

Fakulta matematiky, fyziky a informatiky
Univerzity Komenského
BRATISLAVA



Diplomová práca

Martin Plesch

BRATISLAVA 2001

Fakulta matematiky, fyziky a informatiky
Univerzity Komenského
BRATISLAVA
Katedra teoretickej fyziky

**Entanglement:
Kvantové korelácie
v mnohočasticových systémoch**

Bratislava, Marec 2001

Diplomant:

Martin Plesch

Vedúci diplomovej práce:

Prof. RNDr. Vladimír Bužek, DrSc.

Čestne prehlasujem, že som diplomovú prácu vypracoval samostatne.

Rád by som touto cestou vyslovil poďakovanie svojmu školiteľovi prof. Vladimírovi Bužekovi za povzbudzujúce slová a cenné rady, ktoré v nemalej miere prispeli k vzniku tejto práce.

Obsah

1	Úvod	1
2	Entanglement	3
2.1	Paradox Einsteina, Podolskeho a Rosena	3
2.2	Bellove nerovnosti	5
2.3	CHSH nerovnosť	9
2.4	Experimentálne potvrdenie	10
2.5	Dvojjasticový entanglement	11
2.5.1	Bellove stavy	14
2.5.2	Kritériá separability pre častice so spinom $1/2$	14
2.5.3	Miery entanglementu	16
2.6	Viacčasticový entanglement	20
2.6.1	Trojčasticový model	20
2.6.2	Čo je viacčasticový entanglement?	21
2.6.3	Kritériá separability	23
2.6.4	Entanglované reťazce	24
2.6.5	Entanglované molekuly	25
2.6.6	Miery viacčasticového entanglementu	27
2.6.7	Experimentálne potvrdenie	29
2.7	Entanglement viacrozmerných systémov	31
2.7.1	Dva qdity rozmeru N	32
2.7.2	Spojité premenné	33
2.8	Využitie entanglementu	33
2.8.1	Husté kódovanie	33
2.8.2	Výmena kvantových EPR kľúčov	35
2.8.3	Kvantová teleportácia	35
3	Prenos kvantovej informácie zašumeným kanálom	39
3.1	Problémy otvoreného systému	39
3.2	Dekoherencia	39
3.3	Korekcia chýb	40
3.4	Kvantová korekcia chýb	41
3.5	Pauliho kanál	43
3.6	Symetrizáciou k stabilizácii systému	44
3.7	Fidelita	45
3.8	Symetrizovaný stav prechádzajúci Pauliho kanálom	46

3.8.1	Pauliho kanál pôsobiaci na 1 qbit	46
3.8.2	Pauliho kanál pôsobiaci na všetky qbity	51
3.9	Záver	54
4	Entanglement jednorozmerného Isingovho modelu	56
4.1	Úvod	56
4.2	Hamiltonián	57
4.3	Prípád N=3	57
4.3.1	Faktorizovaný vstupný stav	58
4.3.2	Maximálne dvojčasticovo entanglovaný vstupný stav	60
4.3.3	GHZ vstupný stav	60
4.3.4	Základný stav ako vstupný stav	61
4.4	Prípád N=5	63
4.4.1	Faktorizovaný vstupný stav	63
4.4.2	Symetrický vstupný stav	65
4.4.3	GHZ vstupný stav	65
4.5	Záver	69
5	Záver	71
A	Dôkaz Peres-Horodeckého teorémy	73

Kapitola 1

Úvod

Keď sa začiatkom 20. storočia začala do povedomia nie len fyzikov, ale celej verejnosti dostávať kvantová fyzika, znamenalo to významný prelom. Človek bol nútený pripustiť svoj omyl tak, ako to urobil iba niekoľkokrát v histórii (a že to často nebolo jednoduché, ukazujú kruté osudy prvých zástancov heliocentrickej sústavy). Museli sme si priznať, že všetko to, čo okolo seba vidíme a vnímame, čo považujeme za tak samozrejmé ako modrú oblohu alebo hrejúci oheň, je len priblíženie skutočnosti, ktorá stále zostáva zahalená rúškom tajomstva. Naša každodenná skúsenosť nás učí, že na konkrétne otázky existujú konkrétne odpovede. Vieme povedať, koľko vec váži či meria, ako dlho niečo trvalo a kde presne sa to stalo. Kvantová mechanika ale hovorí, že sa nemôžeme pýtať, čo je to vlastne svetlo, kde presne je elektrón. Nie preto, že by sme odpoveď nepoznali, je predsa úlohou bádateľov klásť si podobné otázky. Odpoveď nikdy nedokážeme pochopiť, rovnako ako nikdy nemôžeme vysvetliť slepému človeku rozdiel medzi červenou a modrou farbou; ako spieval Karel Kryl:

... chceš hluchým vypráveť, čo píseň znamená, a slepým čo jsou křídla labutí? ...

Aj keď bol matematický formalizmus na svete, trvalo niekoľko rokov, kým sa fyzici zhodli na tom, čo vlastne znamená. V dnešnej dobe je vo väčšine odbornej verejnosti preferovaná pravdepodobnostná (kodanská¹) interpretácia kvantovej mechaniky. A to aj napriek tomu, že prináša mnoho vnútorných paradoxov a predpokladá veci, ktoré sú ťažko zlučiteľné s našou každodennou skúsenosťou a priam sa priečia zdravému rozumu. Naučili sme sa bez veľkého pozastavenia prijímať, že pri meraní sa stav častice skokom mení a že meracie prístroje sa nedajú popisovať kvantovomechanicky. Pripúšťame tak hneď na začiatku, že teória nie je úplná, pretože potrebuje elementy popisované inou teóriou, aby sa dala vôbec použiť. Na druhej strane sú ale jej výsledky natoľko prevratné, že musí byť akceptovaná.

Samozrejme, existujú aj iné teórie chápania a interpretovania známej matematiky. Každá z nich má svoje výhody a snaží sa svojím spôsobom spojiť to, čo poznáme z bežného sveta s tým, čo hovoria rovnice. Každá z nich má však aj svoje nevýhody a vnútorné problémy, ktoré ich zaraďujú len do zoznamu alternatívnych interpretácií ku kodanskej.

Všetko toto sú zrejme dôvody, prečo aj na prahu nového tisícročia nachádzame aj v oblastiach jednoduchej kvantovej mechaniky problémy, ktoré sú neprebádané. Myšlienky kvantovej komunikácie a kvantových počítačov lákajú aj laikov, ktorí si od nich sľubujú radikálnu zmenu

¹Kodanská podľa dánskeho mesta, kde sa konalo stretnutie fyzikov, na ktorom bol dohodnutý spoločný pohľad na problematiku interpretácie kvantovej mechaniky.

v spôsobe spracovania dát a informácie, ktorá sa stala v poslednom desaťročí snáď najčastejšie skloňovaným slovom vôbec.

V mojej diplomovej práci sa pokúšam poskytnúť ucelený pohľad na kvantovú väzbu - **entanglement**, podľa možnosti čo najširšiemu okruhu čitateľov. V druhej kapitole je historický a vecný prehľad o tom, ako sa na kvantové korelácie prišlo, ako boli experimentálne dokázané a tiež ako sa dajú teoreticky a prakticky (aj keď to dosiaľ len v laboratóriách) využiť. Snažil som sa, aby každý, kto absolvoval kurz elementárnej kvantovej mechaniky, dokázal bez ďalších znalostí prečítať túto časť a pochopiť, čo to entanglement je, prečo je taký zvláštny a dôležitý a tiež to, prečo sa dosiaľ nepodarilo využívať ho efektívnejšie.

Kvantová informácia, zakódovaná napríklad v stave elektrónu so spinom $\frac{1}{2}$ alebo v polarizácii fotónu je ďaleko krehkejšia a zraniteľnejšia pod vplyvom okolitého prostredia ako klasická. Na to, aby sme boli v budúcnosti schopní využívať prednosti, ktoré poskytuje, musíme vypracovať algoritmy na predchádzanie a nápravu chýb, ktoré vplyvom prostredia vznikajú. V tretej kapitole rozoberám jeden z možných scenárov vhodný hlavne pre prostredie so silným vplyvom a ukazujem, za akých okolností je výhodné ho použiť. Jedná sa o kódovanie bitu kvantovej informácie (v ďalšom texte nazývanom qbit) do priestoru stavov, ktorý vznikol z pôvodnej častice a niekoľkých ďalších rovnakých častíc (je to istá obdoba klasického spôsobu kódovania opakovaním, keď tú istú informáciu posielať niekoľkokrát). Využijem však silu kvantovej väzby a stavy nekódujem do niekoľkonásobných kópií, ale do symetrického stavu. Výsledkom je potom, pre daný model a parametre pôsobenia prostredia, optimálny počet častíc, do ktorých je vhodné stav kódovať.

Štvrtá kapitola je venovaná úplne inému problému. Jedná sa o čisto fenomenologický pohľad na entanglement v konkrétnom fyzikálnom modeli. Vybral som si Isingov model v jednom rozmere s priečnym magnetickým poľom, lebo z klasického pohľadu je veľmi dobre preskúmaný. Snažím sa ukázať, že štúdium časového vývoja entanglementu medzi jednotlivými časticami aj v malých systémoch môže ukázať niektoré zaujímavé skutočnosti, ktoré nie sú z klasického pohľadu na model zrejmé. Pokúsil som sa tiež hľadať náznaky fázových prechodov v modeli s malým počtom častíc a overoval som niektoré nerovnosti pre miery entanglementu, ktoré dosiaľ neboli všeobecne dokázané.

Kapitola 2

Entanglement

2.1 Paradox Einsteina, Podolskeho a Rosena

V roku 1935 mala kvantová mechanika za sebou búrlivý vývoj. Teória, ktorá tak ako žiadna predtým popierala naše skúsenosti z bežného života, sa ukázala ako veľmi presná a produktívna v predpovedaní výsledkov pokusov vo svete elementárnych častíc. Kládla však aj otázky, na ktoré nevieme často odpovedať ani dnes. Na jednu z nich upozornil Einstein et al. v článku [1]. Pokúsili sa na základe vlastnej definície reality poukázať na to, že opis reality pomocou vlnovej funkcie nemôže byť kompletný, teda že znalosť vlnovej funkcie nezodpovedá znalosti všetkých faktov o systéme (svedčí o tom už aj názov článku, v preklade: "Môžeme považovať kvantovo-mechanický opis fyzikálnej reality za kompletný?", ktorý priam navádza odpovedať nie). Pokúsim sa tu pretlmočiť argumenty uvedené v článku a v ďalšom aj argumenty oponentov.

Základná Einsteinova axióma, ktorú považoval za nespochybniteľnú, sa týkala práve definície fyzikálnej reality. Einstein tvrdí: "Postačujúca podmienka na to, aby sme fyzikálnu veličinu považovali za reálnu je to, že dokážeme jej hodnotu pre daný fyzikálny systém predpovedať bez toho, aby sme narušili tento systém". V kvantovej mechanike ale nedokážeme s istotou predpovedať hodnoty veličín reprezentovaných dvoma nekomutujúcimi operátormi. V zmysle tejto argumentácie máme teda len dve možnosti: buď nemôžu byť obe veličiny naraz "reálne", alebo opis prírody a reality pomocou vlnovej funkcie nie je úplný.

Zoberme na začiatok príklad triviálneho systému s jedným stupňom voľnosti, ktorý sa nachádza v stave

$$\Psi(x) = e^{(2\pi i/h)p_0 x} \quad (2.1)$$

kde h je Planckova konštanta, p_0 konštanta a x nezávislá premenná. Uvedená funkcia je vlastným stavom operátora hybnosti

$$p = (h/2\pi i) \frac{\partial}{\partial x} \quad (2.2)$$

s vlastnou hodnotou p_0 . Nie tak ale pre operátor polohy x , kde môžeme zaviesť len hustotu pravdepodobnosti toho, že sa častica nachádza v danom mieste. Ak má častica presne definovanú hybnosť, pojem polohy či súradníc v priestore nemá pre ňu žiaden fyzikálny význam.

Predstavme si teraz ale zložitejší fyzikálny systém, ktorý môžeme rozdeliť na dve časti, **I** a **II**, so súradnicami x_1 a x_2 . Nech tieto časti istý čas, povedzme od $t = 0$ do $t = T$ spolu interagovali. Po tomto čase už nie je možná žiadna interakcia oboch systémov, a preto, podľa

argumentácie v článku, žiadna zmena či meranie, odohrávajúce sa iba na systéme **I**, nemôže ovplyvniť stav systému **II**. Vyberme teraz dve veličiny, **A** a **B**, s vlastnými funkciami ψ_i a φ_i . Celkovú vlnovú funkciu potom môžeme napísať ako rozklad podľa vlastných stavov týchto veličín (pre jednoduchosť predpokladáme nedegenerovanosť):

$$\Psi^{III}(x_1, x_2) = \sum_n \psi_n(x_1)u_n(x_2) = \sum_n \varphi_n(x_1)v_n(x_2). \quad (2.3)$$

Ak teraz prevedieme na systéme **I** meranie veličiny **A**, výsledkom môže byť len jedna z jej vlastných hodnôt. Pritom sa ale vlnová funkcia zredukuje na jeden jediný člen zo sumy v rovnici (2.3). Ak napríklad nameriame hodnotu a_i , druhý systém zostane v stave $u_i(x_2)$. Ak zasa zmeriame veličinu **B** a získame b_j , druhý systém musí byť v stave $v_j(x_2)$. Keďže ale druhý systém "nevie", ktorú veličinu meriame, musia obe funkcie zodpovedať tej istej realite, keďže neexistuje žiadna interakcia medzi systémami. Druhý systém teda musí byť v stave, ktorého "realita" zodpovedá obom funkciám $u_i(x_2)$ i $v_j(x_2)$ naraz. Nič ale nebráni tomu, aby tieto funkcie boli vlastnými funkciami dvoch nekomutujúcich operátorov, napríklad už spomínanej polohy a hybnosti. To by ale znamenalo, že druhý systém má reálne presne určenú aj polohu, aj hybnosť, čo je v príkrom rozpore s tým, čo tvrdí kvantová mechanika.

V závere článku je položená otázka, či je naozaj popis systému pomocou vlnovej funkcie kompletný.

Krátko po uverejnení tohoto článku sa objavila odpoveď, ktorú publikoval Niels Bohr v [2]. Prijal definíciu reality, uvedenú v pôvodnom článku, snažil sa však ukázať, že problém je niekde inde. Totiž, že každý pokus či experiment, ktorý vykonáme, musí byť vyhodnocovaný samostatne a že nemôžeme vytvárať závery na základe toho, čo by sme mohli zmerať, ale len a len na základe toho, čo naozaj zmeriame. A ako vieme, naozaj zmerať môžeme len jeden z nekomutujúcich operátorov, ak zmeriame aj ten druhý, porušíme stav systému.

Einstein vo svojich pamätiach neprijal túto argumentáciu. Považoval aj naďalej za nezvrátitelný fakt, že akékoľvek meranie či iná manipulácia so systémom **I**, ktorý je priestorovo separovaný od zvyšku systému **II**, nemôže ovplyvniť tento systém.

Jednoduchší príklad, zakladajúci sa ale na úplne rovnakej dileme ako predchádzajúce, uverejnil Bohm [3]. Predpokladajme rozpad bezspinovej častice na dve častice so spinom $1/2$ (napríklad $\pi_0 \rightarrow e^+e^-$), ktoré sa od seba veľkou rýchlosťou vzdávajú. Na elektróne môžeme vykonať napríklad meranie spinu v smere osi x . Dostaneme výsledok $\pm 1/2$, ktorý už s určitosťou zafixuje veľkosť spinu v smere osi x aj pre pozitron. Rovnako dobre ale môžeme uskutočniť merania aj spinu v smeroch iných osí, napríklad y či z . Vychádza nám, že spin pozitronu musí byť teda určený vo všetkých osiach, čo je znova v rozpore s predikciami kvantovej mechaniky, ktorá to povoľuje maximálne pre jednu os.

Záver zo všetkých týchto úvah bol jednoznačný. Nie všetky fakty a skutočnosti, ktoré sme považovali až doteraz za nezvrátitelné, môžu ostať v platnosti. Kvantová mechanika vo svojej podstate nie je lokálnou teóriou. Názory, či takou má ostať alebo sa má (ak sa dá) doplniť na kompletnejšiu teóriu, v ktorej sa obnoví lokalita, mali svojich prívržencov i odporcov. Ak totiž prijmeme definíciu fyzikálnej reality, kvantová mechanika vo svojej vtedajšej i súčasnej podobe idú ruka v ruke s porušením lokality. Ak naopak postavíme na prvé miesto požiadavku lokálnosti, poprieme definíciu reality, čo je neakceptovateľné.

2.2 Bellove nerovnosti

Veľký prínos v hľadaní odpovede na otázku, či je potrebné doplniť popis reality vlnovou funkciou ešte o akési skryté parametre, ktoré by zabezpečili zachovanie lokality v kvantovej mechanike, priniesol Bellov článok [4]. Autor v ňom ukazuje, že akákoľvek teória, ktorá v sebe obsahuje skryté parametre a zachováva predpovedné vlastnosti kvantovej mechaniky, musí byť nelokálna. A tiež opačne, akákoľvek lokálna teória skrytých parametrov dáva pri vhodných pokusoch štatisticky iné výsledky ako kvantová mechanika. Kvantová mechanika totiž v štatistických výsledkoch pripúšťa korelácie, ktoré sú príliš silné nato, aby sa dali vysvetliť pomocou klasickej fyziky.

Argumentáciu predviedol na zjednodušenom príklade dvoch častíc spinu $1/2$ z [3]. My sa na začiatok ale pozrime na jednoduchý príklad z klasickej fyziky [5]. Predstavme si malý balón, ktorý po vypustení vo veľkej výške praskne a rozpadne sa na dve časti, ktoré sa od seba vzdalujú. Každá z nich má nejaký moment hybnosti, ale celkový moment hybnosti je nula (predpokladáme, že balón sa pred prasknutím neotáčal). Označme momenty hybností týchto častíc ako \vec{J}_1 a \vec{J}_2 . Určíme tiež dva jednotkové vektory \vec{n}_1 a \vec{n}_2 , v smere ktorých budeme merať momenty hybnosti častí balóna. V skutočnosti nás ani nezaujíma veľkosť momentu, ale len jeho smer, budeme teda merať veličinu $a = \text{sign}(\vec{n} \circ \vec{J})$. Výsledok bude vždy ± 1 , špeciálny prípad nulového priemetu je pri veľkom množstve štatisticky nezaujímavý a môžeme ho obísť napríklad definovaním funkcie sign ako $+1$ aj pre nulový výraz v zátvorke.

Ak použijeme veľa balónov, ktoré necháme prasknúť, môžeme vykonať veľa meraní pri rovnakých hodnotách \vec{n}_1 a \vec{n}_2 . Môžeme hľadať priemernú hodnotu a_1 či a_2 (priemetu momentu hybnosti jedných či druhých častí balóna), ktoré by podľa štatistických zákonov mali klesať s počtom meraní N ako $\langle a \rangle \sim \frac{1}{\sqrt{N}}$. Ak ale hľadáme koreláciu výsledkov meraní, tá už vo všeobecnosti nevymizne. Napríklad pre $\vec{n}_1 = \vec{n}_2$ bude

$$\langle a_1 a_2 \rangle = \sum_j \frac{a_1^j a_2^j}{N} = -1, \quad (2.4)$$

lebo $a_1 = -a_2$ pre ľubovoľné meranie. Toto vyplýva z požiadavky celkovo nulového momentu hybností oboch častí balóna. Ak spočítame výraz (2.4) všeobecne, dostaneme koreláciu

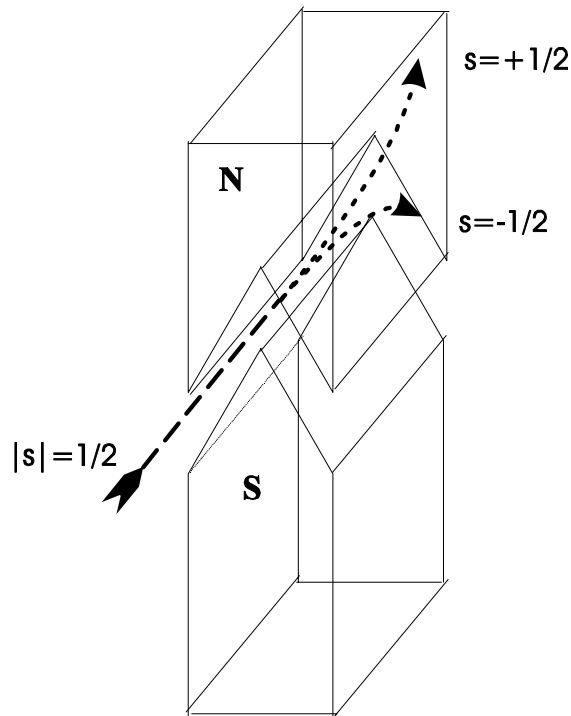
$$\langle a_1 a_2 \rangle = \frac{2\alpha}{\pi} - 1, \quad (2.5)$$

kde α je uhol medzi \vec{n}_1 a \vec{n}_2 v tomto poradí.

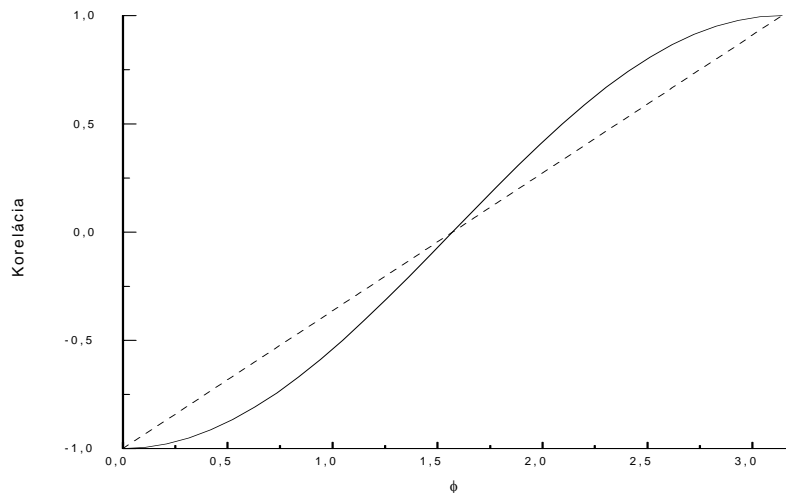
Pokračujme teraz v našich úvahách. Predstavme si, že balón zmenšíme natoľko, že sa začne správať podľa zákonov kvantovej fyziky a označíme si jeho stav ψ . Jeho prasknutie môže zodpovedať napríklad už spomínanému rozpadu $\pi_0 \rightarrow e^+ e^-$ a meranie znamienka momentu hybnosti zameníme za meranie spinu elektrónu a pozitronu pomocou Stern-Gerlachovho prístroja. Meriame teda pozorovateľné $\vec{\sigma}_1 \circ \vec{n}_1$ a $\vec{\sigma}_2 \circ \vec{n}_2$ (priemety spinu na príslušné osi), ktorých vlastné hodnoty sú znova len ± 1 . Ak využijeme skutočnosť, že celkový spin systému je nulový, matematicky vyjadrenú vzťahom $\vec{\sigma}_1 \psi = -\vec{\sigma}_2 \psi$, dostaneme

$$\langle a_1 a_2 \rangle = -\vec{n}_1 \circ \vec{n}_2 = -\cos(\alpha). \quad (2.6)$$

Z obrázku 2.2 je zrejmé, že korelácie v kvantovej mechanike sú pre všetky prípady (okrem triviálnych, keď je korelácia nulová alebo maximálna) silnejšie ako klasicke. Bell ale ukázal,



Obrázok 2.1: Na meranie priemetu spinu častíc so spinom $1/2$ v definovanom smere sa používa takzvaný Stern-Gerlachov prístroj. Medzi dvoma pólmi magnetu je vytvorená úzka štrbina, v ktorej vzniká vysoko nehomogénne magnetické pole. Častica prelietava cez štrbinu a v závislosti od smeru priemetu spinu sa vychýľuje hore alebo dole.



Obrázok 2.2: Na grafe je vidieť porovnanie klasických (čiarkovaná čiara) a kvantových (plná čiara) korelácií. Okrem špeciálnych bodov, kde sú korelácie rovnaké, sú kvantové všade silnejšie ako klasické.

ako uvidíme ďalej, ďaleko viac. Nehovorí o porovnaní klasickej a kvantovej mechaniky. Hovorí o tom, aké vlastnosti musí mať teória, ktorá je lokálna. Zároveň ale ukazuje, že kvantová mechanika tieto vlastnosti nemá a dáva tak možnosť raz a jednoznačne pomocou experimentu overiť, či je možná existencia "lepšej", kompletnejšej teórie, ako to navrhovali Einstein, Podolski a Rosen.

Predstavme si teraz dva lineárne polarizované fotóny, ktoré vznikli napríklad na spoločnej SPS¹ kaskáde a majú rovnakú polarizáciu. Oba fotóny sa rozbehnú preč a v dostatočnej vzdialenosti od seba, aby sme vylúčili akékoľvek vzájomné ovplyvňovanie, budú vystavené meraniu svojej polarizácie. Nazvime pre názornosť aparáty, ktoré budú merať polarizáciu prvej a druhej častice Alica a Bob. Oba majú možnosť zvoliť si smer svojho merania (až potiaľto je scénár zhodný s príkladom s balónom) ako jednu z dvoch možností. Alica má na výber smery \vec{n}_a a \vec{n}_c , Bob \vec{n}_b a \vec{n}_c (tu je dôležité to, že dva z troch prípustných smerov sú presne rovnaké). Označme výsledky meraní a, b a c (nadobúdajú hodnotu ± 1 , znamenajú v prípade $+1$ polarizáciu zhodnú s meraným smerom a v prípade -1 polarizáciu kolmú), pričom vieme, že ak sa obaja rozhodnú pre meranie v smere vektora \vec{n}_c , výsledok im musí vyjsť rovnaký. Vieme teraz napísať identitu, ktorá platí bez ohľadu na to, ktoré merania sa uskutočnili:

$$a(b - c) \equiv \pm(1 - bc). \quad (2.7)$$

Jednoduchým overením prípustných možností pre a, b a c sa môžeme presvedčiť, že skutočne platí, hoci v skutočnosti môžeme na základe merania získať len dva z troch údajov v rovnici. Predpokladajme ale, že máme akúsi (nijak bližšie neurčenú) deterministickú lokálnu teóriu skrytých premenných. V tomto prípade musia byť všetky tri výsledky dopredu a-priori dané a môžu závisieť len na hodnote premenných, ktoré si častice môžu niesť zo sebou. Označme množinu týchto premenných λ_i , kde i označuje poradové číslo pokusu (budeme pracovať s mnohými časticami). Lokálnosť vyžaduje, aby λ_i nezáviseli od smeru merania (častica v Alici nesmie vedieť, v akom smere uskutočňuje meranie v tom okamihu Bob).

Napišme teraz identitu (2.7) pomocou skrytých premenných:

$$a(\lambda_i)(b(\lambda_i) - c(\lambda_i)) \equiv \pm(1 - b(\lambda_i)c(\lambda_i)), \quad (2.8)$$

pričom, samozrejme, táto identita musí stále platiť. Keďže nepoznáme λ_i pre jednotlivé pokusy, ani spôsob ako ovplyvňujú výsledok, rovnica (2.8) nám nedáva žiadnu informáciu. Môžeme ale urobiť priemer cez mnohé pokusy a dostávame vzťah nazývaný **Bellova nerovnosť**:

$$|\langle ab \rangle - \langle ac \rangle| \leq 1 - \langle bc \rangle, \quad (2.9)$$

kde $\langle ab \rangle$ je získané ako súčet všetkých $a(\lambda_i)b(\lambda_i)$ predelených počtom pokusov. Inými slovami je $\langle ab \rangle$ korelácia výsledkov meraní v smeroch \vec{n}_a a \vec{n}_b .

Pozrime sa teraz ale na kvantovú mechaniku. Tá tiež nedokáže predpovedať výsledky jediného pokusu, ale štatistické výsledky áno. Tieto výsledky sa navyše dajú experimentálne pozorovať, teda otázku, či je správna kvantová mechanika alebo nejaká lokálna teória, môže vyriešiť správne postavený experiment. Korelácie v kvantovej mechanike sú dané vzájomnými uhlami medzi smermi merania. Ak označíme odklon smeru \vec{n}_a od definovanej osi α a podobne β a γ , nerovnica (2.9) nadobudne tvar

$$|\cos 2(\alpha - \beta) - \cos 2(\alpha - \gamma)| \leq 1 - \cos 2(\beta - \gamma). \quad (2.10)$$

¹SPS označuje skratku pre typ kaskády, kde elektróny postupne prechádzajú do nižšieho energetického stavu. Všeobecne zo stavu s_1 cez stav p_0 do stavu s_0 , presne to závisí vždy od typu použitých atómov.

Tu už nie je ale žiaden problém nájsť také uhly, pre ktoré by nerovnosť nebola splnená, sú to napríklad

$$\begin{aligned}\alpha &= 0^\circ \\ \beta &= 30^\circ \\ \gamma &= 60^\circ\end{aligned}\tag{2.11}$$

a môžeme teda písať, že za istých okolností kvantová mechanika **porušuje Bellove nerovnosti**.

Uvedme si teraz jeden možno ešte názornejší príklad, podľa článku [6]. Uvážme konkrétny stav dvoch častíc so spinom $\frac{1}{2}$ v tvare

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle),\tag{2.12}$$

teda v stave s nulovým celkovým spinom. Budeme merať spin oboch častíc (znova si pomôžeme označením Alica a Bob) v rôznych smeroch. Označme tentokrát smer, v ktorom meria Alica ako \vec{n}_a a Bobov smer ako \vec{n}_b . Pravdepodobnosť, že nám oba aparáty oznámia výsledky $+1$, teda že oba spiny boli zmerané v smere otočenia meracieho Stern-Gerlachovho prístroja bude závislý len od vzájomného uhla medzi \vec{n}_a a \vec{n}_b (celkový spin je nulový a nie je teda dopredu určený žiaden významný smer) a bude daná

$$P_{++}(\vec{n}_a, \vec{n}_b) = \langle \psi^- | \frac{1}{2}(1 + \vec{n}_a \cdot \vec{\sigma}_1) \otimes \frac{1}{2}(1 + \vec{n}_b \cdot \vec{\sigma}_2) | \psi^- \rangle = \frac{1}{4}(1 - \cos \theta),\tag{2.13}$$

kde $\vec{\sigma}_1$ pôsobí na prvú a $\vec{\sigma}_2$ na druhú časticu a θ je uhol medzi \vec{n}_a a \vec{n}_b . Rovnakú pravdepodobnosť získame aj pre oba spiny otočené opačne, teda pre výsledky -1 :

$$P_{--}(\vec{n}_a, \vec{n}_b) = \langle \psi^- | \frac{1}{2}(1 - \vec{n}_a \cdot \vec{\sigma}_1) \otimes \frac{1}{2}(1 - \vec{n}_b \cdot \vec{\sigma}_2) | \psi^- \rangle = \frac{1}{4}(1 - \cos \theta).\tag{2.14}$$

Zoberme teraz tri rôzne osi $\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3$ s tým, že medzi každými dvoma bude uhol, ktorého kosínus je $1/2$. Podľa kvantovej mechaniky platí pre súčet pravdepodobností, že nameriame na jednotlivých dvojiciach osí spiny hore:

$$P(\mathbf{n}_1, \mathbf{n}_2) + P(\mathbf{n}_1, \mathbf{n}_3) + P(\mathbf{n}_3, \mathbf{n}_2) = 3 \cdot \frac{1}{4} \cdot \frac{1}{2} = \frac{3}{8}\tag{2.15}$$

Rovnako to bude aj pre oba spiny dole, spoločná pravdepodobnosť pre nameranie rovnakého spinu teda bude

$$P_{++} + P_{--} = \frac{3}{4}.\tag{2.16}$$

Podľa klasickej fyziky ale táto pravdepodobnosť musí byť väčšia rovná jednej! Ak je totiž priemet spinu na každú os určený dopredu, mám k dispozícii tri osi a len dva možné výsledky merania (hore-dole), **musí** aspoň na jednej dvojici osí padnúť rovnaký spin. Rovnako, ako keď mám v ruke tri mince a hodím ich na stôl. Nech sa deje, čo sa deje, vždy mi padnú aspoň dva znaky alebo dve hlavy, žiaden iný výsledok nie je možný.

