

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

Katedra fyziky
Obor: Matematické inženýrství
Zaměření: Matematická fyzika



Diskrétní kvantové procházky a kvantová informace

Discrete quantum walks and quantum information

BAKALÁŘSKÁ PRÁCE

Vypracoval: Jan Mareš
Vedoucí práce: prof. Ing. Igor Jex, DrSc.
Rok: 2012

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze podklady uvedené v příloženém seznamu.

V Praze dne

.....
Jan Mareš

Poděkování

Děkuji panu prof. Ing. Igoru Jexovi, DrSc. za velmi zajímavé a aktuální téma a za trpělivost a ochotu, se kterou mou práci vedl. Dále děkuji panu Mgr. Aurélu Gábrisovi, Ph.D. za užitečné konzultace.

Jan Mareš

Název práce:

Diskrétní kvantové procházky a kvantová informace

Autor: Jan Mareš

Obor: Matematické inženýrství

Druh práce: Bakalářská práce

Vedoucí práce: prof. Ing. Igor Jex, DrSc.

Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické v Praze

Konzultant: Mgr. Aurél Gábris, Ph.D.

Katedra fyziky, Fakulta jaderná a fyzikálně inženýrská, České vysoké učení technické v Praze

Abstrakt: Cílem této práce je uvést čtenáře do základů teorie kvantové informace se zvláštním zaměřením na kvantové procházky. Kvantové procházky jsou kvantovou analogií klasických náhodných procházek a představují jednu z nejslibnějších oblastí realizace kvantových výpočtů a zkoumání kvantových systémů. Nejprve uvádíme některé nezbytné poznatky z kvantové mechaniky následované teorií kvantové informace s jejími možnými aplikacemi a popisem několika fyzikálních realizací jednoduchých zařízení pro kvantové výpočty. Zbytek práce je věnován kvantovým procházkám. Poskytujeme obecné definice, srovnání s klasickými náhodnými procházkami a nejpodrobněji popisujeme současné experimentální realizace kvantových procházek, především na optických zařízeních.

Klíčová slova: kvantové procházky, kvantová informace, experimentální realizace

Title:

Discrete quantum walks and quantum information

Author: Jan Mareš

Abstract: The aim of this work is to introduce reader into basics of quantum information theory with special focus on quantum walks. Quantum walk is a quantum analogy of classical random walk and currently represents one of the most promising field of realisation of quantum computing and investigation of quantum systems. First we present some essential knowledge of quantum mechanics followed by quantum information theory with its possible uses and description of several physical realisations of simple quantum computing devices. The rest of the work is devoted to quantum walks. We provide general definitions, comparison with classical random walks and in most detail we describe current experiments realising quantum walks, mostly on optic devices.

Key words: quantum walks, quantum information, experimental realisation

Obsah

Úvod	9
1 Základy kvantové teorie	10
1.1 Diracův formalismus	10
1.1.1 Ket vektory a Bra vektory	10
1.1.2 Skalární součin	11
1.1.3 Lineární operátory	11
1.1.4 Tenzorový součin	13
1.2 Pozorovatelné v kvantové mechanice	14
1.3 Matice hustoty	15
1.4 Časový vývoj	15
1.5 Dvourozměrný prostor	16
2 Kvantová informace	19
2.1 Klasické logické operace	19
2.2 Kvantová informace	20
2.2.1 Jednotka kvantové informace	20
2.2.2 Kvantové logické operace	20
2.2.3 Fázový posun	21
2.2.4 Hadamardovo hradlo	21
2.2.5 Kontrolovaná negace (CNOT)	22
2.3 Kvantové výpočetní obvody	22
2.4 Kvantová Fourierova transformace	23
2.5 Faktorizační algoritmus	24
3 Fyzikální realizace kvantových počítačů	26

3.1	Obecné požadavky	26
3.2	Elektromagnetické pole v dutině	27
3.2.1	Reprezentace qubitu	27
3.2.2	Interakce s látkou	27
3.2.3	Vícequbitové operace	29
3.3	Iontové pasti	30
3.4	Shrnutí	31
4	Náhodné procházky	32
4.1	Grafy	32
4.2	Klasická náhodná procházka	33
4.2.1	Klasická náhodná procházka na přímce	33
4.2.2	Klasická náhodná procházka na grafu	34
4.2.3	Časově spojitá náhodná procházka	35
4.3	Kvantové procházky	36
4.3.1	Diskrétní kvantová procházka na přímce	36
4.3.2	Diskrétní kvantová procházka na grafu	38
4.3.3	Časově spojitá kvantová procházka	39
4.3.4	Dekoherence v kvantových procházkách	39
5	Využití náhodných a kvantových procházek	42
5.1	Využití klasických náhodných procházek	42
5.1.1	Problém s-t propojení	42
5.1.2	2-SAT problém	42
5.1.3	Google PageRank	43
5.2	Využití kvantových procházek	44
5.2.1	Groverův algoritmus	44
5.2.2	Univerzální výpočty pomocí časově spojitě kvantové procházky	45
5.2.3	Univerzální výpočty pomocí diskretní kvantové procházky	46
5.3	Shrnutí	49
6	Fyzikální realizace kvantových procházek	50
6.1	Optická smyčka	50

6.1.1	Jednorozměrná procházka	50
6.1.2	Zkoumání dekoherence na optické smyčce	51
6.1.3	Dvourozměrná kvantová procházka	53
6.2	Integrovaný optický obvod	56
6.3	Shrnutí	59
Závěr		60
Seznam použitých zdrojů		61

Úvod

Cílem této práce je uvést čtenáře do problematiky kvantové informace a speciálně kvantových procházek. Celkem je rozdělena do šesti kapitol. První kapitola obsahuje základy kvantové mechaniky potřebné v dalších částech, nicméně se spíše předpokládá, že čtenář je již s kvantovou mechanikou do určité míry seznámen. Druhá kapitola se zabývá kvantovou informací a popisem kvantového počítače a kvantových algoritmů. Třetí kapitola pak popisuje některé pokusy o fyzikální realizace kvantových počítačů. Zbývající tři kapitoly se zabývají kvantovými procházkami - zavedením konceptu, možnostmi jejich využití a fyzikálními realizacemi.

Kapitola 1

Základy kvantové teorie

V této kapitole, především kvůli ujasnění značení, rozebereme některé partie z kvantové mechaniky potřebné ve zbytku práce. V žádném případě se pochopitelně nejedná o snahu podávat ucelený či úplný výklad kvantové teorie.

1.1 Diracův formalismus

1.1.1 Ket vektory a Bra vektory

V klasické mechanice je stav systému plně určen bodem ve fázovém prostoru (tedy polohou a hybností). Popis stavu v kvantové mechanice se zásadně liší. Je dán (v nejjednodušším případě) vektorem z nějakého *Hilbertova prostoru*.¹ Hilbertův prostor je libovolný úplný vektorový prostor se skalárním součinem. (Budeme uvažovat jen Hilbertovy prostory s nejvýše spočetnou bází.)

Vektory z Hilbertova prostoru $\mathcal{H}$ stavů systému budeme značit $|u\rangle$ a nazývat *ket* (ket vektor). Zde u může být nahrazeno libovolným symbolem, který daný vektor jasně určuje. Lineární superpozice takových vektorů je také prvek stejného Hilbertova prostoru a odpovídá nějakému fyzikálnímu stavu systému. Na Hilbertových prostorech konečné dimenze ($\dim \mathcal{H} = N$) můžeme libovolný vektor vyjádřit jako lineární kombinaci prvků báze $\{|i\rangle\}_{i=1}^N$, tedy

$$|u\rangle = \sum_{i=1}^N c_i |i\rangle, \quad (1.1)$$

kde c_i jsou komplexní čísla. Analogický rozklad můžeme použít i na prostorech nekonečné dimenze, kde však dostaneme řadu (nekonečnou sumu).

Prvky duálního prostoru k $\mathcal{H}$ budeme značit $\langle\varphi|$ a nazývat *bra* (bra vektor). Jedná se tedy o lineární funkcionály na $\mathcal{H}$. Pro konečně-dimenzionální prostor má i jeho duální

¹Přesněji jednorozměrným podprostorem vektorů, tedy vynásobením nenulovým komplexním číslem nemění fyzikální interpretaci stavu.

prostor konečnou, a to stejnou dimenzi. Rieszova věta nám dává antilineární bijekci mezi $\mathcal{H}$ a jeho duálním prostorem. Každému ketu je tedy jednoznačně přiřazen (duální) bra vektor, který označujeme stejným znakem $(|u\rangle \leftrightarrow \langle u|)$.

1.1.2 Skalární součin

Skalární součin dvou ketů $|u\rangle$ a $|v\rangle$ je komplexní číslo značené $(|u\rangle, |v\rangle) \equiv \langle u|v\rangle = \overline{\langle v|u\rangle}$ (pruh značí komplexní sdružení) a někdy nazývané *braket* („bracket“, tedy závorka). Definuje se vztahem $\langle u|v\rangle = u(|v\rangle)$, kde u je lineární funkcionál odpovídající bra vektoru $\langle u|$. Tato operace splňuje všechny požadavky matematické definice skalárního součinu a indukuje na $\mathcal{H}$ normu $\| |u\rangle \| \equiv \| u \|$ vztahem

$$\| u \|^2 = \langle u|u\rangle. \quad (1.2)$$

Dále budeme pro popis kvantových systémů vždy používat *normalizované* vektory, tedy takové, pro které platí $\| u \| = 1$.

Říkáme, že dva vektory jsou *ortogonální* (kolmé), pokud je jejich skalární součin roven nule. Často budeme pracovat s takzvanou *ortonormální* bází. Tou nazveme takovou bázi $\{|u_i\rangle\}$, ve které pro každé dva vektory platí

$$\langle u_i|u_j\rangle = \delta_{ij}. \quad (1.3)$$

Mějme soubor vektorů z $\mathcal{H}$, označme $\mathcal{E}$ množinu všech lineárních kombinací všech vektorů z tohoto souboru a $\mathcal{E}^\perp$ množinu všech vektorů z $\mathcal{H}$ kolmých k vektorům z $\mathcal{E}$. Potom můžeme každý vektor $|u\rangle \in \mathcal{H}$ rozložit na dva vzájemně kolmé vektory

$$|u\rangle = |u_{\mathcal{E}}\rangle + |u_{\mathcal{E}}^\perp\rangle, \quad (1.4)$$

kde $|u_{\mathcal{E}}\rangle \in \mathcal{E}$ a $|u_{\mathcal{E}}^\perp\rangle \in \mathcal{E}^\perp$. Tyto vektory nazýváme *projekce* na odpovídající podprostory.

1.1.3 Lineární operátory

Lineární operátory jsou lineární zobrazení z Hilbertova prostoru stavů $\mathcal{H}$ opět do $\mathcal{H}$. Budeme je v další části potřebovat pro popis měření na kvantových systémech. Působení lineárního operátoru A na ket $|u\rangle$ se zapisuje jednoduše jako $A|u\rangle$.

Ke každému lineárnímu operátoru můžeme pomocí skalárního součinu jednoznačně přiřadit hermitovsky sdružený operátor, který budeme značit symbolem $\dagger$. Konkrétně $\forall |x\rangle, |y\rangle \in \mathcal{H}$ musí platit

$$(|x\rangle, A^\dagger |y\rangle) = (A |x\rangle, |y\rangle). \quad (1.5)$$

Akce A na bra vektor $\langle\varphi|$ je pak definována pomocí skalárního součinu tak, že $\forall |u\rangle \in \mathcal{H}$ platí

$$(A(\langle\varphi|)) |u\rangle = \langle\varphi| (A |u\rangle). \quad (1.6)$$

Potom píšeme

$$A(\langle\varphi|) \equiv \langle\varphi| A. \quad (1.7)$$

Tato definice vede k identitě, která umožňuje používat zjednodušené označení

$$(\langle\varphi| A) |u\rangle = \langle\varphi| (A |u\rangle) \equiv \langle\varphi| A |u\rangle. \quad (1.8)$$

Zvláště nás zde budou zajímat samosdružené operátory s čistě bodovým spektrem. Tedy takové, pro které platí $A^\dagger = A$ a existuje ortonormální báze $\{|a_i\rangle\}$ prostoru $\mathcal{H}$ taková, že pro každý vektor $|a_i\rangle$ existuje obecně komplexní (pro samosdružené operátory reálné) číslo a_i takové, že platí

$$A |a_i\rangle = a_i |a_i\rangle. \quad (1.9)$$

Množinu čísel $\{a_i\}$ nazýváme bodovým *spektr*em operátoru A a kety $\{|a_i\rangle\}$ jeho vlastními vektory.

Speciálním případem jsou takzvané *projekční* operátory. Výše jsme uvedli možnost rozkladu vektoru na dva jiné vektory, kde jeden z nich je prvkem daného podprostoru $\mathcal{E}$ a druhý náleží do jeho ortogonálního doplňku, tedy $|u\rangle = |u_{\mathcal{E}}\rangle + |u_{\mathcal{E}}^\perp\rangle$. Projekční operátor na podprostor $\mathcal{E}$ označený $P_{\mathcal{E}}$ je pak definován jako

$$P_{\mathcal{E}} |u\rangle = |u_{\mathcal{E}}\rangle. \quad (1.10)$$

Takový operátor má pouze vlastní hodnoty $\{0, 1\}$, kde hodnotě 1 přísluší všechny vektory z $\mathcal{E}$ a hodnotě 0 všechny vektory z $\mathcal{E}^\perp$.

Pro libovolný vektor $|\psi\rangle$ můžeme vytvořit projekční operátor na podprostor generovaný tímto vektorem, který v braketovém formalismu s výhodou zapisujeme jako

$$P_\psi = |\psi\rangle \langle\psi|. \quad (1.11)$$

Jeho působení na vektor $|\varphi\rangle$ je pak dáno pomocí skalárního součinu jako násobek vektoru $|\psi\rangle$, konkrétně

$$P_\psi |\varphi\rangle = |\psi\rangle \langle\psi| |\varphi\rangle = \langle\psi| \varphi\rangle |\psi\rangle. \quad (1.12)$$

Takto můžeme vyjádřit projekční operátor na libovolný podprostor $\mathcal{E}$ pomocí jeho báze $\{|\psi_i\rangle\}$ jako

$$P_{\mathcal{E}} = \sum_i |\psi_i\rangle \langle \psi_i|. \quad (1.13)$$

Speciálně pro $\{|u_j\rangle\}$ libovolnou bázi $\mathcal{H}$ platí

$$\sum_j |u_j\rangle \langle u_j| = I, \quad (1.14)$$

kde I je jednotkový operátor (identita).

Obecný operátor A se spektrem $\{a_i\}$ a odpovídajícími vlastními vektory $|a_i\rangle$ můžeme rozložit pomocí projekčních operátorů jako

$$A = \sum_i a_i |a_i\rangle \langle a_i| = \sum_i |a_i\rangle a_i \langle a_i|. \quad (1.15)$$

Na prostorech konečné dimenze můžeme zvolit konečnou bázi a lineární operátory interpretovat pomocí matic. Tyto matice udávají působení operátoru na báze vektory (a tím i na všechny jejich lineární kombinace). Operátorový počet se pak redukuje na počet maticový, kde ket-vektorem odpovídají sloupcové a bra-vektorem řádkové vektory vyjadřující rozklad stavu do zvolené báze.

1.1.4 Tenzorový součin

Tenzorový součin nám umožňuje popisovat kvantové systémy složené z více podsystémů, jejichž popis již známe. Mějme dva systémy a jim odpovídající Hilbertovy prostory $\mathcal{H}^{(1)}$ a $\mathcal{H}^{(2)}$. Je-li stav prvního systému $|U\rangle^{(1)}$ a stav druhého systému $|V\rangle^{(2)}$, potom je stav celého složeného systému popsán *tenzorovým součinem* jednotlivých stavů $|U\rangle^{(1)} \otimes |V\rangle^{(2)} \equiv |U\rangle^{(1)} |V\rangle^{(2)} \equiv |U^{(1)}V^{(2)}\rangle$, který je prvkem tenzorového součinu Hilbertových prostorů jednotlivých systémů $\mathcal{H} = \mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)}$. To je však jen speciální případ. Pokud máme v prvním prostoru bázi $\{|u_i\rangle^{(1)}\}_{i=1}^n$ a ve druhém $\{|v_j\rangle^{(2)}\}_{j=1}^m$, můžeme vytvořit bázi $\mathcal{H}$ jako $\{|u_i\rangle^{(1)} |v_j\rangle^{(2)}\}_{i,j=1}^{n,m}$. Obecný vektor z $\mathcal{H}$ je pak libovolnou lineární kombinací prvků této báze, tedy

$$|\psi\rangle = \sum_{i,j} C_{ij} |u_i\rangle |v_j\rangle. \quad (1.16)$$

Ve speciálním případě, kdy $|\psi\rangle = |U\rangle^{(1)} |V\rangle^{(2)}$ dostáváme

$$|\psi\rangle = \left(\sum_i u_i |u_i\rangle^{(1)} \right) \left(\sum_j v_j |v_j\rangle^{(2)} \right) = \sum_{i,j} u_i v_j |u_i\rangle^{(1)} |v_j\rangle^{(2)}, \quad (1.17)$$

tedy $C_{ij} = u_i v_j$. Každý stav, jehož koeficienty je možné tímto způsobem rozložit, můžeme vyjádřit jako tenzorový součin dvou stavů z dílčích prostorů a nazýváme jej *neprovozaný*. Naopak *provozaný* stav je každý takový, který tímto způsobem rozložit nelze. (Zatím bereme v úvahu jen časté stavy - viz dále.)

