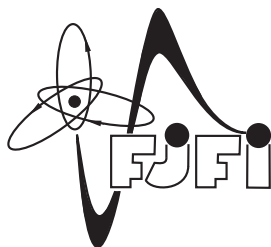


ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA JADERNÁ A FYZIKÁLNĚ INŽENÝRSKÁ
KATEDRA FYZIKY



Optické sítě s několika excitacemi

BAKALÁŘSKÁ PRÁCE

Školitel: Prof. Ing. Igor Jex, DrSc.

Konzultant: Ing. Martin Štefaňák, PhD.

Září 2011

Eliška Greplová

PODĚKOVÁNÍ

Děkuji panu Prof. Ing. Igoru Jexovi, DrSc. za velice zajímavé téma práce, za pozornost, se kterou se zabýval všemi mými poznámkami a nápady a za všechnen čas a trpělivost, které mi během celého roku věnoval.

Za pomoc a užitečné konzultace děkuji Ing. Martinu Štefaňákovi, PhD.

PROHLÁŠENÍ

Prohlašuji, že jsem svou bakalářskou práci vypracovala samostatně a použila jsem pouze literaturu uvedenou v příloženém seznamu. Nemám závažný důvod proti užití tohoto díla ve smyslu § 60 zákona č.121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 6. července 2011

.....

Eliška Greplová

Název práce: **Optické sítě s několika excitacemi**

Autor: Eliška Greplová

Obor: Matematické inženýrství

Druh práce: Bakalářská práce

Vedoucí práce: Prof. Ing. Igor Jex, DrSc.
Katedra fyziky, FJFI, ČVUT v Praze

Konzultant: Ing. Martin Štefaňák, PhD.
Katedra fyziky, FJFI, ČVUT v Praze

Abstrakt:

Cílem této práce je seznámit čtenáře s problematikou optických sítí. Po stručném úvodu do kvantové teorie a kapitole věnované kvantovému provázání následuje přehled logických hradel a možností jejich skládání při tvorbě sítí. Dále jsou uvedeny fyzikální realizace těchto logických operací, především s důrazem na využití nelineárních elementů, zejména v případě více excitací. Tento přehled je zakončen kapitolou, která podrobně rozebírá vlastnosti Isingova typu optické sítě včetně rozdělení provázání pro jedno- a dvou fotonový případ. Závěrečná kapitola se zabývá formulací konkrétní úlohy týkající se náhodné pozice nelineárního elementu v síti a jejím řešením pro případ koherentních stavů.

Klíčová slova: optické sítě, více excitací, kvantový obvod, optické elementy, kerrovský element, analogie s Isingovým modelem.

Title: **Optical networks with several excitations**

Author: Eliška Greplová

Abstract:

The main purpose of this thesis is to acquaint the reader with the optical networks. There is a brief introduction to quantum theory and particular quantum entanglement in the first part. The overview of the logical gates, stated in the next chapter, is followed by a list of their possible physical realizations (especially nonlinear elements with several excitations are introduced). This overview is concluded by the chapter aiming to the description of the Ising-type of network, entanglement distribution for the single- and two-particle states included. The last chapter is the formulation of the particular problem on the random position of the nonlinear element in the network with the solution for the coherent state case.

Key words: quantum networks, several excitations, quantum circuit, optical elements, Kerr-element, Ising-type of networks.

Obsah

1	Úvod	7
1.1	Kvantová mechanika	8
1.2	Stavový prostor	8
1.3	Časový vývoj	9
1.4	Měření	10
1.5	Projekční měření	10
2	Provázání	12
3	Kvantové obvody	17
3.1	Jednoqubitové kvantové operace	19
3.1.1	Pauliho hradla	20
3.1.2	Hadamardovo hradlo	21
3.1.3	NOT hradlo	22
3.1.4	Fázový posun	22
3.2	Vícequbitové operace	24
3.2.1	CNOT hradlo	25
3.2.2	SWAP hradlo	27
3.2.3	Toffoliho hradlo	28
3.2.4	Fredkinovo hradlo	28
3.2.5	Generace Bellových stavů	29
3.2.6	Obvod realizující binární sčítání	31
4	Přehled základních optických elementů	32
4.1	Dělič paprsku	32

4.2	Nelineární dělič paprsku	36
4.3	Interferometr	37
4.4	Kerrovský element	38
4.5	Cross-Kerr element	40
4.6	Nelineární Mach-Zehnderův interferometr	41
4.7	Optická realizace Fredkinova hradla	42
4.8	Symetrický 2N-port	43
4.9	Galtonova deska	46
4.9.1	Modifikace modelu Galtonovy desky pro nelinearity	48
4.10	Kvantová síť analogická s Isingovým modelem	48
4.10.1	Rekurence a zakázané výstupy	50
4.10.2	Provázání v Isingově typu optické sítě	52
4.10.3	Optimalizace rozdělení provázání v pasivní síti s jednou excitací	55
4.10.4	Rozdělení provázání v pasivní síti se dvěma excitacemi	56
5	Řešení optické sítě s náhodnou pozicí nelineárního elementu	59
5.1	Koherentní stavy	60
6	Závěr	63
A	The no-cloning theorem	64
B	Základní vlastnosti koherentních stavů	65
C	QND měření	67
C.1	QND pomocí Kerrovského elementu	68
D	Zeilingerova metoda	71
E	GHZ stavy	74
F	Poznámky k experimentální realizaci Galtonovy desky	76
F.1	Modulace frekvence	76
F.2	Polarizace světla	79
	Literatura	81

Kapitola 1

Úvod

Tato práce je úvodem do problematiky kvantových optických sítí. První kapitola je stručným přehledem postulátů kvantové mechaniky, které budou uvedeny pouze jako soubor pravidel a aplikovány v následujících kapitolách (pro rozsáhlejší matematickou diskuzi lze zvolit například [1]). Druhá kapitola popisuje fenomén provázání, speciální druh kvantových korelací, které nemají žádný klasický ekvivalent. Třetí kapitola slouží jako přehled kvantových hradel, tedy elementárních transformací, jejichž vhodnou kombinací lze sestavit výslednou operaci, kterou má síť realizovat. Čtvrtá kapitola je pak věnována optickým elementům ve smyslu realizace logických operací navržených v předchozí kapitole. Pozornost je věnována realizacím (zejména nelineárním) s více excitami. Konečně pátá kapitola se zabývá konkrétní aplikací předchozí řešeršní části. Jejím cílem je popsat, alespoň v některých speciálních případech, řešení lineární kvantové optické sítě, ve které je náhodně umístěn nelineární prvek. Připojené přílohy se vztahují k použitým metodám a nejčastěji zmiňovaným aplikacím.

1.1 Kvantová mechanika

Kvantová mechanika je teorie, která vznikla na přelomu 19. a 20. století za účelem fyzikální interpretace experimentálních fakt, které nebylo možné vysvělit pomocí 'klasické' teorie jako je tvar spektra záření absolutně černého tělesa, fotoelektrický jev nebo stabilita atomů (viz. např. [2]). Pro popis objektů, pro které je klasická teorie nedostačující (vykazují vlnové i částicové vlastnosti a některé fyzikální veličiny (např. energie) místo klasického spojitého charakteru nabývají diskrétních hodnot), byla zformulována teorie, která má statistický charakter a je založena na postulátech uvedených v následujícím textu.

1.2 Stavový prostor

První postulát ustanovuje prostor, kterým jsou v kvantové mechanice nahrazeny fázový resp. konfigurační prostor, známé z klasické mechaniky:

Každému izolovanému fyzikálnímu systému je přiřazen komplexní vektorový prostor se skalárním součinem (tj. Hilbertův prostor, viz. [1]), který je nazýván také stavovým prostorem systému. Systém je pak úplně popsán jediným jednotkovým vektorem z Hilbertova prostoru \mathcal{H} (tzv. stavovým vektorem).

Jsou-li $|\Psi_1\rangle, |\Psi_2\rangle$ dva možné stavy uvažovaného systému, potom superpozice

$$|\Psi\rangle = c_1|\Psi_1\rangle + c_2|\Psi_2\rangle, \quad (1.1)$$

kde $c_1, c_2 \in \mathbb{C}$, také popisuje možný stav systému. Ekvivalentní reprezentací (ve smyslu kanonické antilienární bijekce $\mathcal{H} \leftrightarrow \mathcal{H}^*$, viz. [3]) stavu (1.1) je tzv. bra vektor

$$\langle\Psi| = c_1^*\langle\Psi_1| + c_2^*\langle\Psi_2|,$$

kde $c_1^*, c_2^* \in \mathbb{C}$ jsou čísla komplexně sdružená k c_1, c_2 .

Překryv mezi dvěma navzájem různými stavy $|\Psi\rangle, |\Phi\rangle$ je dán jejich skalárním součinem $\langle\Psi|\Phi\rangle$. Pokud je tento roven nule, řekneme, že stavy $|\Psi\rangle, |\Phi\rangle$ jsou ortogonální. Skalární součin stavu se sebou samým je vždy striktně pozitivní: $\langle\Psi|\Psi\rangle > 0$ (pokud není roven nule), přičemž v případě $\langle\Psi|\Psi\rangle = 1$ nazveme stav normalizovaným.

1.3 Časový vývoj

Následující postulát objasňuje, jak se stavový vektor systému $|\Psi\rangle$ mění v čase:

Vývoj uzavřeného kvantového systému je popsán unitární transformací, což znamená, že stav systému $|\Psi\rangle$ v čase t_1 je svázán se stavem systému $|\Psi'\rangle$ v čase t_2 pomocí unitárního operátoru \hat{U} : $|\Psi'\rangle = \hat{U}|\Psi\rangle$ resp. $|\Psi(t_2)\rangle = \hat{U}(t_1, t_2)|\Psi(t_1)\rangle$.

Uzavřenost systému požadovaná v postulátu, znamená, že systém během svého časového vývoje neinteraguje s jinými systémy. Časový vývoj takového systému jsme popsali pomocí dvou pevně zvolených časů. Ekvivalentní formulace, jejímž autorem je Schrödinger, je vyjádřit časový vývoj pomocí spojitě změny časové proměnné (dvojice časů t_1, t_2 z formulace postulátu byla volena naprosto libovolně, lze tedy jeden z nich zafixovat a druhý chápat jako proměnnou):

Časový vývoj stavového vektoru uzavřeného kvantového systému je dán Schrödingerovou rovnicí:

$$i\hbar \frac{d}{dt} |\Psi(t)\rangle = \hat{H} |\Psi(t)\rangle, \quad (1.2)$$

kde \hbar je tzv. redukovaná Planckova konstanta a \hat{H} je hermitovský operátor, který nazýváme Hamiltoniánem systému.

Rozebereme-li toto tvrzení podrobněji, můžeme tvrdit toto: obecně platí, že pro každý unitární operátor $\hat{U}(t, t_0)$ existuje hermitovský operátor \hat{H} , takový, že časový vývoj lze vyjádřit jako (Stoneův teorém, viz. [1])

$$\hat{U}(t, t_0) = \exp[-i\hat{H}(t - t_0)], \quad (1.3)$$

z čehož plyne

$$\frac{d}{dt} \hat{U}(t, t_0) = -i\hat{H}\hat{U}(t, t_0). \quad (1.4)$$

Říkáme, že operátor časového vývoje (1.3) je generován hermitovským operátorem \hat{H} . Lze ukázat ([3]), že \hat{H} je úměrné Hamiltonově funkci systému. Vyjádříme-li tedy \hat{H} v jednotkách energie, můžeme jej nazvat Hamiltoniánem systému.

Díky hermitovskosti operátoru je vždy zaručena existence spektrálního rozkladu (viz. [1]):

$$\hat{H} = \sum_E \frac{E|E\rangle\langle E|}{\sqrt{\langle E|E\rangle}},$$

kde E jsou vlastní hodnoty odpovídající vlastním vektorům $|E\rangle$, v tomto případě je E energie odpovídající stavu $|E\rangle$, nejnižší energii pak nazýváme základním stavem systému.

1.4 Měření

Výše uvedené postuláty objasňovaly otázky matematického popisu a časového vývoje uzavřeného systému. Dále je třeba popsat, jak se bude systém chovat v případě, že na něm budeme realizovat měření, tedy přestane-li být uzavřený.

Uskutečníme-li na systému měření, získáme tak informace o nějaké (měřitelné) veličině. Takové veličiny nazveme pozorovatelnými. Každé pozorovatelné pak odpovídá hermitovský operátor na Hilbertově prostoru:

Kvantové měření je popsáno množinou operátorů $\{\hat{M}_m\}$ definovaných na Hilbertově prostoru měřeného systému. Index m probíhá počet všech možných experimentálních výstupů měření. Pokud je systém před uskutečněním měření ve stavu $|\Psi\rangle$, pak je pravděpodobnost, že obdržíme m -tý možný výsledek dána vztahem:

$$p(m) = \langle \Psi | \hat{M}_m^\dagger \hat{M}_m | \Psi \rangle$$

a stav systému po měření:

$$|\Psi'\rangle = \frac{\hat{M}_m |\Psi\rangle}{\sqrt{\langle \Psi | \hat{M}_m^\dagger \hat{M}_m | \Psi \rangle}},$$

přičemž operátory $\{\hat{M}_m\}$ splňují následující relaci úplnosti:

$$\sum_m \hat{M}_m^\dagger \hat{M}_m = 1. \tag{1.5}$$

1.5 Projekční měření

Toto měření je popsáno *pozorovatelnou* \hat{M} , hermitovským operátorem na stavovém prostoru pozorovaného systému. Pozorovatelná má spektrální rozklad

$$\hat{M} = \sum_m m \hat{P}_m,$$

kde \hat{P}_m jsou projektořy na vlastní podprostory operátoru \hat{M} příslušející vlastnímu číslu m . Při uskutečnění měření na stavu $|\Psi\rangle$ je pravděpodobnost, že obdržíme výsledek m

$$p(m) = \langle \Psi | \hat{P}_m | \Psi \rangle.$$

Pokud tato situace nastane, systém se okamžitě po měření bude nacházet ve stavu

$$|\Psi'\rangle = \frac{\hat{P}_m}{\sqrt{p(m)}} |\Psi\rangle.$$

Jedná se tedy o speciální případ situace popsané třetím postulátem: kromě relace úplnosti (1.5), navíc hermitovské operátory M_m splňují podmínku, že se jedná o ortogonální projektořy (tj. $\hat{M}_m \hat{M}_{m'} = \delta_{mm'} \hat{M}_m$). Tím jsme třetí uvedený postulát zúžili na třídu operátorů, která má, především díky ortogonalitě v aplikacích mnoho užitečných vlastností.

Například pro výpočet střední hodnoty platí:

$$E(\hat{M}) = \sum_m m p(m) = \sum_m m \langle \Psi | \hat{P}_m | \Psi \rangle = \langle \Psi | \left(\sum_m m \hat{P}_m \right) | \Psi \rangle = \langle \Psi | \hat{M} | \Psi \rangle \stackrel{ozn.}{=} \langle \hat{M} \rangle.$$

V některých situacích je nicméně výhodnější provádět měření, které pomocí projekčních operátorů popsat nelze. Toto se nazývá POVM (z *Positive Operator Valued Measurement*) a každému výsledku v tomto případě odpovídá jeden z množiny pozitivních operátorů, které nejsou ortogonální, ale splňují pouze podmínku 1.5. Příkladem použití je například rozlišení neortogonálních stavů popsané v [4].

Kapitola 2

Provázání

Uvažujme kvantový systém AB složený ze dvou podsystémů A, B. Tyto můžeme individuálně popsat stavovými vektory $|\Psi^A\rangle$ a $|\Phi^B\rangle$. Dále předpokládejme, že oba subsystémy byly připraveny nezávisle, stav složeného systému můžeme tedy popsat vektorem $|\Psi^A\rangle|\Phi^B\rangle$.

Systémy A,B nazveme neinteragujícími, jestliže jejich Hamiltoniány komutují: $[\hat{H}^A, \hat{H}^B] = 0$ (operace, která je pro každé dva operátory \hat{A}, \hat{B} definována: $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$). Pokud byly systémy připraveny nezávisle, svým vlastním časovým vývojem nikdy nemohou dospět do entaglovaného stavu. Aby se tak stalo, musí dojít k interakci nebo měření.

Uvažujme jako příklad dva systémy - částice se spinem 1/2, jež spolu interagují. Jako příklad interakce zvolíme podle [5] $\hat{H}^{AB} = \epsilon \hat{Z} \otimes \hat{Z}$, ϵ je interakční konstanta, \hat{Z} je Pauliho operátor. Systémy ale nemusí interagovat přímo, aby došlo k provázání, stačí zprostředkovaná interakce se třetím společným systémem.

Uvažujme složený stav obou systémů jako direktní produkt:

$$|\Xi\rangle = |\Psi^A\rangle|\Phi^B\rangle. \quad (2.1)$$

Takto je složený stav zapsán již ve faktorizovaném stavu, lze jednoznačně oddělit komponenty popisující jednotlivé systémy. Ale například stav

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0^A\rangle|0^B\rangle + |1^A\rangle|1^B\rangle),$$

který je superpozicí dvou složených stavů, není možné zapsat jako součin stavů příslušejících jednotlivým systémům. Na tomto faktu je založena definice provázání. Stav $|\Psi\rangle$ nazveme provázaným (entanglovaným), není-li možné jej faktorizovat na součin vlnových funkcí příslušející podsystémům tvořícím uvažovaný systém.

Výše uvedená formální definice provázání je ale nedostačující v praktických aplikacích, už jen kvůli skutečnosti, že často není možné získat stav popsáný jediným vektorem $|\Psi\rangle$ (označujeme jej jako čistý stav), ale statistickou směs takovýchto stavů (stav pak nazýváme smíšeným a vznikne například tak, že zařízení určené k přípravě stavu může s určitou pravděpodobností generovat několik navzájem různých čistých stavů). Abychom mohli tyto stavy popsat, zavedeme obecnější objekt, který budeme nazývat operátorem hustoty a definujeme jej

$$\hat{\rho} = \sum_n p_n |\Psi_n\rangle\langle\Psi_n|,$$

kde p_n je pravděpodobnost toho, že systém se bude nacházet ve stavu $|\Psi_n\rangle$. Takto definovaný operátor je hermitovský a pozitivní.

Operátor hustoty pro vlnovou funkci (2.1) má tvar $\hat{\rho}_{AB} = |\Psi\rangle\langle\Psi| \otimes |\Phi\rangle\langle\Phi|$. Provedeme-li částečnou stopu (viz. např. [6]) přes stavy příslušející systému B, dostame tzv. redukovaný operátor hustoty ($\hat{\rho}_A = \text{Tr}_B \hat{\rho}_{AB}$) pro složený systém

$$\hat{\rho}_A = |\Psi\rangle\langle\Psi|.$$

Je zřejmé, že platí $\hat{\rho}_A^2 = \hat{\rho}_A$ a $\text{Tr}(\hat{\rho}_A^2) = 1$. Jakýkoli neprovázaný stav, jelikož jej lze zapsat ve tvaru rovnice (2.1), vyhovuje podmínce, že stopa jeho kvadrátu je rovna jedné. Pro čisté stavy platí, že jiná hodnota implikuje, že stav je entanglovaný.

Entanglovaný stav dvou systémů s ortonormálními bázemi $|\Psi_n\rangle, |\Phi_n\rangle$ lze zapsat ve tvaru

$$|\Psi\rangle = \sum_n a_n |\Psi_n^A\rangle |\Phi_n^B\rangle.$$

V tomto případě je každý stav $|\Psi_n\rangle$ systému A jednoznačně přiřazen stavu $|\Phi_n\rangle$ systému B. Tato forma zápisu se nazývá Schmidtův rozklad (viz. [6]) a platí, že ortonormální stavy jsou vlastními vektory redukovaných operátorů hustoty pro jednotlivé systémy, tj. $\hat{\rho}_A = \sum_n a_n |\Psi_n\rangle\langle\Psi_n|$, $\hat{\rho}_B = \sum_n a_n |\Phi_n\rangle\langle\Phi_n|$. Tyto dva operátory mají zjevně tytéž

vlastní hodnoty, platí tedy $Tr(\hat{\rho}_A^2) = Tr(\hat{\rho}_B^2)$.

Mezi všemi možnými entanglovanými stavy mají velký význam následující tzv. Bellovy stavy (jedná se o maximálně provázané dvouqubitové stavy [5], které hrají klíčovou roli např. v kvantové teleportaci, což je přenos neznámého kvantového stavu, pomocí známého entanglovaného stavu a klasické komunikace, viz. [7]):

$$\begin{aligned}
 |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle), \\
 |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle), \\
 |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle), \\
 |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|1\rangle \otimes |1\rangle + |0\rangle \otimes |0\rangle).
 \end{aligned} \tag{2.2}$$

Bellovy stavy jsou společnými vlastními stavy operátorů $\hat{\sigma}_x \otimes \hat{\sigma}_x$, $\hat{\sigma}_y \otimes \hat{\sigma}_y$, $\hat{\sigma}_z \otimes \hat{\sigma}_z$ (mají vlastní hodnoty ± 1 ; operátory $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ nazýváme Pauliho operátory a budeme se jimi podrobněji zabývat v dalším textu, viz. (3.4)).

