sin \varphi_2) = (\rho_1 \cos \varphi_1 + \rho_2 \cos \varphi_2) + i(\rho_1 \sin \varphi_1 + \rho_2 \sin \varphi_2)$

### Násobenie komplexných čísel

- $(a + bi)(c + di) = ac + adi + bci - bd = (ac - bd) + (ad + bd)i$
- $\rho_1 e^{i\varphi_1} \cdot \rho_2 e^{i\varphi_2} = \rho_1 \rho_2 e^{i(\varphi_1 + \varphi_2)}$

Operácie rozdielu a podielu sú ľahko odvoditeľné obnorným spôsobom.

### 2.2.2 Základné charakteristiky komplexných čísel

Nech  $\alpha$  je komplexné číslo  $\alpha = a + bi, \alpha \in \mathbb{C}$ . Potom hovoríme, že  $a, b$  sú zložky komplexného čísla  $\alpha$ , pričom  $a$  je reálna a  $b$  je imaginárna zložka. Pri reprezenácii pomocou polárnych súradníc  $\alpha = \rho e^{i\varphi}$  je  $\rho$  nazývané amplitúda (veľkosť, norma) komplexného čísla a  $\varphi$  je fáza komplexného čísla.

Pre komplexné číslo  $\alpha \in \mathbb{C}$  je číslo  $\alpha^\dagger$  ( $\bar{\alpha}$  alebo  $\alpha^*$ ) nazývané združeným komplexným číslom (angl. conjugate of complex number) [3], pričom ak  $\alpha = a + bi$ , potom

$$\alpha^\dagger = a - bi,$$

$$\alpha^\dagger = \rho e^{-i\varphi}.$$

Z geometrickej reprezentácie komplexného čísla na Obr. 2.1 je zrejmé, že  $\rho = \sqrt{a^2 + b^2}$ . Bolo už spomenuté, že  $\rho$  sa nazýva aj norma komplexného čísla. Normu komplexného čísla  $\alpha$  možno označiť aj ako  $|\alpha|$  a platí

$$|\alpha| = \sqrt{\alpha^\dagger \alpha}.$$

Dôkaz:

$$|\alpha| = \sqrt{\alpha^\dagger \alpha} = \sqrt{\rho e^{-i\varphi} \cdot \rho e^{i\varphi}} = \sqrt{\rho^2} = \rho$$

## 2.3 Vektory

Vektor rozmeru  $n$  je usporiadaný súbor prvkov. Vo všeobecnosti je možné vektor  $A$  označiť ako

$$A = \begin{pmatrix} a_1 \\ a_2 \\ \dots \\ a_n \end{pmatrix}$$



No je žiadúce označovať vektory pomocou Diracovho (Bra-ket) zápisu. Čiže vektory  $u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$  a  $v = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$  je lepšie označiť ako

$$|\psi_1\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$$

$$|\psi_2\rangle = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

Toto označenie popisuje vektory v Hilbertovom priestore (viac v kapitole 3.1), pričom platí nasledovné:

Ak  $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$  je ket-vektor, potom

$$\langle\psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}^\dagger = (\alpha^\dagger \beta^\dagger)$$

je bra-vektor, kde  $(\alpha, \beta, \alpha^\dagger, \beta^\dagger \in \mathbb{C})$  a  $\alpha^\dagger, \beta^\dagger$  sú združené komplexné čísla ku  $\alpha$  a  $\beta$ .  $\langle\psi|$  je teda združenou transpozíciou (angl. transposed conjugate), a platí

$$\langle\psi^\dagger| = |\psi\rangle$$

$$|\psi^\dagger\rangle = \langle\psi|$$

## 2.4 Pojmi a definície

Vektor je **normalizovaný**, ak jeho norma (veľkosť) je rovná 1.

$$\left\| \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right\| = \sqrt{|\alpha|^2 + |\beta|^2} = 1$$

Vektory  $\psi_1$  a  $\psi_2$  sú navzájom **ortogonálne**, ak ich skalárny súčin je rovný 0. Ortogonálnosť (angl. orthogonality) je v tomto ponímaní teda možné zameniť s kolmosťou.

