Technicka Univerzita v Kosiciach
Fakulta elektrotechniky a informatiky

Meranie a interakcia kvantových obvodov

Diplomová práca

2020 **Marián Sabat**

Technicka 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, Technicka Univerzita v Kosiciach
Autor:	Marián Sabat
Školiteľ:	prof. Ing. Ján Kollár, CSc.
Konzultant:	
Dátum:	1. 1. 2020
Kľúčové slová:	Kvantove pocitace a ine klucove slova
Abstrakt:	ABSTRAKT

Thesis title:	Measurement and interaction of quantum circutis
Department:	Department of Computers and Informatics, Techincal University of Kosice
Author:	Marián Sabat
Supervisor:	prof. Ing. Ján Kollár, CSc.
Tutor:	
Date:	1. 1. 2020
Keywords:	Quantum comuters and other key words
Abstract:	ABSTRAKT

Tu vložte zadávací list pomocou príkazu
`\thesisspec{cesta/k/suboru/so/zadavacim.listom}`
v preambule dokumentu.

Čestné vyhlásenie

Vyhlasujem, ze vsetko som pisal sam ...

Košice, 1.1.2020 . . . .

Vlastnoručný podpis

Poďakovanie

Obsah

Zoznam obrázkov

Zoznam tabuliek

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 nástrojv, 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. Aj ten najjednoduchší program je nutné zložito vytvárať pomocou internetových nástrojov, nehovoriac o prístupe k reálnemu stroju.

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. Našim cieľom je navrhnúť simulátor tak, aby bolo prirodzene jednoduché zistiť v akom stave sa kvantový systém nachádza.

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 javoch, 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 progamu 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 opýsaný 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 2×2 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 α, β 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

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

kde $i = 1, \ldots, m$, a $j = 1, \ldots, p$ [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]

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

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

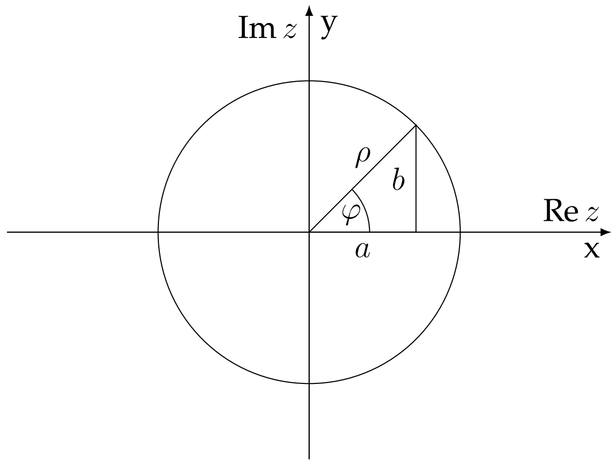
2.2 Komplexné čísla

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 - imagináran os

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

Je zrejme, 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 $\rho > 1$. $e^{i\varphi}$ je komplexná jednotka, inak povedané jej absolútna hodnota je rová 1.

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

A z Eulerovho vzťahu platí

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

2.2.1 Operácie na množine komplexých 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

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

Operácie rozdielu a podielu sú ľahko odvoditeľné obnomným spôsobom.

2.2.2 Základné charakteristiky komplexných čísel

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

Pre komplexné číslo $\alpha \in \mathbb{C}$ je číslo $\alpha^\dagger$ ($\overline{\alpha}$ alebo α^*) 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 ρ sa nazýva aj norma komplexného čísla. Normu komplexného čísla α možno označiť aj ako $|\alpha|$ a platí

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

Dôkaz:

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

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 $u = \binom{\alpha}{\beta}$ a $v = \binom{\gamma}{\delta}$ 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 priesotre (viac v kapitole 3.1), pričom platí nasledovné:

Ak $|\psi\rangle = \binom{\alpha}{\beta}$ 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 α a β. $\langle\psi|$ je teda združenou transpozíciou (angl. transposed conjugate), a platí

$$\left\langle\psi^{\dagger}\right| = |\psi\rangle$$

$$\left|\psi^{\dagger}\right\rangle = \langle\psi|$$

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 ψ_1 a ψ_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 $|0\rangle = \binom{1}{0}$ a $|1\rangle = \binom{0}{1}$, $(|0\rangle, |1\rangle \in \mathbb{C}^2)$. Tieto vektory sú ortonormálne, pretože platí

1. $\langle 0 \,|\, 1\rangle = \langle 0| \,.\, |1\rangle = \left|0^{\dagger}\right\rangle . \,|1\rangle = (10).\binom{0}{1} = 0,$

2. $\|\, |0\rangle \,\|^2 = \langle 0 \,|\, 0\rangle = (10).\binom{1}{0} = 1$
   $\|\, |1\rangle \,\|^2 = \langle 1 \,|\, 1\rangle = (01).\binom{0}{1} = 1.$

Pre **skalárny súčin** dvoch vektorov platí

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

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

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

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 $\langle u \mid v \rangle$, 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 normalizovaý.