Provázání není samozřejmě omezeno pouze na dvojice kvantových systémů. V souvislosti s vícequbitovými systémy je užitečné zmínit GHZ (Greenbeeger-Horne-Zeilinger) stav

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle),$$

pomocí kterého lze dokázat, že pravděpodobnostní charakter je neoddělitelným rysem kvantové teorie, nikoli jenom důsledkem existence skrytých proměnných. Pomocí GHZ stavu lze provést experiment [8], kterým lze i bez použití Bellových nerovností ([9]) dokázat neexistenci zmíněných skrytých proměnných (viz. Příloha E).

Výše jsme prodiskutovali faktorizovatelnost maticové reprezentace operátoru hustoty vzhledem k vlastnosti provázání. Nicméně ne každá korelace dvou systémů musí nutně indikovat provázání. Jinými slovy, termínem entanglement se rozumí výhradně kvantový efekt a nikoli nekvantové statistické korelace. Obecně můžeme tvrdit následující:

- Všechny korelované čisté stavy jsou provázané.
- Pokud je operátor hustoty smíšeného stavu faktorizovatelný (tj. $\hat{\rho} = \hat{\rho}_A \otimes \hat{\rho}_B$), potom jsou systémy A, B nekorelované (jak v kvantovém, tak v klasickém smyslu).
- Smíšený stav není entanglovaný, pokud existuje rozklad $\sum_{ij} P(a_i, b_j) \hat{\rho}_a^i \otimes \hat{\rho}_b^j$, kde

$\{P(a_i, b_j)\}$ je množina sdružených pravděpodobností (tedy kladných čísel).

A naopak, o smíšeném stavu řekneme, že je entanglovaný, pokud uvedený rozklad neexistuje.

Abychom mohli formulovat postačující podmínku pro provázanost smíšeného stavu, uvedeme pojem částečné transpozice matice hustoty. Transpozici matice hustoty:

$$\hat{\rho} = \sum_{mn} \rho_{mn} |m\rangle\langle n|$$

definujeme jako zobrazení $|m\rangle\langle n| \mapsto |n\rangle\langle m|$. Částečné transpozice systému dosáhneme tak, že takto definovanou operaci provedeme pouze na jeden z dvojice systémů. Například pro systém A najdeme částečně transponovanou matici hustoty následujícím způsobem. Zapišeme-li ij -tý element matice hustoty ρ

$$\rho_{ij} = \langle \Psi_i | \rho | \Psi_j \rangle = \langle \Psi_{i,A} | \langle \Psi_{i,B} | \rho | \Psi_{j,A} | \Psi_{j,B} \rangle,$$

potom ij -tý element částečně transponované matice (značíme ρ^{TA}) je dán vztahem

$$\rho_{ij}^{TA} = \langle \Psi_{j,A} | \langle \Psi_{i,B} | \rho | \Psi_{i,A} | \Psi_{j,B} \rangle.$$

Pak může nastat situace, kdy částečně transponovaná matice není pozitivně definitní, tj. není maticí operátoru hustoty - to je postačující podmínka, aby byl smíšený stav entanglovaný.

Na závěr této kapitoly uvedeme některé možnosti, jak určit míru entanglementu daného systému. Za tím účelem nejprve zavedeme pojem von Neumannova entropie:

$$S(\hat{\rho}) = -\text{Tr}(\hat{\rho} \ln \hat{\rho}),$$

kde $\hat{\rho}$ je matice hustoty daného systému. Pro jednoduchost budeme opět uvažovat systém tvořený pouze dvěma podsystemy (označíme je A,B). Míru provázaní nazývanou index korelace definujeme [10]:

$$I_C = S_A + S_B - S,$$

kde S_A resp. S_B je von Neumannova entropie stavu podsystemu A resp. B, S je entropie celkového stavu systému. Index korelace nabývá pouze nezáporných hodnot a pro

neprovázané systémy je roven 0.

Míra provázání ve dvouhladinových systémech, kterou budeme v této práci využívat se nazývá concurrence $C(\hat{\rho})$, kde $\hat{\rho}$ je operátor hustoty a její definice je následující. Uvažujme operátor

$$\hat{R} = \rho(\hat{\sigma}_y \otimes \hat{\sigma}_y)\rho^*(\hat{\sigma}_y \otimes \hat{\sigma}_y). \quad (2.3)$$

Jeho vlastní hodnoty uspořádané od nejvyšší označíme: $\lambda_1, \dots, \lambda_4$. Concurrence je potom definována vztahem

$$C(\rho) = \max\{0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\}. \quad (2.4)$$

Tato veličina nabývá hodnot mezi nulou a jedničkou, kde hodnota jedna indikuje maximální provázání.

Touto definicí ukončíme seznámení s elementy kvantové teorie potřebné v dalším textu a začneme se zabývat otázkou, jak lze kvantovou teorii využít při přenosu informace.

Kapitola 3

Kvantové obvody

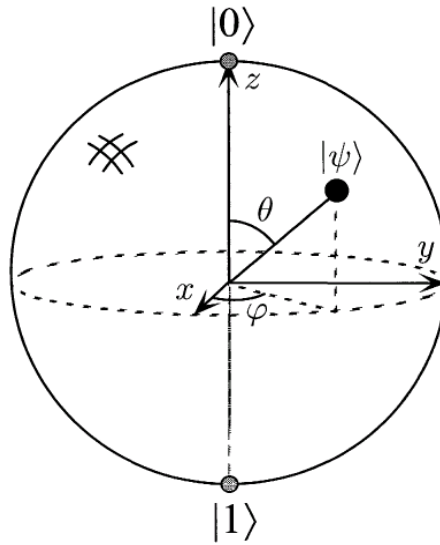
Budeme-li chtít využít jistý stav kvantového systému jako nositele informace, potom jeho dynamický vývoj musíme považovat za zpracování této informace (nebo prostě manipulaci s ní). Právě to je základní myšlenka kvantových sítí. Kvantový obvod je prostředek, kterým můžeme manipulovat se vstupní informací. Tuto manipulaci budeme v souladu se základními postuláty kvantové mechaniky (teoreticky, při zanedbání disipace) reprezentovat jistou unitární transformací.

Pro adekvátní popis logických proměnných v kvantové mechanice zavedeme vhodnou třídu dvouhladinových systémů. Vhodnou třídou rozumíme systém, který může nabývat dvou od sebe jednoznačně experimentálně odlišitelných stavů (těm přiřadíme logické proměnné) i všech superpozic (viz. (1.1)).

Jednotlivé proměnné pak lze asociovat systémům, které lze považovat za klasické - každému bitu budeme chtít jednoznačně přiřadit určitý systém, tzn. každému bitu jednoznačně přiřadíme ortonormální tzv. výpočetní bázi $\{|0\rangle, |1\rangle\}$. Obecný stav dvouhladinového systému pak zapíšeme jako

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (3.1)$$

což pro nás bude analogem klasického bitu - qubit. Koeficienty α, β jsou komplexní čísla, jinými slovy každý stav $|\Psi\rangle$ qbitu je vektor ve dvourozměrném komplexním prostoru. Vzhledem k faktům uvedeným v paragrafu 1.4 je nyní jasné, že při měření obdržíme výsledek 0 s pravděpodobností $|\alpha|^2$ nebo výsledek 1 s pravděpodobností $|\beta|^2$. Suma



Obrázek 3.1: Blochova sféra, převzato z [11].

pravděpodobností musí být rovna jedné, čili v našem případě:

$$|\alpha|^2 + |\beta|^2 = 1, \quad (3.2)$$

což znamená normalizaci stavového vektoru. Vzhledem k podmínce (3.2) můžeme rovnici (3.1) přepsat jako [11]

$$|\Psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right), \quad (3.3)$$

kde $\theta, \varphi, \gamma \in \mathcal{R}$. Faktor γ ovšem odpovídá globální fázi a nemá žádný pozorovatelný efekt (viz. např. [12]), můžeme jej tedy vhodně předefinovat a místo (3.3) psát

$$|\Psi\rangle = \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right),$$

přičemž parametry θ, φ udávají souřadnice bodu na jednotkové sféře. Tuto pak nazýváme Blochova sféra a každý její bod tedy odpovídá jistému stavu qubitů (viz. Obr. 3.1) .

Uvažujme nyní systém dvou qubitů. Pro dva klasické bity by takový systém mohl být ve čtyřech různých stavech: 00, 01, 10, 11. Rozvineme-li tedy výše uvedené zobecnění bitu na systém dvou qubitů, dojdeme k závěru, že výpočetní báze bude tentokrát tvořena čtyřmi vektory, které označíme $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Pro obecný stavový vektor popisující

systém dvou qubitů tak dostáváme

$$|\Psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

Kvantově mechanický stav tedy nese informaci všech možných lineárních kombinací dvou bitů v lineární superpozici. Přípravenému kvantovému stavu nyní přiřadíme jistou lineární transformaci. Tím definujeme kvantový výpočet:

$$\hat{K} : |AB\rangle \Rightarrow |f(A, B)\rangle,$$

kde $f(A, B)$ je booleovská funkce, kterou chceme výpočtem implementovat. Dostáváme:

$$\hat{K}|\Psi\rangle = \alpha_{00}|f(0, 0)\rangle + \alpha_{01}|f(0, 1)\rangle + \alpha_{10}|f(1, 0)\rangle + \alpha_{11}|f(1, 1)\rangle.$$

Tato transformace je kvantovým zobecněním logických funkcí $\{0, 1\}^2 \mapsto \{0, 1\}$.

Mějme dva systémy:

- 1 - vstupní systém ve stavu $|x\rangle_1$, kde x je 2^n -členné binární číslo
- 2 - výstupní systém v tzv. základním stavu, např. $|0\rangle_2$

Uvažujme $|\Psi_{in}\rangle = \sum_x |x\rangle_1 |0\rangle_2$. Výpočetní transformaci potom zapíšeme:

$$\hat{K} \sum_x |x\rangle_1 |0\rangle_2 = \sum_x |x\rangle_1 |f(x)\rangle_2,$$

s tím, že $f(x)$ je námi realizovaná logická funkce. Chceme-li, aby byl výpočet vratný, je třeba požadovat, aby hodnoty $\{f(x)\}$ byly nějakou permutací vstupních hodnot. Z toho plyne, že množina $\{|f(x)\rangle\}$ tvoří bázi 2^n -rozměrného stavového prostoru ($\{|x\rangle_1\}$ je báze). Zobrazili jsme tedy jednu bázi na jinou, tzn. námi definované zobrazení je unitární.

3.1 Jednoqubitové kvantové operace

Obecnou operaci aplikovanou na jeden qubit lze zapsat ve tvaru

$$\hat{U}(c_0|0\rangle + c_1|1\rangle) = a_0|0\rangle + a_1|1\rangle,$$

čili jedná se, jak bylo uvedeno výše, o unitární transformaci aplikovanou na vstupní stav. Dále uvedeme několi nejdůležitějších příkladů takových operací.

3.1.1 Pauliho hradla

Pauliho logická hradla $\hat{\sigma}_1$, $\hat{\sigma}_2$, $\hat{\sigma}_3$:

$$\begin{aligned}\hat{\sigma}_1 &= |0\rangle\langle 1| + |1\rangle\langle 0|, \\ \hat{\sigma}_2 &= -i|1\rangle\langle 0| + i|0\rangle\langle 1|, \\ \hat{\sigma}_3 &= |0\rangle\langle 0| - |1\rangle\langle 1|.\end{aligned}\tag{3.4}$$

V maticové reprezentaci:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\tag{3.5}$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\tag{3.6}$$

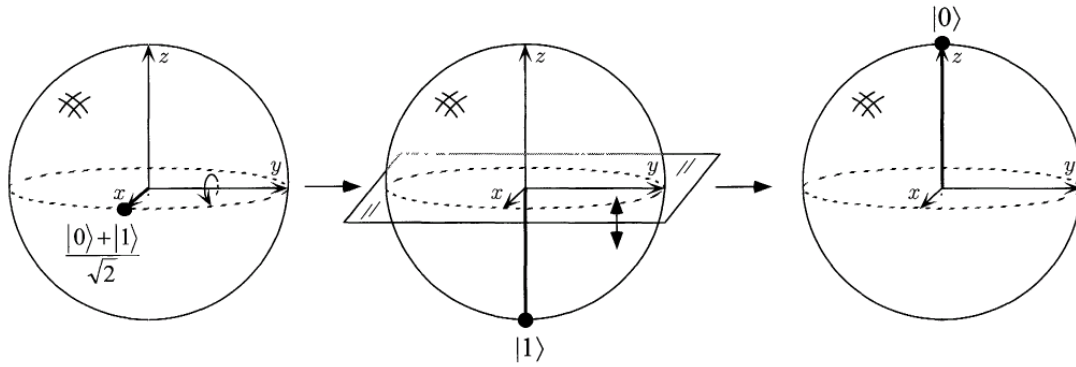
$$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.\tag{3.7}$$

Tyto matice společně s jednotkovou maticí tvoří bázi prostoru matic 2×2 . Je patrné, že σ_1 by alespoň v dobře známém klasickém případě odpovídala záměně obsahu bitu, v případě obecného kvantového stavu je ale toto třeba zobecnit, čímž se budeme zabývat v kapitole 3.1.3. Ze stejného intuitivního pohledu bude σ_3 otočení fáze a, protože platí

$$[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k,\tag{3.8}$$

je σ_2 kombinací předchozího. Determinant Pauliho matic je roven -1 a jejich stopa je nulová. Příslušné exponenciely navíc generují spojitou třídu jednoqubitových rotací, jak bude podrobněji rozebráno níže.

Aplikujeme-li libovolné z předchozích rotací na jistý stav, generujeme tak stavový prostor, který je reprezentován Blochovou sférou. Každý bod na sféře odpovídá určitému stavu a toto přiřazení je, až na globální fázi, jednoznačné. Vlastní stavy kteréhokoli Pauliho operátoru, budou protilehlými póly Blochovy sféry.



Obrázek 3.2: Geometrická interpretace Hadamardovy transformace, převzato z [11].

3.1.2 Hadamardovo hradlo

V termínech Pauliho matic zdefinujeme Hadamardovu transformaci následovně

$$H = \frac{1}{\sqrt{2}}(\sigma_1 + \sigma_3) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (3.9)$$

čili

$$\hat{H}(c_0|0\rangle + c_1|1\rangle) = c_0 \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} + c_1 \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} = \frac{1}{\sqrt{2}}[(c_0 + c_1)|0\rangle + (c_0 - c_1)|1\rangle].$$

Jedná se o speciální případ diskretní Fourierovy transformace (viz. [12]). Vztah Hadamardovy transformace k Pauliho maticím:

$$H\sigma_1 = \sigma_3H \quad \text{resp.} \quad H\sigma_1H = \sigma_3 \quad \text{a} \quad H\sigma_3H = \sigma_1$$

a navíc

$$H\sigma_2H = -\sigma_1.$$

Transformace popsaná rovnicí (3.9) je realizovatelná pomocí jediného optického prvku, symetrického děliče paprsku, kterým se budeme podrobně zabývat v následující kapitole. Charakter samotné transformace můžeme vizualizovat pomocí Blochovy sféry (viz. Obr. 3.2): jedná se o rotaci o $\frac{\pi}{2}$ kolem osy y , následovanou symetrickým přenesením daného bodu vzhledem k rovině xy .

3.1.3 NOT hradlo

Jedná se o operaci dobře známou z klasického kontextu, která je definována jednoduše jako přiřazení bitu opačné hodnoty, než je jeho stávající. Odpovídající pravdivostní tabulka je tato: $0 \mapsto 1$, $1 \mapsto 0$. Lze si snadno rozmyslet, že se jedná o jediný netriviální prvek množiny klasických operací aplikovaných na jeden bit (v klasickém smyslu slova). V kvantovém kontextu je třeba rozšířit tuto definici i na možné superpozice bázeových stavů (viz. (1.1)):

$$\sigma_1(c_0|0\rangle + c_1|1\rangle) = c_0|1\rangle + c_1|0\rangle. \quad (3.10)$$

To ale znamená, že maticová reprezentace této transformace odpovídá, právě Pauliho σ_1 (viz. (3.5)). Navíc je vhodné si uvědomit, že uvedená analogie platí jen do jisté míry, v rovnici (3.10) operátor (3.5) sice zamění kety, nicméně relace ortogonalita se na rozdíl od klasického případu nezachovává.

3.1.4 Fázový posun

Cílem operace je změnit fázi vstupujícího paprsku ve smyslu

$$\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle + \beta e^{i\varphi}|1\rangle.$$

Tomu odpovídá maticová reprezentace:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}.$$

Působení operátoru:

$$\hat{S}(c_0|0\rangle + c_1|1\rangle) = c_0 e^{-i\varphi/2}|0\rangle + c_1 e^{i\varphi/2}|1\rangle = e^{-i\varphi/2}(c_0|0\rangle + c_1 e^{i\varphi}|1\rangle)$$

Transformaci lze přiblížit jako časový vývoj, který ale v daném optickém prvku bude probíhat s jinou rychlostí. V praxi se jedná o aplikaci prostorové anizotropie vzhledem k indexu lomu, lze tedy použít destičku z klasického dvojlomného materiálu.

Jak bylo řečeno výše, pomocí Pauliho matic (3.5), (3.6), (3.7) lze zadefinovat třídy

unitárních matic, které odpovídají rotacím kolem jednotlivých os:

$$R_x(\theta) = e^{-\theta\sigma_1} = \cos(\theta/2)I - i\sin(\theta/2)\sigma_1 = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \quad (3.11)$$

$$R_y(\theta) = e^{-\theta\sigma_2} = \cos(\theta/2)I - i\sin(\theta/2)\sigma_2 = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}, \quad (3.12)$$

$$R_z(\theta) = e^{-\theta\sigma_3} = \cos(\theta/2)I - i\sin(\theta/2)\sigma_3 = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}. \quad (3.13)$$

Operátory rotace jsou zásadní pro popis libovolného jednoqubitového unitárního operátoru. Platí totiž následující:

Rozklad jednoqubitového unitárního operátoru: Pro každý jednoqubitový unitární operátor \hat{U} existují reálná čísla $\alpha, \beta, \gamma, \delta$ taková, že platí

$$\hat{U} = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta).$$

Důkaz se provede pomocí definic (3.11), (3.12), (3.13) a je uveden např. v [11]. Důsledkem existence tohoto rozkladu je následující obecnější tvrzení:

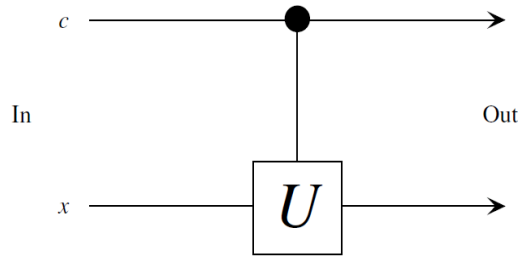
Pro každý jednoqubitový unitární operátor \hat{U} existují unitární jednoqubitové operátory $\hat{A}, \hat{B}, \hat{C}$ takové, že platí $\hat{A}\hat{B}\hat{C} = \hat{I}$ a

$$\hat{U} = e^{i\alpha}\hat{A}\hat{\sigma}_1\hat{B}\hat{\sigma}_1\hat{C}, \quad (3.14)$$

kde $\alpha \in \mathbb{C}$ je celkový fázový faktor.

V souvislosti s rotacemi ještě uvedeme následující zajímavou analogii mezi symetriemi grupy $SU(2)$ a děliči paprsku: Definujme následující zobrazení

$$\begin{aligned} \hat{a}^\dagger\hat{a} - \hat{b}^\dagger\hat{b} &\mapsto \hat{\sigma}_3, \\ \hat{a}^\dagger\hat{b} &\mapsto \hat{L}_+, \\ \hat{a}\hat{b}^\dagger &\mapsto \hat{L}_-. \end{aligned}$$



Obrázek 3.3: Schématické znázornění libovolné podmíněné unitární transformace U , převzato z [12].

\hat{L}_{\pm} jsou posunovací operátory definované

$$\hat{L}_{\pm} = \frac{\hat{\sigma}_1 \pm \hat{\sigma}_2}{2}$$

a $\hat{\sigma}_{1,2,3}$ jsou operátory definované relacemi (3.4). Z komutačních relací (4.2) zjistíme, že vyhovují vztahům (3.8). Navíc vzhledem k faktu, že operátor celkového počtu kvant

$$\hat{N} = \hat{a}^{\dagger}\hat{a} + \hat{b}^{\dagger}\hat{b}$$

komutuje se $\hat{\sigma}_3$ i s \hat{L}_{\pm} , je tedy invariantem vzhledem k rotacím v $SU(2)$. Položíme-li

$$\hat{\sigma}_1 = \hat{a}^{\dagger}\hat{b} + \hat{b}^{\dagger}\hat{a} \quad \text{a} \quad \hat{\sigma}_2 = -i(\hat{a}^{\dagger}\hat{a} - \hat{b}^{\dagger}\hat{b}),$$

pak právě rotační operátor

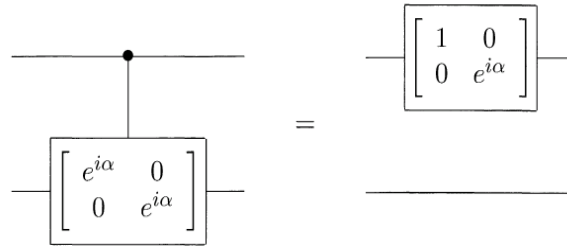
$$\hat{R}(\vec{n}, \theta) = e^{-i\theta\vec{\sigma}\vec{n}/2}$$

přesně odpovídá unitárnímu operátoru časového vývoje pro dělič paprsku s hamiltoniánem (4.4). Podrobně se tímto hamiltoniánem a jeho vlastnostmi budeme zabývat v následující kapitole.

