

**České vysoké učení technické v Praze  
Fakulta jaderná a fyzikálně inženýrská, kat. fyziky**

**S. Vymětal**

**Nelineární zobrazení v kvantové informaci a jeho vlastnosti**

## Obsah

1. Úvod .....	3
2. Provázanost kvantového systému .....	6
3. Konstrukce purifikačních protokolů .....	14
4. Nelineární zobrazení matice hustoty .....	18
5. Závěr .....	28
6. Matematický dodatek: GXOR-zobecněná XOR-brána .....	30
7. Použitá literatura .....	32

# Kapitola č. 1

## Úvod

Teorie kvantové informace (viz [1]) se zabývá možností použití kvantových objektů jako medií pro přenos a práci s informací. Využívá přitom existence tzv. **provázaných stavů** kvantových systémů. Provázanost se rozumí jistý druh korelace, která nemá klasický analog. Takové systémy slouží jako zdroj efektivních řešení mnohých úkolů. V následujícím textu se budu zabývat možností zachování provázanosti systému při přenosu komponent na velké vzdálenosti. Důležitost provázání ukažu na následujícím příkladu.

Nosičem základní logické jednotky bitu (který představuje např. kladnou resp. zápornou odpověď na jistou otázku) je v kvantovém světě **qubit** t.j. dvouhladivá kvantová částice, jejíž stavový Hilbertův prostor je  $\mathcal{H} = \mathbf{C}^2$ .

Předpokládejme nyní situaci, kdy pozorovatel  $A$  by rád poslal vzdálené pozorovatelce  $B$  qubit ozn. 1 ve stavu:

$$|\psi\rangle_1 = a|0\rangle_1 + b|1\rangle_1,$$

$a^2 + b^2 = 1$ ,  $a, b \in [0, 1]$ ,  $\{|0\rangle_1, |1\rangle_1\}$  tvoří ortonormální bázi  $H_1$ .

Klasicky by jistě bylo možné, aby  $A$  sdělil  $B$  hodnoty parametrů  $a, b$  např. prostřednictvím internetu a  $B$  by si částici vyrobila sama. To by ovšem tyto hodnoty  $A$  musel znát. Kvantový teleport takovou znalost po  $A$  nepožaduje.

Za tím účelem nechť  $A$  a  $B$  přísluší qubity 2 resp. 3, jejichž složený systém je ve stavu:

$$|\Psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2 \otimes |1\rangle_3 - |1\rangle_2 \otimes |0\rangle_3).$$

Celkový systém qubitů 1, 2, 3 je:

$$\begin{aligned} |\psi\rangle_1 \otimes |\Psi^-\rangle_{23} &= \frac{1}{\sqrt{2}}(a|0\rangle_1 + b|1\rangle_1) \otimes (|0\rangle_2 \otimes |1\rangle_3 - |1\rangle_2 \otimes |0\rangle_3) = \\ &= |\Phi^+\rangle_{12} \otimes \left(\frac{a}{2}|1\rangle_3 - \frac{b}{2}|0\rangle_3\right) + |\Phi^-\rangle_{12} \otimes \left(\frac{a}{2}|1\rangle_3 + \frac{b}{2}|0\rangle_3\right) + \\ &\quad + |\Psi^-\rangle_{12} \otimes \left(-\frac{a}{2}|0\rangle_3 - \frac{b}{2}|1\rangle_3\right) + |\Psi^+\rangle_{12} \otimes \left(-\frac{a}{2}|0\rangle_3 + \frac{b}{2}|1\rangle_3\right) \end{aligned}$$

kde  $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle)$ ,  $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$ ,  $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$ ,  $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)$  jsou tzv. Bellovské stavy, ortonormální báze  $\mathbf{C}^2 \otimes \mathbf{C}^2$ .

$A$  na 1 a 2 provede nyní náhodé měření tzv. Bellovských stavů a nechť výsledku přiřadí dvoubitovou informaci  $(ij)$ ,  $i, j \in \{0, 1\}$  podle klíče:

$$|\Psi^+\rangle \rightarrow (10)$$

$$|\Psi^-\rangle \rightarrow (01)$$

$$|\Phi^+\rangle \rightarrow (11)$$

$$|\Phi^-\rangle \rightarrow (00)$$

Takovou informaci sdělí  $B$  např. formou e-mailu.  $B$  potom provede na částici 3 jednu z transformací:

$$(10) \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$(01) \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$(11) \rightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$(10) \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

a obdělí částici 3 ve stavu  $|\Psi\rangle$ .

Teleportem k  $B$  byla vytvořena identické kopie částice na jiném místě, aniž by se znal její počáteční stav. Navíc použitím pouze přípustných lokálních transformací a klasického komunikačního kanálu tzv. **LOCC** transformace oběma pozorovateli je teleport nezávislý od vzdálenosti obou pozorovatelů. Tímto postupem však nelze částice klonovat, původní částice se stává součástí provázaného stavu 12. Rychlost teleportu je přitom omezena rychlostí přenosu dvoubitové informace klasickým informačním kanálem, principiálně rychlostí světla. Přenos dvoubitové informace je přitom pro experiment nezbytný. Provede-li  $B$  měření v Bellovské bázi s náhodným výsledkem, přejde částice 3 do stavu:

$$\begin{aligned} & \frac{1}{4}(-a|0\rangle_3 + b|1\rangle_3)(-a^*\langle 0|_3 + b^*\langle 1|_3) + \frac{1}{4}(-a|0\rangle_3 - b|1\rangle_3)(-a^*\langle 0|_3 - b^*\langle 1|_3) + \\ & \frac{1}{4}(-b|0\rangle_3 + a|1\rangle_3)(-b^*\langle 0|_3 + a^*\langle 1|_3) + \frac{1}{4}(b|0\rangle_3 + a|1\rangle_3)(b^*\langle 0|_3 + a^*\langle 1|_3) = \\ & = \frac{1}{2}(\underbrace{(a^2 + b^2)}_{=1}|0\rangle_3\langle 0|_3 + \underbrace{(a^2 + b^2)}_{=1}|1\rangle_3\langle 1|_3). \end{aligned}$$

Polarizace stavu 3 je tak zcela náhodná a neexistuje unitární transformace, kterou by  $B$  získal 3 ve stavu  $|\psi\rangle$ .

Schrňme nyní nutné podmínky pro provedení teleportu. Klíčovým pro kvantový teleport byla existence a měření stavů Bellovské báze. Takové stavy se nazývají maximálně provázané. Druhým důležitým krokem byla možnost jejich sdílení mezi  $A$  a  $B$ . Na začátku musel existovat zdroj takových provázaných stavů ze kterého byly jednotlivé částice k pozorovatelům přeneseny. Přenos částic od zdroje k jednotlivým pozorovatelům však typicky není dokonalý, objeví se jisté „znečištění“ systému. Otázkou je, jak mohou tito pozorovatelé systém „odčistit“ zpět do požadovaného maximálně provázaného stavu. Přitom vzhledem ke vzájemné vzdálenosti mohou provádět jen již zmíněné **LOCC**.

V následujícím textu se zaměřím na zodpovězení této otázky a nastínění řešení problému pro **konečné kvantové systémy** t.j.  $N$ -částicové,  $N < \infty$ ,  $D$ -hladinové,  $D < \infty$ , každá částice tzv. **qudit** se může nacházet v jednom z  $D$  přípustných stavů. Hilbertův stavový prostor takového systému je  $C^D \otimes \dots \otimes C^D$ :  $N$ -krát.

Obecné řešení problému „čistitelnosti“ systému k jistému provázanému stavu má ještě další význam. Klasifikace tříd „čistitelných“ a „nečistitelných“ stavů totiž pomáhá detailněji porozumět provázanosti systému, která není ještě plně prozkoumána.

# Kapitola č. 2

## Provázanost kvantového systému

### 2.1 Definice provázanosti kvantového systému

Podrobný rozbor tématu vychází z textu [2] a [3]. V následujícím textu zavedu základní pojmy, potřebné pro výklad problematiky čistitelnosti systémů.

Nositelům úplné informace o kvantovém systému je jeho matice hustoty  $\rho$  t.j. pozitivní operátor s jednotkovou stopou, viz [14] resp. [1], který působí na Hilbertově stavovém prostoru systému  $H$ . Pozitivita operátoru  $\rho$  ozn.  $\rho \geq 0$  znamená, že operátor je Hermitovský a všechna jeho vlastní čísla jsou nezáporná, viz [14].

**Definice provázanosti** (viz [3]): Mějme konečný  $N$ -částicový,  $D$ -hladinový kvantový systém, tak jak byl definován v první kapitole. Systém nazvu **provázaný**, pokud jeho matici hustoty  $\rho$  nelze zapsat v plně separabilním tvaru t.j. nelze ji zapsat ve tvaru:

$$\rho = \sum_a p(a) \rho_a^{(1)} \otimes \cdots \otimes \rho_a^{(N)}$$

kde  $\rho_a^{(i)}$ ,  $i \in N$  jsou matice hustoty na příslušném  $D$ -dimenzionálním Hilbertově prostoru  $C^D$   $i$ -té částice, a  $p(a)$  je pravděpodobnostní rozdělení možných stavů složeného systému.

Tato formulace dobře odráží přirozený požadavek zmíněný v úvodu. Částice provázaných systémů (na rozdíl od separabilních) jsou jistým způsobem korelované.

Otázkou je, jak takto definovanou provázanost systému kvantifikovat, jak definovat míru provázanosti ve smyslu dodatku A.3 z [14].

Teorie míry provázanosti systémů obecných kvantových systémů vychází ze dvou pojetí: operacionalisticko-abstraktního a finitně-asymptotického viz [3].

**Operacionalistický přístup** měří velikost provázanosti systému pomocí pravděpodobnosti úspěšného provedení procesů, které provázanost systému požadují (např. kvantový teleport či husté kódování).

**Abstraktní přístup** vychází z faktu, že funkce charakterizující míru provázanosti systému musí splňovat některé přirozené požadavky:

1. Provázanost dvou systémů nemůže vzrůst bez kvantové interakce mezi systémy (ať přímé či nepřímé).
2. V modelovém příkladu prostorově oddělených komponent provázaného systému použití pouze klasické komunikace mezi pozorovateli A, B nemůže vést ke zvýšení provázanosti systému.

Na základě těchto tvrzení lze odvodit základní postulát teorie provázanosti:

Provázanost systému je monotonní funkce při použití pouze lokálních transformací na jednotlivých komponentách a klasického komunikačního kanálu tzv. **LOCC transformace**.

V modelovém příkladu odpovídají situaci, kdy pozorovatel A připraví jistou lokální transformaci na sobě příslušné částici systému. Výsledek svého měření sdělí klasickým informačním kanálem pozorovateli B, který na základě takové znalosti provede jistou lokální transformaci na „své“ částici.

Míry provázanosti jsou zde odvozeny ze vzdálenosti daného stavu od množiny nečistitelných stavů.

**Finitní přístup** se zabývá provázaností jediného systému složeného z konečného počtu částic. **Asymptotický přístup** zkoumá provázanost posloupnosti takových systémů resp. kvantového zdroje. Tento režim se také nazývá termodynamikou provázanosti.

Podrobný rozbor měř provázanosti systému lze najít v [2], zde se touto problematikou nebudu dále zabývat, neboť pro vícekomponentové systémy není ani dostatečně prozkoumána. V této souvislosti jenom poznamenám, že jak Bellovské stavy (viz Mat. dodatek) tak čisté symetrické a antisymetrické stavy představují provázané stavy vzhledem k jisté míře provázání. Definuji důležitý pojem. **Projekcí stavu** určeného maticí hustoty  $\sigma$  vůči čistému stavu s maticí hustoty  $\rho$  rozumím funkci  $F : \sigma \rightarrow [0, 1]$ ,  $F(\sigma, \rho) = \text{Tr}(\rho\sigma)$ , kde hodnota 1 odpovídá případu  $\sigma = \rho$ .

## 2.2 Klasifikace stavů kvantových systémů, nutné podmínky separability

Kromě provázaných (entangled) resp. plně separabilních (separable) stavů lze stavy rozdělit na **čistitelné** (distillable) a **nečistitelné** (non-distillable). Důležité je zda k danému stavu systému existuje posloupnost fyzikálně přípustných LOCC operací, které jej převedou na provázaný stav. Zřejmě žádný plně separabilní stav systému nelze pomocí LOCC převést na provázaný. Na druhé straně bylo dokázáno [4], že ne všechny provázané stavy jsou čistitelné. Takové stavy se nazývají omezeně provázané (bound entangled).

Pro zařazení stavu systému mezi provázané slouží především nutné podmínky separability. **Peresovo kritérium**, které bylo původně odvozeno pro dvoučásticové kvantové systémy se stavovými prostory  $\mathcal{H}_1, \mathcal{H}_2$ , říká že nutnou podmínkou separability dvoučásticového stavu s maticí hustoty  $\rho$  je pozitivita její částečné transpozice vzhledem k oběma komponentám t.j.  $\rho^{T_1} \geq 0 \wedge \rho^{T_2} \geq 0$  kde částečné transpozice  $\rho^{T_1, T_2}$  matice  $\rho$  jsou v libovolné ortonormální bázi  $|ab\rangle$  prostoru  $\mathcal{H}_1 \otimes \mathcal{H}_2$  vyjádřeny maticovými elementy  $\langle ab|\rho^{T_1}|a'b'\rangle = \langle a'b|\rho|ab'\rangle$  resp.  $\langle ab|\rho^{T_2}|a'b'\rangle = \langle ab'|\rho|a'b\rangle$ . Kritérium lze rozšířit i na obecné systémy, tak že je požadována pozitivita částečných transpozic vzhledem k libovolné komponentě.