Dva vektory sú **ortonormálne**, ak sú zároveň ortogonálne a normalizované.

Pre príklad nech  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  a  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ,  $(|0\rangle, |1\rangle \in \mathbb{C}^2)$ . Tieto vektory sú ortonormálne, pretože platí

$$1. \langle 0 | 1 \rangle = \langle 0 | \cdot | 1 \rangle = |0^\dagger\rangle \cdot |1\rangle = (10) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0,$$

$$2. \| |0\rangle \|^2 = \langle 0 | 0 \rangle = (10) \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1$$

$$\| |1\rangle \|^2 = \langle 1 | 1 \rangle = (01) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1.$$

Pre skalárny súčin dvoch vektorov platí

$$\langle \psi_1 | \psi_2 \rangle = \langle \psi_1 | \cdot | \psi_2 \rangle = (\alpha_1^\dagger \beta_1^\dagger) \cdot \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \alpha_1^\dagger \alpha_2 + \beta_1^\dagger \beta_2.$$

**Normu** vektora  $|\psi\rangle$  pomocou skalárneho súčinu je možné vypočítať ako

$$\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle},$$

pretože platí  $\langle \psi | \psi \rangle = \alpha^\dagger \alpha + \beta^\dagger \beta = |\alpha|^2 + |\beta|^2 = \| |\psi\rangle \|^2$ .

Operácia **tenzorového súčinu** dvoch vektorov je definovaná ako

$$|\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle \cdot \langle \psi_2| = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \cdot (\alpha_2 \beta_2) = \begin{pmatrix} \alpha_1(\alpha_2 \beta_2) \\ \beta_1(\alpha_2 \beta_2) \end{pmatrix} = \begin{pmatrix} \alpha_1 \alpha_2 & \alpha_1 \beta_2 \\ \beta_1 \alpha_2 & \beta_1 \beta_2 \end{pmatrix}$$

## 3 Teoretické základy kvantových systémov

---

V nasledujúcej kapitole sú uvedené poznatky z teórie kvantových výpočtov a kvantových obvodov.

### 3.1 Základné definície

#### Hilbertov priestor

Hilbertov priestor (angl. Hilber space) je úplný konečnorozmerný vektorový priestor, v ktorom je definovaná operácia skalárneho súčinu  $\langle u | v \rangle$ , kde  $u, v$  sú  $N$ -rozmerné vektory s komplexnými zložkami [4]. Konečnorozmerným vektorovým priestorom nazývame taký priestor, ktorého báza je množina lineárne nezávislých vektorov, a ktorá generuje celý tento priestor. Pre úplný priestor platí, že existuje Cauchyho postupnosť, ktorou je dosiahnuteľný ľubovoľný stav, charakterizovateľný  $N$ -rozmerným vektorom  $|\psi\rangle \in \mathbb{C}^N$ , ktorý je vždy normalizovaný.

#### Unitárne zobrazenie

Unitárne zobrazenie (angl. Unitary map) je rotáciou, čiže zmenou ortonormálnej bázy.

#### Kvantový bit

Za kvantový bit je možné považovať objekt, ktorý popisuje stav kvantového systému. Z matematického pohľadu je to vektor v dvojrozmernom Hilbertovom priestore  $\mathbb{C}^2$ . No v reále ide o fotón. Budeme sa zaoberať dvojstavovými kvantovými systémami, kde je fotón nútený skolabovať do jedného z dvoch stavov. A teda vektor, ktorý bude popisovať tento kvantový bit vyjadríme ako

$u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ ,  $(\alpha, \beta \in \mathbb{C})$  a  $u \in \mathbb{C}^2$  [5]. No vhodnejším sa javí vyjadrenie tohto vektora superpozíciou, teda lineárnou kombináciou základných stavov  $|0\rangle, |1\rangle$ , ktoré zodpovedajú klasickým bitom 0, 1. Teda

