Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE

Juraj Šibík

Kvantové výpočty

Katedra chemické fyziky a optiky

Vedoucí bakalářské práce: Prof. RNDr. Lubomír Skála, DrSc.

Studijní program: Obecná fyzika

2008

Rád by som poďakoval vedúcemu bakalárskej práce Prof. RNDr. Lubomírovi Skálovi, DrSc. za jeho podporu a spoluprácu pri vypracovávaní tejto bakalárskej práce.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a jejím zveřejňováním.

V Praze dne Juraj Šibík

Obsah

Název práce: Kvantové výpočty
Autor: Juraj Šibík
Katedra (ústav): Katedra chemické fyziky a optiky
Vedoucí bakalářské práce: Prof. RNDr. Lubomír Skála, DrSc.
e-mail vedoucího: Lubomir.Skala@mff.cuni.cz

Abstrakt: Cieľom tejto práce je podať základné informácie o princípoch kvantových počítačov. Ukážeme, v čom spočíva rozdiel medzi klasickým a kvantovým počítačom. Definujeme pojmy ako kvantový bit, kvantový register, kvantové hradlo a kvantový obvod. Bližšie sa zaoberáme problematikou kvantových operácií. Najskôr zavedieme základné operácie pôsobiace na jeden kvantový bit, rozšírime ich o kontrolované operácie a nakoniec ukážeme postup, ako môžeme poskladať ľubovolnú ďalšiu operáciu. Popíšeme, ako funguje kvantový paralelizmus. Venujeme sa kvantovej Fourierovej transformácii a jej aplikáciam. Zaoberáme sa zložitosťou použitých operácií a algoritmov.

Klíčová slova: kvantové počítače, kvantové logické hradlá, kvantová Fourierova transformácia

Title: Quantum computing
Author: Juraj Šibík
Department: Department of Chemical Physics and Optics
Supervisor: Prof. RNDr. Lubomír Skála, DrSc.
Supervisor's e-mail address: Lubomir.Skala@mff.cuni.cz

Abstract: Aim of this thesis is to give basic information on quantum computer principles. We discuss the difference between classical and quantum computers. We define objects like a quantum bit, a quantum register, a quantum gate and quantum circuit. We give detailed view on quantum operations. Starting with basic quantum operations on one quantum bit and adding controlled operations we show how one can perform any other operation. We describe the idea of quantum parallelism. We devote some time to the quantum Fourier transform and its applications. We occupy ourselves with the complexity of operations and algorithms being used.

Keywords: quantum computers, quantum logic gates, quantum Fourier transform

Úvod

12. augusta 1981 predstavila spoločnosť IBM prvý úspešný model osobného počítača s názvom IBM PC 5150. Jeho procesor pracoval na frekvencii 4,77 MHz a počítač obsahoval maximálne 256 kB RAM.

Odvtedy sa vývoj počítačov dostal dopredu. Miniaturizácia súčiastok umožnila zväčšiť pamäť a rýchlosť počítača. Tendencia zmenšovania ale má svoje hranice. Pri dosiahnutí atomárnych rozmerov sa objekty prestávajú správať klasicky a k slovu sa dostáva kvantová mechanika. Tá so sebou prináša nové možnosti. Vhodným využitím kvantovej superpozície a interferencie môžeme dosiahnuť exponenciálne urýchlenie výpočtov v porovnaní s klasickým počítačom. Zariadenie, ktoré k tomu budeme používať, nazveme kvantový počítač.

Na čo môžeme využiť výpočetnú silu kvantového počítača? Spomeňme dve aplikácie: diskrétna Fourierova transformácia a prehľadávanie nezotriedenej databázy. Na prvý pohľad nič nové pod Slnkom, veď to dokáže aj klasický počítač. Áno, ale kvantový to dokáže s exponenciálne menším počtom operácií.

Práca je rozdelená na tri kapitoly. V prvej si objasníme základné pojmy ako qubit a kvantové logické hradlo a ukážeme, v čom spočíva rozdiel oproti elementom klasického počítača. Cieľom druhej kapitoly je zaviesť základné kvantové logické operácie a ukázať, ako s nimi môžeme uskutočniť ľubovolnú ďalšiu operáciu. V tretej kapitole ukážeme, v čom spočíva výpočetná sila kvantového počítača a bližšie sa pozrieme na kvantovú Fourierovu transformáciu a jej použitie.

Práca predpokladá základné vedomosti z algebry, logiky a kvantovej mechaniky.

Kapitola 1

Základné pojmy

1.1 Klasický bit, klasický počítač

Klasický bit, skrátene *bit*, predstavuje základnú jednotku informácie. Nadobúda jednu z diskrétnych hodnôt $\{0, 1\}$. Ak spojíme 3 bity, môžeme v nich uchovať hodnoty napr. 101, 010, atď. Triviálna, ale pre nás dôležitá skutočnosť je, že klasický bit nemôže nadobúdať žiadne iné hodnoty.

Pod pojmom *algoritmus* rozumieme konečný deterministický sled krokov, ktorý rieši daný typ problému.

Klasický počítač môžeme interpretovať dvoma spôsobmi: ako Turingov stroj alebo ako zapojenie logických obvodov. Podrobný popis Turingovho stroja je teraz nepodstatný a môžeme ho násjť v [2]. Dôležité je ale nasledujúce tvrdenie [2]:

Tvrdenie 1.1.1 (Churchova - Turingova téza)**.** *Trieda funkcií spočítateľná na Turingovom stroji presne korešponduje s triedou funkcií spočítateľných algoritmom.*

Neformálne povedané, ku každému algoritmu existuje ekvivalentný Turingov stroj. Žiaľ, tézu nemožno brať za definíciu, ale dáva nám dobrú predstavu, čo to znamená, že funkcia je spočítateľná algoritmom.

Iný model klasického počítača je založený na logických obvodoch. Tie sú tvorené logickými hradlami prepojenými elektrickými obvodmi. Tento model má k realite bližšie než model Turingovho stroja, aj keď sú ekviva-

lentné. Vo všeobecnosti, logické hradlo je zariadenie vykonávajúce funkciu f: $\{0,1\}^k \rightarrow \{0,1\}^l$, kde na vstupe je k bitov a na výstupe l bitov. Príkladmi sú hradlá NOT ($\neg$), AND ($\wedge$), OR ($\vee$), vykonávajúce rovnomenné logické operácie. Dá sa ukázať, že všetky hradlá môžu byť poskladané z konečného počtu NAND. Nech a a b sú výrokové atómy. Logicky, a NAND $b \equiv \neg(a \wedge b)$. Ďalej $\neg a \Leftrightarrow \neg(a \wedge a)$; $a \wedge b \Leftrightarrow \neg(\neg(a \wedge b))$ a $a \vee b \Leftrightarrow \neg(\neg a \wedge \neg b)$ (De Morganov zákon). Nakoľko každá výroková formula je ekvivalentná s istou formulou, ktorá je v disjunktívnom normálnom tvare (tj. zložená z výrokových atómov pomocou negácie, disjunkcie a konjunkcie) [5], dôkaz je hotový.

1.2 Kvantový bit, kvantový počítač

Kvantový bit, skrátene *qubit*, je kvantový systém, ktorý reprezentuje hodnoty 0 a 1 pomocou kvantových ortonormálnych stavov $\{|\,0\rangle, |\,1\rangle\}$. Vo všeobecnosti môžeme (čistý) stav qubitu vyjadriť ako $|\,\psi\rangle = \alpha\,|\,0\rangle + \beta\,|\,1\rangle$, kde α a β sú ľubovolné komplexné čísla spĺňajúce normalizačnú podmienku $|\alpha|^2 + |\beta|^2 = 1$. To je základný rozdiel oproti klasickým bitom - qubit môže byť v ľubovolnej superpozícii základných stavov $|\,0\rangle, |\,1\rangle$.