Pro praktické počítání je ovšem použitelná i slabší podmínka, která využívá Schwarzovy nerovnosti (viz [14]). Nutnou podmínkou separability stavu obecného  $N$ -kom-

ponentového systému reprezentovaného maticí hustoty  $\rho$  je platnost následujících nerovností:

$$\sqrt{\langle j_1, \dots, j_N | \rho | j_1, \dots, j_N \rangle} \sqrt{\langle k_1, \dots, k_N | \rho | k_1, \dots, k_N \rangle} \geq \sqrt{\langle \pi_1^1, \dots, \pi_1^N | \rho | \pi_2^1, \dots, \pi_2^N \rangle}$$

kde  $|j_1, \dots, j_N\rangle$  představuje ortonormální bázi stavového prostoru systému a  $\pi^i$  označují permutace dvouprvkových množin  $j_i, k_i$  pro všechna  $i \in \{1, \dots, N\}$ . Toto tvrzení nazvu jako **druhou podmínkou separability**.

Důkazy obou podmínek lze pro dvoukomponentové systémy najít v [5], [6]. Jejich rozšíření na vícekomponentové systémy plyne přímou aplikací užitých postupů.

### 2.3 Třídy přípustných operací na kvantovém systému, speciální třídy stavů systémů

Klasifikace fyzikálně realizovatelných zobrazení na kvantovém systému je podrobně rozebrána v článku [2]. Pro záměr této práce však v následujícím textu provedu shrnutí informací z článku [7].

Položme si nyní otázku, jaké podmínky musí splňovat zobrazení  $\Lambda : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$ , kde  $\mathcal{B}(\mathcal{H})$  značí množinu všech omezených lineárních operátorů na  $\mathcal{H}$  (viz [14]), aby reprezentovalo jistou fyzikálně přípustnou operaci na kvantovém systému. Jistě musí převádět matici hustoty systému  $\rho$  opět na matici hustoty  $\tilde{\rho}$  t.j. nutně zachovájí pozitivitu:  $\rho \geq 0 \Rightarrow \Lambda(\rho)$ . Taková zobrazení se nazývají **pozitivní**. O zobrazeních, pro která platí  $\text{Tr}(\rho) = 1 \Rightarrow \text{Tr}\Lambda(\rho) = 1$ , říkáme že **zachovávají jednotkovou stopu**.

Uvedené podmínky ovšem nemusí být postačující pro fyzikální realizaci zobrazení. Uvažujme systémy  $A, B$  jejichž spojením vznikne systém ve stavu  $\rho_{AB}$ . Pokud byly systémy prostorově odděleny, operaci provedenou na složeném systému lze reprezentovat zobrazením  $\Lambda = \Lambda_A \otimes \Lambda_B$ , kde  $\Lambda_{A,B}$  jsou zobrazení, která reprezentují procesy na jednotlivých systémech  $A, B$ . Odtud plyne další nutná podmínka fyzikálně realizovatelných zobrazení. Jejich tenzorový součin musí být opět pozitivní zobrazení. Pozitivní zobrazení, která splňují tuto podmínku se nazývají **úplně pozitivní**. Z těchto úvah plyne nutná podmínka úplné positivity zobrazení  $\Lambda$ : pro každé přirozené  $N$  je  $\Lambda \otimes I_N$  pozitivní, kde  $I_N$  je operátorem identity na  $N \times N$  maticích. Pro konečné systémy lze podmínku ještě zeslabit, jak bylo ukázáno v dodatku [7].

Uvažujme nyní tři typy zobrazení:

(i)  $\rho \rightarrow \rho \otimes \rho'$  t.j. proces přidání systému  $\rho'$ ,

(ii)  $\rho \rightarrow U\rho U^\dagger$ , kde  $U$  je unitární operátor na  $H$  t.j. unitární transformace na stavovém prostoru,



(iii)  $\rho_{AB} \rightarrow \text{Tr}_B \rho_{AB}$  t.j. rozklad systému definované pomocí elementů v maticovém vyjádření:

$$(\text{Tr}_B \rho_{AB})_{ab} = \sum_{\mu} \langle a\mu | \rho_{AB} | b\mu \rangle.$$

Snadno lze nahlédnout, že všechna tato zobrazení jsou úplně pozitivní a zachovávají stopu. Zobrazení (i), (iii) představují přechod k „více resp. méně“ rozměrným systémům. Proces unitárního zobrazení, reprezentuje realizovatelné procesy, které zachovávají rozměr systému. Přitom v [8] bylo ukázáno, že libovolné fyzikálně realizovatelné zobrazení, lze zapsat ve tvaru těchto tří zobrazení. Každé úplně pozitivní zobrazení, které zachovává stopu lze zkonstruovat právě pomocí těchto tří zobrazení. Pokud k těmto třem typům zobrazení přidáme ještě operaci výběru vhodného systému po měření, obdržíme celou třídu úplně pozitivních zobrazení. V [7] bylo ukázáno, že ne všechna pozitivní zobrazení jsou úplně pozitivní. Rozdíl mezi nimi se projeví v působení na provázaných stavech systému, což nyní ukážu pro dvoukomponentové systémy.

Nechť  $\Lambda$  je pozitivní zobrazení. Mějme dvoukomponentový separabilní stav systému tvaru  $\sum_i p_i \rho_A^i \otimes \rho_B^i$ , kde  $\rho_{A,B}^i$  jsou matice hustot systémů  $A, B$ . Nechť zobrazení  $\Lambda$  působí na matice o rozměrech  $\rho_B^i$ , potom:  $(I \otimes \Lambda)(\sum_i p_i \rho_A^i \otimes \rho_B^i) = \sum_i p_i \rho_A^i \otimes \Lambda(\rho_B^i) \geq 0$ , neboť  $\Lambda(\rho_B^i) \geq 0$  vzhledem k pozitivitě  $\Lambda$ ,  $p_i \geq 0$  vyjadřuje pravděpodobnost výskytu systému ve stavu  $\rho_A^i \otimes \rho_B^i$ .

Rozdíl mezi pozitivitou a úplnou pozitivitou  $\Lambda$  se tedy projeví až u provázaných stavů a pozitivní zobrazení jsou tak výhodná pro studium separability stavů.

V [9] byl proveden důkaz tvrzení: dvoukomponentový stav  $\rho$  je provázaný, právě tehdy když existuje pozitivní zobrazení  $\Lambda$ , pro nějž  $(I \otimes \Lambda)(\rho)$  není pozitivní, kde  $I$  značí operátor identity. Nutnou podmínkou separability takového stavu  $\rho$  je pozitivita zobrazení  $(I \otimes \Lambda)(\rho) \geq 0$  pro každé pozitivní zobrazení  $\Lambda$  tzv. **redukční kritérium**.

V [9] bylo ukázáno, že Peresova podmínka je silnější než redukční kritérium.

Zabývejme se nyní speciálními třídami jednoparametrických stavů dvoukomponentových kvantových systémů.

### Izotropické stavy

Jedná se o dvouquditové kvantové systémy, jejichž stavovým prostorem je  $\mathcal{H} = C^D \otimes C^D$ . Přísluší jim matice hustoty ve tvaru:

$$\rho_{\alpha} = (1 - \alpha) \frac{I}{D^2} + \alpha P$$

kde  $P = |\Psi_+\rangle\langle\Psi_+|$ ,  $|\Psi_+\rangle = \frac{1}{\sqrt{D}} \sum_i |i\rangle \otimes |i\rangle$ .

Stavy jsou  $U \otimes U^*$  invariantní pro  $U$  unitární:

$$\begin{aligned} U \otimes U^* |\Psi^+\rangle &= \frac{1}{\sqrt{D}} \sum_{ijk} u_{ji} u_{ki}^* |j\rangle \otimes |k\rangle = \\ &= \frac{1}{\sqrt{D}} \sum_{ijk} u_{ji} u_{ik}^{-1} |j\rangle \otimes |k\rangle = \frac{1}{\sqrt{D}} \sum_{jk} \delta_{jk} |j\rangle \otimes |k\rangle = \frac{1}{\sqrt{D}} \sum_k |k\rangle \otimes |k\rangle = |\Psi^+\rangle. \end{aligned}$$

Podmínka positivity je splněna pro:  $\frac{-1}{D^2-1} \leq \alpha \leq 1$ .

Pomocí projekce  $F = \text{Tr}(\rho_\alpha P) = D\alpha - 2\alpha + 1$  lze tyto stavy převést na tvar

$$\rho_{\alpha(F)} = \frac{D^2}{D^2 - 1} \left[ (1 - F) \frac{I}{D^2} + \left( F - \frac{1}{D^2} \right) P \right]$$

s podmínkou positivity  $0 \leq F \leq 1$ .

Podmínkou separability i Peresovy nutné podmínky separability je  $F \leq \frac{1}{D}$ .

Tyto stavy jsou jediné  $U \otimes U^*$  invariantní, kde  $U$  je libovolné unitární zobrazení na prostoru  $C^D$ , jak bylo ukázáno v [7].

### Wernerovské stavy

Stavový prostor je opět stejný jako pro izotropické stavy. Stavy jsou charakterizovány maticí hustoty ve tvaru:

$$\rho_p = p \frac{P_-}{N_-} + (1 - p) \frac{P_+}{N_+},$$

$0 \leq p \leq 1$ , kde  $P_\pm$  jsou projektory na symetrický resp. antisymetrický podprostor  $H$ ,  $N_\pm = \frac{D^2 \pm D}{2}$  jsou dimenze těchto podprostorů.

Podmínka positivity je zřejmá:  $0 \leq p \leq 1$ .

Pro projektory  $P_\pm$ :

$$P_+(|ij\rangle \pm |ji\rangle) = \begin{cases} (|ij\rangle + |ji\rangle) \\ 0 \end{cases}$$

$$P_- (|ij\rangle \pm |ji\rangle) = \begin{cases} (|ij\rangle - |ji\rangle) \\ 0 \end{cases}$$

odkud je vidět, že  $P_\pm = \frac{1}{2} \sum_{ij} (|ij\rangle \pm |ji\rangle) \langle ij| = \frac{1}{2} (1 \pm \sum_{ij} |ij\rangle \langle ji|)$

Tyto stavy jsou  $U \otimes U$  invariantní:

$$U \otimes U \rho_p U^\dagger \otimes U^\dagger = U \otimes U \left( \frac{p}{N_-} (1 - |ji\rangle \langle ij|) + \frac{1-p}{N_+} (1 + |ji\rangle \langle ij|) \right) U^\dagger \otimes U^\dagger = \rho_p.$$

Jestliže  $(U)_{ij} = u_{ij}$ , potom totiž:

$$U \otimes U \sum_{ij} |ij\rangle \langle ji| \delta_{kn} U^\dagger \otimes U^\dagger = \sum_{klmnij} u_{ki} u_{lj} u_{ni}^* u_{mj}^* |kl\rangle \langle nm| = \delta_{kn} \delta_{lm},$$

unitarita  $U$  zaručuje  $U^\dagger = U^{-1}$ .

Snadno se též ověří, že pro  $p \leq 1/2$  Wernerovské stavy splňují Peresovo kritérium, za stejné podmínky splňují též nutnou a postačující podmínku separability.

Stejným postupem jako pro izotropické stavy nyní ověřím, že tyto stavy jsou jediné  $U \otimes U$  invariantní kde  $U$  je libovolné unitární zobrazení na prostoru  $C^D$ . Nechť  $\rho$  nyní představuje matici hustoty takového invariantního stavu. Volbou  $U$ , které násobí libovolný, ale pevný vektor  $|m_0\rangle$  ortonormální báze prostoru  $C^D$  číslem  $-1$  a přitom ostatní bazické vektory nemění zjistíme, že nenulové mohou být pouze koeficienty  $\langle ii|\rho|ii\rangle$ , pro  $i \neq j$  potom  $\langle ij|\rho|ij\rangle$ ,  $\langle ij|\rho|ji\rangle$ ,  $\langle ii|\rho|jj\rangle$ . Volbou  $U$ , které vynásobí libovolný, ale pevný vektor  $|n_0\rangle$  číslem  $i$ , zjistíme, že mezi přípustné nenulové koeficienty mohou patřit pouze  $\langle ii|\rho|ii\rangle$ , pro  $i \neq j$  potom  $\langle ij|\rho|ij\rangle$ ,  $\langle ij|\rho|ji\rangle$ . Pokud  $U = \widetilde{U}_2 \oplus I_{D-2}$

kde  $U_2 = \begin{pmatrix} \cos \phi & \sin \phi \\ -\sin \phi & \cos \phi \end{pmatrix}$  působí na  $\mathcal{H}_1$  nějakém dvoudimenzionálním podprostoru  $C^D$  a  $I_{D-2}$  je projektor na ortogonální doplněk  $\mathcal{H}_1$  v  $C^D$ , potom koeficienty z dané „třídy“ nutně nabývají stejných hodnot pro všechna  $i, j \in D$  (stačí totiž  $\phi = \pi/2$ ). Potom  $\rho = aA + bB + cC$  kde  $A = \sum_i |ii\rangle\langle ii|$ ,  $B = \sum_{i \neq j} |ij\rangle\langle ij|$ ,  $C = \sum_{i \neq j} |ij\rangle\langle ji|$ . Přitom taková volba  $U$  nezachovává  $A$ , tedy parametr  $a$  je lineárně závislý na  $b$  a  $c$ . Protože  $\text{Tr}(\rho) = 1$  sníží se počet volných parametrů na jeden. Jedině Wernerovské stavy splňují takovou podmínku.

Nyní se zabýváme speciálními třídami jednoparametrických stavů vícekomponentových kvantových systémů.