3.2 Vícequbitové operace

Hilbertův prostor dvou qubitů získáme jako tenzorový součin Hilbertových prostorů příslušejících jednotlivým qubitům: $H_{12} = H_1 \otimes H_2$. Standartní bázi na tomto prostoru zavedeme jako $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, kde $|00\rangle = |0\rangle \otimes |0\rangle$ atd.

Uvažujme nejprve dvouqubitové operace. V tomto případě jeden bit slouží jako kon-



Obrázek 3.4: K odvození vztahu (3.15) - ekvivalence podmíněného fázového posunutí v obou modech a fázovým posuvem pouze pro druhý mod dodefinovaným identickou transformací na modu prvním, převzato z [12].

trolní a na druhém chceme uskutečnit požadovanou transformaci \hat{U}_c (jenom v případě, že je první qubit v určitém požadovaném stavu):

$$|c\rangle_1|x\rangle_2 \Rightarrow |c\rangle_1\hat{U}_c|x\rangle_2.$$

viz. Obr. (3.3). Jak uvidíme v dalším textu, mít k dispozici alespoň jednu dvouqubitovou transformaci je naprosto esenciální pro vytvoření obecné transformace na prostoru více qubitů.

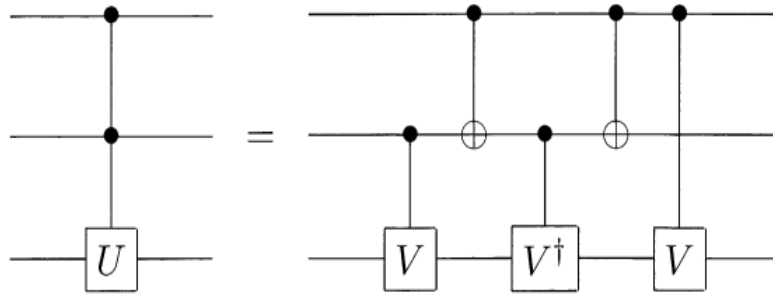
3.2.1 CNOT hradlo

Na výše zavedeném dvouqubitovém prostoru je tato operace definována jako $\mathbf{1} \otimes |0\rangle\langle 1| + \sigma_1 \otimes |1\rangle\langle 1|$. Čili

$$U_{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Lze ukázat [6], že každou obecnou qubitovou transformaci lze složit z jednoqubitových a CNOT operace. Říkáme, že se jedná o univerzální množinu logických operací.

CNOT hradlo lze využít, v jistém smyslu, k vytvoření kopie informace. Víme, že kvantová mechanika nedovoluje vytvořit kopii libovolného náhodného kvantového stavu (viz. (A)). Nicméně nyní jsme v situaci, kdy máme dopředu pevně zvolenou bázi (=výpočetní



Obrázek 3.5: Konstrukce obecné podmíněné unitární operace z prvků univerzální množiny logických hradel, převzato z [12].

báze). Pomocí CNOT hradla realizujeme transformaci:

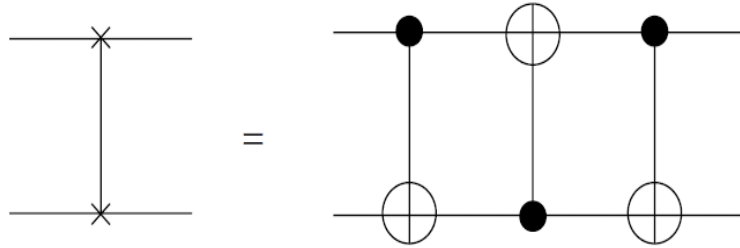
$$(\alpha|0\rangle_1 + \beta|1\rangle_1)|0\rangle_2 \Rightarrow \alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|1\rangle_2,$$

pomocí které jsme stav zakódovali do vícedimenzionálního prostoru. Informaci $\{\alpha, \beta\}$ tak máme uchovánu pomocí obou systémů a do sporu s no-cloning teorémem se nedostáváme z toho důvodu, že v našem případě nemáme na konci procesu dva objekty ve stejném stavu, ale dva různé stavy uchovávající tutéž informaci.

CNOT operaci můžeme samozřejmě implementovat i pro více qubitů - jeden kontrolní bude podmiňovat provedení NOT operace na více systémech najednou. CNOT hradlo je nejtypičtější ukázkou podmíněné logické operace ('je-li splněno A, udělej B'). Je zřejmé, že pro provedení operace jsou třeba dva vstupní qubity (control a target qubit). Jimi tvořenou (výpočetní) bázi označíme $|c\rangle, |t\rangle$. Akci operátoru lze potom zapsat jako: $|c\rangle|t\rangle \mapsto |c\rangle|t \oplus c\rangle$.

Toto lze zobecnit na libovolný unitární operátor \hat{U} . Pokud je první qubit v požadovaném stavu, na druhý je aplikována operace \hat{U} , není-li tomu tak, je druhý qubit ponechán beze změny čili $|c\rangle|t\rangle \mapsto |c\rangle\hat{U}^c|t\rangle$.

Nyní nás bude zajímat, jak popsat obecnou podmíněnou unitární operaci pomocí výše zmíněné univerzální množiny logických operací. K tomu využijeme vztah (3.14). Prvním krokem je aplikace fázového posunu $e^{i\alpha}$ na první qubit. To je totéž jako stejná operace aplikovaná na dvouqubitový systém, pro náš případ: fázový posun bude aplikován na druhý pouze v případě, že první je například ve stavu $|1\rangle$. Schematicky znázorněno, viz Obr. 3.4.



Obrázek 3.6: Schématické znázornění SWAP hradla a jeho konstrukce ze tří CNOT hradel, převzato z [12].

Dále využijeme skutečnosti, že máme zaručenou existenci rozkladu $\hat{U} = e^{i\alpha} \hat{A} \hat{\sigma}_1 \hat{B} \hat{\sigma}_1 \hat{C}$, $\hat{A} \hat{B} \hat{C} = \hat{I}$. V případě, že kontrolní qubit je ve stavu $|1\rangle$, U je aplikováno na druhý qubit. Naopak pro situaci, kdy kontrolní qubit je ve stavu $|0\rangle$, je na druhý qubit aplikováno $\hat{A} \hat{B} \hat{C} = \hat{I}$. Výsledné schéma je na Obr. (3.5).

Dále budeme uvažovat zobecnění na hradla, obsahující libovolné množství qubitů, označíme jej $n+k$. Dále buď \hat{U} k -qubitový unitární operátor. Operaci $\hat{C}^n \hat{U}$ definujeme následovně:

$$\hat{C}^n \hat{U} |x_1 x_2 \dots x_n\rangle |\Psi\rangle = |x_1 x_2 \dots x_n\rangle \hat{U}^{x_1 x_2 \dots x_n} |\Psi\rangle, \quad (3.15)$$

kde exponent $x_1 x_2 \dots x_n$ má smysl produktu. Daný unitární operátor je aplikován na posledních k qubitů tehdy a jen tehdy, je-li n předchozích ve stavu $|1\rangle$. Ve všech ostatních případech zůstává systém beze změny.

3.2.2 SWAP hradlo

SWAP hradlo odpovídá následující operaci:

$$|a, b\rangle \mapsto |b, a\rangle \quad (3.16)$$

Maticová reprezentace:

$$U_{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Již víme, že akci operátoru U_{CNOT} můžeme zapsat jako $|a, b\rangle \Rightarrow |a, a \oplus b\rangle$. Operaci

SWAP lze vytvořit vhodným složením tří operací CNOT (viz. Obr. (3.6)). Platí:

$$|a, b\rangle \Rightarrow |a, a \oplus b\rangle \Rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \Rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle.$$

3.2.3 Toffoliho hradlo

Toffoliho hradlo je tříqubitový systém, který v notaci (3.15) odpovídá operaci $\hat{C}^2\hat{U}$. Funguje vlastně jako dvojitě CNOT hradlo. Bázové stavy zůstávají nezměněné s právě dvěma výjimkami:

$$|110\rangle \mapsto |111\rangle \quad \text{a} \quad |111\rangle \mapsto |110\rangle.$$

Z toho je zřejmé, že se jedná o vratnou logickou operaci, aplikujeme-li toto hradlo dvakrát za sebou, dostaneme původní uspořádání (tj. Toffoliho hradlo je samo sobě inverzním prvkem:

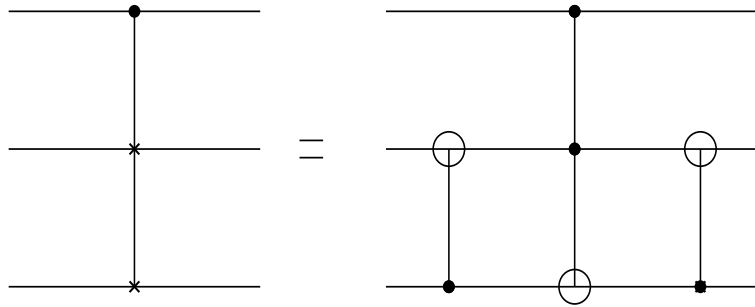
$$(a, b, c) \mapsto (a, b, c \oplus ab) \mapsto (a, b, c).$$

Maticová reprezentace ve výpočetní bázi vypadá následovně:

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

3.2.4 Fredkinovo hradlo

Budeme-li Toffoliho hradlo chápat, jako podmíněnou CNOT operaci, pak Fredkinovo je podmíněnou SWAP operací (viz. (3.16)) ve smyslu, že operace SWAP je aplikována na druhý a třetí qubit, pokud je první ve stavu $|1\rangle$. Je-li první qubit ve stavu $|0\rangle$, jsou



Obrázek 3.7: Konstrukce Fredkinova hradla z Toffoliho a dvou CNOT hradel.

zbylé dva ponechány beze změny [6]:

$$\hat{U}_{Fredkin}|A\rangle \otimes |B\rangle \otimes |C\rangle = |A\rangle \otimes |\hat{U}_{NOT}A \cdot B + A \cdot C\rangle \otimes |\hat{U}_{NOT}A \cdot C + A \cdot B\rangle,$$

kde jsme \hat{U}_{NOT} označili operaci definovanou vztahem (3.10).

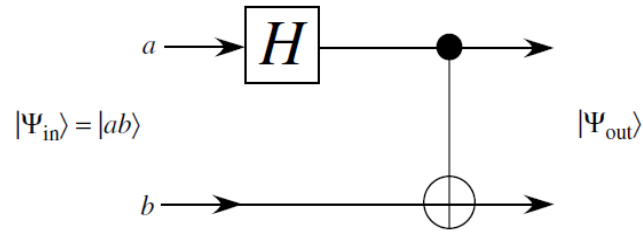
Maticová reprezentace Fredkinova hradla je tato:

$$U_{Fredkin} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Schématické znázornění Fredkinova hradla je na Obr. 3.7. Toto hradlo je možné sestavit s Toffoliho a dvou CNOT hradel, což je rovněž znázorněno na Obr. 3.7, přičemž ověření příslušné rovnosti snadno získáme vynásobením matic reprezentujících operace na pravé straně.

3.2.5 Generace Bellových stavů

Hledejme nyní obvod, který bude uskutečňovat transformaci výpočetní báze v dvouqubitovém prostoru na Bellovy stavy (viz. (2.2)). Uvážíme-li, že chceme jistou lineární kombinaci bázevých stavů: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, bude zjevně třeba použít realizaci

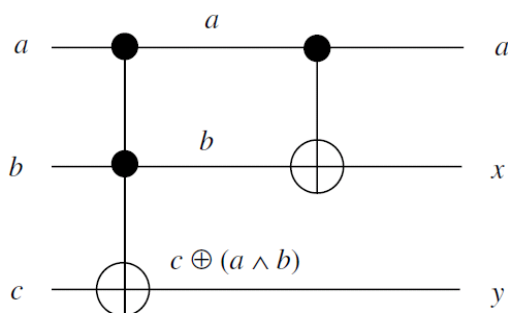


Obrázek 3.8: Hradlo, které transformuje výpočetní bázi na Bellovy stavy, převzato z [12].

Hadamardovy transformace a k dosažení 'správné' lineární kombinace použijeme právě operaci CNOT. Uvažujme například, že máme vstupní stav $|00\rangle$ a chceme z něj vytvořit stav $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Navrhnutý obvod je na Obr. (3.8). Operátorově: $C\hat{N}O\hat{T} \cdot \hat{H} \otimes \hat{1}$. Ověříme správnost ve výpočetní bázi:

$$\begin{aligned} & \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \\ & = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \end{aligned}$$

Aplikací takto definovaného operátoru na ostatní báze stavy obdržíme ostatní Bellovy stavy. V principu ale pro jejich generaci stačí jediný báze stav. Například zobrazení: $|00\rangle \mapsto |10\rangle$ bude realizovat třeba operátor $|0\rangle\langle 1| \otimes \hat{\sigma}_1 + |1\rangle\langle 0| \otimes \hat{1}$ nebo vhodné kombinace SWAP a CNOT, tj. konečným počtem CNOT transformací můžeme přecházet mezi jednotlivými báze stavy a pak už pouze použít obvod (3.8).



Obrázek 3.9: Hradlo realizující operaci binárního sčítání (kombinace Toffoliho a CNOT hradla), převzato z [12].

3.2.6 Obvod realizující binární sčítání

Na závěr tohoto přehledu uvedme obvod realizující binární sčítání (Obr. (3.9)), který je kombinací výše popsaných Toffoliho a CNOT hradla. Realizovaná operace:

$$x = a \oplus b,$$

$$y = 0 \oplus ab = ab,$$

kteřá odpovídá transformaci (3.2.3), kde jsme položili $c = 0$.

Tím ukončíme přehled logických operací. Podrobně jsme rozebrali základní jedno-qubitové operace a operaci CNOT, přičemž už máme k dispozici tvrzení o jejich univerzalitě. Navíc jsme uvedli několik jednoduchých příkladů propojení těchto základních elementů za účelem provedení složitějších operací. Nyní je zřejmě třeba vyřešit proveditelnost nebo alespoň návrh fyzikální realizace těchto teoretických modelů. Jako přehled některých možností poslouží následující kapitola.

Kapitola 4

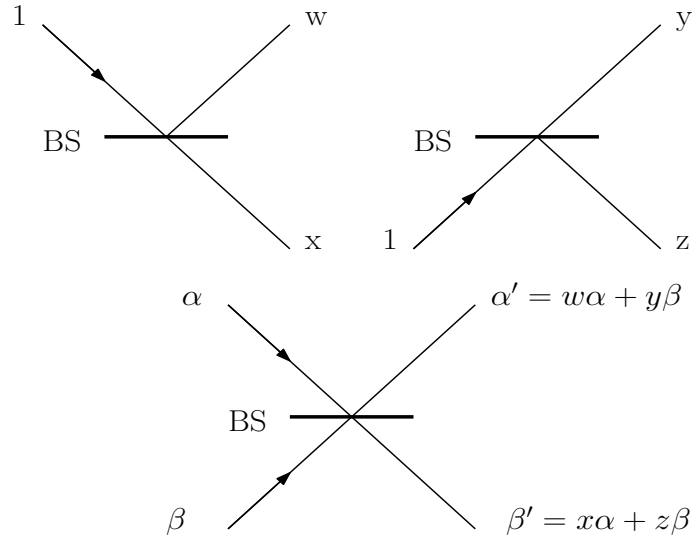
Přehled základních optických elementů

V této kapitole se budeme zabývat fyzikálními realizacemi dříve popsaných logických operací. Fyzikální prakticky využitelnou reprezentací qubitu je foton. Splňuje totiž podmínky, které jsme kladli na vhodný dvouhladinový systém, který bychom chtěli jako qubit použít (jednoznačně rozlišitelné stavy mohou být například navzájem kolmé polarizace), nicméně, jak uvidíme, s použitím fotonů souvisí i řada experimentálních komplikací (jako absorpce při interakci s prostředím). Kvantový obvod, který jsme výše popsali jako prostředek manipulující se vstupním stavem, nyní budeme chápat jako síť složenou z jednotlivých optických prvků, které budou realizací popsaných qubitových operací.

4.1 Dělič paprsku

Jedná se o optický element, který rozdělí vstupní paprsek na dva paprsky s menší intenzitou (polopropustné zrcadlo). Popíšeme situaci z hlediska pravděpodobnostních amplitud pro jediný foton vstupující do děliče. Jak je zřejmé z Obr. 4.1 existují dvě možnosti vstupu paprsku do děliče. Pro každý označíme amplitudu pravděpodobnosti odrazu a průchodu podle Obr. 4.1. Uvažujme dále symetrii v tom smyslu, že pravděpodobnost, že se foton odrazí nebo projde, je tatáž. Označíme-li amplitudy pro foton vstupující do děliče α, β a vystupující α', β' , z principu superpozice dostáváme

$$\begin{aligned}\alpha' &= w\alpha + y\beta, \\ \beta' &= x\alpha + z\beta,\end{aligned}\tag{4.1}$$



Obrázek 4.1: Dělič paprsku - označení amplitud pravděpodobnosti odrazu a průchodu.

čili

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \mapsto \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = \begin{pmatrix} w & y \\ x & z \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Nejjednodušší případ děliče paprsků je symetrický (nebo vyvážený) takový, pro který maticová realizace jím provedené transformace vypadá následovně

$$B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Snadno ověříme, že pro takto realizovaná transformace splňuje normovací podmínku (suma pravděpodobností = kvadrátů amplitud na výstupu je rovna jedné). Praktická realizace této transformace vlastně odpovídá tomu, že je-li "spodní" vstupní paprsek odražen, změní se jeho fáze o π , projde-li děličem, fáze zůstává zachována.

Dále uvedeme podrobnější popis děliče paprsků pomocí kreačních a anihilačních operátorů (viz. [1]), které vyhovují těmto komutačním relacím:

$$[\hat{a}, \hat{a}^\dagger] = [b, b^\dagger] = 1, \quad [\hat{a}, b] = [\hat{a}^\dagger, b^\dagger] = 0, \quad (4.2)$$

kde \hat{a}, \hat{b} jsou anihilační, $\hat{a}^\dagger, b^\dagger$ kreační operátory.

Vztahy (4.1), které jsme obdrželi z intuitivní představy chování paprsku na polopropustném optickém elementu a principu superpozice, můžeme přepsat v termínech výše

zmíněných operátorů jako transformaci mezi vstupními a výstupními mody následovně:

$$\begin{aligned}\hat{a}_{out}^\dagger &= \alpha_1 \hat{a}_{in}^\dagger + \beta_2 \hat{b}_{in}^\dagger, \\ \hat{b}_{out}^\dagger &= \beta_1 \hat{a}_{in}^\dagger + \alpha_2 \hat{b}_{in}^\dagger,\end{aligned}$$

z čehož plyne, že příslušná unitární matice má tvar

$$U = \begin{pmatrix} \alpha_1 & \beta_2 \\ \beta_1 & \alpha_2 \end{pmatrix}.$$

Z požadavku na unitaritu transformace a platnost relací (4.2) obdržíme podmínky, které musí splňovat koeficienty průchodu a odrazu:

$$\begin{aligned}\alpha_1 \beta_1^* + \alpha_2^* \beta_2 &= 0, \\ |\alpha_1|^2 + |\beta_2|^2 &= 1 = |\alpha_2|^2 + |\beta_1|^2,\end{aligned}$$

ze kterých plyne

$$\begin{aligned}|\alpha_1| &= |\alpha_2|, \\ |\beta_1| &= |\beta_2|.\end{aligned}$$

Přejdeme nyní v popisu děličů paprsku ke Schrödingerově reprezentaci. Pro jednoduchost nejprve uvážíme situaci kdy jeden mod je excitovaný a druhý je ve vakuu - vstupní dvoučásticový stav tedy označíme: $|10\rangle$. Potom

$$\begin{aligned}|1_a 0_b\rangle \mapsto |\Psi\rangle &= \hat{U}(\theta)|1_a 0_b\rangle = \hat{U}(\theta)a^\dagger|00\rangle = \hat{U}(\theta)\hat{a}^\dagger\hat{U}^\dagger(\theta)|00\rangle = \\ &= (\cos\theta\hat{a}^\dagger + i\sin\theta\hat{b}^\dagger)|00\rangle = \cos\theta|01\rangle + i\sin\theta|01\rangle.\end{aligned}$$

Při úpravě rovnice využíváme skutečnosti $\hat{U}^\dagger|00\rangle = |00\rangle$ a identit

$$\hat{U}^\dagger(\theta)\hat{a}U(\theta) = \cos\theta\hat{a} + i\sin\theta\hat{b} \quad \text{a} \quad \hat{U}^\dagger(\theta)\hat{b}U(\theta) = i\sin\theta\hat{a} + \cos\theta\hat{b}, \quad (4.3)$$

kde $\hat{U} = e^{-i\hat{H}t}$ je operátor časového vývoje odpovídající Hamiltoniánu

$$\hat{H} = -\lambda(\hat{a}\hat{b}^\dagger + \hat{a}^\dagger\hat{b}), \quad (4.4)$$

který na pole působí po dobu $t = \theta/\lambda$. Souvislost mezi vztahy (4.3) a (4.4) odvodíme pomocí Baker-Hausdorffovy identity [13]

$$\exp(i[\hat{G}\theta]\hat{a})\exp(-i[\hat{G}\theta]) = \hat{a} + i\theta[[\hat{G}, \hat{a}] + \frac{i^2\theta^2}{2!}[[\hat{G}, [[\hat{G}, \hat{a}]]] + \dots + \frac{i^n\theta^n}{n!}[[\hat{G}, [[[\hat{G}, \dots [[\hat{G}, \hat{a}]]]]]] + \dots, \quad (4.5)$$

kde položíme $\hat{G} = -(\hat{a}\hat{b}^\dagger + \hat{a}^\dagger\hat{b})$. Komutátory na pravé straně (4.5) budou pro sudé členy rozvoje úměrné \hat{b} , pro liché členy \hat{a} (protože $[[\hat{G}, \hat{a}]] = \hat{b}$; $[[[\hat{G}, [[\hat{G}, \hat{a}]]]] = \hat{a}$). Koeficienty u \hat{a} resp. \hat{b} pak dávají Taylorův rozvoj funkcí $\sin x$ resp. $\cos x$.