Stavový priestor qubitu je teda dvojdimenzionálny komplexný Hilbertov priestor, označíme ho $\mathscr{H}_q$. Za ortonormálnu bázu môžeme zvoliť $\{|\,0\rangle, |\,1\rangle\}$ (nie nutne) a v maticovom zápise stotožníme

$$|\,0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}; |\,1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}; |\,\psi\rangle = \alpha\,|\,0\rangle + \beta\,|\,1\rangle \equiv \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

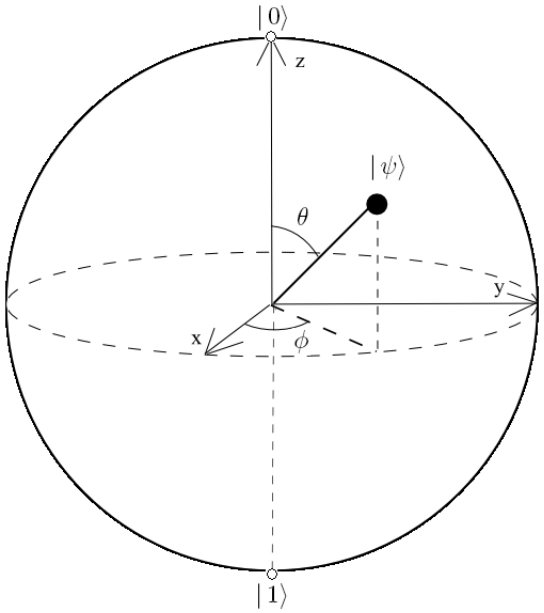
$|\,\psi\rangle$ môžeme vyjadriť aj iným spôsobom:

$$|\,\psi\rangle = \cos\frac{\theta}{2}\,|\,0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|\,1\rangle\,. \tag{1.1}$$

Z matematického hľadiska by mohla exponenciála stáť aj pred $|\,0\rangle$, ale tú vždy môžeme vyňať von z obidvoch členov a postaviť ju do roly globálnej fázy, ktorá nemá vplyv na výsledky fyzikálneho merania.

Vzťah (1.1) nám umožňuje vytvoriť aj geometrickú reprezentáciu qubitu na jednotkovej Poincarého, resp. Blochovej sfére (obr. 1.1).

Ako dobrá fyzikálna predstava qubitu nám môže poslúžiť projekcia spinu



Obr. 1.1: Reprezentácia qubitu na Blochovej sfére

elektrónu do z-ovej osi S_z. Tá môže nadobúdať iba hodnoty $\pm\frac{1}{2}$ a môžeme stotožniť $S_z = +\frac{1}{2} \equiv |\,0\rangle\,, S_z = -\frac{1}{2} \equiv |\,1\rangle$.

Sústavu n qubitov nazývame *kvantový register veľkosti n* [1]. Stav kvantového registra je vyjadrený tenzorovým súčinom stavov jednotlivých qubitov, napríklad $|0\rangle\otimes|1\rangle\otimes|1\rangle$, kde i-ty ket (zľava) reprezentuje stav i-teho qubitu. Pokiaľ nebude hroziť nedorozumenie, budeme používať zjednodušený zápis:

$$|\,0\rangle\otimes|\,1\rangle\otimes|\,1\rangle \equiv |\,0\rangle|\,1\rangle|\,1\rangle \equiv |\,011\rangle \equiv |\,3\rangle\,. \tag{1.2}$$

Posledný stav je zapísaný v desiatkovej sústave.

Stavový priestor kvantového registra veľkosti n je teda tenzorový súčin n priestorov $\mathscr{H}_q$, tj. $\mathscr{H}_q\underbrace{\otimes\ldots\otimes}_{\mathtt{n-krát}}\mathscr{H}_q = \mathscr{H}_q^{\otimes n}$. Tiež ho môžeme zobraziť na sfére, podobne ako v pripade jedného qubitu. Každý qubit nesie so sebou komplexný Hilbertov priestor dimenzie 2. To znamená, že register n qubitov ponesie 2^n-dimenzionálny komplexný Hilbertov priestor, na znázornenie ktorého potrebujeme dvojnásobok reálnych osí, teda 2^{n+1}. Normalizačná podmienka ale znamená jednu väzbu a vo výsledku môžeme kvantový register veľkosti n znázorniť na $(2^{n+1}-1)$-dimenzionálnej sfére.

Nakoľko jeden kvantový bit môže reprezentovať súčasne hodnoty 0 aj 1, ľahko zvážime, že n kvantových bitov môže reprezentovať súčasne všetky hodnoty $0, 1, \ldots, 2^n - 1$. Ľubovolný (čistý) stav kvantového registra veľkosti n môžeme zapísať (v desiatkovej sústave) ako:

$$|\,\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k \,|\,k\rangle\,, \tag{1.3}$$

kde $\alpha_k \in \mathbb{C}$ a $\sum_{k=0}^{2^n-1} |\alpha_k|^2 = 1$. Musíme si však uvedomiť, že keď sa budeme chcieť pozrieť na výstup, musíme uskutočniť meranie na qubitoch. Tým spôsobíme kolaps vlnových funkcií qubitov a kvantový register bude reprezentovať iba jednu z možných hodnôt.

Na *kvantový počítač* sa budeme pozerať ako na prístroj pozostávajúci z kvantových logických obvodov. Podobne, ako u klasického logického obvodu, *kvantový logický obvod* pozostáva z kvantových logických hradiel synchronizovaných v čase a spojovacích kanálov.

Kvantové logické hradlo je zariadenie, ktoré vykonáva pevne danú unitárnu operáciu na vybraných qubitoch s pevne danou periódou [4]. Ak je na vstupe hradla n qubitov, hradlo nazveme *n-qubitové*.

Vývoj uzatvoreného kvantového systému je popísaný evolučným operátorom, ktorý je unitárny [3], tj. zachováva skalárny súčin. Unitárnosť má za následok, že (kvantová) evolúcia je reverzibilný proces. Kvantové hradlá predstavujú určitý kvantový vývoj qubitu. Preto požadujeme, aby aj operácie, ktoré uskutočňujú, boli unitárne. To je zásadný rozdiel oproti klasickým logickým operáciam. Niektoré z nich nie sú vratné a preto nemôžeme nájsť ich kvantovú obdobu. Môžeme ich ale zakomponovať do viacbitových, no vratných hradiel. To znamená, že niekedy budeme potrebovať na vykonanie operácie aj pracovné qubity v pevne daných stavoch. V maticovej reprezentácii budú n-qubitové kvantové hradlá unitárne matice typu $n \otimes n$.

Vynára sa otázka, či existuje univerzálna sada kvantových logických hradiel, ktoré by boli schopné uskutočniť ľubovolnú kvantovú logickú operáciu. V druhej kapitole ukážeme, že áno, avšak realizácia so sebou nesie technické problémy.

1.3 Meranie qubitu

Dôležitým faktom je, že dva neortogonálne kvantové stavy nedokážeme od seba s určitosťou odlíšiť. Dôvod je zrejmý. Uvažujme dva neortogonálne stavy (napr. qubitu) $|\psi_1\rangle$, $|\psi_2\rangle$. Neortogonalita znamená, že $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$, kde $|\alpha|^2, |\beta|^2 > 0$ (samozrejme je splnená normalizačná podmienka) a $\langle\psi_1|\varphi\rangle = 0$ (ortogonálne stavy). S určitou pravdepodobnosťou teda dostaneme meraním $|\psi_1\rangle$ a $|\psi_2\rangle$ rovnaké výsledk a stavy budú vtedy nerozlíšiteľné.

Za bázu qubitu preto volíme dvojicu ortogonálnych stavov. Výpočetná báza $\{|0\rangle, |1\rangle\}$ má svoj význam z hľadiska teórie informácie. V závislosti od experimentálnej realizácie kvantového počítača môžeme použiť aj iné bázy. $|0\rangle$, $|1\rangle$ môžu reprezentovať spin elektrónu „hore" $\left(+\frac{1}{2}\right)$, „dolu" $\left(-\frac{1}{2}\right)$, prípadne horizontálnu $|H\rangle \equiv |0\rangle$ a vertikálnu $|V\rangle \equiv |1\rangle$ polarizáciu fotónu. Naproti tomu, stavy $|L\rangle \equiv \frac{|H\rangle + i|V\rangle}{\sqrt{2}}, |R\rangle \equiv \frac{|H\rangle - i|V\rangle}{\sqrt{2}}$ si môžeme predstaviť ako ľavotočivé a pravotočivé kruhovo polarizované svetlo.

Jeden z postulátov kvantovej mechaniky (o redukcii vlnovej funkcie, [3]) hovorí, že meranie veličiny A s príslušným operátorom $\widehat{A}$ prevedie meraný systém do vlastného stavu tohoto operátora. V prípade qubitu to znamená, že po meraní ponesie iba klasickú informáciu. Kvantové meranie je v určitom zmysle mysteriózny proces. Je nelokálny, nedeterministický, neunitárny, nelineárny, nevratný a pre nekompatibilné veličiny závisí na poradí ich merania.