## 2.5 Zobecněné symetrické a antisymetrické stavy

Definujeme:

$$\rho = (1 - \alpha) \frac{1}{D^N} I + \alpha |\Psi\rangle\langle\Psi|,$$

kde  $I$  je operátor identity na  $\mathcal{H} = \underbrace{C^D \otimes \dots \otimes C^D}_{N \times}$ ,  $0 \leq \alpha \leq 1$  a

$$|\Psi\rangle = |S\rangle = \frac{1}{\sqrt{D}} \sum_j |j\rangle \otimes \dots \otimes |j\rangle, \quad \underbrace{\hspace{10em}}_{N \times}$$

$N, D$  jsou obecně nezávislá resp.

$$|\Psi\rangle = |A\rangle = \frac{1}{\sqrt{D!}} \sum_{\pi} \text{sgn}(\pi) \underbrace{|\pi_1\rangle \otimes \dots \otimes |\pi_N\rangle}_{N \times},$$

kde  $\pi$  jsou permutace množiny  $D$  t.j. v tomto případě  $N = D$ .

Stavy popsané takovými maticemi hustoty nazýváme po řadě zobecněné znečištěné symetrické resp. antisymetrické stavy. Bellovské stavy jsou jejich speciálním případem. Položme si otázku, kdy jsou tyto stavy úplně separabilní.

V [3] bylo ukázáno, že nutnou a postačující podmínkou separability symetrických stavů je:

$$\alpha \leq (1 + D^{N-1})^{-1}.$$

Pro antisymetrické stavy podle druhé podmínky separability je nutnou podmínkou:

$$\alpha \leq (1 + \frac{(D-1)!}{D^{D-1}})^{-1}.$$

Při důkazu jsem vyšel z podobné úvahy jako ve [3]. Separabilitu stačí ověřit pro  $\alpha = (1 + \frac{(D-1)!}{D^{D-1}})$ , neboť s klesajícím  $\alpha$  klesá i provázanost stavu vzhledem k maximálně provázanému  $|\Psi\rangle\langle\Psi|$  viz [10]. Dosazením za takové  $\alpha$  do definiční matice hustoty zjistíme, že stačí ukázat separabilitu stavu

$$\tilde{\rho}_D = \frac{1}{D^D} (I + \sum_{\pi \neq \sigma} |\pi\rangle\langle\sigma|)$$

kde  $|\pi\rangle = |\pi_1, \dots, \pi_D\rangle$ ,  $\pi_i \in \widehat{D}$ . Zkonstruoval jsem rozklady:

Pro  $D = 1$  má  $H$  jediný bazický vektor  $|0\rangle$  a  $\tilde{\rho}_0 = |0\rangle\langle 0|$  separabilní.

Pro  $D = 2$  označím prvky ortonormální báze  $\mathcal{H}$  jako  $\{|ij\rangle\}$ ,  $\{i, j\} \in \{0, 1\}$ , potom  $\tilde{\rho}_{01} = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| - |01\rangle\langle 10| - |10\rangle\langle 01| = \frac{1}{4}((|0\rangle + |1\rangle)(\langle 0| + \langle 1|) \otimes (|0\rangle - |1\rangle)(\langle 0| - \langle 1|) + (|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \otimes (|0\rangle + |1\rangle)(\langle 0| + \langle 1|))$  je separabilní.

Pro  $D = 3$  lze ve smyslu předchozího značení psát  $\tilde{\rho}_{012} = \rho_{01} \otimes \rho_2 + \rho_2 \otimes \rho_{01} + \rho_{20} \otimes \rho_1 + \rho_1 \otimes \rho_{20} + \rho_{21} \otimes \rho_0 + \rho_0 \otimes \rho_{21} + \sum_{ij} (|ij\rangle\langle ij| + |iji\rangle\langle iji| + |jii\rangle\langle jii|) + \sum_{i \neq j \neq k} (|ijk\rangle + |jki\rangle)\langle kij|$ . Tímto způsobem se mi nepodařilo obecně separabilitu dokázat. Konstrukcí purifikačního protokolu pro některé takové antisymetrické stavy však ukážu, že se o obecně separabilní stavy nejedná a podmínka tedy není obecně postačující.

Hledání obecné třídy zobrazení tvaru  $U_1 \otimes \dots \otimes U_D$ , kde  $U_i$  je unitární pro každé  $i \in D$ ,  $D \geq 3$  pro která by symetrické či antisymetrické stavy byly jediné invariantní se mi taktéž nepodařilo nalézt. Uvažujme nyní systémy pro  $N = 3$ ,  $D = 3$ . V obou případech jde o určení obecně 27 koeficientů  $u_{ij}^k$ , které tvoří maticové elementy jednotlivých zobrazení.

Pro symetrické stavy je určují rovnice

$$\sum_{ij} u_{ik}^1 u_{il}^2 u_{im}^3 u_{jn}^{1*} u_{jo}^{2*} u_{jp}^{3*} = \delta_{klm} \delta_{nop}$$

kde  $i, j, k, l, m, n, o, p \in \{1, 2, 3\}$ ,  $\delta_{klm}$  nabývá 1 pro případ  $k = l = m$  a 0 jinak. Řešení těchto rovnic se mi nepodařilo. Zeslabením podmínky na zachování stavu  $|S\rangle$  získám rovnice

$$\sum_i u_{ij}^1 u_{ik}^2 u_{il}^3 = \delta_{jkl}.$$

Podmínky unitarity říkají  $\sum_k u_{ik}^l u_{kj}^{l*} = \delta_{ij}$  pro všechna  $i, j, k, l \in 1, 2, 3$ . To je celkem  $27 + 3 \cdot 6 = 45$  nelineárních rovnic pro 27 neznámých. Rovnice odráží přirozené symetrie stavu  $|S\rangle$ , který je symetrický vůči záměně každých dvou indexů  $i, j, k \in \{1, 2, 3\}$ . Stav systému je dále invariantní vůči záměně libovolných dvou částic. Pokud tyto podmínky vztáhnou i na zobrazení  $U_1 \otimes U_2 \otimes U_3$ , počet podmínek nezávislých rovnic se redukuje na nejvýše  $1 + 1 + 1 + 3 \cdot 6 = 21$ , sčítá se přes skupiny obsahující tři, dva nebo žádný stejný index a podmínky unitarity. V případě  $U_1 = U_2 = U_3 = U$ ,  $U_{ij} = U_{ji}$  (pro nejmenší počet volných parametrů  $3 + (9 - 3)/2 = 6$ ) se redukuje na nejvýše 9 nezávislých rovnic. Řešení, která jsem odhadl na základě symetrií stavu jsou:

$U|m_0\rangle = z_0|m_0\rangle$ ,  $z_0 \in \mathbf{C}$ ,  $|z_0| = 1$  a ostatní vektory ortonormální báze  $C^3$  ponechá beze změny.

$U|m_0\rangle = |n_0\rangle$ ,  $U|n_0\rangle = |m_0\rangle$  a ostatní vektory ortonormální báze  $C^3$  ponechá beze změny.

Tyto podmínky však jednoparametický invariantní systém neurčují jednoznačně. Pro antisymetrické stavy jsou koeficienty určeny podmínkami

$$\sum_{\pi\sigma} \text{sgn}(\pi) \text{sgn}(\sigma) u_{\pi_1 i}^1 u_{\pi_2 j}^2 u_{\pi_3 k}^3 u_{\sigma_1 l}^{1*} u_{\sigma_2 m}^{2*} u_{\sigma_3 n}^{3*} = \text{sgn}(ijk) \text{sgn}(klm).$$

Ani zde se mi nepodřilo problém obecně vyřešit. Přejdem ke slabší podmínce zachování  $|A\rangle$  vznikly rovnice

$$\sum_{\pi} \text{sgn}(\pi) u_{\pi_1 i}^1 u_{\pi_2 j}^2 u_{\pi_3 k}^3 = \text{sgn}(ijk).$$

Opět spolu s podmínkami unitarity obdržím celkem 30 nelineárních rovnic pro 27 neznámých. Stav je symetrický vůči záměně všech tří indexů a částic. Tím se počet rovnic opět sníží na  $2 + 1 + 1 + 3.6 = 22$ . V případě  $U_1 = U_2 = U_3 = U$  (pro nejmenší počet volných parametrů 6) se redukuje nejvýše na 10. Řešení, která jsem odhadl na základě symetrií stavu jsou:

$U$  je operátor rotace o úhel  $\phi$  kolem libovolné osy v  $R^3$  určené jednotkovým směrovým vektorem  $\mathbf{n} = (\mathbf{n}_1, \mathbf{n}_2, \mathbf{n}_3)$  viz P1, takové  $U$  lze reprezentovat maticí

$$U = \begin{pmatrix} q_0^2 + q_1^2 - q_2^2 - q_3^2 & 2(q_1 q_2 - q_0 q_3) & 2(q_1 q_3 + q_0 q_2) \\ 2(q_1 q_2 + q_0 q_3) & q_0^2 - q_1^2 + q_2^2 - q_3^2 & 2(q_2 q_3 + q_0 q_1) \\ 2(q_1 q_3 - q_0 q_2) & 2(q_2 q_3 + q_0 q_1) & q_0^2 - q_1^2 - q_2^2 + q_3^2 \end{pmatrix}$$

kde  $q_0 = \cos(\frac{\phi}{2})$ ,  $\mathbf{q} = (\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3) = \mathbf{n} \sin(\frac{\phi}{2})$ . Dále jsou tyto stavy invariantní pro  $U$ , která byla zmíněna pro symetrické stavy.

# Kapitola č. 3

## Konstrukce purifikačních protokolů

**Purifikačním protokolem** rozumím posloupnost *LOCC* procesů realizovaných úplně pozitivními zobrazeními doplněné měřením pozorovatelných systému viz [1], které v konečném počtu převedou vstupní stav systému na výstupní s vyšší čistotou vzhledem k jistému provázanému stavu, ke kterému chceme čistit. V následujícím textu obrátím pozornost ke konstrukcím purifikačních protokolů.

### Bennett-Brassard

Tento protokol se vztahuje na modelově nejjednodušší provázané systémy: dvoučásticové  $N = 2$ , dvouhladinové  $D = 2$ . Reprezentační prostor je  $\mathcal{H} = C^2 \otimes C^2$ . Podrobný rozbor viz [10].

Prvky Bellovské báze (viz def. 1. kap.) vykazují zajímavé chování. V [1] bylo ukááno, že vektory  $|x\rangle \in C^2$  lze v maticové reprezentaci charakterizovat pomocí polarizačního vektoru  $\mathbf{P} = (P_x, P_y, P_z)$  jako  $|x\rangle\langle x| = \frac{1}{2}(1 + \mathbf{P} \cdot \boldsymbol{\sigma})$  kde  $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ :

$$\sigma_{x,y,z} = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Operace „.” značí standartní skalární součin. V tomto smyslu můžeme uvažovat o reprezentaci  $C^2$  pomocí třídimenzionálního kartézského souřadného systému nad tělesem  $C$  a zavést standartní  $SU(2)$  rotace.

Ověřím následující vlastnosti:

1. Uvažujme operace rotace o úhel  $\pi$  jedné z částic kolem osy  $x$  resp.  $y$  resp.  $z$  ozn.  $\sigma_x, \sigma_y, \sigma_z$  (tzv. unilaterální Pauliho rotace). Tyto transformace jednoznačně zobrazují prvky Bellovské báze na sebe  $\sigma_x : \Psi^\pm \leftrightarrow \Phi^\pm, \sigma_y : \Psi^\pm \leftrightarrow \Phi^\mp, \sigma_z : \Psi^\pm \leftrightarrow \Psi^\mp$  a  $\Phi^\pm \leftrightarrow \Phi^\mp$ .

Ukážu to např. pro  $\sigma_x : P_x \rightarrow P_x, P_y \rightarrow -P_y, P_z \rightarrow -P_z$ , potom:

$|0\rangle\langle 0| \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}(1 + \sigma_z) \rightarrow \frac{1}{2}(1 - \sigma_z) = |1\rangle\langle 1|$ , t.j.  $|0\rangle \leftrightarrow |1\rangle$ . Aplikací  $\sigma_x$  na jednu libovolnou, ale pevně zvolenou částici získáme potom výsledek.

2. Operace rotace o  $\pi/2$  kolem osy  $x, y, z$  každé z částic ozn.  $B_x, B_y, B_z$  (tzv. bilaterální  $\pi/2$  rotace). Tyto transformace zachovávají vždy stav  $|\Psi^-\rangle$  nezměněný a též vždy ještě jeden další, po řadě  $\Phi^-, \Phi^+, \Psi^+$  nezměněný. Pro zbylé dva vždy každá z operací provede vzájemnou záměnu. To vše platí až na fázi.

Ukážu to např. pro  $B_x = R_x(\pi/2) \otimes R_x(\pi/2)$ . Akce  $R_x(\pi/2) : P_x \rightarrow P_x, P_y \rightarrow -P_y, P_z \rightarrow -P_z$ , to znamená

$$|0\rangle\langle 0| \equiv \frac{1}{2}(1 + \sigma_z) \rightarrow \frac{1}{2}(1 - \sigma_y) = \frac{1}{2} \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix} = \frac{1}{2}(|0\rangle - i|1\rangle)(\langle 0| + i\langle 1|) \text{ t.j.:}$$

$$|0\rangle \rightarrow \frac{1}{2}(|0\rangle - i|1\rangle)$$

$$|1\rangle \rightarrow \frac{1}{2}(|0\rangle + i|1\rangle)$$

potom  $B_x|\Psi^\pm\rangle = \frac{1}{4}(|0\rangle - i|1\rangle) \otimes (|0\rangle + i|1\rangle) \pm (|0\rangle + i|1\rangle) \otimes (|0\rangle - i|1\rangle) = \{\Phi_{i\Psi^\pm}^\pm$   
a  $B_x|\Phi^\pm\rangle = \{\Phi_{-i\Psi^\pm}^\pm$ .

