Technická univerzita v Košiciach
Fakulta elektrotechniky a informatiky

Meranie a interakcia kvantových obvodov

Diplomová práca

2020 **Bc. Marián Sabat**

Technická univerzita v Košiciach
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:	prof. Ing. Ján Kollár, CSc.

Košice 2020 **Bc. Marián Sabat**

Názov práce:	Meranie a interakcia kvantových obvodov
Pracovisko:	Katedra počítačov a informatiky, Technická univerzita v Košiciach
Autor:	Bc. Marián Sabat
Školiteľ:	prof. Ing. Ján Kollár, CSc.
Konzultant:	prof. Ing. Ján Kollár, CSc.
Dátum:	3. 5. 2020
Kľúčové slová:	Kvantové počítače, meranie, Haskell, pravdepodobnosť kvantových stavov

Abstrakt: Diplomová práca sa zaoberá témou merania kvantových obvodov. V práci je vysvetlený princíp merania, ktorý je využitý v programovom riešení. Ďalej sa tento program využíta v niekoľkých experimentoch, ktoré potvrdzujú jeho funkčnosť. Kapitola jeden detalnejšie popisuje cieľ tejto práce. Matematická teória, nutná na pochopenie práce je rozpísaná v kapitole 2. Ďalšie dve kapitoly nadvezujú na tieto poznatky a opisujú teóriu kvantových počítačov. Časť "Pravdepodobnostná analýza kvantových obvodov" poukazuje na problémy, ktoré nastávajú pri snahe merať stavy kvantových bitov. V kapitole 6 sú detailne spracované experimenty, ktoré zobrazujú funkčnosť riešenia. Kapitola 7 potom obsahuje návrh a realizáciu programového riešenia pravdepodobnostného modelu v jazyku Haskell. Časť "Kvantová teleportácia" uvádza zložitejšie využitie na obvode so silno previazanými bitmi. V závere sú uvedené všetky dosiahnuté výsledky tejto práce.

Thesis title:	Measurement and interaction of quantum circutis
Department:	Department of Computers and Informatics, Techincal University of Košice
Author:	Bc. Marián Sabat
Supervisor:	prof. Ing. Ján Kollár, CSc.
Tutor:	prof. Ing. Ján Kollár, CSc.
Date:	3. 5. 2020
Keywords:	Quantum computers, measurement, Haskell, probability of quantum states

Abstract: The diploma thesis deals with the topic of measuring quantum circuits. This work explains the principle of measurement, which is used in the software solution. Also there is use of this program in several experiments that confirm its functionality. Chapter one describes the goal of this work in more detail. Mathematical theory necessary to understand the work is described in Chapter 2. The next two chapters build on this knowledge and describe the theory of quantum computers. Section The Probabilistic Analysis of quantum circuits points to problems that occur when trying to measure the states of quantum bits. Detaily processed experiments, in Chapter 6, show the functionality of the solution. Chapter 7 then contains the design and implementation of a software solution for a probabilistic model in Haskell. The Quantum Teleportation section lists more complex use on a circuit with strongly entangled bits. In the end, all achievements are listed in results of this work.

57381

TECHNICKÁ UNIVERZITA V KOŠICIACH

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Katedra počítačov a informatiky

Z A D A N I E
D I P L O M O V E J P R Á C E

Študijný odbor: **Informatika**
Študijný program: **Informatika**

Názov práce:

Analýza a meranie kvantových obvodov

Analysis and Measuring of Quantum Circuits

Študent: **Bc. Marián Sabat**
Školiteľ: **prof. Ing. Ján Kollár, CSc.**
Školiace pracovisko: **Katedra počítačov a informatiky**
Konzultant práce: **prof. Ing. Ján Kollár, CSc.**
Pracovisko konzultanta: **Katedra počítačov a informatiky**

Pokyny na vypracovanie diplomovej práce:
1. Preštudovať matematické základy kvantovej mechaniky.
2. Uviesť reprezentáciu kvantových stavov, ich zmien a princíp merania.
3. Analyzovať pravdepodobnostné vlastnosti kvantového stroja.
4. Navrhnúť a realizovať zjednodušený pravdepodobnostný model kvantového stroja.
5. Záverečnú prácu spracovať podľa pokynov vedúceho diplomovej práce.

Jazyk, v ktorom sa práca vypracuje: slovenský
Termín pre odovzdanie práce: 04.05.2020
Dátum zadania diplomovej práce: 31.10.2019

.....
prof. Ing. Liberios Vokorokos, PhD.
dekan fakulty

Čestné vyhlásenie

Vyhlasujem, že som záverečnú prácu vypracoval samostatne s použitím uvedenej odbornej literatúry.

Košice, 3.5.2020 .....

Vlastnoručný podpis

Poďakovanie

Na tomto mieste by som rád poďakoval svojmu vedúcemu práce za jeho čas, odborné vedenie počas riešenia mojej záverečnej práce a hlavne za jeho železnú trpezlivosť.

Rovnako by som sa rád poďakoval svojim rodičom a priateľom za ich podporu a povzbudzovanie počas celého môjho štúdia.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Často sa hovorí o konci platnosti Moorovho zákona. Je možné, že v blízkej budúcnosti svet bude nútený zmeniť 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. 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.

V našom úmysle bude 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 zviazanie 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 apa-

rátu, ktorý umožňuje simuláciu kvantových programov na klasických strojoch. Priblížime vývoj pravdepodobnostného modelu vytvoreného vo funkcionálnom jazyku Haskell. A poskytneme komplexný návod na jeho použitie.

1 Ciele práce

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 potrebná 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 2×2 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 výsledná matica je typu $mr \times ns$.

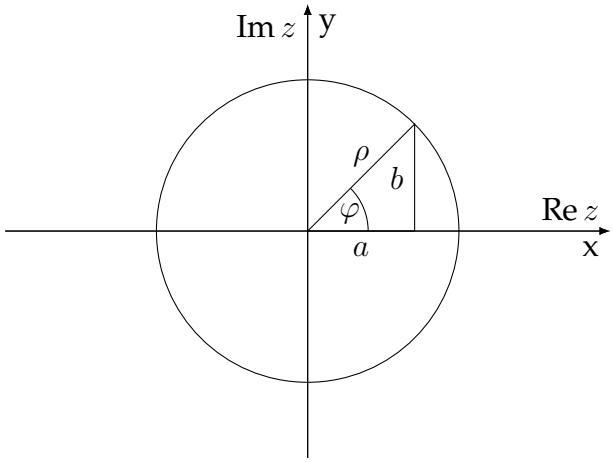
2.2 Komplexné čísla

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 - imaginára os

2. Polárnych súradníc ρ a φ,
   kde $\rho, \varphi \in \mathbb{R}$ a $\rho > 0$. V geometrickej reprezentácii (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 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

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

Operácie rozdielu a podielu sú ľahko odvoditeľné obnobným 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 reprezentácii pomocou polárnych súradníc $\alpha = \rho e^{i\varphi}$ je ρ nazývané amplitúda (veľkosť, norma) komplexného čísla a φ je fáza komplexného čísla [4].

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 [5]. 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 [6]. 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 priestore (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 Pojmy 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 [5]. 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 [5] $|\psi\rangle$ 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 [7] 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 [8]. 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 [9]. Z matematického pohľadu je to vektor v dvojrozmernom Hilberovom 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 vy-

jadríme ako $u = \binom{\alpha}{\beta}$, $(\alpha, \beta \in \mathbb{C})$ a $u \in \mathbb{C}^2$ [10]. 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 množina $\{|0\rangle, |1\rangle\} = \{\binom{1}{0}, \binom{0}{1}\}$ je nazývaná základná báza. Väčšinou je využívaná základná báza $\{|0\rangle, |1\rangle\}$, ale môžeme sa stretnúť aj s bázami $\{|+\rangle, |-\rangle\}$ a $\{|\circlearrowleft\rangle, |\circlearrowright\rangle\}$. 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 má, ale väčší význam využitie ortonormálnych vektorov.

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

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

Previazanosť kvantových bitov

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 [6].

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 samozrejme 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 z 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 $|\beta_1|^2$ [11]. 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 nadobudne 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 Kvantový systém

Stupeň vývoja kvantových počítačov nateraz neumožňuje 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 [12].

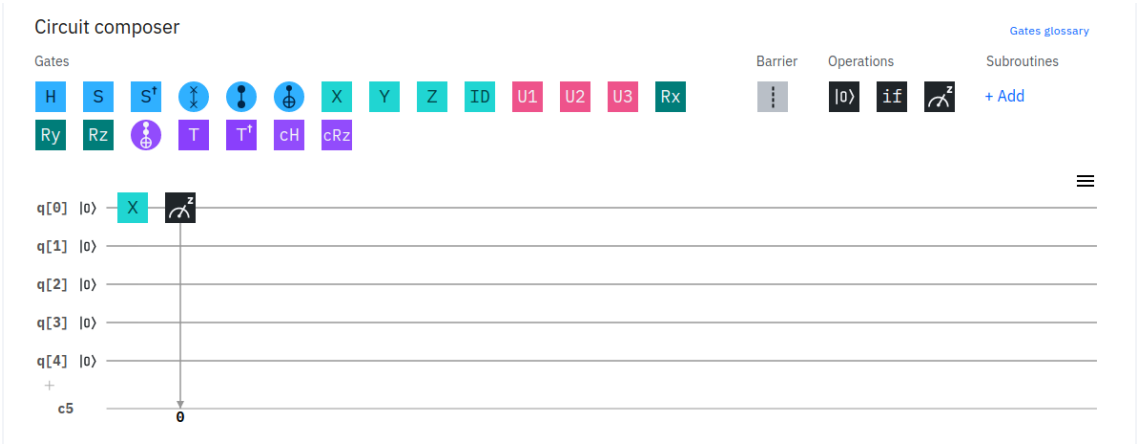
4.1 IBM Quantum Experience

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 simulovaný virtuálny stroj, no IBM QX umožňuje aj odoslanie experimentu na reálny počítač. Simulátor umožňuje relatívne rýchlu prácu s kvantovým počítačom. Tento prístup odľahčuje 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 naštartovať tento program. Na server sa odošle experiment, za predpokladu, že je obvod vykonávaný na simulátore, tak za krátku dobu dostaneme vrátené výsledky.