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

kde monožina  $\{|0\rangle, |1\rangle\} = \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$  je nazývaná základná báza. Väčšinou je využívaná základná báza  $\{|0\rangle, |1\rangle\}$ , no je možné sa stretnúť aj s bázami  $\{|+\rangle, |-\rangle\}$  a  $\{|\odot\rangle, |\oslash\rangle\}$ . Tieto bázy sú dosiahnuteľné zo základnej bázy unitárnymi transformáciami.

### Superpozícia

Superpozíciou (angl. superposition) dvoch vektorov je vyjadrený stav kvantového bitu  $|\psi\rangle$ ,  $|\psi\rangle \in \mathbb{C}^2$ . Ide o lineárnu kombináciu a teda vo všeobecnosti tieto vektory môžu byť dva ľubovoľné, no lineárne nezávislé vektory  $u$  a  $v$ . Čiže

$$|\psi\rangle = \alpha u + \beta v.$$

Pre kvantové výpočty, ale má väčší význam využitie ortonormálnych vektorov.

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

$$|\psi\rangle = \alpha |+\rangle + \beta |-\rangle,$$

$$|\psi\rangle = \alpha |\odot\rangle + \beta |\oslash\rangle,$$

kde  $\alpha, \beta \in \mathbb{C}$  a platí  $|\alpha|^2 + |\beta|^2 = 1$ .

### Previazanosť kvantových bitov

(Quantum Computation and Quantum Information) Majme stav dvoch qbitov

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Pre tento stav neexistuje taká dvojica stavov  $|a\rangle$  a  $|b\rangle$ , že platí  $|\psi\rangle = |a\rangle |b\rangle$ . Hovoríme, že stav zloženého systému, ktorý nemožno zapísať ako súčin stavov jeho komponentov sa nazýva previazaným (angl. entangled) stavom.

V prípade jednoduchého  $n$ -bitového kvantového systému môžeme jeho celkový stav  $|\psi\rangle$  vyjadriť tenzorovým súčinom vektorov stavov jednotlivých bitov  $|\psi_0\rangle, |\psi_1\rangle, \dots, |\psi_{n-1}\rangle$ . Čiže

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes \dots \otimes |\psi_{n-1}\rangle$$

Toto však neplatí, ak dva alebo viac kvantových bitov je navzájom previazaných. Pretože previazané bity sú charakteristické rovnakými vektormi, a to počas celého výpočtu a aj pri meraní.

### 3.2 Systém s jedným kvantovým bitom

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

kde  $\alpha, \beta \in \mathbb{C}$  a  $|\psi\rangle \in \mathbb{C}^2$ . Čiže stav kvantového systému  $|\psi\rangle$  je superpozíciou stavov  $|0\rangle$  a  $|1\rangle$ .

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

$$\langle\psi| = (\alpha^\dagger \beta^\dagger)$$

$$\langle\psi|\psi\rangle = (\alpha^\dagger \beta^\dagger) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha^\dagger \alpha + \beta^\dagger \beta = |\alpha|^2 + |\beta|^2 = ||\psi\rangle||^2$$

### 3.3 System s viacerymi kvantovymi bitmy

### 3.4 Princíp merania

## 4 Kvantovy system

---

### 4.1 IBM QX

#### 4.1.1 Stavy a ich zapis

#### 4.1.2 Operacie kvantovych hradiel

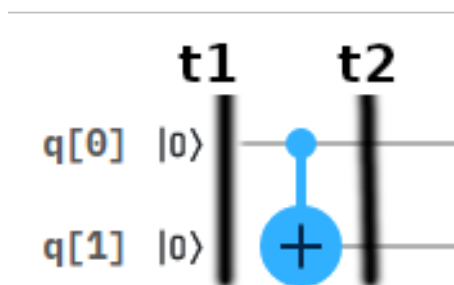
## 5 Pravdepodobnostná analýza kvantových obvodov