Na čo potrebujeme merať výstup z kvantového počítača? Odpoveď je jasná, na zistenie výsledku výpočtu. Zrejmé, no zaujímavé je, že meranie môžeme vždy presunúť až na koniec kvantového výpočtu. Ak sa výsledky merania používajú niekde vo výpočte, vždy môžeme použiť kontrolované operácie a tým sa meraniu vyhnúť. Vďaka tomu môže príslušný obvod zostať reverzibilný.

Pre meranie qubitov budeme používať symbol  .

1.4 Zložitosť

Pre porovnanie zložitosti algoritmov a efektivity kvantových obvodov budeme potrebovať dva symboly.

„Veľké" O určuje horný odhad funkcie. Nech $f(n)$ a $g(n)$ sú dve funkcie na nezáporných celých číslach. Hovoríme, že $f(n)$ je v $O(g(n))$, pokiaľ existujú konštanty c a n_0 také, že pre všetky $n > n_0$ je $f(n) \leq cg(n)$.

„Veľké" Ω bude označovať dolný odhad funkcie. Funkcia $f(n)$ je $\Omega(g(n))$, ak existujú konštanty c a n_0 také, že pre všetky $n > n_0$ je $cg(n) \leq f(n)$.

Problém pokladáme za ľahký (riešiteľný efektívnym spôsobom), ak je možné vyriešiť ho s $O(p(n))$ základných operácií (tiež môžeme hovoriť, že časová náročnosť je $O(p(n))$), kde n je počet bitov na vstupe a $p(n)$ je polynomiálna funkcia. Príkladom sú základné aritmetické operácie ako sčítanie, násobenie, delenie.

Ak je najlepší algoritmus na vyriešenie daného problému exponenciálny v n, problém pokladáme za ťažký (neriešiteľný efektívnym spôsobom). Za takýto problém sa pokladá napríklad faktorizácia prirodzeného čísla (rozklad na prvočíselný súčin), aj keď toto tvrdenie ešte nebolo dokázané.

Kapitola 2

Kvantové logické hradlá

Pri písaní tejto kapitoly sme vo veľkom čerpali z [2].
Operátor identity budeme značiť I. Pre ľubovolný stav qubitu, resp. kvantového registra platí:

$$I \left| x \right\rangle = \left| x \right\rangle . \tag{2.1}$$

2.1 Jednoqubitové hradlá

Keďže stavový priestor qubitu má dimenziu 2, operácie na jednotlivých qubitoch budú popísané unitárnymi maticami typu 2×2. Dôležité jednoqubitové hradlá sú tieto:

- Hadamardovo hradlo
- fázové hradlo
- Pauliho-X hradlo
- Pauliho-Y hradlo
- Pauliho-Z hradlo

Hadamardovo hradlo

Hadamardovo hradlo H vykonáva Hadamardovu transformáciu na qubite. V ortonormálnej báze $\{\left| 0 \right\rangle, \left| 1 \right\rangle\}$ má príslušná matica vyjadrenie:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \left| x \right\rangle — \boxed{H} — (-1)^x \left| x \right\rangle + \left| 1 - x \right\rangle \tag{2.2}$$

Diagram vpravo od matice znázorňuje účinok hradla H na qubit v stave $|\,x\rangle$, kde $x = 0, 1$ [1].

Všimnime si špeciálny prípad, keď je na vstupe $|\,0\rangle$:

$$|\,0\rangle \;\text{—}\boxed{H}\text{—}\; \tfrac{|\,0\rangle+|\,1\rangle}{\sqrt{2}} \tag{2.3}$$

Na výstupe dostaneme superpozíciu $|\,0\rangle$ a $|\,1\rangle$. Tento stav qubitu predstavuje jeden zo základných nebázových kvantových stavov. Jeho význam spočíva v tom, že pri meraní môže nadobudnúť s rovnakou pravdepodobnosťou obidve možné logické hodnoty.

Fázové hradlo

Fázové hradlo ϕ mení fázu časti stavu qubitu odpovedajúcej $|\,1\rangle$ o ϕ. Maticové vyjadrenie hradla je [1]:

$$\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix} \qquad\qquad |\,x\rangle \xrightarrow{\;\phi\;} e^{ixy\phi}\,|\,x\rangle \tag{2.4}$$

Univerzalita Hadamardovho a fázového hradla

Spojením dvoch Hadamardových a dvoch fázových hradiel môžeme vygenerovať ľubovoľný stav qubitu:

$$|\,0\rangle \;\text{—}\boxed{\text{H}}\xrightarrow{\;\theta\;}\boxed{\text{H}}\xrightarrow{\;\frac{\pi}{2}+\phi\;} \cos\frac{\theta}{2}\,|\,0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|\,1\rangle\,. \tag{2.5}$$

Overenie:

$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\left(\frac{\pi}{2}+\phi\right)} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} =$$

$$\frac{1}{2} \begin{bmatrix} 1 + e^{i\theta} \\ e^{\frac{\pi}{2}+\phi}(1 - e^{i\theta}) \end{bmatrix} = e^{i\frac{\theta}{2}} \begin{bmatrix} \cos\frac{\theta}{2} \\ e^{\phi}\sin\frac{\theta}{2} \end{bmatrix}$$

Nakoľko na globálnej fáze qubitu nezáleží, Hadamardovo hradlo a vhodné fázové hradlá môžu skutočne reprezentovať ľubovolné ďalšie hradlo pôsobiace na jeden qubit.

Pauliho-X,Y,Z hradlá

Pauliho matice sú užitočné, pretože pomocou nich môžeme rotovať vektory.

Hradlá X, Y, Z sú významné preto, lebo v maticovej reprezentácii im odpovedajú práve Pauliho matice:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad |\,x\rangle \text{—}\boxed{X}\text{—} \; |\,1-x\rangle\,, \tag{2.6}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad |\,x\rangle \text{—}\boxed{Y}\text{—} \; i(-1)^x\,|\,1-x\rangle\,, \tag{2.7}$$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad |\,x\rangle \text{—}\boxed{Z}\text{—} \; (-1)^x\,|\,x\rangle\,. \tag{2.8}$$

Operátory rotácii okolo osí $\vec{x}, \vec{y}, \vec{z}$ o uhol θ definujeme nasledovne:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{2.9}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}, \tag{2.10}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \tag{2.11}$$

Význam rotácii je zrejmý; unitárne operácie predstavujú vo všeobecnosti rotácie. Euler ale ukázal, že rotáciu okolo ľubovolnej osi môžeme poskladať s použitím iba rotácii okolo dvoch rôznobežných osí.

To môžeme využiť pri kvantových hradlách. Unitárne operácie na qubitoch predstavujú rotácie na Blochovej sfére. Ak za rôznobežné osi vezmeme y-ovú a z-ovú os (tzv. *Z-Y rozklad* pre qubit), pre operáciu U na jednom qubite platí:

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta), \tag{2.12}$$

pre vhodné $\alpha, \beta, \gamma, \delta$. Dôkaz je jednoduchý, stačí do rovnice (2.12) dosadiť vyjadrenia z rovníc (2.10) a (2.11), potom

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\frac{\gamma}{2} \end{bmatrix} \tag{2.13}$$

Nakoľko riadky aj stĺpce U sú ortonormálne, U je unitárna. Užitočné bude aj nasledujúce tvrdenie:

Tvrdenie 2.1.1. *Nech U je unitárne jednoqubitové hradlo. Potom existujú unitárne jedno-qubitové operátory A, B, C také, že $ABC = I$ a $U = e^{i\alpha} AXBXC$, kde α je globálny fázový faktor.*

Toto tvrdenie spolu s dôkazom môžeme násjť v [2]. Podotknime, že v značení podľa (2.12) bude

$$A \equiv R_z(\beta)R_y(\gamma/2), \tag{2.14}$$

$$B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2), \tag{2.15}$$

$$C \equiv R_z((\delta-\beta)/2). \tag{2.16}$$

Tvrdenie 2.1.1 použijeme pri budovaní kontrolovaných hradiel.

Príklad: Nájdime A, B, C a α pre Hadamardovo hradlo.