Obvody je možné navrhovať aj pomocou špeciálneho jazyka OpenQASM, pomocou editora, ktorý 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 dôležité 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:

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

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

$$\dots$$

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];
```

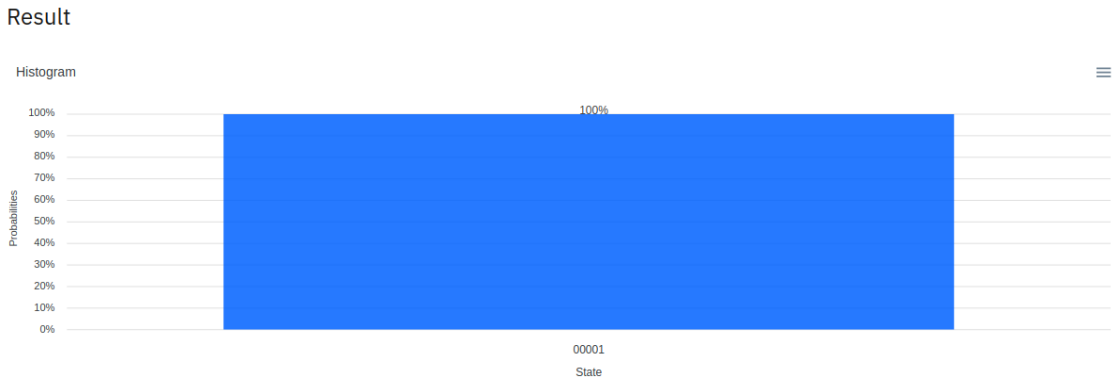
Výsledky experimentov sa zobrazujú v stĺpcovom diagrame, pričom stav systému je zobrazovaný v klasických bitoch opačne ako v kvantových. Teda stav n-bitového systému $\psi = |\psi_0\psi_1\psi_2 \dots \psi_{n-1}\rangle$ je meraný do klasického registra ako

$$c_{n-1} \dots c_2 c_1 c_0$$

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. Výsledok na obrázku 4.2 zobrazuje, že kvantový systém dosiahne so 100% pravdepodobnosťou stav 00001.



Obr. 4.2: Výsledky experimentu z IBM Quantum Experience.

4.1.1 Stavy a ich zápis

Pri výpočtoch je najviac využívaných týchto šesť stavov kvantových bitov [13]:

1. $|0\rangle = \binom{1}{0}$,
2. $|1\rangle = \binom{0}{1}$,
3. $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$,
4. $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$,
5. $|\circlearrowright\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$,
6. $|\circlearrowleft\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$.

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

4.1.2 Operácie kvantových hradiel

Existuje veľké množstvo hradiel. No v našom pravdepodobnostnom modely budeme využívať osem základných hradiel, ktoré sú najviac využívané. V tejto časti ukážeme ako hradlá $X, Y, Z, H, S, S^\dagger, T$ a $T^\dagger$ menia stav kvantového bitu [6]. Definujme bit $|\psi\rangle = \binom{\alpha}{\beta}$, na ktorom aktivujeme dané hradlá.

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

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

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

$$Y\left|\psi\right\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix} = -i\beta\left|0\right\rangle + i\alpha\left|1\right\rangle$$

$$Z\left|\psi\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha\left|0\right\rangle - \beta\left|1\right\rangle$$

$$H\left|\psi\right\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha+\beta \\ \alpha-\beta \end{pmatrix} = \frac{\alpha+\beta}{\sqrt{2}}\left|0\right\rangle + \frac{\alpha-\beta}{\sqrt{2}}\left|1\right\rangle$$

$$S\left|\psi\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ i\beta \end{pmatrix} = \alpha\left|0\right\rangle + i\beta\left|1\right\rangle$$

$$S^{\dagger}\left|\psi\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -i\beta \end{pmatrix} = \alpha\left|0\right\rangle - i\beta\left|1\right\rangle$$

$$T\left|\psi\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \frac{1+i}{\sqrt{2}}\beta \end{pmatrix} = \alpha\left|0\right\rangle + \frac{1+i}{\sqrt{2}}\beta\left|1\right\rangle$$

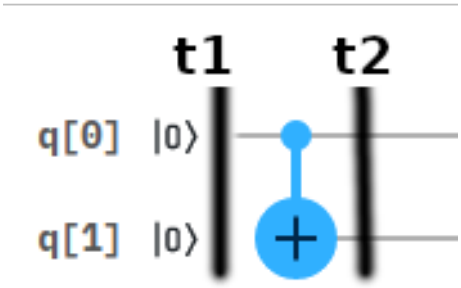
$$T^{\dagger}\left|\psi\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1-i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ \frac{1-i}{\sqrt{2}}\beta \end{pmatrix} = \alpha\left|0\right\rangle + \frac{1-i}{\sqrt{2}}\beta\left|1\right\rangle$$

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 časti 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 ovplyvňovaniu 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: Jednoduchý 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 okamih, 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 vyplýva, 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 vyplýva, 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 ψ priamym využitím tenzorového súčinu. Pri prechode hradom CNOT môžu nastať dve situácie:

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

Z toho je jasné, že v každom 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 $|\beta_0|^2$.

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

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

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

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

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

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

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

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

$|11\rangle$ 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 haradlo $CCNOT$ 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 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 môžme predstaviť ako prevod stavov kvantových bitov do stavu klasického digitálneho systému [8]. 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 [14] . 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 pravdepodobnosťou $|\alpha|^2$ respektíve $|\beta|^2$.

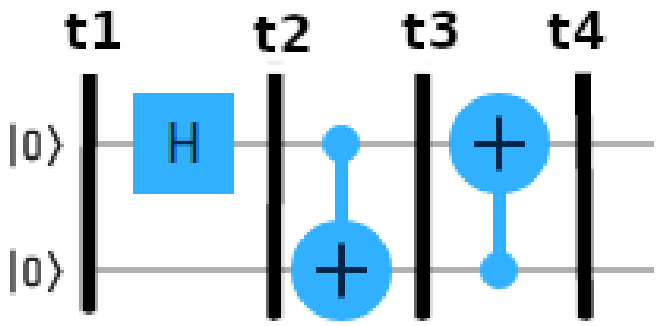
Pri každom fyzikálnom meraní nastáva určitá nepresnosť merania. Takisto pri meraní môže dokonca nastať zničenie obvodu. To vyplýva z toho, že pri skolabovanom kvantovom bite nastáva zmena fyzikálnych vlastností daného bitu.

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

Navrhnime kvantový obvod s dvoma bitmi. Označme ich $|\psi_0\rangle$ a $|\psi_1\rangle$. V prvom kroku aplikujeme Hadamardovo hradlo na bit $|\psi_0\rangle$. Nasledovať budú dve $CNOT$ hradlá s opačnými kontrólnymi a cieľovými bitmi. V IBM QX je tento obvod reprezentovaný ako



Obr. 6.1: Obvod experimentu 1 s označenými časovými úsekmi meraní.

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

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

Jeho grafické zobrazenie je na obrázku 6.1 aj s označenými časovými úsekmi, v ktorých bude meraný stav systému.

Teoretická analýza

Kvantové bity $|\psi_0\rangle$ a $|\psi_2\rangle$ sú definované ako

$$|\psi_0\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle$$

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

a teda je zrejmé, že v čase t_1 pre celkový stav $|\psi\rangle$ platí

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle = \alpha_0\alpha_1 |00\rangle + \alpha_0\beta_1 |01\rangle + \beta_0\alpha_1 |10\rangle + \beta_0\beta_1 |11\rangle$$

Z čoho jasne vyplýva, že systém nadobudne stav

$|00\rangle$ 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 $|\beta_0\beta_1|^2$

Po prechode Hadamardovim hradlom v čase t_2 kvantové bity zmenia svoj stav na

$$|\psi_0\rangle = \frac{\alpha_0 + \beta_0}{\sqrt{2}} |0\rangle + \frac{\alpha_0 - \beta_0}{\sqrt{2}} |1\rangle$$
$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle ,$$

a teda pre celkový stav $|\psi\rangle$ bude platiť

$$|\psi\rangle = \frac{\alpha_0 + \beta_0}{\sqrt{2}}\alpha_1 |00\rangle + \frac{\alpha_0 + \beta_0}{\sqrt{2}}\beta_1 |01\rangle + \frac{\alpha_0 - \beta_0}{\sqrt{2}}\alpha_1 |10\rangle + \frac{\alpha_0 - \beta_0}{\sqrt{2}}\beta_1 |11\rangle$$

Kvantový systém kolabuje v čase t_2 do stavu

$|00\rangle$ s pravdepodobnosťou $|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2$

$|01\rangle$ s pravdepodobnosťou $|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2$

$|10\rangle$ s pravdepodobnosťou $|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2$

$|11\rangle$ s pravdepodobnosťou $|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2$

Zmena nastáva v čase t_3, po prechode $CNOT$ hradlom. Bit $|\psi_1\rangle$ bude preklopený len v prípade, že $|\psi_0\rangle$ kolabuje do stavu $|1\rangle$. Čiže nastávajú dve možnosti. S pravdepodobnosťou $|\frac{\alpha_0+\beta_0}{\sqrt{2}}|^2$, ktorú označíme ako P_1^{t3} sa stavy kvantových bitov nezmenia

$$|\psi_0\rangle = \frac{\alpha_0 + \beta_0}{\sqrt{2}} |0\rangle + \frac{\alpha_0 - \beta_0}{\sqrt{2}} |1\rangle$$
$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$

Naopak, bit $|\psi_0\rangle$ kolabuje do stavu $|1\rangle$ s pravdepodobnosťou $|\frac{\alpha_0-\beta_0}{\sqrt{2}}|^2$ (označme P_2^{t3}), a teda v tomto prípade nastáva zmena v kvantovom bite $|\psi_1\rangle$

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

Platí, že systém v čase t_3 môže kolabovať do stavu

$|00\rangle$ s pravdepodobnosťou $(|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_1^{t3}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2 \times P_2^{t3})$

$|01\rangle$ s pravdepodobnosťou $(|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2 \times P_1^{t3}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_2^{t3})$

$|10\rangle$ s pravdepodobnosťou $(|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_1^{t3}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2 \times P_2^{t3})$

Pravdepodobnosť	**Stavy $\|\psi_0\rangle$ a $\|\psi_1\rangle$**
$P_1^{t4} = \|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1\|^2$	$\|\psi_0\rangle = \frac{\alpha_0+\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0-\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \alpha_1\|0\rangle + \beta_1\|1\rangle$
$P_2^{t4} = \|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1\|^2$	$\|\psi_0\rangle = \frac{\alpha_0-\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0+\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \alpha_1\|0\rangle + \beta_1\|1\rangle$
$P_3^{t4} = \|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1\|^2$	$\|\psi_0\rangle = \frac{\alpha_0+\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0-\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \beta_1\|0\rangle + \alpha_1\|1\rangle$
$P_4^{t4} = \|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1\|^2$	$\|\psi_0\rangle = \frac{\alpha_0-\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0+\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \beta_1\|0\rangle + \alpha_1\|1\rangle$

Tabuľka 6.1: Tabuľka stavov kvantových bitov a pravdepodobností nastatia týchto stavov v čase t_4 experimentu 1.

$|11\rangle$ s pravdepodobnosťou $(|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2 \times P_1^{t3}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_2^{t3})$

Poslendné meranie v tomto experimente je označené ako t_4. Opäť nastáva aktivácia $CNOT$ hradla, to jest podmienená zmena stavov kvantových bitov. V každom prípade bit $|\psi_1\rangle$ ostane nezmenený. No už teraz vychádzame z dvoch možností. Teda môžu nastať celkovo štyri prípady. V tabuľke 6.1 sú všetky možné zmeny stavov $|\psi_0\rangle$ a $|\psi_1\rangle$.

Čiže celkový stav $|\psi\rangle$ nadobudne stav

$|00\rangle$ s pravdepodobnosťou
$(|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_1^{t4}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_2^{t4}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2 \times P_3^{t4}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2 \times P_4^{t4})$

$|01\rangle$ s pravdepodobnosťou
$(|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2 \times P_1^{t4}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2 \times P_2^{t4}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_3^{t4}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_4^{t4})$

$|10\rangle$ s pravdepodobnosťou
$(|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_1^{t4}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_2^{t4}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2 \times P_3^{t4}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2 \times P_4^{t4})$

$|11\rangle$ s pravdepodobnosťou
$(|\frac{\alpha_0-\beta_0}{\sqrt{2}}\beta_1|^2 \times P_1^{t4}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\beta_1|^2 \times P_2^{t4}) + (|\frac{\alpha_0-\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_3^{t4}) + (|\frac{\alpha_0+\beta_0}{\sqrt{2}}\alpha_1|^2 \times P_4^{t4})$

		1.0 00				
	0.5000000000000001 00		0.4999999999999999 10			
0.25 01		0.2499999999999999 11		0.2500000000000001 00		0.25 10
0.25 01	0.2499999999999999 11		0.0 01	0.0 11	0.2500000000000001 00	0.25 10

Tabuľka 6.2: Výstup pravdepodobnostného modelu pre experiment 1 . Ohraničené riadky vymedzujú výsledky v jednotlivých časoch merania. Každá bunka obsahuje pravdepodobnosť dosiahnutia stavu a daný stav systému.

Výpočet pravdepodobností pomocou pravdepodobnostného modelu

Pre použitie pravdepodobnostného modelu je nutné definovať obvod v jazyku Haskell. Vyjadrime jednotlivé hradlá a rozdeľme ich po vertikálnych leveloch.