Lineární operátory definované na některém dílčím prostoru nemají žádný účinek na vektory druhého prostoru. To odpovídá tomu, že operátor $A^{(1)}$ rozšíříme na celý prostor jako $A^{(1)} \otimes I^{(2)}$, kde I je jednotkový operátor. Tedy máme

$$A^{(1)} |u^{(1)} v^{(2)}\rangle = (A^{(1)} |u^{(1)}\rangle) |v^{(2)}\rangle. \quad (1.18)$$

Také pro každé dva operátory $A^{(1)}$ a $B^{(2)}$ platí

$$[A^{(1)}, B^{(2)}] \equiv A^{(1)} B^{(2)} - B^{(2)} A^{(1)} = 0. \quad (1.19)$$

1.2 Pozorovatelné v kvantové mechanice

Víme, že ket-vektor plně určuje stav kvantového systému. Zatím jsme však neuvedli, jaké jsou v tomto stavu hodnoty veličin, které jsme schopni měřit (hybnost, energie, moment hybnosti, spin,...). V klasické mechanice jsou tyto pozorovatelné veličiny reprezentovány funkcemi na fázovém prostoru a jejich hodnoty jsou daným bodem fázového prostoru vždy pevně určeny. Ať se to zdá jakkoli nepřírozené, pozorovatelným v kvantové mechanice odpovídají samosdružené operátory na Hilbertově prostoru stavů. Jediné hodnoty, které mohou tyto veličiny nabývat, jsou dány body spektra příslušných operátorů. (Samosdružené operátory mají reálné spektrum.) Je-li stav našeho systému popsán vektorem $|\psi\rangle$ a pozorovatelná A má vlastní vektory $\{|a_i\rangle\}$, pro které platí $A|a_i\rangle = a_i|a_i\rangle$, je pravděpodobnost naměření hodnoty a_i veličiny A rovna

$$P_{A=a_i} = |\langle\psi|a_i\rangle|^2. \quad (1.20)$$

Konkrétní výsledek však nemůžeme zjistit, dokud měření neprovedeme. Výsledky měření v kvantové mechanice jsou tedy principiálně náhodné (kromě speciálního případu, kdy je měřený stav vlastním stavem příslušného operátoru), i když máme pevně určený stav systému.

Vztah 1.20 nám umožňuje počítat střední hodnoty veličin. Kombinací klasické definice střední hodnoty a identity pro rozklad operátoru dostáváme pro střední hodnotu A systému ve stavu $|\psi\rangle$ tvar

$$\langle A \rangle_\psi = \sum_i a_i |\langle\psi|a_i\rangle|^2 = \sum_i \langle\psi|a_i\rangle a_i \langle a_i|\psi\rangle = \langle\psi| \left(\sum_i |a_i\rangle a_i \langle a_i| \right) |\psi\rangle = \langle\psi| A |\psi\rangle. \quad (1.21)$$

1.3 Matice hustoty

V klasické fyzice můžeme mít plně popsany pohybový stav systému tak, že každé částici přiřadíme konkrétní polohu a hybnost v daném čase. Často však takto přesná informace není k dispozici a je třeba systém popsat statisticky. Potom mu přiřazujeme pravděpodobnostní rozdělení poloh a hybností. Jedná se o funkci, která každému bodu fázového prostoru přiřazuje pravděpodobnost, že se systém právě v tomto bodě nachází. Analogii této situace máme i v kvantové mechanice.

Kvantový stav popsany prvkem Hilbertova prostoru $|\psi\rangle \in \mathcal{H}$ je označován jako *čistý*. Jedná se o ideální případ, který často není možné prakticky realizovat. Existují dvě situace, které se však matematicky popisují stejně. Můžeme mít soubor mnoha systémů, ve kterém se různé stavy vyskytují s četností p_j . Případně máme jeden systém, ale jeho skutečný stav je s patřičnou pravděpodobností vybrán z nějakého souboru možných stavů (nejistota v jeho přípravě). Říkáme, že systém je ve *smíšeném stavu*. Jedná se tedy o klasickou neurčitost systému, která se přidává k principiální kvantové neurčitosti.

Matematická struktura, která výše zmíněnou situaci dokáže vystihnout se nazývá *matice hustoty*. (Na prostorech nekonečné dimenze se dává přednost názvu *operátor hustoty*). Máme-li soubor N systémů, kde četnost stavu $|\psi_j\rangle$ je p_j , je matice hustoty takového systému dána vztahem

$$\rho = \sum_{j=1}^N p_j |\psi_j\rangle \langle \psi_j|. \quad (1.22)$$

S takto zavedeným operátorem ρ můžeme počítat střední hodnotu pozorovatelné celého souboru jako

$$\langle A \rangle = \sum_{j=1}^N p_j \langle \psi_j | A | \psi_j \rangle = \text{Tr}(\rho A). \quad (1.23)$$

Se smíšenými stavy se často setkáváme v situaci, kdy je náš systém provázán s jiným systémem, jehož stav nechceme sledovat. Provedeme proto stopu přes stavy tohoto systému a tím přejdeme ke statistickému popisu. Typicky se jedná o nedokonalou izolaci zkoumaného systému od okolí.

1.4 Časový vývoj

Časový vývoj čistých stavů kvantových systémů se řídí Schrödingerovou rovnicí, která má tvar

$$i\hbar \frac{\partial |\psi(t)\rangle}{\partial t} = H |\psi(t)\rangle, \quad (1.24)$$

kde H je Hamiltonián (operátor energie) a $\hbar$ redukovaná Planckova konstanta. Pro vlastní stavy Hamiltoniánu $H|\psi_j\rangle = E_j|\psi_j\rangle$ dostáváme jednoduchou diferenciální rovnici $i\hbar\frac{\partial|\psi_j(t)\rangle}{\partial t} = E_j|\psi_j(t)\rangle$, jejíž řešení s počáteční podmínkou $|\psi_j(0)\rangle = |\psi_j\rangle$ má tvar

$$|\psi_j(t)\rangle = \exp\left(-\frac{i}{\hbar}E_j t\right)|\psi_j\rangle. \quad (1.25)$$

Toho můžeme využít pro určení časového vývoje obecného stavu pomocí jeho rozkladu do vlastních stavů Hamiltoniánu. Pak dostáváme

$$|\psi(t)\rangle = \sum_j \exp\left(-\frac{i}{\hbar}E_j t\right) \langle\psi_j|\psi(0)\rangle |\psi_j\rangle, \quad (1.26)$$

kde $\langle\psi_j|\psi(0)\rangle$ jsou koeficienty rozkladu, a tedy platí $|\psi(0)\rangle = \sum_j \langle\psi_j|\psi(0)\rangle |\psi_j\rangle$.

Pro stavy popsané maticí hustoty ρ platí analogická rovnice ve tvaru

$$i\hbar\frac{\partial\rho(t)}{\partial t} = [H, \rho(t)] = H\rho(t) - \rho(t)H. \quad (1.27)$$

1.5 Dvourozměrný prostor

Pro přiblížení zmíněných pojmů nyní uvedeme jako příklad kvantový popis polarizace fotonů. Hilbertův prostor odpovídající polarizačnímu stavu jednoho fotonu je dvourozměrný, tedy $\mathcal{H} \equiv \mathbb{C}^2$. Jako báze stavy můžeme zvolit horizontální a vertikální lineární polarizaci $\{|h\rangle, |v\rangle\}$. V maticovém vyjádření tedy platí

$$|h\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |v\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \quad (1.28)$$

Pomocí lineárních kombinací můžeme vytvořit další polarizační stavy a přecházet k jiným bázím. Například k bázi tvořené levotočivě a pravotočivě kruhově polarizovaným světlem:

$$|l\rangle = \frac{1}{\sqrt{2}}(|v\rangle + i|h\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, |p\rangle = \frac{1}{\sqrt{2}}(|v\rangle - i|h\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}. \quad (1.29)$$

Na prostoru matic se provádí sdružení (přechod mezi kety a bra a sdružení operátorů) provedením transpozice a komplexního sdružení složek. Tedy například

$$\langle l| = \frac{1}{\sqrt{2}}(\langle v| - i\langle h|) = \frac{1}{\sqrt{2}}[1, -i]. \quad (1.30)$$

Nyní můžeme spočítat některé skalární součiny. Předně platí

$$\langle l | p \rangle = \frac{1}{\sqrt{2}} [1, -i] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \frac{1}{2}(1 + i^2) = 0, \quad (1.31)$$

a dále

$$\langle l | l \rangle = \frac{1}{\sqrt{2}} [1, -i] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{2}(1 - i^2) = 1. \quad (1.32)$$

Vidíme tedy, že se opravdu jedná o ortonormální bázi. (Ještě bychom měli ověřit, zda i $\langle p | p \rangle = 1$.)

Příkladem operátoru na dvourozměrném prostoru je Hadamardův operátor

$$C_H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (1.33)$$

Působením na stavy $|h\rangle$ a $|v\rangle$ dostáváme

$$C_H |h\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|h\rangle + |v\rangle), \quad (1.34)$$

$$C_H |v\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|h\rangle - |v\rangle). \quad (1.35)$$

Dále ještě můžeme například vytvořit projekční operátor na stav $|l\rangle$ ve tvaru

$$P_{|l\rangle} = |l\rangle \langle l| = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} \frac{1}{\sqrt{2}} [1, -i] = \frac{1}{2} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}. \quad (1.36)$$

Tenzorový součin dvou matic na prostoru $\mathbb{C}^2$ se provádí jako

$$A \otimes B \equiv \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix} = \begin{bmatrix} a_1 B & a_2 B \\ a_3 B & a_4 B \end{bmatrix} = \begin{bmatrix} a_1 b_1 & a_1 b_2 & a_2 b_1 & a_2 b_2 \\ a_1 b_3 & a_1 b_4 & a_2 b_3 & a_2 b_4 \\ a_3 b_1 & a_3 b_2 & a_4 b_1 & a_4 b_2 \\ a_3 b_3 & a_3 b_4 & a_4 b_3 & a_4 b_4 \end{bmatrix}. \quad (1.37)$$

U vektorů to je

$$|a\rangle \otimes |b\rangle \equiv \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 |b\rangle \\ a_2 |b\rangle \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{bmatrix}. \quad (1.38)$$

Důležitými operátory na dvourozměrném prostoru jsou Pauliho matice definované jako

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \quad (1.39)$$

Všechny tyto matice jsou hermitovské, mají nulovou stopu (součet diagonálních prvků) a společně s jednotkovou maticí I tvoří bázi operátorů na dvourozměrném prostoru.

Kapitola 2

Kvantová informace

2.1 Klasické logické operace

V klasických výpočtech se používá jako jednotka informace *bit*. Má dvě hodnoty 0 a 1. Spojením více bitů se vyjadřují čísla ve dvojkové soustavě. Abychom mohli provádět výpočty, potřebujeme nějakou sadu operací, které s hodnotami bitů manipulují.

Jedinou operací působící na jediný bit (kromě identity) je negace (NOT), která převrací jeho hodnotu. Standardní dvoubitové operace jsou logické „nebo“ (OR) a „a“ (AND). Každá z nich společně s negací tvoří univerzální soubor, a je tedy možné pomocí nich vyjádřit libovolnou binární operaci. Dále se používá „exkluzivní nebo“ (XOR), které je také označováno jako „kontrolovaná negace“ (CNOT). Nejednoznačnost v názvu je důsledkem dvou různých definic (reprezentací) vedoucích na stejné zobrazení. Jedním je „Jedno nebo druhé, ale ne obě dvě.“ a druhým „Pokud platí A, pak vrať B, jinak vrať negaci B.“ Působení všech operací je přehledně shrnuto v následující tabulce.

A	B	NOT A ($\neg A$)	A OR B ($A \vee B$)	A AND B ($A \wedge B$)	A CNOT B
0	0	1	0	0	0
0	1	1	1	0	1
1	0	0	1	0	1
1	1	0	1	1	0

Tabulka 1 - Tabulka působení logických operací.

Jelikož jsou vstupem funkcí dvě hodnoty a výstupem pouze jedna, nemohou být operace reverzibilní. Pokud k výstupu funkce CNOT přidáme ještě původní vstup A, dostaneme reverzibilní funkci. Obecně všechny reverzibilní logické funkce jsou permutace souboru $((0,0), (0,1), (1,0), (1,1))$.

2.2 Kvantová informace

2.2.1 Jednotka kvantové informace

Jednotkou kvantové informace je *qubit*. Jedná se o informaci nesenou libovolným dvouhladinovým kvantovým systémem, tedy kromě dvou krajních hodnot (0 a 1) může popisovat i jejich libovolnou superpozici.

Pro provádění výpočtů zvolíme takzvanou *výpočetní bázi* $\{|0\rangle, |1\rangle\}$. V ní má obecný stav qubitu tvar

$$|\psi_1\rangle = \alpha |0\rangle + \beta |1\rangle. \quad (2.1)$$

Dvouqubitový systém je pak popsán stavem

$$|\psi_2\rangle = \alpha_{00} |0\rangle \otimes |0\rangle + \alpha_{01} |0\rangle \otimes |1\rangle + \alpha_{10} |1\rangle \otimes |0\rangle + \alpha_{11} |1\rangle \otimes |1\rangle, \quad (2.2)$$

a analogicky pro vícequbitové systémy. Důležité je, že pokud chceme uchovat úplnou informaci o stavu n -qubitového systému na klasickém počítači, potřebujeme na to 2^n komplexních čísel. Z toho je jasné, že složitost simulace kvantových procesů na klasických počítačích roste exponenciálně s počtem qubitů. Nabízí se otázka, zda je možné tento nepoměr obrátit v náš prospěch při provádění výpočtů na kvantovém počítači. Ukázalo se, že to možné je, ale cesta není přímočará (viz dále).

2.2.2 Kvantové logické operace

Vzhledem k odlišnosti základní informační jednotky se liší i kvantové operace (hradla). Jedná se o unitární transformace působící na vektory popisující stav kvantových systémů.

Jelikož qubit je popsán dvěma komplexními čísly (a ne jen hodnotou 1 nebo 0, jako klasický bit), je třída možných jednoqubitových hradel výrazně bohatší. I zde existují univerzální soubory hradel, která mohou nahradit všechna ostatní. Často se volí *fázový posun* a *Hadamardovo hradlo*. Pokud připojíme ještě dvouqubitové hradlo *CNOT*, máme nástroje pro libovolné dvouqubitové (a tím i vícequbitové) transformace. Konkrétní popis hradel je uveden níže.

Chceme-li aplikovat obecnou booleovskou funkci $f(\alpha, \beta)$ na stav $|\alpha\rangle |\beta\rangle$, použijeme transformaci $T|\alpha\beta\rangle = |f(\alpha, \beta)\rangle$. Ta působí na celý stav $|\psi_2\rangle$ jako

$$T|\psi_2\rangle = \alpha_{00} |f(0, 0)\rangle + \alpha_{01} |f(0, 1)\rangle + \alpha_{10} |f(1, 0)\rangle + \alpha_{11} |f(1, 1)\rangle. \quad (2.3)$$

Díky lineární superpozici tedy získáme výsledky pro všechny možné vstupní hodnoty najednou. Problém je, že z jednoho systému můžeme měřením získat vždy zase jen jeden výsledek. Pro využití superpozice je tedy potřeba sofistikovanější postup.

Pro obecné kvantové výpočty budeme potřebovat dva 2^n -rozměrné systémy - vstupní $|x\rangle_1 \equiv |x_1, x_2, \dots, x_{2^n}\rangle_1$ a výstupní $|y\rangle_2 \equiv |y_1, y_2, \dots, y_{2^n}\rangle_2$. Systém 2 je na začátku výpočtu vždy v daném stavu $|in\rangle_2$ a transformace probíhá podle schématu

$$T \sum_x \alpha_x |x\rangle_1 |in\rangle_2 = \sum_x \alpha_x |x\rangle_1 |f(x)\rangle_2. \quad (2.4)$$

2.2.3 Fázový posun

Fázový posun představuje transformaci $\Phi(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta e^{i\phi}|1\rangle$. Toho je možné docílit využitím Hamiltoniánu ve tvaru

$$H = \frac{\lambda}{2}(1 - \sigma_3) = \lambda \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad (2.5)$$

který určuje časový vývoj $e^{-iHt}(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + \beta e^{i\lambda t}|1\rangle$. Nyní už stačí jen pro dané λ zvolit správnou dobu působení t .

2.2.4 Hadamardovo hradlo

Hadamardovo hradlo je pro jednoqubitový systém definováno jako

$$U_2 \equiv \frac{1}{\sqrt{2}}(\sigma_1 + \sigma_3) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \quad (2.6)$$

Efektivně se vlastně jedná o změnu báze. Pro dimenzi 2^n použijeme rekurentní definici

$$U_{2^n} \equiv \begin{bmatrix} U_{2^{n-1}} & U_{2^{n-1}} \\ U_{2^{n-1}} & -U_{2^{n-1}} \end{bmatrix}. \quad (2.7)$$

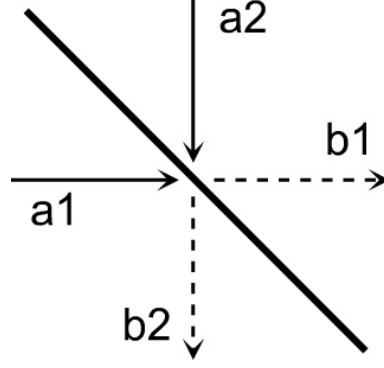
Fyzikálně je možné Hadamardovo hradlo implementovat například pomocí optického elementu zvaného dělič svazku (viz obrázek 2.1). Ten provádí transformaci

$$\begin{bmatrix} b_1 \\ b_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \end{bmatrix}. \quad (2.8)$$

Předefinujeme-li fáze vstupních a výstupních stavů (využijeme hradlo fázového posunu), můžeme transformaci psát jako

$$\begin{bmatrix} b_1 \\ -ib_2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} a_1 \\ ia_2 \end{bmatrix}, \quad (2.9)$$

která nyní funguje jako Hadamardovo hradlo.