2.3 CHSH nerovnosť

Pozornému čitateľovi iste neušlo, že pri odvodzovaní Bellovej nerovnosti sme vybrali istý špeciálny prípad. Hoci oba meracie prístroje, Alica aj Bob, mali každý možnosť vybrať si jeden z dvoch smerov, v ktorých budú merať polarizácie, bolo tam nie veľmi vysvetlené obmedzenie, že dva z týchto štyroch smerov musia byť rovnaké. Vskutku nie je problém sformulovať podobnú nerovnosť ako (2.9) aj pre 4 nezávislé smery. Zaveďme teda smer \vec{n}_d a výsledok z merania v tomto smere d , ktorý pochopiteľne tiež nadobúda hodnoty ± 1 . Úlohu identity (2.7) spĺňa

$$(a + c)b + (a - c)d \equiv \pm 2, \quad (2.17)$$

znova môžeme prejsť k závislosti od skrytých parametrov a urobiť stredné hodnoty. Dostávame nerovnicu

$$|\langle ab \rangle + \langle bc \rangle + \langle cd \rangle - \langle da \rangle| \leq 2. \quad (2.18)$$

Tento výsledok je nazývaný Clauser-Horne-Shimony-Holtova nerovnosť [6]. Rovnako ako Bellova nerovnosť aj CHSH nerovnosť určuje horný limit na korelácie v teóriách lokálnych premenných. V kvantovej mechanike má (2.18) tvar

$$|\cos 2(\alpha - \beta) + \cos 2(\beta - \gamma) + \cos 2(\gamma - \delta) - \cos 2(\delta - \alpha)| \leq 2. \quad (2.19)$$

Napríklad ale pre výber uhlov

$$\begin{aligned} \alpha &= 0^\circ \\ \beta &= 22.5^\circ \\ \gamma &= 45^\circ \\ \delta &= 67.5^\circ \end{aligned} \quad (2.20)$$

nadobúda ľavá strana rovnice (2.19) hodnotu $2\sqrt{2}$, čo je zjavne viac ako 2.

Zaujímavá otázka je, ako veľmi môže stav v kvantovej mechanike porušiť CHSH nerovnosť. Zistili sme, že sa dá nájsť taká konfigurácia experimentu, že ľavá strana rovnice nadobudne hodnotu $2\sqrt{2}$. Je možné nájsť iné, lepšie konfigurácie, kde je táto hodnota ešte väčšia?

Uvážme operátor

$$\mathbf{C} = \mathbf{a}\mathbf{b} + \mathbf{b}\mathbf{c} + \mathbf{c}\mathbf{d} - \mathbf{d}\mathbf{a}, \quad (2.21)$$

kde $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}$ sú operátory merajúce polarizáciu a ich kvadrát je vždy rovný 1. Na základe toho môžeme písať

$$\mathbf{C}^2 = 4 + [\mathbf{a}, \mathbf{b}] [\mathbf{c}, \mathbf{d}] \quad (2.22)$$

a v suprémovej norme pre operátor \mathbf{C} platí

$$\|\mathbf{C}^2\| \leq 4 + 4 \|\mathbf{a}\| \cdot \|\mathbf{b}\| \cdot \|\mathbf{c}\| \cdot \|\mathbf{d}\| = 8. \quad (2.23)$$

Pre samotný operátor dostávame podmienku

$$\|\mathbf{C}\| \leq 2\sqrt{2}. \quad (2.24)$$

Hodnota operátora nemôže nikdy prekročiť hodnotu $2\sqrt{2}$ (nerovnosť (2.24) sa nazýva Cirelsonova nerovnosť). Keďže sme našli prípad, v ktorom dosahujeme rovnosť, našli sme aj maximálnu hodnotu.

2.4 Experimentálne potvrdenie

Publikovanie Bellovho článku samozrejme viedlo k tomu, že sa mnohí experimentátori snažili navrhnúť a zrealizovať experimenty, ktoré by dokázali rozhodnúť, či sú alebo nie sú Bellove nerovnosti porušované. Jedny z prvých dôležitých výsledkov publikoval v roku 1976 Ed Fry [24]. V tom čase ešte rôzne vedecké skupiny publikovali rôzne výsledky, z ktorých niektoré potvrdzovali porušovanie nerovností a iné nie. Nebolo jasné, či sa jedná o nedostatočne presné meranie, alebo ide o závislosť od typu vystavaného experimentu. Citovaný článok s dovtedy najvyššou presnosťou ukázal porušovanie Bellových nerovností a tiež vynikajúcu zhodu s očakávanými výsledkami tak, ako boli spočítané pomocou kvantovej mechaniky, so zarátaním neurčitostí detektorov a experimentálneho zariadenia ako celku.

Napriek tomu ale trvalo viac ako dve desiatky rokov, kým boli zaznamenané prvé skutočné úspechy pri experimentálnom potvrdzovaní porušenia Bellových nerovností. Dôvod bol veľmi prozaický: na vylúčenie všetkých možných lokálnych teórií potrebujeme experiment, ktorý má k dokonalosti a ideálnosti veľmi blízko. Základný problém, s ktorým sa experimenty potýkali, bol problém lokálnosti, tzv. locality loophole. Na to, aby platili všetky predpoklady pre nerovnosti nesmie byť jasné postavenie experimentu v čase, keď ešte nie sú dve častice (či už spiny alebo polarizované fotóny), ktoré neskôr použijeme pre experiment, separované priestorovým intervalom. Inak povedané, celé experimentálne zariadenie by sme mali začať stavať až v okamihu, keď obe častice od seba separujeme. Toto je samozrejme ťažko predstaviteľné, hlavne pokiaľ zamýšľame používať fotóny, ktoré za jedinou sekundu preletia mnohonásobok vzdialeností bežných na Zemi. Ale v skutočnosti stačí oveľa jemnejšia podmienka, ktorú musíme splniť: musíme v čase medzi priestorovou separáciou a detekciou častíc (takpovediac "za letu") zmeniť podmienky experimentu.

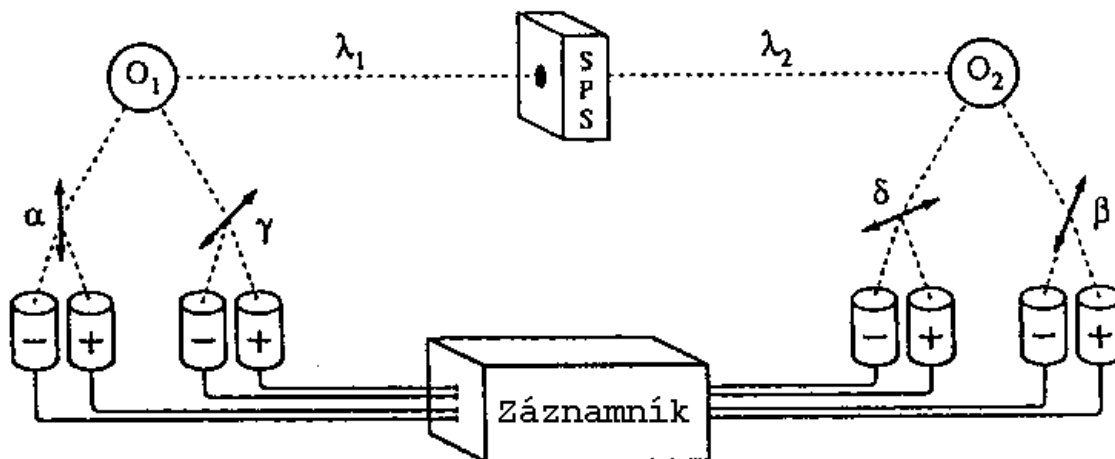
Toto sa prvýkrát úspešne podarilo realizovať A. Aspectovi [12] vo svojich pokusoch v roku 1982, v ktorých použil polarizované fotóny. Zjednodušená schéma je znázornená na obrázku (2.3). Dva fotóny z kalciovej kaskády SPS boli produkované na vlnových dĺžkach 422,7 nm a 551,3 nm. Prechádzali kolimátorom a optoakustickými spínačmi, ktoré pre každý z fotónov pseudonáhodne vyberali dva analyzátory s rôznymi smermi polarizácie. Spínače menili svoju polohu s rôznymi frekvenciami a niekoľkonásobne rýchlejšie, ako bol čas letu fotónu z kaskády (vzdialenosť 12 metrov zodpovedá času asi 40 nm, pričom stredný čas medzi prepnutiami bol cca 10 nm).

Výsledky boli jednoznačné, Bellove nerovnosti boli porušené o viac ako 5 štandardných odchýliek. Stále však neboli vyriešené ďalšie problémy, ktoré aj v tomto prípade umožňovali vytvorenie teórie so skrytými parametrami tak, aby vysvetľovala výsledky Aspectovho experimentu.

Dva fotóny vychádzajúce z kaskády nemajú rovnaké vlnové dĺžky, preto sú v skutočnosti rozlíšiteľné. Nejedná sa teda, ak vezmeme do úvahy aj frekvenciu (energiu) fotónov, o stav typu $|\psi\rangle$ či podobný, o ktorom pojednávajú nerovnosti, ale o stav typu

$$|\Phi\rangle = \frac{1}{\sqrt{2}} (|1E_1\rangle|0E_2\rangle + |0E_1\rangle|1E_2\rangle), \quad (2.25)$$

ktorý môže spôsobovať problémy. Ďalšia medzera v experimente, ktorá umožňovala tvorbu lokálnych teórií, bola len pseudonáhodnosť preklápania analyzátorov v experimente. Túto dieru (loophole) "zatvoril" až Zeilinger et. al. [13] experimentom, kde využil nie pseudonáhodný, ale naozaj náhodný proces na zmenu parametrov experimentu. V dvoch laboratóriách



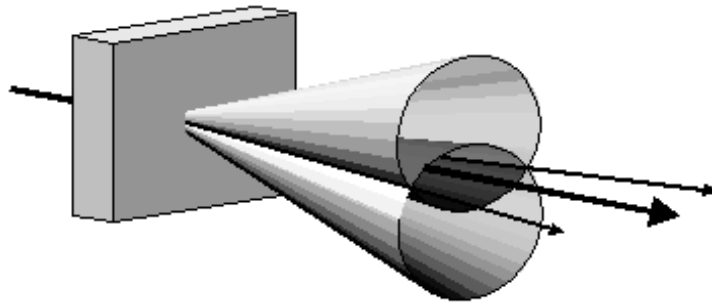
Obrázok 2.3: Schéma Aspectovho experimentu. Fotóny vlnových dĺžok λ_1 a λ_2 letia zo spoločného zdroja (SPS kaskády) v korelovanom stave. Optické prepínače O_1 a O_2 (pseudo) náhodne pre každý fotón vyberú analyzátor α, γ , resp. β, δ a výsledky sa porovnávajú a uchovávajú v záznamníku.

v Innsbrucku, vzdialených od seba 400 metrov, prebiehali merania polarizovaných fotónov, ktoré boli produkované v spoločnom zdroji (laser Down-conversion typu II, obrázok (2.4), fotografia (2.5), zdroj obrázkov [13]). Interval medzi meraniami bol vždy priestorupodobný a podmienky experimentu sa menili náhodne. Schéma je znázornená na obrázku (2.6) [13]. Napriek všetkému, aj pre výsledky posledne popisovaného experimentu je možné zostaviť lokálnu teóriu. Posledná veľká medzera, ktorá čaká na experimentátorov, je detection loophole, problém detektorov [15]. Nedá sa totiž vylúčiť, že účinnosť detektorov je akýmsi spôsobom závislá od toho, v akom celkovom stave sa fotóny nachádzajú, alebo, povedané v reči lokálnych premenných, od hodnôt lokálnych premenných.

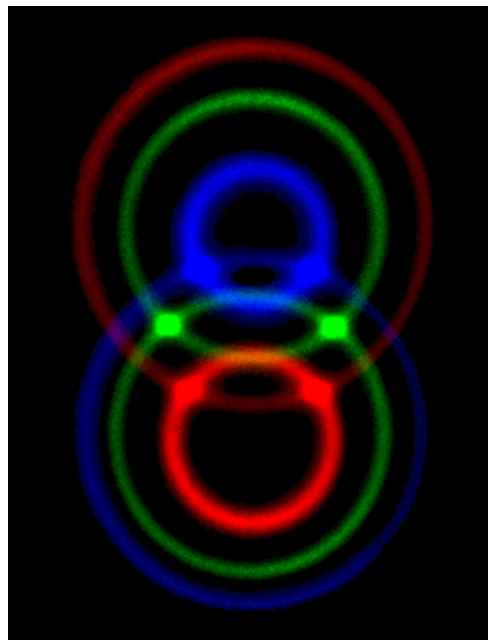
Na prekonanie tejto medzery by sme potrebovali detektory, ktorých účinnosť je dostatočne vysoká (Účinnosť každého detektora je ohraničená zhora číslom jedna. Ak sú skutočné účinnosti ďaleko menšie ako jedna, máme možnosť navrhnúť takú závislosť týchto účinností od skrytých parametrov, aby "simulovala" kvantové výsledky, ale zároveň neporušovala ohraničenie. Pri dostatočne vysokých priemerných účinnostiach detektorov už nie je možné takúto závislosť navrhnúť, lebo pre isté hodnoty lokálnych premenných by požadovala účinnosť detektorov vyššiu ako jedna). V dnešnej dobe ešte stále nie sú k dispozícii podobné detektory, preto, hoci málo pravdepodobná, stále tu zostáva možnosť, že "všetko je inak". Že v skutočnosti je svet naozaj lokálny a všetky doterajšie výsledky, ktoré potvrdzovali kvantovú mechaniku, boli len chybným priblížením skutočného stavu.

2.5 Dvojčasticový entanglement

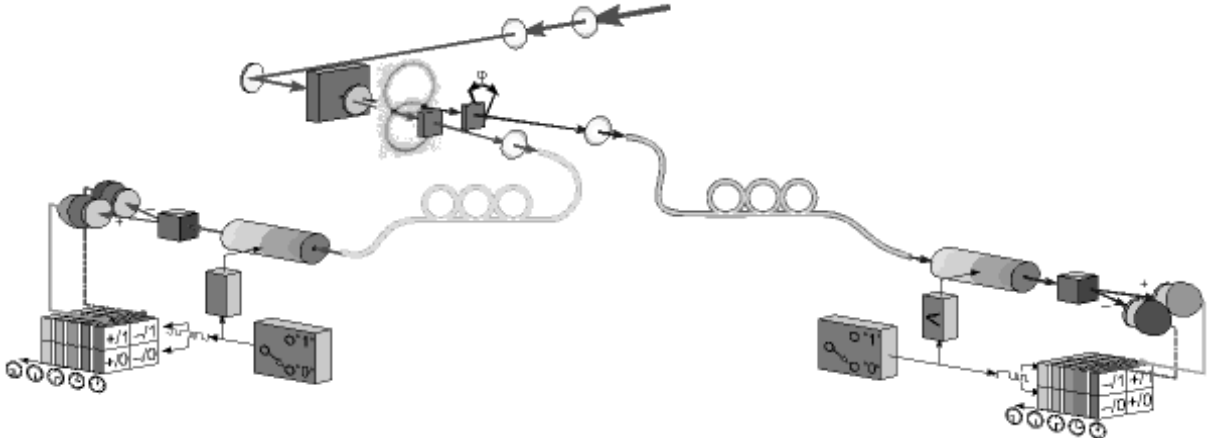
Z vyššie uvedeného je zrejmé, že v kvantovej mechanike existujú stavy, ktoré porušujú lokálnosť v zmysle, na akú sme zvyknutí z bežného života. Napríklad dve častice so spinom $1/2$, pokiaľ



Obrázok 2.4: Laser down-conversion druhého typu. V nelineárnom kryštáli sú produkované dva lúče, riadny a mimoriadny. Na obrázku sú znázornené dvoma kuželmi. V prieseku kuželov môžu vznikáť fotónové páry, ktoré sú v kvantovo korelovanom stave.



Obrázok 2.5: Fotografia lúča, ktorý prešiel nelineárnym kryštálom. Na priesečníkoch kružníc môžu vznikáť entanglované páry fotónov.



Obrázok 2.6: Na obrázku je znázornená podrobná schéma experimentu prevádzaného v Innsbrucku. Dva entanglované fotóny získané zo spoločného zdroja prechádzajú dlhé trasy svetelnými vláknami. Náhodný prepínač založený na parametrickej konverzii druhého typu zabezpečuje výber smeru, v ktorom bude analyzovaná polarizácia toho-ktorého fotónu. Potom nasleduje už len analyzátor a archivačné zariadenie.

sú vo vhodnom stave (napríklad už definovaný $|\psi^-\rangle$), udržiavajú si medzi sebou akési "puto". Nie je dopredu určený spin prvej častice, môže rovnako dobre (s pravdepodobnosťou 50%) byť smerom hore aj dole. Ak ho raz však zmeriame, určíme aj výsledok prípadného neskoršieho merania spinu na druhej častici v tom istom smere. Nezávisle na tom, ako je ďaleko.

Na jednej strane je ťažko predstaviteľné, ako sa informácia o našom meraní môže dostať k druhej častici (čo bol presne bod, ktorý bol považovaný v článku [1] za nemožný). Z pohľadu kvantovej mechaniky sa ale nejedná o dva systémy, ale o jeden jediný systém v stave $|\psi^-\rangle$, ktorý sa zmenil ako celok po zmeraní spinu na prvej častici. A medzi dvoma časťami jedného systému vzniká väzba, entanglement. Hovoríme, že dve časti systému sú entanglované, resp. neseparovateľné, ak nemôžu byť vytvorené pomocou dvoch preparátorov stavov, ktoré si môžu navzájom vymieňať len klasické informácie.

Ak sú dva podsystemy separovateľné, ešte to nemusí znamenať, že nie sú korelované. Stačí zobrať jednoduchý príklad, stav

$$|0\rangle|0\rangle \quad (2.26)$$

je zrejme korelovaný, obe časti majú rovnaký spin. Tento stav je ale zrejme separovateľný, zapisateľný v tvare tenzorového súčinu

$$|0\rangle|0\rangle = |0\rangle \otimes |0\rangle \quad (2.27)$$

a zrejme sa dá vytvoriť na dvoch miestach len pomocou výmeny klasickej informácie (napríklad špecifikovaním jednotkového vektora, v ktorého smere má mať spin hodnotu $1/2$).

Vyvstáva samozrejme otázka, ako zistiť, či je daný stav $|\Phi\rangle$, rozdelený na dva podsystemy, entanglovaný alebo nie. Núka sa použiť Bellove nerovnosti; pokiaľ ich stav porušuje, určite entanglovaný je. Bohužiaľ, táto podmienka je len postačujúca, nie je nutná. Existujú entanglované stavy (v zmysle definície uvedenej vyššie), ktoré Bellove nerovnosti neporušujú. Ďalšia otázka, hlavne v súvislosti s experimentami, je separovateľnosť či neseparovateľnosť zmesí vyjadrených maticami hustoty ρ .

2.5.1 Bellove stavy

Pri práci s entanglovanými stavmi dvoch častíc sa ukazuje, že je veľmi výhodné zaviesť okrem normálnej bázy, ktorú pre dve dvojhladinové častice používame a je typu

$$\begin{aligned} &|0\rangle|0\rangle \\ &|0\rangle|1\rangle \\ &|1\rangle|0\rangle \\ &|1\rangle|1\rangle, \end{aligned} \tag{2.28}$$

aj bázu inú. Stavy (2.28) sú úplným systémom v dvojrozmernom Hilbertovom priestore, ale pochopiteľne nie sú jediným možným a správnym výberom. Používame ich často preto, lebo poskytujú intuitívnu predstavu o klasickom stave dvoch atómov popísaných pomocou týchto vektorov. Všetky bázové vektory sú faktorizované a teda predstaviteľné v rámci klasického prístupu. Z matematického hľadiska ale úplne ekvivalentnú bázu tvoria 4 entanglované, takzvané Bellove stavy, definované nasledovne

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle). \end{aligned} \tag{2.29}$$

Tieto stavy sú ďaleko ťažšie predstaviteľné, ale uľahčia mnoho námahy a vypisovania v ďalších častiach práce.

2.5.2 Kritériá separability pre častice so spinom 1/2

V tejto časti zosumarizujem kritériá, ktoré dokážu viac či menej úspešne určiť, či je daný stav dvoch častíc, určený vo všeobecnosti maticou hustoty, separabilný na podsystémoch.

Ľubovoľná matica hustoty ρ je separovateľná vtedy a len vtedy, ak sa dá zapísať v tvare

$$\rho = \sum_A w_A \rho'_A \otimes \rho''_A, \tag{2.30}$$

kde ρ'_A a ρ''_A sú matice hustoty jednotlivých podsystémov. Avšak nie je, ako by sa mohlo zdať, jednoduché o neznámom stave (špeciálne zmesi) určiť, či je alebo nie je separabilný. Pochopiteľne, jedno kritérium sú Bellove nerovnosti. Ak ich stav porušuje, zákonite musí byť entanglovaný. Naopak to však neplatí. Mnoho stavov, ktoré nie sú separabilné podľa definície (2.30), neporušujú Bellove nerovnosti.

Pre taký jednoduchý systém ako dve častice spinu 1/2 je úplnou a postačujúcou podmienkou na určenie separability konštrukcia čiastočne transponovanej matice hustoty [7], známej tiež pod skratkou PPT, v tvare

$$\sigma = \sum_A w_A (\rho'_A)^T \otimes \rho''_A. \tag{2.31}$$

Aj transponovaná matica hustoty spĺňa všetky podmienky na maticu hustoty (jednotková stopa a nezápornosť), preto zákonite σ musí mať všetky vlastné hodnoty nezáporné. Ak to nie je splnené, dochádzame do sporu s predpokladom z rovnice (2.30), teda že pôvodná matica hustoty sa dá rozložiť a je separovateľná. Samotný dôkaz, že každá neseperabilná matica hustoty pre systémy 2×2 (dve častice spinu $1/2$) má zápornú aspoň jednu z vlastných hodnôt uviedli až Horodecki v článku [8], bližšie v dodatku A.

Uvedme teraz príklad. Uvážme pár častíc so spinom $1/2$, ktoré su v takzvanom Wernerovom stave

$$\rho_{m\mu, n\nu} = xS_{m\mu, n\nu} + (1-x)\delta_{m\mu}\delta_{n\nu}/4, \quad (2.32)$$

kde x je parameter určujúci podiel singletu S a

$$S_{01,01} = S_{10,10} = -S_{01,10} = -S_{10,01} = \frac{1}{2}, \quad (2.33)$$

pričom ostatné komponenty matice S sú nulové. V maticovom tvare to môžeme zapísať takto:

$$\rho = \begin{pmatrix} \frac{(1-x)}{4} & 0 & 0 & 0 \\ 0 & \frac{(1+x)}{4} & -\frac{x}{2} & 0 \\ 0 & -\frac{x}{2} & \frac{(1+x)}{4} & 0 \\ 0 & 0 & 0 & \frac{(1-x)}{4} \end{pmatrix}. \quad (2.34)$$

Wernerov stav už nie je čistý stav, je to zmes. Táto sa nedá zapísať vo forme ket-vektora, ktorú sme doteraz na zápis stavov používali. Samotný singlet S je ale stav čistý, zapísateľný v tvare

$$S = |\psi^-\rangle\langle\psi^-|, \quad (2.35)$$

kde stav $|\psi^-\rangle$ je jeden zo stavov Bellovej bázy.

Operátor čiastočnej transpozície pôsobiaci na maticu (2.34) sa dá zapísať vo forme

$$PPT = T \otimes I, \quad (2.36)$$

čo v preklade znamená, že na časť matice zodpovedajúcu prvej častici pôsobí ako transpozícia a na časť zodpovedajúcu druhej častici ako identita. Operátor transpozície pre maticu 2×2 môžeme zapísať v tvare

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (2.37)$$

a operátor identity je jednotková matica 4×4 . Výsledný operátor PPT bude teda matica 16×16 .

Čiastočne transponovaná matica hustoty má tvar

$$\rho^{T_1} = \begin{pmatrix} \frac{(1-x)}{4} & 0 & 0 & -\frac{x}{2} \\ 0 & \frac{(1+x)}{4} & 0 & 0 \\ 0 & 0 & \frac{(1+x)}{4} & 0 \\ -\frac{x}{2} & 0 & 0 & \frac{(1-x)}{4} \end{pmatrix}. \quad (2.38)$$

A vlastné hodnoty ρ^{T_1} sú trikrát $\frac{1+x}{4}$ a raz $\frac{1-3x}{4}$. Stav je teda určite entanglovaný pre $x > \frac{1}{3}$, Bellove nerovnosti sú porušované ale iba pri $x > \frac{1}{\sqrt{2}}$.

2.5.3 Miery entanglementu

V predchádzajúcej časti som sa venoval tomu, ako sa dá pre známy stav systému zistiť, či je alebo nie je separabilný. To však samozrejme je len časť informácie. Ak vieme, že systém je entanglovaný, má dobrý zmysel sa pýtať, nakoľko. Je intuitívne jasné, že napríklad stav

$$|\psi^+\rangle = \frac{1}{\sqrt{2}} (|10\rangle + |01\rangle) \quad (2.39)$$

je viac entanglovaný ako stav

$$|\phi\rangle = \alpha|10\rangle + \beta|\psi^+\rangle \quad \alpha \longrightarrow 1, \quad (2.40)$$

ktorý je z veľkej časti zložený zo separabilného stavu a len malé jeho percento tvorí entanglovaná časť. Preto je potrebné a žiaduce zaviesť pre entanglement mieru.

Táto miera by mala spĺňať niektoré požiadavky. Ak nazveme všeobecnú mieru entanglementu nejakej matice hustoty $E(\rho)$, sú to napríklad tieto [11]:

- $E(\rho) \geq 0$ pozitivita
- $E(\rho) = 0 \iff \rho$ je separabilná
- $E(|\psi^+\rangle\langle\psi^+|) = 1$ normalizovanosť na maximálne entanglovaných stavoch
- $E(\rho_1 \otimes \rho_2) = E(\rho_1) + E(\rho_2)$ aditivita
- $E(\rho) = E(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger)$ lokálne unitárne operácie nemenia entanglement
- pri lokálnych operáciách len na jednom podsysteme sa nesmie entanglement zväčšovať.

Samozrejme, podmienky je možné rozšíriť podľa toho, aké obmedzenia sme ochotní prijať, tieto sú však ťažko spochybniteľné. Netriviálna je len posledná, tú však musíme vyžadovať, aby sme zabezpečili citlivosť miery práve na entanglement, teda na mieru zviazanosti podsystemov, ktorá sa nemôže pri lokálnych operáciách zväčšovať.

Entanglement čistých stavov

Pre čisté stavy existuje všeobecná zhoda v miere entanglementu. Tá je určená entropiou systému, vzniknutého z pôvodného stavu spravením čiastočnej stopy cez jeden z podsystemov

$$E(\psi) = -Sp(\rho_A \log_2 \rho_A) = -Sp(\rho_B \log_2 \rho_B), \quad (2.41)$$

kde A, B sú jednotlivé podsystemy, $\rho = |\psi\rangle\langle\psi|$ a ρ_A , resp. ρ_B je matica hustoty so spravenou čiastočnou stopou cez druhý podsystem. Obe tieto entropie (získané z matice redukovanej na časticu A alebo B) sú rovnaké a spĺňajú všetky hore uvedené podmienky. Pre každú inú mieru entanglementu, ktorú v ďalšom zavedieme, budeme preto tiež žiadať, aby pre čisté stavy prechádzala na entropiu systému.

Entanglement formovania

Pre zmiešané systémy je zavedenie miery ďaleko komplikovanejšie a neexistuje dosiaľ jednoznačná zhoda, ktorá by mala byť tá správna. Entropia systému pre zmiešaný stav nevyhovuje, lebo nespĺňa podmienku 2, teda aj pre separabilné, klasicky korelované stavy nám dáva nenulový entanglement.

Jedným z kandidátov, v poslednom období často uprednostňovaným, je tzv. entanglement formovania. Motivácia pre jeho zavedenie je jednoduchá. Ak máme k dispozícii nejaký stav, môžeme sa pýtať, koľko maximálne entanglovaných stavov potrebujeme na jeho prípravu spotrebovať. V tomto prípade je uvažovanie trochu abstraktné (ťažko sa predstavuje použitie necelého čísla stavov), ale ak uvážime mnohonásobnú kópiu nášho stavu $\rho^{\otimes N}$, pre veľké N je otázka úplne legálna.

Každá matica hustoty sa dá napísať v mnohých rozkladoch typu $\rho = \sum_i p_i |\psi\rangle_{ii} \langle\psi|$. Potom entanglement formovania matice hustoty ρ je minimum váženého priemeru entanglementu čistých stavov jej dekompozície cez všetky možné dekompozície:

$$E_F(\rho) = \min_{|\psi\rangle} \sum_i p_i E(|\psi\rangle_i). \quad (2.42)$$

Samozrejme, tu sa stretávame s problémom pri výpočte, ako minimalizovať analyticky cez všetky dekompozície.

Ďalším kandidátom, alebo lepšie inou formou špeciálne pre dva dvojrozmerné systémy, je konkurencia. Je vhodná kvôli jednoduchému výpočtu a prehľadnosti. Pre jej vyjadrenie si musíme definovať konjugovanú maticu hustoty

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y) \rho^* (\sigma_y \otimes \sigma_y). \quad (2.43)$$

Čísla $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ nech sú odmocniny vlastných hodnôt matice $\rho\tilde{\rho}$, zoradené nerastúco v uvedenom poradí. Konkurencia pôvodnej matice hustoty ρ potom je [17]

$$C(\rho) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4). \quad (2.44)$$

Keďže entanglement formovania rastie monotónne s konkurenciou daného stavu, kde [18]

$$E_F(C) = h\left(\frac{1 - \sqrt{1 - C^2}}{2}\right) \quad (2.45)$$

$$h(x) = -x \log_2 x - (1 - x) \log_2(1 - x), \quad (2.46)$$

sú tieto miery prakticky rovnocenné. Týmto sme vlastne získali aj jednoduché vyjadrenie entanglementu formovania pre ľubovoľný stav 2 qbitov.

Entanglement destilácie

Presne opačným spôsobom ako entanglement formácie je definovaný entanglement destilácie. Nezaujímá nás, koľko Bellových stavov potrebujeme na vytvorenie nášho stavu ρ , ale naopak, koľko maximálne entanglovaných stavov dokážeme z nášho stavu vytvoriť, vydestilovať (samozrejme aj tu rátame s mnohými kópiami nášho stavu). Definujeme ho

$$E_D(\rho) = \lim_{N \rightarrow \infty} \frac{1}{N} S(\rho_A^{\otimes N}). \quad (2.47)$$

Pochopiteľne, pre čisté stavy bude entanglement destilácie rovný entanglementu formovania, pri lokálnych operáciách na čistých stavoch sa miera entanglementu zachováva. Dnes ale neexistuje spôsob, ako jednoducho vyčíslit' entanglement destilácie pre zmiešaný stav.

Pre tak jednoduché systémy, s akými sa zaoberáme v tejto kapitole, nemá entanglement destilácie natoľko veľký význam ako pri väčších systémoch. V tom prípade sa totiž môže systém nachádzať v stave, ktorý je entanglovaný (podľa kritérií na zistenie entanglementu, nedá sa zapísať ako suma súčinov matíc hustoty) a má aj nenulový entanglement formácie, ale jeho entanglement destilácie je nulový. To znamená, že nemôžeme z tohoto stavu, ani z ľubovoľného počtu jeho kópií lokálnymi operáciami a klasickou komunikáciou získať žiadnu kópiu maximálne entanglovaného, napríklad Bellovho stavu. Viac informácií sa dá nájsť napríklad v článku [32].

Relatívna entropia

Ďalšou mierou entanglementu je relatívna entropia entanglementu [11]. Odráža trochu iný pohľad na problém, keď sa nezaujíname o vývoj daného stavu, ale skôr o jeho polohu v priestore všetkých stavov.

Predstavme si množinu všetkých možných stavov daného systému, zloženého z dvoch podsystémov, ktorých entanglovanosť chceme skúmať. Potom v tejto množine existuje podmnožina všetkých stavov systému, ktoré nie sú entanglované. Ak by sme boli schopní vybrať z týchto stavov nejakým spôsobom vždy jeden, ktorý by kánonicky zodpovedal danému, skúmanému stavu ρ a dokázali definovať vhodnú vzdialenosť na množine stavov, mohla by práve táto vzdialenosť (stavu ρ od priradeného stavu z množiny separabilných stavov) reprezentovať mieru entanglementu. Ako prirodzený separabilný stav k neznámemu stavu ρ sa nika stav $\rho_A \otimes \rho_B$, kde ρ_A je matica hustoty zredukovaná len na systém A , teda

$$\rho_A = Sp_B(\rho) \quad , \quad \rho_B = Sp_A(\rho). \quad (2.48)$$

Možnosť ale samozrejme je aj nešpecifikovať dopredu, vzdialenosť od ktorého zo separabilných stavov budeme uvažovať, ale definovať entanglement ako minimum vzdialenosti ku všetkým separabilným stavom.

Teraz je potrebné zaviesť vhodnú mieru vzdialenosti na množine stavov. Nie všetky vzdialenosti totiž spĺňajú podmienky, ktoré kladieme na mieru entanglementu (hlavne požiadavka, aby pre čisté stavy prechádzala miera na entropiu systému). Okrem toho, z praktických dôvodov, hľadáme vzdialenosť čo možno najjednoduchšiu, umožňujúcu analytickú minimalizáciu cez množinu stavov. Jedna z kandidátok je relatívna entropia dvoch stavov

$$S(\rho||\sigma) = Sp(\rho \ln \rho - \rho \ln \sigma). \quad (2.49)$$

Pozorný čitateľ si iste všimol, že funkcia (2.49) nie je vzdialenosťou v matematickom zmysle slova. Chýba jej napríklad taká základná vlastnosť, ako symetria. Napriek tomu, relatívna entropia spĺňa všetky podmienky na zavedenie miery entanglementu v tvare

$$E_{RE}(\rho) = \min_{\sigma \in Sep} S(\sigma||\rho), \quad (2.50)$$

kde Sep je množina separabilných stavov. (Pokiaľ by sme neuvažovali minimalizáciu, ale zobrali kánonický separabilný stav $\rho_A \otimes \rho_B$, jednalo by sa o von Neumannovu vzájomnú informáciu. Táto sa ale môže zvyšovať pomocou lokálnych operácií kombinovaných s klasickou komunikáciou, teda nie je citlivá na rozdiel medzi klasickými a kvantovými koreláciami).