Jinak se lze k výsledku (4.3) dostat řešením Heisenbergových pohybových rovnic:

$$i\dot{\hat{a}} = [\hat{a}, \hat{H}], \quad i\dot{\hat{b}} = [\hat{b}, \hat{H}].$$

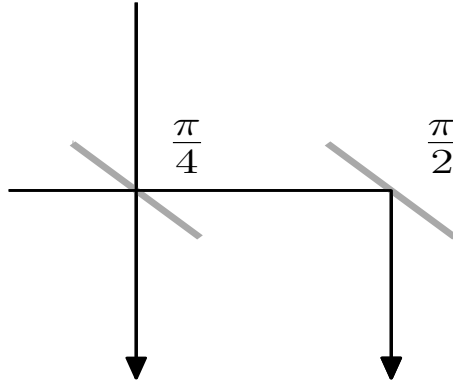
Analogicky budeme postupovat při hledání výsledného stavu pro více fotonů. Mějme tedy n fotonů v prvním modu. Obdobně jako v předchozím dostáváme:

$$\begin{aligned} |n_a 0_b\rangle \mapsto |\Psi\rangle &= \hat{U}(\theta)|n_a 0_b\rangle = \hat{U}(\theta)\frac{(\hat{a}^\dagger)^n}{\sqrt{n!}} = \\ &= \frac{1}{\sqrt{n!}}\hat{U}(\theta)(\hat{a}\hat{a}^\dagger)^n\hat{U}^\dagger(\theta)|00\rangle = \\ &= \frac{1}{\sqrt{n!}}(\cos\theta\hat{a}^\dagger)^n + i\sin\theta\hat{b}^\dagger)^n|00\rangle = \\ &= \sum_{p=0}^n \binom{n}{p}^{\frac{1}{2}} (\cos\theta)^{n-p}(i\sin\theta)^p|n-p, p\rangle. \end{aligned}$$

Výsledná superpozice odpovídá binomickému rozdělení n vstupujících fotonů mezi mody a, b .

Dále budeme na prvním vstupu uvažovat koherentní stav $|\alpha\rangle$ (nejdůležitější vlastnosti koherentních stavů jsou shrnuty v Příloze B)

$$\begin{aligned} |\alpha_a 0_b\rangle \mapsto |\Psi\rangle &= \hat{U}(\theta)e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\hat{U}^\dagger(\theta)|00\rangle = \\ &= \exp(\alpha[\cos\theta\hat{a}^\dagger + i\sin\theta\hat{b}^\dagger] - \alpha^*[\cos\theta\hat{a} - i\sin\theta\hat{b}])|00\rangle = \\ &= |\alpha\cos\theta\rangle_a |i\alpha\sin\theta\rangle_b, \end{aligned}$$



Obrázek 4.2: Experimentální uspořádání pro generování superpozice typu $|n, 0\rangle + |0, n\rangle$, pomocí dvou nelineárních děličů paprsků s parametry $\theta = \frac{\pi}{4}$ resp. $\theta = \frac{\pi}{2}$.

kde jsme použili (B.1), (4.3) a identity [14]

$$\hat{U}f(\hat{A})\hat{U}^\dagger = f(\hat{U}\hat{A}\hat{U}^\dagger). \quad (4.6)$$

Výsledkem je tedy separabilní tenzorový součin koherentních stavů.

4.2 Nelineární dělič paprsku

Toto je první z paragrafů, ve kterých se budeme zabývat nelineárními optickými elementy, jejichž vlastnosti se budou výrazně lišit od uvedených lineárních prvků.

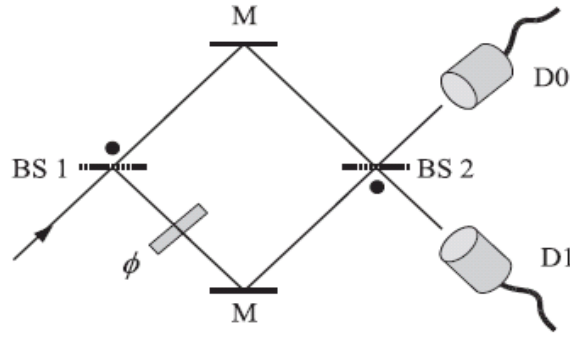
V předchozím textu jsme rozebrali vícefotonový aspekt u lineárního děliče paprsku a viděli jsme, jak více fotonů ovlivní pravděpodobnostní rozdělení výstupního stavu, nicméně u nelineárních prvků hraje vícefotonový aspekt mnohem výraznější roli, která vede k možnostem realizace transformací, které by pouze pomocí lineárních prvků nebyly možné (například experimentální realizace CNOT hradla).

Hamiltonián nelineárního děliče paprsku má tvar [13]:

$$\hat{H}_n = -\hbar\lambda[\hat{a}(\hat{b}^\dagger)^n + \hat{a}^\dagger(\hat{b})^n].$$

Tomu tedy odpovídá transformace jednoho fotonu v modu a na n fotonů v modu b :

$$\begin{aligned} [\hat{a}(\hat{b}^\dagger)^n + \hat{a}^\dagger(\hat{b})^n]|1_a 0_b\rangle &= \sqrt{n!}|0_a n_b\rangle, \\ [\hat{a}(\hat{b}^\dagger)^n + \hat{a}^\dagger(\hat{b})^n]|0_a n_b\rangle &= \sqrt{n!}|1_a 0_b\rangle. \end{aligned}$$



Obrázek 4.3: Schéma Mach-Zehnderova interferometru, převzato z [5].

Kvůli zákonu zachování energie je třeba, aby každý vzniklý foton v modu b měl n -krát menší energii než vstupní stav v modu a . Užitím Baker-Hausdorffovy formule stejně jako v předchozí sekci dostáváme:

$$\begin{aligned} \exp[i\lambda t(\hat{a}(\hat{b}^\dagger)^n + \hat{a}^\dagger(\hat{b})^n)]|10\rangle &= \cos\theta|10\rangle + i\sin\theta|0n\rangle, \\ \exp[i\lambda t(\hat{a}(\hat{b}^\dagger)^n + \hat{a}^\dagger(\hat{b})^n)]|0n\rangle &= i\sin\theta|10\rangle + \cos\theta|0n\rangle, \end{aligned} \quad (4.7)$$

kde nyní $\theta = \frac{\lambda t}{\sqrt{n!}}$. Jinými slovy, teoreticky je možné připravit superpozici fotonu s n dalšími, které budou všechny v tomtéž modu, což lze vhodným experimentálním uspořádáním rozšířit i na superpozice typu $|n, 0\rangle + |0, n\rangle$ (viz. Obr. 4.2).

4.3 Interferometr

Interferometr je optické zařízení, jehož účelem je měření velmi malých fázových posunů, sestávající se ze dvou nebo více děličů paprsků. Jednoduchým příkladem může být například Mach-Zehnderův interferometr (Obr. 4.3): dva symetrické děliče paprsků, dvě zrcadla a fázový posun o úhel Φ v jednom z ramen. Uvážíme-li, že i zrcadlo můžeme chápat jako optický element, jenž odpovídá změně fáze o π , obdržíme následující maticovou reprezentaci:

$$U_{MZ} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & e^{i\Phi} \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Opět vyjdeme od jednofotonového stavu $|10\rangle$. Aplikace BS_1 , Φ , BS_2 podle Obr. 4.3:

$$\begin{aligned}
 |01\rangle &\mapsto \frac{1}{\sqrt{2}}(|10\rangle + i|01\rangle) \mapsto \frac{1}{\sqrt{2}}(|10\rangle + ie^{i\Phi}|01\rangle) \\
 &\mapsto \frac{1}{2}(|10\rangle + i|01\rangle) + i\frac{e^{i\Phi}}{2}(i|10\rangle + |01\rangle) = \\
 &= \frac{1}{2}(1 - e^{i\Phi})|10\rangle + \frac{1}{2}(1 + e^{i\Phi})|01\rangle.
 \end{aligned} \tag{4.8}$$

Počet fotonů S_0 v detektoru D_0 :

$$S_0 \propto \langle \Psi | a^\dagger a | \Psi \rangle = \langle \Psi | a^\dagger | 00 \rangle \langle 00 | a | \Psi \rangle = |\langle 00 | a \Psi \rangle|^2 = \frac{1}{2}(1 - \cos \Phi). \tag{4.9}$$

Počet fotonů S_1 v detektoru D_1 :

$$S_1 \propto \frac{1}{2}(1 + \cos \Phi). \tag{4.10}$$

Provedeme nyní znovu zobecnění na stavy s více fotony. Skládal-li by se Mach-Zehnderův interferometr z nelineárních děličů paprsku, můžeme pomocí výše uvedeného popisu učinit následující závěry.

Při modelu nelinearity (4.7) pro výstupní stav Mach-Zehnderova interferometru dostáváme (viz. (4.8)):

$$|\Psi\rangle = \frac{1}{2}(1 - e^{in\Phi})|10\rangle + \frac{i}{2}(1 + e^{in\Phi})|0n\rangle,$$

což pro počty detekovaných fotonů na jednotlivých detektorech (viz.(4.9), (4.10)):

$$\begin{aligned}
 S_0 &= \frac{1 - \cos n\Phi}{2}, \\
 S_1 &= n \frac{1 + \cos n\Phi}{2}.
 \end{aligned}$$

4.4 Kerrovský element

O materiálu, jehož index lomu závisí na intenzitě procházejícího paprsku jako:

$$n(I) = n + n_2 I, \tag{4.11}$$

říkáme, že vykazuje tzv. Kerrův efekt; n udává 'základní' index lomu, čili první člen v příslušném Taylorově rozvoji, tedy konstantní hodnotu pro dostatečně slabou intenzitu,

n_2 je konstanta udávající rychlost změny indexu lomu v závislosti na intenzitě.

Kvantově mechanicky tento efekt můžeme popsat Hamiltoniánem [11]:

$$\hat{H} = \chi \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b}, \quad (4.12)$$

kde a, b odpovídá dvěma modům šířícím se médiem a χ je interakční konstanta.

Odpovídající unitární transformace (pro krystal délky L):

$$\hat{K} = e^{i\chi L \hat{a}^\dagger \hat{a} \hat{b}^\dagger \hat{b}}.$$

Tuto nelinearitu lze využít ke konstrukci CNOT hradla, které lze sestavit pomocí dvou děličů paprsku a kerrovského elementu. Pokud při průchodu kerrovským médiem dojde k relativnímu fázovému posunu "spodního" paprsku o π . Snadno ověříme, že platí:

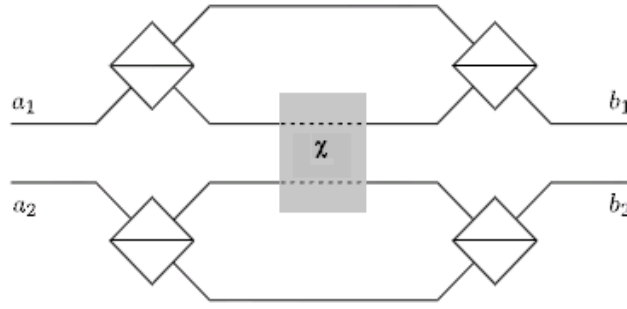
$$\hat{U}_{CNOT} = \hat{I} \otimes \hat{H} \cdot \hat{K} \cdot \hat{I} \otimes \hat{H},$$

kde definice \hat{K} přepsaná v termínech akce na bazické vektory vypadá následovně:

$$\begin{aligned} \hat{K}|00\rangle &= |00\rangle, \\ \hat{K}|01\rangle &= |01\rangle, \\ \hat{K}|10\rangle &= |10\rangle, \\ \hat{K}|11\rangle &= e^{i\chi L}|11\rangle \quad (\text{tj. pro } \chi L = \pi : \hat{K}|11\rangle = -|11\rangle). \end{aligned} \quad (4.13)$$

Skutečná realizace tak velkého fázového posunu je experimentálně problematická. Požadavky na nízkou intenzitu a zároveň vysoký fázový posun si odporují v tom smyslu, že nelineární optické elementy mají vysokou schopnost absorbovat procházející elektromagnetické záření, proto je pravděpodobnost průchodu jediného fotonu kerrovským médiem o dostatečné tloušťce velice nízká.

Kerrovské médium se také využívá při tzv. QND měřeních, která nenarušují měřený systém v tom smyslu, že je možné opakovaně měřit hodnotu pozorovatelné, která při tomto měření zůstává nezměněna (podrobněji viz. Příloha C).



Obrázek 4.4: Cross-Kerr element - schéma, převzato z [15]

4.5 Cross-Kerr element

Schématický model tohoto optického prvku je na Obr. (4.4). Budeme-li uvažovat dva vstupní módy a, b , pak interakční Hamiltonián má tvar 4.12, čemuž odpovídá následující transformace anihilačních operátorů (opět využíváme Baker-Hausdorffovy identity, viz. např. [15]):

$$\begin{aligned}\hat{a}(t) &= \exp(-iHt)\hat{a}_1 \exp(iHt) = \\ &= \hat{a} - i\theta[\hat{a}^\dagger\hat{a}, \hat{a}]\hat{b}^\dagger\hat{b} + \frac{(-i\theta)^2}{2!}[\hat{a}^\dagger\hat{a}, [\hat{a}^\dagger\hat{a}, \hat{a}]](\hat{b}^\dagger\hat{b})^2 + \dots = \\ &= \hat{a} \exp[i\theta\hat{b}^\dagger\hat{b}],\end{aligned}$$

kde $\theta = \chi t$, kde t je doba interakce. Celkem tedy

$$\hat{a}(t) \rightarrow \hat{a} \exp[i\chi\hat{b}^\dagger\hat{b}] \quad \text{a} \quad \hat{b}(t) \rightarrow \hat{b} \exp[i\chi\hat{a}^\dagger\hat{a}]. \quad (4.14)$$

Fázový posun modu a závisí na intenzitě pole v modu b . Pro $\chi = \pi$ a dva vstupující fotony v modech a, b tak dostáváme CZ hradlo (podmíněná transformace daná Pauliho σ_3 maticí), tj. v maticové reprezentaci

$$U_{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Opět tedy narážíme na význam zkoumání vícefotonového aspektu v souvislosti s ne-

lineárními optickými prvky: bude-li tedy n fotonů v modu a , dojde v modu b k fázovému posunu $\Phi = n\theta$.

Obecně dojde v fázovému posunu vertikálně polarizované části modu b , přičemž velikost tohoto fázového posunu závisí na počtu vertikálně polarizovaných fotonů v modu a . Jak už ale bylo řečeno v paragrafu 4.4, pro konstantu χ , která je úměrná příslušné složce susceptibility daného materiálu, v materiálech vykazujících Kerrův efekt platí $\chi \ll \pi$, což je problém, na který jsme narazili při rozboru praktické realizace CNOT hradla (podrobný popis realizace většího fázového posunu lze najít např. v [16]).

4.6 Nelineární Mach-Zehnderův interferometr

Výše popsané schéma Mach-Zehnderova interferometru je nyní modifikováno nelinearitou - Kerrovo médium v jednom z ramen. Odpovídající unitární transformace [17]:

$$\hat{U} = \hat{B}\hat{K}\hat{B},$$

kde

$$\hat{B} = \exp[i\pi(\hat{a}^\dagger\hat{b} + \hat{a}\hat{b}^\dagger)] \quad \text{a} \quad \hat{K} = \exp[-i\chi(\hat{a}^\dagger\hat{a})^2].$$

Bud' $|\Psi_{int}\rangle = |\alpha\rangle_a|\beta\rangle_b$ (koherentní stav). Potom

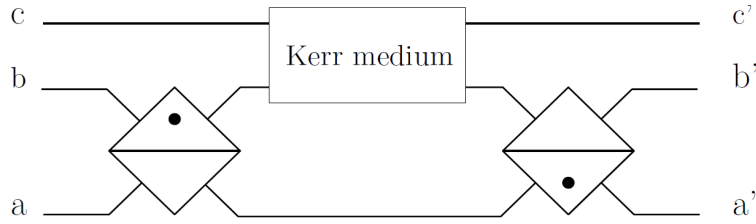
$$|\Psi\rangle_{out} = \hat{U}|\alpha\rangle_a|\beta\rangle_b.$$

Transformace daná děličem paprsku

$$\hat{B}|\alpha\rangle_a|\beta\rangle_b = \frac{1}{\sqrt{2}}(\alpha + i\beta)|\tilde{a}\rangle \frac{1}{\sqrt{2}}(\beta + i\alpha)|\tilde{b}\rangle.$$

Vidíme, že výstupní stav je také produktem koherentních stavů. Transformace koherentního stavu daná unitárním operátorem odpovídajícím Kerrovu elementu:

$$\hat{K}|\alpha\rangle = \exp\left(-\frac{|\alpha|^2}{2}\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} \exp(-i\chi n^2)|n\rangle. \quad (4.15)$$



Obrázek 4.5: Optická realizace Fredkinova hradla

Pro speciální volbu $\chi = \frac{\pi}{2}$ dostáváme [18]

$$\hat{U}|\alpha\rangle_a|\beta\rangle_b = \frac{1}{\sqrt{2}}(e^{-i\frac{\pi}{4}}|\alpha\rangle + e^{i\frac{\pi}{4}}|-\alpha\rangle).$$

Tato konkrétní volba má význam zejména v experimentálních aplikacích (optická analogie tzv. Schrödinger-cat stavů, viz. [19]). Navíc, jak je rozebráno ve [18], tvar řešení není obecně stejný pro všechny hodnoty, jichž může exponent ve (4.15) nabývat. Kombinace Kerrova média a dvou děličů paprsků celkem dává:

$$\hat{U}|\alpha\rangle_a|\beta\rangle_b = \frac{1}{\sqrt{2}}(e^{-i\frac{\pi}{4}}|i\beta\rangle_{a'}|i\beta\rangle_{b'} + e^{i\frac{\pi}{4}}|-\alpha\rangle_{a'}|\beta\rangle_{b'}).$$

Jedná se tedy o superpozici dvou koherentních stavů v různých módech, které ovšem nejsou ortogonální (viz. (B.2)). Pro $\beta \neq \pm\alpha$ se jedná o entanglovaný stav.

4.7 Optická realizace Fredkinova hradla

Hradlo popsané v paragrafu 3.2.4 lze realizovat pomocí dvou děličů paprsků a kerrovského elementu (viz. Obr. 4.5). Takovéto uspořádání představuje unitární transformaci $\hat{U} = \hat{B}^\dagger \hat{K} \hat{B}$, kde \hat{B} je vyvážený dělič paprsku, \hat{K} cross-kerr element (viz.(4.14) , Obr. 4.4):

$$K = \exp[i\xi \hat{b}^\dagger \hat{b} \hat{c}^\dagger \hat{c}],$$

kde značení modů odpovídá Obr. 4.5 a $\xi = \chi L$ je součin interakční konstanty χ a interakční vzdálenosti L .