Obrázek 2.1: Schéma děliče svazku. Šipky označené $a1$ a $a2$ znázorňují dopadající paprsky světla, z nichž se každý částečně odrazí a částečně projde do směrů $b1$ a $b2$.

2.2.5 Kontrolovaná negace (CNOT)

Kontrolovaná negace je dvouqubitová operace, která převrací hodnotu druhého qubitu v případě, že hodnota prvního je 1. V maticovém vyjádření ve standardní výpočetní bázi má CNOT tvar

$$C \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (2.10)$$

Podobným způsobem jako při využití děliče svazku pro implementaci Hadamardova hradla můžeme předdefinováním vstupních a výstupních stavů nahradit CNOT pomocí fázového posunu pro $e^{i\phi} = -1$. V maticovém vyjádření

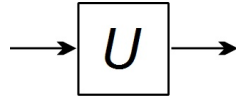
$$\begin{bmatrix} |00\rangle \\ |01\rangle \\ \frac{1}{\sqrt{2}}(|11\rangle + |10\rangle) \\ \frac{1}{\sqrt{2}}(|11\rangle - |10\rangle) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} |00\rangle \\ |01\rangle \\ \frac{1}{\sqrt{2}}(|11\rangle + |10\rangle) \\ \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle) \end{bmatrix}. \quad (2.11)$$

2.3 Kvantové výpočetní obvody

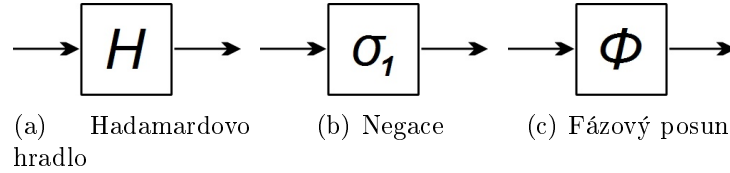
Důležitým krokem na cestě k vytvoření kvantového počítače je možnost provádět na systémech sekvence operací popsaných v předchozí části. Pro obecnou jedno-qubitovou unitární transformaci U , která na stav působí jako

$$U(a_0 |0\rangle + a_1 |1\rangle) = b_0 |0\rangle + b_1 |1\rangle, \quad (2.12)$$

používáme symbol na obrázku 2.2. Symboly pro Hadamardovo hradlo, negaci a fázový posun jsou po řadě na obrázcích 2.3(a), 2.3(b) a 2.3(c).

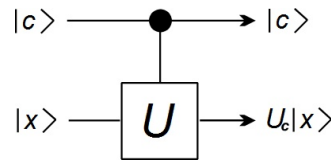


Obrázek 2.2: Značka pro obecnou unitární transformaci.

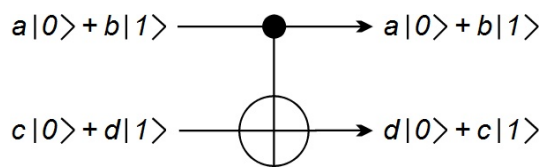


Obrázek 2.3: Jednoqubitová kvantová hradla.

Dále budeme samozřejmě potřebovat vícequbitové transformace. Zde je jeden qubit $|c\rangle$ považován za kontrolní (transformace ho nemění) a na druhý qubit $|x\rangle$ je provedena transformace U_c . Tato transformace je vybrána na základě hodnoty kontrolního qubitu. Odpovídající značka takovéto operace v kvantovém okruhu je na obrázku 2.4. Na obrázku 2.5 je pak kontrolovaná negace jako konkrétní příklad.



Obrázek 2.4: Diagram znázorňující působení hradla U_c na qubit $|x\rangle$, které je závislé na hodnotě kontrolního qubitu $|c\rangle$.



Obrázek 2.5: Diagram dvouqubitového hradla CNOT.

2.4 Kvantová Fourierova transformace

Kvantová Fourierova transformace je důležitý nástroj, který nám konečně umožní využít paralelismus kvantové mechaniky k zásadnímu urychlení algoritmů. (Viz faktorizační algoritmus v další části.) Zde zavedeme Fourierovu transformaci na dimenzi

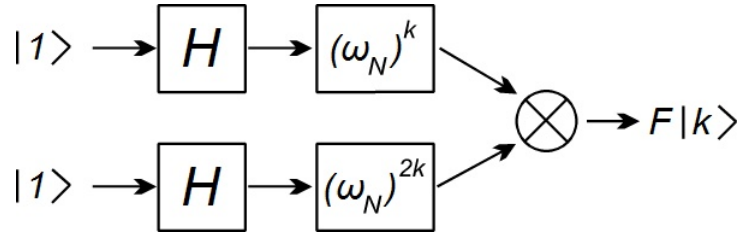
$N = 2^n$, kde n je počet qubitů, se kterými pracujeme. V bázi $\{|0\rangle, |1\rangle, \dots, |N-1\rangle\}$ je definována vztahem

$$F|k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} (\omega_N)^{jk} |j\rangle. \quad (2.13)$$

Zde jsme označili symbolem ω_N N -tou odmocninu z jednotky, tedy

$$\omega_N = \exp\left(i\frac{2\pi}{N}\right). \quad (2.14)$$

Pro přípravu Fourierova obrazu stavu $|k\rangle$ můžeme použít okruh na obrázku 2.6. Musíme však mít klasickou informaci o hodnotě k .



Obrázek 2.6: Okruh pro vytvoření stavu $F|k\rangle$.

2.5 Faktorizační algoritmus

V této části popíšeme, jak je možné využít vlastností kvantové mechaniky k zásadnímu urychlení některých algoritmů. Konkrétně se jedná o algoritmus na hledání dělitelů (faktorů) velkých čísel. Pro klasický počítač roste složitost tohoto problému exponenciálně s velikostí faktorizovaného čísla. Toho se využívá v takzvané aritmetické kryptografii (kryptografie s veřejným klíčem). Máme-li k dispozici něco, co dokáže dostatečně rychle rozkládat velká čísla, můžeme takto zašifrovanou zprávu rozluštit. Shorův algoritmus, který hledá rozklad na (zatím hypotetickém) kvantovém počítači s polynomiální složitostí, vzbudil značný zájem.

Postup faktorizace čísla N můžeme popsat následovně. Zvolíme si y tak, aby bylo s N nesoudělné. Pro některé volby y nemusí procedura vést k cíli, nicméně není možné to zjistit předem. V případě, že postup selže, použijeme jiné y . Hlavním úkolem je pak najít periodu r tak, že platí $y^{l+r} = y^l \pmod{N}$. Potom už máme $y^r = 1 \pmod{N}$, odkud $(y^{r/2} + 1)(y^{r/2} - 1) = y^r - 1 = 0 \pmod{N}$. Jedna ze závorek už musí mít nějaké společné dělitele s N , které snadno najdeme využitím Euklidova algoritmu.

Pro řešení pomocí kvantového algoritmu budeme potřebovat stavový prostor di-

menze D , kde $D > N$, a zařízení schopné provádět transformaci

$$\sum_{j=0}^D |j\rangle_1 |0\rangle_2 = \sum_{j=0}^D |j\rangle_1 |y^j \bmod N\rangle_2. \quad (2.15)$$

Kompletní rozbor Shorova algoritmu v obecném případě je nad rámec této práce. Naším cílem je pouze nastínění využití kvantového počítače jakožto motivace pro rozvíjení tohoto oboru. Proto zde jen uvedeme převzatý příklad z [3] pro $N = 15$ a $y = 7$. Nejprve pomocí zařízení popsaného rovnicí 2.15 připravíme stav

$$\begin{aligned} |\psi\rangle = \frac{1}{\sqrt{16}} (&|0\rangle_1 |1\rangle_2 + |1\rangle_1 |7\rangle_2 + |2\rangle_1 |4\rangle_2 + |3\rangle_1 |13\rangle_2 \\ &+ |4\rangle_1 |1\rangle_2 + |5\rangle_1 |7\rangle_2 + |6\rangle_1 |4\rangle_2 + |7\rangle_1 |13\rangle_2 \\ &+ |8\rangle_1 |1\rangle_2 + |9\rangle_1 |7\rangle_2 + |10\rangle_1 |4\rangle_2 + |11\rangle_1 |13\rangle_2 \\ &+ |12\rangle_1 |1\rangle_2 + |13\rangle_1 |7\rangle_2 + |14\rangle_1 |4\rangle_2 + |15\rangle_1 |13\rangle_2). \end{aligned} \quad (2.16)$$

Vidíme, že perioda r je v tomto případě 4. To je však samozřejmě jen díky tomu, že jsme si klasicky provedli všechny výpočty. Tuto informaci tedy musíme získat jinak. Nejprve provedeme projektivní měření na druhý stav. Výsledkem bude naměření hodnoty y^l a přechod prvního systému do stavu

$$\begin{aligned} |\phi_l\rangle &= \frac{1}{\sqrt{4}} (|l\rangle_1 + |l+r\rangle_1 + |l+2r\rangle_1 + |l+3r\rangle_1) = \\ &= \frac{1}{\sqrt{4}} (|l\rangle_1 + |l+4\rangle_1 + |l+8\rangle_1 + |l+12\rangle_1), \end{aligned} \quad (2.17)$$

kde $l \in \{0, 1, 2, 3\}$. Nyní provedeme Fourierovu transformaci, která stav převede na

$$\begin{aligned} F|\phi_l\rangle &= \frac{1}{\sqrt{4}} \frac{1}{\sqrt{16}} \sum_{j=0}^{15} (\omega_{16})^{jl} |j\rangle (1 + (\omega_{16})^{rj} + (\omega_{16})^{2rj} + (\omega_{16})^{3rj}) \\ &= \frac{1}{8} \sum_{j=0}^{15} (\omega_{16})^{jl} |j\rangle (1 + (e^{2\pi i(\frac{r}{16})j})^1 + (e^{2\pi i(\frac{r}{16})j})^2 + (e^{2\pi i(\frac{r}{16})j})^3). \end{aligned} \quad (2.18)$$

Pro všechna $j \neq \frac{N+1}{r} = \frac{16}{4} = 4$ se čísla v závorce sečtou na nulu a pro $j = 4$ dají součet 4. Tento stav tedy můžeme napsat jako

$$F|\phi_l\rangle = \frac{1}{2} (|0\rangle + (\omega_{16})^{4l} |4\rangle + (\omega_{16})^{8l} |8\rangle + (\omega_{16})^{12l} |12\rangle). \quad (2.19)$$

Nyní provedeme měření, jehož výsledkem bude číslo $m = 4k$. Jelikož víme, že musí platit $m = \frac{N+1}{r}k$ a N i m známe, můžeme r a k určit v polynomiálním čase [4].

Kapitola 3

Fyzikální realizace kvantových počítačů

3.1 Obecné požadavky

Každé laboratorní zařízení, které by mělo potenciálně sloužit jako kvantový počítač, musí splňovat určité základní požadavky. V této části je stručně rozebereme.

Rozlišitelné qubity: Každý qubit musí být nesen jasně lokalizovaným fyzikálním systémem. Musíme mít vždy možnost číst hodnotu zvoleného qubitu a také na něj libovolnou hodnotu zapsat.

Udržitelnost informace: Vzhledem k tomu, že každý kvantový systém nějakým způsobem interaguje se svým okolím, informace, kterou nese, postupně degraduje. Každý takový systém je tedy omezen určitým časem, kdy je ještě informace použitelná. Tento čas spolu s rychlostí provádění operací určuje, kolik výpočtů můžeme se systémem vykonat.

Vzájemné interakce: Jelikož chceme provádět podmíněné (vícequbitové) operace, potřebujeme, aby systémy nesoucí qubity vzájemně interagovaly. Obecně je však problém v tom, že systémy, které jsou odolné vůči narušení okolím (například fotony), málo interagují mezi sebou. Naopak elektrony, které se díky elektrostatickému odpuzování ovlivňují jednoduše, podléhají rychle vlivům vnějšího prostředí.

Univerzalita a škálovatelnost: Abychom mohli z jednotlivých hradel vytvářet komplexní sítě pro kvantové výpočty, je nutné, aby každý výstup mohl sloužit jak vstup pro další operace.

3.2 Elektromagnetické pole v dutině

3.2.1 Reprezentace qubitu

Jedním z možných kandidátů na nositele kvantové informace je foton. Nabízí pohodlnou bázi pro kódování kvantové informace v podobě polarizace. Jelikož je však ve volném prostoru spektrum elektromagnetických vln spojitě, nemůžeme adresovat jednotlivé qubity na základě jejich frekvence. Možné řešení nabízí práce s fotony v dutině délky L , kterou volíme pro jednoduchost popisu jednorozměrnou. Zde máme kvantovací podmínky (vyplývající z okrajových podmínek) ve tvaru $2L = n\lambda$, kde n musí být celé číslo. Tyto podmínky určují jednotlivé módy s diskrétními vlnovými délkami $\lambda_n = \frac{2L}{n}$. Pomocí módů nyní můžeme reprezentovat jednotlivě adresovatelné qubity. Konkrétní tvar módů je

$$u_n(z) = \sqrt{\frac{2}{L}} \sin(k_n z) = \sqrt{\frac{2}{L}} \sin\left(\frac{\pi n}{L} z\right). \quad (3.1)$$

Jelikož každý z těchto módů je možné popsat jako harmonický oscilátor, můžeme použít formalismus kreačních (a_n) a anihilačních ($a_n^\dagger$) operátorů. Pro reprezentaci qubitu využijeme koherentní stavy definované pomocí operátoru

$$D(\alpha) = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha a_n^\dagger} e^{-\alpha^* a_n}, \quad (3.2)$$

jeho působením na vakuový stav $|0\rangle$ jako

$$|\alpha\rangle = D(\alpha) |0\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{n!} |n\rangle. \quad (3.3)$$

Pro malé hodnoty α ($|\alpha| \ll 1$) můžeme pomocí koherentních stavů reprezentovat qubit jako

$$|\alpha\rangle \simeq \frac{|0\rangle + \alpha |1\rangle}{\sqrt{1 + |\alpha|^2}}. \quad (3.4)$$

Podmínka malosti parametru α však také omezuje množství stavů, které se takto dají popsat.

3.2.2 Interakce s látkou

Fotony velmi málo interagují s okolím. To je výhoda, protože se informace v nich uložená dobře uchovává. Na druhou stranu, pro provádění podmíněných hradel (více-qubitových operací), bychom potřebovali jejich vzájemné působení. To k dispozici nemáme a proto je třeba vyřešit situaci zprostředkovaným působením přes atomy látky.

Pro popis atomů použijeme přiblížení Jaynes–Cummingsova modelu. Stav atomu popisujeme pomocí jeho energetických hladin $|i\rangle$ s energií $E_i = \hbar\omega_i$. Pro $E_i > E_j$ může dojít k absorpci fotonu popsané operátorem $a|i\rangle\langle j|$ nebo emisi $a^\dagger|j\rangle\langle i|$. Hamiltonián takového systému je

$$H = \sum_k \hbar\omega_k a_k^\dagger a_k + \sum_i E_i |i\rangle\langle i| + \hbar \sum_{k,i>j} g_{ij} (a_k |i\rangle\langle j| + a_k^\dagger |j\rangle\langle i|), \quad (3.5)$$

kde g_{ij} jsou konstanty. V případě systému obsahujícího pouze jeden mód a dvě energetické hladiny je možné přepsat Hamiltonián do tvaru

$$H = \hbar\omega a^\dagger a + \frac{\hbar\Omega}{2}(1 + \sigma_3) + \hbar g(a\sigma^+ + a^\dagger\sigma^-), \quad (3.6)$$

kde σ_i jsou Pauliho matice a $\sigma^\pm = \frac{1}{2}(\sigma_1 \pm i\sigma_2)$. Řešením Schrödingerovy rovnice pro tento systém jsou funkce

$$|\psi_n\rangle = e^{-i\omega n t} (c_0 |n, 0\rangle + c_1 |n-1, 1\rangle). \quad (3.7)$$

Konstanty $c_0(t)$ a $c_1(t)$ se určí řešením rovnice

$$i \frac{d}{dt} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} 0 & g\sqrt{n} \\ g\sqrt{n} & \Delta \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix}, \quad (3.8)$$

kde $\Delta = \Omega - \omega$. Pokud ještě označíme $\Omega_n^2 = \Delta^2 + 4g^2n$ a nastavíme počáteční podmínky $c_0(0) = 1$ a $c_1(0) = 0$, dostaneme výsledné řešení ve tvaru

$$c_0(t) = \exp\left(-i\frac{\Delta t}{2}\right) \left(\cos\left(\frac{\Omega_n t}{2}\right) + i\frac{\Delta}{\Omega_n} \sin\left(\frac{\Omega_n t}{2}\right)\right), \quad (3.9)$$

$$c_1(t) = -\frac{2ig\sqrt{n}}{\Omega_n} \exp\left(-i\frac{\Delta t}{2}\right) \sin\left(\frac{\Omega_n t}{2}\right). \quad (3.10)$$

Zvolíme-li dobu působení t_π právě tak, aby platilo $\Omega_n t_\pi = \pi$, dostaneme takzvaný π -pulz, který v limitě pro $\Delta \rightarrow 0$ způsobuje inverzi populace. Konkrétně dává koeficienty

$$\begin{aligned} c_0(t_\pi) &\rightarrow 0, \\ c_1(t_\pi) &\rightarrow -i. \end{aligned} \quad (3.11)$$

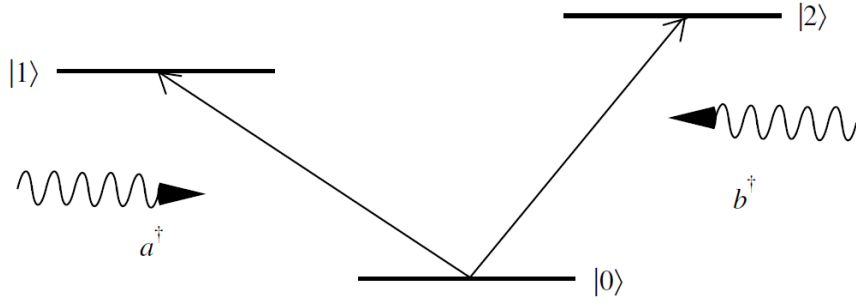
Druhým významným případem je 2π -pulz ($\Omega_n t_{2\pi} = 2\pi$), který vrací populaci do původního stavu, ale s obrácenou fází, tedy

$$\begin{aligned} c_0(t_{2\pi}) &= -\exp\left(-i\frac{\Delta t_{2\pi}}{2}\right) \rightarrow -1, \\ c_1(t_{2\pi}) &= 0. \end{aligned} \quad (3.12)$$

Zde navíc vidíme, že $c_1(t_{2\pi}) = 0$ i pro $\Delta \neq 0$. Toho můžeme využít pro vytvoření fázového posunu. Je třeba upozornit, že takového vyladění $\Omega_n t$ na požadovanou hodnotu je vždy možné jen pro jedno zvolené n .