Všetky dosiaľ uvedené miery entanglementu spĺňali okrem triviálnych podmienok aj tú, že lokálnymi operáciami sa entanglement nemôže zvyšovať, a to podľa žiadnej z uvedených mier. Z toho ale vyplýva veľmi zaujímavá skutočnosť. Predstavme si situáciu, že máme k dispozícii N maximálne entanglovaných stavov $|\psi^+\rangle_{AB}$ a Alica aj Bob majú k dispozícii ešte niekoľko (dostatočne veľa) častíc v známom stave, napríklad $|0\rangle$. Pomocou nich budeme teraz vyrábať iné, nie maximálne entanglované stavy, ktoré nazveme σ . Otázka, koľko maximálne takýchto stavov môžeme vyrobiť, je zodpovedaná entanglementom formácie E_F

$$N(\sigma)_{\max} = \frac{N}{E_F(\sigma)}. \quad (2.51)$$

Pri opätovnom získavaní pôvodných stavov sa nám ale nemusí podariť získať ich pôvodné množstvo N . Tentokrát totiž platí iný vzťah pre počet znovuzískaných stavov $|\psi^+\rangle_{AB}$ M , a to

$$M = E_D(\sigma) \cdot N(\sigma)_{\max} = N \frac{E_F(\sigma)}{E_D(\sigma)}. \quad (2.52)$$

Je známe, že pre niektoré zmiešané stavy je entanglement formácie ostro väčší ako entanglement destilácie, preto nám na konci našej operácie zostane menej entanglementu, ako sme mali na začiatku, ak matica σ nie je čistý stav. Toto nastane práve vtedy, ak prevádzame nereverzibilné lokálne operácie (na to, aby sme dostali z pôvodne čistého stavu maticu hustoty, musíme prestať uvažovať isté množstvo našich častíc). Napríklad Alica zviaže jeden entanglovaný qbit s ďalšími dvoma svojimi qbitmi a potom jeden z nich prestane ďalej používať, to znamená že už na ňom nebude prevádzať ďalšie operácie a bude ho vnímať ako qbit prostredia, nad ktorým nemá kontrolu. Zvyšné častice potom zostanú v zmiešanom stave.

Príklad je uvedený v článku [11]. Ako cieľové stavy si autori vybrali Wernerove stavy podľa (2.34) a namiesto ťažko spočítateľného entanglementu destilácie uvažujú relatívnu entropiu. Využijeme poznatok [10], že každá miera pre entanglement na istom stave dáva väčšie alebo rovné hodnoty ako miera destilácie. Dá sa ukázať, že pre všetky hodnoty parametra $x \in (0, 1)$ je entanglement formácie Wernerovho stavu väčší ako relatívna entropia (pre $x = 0, 1$ sa nejedná o zmiešaný stav). Preto operácia typu

$$|\psi^+\rangle_{AB}^{\otimes N} \rightarrow \sigma_{Werner}^{\otimes \tilde{N}} \rightarrow |\psi^+\rangle_{AB}^{\otimes M} \quad (2.53)$$

pre všetky netriviálne hodnoty parametra x dáva

$$M < N. \quad (2.54)$$

Vo všeobecnosti sa dá povedať, že nereverzibilnými lokálnymi operáciami sa entanglement stráca a získať znova späť sa dá iba nelokálnymi operáciami.

Na záver je asi vhodné podotknúť, že v článku [10] je ukázané, že všetky miery entanglementu, spĺňajúce horeuvedené kritériá plus niektoré ďalšie, týkajúce sa asymptotického správania sa pri veľkom množstve uvažovaných častíc, musia spĺňať pre každý stav podmienku

$$E_D \leq E \leq E_F, \quad (2.55)$$

kde E_D je entanglement destilácie a E_F je entanglement formácie.

2.6 Viacčasticový entanglement

2.6.1 Trojčasticový model

V predchádzajúcej kapitole som sa venoval výlučne dvojčasticovému entanglementu. Bellove a CHSH nerovnosti ukazujú, že na to, aby sme mohli rozlíšiť, či sú dve častice v entanglovanom stave, potrebujeme štatistický súbor rovnakých stavov. Až na základe merania tohoto súboru dokážeme rozlíšiť kvantové vlastnosti.

V prípade troch častíc je už situácia iná. Na základe jediného experimentu dokážeme odlíšiť stav, ktorý vykazuje trojčasticový entanglement. Zoberme tri častice v stave

$$|\psi\rangle = \left(\frac{|0\rangle|0\rangle|0\rangle - |1\rangle|1\rangle|1\rangle}{\sqrt{2}} \right) \quad (2.56)$$

a operátory priemetu spinu i -tej častice na os x, y a z

$$\sigma_{ix}, \sigma_{iy}, \sigma_{iz}. \quad (2.57)$$

Všetky tri častice sú priestorovo separované. Z operátorov (2.57) môžeme konštruovať ďalšie, pričom platia vzťahy

$$\begin{aligned} |\psi\rangle &= \sigma_{1x}\sigma_{2y}\sigma_{3y}|\psi\rangle \\ &= \sigma_{1y}\sigma_{2x}\sigma_{3y}|\psi\rangle \\ &= \sigma_{1y}\sigma_{2y}\sigma_{3x}|\psi\rangle \\ &= -\sigma_{1x}\sigma_{2x}\sigma_{3x}|\psi\rangle. \end{aligned} \quad (2.58)$$

Označme výsledky príslušných meraní m_{ix}, m_{iy}, m_{iz} . Tieto budú nadobúdať len hodnoty ± 1 . Z (2.58) vyplýva podmienka

$$m_{1x}m_{2x}m_{3x} = -1, \quad (2.59)$$

ale musí tiež platiť

$$m_{1y}m_{2x}m_{3x} = m_{1x}m_{2y}m_{3x} = m_{1x}m_{2x}m_{3y} = 1. \quad (2.60)$$

Keďže vieme, že $m_{iy}^2 = 1$, skombinovaním (2.60) dostávame výsledok

$$m_{1x}m_{2x}m_{3x} = 1, \quad (2.61)$$

čo je v jasnej kontradikcii s výsledkom (2.59).

Vysvetlenie sa skrýva na rovnakom mieste, ako to bolo pri Bellových nerovnostiach. Na každej častici môžem previesť iba jeden z experimentov merania priemetu spinu na os x či y . Ak ale uznávam argument Einsteinovej reality, musím predpokladať, že oba tieto výsledky sú dopredu dané, lebo sú s istotou predpovedateľné na základe merania iných, priestorovo vzdialených častíc. Tu sa dostávam okamžite do sporu, bez toho, aby som potreboval robiť štatistický priemer.

2.6.2 Čo je viacčasticový entanglement?

V prvom rade je potrebné si ujasniť, čo vlastne v kontexte viacerých častíc entanglement znamená. Najlepšie sa to vysvetlí na konkrétnom prípade troch častíc, nazvime si ich Alica,

Bob a Carlos. Hovoríme, že stavy Alice a Boba sú entanglované, ak vykazujú kvantové (klasické nestačia) korelácie bez ohľadu na to, v akom stave sa nachádza Carlos. Inak, A a B sú entanglované, ak matica hustoty

$$\rho_{AB} = \text{Sp}_C(\rho_{ABC}) \quad (2.62)$$

je entanglovaná.

Táto definícia ale nemusí byť jediná. Skrýva s sebe totiž problém: ak by Carlos, hoci vzdialený od Alice a Boba, začal s nimi spolupracovať, a vykonával by operácie podľa ich pokynov, entanglement medzi Alicou a Bobom môže vzniknúť. Zoberme si ako príklad stav

$$|\psi\rangle = \left(\frac{|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle}{\sqrt{2}} \right), \quad (2.63)$$

kde jednotlivé qbity postupne ukazujú na stavy Alice, Boba a Carlosa. Matica hustoty ρ_{AB} zodpovedá zmiešanému, klasicky korelovanému, ale neentanglovanému stavu. Pokiaľ ale požiadame o spoluprácu Carlosa, ktorý vykoná merania vo vhodnej báze, môžeme stav $|\psi\rangle$ prerobiť na úplne entanglovaný stav Alice a Boba, ktorý bude separovaný od Carlosovho stavu. Tento stav totiž obsahuje entanglement trojčasticový, ktorý viaže na seba všetky častice dokopy, ale neobsahuje žiaden entanglement dvojčasticový, ktorý by mohli dvaja z trojice získať bez toho, aby tretí spolupracoval.

Priamočiarym spôsobom sa dá táto argumentácia zovšeobecniť aj na viacčasticové systémy. Definujeme preto stavy typu (2.63):

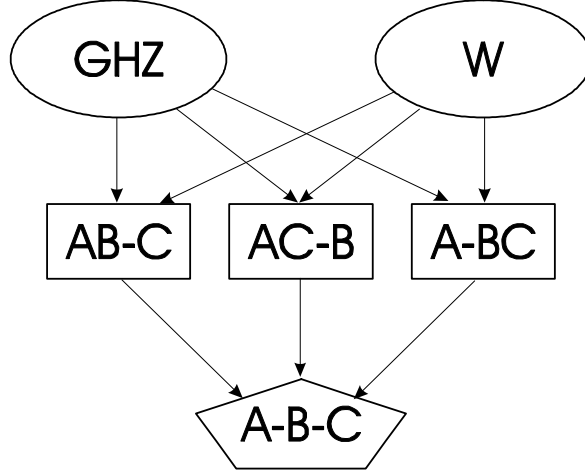
$$|\Phi\rangle_N = \frac{1}{\sqrt{N}} (|0\rangle^{\otimes N} + |1\rangle^{\otimes N}). \quad (2.64)$$

Nazývame ich Greenberger-Horne-Zeilingerove stavy (GHZ stavy) alebo tiež stav zovšeobecnenej Schrödingerovej mačky (Dôvod je prozaický, tento stav skutočne zodpovedá, pre dostatočne veľké N , stavu mačky v uzavretej krabici. Buď je celá živá, alebo celá mŕtva, nič medzi tým). Tieto stavy obsahujú vždy práve N -časticový entanglement, matica hustoty získaná stopou cez ktorúkoľvek časticu zo systému určuje zmiešaný, neentanglovaný stav.

Všeobecný stav N častíc môže obsahovať rôzne druhy entanglementu. Jednak, samozrejme, n -časticový, ale to nie je jediná možnosť. Niektoré dvojice, trojice, alebo k -tice môžu byť entanglované medzi sebou silnejšie ako so zvyškom systému. Napríklad už pri troch časticách nastáva zaujímavá situácia, keď môžeme všetky prípustné stavy rozdeliť do 6 kategórií podľa miery a typu zdieľaného entanglementu. Štyri kategórie sú triviálne, ide o separabilné stavy a stavy, keď sú entanglované vždy len dve z troch častíc systému. Zaujímavý fakt je, že nie všetky stavy, ktoré obsahujú 3-časticový entanglement, môžeme zaradiť do jednej kategórie. Ako je ukázané v článku [22], existujú dve základné kategórie entanglementu. Jedna je reprezentovaná už definovanými GHZ stavmi, druhá Wernerovými stavmi, ktoré sú vo všeobecnosti definované pre N častíc ako stavy symetrické vzhľadom k zámene ľubovoľných dvoch častíc a obsahujúce práve 1 qbit v stave 1 a ostatné v stave 0. V tomto konkrétnom prípade W -stav definujeme ako

$$|W_3\rangle = \frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle). \quad (2.65)$$

Každý stav 3 qbitov patrí do práve jednej z týchto šiestich kategórií v zmysle, že s istou pravdepodobnosťou dokážeme pomocou lokálnych transformácií a klasickej komunikácie tento stav transformovať na typický stav tej-ktorej kategórie (ktorými môžu byť $|W_3\rangle$, $|GHZ_3\rangle$ pre



Obrázok 2.7: 6 množín, do ktorých môžeme jednoznačne rozdeliť všetky stavy troch častíc spinu 1/2. Šípky naznačujú, ktorým smerom sa môžeme medzi množinami pohybovať za pomoci len lokálnych operácií a klasickej komunikácie.

trojčasticový entanglement, $|\Phi^+\rangle|0\rangle$, $|0\rangle|\Phi^+\rangle$ a $|0\rangle_2|\Phi^+\rangle_{13}$ pre dvojčasticový entanglement a nakoniec $|0\rangle|0\rangle|0\rangle$ pre separabilné stavy).

Podstatné je tiež to, že celková miera entanglementu jednej častice a zvyšku je ohraničená, teda ak sa silne viaže na jednu časticu, nemôže byť silne viazaná aj na ďalšie. Uvážme napríklad len zovšeobecnenie z dvoch na tri častice. V článku [19] je ukázané, že ak častice nazveme A, B a C, platí nerovnosť

$$C_{AB}^2 + C_{AC}^2 \leq C_{A(BC)}^2, \quad (2.66)$$

kde C_{AB} značí konkurenciu medzi časticami A a B. Pravá časť nerovnice zodpovedá konkurencii časti A k páru BC, ktorá bude definovaná neskôr. Rozvediem teraz ľavú stranu. Keďže vieme, že stav troch častíc je čistý a matica ρ_{AB} vznikla stopou z matice čistého stavu, matica $\rho_{AB}\tilde{\rho}_{AB}$ (definíciu viď. (2.43)) bude mať maximálne dve nenulové vlastné hodnoty. Potom

$$C_{AB}^2 = (\lambda_1 - \lambda_2)^2 = \lambda_1^2 + \lambda_2^2 - 2\lambda_1\lambda_2 = Sp(\rho_{AB}\tilde{\rho}_{AB}) - 2\lambda_1\lambda_2 \leq Sp(\rho_{AB}\tilde{\rho}_{AB}) \quad (2.67)$$

a celá ľavá strana teda bude

$$C_{AB}^2 + C_{AC}^2 \leq Sp(\rho_{AB}\tilde{\rho}_{AB}) + Sp(\rho_{AC}\tilde{\rho}_{AC}). \quad (2.68)$$

Pravá časť rovnice sa dá zjednodušiť na $4 \det(\rho_A)$. Vieme, že pre čistý stav sa dá konkurencia vyjadriť veľmi jednoducho, $C = 2\sqrt{\det(\rho_A)}$. Ak uvážime, že stav $|\psi\rangle_{ABC}$ je čistý a budeme pokladať pár BC za jeden objekt a nie za dve časti, môžeme definovať $C_{A(BC)}^2$ práve ako $4 \det(\rho_A)$, teda ako konkurenciu časti A k zvyšku systému.

Pokiaľ by stav ρ_{ABC} nebol čistý, môžeme definovať $C_{A(BC)}$ ako minimum cez všetky možné dekompozície matice ρ_{ABC}

$$C_{A(BC)}(\rho) = \min_{\rho=|\psi\rangle_{ABC}\langle\psi|} C_{A(BC)}(|\psi\rangle_{ABC}), \quad (2.69)$$

pričom nerovnosť (2.66) zostáva v platnosti.

2.6.3 Kritériá separability

Ako nutnú podmienku separability môžeme aj pre väčšie systémy používať Peresovu čiastočnú transpozíciu matice hustoty. Avšak už pri troch časticách [8] existujú také stavy, ktoré majú kladnú PPT (stavy s viazaným, čisto viacčasticovým entanglementom). Stále však platí, že PPT je vždy lepšou podmienkou ako Bellove nerovnosti zovšeobecnené pre viac častíc. Inak povedané, každý stav narušajúci Bellove nerovnosti bude mať zápornú PPT.

Ďalšie kritérium predstavuje už nutnú a postačujúcu podmienku pre určenie separability aj viacrozmerných systémov. Jedná sa v podstate o zovšeobecnenie kritéria parciálnej transpozície.

Samotná parciálna transpozícia matice hustoty sa dá chápať ako pozitívne lineárne zobrazenie tejto matice, zachovávajúce stopu. Teda

$$\rho \rightarrow \Lambda(\rho), \quad (2.70)$$

kde Λ má, pri rozdelení na podsystémy A a B, špeciálny tvar

$$\Lambda = \Lambda_A \otimes I_B, \quad (2.71)$$

teda že na podsystéme B pôsobí ako identické zobrazenie. Λ je vždy pozitívne zobrazenie, kompletne pozitívne je ale len vtedy, ak je matica ρ separabilná. Horodecki v článku [9] ukázali, že pre nízkorozmerné systémy práve transpozícia vhodne opisuje všetky prípustné (teda stopu zachovávajúce) zobrazenia, ale pre vyššie rozmery tomu už tak nie je. To zodpovedá situácii, že existujú neseperabilné stavy, ktoré majú splnené PPT (partial transposition) kritérium splnené. Definujeme teda novú požiadavku: chceme, aby nová matica hustoty $\Lambda(\rho)$ spĺňala kritériá na maticu hustoty (kladná definitnosť je jediné netriviálne) pre všetky možné lineárne zobrazenia typu (2.71). Toto kritérium je už aj postačujúcou podmienkou na určenie separability, vyžaduje však obsiahnuť všetky možné lineárne zobrazenia daného typu, čo pre rozsiahlejšie systémy, pre ktoré je toto kritérium stavané, nie je jednoduché. Bližšie v dodatku A.

Pre viacčasticový entanglement musíme znova definovať, čo vlastne znamená separabilný stav. Pokiaľ sa pýtame na separabilitu medzi dvoma časťami systému, zostáva definícia rovnaká ako pre dvojčasticový prípad. Tak isto sú použiteľné už uvedené kritériá, pretože efektívne sa nezaobráame viacčasticovým systémom, ale systémom dvoch častí s viacerými stupňami voľnosti. Nie je zaujímavé, či v časti A máme jeden osemhladinový atóm alebo tri qbity, efektívne je to osemrozmerný systém.

Otázka môže stáť ale aj inak. Ak mám N časticový systém, za akých podmienok ho môžem zapísať v tvare:

$$\rho_{AB\dots M} = \sum_{i=1}^k \rho_A^i \otimes \rho_B^i \otimes \dots \otimes \rho_M^i. \quad (2.72)$$

Intuitívne to znamená, že ľubovoľné dva podsystémy sú separovateľné, ale aj ľubovoľných k systémov medzi sebou je separovateľných. Na to, aby sme mohli použiť už spomenuté kritérium, potrebujeme rozdeliť systém vždy na dve časti, testovať všetky lineárne zobrazenia na kompletnú pozitivitu a pokračovať ďalším možným rozdelením.

2.6.4 Entanglované reťazce

Akýmsi medzistupňom medzi dvojčasticovým a viacčasticovým entanglovaním sú entanglované reťazce. Jedná sa o systém mnohých dvojhladinových častíc, ale entanglement povoľujeme ale len medzi susednými časticami. Vytvárame tak akýsi jednorozmerný reťazec, ktorý môže slúžiť napríklad na transport informácie. V tomto kontexte je zaujímavá napríklad otázka, aký maximálny entanglement môžu mať dve susedné častice v takomto reťazci. Ako vhodnú mieru pre tento problém použijeme konkurenciu. Tu treba zdôrazniť, že vždy počítame len entanglovanosť 2 častíc, pričom ostatné neuvažujeme, a preto je použitie konkurencie úplne legálne.

Zoberme, pre jednoduchosť, nekonečný reťazec, ktorý je uniformný (translačne invariantný; každá z jeho častí je zhodná s ľubovoľnou, rovnako veľkou časťou kdekoľvek inde v reťazci). Pýtame sa teraz, aká maximálna konkurencia môže byť v tomto prípade medzi každými dvoma susedmi. Prvý horný odhad je, samozrejme, 1, čo by znamenalo maximálnu entanglovanosť. Ako ale bolo ukázané, suma druhých mocnín konkurencií danej častice k iným časticiam je ohraničená zovšeobecnenou konkurenciou tejto častice k zvyšku systému, čo nám ohraničuje maximálnu prípustnú hodnotu na $C_{\max} = 1/\sqrt{2}$. Ani táto hodnota ale nie je dosiahnuteľná.

Príklad entanglovaného reťazca sa dá vytvoriť veľmi jednoducho. Zoberme na začiatok stav (nekonečného počtu qbitov)

$$|\Phi\rangle = \dots \otimes \left(\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \right) \otimes \dots \quad (2.73)$$

V tomto stave je každý z qbitov maximálne entanglovaný s jedným zo svojich susedov. Tento stav nie je ale translačne invariantný vzhľadom na posun o nepárny počet pozícií. Problém sa dá vyriešiť veľmi jednoducho: zoberieme ďalší stav $|\Psi\rangle$, ktorý vznikne z $|\Phi\rangle$ posunutím o jednu pozíciu (doprava či doľava). Výsledný stav, ktorý vznikne ako lineárna kombinácia

$$\frac{|\Phi\rangle + |\Psi\rangle}{\sqrt{2}} \quad (2.74)$$

už spĺňa podmienku translačnej invariantnosti. Je tiež dobrý predpoklad, že susedné qbity budú entanglované, keďže niektoré boli entanglované v jednom, iné v druhom zo stavov $|\Psi\rangle, |\Phi\rangle$. Nie je problém entanglement spočítať: matica hustoty stavu $|\Phi\rangle$, zredukovaná len na dva qbity na pozíciách jedna a dva bude:

$$\rho^\Phi = \begin{pmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix} \quad (2.75)$$

a matica hustoty stavu $|\Psi\rangle$

$$\rho^\Psi = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (2.76)$$

Matica hustoty lineárnej kombinácie bude

$$\frac{\rho^\Psi + \rho^\Phi}{2} = \begin{pmatrix} \frac{1}{8} & 0 & 0 & 0 \\ 0 & \frac{3}{8} & -\frac{1}{4} & 0 \\ 0 & -\frac{1}{4} & \frac{3}{8} & 0 \\ 0 & 0 & 0 & \frac{1}{8} \end{pmatrix}. \quad (2.77)$$

Teraz už veľmi jednoducho spočítame konkurenciu priamo z definície, príslušné odmocniny vlastných hodnôt vyjdú $\frac{5}{8}, \frac{1}{8}, \frac{1}{8}, \frac{1}{8}$ a výsledná konkurencia je $C = \frac{1}{4}$. To je ešte ďaleko od horného odhadu uvedeného vyššie. Podľa článku [16] ale za žiadnych podmienok nie je možné hornú hranicu dosiahnuť, čo je veľmi zaujímavý poznatok. Pri istých, rozumne odôvodnených podmienkach na matice hustoty prípustných stavov, týkajúcich sa množstva qbitov v stave 1 a ich pozícií, dostaneme maximum pre konkurenciu

$$C_{\max} \cong 0.4345, \quad (2.78)$$

čo zodpovedá entanglementu formácie približne 0.285 entanglovaných bitov.

2.6.5 Entanglované molekuly

Je intuitívne jasné, že spomínané entanglované reťazce popisujú iba malú časť viacčasticových systémov, ktoré sú neseparabilné. Je prirodzené pripustiť, že každá časť systému (častica) môže byť viazaná s ktoroukoľvek ďalšou časťou systému, prípadne aspoň z nejakej časti podsystemu. Pojem molekula bol zavedený v článku [20] ako reakcia na zavedenie entanglovaných reťazcov vo Wothersovom článku.

V systéme zloženom z N častíc máme $N(N-1)/2$ rôznych dvojíc, a teda toľko isto matíc hustoty redukovaných na dve častice, ktoré môžu byť separabilné alebo entanglované. Pokiaľ je niektorý stav ρ_{kl} entanglovaný, znamená to, že entanglement z neho sa dá vydestilovať, lokálnymi operáciami prerobiť na entanglement čistého stavu 2 qbitov. (V tejto, podobne ako v predchádzajúcej časti neuvažujeme viazaný, viacčasticový entanglement). Dokážeme vytvoriť taký stav, aby entanglement každej dvojice bol práve nejaký, dopredu daný?

Odpoveď je: áno, za podmienky, že celkový požadovaný entanglement nie je väčší ako istá hranica. Označme teda C_{kl} požadované konkurencie medzi časťami k a l systému. Zavedme ďalej stav

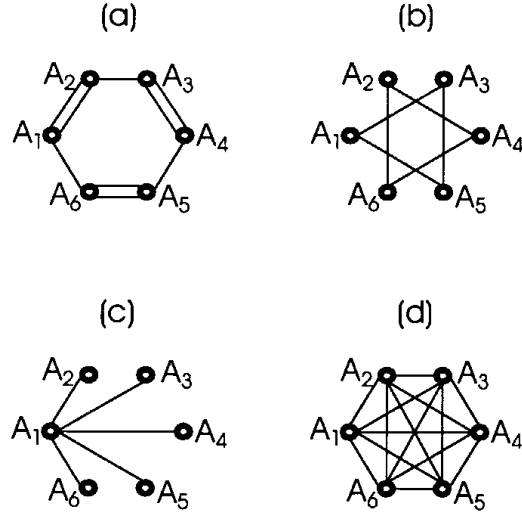
$$|\psi\rangle_{ij} = |\psi^+\rangle_{ij} \otimes |00\dots 00\rangle_{\text{zvyšok}}, \quad (2.79)$$

kde $|\psi^+\rangle_{ij}$ je maximálne entanglovaný stav častíc i a j . Pomocou týchto stavov zavedieme maticu hustoty

$$\begin{aligned} \rho &= \frac{p}{M} x_{kl} |\psi\rangle_{ij} \langle\psi|_{ij} + (1-p) \rho_{sep} \\ M &= \sum_{k<l} x_{kl}, \end{aligned} \quad (2.80)$$

kde ρ_{sep} je akási, plne separabilná matica hustoty a $p \in \langle 0, 1 \rangle$. Po urobení stopy cez všetky častice okrem i, j dostaneme maticu

$$\rho_{ij} = \frac{p}{M} \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & x_{ij}/2 & 0 \\ 0 & x_{ij}/2 & c & 0 \\ 0 & 0 & 0 & d \end{pmatrix} \quad (2.81)$$



Obrázok 2.8: Niekoľko príkladov entanglovania pre molekuly zložené zo 6 častíc. V prípade a) uvažujeme väzbu vždy len medzi susednými časticami, pričom dvoma čiarkami je naznačená silnejšia väzba. Prípad b) znázorňuje nezávislé entanglovanie 3 a 3 častíc, prípad c) zasa väzbu všetkých častíc len s jednou. Konečne d) zobrazuje väzbu medzi všetkými časticami navzájom.

a z nej konkurenciu

$$C_{ij} = p \frac{x_{ij}}{M}. \quad (2.82)$$

Vhodnou zmenou x_{ij} vieme dosiahnuť žiadané pomery medzi konkurenciami jednotlivých dvojíc za každých okolností. Na dosiahnutie požadovanej veľkosti musíme meniť parameter p . Pokiaľ bude menší ako 1, konfigurácia sa dá dosiahnuť a máme aj spôsob, ako to urobiť. Pokiaľ dostaneme $p > 1$, matica z definície (2.80) už nebude kladne definitná. Nedá sa povedať, že sa konfigurácia dosiahnuť nedá, nejde to ale týmto spôsobom.

Maximálnu konkurenciu dosahujeme, pochopiteľne, ak $p = 1$. Vtedy, ak požadujeme rovnakú konkurenciu medzi všetkými dvojicami, vyjde $C_{ij} = \frac{2}{N(N-1)}$. Ukážeme, že toto nie je maximálna možná hodnota pre danú konfiguráciu.

Zoberme stav

$$|W_N\rangle = 1/\sqrt{N}|N-1, 1\rangle, \quad (2.83)$$

čo je symetrizovaný stav N častíc s $N-1$ časticami v stave 0 a jednou časticou v stave 1. Konkurencia každej dvojice v takomto stave je rovnaká a rovná $C_{ij} = \frac{2}{N}$, teda zvlášť pre veľké N sa ukazuje všeobecný algoritmus ako veľmi neefektívny.

Zameriame sa teraz na trochu inú, ale nie menej zaujímavú konfiguráciu. Ak máme k dispozícii N -časticový systém a žiadame, aby prvá častica bola rovnako entanglovaná so všetkými ostatnými, aká je maximálna miera tohoto entanglementu? Ako už bolo spomínané, vďaka nerovnosti $C_{AB}^2 + C_{AC}^2 \leq C_{A(BC)}^2$, ak požadujeme $C_{AB} = C_{AC}$, pre systém aspoň troch častíc je táto konkurencia ohraničená hodnotou $1/\sqrt{2}$. V článku [19] je tiež domnienka, že podobná nerovnosť platí aj pre viacčasticové systémy, čo by posúvalo hranicu prípustnej konkurencie

až na $1/\sqrt{N-1}$. Pritom ale stav

$$|\psi\rangle = \frac{1}{\sqrt{2}}|1\rangle|00\dots 0\rangle + \frac{1}{\sqrt{2(N-1)}}|0\rangle|N-2, 1\rangle \quad (2.84)$$

napĺňa tento horný limit.

V článku [25] je ukázaný dôkaz, že pre entanglované molekuly typu d) (viď. obrázok 2.8) je hranica konkurencie pre každé dve susediace časti práve $\frac{2}{N}$. Dokázaná, avšak dosiaľ nepublikovaná bola aj citovaná domnienka, že pri molekulách typu c) je hranica konkurencie práve na $1/\sqrt{N-1}$.

2.6.6 Miery viacčasticového entanglementu

V prípade viacčasticového stavu je definícia miery ešte komplikovanejšia ako v prípade dvojčasticovom. Musíme v nej zohľadniť entanglement medzi jednotlivými dvojicami stavov, ale aj čistý viacčasticový entanglement. Miera teda nemôže byť jednoduchá funkcia, musí obsahovať v sebe ďaleko viac.

Ako akýsi horný limit, čo všetko musí byť dané, môžeme zobrať určenie miery entanglementu medzi všetkými možnými rozdeleniami častíc, ktoré máme k dispozícii. V tomto prípade ale zadávame množstvá redundantnej informácie.

Zaujímavá miera je navrhovaná v článku [21]. Je to zovšeobecnená Schmidtova miera, pre zmiešané stavy definovaná nasledovne:

$$P(\rho) = \min \sum_i \lambda_i P(|\psi_i\rangle\langle\psi_i|), \quad (2.85)$$

kde minimum je brané cez všetky dekompozície $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$ a miera P na čistých stavoch je

$$\begin{aligned} P(|\psi\rangle\langle\psi|) &= \log_2 r \\ r &= \min R \\ |\psi\rangle &= \sum_{i=1}^R \alpha_i |\psi_1^{(i)}\rangle \otimes \dots \otimes |\psi_N^{(i)}\rangle. \end{aligned} \quad (2.86)$$

Dôležité je, že dekompozícia stavu podľa (2.86) sa chápe len v zmysle častí systému, vzhľadom na ktoré hľadáme entanglement. Pokiaľ máme napríklad systém zložený zo štyroch častí, ale pýtame sa na entanglement skupiny prvých troch vzhľadom na štvrtú, $|\psi_1\rangle$ bude určovať trojčasticový stav a $|\psi_2\rangle$ stav jednočasticový. Na druhej strane, ak nás zaujíma entanglement všetkých štyroch častí navzájom, $|\psi_1\rangle$ až $|\psi_4\rangle$ určujú jednočasticové stavy.

Istou nevýhodou miery P je, že je definovaná pomocou dvojnásobnej minimalizácie (raz hľadáme minimálny počet členov rozkladu čistého stavu, druhýkrát minimum cez všetky možné rozklady). Napriek tomu sa dá spočítať pre mnohé stavy explicitne.

Uvedme teraz tri príklady. Spočítame entanglement rôznych kombinácií rozdelenia systému štyroch častíc v rôznych stavoch. Stavy, ktoré uvažujeme sú:

1. GHZ stav v tvare $|GHZ\rangle_4 = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$

	$ GHZ\rangle_4$	$ W\rangle_4$	$ \phi\rangle_4$	$ \phi^+\rangle \phi^+\rangle$
$A - B - C - D$	1	2	2	2
$AB - C - D$	1	$\log_2 3$	1	1
$AB - CD$	1	1	1	0
$AC - BD$	1	1	2	2
$ABC - D$	1	1	1	1

Tabuľka 2.1: Miera entanglementu rôznych štvorčasticových čistých stavov v závislosti od rozdelenia podsystémov. Stav GHZ má pre všetky rozdelenia entanglement rovnaký, lebo obsahuje len 4-časticový entanglement, naproti tomu u ostatných stavov je výsledok od rozdelenia závislý.

2. W stav v tvare $|W\rangle_4 = \frac{1}{2} (|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$
3. Stav $|\phi\rangle_4 = \frac{1}{2} (|0001\rangle + |0011\rangle + |1100\rangle - |1111\rangle)$
4. Stav získaný z dvoch kópií maximálne entanglovaného stavu dvoch častíc $|\phi^+\rangle|\phi^+\rangle = \frac{1}{2} (|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle)$

Výsledky pre všetky stavy a pre 4 rôzne kombinácie delenia (každá častica samostatne, dvojica AB a zvyšok samostatne, dvojica AB proti CD, dvojica AC proti BD a nakoniec častica D oproti zvyšku) sú uvedené v tabuľke (2.1). Je vidieť, že miera reprodukuje intuitívne očakávania. Pre GHZ stav očakávame rovnaký entanglement pre ľubovoľné delenie, lebo obsahuje iba čisto štvorčasticový entanglement. Naopak, stav $|\phi^+\rangle|\phi^+\rangle$ má najväčší entanglement pri delení AC-BD, ktoré je výhodné, lebo práve takto je entanglement nie v rámci jednej skupiny, ale medzi skupinami.