Pro \hat{U} celkem dostáváme

$$\begin{aligned}\hat{U} &= \exp \left[i\xi \hat{c}^\dagger \hat{c} \left(\frac{\hat{b}^\dagger - \hat{a}^\dagger}{2} \right) \left(\frac{\hat{b} - \hat{a}}{2} \right) \right] = \\ &= e^{i\frac{\pi}{2}\hat{b}^\dagger\hat{b}} e^{\frac{\xi}{2}\hat{c}^\dagger\hat{c}(\hat{a}^\dagger\hat{b}-\hat{b}^\dagger\hat{a})} e^{-i\frac{\pi}{2}\hat{b}^\dagger\hat{b}} e^{i\frac{\pi}{2}\hat{a}^\dagger\hat{a}\hat{c}^\dagger\hat{c}} e^{i\frac{\xi}{2}\hat{b}^\dagger\hat{b}\hat{c}^\dagger\hat{c}}.\end{aligned}$$

První a třetí člen odpovídají konstatnímu fázovému posunu, poslední dva členy vzájemně modulaci módů b, c podle (4.14). Tyto členy ale nejsou pro účely Fredkinova hradla rozhodující a mohou být vykompenzovány vhodným experimentálním uspořádáním. Zbylé poslouží k následující definici Fredkinova operátoru:

$$\hat{F}(\xi) = \exp \left[\frac{\xi}{2} \hat{c}^\dagger \hat{c} (\hat{a}^\dagger \hat{b} - \hat{b}^\dagger \hat{a}) \right].$$

Rozebere takto posanou situaci pro $\xi = \pi$: není-li v modu c foton, platí tedy $a' = a$ a $b' = b$. Je-li na vstupu c foton, pak se mody právě zamění: $a' = b$ a $b' = a$. Jinými slovy dostáváme podníženou operaci s parametrem $\xi \hat{c}^\dagger \hat{c}$. Pro tuto speciální volbu parametru ξ tedy dostáváme CNOT hradlo.

4.8 Symetrický 2N-port

Symetrickým 2N-portem nazýváme zařízení, které vstupní foton v jakémkoli vstupním modu přetransformuje v jakýkoli výstupní se stejnou pravděpodobností $\frac{1}{N}$. Můžeme je chápat jako zobecnění (symetrického) děliče paprsku. Podle předcházející definice tento totiž není nic jiného než 4-port.

Vzhledem k požadavkům na symetrii vzhledem k záměně jak vstupních tak výstupních módů, volíme hamiltonián ve tvaru

$$\hat{H} = \lambda \sum_{s,r} \hat{a}_s^\dagger \hat{a}_r, \quad (4.16)$$

kde λ je inteakční konstanta a lze ji volit reálnou (viz.[20]) Vzhledem k symetrii lze Hamiltonián (4.16) zapsat pomocí úplně symetrických bosonových operátorů:

$$\hat{H} = \lambda N \hat{A}^\dagger \hat{A}, \quad \text{kde} \quad \hat{A}^\dagger = \frac{1}{\sqrt{N}} \sum_s \hat{a}_s^\dagger. \quad (4.17)$$

Jeho vlastními čísly potom jsou λN a 0 s algebraickou násobností 1 resp. $N-1$ (výpočet viz. [20]).

Mějme N modů v počátečním stavu $|\Psi_{in}\rangle$. Výstupní stav má potom tvar

$$|\Psi_{out}\rangle = \exp(-i\hat{H}t)|\Psi_n\rangle,$$

kde \hat{H} je hamiltonián (4.16). Pro vstupní stav s fotony v modech $\{i|i \in \mathcal{C}\}$, kde \mathcal{C} je podmnožina množiny vstupních portů, dostáváme výstupní stav ve tvaru

$$|\Psi_{out}\rangle = \exp(-i\hat{H}t) \prod_{s \in \mathcal{C}} \hat{a}_s^\dagger |0\rangle = \prod_{s \in \mathcal{C}} \hat{a}_s^\dagger(t) |0\rangle,$$

kde

$$\hat{a}_s^\dagger(t) = \exp(-i\hat{H}t)\hat{a}_s^\dagger \exp(i\hat{H}t) = \hat{a}_s^\dagger - \lambda t[\hat{A}^\dagger \hat{A}, \hat{a}_s^\dagger] + \frac{(-i\lambda t)^2}{2!}[\hat{A}^\dagger \hat{A}, [\hat{A}^\dagger \hat{A}, \hat{a}_s^\dagger]] + \dots, \quad (4.18)$$

kde navíc pro komutátory na pravé straně platí

$$\underbrace{[\hat{A}^\dagger \hat{A}, [\hat{A}^\dagger \hat{A}, \dots [\hat{A}^\dagger \hat{A}, \hat{a}_s^\dagger]] \dots]}_k = N^{\frac{2k-1}{2}} \hat{A}^\dagger. \quad (4.19)$$

Čili dostáváme

$$\begin{aligned} \begin{pmatrix} \hat{a}_1^\dagger(t) \\ \hat{a}_2^\dagger(t) \\ \vdots \\ \hat{a}_N^\dagger(t) \end{pmatrix} &= \mathbb{M} \begin{pmatrix} \hat{a}_1^\dagger(0) \\ \hat{a}_2^\dagger(0) \\ \vdots \\ \hat{a}_N^\dagger(0) \end{pmatrix} = \\ &= \exp[-i\hat{H}t] \begin{pmatrix} \hat{a}_1^\dagger(0) \\ \hat{a}_2^\dagger(0) \\ \vdots \\ \hat{a}_N^\dagger(0) \end{pmatrix} \exp[i\hat{H}t] \end{aligned}$$

kde \mathbb{M} je hledaná transformační matice.

Na základě znalosti vlastních čísel, vyjádření (4.17) a komutátorů (4.19) můžeme

rovnici (4.18) zapsat ve tvaru

$$\begin{aligned} \hat{a}_s^\dagger(t) &= \hat{a}_s^\dagger - \frac{1}{\sqrt{N}}\hat{A}^\dagger + \frac{1}{\sqrt{N}}\hat{A}^\dagger \exp(-i\lambda Nt) = \\ &= \hat{a}_s^\dagger \left(\frac{N-1 + \exp(-i\lambda Nt)}{N} \right) + \left(\frac{\exp(-i\lambda Nt) - 1}{N} \right) \sum_{j \neq s} \hat{a}_j^\dagger, \end{aligned} \quad (4.20)$$

z čehož již dostáváme transformační matici ve tvaru

$$\mathbb{M} = \begin{pmatrix} 1 + f(t) & f(t) & \dots & f(t) \\ f(t) & 1 + f(t) & \dots & f(t) \\ f(t) & f(t) & \dots & f(t) \\ f(t) & f(t) & \dots & 1 + f(t) \end{pmatrix}$$

pro $f(t) = \left(\frac{\exp(-i\lambda Nt) - 1}{N} \right)$.

Pravděpodobnost, že nalezneme foton v počátečním modu, spočteme pomocí (4.20):

$$\langle \hat{a}_i^\dagger \hat{a}_i \rangle = \left| \frac{N-1 + \exp(-i\lambda Nt)}{N} \right|^2 = 1 + 2 \frac{N-2}{N} [\cos(\lambda Nt) - 1].$$

Důležitým rysem symetrického děliče paprsků je již dříve zmíněný fakt, že bude-li v obou vstupních modech jeden foton, budou tyto nalezeny ve všech výstupních portech se stejnou pravděpodobností. Chceme-li najít analogii tohoto jevu pro symetrický 2N-port, budeme uvažovat vstupní stav ve tvaru

$$|\Psi_{in}\rangle = \prod_s \hat{a}_s^\dagger |0\rangle,$$

s tím, že budeme chtít zjistit, zda je možné získat výstupní stav ve tvaru

$$|\Psi_{out}\rangle = \frac{1}{\sqrt{N}} \sum_s \exp(i\varphi_s) \frac{(\hat{a}_s^\dagger)^N}{\sqrt{N!}} |0\rangle.$$

Z (4.20) zjistíme, že tento požadavek je ekvivalentní podmínce [20]:

$$\left(\frac{1}{N} \right)^{2N} [[N-1 + \exp(-i\lambda Nt)] \cdot [\exp(-i\lambda Nt) - 1]^{N-1}]^2 = \frac{1}{NN!}.$$

Tato podmínka je ale splněna pouze pro $N = 2$ a pro žádné vyšší N již rovnost ne-

nastává, jinými slovy diskutovaná situace s rovnoměrným rozdělením pravděpodobností výstupních modů je výlučně vlastností děliče paprsků a u symetrického portu s více vstupy ji již nelze realizovat.

4.9 Galtonova deska

Galtonova deska je zařízení, pomocí kterého můžeme simulovat klasickou náhodnou procházku: kolíky ekvidistantně rozmístěné na desce, mezi kterými necháváme propadávat kuličku jenom působením gravitačního pole. Konečné rozložení pozic kuliček pod deskou pak odpovídá binomickému rozdělení.

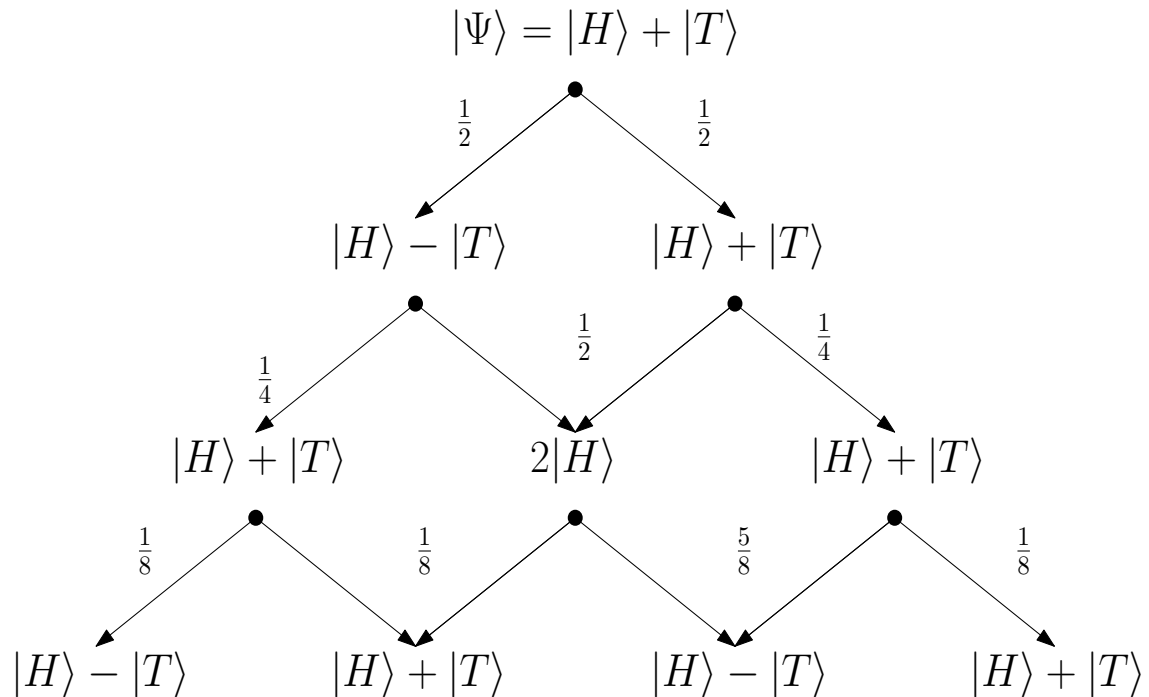
Nahradíme-li kolíky děliči paprsků můžeme simulovat kvantovou procházku (rozdíl mezi vlnovým a kvantovým podáním je v tom, že vlnová verze je klasická (ve smyslu optické vlny), zatímco kvantová interpretace užívá amplitudy vlnové funkce).

Standartní kvantová procházka (QW) koresponduje s diskrétním časovým vývojem jednodimenzionálního systému (chodec) propojeného s vývojem dvoudimenzionálního systému (mince). Označíme H_W Hilbertův prostor chodce, H_C Hilbertův prostor mince. Příslušné báze definujeme jako $\{|m\rangle, m \in Z\}$ a $\{|u\rangle, |d\rangle\}$. Stav celého systému patří do prostoru $H = H_C \otimes H_W$ a v čase t jej lze vyjádřit jako (viz. např. [21])

$$|\Psi(t)\rangle = \sum_m [u_{m,t}|u, m\rangle + d_{m,t}|d, m\rangle],$$

který lze zapsat jako $\hat{U} = \hat{U}_d \hat{U}_c$, tj. $|\Psi(t)\rangle = \hat{U}_d \hat{U}_c |\Psi(t-1)\rangle$. \hat{U}_c je zde operátor hodu mincí, \hat{U}_d operátor podmíněné změny polohy. Hlavním kvantitativním popisem procházky je pravděpodobnostní rozdělení pozice chodce podél mřížky, po které se může pohybovat.

Realizace kvantové procházky může vypadat následovně. Mějme optickou dutinu, do které vstupuje kvazimonochromatické světlo skrz polopropustné zrcadlo. Rozdělíme-li svazek děličem paprsků, má světlo dvě možnosti pohybu. Toto simuluje qubit a dělič paprsků odpovídá unitární transformaci, která realizuje akci operátoru házení mincí. Roli chodce (tedy operátoru \hat{U}_d) hraje frekvence světla, její změna o fixní hodnotu je zajištěna elektrooptickými modulátory - to je první krok procházky. Světlo je pak pomocí zrcadel odraženo zpátky do děliče a může být implementován nový krok atd.

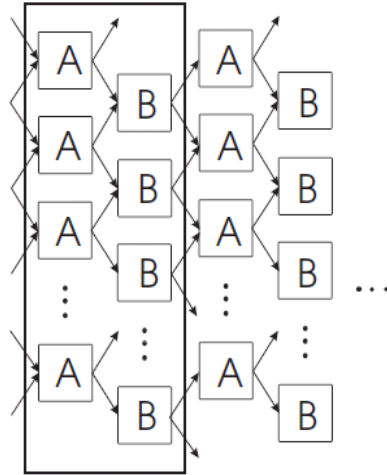


$$\bullet = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{array}{c} \text{H} \\ \swarrow \quad \searrow \\ \text{T} \end{array} \quad H = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad T = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Obrázek 4.6: Příklad: $|\Psi\rangle = |H\rangle + |T\rangle$ při průchodu optickou Galtonovou deskou (tvořenou symetrickými děliči paprsku). Číselné hodnoty uvedené při přechodech odpovídají pravděpodobnostem přechodu do následujícího stavu. Vidíme tedy, že již při použití šesti dochází k odchylce od klasického binomického rozdělení, kterým se řídí klasická Galtonova deska.

V této situaci QW zapříčiní frekvenční rozdělení výsledného pole tak, že intenzita příslušná každé frekvenci hraje roli pravděpodobnosti nalezení chodce v dané pozici. Jinými slovy, po m průchodech děličem, spektrum výsledného pole udává pravděpodobnostní rozdělení QW.

Podrobnější rozbor této myšlenky (podle [22]) je uvedena v Příloze F.1. Další možnou variantu experimentální realizace uvádíme v Příloze F.2.



Obrázek 4.7: Schématické znázornění sítě analogické s Isingovým modelem, kde A,B jsou transformace představované jednotlivými uzly, rámečkem je označený tzv. základní motiv, který se bude obecně M-krát opakovat, převzato z [24]

4.9.1 Modifikace modelu Galtonovy desky pro nelinearity

Stačí předpokládat, že světlo získává nějaké, na intezitě závislé, fáze při pohybu po jedné či druhé dráze umožněné v experimentu. Nicméně nyní nebudou tyto dráhy v lineárním prostředí (vakuum), ale v nelineárním médiu (kerrovský element, optická vlákna apod.). Nyní potřebujeme operátor navíc, který nám dovolí popsat získání na intezintě závislé fáze při průchodu Kerrovým médii. Unitární operátor zobecníme následujícím způsobem (viz. [23])

$$\hat{U}(t) = \hat{U}_d \hat{U}_c \hat{U}_{nl}(t-1).$$

$$\hat{U}_{nl}(t) = \sum_{c=u,d} \sum_m e^{iF_c(m,t)} |c, m\rangle \langle c, m|,$$

kde $F_c(m, t)$, ($c = u, d$) je libovolná funkce pravděpodobností (resp. intenzit v klasickém kontextu).

4.10 Kvantová síť analogická s Isingovým modelem

Dalším případem nekonečné sítě vzájemně propojených kvantových systémů je tzv. nearest-neighbour network. Síť složená z děličů paprsků, z nichž každý je propojen se

čtyřmi sousedními. Snadno si povšimneme jisté analogie s experimentem na binomické rozdělení a jak uvidíme zkoumané experimentální uspořádání pouze jinou interpretací konfigurace popsané v předchozí kapitole (Galtonova deska).

Naší úlohou nyní je najít matici, která dá jednoznačně do souvislosti operátory popisující stav fotonu na vstupu a výstupu každého děliče paprsku. Základní myšlenkou je rozdělit celou síť do opakujících se podstruktur (viz. Obr. 4.7). Budeme-li obecně uvažovat $2N$ ve vertikálním směru a $2M$ uzlů v horizontálním, transformační matice pro celý systém je pak jednoduše M -tou mocninou této dílčí transformační matice, která bude mít tvar (viz. např. [25]):

$$U = \begin{pmatrix} A & \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & \cdots \\ \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} & A & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \times \begin{pmatrix} B_{22} & 0 & 0 & \cdots \\ 0 & 0 & B & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

kde

$$A = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}, \quad B = \begin{pmatrix} \cos \Phi & \sin \Phi \\ -\sin \Phi & \cos \Phi \end{pmatrix},$$

přičemž uvažujeme periodické hraniční podmínky (toroidální topologie sítě).

Matice odpovídají transformaci, kterou realizuje celá síť je pak $W(M) = U^M$. Díky tomu, že matice U je unitární, můžeme matici W zapsat ve tvaru $W(M) = X^{-1}D^M X$, kde D je diagonální matice s vlastními čísly $\exp(\pm i\lambda_n)$ a X je unitární. Tato vlastní čísla dávají konkrétní informaci o typických rysech dané optické sítě (viz. [26]). Budeme-li uvažovat vyvážené děliče paprsku, tzn. $\theta = \Phi = \frac{\pi}{4}$, dostáváme pro vlastní hodnoty rovnici

$$\cos \lambda_n = \frac{1}{2} \left[1 + \cos \left(\frac{2\pi n}{N} \right) \right]. \quad (4.21)$$

Z rovnice (4.21) lze usuzovat na některé obecné rysy vlastních čísel pro libovolné N . Podle [26] platí, že všechny vlastní hodnoty $\exp(\pm i\lambda_n)$ jsou dvakrát degenerované (s výjimkou $\pm i$, je-li N liché). Uvedeme nyní explicitně množinu vlastních čísel pro síť s $N = 2$ a $N = 4$:

$$\begin{aligned} N = 2: & \quad \{1, 1, \pm i\} \quad \lambda_n \in \{0, \frac{\pi}{2}\}, \\ N = 4: & \quad \{1, 1, \pm i, \pm 1^{\frac{1}{3}}, \pm 1^{-\frac{1}{3}}\} \quad \lambda_n \in \{0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}\}. \end{aligned}$$

Bude-li se tedy základní motiv v síti opakovat M -krát, čili transformační matice pro celou síť bude mít tvar U^M , implikují výše uvedená vlastní čísla periodicitu transformací. Pro $N = 2$ se transformační matice stane jednotkovou po opakování 4 motivů, tj. $U^4 = \mathbf{1}$, pro $N = 4$ se totéž stane po 12 motivech, tj. $U^{12} = \mathbf{1}$. Naopak např. pro $N = 3$ se ukazuje, že jisté λ_n musí být nevyhnutelně iracionálním násobkem π . Pro dostatečně vysoká N a malá n platí pro exponenty λ_n následující aproximace

$$\lambda_n \approx \pm \sqrt{2} \frac{\pi n}{N}. \quad (4.22)$$

4.10.1 Rekurence a zakázané výstupy

Již víme, že ve speciálních případech nám znalost vlastních čísel poskytuje úplnou informaci o chování systému, nicméně v případě iracionálních exponentů vlastních čísel toto není pravidlem. Uvažujme funkci $W(M)$, která bude popisovat závislost transformační matice na M - počtu opakování základního motivu v Isingově síti. Uvažujme jednofotonový stav na i -tém vstupním portu, tj. $\hat{a}_i^\dagger|0\rangle$. Pro výstupní kreační operátor pak platí [26]

$$\hat{b}_k^\dagger(M) = \sum_{l=1}^{2N} [W(M)]_{kl} \hat{a}_l^\dagger.$$

Tedy pro foton v i -tém modu vstupující do sítě platí, že v j -tém výstupním modu bude nalezen s pravděpodobností $|W(M)_{ij}|^2$. Lze snadno dojít k závěru, že v klasickém případě bude pravděpodobnostní rozdělení výskytu fotonu ve výstupních modech binomické. V kvantovém případě je situace následující.

Pro $N = 2$ se matice $W(M)$ chová takto [26]

$$W(1) = U = \begin{pmatrix} 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \end{pmatrix}, \quad W(2) = U^2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$W(1) = U = \begin{pmatrix} 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & 1 \end{pmatrix}, \quad W(4) = U^4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Síť tedy vykazuje periodické chování s periodou 4 (po čtyřech opakováních elementárního motivu platí $|\Psi_{in}\rangle = U^4|\Psi_{in}\rangle$). Při pouze dvou opakováních motivu máme nicméně zaručeno, že foton se s pravděpodobností 1 objeví na jediném výstupu (ale v jiném než vstupním modu). Tato periodicitu ukazuje spojení mezi vlastnostmi vlastních čísel matice diskutovaných výše a fyzickým uspořádáním sítě. Můžeme si také všimnout, že matice $W(1)$ je maticí Hadamardovy transformace (použijeme-li značení (3.9) platí $W(1) = H \otimes H$).