3.2.3 Vícequbitové operace

Jednou z možností provádění podmíněných operací na stavech elektromagnetického pole v dutině je využití tříhladinového systému. Máme atom, který se může nacházet ve třech energetických stavech $|0\rangle$, $|1\rangle$ a $|2\rangle$. Operátory odpovídajících modů pole, které excitují atom na první, respektive druhou hladinu označíme $a^\dagger$, respektive $b^\dagger$. Situace je znázorněna na obrázku 3.1. Qubity budeme reprezentovat přítomností/absencí fotonu daného modu.



Obrázek 3.1: Tříúrovňový systém energetických hladin atomu umožňující provádět podmíněné operace na modech elektromagnetického pole v dutině. Převzato z [3].

Výchozí stav celého systému je

$$|\psi\rangle_{in} = (\alpha_0 + \alpha_1 a^\dagger)(\beta_0 + \beta_1 b^\dagger) |0\rangle \quad (3.13)$$

a interakční Hamiltonián

$$H_I = \hbar g(a |1\rangle \langle 0| + a^\dagger |0\rangle \langle 1| + b |2\rangle \langle 0| + b^\dagger |0\rangle \langle 2|), \quad (3.14)$$

kde g je konstanta.

Samotnou operaci provedeme pomocí 2π -pulzu. Není-li přítomen foton $a^\dagger$, máme vlastně dvouúrovňový systém se stavy $|0\rangle$ a $|2\rangle$ a jediným módem, tedy situaci popsanou dříve. Dochází tedy k transformaci stavu $(\beta_0 + \beta_1 b^\dagger) |0\rangle \rightarrow (\beta_0 - \beta_1 b^\dagger) |0\rangle$ a analogicky pro nepřítomnost fotonu $b^\dagger$. V případě, kdy jsou excitovány oba módy, však dostaneme obecný fázový posun $e^{i\phi}$. Celkově můžeme transformaci popsat maticí

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix}. \quad (3.15)$$

Uvedená metoda je pouze náznak použití přechodů mezi energetickými hladinami atomů k provádění vícequbitových operací. Její nevýhodou je především využití nepřítomnosti fotonu jako nosiče informace. Falešné signály tak mohou způsobovat chyby.

3.3 Iontové pasti

Současná laserová technika umožňuje zchladit atomy nebo ionty na velmi nízké teploty. Systém se pak blíží stavům s nejnižšími možnými energiemi. Takové ionty je poté možno uvěznit v rychle se měnícím potenciálu, jehož efekt se v čase vystředuje na nulu. Přesto, že toto vnější pole ovlivňuje pohyb iontů, můžeme je stále alespoň přibližně popisovat jako harmonické oscilátory (Paul trap).

Máme-li v pasti více iontů, vzájemně na sebe intenzivně působí odpudivou silou a uspořádávají se do pravidelných struktur (nejjednodušeji řetízku). Společně uvězněné ionty vykonávají kolektivní pohyby. Především oscilace těžiště celého systému a „dýchací“ pohyb, kdy se periodicky zvětšují a zmenšují jejich vzájemné vzdálenosti. Kolektivní pohyby mohou sloužit jako přenašeče informací umožňující podmíněné transformace, zatímco prostorová vzdálenost umožňuje zaměřování světelných prsků na konkrétní iont, a tím jeho individuální adresování.

Působením laseru na dvouúrovňový systém se základním stavem $|g\rangle$ a excitovaným stavem $|e\rangle$ (vnitřní parametr iontu) vyvoláme provázání

$$\Sigma = a |e\rangle \langle g| + a^\dagger |g\rangle \langle e|. \quad (3.16)$$

Zde a a $a^\dagger$ působí na oscilační stav. Odpovídající transformace je

$$U_\theta = \exp(-i\theta\Sigma), \quad (3.17)$$

kde θ je parametr úměrný času působení a můžeme ho tedy volit libovolně. Rozvojem exponenciály do řady dostaneme působení na stavy $\{|e, 0\rangle, |g, 1\rangle\}$ jako

$$\begin{aligned} U_\theta |e, 0\rangle &= \cos(\theta) |e, 0\rangle - i \sin(\theta) |g, 1\rangle \\ U_\theta |g, 1\rangle &= \cos(\theta) |g, 1\rangle - i \sin(\theta) |e, 0\rangle. \end{aligned} \quad (3.18)$$

Speciálně pro $\theta = \pi/2$ má transformace tvar

$$\begin{aligned} U_{\pi/2} |e, 0\rangle &= -i |g, 1\rangle \\ U_{\pi/2} |g, 1\rangle &= -i |e, 0\rangle \end{aligned} \quad (3.19)$$

a pro $\theta = \pi$

$$\begin{aligned} U_\pi |e, 0\rangle &= -|e, 0\rangle \\ U_\pi |g, 1\rangle &= -|g, 1\rangle. \end{aligned} \quad (3.20)$$

Nyní budeme potřebovat dva uvězněné ionty, na kterých budeme provádět výpočet a jeden pomocný. Transformace $U_{\pi/2}^1$ a U_π^2 působí na první a druhý systém. U_π^3 spojuje druhý systém s pomocným a efektivně provádí transformaci $|g\rangle_2 \rightarrow -|g\rangle_2$. Definujeme-li nyní hradlo $U = U_\pi^3 U_\pi^2 U_{\pi/2}^1$, můžeme jej v maticovém vyjádření napsat jako

$$U \approx \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}. \quad (3.21)$$

Tato transformace je ekvivalentní hradlu CNOT, a tedy postačuje pro provádění libovolných logických operací na dvou qubitech. Získáváme tak základní stavební prvek pro kvantový počítač.

3.4 Shrnutí

Přesto, že se již podařilo laboratorně realizovat zařízení schopná udržet určité množství qubitů a provést na nich kvantové operace, do realizace skutečných kvantových počítačů je ještě velmi daleko. Především je zde problém se škálovatelností. Nejpokročilejší experimenty dokáží provádět operace s několika desítkami qubitů (například [5]) a stále se svým výkonem nemohou rovnat klasickým počítačům. Až čas ukáže kdy, na jakém fyzikálním principu a zda vůbec budou fungovat kvantové počítače schopné vysněného faktorizování obrovských čísel a řešení dalších úloh mimo možnosti klasické výpočetní techniky.

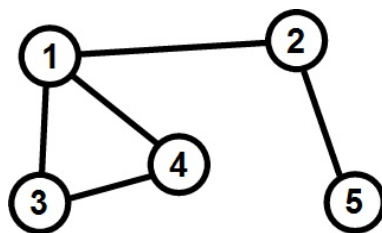
Kapitola 4

Náhodné procházky

4.1 Grafy

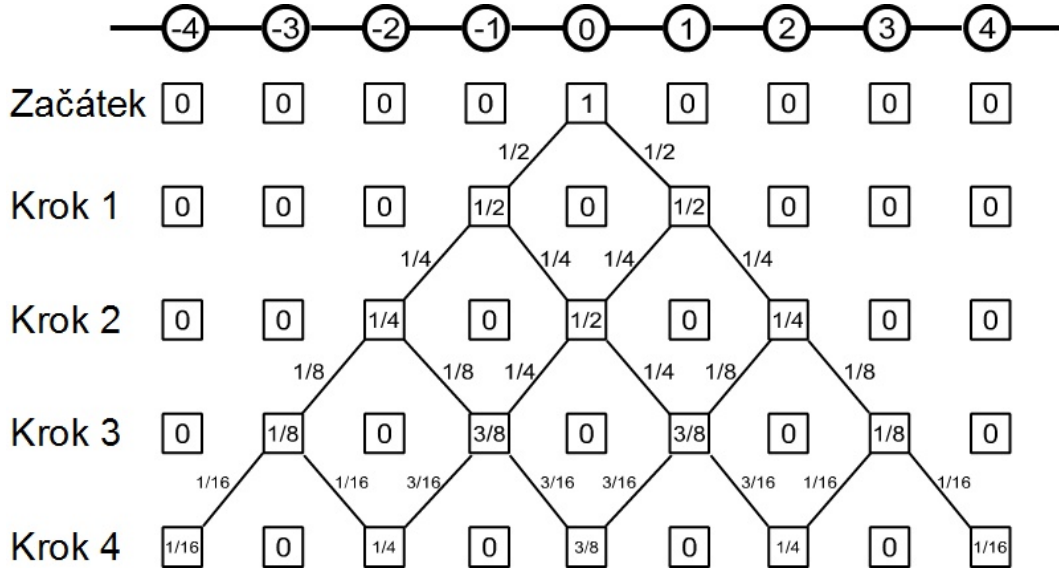
Grafem budeme rozumět uspořádanou dvojici (V, E) množiny vrcholů a množiny hran. Množina V může být i spočetně nekonečná. E je množina vybraných dvojic vrcholů. V tomto podání se tedy jedná o graf neorientovaný (hrany jako dvojice vrcholů jsou neuspořádané) a neohodnocený (všechny hrany jsou „stejně dlouhé“). Téměř výhradně budeme uvažovat *propojené* grafy, tedy takové, kde mezi každými dvěma vrcholy existuje spojnice, která však může být tvořena i více hranami. (Výjimkou je příklad „s-t propojení“.) Ukázka jednoduchého grafu je na obrázku 4.1.

Graf je možné popsat takzvanou *maticí sousednosti*. Jedná se o čtvercovou matici $\mathbf{A} = \{a_{i,j}\}$, kde $a_{i,j} = 1$ pokud E obsahuje hranu mezi i -tým a j -tým vrcholem a $a_{i,j} = 0$ všude jinde. V případě neorientovaného grafu je tedy matice sousednosti symetrická.



Obrázek 4.1: Příklad grafu: množina vrcholů $V = \{1, 2, 3, 4, 5\}$ a množina hran $E = \{\{1, 2\}, \{1, 3\}, \{1, 4\}, \{3, 4\}, \{2, 5\}\}$

Stupeň vrcholu je počet hran, které z daného vrcholu vychází. Je-li stupeň všech vrcholů v daném grafu stejný, nazýváme takový graf *regulárním*.



Obrázek 4.2: 1D náhodná procházka: Čísla ve čtvercích představují pravděpodobnost, s jakou se chodec nachází v tomto místě. Čísla u spojnic jsou pravděpodobnosti uskutečnění právě daného přechodu.

4.2 Klasická náhodná procházka

V této kapitole práce se budeme zabývat kvantovými náhodnými procházkami. Nejprve však zavedeme klasické náhodné procházky a až následně přejdeme k jejich kvantové verzi. Jednoduchým ilustračním příkladem je náhodná procházka na přímce, kterou následně zobecníme na procházky na složitějších grafech. Popíšeme zde jak diskrétní náhodnou procházku, která probíhá v krocích, tak i časově spojitou procházku.

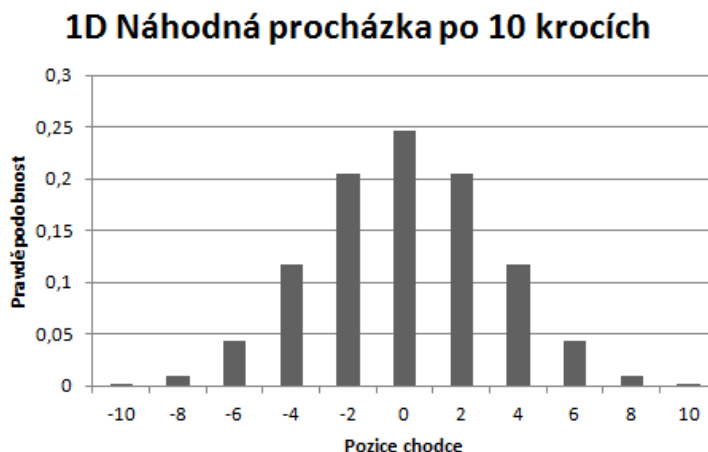
4.2.1 Klasická náhodná procházka na přímce

Nejjednodušším příkladem klasické náhodné procházky je diskrétní náhodná procházka na přímce. V tomto případě se jedná o procházku na grafu, jehož vrcholy jsou reprezentovány celými čísly a hrany jsou vždy jen mezi sousedními vrcholy¹. Na začátku je chodec v bodě 0. Je vybaven mincí, na které s pravděpodobností p padne panna a s pravděpodobností $(1 - p)$ orel. V každém časovém kroku si chodec hodí mincí. Padne-li panna, udělá jeden krok doleva a padne-li orel, udělá krok doprava. Pravděpodobnost, že se po t krocích chodec nachází v místě x označíme $P_t(x)$. Pak P_t je funkce popisující rozdělení pravděpodobnosti polohy chodce v čase t . Příklad prvních kroků této procházky se symetrickou mincí je znázorněn na obrázku 4.2.

Je zřejmé, že v lichém kroku se může chodec nacházet pouze na liché pozici a v sudém na sudé. Pokud v každém kroku bereme pouze body přímky s paritou (sudost/lichost) odpovídající paritě časového kroku, dostáváme na takto vybraných

¹Tedy $V = \mathbb{Z}$ a $a_{i,j} = \delta_{i,j-1} + \delta_{i,j+1}$, kde $\delta_{i,j}$ je Kroneckerovo delta.

bodech binomické rozdělení pravděpodobnosti (viz obrázek 4.3).



Obrázek 4.3: 1D náhodná procházka: Pravděpodobnostní rozdělení polohy chodce po deseti krocích.

Pro následné srovnání s kvantovou procházkou zde uvedeme dvě vlastnosti náhodné procházky. Jednou z nich je střední kvadratická odchylka polohy chodce, která je zde po n krocích úměrná $\sqrt{n}$. Tato veličina v podstatě popisuje rychlost šíření procházky po grafu. Dále je zde fakt, že klasická náhodná procházka je proces bez paměti. Stav v každém kroku je tedy určen pouze polohou chodce v kroku bezprostředně předcházejícím. Zbytek trajektorie, po které se chodec do daného místa dostal, nemá žádný vliv na další průběh procházky.

4.2.2 Klasická náhodná procházka na grafu

Náhodnou procházku můžeme snadno zobecnit na jiné grafy. Omezíme se na takové, ve kterých z každého vrcholu m (nejvýše spočetné množství vrcholů můžeme očíslovat) vede jen konečný počet $d(m)$ hran. Obecně bychom mohli v každém bodě definovat pro každou hranu vedoucí z tohoto bodu pravděpodobnost, že se chodec vydá daným směrem. Tím bychom vlastně získaly orientovaný (pravděpodobnost přechodu z i do j nemusí být stejná jako z j do i) a ohodnocený (pravděpodobnostmi přechodu) graf. My se však omezíme na procházky, kde pravděpodobnost pohybu chodce určitým směrem z vrcholu m závisí pouze na jeho stupni a je ve všech směrech stejná, tedy $1/d(m)$.

Pokud pro rozdělení pravděpodobnosti polohy chodce na začátku P_0 a po jednom kroku P_1 platí $P_0 = P_1$ (a tedy i $P_0 = P_T$ pro libovolné T), nazýváme takové rozdělení *stacionární*. Pro každý graf s konečným počtem vrcholů N existuje nejvýše jedno stacionární rozdělení a to

$$\pi(m) = \frac{d(m)}{2N}. \quad (4.1)$$

Stacionárního rozdělení pro graf s konečným počtem vrcholů má tu vlastnost, že bez ohledu na počáteční rozdělení se k němu náhodná procházka přibližuje pro počet kroků T jdoucí do nekonečna. Rychlost toho přibližování je popsána veličinou zvanou *mixing time*.

Další důležitou vlastností náhodné procházky na grafu je *hitting time* H_{ij} , což je očekávaný počet kroků potřebný k tomu, aby se chodec dostal z vrcholu i do vrcholu j . Souvisejícím parametrem je pak *cover time*, tedy očekávaný počet kroků potřebný k tomu, aby chodec navštívil všechny vrcholy grafu. Cover time je možné shora i zdola omezit násobkem nejhoršího, respektive nejlepšího hitting time daného grafu. Pro klasickou procházku je cover time pro libovolný graf principiálně úměrný alespoň $N \log N$.