Všetky spomínané stavy boli čisté. Na druhom príklade ukážem použitie miery na zmiešaných stavoch. Využijem Wernerov stav ρ definovaný v (2.34). V tomto prípade dáva miera nezávisle od zvolenej dekompozície hodnotu

$$P(\rho) = \begin{cases} \frac{3}{2}x - \frac{1}{2} & \text{pre } \frac{1}{3} < x \leq 1 \\ 0 & \text{pre } 0 \leq x \leq \frac{1}{3}, \end{cases} \quad (2.87)$$

čo je v plnom súlade s výsledkom uvedeným v kapitole o dvojčasticovom entanglemente, teda že pre $x < \frac{1}{3}$ je stav ρ separabilný a inak entanglovaný.

Tretí príklad uvažuje trojčasticový systém a dva zmiešané stavy, jednak kombináciu GHZ stavu a nulového stavu v tvare

$$\rho_G(\lambda) = \lambda|GHZ\rangle_3\langle GHZ|_3 + (1 - \lambda)|000\rangle\langle 000| \quad (2.88)$$

a zložitejší stav v tvare

$$\rho(\lambda, \mu) = \lambda|\phi^+\rangle_{12}|0\rangle_3\langle 0|_3\langle\phi^+|_{12} \quad (2.89)$$

$$+ \mu|\phi^+\rangle_{23}|0\rangle_1\langle 0|_1\langle\phi^+|_{23} \quad (2.90)$$

$$+ (1 - \lambda - \mu)|\phi^+\rangle_{13}|0\rangle_2\langle 0|_2\langle\phi^+|_{13}. \quad (2.91)$$

Výsledky pre tieto stavy sú uvedené v tabuľke (2.2). Znova sa dá povedať, že sme dostali

	$\rho_G(\lambda)$	$\rho(\lambda, \mu)$
A-B-C	λ	1
AB-C	λ	$1 - \lambda$
AC-B	λ	$\lambda + \mu$
A-BC	λ	$1 - \mu$

Tabuľka 2.2: Miera entanglementu rôznych trojčasticových zmiešaných stavov v závislosti od rozdelenia podsystémov. Znova stav obsahujúci GHZ je nezávislý od rozdelenia, stav obsahujúci len dvojčasticový entanglement od rozdelenia silne závisí.

to, čo očakávame. V prvom prípade, keďže v hre je čistý trojčasticový entanglement, je v poriadku, ak výsledok nezávisí od voľby skupín. V druhom, naopak, máme kombináciu dvojčasticovo entanglovaných stavov, pričom entanglement medzi každými dvojicami je vyjadrený koeficientami μ, λ a ich doplnkom do jednotky. Pri entanglemente dvojice častíc oproti tretej (napr. AB-C) je pochopiteľné, že dostaneme súčet entanglementu A-C a B-C.

2.6.7 Experimentálne potvrdenie

V posledných rokoch sa experimenty zamerali na tvorenie stavov z viacerých ako dvoch častíc, ktoré by porušovali očakávania klasickej fyziky. Stav troch fotónov v GHZ entanglovanom stave sa podarilo vytvoriť A. Zeilingerovi et. al. [14]. Schéma jeho aparatury je na obrázku (2.9). Pri pokuse používal Ti-zafírový laser so zdvojenou frekvenciou, ktorý produkoval fotóny na vlnovej dĺžke 394 nm v extrémne krátkych pulzoch trvajúcich okolo 200 fs . S pravdepodobnosťou na úrovni 0.1% vznikne v laseri pár fotónov v stave

$$\frac{1}{\sqrt{2}} (|H\rangle_a |V\rangle_b - |V\rangle_a |H\rangle_b), \quad (2.92)$$

kde písmená H, V označujú smery polarizácie a a, b prvý a druhý fotón z páru. S veľmi nízkou pravdepodobnosťou však môžu vzniknúť až dva páry takýchto fotónov, pričom každý pár bude rozdelený tak, že jeden člen pôjde ramenom a a druhý ramenom b . Za vhodných okolností sa môže stať, že v každom z detektorov T, D_1, D_2, D_3 bude v rovnakom čase zaznamenaný jeden impulz (z dôvodu požiadavky nemožnosti rozlíšenia časov oboch dvojíc fotónov je detekčný čas umelo predĺžovaný). Ak si odmyslíme fotón z detektora T , ktorého meranie vlastne umožnilo vznik trojice entanglovaných fotónov, sú dve možnosti, v akom stave mohli fotóny prísť do detektorov. Jedna možnosť je, že pôvodný pár k fotónu detekovanému v T je fotón detekovaný v D_3 a zvyšný pár prešiel do detektorov D_1, D_2 . V tomto prípade museli byť fotóny v stave

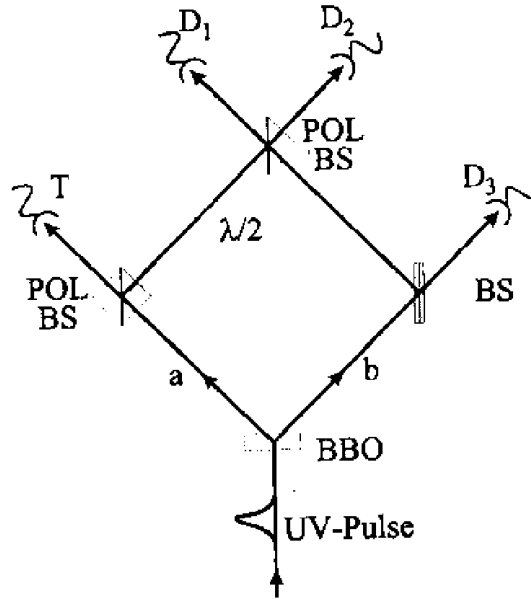
$$|H\rangle_1 |H\rangle_2 |V\rangle_3. \quad (2.93)$$

Iná možnosť je, že pár k T fotónu bol detekovaný v D_2 a zvyšný pár v D_1, D_3 . Vtedy sú (boli pred detekciou) fotóny v stave

$$|V\rangle_1 |V\rangle_2 |H\rangle_3. \quad (2.94)$$

Keďže nepresnou detekciou času impulzu nevieme zistiť, fotón z ktorého páru spôsobil príslušný impulz, môžeme predpokladať, že fotóny sa nachádzali vo zviazanom stave

$$\frac{1}{\sqrt{2}} (|H\rangle_1 |H\rangle_2 |V\rangle_3 + |V\rangle_1 |V\rangle_2 |H\rangle_3). \quad (2.95)$$



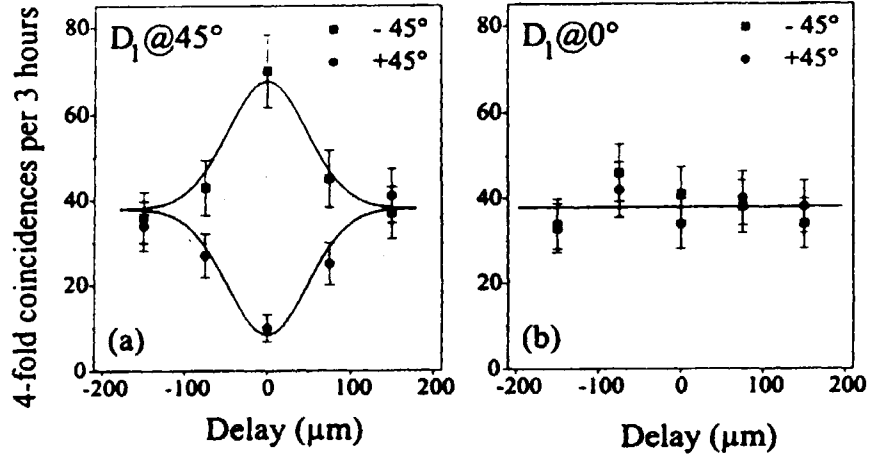
Obrázok 2.9: Schéma aparatury použitej pri pokuse, pri ktorom vznikali trojčasticové entanglované stavy. Extrémne krátky pulz UV lasera prechádza cez nelineárny kryštál (BBO), kde sa rozdeľuje na dve časti. Polarizačné zrkadlá (POL BS) odrážajú vertikálne polarizované fotóny, ale prepúšťajú horizontálne. BS odráža, nezávisle od polarizácie, s pravdepodobnosťou 50% a prepúšťa tiež s pravdepodobnosťou 50%. V ramene a je umiestnená polvlnná platnička.

Ešte je ale potrebné ukázať, že sa nejedná len o štatistickú zmes týchto stavov, ale naozaj je každý jeden stav entanglovaný. Ak vložíme pred detektory ešte polarizačné filtre, môžeme sledovať, ako sa mení množstvo nameraných 4-fotónových prípadov v závislosti od otočenia polarizátora a časového rozdielu v meraní fotónov. V prípade, že detekujeme v detektore D_1 pod uhlom 45° , pri nízkych časových rozdieloch sa ukazuje významný rozdiel medzi množstvom stavov detekovaných v prípade, ak je polarizátor pred detektorom D_3 nastavený pod uhlom 45° a -45° (obrázok 2.10). V ideálnom prípade pre nulový rozdiel by sme očakávali detekciu len v prípade nastavenia filtra pod uhlom -45° . Stav (2.95) totiž prejde, ak uvážime len stavy prvého a tretieho fotónu a meranie na polarizačnom filtri prvého detektora, do stavu

$$\frac{1}{\sqrt{2}} (|45\rangle_1 - |45\rangle_3), \quad (2.96)$$

a teda neobsahuje žiaden člen s polarizáciou -45° na detektore D_3 . Pre väčšie časové rozdiely sa fotóny stávajú rozlíšiteľnými a interferencia sa stráca.

V tomto pokuse sa podarilo vyrobiť stav troch fotónov, ktoré boli navzájom entanglované. Problémom zostáva, že pravdepodobnosť ich vzniku je extrémne nízka (aj pri vysokej kadencii lasera 7.6×10^7 krát za sekundu vieme produkovať podobné trojice len približne raz za 150 sekúnd) a to, že vznikli, môžeme vlastne zistiť len tak, že trojicu zničíme.



Obrázok 2.10: Overenie, že pri pokusoch s trojčasticovým entanglementom sa skutočne jedná o entanglované stavy a nie štatistické zmesy. Graf vľavo ukazuje, že je jasne pozorovateľná závislosť množstva detekovaných prípadov od času podľa toho, ako je nastavený polarizačný filter pri detektore D_3 . Graf na pravej strane ukazuje, že ak zmeníme nastavenie polarizačného filtra na D_1 , závislosť od nastavenia filtrov na D_3 sa podľa očakávania stratí. Grafy pochádzajú z článku [14].

2.7 Entanglement viacrozmerých systémov

Doteraz sme sa zaoberali iba systémami, ktoré boli zložené z dvoch alebo viacerých qbitov. Pod qbitmi rozumieme časti systému, ktoré sa môžu nachádzať iba v dvoch rôznych rozlíšiteľných stavoch (a pochopiteľne, keďže pracujeme s kvantovými systémami, aj v ich ľubovoľnej superpozícii). Je vcelku pochopiteľné, že väčšina pozornosti sa venuje práve týmto systémom. Svojou jednoduchosťou umožňujú mnohé veci a javy rozobrať ďaleko podrobnejšie, ako sa to podarí pri viacrozmerých systémoch. Klasické počítače tiež pracujú s bitmi a nie vyššími jednotkami a experimentálna realizácia qbitov je omnoho jednoduchšia ako akýchkoľvek iných systémov. Máme totiž k dispozícii dve elementárne častice, ktoré sa vo svojej podstate správajú ako qbity: fotón s jeho polarizáciou a elektrón so spinom $\frac{1}{2}$.

Napriek všetkému ale stojí za to, aby sme sa aspoň v stručnosti venovali viacrozmerým systémom, ktoré budeme v ďalšom nazývať *qdit*. Qdit je systém, ktorý sa môže nachádzať v istom, dopredu definovanom počte rôznych rozlíšiteľných stavov $1 \dots N$. Samozrejme, okrem toho sa môže nachádzať aj v ľubovoľnej superpozícii týchto stavov. Dá sa zapísať ako

$$|\Phi\rangle = \sum_{i=1}^N a_i |i\rangle \quad (2.97)$$

za podmienky normovania

$$\sum_{i=1}^N a_i^2 = 1. \quad (2.98)$$

V experimentoch sa dajú napríklad použiť atómy, ktoré majú viac stabilných hladín, medzi ktorými môžeme prechádzať vhodnými impluzami laserov.

2.7.1 Dva qdity rozmeru N

Podobne ako pri qbitoch, aj tu začneme jednoduchými systémami skladajúcimi sa len z dvoch častíc. Pre uľahčenie niektorých definícií tiež predpokladáme, že oba systémy majú rovnaký rozmer N . Zavedieme maximálne entanglovaný stav, ekvivalent GHZ stavu pre qbity

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle \otimes |i\rangle. \quad (2.99)$$

Zoberme teraz maticu hustoty nejakého stavu, ktorá je zložená z dvoch častí. Jednak z maximálne zmiešaného stavu reprezentovaného jednotkovou maticou, a jednak z časti maximálne entanglovanej:

$$\rho = (1 - \varepsilon)I + \varepsilon|\Psi\rangle\langle\Psi|. \quad (2.100)$$

Snažíme sa skúmať, za akých podmienok je táto matica separabilná a kedy je entanglovaná. Očakávame, že pre $N = 2$ by sme mali dostať podmienku $\varepsilon > \frac{1}{3}$. V článku [33] sa pomocou vhodnej zmeny bázy na dvojčasticovom priestore ukazuje, že všeobecná podmienka je

$$\varepsilon > \frac{1}{1 + N}, \quad (2.101)$$

čo je v plnej zhode s očakávaniami. Zaujímavé je, že so zväčšujúcim sa rozmerom systému sa znižuje podiel maximálne entanglovaného stavu potrebný na to, aby bol výsledný stav entanglovaný.

2.7.2 Spojité premenné

Druhým extrémom oproti dvojhľadinovým systémom - qbitom je situácia, keď uvažujeme vysokorozmerné systémy v limite $N \rightarrow \infty$ alebo dokonca prechádzame od diskretných premenných k spojitým. V istom zmysle sa uzatvára kruh, ktorý sa začal článkom Einsteina, Podolskeho a Rosena [1]. Tu sa ukazoval paradox na systéme dvoch častíc so spojitým spektrom vlastných stavov polohy a hybnosti. Potom sa ale z dôvodov jednoduchosti prešlo k systémom diskretným.

Pri spojitých systémoch sa stretávame so všetkými problémami známymi už zo základov klasickej mechaniky. Sumy sú nahrádzané integrálmi, stavy sú normované na delta-funkciu namiesto jednotky alebo sa spojité premenné umelo diskretizujú (napríklad obmedzením na konečný objem sa dosiahne diskkrétne spektrum v hybnosti). Napriek týmto problémom bolo vypracovaných niekoľko použití kvantových systémov so spojitými parametrami. V článku [34] je rozobraná možnosť teleportovať jeden mód elektromagnetického poľa za použitia podobných techník ako pri qbitoch (podrobnejšie sú popísané v nasledujúcej sekcii). Článok [35] sa zasa podrobne venuje možnostiam klonovania systémov. Ukazuje sa, že mechanizmus pre optimálne klonovanie je všeobecný a funguje rovnako dobre pre nízkorozmerné ako pre vysokorozmerné systémy. Okrem toho, zariadenia pracujúce pri vysokých rozmeroch sa veľmi podobajú na klasické, čo sa v zmysle klasickej limity dalo očakávať.

2.8 Využitie entanglementu

2.8.1 Husté kódovanie

Keď sa ukázalo, že zákony kvantovej mechaniky aplikované na časticách spinu $1/2$ dávajú veľmi zaujímavé výsledky, otvorila sa aj otázka, ako by sa dali využiť. Jednou z možných oblastí je komunikácia.

Veľmi zaujímavou výzvou pre ďalšie skúmanie bolo, či by nebolo možné posielaním kvantovej informácie namiesto klasickej dosiahnuť vyššiu kapacitu linky. To znamená, že pomocou jednej poslanej častice spinu $1/2$ by sme dokázali zaslať viac ako očakávaný 1 bit informácie (Zaslanie práve jedného bitu je triviálne, posielam častice pripravené vo vlastnom stave operátora spinu na os z a na príjme ich znova projektujem na tú istú os. S istotou, odhliadnuc od možných chýb, dostávam výsledok $\pm 1/2$, podľa toho, ako som častice pripravil). Veď samotná orientácia spinu v sebe skrýva dva spojité parametre. V roku 1973 ale bolo dokázané [28], že nijakým špeciálnym spôsobom prípravy a merania častíc na výstupe a vstupe nemôžeme dosiahnuť väčšiu priepustnosť ako v klasickej príhode.

Iná je situácia, ak pripustíme, že na posielanie informácie sa môžeme dopredu pripraviť. Túto situáciu rozpracovali Ch. Bennett a S. Wiesner v článku [23]. Predstavme si dva subjekty, ktoré potrebujú komunikovať, Alicu a Boba. Keď sa niekedy stretnú, dohodnú sa a pripraví sa do zásoby množstvo dvojčasticových systémov v stave

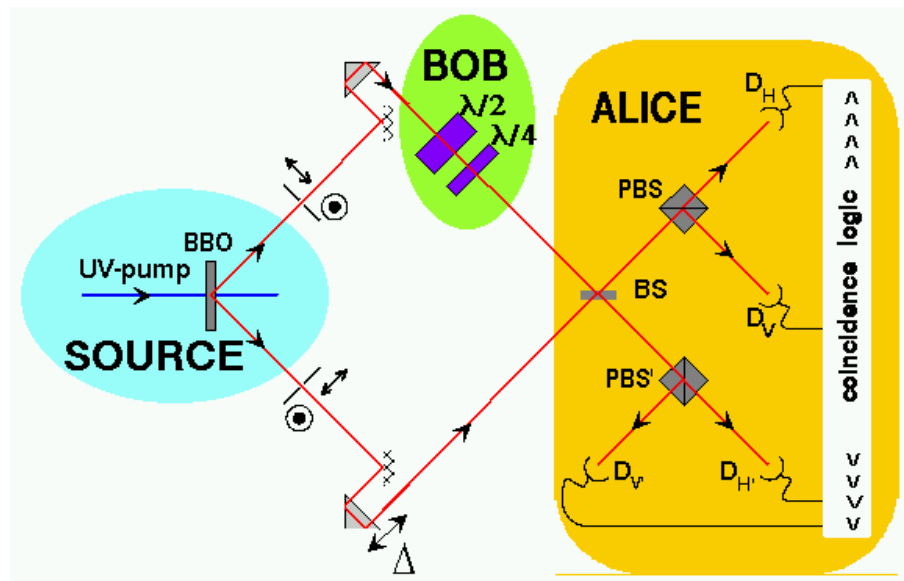
$$|\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle). \quad (2.102)$$

Kým sa rozídu, Alica si zoberie z každého systému jednu časticu a Bob druhú. V prípade, že bude Alica potrebovať poslať informáciu Bobovi, môže to urobiť veľmi efektívne. Zoberie svoju časticu zo spoločného páru, prevedie na nej jednu z možných operácií:

$$I, \sigma_x, \sigma_y, \sigma_z \quad (2.103)$$

a pod vplyvom týchto operácií sa stav buď zachová (v prvom prípade), alebo zmení na jeden z troch ortogonálnych stavov z Bellovej bázy. Ak Alica takto upravenú časticu pošle Bobovi, ten bude mať k dispozícii (spolu so svojou časticou) celý systém a bude môcť zistiť (znovu odhliadnuc od možných chýb) nad akúkoľvek pochybnosť, v ktorom zo štyroch stavov sa nachádza. Alica teda zaslaním jednej častice (jedného qbitu) dokázala Bobovi doručiť informáciu ekvivalentnú dvom bitom.

Husté kódovanie teda dokáže (s tým, že vyžaduje prípravu stavov dopredu) pomocou jedného kvantového bitu zabezpečiť zaslanie dvoch klasických bitov informácie. To však nie je všetko. Husté kódovanie zároveň zabezpečuje bezpečnosť prenášaného signálu. Samotná častica posielaná od Alice k Bobovi totiž nenesie v sebe žiadnu informáciu. Ak nemáme k dispozícii Bobovu časť, z nášho pohľadu sa vo všetkých 4 možných prípadoch častica nachádza v zmiešanom stave $\rho = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a nemáme žiadnu možnosť informáciu z nej získať. Inak povedané, celá zasielaná informácia je práve v entanglemente medzi oboma časticami a nie v častici samotnej.



Obrázok 2.11: Schéma skutočnej aparatúry tak, ako bola použitá v laboratóriách v Innsbrucku. Zdroj vyrába entanglované páry fotónov, z ktorých jeden ide priamo k Alici a druhý ide cez iné zariadenie, Boba. Ten, podľa toho, ktorú zo štyroch možných správ chce poslať, aplikuje jednu z možných 4 kombinácií polvlnovej a štvrtvlnovej platničky (žiadnu, obe alebo jednu z nich). Alica potom meria vo svojom zariadení, v akom stave pár prichádza. Dokáže pritom rozlíšiť len tri druhy stavov, dve z možností dávajú rovnaké interferenčné krivky. Efektívne toto zariadenie teda dokáže pomocou jedného qbitu preneseného medzi Bobom a Alicou preniesť cca. 1.58 bitu informácie. Konkrétne to bolo testované na prenášaní ASCII znakov, keď sa na prenesenie miesto 8 bitov použilo len 5 entanglovaných párov.

2.8.2 Výmena kvantových EPR kľúčov

Táto metóda, prvýkrát navrhnutá Ekertom v roku 1991 [29], je určená nie na samotnú komunikáciu, ale na prípravu komunikácie pomocou klasického kanála, ktorá bude tajná. Na to potrebujeme mať k dispozícii kód, ktorý nebude okrem nás poznať nikto iný. A práve pomocou entanglovaných stavov si môžeme takýto kód pripraviť.

Znova predpokladáme, že obaja účastníci zdieľajú časť systému, ktorý je tentokrát v stave

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle). \quad (2.104)$$

Na to, aby vytvorili kód dĺžky N bitov potrebujú mať k dispozícii približne $2N$ takýchto stavov. Obaja vykonajú na svojich častiach systému merania spinu v smere osi x alebo z , pričom to, ktoré meranie to bude, vyberú náhodne, obe s rovnakou pravdepodobnosťou. Potom jeden druhému oznámi, či to-ktoré meranie urobili v smere osi x alebo osi z .

Pre dostatočne veľké N bude pri približne polovici týchto systémov meranie rovnaké, teda obaja merali v smere tej istej osi. V týchto prípadoch vedia, že výsledky sú úplne antikorelované, teda ak Alica namerala spin hore, Bob ho namerlal určite smerom dole. Ak si zostavia úspešné pokusy za sebou a Alica si zapíše za každý nameraný spin hore 1 a spin dole 0 a Bob opačne, budú mať k dispozícii kód, ktorý je pre všetkých okolitých pozorovateľov tajný. Tí vidia len to, v akých smeroch boli merané spiny, nevedia už, aké výsledky Alica či Bob dosiahli.

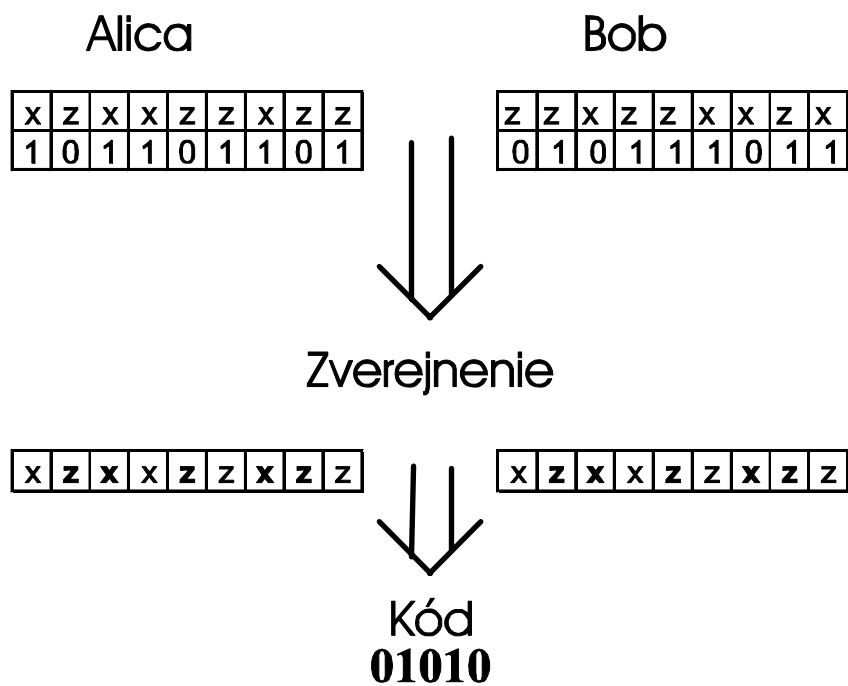
Keď máme k dispozícii tento kód, môžeme komunikovať klasickým kanálom bez možnosti, že by nás niekto mohol odpočúvať. Jednoducho, ku každému zasielanému bitu informácie pripočítame modulo dva bit tajného kódu. Takto posielame verejnú informáciu, ktorá je bez kódu úplne bezcenná, avšak s kódom z nej Bob dokáže zasa bez problémov, opätovným pričítaním modulo dva, získať pôvodnú tajnú informáciu. Táto metóda však nedokáže zabrániť vonkajšiemu zásahu do zasielanej verejnej informácie.

2.8.3 Kvantová teleportácia

V prípade využitia entanglementu pre husté kódovanie sme dokázali pomocou transportu kvantovej informácie a využitia kvantového kanála transportovať veľmi efektívnym spôsobom klasickú informáciu. Kvantová teleportácia hovorí o opačnom procese: tu dokážeme pomocou párov entanglovaných častíc a transportu klasickej informácie transportovať kvantovú informáciu.

Prepraviť qbit pomocou klasického kanála sa zdá byť na prvý pohľad nemožné. Jednak, ak máme k dispozícii len jednu kópiu stavu, nemôžeme ju zmerať a ani nijak inak z nej vyextrahovať všetky potrebné informácie na klasickej úrovni, aby sme vedeli stav na druhej strane, u Boba, vytvoriť. Keby sme aj mali potrebné informácie, mali by sme problém, ako pomocou diskretných jednotiek (bitov) zaslať spojité parametre. Entanglement nám pomôže vyriešiť oba problémy.

Je jasné, že Alica, ktorá sa bude snažiť prepraviť qbit $|\psi_C\rangle$ k Bobovi, na ňom nesmie prevádzať žiadne priame merania, inak by zákonite stratila aspoň časť informácie. Iná je však situácia, ak má Alica k dispozícii ešte svoju časť entanglovaného páru, ktorý je v stave $|\phi^+\rangle$. Môže na dvojici qbitov $|\psi_C\rangle$ a $|\phi^+\rangle_A$ urobiť kolektívne Bellove meranie, ktoré ich sprojektuje do jedného zo štyroch možných, maximálne entanglovaných Bellových stavov $|\psi^\pm\rangle, |\phi^\pm\rangle$.



Obrázok 2.12: Postup pri vytváraní EPR kľúča. Alica aj Bob náhodne vykonajú merania. Potom zverejnia smery, v ktorých meranie prebehlo a na základe toho vedia, v ktorých prípadoch získali použiteľné informácie (vyznačené hrubou). Bob vymení svoje čísla za opačné a obaja majú k dispozícii rovnaký, ale pre iného neznámy kód.

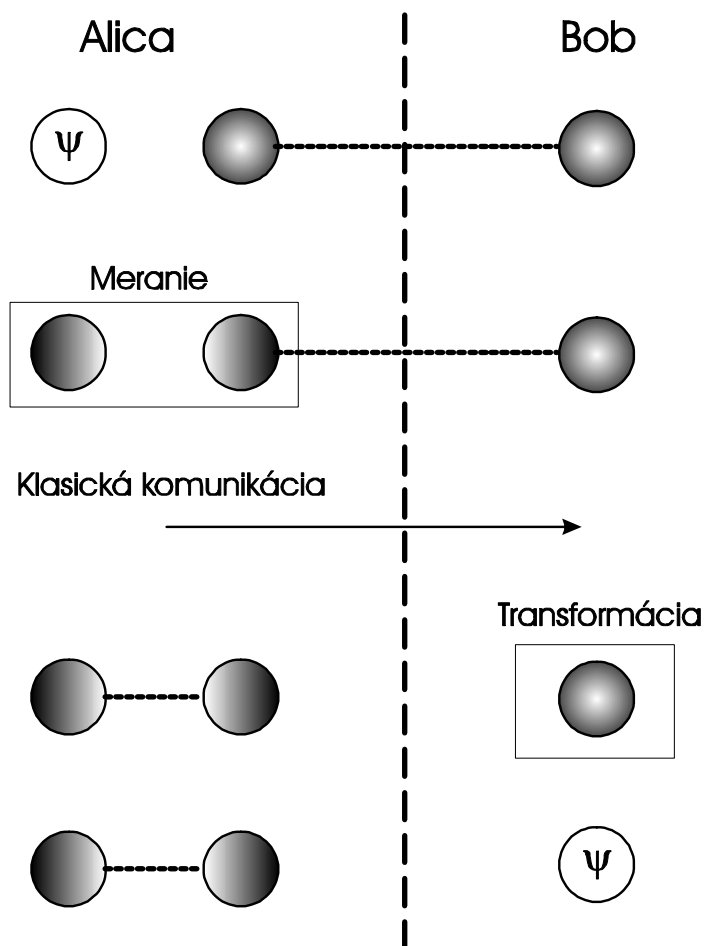
Výsledok tohoto merania vo forme dvoch bitov klasickej informácie (máme k dispozícii 4 rôzne možné výsledky merania) zašle Alica Bobovi. Ten na svojom qbite (tu je dobré podotknúť, že pokiaľ Alica má k dispozícii už dva qbity, jeden z dvojice pôvodne entanglovaných qbitov spoločných s Bobom a jeden vzor, ktorý má transportovať, Bob má stále k dispozícii len jeden qbit zo spoločného páru) urobí, podľa výsledku Alicinho merania, jednu zo štyroch operácií rotácie spinu (ponechá ho nezmenený alebo zrotuje okolo jednej z troch osí x, y a z). Tomu zodpovedá ako operátor jedna z vektora Pauliho matíc

$$\vec{\sigma} = (I, \sigma_x, \sigma_y, \sigma_z) = \left(\left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right), \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right), \left(\begin{array}{cc} 0 & i \\ -i & 0 \end{array} \right), \left(\begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right) \right). \quad (2.105)$$

Po tejto operácii bude Bobov qbit naozaj v stave $|\psi_C\rangle$. Aby sme toto tvrdenie dokázali, prepíšeme si neznámy qbit do tvaru $|\psi_C\rangle = a|0\rangle + b|1\rangle$. Teraz môžeme písať:

$$\begin{aligned} |\psi_C\rangle|\phi^+\rangle_{AB} &= (a|0\rangle + b|1\rangle) \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\ &= \frac{1}{2}a (|\phi^+\rangle_{CA} + |\phi^-\rangle_{CA}) |0\rangle_B + \frac{1}{2}b (|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA}) |1\rangle_B \\ &\quad + \frac{1}{2}b (|\phi^+\rangle_{CA} - |\phi^-\rangle_{CA}) |1\rangle_B + \frac{1}{2}a (|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA}) |0\rangle_B \\ &= \frac{1}{2}|\phi^+\rangle_{CA}|\psi\rangle_B + \frac{1}{2}|\psi^+\rangle_{CA}\sigma_1|\psi\rangle_B \\ &\quad + \frac{1}{2}|\psi^-\rangle_{CA}\sigma_2|\psi\rangle_B + \frac{1}{2}|\phi^-\rangle_{CA}\sigma_3|\psi\rangle_B. \end{aligned} \quad (2.106)$$

Ako vidíme, po prevedení vhodných operácií (a s využitím $\sigma_i^2 = 1$) dostane Bob vždy správny výsledok. Vyvstáva otázka, akým spôsobom bola samotná informácia o qbite $|\psi_C\rangle$ zaslaná. Ťažko predpokladať, že to bolo v samotných dvoch klasických bitoch. Neobsahujú dosť parametrov na presné špecifikovanie stavu so spinom $1/2$, na to treba jeden komplexný parameter, resp. dva reálne uhly. Okrem toho výsledok Bellovho merania, ako je zjavné z rovnice (2.106), je celkom náhodný a všetky 4 možné stavy sa vyskytujú s rovnakou pravdepodobnosťou.



Obrázok 2.13: Teleportácia stavu ψ od Alice k Bobovi. Najskôr na neznámom stave spolu s jednou časťou entanglovaného páru prevedieme kolektívne Bellove meranie. Jeho výsledok za pomoci klasickej komunikácie preniesieme k Bobovi, ktorý vykoná (v závislosti od obdržanej informácie) príslušnú transformáciu. Po úspešnej operácii Bob získa neznámy stav, ale stratí entanglement s Alicou, ktorý sa presunie medzi dve častice patriace Alici.

