

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

Diplomová práce

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

Vlastnosti a implementace
univerzálních procesů pro více částic

Vojtěch Košťák

Katedra fyziky

Akademický rok: 2004/2005

Školitel: Prof. Ing. Igor Jex, DrSc., KF, FJFI, ČVUT v Praze

V Praze 19. dubna 2005

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW atd.) uvedené v příloženém seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 19. dubna 2005

.....
podpis

Obsah

Úvod	3
1 Vývoj kvantového systému	5
1.1 Kvantové operace	5
1.2 Krausova reprezentace	7
2 Univerzální procesy	10
2.1 Definice univerzálního procesu	10
2.2 Univerzální procesy pro dvě částice	12
2.3 Příklady univerzálních procesů na dvou částicích	15
2.3.1 Univerzální kopírovací proces 1 částice na 2	15
2.3.2 Třída univerzálních provazovacích procesů	17
3 Realizace univerzálních procesů na dvou částicích	19
3.1 Procesy generované projektory S_2 a A_2	20
3.2 Zobecnění realizace univerzálních procesů projektory	24
3.3 Univerzální procesy na dvou částicích pro $M=3$	27
3.3.1 Proces kopírování	32
3.3.2 Procesy provázání	32
3.4 Unitární realizace univerzálního procesu pomocí Krausových operátorů	35
4 Realizace univerzálních procesů na třech částicích	39
Závěr	48
A Výstupní stavy univerzálního procesu na třech částicích realizovaného projektory	50
A.1 Tříčásticová matice hustoty	50
A.2 Dvoučásticové redukováná matice hustoty	51
Literatura	54

Úvod

Současně s vývojem teorie a experimentální praxe kvantové optiky vznikl i zcela nový obor: teorie kvantové informace. Možnosti superpozice a provázání kvantových stavů, které jsou přímými důsledky linearity kvantové mechaniky, dávají kvantové teorii informace nástroje, kterými její klasický protějšek nedisponuje. Některé problémy, jejichž řešení v klasické informatice vyžadují exponenciální nároky na prostředky nebo čas, lze v rámci kvantové teorie řešit pouze s polynomiální složitostí. Mezi takové úlohy patří například faktorizace velkých čísel na prvočísla. Exponenciální časové náročnosti řešení této úlohy v klasickém světě využívá i kryptografie a téměř každému z nás dnes tento fakt chrání informace či soukromí. V roce 1994 publikoval P. Shor algoritmus [1], který s využitím principů kvantové teorie řeší faktorizaci s polynomiální složitostí.

Linearita - stejný prvek, který obohacuje možnosti kvantové informace, na ní spolu s dalšími podmínkami, jako je úplná pozitivita, uvaluje i přísná omezení, která znemožňují realizaci některých, klasické informatice naprosto vlastních, procesů. Příkladem operace, která je kvantové infomaci „zapovězená“, je vytvoření přesné kopie neznámého kvantového stavu [2]. Musíme se proto spokojit s procesy produkující nedokonalé kopie popsané např. Wernerem [3]. Jeho klonovací proces patří do třídy tzv. univerzálních procesů, které jsou stěžejním pojmem této diplomové práce.

Univerzální kvantové procesy lze charakterizovat tzv. podmínkou kovariance, která znamená, že daný proces působí na všechny vstupní stavy v jistém smyslu „stejně“. Tato třída zobrazení je zajímavá a důležitá právě proto, že se v ní dá nalézt mnoho procesů, které optimálně aproximují operace, kvantové fyzice jinak zapovězené, a z informatického hlediska tedy leží na samé hranici kvantové fyziky.

Cílem této diplomové práce je navrhnout způsob implementace širší třídy univerzálních procesů na více částicích. Pod implementací procesu budeme rozumět nalezení unitárního operátoru na nějakém Hilbertově prostoru, který danou operaci realizuje.

Pomocí teorie reprezentací unitární grupy odvodíme ansatz pro imple-

mentaci určité podtřídy univerzálních procesů na libovolném počtu částic, které jsou realizovány projekty, a zaměříme se na realizaci dvou a tříčásticových procesů, pro které je známa širší klasifikace [4], [5].

Text diplomové práce je organizován následovně: V první kapitole je uveden formalismus kvantových operací a s ním související Krausova reprezentace. Druhá kapitola je věnována klasifikaci univerzálních procesů na dvou částicích tak, jak byla provedena v práci [4]. Ve třetí kapitole odvodíme postup realizace velmi obecné podtřídy univerzálních procesů, kterou lze konstruovat pomocí projektorů na invariantní podprostory vícečásticových reprezentací jednočásticové unitární grupy. Blíže se zaměříme na dvoučásticové procesy a v této podtřídě identifikujeme několik důležitých příkladů. Poslední kapitola je věnována realizaci univerzálních procesů na třech částicích. Speciální pozornost je věnována procesům, které jsou realizované projekty na symetrické a antisymetrické stavy.

Kapitola 1

Vývoj kvantového systému

Tato kapitola je věnována matematickému formalismu, který popisuje obecnější dynamiku kvantových systémů, než jakou je unitární vývoj. Klíčovým pojmem je kvantová operace, kterou lze popsat nejen vývoj uzavřených kvantových systémů, ale i evoluci otevřených systémů, které jsou silně vázány se svým okolím, a dokonce i extrémní případ interakce, jakým je proces měření. Formalismus kvantových operací se opírá zejména o Krausovu reprezentaci, která je popsána v sekci 1.2.

1.1 Kvantové operace

Časový vývoj operátoru hustoty $\rho(t)$ uzavřeného kvantového systému je popsán Liouvillovou rovnicí

$$i\hbar \frac{\partial \rho(t)}{\partial t} = H\rho(t) - \rho(t)H = [H, \rho(t)], \quad (1.1)$$

kde H je Hamiltonián systému, $2\pi\hbar$ je Planckova konstanta. Vývoj na časovém intervalu J , kdy se systém izolovaně od okolí vyvíjel, je ekvivalentní působení unitárního propagátoru $U(t, s)$ na matici hustoty $\rho(t)$. Tedy

$$\rho(t) = U(t, s)\rho(s)U^\dagger(t, s) \quad \forall s, t \in J. \quad (1.2)$$

Unitární vývoj kvantových systémů je pro kvantovou informatiku v mnoha aplikacích nedostačující. Za prvé, v praxi si lze jen těžko představit systém, který je od svého okolí úplně izolován a chceme-li například přenášet informaci kvantovým kanálem, musíme počítat i s kvantovým šumem. Náš nosič informace, ať už je to foton, elektron nebo iont, vždy interaguje s okolím a jeho vývoj, chápeme-li ho jako vývoj podsystému nějakého většího celku kanál-nosič, již nemusí být sám o sobě unitární. Za druhé, pokud bychom se

omezili v kvantových algoritmech pouze na unitární transformace, třída úloh, která by byla tímto způsobem realizovatelná, by se velmi zúžila. Lze využít nevýhody prvního případu v náš prospěch. Systém můžeme rozšířit o další částice nebo stupně volnosti, tzv. ancilly, a na rozšířeném systému realizovat vhodnou unitární transformaci. Pokud ve výsledném stavu vypustíme ancillu, tj. provedeme operaci částečné stopy přes podsystém příslušející ancille, transformace realizovaná na původním systému nemusí být unitární. Za třetí, v realizaci kvantových algoritmů se velmi často vyskytuje proces měření, který zcela jistě není unitární, a do konzistentního popisu nejobecnější dynamiky kvantového systému je potřeba i tento proces zahrnout.

Hledáme nejobecnější tvar zobrazení \mathcal{E} , které vstupní matici hustoty ρ_{in} na nějakém Hilbertově prostoru \mathcal{H}_{in} zobrazí na výstupní $\rho_{out} = \mathcal{E}(\rho_{in})$ na Hilbertově prostoru \mathcal{H}_{out} , přičemž netrváme na podmínce $\mathcal{H}_{in} = \mathcal{H}_{out}$. Fakt, že \mathcal{E} má zobrazit matici hustoty na matici hustoty, klade na \mathcal{E} určité podmínky [6]:

$$\mathcal{E} \text{ zachovává pozitivitu: } \rho_{in} \geq 0 \Rightarrow \mathcal{E}(\rho_{in}) \geq 0, \quad (1.3)$$

$$\mathcal{E} \text{ zachovává stopu: } \quad \text{Tr}\mathcal{E}(\rho_{in}) = 1. \quad (1.4)$$

Pokud připustíme i nedeterministickou dynamiku systému, lze podmínku zeslabit na

$$\mathcal{E} \text{ nezvyšuje stopu: } \quad \text{Tr}\mathcal{E}(\rho_{in}) \leq 1. \quad (1.5)$$

Tento typ procesů je realizován deterministickým vývojem, po němž následuje proces měření. Podle výsledku měření rozhodneme, zda proces \mathcal{E} nastal či ne. Pravděpodobnost realizace \mathcal{E} je $\text{Tr}\mathcal{E}(\rho_{in})$ a výsledným stavem je

$$\rho_{out} = \frac{\mathcal{E}(\rho_{in})}{\text{Tr}\mathcal{E}(\rho_{in})}. \quad (1.6)$$

Pokud má být definice kvantové operace konzistentní se statistickou interpretací matice hustoty, musí být další podmínkou kladenou na kvantovou operaci linearita vůči vstupnímu stavu.

$$\mathcal{E} \text{ lineární vůči vstupu } \rho_{in}: \quad \mathcal{E} \left(\sum_i p_i \rho_i \right) = \sum_i p_i \mathcal{E}(\rho_i). \quad (1.7)$$

Poslední podmínkou, kterou na kvantovou operaci na systému A klademe, je tzv. úplná pozitivita, tedy

$$\mathcal{E} \text{ úplně pozitivní: } \rho_{AB} \geq 0 \Rightarrow (I \otimes \mathcal{E})\rho_{AB} \geq 0, \quad (1.8)$$

kde ρ_{AB} je matice hustoty na libovolném rozšířeném systému AB a I je identické zobrazení na podsystému B . Tato podmínka plyne z přirozeného požadavku, že pokud je námi zkoumaný systém A součástí nějakého většího AB , nesmí kvantová operace \mathcal{E} na podsystému převést fyzikální stav celého systému AB na stav nefyzikální. Názorným příkladem je transformace T , která převede matici hustoty jednoho qubitu na transponovanou, která je též platnou maticí hustoty, a takové zobrazení je tedy pozitivní. Předpokádejme ale, že je tento qubit součástí dvou-qubitového systému v provázaném stavu

$$\frac{1}{\sqrt{2}}|11\rangle + |00\rangle. \quad (1.9)$$

První qubit nechť podléhá transpozici a druhý triviálnímu vývoji; transformace je tvaru $T' = T \otimes I$. Matice hustoty odpovídající stavu (1.9) je

$$\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \quad (1.10)$$

a po transformaci T' přejde na tvar

$$\frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \quad (1.11)$$

Matice (1.11) má ale vlastní čísla $\frac{1}{2}$, $\frac{1}{2}$, $\frac{1}{2}$ a $-\frac{1}{2}$ a není tedy maticí hustoty. Transpozice T je příklad zobrazení, které je pozitivní, ale není úplně pozitivní, a proto nemůže hrát roli fyzikálně realizovatelné dynamiky systému. Jedna z možných definic kvantové operace je následující.

Definice. Zobrazení \mathcal{E} transformující matici hustoty ρ_{in} na matici hustoty ρ_{out} je kvantová operace právě tehdy, když splňuje axiomy (1.5), (1.7) a (1.8).

Tato definice je sice užitečná v tom smyslu, že vychází z minimálního počtu fyzikálně motivovaných axiomů, ale pro praktické počítání není příliš vhodná, neboť například podmínka úplné positivity se přímo dokazuje velmi obtížně. V následující sekci ukážeme ekvivalentní definici, se kterou se pracuje lépe.

1.2 Krausova reprezentace

Jak bylo řečeno v úvodu této kapitoly, jednou z motivací k zavedení pojmu kvantové operace je potřeba popsat časový vývoj otevřených kvantových

systémů. Další motivací může být snaha najít jednotný formalismus, který umožní popsat působení okolního prostředí na systém. Přirozenou cestou, jak zahrnout do modelu interakci kvantového systému S s okolím E, je rozšířit Hilbertův prostor \mathcal{H}_S příslušející S o stavy popisující okolní prostředí \mathcal{H}_E a nahlížet na $\mathcal{H}_S \otimes \mathcal{H}_E$ jako na stavový prostor jednoho uzavřeného systému, který podléhá již unitární interakci U . Předpokládejme, že celý systém S-E je na vstupu ve faktorizovaném stavu, tedy $\rho_{in} = \rho_S \otimes \rho_E$. Po interakci je stav podsystému S dán rovnicí

$$\mathcal{E}(\rho_S) = \text{Tr}_E [U(\rho_S \otimes \rho_E)U^\dagger]. \quad (1.12)$$

Úpravou rovnice (1.12) lze dojít k jiné, elegantní formě vyjádření operace \mathcal{E} známé jako Krausova reprezentace [6], [7].

Nechť $|e_k\rangle$ je ortonormální báze konečněrozměrného Hilbertova prostoru podsystému E a $\rho_E = |e_0\rangle\langle e_0|$ je jeho počáteční stav. Předpoklad, že se na začátku prostředí nachází v čistém stavu, tzn. ρ_E je projektor na jednorozměrný podprostor, nijak neubírá postupu na obecnosti, neboť vždy lze \mathcal{H}_E rozšířit tak, aby počáteční smíšený stav E byl v rozšířeném systému čistý. Tomuto postupu se říká purifikace stavu. Nechť

$$\rho_E = \sum_k \alpha_{kk} |k\rangle\langle k| \quad (1.13)$$

je libovolná matice hustoty na \mathcal{H}_E a $|k\rangle$ je ortonormální báze, ve které je ρ_E diagonální. Systém E můžeme rozšířit o druhý E' stejné dimenze jako E a s bází $|f_k\rangle$. Definujme stav

$$|\psi\rangle = \sum_k \sqrt{\alpha_{kk}} |k\rangle |f_k\rangle. \quad (1.14)$$

Tento stav je čistý a navíc platí $\rho_E = \text{Tr}_{E'} |\psi\rangle\langle\psi|$. Dokud se tedy zajímáme pouze o měření na systému S, není předpoklad čistoty stavu systému E omezující. Rovnici (1.12) lze dále upravit na tvar

$$\mathcal{E}(\rho_S) = \sum_k \langle e_k | U (\rho_S \otimes |e_0\rangle\langle e_0|) U^\dagger | e_k \rangle = \sum_k E_k \rho_S E_k^\dagger, \quad (1.15)$$

kde $E_k = \langle e_k | U | e_0 \rangle$ je již operátor na Hilbertově prostoru systému S. Množina $\{E_k\}_k$ se nazývá Krausova reprezentace zobrazení \mathcal{E} a operátory E_k se nazývají operační či Krausovy elementy nebo též Krausovy operátory operace \mathcal{E} .