3. Nyní definujme operaci  $BXOR$  tzv. bilaterální  $XOR$ .  $BXOR$  působí na dvou párech qubitů. Jeden pár označíme terčový a druhý zdrojový, přitom jeden qubit z každého páru přísluší pozorovateli  $A$ , druhý pozorovateli  $B$ . Akce  $BXOR$  pak spočívá v akci  $XOR$  provedené každým z pozorovatelů na své dvojici t.j. terčový qubit změní svoji hodnotu, vždy když zdrojový nabyl hodnoty 1. Pokud pro dvojici složíme zdrojový a terčový do jednoho systému, jeho stav vyjádříme na reprezentacním prostoru  $C^2 \otimes C^2 \otimes C^2 \otimes C^2$  a provedeme operaci  $BXOR$  zjistíme, že zachovává dvojici  $|\Phi^+\rangle \otimes |\Phi^+\rangle$ .

4. Kromě předchozích tří unitárních operátorů definuji ještě další pomocné zobrazení, které měří spiny obou částic kolem osy  $z$ . Z polarizačního tvaru  $|0\rangle\langle 0|$ ,  $|1\rangle\langle 1|$  je vidět, že tímto měřením se rozliší stavy  $\Psi$  od stavů  $\Phi$ , pro první z částic obdržíme hodnoty různých znamení, pro druhé stejná.

Následující purifikační protokol má za úkol vstupní smíšený stav převést na stav s vyšší hodnotou projekci na  $|\Psi^-\rangle$ , přitom předpokládáme, že máme k dispozici rezervuár znečištěných stavů s pevnou vstupní projekcí systému ve stavu  $|\Psi^-\rangle$ .

K1: Na dvojici vstupních smíšených stavů necháme zapůsobit náhodně zvoleným operátorem z množiny  $\{B_x, B_y, B_z\}$ . S pravděpodobností  $F$  obdržíme ze směsi stav  $|\Psi^-\rangle$ . Ostatní stavy z Bellovské báze se ve směsi objeví s pravděpodobností  $(1 - F)/3$ , neboť pravděpodobnost naměření jiného stavu než  $|\Psi^-\rangle$  u vstupního stavu je  $1 - F$  a pravděpodobnost zachování každého takového stavu po provedení náhodné rotace je  $1/3$ . Stav každého systému lze po provedení této operace charakterizovat maticí hustoty:

$$\rho = F|\Psi^-\rangle\langle\Psi^-| + \frac{1-F}{3}|\Psi^+\rangle\langle\Psi^+| + \frac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \frac{1-F}{3}|\Phi^+\rangle\langle\Phi^+|$$

Což je Wernerovský stav s parametrem  $p = F$ .

K2: Aplikace  $\sigma_y$  převede každý ze systémů do stavu

$$\rho = F|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}|\Psi^+\rangle\langle\Psi^+| + \frac{1-F}{3}|\Phi^-\rangle\langle\Phi^-| + \frac{1-F}{3}|\Psi^-\rangle\langle\Psi^-|.$$

K3: Pokud se oba systémy nacházely ve stavu  $\Phi^+$ , zůstanou po akci  $BXOR$  nezměněny. Na terčovém systému se následně provede měření spinu ve směru osy  $z$  a zdrojový systém se ponechá, pokud byly naměřené spiny stejně orientované. Stav zdrojového systému je potom:

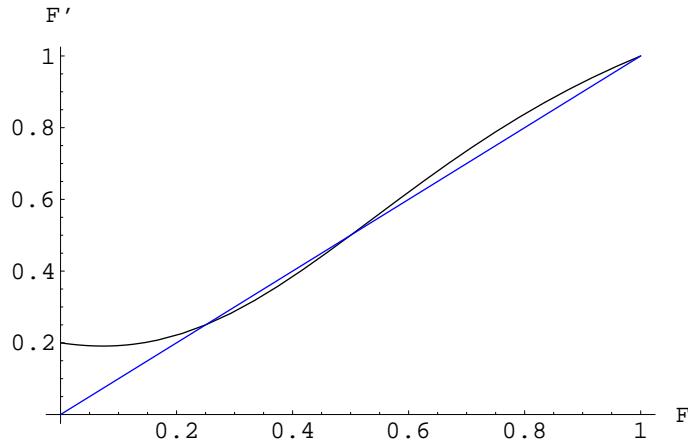
$$\frac{1}{F^2 + \frac{2F(1-F)}{3} + 5\frac{(1-F)^2}{9}} \left( (F^2 + \frac{1-F^2}{9}) |\Phi^+\rangle\langle\Phi^+| + \frac{2F(1-F)}{3} |\Phi^-\rangle\langle\Phi^-| + 3\frac{1-F^2}{9} |\Psi^-\rangle\langle\Psi^-| + \frac{1-F^2}{9} |\Psi^+\rangle\langle\Psi^+| \right).$$

Čistota systému je:  $F' = \frac{F^2 + \frac{1-F^2}{9}}{F^2 + \frac{2F(1-F)}{3} + 5\frac{1-F^2}{9}}$ . Tato funkce je spojitá na celém  $F \in (0; 1]$ . Graf průběhu znázorňuje obr. 1. Průsečíky grafů funkcí  $F'(F)$  a  $F' = F$  jsou body 0.25 a 0.5. Pro  $F \in (1/2; 1]$  je  $F'(F) > F$ , což přesně odpovídá narušení Peresovy podmínky separability pro Wernerovské stavy.

K4: Na terčový systém použijeme operaci  $\sigma_y$ . Tím přejdeme k „čistějšímu“  $|\Psi^-\rangle$  stavu.

Opakováním těchto kroků nakonec dospějeme k požadované čistotě.

obr. 1:



## Horodecki

Následující protokol je jistým způsobem rozšířením předchozího protokolu. Předpokládejme, že máme vyčistit dvoukomponentové  $D$ -hladinové systémy ve stavu reprezentovaném maticí hustoty  $\rho$ , jejich stavový prostor je  $\mathcal{H} = C^D \otimes C^D$ , k provázanému stavu  $|\psi\rangle = \sum_{mn} a_{mn} |m\rangle \otimes |n\rangle$ . K takovému čistému stavu jistě existuje zobrazení  $A$ , které jej ze stavu  $|\psi_+\rangle$  generuje:

$$|\psi\rangle = A \otimes I |\psi_+\rangle, \quad (A)_{mn} = a_{mn}.$$

Definujme nyní nový stav

$$\rho' = \frac{A^\dagger \otimes I \rho A \otimes I}{\text{Tr}(\rho A A^\dagger \otimes I)}.$$

Z definice  $A$ :  $(A A^\dagger)_{mn} = \sum_p (A)_{mp} (A^\dagger)_{pn} = a_{mp} a_{np}^*$ . Přitom  $D(\rho_A^\psi)_{mn} = a_{mp} a_{np}^*$ , tedy  $A A^\dagger = D\rho_A^\psi$ . Tohoto zápisu lze využít pro určení podmínky čistitelnosti systému.



Z podmínky separability Izotropického stavu, který ze stavu  $\rho'$  vznikne aplikací zobrazení  $U \otimes U^*$  pro náhodně zvolené unitární  $U$ :

$$\text{Tr}(\rho P_\psi) = \text{Tr}(\rho' P_+) > 1/D, P_\psi = |\psi\rangle\langle\psi|, P_+ = |\psi_+\rangle\langle\psi_+|.$$

Otázkou je, jak takové stavy vyčistit k  $P_\psi$ . Procedura bude obdobná předchozímu protokolu.

K1: Aplikací  $A \otimes 1$  přejdeme ze stavu  $\rho$  ke stavu  $\rho'$ .

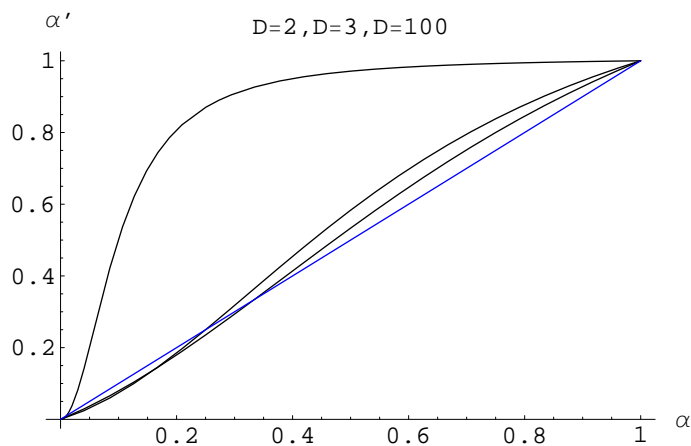
Důležitým prvkem pro konstrukci protokolu je invariance  $P_+$  vůči  $U \otimes U^*$ . Dále pak skutečnost, že na stavovém prostoru  $\mathcal{H}$  existuje pouze jediný jednoparametrický systém, který je  $U \otimes U^*$  invariantní, potom totiž:

K2: Použitím náhodně vybraného  $U \otimes U^*$  přejde  $\rho'$  na  $\rho_\alpha = (1 - \alpha)\frac{I}{D^2} + \alpha P_+$ . To plyne z obdobné úvahy jako v předchozím případě: jestliže čistota vstupního stavu  $\rho$  vůči stavu  $P_\psi$  je  $F$ , potom  $F$  je čistota stavu  $\rho'$  vůči  $P_+$ . S koeficientem  $\alpha = \frac{D^2 F - 1}{D^2 - 1}$  se ve výstupním stavu objeví  $P_+$ , který se ze vstupu zachová. Ostatní přípustné stavy se ve vstupu vyskytují s koeficientem  $1 - \alpha$ . Jediným dalším invariantním stavem tohoto zobrazení je úplně depolarizovaný stav  $\frac{I}{D^2}$ . Protože náhodně zvolené zobrazení a jeho následné „zapomenutí“ se efektivně chová jako operátor identity, musí pro takové zobrazení výstupní stav odpovídat těmto invariantním stavům. Pomocí takové operace si připravíme nové stavy jak terčového, tak kontrolního systému.

K2: Bilaterální  $G XOR$  t.j. zobrazení  $G XOR \otimes G XOR$  doplněné projekcí terčového systému na libovolný stav  $|i\rangle\langle i|$  převede kontrolní do stavu  $\rho_{\alpha'}$  kde  $\alpha' = \alpha \frac{[D(D+1)-2]\alpha+2}{(D+1)[1+(D-1)\alpha^2]}$ . Závislost  $\alpha'(\alpha)$  je funkcí spojitou a rostoucí pro  $\alpha \in [1/(D+1), 1]$ , tedy pokud vstupní hodnota  $\alpha$  byla větší než  $1/D$  výstupní hodnota  $\alpha'$  vzroste. To přesně souhlasí s redukčním kriteriem.

Opakováním posloupnosti kroků K1, K2 přejdeme od  $\rho'$  ke stavu  $|\psi_+\rangle$ . Aplikací  $A \otimes 1$  potom přejdeme ke stavu  $|\psi\rangle$ . Grafická závislost čistoty stavů na počtu provedených kroků iterace pro dané konkrétní vstupní čistoty ukazuje následující obrázek:

obr. 2:



## Kapitola č. 4

### Nelineární zobrazení matice hustoty

Následující text se bude zabývat protokoly, které nutně nezachovávají pevný tvar čištěného stavu. Pro tyto protokoly bude mít ovšem zásadní význam existence jistého nelineárního zobrazení, které doplněné lokálně unitárními, bilaterálními resp. unilaterálními, zobrazeními povedou k požadovanému vyčištění vstupního systému. Následující text bude úvodem do studia nelineárních zobrazení, úzká návaznost této problematiky na teorii stability řešení resp. teorii chaosu zde nebude řešena.

Nyní představím protokol, který má za úkol čistit stejně rozměrné stavy jako protokol Bennett-Brassard. Protokol byl již zmíněn v [1], nicméně pro úplnost textu zde bude představen poněkud podrobněji.

Jde o problém dvoučásticového, dvouhladinového kvantového systému. Předpokládá se, že jsou k dispozici identické kopie systému, který bylo třeba čistit. Tento požadavek je opět splnitelný náhodným provedením některé z operací  $B_x, B_y, B_z$  na vstupních systémech, za předpokladu konstantní čistoty systému, ke stavu, ke kterému bychom rádi systém vyčistili. Vždy jedna komponenta systému se pohybovala v oblasti dosahu pozorovatele A a druhá v dosahu pozorovatele B, systémy byly na sobě nezávislé. Purifikační procedura se získala lokálním použitím zobrazení, která v již dříve zmíněné ortonormální bázi mají maticovou reprezentaci:

$$U_A = \begin{pmatrix} -i\sigma_y & 0 \\ 0 & 1 \end{pmatrix}, U_B = \begin{pmatrix} i\sigma_y & 0 \\ 0 & 1 \end{pmatrix} \text{ kde } \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Tyto transformace jsou unitární. S branou  $XOR$  jsou svázány pomocí unitární transformace. Dále se též užila projekce  $P_- = |1\rangle\langle 1|$  na stav se spinem  $-1/2$ .