Riešenie: Najskôr určime α, β, γ a δ v rovnici (2.13), kde $U = H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$: $\alpha = \pi/2, \beta = 0, \gamma = \pi/2, \delta = \pi$. Potom

$A = R_z(0)R_y(\pi/4) = \begin{bmatrix} \cos\frac{\pi}{8} & -\sin\frac{\pi}{8} \\ \sin\frac{\pi}{8} & \cos\frac{\pi}{8} \end{bmatrix}$,

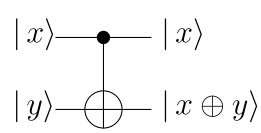
$B = R_y(-\pi/4)R_z(-\pi/2) = \begin{bmatrix} \cos\frac{\pi}{8}e^{i\pi/4} & \sin\frac{\pi}{8}e^{-i\pi/4} \\ -\sin\frac{\pi}{8}e^{i\pi/4} & \cos\frac{\pi}{8}e^{-i\pi/4} \end{bmatrix}$,

$C = R_z(\pi/2) = \begin{bmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$.

2.2 Kontrolované hradlá

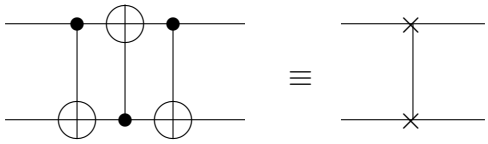
Veľmi dôležité kontrolované hradlo je kontrolovaná negácia, C-NOT. Na vstupe C-NOT sú dva qubity, kontrolný a cieľový. Ak je kontrolný qubit v stave $|1\rangle$, cieľový qubit sa zneguje. Ak je kontrolný qubit v stave $|0\rangle$, cieľový qubit sa nezmení. Hradlu C-NOT odpovedá nasledujúca matica a diagram:

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{2.17}$$



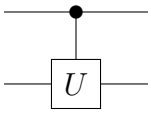
kde $x, y = 0$ alebo 1 a $\oplus$ značí sčítanie modulo 2 (XOR) [1]. Pomocou C-NOT hradiel môžeme zostrojiť obvod, ktorý zamení dva qubity, tzv. *swap* (obr. 2.1).

Ukážme si postup, ako môžeme zostrojiť kontrolované-U hradlo, kde U je ľubovolná unitárna matica 2×2. Príslušný diagram je na obr. 2.2. Budeme potrebovať hradlo, ktoré v prípade, že kontrolný qubit je $|1\rangle$, posunie fázu

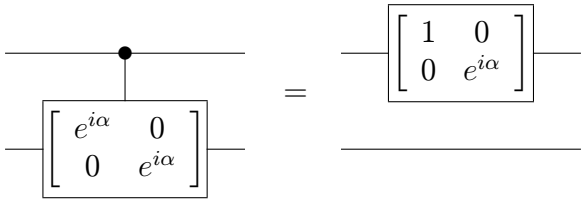


Obr. 2.1: Obvod vykonávajúci zámenu dvoch qubitov

cieľového qubitu o α, teda prenásobí cieľový qubit faktorom $e^{i\alpha}$. Obvod, ktorý toto uskutoční, je možné poskladať s použitím jednoqubitového fázového hradla (obr. 2.3).



Obr. 2.2: Kontrolované-U



Obr. 2.3: Kontrolovaný posun fázy a jeho ekvivalentný obvod pre dva qubity.

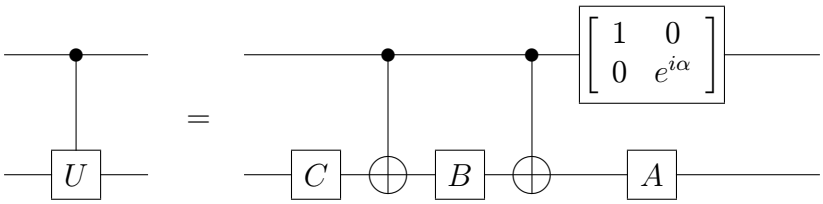
Ak si uvedomíme, že hradlo X pôsobí ako negácia a využijeme tvrdenie 2.1.1, môžeme skonštruovať obvod na obr. 2.4.

Problém kontrolovaného-U hradla môžeme zovšeobecniť: Majme n kontrolných qubitov a nech U je unitárny operátor pôsobiaci na k qubitov (obr. 2.5). Potom definujeme $C^n(U)$ operáciu ako

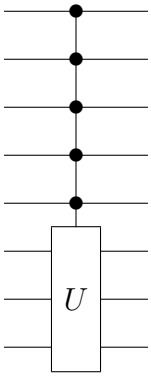
$$C^n(U)\,|\,x_1x_2\ldots x_n\rangle\,|\,\psi\rangle = |\,x_1x_2\ldots x_n\rangle\,U^{x_1x_2\ldots x_n}\,|\,\psi\rangle\,, \tag{2.18}$$

kde $x_1x_2\ldots x_n$ v exponente je súčin hodnôt $x_1, x_2, \ldots, x_n$. Význam je jasný - ak pre každé $i = 1, \ldots, n$ platí $x_i = 1$, tak na cieľové qubity aplikujeme U, ak aspoň pre jedno i platí $x_i = 0$, cieľové qubity zostanú nezmenené. Podotknime, že $|\,\psi\rangle \in \mathscr{H}_q^{\otimes k}$.

Významné kontrolované hradlé sú *Fredkin* a *Toffoli* hradlá. *Fredkin hradlo* (obr. 2.6) vykonáva kontrolovaný swap, teda ak je kontrolný qubit v stave

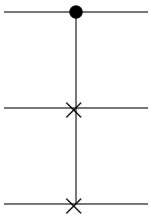


Obr. 2.4: Obvod, ktorý vykonáva kontrolované-U. Ak je kontrolný qubit $|\,0\rangle$, na cieľový qubit pôsobí $ABC = I$.



Obr. 2.5: Obvod, ktorý vykonáva $C^n - U$, kde U pôsobí na k qubitov; $n = 5$ a $k = 3$.

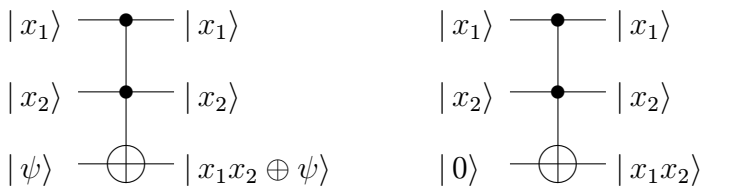
$|\,1\rangle$, tak dva cieľové qubity vymení, ak je kontrolovaný qubit v stave $|\,0\rangle$, nechá cieľové qubity nezmenené. Klasické Fredkin hradlo je ďalšie reverzibilné a univerzálne hradlo.



Obr. 2.6: Fredkin hradlo, kontrolovaný-swap

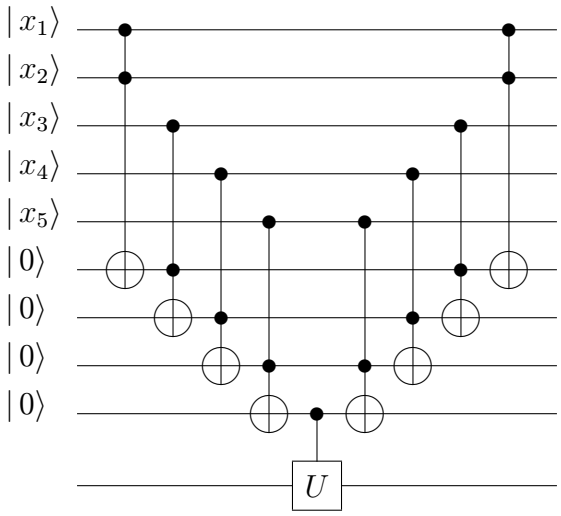
Toffoli hradlo, resp. $C^2 - NOT$ (kontrolovaná kontrolovaná negácia), vykoná negáciu cieľového qubitu, ak sú kontrolné qubity v stave $|\,x_1\rangle|\,x_2\rangle = |\,1\rangle|\,1\rangle$. Ak je cieľový qubit na začiatku v stave $|\,\psi\rangle = |\,0\rangle$, na výstupe je v stave $|\,\psi\rangle = |\,x_1 \wedge |\,x_2\rangle\rangle$ (obr. 2.7). Takto sme schopní uskutočniť logickú operáciu AND, ktorá je klasicky irreverzibilná. Na druhú stranu, ak je na vstupe cieľový qubit v stave $|\,1\rangle$, Toffoli hradlo sa správa ako NAND hradlo. Nakoľko NAND hradlo je univerzálne pre klasické výpočty (viď podkapitolu 1.1), bude aj Toffoli hradlo univerzálne (pre klasické výpočty). Dokonca sa dá

ukázať, že Hadamardovo a Toffoli hradlo tvoria univerzálnu sadu hradiel pre kvantové výpočty [6].