Tento postup lze snadno zobecnit pro různé dimenze vstupního a výstupního Hilbertova prostoru. Stačí uvažovat systém S_1 v neznámém počátečním

stavu ρ_1 , který necháme unitárně interagovat se systémem S_2 připraveném v nějakém specifickém stavu $\rho_2 = |e_0^2\rangle\langle e_0^2|$. Po interakci provedeme stopu přes S_1 a na S_2 tím získáme výstupní stav.

Z rovnice (1.15) a z požadavku $\text{Tr}\mathcal{E}(\rho) \leq 1$ (nerovnost připouštíme pro nedeterministické procesy, tedy takové, které realizují danou dynamiku pouze s určitou pravděpodobností) plyne pro Krausovy operátory tzv. relace úplnosti. Pro každé ρ platí

$$1 \geq \text{Tr}\mathcal{E}(\rho) = \text{Tr}\sum_k E_k \rho E_k^\dagger = \sum_k \text{Tr}\{E_k^\dagger E_k \rho\}, \quad (1.16)$$

z čehož plyne

$$\sum_k E_k^\dagger E_k \leq I. \quad (1.17)$$

Z předchozích úvah plyne druhá definice kvantové operace.

Definice. *Nechť \mathcal{E} je zobrazení z matic hustoty na \mathcal{H}_{in} na matice hustoty na \mathcal{H}_{out} . Potom \mathcal{E} je kvantová operace právě tehdy, když existuje množina lineárních zobrazení $\{E_k\}_{k=1}^K$ z \mathcal{H}_{in} do \mathcal{H}_{out} takových, že platí následující dvě podmínky*

$$\mathcal{E}(\rho_{in}) = \sum_k E_k \rho_{in} E_k^\dagger, \quad (1.18)$$

$$\sum_k E_k^\dagger E_k \leq I. \quad (1.19)$$

Zobrazení \mathcal{E} je tedy kvantová operace právě tehdy, když existuje jeho Krausova reprezentace.

Ekvivalence první a druhé definice kvantové operace je předmětem tzv. Krausova teorému [6], [7], který říká, že zobrazení \mathcal{E} z matic hustoty na \mathcal{H}_{in} na matice hustoty na \mathcal{H}_{out} splňuje axiomy (1.5), (1.7) a (1.8) právě tehdy, když pro \mathcal{E} existuje rozklad (1.18) splňující (1.19). V dalších kapitolách bude krausova reprezentace kvantových procesů často používána.

Kapitola 2

Univerzální procesy

V této kapitole definujeme pojem univerzálního procesu, který je stěžejním pojmem celé práce. Jednoduchým příkladem motivujeme vyslovení podmínky kovariance a podle práce [4] stručně zmíníme parametrizaci třídy univerzálních procesů na dvou částicích. V závěru kapitoly uvedeme dva důležité příklady univerzálních procesů: univerzální optimální kopírovací proces a třídu univerzálních provazovacích procesů.

2.1 Definice univerzálního procesu

Děje kvantové fyziky podléhají, vzhledem k její lineární povaze, určitým omezením, a proto ne každý formální matematický proces je fyzikálně realizovatelný. Příkladem takového omezení může být proces klonování kvantového stavu [2], univerzální provazovací proces [4] nebo přesný kvantový analog operace NOT [8],[9]. Předpokládejme lineární transformaci T_{clon} na Hilbertově prostoru dvou rozlišitelných částic stejné dimenze, pro jednoduchost řekněme dvou qubitů, která kopíruje zcela přesně dva ortogonální stavy první částice, platí tedy

$$\begin{aligned} T_{clon}|0\rangle|0\rangle &= |0\rangle|0\rangle, \\ T_{clon}|1\rangle|0\rangle &= |1\rangle|1\rangle. \end{aligned} \tag{2.1}$$

Potom vzhledem k linearitě transformace T_{clon} se stav $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ transformuje na $\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$, což neodpovídá přesné kopii vstupního stavu, tedy vektoru $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$. Při popisu maticemi hustoty je rozdíl mezi ideální kopii a výsledným jednočásticovým stavem po transformaci T_{clon} ještě názornější,

$$\rho_{in} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad \text{Tr}_2 \left(T_{clon} \rho_{in} T_{clon}^\dagger \right) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.2}$$

Matice hustoty odpovídající vstupnímu stavu $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ se tedy zobrazí na zcela depolarizovaný stav.

Vyvstává otázka, zda existuje, a případně jak vypadá, lineární transformace, která sice nekopíruje žádný kvantový stav přesně, ale určitá míra vzdálenosti výsledného stavu od ideální kopie je pro všechny vstupy stejná a navíc minimální na množině fyzikálně přípustných transformací. Univerzální kvantový proces můžeme vágně definovat jako kvantově mechanicky realizovatelnou transformaci, která se, vzhledem k nějakému kvantitativnímu kritériu, chová ke všem stavům "stejně". Před formálním zavedením pojmu univerzálního kvantového procesu uveďme příklad, kterým bude definice motivována.

Předpokládejme systém dvou rozlišitelných částic se spinem $\frac{1}{2}$ v následujícím stavu

$$\rho_1(\mathbf{m}) = \rho_{in} \otimes \frac{1}{2}I, \quad (2.3)$$

kde čistý stav $\rho_{in} = |\mathbf{m}\rangle\langle\mathbf{m}|$ je popsán Blochovým vektorem \mathbf{m} . Nyní uvažujme následující proces

$$\rho_2(\mathbf{m}) = \frac{\mathbf{P}_J \rho_1(\mathbf{m}) \mathbf{P}_J}{\text{Tr}(\mathbf{P}_J \rho_1(\mathbf{m}) \mathbf{P}_J)}, \quad (2.4)$$

kde $\mathbf{P}_J = \sum_M |J, M\rangle\langle J, M|$ je projektor na stav s celkovým orbitálním momentem J , který může nabývat hodnot 1 nebo 0. V závislosti na hodnotě J realizujeme dva procesy

$$\begin{aligned} \rho_2(\mathbf{m}) &= \frac{2}{3} |J=1, M=1\rangle\langle J=1, M=1| \\ &+ \frac{1}{3} |J=1, M=0\rangle\langle J=1, M=0|, \end{aligned} \quad (2.5)$$

nebo

$$\rho_2(\mathbf{m}) = |J=0, M=0\rangle\langle J=0, M=0|. \quad (2.6)$$

Oba tyto kvantové procesy jsou univerzální v tom smyslu, že pravděpodobnosti vystupující před výrazy v rovnicích (2.5) a (2.6) nejsou závislé na vstupním stavu $|\mathbf{m}\rangle$. Navíc pro každou unitární transformaci U na jednočásticovém Hilbertově prostoru, která transformuje libovolný čistý stav $|\mathbf{m}_0\rangle$ na jiný, řekněme $|\mathbf{m}\rangle = U(\mathbf{m})|\mathbf{m}_0\rangle$, platí

$$\rho_2(\mathbf{m}) = U(\mathbf{m}) \otimes U(\mathbf{m}) \rho_2(\mathbf{m}_0) U^\dagger(\mathbf{m}) \otimes U^\dagger(\mathbf{m}). \quad (2.7)$$

Tato vlastnost tzv. kovariance hraje klíčovou roli v následující definici univerzálního kvantového procesu.

Definice. *Lineární zobrazení*

$$\mathcal{P} : \rho_{in} \rightarrow \rho_{out}, \quad (2.8)$$

kde ρ_{in} je matice hustoty na \mathcal{H} a ρ_{out} je M -částicová matice hustoty na $\mathcal{H}^{\otimes M}$, nazveme univerzální proces na M částicích, právě když pro každý $|\mathbf{m}_0\rangle \in \mathcal{H}$ a každou jednočásticovou unitární transformaci U platí

$$\rho_{out}(|\mathbf{m}\rangle\langle\mathbf{m}|) = U^{\otimes M} \rho_{out}(|\mathbf{m}_0\rangle\langle\mathbf{m}_0|) U^{\otimes M\dagger}, \quad (2.9)$$

kde $U|\mathbf{m}_0\rangle = |\mathbf{m}\rangle$.

Z podmínky kovariance plyne, že univerzální kvantové procesy nemají vůči vstupnímu stavu v Hilbertově prostoru žádný preferovaný směr. Proto je jejich studium zajímavé nejen z hlediska kvantové informace, ale i v rámci studia symetrií Hilbertova prostoru.

2.2 Univerzální procesy pro dvě částice

Předpokládejme nejobecnější případ zobrazení \mathcal{P} mezi maticemi hustoty na dvou částicích dimenze N ve tvaru

$$\mathcal{P} : \rho_{in}(\mathbf{p}) \otimes \rho_{ref} \longrightarrow \rho_{out}(\mathbf{p}), \quad (2.10)$$

kde $\rho_{in}(\mathbf{p})$ je projektor na čistý stav charakterizovaný zobecněným Blochovým vektorem \mathbf{p} , tedy $\rho_{in}(\mathbf{p}) = |\mathbf{p}\rangle\langle\mathbf{p}|$ a operátor ρ_{ref} je pevně zvolená jednočásticová referenční matice hustoty. Stav ρ_{ref} se zpravidla volí tak, aby byl invariantní vůči působení lokálních unitárních transformací. V případě jednočásticového referenčního stavu je jediným takovým operátorem hustoty úplně depolarizovaný stav.

Každou matici hustoty systému dimenze N lze zapsat ve tvaru

$$\rho_{in} = \frac{1}{N} \left(I + \sum_{i,j=1}^N p_{ij} \mathbf{A}_{ij} \right), \quad (2.11)$$

kde matice \mathbf{A}_{ij} jsou definovány předpisem

$$(\mathbf{A}_{ij})^{kl} = \delta_{ik}\delta_{jl} - \frac{1}{N}\delta_{ij}\delta_{kl}. \quad (2.12)$$

Volba \mathbf{A}_{ij} právě vztahem (2.12) je motivována skutečností, že akce matic tvaru $U \otimes U$ na \mathbf{A}_{ij} je velmi jednoduchá, což v dalším výrazně zjednoduší postup.

Z podmínky samosdruženosti matice hustoty a z (2.12) plyne omezení $\bar{p}_{ij} = p_{ji}$ (aby rovnice (2.11) definovala matici hustoty, musí koeficienty p_{ij} zřejmě splňovat další podmínky). Dále je patrné, že matice \mathbf{A}_{ij} nejsou lineárně nezávislé, neboť $\sum_{i=1}^N \mathbf{A}_{ii} = 0$, a proto lze volit například $p_{NN} = 0$.

Výsledný stav kvantového procesu \mathcal{P} je realizován na tenzorovém součinu jednočásticových Hilbertových prostorů, a $\rho_{out}(\mathbf{p})$ lze proto také zapsat pomocí matic \mathbf{A}_{ij} ¹

$$\begin{aligned} \rho_{out}(\mathbf{p}) &= \frac{1}{N^2} I \otimes I + \alpha_{ij}^{(1)}(\mathbf{p}) \mathbf{A}_{ij} \otimes \mathbf{I} + \alpha_{ij}^{(2)}(\mathbf{p}) \mathbf{I} \otimes \mathbf{A}_{ij} \\ &\quad + K_{ijkl}(\mathbf{p}) \mathbf{A}_{ij} \otimes \mathbf{A}_{kl}. \end{aligned} \quad (2.13)$$

Má-li zobrazení \mathcal{P} definovat univerzální proces, musí splňovat podmínku kovariance (2.7). Porovnáním koeficientů $U(\mathbf{p}) \otimes U(\mathbf{p}) \rho_{out}(\mathbf{p}_0) U^\dagger(\mathbf{p}) \otimes U^\dagger(\mathbf{p})$ a $\rho_{out}(\mathbf{p})$ vyjádřených pomocí vztahu (2.13) získáme sadu rovnic:

$$\alpha_{ij}^{(1,2)}(\mathbf{p}) \mathbf{A}_{ij} \otimes \mathbf{I} = \alpha_{ij}^{(1,2)}(\mathbf{p}_0) U(\mathbf{p}) \mathbf{A}_{ij} U^\dagger(\mathbf{p}) \otimes \mathbf{I}, \quad (2.14)$$

$$\begin{aligned} K_{ijkl}(\mathbf{p}) \mathbf{A}_{ij} \otimes \mathbf{A}_{kl} &= K_{ijkl}(\mathbf{p}_0) (U(\mathbf{p}) \otimes U(\mathbf{p})) \times \\ &\quad \times (\mathbf{A}_{ij} \otimes \mathbf{A}_{kl}) (U^\dagger(\mathbf{p}) \otimes U^\dagger(\mathbf{p})). \end{aligned} \quad (2.15)$$

Dále požadujeme, aby vztah (2.13) splňoval podmínku linearitu vůči \mathbf{p} . Ta platí tehdy, jsou-li koeficienty $\alpha_{ij}^{(1,2)}(\mathbf{p})$ a $K_{ijkl}(\mathbf{p})$ lineárními funkcemi v p_{ij} .