K1: Nelineární zobrazení bylo definováno následovně:

$$(1 \otimes P_-)_A (1 \otimes P_-)_B U_A U_B (\rho^{in} \otimes \rho^{in}) U_B^\dagger U_A^\dagger (1 \otimes P_-)_B (1 \otimes P_-)_A = \rho^{out} \otimes P_-$$

$$\text{kde } \rho^{in} \rightarrow \rho^{out} = \begin{pmatrix} \rho_{11}^2 & -\rho_{12}^2 & \rho_{13}^2 & -\rho_{14}^2 \\ -\rho_{21}^2 & \rho_{22}^2 & -\rho_{23}^2 & \rho_{24}^2 \\ \rho_{31}^2 & -\rho_{32}^2 & \rho_{33}^2 & -\rho_{34}^2 \\ -\rho_{41}^2 & \rho_{42}^2 & -\rho_{43}^2 & \rho_{44}^2 \end{pmatrix}$$

je výstupní stav sdílený mezi pozorovateli A,B. Schéma je korektní, neboť jsou použity jen úplně pozitivní operátory.

Transformace zachovává singletní stavy

$$\begin{aligned} \psi^- &= \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle), \\ \phi^- &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle). \end{aligned}$$

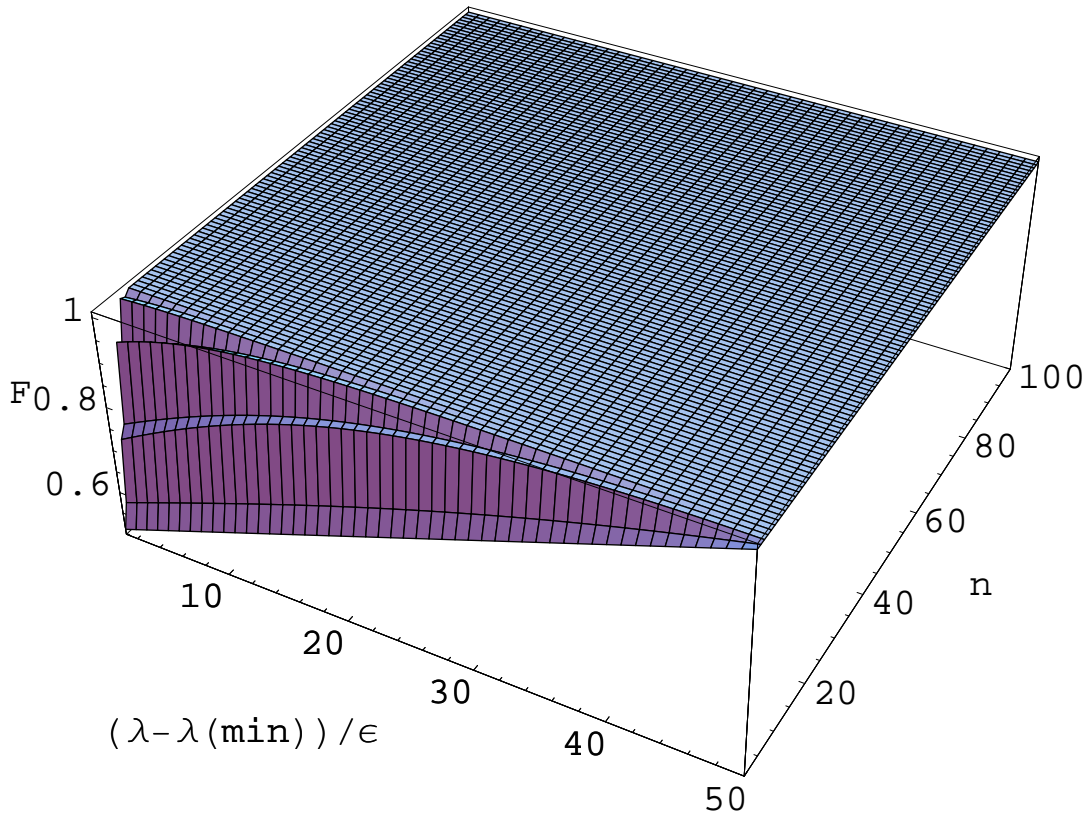
K2: Následně A a B provedou operaci  $B_x$ . Tím dojde k zaměně

$$\psi^+ = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \text{ a } \phi^+ = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle),$$

aniž by změnila ostatní Bellovské stavy. Krok čistícího protokolu je nyní kompletní. Na počátku procedury může dojít k poklesu čistoty, ale opakováním kroků nakonec dojde k vyčištění všech systémů se vstupní čistotou  $F^{in} > \frac{1}{2}$ , což odpovídá nutné podmínce provázanosti.

Grafická závislost čistoty stavů na počtu provedených kroků iterace pro dané konkrétní vstupní čistoty ukazuje obr. 4. Projekce vstupního stavu je charakterizována  $\lambda \in [1/2, 1]$ . Počet kroků čistící procedury (t.j. nelineární zobrazení + rotace) probíhá  $n \in \{1, \dots, 100\}$ . Volba parametru  $\lambda$  není spojitá, ale mění se o hodnotu 0.01, tato hodnota byla použita také pro rozlišení, zda se vstupní stav podařilo dostatečně odčistit do stavu výstupního stavu s  $F = 0.99$ .

obr. 4:



### Deterministický protokol

Použitím *GXOR* brány definujeme zajímavou třídu nelineárních zobrazení, kterou dále využijeme pro konstrukci purifikačních protokolů.

Předpokládejme, že máme k dispozici dva kvantové  $D$ -hladinové systémy ve stavech  $\sigma^c, \sigma^t$  tzv. kontrolní, terčový systém. Těm odpovídají stavové Hilbertovy prostory  $H^c, H^t$ . Definujme operátor:

$$T : \mathcal{B}(H^c) \otimes \mathcal{B}(H^t) \rightarrow \mathcal{B}(H^c) \otimes \mathcal{B}(H^t) \text{ takové, že } T(\sigma^c, \sigma^t) = \frac{A(\sigma^c \otimes \sigma^t)A^\dagger}{\text{Tr}(A(\sigma^c \otimes \sigma^t)A^\dagger)}$$

kde  $A = (1_c \otimes P)GXOR_{ct}$ ,  $1_c$  značí jednotkový operátor na Hilbertově prostoru kontrolního systému a  $P = |p\rangle_t\langle p|_t$  je projektor na stav  $|p\rangle_t$  terčového systému. Dosadím za:

$$\sigma^c = \sum_{ij}^{D-1} \sigma_{ij}^c |i\rangle_c \langle j|_c$$

$$\sigma^t = \sum_{ij}^{D-1} \sigma_{ij}^t |i\rangle_t \langle j|_t$$

do

$$T(\sigma^c, \sigma^t) = \frac{A(\sigma^c \otimes \sigma^t)A^\dagger}{\text{Tr}(A(\sigma^c \otimes \sigma^t)A^\dagger)} = (1_c \otimes P)GXOR_{ct}(\sigma^c \otimes \sigma^t)GXOR_{ct}(1_c \otimes P)/\text{Tr}(\dots) =$$

$$= (1_c \otimes P)GXOR_{ct}\left(\sum_{ijkl}^{D-1} \sigma_{ij}^c \sigma_{kl}^t |i\rangle_c |k\rangle_t \langle j|_c \langle l|_t\right)GXOR_{ct}(1_c \otimes P)/\text{Tr}(\dots) =$$

$$= \frac{\sum_{ijkl}^{D-1} \sigma_{ij}^c \sigma_{kl}^t |i\rangle_c \langle j|_c \otimes P_c |i \ominus k\rangle_t \langle j \ominus l|_c P}{\sum_{ikl}^{D-1} \sigma_{ii}^c \sigma_{kl}^t \langle p|i \ominus k\rangle_t \langle i \ominus l|p\rangle} = \sigma_{out}^c \otimes P_t$$

kde

$$\sigma_{out}^c = \frac{\sum_{i,j}^{D-1} \sigma_{ij}^c \sigma_{i-p,j-p}^t |i\rangle_c \langle j|_c}{\sum_i^{D-1} \sigma_{ii}^c \sigma_{i-p,i-p}^t}.$$

Za předpokladu  $\sigma^c = \sigma^t = \sigma$  se tvar zjednoduší na

$$T(\sigma, \sigma) = \sigma_{out} \otimes P$$

kde

$$\sigma_{out} = \frac{\sum_{i,j}^{D-1} \sigma_{ij} \sigma_{i-p,j-p} |i\rangle_c \langle j|_c}{\sum_i^{D-1} \sigma_{ii} \sigma_{i-p,i-p}}.$$

Zobrazení převádí matici hustoty na matici hustoty, přitom není injektivní a je nelineární. Vhodnou volbou parametru  $p$  můžeme docílit zachování jistých vstupních stavů.

Provedme nyní rozšíření zobrazení. Předpokládejme, že máme k dispozici  $N$  identických terčových systémů a kontrolní i terčový systém jsou vždy  $M$  quditové systémy tvaru

$$\sigma^c = \sum_{\mathbf{ij}} \sigma_{\mathbf{ij}}^c |\mathbf{i}\rangle_c \langle \mathbf{j}|_c$$

$$\sigma^t = \sum_{\mathbf{ij}} \sigma_{\mathbf{ij}}^t |\mathbf{i}\rangle_t \langle \mathbf{j}|_t$$

kde  $\mathbf{i} = (\mathbf{i}_1, \dots, \mathbf{i}_M), \mathbf{j} = (\mathbf{j}_1, \dots, \mathbf{j}_M)$ , nyní

$$A = (1_c \otimes P) \prod_{j=1}^m \Pi_i^N GXOR_{ct_i}^{(j)}$$

kde  $P = \prod_{i=1}^N \otimes P_{t_i}$  a

$$P_{t_i} = |\mathbf{p}_i\rangle_{t_i} \langle \mathbf{p}_i|_{t_i}$$

je projektor na stav  $i$ -tého terčového systému.  $GXOR_{ct_i}^{(j)}$  je operátor  $GXOR$  působící na  $j$ -tou komponentu kontrolního a  $i$ -tého terčového systému. Pro zobrazení  $T$  potom platí:

$$\begin{aligned} T(\sigma^c, \sigma^t, \dots, \sigma^t) &= (1_c \otimes P) \prod_{j=1}^M \prod_{i=1}^N GXOR_{ct_i}^{(j)}(\sigma^c \otimes \sigma^t) ((1_c \otimes P) \prod_{j=1}^M \prod_{i=1}^N GXOR_{ct_i}^{(j)})^\dagger / \text{Tr}(\dots) = \\ &= (1_c \otimes P) \prod_{j=1}^M \prod_{i=1}^N GXOR_{ct_i}^{(j)}(\sigma^c \otimes \sigma^t) \prod_{j=M}^1 \prod_{i=N}^1 GXOR_{ct_i}^{(j)}(1_c \otimes P) / \text{Tr}(\dots) = \\ &= (1_c \otimes P) \prod_{j=1}^M \prod_{i=1}^N GXOR_{ct_i}^{(j)} \left( \sum_{\mathbf{kl}} \sigma_{\mathbf{kl}}^c |\mathbf{k}\rangle \langle \mathbf{l}| \otimes \sum_{\mathbf{k}_1 \mathbf{l}_1} \sigma_{\mathbf{k}_1 \mathbf{l}_1}^t |\mathbf{k}_1\rangle \langle \mathbf{l}_1| \otimes \sum_{\mathbf{k}_2 \mathbf{l}_2} \sigma_{\mathbf{k}_2 \mathbf{l}_2}^t |\mathbf{k}_2\rangle \langle \mathbf{l}_2| \otimes \dots \right. \\ &\quad \left. \dots \otimes \sum_{\mathbf{k}_N} \sigma_{\mathbf{k}_N \mathbf{l}_N}^t |\mathbf{k}_N\rangle \langle \mathbf{l}_N| \right) ((1_c \otimes P) \prod_{j=1}^M \prod_{i=1}^N GXOR_{ct_i}^{(j)})^\dagger / \text{Tr}(\dots) = \\ &= \sum_{\mathbf{kl}} \sigma_{\mathbf{kl}}^c |\mathbf{k}\rangle_c \langle \mathbf{l}|_c \otimes \sigma_{\mathbf{k} \ominus \mathbf{p}_1, \mathbf{l} \ominus \mathbf{p}_1}^t \otimes \dots \otimes \sigma_{\mathbf{k} \ominus \mathbf{p}_N, \mathbf{l} \ominus \mathbf{p}_N}^t \otimes P / \text{Tr}(\dots) \end{aligned}$$

kde  $\mathbf{i} \ominus \mathbf{p} = (i_1 \ominus p_1, \dots, i_M \ominus p_M)$ .

Jsouli terčové systémy identické s kontrolním a také projekce na jednotlivé komponenty jsou stejné, výsledkem je:

$$T(\sigma, \sigma, \dots, \sigma) = \frac{\sum_{\mathbf{kl}} \sigma_{\mathbf{kl}} \sigma_{\mathbf{k} \ominus \mathbf{p}, \mathbf{l} \ominus \mathbf{p}}^N |\mathbf{k}\rangle_c \langle \mathbf{l}|_c}{\sum_{\mathbf{k}} \sigma_{\mathbf{k}\mathbf{k}} \sigma_{\mathbf{k} \ominus \mathbf{p}, \mathbf{k} \ominus \mathbf{p}}^N}$$

Snadno lze nahlédnout, že takovéto zobrazení zobrazuje vstupní matice hustoty na matici hustoty. Není injektivní a je nelineární. Také existují stavy, které jsou mu invariantní.

Tohoto zobrazení využijeme ke konstrukci deterministické purifikačního protokolu, který bude mít za úkol odčistit co možná nejširší třídu znečištěných stavů k jistému předem známému provázanému stavu s maticí hustoty  $\rho$ , deterministický přitom znamená, že během celého procesu jsou použity předem známé  $LOCC$  transformace, doplněné předem známými filtry, viz [1]. Nyní definuji dva užitečné pojmy viz [11].