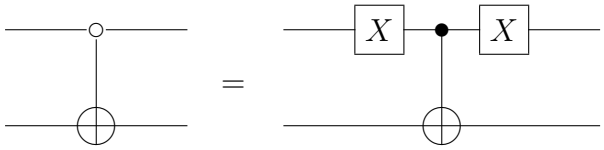
Obr. 2.7: Toffoli hradlo a špeciálny prípad so vstupom $|\psi\rangle = |0\rangle$

Pomocou Toffoli hradiel môžeme vytvoriť obvod $C^n(U)$, kde U pôsobí na jeden qubit (a hradlo U môžeme vytvoriť zo základných jednoqubitových hradiel)(obr. 2.8). Pri implementácii budeme naviac potrebovať $n-1$ pracovných qubitov, ktoré budú na vstupe aj na výstupe v stave $|0\rangle$.



Obr. 2.8: Kvantový obvod vykonávajúci $C^n(U)$ pre $n = 5$ a U pôsobiace na jeden qubit.

Na koniec podkapitoly zavedieme obdobou C-NOT hradla. Hradlo C-NOT negovalo cieľový qubit, ak bol kontrolný v stave $|1\rangle$. Voľba stavu kontrolného qubitu je de facto na nás, a preto môžeme zostrojiť aj kontrolované hradlo, ktoré neguje cieľový qubit v prípade, že kontrolný qubit je v stave $|0\rangle$ a nerobí nič, ak je kontrolný qubit v stave $|1\rangle$. Takéto hradlo je znázornené na obr. 2.9.



Obr. 2.9: Kontrolovaná negácia s opačnou podmienkou.

2.3 Univerzálne hradlo

Predstavme si unitárnu maticu U, ktorá pôsobí na 3-dimenzionálnom Hilbertovom priestore (kvantové hradlo s 3 vstupmi). Táto matica sa dá rozložiť na súčin *dvojúrovňových matíc*, tj. matíc netriviálne pôsobiacich na dve a menej zložiek vektora, nasledujúcim spôsobom:

Nech

$$U = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \tag{2.19}$$

Našim cieľom je nájsť dvoj-úrovňové matice U_1, U_2, U_3 tak, aby

$$U_3 U_2 U_1 U = I, \tag{2.20}$$

kde I je jednotková matica. Využitím unitarity U dostaneme:

$$U = U_1^\dagger U_2^\dagger U_3^\dagger. \tag{2.21}$$

Postupujme nasledovne:

$$a_{21} \begin{cases} = 0;\ U_1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ \\ \neq 0;\ U_1 \equiv \begin{bmatrix} \frac{a_{11}^*}{\sqrt{\left|a_{11}^2\right|+\left|a_{21}^2\right|}} & \frac{a_{21}^*}{\sqrt{\left|a_{11}^2\right|+\left|a_{21}^2\right|}} & 0 \\ \frac{a_{21}}{\sqrt{\left|a_{11}^2\right|+\left|a_{21}^2\right|}} & \frac{-a_{11}}{\sqrt{\left|a_{11}^2\right|+\left|a_{21}^2\right|}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \end{cases} \tag{2.22}$$

Potom

$$U_1 U = \begin{bmatrix} a'_{11} & a'_{12} & a'_{13} \\ 0 & a'_{22} & a'_{23} \\ a'_{31} & a'_{32} & a'_{33} \end{bmatrix}, \tag{2.23}$$

teda v druhom riadku na prvom mieste bude 0. Presné hodnoty ďalších elementov nie sú podstatné.

Podobným postupom nájdime U_2:

$$a'_{31}\begin{cases} = 0;\ U_2 \equiv \begin{bmatrix} a'^{*}_{11} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \\ \neq 0;\ U_2 \equiv \begin{bmatrix} \frac{a'^{*}_{11}}{\sqrt{|a'^{2}_{11}|+|a'^{2}_{31}|}} & 0 & \frac{a'^{*}_{31}}{\sqrt{|a'^{2}|+|a'^{2}_{31}|}} \\ 0 & 1 & 0 \\ \frac{a'_{31}}{\sqrt{|a'^{2}_{11}|+|a'^{2}_{31}|}} & 0 & \frac{-a'_{11}}{\sqrt{|a'^{2}_{11}|+|a'^{2}_{31}|}} \end{bmatrix} \end{cases} \tag{2.24}$$

Tým dosiahneme, že súčin U_2U_1U bude mať nulu aj v ľavom dolnom rohu:

$$U_2U_1U = \begin{bmatrix} 1 & a''_{12} & a''_{13} \\ 0 & a''_{22} & a''_{23} \\ 0 & a''_{32} & a''_{33} \end{bmatrix} = \begin{bmatrix} 1 & a''_{12} & a''_{13} \\ 0 & a''_{22} & a''_{23} \\ 0 & a''_{32} & a''_{33} \end{bmatrix} \tag{2.25}$$

Keďže U_2, U_1 aj U, musí byť aj U_2U_1U unitárna a teda požadujeme $a''_{12} = 0$, $a''_{13} = 0$ (riadky, resp. stĺpce unitárnej matice musia mať normu rovnú 1).

Nakoniec určíme U_3:

$$U_3 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & a''^{*}_{22} & a''^{*}_{23} \\ 0 & a''^{*}_{32} & a''^{*}_{33} \end{bmatrix} \tag{2.26}$$

Ľahko overíme, že $U_3U_2U_1U = I$. Takže dostávame $U = U_1^{\dagger}U_2^{\dagger}U_3^{\dagger}$.

Uvedený postup môžeme použiť aj na matice typu $d \times d$. Nájdeme dvojúrovňové matice $U_1, \ldots, U_{d-1}$ tak, že súčin $U_{d-1}U_{d-2}\ldots U_1U$ má jednotku v ľavom hornom rohu a zvyšné prvky prvého riadka a stĺpca nulové. Takto postupujeme ďalej pre maticu $(d-1) \times (d-1)$. U dostaneme ako súčin k dvojúrovňových matíc, kde

$$k \leq (d-1) + (d-2) + \ldots + 1 = d(d-1)/2 \tag{2.27}$$

Hradlá pôsobiace na n qubitov sú reprezentované maticami rádu 2^n, takže vo výsledku ich môžeme nahradiť $2^{n-1}(2^n - 1)$ dvojbitovými hradlami. Toto je horný odhad a v špeciálnych prípadoch môže byť samozrejme počet hradiel menší.

Zostáva ešte vyriešiť implementáciu dvojúrovňových hradiel pôsobiacich na n qubitov (z toho na $n-2$ qubitov triviálne, identicky). Použijeme na to jednoqubitové hradlá, C-NOT a *Šedé kódy*[1]. Predstavme si dva rozdielne n-bitové reťazce, s a t. *Šedý kód* je postupnosť binárnych reťazcov začínajúca s a končiaca t, pričom každý nasledujúci člen postupnosti sa od predchádzajúceho líši iba o jeden bit. Ďalej uvažujme maticu $\widetilde{U}$ ako netriviálnu podmaticu U typu 2×2 a $g_1, g_2, \ldots, g_m$ nech predstavuje Šedý kód, pričom $g_1 = s$, $g_m = t$ a $m \leq n+1$. Myšlienka je nasledovná. Najskôr vykonáme zmeny $|\, g_1\rangle \rightarrow |\, g_2\rangle \rightarrow \ldots \rightarrow |\, g_{m-1}\rangle$, potom zapôsobíme kontrolovaným-$\widetilde{U}$ pôsobiacim na qubit, v ktorom sa líši $|\, g_{m-1}\rangle$ a $|\, g_m\rangle$ a vrátime späť zmeny vykonané na ostatných qubitoch, tj. $|\, g_{m-1}\rangle \rightarrow |\, g_{m-2}\rangle \rightarrow \ldots \rightarrow |\, g_1\rangle$. Ukážme si to na príklade.