```
let l1 = Level [E, E] True
    l2 = Level [H, E] True
    l3 = Level [Cc, Ct] True
    l4 = Level [Ct, Cc] True
```

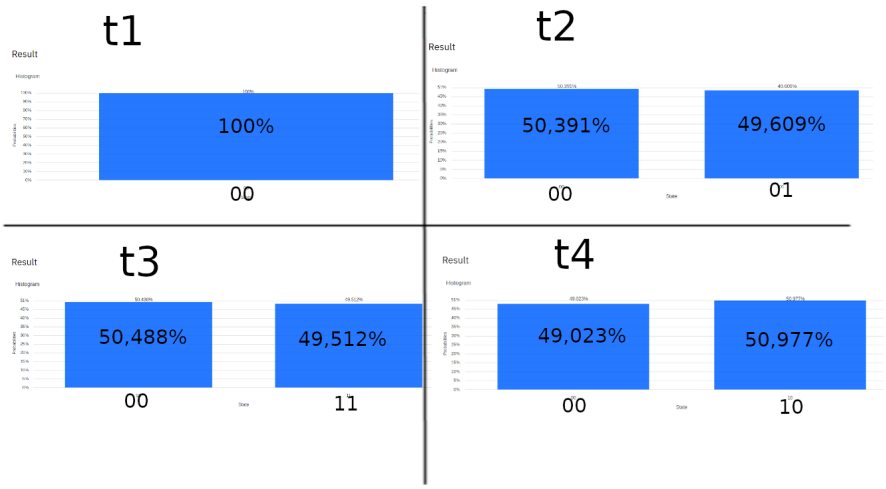
Pre meranie aj v čase t_1, ešte pred aktiváciou akéhokoľvek hradla, sme vložili jeden prázdny level navyše. Uložme tento obvod do spoločného listu a definujme aj stromové štruktúry pre stavy a výsledky.

```
c = [l1, l2, l3, l4]
st = StateTree 1 [q0, q0] []
rt = RT st []
```

Teraz už len aktivujme pravdepodobnostný model a uložme výsledky.

```
let resultRT = processCircuit c rt
```

Pre vstupy kde na začiatku obvodu je $|\psi_0\rangle = |0\rangle$ a zároveň $|\psi_1\rangle = |0\rangle$ nám model vypočítal výsledky, ktoré sú zaznamenané v tabuľke 6.2. Každý ohraničený



Obr. 6.2: Výsledky experimentu 1 z Quantum Experience so zvýraznenými údajmi.

riadok predstavuje časový úsek. Každá bunka potom obsahuje možný stav systému v daný časový úsek, kde horné číslo je pravdepodobnosť dosiahnutia tohto stavu v rozmedzí 0 až 1 a spodná hodnota určuje daný stav v tvare $\psi_0\psi_1$.

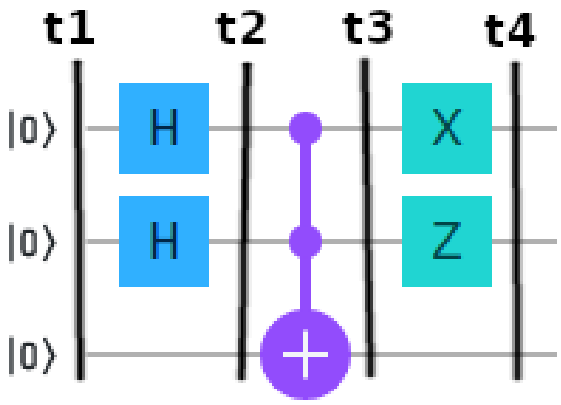
Porovnajme naše výsledky so simulátorom IBM Quantum Experience. V IBM QX bolo nutné vykonať štyri experimenty s rôznym časom merania, pretože tento simulátor nepodporuje fiktívne meranie. Dosiahnuté výsledky sú na obrázku 6.2. Pripomeňme, že notácia dosiahnutých stavov v IBM QX je $\psi_1\psi_0$, to znamená, že sú v opačnom poradí ako zápis v našej tabuľke. V prvých dvoch meraniach sú výsledky totožné. Rozdiel nastáva pri prechode hradlom $CNOT$. Pravdepodobnostný model, ktorý využívame, funguje na istom matematickom aparáte. IBM QX je ale simulátor kantového počítača, a preto môže brať do úvahy iné fyzikálne vlastnosti kvatových bitov, ktoré môžu vysvetľovať rozdiel v našich výsledkoch.

6.2.2 Experiment 2

Definujme kvantový obvod tak ako je na obrázku 6.3. Majme tri kvantové bity, ktoré označíme ako ψ_0, ψ_1 a ψ_2. Na prvých dvoch bitoch aktivujeme Hadamardové hradlá a potom tieto bity využijeme ako kontrólne bity v Tuffliho hradle. Nakoniec aplikujeme hradlo X a Z.

V OpenQASM je tento obvod zostrojený ako

```
qreg q[3];
```



Obr. 6.3: Obvod experimentu 2 s označenými časovými úsekmi meraní.

```
creg c[3];

h q[0];
h q[1];
ccx q[0],q[1],q[2];
x q[0];
z q[1];
```

Teoretická analýza

Stále platí, že

$$|\psi_0\rangle = \alpha_0 |0\rangle + \beta_0 |1\rangle$$
$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$
$$|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

Zistiť stav systému v čase t_1 je preto priamočiare

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle$$

V čase t_2 nastala aktivácia hradla H a preto sa zmení stav kvantových bitov na

$$|\psi_0\rangle = \frac{\alpha_0 + \beta_0}{\sqrt{2}} |0\rangle + \frac{\alpha_0 - \beta_0}{\sqrt{2}} |1\rangle$$
$$|\psi_1\rangle = \frac{\alpha_1 + \beta_1}{\sqrt{2}} |0\rangle + \frac{\alpha_1 - \beta_1}{\sqrt{2}} |1\rangle$$
$$|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

Stav	**Pravdepodobnosti**	
	t_1	t_2
$\|000\rangle$	$\|\alpha_0\alpha_1\alpha_2\|^2$	$\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2$
$\|001\rangle$	$\|\alpha_0\alpha_1\beta_2\|^2$	$\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2$
$\|010\rangle$	$\|\alpha_0\beta_1\alpha_2\|^2$	$\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\alpha_2\|^2$
$\|011\rangle$	$\|\alpha_0\beta_1\beta_2\|^2$	$\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\beta_2\|^2$
$\|100\rangle$	$\|\beta_0\alpha_1\alpha_2\|^2$	$\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2$
$\|101\rangle$	$\|\beta_0\alpha_1\beta_2\|^2$	$\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2$
$\|110\rangle$	$\|\beta_0\beta_1\alpha_2\|^2$	$\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\alpha_2\|^2$
$\|111\rangle$	$\|\beta_0\beta_1\beta_2\|^2$	$\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\beta_2\|^2$

Tabuľka 6.3: Vyjadrenie meraní pravdepodobnosti v čase t_1 a t_2 experimentu 2.

Vyjadrenie pravdepodobností dosiahnutia stavov z meraní 1 a 2 sú zaznamenané v tabuľke 6.3

Časový okamih t_3 predstavuje stav po prechode Tuffliho hradlom. Ak obe kontrólne bity $|\psi_0\rangle$ a $|\psi_1\rangle$ skolabujú do stavu $|1\rangle$, tak cieľový bit $|\psi_2\rangle$ bude preklopený hradlom X. Čiže v tomto momente $|\psi_0\rangle$ kolabuje do $|1\rangle$ s pravdepodobnosťou $|\frac{\alpha_0-\beta_0}{\sqrt{2}}|^2$ a podobne $|\psi_1\rangle$ s pravdepodobnosťou $|\frac{\alpha_1-\beta_1}{\sqrt{2}}|^2$. Z toho vyplýva, že preklopenie bitu $|\psi_2\rangle$ nastane s pravdepodobnosťou $|\frac{\alpha_0-\beta_0}{\sqrt{2}} \times \frac{\alpha_1-\beta_1}{\sqrt{2}}|^2 = \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}$

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

Naopak s pravdepodobnosťou $1 - \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}$ nenastane žiadna zmena

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

Toto rozdvojenie možných výsledkov sa nesie aj do merania t_4, no zmena nastáva len v prvých dvoch kvantových bitoch a tie sú v oboch prípadoch totožné. Nový stav týchto bitov je

$$|\psi_0\rangle = \frac{\alpha_0 - \beta_0}{\sqrt{2}} |0\rangle + \frac{\alpha_0 + \beta_0}{\sqrt{2}} |1\rangle$$

$$|\psi_1\rangle = \frac{\alpha_1 + \beta_1}{\sqrt{2}} |0\rangle - \frac{\alpha_1 - \beta_1}{\sqrt{2}} |1\rangle$$

Merania t_3 a t_4 sú zaznamenané v tabuľke 6.4.

Stav	**Pravdepodobnosti**
	t_3
$\|000\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|001\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
$\|010\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|011\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
$\|100\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|101\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
$\|110\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|111\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1-\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
	t_4
$\|000\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|001\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
$\|010\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|011\rangle$	$(\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0-\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
$\|100\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|101\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\alpha_1+\beta_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$
$\|110\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\beta_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\alpha_2\|^2 \times P_2^{t3})$
$\|111\rangle$	$(\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\alpha_2\|^2 \times P_1^{t3}) + (\|\frac{\alpha_0+\beta_0}{\sqrt{2}}\frac{\beta_1-\alpha_1}{\sqrt{2}}\beta_2\|^2 \times P_2^{t3})$

Tabuľka 6.4: Vyjadrenie meraní pravdepodobnosti v čase t_3 a t_4 experimentu 2, kde $P_1^{t3} = \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}$ a $P_2^{t3} = 1 - \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}$.

			1.0 000				
		0.25 000	0.25 010	0.25 100	0.249 110		
6.25e-2 001	6.249e-2 011	6.249e-2 101	6.249e-2 111	0.1875 000	0.1875 010	0.1875 100	0.18749 110
6.25e-2 001	6.249e-2 011	6.249e-2 101	6.249e-2 111	0.1875 000	0.1875 010	0.1875 100	0.18749 110

Tabuľka 6.5: Výsledky merania experimentu 2 pomocou pravdepodobnostného modelu. Ohraničené riadky vymedzujú výsledky v jednotlivých časoch merania. Každá bunka obsahuje pravdepodobnosť dosiahnutia stavu a daný stav systému.

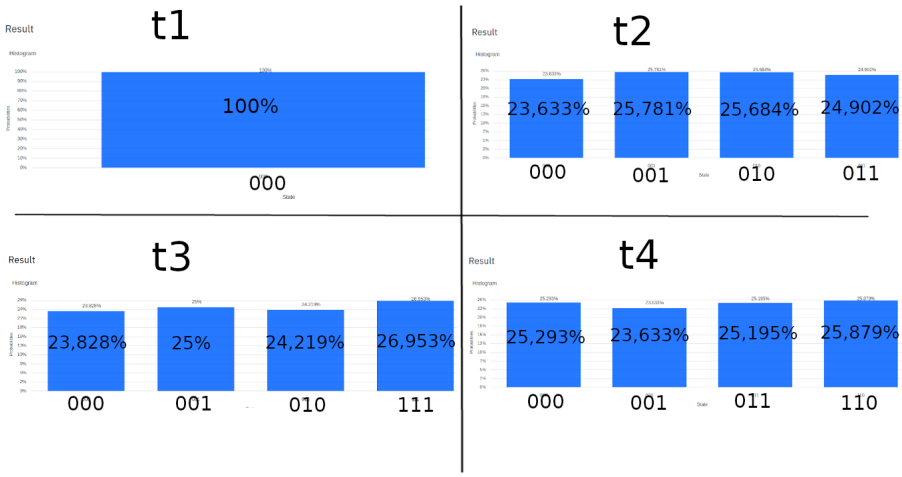
Výpočet pravdepodobností pomocou pravdepodobnostného modelu

Je nutné vyjadriť kvantový obvod v jazyku Haskell. Obvod obsahuje tri vertikálne levely. Pre meranie štyroch časových úsekov, ale definujeme štyri levely a štruktúry na ukladanie medzivýsledkov