Říkáme, že  $\sigma^c$  je invariantní působení  $T$  pokud  $\sigma_{out}^c = \sigma^c$ , pro všechna  $N$ . Říkáme, že  $\omega$  invariantní stav je **atraktorem** zobrazení  $T$ , pokud existuje množina vstupních stavů  $\Omega$ , takových že

$$\lim_{N \rightarrow \infty} T(\sigma^c, \sigma^{t_1}, \dots, \sigma^{t_N}) = \omega,$$

pro každé  $\sigma^c \in \Omega$ . Atraktory tedy představují invariantní stavy jejichž jisté okolí se pod vlivem nelineárního zobrazení opět zobrazí na jejich dostatečně blízké okolí.

Konstrukci protokolu provedu pro případ  $\sigma^c = \sigma^t = \sigma$ . Diskutujme nyní body konstrukce obecného zobrazení, stav ke kterému čistíme má matici hustoty  $\rho$ .

1. Protokol musí zachovávat stav  $\rho$ , ke kterému se má čistit. Proto  $T$  by mělo zachovávat matici hustoty  $\rho$ , t.j.  $T(\rho, \rho, \dots, \rho) = \rho$ . Pro dané  $\rho$  je třeba naléznout všechna taková nelineární zobrazení. Ta jsou určena parametry  $N$  a  $\mathbf{p}$  ozn.  $\{T_{\mathbf{p}}^N\}$ .

2. Pro nalezená nelineární zobrazení  $\{T_{\mathbf{p}}^N\}$  prozkoumám všechny atraktory. Pro konstrukci protokolu zvolím ta z nich, která mají nejmenší počet invariantních stavů. Budu požadovat aby použité zobrazení mělo stav  $\rho$  jako atraktor s co nejmohutnější množinou  $\Omega$ . Pro ostatní atraktory požaduji co nejmenší mohutnost  $\Omega$ .

3. Twirlingem rozumím složení lokálně unitárních zobrazení provedených na jednotlivé částice kontrolního systému, které efektivně odstíní nežádoucí členy po působení nelineárního zobrazení a tím v konečném důsledku zvýší čistotu výstupního stavu. Otázkou je, jak tento požadavek precizovat. Vzhledem k bodu 2 musí twirling zachovávat matici hustoty  $\rho$ . Také by bylo žádoucí, aby twirling převáděl výstup po nelineárním zobrazení do stavu co možná nejbližšího prvkům  $\Omega$  pro  $\rho$ , co nejbližší  $\rho$  resp. aby v co největší míře byla množina  $\Omega$  stavu  $\rho$  vůči twirlingu uzavřená, přitom aby měl co nejméně vlastních stavů různých od  $\rho$ .

V kapitole č. 2 jsem klasifikoval lokálně unitární zobrazení, která zachovávají jistý provázaný stav. Nalezení zobrazení, pro která by společné invariantní stavy byly pouze  $\rho$  a úplně depolarizovaný stav (s maticí hustoty úměrné operátoru identity  $I$ ) by mělo za následek, že všechny znečištěné stavy bychom pomocí náhodné aplikace zobrazení mohli převést do jednoparametrického stavu s maticí hustoty ve tvaru lineární kombinace  $\rho$  a  $I$ . Pro takový pevný tvar vstupních stavů bych diskutoval jejich čistitelnost. Měl bych tím zajištěno, že čistím skutečně všechny možné vstupní stavy. Pro tříčásticové systémy jsem v tomto smyslu nejvíce prozkoumal antisymetrické stavy. Modelově právě pro ně předvedu konstrukci purifikačního protokolu (viz kap 2).

1. Stavový prostor systému je  $\mathcal{H} = C^3 \otimes C^3 \otimes C^3$ . Antisymetrický stav má pro orthonormální bázi  $|i\rangle \in C^3$  tvar

$$|A\rangle = \frac{1}{\sqrt{3!}} \sum_{\pi} \text{sgn}(\pi) |\pi_1 \pi_2 \pi_3\rangle,$$

jeho znečištění uvažuji ve tvaru

$$\begin{aligned} \lambda |A\rangle \langle A| + \frac{1-\lambda}{27} I &= \left( \frac{\lambda}{6} + \frac{1-\lambda}{27} \right) \sum_{\pi} |\pi_1 \pi_2 \pi_3\rangle \langle \pi_1 \pi_2 \pi_3| + \\ &+ \frac{1-\lambda}{27} \sum_{(i=j) \vee (j=k) \vee (i=k)} |ijk\rangle \langle ijk| + \frac{\lambda}{6} \sum_{\pi \neq \sigma} \text{sgn}(\pi) \text{sgn}(\sigma) |\pi_1 \pi_2 \pi_3\rangle \langle \sigma_1 \sigma_2 \sigma_3|. \end{aligned}$$

Nelineární zobrazení  $T$  má zachovávat  $\sigma^c = |A\rangle\langle A|$ , to je z definice  $T$  ekvivalentní podmínce:

$$\sigma_{\mathbf{i},\mathbf{j}}^c = \frac{\sigma_{\mathbf{i},\mathbf{j}}^c(\sigma_{\mathbf{i}\ominus\mathbf{p},\mathbf{j}\ominus\mathbf{p}}^c)^N}{\sum_{\mathbf{i}} \sigma_{\mathbf{i},\mathbf{i}}^c(\sigma_{\mathbf{i}\ominus\mathbf{p},\mathbf{i}\ominus\mathbf{p}}^c)^N}$$

kde  $\sigma_{\mathbf{i},\mathbf{j}}^c = \text{sgn}(\mathbf{i}) \text{sgn}(\mathbf{j}) \in \{0, \pm 1\}$ . Označme  $\mathbf{p} = (p_1, p_2, p_3)$ . Pro konstrukci nelineárního zobrazení je důležitá skutečnost, že zobrazení  $\ominus : \{0, 1, 2\} \times i \rightarrow \{0, 1, 2\}$ , zobrazuje množinu  $\{0, 1, 2\}$  na sebe jednoznačně pro každé pevné  $i \in \{0, 1, 2\}$

Bude-li  $p_1 = p_2 = p_3 \in \{0, 1, 2\}$ , potom pro  $\pi = (\pi_1, \pi_2, \pi_3)$  permutaci  $\{0, 1, 2\}$  je  $\pi \ominus \mathbf{p}$  také permutace. Bude-li např.  $p_1 \neq p_2$ , potom pro každé  $i \in \{0, 1, 2\}$  existuje  $j \in \{1, 2, 3\}$ ,  $j \neq i$  takové že  $p_1 \ominus i = p_2 \ominus j$  např.  $i = 1$ ,  $p_1 = 1$ ,  $p_1 = 2$ , je  $j = 2$  a  $(123) \rightarrow (0, 0, 3 \ominus \pi_3)$ . To tedy znamená, že jedinou přípustnou volbou  $\mathbf{p}$  je  $p_1 = p_2 = p_3 = p$ . Protože pro tuto volbu  $\text{sgn}(\pi) = \pi \ominus \mathbf{p}$ , vzhledem ke kladné hodnotě  $\sigma_{\mathbf{p},\mathbf{p}}^c$  musí  $N = 2k$  pro  $k \in \mathbf{N}$ .

Dále

$$\frac{(\sigma_{\mathbf{i}\ominus\mathbf{p},\mathbf{j}\ominus\mathbf{p}}^c)^N}{\sum_{\mathbf{i}} \sigma_{\mathbf{i},\mathbf{i}}^c(\sigma_{\mathbf{i}\ominus\mathbf{p},\mathbf{i}\ominus\mathbf{p}}^c)^N} = \frac{(\frac{1}{\sqrt{6}})^{2k}}{6 \cdot \frac{1}{6} (\frac{1}{\sqrt{6}})^{2k}} = 1,$$

tedy jediná vyhovující nelineární zobrazení jsou určena parametry  $\mathbf{p} = (p, p, p)$  a  $N = 2k$ .

2. Pro takové zobrazení naleznou tvar prvků z  $\Omega$  vyhledem k  $|A\rangle\langle A|$ :  
 $p = 0$ :

$$\lim_{N \rightarrow \infty} T(\sigma, \sigma, \dots, \sigma)_{\mathbf{i},\mathbf{j}} = \lim_{k \rightarrow \infty} \frac{\sigma_{\mathbf{i},\mathbf{j}}^{N+1}}{\sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}}^{N+1}} = \frac{1}{6} \text{sgn}(\mathbf{i}) \text{sgn}(\mathbf{j})$$

$\Leftrightarrow$

$$\lim_{k \rightarrow \infty} \frac{1}{\sum_{\mathbf{k}} \left(\frac{\sigma_{\mathbf{k},\mathbf{k}}}{\sigma_{\mathbf{i},\mathbf{j}}}\right)^{2k+1}} = \frac{1}{6} \text{sgn}(\mathbf{i}) \text{sgn}(\mathbf{j})$$

Je-li  $\mathbf{i} = \mathbf{j} = \pi$ , potom

$$\lim_{k \rightarrow \infty} \frac{1}{\sum_{\mathbf{k}} \left(\frac{\sigma_{\mathbf{k},\mathbf{k}}}{\sigma_{\mathbf{i},\mathbf{j}}}\right)^{2k+1}} = \frac{1}{6}$$

$\Leftrightarrow$

$\sigma_{\pi,\pi} = K \wedge \sigma_{\mathbf{k},\mathbf{k}} < \sigma_{\pi,\pi}$  pro všechny  $\pi$  a  $\mathbf{k} \neq \pi$ .

Je-li  $\pi \neq \sigma$ , potom

$$\lim_{k \rightarrow \infty} \frac{1}{\sum_{\mathbf{k}} \left(\frac{\sigma_{\mathbf{k},\mathbf{k}}}{\sigma_{\pi,\sigma}}\right)^{2k+1}} = \frac{1}{6} \text{sgn}(\pi) \text{sgn}(\sigma)$$

$\Leftrightarrow$

$\sigma_{\pi,\sigma} = K \cdot \text{sgn}(\pi) \text{sgn}(\sigma)$

Je-li  $\mathbf{i} \neq \pi$  potom

$$\lim_{k \rightarrow \infty} \frac{1}{\sum_{\mathbf{k}} \left( \frac{\sigma_{\mathbf{k},\mathbf{k}}}{\sigma_{\mathbf{i},\mathbf{j}}} \right)^{2k+1}} = 0$$

$$\Leftrightarrow$$

$|\sigma_{\mathbf{i},\mathbf{j}}| < \sigma_{\mathbf{k},\mathbf{k}}$  pro alespoň jedno  $\mathbf{k}$ .

To jsou tedy nutné a postačující podmínky takových stavů.

Pro  $p \in 1, 2$

$$\lim_{N \rightarrow \infty} T(\sigma, \sigma, \dots, \sigma)_{\mathbf{i},\mathbf{j}} = \lim_{k \rightarrow \infty} \frac{\sigma_{\mathbf{i},\mathbf{j}} \sigma_{\mathbf{i} \ominus \mathbf{p}, \mathbf{j} \ominus \mathbf{p}}^{2k}}{\sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}} \sigma_{\mathbf{k} \ominus \mathbf{p}, \mathbf{k} \ominus \mathbf{p}}^{2k}} = \frac{1}{6} \operatorname{sgn}(\mathbf{i}) \operatorname{sgn}(\mathbf{j})$$

Z faktu  $i \ominus j = k \ominus j \Leftrightarrow i = k$  se snadno stejným způsobem odvodí podmínky na atraktory, ty jsou naprosto shodné s podmínkami pro  $p = 0$ .

Podívejme se na invariantní stavy odvozených nelineárních zobrazení. To klade na jejich matici hustoty podmínku

$$\frac{\sigma_{\mathbf{i},\mathbf{j}} \sigma_{\mathbf{i} \ominus \mathbf{p}, \mathbf{j} \ominus \mathbf{p}}^{2k}}{\sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}} \sigma_{\mathbf{k} \ominus \mathbf{p}, \mathbf{k} \ominus \mathbf{p}}^{2k}} = \sigma_{\mathbf{i},\mathbf{j}}$$

$$\Leftrightarrow$$

$$(\sigma_{\mathbf{i} \ominus \mathbf{p}, \mathbf{j} \ominus \mathbf{p}})^{2k} = \sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}} (\sigma_{\mathbf{k} \ominus \mathbf{p}, \mathbf{k} \ominus \mathbf{p}})^{2k}$$

Je-li  $p = 0$ :

$$\sigma_{\mathbf{i},\mathbf{j}}^{2k} = \sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}}^{2k+1}$$

Pro  $\mathbf{i} = \mathbf{j}$  je  $\sigma_{\mathbf{i},\mathbf{i}}^{2k} = \sum_{\mathbf{k}} \sigma_{\mathbf{k},\mathbf{k}}^{2k+1}$ . Protože  $\sigma_{\mathbf{i},\mathbf{i}} > 0$  je nutně  $\sigma_{\mathbf{i},\mathbf{i}} = C > 0$ . Dosazením do rovnice vychází  $C = 1/K$  kde  $K$  je počet nenulových  $\sigma_{\mathbf{i},\mathbf{i}}$ . Pro  $\mathbf{i} \neq \mathbf{j}$  z Moirovy věty [Jar]:  $\sigma_{\mathbf{i},\mathbf{j}} = \frac{1}{K} \exp(i \frac{2\pi n}{2k})$ ,  $n = 0, \dots, 2k - 1$ . Postupem stejným předešlému se ověří, že množiny  $\Omega$  pevných bodů  $\sigma$  zobrazení jsou ve tvaru:

$$\delta_{\mathbf{ii}} = \tilde{C} > 0 \text{ pro } \sigma_{\mathbf{ii}} = 1/K > 0,$$

$$\delta_{\mathbf{ij}} = C \cdot \exp(i \frac{2\pi n}{2k}) \text{ pro } \sigma_{\mathbf{ij}} = 1/K \cdot \exp(i \frac{2\pi n}{2k}),$$

$$|\delta_{\mathbf{ij}}| < 1/K \text{ pro } \sigma_{\mathbf{ij}} = 0.$$

Podmínka  $\operatorname{Tr}(\sigma) = 1$  je jistě zaručena, podmínka nezápornosti vlastních čísel je také splněna, zbývá prozkoumat podmínku hermitovosti  $\sigma$ :  $\sigma_{\mathbf{ij}} = \sigma_{\mathbf{ji}}^\dagger \Leftrightarrow n(\mathbf{ji}) = 2l - n(\mathbf{ij})$  pro nějaké  $l \in \mathbf{N}$ .