Príklad: Navrhnime obvod na implementáciu operácie

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix},$$

pričom a, b, c, a d sú komplexné čísla také, že $\widetilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$ je unitárna matica.

Riešenie: U pôsobí netriviálne iba na stavy $|\, 000\rangle$ a $|\, 111\rangle$. Šedý kód spájajúci 000 a 111 je:

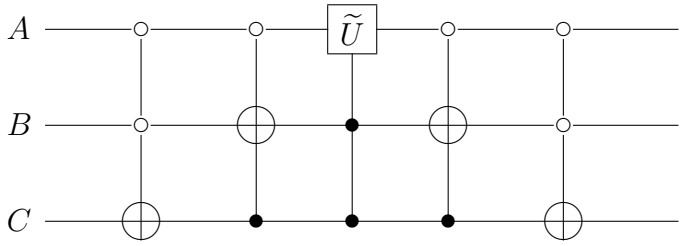
A	B	C
0	0	0
0	0	1
0	1	1
1	1	1

.

Obvod pre implementáciu je znázornený na obr. 2.10. Najskôr zameníme

[1] Anglický názov je *Gray codes*. Autor bakalárskej práce sa s týmto pojmom stretol prvý krát a preto sa uchýlil k doslovnému prekladu.

stav $|000\rangle$ za $|011\rangle$, potom zapôsobíme $\widetilde{U}$ na prvý qubit stavov $|011\rangle$ a $|111\rangle$ a vrátime späť $|011\rangle$ do stavu $|000\rangle$.



Obr. 2.10: Obvod implementujúci zadané U

2.4 Náročnosť a aproximácie

Štandardná sada univerzálnych hradiel pozostáva z Hadamardovho, fázového a C-NOT hradla. Odhadnime, koľko takýchto hradiel potrebujeme na vykonanie ľubovolnej operácie U na n qubitoch. Ako sme ukázali pred pár riadkami, každú takúto operáciu môžeme vykonať pomocou $O(2^{2n}) = O(4^n)$ dvojúrovňových matíc. Pre dvojúrovňovú maticu bude implementácia Šedého kódu vo všeobecnosti vyžadovať $2(n-1)$ kontrolovaných operácií, pričom každú z nich môžeme realizovať pomocou $O(n)$ jednoqubitových a C-NOT hradiel. Kontrolované-$\widetilde{U}$ tiež vyžaduje $O(n)$ hradiel. Dohromady teda implementácia ľubovolnej operácie U na n qubitoch vyžaduje $O(n^2 4^n)$ jednoqubitových a C-NOT hradiel, čo je exponenciálne mnoho.

Nakoľko je množina unitárnych operácií spojitá, je zrejmé, že diskrétna sada unitárnych operácií nemôže simulovať všetky operácie úplne presne, ale môže ich dostatočne presne aproximovať. Chybu, kedy operácia V nahradí (aproximuje) operáciu U definujeme takto:

$$E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)\,|\psi\rangle\| \tag{2.28}$$

Dá sa ukázať, že ak $E(U,V)$ bude malé, tak ľubovolné meranie uskutočnené na stave $V\,|\psi\rangle$ dá približne rovnaké štatistické výsledky, ako meranie na stave $U\,|\psi\rangle$, kde $|\psi\rangle$ je inicializačný stav. Aká je efektivita aproximácie operácií s použitím diskrétnej sady hradiel? Podľa Solovayovho-Kitaevovho teorému sa ľubovolná jednoqubitová operácia dá aproximovať použitím $O(log^c\,(1/\epsilon))$ hradiel z diskrétnej sady, kde ϵ je požadovaná presnosť ($E(U,V) \leq \epsilon$). Problémom ale je, že niektoré n-qubitové operácie nie

je možné aproximovať efektívnejšie, ako s použitím $\Omega(2^n \log(1/\epsilon) / \log(n))$ operácií, čo je opäť exponenciálna závislosť na n.

Veľký počet hradiel nesie so sebou technické problémy. Okrem výpočetných chýb je to aj priestorová a časová náročnosť, čo má za následok väčšiu náchylnosť na chyby vzniknuté dekoherenciou qubitov. Exponenciálna náročnosť dáva aj odpoveď na otázku, prečo sa neuspokojíme iba so štandardnou sadou univerzálnych hradiel. Podľa problému, ktorý riešime, môžeme zostrojiť ďalšie a ďalšie hradlá na zefektívnenie výpočtu. Príkladom toho môžu byť práve Toffoli a Fredkin hradlá, ktoré sa dajú vyrobiť ako samostatné objekty. Ich konštrukcia je popísaná napríklad v [7]. Druhým parametrom charakterizujúci kvantový obvod je počet pomocných qubitov. Samozrejme, tiež požadujeme ich minimum.

Kapitola 3

Aplikácie kvantového počítača

3.1 Kvantový paralelizmus

Superpozícia stavov kvantového registra je kľúč ku *kvantovému paralelizmu*. Predstavme si jednobitovú funkciu $f(x) : \{0,1\} \to \{0,1\}$. Principiálne sme schopní zostrojiť dvojqubitové hradlo U_f, ktoré z počiatočný stav qubitov $|\,x\rangle\,|\,y\rangle$ prevedie na $|\,x\rangle\,|\,y \oplus f(x)\rangle$. Špeciálne pre $|\,y\rangle = |\,0\rangle$ dostaneme na výstupe $|\,x\rangle\,|\,f(x)\rangle$. To znamená:

$$\frac{(|\,0\rangle+|\,1\rangle)}{\sqrt{2}}\,|\,0\rangle \quad \text{---}\boxed{U_f}\text{---} \quad \frac{|\,0\rangle|\,f(0)\rangle+|\,1\rangle|\,f(1)\rangle}{\sqrt{2}}. \tag{3.1}$$

S využitím superpozície sme mohli uskutočniť v jednom cykle výpočet $f(x)$ pre obidve možné hodnoty $x = 0, 1$. Tento príklad môžeme zovšeobecniť. Predstavme si funkciu $f(x) : \{0,1\}^n \to \{0,1\}$ a hradlo U_f pôsobiace na kvantový register veľkosti $n+1$, ktoré stav $|\,x\rangle\,|\,y\rangle$ zobrazí na stav $|\,x\rangle\,|\,y \oplus f(x)\rangle$, $x \in \{0,1\}^n \equiv \{0, 1, \ldots, 2^n - 1\}$, $y \in \{0,1\}$. Voľbou stavov $|\,x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\,k\rangle$ (pre prehľadnosť sme radšej zvolili zápis v desiatkovej sústave) a $|\,y\rangle = |\,0\rangle$ dostaneme

$$\frac{\sum_{k=0}^{2^n-1}|\,k\rangle}{\sqrt{2^n}}\,|\,0\rangle \quad \text{---}\boxed{U_f}\text{---} \quad \frac{\sum_{k=0}^{2^n-1}|\,k\rangle|\,f(k)\rangle}{\sqrt{2^n}}. \tag{3.2}$$

V tomto zmysle je rýchlosť výpočtov kvantového počítača exponenciálne rýchlejšia ako počítača klasického - zatiaľ čo klasický počítač musí vypočítať $f(x)$ pre každú hodnotu x zvlášť, kvantový počítač dokáže uskutočniť všetky tieto výpočty paralelne v jednom cykle. Znovu ale pripomíname, že

meraním kvantového registra dostaneme iba jednu hodnotu $|\,x\rangle\,|\,f(x)\rangle$. Paralelizmus má význam iba ak ho správne využijeme. Ak chceme spočítať nejakú hodnotu $f(x)$, môžeme kľudne použiť klasický počítač. To, čo dáva kvantovému počítaču význam, je schopnosť odpovedať na otázky týkajúce sa *vlastností* funkcie $f(x)$. Ukážeme si to na jednoduchom príklade.

3.2 Deutschov algoritmus

Uvažujme funkciu $f(x) : \{0,1\} \to \{0,1\}$. Chceme rozhodnúť, či $f(x)$ je konštantá, tj. $f(0) = f(1)$, alebo nie, tj. $f(0) \neq f(1)$. V klasickom počítači nemáme inú možnosť, ako spočítať hodnoty $f(0)$, $f(1)$ a potom ich porovnať. S využitím kvantového paralelizmu ale môže kvantový počítač vyriešiť tento problém jedným výpočtom.