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 Hilberovom priesotre $\mathbb{C}^2$. 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

$u = \binom{\alpha}{\beta}$, $(\alpha, \beta \in \mathbb{C})$ 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 zodpovedajé 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 $\{|0\rangle\,, |1\rangle\} = \{\binom{1}{0}, \binom{0}{1}\}$ je nazývaná základná báza. Väčšinou je využívaná základná báza $\{|0\rangle\,, |1\rangle\}$, no je možné sa stretnúť aj s bázami $\{|+\rangle\,, |-\rangle\}$ a $\{|\circlearrowright\rangle\,, |\circlearrowleft\rangle\}$. 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.

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

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

$$|\psi\rangle = \alpha\,|\circlearrowright\rangle + \beta\,|\circlearrowleft\rangle\,,$$

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. entagled) stavom.

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

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

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

Majme kvantový systém, ktorý obsahuje jediný kvantový bit. Označme ho ψ a platí

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

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 $|1\rangle$.

Používame Bra-ket zápis, ktorý bol vysvetlený v časti Vektory 2.3. Čiže platí to isté ako pre vektory

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

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

a teda normu tohto kvantového bit možno odvodiť zo

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

a samozreme platí

$$|\alpha|^2 + |\beta|^2 < 1$$

3.3 Systém s viacerými kvantovými bitmi

Majme kvantový systém, ktorý je zložený z troch nepreviazaných kvantových bitov. Označme ich ψ_1, ψ_2 a ψ_3 . Platí

$$\psi_1 = \alpha_1\,|0\rangle + \beta_1\,|1\rangle$$

$$\psi_2 = \alpha_2\,|0\rangle + \beta_2\,|1\rangle$$

$$\psi_3 = \alpha_3\,|0\rangle + \beta_3\,|1\rangle$$

Stav tohto systém možno odvodiť ako

$$\psi = |\psi_1\psi_2\psi_3\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} \otimes \begin{pmatrix}\alpha_3\\ \beta_3\end{pmatrix}$$

, a to sa rovná

$$\begin{pmatrix} \alpha_1\alpha_2\alpha_3 \\ \alpha_1\alpha_2\beta_3 \\ \alpha_1\beta_2\alpha_3 \\ \alpha_1\beta_2\beta_3 \\ \beta_1\alpha_2\alpha_3 \\ \beta_1\alpha_2\beta_3 \\ \beta_1\beta_2\alpha_3 \\ \beta_1\beta_2\beta_3 \end{pmatrix}$$

3.4 Princíp merania

Pre príklad nám poslúži jednoduchý obvod s tromi nepreviazanými kvantovými bitmi ψ_1, ψ_2 a ψ_3. Každý s týchto bitov môže kolabovať do jedného z dvoch stavov. A to $|0\rangle$ a $|1\rangle$ ($\binom{1}{0}$ a $\binom{1}{0}$). Platí

$$|\alpha_1\alpha_2\alpha_3|^2 + |\alpha_1\alpha_2\beta_3|^2 + \cdots + |\beta_1\beta_2\beta_3|^2 = 1$$

Povedzme, že bit ψ_1 skolabuje. Pravdepodobnosť s akou skolabuje do stavu $\binom{1}{0}$ vypočítame ako $|\alpha_1|^2$. Pravdepodobnosť s akou skolabuje do stavu $\binom{0}{1}$ vypočítame ako $|\beta_1|^2$. Bez ohľadu na to, aký stav tento kvantový bit nadobudne, pre kvantový systém bude platiť

$$|\alpha_2\alpha_3|^2 + |\alpha_2\beta_2|^2 + |\beta_2\alpha_3|^2 + |\beta_2\beta_3|^2 = 1$$