Je-li  $p \in \{1, 2\}$ , potom se snadno nahlédne, že platí naprosto stejné podmínky.

Nyní se podívejme, kolik takových stavů je čistých. Je-li

$$\sigma = \frac{1}{K} \sum_{m,n=1}^K \exp(i \frac{2\pi(\alpha_{\mathbf{i}_m} - \alpha_{\mathbf{i}_n})}{2k}) |\mathbf{i}_m\rangle \langle \mathbf{i}_n|,$$



potom:

$$\begin{aligned}\alpha_{\mathbf{i}_m} - \alpha_{\mathbf{i}_n} &= n(\mathbf{i}_m \mathbf{i}_n) + 2q \\ \alpha_{\mathbf{i}_n} - \alpha_{\mathbf{i}_m} &= n(\mathbf{i}_n \mathbf{i}_m) + 2r = 2k - n(\mathbf{i}_m \mathbf{i}_n) + 2r\end{aligned}$$

odtud tedy  $q + r + k = 0$ ,  $q, r \in \mathbf{N}$

### 3. Konstrukce twirlingu

Vstupní čistota antisymetrického stavu je podle definice  $F_{in} = \lambda + \frac{1-\lambda}{27}$ . Nutná podmínka separability říká, že  $\lambda \leq (1 + 2/9)^{-1} = 9/11$ . Uvidíme, že se nám podaří zkonstruovat purifikační protokol, který efektivně odčistí mnohem více znečištěné stavy, tedy ukážeme, že tato nutná podmínka separability není pro antisymetrické stavy postačující.

Z definice antisymetrického znečištěného stavu se snadno nahlédne, že pro  $\lambda > 0$  jsou to prvky  $\Omega$  pro  $|A\rangle\langle A|$  a libovolné  $p \in \{0, 1, 2\}$ . To je vidět přímo porovnáním tvaru antisymetrického stavu a prvků  $\Omega$ :  $\sigma_{\pi, \pi} = \frac{\lambda}{6} + \frac{1-\lambda}{27} > \frac{\lambda}{6} = |\sigma_{\mathbf{i}, \mathbf{j}}|$  pro  $\mathbf{i} \neq \pi$ . Pro dostatečně vysoké  $N$  resp.  $k$  se již po prvním kroku purifikačního protokolu dostaneme dostatečně blízko čistému antisymetrickému stavu. Pro efektivitu protokolu je ovšem žádoucí, aby počet používaných terčových systémů byl co možná nejmenší. Podívejme se tedy jak vypadá výstup po první aplikaci nelineárního zobrazení. Již z dříve uvedených vlastností operace  $\otimes$  se snadno nahlédne, že pro libovolné  $p \in \{0, 1, 2\}$  má výstup po nelineárním zobrazení tvar  $6.\alpha_1 |A\rangle\langle A| + 27.\beta_1 \frac{1}{27} + (\gamma_1 - \alpha_1) \sum_{\pi} |\pi\rangle\langle \pi|$  kde

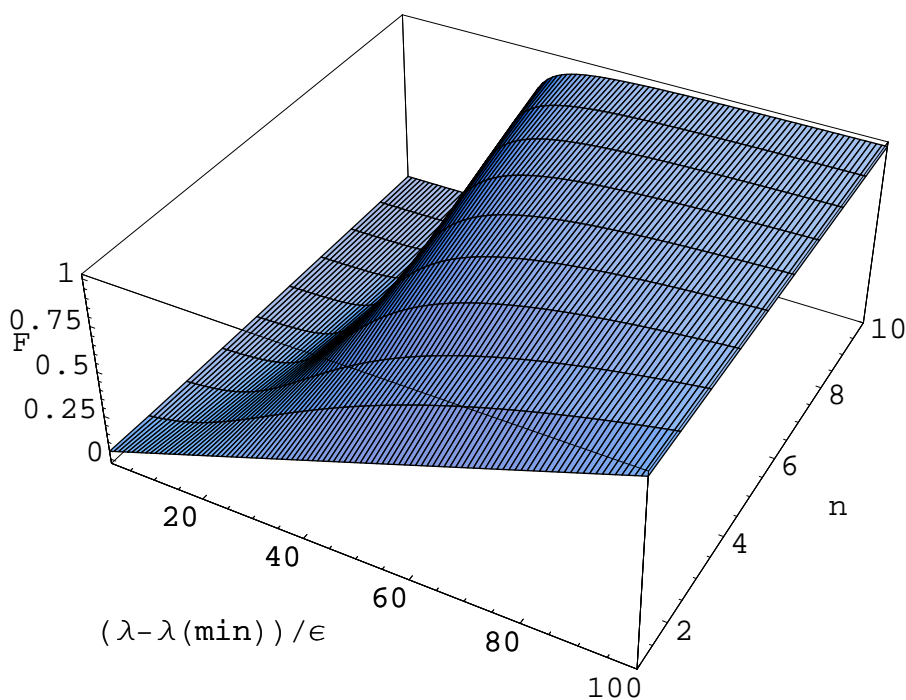
$$\begin{aligned}\alpha_1 &= \left(\frac{\lambda}{6}\right)^{2k+1} . \delta_1 \\ \beta_1 &= \left(\frac{1-\lambda}{27}\right)^{2k+1} . \delta_1 \\ \gamma_1 &= \left(\frac{\lambda}{6} + \frac{1-\lambda}{27}\right)^{2k+1} . \delta_1 \\ \delta_1 &= (6.\gamma + 27.\beta)^{-1}.\end{aligned}$$

tento stav je prvkem  $\Omega$  pro  $|A\rangle\langle A|$ . Pokusme se nyní zkonstruovat purifikační protokol pro nejmenší přípustné  $k = 1$ . Abychom vytvořili efektivní protokol, potřebujeme zkonstruovat twirling. Na výběr podle kapitoly 2 mám ze tří zobrazení resp. jejich složení, neboť složením unitárních zobrazení vznikne opět unitární zobrazení. První dvě zobrazení jsou pevně definována, množinu  $\Omega$  stavu  $|A\rangle\langle A|$  převádí do sebe. Invariantní stavy prvního z nich jsou dány podmínkami na maticové elementy:  $\sigma_{\mathbf{i}, \mathbf{j}} \neq 0 \Leftrightarrow \{i_1, i_2, i_3\} = \{j_1, j_2, j_3\}$  pro prvé z nich. Pro druhé z nich jsou podmínky na maticové koeficienty invariantních stavů  $\sigma_{(ijm_0), ((ijn_0))} = \sigma_{(ijn_0), ((ijm_0))}$  atd. Pro třetí z nich se obecné ověření vlastností bodu 3 stalo nereálné. Z obecných rotací jsem se proto omezil na pokud možno, co nejjednodušší z nich, rotace kolem vybrané osy  $|i\rangle$ ,  $i \in \{0, 1, 2\}$ . Taková zobrazení jsou jednoparametrická a jejich matice obsahují maximální přípustný počet nulových koeficientů (4), přitom neuvažují triviální identitu. Snadno se nahlédne, že podmínky kladené předchozími zobrazeními jsou nutná i pro tyto rotace. Jako nejvdnější kandidát se přitom jeví zobrazení rotací o  $n.\pi/4$ ,  $n \in \{1, 2, 3\}$ , neboť jejich akce na  $\sum_{\pi} |\pi\rangle\langle \pi|$  způsobila rozklad takového součtu, matice přitom obsahovaly minimální počet nenulových prvků (24), všechny nenulové koeficienty měly přitom stejnou absolutní hodnotu a polovina z nich nabývala kladnou resp. zápornou hodnotu. Taková

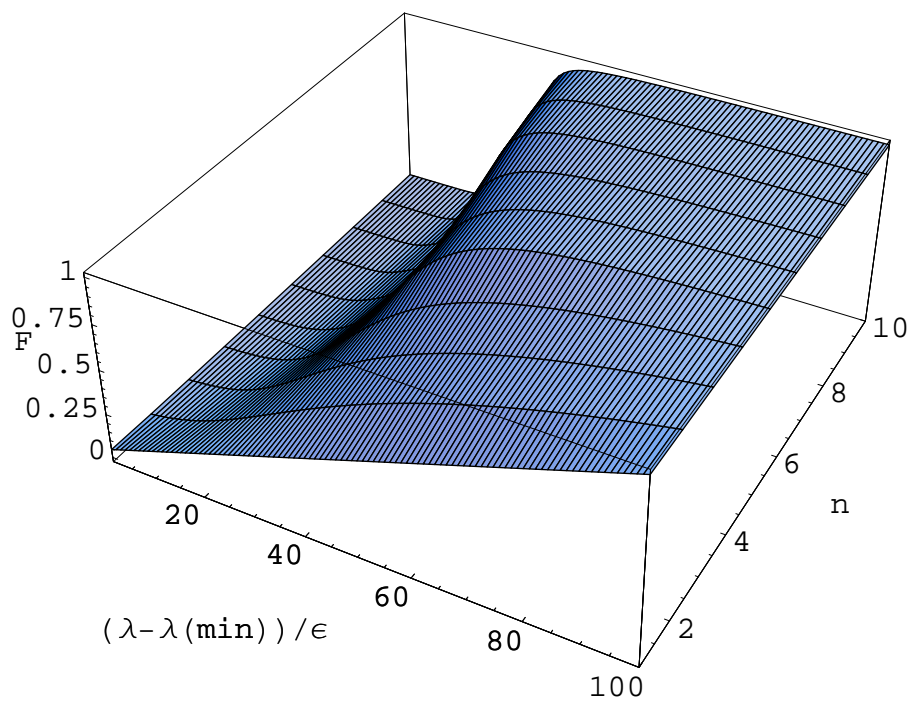
zobrazení dobře vystihovala symetrii antisymetrických stavů. Dopad takových twirlingů na další průběh čištění jsem dále zkoumal přímou konstrukcí protokolů. Ze všech přípustných kombinací twirlingu se jako nejvhodnější jevila volba složení rotací o  $\pi/4$  kolem os  $x, y, z$  t.j.  $U = R_z(\frac{\pi}{4})R_y(\frac{\pi}{4})R_x(\frac{\pi}{4})$  resp. jejich cyklická permutace.

Grafické znázornění průběhu čistící procedury pro  $p = 0, 1, 2$  znázorňují obr. 4–6. Výstupní čistotu stavu  $F$  závisí od vstupní hodnoty  $\lambda$  a počtu iteračních kroků  $n$ . Graf znázorňuje situaci kdy v deseti iteračních krocích má dojít k co největšímu odčištění. Parametry  $\lambda(\min) = 0.01$   $\epsilon = 0.01$ . Pro volbu  $p = 0, 2$  bylo dosaženo přesnosti odčištění  $F > 0.99$  i pro vstupní  $\lambda = 0.51$  resp.  $\lambda = 0.35$ , pro  $p = 1$  protokol pouze lokálně zvyšoval čistotu systému a to od hodnoty  $\lambda = 0.35$ .

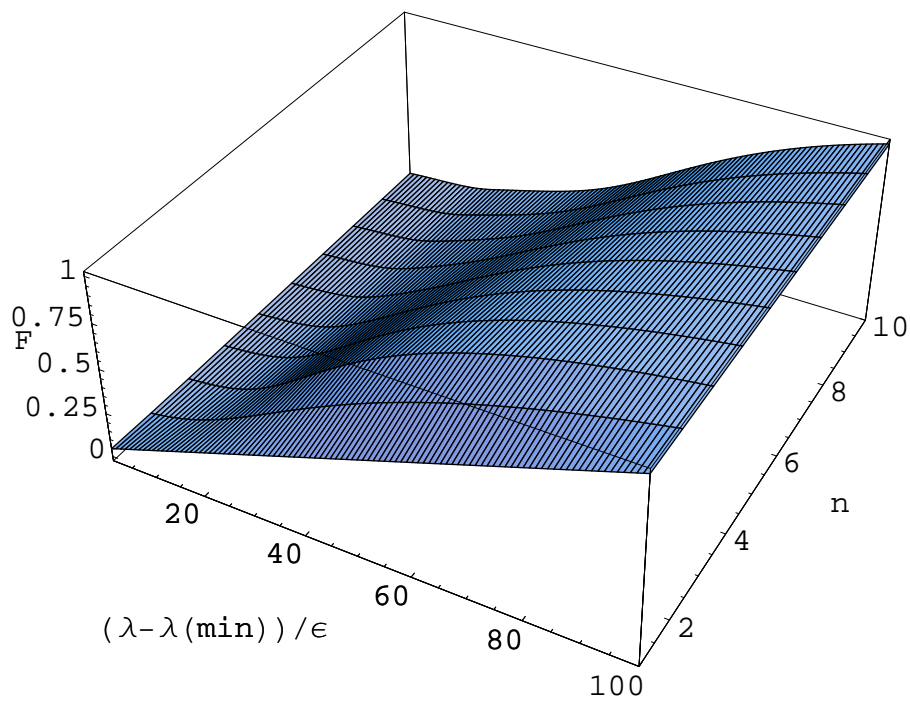
$p = 2$ , obr. 4:



$p = 0$ , obr. 5:



$p = 1$ , obr. 6:



# Kapitola č. 5

## Závěr

Motivován příkladem kvantového teleportu, zaměřil jsem se v této práci na řešení problému přenosu komponent provázaných konečných systémů na velké vzdálenosti za použití přípustných *LOCC* operací.