---

V predošlých kapitolách bola vysvetlená problematika kvantových obvodov. Našou úlohou je merať stavy kvantových bitov v rôznych časových okamihoch. Je možné zostrojiť nekonečné množstvo rôznych kvantových obvodov, a preto v tejto kapitole priblížime spôsob tohto merania. Vo všeobecnosti môžeme rozdeliť kvantové obvody na dva druhy, v ktorých meranie má iný charakter. Sú to obvody s nepreviazanými bitmi a obvody s previazanými kvantovými bitmi.

### 5.1 Analýza nepreviazaných stavov

Na obrázku 7.2 je vygenerovaný jednoduchý kvantový obvod pomocou nástroja IBM Quantum Experience. Označili sme dva časové úseky  $t_1$  a  $t_2$ . V tomto obvode sú dva kvantové bity, ktoré prechádzajú hradlom CNOT. Pre zachovanie notácie budeme ďalej označovať tieto bity ako  $\psi_0$  a  $\psi_1$ . Z kvantového obvodu je zrejmé, že v čase  $t_1$  sú oba kvantové bity v stave  $|0\rangle$ , to ale nebudeme brať v úvahu. Zaujímá



Obr. 5.1: Jednoduchý kvantový obvod (namodelovaný v IBM Quantum Experience)

nás pravdepodobnosť namerania stavov  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  a  $|11\rangle$ .

Vieme, že platí  $|\psi_0\rangle = \begin{pmatrix} \alpha_0 \\ \beta_0 \end{pmatrix}$  a  $|\psi_1\rangle = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix}$ , a teda pre celkový stav  $\psi$  platí

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle = \begin{pmatrix} \alpha_0 \\ \beta_0 \end{pmatrix} \otimes \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\alpha_1 \\ \alpha_0\beta_1 \\ \beta_0\alpha_1 \\ \beta_0\beta_1 \end{pmatrix}$$

Z toho vyplíva, že celkový stav  $|\psi\rangle$  v čase  $t_1$  nadobúda hodnoty

$|00\rangle$  s pravdepodobnosťou  $\|\alpha_0\alpha_1\|^2$

$|01\rangle$  s pravdepodobnosťou  $\|\alpha_0\beta_1\|^2$

$|10\rangle$  s pravdepodobnosťou  $\|\beta_0\alpha_1\|^2$

$|11\rangle$  s pravdepodobnosťou  $\|\beta_0\beta_1\|^2$

Toto tvrdenie platí, pretože platí  $|\psi_0\rangle = \alpha_0|0\rangle + \beta_0|1\rangle$ , čiže  $|\alpha_0|^2 + |\beta_0|^2 = 1$ , z čoho vyplíva, že

$|\psi_0\rangle$  nadobúda hodnotu 0 s pravdepodobnosťou  $|\alpha_0|^2$  a

$|\psi_0\rangle$  nadobúda hodnotu 1 s pravdepodobnosťou  $|\beta_0|^2$ .

Obdobne to platí aj pre  $|\psi_1\rangle$ . K rovnakému záveru sa dopracujeme aj pomocou

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) =$$

$$\alpha_0\alpha_1(|0\rangle \otimes |0\rangle) + \alpha_0\beta_1(|0\rangle \otimes |1\rangle) + \beta_0\alpha_1(|1\rangle \otimes |0\rangle) + \beta_0\beta_1(|1\rangle \otimes |1\rangle)$$

, čo by sme mohli vyjadriť aj iným zápisom ako  $\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ , pričom súčet noriem musí byť rovný 1.