Ak bit ψ_1 kolabuje do $|0\rangle$ tak sa systém bude nachádzať v tomto stave

$$\begin{pmatrix} \alpha_2\alpha_3 & \alpha_2\beta_3 & \beta_2\alpha_3 & \beta_2\beta_3 & 0 & 0 & 0 & 0 \end{pmatrix}^T$$

obdobne, ak naodbudne druhý stav

$$\begin{pmatrix} 0 & 0 & 0 & 0 & \alpha_2\alpha_3 & \alpha_2\beta_3 & \beta_2\alpha_3 & \beta_2\beta_3 \end{pmatrix}^T$$

4 Kvantovy system

Stupeň vývoja kvantových počítačov nateraz neumožnuje priamy prístup k fyzickému stroju. Tieto prototypy sú veľmi veľké a prísne strážené v laboratóriách. Našťastie existujú nástroje, ktorými je umožnená práca aj obyčajným ľuďom. Jedným z najpoužívanejším nástrojom je IBM Quantum Experience.

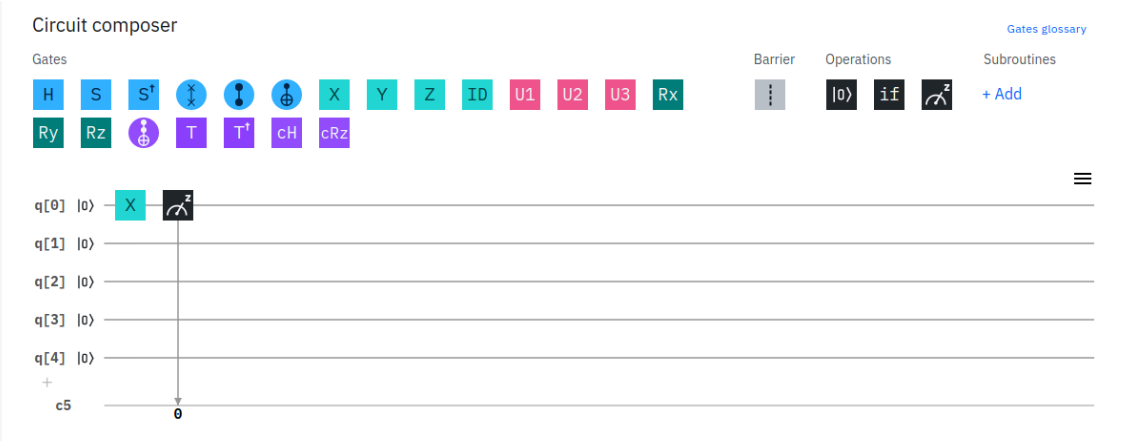
4.1 IBM Quantum Experience

IBM Quantum Experience (ďalej len IBM QX) je webová aplikácia, ktorá slúži na experimentovanie s kvantovým počítačom. Medzi jej funkcionality možno zahrnúť vytváranie a ukladanie kvantových obvodov ako aj ich vykonávanie na kvantovom počítači. Tento počítač je symulovaný virtuálny stroj, no IBM QX umožnuje aj odoslanie experimentu na reálny počítač. Symulátor umožnuje relatívne rýchlu prácu s kvantovým počítačom. Tento prístup odľachčuje skutočný systém od veľkej sieťovej premávky a takisto zlepšuje používateľský zážitok.

Vytáranie nového obvodu je veľmi intuitívne. Na obrázku 4.1 je nástroj na to určený. Prednastavené hradlá je spôsobom ťahaj a pusť (angl. drag and drop) možné presúvať na plán kvantového obvodu. Po uložení je možné spustiť tento program. Na server sa odošle experiment, za predpokladu, že je obvod spúšťaný na simulátore, tak za krátku dobu sú vrátené výsledky.

Obvody je možné navrhovať aj pomocou špeciálneho jazyka OpenQASM, pomocou editora, ktroý IBM QX obsahuje. Pri zobrazovaní výsledkov sa stav systému označuje pomocou klasických bitov. Teda pri navrhovaní programu pomocou OpenQASM, je nutné definovať jednak počet kvantových a súčasne aj počet klasických bitov v systéme.

```
qreg q[5];
creg c[5];
```



Obr. 4.1: Nástroj na tvorbu kvantových obvodov v IBM Quatnum Experience.