```
let l1 = Level [E, E, E] True
    l2 = Level [H, H, E] True
    l3 = Level [Cc, Cc, Ct] True
    l4 = Level [X, Z, E] True
    c = [l1, l2, l3, l4]
    st = StateTree 1 [q0, q0, q0] []
    rt = RT st []
```

Po spustení modelu sme dosiahli výsledky, ktoré sú zaznamenané v tabuľke 6.5

Nakoľko na vstupe do systému sú kvantové bity v stave $|0\rangle$ je jasné, že meranie v čase t_1 môže dosiahnúť len jediný výsledok, a to 000. V čase t_2 sa vďaka Hadamardovému hradlu bity $|\psi_0\rangle$ a $|\psi_1\rangle$ dostanú do stavu $|+\rangle$ a teda obe môžu s 50%-tnou šancou kolabovať do $|1\rangle$ alebo $|0\rangle$. Čo naznačujú aj výsledky. Pri prechode Tuffliho hradlom systém môže zmeniť stav len ak prvé dva bity sú v stave



Obr. 6.4: Výsledky experimentu 2 z Quantum Experience so zvýraznenými údajmi.

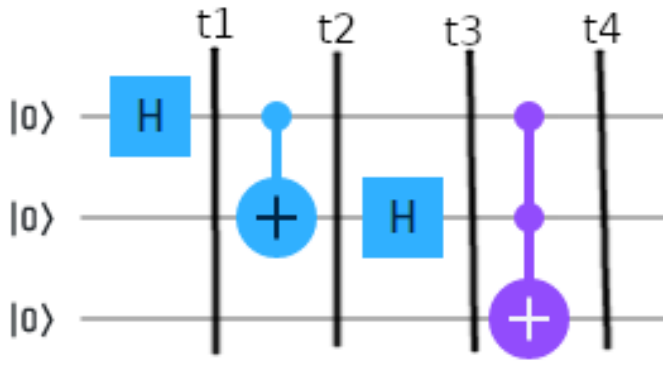
$|1\rangle$, a to môže nastať s 25%-tnou pravdepodobnosťou. Teda aj výsledky zohľadňujú to, že je oveľa nižšia šanca že bit $|\psi_2\rangle$ je v preklopenom stave $|1\rangle$. Pri poslednom meraní sa pravdepodobnosti nemenia nakoľko aplikáciou hradla X na stav $|+\rangle$ nenastane žiadna zmena a aplikáciou Z sa stav zmení na $|-\rangle$, čo nemá vplyv na výsledok.

Taktiež sme vykonali štyri merania v IBM QX, ktorých hodnoty sú zaznamenané na obrázku 6.4. Pripomeňme, že stav merania je zobrazovaný v opačnom poradí ako v tabuľke 6.5. Kým u nás stav je v tvare $c_0c_1c_2$, IBM QX využíva tvar $c_2c_1c_0$. Ako sme očakávali, prvé dve merania skončili s výsledkom totožným s našim. Meranie v časoch t_3 a t_4 sa líšia. Predpokladom pre rozdiel môže byť, že IBM QX využíva pri simulácii fyzikálny model nejakej častice, no náš pravdepodobnostný model vychádza z matematickej reprezentácie kvantového bitu.

6.2.3 Experiment 3

V treťom meraní použijeme ako hradlo $CNOT$ aj $CCNOT$. Na obrázku 6.5 je zobrazený tento obvod. Nakoľko je známy stav systému úplne na začiatku obvodu, tak tento časový úsek vynecháme a vykonáme opäť štyri merania. Tento obvod je možné v IBM QX definovať pomocou OpenQASM nasledovne.

```
qreg q[3];
creg c[3];
```



Obr. 6.5: Obvod experimentu 3 s označenými časovými úsekmi meraní.