Pro $N = 3$ je ve [26] ukázána existence zakázaného výstupu, konkrétně díky destruktivní interferenci má každý $i+3$ vstup nulovou pravděpodobnost, že by se nějaký foton objevil ve kterémkoli z výstupních modů.

Pro $N = 4$ je síť přesně periodická (jedná se o čtyři děliče paprsků v řadě) a platí $W(12) = 1$.

Pro obecné N lze vyslovit následující závěry. Je-li N liché, bude existovat právě jeden výstup s nulovou populací. Pokud jde o periodické vlastnosti, z odhadu (4.22) můžeme usuzovat, že uspořádání s $N = 2$, resp. $N = 4$ budou jediné případy vykazující přesnou periodocitu.

Fakt, že se nám podařilo popsat transformaci danou řadou děličů paprsků umístěných za sebou můžeme využít k nalezení maticové reprezentace transformace realizované Galtonovou deskou, diskutovanou výše. Tuto lze zapsat rekurentně tak, že známe-li transformaci U_N odpovídající prvním N řadám děličů paprsků, transformaci realizovanou po přidání $N+1$ -ní řady obrázíme jako produkt

$$U_{N+1} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ 0 & 0 & 1 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \dots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & & & & 0 \\ \vdots & & U_N & & \vdots \\ 0 & & & & 0 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

Máme-li několik izolovaných systémů popsaných pravděpodobnostními veličinami, mohou tyto, propojíme-li je, vykazovat kritické chování. Tím rozumíme prudkou změnu fundamentálních vlastností systému na základě změny vnějších parametrů. Toto chování

má v kvantových sítích svou analogii. Ke kritickým jevům ale nedochází na základě změny vnějších parametrů, nýbrž jsou zapříčiněny kvantovou povahou sítě.

Uvažujme síť, kde jednotlivé uzly vzájemně interagují pouze s nejbližším sousedem (Isingův model), jak už bylo popsáno výše. Abychom našli bod přechodu, je třeba zkoumat nespojitosti v globálních parametrech sítě. Vlastní hodnoty výše uvedeného unitární transformace pro Isingovu síť můžeme zapsat v integrálním tvaru jako [27]:

$$\gamma(\nu) = \frac{1}{\pi} \int_0^\pi d\nu' \log[2 \cosh 2\Phi \coth 2\Phi - 2(\cos \nu + \cos \nu')],$$

kde Φ je parametr určující reflexivitu, resp. refraktivitu použitých děličů.

4.10.2 Provázání v Isingově typu optické sítě

Vývoj pravděpodobnostního rozdělení jednočásticového stavu v pasivních optických sítích velice úzce souvisí s vývojem provázání v dané síti (existence kvantové korelace mezi výstupními mody), a to níže popsaným způsobem. Uvažujme obecný jednočásticový stav v rámci obecné sítě. Obecná pasivní optická síť je charakterizována jediným unitárním operátorem, který udává transformaci mezi vstupními a výstupními kreačními operátory:

$$\begin{pmatrix} \hat{b}_1^\dagger \\ \hat{b}_2^\dagger \\ \vdots \\ \hat{b}_n^\dagger \end{pmatrix} = \hat{U} \begin{pmatrix} \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \\ \vdots \\ \hat{a}_n^\dagger \end{pmatrix}.$$

Uvažujme částici ve stavu

$$|\Psi_{in}\rangle = \sum_{i=1}^N \alpha_i |1_i\rangle = \sum_{i=1}^N \alpha_i \hat{a}_i |0\rangle, \quad \sum_{i=1}^N |\alpha_i|^2 = 1,$$

kde $|1_i\rangle$ je vektor, který má, až i-tou, která je rovna jedné, všechny složky nulové, čili se jedná o i-tý mód s jednou excitací. Po aplikaci unitární transformace, pro výstupní stav dostáváme:

$$|\Psi_{out}\rangle = \hat{U} |\Psi_{in}\rangle = \sum_{i=1}^N \alpha_i \hat{U} \hat{a}_i^\dagger \hat{U}^\dagger \hat{U} |0\rangle = \sum_{i=1}^N \left(\sum_{k=1}^N U_{ki} \alpha_i \right) |1_k\rangle$$

Pro pravděpodobnost nalezení v n -tém výstupním modu dostáváme:

$$P(n) = |\langle 1_n | \Psi_{out} \rangle|^2 = \left| \sum_{i=1}^N U_{ni} \alpha_i \right|^2.$$

Budeme-li se zabývat dvou částicovým případem, musíme uvážit efekt provázání. Jak již bylo uvedeno v kapitole 2 pro popis entanglementu ve dvouhladinových systémech se užívá tzv. concurrence $C(\hat{\rho})$, kde $\hat{\rho}$ je operátor hustoty, definované vztahem 2.4.

Pomocí concurrence nyní můžeme určit provázání mezi i -tým a j -tým modem $|\Psi_{out}\rangle$. Najdeme redukovaný operátor hustoty [12]:

$$\rho_{ij} = Tr_{rest \neq i,j} (|\Psi_{out}\rangle \langle \Psi_{out}|)$$

s jedinou nenulovou vlastní hodnotou. Celkem dostáváme

$$C(\rho_{i,j}) = 2\sqrt{P(i)P(j)}. \quad (4.23)$$

Tento výsledek platí pro libovolný typ pasivní optické sítě a výstupního jednočásticového stavu. V podstatě jsme zjistili, že všechny mody (s nenulovou pravděpodobností $P(n)$) jsou vzájemně provázány a míra jejich provázání nezávisí na jejich relativní fázi. Tím jsme vyřešili otázku, jaká míra provázání se může vyskytnout v libovolně zvolené pasivní optické síti. Prakticky důležitější je nicméně řešení obrácené úlohy. Mějme zadanou určitou míru provázání, kterou chceme při průchodu sítí dosáhnout, hledejme odpovídající síť, která bude požadované provázání realizovat.

Víme, že všechny možné výstupní výstupní módy jsou navzájem provázané. Bez újmy na obecnosti předpokládejme, že foton se může s nenulovou pravděpodobností vyskytnout pouze v prvních $n \leq N$ módech, ke kterým máme určenu množinu concurrencí $C_{ij}, (C_{i,j} \neq 0), C_{ij} = C_{ji}$ pro $i \neq j$. Všechny stavy generované pasivní optickou sítí můžeme psát

$$|\Psi\rangle = \sum_{i=1}^N \lambda_i |1_i\rangle, \quad \sum_{i=1}^N |\lambda_i|^2 = 1 \quad (4.24)$$

a concurrenci zapsat ve tvaru

$$C_{ij} = 2|\lambda_i||\lambda_j|. \quad (4.25)$$

Pro pravděpodobnosti pak platí:

$$|\lambda_j|^2 = \frac{C_{ij}C_{kj}}{2C_{ik}}, \quad i \neq k \neq j. \quad (4.26)$$

Čili C_{ij} musí splňovat podmínku

$$\frac{C_{ij}C_{kj}}{C_{ik}} = \frac{C_{aj}C_{bj}}{C_{ab}},$$

pro všechna $i, j, k, a, b \in \hat{n}$. Zafixujeme-li nyní tři navzájem různé indexy i, j, k , platí pro $a, b \neq i$:

$$C_{ab} = \frac{C_{ia}C_{ib}}{C_{ij}C_{ik}}C_{jk}. \quad (4.27)$$

Speciálně pro $b = j$

$$C_{aj} = C_{ia} \frac{C_{ik}}{C_{jk}}.$$

Pomocí vztahů (4.25) a (4.26) přeformulujeme podle [24] vztah (4.24) jako

$$2 = \frac{C_{ij}C_{ik}}{C_{jk}} + \frac{C_{jk}}{C_{ij}C_{ik}} \sum_{a \neq i, a=1}^n C_{ia}^2. \quad (4.28)$$

Rovnici (4.28) nyní zapíšeme ve tvaru

$$2 = x + \frac{K}{x}, \quad \text{kde } x = \frac{C_{ij}C_{ik}}{C_{jk}} \text{ a } K = \sum_{a \neq i, a=1}^n C_{ia}^2. \quad (4.29)$$

Rovnice (4.29) má dvě řešení

$$x = 1 \pm \sqrt{1 - K},$$

kde

$$0 < K = \sum_{a \neq i, a=1}^n C_{ia}^2 \leq 1. \quad (4.30)$$

Po dosazení ze (4.29) dostáváme

$$C_{jk} = \frac{C_{ij}C_{ik}}{1 + \sqrt{1 - K}} \quad \text{nebo} \quad C_{jk} = \frac{C_{ij}C_{ik}}{1 - \sqrt{1 - K}}. \quad (4.31)$$

Obě tato řešení mají fyzikální význam, protože výsledné concurrence vyhovují podmínce $0 < C_{jk} < 1$.

Navíc pomocí (4.31) můžeme přepsat (4.27):

$$C_{ab} = \frac{C_{ia}C_{ib}}{1 \pm \sqrt{1-K}}. \quad (4.32)$$

Podle [24] vyjádříme koeficienty ze vztahu (4.24) v termínech concurrencí jako

$$|\lambda_j|^2 = \frac{C_{1j}^2}{2(1 \pm \sqrt{1-K})} \quad (i \neq j),$$

$$|\lambda_i|^2 = \frac{1}{2}(1 \pm \sqrt{1-K}).$$

Získané výsledky shrnuje následující věta:

Věta: Mějme množinu C_{ij} , $C_{ij} \neq 0$, která zadává vzájemné provázání pro všechny indexy i, j výstupních modu pasivní optické sítě. Tato může být popsána jediným čistým stavem (4.24) tehdy a jen tehdy, je-li pro libovolně, ale pevně zvolený index (mod) i splněna podmínka (4.30) a pro všechny indexy a, b ($a, b \neq i$) je současně splněno (4.32). Jsou-li obě podmínky splněny lze tedy provázání charakterizovat pomocí (4.24), kde $|\lambda_j|^2 = \frac{C_{ij}^2}{2(1 \pm \sqrt{1-K})}$, $j \neq i$ a $|\lambda_i|^2 = \frac{1}{2}(1 \pm \sqrt{1-K})$.

Provázání je generováno množinou concurrencí $\{C_{ij}\}$ mezi i -tým vybraným modem a zbylými možnými výstupními mody. Síť generující požadovaný stav ale není určena jednoznačně. Hledali jsme síť, kde na vstupu bude jediný foton v jistém vybraném módu - tím jsme vybrali jediný řádek matice unitární transformace, která danou síť bude charakterizovat, jedinou podmínkou na ostatní matickové elementy je tedy nenarušení výše zmíněné unitarity. Tuto nejednoznačnost lze (viz. [24]) využít ke zjednodušení schématu hledané sítě (viz. například Zeilingerova metoda pro síť složenou jen z děličů paprsků a fázových posunů, což je podrobněji okomentováno v Příloze D).

4.10.3 Optimalizace rozdělení provázání v pasivní síti s jednou excitací

Nejprve zavedeme následující označení: $C_{ij} = C(\rho_{ij}, i \neq j)$ a $C_{ii} = 0$. Dále definujeme funkci, která bude danou síť charakterizovat z hlediska celkového provázání systému:

$$\tau(\rho) = \sum_{ij} C_{ij}^2,$$

kde v sumě sčítáme přes všechny dvojice indexů. Optimalizací provázání budeme tedy dále chápat maximalizaci této funkce. Ze vztahu (4.23) po vysčítání přes j dostáváme

$$\sum_j C_{ij}^2 = 4P(i)[1 - P(i)],$$

protože

$$P_j = \frac{C_{ij}C_{kj}}{2C_{ik}}$$

$$\sum_{a=1, a \neq i, j} C_{ia}^2 = \frac{C_{ij}C_{ik}}{C_{jk}} \left(2 - \frac{C_{ij}C_{ik}}{C_{jk}}\right) \quad (\text{normalizační podmínka})$$

a tedy

$$\sum_{ij} C_{ij}^2 = 4(1 - P(i)^2).$$

Je ovšem třeba uvědomit si, že výše popsaným postupem, jsme všechny dvojice indexů zahrnuli do sumy dvakrát. Čili pro součet kvadrátů udané množiny concurrencí dostáváme

$$\sum_{ij} C_{ij}^2 = 2(1 - P(i)^2),$$

což je funkce jejíž maximum hledáme, ovšem s ohledem na podmínku $\sum_i P(i) = 1$. Řešením této úlohy na vázané extrémny je

$$\tau_{max}(N) = 2\left(1 - \frac{1}{N}\right) \quad \text{pro} \quad P(i) = \frac{1}{N}.$$

Všechny dvojice modů jsou tedy provázány stejně a pro concurrenci platí

$$C = C_{ij} = \frac{2}{N}.$$

4.10.4 Rozdělení provázání v pasivní síti se dvěma excitacemi

Budeme uvažovat limitní případ sítě - síť dostatečně velkou na to, aby pravděpodobnost detekovat dva fotony na tomtéž výstupu byla prakticky nulová. Pro popisované stavy to

znamená tvar

$$|0_i\rangle|1_j\rangle \dots |1_k\rangle \dots |0_l\rangle \quad \text{pro } j \neq k.$$

Dvoučásticový vstupní stav

$$\begin{aligned} |\Psi_{in}\rangle &= \sum_{ij} \alpha_{ij} a_i^\dagger a_j^\dagger |0\rangle + \frac{1}{\sqrt{2}} \sum_i^N \alpha_i \hat{a}_i^{\dagger 2} |0\rangle = \\ &= \sum_{ij} \alpha_{ij} |1_i 1_j\rangle + \sum_i \alpha_i |2_i\rangle. \end{aligned} \quad (4.33)$$

Tříčásticový bude vypadat:

$$|\Psi_{in}\rangle = \sum_{i_1, i_2, i_3} \alpha_{i_1 i_2 i_3} \hat{a}_{i_1}^\dagger \hat{a}_{i_2}^\dagger a_{i_3}^\dagger |0\rangle + \frac{1}{\sqrt{2}} \sum_{i_1, i_2} \alpha_{i_1 i_2} \hat{a}_{i_1}^{\dagger 2} \hat{a}_{i_2}^\dagger |0\rangle + \frac{1}{\sqrt{6}} \sum_{i_1} \alpha_{i_1} \hat{a}_{i_1}^{\dagger 3} |0\rangle.$$

Zobecnění pro více fotonů, které by se nabízelo, ale rozhodně nebude přímočaré, protože už u čtyř fotonů formule budovaná rekurentně na základě předchozích dvou vztahů neobsáhne například možnost $\hat{a}_{i_1}^{\dagger 2} \hat{a}_{i_2}^{\dagger 2}$ atd.

Nicméně pro vstupní stav tvaru (4.33) bude výstupní stav vypadat

$$|\Psi_{out}\rangle = \sum_{k,l=1}^N \left[\sum_{(ij)} U_{ki} U_{lj} \alpha_{ij} + \sum_{i=1}^N \frac{1}{\sqrt{2}} U_{ki} U_{li} \alpha_i \right] \hat{b}_k^\dagger \hat{b}_l^\dagger |0\rangle, \quad (4.34)$$

kde v sumě s indexem (ij) sčítáme přes všech $\binom{n}{2}$ dvojic indexů. Označíme

$$\begin{aligned} \beta_{kl} &= \sum_{(ij)} 2U_{ki} U_{lj} \alpha_{ij} + \sum_{i=1}^N \sqrt{2} U_{ki} U_{li} \alpha_i \\ \beta_k &= \sum_{(ij)} \sqrt{2} U_{ki} U_{kj} \alpha_{ij} + \sum_{i=1}^N U_{ki} U_{ki} \alpha_i \end{aligned}$$

díky čemuž se vztah 4.34 redukuje na

$$|\Psi_{out}\rangle = \sum_{kl} \beta_{kl} |1_k 1_l\rangle + \sum_{k=1}^N \beta_k |2_k\rangle,$$

který je díky limitnímu předpokladu tohoto odstavce po provedení normalizace roven

$$|\Psi_{out}\rangle = \frac{1}{K} \sum_{kl} \beta_{kl} |1_k 1_l\rangle, \quad \text{kde} \quad K^2 = \sum_{kl} |\beta_{kl}|^2.$$

Další postup je analogický výše uvedenému pro jednočásticový stav. Pro dva pevně zvolené mody a, b opět vypočteme redukovanou matici hustoty (její explicitní tvar lze nalézt v [24]) a jí asociovanou matici (2.3), pro niž najdeme vlastní hodnoty a podle (2.4) zjistíme, že pro concurrenci mezi těmito zvolenými mody platí

$$C_{ab} = 2 \max \left[\left| \sum_{k \neq a, b} \beta_{ak} \beta_{ak}^* \right| - |\beta_{ab}| \sqrt{\sum_{(k,l) \neq a, b} |\beta_{kl}|^2}, 0 \right].$$

Kapitola 5

Řešení optické sítě s náhodnou pozicí nelineárního elementu

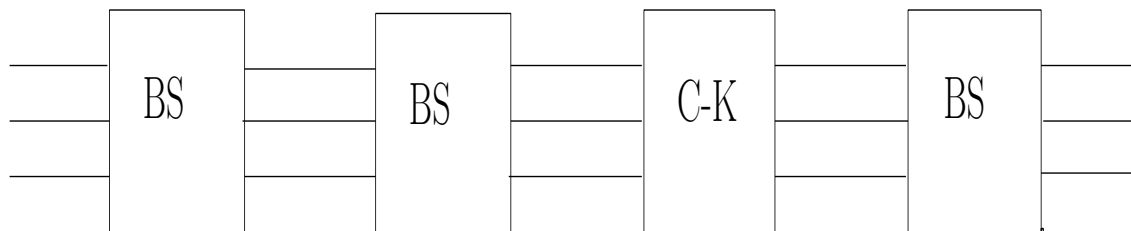
V předchozích kapitolách jsme probrali funkci logických hradel a jejich fyzikální realizace, zejména pokud šlo o využití nelineárních prvků, jejichž vlastnosti začnou být zajímavé ve vícefotonových případech. Dospíváme tak k následujícímu zobecnění: začlenění nelineárního prvku do rozsáhlejší sítě s více excitacemi s tím, že jeho poloha bude náhodná (Obr. 5.1).

Nechť je studovaná síť tvořena N děliči paprsku s tím, že na k -tém místě se nachází cross-kerr element. Budeme uvažovat n vstupních a n výstupních módů. Hamiltonián bude tedy mít tvar

$$\hat{H} = \sum_{i=1}^n \hat{a}_i^\dagger \hat{a}_{i+1} + \sum_{i=1}^n \chi_i (\hat{b}_i^\dagger \hat{b}_i)^2.$$

Začneme s jednoduchým případem stavu se dvěma možnými mody, které označíme a, b .

Podle (4.12) a (4.14) zjistíme, že pro jednofotonový stav se nelinearita neprojeví



Obrázek 5.1: Schéma optické sítě s náhodnou pozicí nelineárního elementu (C-K) mezi děliči paprsků (BS) v řadě.

(explicitně viz. (4.13)). Tím můžeme síť pokládat za vyřešenu pro libovolný vstupní jednofotonový stav. Vzhledem k periodicitě řady děličů paprsků (která bude objasněna v následujícím paragrafu, viz. (5.4) a faktu, že pro jednofotonový stav se unitární operátor příslušející akci kerrovského elementu bude chovat prostě jako identita, stačí spočítat $N \bmod 8$ a vybrat z (5.4) příslušný stav.

Nicméně už pro dva fotony v síti, bude situace komplikovanější. Víme, že akce operátoru (4.12) na dvoufotonový stav je

$$\hat{K}|1_a 1_b\rangle = e^{i\chi}|1_a 1_b\rangle, \quad (5.1)$$

což nás, uvážíme-li definici koherentního stavu B.1, platnost identity (4.6) (kterou podle [14] splňují všechny funkce rozvinutelné do řady) a Baker-Hausdorffovu identitu (4.5), vede k myšlence přímočarého řešení sítě pro dvojici koherentních stavů, čímž bychom navíc mohli rozšířit jejich využití uvedené v paragrafu 4.6.

5.1 Koherentní stavy

Označíme-li \hat{B} unitární transformaci realizovanou děličem paprsků, \hat{K} unitární transformaci realizovanou kerrovským elementem, snadno zjistíme, že pro dvojici koherentních stavů platí

$$\hat{B}^8|\alpha\rangle|\beta\rangle = |\alpha\rangle|\beta\rangle \quad (5.2)$$

a pro akci kerrovského elementu s hamiltoniánem $\hat{H}_K = \chi(\hat{a}^\dagger\hat{a})^2$ platí (viz. např. [17])

$$\hat{K}|\alpha\rangle|\beta\rangle = \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|\alpha\rangle|\beta\rangle + e^{i\frac{\pi}{4}}|-\alpha\rangle|\beta\rangle]. \quad (5.3)$$

Vzhledem k faktu, že výsledkem takovéto transformace jsou koherentní stavy a uvážíme-li navíc periodicitu podle (5.4), můžeme očekávat analogické chování i u stavu (5.3).