Je nutné podotknúť, že kvantový bit ψ_0 je v IBM QX reprezentovaný ako $q[0]$, $psi_1 = q[1]$ a tak ďalej. Pri meraní sa tieto bity zobrazia do príslušných c registrov:

$q[0] \rightarrow c[0]$

$q[1] \rightarrow c[1]$

$\ldots$

Po inicializácií potrebných registrov je možné pristúpiť k definovaniu samotného obvodu. Pre dosiahnutie obvodu ako na obrázku 4.1 vyvoláme aplikáciu hradla X na bite $q[0]$ a následne využijeme meranie.

```
x q[5];
measure q[0] -> c[0];
```

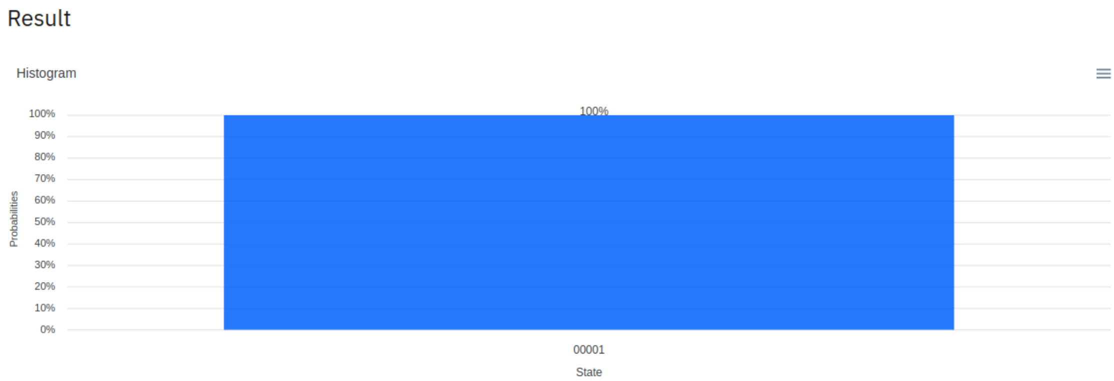
Výsledky experimentov sa zobrazujú v stĺpcovom diagrame. Pričom stav systému je zobrazovaný v klasických bitoch opačne ako v kvantových. Teda stav n-bitového systému $\psi = |\psi_0\psi_1\psi_2 \ldots \psi_{n-1}\rangle$ je meraný do klasického registra ako

$$c_{n-1} \ldots c_2c_1c_0$$

V našom prípade je

$$q[0] = X\,|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

, čo je 1 s pravdepodobnosťou 1. Teda výsledok na obrázku 4.2 zobrazuje, že kvantový systém dosiahne so 100% pravdepodobnosťou stav 00001.



Obr. 4.2: Výsledky exprimentu z IBM Quantum Experience.

4.1.1 Stavy a ich zápis

Pri výpočtoch je najviac využívaných týchto šesť stavov kvantových bitov:

$$|0\rangle = \binom{1}{0}$$

$$|1\rangle = \binom{0}{1}$$

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

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

$$|\circlearrowright\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

$$|\circlearrowleft\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$$

Zmena stavu kvantového bitu je možná pomocou hradiel. Existuje viacero hradiel, ktoré možno používať v kvantových systémoch. Aplikovaním hardiel na rôznych stavoch dosiahneme rôznu zmenu. Prehľad aplikácií základných hradiel je v tabuľke 4.1.

		$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$	$\lvert \circlearrowright\rangle$	$\lvert \circlearrowleft\rangle$
		$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$
X	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}i\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-i\\1\end{pmatrix}$
Y	$\begin{pmatrix}0 & -i\\i & 0\end{pmatrix}$	$\begin{pmatrix}0\\i\end{pmatrix}$	$\begin{pmatrix}-i\\0\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-i\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}i\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}-1\\i\end{pmatrix}$
Z	$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\-1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$
H	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}\frac{1+i}{\sqrt{2}}\\\frac{1-i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}\frac{1-i}{\sqrt{2}}\\\frac{1+i}{\sqrt{2}}\end{pmatrix}$
S	$\begin{pmatrix}1 & 0\\0 & i\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$
$S^\dagger$	$\begin{pmatrix}1 & 0\\0 & -i\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\-i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$
T	$\begin{pmatrix}1 & 0\\0 & \frac{1+i}{\sqrt{2}}\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\\frac{1+i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{1+i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{-1-i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{-1+i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{1-i}{\sqrt{2}}\end{pmatrix}$
$T^\dagger$	$\begin{pmatrix}1 & 0\\0 & \frac{1-i}{\sqrt{2}}\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\\frac{1-i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{1-i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{-1+i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{1+i}{\sqrt{2}}\end{pmatrix}$	$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\\frac{-1-i}{\sqrt{2}}\end{pmatrix}$