```
h q[0];
cx q[0],q[1];
h q[1];
ccx q[0],q[1],q[2];
```

Teoretická analýza

Z obvodu je jasné, že v čase t_1 zmena stavu nastane len pre bit $|\psi_0\rangle$. A teda stavy budú nasledovné

$$|\psi_0\rangle = \frac{\alpha_0 + \beta_0}{\sqrt{2}} |0\rangle + \frac{\alpha_0 - \beta_0}{\sqrt{2}} |1\rangle$$
$$|\psi_1\rangle = \alpha_1 |0\rangle + \beta_1 |1\rangle$$
$$|\psi_2\rangle = \alpha_2 |0\rangle + \beta_2 |1\rangle$$

Odvodenie pravdepodobností je potom triviálne, $|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle$.

Hradlo $CNOT$ v čase t_2 spôsobí vetvenie možných výsledkov. Čiže s pravdepodobnosťou $P_1^{t2} = \frac{(\alpha_0+\beta_0)^2}{2}$ nadobudne bit $|\psi_0\rangle$ stav $|0\rangle$, čo znamená, že $|\psi_1\rangle$ ostane nezmenené. Naopak s pravdepodobnosťou $P_2^{t2} = \frac{(\alpha_0-\beta_0)^2}{2}$ nadobudne $|\psi_0\rangle$ stav $|1\rangle$, čo vedie k preklopeniu kvantového bitu $|\psi_1\rangle$ na $X|\psi_1\rangle$.

Toto vetvenie sa takisto prenesie aj na meranie v čase t_3. Takže aplikáciou Hadamardovho hradla na $|\psi_1\rangle$ dostaneme

$$|\psi_1\rangle = \tfrac{\alpha_1+\beta_1}{\sqrt{2}} |0\rangle + \tfrac{\alpha_1-\beta_1}{\sqrt{2}} |1\rangle \text{ s pravdepodobnosťou } P_1^{t2} = \tfrac{(\alpha_0+\beta_0)^2}{2}$$
$$|\psi_1\rangle = \tfrac{\beta_1+\alpha_1}{\sqrt{2}} |0\rangle + \tfrac{\beta_1-\alpha_1}{\sqrt{2}} |1\rangle \text{ s pravdepodobnosťou } P_2^{t2} = \tfrac{(\alpha_0-\beta_0)^2}{2}$$

Znovupreviazaním kvantových bitov v obvode narastá počet možných stavov geometricky. A preto v čase t_4 už dostávame štyri možné výsledky s pravdepodobnosťami:

$$P_1^{t4} = |\tfrac{\alpha_0-\beta_0}{\sqrt{2}} \times \tfrac{\alpha_1-\beta_1}{\sqrt{2}}|^2 \times P_1^{t2} = \tfrac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2(\alpha_0+\beta_0)^2}{8}$$

$$P_2^{t4} = (1 - |\tfrac{\alpha_0-\beta_0}{\sqrt{2}} \times \tfrac{\alpha_1-\beta_1}{\sqrt{2}}|^2) \times P_1^{t2} = (1 - \tfrac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}) \times \tfrac{(\alpha_0+\beta_0)^2}{2}$$

$$P_3^{t4} = |\tfrac{\alpha_0-\beta_0}{\sqrt{2}} \times \tfrac{\beta_1-\alpha_1}{\sqrt{2}}|^2 \times P_2^{t2} = \tfrac{(\alpha_0-\beta_0)^2(\beta_1-\alpha_1)^2(\alpha_0-\beta_0)^2}{8}$$

$$P_4^{t4} = (1 - |\tfrac{\alpha_0-\beta_0}{\sqrt{2}} \times \tfrac{\beta_1-\alpha_1}{\sqrt{2}}|^2) \times P_2^{t2} = (1 - \tfrac{(\alpha_0-\beta_0)^2(\beta_1-\alpha_1)^2}{4}) \times \tfrac{(\alpha_0-\beta_0)^2}{2}$$

Dajme do pozornosti, že $(\alpha_1 - \beta_1)^2 = (\beta_1 - \alpha_1)^2$, teda ak označíme $P_x = \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}$ môžme pre tento experiment zapísať, že platí

$$P_1^{t4} = P_x \times P_1^{t2}$$

$$P_2^{t4} = (1 - P_x) \times P_1^{t2}$$

$$P_3^{t4} = P_x \times P_2^{t2}$$

$$P_4^{t4} = (1 - P_x) \times P_2^{t2}$$

V tabuľke 6.6 sú zapísané stavy kvantových bitov v čase t_4, pre všetky možné výsledky. Pre výpočet výsledných pravdepodobností použijeme pre každú možnosť

$$|\psi\rangle = |\psi_0\rangle \otimes |\psi_1\rangle \otimes |\psi_2\rangle$$

Označme vyjadrenie pravdepodobnosti dosiahnutia nejakého celkového stavu ako P_{sn}, kde $1 \leq n \leq 4$ a s je stav. Potom platí

$$s = (P_{s1} \times P_1^{t4}) + (P_{s2} \times P_2^{t4}) + (P_{s3} \times P_3^{t4}) + (P_{s4} \times P_4^{t4})$$

Čo vieme pomocou známych P_n^{t4} upraviť na

$$s = (P_x \times P_1^{t2})(P_{s1} - P_{s2} \times P_1^{t2}) + (P_x \times P_2^{t2})(P_{s3} - P_{s4} \times P_2^{t2}) =$$

$$= (\frac{(\alpha_0^2 - \beta_0^2)(\alpha_1 - \beta_1)}{8})(P_{s1} - P_{s2} \times P_1^{t2}) + (\frac{(\alpha_0 - \beta_0)^2(\alpha_1 - \beta_2)^2}{8})(P_{s3} - P_{s4} \times P_2^{t2}) =$$

$$= \frac{(\alpha_1 - \beta_1)^2}{8}((\alpha_0^2 - \beta_0^2)(P_{s1} - P_{s2} \times \frac{(\alpha_0 + \beta_0)^2}{2})) + ((\alpha_0 - \beta_0)^2(P_{s3} - P_{s4} \times \frac{(\alpha_0 - \beta_0)^2}{2}))$$

Potom pre jednotlivé stavy sú dosiahnuteľné s pravdepodobnosťou

$$|000\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0+\beta_0)^2(\alpha_1+\beta_1)^2}{4}\beta_2^2 - \frac{(\alpha_0+\beta_0)^2(\alpha_1+\beta_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0+\beta_0)^2(\beta_1+\alpha_1)^2}{4}\beta_2^2 - \frac{(\alpha_0+\beta_0)^2(\beta_1+\alpha_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|001\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0+\beta_0)^2(\alpha_1+\beta_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0+\beta_0)^2(\alpha_1+\beta_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0+\beta_0)^2(\beta_1+\alpha_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0+\beta_0)^2(\beta_1+\alpha_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|010\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0+\beta_0)^2(\alpha_1-\beta_1)^2}{4}\beta_2^2 - \frac{(\alpha_0+\beta_0)^2(\alpha_1-\beta_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0+\beta_0)^2(\beta_1-\alpha_1)^2}{4}\beta_2^2 - \frac{(\alpha_0+\beta_0)^2(\beta_1-\alpha_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|011\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0+\beta_0)^2(\alpha_1-\beta_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0+\beta_0)^2(\alpha_1-\beta_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0+\beta_0)^2(\beta_1-\alpha_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0+\beta_0)^2(\beta_1-\alpha_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|100\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0-\beta_0)^2(\alpha_1+\beta_1)^2}{4}\beta_2^2 - \frac{(\alpha_0-\beta_0)^2(\alpha_1+\beta_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0-\beta_0)^2(\beta_1+\alpha_1)^2}{4}\beta_2^2 - \frac{(\alpha_0-\beta_0)^2(\beta_1+\alpha_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|101\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0-\beta_0)^2(\alpha_1+\beta_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0-\beta_0)^2(\alpha_1+\beta_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0-\beta_0)^2(\beta_1+\alpha_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0-\beta_0)^2(\beta_1+\alpha_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|110\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}\beta_2^2 - \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0-\beta_0)^2(\beta_1-\alpha_1)^2}{4}\beta_2^2 - \frac{(\alpha_0-\beta_0)^2(\beta_1-\alpha_1)^2}{4}\alpha_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

$$|111\rangle = \frac{(\alpha_1-\beta_1)^2}{8}((\alpha_0^2-\beta_0^2)(\frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0-\beta_0)^2(\alpha_1-\beta_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0+\beta_0)^2}{2})) + ((\alpha_0-\beta_0)^2(\frac{(\alpha_0-\beta_0)^2(\beta_1-\alpha_1)^2}{4}\alpha_2^2 - \frac{(\alpha_0-\beta_0)^2(\beta_1-\alpha_1)^2}{4}\beta_2^2 \times \frac{(\alpha_0-\beta_0)^2}{2}))$$

Výpočet pravdepodobností pomocou pravdepodobnostného modelu

Definujme kvantový obvod pre pravdepodobnostný model.

```
let l1 = Level [H, E, E] True
    l2 = Level [Cc, Ct, E] True
    l3 = Level [E, H, E] True
    l4 = Level [Cc, Cc, Ct] True
    c = [l1, l2, l3, l4]
    st = StateTree 1 [q0, q0, q0] []
    rt = RT st []
```

Pravdepodobnosť	**Stavy $\|\psi_0\rangle$, $\|\psi_1\rangle$ a $\|\psi_2\rangle$**
$P_1^{t4} = P_x \times P_1^{t2}$	$\|\psi_0\rangle = \frac{\alpha_0+\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0-\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \frac{\alpha_1+\beta_1}{\sqrt{2}}\|0\rangle + \frac{\alpha_1-\beta_1}{\sqrt{2}}\|1\rangle$ $\|\psi_2\rangle = \beta_2\|0\rangle + \alpha_2\|1\rangle$
$P_2^{t4} = (1 - P_x) \times P_1^{t2}$	$\|\psi_0\rangle = \frac{\alpha_0+\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0-\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \frac{\alpha_1+\beta_1}{\sqrt{2}}\|0\rangle + \frac{\alpha_1-\beta_1}{\sqrt{2}}\|1\rangle$ $\|\psi_2\rangle = \alpha_2\|0\rangle + \beta_2\|1\rangle$
$P_3^{t4} = P_x \times P_2^{t2}$	$\|\psi_0\rangle = \frac{\alpha_0+\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0-\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \frac{\beta_1+\alpha_1}{\sqrt{2}}\|0\rangle + \frac{\beta_1-\alpha_1}{\sqrt{2}}\|1\rangle$ $\|\psi_2\rangle = \beta_2\|0\rangle + \alpha_2\|1\rangle$
$P_4^{t4} = (1 - P_x) \times P_2^{t2}$	$\|\psi_0\rangle = \frac{\alpha_0+\beta_0}{\sqrt{2}}\|0\rangle + \frac{\alpha_0-\beta_0}{\sqrt{2}}\|1\rangle$ $\|\psi_1\rangle = \frac{\beta_1+\alpha_1}{\sqrt{2}}\|0\rangle + \frac{\beta_1-\alpha_1}{\sqrt{2}}\|1\rangle$ $\|\psi_2\rangle = \alpha_2\|0\rangle + \beta_2\|1\rangle$

Tabuľka 6.6: Tabuľka stavov kvantových bitov a pravdepodobností nastatia týchto stavov v čase t_4 experimentu 3.

Za povšimnutie stojí fakt, že hradlá $CNOT$ a $CCNOT$ sú implementované pomocou jednej funkcie. Takže aj v definícií obvodu nie je potrebná špeciálna štruktúra pre zabezpečenie týchto hradiel, ale kontrólne bity sú jednoducho označené ako Cc a cieľový bit ako Ct.

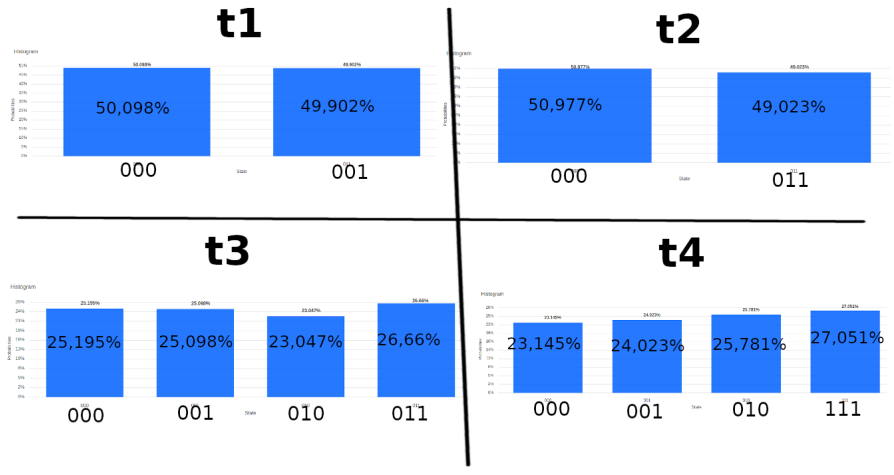
Po spustení pravdepodobnostného modelu dostávame tabuľku s výsledkami 6.7

Náš pravdepodobnostný model nesčítava pravdepodobnosti pri výskyte rovnakých stavov a automaticky sa meranie formátuje do jedného riadku. Z toho dôvodu sme naformátovali tabuľku tak, aby boli všetky výsledky zobrazené.

Výsledky z IBM Quantum Experience sú zobrazené na obrázku 6.6

			0.50 000	0.49 100			
		0.25 010	0.249 110	0.250 000	0.25 100		
0.125 000	0.1249 010	0.1249 100	0.1249 110	0.125 000	0.125 010	0.125 100	0.1249 110
3.1249e-2 001	3.1249e-2 011	3.1249e-2 101	3.1249e-2 111	9.375e-2 000	9.3749e-2 010	9.3749e-2 100	9.3749e-2 110
3.1251e-2 001	3.1249e-2 011	3.1249e-2 101	3.1249e-2 111	9.375e-2 000	9.3754e-2 010	9.3754e-2 100	9.375e-2 110

Tabuľka 6.7: Výsledky merania experimentu 3 pomocou pravdepodobnostného modelu. Ohraničené riadky vymedzujú výsledky v jednotlivých časoch merania. Každá bunka obsahuje pravdepodobnosť dosiahnutia stavu a daný stav systému.



Obr. 6.6: Výsledky experimentu 3 z Quantum Experience so zvýraznenými údajmi.

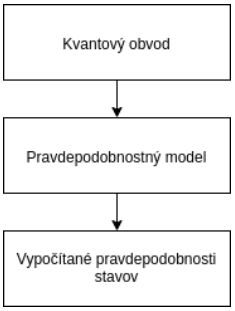
7 Pravdepodobnostný model kvantového výpočtu - návrh a realizácia

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.

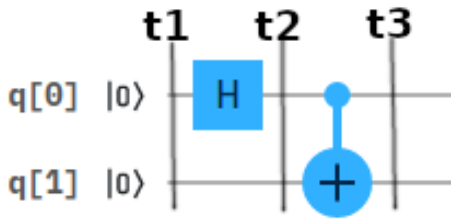
Pri pohľade na jednoduchý konceptuálny model (obrázok 7.1) je zrejmé, čo chceme dosiahnuť. Na vstupe je očakávaný kvantový obvod. Samotný program prebehne týmto obvodom ako interpreter a zároveň pomerá stavy na daných miestach v obvode. Nakoniec vypíše výstup v zrozumiteľnej podobe.

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, môžme definovať prázdny element. V obvode bude možné vyžiť osem základných hradiel, ktoré boli definované v časti 4.1.2 Operácie kvan-



Obr. 7.1: Konceptuálny návrh programu



Obr. 7.2: Kvantový obvod s previazanými kvantovými bitmi.

tových hradiel, a hradlo C^{n}NOT.