Rovnice (2.14) a (2.15), spolu s podmínkou linearitu $\alpha_{ij}^{(1,2)}(\mathbf{p})$ a $K_{ijkl}(\mathbf{p})$ vůči \mathbf{p} , jsou splněny právě tehdy, když koeficienty mají následující tvar

$$\alpha_{ij}^{(1,2)}(\mathbf{p}) = \alpha^{(1,2)} p_{ij}, \quad (2.16)$$

$$K_{ijkl}(\mathbf{p}) = C \delta_{il} \delta_{jk} + \beta p_{il} \delta_{jk} + \bar{\beta} p_{jk} \delta_{il}, \quad (2.17)$$

kde $\alpha^{(1,2)}$, $C \in \mathbb{R}$ a $\beta \in \mathbb{C}$ a výslednou matici hustoty tedy lze vyjádřit ve tvaru

$$\begin{aligned} \rho_{out}(\mathbf{p}) &= \frac{1}{N^2} I \otimes I + \alpha^{(1)} p_{ij} \mathbf{A}_{ij} \otimes \mathbf{I} + \alpha^{(2)} p_{ij} \mathbf{I} \otimes \mathbf{A}_{ij} + C \mathbf{A}_{ij} \otimes \mathbf{A}_{ji} \\ &\quad + \beta p_{il} \mathbf{A}_{ij} \otimes \mathbf{A}_{jl} + \bar{\beta} p_{il} \mathbf{A}_{ji} \otimes \mathbf{A}_{lj}. \end{aligned} \quad (2.18)$$

Díky vztahu (2.13) a vlastnosti $\text{Tr} \mathbf{A}_{ij} = 0$ pro všechna i, j je zajištěna platnost $\rho_{out} = 1$. Volné parametry stále nemohou být libovolné. Aby byl operátor definovaný v (2.18) maticí hustoty, musí být pozitivní. Tuto podmínku lze splnit, pokud nalezneme vlastní čísla této matice a určíme podmínky na $\alpha^{(1,2)}$, C a β tak, aby byla vždy nezáporná a menší než jedna. Z podmínky kovariance (2.7) plyne, že pokud je λ vlastní číslo $\rho(\mathbf{p}_0)$, pak je i vlastním číslem

¹Ke zjednodušení zápisu užíváme v dalším Einsteinovo sumační pravidlo

matice $U(\mathbf{p}) \otimes U(\mathbf{p})\rho_2(\mathbf{p}_0)U^\dagger(\mathbf{p}) \otimes U^\dagger(\mathbf{p})$, a proto se při hledání vlastních čísel můžeme omezit pouze na konkrétní vstupní stav $\rho_{in} = |1\rangle\langle 1|$, který je z výpočetního hlediska jednodušší a odpovídá volbě $p_{ij} = N\delta_{1i}\delta_{1j}$. Matici (2.18) v tomto případě lze zapsat ve tvaru

$$\rho_{out}(p_{ij} = N\delta_{1i}\delta_{1j}) = \sum_{i=1}^4 \oplus p_i \rho_i, \quad (2.19)$$

kde operátory hustoty ρ_i jsou

$$\begin{aligned} \rho_1 &= |11\rangle\langle 11|, \\ \rho_2 &= \sum_{j=2}^N \left[|1j\rangle\langle 1j| \left(\frac{1}{2(N-1)} + N \frac{\alpha^{(1)} - \alpha^{(2)}}{2p_2} \right) + \right. \\ &\quad + |j1\rangle\langle j1| \left(\frac{1}{2(N-1)} + N \frac{\alpha^{(2)} - \alpha^{(1)}}{2p_2} \right) + \\ &\quad \left. + |1j\rangle\langle j1| \frac{C + N\beta}{p_2} + |j1\rangle\langle 1j| \frac{C + N\bar{\beta}}{p_2} \right], \\ \rho_3 &= \frac{1}{N-1} \sum_{j=2}^N |jj\rangle\langle jj|, \\ \rho_4 &= \sum_{2=i<j}^N \left[|ij\rangle\langle ij| \frac{1}{(N-1)(N-2)} + \right. \\ &\quad + |ji\rangle\langle ji| \frac{1}{(N-1)(N-2)} + \\ &\quad \left. + (|ij\rangle\langle ji| + |ji\rangle\langle ij|) \frac{C}{p_4} \right] \end{aligned} \quad (2.20)$$

a pravděpodobnosti p_i jsou

$$\begin{aligned} p_1 &= \frac{1}{N^2} + (N-1)(\alpha^{(1)} + \alpha^{(2)}) + C(1 - \frac{1}{N}) + (\beta + \bar{\beta}) \frac{(N-1)^2}{N}, \\ p_2 &= (N-1) \left(\frac{2}{N^2} + (N-2)(\alpha^{(1)} + \alpha^{(2)}) - \frac{2C}{N} - 2 \frac{N-1}{N} (\beta + \bar{\beta}) \right), \\ p_3 &= (N-1) \left(\frac{1}{N^2} - (\alpha^{(1)} + \alpha^{(2)}) + C(1 - \frac{1}{N}) + \frac{(\beta + \bar{\beta})}{N} \right), \\ p_4 &= (N-1)(N-2) \left(\frac{1}{N^2} - (\alpha^{(1)} + \alpha^{(2)}) + \frac{C}{N} + \frac{(\beta + \bar{\beta})}{N} \right). \end{aligned} \quad (2.21)$$

Z podmínky $\text{Tr}\rho_{out} = 1$ a výrazu (2.19) plyne, že p_i splňují

$$p_1 + p_2 + p_3 + p_4 = 1. \quad (2.22)$$

Ze vztahů (2.20) a (2.21) spočítáme vlastní čísla matice hustoty (2.19):

$$\begin{aligned} \lambda_1 &= p_1, \\ \lambda_{2\pm} &= \frac{p_2}{2(N-1)} \pm \sqrt{\frac{N^2}{4} (\alpha^{(1)} - \alpha^{(2)})^2 + |C + \beta N|^2}, \\ \lambda_3 &= \frac{p_3}{N-1}, \\ \lambda_{4\pm} &= \frac{p_4}{(N-1)(N-2)} \pm |C|. \end{aligned} \quad (2.23)$$

Matice ρ_{out} je operátorem hustoty, pokud má všechna vlastní čísla nezáporná a menší než jedna.

V případě $N \geq 3$ lze tři nezávislé reálné parametry $(\alpha^{(1)} + \alpha^{(2)})$, $(\beta + \bar{\beta})$ a C vyjádřit z rovnic (2.21) a (2.22) pomocí, řekněme, p_1 , p_3 , p_4 . Tyto vztahy mají tvar

$$\begin{aligned} \beta + \bar{\beta} &= -\frac{1}{N(N-1)} + \frac{p_4}{(N-1)(N-2)} + \frac{p_1}{(N-1)}, \\ \alpha^{(1)} + \alpha^{(2)} &= \frac{N-2}{N^2(N-1)} - \frac{p_4 - p_1 + p_3}{N(N-1)}, \\ C &= \frac{p_3}{N-1} - \frac{p_4}{(N-1)(N-2)}. \end{aligned} \quad (2.24)$$

K jednoznačné specifikaci dvoučásticového univerzálního procesu je třeba specifikovat navíc parametry $\alpha^{(1)} - \alpha^{(2)}$ a $\beta - \bar{\beta}$.

2.3 Příklady univerzálních procesů na dvou částicích

2.3.1 Univerzální kopírovací proces 1 částice na 2

Jak již bylo v sekci 2.1 naznačeno, nelze vzhledem k linearitě kvantové fyziky realizovat ideální kopírovací proces na celém Hilbertově prostoru. Můžeme se ale zajímat, jak lze proces kopírování nejlépe aproximovat. Podmínky kladené na takové zobrazení z prostoru jednočásticových matic hustoty na dvoučásticové může být následující. Požadujeme, aby jednočásticové stavy výsledné dvoučásticové matice hustoty byly shodné a aby kvalita výstupu,

tedy jistá míra vzdálenosti od ideální kopie, byla pro všechny vstupní čisté stavy stejná².

R. F. Werner definoval klonovací proces kopírující stav L identických rozlišitelných částic dimenze N na M [3]:

$$T(\rho^{\otimes L}) = \frac{d[L]}{d[M]} S_M(\rho^{\otimes L} \otimes I^{\otimes M-L}) S_M, \quad (2.25)$$

kde S_M je projektor na symetrický podprostor $\mathcal{H}^{\otimes M}$ o dimenzi $d[M]$

$$d[M] = \binom{N + M - 1}{M}. \quad (2.26)$$

O tomto zobrazení ukázal, že je optimální a jediné, které nabývá maximální fidelity³

$$\mathcal{F} = \frac{d[L]}{d[M]}. \quad (2.27)$$

Pro $L = 1$, $M = 2$ tento proces splňuje podmínku kovariance⁴ (2.7) a ve formalizmu ukázaném v přechozích odstavcích lze charakterizovat parametry

$$\begin{aligned} \alpha^{(1)} &= \alpha^{(2)} = \frac{N + 2}{2N^2(N + 1)}, \\ \beta &= \bar{\beta} = \frac{1}{2N(N + 1)}, \\ C &= 0 \end{aligned} \quad (2.28)$$

a pravděpodobnosti odpovídající jednotlivým ρ_i jsou

$$\begin{aligned} p_1 &= \frac{2}{N + 1}, \\ p_2 &= \frac{N - 1}{N + 1}, \\ p_3 &= p_4 = 0. \end{aligned} \quad (2.29)$$

Projektor S_2 splňuje podmínky (1.18) a (1.18), a je tedy Krausovým operátorem operace (2.25).

²Tyto podmínky lze různým způsobem zeslabovat, například není nutné požadovat symetrii jednočásticových stavů [10], [11].

³Werner zvolil stav, vůči kterému měřil fidelitu, jako $\sigma^{\otimes M}$, kde σ je jednočásticový vstupní stav.

⁴V následující kapitole uvidíme, že zobrazení (2.25) splňuje kovariantní podmínku pro každé L a M .

2.3.2 Třída univerzálních provazovacích procesů

V této sekci popíšeme třídu univerzálních procesů, které provazují dvě částice [4]. Za kritérium provázanosti je zvolena podmínka, že výsledný stav procesu neobsahuje žádnou separabilní komponentu. Lze dokázat, [12], že každý stav dvoučásticového systému ρ lze rozdělit na část separabilní, ρ_{sep} , a neseperabilní, ρ_{insep} , tak, že platí

$$\rho = \lambda\rho_{sep} + (1 - \lambda)\rho_{insep}, \quad (2.30)$$

kde $0 \leq \lambda \leq 1$. Ačkoli sama dekompozice není jednoznačná, maximální možná hodnota λ už jednoznačná je. Budeme tedy hledat parametry univerzálních procesů, jejichž výstupní stavy mají maximální λ rovno nule.

Začneme opět od rovnice (2.19). Je patrné, že pokud nemá výsledný stav obsahovat žádnou separabilní komponentu, nesmí obsahovat členy typu $|ii\rangle\langle ii|$. Nutnou podmínkou na takový proces tedy je

$$p_1 = 0, \quad p_3 = 0. \quad (2.31)$$

V práci [4] je ukázáno, že jde dokonce o podmínku postačující k tomu, aby výsledný stav už žádnou separabilní komponentu neobsahoval. Při těchto parametrech plyne ze vztahů (2.23) $\lambda_{4-} = 0$. Z podmínky nezápornosti vlastních čísel matice hustoty a vztahu pro λ_{2-} dostaneme

$$\begin{aligned} \alpha^{(1)} &= \alpha^{(2)}, \\ \beta &= \bar{\beta}, \\ \rho_2^{(ent)} &= \frac{1}{2(N-1)} \sum_{j=2}^N (|1j\rangle\langle 1j| + |j1\rangle\langle j1| - \\ &\quad |1j\rangle\langle j1| - |j1\rangle\langle 1j|), \\ \rho_4^{(ent)} &= \frac{1}{(N-1)(N-2)} \sum_{2=i<j}^N (|ij\rangle\langle ij| + |ji\rangle\langle ji| - \\ &\quad |ij\rangle\langle ji| - |ji\rangle\langle ij|). \end{aligned} \quad (2.32)$$

Společně s parametry (2.31) a vztahem (2.19) získáváme

$$\rho_{out}^{(ent)}(\mathbf{m}_0 = N\mathbf{A}_{11}) = (1 - p_4)\rho_2^{(ent)} \oplus p_4\rho_4^{(ent)}. \quad (2.33)$$

Univerzální procesy, jejichž výsledné stavy neobsahují žádnou separabilní komponentu, tedy tvoří jednoparametrickou třídu.

Další otázkou zůstává, které z těchto procesů maximalizují určitou míru provázání, v práci [4] zvolili tzv. Vidalovu a Wernerovu míru [13]. Dle této

práce je negativita $N(\rho)$ libovolné dvoučásticové matice hustoty mírou provázání, kde

$$N(\rho) = \sum_i |\mu_i| \quad (2.34)$$

a μ_i jsou záporná vlastní čísla částečné transpozice ρ^T matice hustoty ρ [14],[15]. Z vlastností $N(\rho)$ a tvaru (2.33) plyne horní odhad

$$N(\rho_{out}(\mathbf{m}_0)) \leq \frac{1}{2\sqrt{N-1}} + p_4 \left(\frac{1}{N-1} - \frac{1}{2\sqrt{N-1}} \right), \quad (2.35)$$

kde $0 \leq p_4 \leq 1$. Navíc pro krajní hodnoty p_4 nastává ve výrazu rovnost. Zároveň je zřejmé, že pro $N < 5$ je míra provázání maximální při parametru $p_4 = 1$, a tedy $p_2 = 0$, a pro $N > 5$ je optimální provazovací proces určen podmínkou $p_4 = 0$, a tedy $p_2 = 1$.

Pro případ $p_4 = 0$ a $p_2 = 1$ je znám Krausův operátor tohoto procesu. Je jím projektor na antisymetrický podprostor A dvoučásticového Hilbertova prostoru, tj.

$$\mathcal{E}^{ent}(\rho) = \frac{2}{N-1} A(\rho \otimes I)A. \quad (2.36)$$

Uvedená klasifikace kovariantních zobrazení na dvou částicích poskytuje důležité informace o struktuře této množiny. Nezbyvá se však otázkou úplné positivity zkoumaných procesů, která je nutnou podmínkou pro jejich realizovatelnost. Důkaz této vlastnosti, alespoň pro určitou podtřídu univerzálních procesů, je jedním z cílů následující kapitoly.