Pojem provázanosti byl precizován ve druhé kapitole. Zavedením kritérií separability kvantových systémů došlo k propojení provázanosti kvantového systému s otázkou jeho čistitelnosti k jistému maximálně provázanému stavu. Žádný separabilní systém není možné odčistit do nějakého provázaného stavu. Na druhou stranu, ale ne všechny provázané systémy lze odčistit k jistému maximálně provázanému stavu (bound entangled systems). Pro kritérium čistoty  $\sigma$  vzhledem k  $\rho$  jsem zvolil projekci  $F = \text{Tr}(\rho\sigma)$ .

Definicí Wernerových a izometrických stavů jsem získal jediné třídy  $U \otimes U$  resp.  $U \otimes U^*$ ,  $U$  unitární, invariantních stavů dvoučásticových  $D$ -hladinových systémů. Studium čistitelnosti takových systémů potom charakterizuje obecně čistitelnost dvouquditových stavů. Pro stejný účel u  $N$ -quditových systémů byla diskutována třída symetrických a antisymetrických stavů.

Konstrukce protokolů qubitových systémů úzce souvisí s vratnou branou *XOR* resp. *GXOR*, jejím rozšířením pro quditové systémy. Ta byla studována v dodatku.

Protokol Benneth-Brasard slouží k odčištění dvouqubitových Wernerovských systémů k jistému maximálně provázanému Bellovskému stavu a funguje pro všechny neseperabilní stavy systému, v dobré shodě s Peresovou nutnou podmínkou separability  $F_{in} > 1/2$ . Pro obecně dvouquditové systémy byl sestrojen Hordockého protokol, který slouží k odčištění izometrických stavů systému. Protokol čistí pro stavy se vstupní hodnotou  $F > 1/(1 + D)$ , což je v dobré shodě s druhou podmínkou separability (podle [3] platilo, že pro obecně  $N$ -quditové symetrické stavy je i postačující). Zmíněné protokoly jsou výborně funkční, ovšem obsahují náročný konstrukční prvek. Na začátku každého iteračního kroku musí být totiž systém ve tvaru Wernerovského resp. izotropického stavu, musí být provedena tzv. depolarizace.

Tento nedostatek mají odstranit deterministické protokoly, které se skládají z aplikace jistého nelineárního zobrazení a dodatečných lokálně unitárních zobrazení tzv. twirlingu. Nelineární zobrazení je určeno počtem kopií tzv. terčových systémů, pro zjednodušení byly požadovány ve stejném stavu jako vstupní systém. Dalším parametrem je volba projekce terčových systémů na jistý stav z ortonormální báze stavového prostoru terčového quditu. Exponenciální náročnost protokolu na počet terčových systémů, které nelineární zobrazení vyžaduje efektivní volbu twirlingu.

Obě zobrazení musí zachovávat stav, ke kterému se potřebuje čistit. Navíc počet atraktorů nelineárního zobrazení má být co největší, počet invariantních stavů nelineárního zobrazení a i twirlingu co možná nejmenší. Twirling by dále měl v co největší míře zachovávat tvar atraktorů nelineárního zobrazení, jakožto stavů, které pro jistý vysoký počet terčových systémů lze odčistit pouze aplikací nelineárního zobrazení. Jeho úkol je „rozházet“ nežádoucí členy, které by jen při použití nelineárního zobrazení znemožnily čistící proceduru.

Pro obecně dvouquditové systémy byla taková zobrazení nalezena. Pro dvouqubitové systémy bylo zkonstrováno zobrazení, které stejně jako Bennett-Brassard protokol odčistilo všechny neseperabilní Wernerovské stavy k čistému antisymetrickému stavu  $|\Psi^-\rangle$  Bellovské báze. K Horodeckému protokolu byl ve [13] sestrojen deterministický

protokol, který až na nízké hodnoty znečištění byl plně funkční a efektivnější co do počtu nutných opakování iteračních kroků pro dosažení dané čistoty. Konstrukcí purifikačního protokolu pro tříčasticové antisymetrické stavy jsem nahlédl na problém provázanosti vícečasticových systémů. Výběr použitého nelineárního zobrazení byl poměrně snadnou záležitostí, neboť v úvahu připadaly pouze tři zobrazení, se stejnými vlastnostmi co počtu a tvaru atraktorů.

Při hledání twirlingu jsem pro značnou numerickou náročnost musel přistoupit ke zjednodušujícím krokům. Omezil jsem se na třídu  $U \otimes U \otimes U$ , kde  $U$  je rotace kolem osy procházející počátkem. Pro takovou volbu twirlingu jsem věděl, že zachovává antisymetrické stavy. Dále jsem se omezil na rotace kolem os  $x, y, z$  jako nejjednodušší skupinu. Pro ty jsem přímou konstrukcí purifikačních protokolů našel nejvhodnější případ, rotaci o úhel  $\pi/4$ . Složením rotací kolem os  $x, y, z$  o úhel  $\pi/4$  jsem našel twirling, který do deseti iterčních kroků efektivně odčistil širokou třídu znečištěných vstupních stavů. Možná volba ze dvou parametrů, které charakterizovaly projekci, zvyšovala pravděpodobnost úspěchu protokolu.

Otázka purifikačních protokolů vícečasticových systémů je náročným numerickým problémem. Také problematika přístupu řešení problému je otevřená. V dalším studiu se zaměřím na preciznější přístup k problematice, také třeba z hlediska čistící procedury jako dynamického vývoje čištěného systému.

## Kapitola č. 6

### Matematický dodatek: *GXOR*-zobecněná *XOR*-brána

Pro dvojici qubitů byla *XOR*-brána definována jako lineární operátor na  $\mathcal{H} \equiv C^2 \otimes C^2$ :

$$XOR|i\rangle_1|j\rangle_2 = |i\rangle_1|i \oplus j\rangle_2 = |i\rangle_1|(i + j) \bmod 2\rangle_2$$

kde  $i, j \in \{1, 2\}$  označuje jednotlivé qubity.

Tento operátor je unitární: z definice viz [2] je třeba ověřit zda je *XOR* izomorfismus Hilbertova prostoru  $C^2 \otimes C^2$  na sebe. To plyne z následujícího:

pro libovolné  $x \in H$  lze  $x = \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$  kde  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  je ortonormální báze  $H$ . Platí  $\|XORx\| = \|\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle\| = \|\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|11\rangle + \alpha_4|10\rangle\| = |\alpha_1| + |\alpha_2| + |\alpha_3| + |\alpha_4| = \|x\|$ . Surjekvita *XOR* plyne z transformace ortonormální báze  $H$  pod vlivem *XOR* na sebe.

Z unitarity operátoru plyne jeho invertibilita, tedy vratnost brány.

Tento operátor je hermitovský: z definice viz [2] je třeba ověřit  $XOR = XOR^\dagger$ , kde  $XOR^\dagger$  značí hermitovky združený operátor k *XOR*. Rovnost definičních oborů a oborů hodnot obou operátorů je zřejmá z předchozí úvahy, maticová reprezentace obou operátorů na  $H$  má totožný tvar.

Dále platí:  $i \oplus j = 0$  právě když  $i = j$ .

Provedme nyní zobecnění této brány tzv. *GXOR* na dva quidity:

$$GXOR|i\rangle_1|j\rangle_2 = |i\rangle_1|i \oplus j\rangle_2 = |i\rangle_1|(i + j) \bmod D\rangle_2$$

kde  $i, j \in \{0, 1, \dots, D-1\}$  dostali bychom opět unitární operátor. Izomorfismus a surjektivita opět plyne z faktu: je-li  $i, j_1, j_2 \in \{0, 1, \dots, D-1\}$  a  $j_1 \neq j_2$ , potom  $(i+j_1) \bmod D \neq (i+j_2)$ . Ortonormální báze  $H \equiv C^D \otimes C^D$  se pomocí *GXOR* zobrazí opět na ortonormální bázi, porovnáním *GXOR* a  $GXOR^\dagger$  na  $H$  ale zjistíme, že takto definovaný operátor pro  $D > 2$  není hermitovský. Také neplatí  $i \oplus j = 0$  právě když  $i = j$ , stačí pro každé  $i$  definovat  $j = D - i$ .

Požadované zobecnění dostaneme pokud definujeme

$$GXOR|i\rangle_1|j\rangle_2 = |i\rangle_1|i \ominus j\rangle_2 = |i\rangle_1|(i - j) \bmod D\rangle_2.$$

Pro qubity je tato definice totožná s definicí *XOR*. Takto definovaný operátor je unitární, hermitovský a platí:  $i \ominus j = 0$  právě když  $i = j$ . Fyzikální realizace *GXOR* je úzce spojena s nelineárními optickými prvky. Klíčovou roli realizace *GXOR* hraje diskrétní Fourierovou transformací  $F : C^D \rightarrow C^D$  kde  $F|k\rangle \equiv 1/\sqrt{D} \sum_{n=0}^{D-1} \exp(i2\pi kn/D)|n\rangle$ , celá konstrukce byla podrobněji diskutována v [1].

Významnou aplikací *GXOR* je příprava provázaných stavů dvou quiditových systémů. Nechť  $|i\rangle|j\rangle$ ,  $i, j \in \{0, \dots, D-1\}$  je ortonormální báze  $\mathcal{H} = C^D \otimes C^D$ , potom:

$$|\psi_{lm}\rangle = GXOR_{12}[F|l\rangle_1|m\rangle_2]$$

kde  $F$  je operátor Fourierovy transformace. Pro  $D=2$  získáme tzv. Bellovské stavy viz [1]. Pro  $D > 2$  získáme tzv. zobecněné Bellovské stavy, dále jen Bellovské stavy. Snadno se nahlédne, že tyto stavy jsou ortogonální:

$$\begin{aligned}
\langle \psi_{lm} | \psi_{kn} \rangle &= \langle GXOR_{12}[F|l\rangle_1|m\rangle_2] | GXOR_{12}[F|k\rangle_1|n\rangle_2] \rangle = \\
&= \frac{1}{D} \sum_x \sum_y \exp(i2\pi(yk - xl)/D) \langle x|y \rangle \langle x \ominus m | y \ominus n \rangle = \delta_{kl} \delta_{mn}
\end{aligned}$$

kde  $\delta_{ab}$  je Kroneckerovo delta. To plyne z faktu, že k nenulovému součtu mohou přizpívat jen členy  $x = y$ ,  $m = n$ , přitom pro  $k \neq l$  je  $\frac{1}{D} \sum_x \exp(i2\pi x(k - l)/D) = 0$ , pro  $k = l$  je součet 1.

Tyto stavy tvoří ortonormální bázi, neboť jejich počet je  $D^2$ , což je dimenze  $H$ . Provázanost plyne z faktu, že znalost stavu jedné komponenty určuje pro daný Bellovský stav stavy ostatních komponent. Podmínka provázanosti je splněna, kromě matic hustot obsahujících  $|i\rangle\langle i| \otimes |j\rangle\langle j|$  se v rozkladu matice hustoty systému objeví vždy členy, které již za matice hustoty považovat nelze, tím pádem je narušena separabilita systému.

Protože  $GXOR$  je unitární, hermitovký, lze proces provázanosti snadno obrátit a provést proces rozvázání invertováním procesu, ten má význam pro teorii kódování a pro proces teleportace, blíže viz [3].

# Kapitola č. 7

## Literatura

- [1] Vymětal S.: Rešeršní práce, FJFI-ČVUT, kat. fyziky, (2001)
- [2] Horodecki M.: Entanglement Measures, Quant. Inf. and Comp., Vol. 1, No. 1, (2001)
- [3] Pittenger A. O., Rubin M. H.: Note on separability of the Werner states in arbitrary dimensions, Optics Communications 179, (2000)
- [4] Horodecki P., Horodecki R.: Distillation and bound entanglement, Quant. Inf. and Comp., (2001)
- [5] Peres A.: Phys. Rev. Lett. 77, (1996)
- [6] Pittenger A. O., Rubin M. H.: Complete separability and Fourier representations of  $n$ -qubit states, quant-ph/9912116
- [7] Horodecki M., Horodecki P.: Reduction criterion of separability and limits for a class of distillation protocols, Phys. Rev. A, Vol. 59, No. 6, (1999)
- [8] G.Lindbad, Commun. Math. Phys. 40, 147 (1975); W.F. Stinespring, Proc. Am. Math. Soc. 26, 211 (1955)
- [9] Horodecki M., Horodecki P., Horodecki R., Phys. Lett. A, 210, 377,1 (1996)
- [10] Bennett Ch. H., Brassard G., Popescu S., Schumacher B., Smolin J. A., Wootters W. K.: Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett., Vol. 76, No. 5, (1996)
- [11] Bechmann-Pasquinucci H., Huttner B., Gisin N.: Nonlinear quantum state transformation of spin 1/2, quant-ph/9708040, (1997)
- [12] Delgado A., Alber G., Jex I.: Note on the attractors, (2000)
- [13] Delgado A., Alber G., Gisin N., Jex I.: Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces, J.Phys. A: Math. Gen. 34, (2001)
- [14] Blank J., Exner P., Havlíček M.: Lineární operátory v kvantové fyzice, Karolinum (1993)
- [15] Jarník V., Matematická analýza I., SPN, 1968