```
data Element = X
     | Y
     | Z
     | H
     | S
     | Sd
     | T
     | Td
     | Ct
     | Cc
     | E
```

Kvantový obvod môžeme definovať ako list levelov, pričom level je dátová štruktúra, ktorá obsahuje list hradiel. Okrem hradiel každý level bude obsahovať prepínač, ktorý signalizuje či má nastať fiktívne meranie po aktivácií hradiel v leveli.

```
type LevelGates = [Element]
data Level = Level LevelGates Bool
```

7.2 Pravdepodobnostný model

Pravdepodobnostný model možno vo funkčnosti prirovnať k interpreteru 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). Našim cieľom nie je vytvoriť 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.

Pravdepodobnostný model si uchováva stavy všetkých kvantových bitov a v stromovej štruktúre.

```
type QBit = [[Complex Double]]
type States = [QBit]
type SubTrees = [StateTree]

data StateTree = StateTree Double States SubTrees
```

Pri prechode levelom si uloží nové stavy do listov tohto stromu. Ak sa v leveli nachádzajú len obyčajné 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.

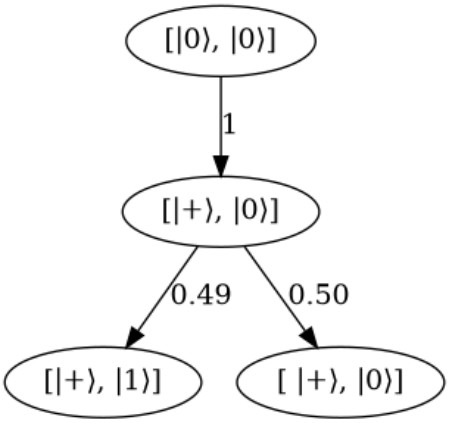
Pri meraní (fiktívnom meraní) sa spočítajú pravdepodobnosti všetkých listov stromu a výsledky sa uložia do tabuľky.

```
data R = R Double [Int]
type T = [R]
type Ts = [T]
```

Dátová štruktúra R popisuje pravdepodobnosť dosiahnutia stavu, ktorý je reprezentovaný ako list celých čísel $c_0 c_1 \ldots c_n$. 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 dátové štruktúry v jazyku Haskell.

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



Obr. 7.3: Strom stavov (StateTree) po vykonaní kvantového obvodu, kde hrany stromu sú označené pravdepodobnosťou dosiahnutia daného podstromu.

- 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 podstromy. Štruktúra RT slúži na ukladanie výsledkov meraní. Spustením pravdepodobnostného modelu dostaneme výslednú tabuľku typu RT.

```
processRT = processCircuit c rt
```

Pričom štruktúra RT je definovaná ako

```
data RT = RT StateTree Ts
```

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 isté 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 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 $|\alpha_0\alpha_1|^2 = |\left(\frac{1}{\sqrt{2}}\right) \times 0|^2 = 0$
- $|01\rangle$ 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. Preto všetky tieto pravdepodobnosti kolabovania musíme 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

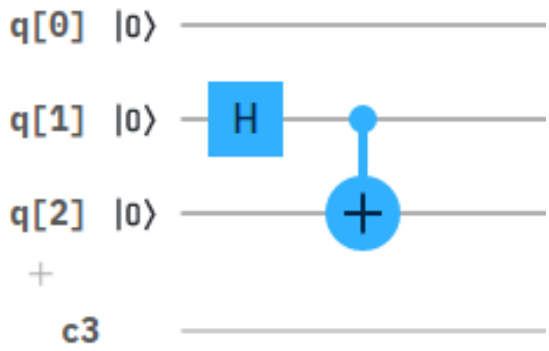
Predstavme si situáciu, že chceme na diaľku komunikovať. Chceme poslať informáciu o stave kvantového bitu. Zaznamenať komplexné číslo úplne presne na číslicovom počítači nejde, a teda nemožno poslať niekomu informáciu o presnom stave. Takisto platí, že kvantové bity je nemožné kopírovať či klonovať. Spôsobom akým sa dá riešiť tento problém je takzvaná kvantová teleportácia [15].

Medzi účastníkov komunikácie sa rozdelí dvojica previazaných bitov. Ak tieto kvantové bity nemeriame, zachovajú si svoj stav aj previazanie, nehľadiac na fyzickú vzdialenosť medzi nimi. Teda je možné komunikovať aj na diaľku.

Uveďme si všeobecne známy príklad na kvantovú teleportáciu. Povedzme, že Bob chce poslať kvantový bit Alici. Najprv je nutné aby obaja vlastnili pár previazaných kvantových bitov. Ak teraz chce Bob poslať bit Alici, jediné čo musí spraviť je aplikovať CNOT hradlo na svoj previazaný bit, ktorý bude kontrolovaný kvantovým bitom, ktorý chce odoslať. Potom aplikuje Hadamardovo hradlo na odosielaný bit a pomeria obe bity. Alici odošle informáciu o stavoch, ktoré kolabovaním dostal. Alica z tejto informácie vie, ako má použiť hradlá X a Z, tak aby dosiahla rovnaký stav bitu, ktorý pôvodne vlastnil Bob.

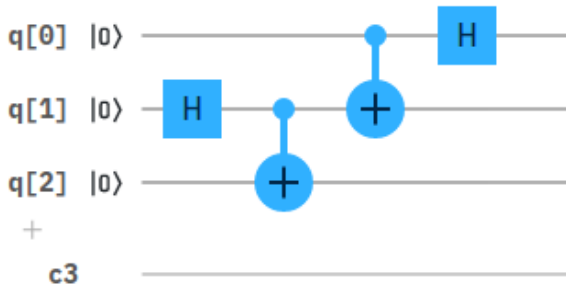
Týmto spôsobom je možné informáciu poslať, pretože sa jedná o celé čísla. Tak isto nie je porušená veta o kopírovaní ani klonovaní kvantových bitov, lebo Bob svoj bit stratil [16].

Ukážme si to na kvantovom obvode. Vytvoríme previazaný pár kvantových bitov ako na obrázku 8.1. Povedzme, že bit q_1 patrí Bobovi a q_2 je Alicin.



Obr. 8.1: Previazanie kvantových bitov na kvantovú teleportáciu.

Ako bolo spomenuté, na to aby mohol Bob poslať bit q_0, musí aplikovať CNOT a následne Hadamardovo hradlo, tak ako na obrázku 8.2.



Obr. 8.2: Obvod popisujúci kvantovú teleportáciu.

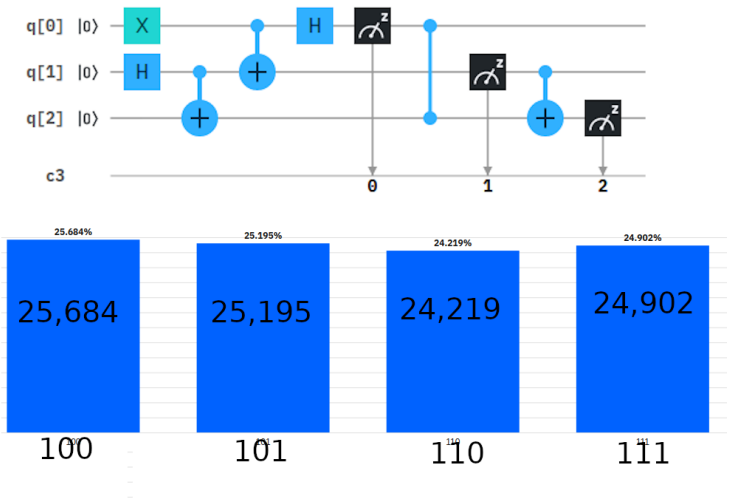
Bob pomeria svoje bity a pošle tieto merania Alici. Alica na základe týchto meraní vie, že ak

Bobov bit q_0 nadobudne stav 1, aplikuj hradlo Z na q_2

Bobov bit q_1 nadobudne stav 1, aplikuj hradlo X na q_2

IBM Quantum Experience výsledky

Dokončime obvod. Povedzme, že posielame stav $|1\rangle$, preto pridáme hradlo X na začiatok obvodu a plikujeme na q_0. Nakoniec pridáme podmienené aplikácie hradiel Z a X. IBM QX podporuje variantu hradla $CNOT$, kde namiesto preklopenia X aplikujeme Z. Výsledný obvod aj s meraniami je na obrázku 8.3.



Obr. 8.3: Výsledky príkladku kvanovej teleportácie.

Podľa výslekov je jasné, že teleportácia bola úspešná. Najhlavnejší bit všetkých výsledkov je 1. To znamená, že Alicin kvantový bit vždy nadobudne taký stav aký mal pôvodne Bob, čo bolo $|1\rangle$.

Pravdepodobnostný model

Definujeme kvantový obvod pre program v jazyku Haskell.