4.2.3 Časově spojitá náhodná procházka

Jinou verzí nekvantové náhodné procházky je časově spojitá náhodná procházka na grafu. V tomto případě procházka neprobíhá v diskrétních krocích, ale chodec může v každém vrcholu strávit libovolný časový úsek. Budeme zde opět uvažovat procházku, ve které je pravděpodobnost přesunu do všech sousedících (spojených hranou) vrcholů stejná.

Vyjdeme z diskrétní verze procházky. Mějme matici M , jejíž prvek M_{ij} udává pravděpodobnost přechodu z vrcholu i do vrcholu j , tedy $M_{ij} = 1/d(i)$ v sousedících vrcholech a $M_{ij} = 0$ jinde. Pravděpodobnostní rozdělení procházky $p_i(t)$ se pak v čase (v diskrétních krocích) vyvíjí podle vztahu

$$p_i(t+1) = \sum_j M_{ij} p_j(t). \quad (4.2)$$

Nyní vytvoříme časově spojitou náhodnou procházku přechodem k malé časově nezávislé konstantě γ . Namísto matice M zadefinujeme matici H ² vztahem

$$H_{ij} = \begin{cases} -\gamma & \text{pro } i \neq j \text{ sousedící} \\ 0 & \text{pro } i \neq j \text{ nesousedící} \\ d(i)\gamma & \text{pro } i = j \end{cases} \quad (4.3)$$

Procházka se pak vyvíjí podle diferenciální rovnice

$$\frac{dp_i(t)}{dt} = - \sum_j H_{ij} p_j(t). \quad (4.4)$$

Řešením této rovnice ve vektorovém tvaru pro $\vec{p}(t) = (p_1(t), p_2(t), \dots, p_N(t))$ je $\vec{p}(t) = e^{-Ht} \vec{p}(0)$.

²Označení není náhodné a v kvantovém případě bude tato matice nahrazena Hamiltoniánem.

4.3 Kvantové procházky

4.3.1 Diskrétní kvantová procházka na přímce

Soustředme se nyní na kvantovou verzi náhodné procházky. Zde se již nepoužívá označení náhodná, protože proces je ve skutečnosti deterministický. Náhodnost vychází až z pravděpodobnostního chování při finálním měření. Na rozdíl od klasické částice se chodec v kvantovém světě nenachází daném vrcholu grafu, ale v lineární superpozici různých poloh. Může se tedy v podstatě vydat více směry najednou.

Pro jednoduchost nejprve opět vezmeme případ procházky na přímce s vrcholy označenými celými čísly. Mějme $\mathcal{H}_P$ Hilbertův prostor popisující polohu chodce a stavy odpovídající umístění chodce ve vrcholu m označíme $|m\rangle$. Stejně jako v klasickém případě probíhá vývoj procházky v krocích, které jsou podmíněny stavem mince. I ta je zde ale kvantová. Je reprezentována nějakým vnitřním stavem částice (například spinem u elektronu nebo polarizací u fotonu). Nechť $\mathcal{H}_C$ je Hilbertův prostor pro minci s bázovými stavy $|L\rangle$ a $|R\rangle$. Celkově je tedy stav našeho chodce prvkem $\mathcal{H} = \mathcal{H}_P \otimes \mathcal{H}_C$ a obecně vypadá jako

$$|\psi\rangle = \sum_m (\psi_{mL} |mL\rangle + \psi_{mR} |mR\rangle). \quad (4.5)$$

kde ψ_{mL} a ψ_{mR} jsou komplexní čísla splňující $\sum_m (|\psi_{mL}|^2 + |\psi_{mR}|^2) = 1$.

Jeden krok procházky se pak skládá ze dvou transformací. Transformace C změní stav mince a transformace S na základě stavu mince vykoná patřičný posun chodce na grafu. Zde C může být libovolná unitární transformace na prostoru odpovídající dimenze. (Na složitějších grafech, než je přímka, někdy potřebujeme vícerozměrnou minci.) Jako jednoduchý příklad si vezmeme Hadamardovu transformaci

$$C_H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (4.6)$$

která působí jako

$$\begin{aligned} C_H |L\rangle &= \frac{1}{\sqrt{2}}(|L\rangle + |R\rangle), \\ C_H |R\rangle &= \frac{1}{\sqrt{2}}(|L\rangle - |R\rangle). \end{aligned} \quad (4.7)$$

Vzhledem k tomu, že tato operace působí jen na stav mince, je výsledná transformace celého stavu dána operátorem $C = C_H \otimes I_P$, kde I_P je jednotkový operátor na $\mathcal{H}_P$. Posun chodce je dán operátorem

$$S = |m-1, L\rangle \langle mL| + |m+1, R\rangle \langle mR|, \quad (4.8)$$

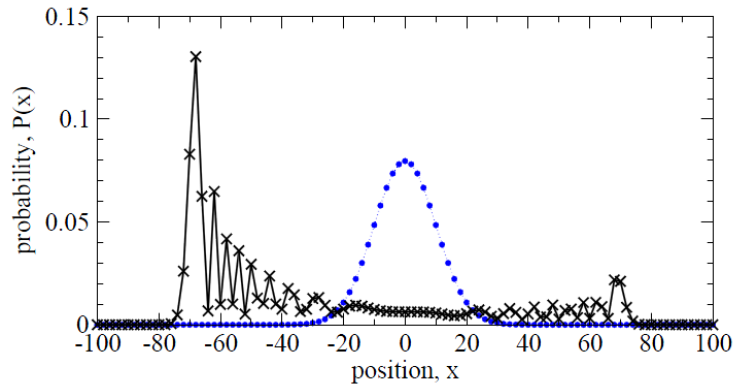
který jednotlivé stavy transformuje jako

$$\begin{aligned} S|mL\rangle &= |m-1, L\rangle, \\ S|mR\rangle &= |m+1, R\rangle. \end{aligned} \quad (4.9)$$

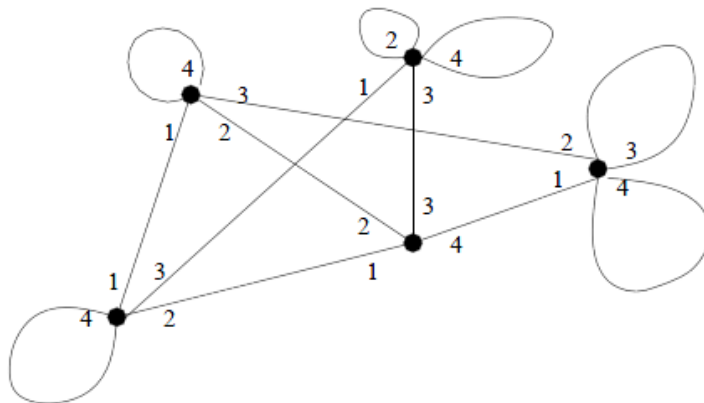
Procházka, která začíná například ve stavu $|0L\rangle$, je po n krocích ve stavu $|\psi_n\rangle = (CS)^n |0L\rangle$.

Měření polohy, které způsobí kolaps vlnové funkce do některého konkrétního stavu, je třeba provést až po určitém počtu kroků. Kdybychom prováděli měření po každém kroku, dostali bychom klasickou náhodnou procházku. Transformace mince pak odpovídá rozložení pravděpodobností na klasické minci a kvantový krok následovaný měřením představuje hod klasickou mincí a klasický krok v patřičném směru. Naopak, pokud provedeme měření až po vykonání většího počtu kroků (pro procházku na přímce s Hadamardovou mincí alespoň 3), dostaneme jiné rozdělení pravděpodobností.

Jedním ze zásadních rozdílů oproti klasické náhodné procházce je to, že se kvantová procházka šíří po grafu úměrně počtu kroků n . To je oproti klasické procházce, kde je rychlost šíření úměrná $\sqrt{n}$, kvadratické urychlení. Další odlišností je, že pro úplný popis kvantové procházky musíme znát kompletní hodnoty koeficientů rozkladu do báze $\mathcal{H}$. To znamená včetně fáze komplexních čísel a ne jen jejich absolutní hodnoty. Proto není následující krok kvantové procházky plně určen pouhým pravděpodobnostním rozdělením v předchozím kroku, jako je tomu u klasické náhodné procházky. Na obrázku 4.4 jsou znázorněna rozdělení pravděpodobnosti nalezení chodce v daném místě po 100 krocích klasické náhodné procházky se symetrickou mincí a kvantové procházky s Hadamardovou mincí. Převaha pravděpodobnosti v levé části grafu je dána volbou stavu mince v počátečním stavu $|0L\rangle$.



Obrázek 4.4: Klasická náhodná procházka se symetrickou mincí (tečky) a kvantová procházka s Hadamardovou mincí a počátečním stavem $|0L\rangle$ (křížky) po 100 krocích. Převzato z [6].



Obrázek 4.5: Příklad grafu pro kvantovou procházku s dodefinovanými hranami na počet maximálního stupně grafu. Převzato z [7].

4.3.2 Diskrétní kvantová procházka na grafu

Nyní se budeme zabývat zobecněním diskrétní kvantové procházky pro případ obecnějšího grafu. Konkrétně půjde o graf, pro který existuje maximální stupeň vrcholu d . (Tedy všechny vrcholy daného grafu mají stupeň d nebo nižší.) Vrcholy opět můžeme očíslovat a stav odpovídající umístění chodce v m -tém vrcholu značit $|m\rangle$. Co se týče hran, máme zde problém s jejich různým počtem v různých vrcholech. V zásadě máme dvě možnosti, jak situaci řešit.

Jedním východiskem je dodefinování potřebného počtu „smyček“ v každém vrcholu. Tedy takových hran, které vedou z vrcholu m opět do m . Potom můžeme v každém vrcholu označit hrany čísla od 1 do d a použít všude stejnou d -rozměrnou minci. Příklad takového grafu je na obrázku 4.5. Transformace mince je v tomto případě zcela analogická jako u procházky na přímce, jen zde máme místo báze $\{|0\rangle, |1\rangle\}$ bázi $\{|J\rangle\}_{J=1}^d$. Krok procházky je pak dán transformací S působící na báze $|mJ\rangle$ způsobem $S|mJ\rangle = |kJ\rangle$, kde k je vrchol, do kterého míří hrana označená ve vrcholu m číslem J . (Ve vrcholu k může mít tato hrana jiné označení.) V případě, že stav mince odpovídá hraně vedoucí zpět do původního vrcholu (smyčce), se při kroku procházky takový stav nezmění.

Druhou možností je nechat graf v původní podobě a definovat různé mince podle stupně příslušného vrcholu. (Samozřejmě je možné definovat i více druhů mince pro různé vrcholy se stejným stupněm.) Nyní už však transformace mince závisí na poloze chodce a není ji možné popsat jako $C = C_C \otimes I_P$, kde C_C označuje působení na Hilbertově prostoru mince a I_P je identita na prostoru poloh.

Pokud chceme i ve vrcholech se stupněm $d > 2$ docílit rovnoměrného rozdělení pravděpodobnosti mezi všechny hrany, jednou z možností je využít takzvané DFT mince (diskrétní Fourierova transformace). Ta je popsána vzorcem (2.13) (po záměně N za d) a pro případ $d = 2$ přechází v Hadamardovu transformaci.

Ukázali jsme zde způsob, jak je možné zavést diskrétní kvantovou procházku na

velmi obecné třídě grafů. Bez znalosti další struktury grafu však nejsme schopni říct mnoho o jejím vývoji. Proto se často přechází ke zkoumání konkrétnějších, nějakým způsobem pravidelných grafů.

4.3.3 Časově spojitá kvantová procházka

Časově spojitá kvantová procházka je analogií spojitě náhodné procházky. Neprobíhá tedy v diskrétních časových krocích, ale vyvíjí se spojitě a finální měření můžeme provést v libovolném okamžiku. Spojitá kvantová procházka odpovídá Schrödingerovu časovému vývoji částice s Hamiltoniánem odvozeným z matice sousednosti grafu, na kterém je procházka prováděna. Konkrétně $H = \gamma A$, kde γ představuje pravděpodobnost přechodu přes hranu za jednotku času a A je matice sousednosti. Formálním řešením Schrödingerovy rovnice dostaneme stav chodce v čase t ve tvaru

$$|\psi(t)\rangle = e^{-i\gamma A t} |\psi(0)\rangle. \quad (4.10)$$

V této verzi kvantové procházky není žádná mince a stav je tedy určen jen v prostoru poloh.

Získaný časový vývoj je do jisté míry obdobný diskrétní kvantové procházce, kde operátor časového vývoje $U = SC$ nahradíme operátorem $U = e^{-i\gamma A}$. Časový vývoj v obou variantách pak můžeme zapsat jako $|\psi(t)\rangle = U^t |\psi(0)\rangle$. Jsou zde ale i některé rozdíly. Díky absenci mince například výsledné rozdělení a chování procházky daleko méně závisí na počátečním stavu.

Na rozdíl od klasických procházek není časově spojitá kvantová procházka přímo limitou diskrétní kvantové procházky pro malé kroky. Absence mince například způsobuje, že je zde vždy rozdíl ve velikosti Hilbertova prostoru, na kterém procházka probíhá.

4.3.4 Dekohherence v kvantových procházkách

Žádný systém nemůžeme dokonale izolovat od vnějších vlivů. Kvantové systémy jsou proto náchylné k takzvané *dekoherenci*. Dochází k provázání zkoumaného systému s okolím (jinými systémy, jejichž stavy nemůžeme kontrolovat). Výsledný celkový provázaný stav se sice může vyvíjet unitárně, nicméně vývoj jednotlivých podsystémů unitární obecně není. Tím jsou tedy efektivně prováděny neunitární transformace na našem systému. Dalším důležitým příkladem neunitárního vývoje jsou měření. Ke ztrátě kvantových vlastností může docházet i v důsledku unitárních transformací, které jsou však aplikovány náhodně. (Například v každém kroku náhodně změním minci nebo provedeme náhodný fázový posun [6].) Je nutné takové jevy zkoumat, abychom měli přehled o tom, do jaké míry se zachovává námi požadovaný stav. Neunitární transformace nám navíc dávají širší třídu nástrojů, díky kterým můžeme někdy záměrně měnit průběh procházky v náš prospěch.

Ve většině případů dekoherence způsobuje ztrátu kvantových vlastností a přechod

ke klasickému vývoji. Extrémní příklad neunitárního vývoje jsme zde již zmínili - případ diskrétní kvantové procházky, která měřena po každém kroku, je přímo klasickou diskrétní náhodnou procházkou.

Kvůli neunitaritě transformací již nemáme čisté stavy, ale musíme systém popisovat pomocí matice hustoty. Její obecný tvar pro diskrétní kvantovou procházku je

$$\rho = \sum_{xc} \sum_{x'c'} c_{xcx'c'} |xc\rangle \langle x'c'|, \quad (4.11)$$

kde xc a $x'c'$ jsou všechny přípustné stavy vrcholů grafu a stavu mince. Operátor $\mathcal{U}$ zobrazuje matici hustoty opět na matici hustoty právě tehdy, když je možné ho zapsat pomocí Krausových operátorů jako

$$\mathcal{U}\rho = \sum_{i \in \Theta} \mathbb{U}_i^\dagger \rho \mathbb{U}_i, \quad (4.12)$$

kde $\sum_{i \in \Theta} \mathbb{U}_i^\dagger \mathbb{U}_i = I$. Pro unitární vývoj máme tento operátor jen jeden a to $\mathcal{U} = SC$, který působí jako

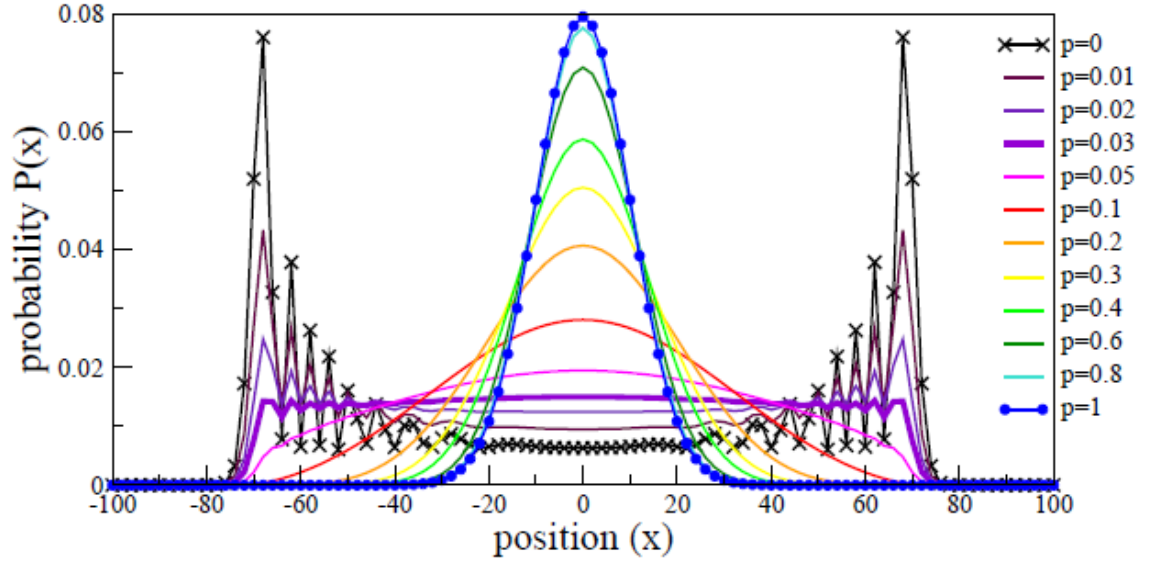
$$\mathcal{U}\rho = SC\rho C^\dagger S^\dagger. \quad (4.13)$$

Neunitární vývoj můžeme dostat tak, že použijeme neunitární minci či neunitární operátor přesunu nebo k některým krokům přidáme měření. Vývoj procházky s měřeními je pak popsán rovnicí

$$\mathcal{U}\rho = \sum_{i \in \Theta} \mathbb{P}_i SC\rho C^\dagger S^\dagger \mathbb{P}_i. \quad (4.14)$$

Rovnice (4.14) je výchozím bodem pro další zkoumání jak analytické, tak numerické. Přehled pro různé varianty grafu (přímka, cyklus, hyperkrychle) a dekoherence (jen mince, jen vrcholy, obojí) je možné najít v práci [6].