Zoberme hradlo U_f pôsobiace na 2 qubity, $U_f\,|\,x\rangle\,|\,y\rangle = |\,x\rangle\,|\,y \oplus f(x)\rangle$. Deutschov algoritmus v sebe okrem kvantového paralelizmu využíva aj kvantovú interferenciu, v našom popise reprezentovanú násobením relatívnych fáz jednotlivých qubitov z registra.
Obvod vykonávajúci Deutschov algoritmu je znázornený na obr. 3.1. Postup je nasledovný:

1. Začneme s kvantovým registrom v stave $|\,\psi_1\rangle = |\,0\rangle\,|\,1\rangle$
2. Pomocou Hadamardových hradiel dáme register do stavu $|\,\psi_2\rangle = \left[\frac{|\,0\rangle+|\,1\rangle}{\sqrt{2}}\right]\left[\frac{|\,0\rangle-|\,1\rangle}{\sqrt{2}}\right] = |\,+\rangle\,|\,-\rangle = \frac{|\,00\rangle-|\,01\rangle+|\,10\rangle-|\,11\rangle}{2}$
3. Pôsobením U_f na $|\,\psi_2\rangle$ dostaneme $|\,\psi_3\rangle$:
   $f: \begin{matrix}0\to 0\\ 1\to 0\end{matrix}$ $\quad |\,\psi_3\rangle = \frac{|\,00\rangle-|\,01\rangle+|\,10\rangle-|\,11\rangle}{2} = |\,+\rangle\,|\,-\rangle$

   $f: \begin{matrix}0\to 1\\ 1\to 1\end{matrix}$ $\quad |\,\psi_3\rangle = \frac{|\,01\rangle-|\,00\rangle+|\,11\rangle-|\,10\rangle}{2} = -\,|\,+\rangle\,|\,-\rangle$

   $f: \begin{matrix}0\to 1\\ 1\to 0\end{matrix}$ $\quad |\,\psi_3\rangle = \frac{|\,01\rangle-|\,00\rangle+|\,10\rangle-|\,11\rangle}{2} = -\,|\,-\rangle\,|\,-\rangle$

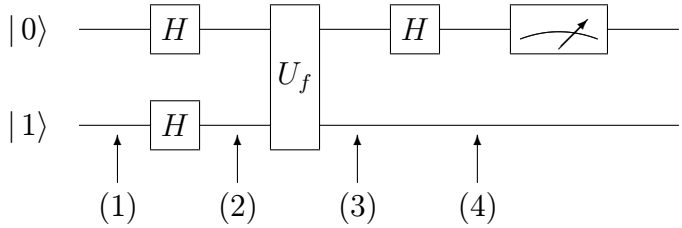
   $f: \begin{matrix}0\to 0\\ 1\to 1\end{matrix}$ $\quad |\,\psi_3\rangle = \frac{|\,00\rangle-|\,01\rangle+|\,11\rangle-|\,10\rangle}{2} = |\,-\rangle\,|\,-\rangle$
4. Vidíme, že v prvom qubite je obsiahnutá informácia o tom, či je $f(x)$ konštantná; $|\,+\rangle$ znamená áno, $|\,-\rangle$ znamená nie. V podstate môžeme meraním v báze $\{|\,+\rangle\,, |\,-\rangle\}$ získať výsledok už teraz, pre úplnosť ale

ešte aplikujeme Hadamardovo hradlo (využijeme vlastnosť $H^{-1} = H$). Dostaneme tak konenčný stav registra $|\psi_4\rangle$:

$f(x)$ je konštantná $\quad |\psi_4\rangle = \pm|0\rangle|-\rangle$

$f(x)$ nie je konštantná $\quad |\psi_4\rangle = \pm|1\rangle|-\rangle$

Nakoniec stačí zmerať hodnotu prvého qubitu.



Obr. 3.1: Implementácia Deutschovho algoritmu

3.3 Kvantová Fourierova transformácia

Silným nástrojom na riešenie niektorých matematických problémov je transformácia na iný problém, ktorého riešenie už poznáme. Jednou z nich je diskrétna Fourierova transformácia. Definujeme ju ako zobrazenie komplexného vektoru $[x_0, x_1, \ldots, x_{N-1}]$ na iný komplexný vektor, $[y_0, y_1, \ldots, y_{N-1}]$, kde:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N} \tag{3.3}$$

Kvantová Fourierova transformácia (QFT) je na ortonormálnej báze $|0\rangle$, $|1\rangle$, ..., $|2^n - 1\rangle$ definovaná ako:

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n} |k\rangle . \tag{3.4}$$

De facto sa jedná o diskrétnu Fourierovu transformáciu, rozdiel spočíva v zavedenej notácii. Naviac sme zvolili $N = 2^n$, čo predstavuje počet bázových stavov kvantového registra veľkosti n.

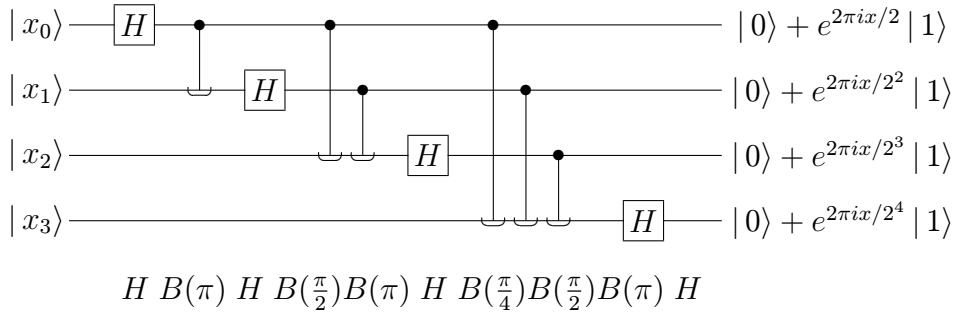
Na skonštruovanie príslušného obvodu potrebujeme iba dva typy hradiel: Hadamardovo H a kontrolované fázové hradlo, ktoré budeme značiť $B(\phi)$ (viď 2.4). Môžeme postupovať nasledovným spôsobom:

1. V prvom kroku zostrojíme QFT obvod pre jeden qubit - obvod pozostávajúci z jedného Hadamardovho hradla.

2. Pre dvojqubitovú QFT naviac pridáme kontrolované fázové hradlo $B(\pi)$ a H hradlo pôsobiace na druhý qubit

3. Postupne pridávame ďalšie $B(\phi)$ a H hradlá. ϕ je určené vstupnými qubitmi $B(\phi)$, tj. ak j-ty qubit je kontrolný a k-ty qubit cieľový (j ¿ k), tak $\phi = 2\pi/2^{j-k}$.

Napríklad pre štyri qubity vyzerá QFT obvod nasledovne:

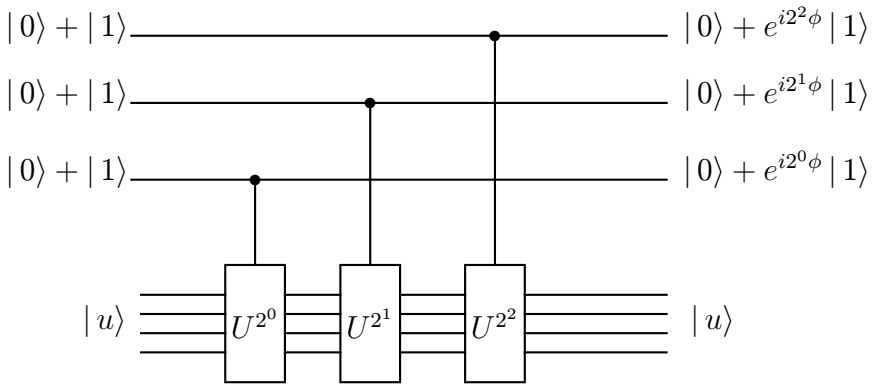


Obr. 3.2: Štvorqubitová QFT [1]

Nakoľko každá použitá operácia je unitárna, takto uskutočnená kvantová Fourierova transformácia je tiež unitárna. Obvod, ktorý vykonáva QFT na n qubitoch bude potrebovať n hradiel H a $n(n-1)/2$ kontrolovaných fázových hradiel B, čo spolu predstavuje $n(n+1)/2$ základných hradiel. Môžeme povedať, že náročnosť QFT je $O(n^2)$.