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

## 5.2 Analýza previazaných stavov

Pri meraní stavov v čase  $t_2$ , už nemožno dostať výsledný stav  $\psi$  priamim využitím tenzorového súčinu. Pri prechode hradom CNOT môžu nastať dve situácie:



1. Kvantový bit  $\psi_0$ , ktorý je kontrolným bitom, je v stave  $|1\rangle$  a teda nastane preklopenie bitu  $\psi_1$ , čo je cieľovým bitom, pomocou hradla X,
2. Kvantový bit  $\psi_0$  nie je v stave  $|1\rangle$  a teda bit  $\psi_1$  pokračuje bez zmeny.

Z toho je jasné, že v kažom prípade sa stav  $|\psi_0\rangle$  nemení no stav  $|\psi_1\rangle$  nadobúda hodnotu:

- $|\psi_1\rangle$  s pravdepodobnosťou  $|\alpha_0|^2$ ,
- $X|\psi_1\rangle$  s pravdepodobnosťou  $|\beta_0|^2$ .

Berme v úvahu to, že v príklade sme využili hradlo CNOT. Pri pohľade na viac-bitový systém s využitím hradla CCNOT, kde máme viacero kontrolných bitov, zisťujeme, že odvodzovanie je netriviálne a tento problém je nutné riešiť pomocou pravdepodobnostného rozhodovacieho stromu (o tom v ďalších kapitolách).

## 6 Meranie kvantových obvodov

---

Jediným spôsobom ako zistiť skutočný stav kvantového obvodu je meraním. Merať možno všetky bity súčasne ako aj jednotlivé kvantové bity samostatne.

### 6.1 Princíp merania kvantových obvodov

Kvantový bit môže existovať v nekonečnom množstve stavov. Meranie si môžeme predstaviť ako prevod stavov kvantových bitov do stavu klasického digitálneho systému [4]. Pre príklad môžeme reprezentovať kvantový stav  $\alpha|0\rangle + \beta|1\rangle$  pomocou nulového a excitovaného stavu atómu. Skutočný kvantový počítač by tak mohol merať tieto stavy. Pri meraní by daný atóm skolaboval do jedného zo stavov  $|0\rangle$  alebo  $|1\rangle$ . Pre skolabovanie samozrejme rovnako platí to, že do jednotlivých stavov by sa atóm dostal s pravdepodobnosťami  $|\alpha|^2$  respektíve  $|\beta|^2$ .

Pri každom fyzikálnom meraní nastáva určitá nepresnosť merania. Takisto pri meraní môže dokonca nastať zničenie obvodu. To vyplíva z toho, že pri skolabovanom kvantovom bite nastáva zmena fyzikálnych vlastností daného bitu.

### 6.2 Fiktívne meranie

Naším cieľom je navrhnúť pravdepodobnostný model, ktorý by umožnil merať stavy kvantových obvodov aj bez skolabovania jednotlivých kvantových bitov.

#### 6.2.1 Experiment 1

#### 6.2.2 Experiment 2

#### 6.2.3 Experiment 3

## 7 Pravdepodobnostný model kvantového výpočtu - návrh a realizácia

---

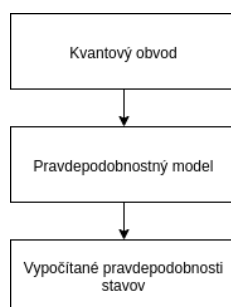
Cieľom je vytvoriť v jazyku Haskell model, ktorý by dokázal merať stavy kvantových bitov aj bez ich kolabovania. Na rozdiel od IBM Quantum Experience tento model môže realizovať unitárne operácie aj paralelne.

Pri pohľade na jednoduchý konceptuálny model (obrázok 7.1) je zrejmé čo cheme dosiahnuť. Na vstupe je očakávaný kvantový obvod. Samotný program prebehne týmto obvodom ako interpreter a zároveň pomerá stavy na daných miestach v obvode. Nakoniec vypíše výstup v zrozumiteľnej podobe.