Kapitola 3

Realizace univerzálních procesů na dvou částicích

Na konci minulé kapitoly jsme uvedli Krausovy operátory dvou zástupců z pětiparametrické třídy univerzálních procesů. Cílem této kapitoly a těžištěm celé diplomové práce je najít Krausovy operátory širší třídy univerzálních procesů a jejich pomocí zkonstruovat unitární transformace, které tyto procesy realizují. V literatuře se setkáme většinou se dvěma přístupy k realizaci obecných zobrazení na maticích hustoty. Prvním z nich je princip projektivního měření, kdy výstupní stav získáme aplikací určitého projektoru na vstupní částice, což je ekvivalentní realizaci vhodného měření na vstupním stavu. Druhý princip spočívá v rozšíření systému o další částice. Na rozšířeném Hilbertově prostoru hledáme unitární transformaci, která na vstupním podsystemu realizuje předepsané zobrazení.

V sekci 3.1 nejprve zkonstruujeme Krausovy operátory jisté omezené třídy univerzálních procesů. Inspirujeme se procesem univerzálního optimálního kopírování a jedním z procesů provázání, pro $p_4 = 0$, jejichž Krausovy operátory jsme uvedli v příkladech na konci minulé kapitoly. V další sekci tento postup zobecníme a zavedeme obecnější ansatz, který vede k univerzálnímu procesu. Poté provedeme stručnou analýzu druhé třídy takto získaných procesů a identifikujeme v ní některé důležité příklady. Poslední odstavce této kapitoly se budou věnovat unitární realizaci pomocí nalezených Krausových operátorů.

V celé práci nadále předpokládáme konečněrozměrné částice, tzn. pro její stavový Hilbertův prostor platí $\dim \mathcal{H} = N < \infty$, a pokud nebude uvedeno jinak, předpokládáme navíc $N \geq 3$. Pro $N = 2$ jsou všechny uvedené postupy analogické, musíme pouze vzít v úvahu, že v takovém případě neexistují tři navzájem ortonormální stavy, čímž se některé výrazy zjednoduší.

3.1 Procesy generované projektory S_2 a A_2

Proces kopírování jedné částice na dvě, realizovaný projektorem na symetrické dvoučásticové stavy, splňuje, stejně jako operace univerzálního provázání popsaná projektorem na antisymetrické stavy, podmínku kovariance. Nabízí se otázka, zda ani kombinace těchto projektorů tuto podmínku nenaruší.

Předpokládejme dvoučásticový Hilbertův prostor $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, vstupní stav $\rho = \frac{1}{N}\rho_{in} \otimes I$, kde ρ_{in} je jednočásticový čistý stav, dále

$$P^{(2)} = \sigma S_2 + \alpha A_2, \quad (3.1)$$

kde σ a α jsou zatím libovolná komplexní čísla a S_2 , resp. A_2 je projektor na symetrické, resp. antisymetrické dvoučásticové stavy, a U nechť je jednočásticová libovolná unitární transformace. Výstupní stav obdržený aplikací zobrazení $P^{(2)}$ je

$$\rho_{out}(\rho_{in}) = \frac{P^{(2)}(\rho_{in} \otimes I)P^{(2)\dagger}}{\text{Tr}\left(P^{(2)}(\rho_{in} \otimes I)P^{(2)\dagger}\right)}. \quad (3.2)$$

Aby zobrazení $P^{(2)}$ bylo Krausovým operátorem, musí splňovat vztah (1.19). Vzhledem k ortogonalitě projektorů S_2 a A_2 platí

$$P^{(2)}P^{(2)\dagger} = (\sigma S_2 + \alpha A_2)(\bar{\sigma} S_2 + \bar{\alpha} A_2) = |\sigma|^2 S_2 + |\alpha|^2 A_2, \quad (3.3)$$

a protože platí $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = S_2 \mathcal{H} S_2 \oplus A_2 \mathcal{H} A_2$, bude podmínka (1.19) splněna právě tehdy, když $|\sigma|^2 \leq 1$ a $|\alpha|^2 \leq 1$.

Ověřme, zda (3.2) splňuje podmínku kovariance. Nechť $\{|i\rangle\}_{i=1}^N$ je ortonormální báze jednočásticového Hilbertova prostoru. Každou unitární transformaci na tomto prostoru lze psát ve tvaru $U = \sum u_{ij}|i\rangle\langle j|$. Platí

$$\begin{aligned} U^{\otimes 2} S_2 &= \sum_{a,b,c,d} u_{ab} u_{cd} |ac\rangle\langle bd| \left(\sum_i |ii\rangle\langle ii| + \frac{1}{2} \sum_{i<j} (|ij\rangle + |ji\rangle)(\langle ij| + \langle ji|) \right) \\ &= \sum_{a,b,c} u_{ab} u_{cb} |ac\rangle\langle bb| + \frac{1}{2} \sum_{a,c,b \neq d} (u_{ab} u_{cd} + u_{cb} u_{ad}) |ac\rangle(\langle bd| + \langle db|) \\ &= \sum_{abd} u_{ab} u_{ad} |aa\rangle\langle bd| + \frac{1}{2} \sum_{b,d,a<d} (u_{ab} u_{cd} + u_{cb} u_{ad}) (|ac\rangle + |ca\rangle)\langle bd| \\ &= S_2 U^{\otimes 2}. \end{aligned} \quad (3.4)$$

Projektor na symetrické stavy S_2 tedy komutuje s každou unitární transformací $U \otimes U$. Stejně tvrzení lze analogicky odvodit pro A_2 , a proto z (3.2)

získáme

$$\begin{aligned} U \otimes U \rho_{out}(\rho_{in}) U^\dagger \otimes U^\dagger &= \frac{P^{(2)} U \otimes U (\rho_{in} \otimes I) U^\dagger \otimes U^\dagger P^{(2)\dagger}}{\text{Tr} \left(P^{(2)} (\rho_{in} \otimes I) P^{(2)\dagger} \right)} \\ &= \rho_{out}(U \rho_{in} U^\dagger), \end{aligned} \quad (3.5)$$

což je přesně podmínka kovariance.

Nyní stručně rozebereme třídu procesů, kterou získáme zobrazením typu (3.2). Na první pohled je zřejmé, že pokud vynásobíme oba parametry σ a α libovolným komplexním číslem λ takovým, že $|\lambda| \leq 1$, obdržíme stejnou výslednou matici hustoty¹. V tomto smyslu jsou jedinými nezávislými proměnnými poměr absolutních hodnot a vzájemná fáze obou komplexních parametrů σ a α .

Díky platnosti podmínky kovariance (2.7) stačí opět uvažovat jeden konkrétní vstupní stav, řekněme $|1\rangle\langle 1|$. Zobrazení $P^{(2)}$ můžeme zapsat jako

$$P^{(2)} = P_1 \oplus P_2,$$

kde

$$P_1 = \sum_i \sigma |ii\rangle\langle ii|, \quad (3.6)$$

$$P_2 = \sum_{i < j} \left[\frac{\sigma}{2} (|ij\rangle + |ji\rangle)(\langle ij| + \langle ji|) + \frac{\alpha}{2} (|ij\rangle - |ji\rangle)(\langle ij| - \langle ji|) \right] \quad (3.7)$$

a výstupní matice hustoty je

$$\begin{aligned} \rho_{out} &= \frac{P_1 |11\rangle\langle 11| P_1^\dagger + P_2 \sum_{i \neq 1} |1i\rangle\langle 1i| P_2^\dagger}{\text{Tr} \sum_i P^{(2)} (|1i\rangle\langle 1i|) P^{(2)\dagger}} = \frac{2}{(N+1)|\sigma|^2 + (N-1)|\alpha|^2} \times \\ &\times \left\{ |\sigma|^2 |11\rangle\langle 11| + \sum_{i \neq 1} \left[\left| \frac{\sigma}{2} + \frac{\alpha}{2} \right| |1i\rangle\langle 1i| + \left| \frac{\sigma}{2} - \frac{\alpha}{2} \right| |i1\rangle\langle i1| \right. \right. \\ &\left. \left. + \left(\frac{\sigma}{2} + \frac{\alpha}{2} \right) \left(\frac{\bar{\sigma}}{2} - \frac{\bar{\alpha}}{2} \right) |1i\rangle\langle i1| + \left(\frac{\sigma}{2} - \frac{\alpha}{2} \right) \left(\frac{\bar{\sigma}}{2} + \frac{\bar{\alpha}}{2} \right) |i1\rangle\langle 1i| \right] \right\}. \end{aligned} \quad (3.8)$$

Z posledního vztahu je vidět první omezení, které vymezuje třídu univerzálních procesů, které lze realizovat přímo projekcemi. Ve výrazu (3.8) se nevyskytují členy typu $|ii\rangle\langle ii|$, $|ij\rangle\langle ij|$ a $|ij\rangle\langle ji|$ pro $i, j \neq 1$. Pro parametry zavedené v předchozí kapitole z toho plyne

$$p_3 = 0, \quad p_4 = 0. \quad (3.9)$$

¹Omezení na absolutní hodnotu λ klademe z důvodu zachování konzistence s podmínkou (1.19).

Jak jsme se už zmínili, jedinými relevantními proměnnými ve výrazu (3.2) jsou relativní fáze parametrů α a σ , označme ji φ , a poměr jejich absolutních hodnot $|\alpha| = \gamma |\sigma|$. Pokud by bylo $\sigma = 0$, jedná se o výše zmíněný univerzální provazovací proces, v případě $\alpha = 0$ jde o proces univerzálního kopírování. Předpokládáme dále, že $\sigma \neq 0$, $\alpha \neq 0$ a σ volíme reálnou. Porovnáním výrazů (3.8) a (2.20) získáme vyjádření parametrů p_1 , $\Delta\alpha = \alpha^{(1)} - \alpha^{(2)}$ a $\Delta\beta = \beta - \bar{\beta}$ pomocí γ a φ

$$\begin{aligned} p_1 &= \frac{2}{(N+1) + \gamma^2(N-1)}, \\ \Delta\alpha &= \frac{2\gamma \cos \varphi}{N [(N+1) + \gamma^2(N-1)]}, \\ \Delta\beta &= \frac{2i\gamma \sin \varphi}{N [(N+1) + \gamma^2(N-1)]}. \end{aligned} \quad (3.10)$$

Z posledních dvou rovnic vidíme, že ani parametry $\Delta\alpha$ a $\Delta\beta$ nemohou být libovolné, neboť má-li být proces charakterizovaný parametry p_1 , $\Delta\alpha$ a $\Delta\beta$, musí platit

$$(\Delta\alpha)^2 - (\Delta\beta)^2 = 2\gamma ((N+1) + \gamma^2(N-1))^{-1}. \quad (3.11)$$

Toto omezení lze obejít, pokud budeme uvažovat operaci se dvěma Krausovými operátory tvaru (3.1) charakterizovanými $\alpha_{1(2)}$ a $\sigma_{1(2)}$. Potom

$$\rho_{out}(\rho_{in}) = \frac{1}{\mathcal{N}} \left[P_1^{(2)}(\rho_{in} \otimes I)P_1^{(2)\dagger} + P_2^{(2)}(\rho_{in} \otimes I)P_2^{(2)\dagger} \right], \quad (3.12)$$

kde $\mathcal{N} = \frac{1}{2} ((N+1)(|\sigma_1|^2 + |\sigma_2|^2) + (N-1)(|\alpha_1|^2 + |\alpha_2|^2))$. Vzhledem k počtu volitelných parametrů v rovnici (3.12) lze volit $|\alpha_1| = |\alpha_2|$ a $|\sigma_1| = |\sigma_2|$. Porovnáním příslušných výrazů v (3.8) a (2.20) opět získáme závislosti parametrů p_1 , $\Delta\alpha$ a $\Delta\beta$ na γ_1 , φ_1 a φ_2

$$\begin{aligned} p_1 &= \frac{2}{(N+1) + \gamma_1^2(N-1)}, \\ \Delta\alpha &= \frac{\gamma_1(\cos \varphi_1 + \cos \varphi_2)}{N [(N+1) + \gamma_1^2(N-1)]}, \\ \Delta\beta &= \frac{i\gamma_1(\sin \varphi_1 + \sin \varphi_2)}{N [(N+1) + \gamma_1^2(N-1)]}. \end{aligned} \quad (3.13)$$

Dalšími úpravami lze dospět ke vztahům

$$\begin{aligned} (\Delta\alpha)^2 + (\Delta\beta)^2 &= \frac{2\gamma_1^2 \cos(\varphi_1 + \varphi_2)(1 + \cos(\varphi_1 - \varphi_2))}{N^2 [(N+1) + \gamma_1^2(N-1)]^2}, \\ (\Delta\alpha)^2 - (\Delta\beta)^2 &= \frac{2\gamma_1^2(1 + \cos(\varphi_1 - \varphi_2))}{N^2 [(N+1) + \gamma_1^2(N-1)]^2} \end{aligned} \quad (3.14)$$

a výslednou závislost lze vyjádřit následovně

$$\begin{aligned}\cos(\varphi_1 + \varphi_2) &= \frac{\Delta_+}{\Delta_-}, \\ \cos(\varphi_1 - \varphi_2) &= -1 + \Gamma\Delta_-, \\ \gamma_1 &= \left(\frac{2 - (N+1)p_1}{p_1(N-1)} \right)^{\frac{1}{2}}\end{aligned}\quad (3.15)$$

kde $\Delta_{\pm} = (\Delta\alpha)^2 \pm (\Delta\beta)^2$ a $\Gamma = \frac{2N^2(N-1)}{p_1(2-(N+1)p_1)}$. Systém (3.15) má obecně čtyři řešení, z nichž (v závislosti na znaménkách $\Delta\alpha$ a $i\Delta\beta$) vždy dvě řeší (3.13). Tato dvě řešení jsou ekvivalentní ve smyslu symetrie soustavy (3.13) vůči záměně φ_1 a φ_2 . Jmenovatele v Γ se obávat nemusíme, protože ten je nulový právě tehdy, když je $\alpha = 0$ nebo $\sigma = 0$, což jsou případy, které jsme diskutovali již dříve. Příklad $\Delta_- = 0$ implikuje² $\Delta\alpha = \Delta\beta = 0$ a řešení (3.13) lze volit $\varphi_1 - \varphi_2 = \pi$, $\varphi_1 + \varphi_2$ libovolné a γ_1 je dána první rovnicí v systému (3.13). Z (3.15) plyne, že parametry p_1 , $\Delta\alpha$ a $\Delta\beta$ musí splňovat nerovnosti

$$\left| \frac{\Delta_+}{\Delta_-} \right| = \left| \frac{|\Delta\alpha|^2 - |\Delta\beta|^2}{|\Delta\alpha|^2 + |\Delta\beta|^2} \right| \leq 1, \quad (3.16)$$

$$0 \leq \Gamma\Delta_- \leq 2. \quad (3.17)$$

Podmínka (3.16) je splněna identicky. Druhá nerovnost vede na nerovnici

$$p_1^2(N+1) - 2p_1 + N^2(N-1)\Delta_- \leq 0, \quad (3.18)$$

jejímž řešením je interval

$$p_1 \in \left\langle \frac{1 - \sqrt{1 - N^2(N^2 - 1)\Delta_-}}{N+1}, \frac{1 + \sqrt{1 - N^2(N^2 - 1)\Delta_-}}{N+1} \right\rangle. \quad (3.19)$$

To je ovšem stejná podmínka, kterou získáme požadavkem nezápornosti vlastních čísel (2.23) pro případ $p_3 = p_4 = 0$. Z poslední rovnice (3.13) také jasně plyne, že při těchto procesech je maximální dosažitelná hodnota p_1 rovna $\frac{2}{N+1}$, což přesně koresponduje s hodnotou p_1 odpovídající optimálnímu kopírovacímu procesu.