Pro ilustraci zde uvedeme zajímavý případ chování procházky na přímce. Numerický model procházky po 100 krocích pro různé úrovně dekoherence (mince i pozice) je na obrázku 4.6. Významná je zde hodnota $p = 0,03$, při které má pravděpodobnostní rozdělení procházky téměř obdélníkový tvar. Tato vlastnost může být výhodná při případném algoritmickém použití kvantových procházek.



Obrázek 4.6: Diskrétní náhodná procházka po 100 krocích. Hodnota p je pravděpodobnost, s jakou je v každém kroku provedeno náhodné měření části systému. Převzato z [6].

Pro časově spojitě kvantové procházky je obecně méně výsledků. Jednak jsou zde náročnější numerické simulace, jednak není možné zkoumat dekoherenci mince, pro kterou bylo nalezeno mnoho analytických výsledků [6].

Kapitola 5

Využití náhodných a kvantových procházek

5.1 Využití klasických náhodných procházek

Nejprve uvedeme dva příklady použití klasické náhodné procházky v oblasti informatiky převzaté z [7] a následně jednoduchý popis využití náhodné procházky při hodnocení webových stránek.

5.1.1 Problém s-t propojení

Jedná se o úlohu, kde nás zajímá, zda existuje cesta mezi vrcholy s a t . Jednou možností řešení této úlohy je zřejmě postupné procházení grafu s ukládáním celé historie. Takový algoritmus po konečném čase (předpokládáme konečný graf) najde patřičnou spojující cestu, nebo projde celou oddělenou část grafu, ve které se vrchol t nenachází. V obou případech máme stoprocentně správnou odpověď za cenu nároků na paměť úměrných počtu vrcholů N . Musíme-li paměti šetřit, můžeme využít náhodnou procházku. Náš algoritmus si bude pamatovat jen své umístění a z něj se vždy vydá náhodným směrem. Pokud dorazí do vrcholu t , máme jistotu, že spojnice existuje. Podle [7] bylo ukázáno, že pokud spojnice existuje, pak bude nalezena s pravděpodobností alespoň $1/2$ po vykonání N^3 kroků náhodné procházky. Pro zvýšení pravděpodobnosti můžeme proces vícekrát opakovat. Nikdy však nezískáme stoprocentní jistotu, že spojnice neexistuje.

5.1.2 2-SAT problém

Tato zdánlivě velmi akademická úloha má velký význam v teoretické informatice. Jedná se o speciální případ obecnější třídy SAT problémů. Máme soubor k logických výroků $C_1, \dots, C_k$ typu $C_i = A \vee B$.¹ A a B jsou v každém výroku

¹Obecně pro n -SAT problém je zde n členů spojených $\vee$.

nahrazeny nějakými booleovskými veličinami (nabývají jen hodnoty 0-TRUE a 1-FALSE) z daného souboru $X_1, \dots, X_l$ nebo jejich negacemi (například $C_1 = (X_2) \vee (\neg X_4)$). Konkrétní výběr hodnot těchto veličin pak můžeme reprezentovat číslem ve dvojkové soustavě $X = X_1 \dots X_l$. (Například pro $l = 3$ a volbu $X_1 = 0$, $X_2 = 1$ a $X_3 = 0$ máme $X = 010$.) Ze všech výroků vytvoříme jeden způsobem: $C = C_1 \wedge C_2 \wedge \dots \wedge C_k$. Pokud existuje takový výběr X , pro který jsou všechny výroky splněny, je výrok C uspokojitelný.

Předpokládejme, že řešení našeho 2-SAT problému existuje a je jediné. Pro jeho nalezení využijeme náhodnou procházku. Na začátku zvolíme sekvenci X náhodně a kontrolujeme její správnost pro jednotlivé výroky dokud nenarazí na takový, který touto volbou není splněn. Ten obsahuje dvě veličiny X_a a X_b . Víme, že alespoň jednu z nich musíme změnit. Jednu tedy náhodně zvolíme a otočíme její hodnotu. Nyní se opět vracíme ke kontrolování. Vzdálenost našeho současného stavu od správného řešení můžeme měřit pomocí takzvané Hammingovy vzdálenosti. Pro dvě binární čísla je to počet bitů, ve kterých se od sebe liší. V našem případě prohozením hodnoty jedné veličiny tuto vzdálenost vždy o 1 zmenšíme nebo zvětšíme (obojí s pravděpodobností $1/2$). Jedná se tedy o náhodnou procházku na úsečce délky k se symetrickou mincí. Pozice chodce je dána Hammingovou vzdáleností našeho odhadu od správného řešení. Z teorie víme, že taková náhodná procházka má cover time ² v řádu k^2 a po tomto počtu kroků se dostane ³ i do bodu 0, tedy správného řešení.

5.1.3 Google PageRank

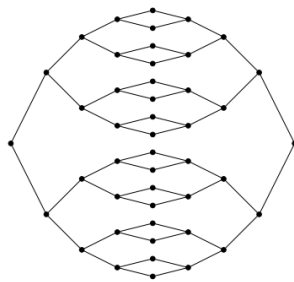
Těžko bychom dnes hledali někoho, kdo nikdy neslyšel o vyhledávači Google.com. Firma Google pochopitelně nezveřejňuje detaily kódů svých programů a neodhaluje všechna svá tajemství. Nicméně základní myšlenka jeho hodnocení obsahu stránek (jeden z klíčových kroků k úspěchu Googlu) je k dispozici. (Podrobnější popis s příklady v [8].)

Kritérium hodnocení obsahu je jednoduché: Webová stránka A předává každé stránce B , na kterou z ní vede odkaz určitou hodnotu významu. Tato hodnota je přímo úměrná hodnocení stránky A a nepřímo úměrná celkovému počtu odkazů vedoucích z A . Chceme-li, aby se náš web objevoval na předních místech vyhledávání, musí na něj odkazovat co nejvíce dobře hodnocených webů. (Dalším kritériem je samozřejmě relevance k vyhledávanému výrazu.)

Proces hodnocení je možné chápat jako náhodnou procházku na orientovaném grafu. Chodec („surfer“) začne na nějaké stránce a přemístí se na náhodně vybraný odkaz, který na ní najde. A tak se pohybuje stále dál. Ve výsledku (po dostatečném počtu kroků) dostaneme stacionární rozdělení, kde pravděpodobnost nalezení chodce v určitém vrcholu grafu odpovídá hodnocení stránky. Kvůli orientovanosti grafu (ne vždy vede cesta zpět) musíme ještě vyřešit problém stránek, které neodkazují nikam nebo jsou částí uzavřeného cyklu. To nejjednodušeji uděláme tak, že přejdeme k náhodné procházce s *teleportací*. Stanovíme pravděpodobnost s jakou se chodec

²Tedy počet kroků, po kterém procházka navštíví všechny vrcholy grafu.

³Samozřejmě jen s určitou pravděpodobností, stejně jako v předchozím případě.



Obrázek 5.1: Graf „slepených stromů”. Převzato z [9].

místo přesunu po odkazu teleportuje do zcela náhodně zvoleného vrcholu.

Výsledkem výše popsaného algoritmu je velmi úspěšný systém hodnocení, který je odolný vůči snaze uměle zvyšovat hodnocení určitého webu. (Můžeme ovlivnit rozdělení hodnoty jednotlivých stránek na vlastním rozsáhlejší webu, ale ne jeho celkovou hodnotu.)

5.2 Využití kvantových procházek

Jednu možnost využití kvantových procházek představují algoritmy pro klasické procházky. Zde v některých případech můžeme dosáhnout zásadního urychlení. Typicky se však jedná o grafy s nějakou pravidelnou strukturou. Například na grafu takzvaných „slepených stromů” (viz obrázek 5.1) dorazí kvantová procházka z jednoho konce na druhý exponenciálně rychleji, než klasická [9]. To však samo o sobě neposkytuje žádné algoritmické využití.

5.2.1 Groverův algoritmus

Slibnou oblastí pro aplikaci kvantových procházek je vyhledávání v nesetříděné databázi (seznamu). Jde tedy o problém, kdy máme najít daný prvek z nějakého souboru, který nemá žádnou další strukturu (například hledání jména k zadanému číslu v telefonním seznamu). Prozkoumání jednoho prvku nám nedává žádnou informaci o tom, kde by bylo dobré s hledáním pokračovat, a proto jakýkoli klasický algoritmus bude potřebovat alespoň $O(N)$ operací, kde N je počet záznamů v seznamu. Naproti tomu Groover v článku [10] popisuje kvantový algoritmus, kterému na nalezení zadaného prvku stačí jen $O(\sqrt{N})$ kroků.

Mějme řetězec o n bitech (v našem případě tedy qubitech). Ten má $N = 2^n$ možných hodnot, které zde představují položky seznamu. Existuje právě jeden hledaný stav S_h , pro který testovací podmínka $C(S_h) = 1$ a pro všechny ostatní stavy platí $C(S) = 0$. Předpokládáme, že výpočet $C(S)$ pro jeden daný stav je možné provést v jednom kroku.

Krok 1: Vezměme jako počáteční stav takový, že hodnoty všech qubitů jsou 1.

Na každý qubit aplikujeme Hadamardovu transformaci

$$M = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (5.1)$$

kteřá dává $M|1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle)$. Tím tedy získáme stav, ve kterém jsou všechny možnosti zastoupeny s amplitudou $2^{-\frac{N}{2}}$. (Stejně jsou přímo amplitudy, ne jen jejich absolutní hodnoty.) Na tento krok potřebujeme jen $O(n)$, tedy $O(\log(N))$ kroků.

Krok 2: Následující proceduru budeme opakovat $O(\sqrt{N})$ krát a tím je vlastně dána složitost celého algoritmu. Nejprve je provedena transformace, která otočí znaménko u amplitudy stavu S_h (fázový posun o π) a ostatní ponechá beze změny. Dále použijeme takzvanou difuzní transformaci D definovanou maticí

$$D_{ij} = \begin{cases} \frac{2}{N} & i \neq j \\ \frac{2}{N} - 1 & i = j \end{cases}. \quad (5.2)$$

Krok 3: Provedeme měření systému. Díky předchozímu postupu je nyní pravděpodobnost přechodu systému do stavu S_h alespoň $\frac{1}{2}$ [10].

5.2.2 Univerzální výpočty pomocí časově spojitě kvantové procházky

Childs [11] jako první ukázal, že kvantové procházky mohou sloužit jako univerzální kvantový počítač. Konkrétně se jedná o konstrukci hradla CNOT, fázového posunu a hradla pro změnu báze. Jeho odvození využívající právě časově spojitou náhodnou procházku je v následující části stručně popsáno.

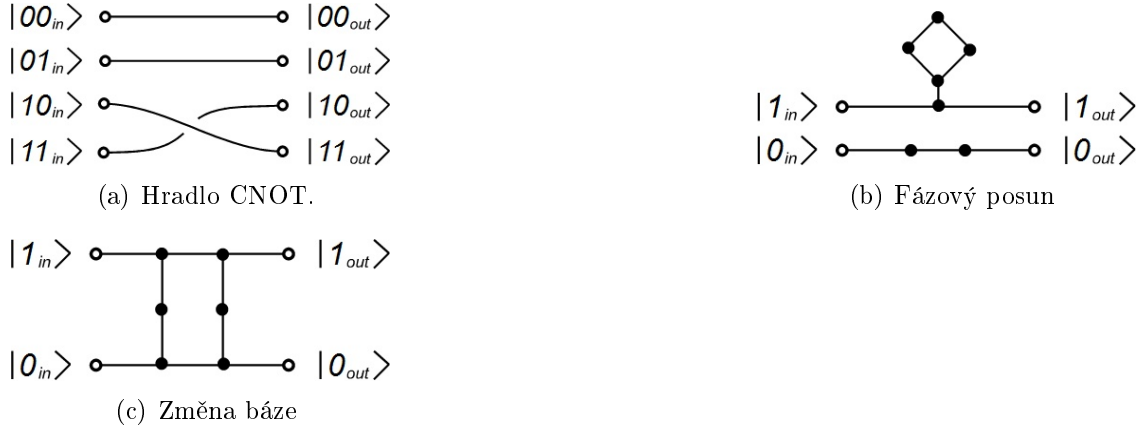
Mějme nějaký graf s maticí sousednosti A . Hilbertův prostor naší kvantové procházky je generován ortogonálními stavy reprezentujícími umístění chodce v daném vrcholu grafu. Samotná procházka pak odpovídá Schrödingerovu vývoji částice pohybující se na grafu. Odpovídající unitární operátor časového vývoje za čas t je e^{-At} .

Je-li grafem procházky nekonečný řetízek - každý vrchol je spojen se dvěma sousedními ($x \in \mathbb{Z}$), pak vlastní stavy dané matice sousednosti A jsou vlastní stavy hybnosti. Pro příchozí vlnu o hybnosti $k \in (-\pi, 0)$ označenou jako $|k\rangle$ máme

$$\langle x | k \rangle = e^{ikx}. \quad (5.3)$$

V této konstrukci se využívá popisu hradla jako konečného grafu, na jehož některých vrcholech jsou připojeny nekonečné řetízky přenášející vstupní a výstupní signál. Díky konečné rychlosti šíření v praxi stačí použít dostatečně dlouhé konečné vedení aniž by tím byla narušena adekvátnost popisu.

Hradlo CNOT získáme pouhým překřížením příslušných vedení, jak je ukázáno na obrázku 5.2(a).



Obrázek 5.2: Implementace kvantových hradel pomocí časově spojitě kvantové procházky. Převzato z [11].

Schéma pro fázový posun je na obrázku 5.2(b). Jeho efektivní délka odpovídající přímému šíření je 2 (tento počet vrcholů je tedy umístěn na druhém vlákně). Hradlo dobře funguje jen pro stavy s hybností blízkou $-\pi/4$. To nás však neomezuje, protože je možné veškeré výpočty provádět pouze se stavy s hybností blízkou právě této hodnotě. Pro vhodné stavy pak hradlo fázového posunu provádí transformaci

$$U_b = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}. \quad (5.4)$$

Při implementaci hradla pro změnu báze budeme potřebovat interakci mezi dvěma vodícími linkami. Schéma je na obrázku 5.2(c). Konkrétní tvar transformace je

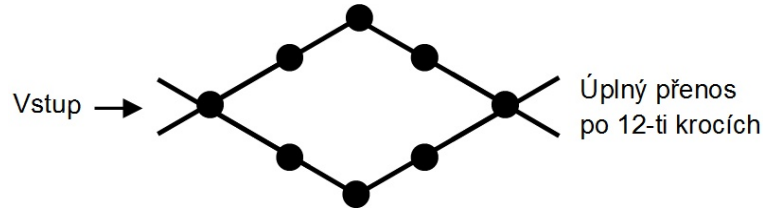
$$U_c = -\frac{1}{\sqrt{2}} \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}. \quad (5.5)$$

Díky tomu, že pro stavy s hybností $-\pi/4$ v uvedených konstrukcích nedochází k odrazu, můžeme tři výše popsaná hradla libovolně řetězit a vytvářet tak libovolné kvantové výpočetní okruhy. Například Hadamardovo hradlo získáme jako $U_H = U_b^2 U_c U_b^2$. Při konstrukci okruhů sice vyvstávají další problémy například s přípravou stavů dostatečně podobných vlastním stavům hybnosti a s vázanými stavy, nicméně v [11] je popsáno, jak je možné je vyřešit.

5.2.3 Univerzální výpočty pomocí diskrétní kvantové procházky

V návaznosti na práci [11] ukázal kolektiv autorů v článku [12], že i diskrétní kvantová procházka může provádět veškeré kvantové výpočty.

Nejprve budeme potřebovat vedení schopné přenášet procházku jedním směrem. Obecně totiž dochází na vrcholech grafu k interferenci, jejímž výsledkem je částečný odraz chodce zpět do původního směru. Pro tento účel použijeme strukturu na obráz-



Obrázek 5.3: Struktura, která během 12-ti kroků úplně přenesení stav z jednoho konce na druhý. Převzato z [12].

ku 5.3. Používá se zde takzvaná Groverova mince, která má pro dimenzi 4 tvar

$$G^{(4)} = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}. \quad (5.6)$$

Tuto minci použijeme ve všech vrcholech se stupněm 4. (Celá konstrukce je provedena tak, aby se ve všech vrcholech daného stupně používala stejná mince.) Důležité pro přenos stavu je, aby byla tato struktura napojena dvěma hranami. Při napojení jednou hranou by i zde docházelo ke zpětným odrazům. Ve vrcholech stupně 2 se používá dvoudimenzionální Groverova mince, která má tvar

$$G^{(2)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (5.7)$$

Budeme zde opět konstruovat hradlo CNOT, fázový posun $P_{\frac{\pi}{8}}$ (rovnice 5.8) a dále jednoqubitové Hadamardovo hradlo.

$$P_{\frac{\pi}{8}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \quad (5.8)$$

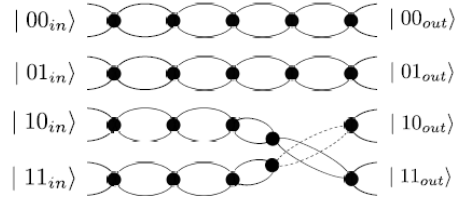
CNOT vytvoříme stejně jako ve spojitém případě pouze prohozením vláken na druhém qubit. Schéma je na obrázku 5.4.