```
let l1 = Level [E, H, E] True
    l2 = Level [E, Cc, Ct] True
    l3 = Level [Cc, Ct, E] True
    l4 = Level [H, E, E] True
    c = [l1, l2, l3, l4]
    st = StateTree 1 [q1, q0, q0] []
    rt = RT st []
```

Bit q_0 nastavíme na stav $|1\rangle$, ostatné na $|0\rangle$. V našom pravdepodobnostnom modely nejestvuje možnosť podmienených aplikácií hradiel, tak si budeme musieť vystačiť s neúplnou teleportáciou.

Fiktívne meranie je nastavené za každým levelom, výsledky meraní su v tabuľke 8.1.

Opäť pripomeňme, že poradie bitov vo výsledkoch z pravdepodobnostného modelu a výsledkoch IBM QX je opačné. Pozornému oku neunikne, že v niekto-

			0.50 100	0.49 110			
		0.25 101	0.249 111	0.25 100	0.25 110		
	0.25 101	0.249 111	0.0 101	0.0 111	0.25 100	0.25 110	0.0 100	0.0 110
0.125 001	0.1249 011	0.1249 101	0.1249 111	0.125 000	0.125 010	0.125 100	0.1249 110

Tabuľka 8.1: Výsledky merania experimentu kvantovej teleportácie pomocou pravdepodobnostného modelu. Ohraničené riadky vymedzujú výsledky v jednotlivých časoch merania. Každá bunka obsahuje pravdepodobnosť dosiahnutia stavu a daný stav systému.

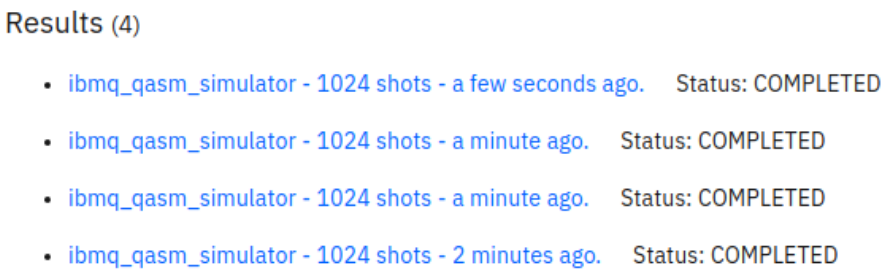
rých prípadoch výsledky po použití hradiel X a Z nebudú dávať správny výsledok. Je nutné podotknúť, že pravdepodobnostný model nepracuje až tak na základe vstupných stavov kvantových bitov v obvode ako na základe matematikého modelu pravdepodobností dosiahnutia stavov $|0\rangle$ a $|1\rangle$. Tak isto je vidno, že niektoré možnosti sú nedosiahnuteľné. Teda výsledky pravdepodobnostného modelu sú narozdiel od IBM QX odvodzované od všeobecných stavov kvantových bitov $|\psi\rangle$ a vstupné hodnoty stavov týchto bitov sú použité len na upravenie pravdepodobností do finálnej podoby.

9 Celkové vyhodnotenie

V tejto práci sme uviedli spôsob vykonávania a merania kvantových obvodov. Využitím vedomostí z matematiky a funkcionálneho programovania sme úspešne navrhli a implementovali model pre počítanie fiktívnych meraní kvantových bitov v kvantových obvodoch.

I keď nie je možné porovnávať simulátor kvantového stroje IBM Quantum Experience s pravdepodobnostným modelom je nutné vyzdvihnúť fakt, že k výsledkom a teda k predstave ako prebieha kvantový program sa dostaneme oveľa rýchlejšie. Na obrázku 9.1 sú zobrazené výpisy o dokončení meraní experimentu v IBM QX. Pri experimentoch, ktoré sme vykonávali sme robili štyri fiktívne merania. Pre zistenie výsledkov zo simulátora kvantového stroja, bolo potrebné vykonať jednotlivé merania osobitne a to zabralo relatívne veľa času. Ako vidíme na obrázku (9.1), vykonanie štyroch takýchto meraní trvalo viac ako dve minúty. Kde náš pravdepodobnostný model vďaka tomu, že nemusí robiť reálne meranie ale len to fiktívne, vracia výsledky okamžite.

Samozrejme, že ak potrebujeme presné merania, je lepšie použiť kompletný simulátor. No výhodou nášho riešenia je zobrazenie zmien stavov kvantových bitov. IBM QX dokáže zobraziť len skolabované výsledky meraní, i keď veľmi presne,



Obr. 9.1: Časy dokončení meraní experimetov.

no niekedy je vhodnejšie vedieť stav ešte pred kolabovaním. Náš pravdepodobnosný model generuje stromovú štruktúru, v ktorej si zaznamenáva priebežné stavy kvantových bitov. Získané stromy z našich experimentov sme pridali do príloh tejto práce.

Funkčnosť modelu sme otestovali na troch experimetoch. V každom experimente sme odvodili vzorce pre výpočet pravdepodobností kolabovania do jednotlivých stavov pre všetky definované časové okamihy. Uviedli sme výsledky, ktoré sú dosiahnuteľné pomocou kvantového stroja IBM Quantum Experience. Nakoniec sme pre každý experiment uskutočnili meranie pomocou nášho pravdepodobnostného modelu.

V neposlednej rade sme preskúmali aj možnosť využitia tohto pravdepodobnostného modelu aj pri zložitejšom príklade, v ktorom prebiehal kvantový jav zvaný kvantová teleportácia.

10 Záver

Úlohou tejto práce bolo zostaviť programové riešenie problému merania stavov kvantových bitov počas behu kvantového obvodu. Poskytli sme výstižný úvod do problematiky kvantových počítačov z pohľadu matematických definýcií. Po prečítaní tejto práce by aj laikovi malo byť jasné ako prebieha kvantový obvod a na akom princípe fungujú merania bitov.

Ešte pred samotnou implementáciou Haskellovského programu sme sa snažili detailne priblížiť na akom matematickom princípe postavíme pravdepodobnostný model. Analýzu návrhu a proces implementácie tohto pravdepodobnostného modelu sme rozobrali v jednej z kapitol. Vďaka tomu sme mohli ukázať aj riešenie zložitejšieho príkladu kvantového obvodu.

Tak ako sme dokázali pri experimentoch, náš pravdepodobnostný model je využiteľný pri tvorbe a analýze kvatnových obvodov. Značne urýchľuje výpočty, ktoré je nutné vykonávať a odvodzovať pri práci s spomínanými obvodmi. Poskytuje grafickú podobu zmien stavov, čo len ďalej zjednodušuje pochopenie práce kvantových počítačov.

Do budúcna by bolo dobré vytvoriť grafické prostredie, ktoré by bolo nadstavbou tejto práce. Uľahčilo by to prácu, pretože by nebolo nutné poznať jazyk Haskell pre realizáciu experimentu. Experimenty, ktoré táto práca popisuje sú ale dobrým návodom ako tento program využívať. Taktiež obohatenie tohto pravdepodobnostného modelu o sofistikovanejší simulátor kvantového stroja by priniesol presnejšie výsledky, najmä pri obvodoch s previazanými kvantovými bitmi. V takom prípade by bolo možné úplne nahradiť kvantový simulátor IBM Quantum Experience, pri návrhu a prvotnom testovaní kvantových obvodoch, čo by v konečnom dôsledku malo za vplyv rýchlejší rozvoj tejto technológie.

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] Richard D. Nation Richard N. Aufmann Vernon C. Barker. *College Algebra and Trigonometry*. Cengage Learning, 2007.

[5] Dennis Bernstein. *Scalar, Vector, And Matrix Mathematics: Theory, Facts, And Formulas*. Princeton University Press, 2018.

[6] Michael A. Nielsen a Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[7] Thomas W. Hungerford. *Algebra*. Springer, 2003.

[8] Issac L. Chuang Michael A. Nielsen. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[9] B. Schumacher. "Quantum coding". In: *Physical Review A.* (1995).

[10] Michele Mosca Phillip Kaye Raymond LaFlamme. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[11] A. Yu. Kitaev. *Quantum measurements and the Abelian stabilizer problem*. 12 November 1995. eprint: `quant-ph/9511026`.

[12] *IBM Quantum Experience*. 2020. URL: `https://quantum-computing.ibm.com/`.

[13] S. Weinberg. *The Quantum Theory of Fields*. Cambridge University Press, 2002.

[14] Daniel Simon. "On the power of quantum computation". In: *SIAM Journal on Computing* 26.5 (1997). Earlier version in FOCS'94, s. 1474–1483.

[15] John Watrous. "Quantum algorithms for solvable groups". In: *Proceedings of 33rd ACM STOC*. 2001, s. 60–67.

[16] Ronald de Wolf. "Quantum Computing and Communication Complexity". Diz. pr. University of Amsterdam, 2001.

Zoznam príloh

Príloha A Používateľská príručka

Príloha B Systémová príručka

Príloha C CD médium – záverečná práca v elektronickej podobe,

A Používateľská príručka

A.1 Funkcia programu

Program slúži na meranie kvantového obvodu. Do programu je nutné vložiť definíciu kvantového obvodu aj s označenými časmi merania. Program vygeneruje latexové súbory pripravené na preklad pomocou latexového prekladača. Vygenerované sú dva súbory

1. Strom zmien stavov kvantových bitov (zn. 1),
2. Tabuľka výsledkov fiktívnych meraní v daných časových úsekoch (zn. 2).

A.2 Systémové požiadavky

Pre spustenie programu je nutné mať nainštalované:

- interpreter jazyka Haskell,
- latex.

A.3 Inštalácia programu

Samotný program nie je potrebné nijako inštalovať. Programové skripty sú v adresári program, pripravené na spustenie. Je ale nutné si pripraviť prostredie. Pre inštaláciu jazyka Haskell postupujte podľa návodu na oficiálnej stránke `www.haskell.org`. Pre operačný systém linux použite svojho správcu balíkov a nainštalujte haskell-platform. Príklad pre Ubuntu:

```
> sudo apt-get install haskell-platform
```

Na preklad výstupu do formátu .pdf je nutné použiť latex. Pre linux je inštalácia jednoduchá, pomocou správcu balíkov nainštalujte texlive. Príklad pre Ubuntu:

```
> sudo apt-get install texlive
```

Pre inštaláciu na Windows postupujte podľa pokynov na `http://www.tug.org/texlive/` alebo využite online nástroj Overleaf na `https://www.overleaf.com/`.

A.4 Spustenie programu

Pre definovanie kvantového obvodu je nutné upraviť súbor QWriter.hs. Vo funkcii main sú zakomentované štyri definície obvodov, ktoré boli použité v experimentoch diplomovej práce. Odkomentujte jeden alebo definujte nový obvod rovnakým spôsobom.

1. Nadefinujte vertikálne levely (odporúčanie: pomenujte ich l1..ln),
2. Uložte levely do listu ako premennú c,
3. Definujte strom stavov ako premennú st
4. Definujte tabuľku výsledkov ako rt.

Definícia levelu obsahuje konštruktor Level, list hradiel v danom vertikálnom levely (E - emplty, X, Y, Z, H, S, Sd, T, Td, Ct - cieľový bit CNOT hradla, Cc - kontrólny bit CNOT hradla) a indikátor, či má byť vykonané fiktívne meranie za daným levelom. Príklad:

```
Level [E, H, X] True
```

Definícia stromu stavov obsahuje konštruktor StateTree, počiatočnú pravdepodobnosť (odporúčanie: nastaviť na 1), list počiatočných stavov kvantových bitov (q1, q0, qP, qM, qR, qL alebo ľubovoľný stav definovaný ako [[Complex Double]], príklad [[0.0 :+ 0.0],[1.0 :+ 0.0]]). Veľkosť tohto listu určuje počet kvantových bitov v obvode. Posledný prvok definície stromu stavov je list podstromov (odporúčanie: nastaviť prázdny list). Príklad:

```
StateTree 1 [q0, q1] []
```

Definícia tabuľky výsledkov obsahuje konštruktor RT, strom stavov a list reprezentujúci samotnú tabuľku (odporúčanie: nastaviť prázdny list). Príklad:

```
RT st []
```

Po definovaní kvantového obvodu je možné spustiť meranie. Spustite interpreter jazyka haskell ghci v adresári program.

```
> ghci
```

Načítajte modul QWriter.

```
> :l QWriter
```

Nakoniec spustite funkciu main.

```
> main
```

Program si vypýta názov súboru pre uloženie výsledkov. Odporúčame mať vytvorený samostatný adresár pre výsledky, ale nie je to nevyhnutné. Povedzme, že chceme uložiť do adresára out, ktorý je v adresári program. Zadáme názov súboru aj s cestou k nemu. Prípona sa doplní samostatne.