Kapitola 3

Prenos kvantovej informácie zašumeným kanálom

3.1 Problémy otvoreného systému

Tak ako v iných oblastiach fyziky, pochopiteľne aj tu sa stretávame pri prechode od teórie k praxi s problémom, že všetky idealizácie, ktoré sme v teórii urobili, v reálnom svete neplatia. Žiaden stav nie je pripravený presne tak, ako sme predpokladali. Nikdy nemáme k dispozícii nekonečné množstvo rovnakých stavov, ako sa to často pri pokusoch požaduje. Aparáty na transformáciu stavov sú nedokonalé a nie vždy pracujú podľa našich predstáv, detektory majú nízke účinnosti. Toto všetko sú ale veci, ktoré sa opakujú v každom odvetví, či už ide o časticovú fyziku, optiku alebo astronómiu. V našom prípade ale ku všetkým týmto problémom prichádza ešte ďalší, nie síce nový, ale nadobúdajúci v kontexte kvantovej mechaniky a entanglementu nové rozmery. Naša častica totiž pri každom kontakte s okolitým prostredím môže zostať naňho naviazaná. Vzniká tak entanglement medzi časticou a prostredím, o ktorom vieme len veľmi málo a nemáme ho pod kontrolou. Efektívne máme k dispozícii len stav našej častice, už ale nie čistý. Tento jav sa nazýva dekoherencia.

3.2 Dekoherencia

V mnohých myšlienkových pokusoch z predchádzajúcej kapitoly sme využívali maximálne entanglované páry, či dokonca väčšie skupiny častíc. Zároveň bolo ale ukázané, že ak sú dve častice maximálne entanglované, nesmú byť viazané na žiadnu ďalšiu časticu a teda ani systém. Ak sa dostaneme do situácie, že naša entaglovaná dvojica alebo len jeden jej člen reaguje s prostredím a viaže sa naň, zákonite strácame časť entanglementu, čo je nechcený jav. Pritom dostávame štatistickú zmes, ktorá môže v jednotlivých meraniach dávať úplne rovnaké výsledky.

Vo väčšine prípadov reagujú skúmané systémy s okolím pomocou termálnych fotónov, ktoré sú prítomné všade a zbaviť sa ich dá len prevádzaním experimentu za absolútne nulovej teploty, čo, pochopiteľne, nie je fyzikálne možné. Fotóny spôsobujú zmenu matice hustoty daného stavu tak, že pri zápise v energetickej báze (táto báza je vo väčšine prostredí preferovaná; vo všeobecnosti sa jedná o bázu, v ktorej sa deje najväčší kontak s prostredím) exponenciálne s

časom klesajú nediagonálne elementy. Typicky napríklad v magnetickom poli sa bude stav

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|1\rangle|0\rangle + |0\rangle|1\rangle) \quad (3.1)$$

meniť na maticu hustoty zmiešaného stavu

$$|\psi\rangle\langle\psi| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \rightarrow \rho = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (3.2)$$

Táto matica sa líši od predchádzajúceho stavu len pri meraniach prevádzaných na oboch časticiach a ich jednotlivom porovnaní. Štatistické výsledky dáva zhodné s pôvodným stavom.

3.3 Korekcia chýb

Je zřejmé, že chybám spôsobeným neideálnymi zariadeniami a dekoherenciou nemôžeme úplne zabrániť. Môžeme sa ich snažiť minimalizovať, ale nikdy sa ich nezbavíme úplne. Preto je nutné hľadať spôsoby, ako tieto chyby opravovať. Na to sú určené error correction algoritmy.

Zoberme konkrétny príklad, keď chceme pomocou kvantového kanála posielat' kvantové bity a porovnajme ho s klasickým prípadom, keď napríklad bežným optickým káblom posielame signál z počítača. Aj v klasickom prípade môžu nastať chyby, avšak na každom bite len chyba jedného druhu. Buď sa ten-ktorý bit preklopí, alebo zostane tak, ako je, žiadna ďalšia možnosť neexistuje. Na takéto jednoduché chyby existujú aj jednoduché spôsoby, ako sa im brániť.

Ak chyba nastáva veľmi zriedka, stačí, ak sa za každý n -tý bit (v závislosti od očakávanej frekvencie chýb, v bežnej pamäti počítača sa používa $n = 8$) vloží jeden takzvaný paritný bit. Tento bude obsahovať sumu všetkých predošlých n bitov modulo 2. V prípade, ak sa preklopí práve jeden z n bitov, príjemca to zistí a môže si príslušnú sekvenciu vyžiadať znova. Existujú samozrejme aj zložitejšie spôsoby, ako paritné bity umiestňovať a tieto umožňujú aj lokalizáciu chyby. Ak okrem už spomínaných paritných bitoch vložím po 64 bitoch ďalších 8 paritných bitov, pričom v prvom bude suma 1., 9., 17., ... bitu, v druhom suma 2., 10., 18., ... bitu a tak ďalej, ak nastane medzi týmito 64, resp. spolu s paritnými bitmi 80 bitmi len k jedinej chybe, môžeme ju presne lokalizovať a opraviť bez toho, aby sme museli vysielateľ žiadať o opätovné zaslanie informácie.

Ak predpokladáme, že chyba nastáva častejšie, je rozumné každý bit zasielať viackrát. Ak ho posielame dvakrát, zistíme, že sa stala chyba, ak dostaneme dva rôzne bity, nevieme ju však opraviť. Preto má zmysel posielat' informáciu trikrát, prípadne 5 a viackrát. Z každej trojice či päťice potom vyberieme výsledok, ktorý sa vyskytuje častejšie a ten vyhlásime za správny.

Bohužiaľ ale žiaden z uvedených postupov nie je priamo aplikovateľný na prípad kvantovej komunikácie. Dôvodov je viacero. Chyby, ktoré môžu nastať na jednom qbite, sú komplikovanejšie. Jednak, samozrejme, môže prísť k preklopeniu qbitu rovnako ako tomu bolo v klasickom prípade. Qbit sa môže ale aj pootočiť, napríklad zo spinu s vlastným stavom v smere osi z sa môže stať spin s vlastným stavom v smere osi x . Môže sa meniť len fáza stavu, čo síce neovplyvní výsledok žiadneho merania samotného stavu, ale môže ovplyvniť výsledky zahrňujúce viac koherentných stavov. Kvantový bit sa môže viazať na prostredie a stáva sa z

neho štatistická zmes. Voči všetkému podobnému sa potrebujeme brániť. Máme ale výrazne obmedzené možnosti.

Ak posielame stavy, ktoré si vyrábame podľa určitého klasického predpisu, môžeme ich jednoducho vyrobiť viacej a poslať ich všetky. Na konci potom urobíme akýsi priemer obdržaných stavov. V takomto prípade je ale často jednoduchšie zaslať klasickým kanálom návod, ako si stavy pripravovať.

Môže sa ale stať, že potrebujeme posielat' stavy, ktoré dopredu nepoznáme. V tomto prípade nevieme bez toho, aby sme stav zničili, vyrobiť jeho kópiu, nemôžeme ich zaslať jednoducho opakovan. Nefungujú žiadne z klasických spôsobov korekcie chýb, musíme vyvinúť nové, určené špeciálne pre kvantovú komunikáciu.

3.4 Kvantová korekcia chýb

Prvý postup, ktorý riešil aspoň čiastočne problémy s kvantovými chybami, navrhovali Steane a Shor [30]. Pretože ide o jednoduché zovšeobecnenie kódu získaného nahradením jedného bitu tromi rovnakými spomínaného vyššie, budem sa práve tomuto kódu venovať podrobnejšie.

Pre začiatok si teda zoberme jednoduché kódovanie jedného qbitu do troch podľa predpisu

$$\begin{aligned} |0\rangle &\rightarrow |000\rangle \\ |1\rangle &\rightarrow |111\rangle, \end{aligned} \tag{3.3}$$

pričom ale superpozícia sa kóduje

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle \tag{3.4}$$

a nejedná sa o klonovanie, kde by platilo

$$\alpha|0\rangle + \beta|1\rangle \rightarrow (\alpha|0\rangle + \beta|1\rangle)^{\otimes 3}, \tag{3.5}$$

lebo chýbajú krížne členy typu $\alpha\beta^2|011\rangle$. Ukážem teraz, ako sa dá opraviť chyba preklopenia jedného (a iba jedného) qbitu (štandardná chyba vyskytujúca sa aj pri diskretných bitoch):

$$\alpha|000\rangle + \beta|111\rangle \rightarrow \alpha|100\rangle + \beta|011\rangle \tag{3.6}$$

(v tomto prípade sa preklopil prvý qbit, ale zo symetrie by to mohol byť ktorýkoľvek iný). Zavedme operátory, ktoré budú merať súčet prvého a druhého qbitu modulo dva, a tiež druhého a tretieho qbitu modulo dva. Ak oba tieto operátory majú nulovú hodnotu, znamená to, že všetky tri qbity sú rovnaké, majú hodnotu buď nula alebo jedna a chyba nenastala. Môže sa stať, že jeden alebo oba operátory budú mať jednotkový výsledok. Potom vieme povedať, že chyba nastala a dokonca vieme určiť aj qbit, v ktorom sa stala. Ak je jednotkový prvý operátor, chyba je v prvom qbite, ak druhý, chyba je v treťom qbite. Ak sú jednotkové oba, znamená to, že chyba nastala v prostrednom, druhom qbite.

Takto sa podarilo vyriešiť prvý druh chýb, ktorý mohol nastávať. Na tom ale nie je nič prekvapujúce, pretože sa jedná o rovnaký kód a rovnaké chyby ako v klasickom prípade, preto nie je dôvod, aby postup nefungoval. Dôležité je len to, že pri zisťovaní chyby sme *nezmerali* samotnú informáciu, a teda sme ju ani nijako nepoškodili. Oba operátory rozlišovali iba medzi priestorom stavov, ktoré sú chybové a priestorom bezchybných stavov a nerobili žiadne rozdelenia v priestore bezchybných stavov.

Druhý typ chýb, ktorý môže nastávať, sú malé chyby. Tie sa dajú zapísať vo forme

$$\begin{aligned} |000\rangle &\rightarrow |000\rangle + \varepsilon|100\rangle \\ |111\rangle &\rightarrow |111\rangle + \varepsilon|011\rangle, \end{aligned} \quad (3.7)$$

kde sme zasa z dôvodu symetrie mohli vybrať práve prvý qbit ako chybový. Na upravenie týchto chýb nemusíme do postupu zavádzať žiadne nové prvky. Nový stav nie je vlastným stavom operátora merajúceho súčet prvého a druhého qbitu modulo dva. Pri tomto meraní, ktoré pôvodne zisťovalo len chybu preklopenia spinu, sa stav s vysokou pravdepodobnosťou vyprojektuje späť do bezchybného stavu. Iba s pravdepodobnosťou $|\varepsilon|^2$ dostaneme chybový stav. Tento stav ale už máme ošetrený, lebo sa jedná o preklopenie bitu a pomocou vyššie opísaného spôsobu ho môžeme napraviť bez toho, aby sme narušili informáciu v ňom obsiahnutú.

Tretí typ chýb bude spôsobovať najväčšie problémy; jedná sa o fázový posun

$$\begin{aligned} |000\rangle &\rightarrow |000\rangle \\ |111\rangle &\rightarrow -|111\rangle. \end{aligned} \quad (3.8)$$

Voči tomuto typu je kód v pôvodnej podobe bezmocný. Musíme ho istým spôsobom upraviť, rozšíriť tak, aby mohol hľadať a naprávať nie len chyby preklopenia spinu, ale aj fázové chyby. Najjednoduchší spôsob je zaviesť redundanciu aj vo fáze. Inak povedané, ak sme si každý qbit zapísali pre istotu trikrát, nie je dôvod, aby sme fázu tiež nezapísali trikrát a tak sa bránili jej strate. Zavedieme nové kódovanie, kde budeme na rozdiel od kódovania (3.3) používať až 9 qbitov, 3 na bity krát 3 na fázy

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2^3}} (|000\rangle + |111\rangle) (|000\rangle + |111\rangle) (|000\rangle + |111\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2^3}} (|000\rangle - |111\rangle) (|000\rangle - |111\rangle) (|000\rangle - |111\rangle). \end{aligned} \quad (3.9)$$

Predstavme si teraz, že nastane fázová chyba typu (3.8). Jedna z troch zátvoriek sa zmení

$$\begin{aligned} |000\rangle + |111\rangle &\rightarrow |000\rangle - |111\rangle \\ |000\rangle - |111\rangle &\rightarrow |000\rangle + |111\rangle \end{aligned} \quad (3.10)$$

a ostatné dve zostanú rovnaké. Znovu, podobne ako v prípade preklápania spinu, môžeme zaviesť operátory, ktoré budú merať iba či sú rovnaké znamienka v prvej a druhej a v prvej a tretej zátvorke. Tak zistíme, či chyba nastala a ak áno, kde. To všetko samozrejme bez toho, aby sme akýmkoľvek spôsobom nabúrili informáciu uloženú teraz už v deviatich qbitoch.

Tento kód, pokiaľ by fungoval dokonale, rieši už všetky možné chyby. Posledná, malá fázová chyba je riešená rovnako ako malá chyba v preklopení spinu. Operátor vo väčšine prípadov stav sprojektuje späť na bezchybný a s malou pravdepodobnosťou na stav s úplne otočenou fázou, ktorý vieme opravovať.

Tu je ale potrebné zdôrazniť dva predpoklady, ktoré sme implicitne uvažovali:

- Predpokladáme, že operácie ohľadne merania a opráv kódu sú bezchybné. Takáto situácia nemôže v skutočnosti nastať a preto do ďalších úvah musíme zahrnúť aj to, ako vyriešiť, keď napríklad práve pri snahe opraviť chybu informáciu ešte viacej pokazíme.

- Predpokladáme, že chyby sa na jednotlivých qbitoch vyskytujú nezávisle. Ak k tomu pridáme malú pravdepodobnosť výskytu jednotlivých chýb, môžeme zanedbať situácie, keď by vznikla chyba na dvoch qbitoch naraz. Je ale jednoducho predstaviteľná situácia, že chyby sa budú napríklad často vyskytovať na dvoch susedných qbitoch (nejaká vonkajšia porucha zasahujúca viac častíc). Na riešenie tohoto problému by sme potrebovali robustnejší kód.

Z teoretického hľadiska je kód nesporne zaujímavý. Prakticky ale vyžaduje veľmi zložité operácie (pri zisťovaní a opravovaní fázových chýb potrebujeme merať naraz stav 6 qbitov bez toho, aby sme zistili ich jednotlivý stav) a preto je potrebné skúmať aj ďalšie možnosti. Jednoduchým rozšírením a kombinovaním horeuvedených postupov môžeme dostať kód so siedmimi alebo iba piatimi qbitmi, opravujúci chyby preklopenia bitu aj fázy. Ďalším zväčšovaním počtu qbitov môžeme zväčšovať robustnosť schémy, alebo hľadať celkom iné spôsoby, ako si poradiť so situáciami, keď je pravdepodobnosť výskytu chýb veľká.

3.5 Pauliho kanál

Aby sme mohli posudzovať úspešnosť a efektívnosť jednotlivých algoritmov na korekciu či predchádzanie chýb, musíme nájsť spôsob, ako chyby kontrolovane simulovať. Potrebujeme matematicky čo najpresnejšie ale zároveň najjednoduchšie opísať vplyv prostredia. Tieto požiadavky dobre spĺňa Pauliho kanál, ktorý som zvolil pre ďalšie výpočty. V podstate sa jedná o operátor, ktorý s definovanými pravdepodobnosťami otáča spin častice v smere x , y alebo z . Pripúšťa teda preklopenie spinu, jeho pootočenie i zmenu fázy. Týmto sa stáva veľmi všeobecným modelom pre chyby vznikajúce na jednotlivých qbitoch. Každý Hamiltonián, ktorý má takú formu, že sa dá zapísať ako direktný súčin Hamiltoniánov pôsobiacich na jednotlivé qbity je totiž Pauliho kanál. Takýto Hamiltonián (obmedzený na jeden qbit) je hermitovská matica 2×2 a Pauliho matice spolu s jednotkovou sú bázou pre matice tohoto typu. (Viac o Pauliho kanáloch sa dá nájsť v knihe [31]).

Mnohé ďalšie prípustné chyby ale kanál neimplementuje. Nepripúšťa totiž, že to, ako sa mení ten-ktorý spin, môže závisieť aj od toho, aké spiny išli pred ním alebo po ňom. Teda nevytvára väzby medzi po sebe nasledujúcimi spinmi, čo sa v skutočnej komunikácii môže diať. Nesimuluje realistické chyby spomínané v závere predošlej sekcie, keď určitá chyba vzniká na niekoľkých susedných (resp. po sebe idúcich) qbitoch.

Analyticky sa dá Pauliho kanál popísať ako

$$|\Psi\rangle \rightarrow \rho = (1 - p)|\Psi\rangle\langle\Psi| + p_x\sigma_x|\Psi\rangle\langle\Psi| + p_y\sigma_y|\Psi\rangle\langle\Psi| + p_z\sigma_z|\Psi\rangle\langle\Psi|, \quad (3.11)$$

kde σ_i sú Pauliho matice a $0 \leq p_i \leq 1$ sú pravdepodobnosti charakterizujúce Pauliho kanál. Pochopiteľne musí platiť, že $p = \sum p_i \leq 1$, lebo súčet pravdepodobností, že nastane nejaká z navzájom sa vylučujúcich porúch je tiež pravdepodobnosť, a teda ohraničená zvrchu číslom 1. Pre špeciálne výbery pravdepodobností sa rovnica značne zjednodušuje. Definujeme depolarizačný kanál, kde sú všetky pravdepodobnosti rovnaké a charakterizujú sa len jedným parametrom

$$\rho = (1 - \frac{4}{3}p)|\Psi\rangle\langle\Psi| + \frac{2}{3}pI. \quad (3.12)$$

Tento kanál vedie na maticu úplnej zmesi a je zaujímavé, že práve pre $p = \frac{3}{4}$ sa stratí všetka informácia o pôvodnom stave a výsledok je len normovaná jednotková matica.

Druhý zaujímavý kanál je σ_i kanál, kde je len jedna z pravdepodobností nemulová, teda $p_i = p, p_j = p_k = 0$

$$\rho = (1 - p)|\Psi\rangle\langle\Psi| + p\sigma_i|\Psi\rangle\langle\Psi|\sigma_i. \quad (3.13)$$

Tento kanál zodpovedá rotácii spinu okolo niektorej z troch osí o uhol charakterizovaný parametrom p .

3.6 Symetrizáciou k stabilizácii systému

Adriano Barenco a ďalší spolupracovníci už v roku 1996 navrhli spôsob, ako stabilizovať kvantové počítanie za pomoci redundantnej informácie. Namiesto jednoduchého kódovania stavu qbitu do všetkých stavov N qbitov budeme využívať iba malý podpriestor 2^N rozmerného Hilbertovho priestoru, a to len podpriestor symetrických stavov. Predpokladalo sa, že ak sa nám vstupný stav podarí dostatočne efektívne zakódovať ako symetrický stav, väčšina náhodných chýb bude vynášať tento stav mimo symetrického podpriestoru. S rastúcim N totiž rastie rozmer symetrického podpriestoru len lineárne (každý symetrizovaný stav je plne charakterizovaný počtom qbitov, ktoré sú v stave $|1\rangle$, a tento počet je rovný $N + 1$), kdežto rozmer celého Hilbertovho priestoru rastie exponenciálne (máme N pozícií, kde môžeme voliť jeden z dvoch stavov, a teda tento rozmer bude 2^N). Ak predpokladáme, že chyby sú v istom zmysle náhodné, nie je dôvod domnievať sa, že budú uprednostňovať symetrický podpriestor pred oveľa rozmernejším zvyškom priestoru a chybové stavy budú zväčša nesymetrické. S istou frekvenciou počas počítania teda budeme projektovať náš stav späť do symetrického podpriestoru a tým odstraňovať väčšinu chýb.

Toľko hovorila teória. Hneď prvý problém ale nastáva v tom, že pokiaľ pracujeme s neznámym stavom $|\psi\rangle$, nedokážeme ho zakódovať bez straty istej časti informácie do symetrického stavu N qbitov. Optimálny spôsob, ako zakódovať neznámy stav do symetrického N -časticového stavu rozoberá článok [27]. Prejdeme na trochu inú parametrizáciu stavov, ako sme používali doteraz. Stav $|\psi\rangle$ budeme charakterizovať dvoma uhlami, ktoré zodpovedajú pozícii čistého stavu na Blochovej sfére

$$|\psi\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle. \quad (3.14)$$

Jeden z možných úplne symetrických stavov, v ktorom bude zakódovaný stav $|\psi\rangle$, má tvar

$$|\Psi\rangle \cong (|\psi, 0, \dots, 0\rangle + |0, \psi, \dots, 0\rangle + \dots + |0, \dots, 0, \psi\rangle), \quad (3.15)$$

kde stav $|0\rangle$ je len referenčný a mohol by byť nahradený ľubovoľným iným stavom, ktorý musí byť ale nezávislý od $|\psi\rangle$. Po roznásobení a zlúčení rovnakých členov dostávame

$$|\Psi(\vartheta, \varphi)\rangle = \cos\frac{\bar{\vartheta}}{2}|N, 0\rangle + e^{i\bar{\varphi}}\sin\frac{\bar{\vartheta}}{2}|N, 1\rangle, \quad (3.16)$$

kde stav

$$|N, 0\rangle = |0, 0, \dots, 0\rangle \quad (3.17)$$

a $|N, 1\rangle$ je úplne symetrický stav obsahujúci práve 1 qbit v stave $|1\rangle$ a všetky ostatné v stave $|0\rangle$. Čiarkované uhly vyjdú po dosadení z (3.14)

$$\cos\frac{\bar{\vartheta}}{2} = \frac{\sqrt{N}\cos\frac{\vartheta}{2}}{\sqrt{\sin^2\frac{\vartheta}{2} + N\cos^2\frac{\vartheta}{2}}}, \quad \bar{\varphi} = \varphi. \quad (3.18)$$

Problém ale je, že pre neznámy stav podobný scenár nie je možný. Vyžaduje totiž kompletnú klasickú znalosť o systéme (3.14), ktorú nemusíme mať. V skutočnosti, ak by sme ju mali, bolo by ďaleko jednoduchšie chrániť pred vplyvmi prostredia túto klasickú informáciu ako samotný stav. Inak povedané, namiesto toho, aby sme bránili vplyvu prostredia na stav, budeme chrániť klasický návod, ako stav pripraviť a vo vhodnom čase si vždy pripravíme nový stav.

Existujú operátory, nazývané optimálne entanglery, ktoré optimálnym spôsobom entanglujú qbity. V našom prípade potrebujeme entanglovať vstupný qbit v neznámom stave so zvyšnými $N - 1$ qbitmi v stave známom, povedzme $|0\rangle$. Postup môžeme napísať nasledovne

$$\begin{aligned} |0\rangle|N-1,0\rangle|e_0\rangle &\rightarrow [\gamma_N|N,0\rangle|e_1\rangle + \delta_N|N,1\rangle|e_2\rangle] \\ |1\rangle|N-1,0\rangle|e_0\rangle &\rightarrow [\delta_N|N,0\rangle|e_3\rangle + \gamma_N|N,1\rangle|e_1\rangle], \end{aligned} \quad (3.19)$$

kde stavy $|e_i\rangle$ sú stavy entanglera, vonkajšieho zariadenia, cez ktoré budeme neskôr robiť stopu, a konštanty

$$\gamma_N = \sqrt{\frac{N+1}{2(N+1-\sqrt{N})}} \quad ; \quad \delta_N = \sqrt{1-\gamma_N^2} \quad (3.20)$$

určujú optimálnosť entanglera. Stav $|\psi\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle = \alpha|0\rangle + \beta|1\rangle$ môžeme podľa predpisu (3.19) previesť na čistý stav N qbitov a entanglera. Urobením stopy cez entangler získame vo všeobecnosti zmiešaný stav N qbitov vo forme

$$\begin{aligned} \rho^{in} &= (|\alpha|^2\gamma_N^2 + |\beta|^2\delta_N^2) |N;0\rangle\langle N;0| + (|\alpha|^2\delta_N^2 + |\beta|^2\gamma_N^2) |N;1\rangle\langle N;1| + \\ &+ \alpha\beta^*\gamma_N^2 |N;0\rangle\langle N;1| + \alpha^*\beta\gamma_N^2 |N;1\rangle\langle N;0|. \end{aligned} \quad (3.21)$$

Maticovo sa dá zapísať

$$\rho^{in} = \begin{pmatrix} |\alpha|^2\gamma_N^2 + |\beta|^2\delta_N^2 & \alpha\beta^*\gamma_N^2 \\ \alpha^*\beta\gamma_N^2 & |\alpha|^2\delta_N^2 + |\beta|^2\gamma_N^2 \end{pmatrix}, \quad (3.22)$$

pričom sme použili bázu len dvoch využitých symetrických stavov, so žiadnym a s jedným qbitom v stave $|1\rangle$. Čo je ale veľmi dôležité, táto matica hustoty už neobsahuje kompletnú informáciu o pôvodnom systéme.

3.7 Fidelita

Na to, aby sme mohli porovnávať, koľko informácie sme stratili napríklad pri entanglovaní a pri prechode stavu Pauliho kanálom, potrebujeme zaviesť mieru. Pre čisté stavy je to jednoduché, na porovnanie dvoch stavov stačí urobiť ich skalárny súčin. Ak porovnáваме stavy $|\psi\rangle$ a $|\phi\rangle$, veličina

$$|\langle\phi|\psi\rangle|^2 \quad (3.23)$$

dáva hodnoty vždy medzi nulou a jednotkou a dobre odráža intuitívne chápanú podobnosť stavov. Pre matice hustoty môžeme definovať podobnú veličinu, ktorú pre jednoduchosť budeme nazývať fidelita (o mierach vzdialenosti na priestore stavov sa dá viac dočítať napríklad v deviatej kapitole knihy Nielsen, Chuang [31]). Dokáže určiť podobnosť čistého stavu

a matice hustoty (to nám vyhovuje, pretože v zásade môžeme žiadať, aby vstupný stav bol čistý) a je definovaná

$$F = \langle \psi | \rho | \psi \rangle. \quad (3.24)$$

Je zrejmé, že pre prípad čistého stavu $\rho = |\phi\rangle\langle\phi|$ sa redukuje fidelita na skalárny súčin (3.23). Pre všetky vstupné stavy nadobúda fidelita hodnoty medzi nulou a jednotkou (Overiť sa to dá jednoducho tak, že si zapíšeme maticu ρ v báze, ktorá obsahuje stav $|\psi\rangle$. Potom je fidelita práve koeficient na diagonále tejto matice zodpovedajúci stavu $|\psi\rangle\langle\psi|$, ktorý je vždy nezáporný, reálny a menší-rovný jednotke).

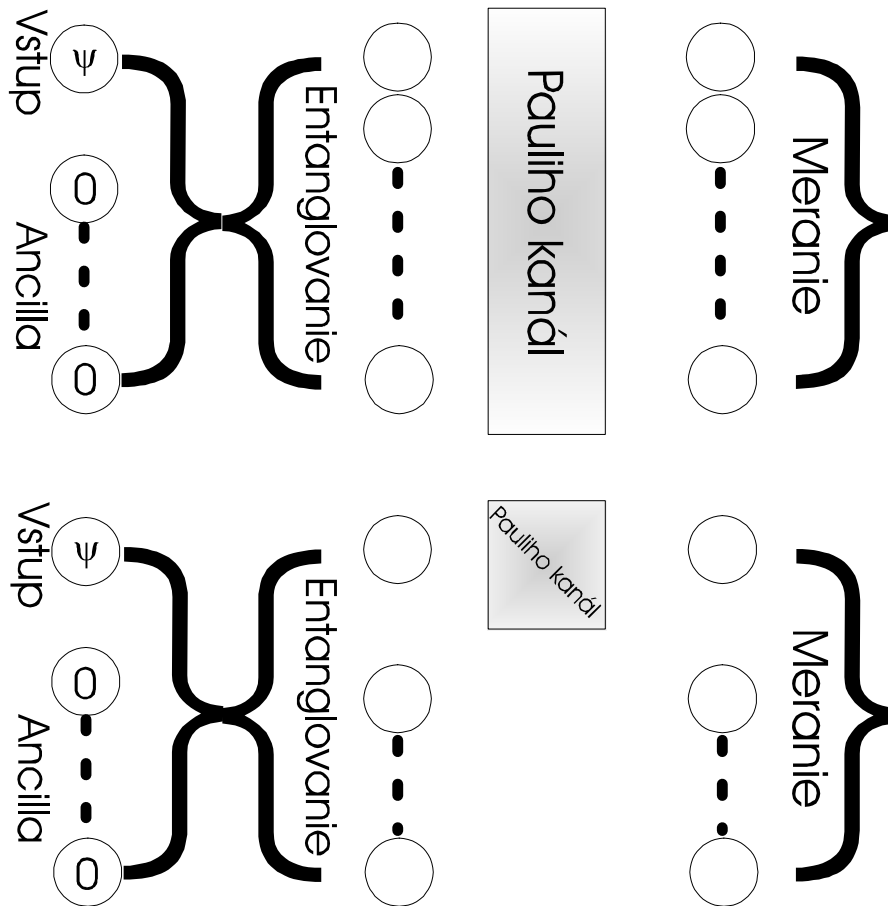
3.8 Symetrizovaný stav prechádzajúci Pauliho kanálom

Máme definovaný Pauliho kanál pôsobiaci na jeden qbit ako aj spôsoby, ako informáciu obsiahnutú v stave jedného qbitu rozdistribuovať na viacero častíc a ako porovnávať, koľko informácie sa stratilo. Môžeme teda urobiť nasledujúce:

Pre rôzne typy Pauliho kanálov (rôzne absolútne veľkosti parametrov, depolarizačný aj σ_i kanál) môžeme porovnávať fidelitu v prípade, ak sme cez Pauliho kanál poslali stav tak, ako sme ho pôvodne dostali (3.14) a v prípade, ak sme stav najskôr zakódovali do symetrického stavu viacerých qbitov. Tu sú možné dve alternatívy, ako vplyv prostredia implementovať. Jedna, jednoduchšia, hovorí, že prostredie, teda Pauliho kanál, bude pôsobiť stále len na jednu pôvodnú časticu a ostatné budú od chýb uchránené. Predstava môže byť taká, že Alica potrebuje poslať niekam ďaleko k Bobovi jeden qbit, tam na ňom Bob vykoná akúsi operáciu a vráti ho Alici späť. Vtedy môže Alica ostatné qbity nechať v dobre chránenom skladiisku a zabrániť väčšine chýb. Druhá alternatíva hovorí, že potrebujeme zaslať informáciu jedným smerom a vtedy musíme posielat' všetky qbity, teda chyby (Pauliho kanál) sa budú uplatňovať na všetkých časticách.