Pro vytvoření fázového posunu částečně předdefinujeme minci ve vrcholech stupně 4 na tvar

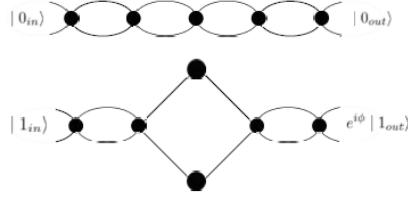
$$G_{\varphi}^{(4)} = e^{i\varphi} G^{(4)}, \quad (5.9)$$

kde pro naši volbu hradla $P_{\frac{\pi}{8}}$ zvolíme $\varphi = \frac{\pi}{4}$. Při průchodu každým takový vrcholem tedy nabýváme fázový posun, který však nemá žádný vliv, dokud je na všech vláknech stejný. Nyní můžeme implementovat hradlo fázového posunu podle schématu na obrázku 5.5.

Nejsložitější je vytvoření Hadamardova hradla, jelikož vyžaduje vzájemnou interakci dvou qubitů a budeme zde mít vrchol stupně 8. V takových vrcholech definujeme



Obrázek 5.4: Schéma pro CNOT. Obloučky představují vedení z obrázku 5.3. Převzato z [12].



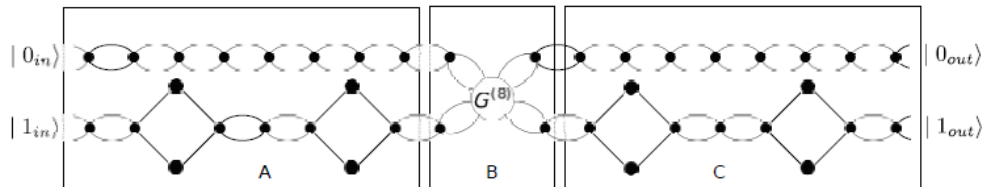
Obrázek 5.5: Schéma pro fázový posun. Obloučky představují vedení z obrázku 5.3. Převzato z [12].

minci ve tvaru

$$G^{(8)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & i & i & -1 \\ 0 & 0 & 0 & 0 & i & 1 & -1 & i \\ 0 & 0 & 0 & 0 & i & -1 & 1 & i \\ 0 & 0 & 0 & 0 & -1 & i & i & 1 \\ i & -1 & 1 & i & 0 & 0 & 0 & 0 \\ -1 & i & i & 1 & 0 & 0 & 0 & 0 \\ 1 & i & i & -1 & 0 & 0 & 0 & 0 \\ i & 1 & -1 & i & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (5.10)$$

Výsledné schéma pro Hadamardovo hradlo je na obrázku 5.6.

Takto vytvořená hradla můžeme libovolně spojovat a provádět tak komplexní výpočty. Na rozdíl od verze se spojitou procházkou zde nevzniká problém s přípravou počátečního



Obrázek 5.6: Schéma pro Hadamardovo hradlo. Obloučky představují vedení z obrázku 5.3. Převzato z [12].

stavu. Na druhou stranu je pro provedení stejného výpočtu potřeba o něco více kroků. (Každé hradlo fázového posunu spotřebuje jeden krok navíc oproti spojitě procházce.)

5.3 Shrnutí

Stejně, jako se náhodné procházky uplatňují v klasické informatice, tak i kvantové procházky hrají důležitou roli ve zpracování kvantové informace. Mohou v principu nahradit zcela obecný kvantový počítač a navíc najít své další specifické aplikace. V současnosti se jedná o bouřlivě se vyvíjející oblast a kromě množství teoretických prací jsou realizovány i laboratorní experimenty, kterými se budeme zabývat v následující kapitole.

Kapitola 6

Fyzikální realizace kvantových procházek

Již bylo realizováno více experimentů provádějících jednorozměrnou kvantovou procházku s použitím různých fyzikálních principů: procházky s uvězněnými atomy [13] a ionty [14, 15], dále s energetickými hladinami v NMR (nukleární magnetická rezonance) [16, 17], fotony ve vlnovodových strukturách [18], fotony v polích děličů svazku [19] a se smyčkou s optickými vlákny, kterou rozebereme podrobněji.

6.1 Optická smyčka

6.1.1 Jednorozměrná procházka

Jedná se o realizaci kvantové procházky na přímce. Kolektiv autorů v článku [20] prezentuje experiment, ve kterém je kvantová procházka realizována pomocí optických vláken a statických optických prvků. Poloha chodce je zde určena časovým posunem příchodu signálu do konečného detektoru. Stav kvantové mince je uložen v polarizaci světla a průchod fotonu půlvlnovou destičkou zajišťuje požadovanou transformaci. Jednoduché schéma je na obrázku 6.1.

Pomocí neutral density filtru je snížena intenzita svazku až na úroveň jednotlivých fotonů. Následně je pomocí polarizačního děliče svazku a půlvlnové a čtvrtvlnové destičky připraven výchozí stav ve formě

$$|\psi\rangle = \alpha |H\rangle + \beta |V\rangle, \quad (6.1)$$

kde $|H\rangle$ a $|V\rangle$ jsou stavy odpovídající horizontální a vertikální polarizaci světla. (Pro symetrické rozložení výsledné procházky se používá kruhová polarizace.) Dále foton vstupuje do okruhu přes dělič svazku, nebo projde a je detekován diodou. Pomocí další půlvlnové destičky může být provedena libovolná transformace stavu chodce

tvaru

$$C(\theta) = \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix}. \quad (6.2)$$

Následně polarizační dělič svazku rozdělí horizontálně a vertikálně polarizovanou část světla do dvou vláken, přičemž jedno z nich je delší a vznikne tak časový posun. Obě části jsou poté opět koherentně sloučeny do výsledného stavu. Tím je proveden krok procházky. Pomocí zrcadel je svazek opět nasměrován na dělič, který ho propustí do další iterace, nebo pošle k výslednému naměření.

Na obrázku 6.2 je znázorněn druhý krok procházky s Hadamardovou mincí pro počáteční stav $|0V\rangle$. Po prvním kroku se chodec nachází v rovnoměrné superpozici stavů $|-1, V\rangle$ a $|1, H\rangle$. Nejprve prochází přes půl-vlnovou destičku, čímž je provedena transformace

$$C(\pi/4) \frac{1}{\sqrt{2}} (|-1, V\rangle + |1, H\rangle) = \frac{1}{\sqrt{2}} \left(|-1\rangle \otimes \frac{1}{\sqrt{2}} (|V\rangle + |H\rangle) + |1\rangle \otimes \frac{1}{\sqrt{2}} (|V\rangle - |H\rangle) \right). \quad (6.3)$$

Dále dochází k rozdělení podle polarizace a zpoždění vertikálně polarizované části. Výsledný stav po dvou krocích je tedy dán výrazem

$$(SC(\pi/4))^2 |0, V\rangle = \frac{1}{2} (|-2, V\rangle) + \frac{1}{2} |0\rangle \otimes (|V\rangle + |H\rangle) + \frac{1}{2} (|2, H\rangle). \quad (6.4)$$

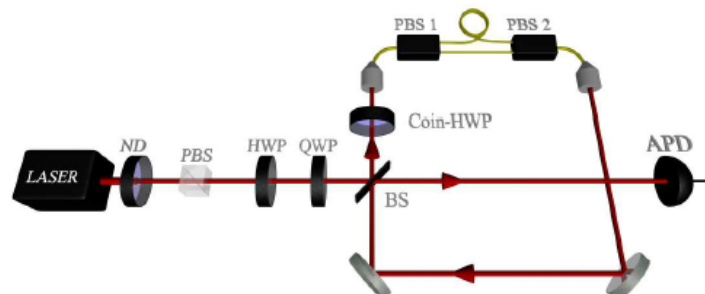
Rozdělení pravděpodobnosti je zde stále stejné jako u klasické procházky se symetrickou mincí. Rozdíly se objeví až od třetího kroku.

Díky jednoduché realizaci je možné udělat velké množství opakování pokusů a tak získat velmi přesnou statistiku rozložení chodce pro různé počty kroků. V článku jsou prezentovány výsledky pro 5 kroků s Hadamardovou mincí a pro tři kroky s různými volbami mince. V pozdější práci [21] bylo popsáno dosažení 28 kroků a podle odhadu autorů by mělo být možné další optimalizací zařízení realizovat 100 kroků kvantové procházky.

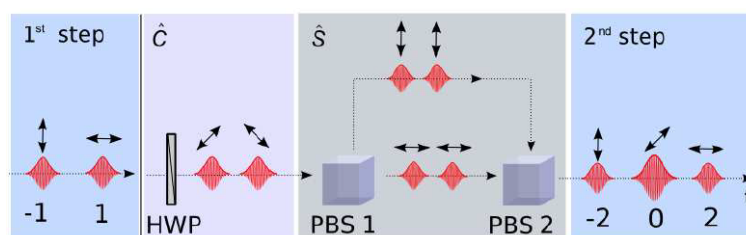
6.1.2 Zkoumání dekoherence na optické smyčce

V návaznosti na [20] publikovala stejná skupina článek [21], ve kterém popisuje zkoumání různých druhů dekoherence na výše popsaném laboratorním zařízení. Je zde navíc přidán elektro-optický modulátor (EOM), který umožňuje vytvářet fázový posun mezi polarizačními stavy mince. Díky tomu, že EOM může měnit své působení v čase, je možné vytvářet transformaci mince závislou na poloze chodce. Celkově má použitá mince tvar

$$C(c) = \begin{bmatrix} e^{i\phi_h(c)} & 0 \\ 0 & e^{i\phi_v(c)} \end{bmatrix} \begin{bmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{bmatrix}, \quad (6.5)$$



Obrázek 6.1: Shéma optické smyčky pro kvantovou procházku: (ND) neutral density filtr, (BS) dělič svazku, (HWP/QWP) půl/čtvrt-vlnová destička, (PBS) polarizační dělič svazku, (APD) lavinová fotodioda. Převzato z [20].



Obrázek 6.2: Průběh druhého kroku procházky s Hadamardovou mincí. Převzato z [20].

kde $\phi_h(c)$ a $\phi_v(c)$ určují fázový posun pro horizontálně a vertikálně polarizovanou část světla.

V článku jsou popsány tři případy pro různý způsob dekoherence a navíc případ s homogenní časově neměnnou mřížkou, kde probíhá standardní kvantová procházka. Ve všech případech se výsledné rozdělení pravděpodobnosti středuje přes velké množství realizací procházky.

Nejprve vezměme případ *statické poruchy*, kdy se transformace mince nemění v čase, ale na každé pozici je proveden určitý fázový posun $\phi_{h/v}(x)$. Byla provedena měření pro různá rozložení fázových posunů pro jednotlivé polohy. Výsledkem bylo pozorování očekávané Andersonovy lokalizace, kdy pravděpodobnost nalezení chodce v dané pozici exponenciálně klesá se vzdáleností od výchozího bodu.

Dále byly zkoumány *rychlé fluktuace*. Prodloužením intervalů mezi změnami fázového posunu v minci dojde k tomu, že působení již není závislé na poloze chodce, ale na kroku procházky. Výsledkem této konfigurace je klasická náhodná procházka s binomickým rozdělením pravděpodobnosti. Nastavením velikosti fázového posunu v jednotlivých krocích můžeme volně přecházet od čistě kvantového až po klasické chování.

Poslední variantou jsou *pomalé fluktuace*. Zde se intervaly změn ještě prodlouží natolik, že celý vývoj konkrétní procházky probíhá na statické homogenní mřížce. Postupně dostáváme soubor výsledků pro různé parametry procházky. V tomto případě byl měněn parametr $\theta \in [0, \pi/4]$ po krocích velikosti $\pi/18$. Výsledkem bylo téměř rovnoměrné rozdělení se zajímavou vlastností, kdy je pravděpodobnost nalezení chodce v úplně krajních bodech dokonce větší, než u kvantové procházky bez dekoherence.

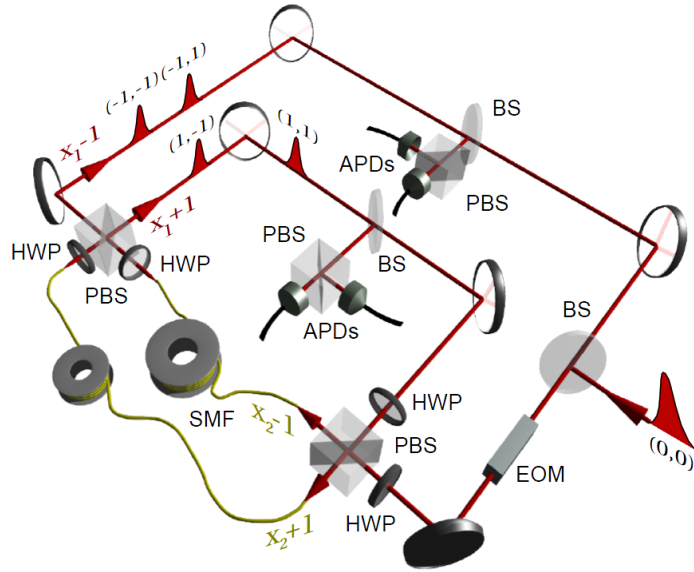
Časová změna mince tedy umožňuje modelovat a zkoumat různé fyzikální situace a navíc je zásadním krokem vpřed k realizaci výpočetních protokolů pomocí kvantových procházek.

6.1.3 Dvourozměrná kvantová procházka

Velice nedávno byla v článku [22] prezentována realizace dvourozměrné kvantové procházky. Chodcem je zde opět foton a k realizaci mince je použita jeho polarizace. Bázové stavy chodce jsou ve tvaru $|x_1 x_2\rangle |c_1 c_2\rangle$, kde x_1 a x_2 představuje pozici na dvourozměrné mřížce a $c_1, c_2 \in \{-1, +1\}$ jsou stavy mince.

Mince je částečně realizována pomocí lineární polarizace, tedy stavy $|H\rangle$ a $|V\rangle$ a dále využitím prostorového parametru se stavy $|a\rangle$ a $|b\rangle$. Konkrétní přiřazení je následující

$$\begin{aligned} |H, a\rangle &= |-1, -1\rangle \\ |H, b\rangle &= |+1, +1\rangle \\ |V, a\rangle &= |-1, +1\rangle \\ |V, b\rangle &= |+1, -1\rangle. \end{aligned} \tag{6.6}$$



Obrázek 6.3: Shéma pro 2D optickou kvantovou procházku: (ND) neutral density filtr, (BS) dělič svazku, (HWP/QWP) půl/čtvrt-vlnová destička, (PBS) polarizační dělič svazku, (APD) lavinová fotodioda, (EOM) elektro-optický modulátor. Převzato z [22].

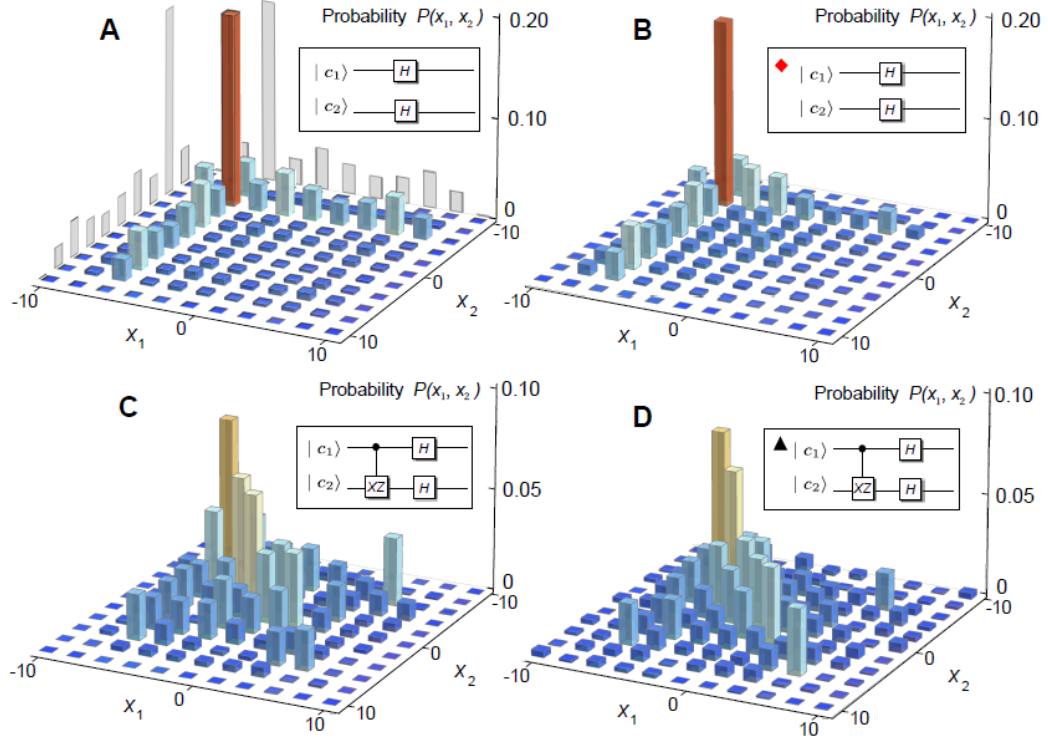
Transformace stavu mince (čtyřrozměrná) je provedena pomocí působení čtyř půl-vlnových destiček (dvourozměrných transformací) na různé dvojice bazových stavů a elektro-optického modulátoru. Půl-vlnové destičky provádí opět transformaci 6.5 (na odpovídající dvojici stavů) a elektro-optický modulátor vytváří fázový posun jednotlivých stavů. (Různé stavy $|a\rangle$ a $|b\rangle$ jsou adresovány rychlými časovými změnami působení.) Tímto způsobem je možné vytvořit libovolnou minci.