Shrňme tedy, že zobrazení (3.12) nabízí možnost realizace všech univerzálních procesů, které jsou charakterizovány podmínkou $p_3 = p_4 = 0$, tj. neobsahují členy ρ_3 a ρ_4 v rozkladu (2.19). Konstrukce Krausových operátorů kvantové operace \mathcal{E} je postačující podmínkou pro její úplnou pozitivitu. Vztahy (3.12), (3.13) a (3.15) dávají pro Krausovy operátory explicitní předpis, a proto docházíme k důležitému závěru, že všechny univerzální procesy na dvou částicích dané podmínkou (3.9) jsou úplně pozitivní.

²Připomeňme, že $\Delta\beta$ je ryze imaginární, a proto $\Delta_- = |\Delta\alpha|^2 + |\Delta\beta|^2 \geq 0$.

3.2 Zobecnění realizace univerzálních procesů projektory

Základním faktem, který v předchozí sekci umožnil důkaz kovariance, byla skutečnost, že pro každou jednočásticovou unitární transformaci U komutuje matice $U \otimes U$ s projektory na symetrický a antisymetrický podprostor dvoučásticového Hilbertova prostoru. Nabízí se přímočarý způsob, jak tuto konstrukci zobecnit na větší počet částic: budeme hledat zobrazení, která komutují s každou unitární transformací tvaru $U^{\otimes M}$, kde M je počet částic.

Matice tvaru $U^{\otimes M}$, kde U je matice unitární transformace na jednočásticovém Hilbertově prostoru \mathcal{H} dimenze N , tvoří reprezentaci unitární grupy $U(N)$ na Hilbertově prostoru $\mathcal{H}(M) = \mathcal{H}^{\otimes M}$. Pro $M \geq 2$ je tato reprezentace reducibilní. Víme tedy, že

$$\mathcal{H}(M) = \bigoplus_i^{r(M)} \mathcal{H}_i, \quad (3.20)$$

kde i probíhá množinu všech ireducibilních reprezentací (i ekvivalentních, tedy včetně násobností), které se v reprezentaci $U(N)^{\otimes M}$ nacházejí³ a \mathcal{H}_i jsou jim příslušné invariantní podprostory. Nechť $\Phi_i = \{|\varphi_{i1}\rangle, \dots, |\varphi_{iD_i}\rangle\}$ je báze \mathcal{H}_i a D_i jeho dimenze. Podle Schurova lemmatu, [16], víme, že matice \tilde{P} komutuje se všemi maticemi ireducibilní reprezentace právě tehdy, když je násobkem identity. Vzhledem k (3.20) lze v bázi

$$\Phi = \bigcup_i \Phi_i \quad (3.21)$$

zapsat každou matici $U^{\otimes M}$ v blokově diagonálním tvaru

$$U^{\otimes M} = \begin{pmatrix} U_1 & & & \\ & U_2 & & \\ & & \ddots & \\ & & & U_{r(M)} \end{pmatrix}, \quad (3.22)$$

a proto matice v odpovídajícím blokovém tvaru

$$P^{(M)} = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_{r(M)} \end{pmatrix}, \quad (3.23)$$

³Bez rizika nedorozumění užíváme stejné označení pro grupu unitárních transformací a její základní reprezentaci.

kde submatice A_i je libovolný α_i -násobek identity na \mathcal{H}_i , komutuje se všemi prvky $U(N)^{\otimes M}$. Matice $P^{(M)}$ není nic jiného, než direktní součet násobků projektorů na invariantní podprostory reducibilní reprezentace $U(N)^{\otimes M}$. Získáváme tím návod, jak zkonstruovat určitou třídu univerzálních procesů na M částicích:

$$\rho_{out} = \mathcal{E}(\rho_{in}) = \frac{P^{(M)} \rho_{in} \otimes I^{\otimes(M-1)} P^{(M)\dagger}}{\text{Tr} \left(P^{(M)} \rho_{in} \otimes I^{\otimes(M-1)} P^{(M)\dagger} \right)}. \quad (3.24)$$

V tomto smyslu je předchozí sekce pouze speciálním případem předchozích úvah pro dvě částice. Vzhledem k tomu, že pro $M = 2$ jsou jedinými invariantními podprostory reprezentace $U(N) \otimes U(N)$ symetrický a antisymetrický podprostor dvoučásticového Hilbertova prostoru, nezískáme touto konstrukcí žádné nové univerzální procesy na dvou částicích, které by už nebyly zahrnuty ve třídě definované (3.2). Jak bude ukázáno v následující sekci, umožní nám to až následující ansatz, který v sobě kombinuje princip projektivního měření a ancilly:

Tvrzení. *Nechť*

$$\rho_{out} = \mathcal{E}(\rho_{in}) = \frac{\text{Tr}_{i_1, \dots, i_L} \left(P^{(M)} \rho_{in} \otimes I^{\otimes(M-1)} P^{(M)\dagger} \right)}{\text{Tr} \left(P^{(M)} \rho_{in} \otimes I^{\otimes(M-1)} P^{(M)\dagger} \right)}, \quad (3.25)$$

kde ρ_{in} je jednočásticový čistý stav na Hilbertově prostoru \mathcal{H} , $M \in \mathbb{N}$, $L \in \mathbb{N}_0$, $M > L$, $\mathcal{I}_{\mathcal{E}} = \{i_1, \dots, i_L\} \subset \{1, \dots, M\}$ je množina navzájem různých indexů a $P^{(M)}$ je matice komutující za všemi prvky reprezentace $U(N)^{\otimes M}$ unitární grupy $U(N)$, a tedy matice, která má v bázi (3.21) tvar (3.23). Konstanty α_i vystupující v blocích (3.23) splňují

$$\forall i \quad |\alpha_i|^2 \leq 1, \quad \sum_i |\alpha_i|^2 > 0.$$

Potom zobrazení $\rho_{in} \rightarrow \rho_{out}$ definuje univerzální kvantový proces na $M - L$ částicích.

K důkazu tohoto tvrzení je třeba ověřit podmínku kovariance. Stačí dokázat následující tvrzení:

Tvrzení. *Pro každou jednočásticovou unitární transformaci U na \mathcal{H} , každou matici A na M -částicovém Hilbertově prostoru $\mathcal{H}^{\otimes M}$ a $t \in \{1, \dots, M\}$ libovolné platí*

$$\text{Tr}_t \left(U^{\otimes M} A U^{\otimes M\dagger} \right) = U^{\otimes(M-1)} \left(\text{Tr}_t A \right) U^{\otimes(M-1)\dagger}. \quad (3.26)$$

Důkaz. Zřejmě platí

$$\begin{aligned}
\mathrm{Tr}_t \left(U^{\otimes M} A U^{\otimes M \dagger} \right) &= \mathrm{Tr}_t \left(U^{\otimes M} \sum_{i,j} \alpha_{ij} |i\rangle_t \langle j|_t \otimes A_{ij}^t U^{\otimes M \dagger} \right) \\
&= \sum_{i,j,k} \alpha_{ij} \langle k|U|i\rangle_t \langle j|_t U^\dagger|k\rangle \otimes U^{\otimes(M-1)} A_{ij}^t U^{\otimes(M-1)\dagger} \\
&= U^{\otimes(M-1)} \sum_k \alpha_{kk} A_{kk}^t U^{\otimes(M-1)\dagger} = U^{\otimes(M-1)} (\mathrm{Tr}_t A) U^{\otimes(M-1)\dagger}.
\end{aligned}$$

□

Využitím komutace $P^{(M)}$ s $U^{\otimes M}$ a aplikací předchozího tvrzení postupně pro $t = i_1$ až $t = i_L$ je důkaz kovariance procesu definovaného (3.25) hotov.

Stejně jako v předchozí sekci i zde je patrné, že vynásobením zobrazení $P^{(M)}$ libovolnou nenulovou komplexní konstantou takovou, aby nepřestala platit podmínka (1.19), se výsledná matice hustoty nezmění. Proces je tedy charakterizován pouze vzájemnými poměry amplitud a relativními fázemi koeficientů α_i . Poznamenejme ale, že pravděpodobnost, že daný proces při realizaci skutečně nastane, na absolutních velikostech těchto parametrů závisí.

Dodejme, že zobrazení tvaru (3.23) není nejobecnější zobrazení, které komutuje se všemi maticemi tvaru $U^{\otimes M}$. Zobrazení tohoto typu však generuje velkou třídu univerzálních procesů, a proto se v dalším zkoumání spokojíme s ansatzem (3.25).

Postup konstrukce univerzálního procesu podle (3.25) umožňuje nalézt Krausovy operátory těchto kvantových operací. Na rozdíl od případu v předchozí sekci, kde bylo $M = 2$ a $L = 0$, nehraje $P^{(M)}$ obecně pro $L \neq 0$ přímo roli Krausova operátoru. Vztah (3.25) lze dále upravit jako

$$\rho_{out} = \frac{1}{N^{M-1} \mathcal{N}} \sum_{j_1, \dots, j_L}^N \left(K_{j_1, \dots, j_L}^{i_1, \dots, i_L} \rho_{in} \otimes I^{\otimes(M-1)} K_{j_1, \dots, j_L}^{i_1, \dots, i_L \dagger} \right),$$

kde

$$\mathcal{N} = \frac{1}{N^{M-1}} \mathrm{Tr} \left(P^{(M)} \rho_{in} \otimes I^{\otimes(M-1)} P^{(M)\dagger} \right), \quad (3.27)$$

výrazem $\langle j|_i$ míníme bra-vektor $\langle j| \in \mathcal{H}^\#$ působící na i -tou komponentu tenzorového součinu a zobrazení $K_{j_1, \dots, j_L}^{i_1, \dots, i_L} : \mathcal{H}^{\otimes M} \rightarrow \mathcal{H}^{\otimes M-L}$ definujeme jako

$$K_{j_1, \dots, j_L}^{i_1, \dots, i_L} = \langle j_1|_{i_1} \otimes \dots \otimes \langle j_L|_{i_L} P^{(M)}. \quad (3.28)$$

Množina $\{K_{j_1, \dots, j_L}^{i_1, \dots, i_L}\}_{j_1, \dots, j_L=1}^N$ definuje Krausovy operátory⁴ univerzálního procesu (3.25). Je možné definovat Krausovy operátory i z $\mathcal{H}^{\otimes M-L}$ na $\mathcal{H}^{\otimes M-L}$:

$$\mathcal{K}_{j_1, \dots, j_L, k_1, \dots, k_L}^{i_1, \dots, i_L} |\varphi\rangle = \langle j_1 |_{i_1} \otimes \dots \otimes \langle j_L |_{i_L} P^{(M)} |\varphi\rangle \otimes |k_1\rangle \otimes \dots \otimes |k_L\rangle. \quad (3.29)$$

Prezentovaný postup umožňuje konstrukci veliké třídy univerzálních procesů pro libovolný počet částic, což je výhoda zejména v případě, kdy $M \geq 4$, kde není dosud provedena širší klasifikace. Další výhodou je možnost přímočarého zobecnění na situaci, kdy je vstupní stav vícečásticový a kovariantní podmínka definovaná takto:

$$\rho_{out} \left(\hat{U} \rho_{in} \hat{U}^\dagger \right) = \hat{U}^{\otimes L} \rho_{out}(\rho_{in}) \hat{U}^{\otimes L \dagger}, \quad (3.30)$$

kde

$$\hat{U} = U_1 \otimes \dots \otimes U_R \quad (3.31)$$

pro každý čistý vstupní R -částicový stav ρ_{in} a každou R -tici jednočásticových unitárních transformací \hat{U} . V takovém případě bychom hledali ireducibilní reprezentace grupy $U(N)^{\otimes R}$ v reprezentaci $(U(N)^{\otimes R})^{\otimes L}$.

3.3 Univerzální procesy na dvou částicích pro $M=3$

Uvažujme třídu univerzálních procesů na třech částicích tvaru (3.2)

$$\rho_{out}^3 = \frac{P^{(3)}(\rho_{in} \otimes I \otimes I) P^{(3) \dagger}}{\text{Tr} [P(\rho_{in} \otimes I \otimes I) P^\dagger]}. \quad (3.32)$$

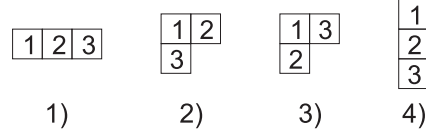
Reprezentace unitární grupy $U(N)$ maticemi tvaru $U \otimes U \otimes U$ je direktním součtem čtyř ireducibilních reprezentací, které odpovídají Youngovým schématům, [17] na následujícím obrázku. Zobrazení $P^{(3)}$ má proto tvar

$$P^{(3)} = \sigma S \oplus \alpha A \oplus \mu M_1 \oplus \nu M_2, \quad (3.33)$$

kde konstanty σ , α , μ a ν jsou libovolná komplexní čísla splňující podmínku

$$\begin{aligned} |\sigma|^2 \leq 1, \quad |\alpha|^2 \leq 1, \quad |\mu|^2 \leq 1, \quad |\nu|^2 \leq 1, \\ |\sigma|^2 + |\alpha|^2 + |\mu|^2 + |\nu|^2 > 0 \end{aligned}$$

⁴V obecném případě, kdy $L \neq 0$ nejde vlastně o operátory, protože vstupní a výstupní prostory nejsou totožné. Nicméně i v tomto případě je vžité názvosloví "Krausův operátor".