Explicitní vyjádření je následující. Pro dělič paprsku:

$$\begin{aligned}
 \hat{B}|\alpha\rangle|\beta\rangle &= \left|\frac{1}{\sqrt{2}}(\alpha + i\beta)\right|\left|\frac{1}{\sqrt{2}}(\beta + i\alpha)\right\rangle, \\
 \hat{B}^2|\alpha\rangle|\beta\rangle &= |i\alpha\rangle|i\beta\rangle, \\
 \hat{B}^3|\alpha\rangle|\beta\rangle &= \left|\frac{1}{\sqrt{2}}(-\alpha + i\beta)\right|\left|\frac{1}{\sqrt{2}}(-\beta + i\alpha)\right\rangle, \\
 \hat{B}^4|\alpha\rangle|\beta\rangle &= |-\alpha\rangle|-\beta\rangle, \\
 \hat{B}^5|\alpha\rangle|\beta\rangle &= \left|\frac{1}{\sqrt{2}}(-\alpha - i\beta)\right|\left|\frac{1}{\sqrt{2}}(-\beta - i\alpha)\right\rangle, \\
 \hat{B}^6|\alpha\rangle|\beta\rangle &= |-i\alpha\rangle|-i\beta\rangle, \\
 \hat{B}^7|\alpha\rangle|\beta\rangle &= \left|\frac{1}{\sqrt{2}}(\alpha - i\beta)\right|\left|\frac{1}{\sqrt{2}}(\beta - i\alpha)\right\rangle, \\
 \hat{B}^8|\alpha\rangle|\beta\rangle &= |\alpha\rangle|\beta\rangle
 \end{aligned} \tag{5.4}$$

a pro kerrovský element:

$$\begin{aligned}
 \hat{B}\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|\alpha + i\beta\rangle|\beta + i\alpha\rangle + e^{i\frac{\pi}{4}}|-\alpha + i\beta\rangle|\beta - i\alpha\rangle], \\
 \hat{B}^2\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|i\beta\rangle|i\alpha\rangle + e^{i\frac{\pi}{4}}|i\beta\rangle|-\alpha\rangle], \\
 \hat{B}^3\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|-\alpha + i\beta\rangle|i\alpha - \beta\rangle + e^{i\frac{\pi}{4}}|i\beta + \alpha\rangle|-\alpha - \beta\rangle], \\
 \hat{B}^4\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|-\alpha\rangle|-\beta\rangle + e^{i\frac{\pi}{4}}|\alpha\rangle|-\beta\rangle], \\
 \hat{B}^5\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|-\alpha - i\beta\rangle|-\beta - i\alpha\rangle + e^{i\frac{\pi}{4}}|\alpha - i\beta\rangle|\beta - i\alpha\rangle], \\
 \hat{B}^6\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|-\beta\rangle|-\alpha\rangle + e^{i\frac{\pi}{4}}|-\beta\rangle|i\alpha\rangle], \\
 \hat{B}^7\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|\alpha - i\beta\rangle|-\alpha + \beta\rangle + e^{i\frac{\pi}{4}}|-\beta - \alpha\rangle|i\alpha + \beta\rangle], \\
 \hat{B}^8\hat{K}|\alpha\rangle|\beta\rangle &= \frac{1}{\sqrt{2}}[e^{-i\frac{\pi}{4}}|\alpha\rangle|\beta\rangle + e^{i\frac{\pi}{4}}|-\alpha\rangle|\beta\rangle] = \hat{K}|\alpha\rangle|\beta\rangle.
 \end{aligned} \tag{5.5}$$

Využitím této periodicity můžeme řešení sítě rozdělit na dva případy: je-li kerrovský element umístěn na prvním místě vypočteme pouze $N \bmod 8$ děličů paprsků, které se nacházejí za ním a výsledek určíme podle (5.5), pokud kerrovskému elementu m děličů paprsků navíc předcházelo, opět s využitím periodicity transformace už jen upravíme výsledný vztah podle (5.4) (odpovídající rovnici opět vybereme jako $m \bmod 8$).

Z toho už je zřejmé, že výsledná matice hustoty pro daný systém bude součet 64

možných matic hustoty odpovídající jednotlivým konfiguracím. V podstatě jsme ze sumy $\hat{\rho} = \sum_{i=1}^n p_i |\Psi_i\rangle\langle\Psi_i|$ vybrali jenom všechny možné navzájem různé výstupní funkce. Aby ale byla současně splněna podmínka na normalizaci pravděpodobnosti (součet koeficientů p_i musí být roven jedné), je třeba započítat degenerace jednotlivých variant kombinací počtů děličů paprsků, které předchází resp. následují kerrovský element. Budou tedy samozřejmě záviset na pravděpodobnostním rozložení výskytu kerrovského elementu v síti. Jako nejjednodušší příklad můžeme uvažovat, že pravděpodobnost bude pro všechny pozice v síti tatáž: $\frac{1}{N}$. Všechny koeficienty při sčítání přes všechny navzájem různé matice hustoty pak musíme, kvůli zachování normalizace, vynásobit koeficientem $[\frac{N}{16}]$.

Tím jsme zodpověděli otázku chování dvojice koherentní stavů v síti 5.1. Navázali jsme tak na diskuzi uvedenou v sekci 4.6 a článku [17], čímž jsme pro tento případ vyřešili možnost zařazení nelineárního Mach-Zehnderova interferometru do složitější sítě.

Kapitola 6

Závěr

V této práci byl čtenář seznámen s optickými kvantovými sítěmi jak z teoretického hlediska skládání jednotlivých unitárních transformací do výsledné logické operace, tak z hlediska možných fyzikálních realizací s důrazem na vícefotonový aspekt. Podrobně byly rozebrány zejména možnosti použití kerrovského média, Galtonova deska a síť analogická s Isingovým modelem.

Bylo uvedeno řešení optické sítě s náhodnou pozicí nelineárního elementu pro dvojici koherentních stavů a také nejobecnější možná formulace úlohy na náhodný výskyt nelinearity v síti, což je bod, ve kterém lze na tuto práci navázat, klíčové je rozšíření řešení na vícefotonové stavy.

Příloha A

The no-cloning theorem

Není možné vytvořit přesnou kopii náhodného kvantového stavu: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Při důkazu budeme postupovat sporem podle [15]. Představme si, že vytvořit přesnou kopii je možné a lze to uskutečnit prostřednictvím unitární operace \hat{U} . Tato bude působit na stav $|\Psi\rangle_1$ na prvním qubitu a současně na druhém na počáteční stav $|i\rangle$. Výstup takové procedury musí mít tvar: $|\Psi\rangle_1|\Psi\rangle_2$. To znamená, že pro stavy $|0\rangle$ a $|1\rangle$ Musí platit

$$\hat{U}|0\rangle_1|i\rangle_2 = |0\rangle_1|0\rangle_2 \quad \hat{U}|1\rangle_1|i\rangle_2 = |1\rangle_1|1\rangle_2.$$

Z linearity pak dostáváme

$$\begin{aligned} \hat{U}|\Psi\rangle_1|i\rangle_2 &= \alpha\hat{U}|0\rangle_1|i\rangle_2 + \beta\hat{U}|1\rangle_1|i\rangle_2 = \\ &= \alpha|0\rangle_1|0\rangle_2 + \beta|1\rangle_1|1\rangle_2 \neq |\Psi\rangle_1|\Psi\rangle_2. \end{aligned}$$

Skutečnost, že nemůžeme vytvořit přesnou kopii neznámého kvantového stavu, zaručuje neprolomitelnost procesů používaných v kvantové kryptografii (jako jednoduchý příklad může posloužit protokol BB84, popsany např. v [12]).

Na závěr je třeba poznamenat, že toto zdůvodnění plně postačující pro naše účely, není obecným důkazem (předpokládáme čistý stav, nikoli smíšený), více např. v [28].

Příloha B

Základní vlastnosti koherentních stavů

Koherentní stav zvoleného modu je definován jako výsledek translace stavu $|0\rangle$ ve fázovém prostoru (viz. Obr. B.1). Tato translace je popsána unitárním operátorem

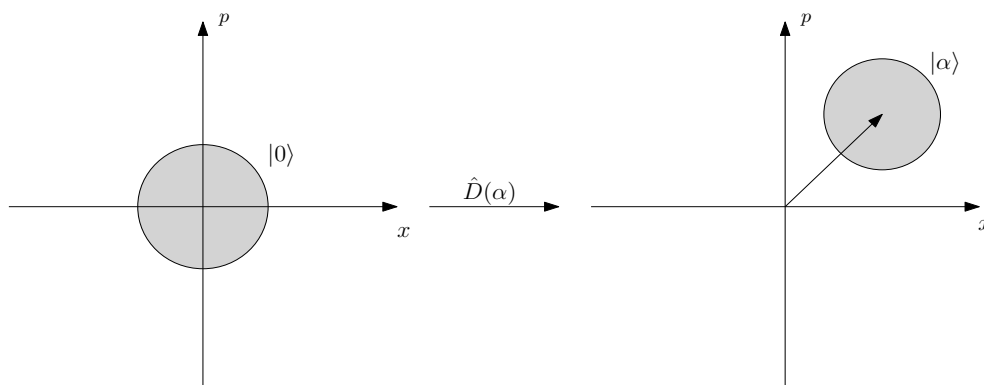
$$\hat{D}(\alpha) = \exp[\alpha\hat{a}^\dagger - \alpha^*\hat{a}] = \exp\left(-\frac{|\alpha|^2}{2}\right) \exp(\alpha\hat{a}^\dagger) \exp(-\alpha^*\hat{a}), \quad (\text{B.1})$$

kde $\alpha \in \mathbb{C}$. Označení: $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$. Pro časový vývoj (Obr. B.2) koherentního stavu platí

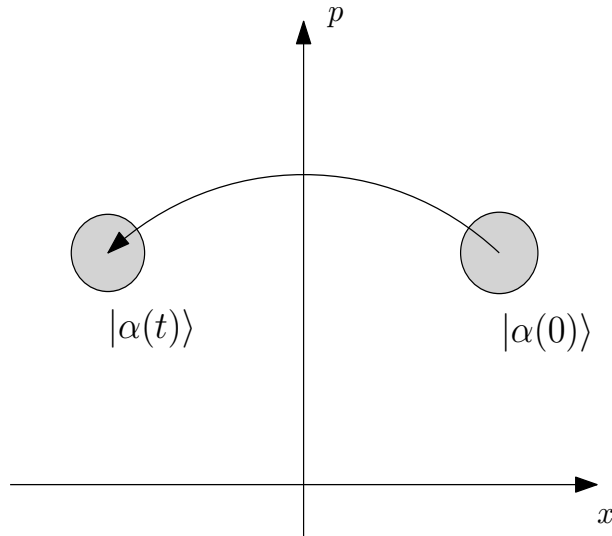
$$|\Psi(t)\rangle = e^{-i\omega t/2} |\alpha e^{-i\omega t}\rangle.$$

Koherentní stav ve Fockově bázi (viz. [1]):

$$|\alpha\rangle = \sum_n C_n(\alpha) |n\rangle \quad \text{pro} \quad C_n(\alpha) = \exp\left(-\frac{|\alpha|^2}{2}\right) \frac{\alpha^n}{\sqrt{n!}}.$$



Obrázek B.1: Translace vakua ve fázovém prostoru



Obrázek B.2: Časový vývoj koherentního stavu

Pro skalární součin dvou koherentních stavů platí:

$$\langle \alpha | \beta \rangle = \exp[-|\alpha|^2/2 - |\beta|^2/2 + \alpha^* \beta],$$

z čehož dostáváme

$$|\langle \alpha | \beta \rangle|^2 = \exp[-|\alpha - \beta|^2], \quad (\text{B.2})$$

jinými slovy koherentní stavy nejsou navzájem ortogonální. Podrobnější diskuzi a odvození všech výše uvedených vztahů lze najít například v [29].

Příloha C

QND měření

Obecné schéma QND měření (název z 'Quantum nondemolition measurements') je následující: pozorovatelná \hat{A}_S systému S je měřena pomocí detekce změny pozorovatelné \hat{A}_P příslušející systému P , který je propojen se systémem P po čas měření T . Díky tomu lze získat sadu přesných měření \hat{A}_S a to tak, že výsledek každého měření je úplně předpověditelný z výsledku měření předchozího. Hamiltonián $S - P$ systému zapíšeme jako

$$\hat{H} = \hat{H}_S + \hat{H}_P + \hat{H}_1, \quad (\text{C.1})$$

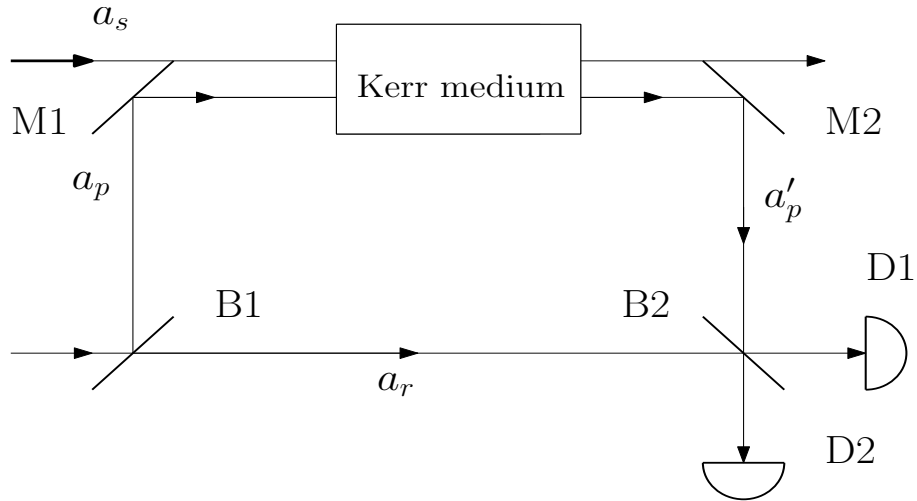
kde \hat{H}_S je hamiltonián systému S , \hat{H}_P je hamiltonián systému P a \hat{H}_1 je interakční hamiltonián. Pro časový vývoj pozorovatelných A_S, A_P potom platí:

$$\begin{aligned} i\hbar\dot{\hat{A}}_S &= [\hat{A}_S, \hat{H}_S + \hat{H}_1], \\ i\hbar\dot{\hat{A}}_P &= [\hat{A}_P, \hat{H}_P + \hat{H}_1]. \end{aligned}$$

Pokud chceme aby \hat{A}_S byla QND pozorovatelná, musí pozorovatelná \hat{A}_P a interakční hamiltonián \hat{H}_1 splňovat následující podmínky:

- Aby bylo možné \hat{A}_S měřit musí být interakční hamiltonián funkcí \hat{A}_S čili

$$\frac{\partial H_1}{\partial A_S} \neq 0 \quad (\text{C.2})$$



Obrázek C.1: Schéma QND měření prováděného prostřednictvím Kerrovského elementu

- \hat{A}_P používáme k měření \hat{A}_S , nesmí tedy být integrálem pohybu:

$$[\hat{A}_P, \hat{H}_1] \neq 0 \quad (C.3)$$

- Naopak hodnota A_S nesmí být ovlivněna vazbou danou H_1 :

$$[\hat{A}_S, \hat{H}_1] = 0 \quad (C.4)$$

- navíc:

$$\frac{\partial \hat{H}_S}{\partial \hat{A}_S^\dagger} = 0 \quad (C.5)$$

C.1 QND pomocí Kerrovského elementu

Průběh indexu lomu v nelineárních materiálech je dán rovnicí (4.11). Schéma experimentálního uspořádání je na Obr. C.1. Díky změně indexu lomu v závislosti na intenzitě vzniká fázový posun mezi tzv. řádným a mimořádným paprskem. Fáze mimořádného paprsku je modulována intenzitou řádného. Hamiltonián jejich interakce v kerrovském

médiu je dán (C.1), kde

$$\begin{aligned}\hat{H}_S &= \hbar\nu_S(\hat{a}_S^\dagger\hat{a}_S + \frac{1}{2}), \\ \hat{H}_P &= \hbar\nu_S(\hat{a}_S^\dagger\hat{a}_S + \frac{1}{2}), \\ \hat{H}_1 &= \hbar\chi\hat{a}_S^\dagger\hat{a}_S\hat{a}_P^\dagger\hat{a}_P.\end{aligned}$$

Pozorovatelná, kterou chceme změřit bude operátor počtu kvant

$$\hat{A}_S = \hat{a}_S^\dagger\hat{a}_S. \quad (\text{C.6})$$

Pozorovatelná měřená bude vhodný fázový operátor $\hat{\Phi}_P$. Tento je vhodné definovat například [30]

$$\begin{aligned}\hat{a}_p &= \sqrt{\hat{a}_P^\dagger\hat{a}_P + 1} \exp[i\hat{\Phi}_P], \\ \hat{a}_p^\dagger &= \exp[-i\hat{\Phi}_P] \sqrt{\hat{a}_P^\dagger\hat{a}_P + 1}.\end{aligned}$$

Operátory $\exp[\pm i\hat{\Phi}_p]$ nejsou hermitovské, nicméně lze z nich hermitovské operátory vytvořit vhodnou lineární kombinací:

$$\cos \Phi_P = \frac{1}{2}[\exp[i\hat{\Phi}_p] + \exp[-i\hat{\Phi}_p]], \quad (\text{C.7})$$

$$\sin \Phi_P = \frac{1}{2i}[\exp[i\hat{\Phi}_p] - \exp[-i\hat{\Phi}_p]]. \quad (\text{C.8})$$

Dále zvolíme:

$$\hat{A}_P = \sin \hat{\Phi}_P \quad (\text{C.9})$$

Z (C.7), (C.8) a (C.9) dostáváme

$$\hat{A}_P = \frac{1}{2i} \left(\frac{1}{\sqrt{\hat{a}_P^\dagger\hat{a}_P + 1}} \hat{a}_P - \frac{1}{\sqrt{\hat{a}_P^\dagger\hat{a}_P + 1}} \right). \quad (\text{C.10})$$

Nyní snadno ověříme, že podmínky (C.2) - (C.5) jsou pro \hat{A}_S (viz. (C.6)) a \hat{A}_P (viz. (C.10)) splněny.

Pohybová rovnice pro \hat{a}_P (viz. [3]):

$$\dot{\hat{a}}_P = -i\chi\hat{A}_S\hat{a}_P$$

a po záměně proměnných $t = -\frac{z}{v}$, kde z je souřadnice v kladném směru osy z , v je rychlost šíření vlny v daném prostředí:

$$\frac{d}{dz}\hat{a}_P(z) = \frac{i\chi}{v}\hat{A}_S\hat{a}_P(z), \quad z \in [0, L],$$

tzn.

$$\hat{a}_P(L) = \exp\left(\frac{i\chi}{v}\hat{A}_SL\right)\hat{a}_P(0).$$

Operátor $\frac{\chi\hat{A}_SL}{v}$ v rovnici tedy odpovídá fázovému posunu v \hat{a}_P .

Podrobnější rozbor této problematiky lze najít např. v [31].

Příloha D

Zeilingerova metoda

Víme, že akci každého z výše popsaných prvků optické sítě lze reprezentovat jistým unitárním operátorem. Otázkou zůstává, zda pro každý unitární operátor existuje experimentální realizace. Zeilingerova metoda je obecný algoritmus, který umožňuje tuto realizaci pro libovolné $N \times N$ unitární matice.

Mějme nyní vstupní stav s mody (k_1, k_2) . Podle [32] zvolíme výstupní stav s mody (k'_1, k'_2) ve tvaru:

$$\begin{pmatrix} k'_1 \\ k'_2 \end{pmatrix} = \begin{pmatrix} e^{i\Phi} \sin \omega & e^{i\Phi} \cos \omega \\ \cos \omega & -\sin \omega \end{pmatrix} \begin{pmatrix} k_1 \\ k_2 \end{pmatrix}, \quad (\text{D.1})$$

kde ω je parametr, který popisuje jak reflexivitu ($\sqrt{R} = \sin \omega$), tak transmisivitu ($\sqrt{T} = \cos \omega$) děliče, parametr Φ udává fázový posun. Tento stav tedy vznikl průchodem děličem paprsku s možností fázového posunu na jednom z výstupů (realizací děliči paprsku s proměnnou reflexivitou je Mach-Zehnderův interferometr se symetrickými děliči, popsáný v sekci 4.3).

Nyní budeme chtít ukázat, že pro každou $U(N)$ matici existuje ekvivalentní uspořádání využívající pouze matice $U(2)$ (tedy transformaci na N -rozměrném Hilbertově prostoru rozložíme na dílčí kroky realizované na jeho dvourozměrných podprostorech).

Vzhledem k faktu, že postupná aplikace optických prvků odpovídá produktu příslušných unitárních matic, úlohou je vlastně faktorizovat původní matici na produkt blokových matic takových, že realizovaná unitární transformace bude zahrnovat právě jeden optický element - v našem případě jediný dělič paprsku s příslušným fázovým posunem.