```
> out/vysledok
```

Program vytvorí dva súbory pomenované vysledok1.tex a vysledok2.tex. Súbor s označením 1 obsahuje vygenerovaný strom stavov pomocou latexového balíčka tikz. Súbor s označením 2 obsahuje tabuľku výsledkov meraní.

Tieto súbory je možné preložiť pomocou latexu. Či už využitím nástroja Overleaf alebo napríklad pre linux:

```
> latexmk -pdf vysledok1
> latexmk -pdf vysledok2
```

B Systémová príručka

Všetky potrebné skripty sa nachádzajú v adresári program. Pri načítaní modulu QWriter sa automaticky načítajú aj ostatné.

- QCircuits.hs - obsahuje pravdepodobnostý model a celú logiku merania,
- QDefinitions.hs - obsahuje definície základných kvantových stavov a hradiel,
- QEntanglement.hs - obsahuje funkcie pre výpočet alfa a beta normy,
- QMatrix.hs - obsahuje oprerácie pre prácu s maticami,
- QOperations.hs - obsahuje definície operácií s kvanotvými bitmi
- QWriter.hs - obsahuje funkciu main a proces prekladu a zápisu do latexu.

B.1 Popis algoritmu pravdepodobnostného modelu

Algoritmus je založený na rekurzívnej aktivácií funkcie modelu nad obvodom. Každý level je postupne spracovaný pričom sa vytovrý nový strom stavov, hradlá daného levelu sú aplikované na listy priebežného stromu stavov kvantových bitov a tabuľka výsledkov je aktualizovaná, ak je level označený pre meranie.

Tvorba nového stromu je závislá na hradlách, ktoré level obsahuje. Ak v leveli nastáva previazanie niektorých z bitov pomocou hradla CNOT, je nutné rozvetviť strom na dva podstromy. Tieto vetvy určujú možnosti kde kontrólne bity sú v stavoch $|1\rangle$, a teda nastane preklopenie cieľového bitu a možnosť kde preklopenie nenastane.

B.2 Popis implementácie

Ukladanie stavov kvantových bitov zabezpečujú dátové štruktúry

```
type QBit = [[Complex Double]]
type States = [QBit]
type SubTrees = [StateTree]

data StateTree = StateTree Double States SubTrees deriving Show
```

Kvantový bit nie je nič iné ako matica komplexných čísel a typ States je potom list týchto bitov. Strom stavov obsahuje 3 časti. Pravdepodobnosť vykonania, typu Double, list stavov koreňa tohto stromu a odkaz na potomkov. List stromu je teda takisto strom, ale nemá žiadnych potomkov.

Tabuľka výsledkov je dvojrozmerným poľom, ktoré obsahuje v riadkoch merania v jednotlivých časových okamihoch. Stĺpce tejto tabuľky obsahujú štruktúru, ktorá obaľuje pravdepodobnosť dosiahnutia daného stavu systému a list bitov do ktorých systém kolabuje.

```
data R = R Double [Int]
    deriving (Show)
type T = [R]
type Ts = [T]
```

Pre jednoduchšiu prácu pravdepodobnostný model pracuje so štruktúrou, ktorá zaobaľuje tieto entity.

```
data RT = RT StateTree Ts
    deriving (Show)
```

Posledným datovým typom, ktorý je nevyhnutné spomenúť je reprezenácia kvantového obvodu.

```
data Element = X
    | Y
    | Z
    | H
    | S
```

```
    | Sd
    | T
    | Td
    | Ct   -- CNOT target bit
    | Cc   -- CNOT control bit
    | E    -- empty
    deriving (Show, Eq)

type LevelGates = [Element]
data Level = Level LevelGates Bool deriving Show
type Circuit = [Level]
```

Obvod je reprezentovaný ako list vertikálnych levelov. Každý level je zostavený z hradiel (typu LevelGates) a indikátora, ktorý označuje či má byť daný level meraný (typu Bool). Jednotlivé hradlá levelu sú typu Element a obsahujú základné kvantové hradlá, pričom Ct označuje cieľový bit hradla CNOT, Cc označuje kontrólny bit hradla CNOT a E označuje absenciu hradla na danej pozícii. Ostané hradlá je prirodzene jasné odlíšiť.

Nasleduje popis jednotlivých funkcií.

processCircuit :: Circuit -> RT -> RT

Vstup: Na vstupe je kvantový obvod a tabuľka výsledkov.
Výstup: Nová tabuľka výsledkov s pravdepodobnosťami meraní a stromom stavov kvantových bitov.
Popis: Hlavná funkcia merania obvodu. Rekurzívne prechádza list levelov. Ak je level meraný, aktualizuje tabuľku Ts. Takisto vyvolá aktiváciu hradiel z levela na strome stavov.

upTs :: Ts -> StateTree -> Ts

Vstup: Tabuľka výsledkov a strom stavov.
Výstup: Nová tabuľka so skolabovanými stavmi.
Popis: Funkcia vyvolá kolabovanie listov stromu stavov a zapíše výsledok do tabuľky výsledkov.

collapseR :: StateTree -> T

Vstup: Strom stavov.
Výstup: Namerané výsledky z jedného časového okamihu.
Popis: Funkcia skolabuje všetky kvantové bity v listoch stromu stavov a vráti list týchto meraní.

isLMeasured :: Level -> Bool

Vstup: Level.
Výstup: Inikátor merania.
Popis: Funkcia vráti True, ak má byť level meraný, False inak.

processLevel :: Level -> StateTree -> StateTree

Vstup: Level, ktorý sa má spracovať a strom stavov.
Výstup: Nový strom stavov.
Popis: Funkcia rekurzívne prechádza stromom stavov až kým nedosiahne koncové listy. Pri listoch vyvolá funkciu na aktivovanie hradiel levelu na daných bitoch. Nové stavy sú zapísané do nového stromu stavov kvantových bitov.

calculateStateTrees :: LevelGates -> States -> Double -> [StateTree]

Vstup: Hradlá levelu, ktorý sa aplikuje, Stavy bitov, ktoré hradlami prechádzajú a pravdepodobnosť nastatia tejto situácie.
Výstup: Nové stromy stavov, ktoré budú pridané ako listy do hlavého stromu.
Popis: Ak list hradiel obsahuje hradlo CNOT, funkcia vyvolá tvorbu dvoch stromov pre 2 prípady, ktoré môžu nastať. V inom prípad funkcia zavolá aplikáciu hradiel na jednotlivé kvantové bity a nové stavy vráti v novom podstrome.

applyCNot :: LevelGates -> States -> Double -> [StateTree]

Vstup: Hradlá levelu, ktorý sa aplikuje, Stavy bitov, ktoré hradlami prechádzajú a pravdepodobnosť nastatia tejto situácie.
Výstup: List s dvoma stromami stavov.

Popis: Funkcia prepočíta pravdepodobnosť s akou kontrólne bity kolabujú do stavu $|1\rangle$. Ak je táto pravdepodobnosť nulová, je vytvorený jediný podstrom a nie sú aplikované žiadne hradlá. V opačnom prípade sú vytvorené stromy dva, kde jeden aplikuje preklopenie cieľového bitu hradla CNOT a druhý nie. Vstupná pravdepodobnosť je využitá pri prepočte pravdepodobnosti nastatia nových podstromov.

cnPasP :: [Element] -> [QBit] -> Double

Vstup: Hradlá levelu a stavy bitov na ktorých sa dané hradlá aplikujú.
Výstup: Pravdepodobnosť.
Popis: Funkcia prepočítava pravdepodobnosť s akou kontrólne bity hradla CNOT kolabujú do stavu $|1\rangle$.

probCt1 :: Element -> QBit -> Double

Vstup: Hradlo a bit, ktorý daným hradlom prechádza.
Výstup: Pravdepodobnosť bitu dosiahnutia stav $|1\rangle$.
Popis: Ak je na vstupe hradlo Cc (kontrólny bit hradla CNOT), funkcia vracia pravdepodobnosť daného bitu kolabovať do stavu $|1\rangle$. Pre akékoľvek iné hradlo, funkcia vracia -1. Funkcia sa používa pri prepočťe cnPasP.

applyGate :: Element -> QBit -> QBit

Vstup: Hradlo a bit, ktorý daným hradlom prechádza.
Výstup: Nový stav po prechode hradlom.
Popis: Funkcia vykonáva operáciu |* so správnymi hradlami. Slúži vpodstate na preklad z typu Element na typ [[Complex Double]].

toBin :: Int -> [Int]

Vstup: Celé číslo v desiatkovej sústave.
Výstup: List reprezentujúci binárne číslo.
Popis: Funkcia slúži na prevod medzi desiatkovou a dvojkovou sústavou.

formatBin len n

Vstup: Požadovaná dĺžka.
Výstup: Binárne číslo.
Popis: Funkcia formátuje binárne číslo na správnu veľkosť. Pridáva nuly na začiatok až kým číslo nemá správnu veľkosť.

createResList :: Int -> [[Int]]

Vstup: Počet kvantových bitov v obvode.
Výstup: Tabuľka možných výsledkov.
Popis: Funkcia slúži na vytvorenie všetkych možností n bitového binárneho čísla. Vracia všetky možné prípady, ktoré by kolabovaním mohli nastať.

collapseStates :: States -> T

Vstup: Stavy, ktoré majú byť kolabované.
Výstup: Meranie v danom časovom úseku.
Popis: Funkcia vytvorí list s výsledkami pre každú možnosť, ktorá môže nastať.

createRList :: States -> [Int] -> R

Vstup: Stavy, ktoré majú byť kolabované a binárne číslo popisujúce skolabovaný stav.
Výstup: Výsledok pre daný stav.
Popis: Funkcia slúžiaca na konštrukciu výsledku pre daný stav.

calculateProbs :: States -> [Int] -> [Double]

Vstup: Stavy, ktoré majú byť kolabované a binárne číslo popisujúce skolabovaý stav.
Výstup: List pravdepodobností.
Popis: Funkcia zavolá prepočet pravdepodobnosti kolabovania do stavov $|0\rangle$ alebo $|1\rangle$ a vráti ich list.

calcP :: QBit -> Int -> Double

Vstup: Stav kvantového bitu a požadovaný skolabovaný stav.
Výstup: Pravdepodobnosť skolabovania do daného stavu.
Popis: Vracia pravdepodobnosť, že daný kvantový bit skolabuje do daného stavu 0 alebo 1.

isRgt0 :: R -> Bool

Vstup: Výsledok.
Výstup: Indikátor možnosti dosiahnutia daného výsledku.
Popis: Funkcia vracia True, ak pravdepodobnosť daného výsledku je viac ako 0.

mulR :: Double -> R -> R

Vstup: Násobiteľ a výsledok, ktorý má byť násobený.
Výstup: Vynásobený výsledok.
Popis: Vracia nový výsledok kde pôvodná pravdepodobnosť je vynásobená vstupom.