Obrázek 3.1: Youngovy schemata odpovídající ireducibilním reprezentacím jednočasticové unitární grupy $U(N)$ zastoupeným v $U(N)^{\otimes 3}$: 1) symetrická, 2),3) smíšené, 4) antisymetrická.

a zobrazení S , resp. A , resp. $M_{1(2)}$ jsou projektory na invariantní podprostory tříčasticového Hilbertova prostoru reprezentace $U \otimes U \otimes U$; symetrický⁵, resp. antisymetrický, resp. dva "smíšené" podprostory. Zvolíme báze těchto podprostorů následujícím standardním způsobem, [18]:

báze symetrického podprostoru:

$$\begin{array}{ll} |iii\rangle & i \in \{1, \dots, N\} \\ \frac{1}{\sqrt{3}} [|iij\rangle + |iji\rangle + |jii\rangle] & i \neq j \\ \frac{1}{\sqrt{6}} [|ijk\rangle + |ikj\rangle + |jki\rangle + |jik\rangle + |kij\rangle + |kji\rangle] & i < j < k \end{array}$$

báze antisymetrického podprostoru:

$$\frac{1}{\sqrt{6}} [|ijk\rangle - |ikj\rangle + |jki\rangle - |jik\rangle + |kij\rangle - |kji\rangle] \quad i < j < k$$

báze "smíšeného" podprostoru M_1 :

$$\begin{array}{ll} \frac{1}{\sqrt{12}} [2(|ijk\rangle + |jik\rangle) - |ikj\rangle - |jki\rangle - |kij\rangle - |kji\rangle] & i < j < k \\ \frac{1}{2} [|ikj\rangle + |kij\rangle - |jki\rangle - |kji\rangle] & i < j < k \\ \frac{1}{\sqrt{6}} [2|iij\rangle - |jii\rangle - |iji\rangle] & i \neq j \end{array}$$

báze "smíšeného" podprostoru M_2 :

$$\begin{array}{ll} \frac{1}{\sqrt{12}} [2(|ijk\rangle - |jik\rangle) + |ikj\rangle - |jki\rangle - |kij\rangle + |kji\rangle] & i < j < k \\ \frac{1}{2} [|ikj\rangle + |jki\rangle - |kij\rangle - |kji\rangle] & i < j < k \\ \frac{1}{\sqrt{2}} [|jii\rangle - |iji\rangle] & i \neq j \end{array}$$

$P^{(3)}$ lze nyní zapsat jako direktní součet zobrazení působících na ortogonálních podprostorech typu $|iii\rangle$, $|iij\rangle$ a $|ijk\rangle$

$$P^{(3)} = P_1 \oplus P_2 \oplus P_3, \quad (3.34)$$

⁵Označení podprostorů názvy symetrický, antisymetrický, apod. odráží jejich chování vzhledem k transpozicím částic.

kde

$$P_1 = \sum_{i=1}^N \sigma |iii\rangle \langle iii|, \quad (3.35)$$

$$\begin{aligned} P_2 = & \sum_{i \neq j} \left\{ \frac{\sigma}{3} (|ii\rangle + |ji\rangle + |jii\rangle) (\langle iij\rangle + \langle iji\rangle + \langle jii\rangle) \right. \\ & + \frac{\mu}{6} (2|ii\rangle - |ji\rangle - |jii\rangle) (2\langle iij\rangle - \langle iji\rangle - \langle jii\rangle) \\ & \left. + \frac{\nu}{2} (|ji\rangle - |jii\rangle) (\langle iji\rangle - \langle jii\rangle) \right\}, \quad (3.36) \end{aligned}$$

$$\begin{aligned} P_3 = & \sum_{i < j < k} \left\{ \frac{\alpha}{6} (|ijk\rangle - |ikj\rangle + |jki\rangle - |jik\rangle + |kij\rangle - |kji\rangle) \times \right. \\ & \times (\langle ijk\rangle - \langle ikj\rangle + \langle jki\rangle - \langle jik\rangle + \langle kij\rangle - \langle kji\rangle) \\ & + \frac{\sigma}{6} (|ijk\rangle + |ikj\rangle + |jki\rangle + |jik\rangle + |kij\rangle + |kji\rangle) \times \\ & \times (\langle ijk\rangle + \langle ikj\rangle + \langle jki\rangle + \langle jik\rangle + \langle kij\rangle + \langle kji\rangle) \\ & + \frac{\mu}{12} [2(|ijk\rangle + |jik\rangle) - |ikj\rangle - |jki\rangle - |kij\rangle - |kji\rangle] \times \\ & \times [2(\langle ijk\rangle + \langle jik\rangle) - \langle ikj\rangle - \langle jki\rangle - \langle kij\rangle - \langle kji\rangle] \\ & + \frac{\mu}{4} (|ikj\rangle + |kij\rangle - |jki\rangle - |kji\rangle) (\langle ikj\rangle + \langle kij\rangle - \langle jki\rangle - \langle kji\rangle) \\ & + \frac{\nu}{12} [2(|ijk\rangle - |jik\rangle) + |ikj\rangle - |jki\rangle - |kij\rangle + |kji\rangle] \times \\ & \times [2(\langle ijk\rangle - \langle jik\rangle) + \langle ikj\rangle - \langle jki\rangle - \langle kij\rangle + \langle kji\rangle] \\ & \left. + \frac{\nu}{4} (|ikj\rangle + |jki\rangle - |kij\rangle - |kji\rangle) (\langle ikj\rangle + \langle jki\rangle - \langle kij\rangle - \langle kji\rangle) \right\}. \quad (3.37) \end{aligned}$$

Ke klasifikaci nám, vzhledem ke kovariantní podmínce, kterou proces (3.32) splňuje, stačí zkoumat jeho působení na jeden konkrétní vstupní stav, řekněme $\rho_{in} = |1\rangle\langle 1|$. Potom

$$\begin{aligned} \rho_{out}^3 = & \frac{1}{\mathcal{N}} P^{(3)} \left(\sum_{a,b=1}^N |1ab\rangle \langle 1ab| \right) P^{(3)\dagger} = \frac{1}{\mathcal{N}} P_1 |111\rangle \langle 111| P_1^\dagger \\ & + \frac{1}{\mathcal{N}} P_2 \sum_{a \neq 1} (|1a1\rangle \langle 1a1| + |11a\rangle \langle 11a| + |1aa\rangle \langle 1aa|) P_2^\dagger \\ & + \frac{1}{\mathcal{N}} P_3 \sum_{1 \neq a \neq b \neq 1} |1ab\rangle \langle 1ab| P_3^\dagger, \quad (3.38) \end{aligned}$$

kde

$$\mathcal{N} = \text{Tr} \left[P^{(3)} \left(\sum_{a,b=1}^N |1ab\rangle\langle 1ab| \right) P^{(3)\dagger} \right].$$

Užitím vztahů (3.35) až (3.37) získáváme

$$P_1|111\rangle = \sigma|111\rangle, \quad (3.39)$$

pro $a \neq 1$

$$\begin{aligned} P_2|11a\rangle &= |11a\rangle \left(\frac{\sigma}{3} + \frac{2}{3}\mu \right) + |1a1\rangle \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) + |a11\rangle \left(\frac{\sigma}{3} - \frac{\mu}{3} \right), \\ P_2|1a1\rangle &= |11a\rangle \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) + |1a1\rangle \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) + |a11\rangle \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right), \\ P_2|1aa\rangle &= |1aa\rangle \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) + |aa1\rangle \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) + |a1a\rangle \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) \end{aligned} \quad (3.40)$$

a pro $1 \neq a \neq b \neq 1$

$$\begin{aligned} P_3|1ab\rangle &= |1ab\rangle \left(\frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right) + |1ba\rangle \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \\ &+ |ab1\rangle \left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) + |a1b\rangle \left(\frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right) \\ &+ |b1a\rangle \left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) + |ba1\rangle \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right). \end{aligned} \quad (3.41)$$

Dosazením rovnic (3.39) až (3.41) do (3.38) dostaneme tříčásticovou výstupní matici hustoty, kterou, vzhledem k její složitosti, uvádíme v dodatku A, sekce A.1. Ke získání výsledného dvoučásticového stavu můžeme z matice (A.1) vyloučit jednu ze tří částic, tj. provést operaci částečné stopy přes příslušný jednočásticový Hilbertův prostor, a podle úvah v předchozí sekci budou výsledkem tři třídy výstupních matic hustoty na dvou částicích $\rho_{out}^{(3)}$, resp. $\rho_{out}^{(2)}$, resp. $\rho_{out}^{(1)}$, při vyloučení třetí, resp. druhé, resp. první částice. Tyto matice jsou ze stejného důvodu jako v případě tříčásticového stavu uvedeny v dodatku A v sekci A.2

Porovnáním koeficientů u příslušných maticových elementů získáme vyjádření parametrů $p_1, p_3, p_4, \alpha^{(1)} - \alpha^{(2)}$ a $\beta - \bar{\beta}$ charakterizující univerzální proces v klasifikaci uvedené v druhé kapitole (podle [4]) pomocí parametrů

σ, μ, ν a α . Z (A.4) získáme

$$\begin{aligned}
p_1 &= \frac{1}{\mathcal{N}} \left[|\sigma|^2 + (N-1) \left(\left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right) \right], & (3.42) \\
p_3 &= \frac{1}{\mathcal{N}} (N-1) \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2, \\
p_4 &= \frac{2}{\mathcal{N}} (N-1)(N-2) \left(\left| \frac{\sigma}{6} - \frac{\mu}{6} \right|^2 + \left| \frac{\alpha}{6} - \frac{\nu}{6} \right|^2 \right), \\
\alpha^{(1)} - \alpha^{(2)} &= \frac{1}{\mathcal{N}} \left[\frac{(N+2)}{6N} (\sigma\bar{\nu} + \bar{\sigma}\nu) + \frac{(N-2)}{6N} (\mu\bar{\alpha} + \bar{\mu}\alpha) + \frac{1}{6} (\mu\bar{\nu} + \bar{\mu}\nu) \right], \\
\beta - \bar{\beta} &= \frac{1}{\mathcal{N}} \left[\frac{(N+2)}{6N} (\bar{\sigma}\nu - \sigma\bar{\nu}) + \frac{(N-2)}{6N} (\bar{\mu}\alpha - \mu\bar{\alpha}) + \frac{1}{6} (\bar{\mu}\nu - \mu\bar{\nu}) \right],
\end{aligned}$$

z matice (A.3) plyne

$$\begin{aligned}
p_1 &= \frac{1}{\mathcal{N}} \left[|\sigma|^2 + (N-1) \left(\left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right) \right], & (3.43) \\
p_3 &= \frac{1}{\mathcal{N}} (N-1) \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2, \\
p_4 &= \frac{1}{\mathcal{N}} (N-1)(N-2) \left(\left| \frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right|^2 \right), \\
\alpha^{(1)} - \alpha^{(2)} &= \frac{1}{\mathcal{N}} \left[\frac{N+2}{12N} (|\mu|^2 + \sigma(\bar{\mu} + \bar{\nu}) + \bar{\sigma}(\mu + \nu)) + \frac{1}{12} (\mu\bar{\nu} + \bar{\mu}\nu) + \right. \\
&\quad \left. + \frac{N-2}{12N} (|\nu|^2 + \alpha(\bar{\mu} + \bar{\nu}) + \bar{\alpha}(\mu + \nu)) \right], \\
\beta - \bar{\beta} &= \frac{1}{\mathcal{N}} \left[\frac{(N+2)}{12N} (\bar{\sigma}\nu - \sigma\bar{\nu} + \bar{\sigma}\mu - \sigma\bar{\mu}), \right. \\
&\quad \left. + \frac{(N-2)}{12N} (\bar{\mu}\alpha - \mu\bar{\alpha} + \bar{\nu}\alpha - \nu\bar{\alpha}) + \frac{1}{6} (\mu\bar{\nu} - \bar{\mu}\nu) \right]. & (3.44)
\end{aligned}$$

Porovnáním koeficientů v případě vyloučení první částice dostaneme stejný systém rovnic jako (3.43) jen s tím rozdílem, že parametry ν a α změni znaménko. Třída procesů realizovatelných tímto způsobem je tedy stejná jako a (A.3) a v klasifikaci stačí uvažovat pouze jednu z nich.

V souladu s úvahami provedenými v předchozí sekci vykazují systémy rovnic (3.42) a (3.43) symetrii vůči vynásobení všech parametrů σ, μ, ν a α libovolným nenulovým komplexním číslem.

V následujících odstavcích identifikujeme v třídě (3.25) pro $M = 3$ několik významných příkladů univerzálních procesů na dvou částicích ($L = 1$).

3.3.1 Proces kopírování

Proces optimálního univerzálního kopírování jedné částice na dvě je speciálním případem (3.1) diskutovaným v sekci 3.1. Lze ho ale identifikovat i v třídě procesů tvaru (3.25) pro $M = 3$ a $\mathcal{I} = \{3\}$.

Ze vztahů (2.28), (2.29) a soustavy (3.42) získáme systém rovnic určující parametry σ , μ , ν a α procesu kopírování pro případ vyloučení třetí částice:

$$\begin{aligned} \frac{2}{N+1} &= \frac{1}{\mathcal{N}} \left[|\sigma|^2 + (N-1) \left(\left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right) \right], & (3.45) \\ 0 &= \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2, \\ 0 &= \left| \frac{\sigma}{6} - \frac{\mu}{6} \right|^2 + \left| \frac{\alpha}{6} - \frac{\nu}{6} \right|^2, \\ 0 &= (N+2)(\sigma\bar{\nu} + \bar{\sigma}\nu) + (N-2)(\mu\bar{\alpha} + \bar{\mu}\alpha) + N(\mu\bar{\nu} + \bar{\mu}\nu), \\ 0 &= (N+2)(\bar{\sigma}\nu - \sigma\bar{\nu}) + (N-2)(\bar{\mu}\alpha - \mu\bar{\alpha}) + N(\bar{\mu}\nu - \mu\bar{\nu}). \end{aligned}$$

Řešením této soustavy je

$$\sigma = \mu, \quad \alpha = 0, \quad \nu = 0. \quad (3.46)$$

Pokud hledáme proces, který realizuje kopírování s maximální pravděpodobností, zvolíme $|\sigma| = 1$. Tato pravděpodobnost p_{clon}^{max} je pak rovna

$$p_{clon}^{max} = \frac{(N+1)}{2N}. \quad (3.47)$$

Při vyloučení druhé částice získáme z (3.43) soustavu analogickou k (3.45). Ta ovšem nemá řešení, a proces kopírování se v této třídě proto nevyskytuje. Je to také jednoduchá demonstrace faktu, že třídy univerzálních procesů, které získáme vyloučením různých částic, nejsou obecně stejné.