K odlišení prostorového stavu se opět používá časový rozestup. Nyní je však potřeba použít dva různě dlouhé časové skoky τ_1 a τ_2 odpovídající dvěma prostorovým souřadnicím. Velký posun o τ_2 určí jednu souřadnici a malý posun o τ_1 upřesní druhou souřadnici. Aby nedocházelo k „promíchání“ souřadnic, musí platit $2N\tau_1 < \tau_2$, kde N je počet kroků procházky, který chceme provést.

Využívá se zde rozšířené zapojení z jednorozměrné verze. Schéma je na obrázku 6.3. Foton opět vstupuje do okruhu přes dělič svazku s vertikální polarizací. Následně je jeho polarizace transformována a dojde k rozdělení na dvě větve a posunu jedné z nich o τ_2 . Dále je opět stav mince v každé větvi transformován a dojde k rozdělení do dvou částí okruhu odpovídajících stavům $|a\rangle$ a $|b\rangle$. Tím je proveden jeden krok procházky a chodec je zachycen fotodiodami, nebo propuštěn do dalšího kroku.

Význam takovéto procházky je i v tom, že může místo jednoho chodce ve dvou rozměrech simulovat současnou procházku dvou vzájemně interagujících chodců na jednorozměrné přímce. To umožňuje měnit úroveň tříd komplexnosti problémů, které můžeme řešit.

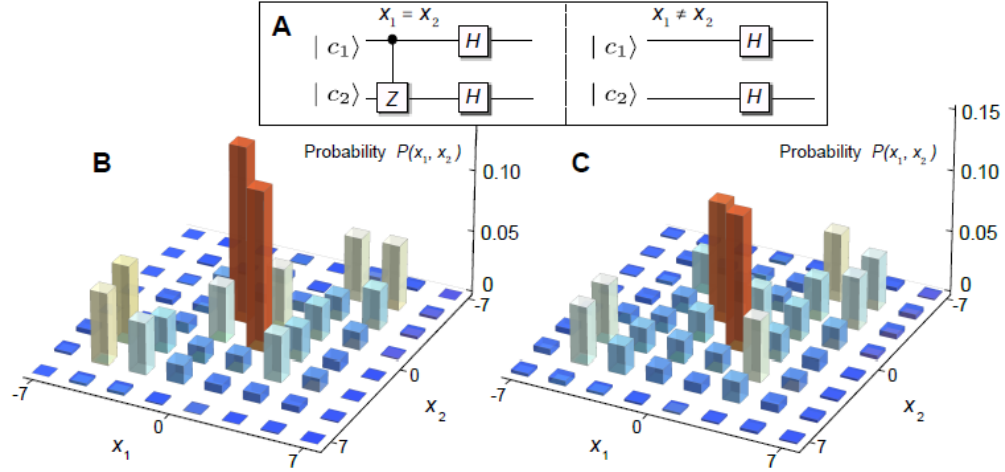
S popsanou aparaturou byl nejprve proveden experiment se separovatelnou mincí



Obrázek 6.4: Výsledky měření pro dvourozměrnou procházku. Části A a B znázorňují teoretické a naměřené rozdělení pravděpodobnosti pro procházku se separovatelnou mincí a části C a D pro procházku s podmíněnou operací. Převzato z [22].

$C = C_1 \otimes C_2$ a separovatelným počátečním stavem. Výsledkem je opět separovatelné rozdělení pravděpodobnosti, které odpovídá dvěma nezávislým chodcům (viz obrázek 6.4 A a B). Dvourozměrná procházka nám však umožňuje mnohem komplexnější uspořádání, kdy je na minci provedena podmíněná transformace. Vývoj v jednom rozměru (jednoho chodce) je tedy ovlivněn stavem ve druhém rozměru (stavem druhého chodce). Na obrázku 6.4 C a D je vidět výsledné neseparovatelné rozdělení.

Vzájemná interakce chodců může být popsána jako působení na dálku, jehož síla nezávisí na vzdálenosti. Tento velmi netriviální efekt je možné jen velmi těžko realizovat pomocí skutečných částic. Pomocí elektro-optického modulátoru však můžeme simulovat ještě jinou situaci. Díky možnosti různé transformace mince v závislosti na poloze chodce ve dvourozměrné síti můžeme přejít k síle působící jen na krátkou vzdálenost (rozptyl částic). Minci s podmíněnou transformací aplikujeme pouze na diagonálních pozicích sítě, kde se oba chodci nacházejí na stejné pozici. V popisovaném experimentu byl použit výchozí stav invariantní vůči záměně částic, který implikuje bosonové chování. Výsledky, které potvrdili očekávané nelineární chování, jsou na obrázku 6.5.



Obrázek 6.5: Výsledky měření pro dvourozměrnou procházku s pozičně závislou mincí. Části A znázorňuje teoretické a část B naměřené rozdělení pravděpodobnosti. Převzato z [22].

6.2 Integrovaný optický obvod

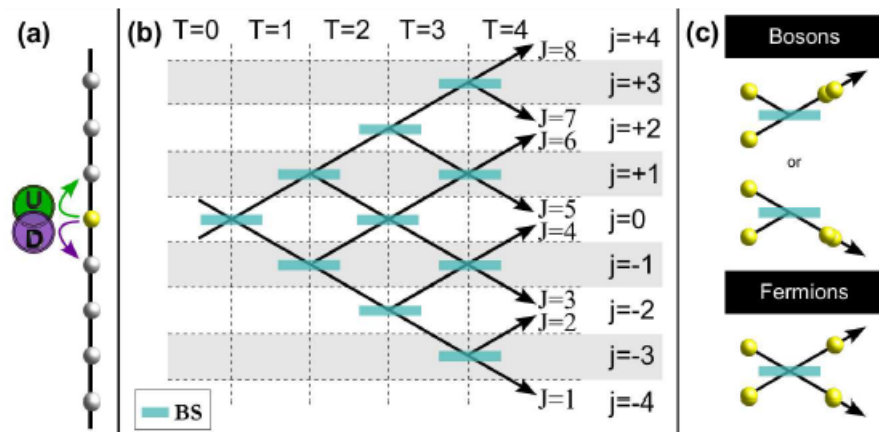
Článek [23] prezentuje realizaci kvantové procházky se dvěma chodci pomocí integrovaného optického obvodu. V podstatě se jedná o kvantovou procházku na poli sestaveném z děličů svazku, kde je pozice chodce určena umístěním v poli a mince je realizována pomocí polarizace světla (schéma na obrázku 6.6). Každý dělič svazku provádí Hadamardovu transformaci na minci a následně rozdělení podle polarizace.

Realizace takového pole děličů svazku s potřebnou přesností je při použití standardních (velkých) optických prvků velmi náročná i pro malý počet kroků procházky. V tomto experimentu je proto použita integrovaná součástka vyrobená pomocí laseru ze substrátu borosilikátového skla (schéma na obrázku 6.7). Ta zajišťuje jak vedení paprsku, tak i potřebné transformace.

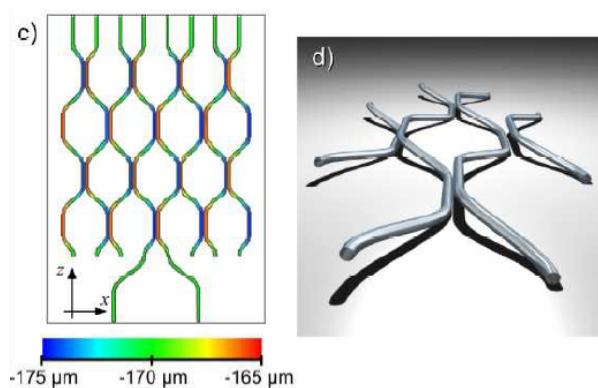
Jako výchozí je zde použit stav dvou fotonů provázaných pomocí polarizace, který je popsán jako

$$|\psi\rangle_{in} = \frac{1}{\sqrt{2}} (|H\rangle_A \otimes |V\rangle_B + e^{i\phi} |V\rangle_A \otimes |H\rangle_B). \quad (6.7)$$

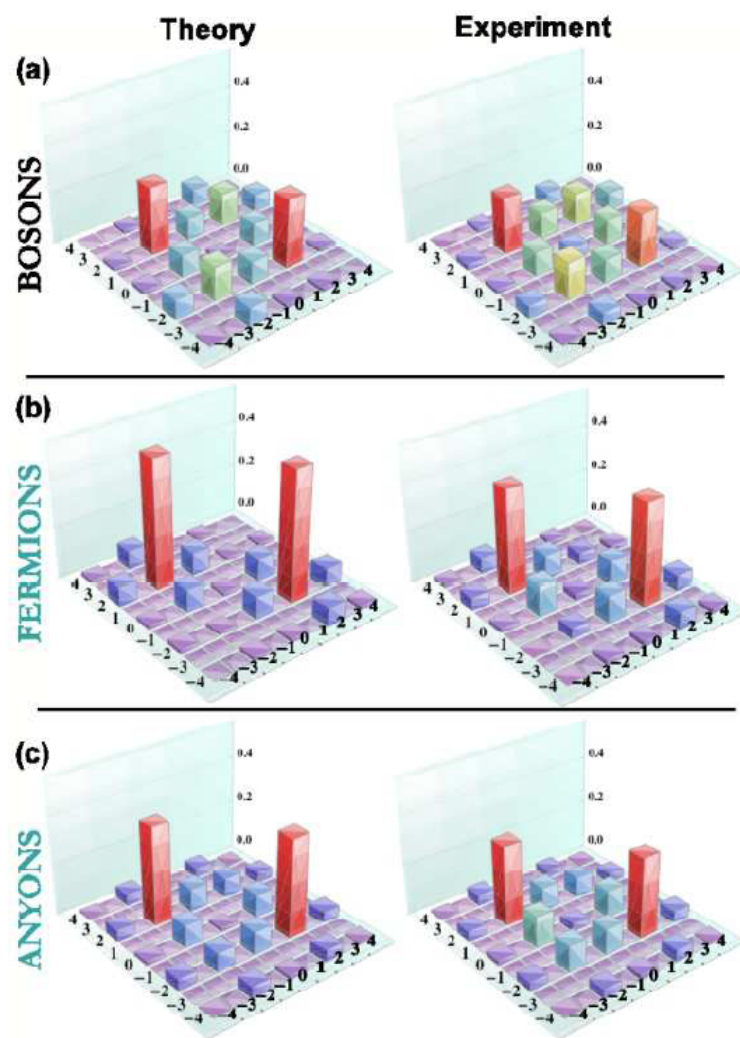
Nastavením fáze můžeme měnit symetrii stavu a tím simulovat bosonové ($\phi = 0$) nebo fermionové ($\phi = \pi$) chování chodců. Pro bosony zde dochází ke spojování (velká pravděpodobnost nalezení na podobných pozicích) a pro fermiony k odrazům (pravděpodobnost více rozložena do vzájemně odlehlých pozic). (Viz obrázek 6.6.) Volbou libovolné jiné fáze ϕ je možné vytvořit stav, který odpovídá takzvaným *anyonům*. Jedná se o zobecnění konceptu bozonů/fermionů na částice, které nemusí mít celočíselný ani poločíselný spin. Experiment ukázal ve všech případech dobrou shodu s teorií. Výsledky jsou graficky zobrazeny na obrázku 6.8.



Obrázek 6.6: Procházka na integrované optické síti: a) Přímka, na které probíhá procházka, kde U a D představují stavy mince. b) Čtyři kroky kvantové procházky, kde na svislé ose je poloha chodce a na vodorovné krok procházky. c) Znárodně chování bosonů, respektive fermionů. Převzato z [23].



Obrázek 6.7: Vizualizace pole pro čtyři kroky kvantové procházky: V části c) je barevně vyznačen výškový profil, který je ve 3D detailu znázorněn v části d). Převzato z [23].



Obrázek 6.8: Výsledky realizace pro bosony, fermiony a anyony. Převzato z [23].

6.3 Shrnutí

Stejně jako v jiných oblastech pracujících s kvantovou informací je i v případě kvantových procházek teorie daleko mimo možnosti současných experimentů. Přesto, že v teorii existují algoritmy využívající kvantové procházky, na jejich aplikaci (konkurenceschopnost s klasickými počítači) si budeme muset ještě počkat. V posledních letech se však začíná objevovat množství experimentů schopných kvantovou procházku provádět. Hlavní současnou aplikací kvantových procházek je možnost simulovat jiné kvantové systémy. Zásadní uplatnění mohou mít především procházky s více chodci (respektive vícerozměrné s jedním chodcem). Dále je možné například testovat vyhledávací algoritmus a celkově zkoumat teoreticky předpovězené možnosti kvantových počítačů.

Závěr

Tato práce souhrnně podává poznatky potřebné k základnímu seznámení s problematikou kvantových procházek. Postupuje od základních poznatků kvantové mechaniky přes obecný úvod do teorie kvantové informace až konečně ke kvantovým procházkám. Zabývá se jak teoretickým rozborem problematiky, tak i konkrétními fyzikálními realizacemi. U čtenáře se předpokládá jen základní znalost kvantové mechaniky a lineární algebry. Tuto práci může ocenit především čtenář, který má problém s využitím anglicky psané literatury, jelikož množství česky psaných publikací o kvantových procházkách je značně omezené. Proto doufám, že v budoucnu někomu poskytne odrazový můstek při pronikání do tohoto dynamicky se rozvíjejícího oboru.

Seznam použitých zdrojů

- [1] HLAVATÝ, L. *Slabikář kvantové mechaniky* [online]. Praha, 2010 [cit. 22. dubna 2012]. Dostupné z: <<http://wikiskripta.fjfi.cvut.cz/wiki/index.php/02KVAN>>
- [2] MESSIAH, A. *Quantum mechanics: Volume I*. Amsterdam: North-Holland publishing company, 1961.
- [3] STENHOLM, S. a SUOMINEN, K. A. *Quantum approach to informatics*. Hoboken, N.J.: Wiley-Interscience, c2005, 238 s.
- [4] SHOR, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Scientific and Statistical Computing*. 1997, **26**, 1484, 28 s.
- [5] BIAN, Z. Experimental determination of Ramsey numbers with quantum annealing. 2012, 6 s.
- [6] KENDON, V. Decoherence in quantum walks: a review. *Mathematical Structures in Computer Science*. 2006, **17**, 6, s. 1169-1220.
- [7] KEMPE, J. Quantum random walks: an introductory overview. *Contemporary Physics*. 2003, **4**, s. 307-327.
- [8] HIGHAM, D. J. a A. TAYLOR. The Sleekest Link Algorithm. *Mathematics Today*. 2003, **39**, s. 192-197.
- [9] CHILDS, A. M. *et al.* An example of the difference between quantum and classical random walks. *Quantum Information Processing*. 2002, **1**, 35, 4 s.
- [10] GROVER, L. K. A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*. 1996, s. 212-219.
- [11] CHILDS, A. Universal Computation by Quantum Walk. *Physical Review Letters*. 2009, **102**, 180501, 9 s.
- [12] LOVETT, N. B. *et al.* Universal quantum computation using the discrete-time quantum walk. *Physical Review A. Physical Review Letters A*. 2010, **81**, 042330, 9 s.

- [13] KARSKI, M. *et al.* Quantum Walk in Position Space with Single Optically Trapped Atoms. *Science* 2009, **325**, 5937, s. 174-177.
- [14] SCHMITZ, H. *et al.* Quantum walk of a trapped ion in phase space. *Physical review letters* 2009, **103**, 090504, 4 s.
- [15] ZÄHRINGER, F. *et al.* Realization of a quantum walk with one and two trapped ions. *Physical review letters* 2010, **104**, 100503, 5 s.
- [16] DU, J. *et al.* Experimental Implementation of Quantum Random Walk Algorithm. *Physical review letters* 2003, **67**, 042316, 5 s.
- [17] RYAN, C. A. *et al.* Experimental Implementation of Discrete Time Quantum Random Walk on an NMR Quantum Information Processor. *Physical review letters* 2005, **72**, 062317, 8 s.
- [18] PERETS, H. B. *et al.* Realization of quantum walks with negligible decoherence in waveguide lattices. *Physical review letters* 2008, **100**, 170506, 4 s.
- [19] BROOME M. A. *et al.* Discrete single-photon quantum walks with tunable decoherence. *Physical review letters* 2010, **104**, 153602, 5 s.
- [20] SCHREIBER, A. *et al.* Photons Walking the Line: A quantum walk with adjustable coin operations. *Physical review letters*. 2010, **104**, 050502, 4 s.
- [21] SCHREIBER, A. *et al.* Decoherence and disorder in quantum walks: From ballistic spread to localization. *Physical review letters*. 2011, **106**, 180403, 5 s.
- [22] SCHREIBER, A. *et al.* A 2D Quantum Walk Simulation of Two-Particle Dynamics. *Science*. 2012, **336**, 6077, s. 55-58.
- [23] SANSONI, L. *et al.* Two-particle bosonic-fermionic quantum walk via integrated photonics. *Physical review letters* 2012, **108**, 010502, 4 s.