3.8.1 Pauliho kanál pôsobiaci na 1 qbit

V tejto časti rozoberiem prvú alternatívu spomenutú vyššie. Uvažujeme jeden qbit v neznámom stave $|\psi\rangle$, ktorý entanglujeme pomocou univerzálneho entanglera a necháme naňho pôsobiť Pauliho kanál. Výslednú maticu hustoty môžeme zapísať pre $N > 1$ (pre $N = 1$ je



Obrázok 3.1: Na obrázku sú dva možné scenáre pôsobenia Pauliho kanálu. V oboch sa vstupný qbit najskôr musí entanglovať s referenčnými qbitmi. Potom pôsobí Pauliho kanál, buď na všetky qbity (v prípade hore), alebo len na jeden qbit (referenčné qbity zostávajú nedotknuté, prípad dole). Potom nastáva meranie, resp. ďalšie použitie, my sa zaujímame iba o fidelitu výsledného stavu.

matica triviálna):

$$\begin{aligned}
\rho^{out} = & (|\alpha|^2\gamma_N^2 + |\beta|^2\delta_N^2) (1 - p + pz) |N; 0\rangle\langle N; 0| + \\
& + (|\alpha|^2\gamma_N^2 + |\beta|^2\delta_N^2) \frac{p_x + p_y}{N} |N; 1\rangle\langle N; 1| + \\
& + (|\alpha|^2\delta_N^2 + |\beta|^2\gamma_N^2) \frac{p_x + p_y}{N} |N; 0\rangle\langle N; 0| + \\
& + (|\alpha|^2\delta_N^2 + |\beta|^2\gamma_N^2) \left(1 - p + pz \left(1 - \frac{4}{N} + \frac{4}{N^2}\right)\right) |N; 1\rangle\langle N; 1| + \\
& + \left(\alpha\beta^*\gamma_N^2 \left(1 - p + pz - \frac{2p_z}{N}\right) + \alpha^*\beta\gamma_N^2 \frac{p_x - p_y}{N}\right) |N; 0\rangle\langle N; 1| + \\
& + \left(\alpha^*\beta\gamma_N^2 \left(1 - p + pz - \frac{2p_z}{N}\right) + \alpha\beta^*\gamma_N^2 \frac{p_x - p_y}{N}\right) |N; 1\rangle\langle N; 0| + \\
& + (p_x + p_y) (|\alpha|^2\delta_N^2 + |\beta|^2\gamma_N^2) \frac{2}{N^2} |N; 2\rangle\langle N; 2| \\
& + \dots
\end{aligned} \tag{3.25}$$

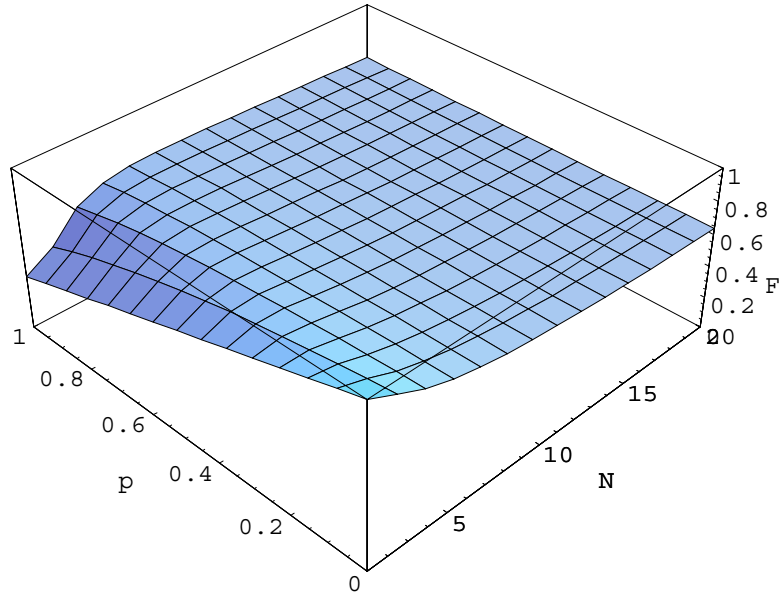
Pre skrátenie sme použili symbol $p = p_x + p_y + p_z$. V matici (3.25) už vôbec neuvádzam členy, ktoré vystupujú zo symetrického podpriestoru. Tým pádom ale táto matice nie je normovaná, takže projekcia do symetrického podpriestoru je ekvivalentá práve zrušeniu členov označených bodkami a nanormovaniu matice na jednotkovú stopu. Na to ju musíme celú predeliť jej terajšou stopou, ktorá je

$$\begin{aligned}
Norm = & (|\alpha|^2\gamma_N^2 + |\beta|^2\delta_N^2) \left(1 - p + pz + \frac{p_x + p_y}{N}\right) + \\
& + (|\alpha|^2\delta_N^2 + |\beta|^2\gamma_N^2) \times \\
& \times \left(1 - p + pz + \frac{(p_x + p_y - 4p_z)}{N} + \frac{(2p_x + 2p_y + 4p_z)}{N^2}\right).
\end{aligned} \tag{3.26}$$

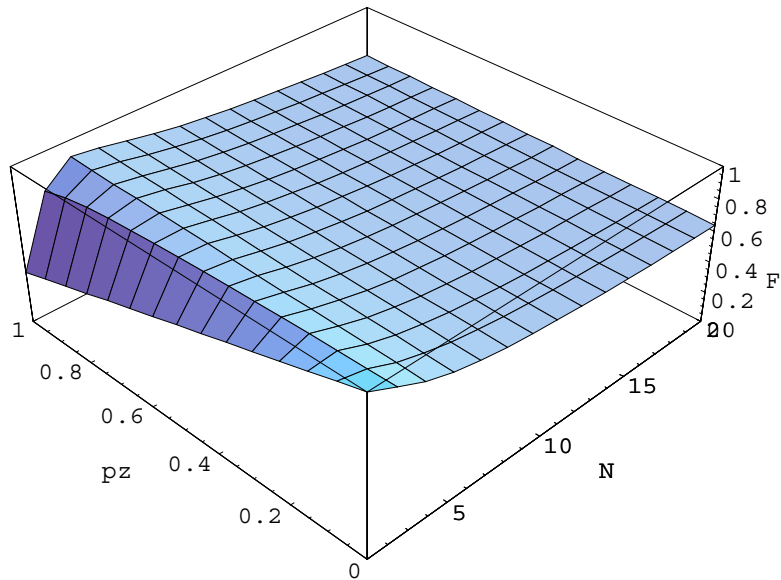
Potom počítame fidelitu výslednej, normovanej matice hustoty voči ideálnemu symetrizovanému stavu (3.15). Táto je ale závislá od parametrov stavu $|\psi\rangle$, uhlov ϑ a φ , takže musíme zaviesť strednú fidelitu definovanú

$$\begin{aligned}
\overline{F} = & \frac{1}{4\pi} \int_0^\pi \sin \vartheta d\vartheta \int_0^{2\pi} d\varphi F(\vartheta, \varphi) \\
= & \frac{1}{4\pi} \int_0^\pi \sin \vartheta d\vartheta \int_0^{2\pi} d\varphi \langle \psi(\vartheta, \varphi) | \rho(\vartheta, \varphi) | \psi(\vartheta, \varphi) \rangle.
\end{aligned} \tag{3.27}$$

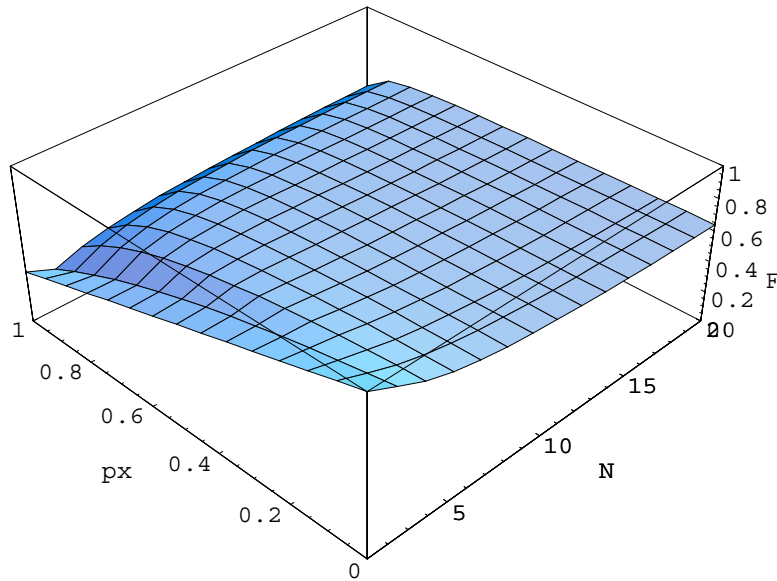
Výsledky pre rôzne počty referenčných qbitov, rôzne hodnoty parametrov a rôzne typy kanálov sú znázornené v grafoch (3.2, 3.3 a 3.4). Ako je vidieť, pre malé hodnoty parametrov p je maximum fidelity pri počte qbitov jedna. Znamená to asi toľko, že strata informácie, ktorá sa udeje pri entanglovaní stavov je väčšia ako zisk, ktorý máme z dôvodu lepšej stability. Situácia sa obráti až pre veľké hodnoty parametra p , teda v prípade, keď je šum v kanáli veľmi silný. Vtedy hrá stabilita voči chybám dôležitú úlohu. V tabuľke (3.1) sú uvedené hodnoty parametra p , od ktorých je výhodnejšie použiť vyšší počet qbitov.



Obrázok 3.2: Fidelita deplarizačného kanála. Zvislá os na grafe znázorňuje fidelitu, označenú písmenom F. Vodorovné osi označujú jednak celkový počet qbitov N a jednak parameter Pauliho kanála p. Je zrejmé, že pre malé hodnoty parametra p je fidelita ako funkcia počtu qbitov monotónne klesajúca. Pre väčšie hodnoty to už nie je pravda a fidelita má maximum, v závislosti od p, pri 2 až 8 qbitoch.



Obrázok 3.3: Fidelita pre Pauliho kanál typu σ_z , teda len pôsobenie matice preklopenia spinu. Z obrázku je zrejmé, že závislosť fidelity je veľmi podobná ako v predchádzajúcom prípade. Rozdiel je v tom, že nárast, pre veľké hodnoty parametra p, je rýchlejší a maximálna funkcia nadobúda pre 1 až 4 qbity.



Obrázok 3.4: Do tretice graf pre kanál typu σ_x . Tu je závislosť ešte zaujímavejšia, pretože pre veľké hodnoty parametra p nadobúda fidelita dokonca lokálne minimum pre počet qbitov rovný dvom. Potom znova stúpa a maximum sa posúva k veľmi veľkým hodnotám N . Graf pre tretí kanál σ_y neuvádzam, lebo je úplne rovnaký ako σ_x . Spôsobené je to tým, že cez fázy, v ktorých sa kanály líšia, sme preintegrovali.

N	p	p_z	p_x
2	0.22	0.10	–
3	0.29	0.44	0.35
4	0.48	0.86	0.41
5	0.63	–	0.52
6	0.76	–	0.60
7	0.86	–	0.66
8	0.95	–	0.71

Tabuľka 3.1: V tabuľke sú uvedené minimálne hodnoty parametra p , pri ktorých je výhodnejšie prejsť na väčší počet referenčných qbitov. Napríklad pre depolarizačný kanál je pre $p > 0.22$ výhodnejšie použiť 2 qbity, pre $p > 0.29$ je už lepšie použiť 3 qbity a tak ďalej. Pre depolarizačný kanál je maximálny počet qbitov, ktoré sa oplatí používať, 8. To znamená, že pre 9 a viac qbitov nikdy nedostaneme lepšie výsledky ako pre 8 a menej qbitov. Pre kanál σ_z je táto maximálna hodnota 4. Pre kanál σ_x je maximálna hodnota veľká (prípadne vôbec neexistuje), preto uvádzam tabuľku len do 8 qbitov. Zaujímavé je tiež, že v σ_x kanáli sa v nijakom prípade nevyplatí používať 2 častice. Pre hodnotu $p < 0.35$ je lepšie použiť len 1 qbit, pre $p \geq 0.35$ zasa až 3 qbity.

Ale pokiaľ je aj fidelita matice hustoty viacerých entanglovaných stavov vyššia, ako keby sme poslali len stav samotný, nemusí to ešte znamenať, že sme vyhrali. Pretože nakoniec potrebujeme všetku informáciu, obsiahnutú v N qbitoch, koncentrovať späť do jediného qbitu. A potom efektívne porovnať, či bolo výhodnejšie poslať informáciu tak, ako bola, alebo absolvovať zložitejší proces vo forme entanglovanie \rightarrow posielanie \rightarrow projekcia na symetrický podpriestor \rightarrow koncentrácia informácie.

Táto úloha sa dá jednoducho realizovať v našom prípade len pre kanál σ_z , pretože tu vo výsledku nevystupujú symetrické stavy s dvoma bitmi v stave $|1\rangle$, teda $|N, 2\rangle$. Priestor, v ktorom sa nachádzajú naše stavy je len dvojrozmerný, skladajúci sa zo stavov s 0 a 1 qbitmi v stave $|1\rangle$, a preto môžeme použiť algoritmus nazývaný *merací scenár*, opísaný v článku [27], ktorý optimálnym spôsobom extrahuje informáciu z normovanej matice hustoty (3.25) do zmiešaného stavu jedného qbitu. Pokiaľ by sme postupovali podobne aj pri stavoch získaných pri prechode depolarizačným či σ_x kanálom, mali by sme problém, ako a kam mapovať stav $|N, 2\rangle$.

Zvolíme si náhodne dva uhly, ϑ' a φ' , ktoré budú charakterizovať N -časticový stav nasledovne

$$\begin{aligned} |\Xi_0\rangle &= \cos \frac{\vartheta'}{2} |N, 0\rangle + e^{i\varphi'} \sin \frac{\vartheta'}{2} |N, 1\rangle \\ |\Xi_1\rangle &= e^{i\varphi'} \sin \frac{\vartheta'}{2} |N, 0\rangle - \cos \frac{\vartheta'}{2} |N, 1\rangle \end{aligned} \quad (3.28)$$

a jednočasticový stav

$$\begin{aligned} |\phi_0\rangle &= \cos \frac{\vartheta'}{2} |0\rangle + e^{i\varphi'} \sin \frac{\vartheta'}{2} |1\rangle \\ |\phi_1\rangle &= e^{i\varphi'} \sin \frac{\vartheta'}{2} |0\rangle - \cos \frac{\vartheta'}{2} |1\rangle. \end{aligned} \quad (3.29)$$

Teraz môžeme získať jednočasticovú maticu hustoty, ktorá bude funkciou jednak parametrov vstupujúceho stavu ϑ a φ a jednak parametrov stavu, ktorý používame na extrahovanie informácie ϑ' a φ'

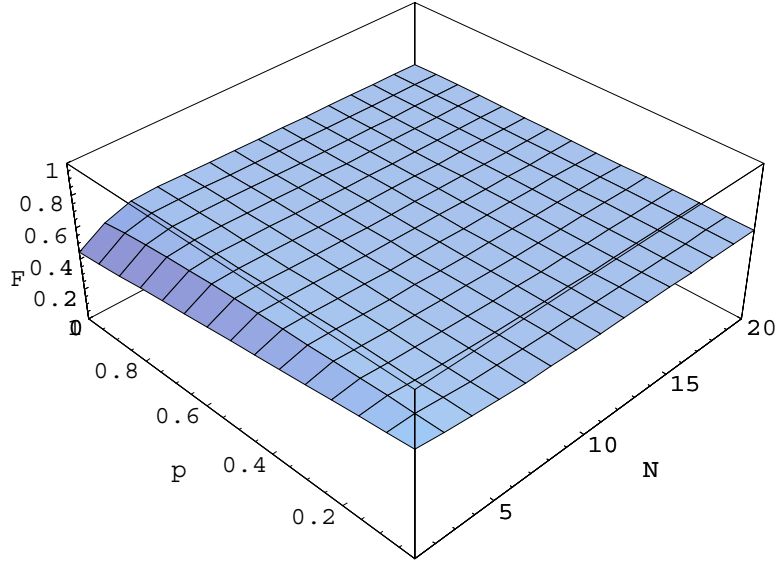
$$\rho^M(\vartheta, \varphi, \vartheta', \varphi') = |\langle \Xi_0 | \rho^{out} | \Xi_0 \rangle| \cdot |\phi_0\rangle \langle \phi_0| + |\langle \Xi_1 | \rho^{out} | \Xi_1 \rangle| \cdot |\phi_1\rangle \langle \phi_1|. \quad (3.30)$$

Spočítame fidelitu tejto matice hustoty so vstupným stavom $|\psi\rangle$ a preintegrujeme ju rovnako, ako to bolo definované v (3.27) ako cez uhly ϑ a φ , tak aj cez uhly ϑ' a φ' . Na grafe (3.5) je znázornená závislosť fidelity od parametrov N a p_z .

3.8.2 Pauliho kanál pôsobiaci na všetky qbity

V tejto časti sa budem venovať druhej alternatíve tak, ako bola spomínaná v úvode sekcie. Teda, že všetky qbity, do ktorých zakódujem informáciu, budú vystavené pôsobeniu chýb. Je zrejmé, že v tomto prípade nemôžeme očakávať ani také optimistické výsledky, ako v predošlej časti; chýb je jednoducho viac.

Hneď na začiatok je potrebné uviesť, že nebolo v mojich silách výpočtovo zvládnuť problém pre všeobecný počet qbitov, ako by sa zrejme očakávalo. Ak pôsobíme šumom na všetky častice, aj keď sa obmedzíme len na symetrický podpriestor, počet povolených stavov narastá



Obrázok 3.5: Merací scenár - fidelita výslednej jednočasticovej matice hustoty a pôvodného stavu. Je zrejmé, že základný tvar plochy zostal zachovaný, ale do veľkej miery sa zotrelí rozdiely a fidelita je pre všetky parametre skoro rovnaká. Stojí za zmienku, že pre $p = 0$ a $N = 1$, teda keď sme len zachovali pôvodný stav $|\psi\rangle$, je hodnota fidelity $\frac{2}{3}$, čo zodpovedá maximálnej nožnej informácii získateľnej (priemerne) z neznámeho stavu meraním.

lineárne s N a nie je konštantný ako v predošlom prípade, kde stačilo uvažovať len stavy so žiadnym, jedným alebo nanajvýš dvoma qbitmi v stave $|1\rangle$. Preto som sa obmedzil na jednoduché porovnanie situácie, keď posielať qbit v pôvodnom stave a keď ho zakódujem do dvoch qbitov. Matematika je v takomto prípade oveľa jednoduchšia a je možné spočítať skoro všetko analyticky.

Zopakujme teda, že máme stav $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, ktorý nevieme opakovane pripravovať (máme k dispozícii iba jeden exemplár). Ideálny symetrizovaný stav dvoch qbitov kódujúci (3.14) by bol

$$|\Psi_2\rangle = \frac{(2\alpha|00\rangle + \sqrt{2}\beta|+\rangle)}{(4|\alpha|^2 + 2|\beta|^2)^{1/2}}. \quad (3.31)$$

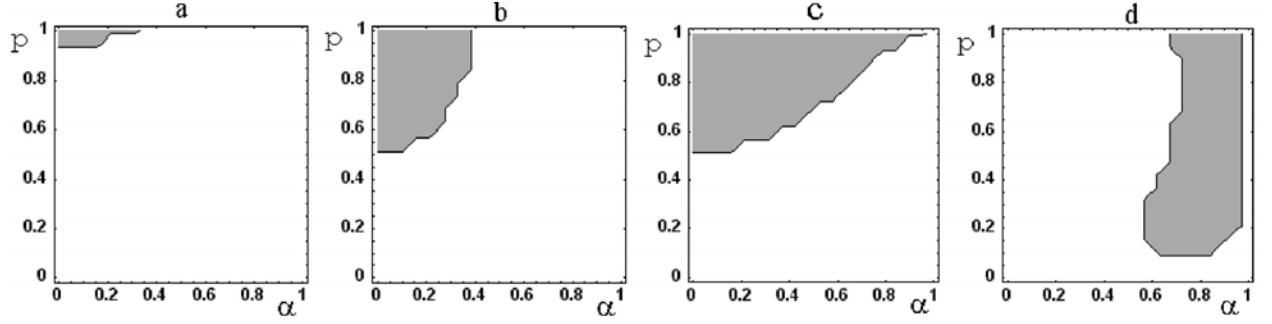
Tento stav vo všeobecnosti dosiahnuť nemôžeme, ale pomocou univerzálneho entanglera (3.19) môžeme získať maticu hustoty vo forme

$$\rho^{in} = \begin{pmatrix} |\alpha|^2\gamma_2^2 + |\beta|^2\delta_2^2 & \alpha\beta^*\gamma_2^2 \\ \alpha^*\beta\gamma_2^2 & |\alpha|^2\delta_2^2 + |\beta|^2\gamma_2^2 \end{pmatrix}, \quad (3.32)$$

kde

$$\begin{aligned} \gamma_2^2 &= \frac{3}{2(3 - \sqrt{2})} \cong 0.9459 \\ \delta_2^2 &= 1 - \gamma_2^2 \cong 0.0541 \end{aligned} \quad (3.33)$$

a matica hustoty je napísaná v báze stavov $|00\rangle$ a $|+\rangle := \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Ako zvyšné dva vektory bázy zvolíme tretí symetrický stav $|00\rangle$ a jediný antisymetrický stav na priestore dvoch častíc $|-\rangle := \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

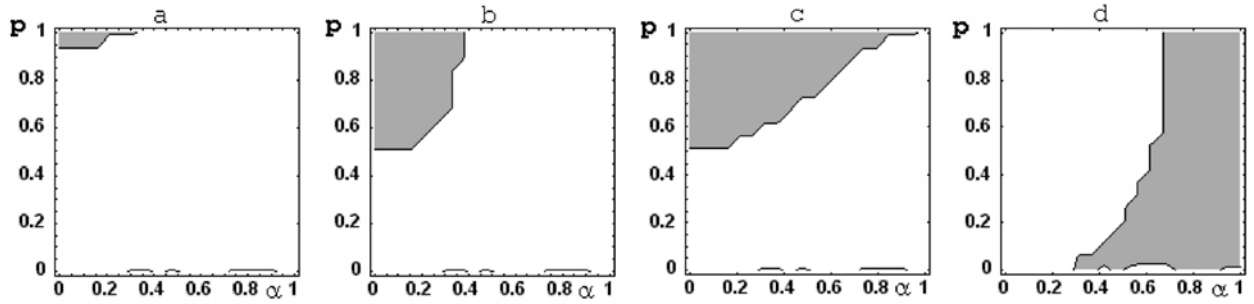


Obrázok 3.6: Výsledky porovnania fidelity stavu získaného transportovaním jedného qbitu cez Pauliho kanál a stavu dvoch qbitov v symetrizovanom stave. Sivá oblasť označuje hodnoty parametrov, pre ktoré je výhodnejšie použiť na transport 2 qbity aj za cenu straty časti informácie pri entanglovaní. Písmená *a* až *d* zodpovedajú depolarizačnému a σ_x, σ_y a σ_z kanálu. Hlavne na grafe *d* pozorujeme silnú stavovú závislosť. Dá sa to vysvetliť tým, že σ_z kanál spôsobuje chyby na stavoch $|1\rangle$ a na stavoch $|0\rangle$ nie, takže pre malé α je strata informácie pri entanglovaní oproti chybe veľká, naopak pre veľké α dostatočne malá.

Vo všeobecnosti môže byť pôsobenie Pauliho kanála na oba qbity rôzne. Avšak vzhľadom na to, že predpokladáme spoločné posielanie qbitov jednou cestou od Alice k Bobovi, a tiež v snahe minimalizovať počet voľných parametrov, zvolíme kanál symetrický, to znamená, že pôsobenie na oba qbity bude rovnaké. Zostanú znova len tri parametre p_x, p_y a p_z . Pauliho kanál upraví jednotlivé členy matice hustoty nasledovne

$$\begin{aligned}
|00\rangle\langle 00| &\rightarrow (1 - p + p_z)^2 |00\rangle\langle 00| + (p_x + p_y)^2 |11\rangle\langle 11| + \\
&\quad + (1 - p + p_z)(p_x + p_y) (|+\rangle\langle +| + |-\rangle\langle -|) \\
|+\rangle\langle +| &\rightarrow \left((1 - p)^2 + \sum_{i=x}^z p_i^2 \right) |+\rangle\langle +| + 2((1 - p)p_z + p_x p_y) |-\rangle\langle -| + \\
&\quad + ((1 - p)p_x + p_y p_z) (|00\rangle + |11\rangle) (\langle 00| + \langle 11|) + \\
&\quad + ((1 - p)p_y + p_x p_z) (|00\rangle - |11\rangle) (\langle 00| - \langle 11|) \\
|+\rangle\langle 00| &\rightarrow ((1 - p)^2 - p_z^2) |+\rangle\langle 00| + (1 - p + p_z)(p_x - p_y) |00\rangle\langle +| + \\
&\quad + (1 - p - p_z)(p_x + p_y) |11\rangle\langle +| \\
|00\rangle\langle +| &\rightarrow ((1 - p)^2 - p_z^2) |00\rangle\langle +| + (1 - p + p_z)(p_x - p_y) |+\rangle\langle 00| + \\
&\quad + (1 - p - p_z)(p_x + p_y) |+\rangle\langle 11|,
\end{aligned} \tag{3.34}$$

pričom používame označenie $p = p_x + p_y + p_z$. Zvolením jedného zo štyroch kanálov sa parametre zredukujú na jeden. V grafoch (3.6) sú uvedené výsledky pre rôzne typy kanálov ako funkcie parametra p a parametra vstupného stavu α . Je nutné podotknúť, že boli uvažované len reálne hodnoty α . Sivá je tá oblasť parametrov, kde je fidelita stavu získaného entanglovaním pôvodného stavu $|\psi\rangle$ s referenčným stavom nula pomocou univerzálneho entanglera (3.19) a pôsobením Pauliho kanálu (fidelitu počítame vzhľadom na ideálny symetrizovaný stav (3.31)) väčšia ako fidelita stavu $|\psi\rangle$, ktorý prešiel Pauliho kanálom. Podobne ako v predchádzajúcom prípade, aj tu je vidieť, že zaujímavé výsledky dostávame hlavne pre veľké hodnoty parametra p . Výnimkou je kanál σ_z , kde sú výsledky dobré aj pre malé p , tentokrát sú ale silne závislé



Obrázok 3.7: Pre porovnanie uvádzam grafy fidelity v prípade, ak by sme nepoužívali entanglovanie pomocou univerzálneho entanglera, ale mali k dispozícii priamo stavy v ideálnom symetrickom stave. Ako je vidieť, žiaden podstatný rozdiel nie je pozorovateľný. Mierne sa rozšírila oblasť pre σ_z kanál a pribudli body pre $p = 0$ (čo je úplne logické, pretože tu je pre oba prípady fidelity rovná jednej), ale inak je výsledok rovnaký. Z toho sa dá usudzovať, že problémom v tomto prípade nie je až natoľko strata informácie spôsobená neideálnym entanglovaním, ako skôr to, že pri viacerých zúčastnených qbitoch sa chyby kumulujú.

od parametra stavu α . Druhou zaujímavou skutočnosťou je, že úplne najhoršie výsledky (prakticky nulová oblasť) dostávame pre depolarizačný kanál, ktorý je kombináciou troch kanálov $\sigma_x, \sigma_y, \sigma_z$ a očakávalo sa, že bude mať podobné výsledky ako tieto kanály. Nie je tomu tak, lebo každý kanál dosahuje dobré výsledky iba v istej oblasti stavov, ktoré sa len málo prekrývajú. V iných oblastiach stavov zasa dosahuje veľmi zlé výsledky. Preto pri skombinovaní je celkový výsledok negatívny.

Pre porovnanie uvádzam na grafe (3.7) aj výsledky pre prípad, ak by sme nepoužívali na entanglovanie univerzálny entangler, ale mali k dispozícii priamo ideálne symetrizovaný stav (3.31). Napriek očakávaniu výsledky nie sú podstatne lepšie. Ukazuje sa, že ak necháme Pauliho kanál pôsobiť na dva qbity simultánne, chyby môžu vzniknúť naraz na dvoch miestach (na prvej či na druhej častici) a tak sa pravdepodobnosť ich výskytu zväčšuje. A ani istá robustnosť systému, ktorý je v symetrickom stave, nedokáže tieto chyby napraviť.

3.9 Záver

V tejto kapitole som zhrnul výsledky pre jeden konkrétny spôsob, ako brániť dekoherencii a stabilizovať kvantovomechanický systém voči vplyvu prostredia. Je potrebné otvorene uviesť, že pre malé hodnoty parametra p charakterizujúceho Pauliho kanál, a teda malé hodnoty chýb sme nedostali povzbudivé výsledky. Bolo to spôsobené tým, že už pri samotnom entanglovaní systému strácame časť informácie a táto nie je závislá od Pauliho kanála ako takého. Je preto pochopiteľné, že pre malé chyby je spôsob nevhodný. Okrem toho, v druhom prípade sme uvažovali aj chyby pôsobiace simultánne na oba qbity, čím sa znásobovala samotná pravdepodobnosť vzniku chyby.

Na druhej strane je známe, že pre dostatočne malé pravdepodobnosti máme už fungujúce a viac-menej vyhovujúce scenáre kvantovej korekcie chýb, ako sú popisované na začiatku tejto kapitoly. Tieto umožňujú za predpokladu ideálneho zariadenia a zanedbateľnej pravdepodobnosti vzniku viacnásobných chýb chyby nielen zistiť a kvantifikovať, ale aj opraviť.

Postup využívajúci projekciu na symetrický podpriestor by mohol tvoriť akýsi doplnok pre vyššie miery chýb. Je efektívny v prípadoch, keď sa vôbec o bežných korekčných schémach uvažovať nedá, lebo pravdepodobnosť násobných chýb je veľká. Jeho úspešnosť je síce stavovo závislá, ale to môže znamenať aj výhodu v prípade, že vieme, z akej oblasti stavového priestoru budú transportované stavy preferenčne pochádzať. Vtedy ich môžeme unitárnymi operáciami upraviť tak, aby sme využívali tú oblasť priestoru, kde dosahujeme dobré výsledky. Postup by mohol byť zaujímavý hlavne vtedy, ak nepotrebuje transportovať stav presne, ale stačí nám jeho priblíženie.

Kapitola 4

Entanglement jednorozmerného Isingovho modelu

4.1 Úvod

Isingov model bol dosiaľ skúmaný z mnohých stránok. Fyzikov lákal, pretože poskytuje vysvetlenia javov ako feromagnetizmus a narušenie symetrie, ktoré sa na prvý pohľad zdajú byť komplikovanými a ťažko pochopiteľnými. Preto by sa mohlo zdať, že všetky problémy týkajúce sa tohoto modelu sú už dávno dokonale preskúmané a vyriešené.

Napriek tomu sa v tejto kapitole pokúsím načrtnúť nový pohľad na Isingov model. Nebudem sa zaujímať o energie základných stavov, ale o entanglement a jeho dynamiku. Bude ma zaujímať, ako sa v čase vyvíjajú kvantové korelácie medzi dvojicami qbitov, ktoré priamo susedia, aj tými, ktoré sú od seba vzdialenejšie. Obmedzím sa na najjednoduchší prípad, lineárnu jednorozmernú reťazku qbitov (ktoré reprezentujú ľubovoľné systémy s dvoma možnými stavmi) a cyklickými okrajovými podmienkami. Porovnam miery dvojčasticového a viacčasticového entanglementu a ich vývoj v čase v závislosti od sily väzieb medzi jednotlivými atómami v porovnaní s vlastnými energiami.

Isingov model v klasickom ponímaní vysvetľuje zaujímavým spôsobom fázový prechod. Do istej miery problémom ale zostáva, že sa tak deje len pre nekonečný počet častíc. Pritom vieme, že v reálnych systémoch sú počty častíc vždy veľké, ale konečné, a napriek tomu fázové prechody bežne pozorujeme. Budem sa snažiť zistiť, či sa v správaní entanglementu v modeli s malým počtom častíc nedá pozorovať zaujímavá zmena pre oblasti parametrov, kde vzniká fázový prechod pri veľkom počte častíc. To by nám umožnilo predpokladať a vysvetľovať prechody už na modeloch s konečným počtom častíc, prípadne zistiť ďalšie zaujímavé správanie, ktoré pre nekonečné počty častíc zaniká.

Ďalšia motivácia je trochu všeobecnejšia. Je známe, že Isingov model sa zvyčajne študuje z pohľadu vlastných stavov jednotlivých spinov, teda pozorovateľných. Štúdium z hľadiska vzájomných korelácií by mohlo priniesť mnoho nového. Bellove nerovnosti ukázali, že kvantové korelácie nie sú vysvetliteľné žiadnou klasickou teóriou doplnenou o skryté parametre. Na to, aby mohli vzniknúť, sme museli zmeniť pohľad a prestať sa zaujímať o jednotlivé stavy, ale o mieru ich zviazanosti. Podobný návod chcem aplikovať na Isingov model a zistiť, či odhalí niečo dosiaľ nepoznané.

4.2 Hamiltonián

Budem používať Hamiltonián pre Isingov model v jednom rozmere s priečnym magnetickým poľom, ktorý má tvar

$$H = -C_I \sum_{n=1}^N \sigma_n^x \sigma_{n+1}^x + B \sum_{n=1}^N \sigma_n^z \quad (4.1)$$

s cyklickými okrajovými podmienkami

$$\sigma_{N+1}^\alpha = \sigma_1^\alpha \quad \alpha = x, y, z. \quad (4.2)$$

Pritom N je počet qbitov, ktoré vo výpočtoch budeme uvažovať, σ_i je Pauliho matica pôsobiaca na i -ty qbit. B je magnetické pole v smere osi z a C_I je interakčná konštanta, určujúca silu vzájomnej interakcie qbitov. Ako je zrejmé, vzájomne sa dokážu ovplyvňovať len qbity susedné, všetky ďalšie iba prostredníctvom nich.

Z dôvodov uľahčenia výpočtov a zmenšenia počtu konštánt môžeme prepísať (4.1) do tvaru

$$H = E \left(-\lambda \sum_{n=1}^N \sigma_n^x \sigma_{n+1}^x + \sum_{n=1}^N \sigma_n^z \right), \quad (4.3)$$

kde $E = B$ a $\lambda = \frac{C_I}{B}$ je bezrozmerná konštanta, určujúca pomer medzi silou vzájomnej interakcie a vlastnými energiami neinteragujúcej sústavy. Teraz môžeme uvažovať už iba jeden bezrozmerný parameter namiesto doterajších dvoch rozmerých, lebo celková konštanta nebude ovplyvňovať výsledok (okrem rýchlosti časového vývoja, o ktorom sa ešte neskôr zmienim).

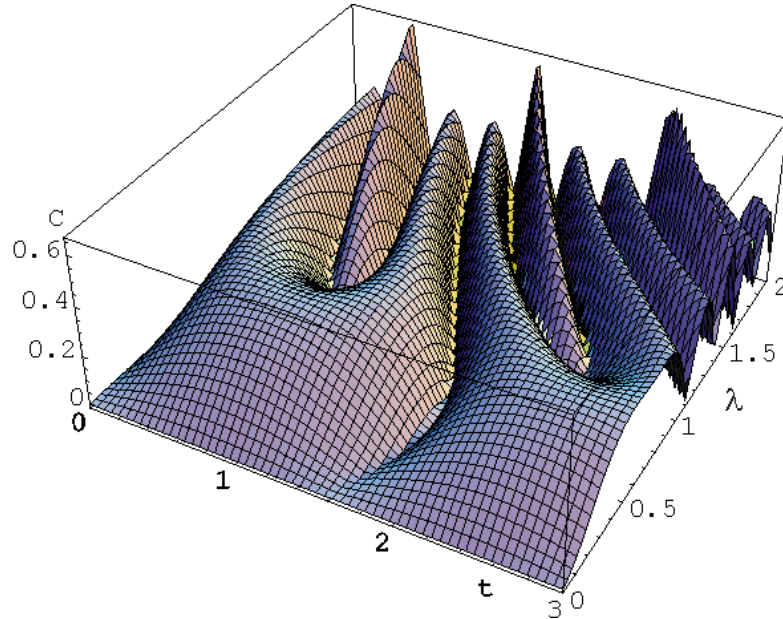
4.3 Prípád N=3

Najjednoduchší netriviálny počet qbitov, s ktorými má zmysel rátať entanglement, sú tri. Pre jeden totiž entanglement nie je vôbec definovaný a pre dva je výsledok triviálne závislý od vstupného stavu.