3.3.2 Procesy provázání

V sekci 2.3.2 byl uveden Krausův operátor univerzálního provazovacího procesu (2.36), který lze identifikovat s procesem (3.1) pro $\alpha = 1$ a $\sigma = 0$. Je to také jediný provazovací proces, který lze ve třídě definované (3.1) najít, neboť jako jediný nemá v rozkladu (2.19) zastoupen člen ρ_4 . V následujících odstavcích najdeme Krausovy operátory širší třídy provazovacích procesů, které se vyskytují v (3.25) pro $M = 3$ a $L = 1$.

Nejprve rozebereme případ vyloučení třetí částice. Ze vztahů (2.31), (2.32) a rovnic (3.43) dostaneme soustavu

$$\begin{aligned}
0 &= |\sigma|^2 + (N-1) \left(\left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right), \\
0 &= \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2, \\
p_4 &= \frac{2}{\mathcal{N}}(N-1)(N-2) \left(\left| \frac{\sigma}{6} - \frac{\mu}{6} \right|^2 + \left| \frac{\alpha}{6} - \frac{\nu}{6} \right|^2 \right), \\
0 &= (N+2)(\sigma\bar{\nu} + \bar{\sigma}\nu) + (N-2)(\mu\bar{\alpha} + \bar{\mu}\alpha) + N(\mu\bar{\nu} + \bar{\mu}\nu), \\
0 &= (N+2)(\bar{\sigma}\nu - \sigma\bar{\nu}) + (N-2)(\bar{\mu}\alpha - \mu\bar{\alpha}) + N(\bar{\mu}\nu - \mu\bar{\nu}).
\end{aligned} \tag{3.48}$$

Její řešení je, v závislosti na parametru p_4 , dáno rovnicemi

$$\begin{aligned}
\sigma &= 0, \\
\mu &= 0, \\
0 &= g^2(N-2)(1-3p_4) - 2(N-2)\cos\varphi g \\
&\quad + [N(1-6p_4) - 2(1+3p_4)],
\end{aligned} \tag{3.49}$$

kde jsme využili možnosti volby globální fáze a závislosti výsledné matice hustoty pouze na poměru amplitud α, ν a položili⁶

$$\alpha = |\alpha| \exp i\varphi, \quad 0 \leq \nu \in \mathbb{R}, \quad g = \frac{|\alpha|}{|\nu|}.$$

Tato rovnice ale nemá řešení pro všechna p_4 . Musí být navíc splněno

$$\cos^2 \varphi \geq \frac{(1-3p_4)(N(1-6p_4) - 2(1+3p_4))}{(N-2)}, \tag{3.50}$$

z čehož pro p_4 plyne omezení

$$0 \leq p_4 \leq \frac{N}{2(N+1)}. \tag{3.51}$$

Tato třída tedy neobsahuje všechny provazovací procesy. Asymptoticky, pro $N \rightarrow \infty$, popíšeme pouze procesy $p_4 \leq \frac{1}{2}$.

Množina přípustných hodnot g , pro které existuje φ tak, že g a φ řeší (3.49), je pro dané p_4 shora omezena funkcí

$$g^{max}(p_4) = \left| \frac{(N-2) + 3\sqrt{p(N-2)(N-2(N+1)p)}}{(1-3p)(N-2)} \right| \tag{3.52}$$

⁶Vzhledem k tomu, že $|\nu| \geq 0$ lze v případě $\nu = 0$ položit $g = \infty$.

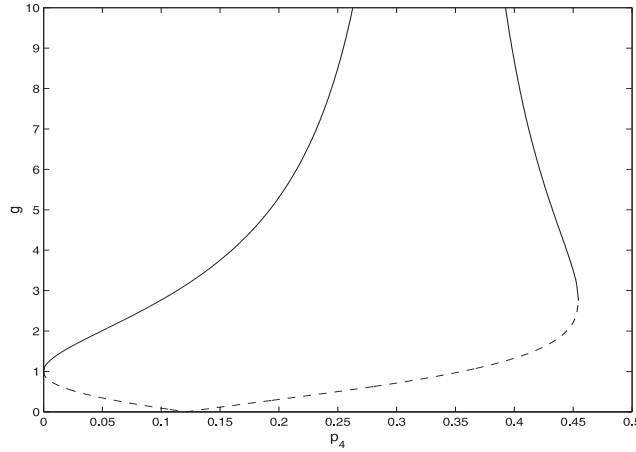
a zdola

$$g^{min}(p_4) = \left| \frac{(N-2) - 3\sqrt{p(N-2)(N-2(N+1)p)}}{(1-3p)(N-2)} \right|. \quad (3.53)$$

Příslušná hodnota φ je dána vztahem

$$\cos \varphi = \frac{g^2(N-2)(1-3p_4) + N(1-6p_4) - 2(1+3p_4)}{2g(N-2)}. \quad (3.54)$$

Pro $p_4 = \frac{1}{3}$ není maximální hodnota g omezena, což odpovídá možnosti volby $\nu = 0$, a hodnotě $g = 0$ odpovídá volba $\alpha = 0$. V obou případech je fáze φ libovolná. Struktura množiny přípustných hodnot g pro $N = 10$ je znázorněna na obrázku 3.2.



Obrázek 3.2: Struktura množiny přípustných hodnot g pro $N = 10$. Plná, resp. přerušovaná čára shora, resp. zdola omezuje možné hodnoty.

Z hlediska realizace je zajímavé hledat v přípustné množině řešení parametry, které maximalizují pravděpodobnost toho, že daný proces skutečně nastane. Pro $p_4 \in \left\langle 0, \frac{4(N-2)}{9N} \right\rangle$ nastává maximum při $g = 1$ a $|\alpha| = |\nu| = 1$ a jeho hodnota je

$$p_{ent}^{max} = \frac{(N-1)}{2N} \quad (3.55)$$

a pro $p_4 \in \left\langle \frac{4(N-2)}{9N}, \frac{N}{2(N+1)} \right\rangle$ je optimální volbou g spodní hranice (3.53) přípustné množiny a $\alpha = 1$. Maximální pravděpodobnost realizace těchto procesů je dána vztahem

$$p_{ent}^{max} = \frac{(N-1)}{6N^2} \left((N-2) + 2(N+1)\frac{1}{g^2} \right). \quad (3.56)$$

Při vypuštění druhé částice je možné realizovat univerzální provazovací proces pouze pro $p_4 = \frac{1}{3}$. Řešením příslušných rovnic jsou parametry

$$\sigma = \mu = \nu = 0, \quad 0 \leq |\alpha| \leq 1. \quad (3.57)$$

Maximální hodnota p_{ent}^{max} nastane pro $|\alpha| = 1$

$$p_{ent}^{max} = \frac{(N-1)}{6N^2}(N-2). \quad (3.58)$$

Tato hodnota je pro každé N menší než (3.55) a (3.56) pro stejný proces, a proto je vždy efektivnější realizovat provazovací proces pro $p_4 = \frac{1}{3}$ vypuštěním třetí částice.

3.4 Unitární realizace univerzálního procesu pomocí Krausových operátorů

Znalost Krausových operátorů kvantové \mathcal{E} operace dovoluje kanonickým způsobem zkonstruovat její unitární realizaci [6]. Předpokládejme množinu Krausových operátorů $\{E_k\}_{k=1}^J$ na \mathcal{H} deterministického procesu \mathcal{E} , tj.

$$\mathcal{E}(\rho) = \sum_{k=1}^J E_k \rho E_k^\dagger, \quad \sum_{k=1}^J E_k^\dagger E_k = I. \quad (3.59)$$

Potom matice U konstruovaná blokovým způsobem

$$U = \begin{pmatrix} E_1 & & \\ & \tilde{A} & \\ & & E_J \end{pmatrix}, \quad (3.60)$$

kde blok \tilde{A} je libovolný takový, že matice U je unitární, realizuje operaci \mathcal{E} v následujícím smyslu. Necht' $\tilde{\mathcal{H}}$ je rozšířený Hilbertův prostor

$$\tilde{\mathcal{H}} = \mathcal{H} \otimes \mathcal{H}', \quad (3.61)$$

kde \mathcal{H}' je Hilbertův prostor nějakého J -rozměrného systému a $\{|i\rangle\}_{i=1}^J$ je jeho báze. Buď $\rho \otimes |1\rangle\langle 1|$ počáteční stav tohoto složeného systému. Potom platí

$$\mathcal{E}(\rho) = \sum_{k=1}^J E_k \rho E_k^\dagger = \text{Tr}_3 [U \rho \otimes |1\rangle\langle 1| U^\dagger]. \quad (3.62)$$

V případě nedeterministického procesu, tj. v podmínce úplnosti (1.19) platí nerovnost, je potřeba nejprve množinu Krausových operátorů doplnit tak, aby rozřířená množina splňovala v (1.19) rovnost. Necht' $\{E_k\}_{k=1}^J$ je množina Krausových operátorů kvantové operace \mathcal{E} . Dodefinujeme operátor E_{J+1} následovně

$$E_{J+1} = \sqrt{I - \sum_{k=1}^J E_k^\dagger E_k}. \quad (3.63)$$

Vzhledem tomu, že $\sum_{k=1}^J E_k^\dagger E_k \leq I$, je operátor pod odmocninou pozitivní, a E_{J+1} je proto vždy dobře definován.

Kvantový proces \mathcal{E}' charakterizovaný rozšířenou množinou Krausových operátorů $\{E_k\}_{k=1}^{J+1}$ je už deterministický a lze na něj aplikovat předchozí postup. Platí

$$\mathcal{E}'(\rho) = \mathcal{E}(\rho) + E_{J+1}\rho E_{J+1}^\dagger. \quad (3.64)$$

K realizaci pouze procesu \mathcal{E} je ale třeba provést místo operace částečné stopy ve výrazu (3.62) projekční měření na podprostor \mathcal{H}' tvořený lineárním obalem z vektorů $\{|1\rangle, \dots, |J\rangle\}$. V případě pozitivního výsledku tohoto měření nastane proces \mathcal{E} , v opačném případě bude výstupním stavem

$$\rho_{out} = \frac{E_{J+1}\rho E_{J+1}^\dagger}{\text{Tr} [E_{J+1}\rho E_{J+1}^\dagger]}. \quad (3.65)$$

Pravděpodobnost $p_{\mathcal{E}}$ kladného výsledku je rovna

$$p_{\mathcal{E}} = \text{Tr} \left[\sum_{k=1}^J E_k \rho E_k^\dagger \right]. \quad (3.66)$$

Postup kanonické konstrukce unitární realizace můžeme po drobné modifikaci demonstrovat například na podtřídě provazovacích procesů \mathcal{E}_{p_4} pro $p_4 \in \left\langle 0, \frac{4(N-2)}{9N} \right\rangle$. Zároveň, jak se ukáže, tím realizujeme optimální kopírování. Podle paragrafu 3.3.2, jde o jednoparametrickou třídu charakterizovanou $P^{(3)} = M_2 + e^{i\varphi}A$ a $\mathcal{I}_{\mathcal{E}} = \{3\}$. Explicitní předpis maticových elementů Krausových operátorů lze získat z (3.29) předpisem

$$(\mathcal{K}_{i,j}^3)_{ab,cd} = \langle abi | (M_2 + e^{i\varphi}A) |cdj\rangle. \quad (3.67)$$

K využití předchozího postupu tedy zbývá doplnit tyto operátory tak, aby splňovali podmínku úplnosti. Platí,

$$I - P^{(3)\dagger}P^{(3)} = S + M_1 = \sqrt{S + M_1}, \quad (3.68)$$

druhý s pravděpodobností

$$p = \frac{1}{N^2} \text{Tr} [(S + M_1) \rho_{in} \otimes I^{\otimes 2} (S + M_1)]. \quad (3.76)$$

Z odstavce 3.3.1 ale víme, že Krausovy operátory získané z procesu tvaru (3.25) pro $P^{(3)} = S + M_1$ a volbu $\mathcal{I} = \{3\}$ pomocí konstrukce (3.29) odpovídají procesu optimálního univerzálního kopírování.

Kanonická konstrukce unitární evoluce uvedená v této sekci umožňuje realizovat každý univerzální proces popsany vztahem (3.25). Otázkou zůstává, jak velká třída úplně pozitivních kovariantních zobrazení v této třídě leží. Dalšího rozšíření je možno dosáhnout, jak bylo demonstrováno v sekci 3.1, nekoherentní kombinací obkladů projektory, tedy

$$\rho_{out} = \frac{\text{Tr}_{i_1, \dots, i_L} \left[\sum_g \gamma_g \left(P_g^{(M)} \rho_{in} \otimes I^{\otimes (M-1)} P_g^{(M)\dagger} \right) \right]}{\sum_g \gamma_g \text{Tr} \left(P_g^{(M)} \rho_{in} \otimes I^{\otimes (M-1)} P_g^{(M)\dagger} \right)}, \quad (3.77)$$

kde γ_g jsou nezáporná a platí $\sum_g \gamma_g = 1$. I v tomto případě lze popsany postup k realizaci unitární evoluce použít.

Kapitola 4

Realizace univerzálních procesů na třech částicích

Tato kapitola je věnována realizaci univerzálních procesů na třech částicích. Jejich částečná klasifikace byla provedena v [5]. Vzhledem k velké algebraické náročnosti této úlohy (třídou všech univerzálních procesů na třech částicích lze parametrizovat 23 reálnými parametry) se podařilo najít explicitní předpis pro vlastní čísla výstupní matice hustoty pouze v několika speciálních případech. Konstrukce univerzálního procesu odvozená v sekci 3.2 umožní nalézt vlastní čísla široké třídy univerzálních procesů.