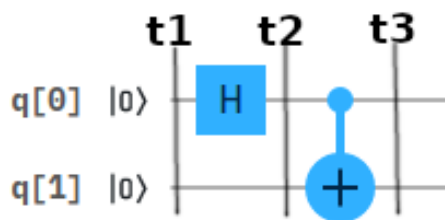
### 7.1 Definícia vstupu

Celý kvantový obvod je možné rozdeliť do vertikálnych blokov alebo levelov. Každý level obsahuje hradlá, ktorých počet je maximálne rovný počtu kvantových bitov, s ktorými daný obvod pracuje. Ak v danom levely nechceme aplikovať žiadnu operáciu nad bitom, môžeme definovať prázdny element.

Čiže kvantový obvod môžeme definovať ako list levelov, pričom level je datová



Obr. 7.1: Konceptuálny návrh programu



Obr. 7.2: Kvantový obvod s previazanými kvantovými bitmi.

štruktúra, ktorá obsahuje list hradiel. Okrem hradiel každý level bude obsahovať prepínač, ktorý signalizuje či má nastať meranie po aktivácii hradiel v leveli.

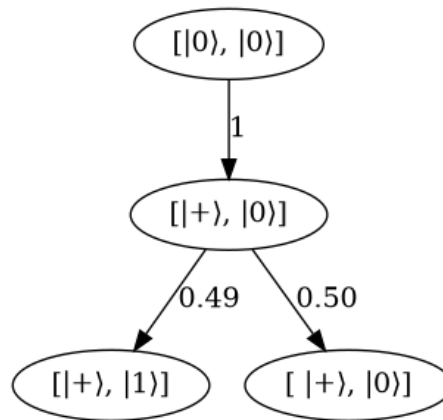
## 7.2 Pravdepodobnostný model

Pravdepodobnostný model možno vo funkčnosti prirovnať k interpretu kvantového obvodu. Tak ako bolo spomenuté v Pravdepodobnostnej analýze (kapitola 5) je nutné brať v úvahu previazané a nepreviazané kvantové bity. Previazanie je možné dosiahnuť hradlom CNOT (respektíve  $C^n$ NOT). Naším cieľom nie je vytvoriť dokonalý interpret, z tohto dôvodu budeme využívať zjednodušenú verziu týchto hradiel. Čo znamená, že ak kontrolné bity sú v stave  $|1\rangle$  tak cieľový kvantový bit bude preklopený hradlom  $X$ . V inom prípade nenastane zmena v stavoch.

Pravdepodobnostný model si uchováva stavy všetkých kvantových bitov v stromovej štruktúre. Pri prechode levelom si uloží nové stavy do listov tohto stromu. Ak sa v leveli nachádzajú len obvyklé hradlá, vzniká len jediný nový list. Rozdiel nastáva pri prechode hradlom CNOT. Je zrejmé, že toto hradlo musí rozvetvovať stromovú štruktúru na dva podstromy. Každý z podstromov je označený pravdepodobnosťou, s akou môže nastať daná zmena stavov.

Pri meraní (fiktívnom meraní) sa spočítajú pravdepodobnosti všetkých listov stromu a výsledky sa uložia do listu. Pre lepšie pochopenie funkčnosti programu opíšeme príklad. Majme kvantový obvod, ktorý je definovaný na obrázku 7.2. Na vstupe máme dva kvantové bity v stavoch  $|0\rangle$ . Definujme všetky potrebné datové štruktúry v jazyku Haskell.

```
l1 = Level [E, E] True
l2 = Level [H, E] True
l3 = Level [Cc, Ct] True
```



Obr. 7.3: Strom stavov (StateTree) po vykonaní kvantového obvodu.

```

c = [l1, l2, l3]
st = StateTree 1 [q0, q0] []
rt = RT st []
  
```

Chceme merať v troch časových okamihoch, čo dosiahneme definovaním levelov l1, l2 a l3. Každý level je označený na meranie pomocou True a využité hradlá sú nasledovné:

- E - prázdne
- H - Hadamardovo hradlo
- Cc - Kontrólly bit (angl. control bit) hradla CNOT
- Ct - Cieľový bit (angl. target bit) hradla CNOT