Budem teda skúmať pre isté vstupné stavy, ako sa s časom mení entanglement prvého a druhého qbitu v závislosti od parametra λ . Keďže budem uvažovať translačne invariantné vstupné stavy a časový vývoj mi túto invariantnosť nemôže pokaziť, entanglement medzi prvým a druhým qbitom bude vždy rovnaký ako medzi druhým a tretím, a z dôvodu cyklických okrajových podmienok aj ako medzi prvým a tretím.

Hamiltonián, zapísaný v štandardnej báze má tvar

$$H = \begin{pmatrix} 3 & 0 & 0 & -\lambda & 0 & -\lambda & -\lambda & 0 \\ 0 & 1 & -\lambda & 0 & -\lambda & 0 & 0 & -\lambda \\ 0 & -\lambda & 1 & 0 & -\lambda & 0 & 0 & -\lambda \\ -\lambda & 0 & 0 & -1 & 0 & -\lambda & -\lambda & 0 \\ 0 & -\lambda & -\lambda & 0 & 1 & 0 & 0 & -\lambda \\ -\lambda & 0 & 0 & -\lambda & 0 & -1 & -\lambda & 0 \\ -\lambda & 0 & 0 & -\lambda & 0 & -\lambda & -1 & 0 \\ 0 & -\lambda & -\lambda & 0 & -\lambda & 0 & 0 & -3 \end{pmatrix}. \quad (4.4)$$



Obrázok 4.1: Závislosť konkurencie dvoch susedných qbitov v závislosti od času a parametra λ . Vstupný stav je $|000\rangle$. Ako je zrejmé, pre $\lambda = 0$ aj pre $t = 0$ zostáva konkurencia stále nulová (jedná sa o faktorizovaný stav).

Teraz už môžeme jednoducho získať vlastný systém. Je zaujímavé, že vlastné vektory sa delia na akési dva druhy, párne a nepárne. Prvé, rozložené do štandardnej bázy, obsahujú vektory s párnym počtom qbitov v stave $|1\rangle$, pre $N = 3$ sú to konkrétne vektory $|000\rangle, |110\rangle, |011\rangle, |101\rangle$. Tie druhé obsahujú len kombinácie vektorov s nepárnym počtom qbitov v stave $|1\rangle$. Ak teda náš vstupný stav bude mať presne definovaný párný či nepárny počet qbitov v stave $|1\rangle$, časovým vývojom zostane táto vlastnosť zachovaná a z celkového Hilbertovho priestoru, ktorého bázou je 8 stavov, sa môžeme obmedziť len na príslušné štyri stavy.

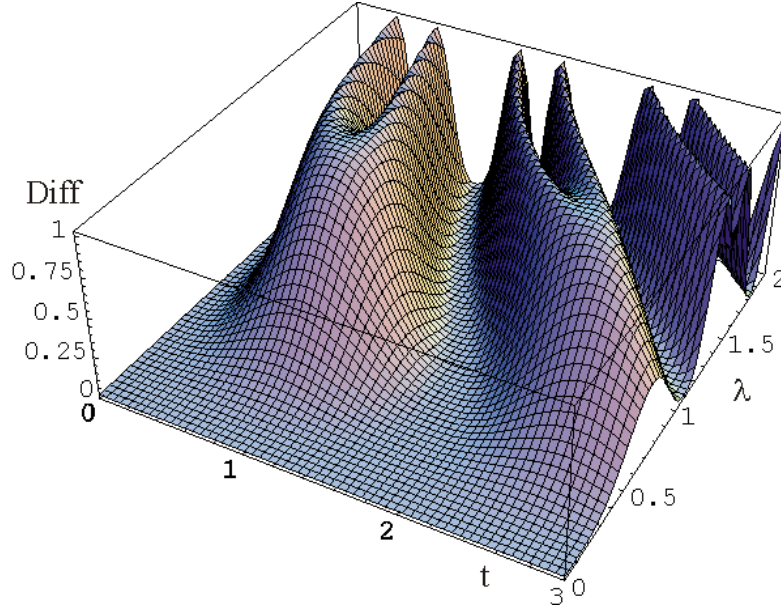
4.3.1 Faktorizovaný vstupný stav

Tu som sa zameral na konkrétny vstupný stav - základný stav $|000\rangle$. Tento stav je až na unitárnu transformáciu zhodný s inými faktorizovanými stavmi, preto pre jednoduchosť skúmam práve tento. Zaujíma ma, ako sa mení konkurencia susedných qbitov v závislosti od času a bezrozmerného parametra λ . Výsledky sú na grafe (4.1).

Tu je ale potrebné podotknúť, že rozmerná časová škála závisí od voľby konštanty E , ktorú sme po úprave Hamiltoniánu ďalej neuvažovali a jednotky na osi nie sú v sekundách alebo inej časovej miere, ale závisia práve od E . Špeciálne pre prípad $E = 1$ sú to práve sekundy.

Na grafe je viditeľné veľmi zaujímavé správanie sa konkurencie v okolí $\lambda = 1$. Časová perióda nárastu a klesania entanglementu sa menila postupne aj pre malé hodnoty λ . Pre $\lambda > 0.5$ sa ale na miestach maxím začínajú tvoriť minimá a pre $\lambda > 1$ v strede týchto miním vznikajú nové maximá. Pritom stále zostáva zachovaný trend znižovania periódy so zväčšujúcim sa λ .

Maximálna konkurencia, ktorá je v priebehu časového vývoja dosahovaná, je približne 0.65. Toto zodpovedá hornej hranici dosiahnuteľnej konkurencie, ktorá je daná podľa článku [36]



Obrázok 4.2: Ľavá strana rovnice (4.7) v závislosti od času a parametra λ . Vyjadruje rozdiel medzi celkovým a dvojčasticovým entanglementom prvého qbitu a keďže máme iba trojčasticový systém, jedná sa práve o trojčasticový entanglement. Nulová hodnota znamená, že nie je prítomný žiaden trojčasticový entanglement. V miestach, kde je rozdiel rovný jednotke, je stav maximálne trojčasticovo entanglovaný.

pre symetrický stav N qbitov (keď každé dva qbity medzi sebou majú rovnakú konkurenciu, čo je náš prípad) ako

$$C_{\max} = \frac{2}{N} \cong 0.66 \quad (4.5)$$

Znamená to, že pre isté hodnoty parametra λ v istých časoch dosiahneme maximálne entanglovaný stav.

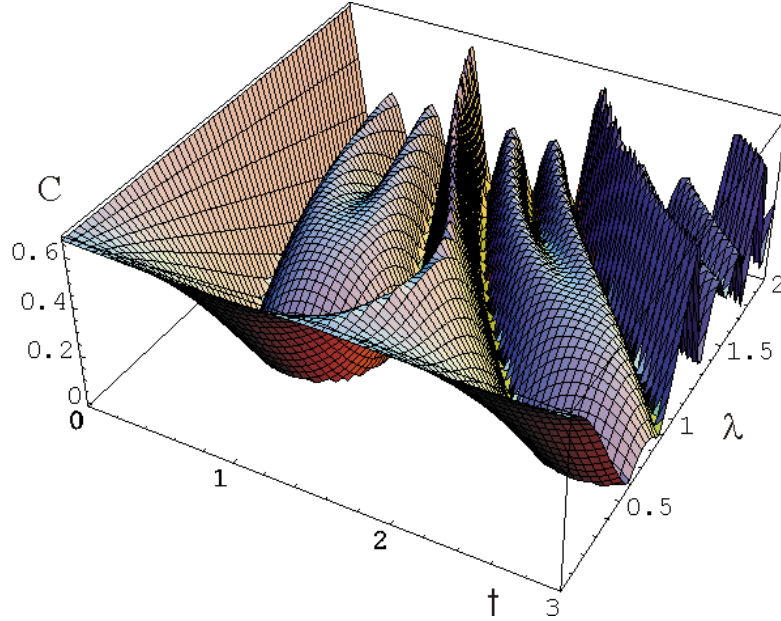
Je zaujímavé pozrieť sa tiež na zachovanie nerovností medzi dvojčasticovým a viacčasticovým entanglementom. V článku [19] je ukázaná platnosť nerovnosti pre prípad troch qbitov

$$C_{AB}^2 + C_{BC}^2 \leq C_{A(BC)}^2. \quad (4.6)$$

Teda že súčet druhých mocnín konkurencie prvého qbitu s druhým a tretím nesmie byť väčší ako druhá mocnina konkurencie prvého qbitu a zvyšku. Ďalej je tu tiež ukázané, že pravá strana rovnice (4.6) sa dá zapísať ako štvornásobok determinantu matice redukovanej na prvý qbit. Keďže aj konkurencie všetkých susedných qbitov sú rovnaké, nerovnosť môžeme prepísať do tvaru

$$4 \det(\rho_A) - 2C \geq 0. \quad (4.7)$$

Skúmal som hodnoty ľavej strany rovnice (4.7) a výsledky sú uvedené v grafe (4.2). Je zrejmé, že v priebehu časového vývoja stav prechádza od separabilného (na začiatku) cez maximálne dvojčasticovo entanglované stavy (miesta, kde je maximálna konkurencia dvoch qbitov) aj cez maximálne trojčasticovo entanglované stavy (miesta, kde je ľavá strana rovnice veľká, teda je prítomný entanglement, ale nie je to dvojčasticový).



Obrázok 4.3: Konkurencia v závislosti od času a parametra λ pre maximálne entanglovaný počiatočný stav. Podobne ako pri faktorizovanom stave, aj tu pre $\lambda = 0$ a pre $t = 0$ zostáva konkurencia konštantná. V tomto prípade ale dosahuje hornú hranicu $2/3$.

4.3.2 Maximálne dvojčasticovo entanglovaný vstupný stav

V tejto časti som pracoval znova s konkrétnym prípadom maximálne entanglovaného stavu, a to

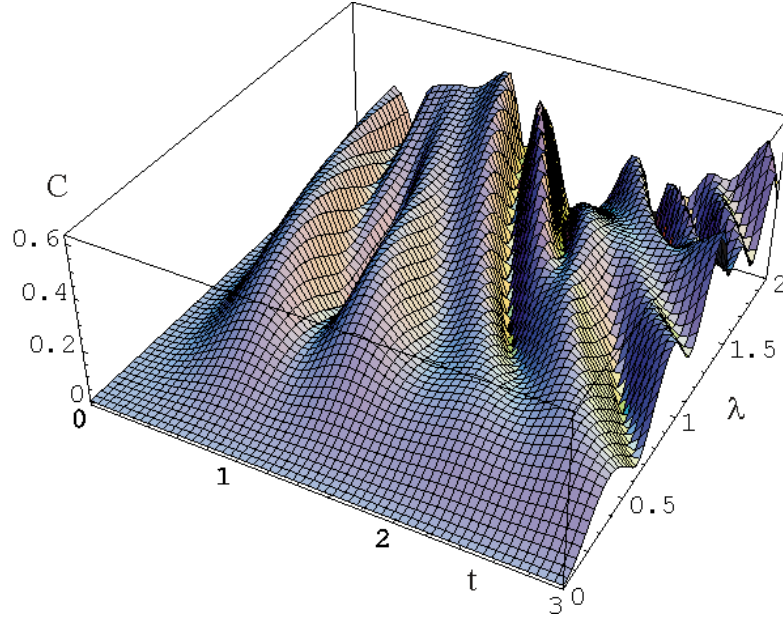
$$\psi = \frac{1}{\sqrt{3}} (|011\rangle + |101\rangle + |110\rangle). \quad (4.8)$$

Vybral som si tento stav preto, lebo obsahuje párny počet jednotiek, takže sa rozkladá na rovnaké štyri základné stavy Hamiltoniánu (4.1) ako vyššie spomínaný stav $|000\rangle$. Výsledky konkurencie sú uvedené na grafe (4.3).

Výsledky sú veľmi podobné tým, ktoré boli zreteľné pre faktorizovaný stav. Časový vývoj štartuje z maximálne možnej konkurencie a tá sa periodicky mení, pričom aj pre veľké hodnoty λ sa konkurencia vracia k vysokým hodnotám okolo 1. Zvláštne správanie okolo $\lambda = 1$ zostalo zachované.

4.3.3 GHZ vstupný stav

Ďalší zaujímavý stav pre skúmanie vývoja konkurencie je GHZ vstupný stav $|GHZ\rangle_3 = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)$. Jeho konkurencia na začiatku je nulová, hoci je maximálne entanglovaný. Vykazuje totiž maximálnu mieru trojčasticového entanglementu a žiaden dvojčasticový. Na grafe (4.4) je znázornená konkurencia susedných qbitov v závislosti od času a parametra λ . Charakteristický priebeh pre vyššie uvedené dva stavy (faktorizovaný a maximálne dvojčasticovo entanglovaný) už nie je pozorovateľný, priebeh je chaotickejší a je ťažké, zvlášť pre väčšie hodnoty λ , vystihnúť pravidelnosti. Môže to byť spôsobené tým, že kým dosiaľ sme pracovali stále len so stavmi, ktoré boli *párne*, GHZ stav je kombináciou párneho stavu $|000\rangle$ a nepárne-



Obrázok 4.4: Konkurencia pre vstupný GHZ stav v závislosti od λ a času. Časová závislosť je chaotickejšia ako v predchádzajúcich prípadoch, stále sú však pozorovateľné zmeny priebehu pre parametre $\lambda \simeq 0.5$ a $\lambda \simeq 1$.

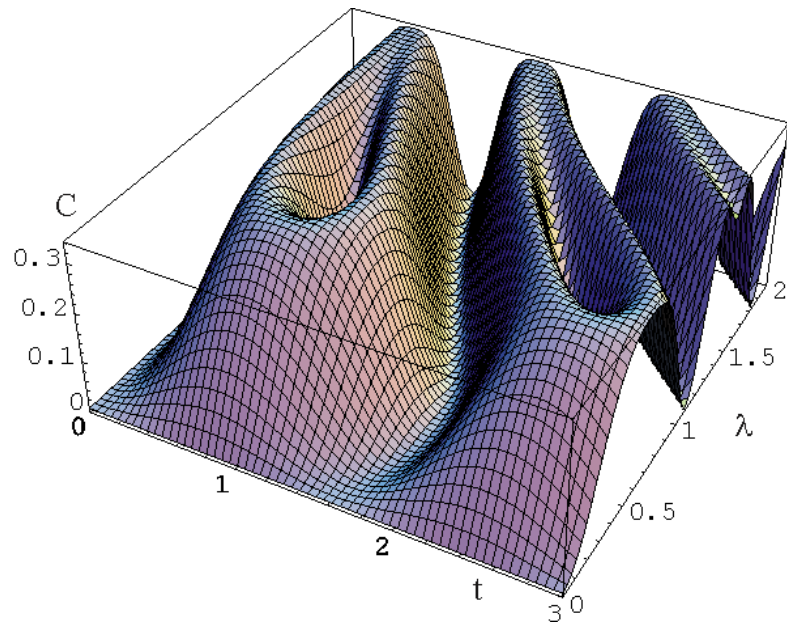
ho stavu $|111\rangle$. GHZ stav sa rozkladá do všetkých ôsmich základných stavov Hamiltoniánu a preto aj jeho časový vývoj je zložitejší a perióda dlhšia, keďže sa kombinuje vývoj nie podľa štyroch, ale už podľa ôsmich vlastných hodnôt. Zostala však zachovaná vlastnosť pozorovaná na párných stavoch, že pre $\lambda = 0.5$ a pre $\lambda = 1$ vykazuje graf isté zmeny správania, avšak pre $\lambda > 1$ sú už výsledky ťažko porovnateľné.

4.3.4 Základný stav ako vstupný stav

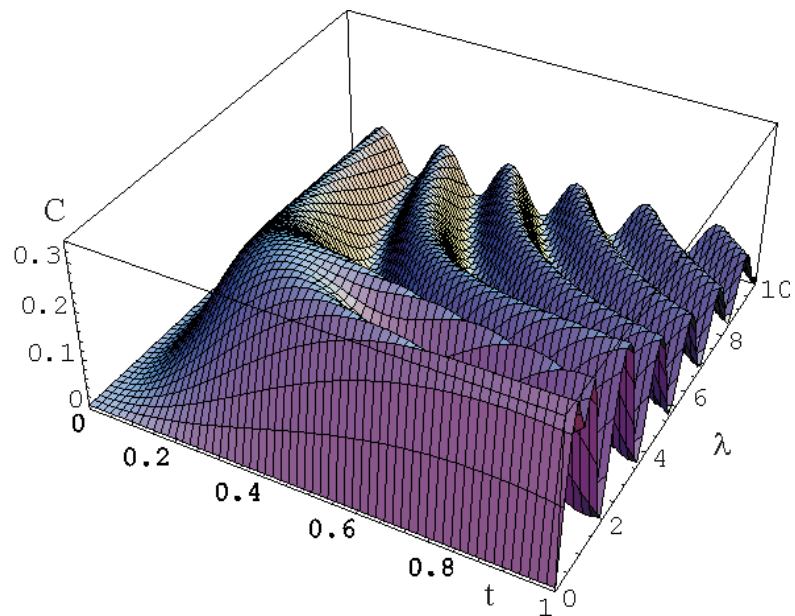
Štvrtým a posledným stavom, ktorému sa tu budem podrobnejšie venovať, je základný stav Hamiltoniánu. Samozrejme, tento základný stav je závislý od voľby parametra λ . Pre špeciálny prípad $\lambda = 0$ je to už uvažovaný stav $|000\rangle$, ale zaujímavý je tiež druhý špeciálny prípad, keď je λ dostatočne veľké. V tomto prípade bude základný stav podľa [37] typu

$$\psi = \frac{1}{2} (|000\rangle + |011\rangle + |101\rangle + |110\rangle). \quad (4.9)$$

Môžeme teraz skúmať časový vývoj takéhoto stavu pod vplyvom rôznych Hamiltoniánov. Očakávame, že pre veľké λ bude časový vývoj konštantný, keď tento stav je základným stavom Hamiltoniánu. Výsledky (pre rovnaké hodnoty parametrov ako v predošlých prípadoch) sú uvedené v grafe (4.5). Ako je zrejmé zo zápisu základného stavu, je to *párny* stav, a preto podľa očakávania dostávame jednoduchší vývoj ako pri GHZ stave. Tu ale nie je jasná tendencia, že pre veľké λ sa časový vývoj ustáľuje. Preto uvádzam aj graf (4.6), kde je os v λ predĺžená až do 10. Tu už je jasné, že vrcholy klesajú k nule a je dobrý predpoklad, že v limite $\lambda \rightarrow \infty$ zaniknú.



Obrázok 4.5: Časový vývoj konkurencie susedných qbitov stavu, ktorý je základným stavom Hamiltoniánu pre veľké λ . Je vidieť, že tvar kriviek sa čiastočne zmenil, ale je zreteľný istý prelom okolo $\lambda = 0.5$.



Obrázok 4.6: Vývoj základného stavu Hamiltoniánu pre $\lambda \rightarrow \infty$, ale tentokrát pre kratší čas a väčšie hodnoty λ . Je zrejmé, že peaky klesajú postupne k nule.

4.4 Prípád N=5

Pre porovnanie a overenie výsledkov získaných pre 3 qbity som zopakoval niekoľko podobných výpočtov aj pre 5 qbitov. Číslo 4 som preskočili z toho dôvodu, že pre párny počet častíc sa predpokladajú opačné okrajové podmienky a to by mohlo meniť naše výsledky. Väčší počet častíc skrýva v sebe ale aj niekoľko problémov.

Jednak je to väčšia výpočtová náročnosť. Hamiltonián je už matica 32×32 a 32 je aj počet vlastných vektorov, do ktorých sa vstupné stavy rozkladajú. Aj v tomto prípade môžeme deliť stavy na párne a nepárne, 16 stavov je však stále dosť veľké množstvo. Väčšina výpočtov preto bola robená numericky, náročnosť na strojový čas však dovolila vyprodukovať iba grafy s menším rozlíšením.

Ďalším problémom je, že pri väčšom počte častíc nám na charakterizovanie systému nestačí len jedna konkurencia. V tomto prípade musíme uvádzať minimálne dve, jednu medzi susednými qbitmi a ďalšiu medzi qbitmi, ktoré nesusedia. Žiadne ďalšie možnosti dvojčasticovej konkurencie už neexistujú, lebo keď si predstavíme 5 častíc v akomsi kruhu, tak nech vyberieme hociktoré dve z nich, buď budú susedmi, alebo bude medzi nimi z jednej strany práve jeden qbit. Pri piatich qbitoch je ale oprávnený predpoklad, že viacčasticový entanglement bude hrať oveľa väčšiu úlohu ako v predošlom prípade. Na overenie tejto domnienky uvádzam aj výsledky konkurencie typu jedna-zvyšok, ktorá meria entanglement jednej častice voči celému zvyšku systému. Ako sa ukáže, tento entanglement (na rozdiel od dvojčasticového) bude aj pre 5 qbitov periodický a bude dosahovať hraničné hodnoty.

4.4.1 Faktorizovaný vstupný stav

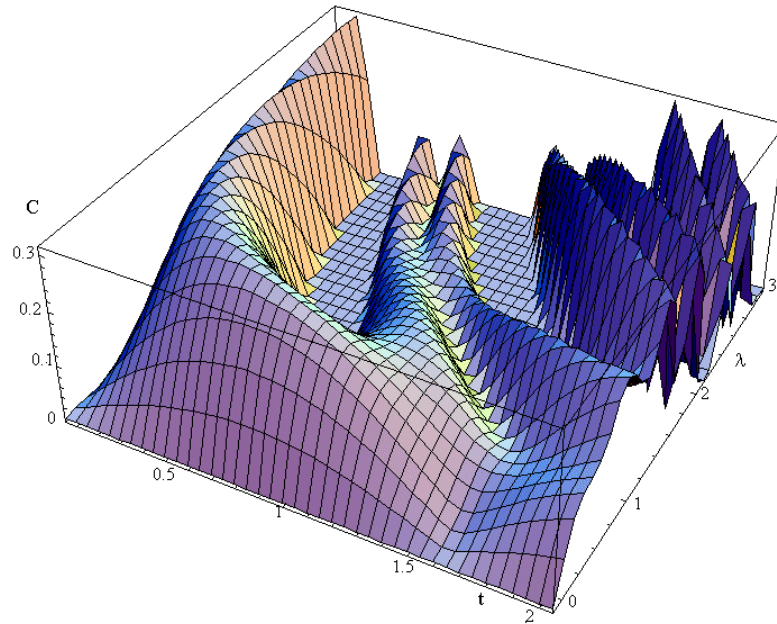
Podobne ako pre 3 qbity, aj tu sa zo začiatku sústredím na faktorizovaný stav. Použijem pre jednoduchosť stav $|00000\rangle$. Výsledky konkurencie pre susedné i nesusedné qbity sú uvedené na grafoch (4.7,4.8). Porovnanie oboch grafov ukazuje, že konkurencia susedných qbitov vzniká omnoho rýchlejšie ako vzdialenejších. Podobne maximálna konkurencia v priebehu sledovaného času je pri susedných qbitoch väčšia. Je to celkom pochopiteľné, keďže samotný Hamiltonián priamo viaže len susedné častice. Na druhej strane je zjavná tendencia poklesu konkurencie susedných častíc v oblastiach, kde prudko stúpa konkurencia vzdialenejších.

Okrem toho sa výrazne zväčšili oblasti nulovej konkurencie. V prípade troch qbitov bola nulová konkurencia dosahovaná len v časových bodoch (okrem triviálneho prípadu $\lambda = 0$), teraz sú to veľké časové úseky pre všetky parametre λ . Dôvodom je to, že entanglement sa musí deliť na dvojčasticový a viacčasticový a v prípade štych častíc môže vznikáť mnoho druhov viacčasticového entanglementu. Z iného pohľadu, konkurencia je definovaná pomocou vlastných hodnôt matice systému zredukovanej len na príslušné dva qbity. A čím bol pôvodný systém väčší, tým sa v priemere bude redukovaná matica blížiť úplnej zmesi. Vlastné hodnoty takejto matice budú navzájom blízke a preto vyjadrenie

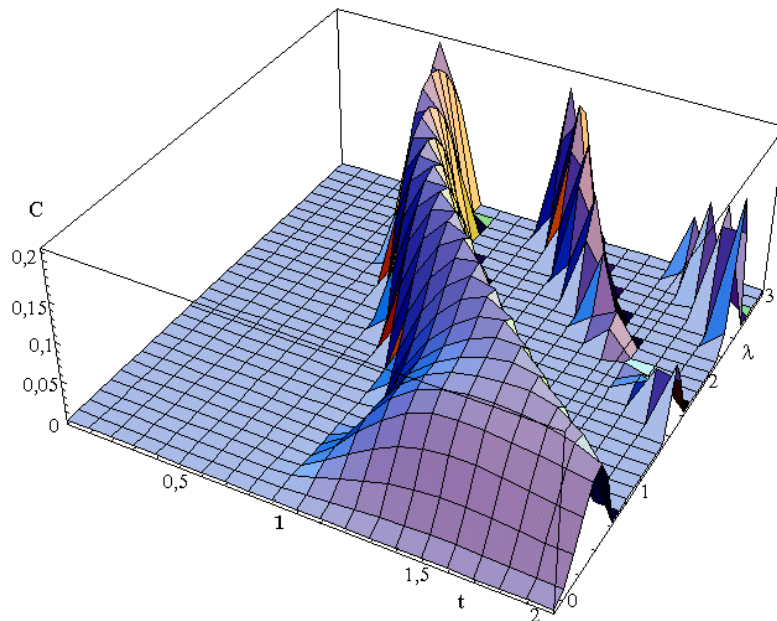
$$\text{Max}(\lambda_i) - \sum_i \lambda_i \quad (4.10)$$

bude stále záporné. Konkurencia, definovaná ako maximum z (4.10) a 0 bude zrejme nulová.

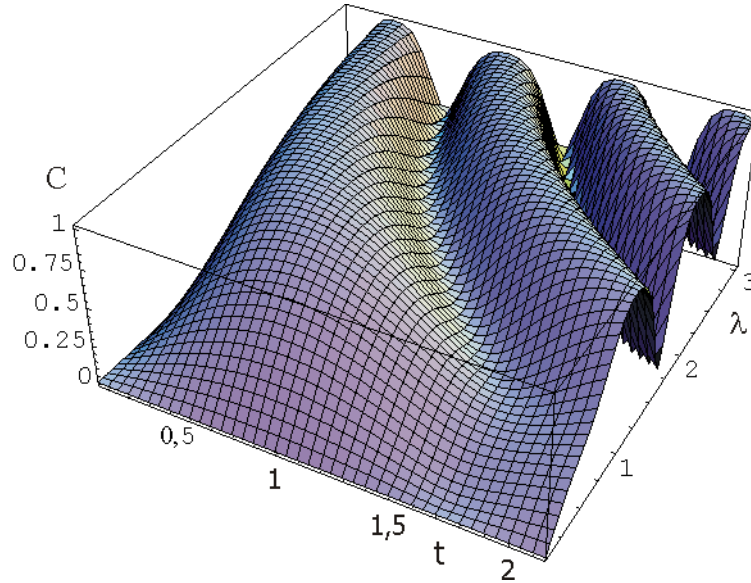
Pre porovnanie je nesporné zaujímavé uviesť aj konkurenciu prvej častice voči zvyšku, ktorá je na grafe (4.9). Táto závislosť je veľmi podobná rovnakej závislosti pri troch qbitoch. Je tiež vidieť, že konkurencia sa blíži svojej maximálnej hodnote 1, takže pre isté hodnoty



Obrázok 4.7: Závislosť konkurencie dvoch susedných qbitov od času a parametra λ pre faktorizovaný vstupný stav $|00000\rangle$. Oproti prípadu troch qbitov sa rozšírili oblasti nulovej konkurencie, ale zostala zachovaná vlastnosť grafu v okolí bodov 0.5 a 1 v parametre λ .



Obrázok 4.8: Konkurencia dvoch vzdialenejších qbitov pre faktorizovaný stav 5 qbitov. Zrejme sú rozsiahle oblasti nulovej konkurencie, pretože hlavne na začiatku vývoja Hamiltonián neumožňuje interakciu medzi nesusednými časticami. Možná je len sprostredkovaná interakcia, ktorá si vyžaduje istý čas, aby sa prejavila aj v konkurencii.



Obrázok 4.9: Konkurencia prvého qbitu voči zvyšnému systému pri faktorizovanom vstupnom stave piatich qbitov.

λ a isté časy dostávame stavy, ktoré sú blízke maximálne entanglovaným. Entanglement je však rozdelený medzi dvojčasticový a viacčasticový a pre mnohé časy je práve dvojčasticový entanglement nulový. Prakticky úplne sa však stratilo zvláštne správanie v okolí bodov $\lambda = 0.5$ a $\lambda = 1$. Je odôvodnený predpoklad, že v tomto prípade sa jednalo o špeciálnu vlastnosť trojčasticového systému.

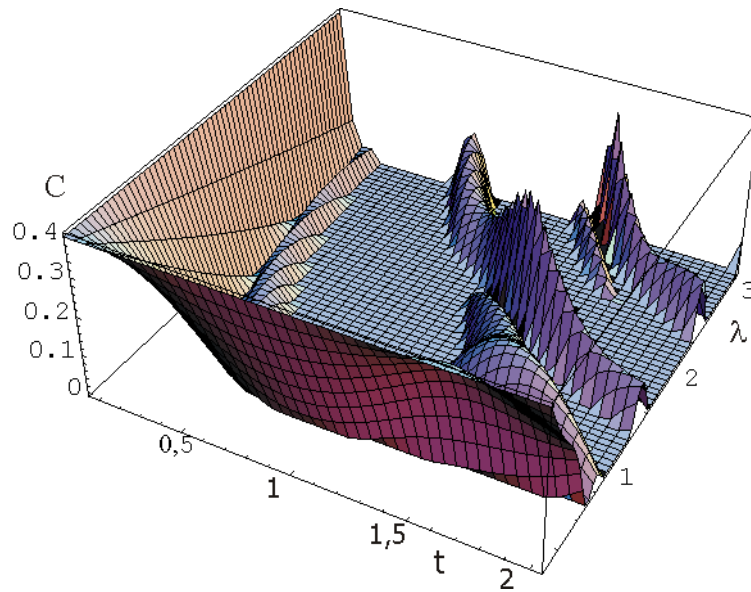
4.4.2 Symetrický vstupný stav

V tomto prípade som použil ako vstupný stav úplne symetrický stav 5tich qbitov, ktorý obsahuje práve jeden qbit v stave $|1\rangle$. Výsledky pre konkurenciu dvoch susedných qbitov, dvoch vzdialenejších qbitov aj konkurenciu prvého voči zvyšku systému je na grafoch (4.10 až 4.12).

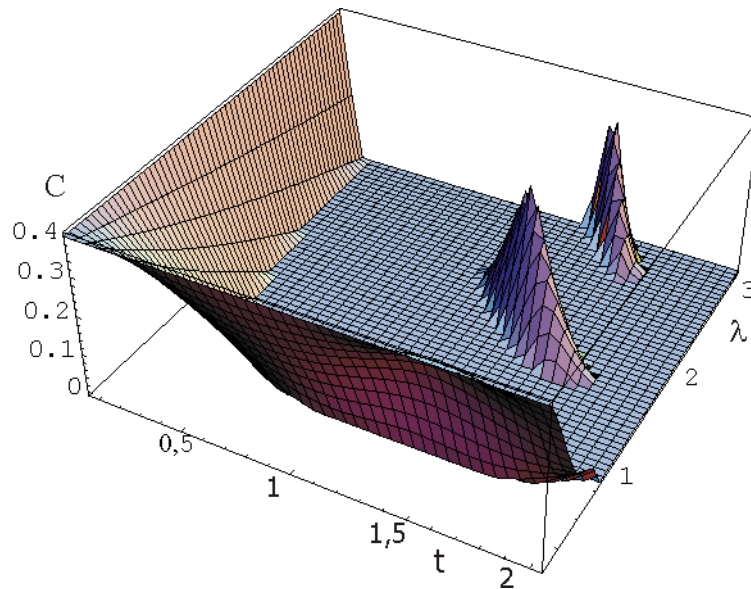
Najzaujímavejší je asi prvý graf. Silný dvojčasticový entanglement sa pôsobením Hamiltoniánu stráca prekvapivo rýchlo a nie je pozorovateľné periodické správanie, takže entanglement sa už nevracia do pôvodných veľkostí. Porovnanie ale ukazuje, že celkový entanglement sa nezmenšuje natrvalo, takže usudzujem, že z dvojčasticového entanglementu susedných častíc vzniká entanglement nesusedných častíc a viacčasticový entanglement. Dá sa predpokladať, že ani v priebehu ďalšieho časového vývoja sa situácia nezmení.