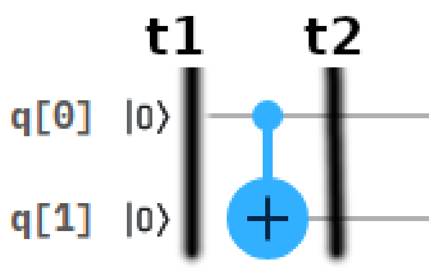
Tabuľka 4.1: Tabuľka stavov kvantových bitov a výsledky aplikácií hradiel na tieto stavy.

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 môžme rozdeliť kvantové obvody na dva druhy, v ktorých meranie má iný charakter. Sú to obvody s nepreviazanými bitmi a obvody s previazanými kvantovými bitmi. Totižto pri nepreviazaných bitoch, ako už vychádza z názvu, nedochádza k ovplivňovaniu stavu bitu inými kvantovými bitmi. A naopak ak sú jednotlivé bity previazané, ich stav silno závisí od stavu ostatných bitov.

5.1 Analýza nepreviazaných stavov

Na obrázku 7.2 je vygenerovaný jednoduchý kvantový obvod pomocou nástroja IBM Quantum Experience. V jazyku OpenQASM je možné definovať tento obvod ako:



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

```
qreg q[2];
creg c[2];

cx q[0],q[1];
```

V tomto obvode sú dva kvantové bity, ktoré prechádzajú hradlom CNOT. Pre zachovanie notácie budeme ďalej označovať tieto bity ako ψ_0 a ψ_1. Označili sme dva časové úseky t_1 a t_2. t_1 označuje čas na začiatku programu a t_2 je časový okamich, v ktorom prebehla aktivácia hradla CNOT. Z kvantového obvodu je zrejmé, že v čase t_1 sú oba kvantové bity v stave $|0\rangle$. Tento fakt ale nie je pre nás zaujímavý. Pozrieme sa na meranie pravdepodobnosti dosiahnutia namerania stavov $|00\rangle, |01\rangle, |10\rangle$ a $|11\rangle$.

Vieme, že platí $|\psi_0\rangle = \binom{\alpha_0}{\beta_0}$ a $|\psi_1\rangle = \binom{\alpha_1}{\beta_1}$, a teda pre celkový stav ψ 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 hodontu 0 s pravdepodobnosťou $|\alpha_0|^2$ a

$|\psi_0\rangle$ nadobúda hodontu 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 $\alpha_{00}\left|00\right\rangle+\alpha_{01}\left|01\right\rangle+\alpha_{10}\left|10\right\rangle+\alpha_{11}\left|11\right\rangle$, 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 ψ priamim využitím tenzorového súčinu. Pri prechode hradom CNOT môžu nastať dve situácie:

1. Kvantový bit ψ_0, ktorý je kontrólnym bitom, je v stave $\left|1\right\rangle$ a teda nastane preklopenie bitu ψ_1, čo je cieľoým bitom, pomocou hradla X,
2. Kvantový bit ψ_0 nie je v stave $\left|1\right\rangle$ a teda bit ψ_1 pokračuje bez zmeny.

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

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

A teda s pravdepodobnosťou $|\alpha_0|^2$ systém skončí v stave

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

a s pravdepodobnosťou $|\beta_0|^2$ dosiahne stav

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

Po zarátaní oboch možností dostávame, že celkový stav $\left|\psi\right\rangle$ v čase t_2 nadobúda hodnoty

$\left|00\right\rangle$ s pravdepodobnosťou $(|\alpha_0\alpha_1|^2 \times |\alpha_0|^2) + (|\alpha_0\beta_1|^2 \times |\beta_0|^2)$

$\left|01\right\rangle$ s pravdepodobnosťou $(|\alpha_0\beta_1|^2 \times |\alpha_0|^2) + (|\alpha_0\alpha_1|^2 \times |\beta_0|^2)$

$\left|10\right\rangle$ s pravdepodobnosťou $(|\beta_0\alpha_1|^2 \times |\alpha_0|^2) + (|\beta_0\beta_1|^2 \times |\beta_0|^2)$