Pre ďalšie spracovanie spojíme levely do jedného obvodu *c*. Na ukladanie stavov slúži stromová štruktúra StateTree. Jej definovaním hovoríme, že počiatočné stavy sú q0, čo je označenie pre stav  $|0\rangle$ . Pravdepodobnosť dosiahnutia týchto stavov je 1 a zatiaľ neexistujú žiadne podstromy. Štruktúra RT slúži na ukadanie výsledkov meraní. Spustením pravdepodobnostného modelu dostaneme výslednú tabuľku typu RT.

```

processRT = processCircuit c rt
  
```

To ako sa menili stavy kvantových bitov môžeme vidieť na obrázku 7.3. Je zrejmé, že využitím operácie Hadarmardovho hradla nenastane vetvenie stromu

stavov. To isé ale už neplatí pre hradlo CNOT. Nakoľko stav kontrolného bitu  $|+\rangle$  má 50%-tnú šancu skolabovať do stavu  $|0\rangle$  ako aj do stavu  $|1\rangle$ , tak je prirodzené, že strom stavov sa rozvetví a každý podstrom má pravdepodobnosť dosiahnutia približne 0.5.

Pri výpočte výsledkov je nutné započítať nie len pravdepodobnosti kolabovania výsledných stavov ale aj pravdepodobnosti dosiahnutia podstromov, v ktorých sa dané stavy kvantových bitov nachádzajú. Meriame pravdepodobnosti kolabovania bitov do stavov  $|0\rangle$  a  $|1\rangle$ . Ide o dva stavy takže počet kombinácií výsledkov je  $2^n$ , kde  $n$  je počet kvantových bitov v obvode. Teda pre dva bity možné kombinácie sú  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  a  $|11\rangle$ . Vypočítajme výsledky pre level l3, čiže vychádzame z listov finálneho stromu stavov. Pre prvý list pravdepodobnosť dosiahnutia stavu:

- $|00\rangle$  je  $|\alpha_0\alpha_1|^2 = \left|\left(\frac{1}{\sqrt{2}}\right) \times 0\right|^2 = 0$
- $|01\rangle$  je  $|\alpha_0\beta_1|^2 = \left|\left(\frac{1}{\sqrt{2}}\right) \times 1\right|^2 = 0.5$
- $|10\rangle$  je  $|\beta_0\alpha_1|^2 = \left|\left(\frac{1}{\sqrt{2}}\right) \times 0\right|^2 = 0$
- $|11\rangle$  je  $|\beta_0\beta_1|^2 = \left|\left(\frac{1}{\sqrt{2}}\right) \times 1\right|^2 = 0.5$

Pre druhý list obdobne platí to isté. Samozrejme treba započítať aj pravdepodobnosť vykonania podstromu. Čiže všetky tieto pravdepodobnosti kolabovania je nutné vynásobiť príslušnými hodnotami. Teda dostávame výsledky:

- $|00\rangle$  dosiahneme s pravdepodobnosťou 0.25
- $|01\rangle$  dosiahneme s pravdepodobnosťou 0.25
- $|10\rangle$  dosiahneme s pravdepodobnosťou 0.25
- $|11\rangle$  dosiahneme s pravdepodobnosťou 0.25

## 8 Kvantová teleportácia

---

## 9 Celkové vyhodnotenie

---



## 10 Závěr

---

# Literatúra

---

- [1] Lieven Vandenberghe Stephen Boyd. *Introduction to Applied Linear Algebra*. Cambridge University Press, 2018.
- [2] Alexander Graham. *Kronecker Products and Matrix Calculus with Applications*. Ellis Horwood limited, 1981.
- [3] Dorin Andrica Titu Andreescu. *Complex Numbers from A to...Z*. Birkhäuser, 2006.
- [4] Issac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.
- [5] Michele Mosca Phillip Kaye Raymond LaFlamme. *An Introduction to Quantum Computing*. Oxford University Press, 2007.