4.4.3 GHZ vstupný stav

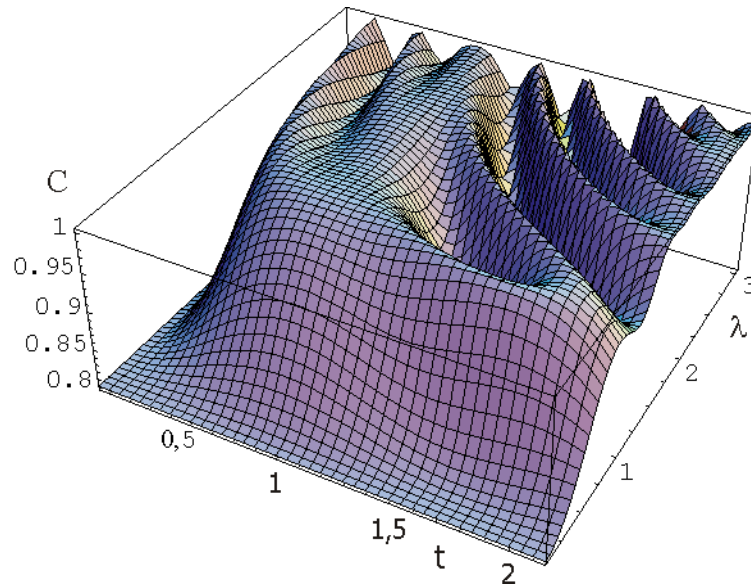
Ako posledný zaujímavý vstupný stav som uvažoval GHZ stav. Rovnako ako v prípade troch qbitov, aj pri piatich sa v rozklade GHZ stavu do vlastných stavov Hamiltoniánu nachádzajú párne aj nepárne vlastné stavy. Týmto sa stav líši od predtým uvádzaného faktorizovaného a symetrického stavu. Predpokladáme teda komplikovanejší časový vývoj (grafy 4.13 až 4.15), ktorý je pozorovateľný hlavne na poslednom grafe, ukazujúcom vývoj konkurencie jednazyšok. Rovnako ako v prípadoch predošlých, aj tu sa ukazuje, že v priebehu časového



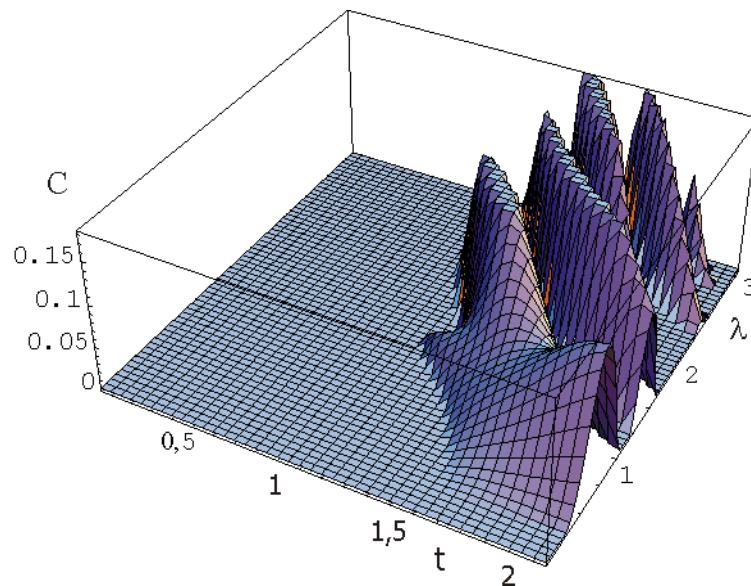
Obrázok 4.10: Konkurencia dvoch susedných qbitov pri symetrickom vstupnom stave. Tento stav obsahuje na začiatku silný dvojčasticový entanglement, ktorý sa ale rýchlo stráca a v skúmanej oblasti parametrov sa už nevytvára, aspoň nie v pôvodnej miere.



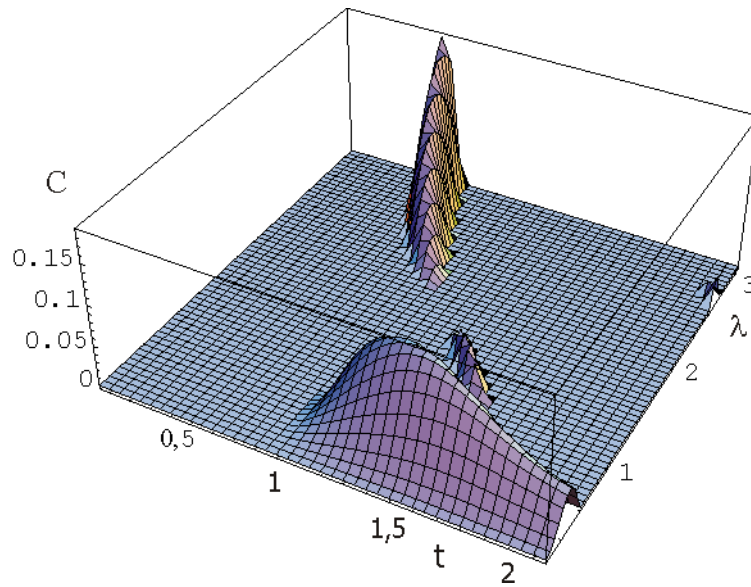
Obrázok 4.11: Konkurencia dvoch vzdialenejších qbitov pri vstupnom symetrickom stave. Tento stav je symetrický voči zámene dvoch qbitov, preto pre nulový čas vykazuje rovnakú hodnotu konkurencie ako pre susedné qbity. Pod časovým vývojom však rýchlo klesá k nule, ale niektorých časoch je jeho hodnota na malom úseku pomerne veľká.



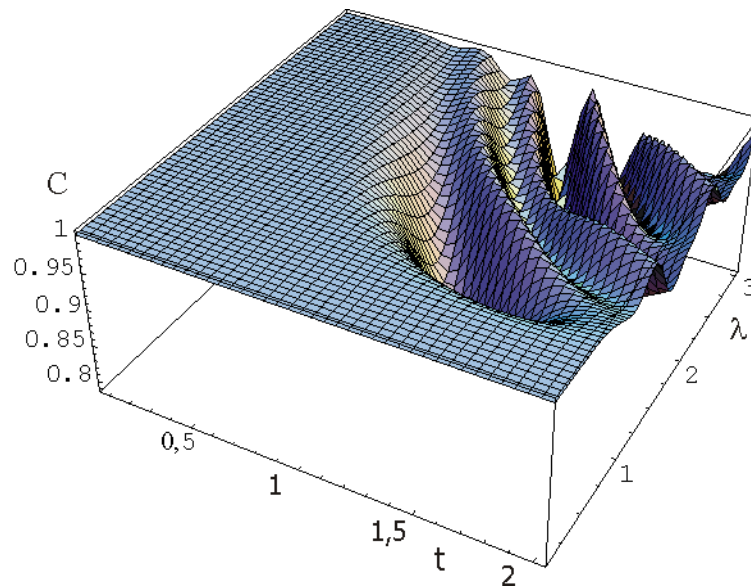
Obrázok 4.12: Konkurencia prvej častice voči zvyšku systému pre symetrický vstupný stav. Vstupný stav je maximálne entanglovaný, časový priebeh sa podobá závislosti pozorovanej pre 3 qbity. Hodnota 0.8 je hodnota entanglementu vstupného stavu. Veľmi zaujímavé je, že v priebehu časového vývoja konkurencia nikde neklesá pod túto hodnotu.



Obrázok 4.13: Konkurencia dvoch susedných qbitov pre GHZ vstupný stav. Ten obsahuje len mnohočasticový entanglement, takže je pochopiteľné, že istý čas trvá, kým dvojčasticový entanglement vznikne. Ani jeho absolútne veľkosti nedosahujú limity, pretože sa musí deliť s ostatnými formami entanglementu.



Obrázok 4.14: Konkurencia dvoch nesusediacich qbitov pre GHZ vstupný stav. Je zaujímavé, že závislosť je hladšia ako v prípade susediacich qbitov.



Obrázok 4.15: Konkurencia prvého qbitu voči zvyšku pre vstupný GHZ stav. Pôvodný, päťčas-ticový entanglement je veľmi robustný a počas dlhej periódy sa vôbec nenaruší maximálna entanglovanosť. Až po dlhšom čase a pre väčšie hodnoty λ klesá entanglement z jednotky nižšie.

vývoja sa miera celkového entanglementu v systéme pohybuje na vysokej úrovni a do nuly, z ktorej štartuje, sa už nevracia. Keďže dvojčasticový entanglement predstavuje len jednu z mnohých možností entanglovania, je pochopiteľné, že sa objavuje len málokedy a rýchlo mizne. Z porovnania grafov vyplýva, že vo väčšine prípadov zrejme dominuje 3- a viac-časticový entanglement.

4.5 Záver

V tejto kapitole som sa pokúsil poskytnúť fenomenologický pohľad na entanglement v jednorozmernom Isingovom modeli s priečnym magnetickým poľom. Ako ukazujú výsledky, časový vývoj entanglementu v sebe skrýva mnoho zaujímavého a možno aj dosiaľ neznámeho. Pokúsil som sa čo najlepšie určiť, čo sa s entanglementom deje a v niektorých prípadoch aj to, prečo je to tak.

V článku [19] je okrem vyššie spomínanej nerovnosti pre 3 qbity, ktorá bola dokázaná a platnosť ktorej som uvedenými výsledkami potvrdil, aj všeobecnejšia nerovnosť, ktorá ale dokázaná nie je. Táto nerovnosť má pre N qbitov tvar

$$C_{12}^2 + C_{13}^2 + \dots + C_{1N}^2 \leq C_{1(2\dots N)}^2. \quad (4.11)$$

Na ľavej strane je súčet druhých mocnín všetkých dvojčasticových konkurencií prvého qbitu a na pravej strane celková konkurencia prvého qbitu voči zvyšku systému. Táto nerovnosť je logickým rozšírením nerovnosti (4.6) pre viac qbitov, lebo tvrdí len to, že celkový dvojčasticový entanglement nikdy nemôže byť väčší ako celkový entanglement.

Výsledky pre N qbitov potvrdzujú platnosť nerovnice (4.11). Pre GHZ a symetrický vstupný stav to je zrejme už z letného pohľadu na grafy. Celkový entanglement nikdy neklesá pod hodnotu 0.8, teda jeho druhá mocnina je zdola ohraničená (aspoň v skúmanom intervale) hodnotou 0.64. Ľavá strana (4.11) sa dá prepísať ako

$$2.C_{sus}^2 + 2.C_{vzdial}^2, \quad (4.12)$$

pričom hodnota dvojčasticových entanglementov je pre symetrický stav ohraničená hodnotou 0.4 a pre GHZ stav dokonca ešte menšou hodnotou 0.2. Je preto zrejme, že pre tieto dva stavy nerovnosť určite narušená nebude. Pre faktorizovaný vstupný stav sa podobné odhady urobiť nedajú (lebo obe strany nadobúdajú nulovú hodnotu pre vstupný stav), ale jednoduchá kontrola získaných výsledkov ukázala, že v skúmaných intervaloch hodnôt nerovnosť narušená nie je. Môžem teda uzavrieť, že pre istú oblasť stavov 5 qbitov som potvrdil platnosť navrhovanej nerovnosti.

Bolo by nesporne veľmi zaujímavé porovnávať nie len dvojčasticový a viacčasticový entanglement, ale rôzne typy entanglementu (troj-, štvorčasticový) navzájom. Toto bolo možné pre špecifický prípad $N = 3$, kde sme dokázali spočítať dvojčasticový aj celkový entanglement a z toho jednoduchým rozdielom aj trojčasticový. Pre väčšie systémy to už bohužiaľ nie je možné. V súčasnosti neexistuje spôsob, ako priamo kvantifikovať viacčasticový entanglement. Dokonca neexistuje ani zhoda v tom, či viacčasticový entanglement je len istá forma dvojčasticového, alebo sa jedná o čosi celkom iné. V prospech prvej možnosti hovorí to, že aj pomocou dvojčasticových operácií dokážeme vytvárať viacčasticový entanglement (čo je v kontraste so známym faktom, že jednočasticovými operáciami sa entanglement, ani dvojčasticový, nevytvorí). V prospech druhej možnosti zasa hovorí to, že z rýdzo trojčasticového

entanglementu sa klasickou komunikáciou a jednočasticovými operáciami nedá vyrobiť entanglement dvojčasticový. Pokiaľ by sa ale v budúcnosti našli spôsoby, ako výpočtovo jednoducho získať veľkosti viacčasticového entanglementu pre všeobecné stavy, určite by bolo zaujímavé skúmať aj tento model.

Zaujímavé by bolo zistiť, či zvláštne správanie sa dynamiky pre 3 qbity je naozaj viazané iba na tento počet alebo sa znova objavuje pri väčších množstvách častíc. Tiež to, či aj pri zvyšujúcom sa počte qbitov zostane priebeh konkurencie jedna-zvyšok podobný ako pre malé počty, čo by zodpovedalo logike, že entanglement vzniká vždy, len sa podľa počtu častíc delí na dvoj a viacčasticový. Predpoklad, že so zväčšujúcim sa počtom častíc sa bude postupne vytrácať dvojčasticový entanglement (špeciálne nesusedných častíc; susedné majú to exkluzívne postavenie, že môžu priamo interagovať a predpokladá sa, že to bude zaručovať istú mieru entanglementu aj vo veľkých systémoch), by si tiež zaslúžil potvrdenie.

Z celkového pohľadu na výsledky sa dá usudzovať, že tam, kde je badateľná časová perióda vývoja sa táto skracaje so zväčšujúcim sa λ . Bolo by zaujímavé overiť túto skutočnosť aj na dlhších časových úsekoch. Podobne tiež to, či sa pri väčších systémoch dvojčasticový entanglement z pôvodného stavu skutočne stráca natrvalo, alebo sa jedná len o dej s periódou väčšou ako skúmané časy.

V priebehu kompletizovania výsledkov bol uverejnený článok [38], ktorý sa zaoberá podobnou problematikou. Rozoberá entanglement Isingovho modelu len dvoch častíc, ale nie v závislosti na čase, ale na teplote. Okrem iných výsledkov prišli na zaujímavý poznatok: pri nulovej teplote sa pre nulové magnetické pole odohráva fázový prechod druhého druhu, keď sa skokom mení entanglement z nulového na nenulový.

Kapitola 5

Záver

Táto diplomová práca má tri hlavné kapitoly, v ktorých sa snažím naplniť tri základné ciele: urobiť prehľad problematiky, predložiť spracované výsledky a navrhnúť smery ďalšieho skúmania. Prvá z kapitol vytvára ucelený prehľad o entanglemente a snažil som sa, aby bola uzavretým celkom. Mala poskytnúť všetky potrebné informácie o entanglemente, zameral som sa pri tom primárne na jednoduché systémy - qbity. Zozbieral som informácie z kníh, ktoré boli publikované a doplnil som ich o najnovšie poznatky z vedeckých článkov. Vyberal som fakty, ktoré sú z môjho pohľadu najdôležitejšie pre pochopenie podstaty javu a snažil som sa vyhnúť komplikovanej matematike, pokiaľ nebola naozaj potrebná. Dôkazy všetkých tvrdení (ak nie sú uvedené v texte) a možno detailnejšie sformulované vety sa dajú nájsť v referenciách. Dúfam, že sa mi podarilo nájsť kompromis medzi požiadavkou, aby bol text ľahko čitateľný a nevyžadoval prílišnú hĺbku ponorenia sa do problematiky a tým, aby sa nevynechali dôležité fakty.

Vlastné výsledky sú publikované v ďalšej kapitole. Podrobne je rozobratá možnosť posielat' kvantový bit informácie cez zašumený kanál pomocou symetrizácie a použitia redundantných qbitov. Napriek tomu, že výsledky neboli veľmi povzbudzujúce a ukázalo sa, že postup nie je vo všeobecnosti veľmi efektívny, za hlavný prínos považujem výslednú tabuľku. Je v nej uvedené, pre dané parametre chybového Pauliho kanála, optimálne množstvo qbitov na prepravu informácie. Veľmi zaujímavým bolo zistenie, že ako optimálne sa ukazujú byť reálne počty častíc, keď pre depolarizačný kanál (ktorý je najrealistickejší z Pauliho kanálov, pretože nemá určenú os, v smere ktorej chyby primárne pôsobia) dostávame maximum 8 qbitov. Zároveň je ale potrebné zdôrazniť, že k praktickej aplikácii má navrhovaný spôsob ešte ďaleko, lebo vyžaduje operácie pôsobiace naraz na všetkých časticiach, čo je zatiaľ veľký problém v praxi uskutočniť.

Kapitola venovaná Isingovmu modelu kladie viac otázok, ako dáva odpovedí. Snažil som sa v nej ukázať, že štúdium entanglementu v Isingovom modeli, ktorý zdanlivo už nemôže skrývať nič nové, prináša zaujímavé zistenia. Prezentujem výsledky pre malé počty častíc (3 a 5 qbitov) s tým, že sa snažím odhaľovať zaujímavé tendencie na grafoch časovej závislosti. Na skúmaných stavoch sa potvrdil dohad o platnosti nerovnosti medzi viacčasticovým a dvojčasticovým entanglementom, navrhnutý v článku [19].

Bohužiaľ, nepodarilo sa mi nájsť záchytné body, podľa ktorých by sa dali predpovedať fázové prechody pri väčšom počte častíc. Hoci pre 3 qbity sa ukazovali niektoré zmeny v správaní sa grafov pre $\lambda = 1$, neboli potvrdené pre 5 častíc. To samozrejme neznamená, že pri ďalšom skúmaní väčšieho počtu qbitov sa náznaky fázových prechodov nezačnú prejavovať.

Za veľmi zaujímavý pokladám zistený fakt, že nezávisle od vstupného stavu aj Hamiltonián, ktorý viaže vždy len susedné častice, vytvára mnohočasticový entanglement. V priebehu časového vývoja sa entanglement udržiava na veľmi vysokej úrovni, čo poukazuje na dôležitú rolu, ktorú zrejme entanglement pri podobných modeloch zohráva. Okrem toho, zdá sa, že dvojčasticový entanglement nie je žiadnym spôsobom preferovaný oproti viacčasticovému. Hrubé odhady priemernej hodnoty dvojčasticového entanglementu v priebehu časového vývoja v porovnaní s priemerom celkového entanglementu zodpovedajú počtu možných dvojíc v systéme v porovnaní s počtom všetkých možných skupín (dvojíc, trojíc, štvoric a päťice pre 5 qbitov). Znamená to, že pokiaľ by sme mali možnosti kvantitatívne počítať aj viacčasticové entanglementy, zrejme by sa ukázalo, že všetky sú v priebehu časového vývoja približne rovnako zastúpené.

Tento poznatok je veľmi dôležitý, okrem iného, aj z praktického pohľadu. S využitím len dvojčasticových operácií, ktoré sú experimentálne relatívne ľahko dosiahnuteľné, dokážeme produkovať stavy, ktoré vykazujú silné mnohočasticové korelácie.

Na záver by som rád zhrnul výsledky, ktoré som vo svojej práci dosiahol:

- Ukázalo sa, že napriek optimistickým návrhom uvádzaných v článku [26] nie je symetrizácia vhodný spôsob na stabilizáciu systému.
- Aj pre tie parametre, kde sa ukazuje výhodnejšie používať viac qbitov ako jeden, je zisk veľmi diskutabilný, lebo chyby sú v každom prípade veľmi veľké a získaný rozdiel vo fidelite je oproti celkovej strate pri prenose prakticky zanedbateľný.
- Pre špecifický prípad, ak chyby pôsobia iba na jeden qbit systému, sa podarilo nájsť optimálne počty qbitov.
- Pri skúmaní Isingovho modelu sa ukázalo, že hľadané fázové prechody nie je dostatočne dobre možné odpozorovať už pri malých počtoch častíc, ako sme dúfali, a to ani za pomoci entanglementu.
- Časový vývoj už pri piatich qbitoch je veľmi komplikovaný a je problematické hľadať v ňom periodicity.
- Celkový entanglement systému je počas celého časového vývoja a pre prakticky celú oblasť parametrov Hamiltoniánu veľmi vysoký. Svoje horné hranice dosahuje veľmi rýchlo nezávisle na vstupnom stave, pričom dvojčasticový entanglement nie je nijako uprednostňovaný.
- Podarilo sa potvrdiť pre skúmané stavy nerovnosti z článku [19], ktoré boli z časti uvádzané len ako domnienky.

Dúfam, že sa mi čitateľovi podarilo presvedčiť o nesmiernej zaujímavosti problematiky entanglementu a vecí súvisiacich. Rád by som sa tomu naďalej venoval a prispieval svojou troškou k vnášaniu svetla do oblastí dosiaľ zahalených tajomstvom. Som presvedčený, že kvantové korelácie skrývajú v sebe nečakaný potenciál a verím, že v budúcnosti ho dokážeme vo veľkej miere aj prakticky využívať.

Dodatok A

Dôkaz Peres-Horodeckého teorémy

V tomto dodatku uvediem dôkaz Peres-Horodeckého teorémy, týkajúcej sa podmienok separability nízkorozmerných systémov. Hovorí, že pre systémy typu 2×2 až 2×3 je podmienka kladnej čiastočnej transpozície (PPT) nutnou a postačujúcou podmienkou separability systému, pre systémy vyšších rozmerov zostáva nutnou podmienkou. Myšlienka dôkazu pochádza z článku [8].

Zaveďme si potrebné označenia. Hilbertov priestor, v ktorom pracujeme, a jeho dva podpriestory prislúchajúce prvej a druhej časti systému označme H, H_1 a H_2 ;

$$H = H_1 \otimes H_2. \quad (\text{A.1})$$

Operátor ρ na tomto priestore budeme nazývať stavom vtedy a len vtedy, ak je normovaný ($\text{Tr}(\rho) = 1$) a pre každý projektor P na priestore H platí

$$\text{Tr}(\rho P) \geq 0. \quad (\text{A.2})$$

Stav budeme nazývať separabilným vtedy, ak platí

$$\rho = \sum_{i=1}^k p_i \rho_i \otimes \tilde{\rho}_i, \quad (\text{A.3})$$

kde $\rho_i, \tilde{\rho}_i$ sú stavy na priestoroch H_1 a H_2 . Množiny A_1 a A_2 označujú operátory pôsobiace na príslušné Hilbertove priestory. Ďalej $\mathcal{L}(A_1, A_2)$ je množina všetkých zobrazení z priestoru A_1 do priestoru A_2 . Zobrazenie

$$\Lambda \in \mathcal{L}(A_1, A_2) \quad (\text{A.4})$$

je pozitívne vtedy, ak pre každé $K \geq 0$ je $\Lambda(K) \geq 0$. Zobrazenie je úplne pozitívne, ak

$$\Lambda_n = \Lambda \otimes I_n : A_1 \otimes M_n \rightarrow A_2 \otimes M_n, \quad (\text{A.5})$$

kde M_n je priestor štvorcových matíc $n \times n$, je pozitívne pre každé n . Je dôležité zdôrazniť, že existujú zobrazenia, ktoré sú pozitívne, ale nie sú úplne pozitívne, teda samé osebe zobrazujú pozitívne stavy na pozitívne, ale v kombinácii s operátorom identity už môžu zobrazovať pozitívne stavy na nepozitívne.

Metóda čiastočnej transpozície matice hustoty je práve zobrazením, ktoré je pozitívne, ale nie nutne úplne pozitívne. Je pochopiteľné, že na faktorizovanom stave $\rho \otimes \tilde{\rho}$ je operátor $\Lambda \otimes I_n$ pozitívny, lebo sa dá zapísať:

$$(\Lambda \otimes I_n) \rho \otimes \tilde{\rho} = \Lambda \rho \otimes I_n \tilde{\rho}. \quad (\text{A.6})$$

Na nefaktorizovaných stavoch to už ale nemusí byť pravda. V ďalšom sa pokúsim ukázať, že práve zobrazenie **transpozícia** reprezentuje na priestore 2×2 a 2×3 všetky možné prípustné nie úplne pozitívne zobrazenia a preto pozitívita PPT je nutnou a postačujúcou podmienkou na separabilitu systému.

Využijeme lemmu, ktorá hovorí:

Lemma 1 *Pre každý neseparabilný stav $\rho \in A_1 \otimes A_2$ existuje Hermitovský operátor \tilde{A} taký, že*

$$\text{Tr}(\tilde{A}\rho) < 0 \quad \text{a} \quad \text{Tr}(\tilde{A}\sigma) \geq 0 \quad (\text{A.7})$$

pre každú separabilnú maticu hustoty σ .

Dôkaz (s využitím Hahn-Banachovej vety explicitnou konštrukciou operátora \tilde{A}) je uvedený v článku [8]. S využitím tejto lemmy môžeme formulovať

Theorem 2 *Stav $\rho \in A_1 \otimes A_2$ je separabilný vtedy a len vtedy, ak*

$$\text{Tr}(A\rho) \geq 0 \quad (\text{A.8})$$

platí pre každý Hermitovský operátor A spĺňajúci podmienku $\text{Tr}(AP \otimes Q) \geq 0$, kde P a Q sú projektory na príslušné priestory H_1 a H_2 .

Proof. Ak je ρ separabilná, zrejme spĺňa rovnicu (A.8). Predpokladajme teraz, že existuje stav spĺňajúci (A.8) a nie je separabilný. V tom prípade by sme, podľa Lemmy 1, dokázali nájsť operátor A , pre ktorý by platilo $\text{Tr}(A\rho) < 0$. Pritom by ale platilo, že $\text{Tr}(A\sigma) \geq 0$ pre všetky separabilné σ . Každá σ sa ale dá zapísať ako súčin projektorov $P \otimes Q$ a tým sa dostávame do sporu s predpokladom vety. ■

Teraz ešte potrebujeme previesť vetu do jazyka lineárnych zobrazení. Na to využijeme izomorfizmus medzi priestorom lineárnych zobrazení $\mathcal{L}(A_1, A_2)$ a stavov na $A_1 \otimes A_2$:

$$\Lambda \in \mathcal{L}(A_1, A_2) \quad \rightarrow \quad S(\Lambda) = \sum_i E_i^+ \otimes \Lambda(E_i) \in A_1 \otimes A_2. \quad (\text{A.9})$$

Zavedme bázu na priestore A_1 : budú to operátory $\{P_{ij}\}_{i,j=1}^{\dim H_1}$ určené podmienkou $P_{ij}e_l = \delta_{ij}e_l$ pre všetky i, j, l pre danú bázu e_l v priestore H_1 . Potom môžeme rovnicu (A.9) prepísať na

$$\text{Tr} \left\{ \left[(I \otimes \Lambda) \sum_{ij} P_{ji} \otimes P_{ij} \right] \rho \right\} \geq 0 \quad (\text{A.10})$$

a ďalej, ak zavedieme symbol pre transpozíciu T , $T^2 = 1$

$$\text{Tr} \left\{ \left[(I \otimes T\Lambda) \sum_{ij} P_{ji} \otimes TP_{ij} \right] \rho \right\} \geq 0. \quad (\text{A.11})$$

Zrejme pre každé pozitívne Λ je aj $T\Lambda$ pozitívne. Ak zavedieme operátor

$$P_0 = \frac{1}{\dim H_1} \sum_{ij} P_{ji} \otimes P_{ji}, \quad (\text{A.12})$$

môžeme rovnicu prepísať do podoby

$$\langle \rho, (I \otimes \Lambda P_0)^+ \rangle \geq 0 \quad (\text{A.13})$$

a s využitím hermitovosti Λ , a teda aj $I \otimes \Lambda$ a tiež P_0

$$\langle \rho, I \otimes \Lambda P_0 \rangle \geq 0 \quad (\text{A.14})$$

Ďalšou úpravou získame rovnicu

$$\langle I \otimes \Lambda \rho, P_0 \rangle \equiv \text{Tr} [P_0(I \otimes \Lambda \rho)] \geq 0, \quad (\text{A.15})$$

ktorá má platiť pre každé pozitívne zobrazenie Λ . Zrejme, ak je ρ separabilný stav, potom rovnica (A.15) splnená je. Naopak, ak $I \otimes \Lambda \rho$ je pozitívny pre každé Λ , potom keďže P_0 je projektor, rovnica (A.15) je splnená a stav je separabilný. To nám umožňuje formulovať Peres-Horodeckého teorému pre všeobecný rozmer:

Theorem 3 *Nech ρ je stav na priestore $H_1 \otimes H_2$. Potom ρ je separabilná vtedy a len vtedy, keď pre každé pozitívne zobrazenie $\Lambda \in \mathcal{L}(A_1, A_2)$ operátor $I \otimes \Lambda \rho$ je pozitívny.*

V článku [8] je bližšie rozobratý prípad nízkych rozmerov H_1 a H_2 , konkrétne 2×2 a 3×2 . Pre tieto rozmery platí, že každé pozitívne zobrazenie Λ sa dá zapísať vo forme

$$\Lambda = \Lambda_1^{UP} + \Lambda_2^{UP} T, \quad (\text{A.16})$$

kde skratka UP znamená úplnu pozitivitu. Dôsledkom je, že jediné zobrazenie, ktoré musíme reálne skúmať v takýchto prípadoch je práve transpozícia, čo umožňuje formulovať vetu pre rozmery priestorov 2×2 a 3×2 :

Theorem 4 *Stav ρ na priestoroch $C^2 \otimes C^2$ a $C^3 \otimes C^2$ je separabilný vtedy a len vtedy, keď má kladnú čiastočnú transpozíciu PPT.*

Literatúra

- [1] Einstein, Podolsky, Rosen: Can quantum-mechanical description of physical reality be considered complete?, *Physical Review* 47, 777 (1935)
- [2] N. Bohr: Can quantum-mechanical description of physical reality be considered complete?, *Physical Review* 48, 696 (1935)
- [3] D. Bohm: *Quantum theory*, Prentice-Hall, New York, 614 (1951)
- [4] J. S. Bell: On the Einstein-Podolsky-Rosen paradox, *Physics* 1, 195-200 (1964)
- [5] A. Peres: *Quantum theory: Concepts and methods*, Kluwer Academic Publishers
- [6] J. Preskill: *Quantum Information and Computation*, lecture notes, (1998)
- [7] A. Peres: Separability Criterion for Density Matrices, *quant-ph* 9604005
- [8] M. Horodecki, P. Horodecki, R. Horodecki: Separability of mixed states: necessary and sufficient conditions, *quant-ph*/9605038
- [9] M. Horodecki, P. Horodecki, R. Horodecki: Separability of n-particle mixed states: necessary and sufficient conditions in terms of linear maps, *quant-ph*/0006071
- [10] M. Horodecki, P. Horodecki, R. Horodecki: Limits for Entanglement Measures, *Physical Review Letters* 84, 2014 (2000)
- [11] M. B. Plenio, V. Vedral: Teleportation, entanglement and thermodynamics in the quantum world, *Contemporary physics* 39/6, 431 (1998)
- [12] A. Aspect, J. Dalibard, G. Roger: Experimental Test of Bell's Inequalities Using Time-Varying Analyzers, *PRL* 49, 1804 (1982)
- [13] www.uibk.ac.at
- [14] A Zeilinger et al.: Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement, *PRL* 82, 1345 (1999)
- [15] I. C. Percival: Why do Bell experiments?, *quant-ph*/0008097
- [16] W. K. Wootters: Entangled Chains, *quant-ph*/0001114
- [17] W. K. Wootters: Entanglement of Formation of an Arbitrary State of Two Qubits, *PRL* 80, 2245 (1998)

- [18] S. Hill, W. K. Wootters: Entanglement of a pair of quantum bits, PRL 78, 5022 (1997)
- [19] V. Coffman, J. Kundu, W. K. Wootters: Distributed entanglement, PRA 61, 052306 (2000)
- [20] W. Dür: Entanglement molecules, quant-ph/0006105
- [21] J. Eisert, H. J. Briegel: Quantification of Multi-Particle Entanglement, quant-ph/0007081
- [22] W. Duer, G. Vidal, J. I. Cirac: Three qubits can be entangled in two inequivalent ways, quant-ph/0005115
- [23] Ch. H. Bennett, S. J. Wiesner: Communication via One- and Two-Particle Operators on EPR States, PRL 69, 2881 (1992)
- [24] E. S. Fry, R. C. Thompson: Experimental Test of Local Hidden-Variable Theories, PRL 37, 465 (1976)
- [25] M. Koashi, V. Bužek, N. Imoto: Entangled webs: Tight bound for symmetric sharing of entanglement, PRA 62, 50302 (2000)
- [26] A. Barenco et al.: Stabilisation of Quantum Computations by Symmetrisation, quant-ph/9604028
- [27] Vladimír Bužek, Mark Hillery: Quantum disentanglers, PRL 62, 52303 (2000)
- [28] A. S. Holevo: Some estimates of the information transmitted by a quantum communication channel, Probl. Inf. Transm. 9, 177-183 (1973).
- [29] A. K. Ekert: Quantum cryptography based on Bell's theorem, PRL 67, 6, 661-663 (1991).
- [30] A. M. Steane: Error correction codes in quantum theory, PRL 77, 5, 793-797 (1996).
- [31] M. A. Nielsen, I. L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press, 2000
- [32] M. Lewenstein et. all.: Separability and distillability in composit quantum systems, quant-ph/0006064
- [33] P. Rungta et. all.: Qudit Entanglement, quant-ph/0001075
- [34] S. L. Braunstein: Teleportation of Continuous Quantum Variables, PRL 80, 869 (1998)
- [35] S. L. Braunstein, V. Bužek, M. Hillery: Quantum information distribution: Quantum network for symmetric and assymetric cloning in arbitrary dimensions and continuous limit
- [36] V. Bužek, osobná komunikácia.
- [37] P. Štelmachovič: Ising Model from the point of entanglement; to be published.
- [38] D. Gunlycke et al.: Thermal concurrence mixing in a 1D Ising model, quant-ph/0102137