$\left|11\right\rangle$ s pravdepodobnosťou $(|\beta_0\beta_1|^2 \times |\alpha_0|^2) + (|\beta_0\alpha_1|^2 \times |\beta_0|^2)$

Berme v úvahu to, že v príklade sme využili hradlo $CNOT$. Je samozrejmé, že v obvode môže dôjsť k previazaniu viacerých bitov na rôznych miestach. Takisto je možné vo viacbitovom systéme využiť haradl $CCNOT$ resp. C^nNOT, kde máme viacero kontrólnych bitov a cieľový bit sa preklápa za predpokladu, že všetky kontrólne bity majú stav $|1\rangle$. 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 kvnatového 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 môžme 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 kolabovanie 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 fizykálnych vlastností daného bitu.

6.2 Fiktívne meranie

Našim cieľom je navrhnúť pravdepodobnostný model, ktorý by umožnil merať stavy kvantových obvodov aj bez kolabovania 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

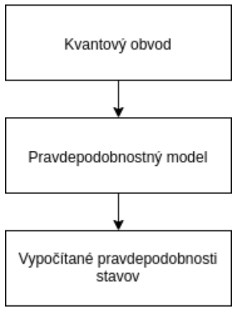
Cieľom je vytvoriť v jazyku Haskell model, ktorý by dokázal merať stavy kvantových bitov aj bez ich kolabovania. Na rozdiel od IBM Quantum Experience tento model môže realizovať unitárne operácie aj paralelne.

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

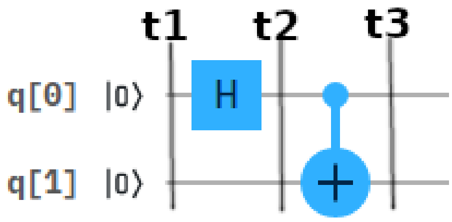
7.1 Definícia vstupu

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, môžme 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 siganlizuje či má nastať meranie po aktivácií hradiel v leveli.

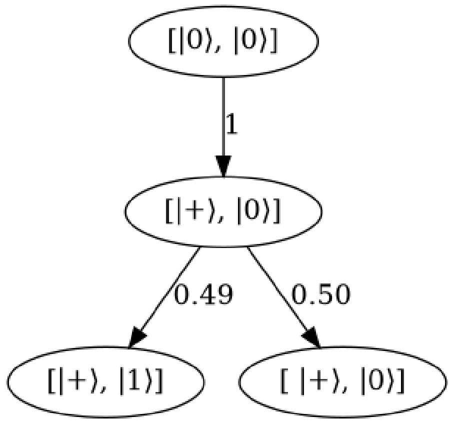
7.2 Pravdepodobnostný model

Pravdepodobnostný model možno vo funkčnosti prirovnať k interpreteru kvatového 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^nNOT). Našim cieľom nie je vytovoriť dokonalý interpreter, z tohto dôvodu budeme využívať zjednodušené verzie týchto hradiel. Čo znamená, že ak kontrólne bity sú v stave $|1\rangle$ tak cieľový kvantový bit bude preklopený hradom X. V inom prípade nenastane zmena v stavoch.

Pravdepodbnostný model si uchováva stavy všetkých kvantových bitova v stromovej štruktúre. Pri prechode levelom si uloží nové stavy do listov tohto stromu. Ak sa v leveli nachádzajú len običajné hradlá, vzniká len jediný nový list. Rozdiel nastáva pri prechode hradlom CNOT. Je zrejmé, že toto hradlo musí rozvetvovať stromovú štruktúru na dva podstromi. Každý z podstromov je označený pradvdepodobnosťou, 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 - Kontrólny 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 podstromi. 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 kontrólneho 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 pravdepodobonsť dosihuntia 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 $|\alpha_0\alpha_1|^2 = |\left(\frac{1}{\sqrt{2}}\right) \times 0|^2 = 0$
- $|01\rangle$ je $|\alpha_0\beta_1|^2 = |\left(\frac{1}{\sqrt{2}}\right) \times 1|^2 = 0.5$
- $|10\rangle$ je $|\beta_0\alpha_1|^2 = |\left(\frac{1}{\sqrt{2}}\right) \times 0|^2 = 0$
- $|11\rangle$ je $|\beta_0\beta_0|^2 = |\left(\frac{1}{\sqrt{2}}\right) \times 1|^2 = 0.5$

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 Záver

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.