3.4 Odhad fázy

Nech U je unitárny operátor na m qubitoch s vlastným vektorom $|u\rangle$ a vlastnou hodnotou $e^{2\pi i\varphi}$, kde φ je neznáme. Kvantovú Fourierovu transformáciu môžeme využiť k n-bitovému odhadu φ. Predstavme si, že máme k dispozícii čierne skrinky schopné pripraviť stav $|u\rangle$ a previesť operáciu kontrolované-U^{2^j}, kde j je predstavuje čísla 0, 1, ..., $n-1$. Na začiatku zostrojíme nasledujúci obvod [1]:



Na konci máme druhý, m-bitový, register v pôvodnom stave $|u\rangle$, zatiaľ čo prvý, n-bitový, je v stave

$$\frac{1}{2^{n/2}}(|0\rangle+e^{i2^{n-1}\phi}|1\rangle)(|0\rangle+e^{i2^{n-2}\phi}|1\rangle)\cdots(|0\rangle+e^{i\phi}|1\rangle) = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi i\frac{\phi k}{2^n}}|k\rangle\,. \tag{3.5}$$

V ďalšom kroku aplikujeme na prvý register inverznú Fourierovu transformáciu použitím obráteného obvodu pre QFT na 3.5:

$$\frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi i\frac{\phi k}{2^n}}|k\rangle \rightarrow \left|\widetilde{\phi}\right\rangle \tag{3.6}$$

a nakoniec zmeriame $\left|\widetilde{\phi}\right\rangle$, čím dostaneme dobrý odhad ϕ. Presnejšie, ak $\phi = 2\pi x/2^n$, kde $x = \sum_{i=0}^{n-1} 2^i x_i$ je n-bitové celé číslo, tak vyššie uvedený algoritmus dá presnú hodnotu ϕ [1]. Vo všeobecnosti je odhad ϕ správny v $n - \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ bitoch s pravdepodobnosťou úspechu $1-\epsilon$ ($\lceil x\rceil$ je celá horná časť x) [2].

3.5 Hľadanie rádu

Nech dve prirodzené čísla a a N, $a < N$ sú nedeliteľné. Rád a modulo N je definovaný ako najmenšie prirodzené číslo r také, že $a^r = 1(\text{mod } N)$. Problém hľadania rádu spočíva nájsť r pre zadané a a N. Kvantový algoritmus spočíva iba v použití algoritmu pre odhad fázy aplikovanom na unitárny operátor

$$U|y\rangle \equiv |ay(\text{mod } N)\rangle\,. \tag{3.7}$$

Na rád r sa môžeme pozrieť aj ako na periódu funkcie $f(x) = a^x \bmod N$, tj. najmenšie $r > 0$ také, že $f(x) = f(x+r)$ pre všetky x. Pre $0 \leq s \leq r-1$ sú vlastné stavy U vektory

$$|\, u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[-\frac{2\pi i s k}{r}\right] \Big|\, a^k \bmod N\Big\rangle \tag{3.8}$$

s vlastnými hodnotami $\exp\left[\frac{2\pi i s}{r}\right]$, odkiaľ môžeme dopočítať rád r.

Na uskutočnenie tohoto algoritmu potrebujeme dve veci: za prvé, musíme dokázať efektívne implementovať kontrolované-U^{2^j} operácie, za druhé, musíme vedieť efektívne pripraviť vlastné stavy $|\, u_s\rangle$. Prvú požiadavku môžeme uskutočniť pomocou tzv. *modulárneho umocňovania*. Potrebujeme k tomu $O(L^3)$ operácií, kde $n = 2L + 1 + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ [2].

Priama príprava $|\, u_s\rangle$ vyžaduje znalosť r, ktorú ale nemáme. Môžeme však použiť malý trik. Ak si všimneme, že

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\, u_s\rangle = |\, 1\rangle\,, \tag{3.9}$$

v procedúre odhadu fázy použijeme v prvom registri $n = 2L+1+\left\lceil \log\left(2 + \frac{1}{2\epsilon}\right)\right\rceil$ a druhý register pripravíme do stavu $|\, 1\rangle$, tak pre každé $s = 0, 1, \ldots, r-1$ dostaneme na výstupe $2L+1$-bitový odhad fázy $\phi \approx s/r$ s pravdepodobnosťou najmenej $(1-\epsilon)/r$.

3.6 Faktorizácia

Predstavme si, že chceme nájsť prvočíselné delitele nejakého zloženého prirodzeného čísla (tj. nie prvočísla) N. Dá sa ukázať ([2]), že problém faktorizácie môžeme previesť na hľadanie rádu nasledujúcim postupom:

1. Ak je N párne, vráť číslo 2.
2. Over, či $N = a^b$ pre nejaké prirodzené čísla $a \geq 1$ a $b \geq 2$ a ak áno, vráť čislo a (toto môžeme urobiť s použitím klasického algoritmu).
3. Náhodne vyber $x \in \{1, 2, \ldots, N-1\}$. Ak $\gcd(x, N) > 1$, tak vráť $\gcd(x, N)$ ($\gcd(a, b)$ je najväčší spoločný deliteľ a a b).
4. Použi podprogram na nájdenie rádu r čísla x modulo N.

5. Ak r je párne a $x^{r/2} \neq -1 (\text{mod } N)$, tak vypočítaj $\gcd(x^{r/2}-1, N)$, $\gcd(x^{r/2}+1, N)$ a otestuj, či nejaké z nich je netriviálny deliteľ. Ak áno, navráť ho. V inom prípade algoritmus zlyhá.

Takýto proces faktorizácie vyžaduje $O((\log N)^3)$ operácií, no nemusí vždy uspieť (pravdepodobnosť úspechu je $O(1)$). Na druhú stranu, ak máme na výstupe nejaké číslo, vieme ľahko overiť, či delí N.

Na čo môžeme využiť faktorizáciu? V súčasnosti je jednou z najpoužívanejších kryptografických metód tzv. RSA. Na jej zlomenie je potrebné rozfaktorizovať veľké číslo N na dve prvočísla p a q, $N = pq$. Najlepší známy klasický algoritmus GNFS - General Number Field Sieve je $O\left(\exp\left[\left(\frac{64}{9}k\right)^{1/3}(\log\ k)^{2/3}\right]\right)$, kde k je počet bitov faktorizovaného čisla, čo z praktického hľadiska znamená, že RSA je klasicky neoblomná. Kvantové počítače umožňujú zlomiť RSA efektívnym spôsobom.

Záver

Práca bola konceptovaná tak, aby obsiahla základné stavebné kamene kvantového počítača a ukázala niektoré jeho aplikácie. Problematika kvantových výpočtov nekončí pri univerzálnom hradle, ale je to nevyhnutný začiatok pri budovaní kvantových logických obvodov. Druhým nevyhnutným predpokladom je pochopenie paralelizmu kvantového počítača.

Nakoniec sa ešte pozrime na dosiahnuté úspechy v realizácii kvantového počítača. Ako uviedol server News.com[8], vo februári 2007 predstavila Kanadská firma D-Wave kvantový počítač Orion, ktorý obsahoval 16 qubitov. Pri demonštrácii vyriešil Sudoku, z chemickej databázy vyhľadal molekuly s podobnou štruktúrou ako Prilosec a našiel zasadací poriadok s najmenším počtom porušení požiadavok hostí. Pre skutočné využitie je však potrebné nielen zväčšiť počet qubitov, ale aj vytvoriť hradlá vnášajúce čo najmenšie chyby do výpočtu a zlepšiť stabilitu kvantových stavov.

Literatúra

[1] Ekert A., Hayden P., Inamori H.: *Basic concepts in quantum computation*, arXiv e-print quant-ph/0011013v1, 2000

[2] Nielsen M. A., Chuang L. I.: *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000

[3] Skála L.: *Úvod do kvantové mechaniky*, Academia, Praha, 2005

[4] Deutsch D.: *Proc. R. Soc. Lond. A* **425** 73 1989

[5] Švejdar V.: *Logika - neúplnost, složitost a nutnost*, Academia, Praha, 2002

[6] Aharonov D.: *A Simple Proof that Toffoli and Hadamard are Quantum Universal*, arXiv e-print quant-ph/0301040v1, 2003

[7] Fiurášek J.: *Linear optics quantum Toffoli and Fredkin gates*, arXiv e-print quant-ph/0602220v1, 2006

[8] http://news.cnet.com/Start-up-demos-quantum-computer/2100-1008_3-6159152.html