Definujeme matici T_{pq} , N -rozměrnou identitu s tím, že elementy $I_{pp}, I_{pq}, I_{qp}, I_{qq}$ jsou

nahrazeny prvky matice (D.1). Právě ta odpovídá unitární transformaci na dvourozměrném podprostoru a zbytek H-prostoru ponechává nezměněn. Metodou podobnou Gaussově eliminační vynulujeme všechny mimodiagonální elementy matice $U(N)$. Původní unitární matici budeme postupně zprava násobit maticemi představující unitární transformace na dvoudimenzionálním podprostoru $T_{N,q}, q = N - 1, \dots, 1$. Tím se vynulují všechny mimodiagonální elementy na posledním řádku. Dostáváme:

$$U(N) \cdot T_{N,N-1} \cdot T_{N,N-2}, \dots, T_{N,1} = \begin{pmatrix} U(N-1) & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

Na tuto posloupnost transformací lze pohlížet jako na rotaci N-rozměrného vektoru v N-dimenzionálním vektorovém prostoru. Jinými slovy, experimentální realizace rotace v N-rozměrném prostoru je dána následujícím operátorem:

$$R(N) = T_{N,N-1} \cdot T_{N,N-2}, \dots, T_{N,1}.$$

Tím ale můžeme inovovat interpretaci výše nastíněného algoritmu. Zapišeme-li původní unitární matici jako vektor tvořený ortonormálními řádkovými vektory v N-rozměrném Hilbertově prostoru:

$$U(N) = \begin{pmatrix} \langle 1| \\ \langle 2| \\ \vdots \\ \langle N| \end{pmatrix}$$

V tomto prostoru bude operace reprezentovaná maticí $R(N)$ otáčet zvolený bázev vektor následovně:

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}^T \cdot R(N)^{-1} = \begin{pmatrix} e^{-i\Phi_1} \cos \omega_1 \\ -e^{-i\Phi_2} \cos \omega_2 \sin \omega_1 \\ \vdots \\ \pm \sin \omega_{N-1} \sin \omega_{N-2} \dots \sin \omega_1 \end{pmatrix}^T,$$

kde parametry ω_i, Φ_i jsou souřadnice na N-rozměrné sféře. Tyto již mohou být

implementovány pomocí děličů paprsků a fázových posunů. A z rovnice

$$U(N)T_{N,N-1} \cdot T_{N,N-2}, \dots, T_{2,1} \cdot D = I(N).$$

již vyplývá požadované tvrzení.

Příloha E

GHZ stavy

GHZ souvisí s experimentem skutečným za účelem vytvořit další argument proti teorii skrytých proměnných (viz. EPR paradox a snaha popsat kvantovou mechaniku jako teorii, která nemá pravděpodobnostní charakter [33]) - v experimentu jsou jasně dané výstupy, jež mohou nastat s pravděpodobností 0 nebo 1. Uvažujme tři systémy rozdělené mezi Alici, Boba a Charlese. Účastníci experimentu mohou měřit veličiny X^A, Y^A , resp. X^B, Y^B resp. X^C, Y^C . Všechny mohou nabývat pouze hodnot 1 nebo -1. Korelace je následující: pro jedno měření na systémech X a dvě měření na systémech Y platí, že produkt výsledků je vždy roven 1 (to pro naměřitelné hodnoty znamená: [(1,1,1)], [1,-1,-1]). Tuto podmínku nazveme XYY.

$$(X^A Y^B Y^C)(Y^A X^B Y^C)(Y^A Y^B X^C) = (X^A X^B X^C).$$

Platí totiž $(Y^A)^2 = (Y^B)^2 = (Y^C)^2 = 1 \Rightarrow (X^A X^B X^C) = 1$. Čili naměříme-li veličinu X na všech třech systémech, produkt získaných hodnot musí být roven 1 = podmínka XXX.

Celkem tedy máme, že je-li za předpokladu existence skrytých proměnných splněna podmínka XXY, je pak vždy splněna podmínka XXX.

Mají-li nyní všechny zúčastněné osoby qubit, s tím, že společný stav systému je GHZ, přičemž na každém qubitu můžeme měřit pozorovatelné X,Y. Platí

$$X \otimes Y \otimes Y |GHZ\rangle = |GHZ\rangle$$

čili GHZ je vlastní stav uvedeného tenzorového produktu s vlastní hodnotou 1. Kromě toho je vlastním stavem operátorů $Y \otimes X \otimes Y$ a $Y \otimes Y \otimes X$ (s toutéž vlastní hodnotou). Jinými slovy systém ve stavu GHZ splňuje podmínku XXY . Přitom ale

$$X \otimes X \otimes X|GHZ\rangle = -|GHZ\rangle. \quad (\text{E.1})$$

Měření XXX tedy vždy vede k výsledku -1 (operátory ale splňují identitu [5]:

$X \otimes Y \otimes Y)(Y \otimes X \otimes Y)(Y \otimes Y \otimes X) = (X \otimes X \otimes X)$), což je ve sporu s výše uvedenou implikací (tři GHZ qubity odporují XXX podmínce) a tedy korelace v rámci takto definovaného systému nikdy nemohou být lokálně popsány teorií, která obsahuje skryté proměnné.

Příloha F

Poznámky k experimentální realizaci

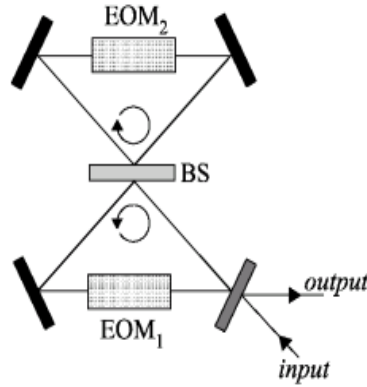
Galtonovy desky

V této příloze uvedeme dvě možnosti experimentální realizace optické Galtonovy desky, první využívá modulaci frekvence (jedná se o podrobnější rozbor přístupu, který jsme v 4.9 použili pro vysvětlení principu Galtonovy desky). Druhá varianta je založena na využití polarizace světla.

F.1 Modulace frekvence

Mějme lineární optický rezonátor s ekvidistantním rozdělením rezonančních frekvencí. Omezíme-li naši pozornost pouze na podélné mody (ozn. $m = \pm 1, \pm 2 \dots$), kde m je relativní index modu zvolený relativně k libovolně zvolenému 'centrálnímu' modu. Každý mod je polarizačně nezávislý, tj. má dvojnásobnou degeneraci. Tato degenerace je zvýšena vložением dvojlomného krystalu - ve formě elektrooptického modulátoru (EOM1) do rezonátoru. Zvyšování dvojlomnosti jako funkce času (prakticky proveditelné zvyšováním napětí). Druhý dvojlomný krystal (EOM2) umístěný uvnitř rezonátoru nechť má osy pootočené o $\pi/4$ vzhledem k osám prvního.

Původní stav Galtonovy optické desky je připraven pomocí laserového paprsku na specifické rezonanční frekvenci a jeho polarizací v rezonátoru. Jakmile intenzita v rezonátoru dosáhne učitě hodnoty, laser se vypne a napětí na prvním elektrooptickém modulátoru se začne lineárně zvětšovat, zatímco na druhém je udržováno konstantní (viz. Obr. (F.1)).



Obrázek F.1: Schéma experimentální realizace: EOM1,2 jsou elektrooptické modulátory, BS dělič paprsku, převzato z [23]

Maticový formalismus pro Galtonovu desku: polarizace populace v jednotlivých modech je reprezentována vektorem $\vec{E}(x(t), y(t))$, kde $x(t)$, $y(t)$ jsou amplitudy x-ové a y-ové polarizační složky a mění se pomalu vzhledem k frekvenci laserového paprsku. Každý optický element odpovídající změně polarizace je reprezentován maticí působící na vektor \vec{E} . Transformace vstupního stavu uskutečněná elektrooptickými modulátory v maticové reprezentaci (viz. [22]):

$$B_1(t) = \begin{pmatrix} e^{i\Phi_1/2} & 0 \\ 0 & e^{-i\Phi_1/2} \end{pmatrix},$$

$$B_2(t) = \begin{pmatrix} \cos(\Phi_2/2) & -i \cdot \sin(\Phi_2/2) \\ -i \cdot \sin(\Phi_2/2) & \cos(\Phi_2/2) \end{pmatrix},$$

přičemž $\Phi_{1,2}$ jsou fázové rozdíly, které získají dvě ortogonální polarizace průchodem oběma EOM (vzhledem k ose dvojlomnosti). Pro transformaci uskutečněnou při jednom průchodu modulátory uspořádanými podle Obr. (F.1) dostáváme:

$$M(t) = B_2 B_1 B_1 B_2. \quad (\text{F.1})$$

Předpokládejme, že $M(t)$ je přibližně konstantní při jedné periodě (ozn. T). To znamená, že změna v dvojlomnosti při jedné periodě bude minimální (vzhledem ke 2π).

Časový vývoj vektoru pak vzhledem k této podmínce lze zapsat jako

$$\vec{E}(t+T) = M(t)\vec{E}(t). \quad (\text{F.2})$$

Změnu \vec{E} v čase pak můžeme zapsat ([22]):

$$\frac{d\vec{E}}{dt} = -\frac{i}{T}H\vec{E}, \quad (\text{F.3})$$

kde elementy H jsou vyjádřeny ve fázových posunech za čas T (očekáváme, že existuje vztah mezi maticemi H a M). Dosazením (F.2) do (F.3) dostáváme:

$$\vec{E}(t+T) = \exp\left(\frac{i}{T} \int_t^{t+T} H(t')dt'\right)\vec{E}(t).$$

V případě, že H je během času T přibližně konstantní tedy máme

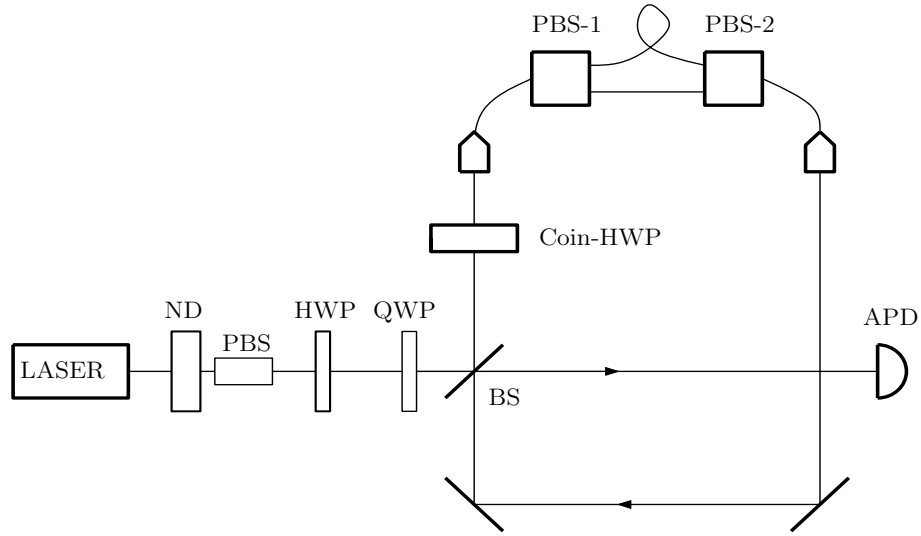
$$M(t) = \exp(-iH(t))$$

Poslední dvě rovnice představují tedy zobrazení klasického systému na kvantově mechanický. Pro matici (F.1) obdržíme následující Hamiltonián:

$$H(t) = \frac{\varphi(t)}{\sin \varphi(t)} \begin{pmatrix} \sin \Phi_1 & \cos \Phi_1 \sin \Phi_2 \\ \cos \Phi_1 \sin \Phi_2 & -\sin \Phi_1 \end{pmatrix},$$

kde $\varphi(t) = \arccos(\cos \Phi_1 \cos \Phi_2)$. Vlastní hodnoty Hamiltoniánu jsou $\pm\varphi(t)$ (pro konstantní hodnotu Φ_2). V případě, že $\Phi_1 = \alpha t$ a $\Phi_2 = \Delta$ (pro případ, že oba úhly jsou malé vzhledem k 2π) se model redukuje na tzv. Landau-Zenerův hamiltonián (viz. např. [34]):

$$H_{LZ}(t) = \begin{pmatrix} \alpha t & \Delta \\ \Delta & -\alpha t \end{pmatrix}.$$



Obrázek F.2: Experimentální uspořádání (podle [35]): ND - filtr (maximální snížení intenzity svazku, BS - symetrický dělič paprsku, HWP - půlvlnová destička, QWP - čtvrtvlnová destička, PBS - polarizační dělič paprsku, APD - fotodioda).

F.2 Polarizace světla

Další možnou realizací Galtonovy desky je varianta popsaná v [35], která využívá polarizaci fotonu jako vnitřní stupeň volnosti. Popíšeme ho v bázi

$$|H\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{a} \quad |V\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (\text{F.4})$$

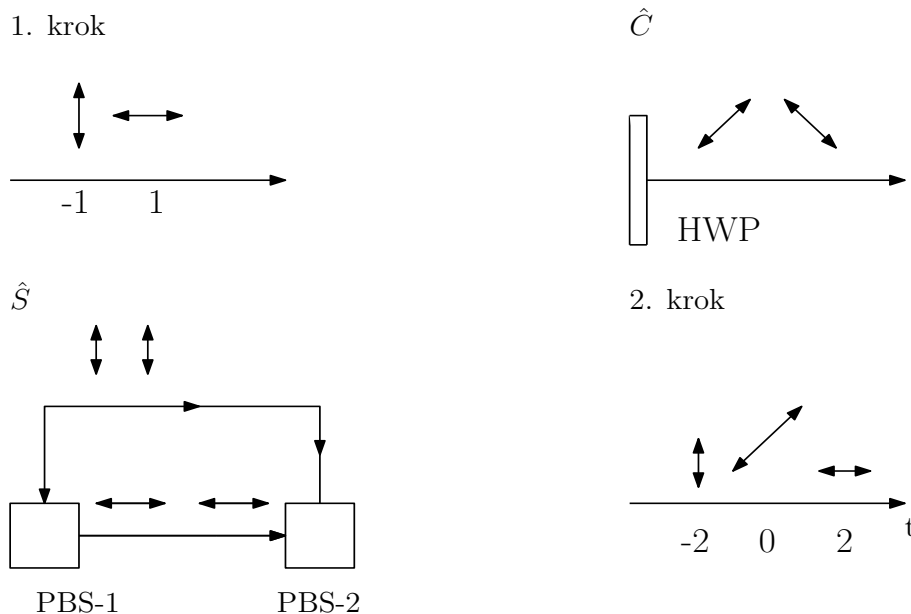
Evoluční operátor po n krocích je dán

$$\hat{U} = (\hat{S}\hat{C})^n,$$

kde \hat{C} je operátor hodů mincí (viz. 4.9), jehož akce bude v našem případě simulována právě polarizací fotonu. Operátor \hat{S} odpovídá operátoru chodce a platí

$$\hat{S} = \sum_x |x-1\rangle\langle x| \otimes |v\rangle\langle V| + |x+1\rangle\langle x| \otimes |H\rangle\langle H|.$$

V této implementaci poloze chodce odpovídají časy, ve kterých foton dorazí na detektor, a akci operátoru mince simuluje půlvlnová destička. Maticová reprezentace této



Obrázek F.3: První dva kroky náhodné procházky, šipkami je znázorněna polarizace fotonu.

transformace v bázi (F.4)

$$C = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix},$$

kde θ odpovídá relativnímu pootočení půlvlnové destičky vzhledem k jedné z optických os. Časový vývoj je pak simulován pomocí smyčky na Obr. F.2. Laserové pulzy jsou zeslabeny filtrem až na jednofotonovou intenzitu. Počáteční polarizace fotonu je připravena pomocí půl- a čtvrtvlnové destičky. Hod mincí je simulován půlvlnovou destičkou zařazenou v horním rameni za děličem paprsku a pohyb chodce dvěma polarizačními děliči paprsku a smyčkou z optického vlákna. Po průchodu prvním polarizačním děličem paprsku, je pomocí smyčky uměle prodloužena trajektorie pro fotony s vertikální polarizací, které jsou na výstupu opět rekombinovány s horizontálně polarizovanými. Výsledný stav pak projde zpět do děliče a může být realizován další krok. Jak je podrobně rozebráno v [35], už při druhém kroku dochází k interferenci s fotonem procházejícím děličem přímo k fotodiodě (schématicky znázorněno na Obr. F.3).

Literatura

- [1] J. Blank, P. Exner, and M. Havlíček. *Hilbert space operators in quantum physics*. Theoretical and mathematical physics. Springer, 2008.
- [2] R.P. Feynman, R.B. Leighton, and M.L. Sands. *The Feynman Lectures on Physics: Quantum mechanics*. The Feynman Lectures on Physics. Addison-Wesley, 1966.
- [3] P.A.M. Dirac. *The principles of quantum mechanics*. Clarendon Press, 1992.
- [4] M. Dušek. *Koncepční otázky kvantové teorie*. Univerzita Palackého, 2002.
- [5] B. Schumacher and M. Westmoreland. *Quantum Processes Systems, and Information*. Cambridge University Press, 2010.
- [6] S.M. Barnett. *Quantum Information*. Oxford University Press, 2009.
- [7] D. Bouwmeester, J.W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, Dec 1997.
- [8] D.M. Greenberger, M.A. Horne, and A. Zeilinger. Going beyond Bell theorem. In *Bells theorem, Quantum theory and conceptions of the universe*, volume 37, pages 69–72. Kluwer Academic Publ., 1989.
- [9] J. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1, 1964.
- [10] S.M. Barnett and S.J.D. Phoenix. Entropy as a measure of quantum optical correlation. *Phys. Rev. A*, 40(5):2404–2409, Sep 1989.
- [11] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [12] S. Stenholm and K.A. Suominnen. *Quantum Approach to Informatics*. Wiley, 2005.

- [13] D. Esteve, J.M. Raimond, and J. Dalibard, editors. *Quantum entanglement and information processing*. Elsevier, 2003.
- [14] W.H. Louisell. *Quantum statistical properties of radiation*. Wiley, 1990.
- [15] P. Kok and B.W. Lovett. *Introduction to Optical Quantum Information Processing*. Cambridge University Press, 2010.
- [16] E. Bruning and F. Petruccione. *Theoretical Foundations of Quantum Information Processing and Communication: Selected Topics*. Lecture Notes in Physics. Springer, 2009.
- [17] B.C. Sanders. Entangled coherent states. *Phys. Rev. A*, 45(9):6811–6815, May 1992.
- [18] B. Yurke and D. Stoler. Generating Quantum-mechanical superpositions of macroscopically distinguishable states via amplitude dispersion. *Phys. Rev. Lett.*, 57(1):13–16, Jul 1986.
- [19] E. Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23:807–812, 1935.
- [20] I. Jex, S. Stenholm, and A. Zeilinger. Hamiltonian theory of a symmetrical multiport. *Opt. Commun.*, 117(1-2):95–101, May 1995.
- [21] Y. Aharonov, L. Davidovich, and N. Zagury. Quantum random-walks. *Phys. Rev. A*, 48(2):1687–1690, Aug 1993.
- [22] D. Bouwmeester, I. Marzoli, G.P. Karman, W. Schleich, and J.P. Woerdman. Optical Galton board. *Phys. Rev. A*, 61(1), Jan 2000.
- [23] C. Navarrete-Benlloch, A. Perez, and E. Roldan. Nonlinear optical Galton board. *Phys. Rev. A*, 75(6), Jun 2007.
- [24] J. Novotny, M. Stefanak, T. Kiss, and I. Jex. Control of entanglement in Ising-type networks with one and two excitations. *J. Phys. A: Mathematical and general*, 38(41):9087–9103, Oct 2005.
- [25] P. Torma, I. Jex, and W.P. Schleich. Localization and diffusion in Ising-type quantum networks. *Phys. Rev. A*, 65(5, Part A), May 2002.

- [26] P. Torma and I. Jex. Properties of Ising-type linear networks. *J. Opt. B: Quantum Semiclass. Opt.*, 1(1):8–13, Feb 1999.
- [27] K. Huang. *Statistical Mechanics*. Wiley, 1987.
- [28] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.
- [29] R.J. Glauber. Coherent and incoherent states of radiation field. *Phys. Rev.*, 131(6):2766–&, 1963.
- [30] M.O. Scully and M.S. Zubairy. *Quantum Optics*. Cambridge University Press, 1997.
- [31] N. Imoto, H.A. Haus, and Y. Yamamoto. Quantum nondemolition measurement of the photon number via the optical Kerr effect. *Phys. Rev. A*, 32(4):2287–2292, Oct 1985.
- [32] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73(1):58–61, Jul 1994.
- [33] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):0777–0780, May 1935.
- [34] G.W.F. Drake. *Springer handbook of atomic, molecular, and optical physics*. Number sv. 1 in Springer Handbook of Atomic, Molecular, and Optical Physics. Springer, 2006.
- [35] A. Schreiber, K.N. Cassemiro, V. Potocek, A. Gabris, P. J. Mosley, E. Andersson, I. Jex, and Ch. Silberhorn. Photons Walking the Line: A Quantum Walk with Adjustable Coin Operations. *Phys. Rev. Lett.*, 104(5), Feb 2010.