Ke konstrukci univerzálních procesů na třech částicích lze využít obecného vztahu (3.25),

$$\rho_{out} = \frac{\text{Tr}_{i_1, \dots, i_{M-3}} \left(P^{(M)} \rho_{in} \otimes I^{\otimes (M-1)} P^{(M)\dagger} \right)}{\text{Tr} \left(P^{(M)} \rho_{in} \otimes I^{\otimes (M-1)} P^{(M)\dagger} \right)}, \quad (4.1)$$

kde $M \geq 3$ je přirozené číslo, $\{i_1, \dots, i_{M-3}\} \subset \{1, \dots, M\}$ je množina navzájem různých indexů a $P^{(M)}$ je lineární kombinace projektorů P_i na invariantní podprostory M -částicové reprezentace unitární grupy $U(N)$ s komplexními koeficienty $|\alpha_i| \leq 1$.

Tato třída je obecně velmi široká. Omezíme se proto na analýzu speciálního případu, kdy $M = 3$ a univerzální proces se realizuje výhradně projekcemi. V tomto případě je

$$P^{(3)} = \sigma S + \mu M_1 + \nu M_2 + \alpha A, \quad (4.2)$$

kde S , resp. A , resp. $M_{1(2)}$ jsou projektory na symetrický, resp. antisymetrický, resp. "smíšený" invariantní podprostor a absolutní hodnoty komplexních parametrů σ , α , μ a ν jsou menší než jedna.

Obecný tvar výsledého tříčásticového stavu byl odvozen v předchozí kapitole v rámci klasifikace dvoučásticových univerzálních procesů a je uveden v dodatku A vztahem (A.1). Vlastní čísla této matice, která mohou být obecně nenulová, jsou

$$\begin{aligned}
\lambda_1 &= \frac{1}{\mathcal{N}} |\sigma|^2 \\
\lambda_{2\pm} &= \frac{1}{2\mathcal{N}} \left[\frac{2}{3} |\sigma|^2 + \frac{5}{6} |\mu|^2 + \frac{1}{2} |\nu|^2 \right. \\
&\quad \left. \pm \sqrt{\frac{1}{4} (|\mu|^2 - |\nu|^2)^2 + \frac{4}{9} (|\sigma|^2 - |\mu|^2)^2} \right] \\
\lambda_3 &= \frac{1}{\mathcal{N}} \left(\frac{1}{3} |\sigma|^2 + \frac{1}{6} |\mu|^2 + \frac{1}{2} |\nu|^2 \right) \\
\lambda_4 &= \frac{1}{\mathcal{N}} \left(\frac{1}{3} |\alpha|^2 + \frac{1}{6} |\nu|^2 + \frac{1}{2} |\mu|^2 \right)
\end{aligned} \tag{4.3}$$

s násobností 1 pro λ_1 , $(N-1)$ pro $\lambda_{2\pm}$, $\frac{1}{2}N(N-1)$ pro λ_3 a $\frac{1}{2}(N-1)(N-2)$ pro λ_4 , kde \mathcal{N} je dáno vztahem (A.2). Výsledná matice hustoty ρ_{out}^3 má tedy nejvýše N^2 nenulových a alespoň $N^2(N-1)$ nulových vlastních čísel, které, na rozdíl od vlastních vektorů, závisejí pouze na velikostech parametrů σ , α , μ a ν a nikoli na jejich fázích. Poznamenejme, že závislost vlastních vektorů na fázích způsobuje, že vlastní čísla redukovaných matic hustoty jedno a dvoučásticových podsystémů mohou už na fázi záviset mohou, jak ukazuje následující odstavec.

Symbolem $\rho^{(ij)}$, resp. $\rho^{(i)}$ budeme značit redukovaný dvoučásticový stav obsahující částice i a j , resp. jednočásticový stav obsahující částici i příslušející výsledné tříčásticové matici hustoty ρ . Vlastní čísla redukovaných stavů budeme indexovat stejným způsobem. V dodatku A uvádíme obecné tvary dvoučásticových redukovaných matic hustoty, ze kterých lze odvodit vlastní čísla těchto stavů $\rho^{(12)}$, $\rho^{(23)}$, $\rho^{(13)}$:

$$\begin{aligned}
\lambda_1^{(ij)} &= c_1^{(ij)} \\
\lambda_{2\pm}^{(ij)} &= \left[(c_{21}^{(ij)} + c_{22}^{(ij)}) \pm \sqrt{(c_{21}^{(ij)} - c_{22}^{(ij)})^2 + 4 |c_{23}^{(ij)}|^2} \right], \\
\lambda_3^{(ij)} &= c_3^{(ij)}, \\
\lambda_{4\pm}^{(ij)} &= c_{41}^{(ij)} \pm |c_{42}^{(ij)}|^2,
\end{aligned} \tag{4.4}$$

s násobností 1 pro $\lambda_1^{(ij)}$, $(N-1)$ pro $\lambda_{2\pm}^{(ij)}$ a $\lambda_3^{(ij)}$, $\frac{1}{2}(N-1)(N-2)$ pro $\lambda_{4\pm}^{(ij)}$ a konstanty $c_1^{(ij)}$, resp. $c_{21}^{(ij)}$, resp. $c_{22}^{(ij)}$, resp. $c_{23}^{(ij)}$, resp. $c_3^{(ij)}$, resp. $c_{41}^{(ij)}$, resp. $c_{42}^{(ij)}$

jsou koeficienty u členů $|11\rangle\langle 11|$, resp. $|1a\rangle\langle 1a|$, resp. $|a1\rangle\langle a1|$, resp. $|1a\rangle\langle a1|$, resp. $|aa\rangle\langle aa|$, resp. $|ab\rangle\langle ab|$, resp. $|ab\rangle\langle ba|$ ve výrazech (A.4) pro $i = 1, j = 2$ a (A.3) pro $i = 1, j = 3$. Vlastní čísla $\rho_{out}^{(1)}$ jsou stejná jako pro matici (A.3) jen s tím rozdílem, že se opět změní znaménka parametrů α a ν . Vlastní čísla jednočásticových stavů jsou

$$\begin{aligned}
\lambda_1^{(1)} &= \frac{1}{\mathcal{N}} \left[|\sigma|^2 + (N-1) \left(2 \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + 2 \left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 \right) \right. \\
&\quad \left. + (N-1)(N-2) \left(\left| \frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right|^2 \right) \right], \\
\lambda_2^{(1)} &= \frac{1}{\mathcal{N}} \left[2 \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 + 2 \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + (N-2) \left(2 \left| \frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right|^2 \right. \right. \\
&\quad \left. \left. + \left| \frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right|^2 \right) \right], \\
\lambda_1^{(3)} &= \frac{1}{\mathcal{N}} \left[|\sigma|^2 + (N-1) \left(3 \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 \right) \right. \\
&\quad \left. + 2(N-1)(N-2) \left(\left| \frac{\sigma}{6} - \frac{\mu}{6} \right|^2 + \left| \frac{\alpha}{6} - \frac{\nu}{6} \right|^2 \right) \right], \\
\lambda_2^{(3)} &= \frac{1}{\mathcal{N}} \left[2 \left| \frac{\sigma}{3} + \frac{\mu}{6} \right|^2 + 2 \left| \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 \right. \\
&\quad \left. + 2(N-2) \left(\left| \frac{\sigma}{6} + \frac{\mu}{3} \right|^2 + \left| \frac{\alpha}{6} + \frac{\nu}{3} \right|^2 + \left| \frac{\sigma}{6} - \frac{\mu}{6} \right|^2 + \left| \frac{\alpha}{6} - \frac{\nu}{6} \right|^2 \right) \right] \quad (4.5)
\end{aligned}$$

s násobností 1 pro $\lambda_1^{(1)}$ a $\lambda_1^{(3)}$ a $(N-1)$ pro $\lambda_2^{(1)}$ a $\lambda_2^{(3)}$. Vlastní čísla k matici $\rho^{(2)}$ vypadají stejně jako pro $\rho^{(1)}$, jenom s tím rozdílem, že koeficienty α a ν změni znaménko.

Se znalostí vlastních čísel neredukovaných i redukováných stavů můžeme principiálně vyšetřovat mnoho vlastností tříčásticových univerzálních procesů (4.1) pro $M = 3$. Výstupní matice hustoty však závisí obecně na šesti reálných parametrech¹ a vztahy (4.3)-(4.5) jsou velmi komplikované. Omezíme se proto na podtřídu, jejímiž hraničními případy jsou fyzikálně zajímavé procesy: optimální univerzální kopírování jedné částice na tři a proces realizující pouze antisymetrické stavy, tj.

$$P^{(3)} = \sigma S + \alpha A. \quad (4.6)$$

¹Jak bylo ukázáno v kapitole 3, výsledná matice hustoty je invariantní vůči změně globální fáze a násobení reálným faktorem koeficientů σ, α, μ a ν . Viz sekce 3.2.

Potom platí

$$\mu = \nu = 0, \quad (4.7)$$

$$\rho_{out} = \frac{6(\sigma S + \alpha A) \rho_{in} \otimes I^{\otimes 2} (\bar{\sigma} S + \bar{\alpha} A)}{(N+1)(N+2)|\sigma|^2 + (N-1)(N-2)|\alpha|^2}. \quad (4.8)$$

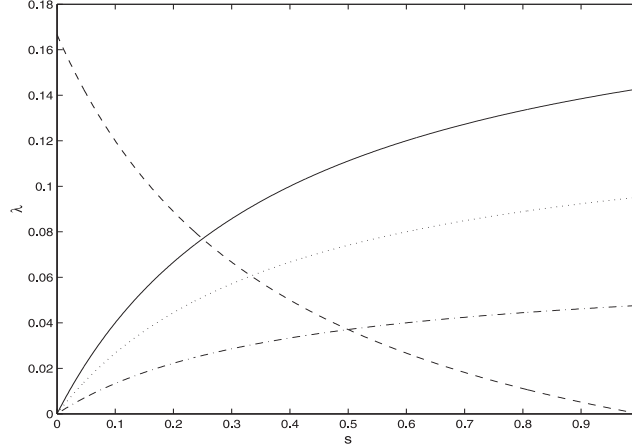
Všechny vlastnosti, které budeme zkoumat, budou záviset pouze na vlastních číslech (4.3)-(4.5), které v tomto případě závisí pouze na kvadrátech absolutních hodnot koeficientů σ a α , a proto, i když se jedná o podtřídou efektivně dvouparametrickou, můžeme volit následující parametrizaci

$$s = |\sigma|^2, \quad |\alpha|^2 = 1 - |\sigma|^2 = 1 - s. \quad (4.9)$$

Navíc platí

$$\rho_{out}^{(12)} = \rho_{out}^{(23)} = \rho_{out}^{(13)}, \quad \rho_{out}^{(1)} = \rho_{out}^{(2)} = \rho_{out}^{(3)}. \quad (4.10)$$

Pomocí nenulových vlastních čísel matice ρ_{out} , jejichž průběh v závislosti na parametru s znázorňuje obrázek 4.1, můžeme spočítat von Neumannovu entropii výsledného stavu podle vztahu²



Obrázek 4.1: Průběh nenulových vlastních čísel λ_1 (plná čára), λ_{2+} (tečkovaná čára), λ_3 (čerchovaná čára) a λ_4 (čárkovaná čára) matice hustoty ρ_{out} pro $N = 5$ v závislosti na parametru s .

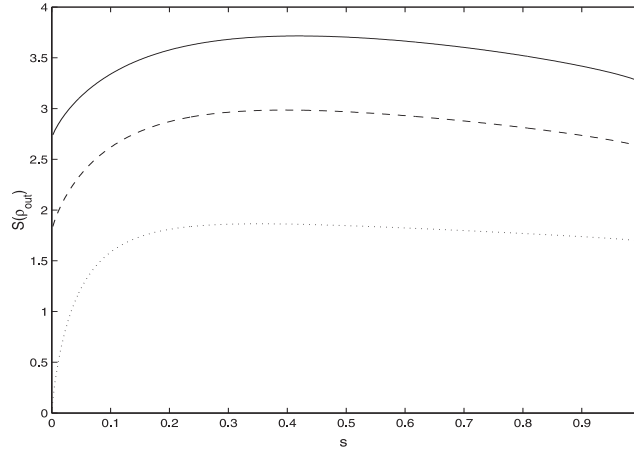
$$S(\rho_{out}) = - \sum_{\lambda_i} \mu(\lambda_i) \lambda_i \ln \lambda_i, \quad (4.11)$$

²Ve standardní definici je navíc suma násobena Boltzmanovou konstantou k .

kde suma probíhá přes všechna různá vlastní čísla matice ρ_{out} a $\mu(\lambda_i)$ je násobnost vlastního čísla λ_i . Explicitní výrazy pro entropie zde pro jejich objemnost a nepřehlednost uvádět nebudeme, jde o pouhé dosazení příslušných vlastních čísel do definičního vztahu (4.11). Entropie $S(\rho_{out})$ je, jako funkce s , konkávní a nabývá minima vždy pro $s = 0$. Hodnota minima je

$$S_{min}(\rho_{out}) = \ln \left(\frac{(N-1)(N-2)}{2} \right). \quad (4.12)$$

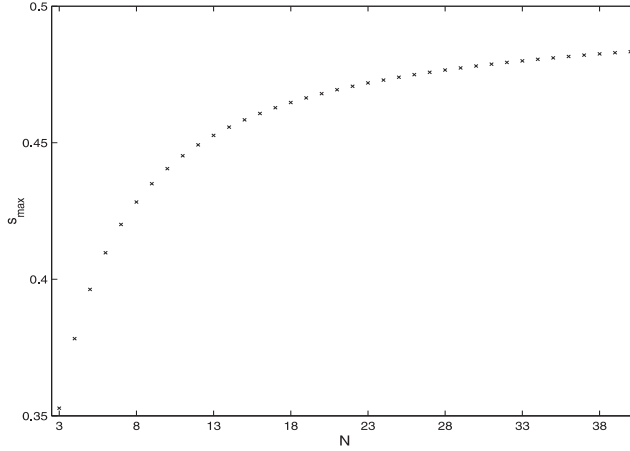
Pro $s = 1$ a N jdoucí do nekonečna se entropie shora blíží k $S_{min}(\rho_{out})$.



Obrázek 4.2: Průběh von Neumannovy entropie stavu ρ_{out} v závislosti na parametru s pro $N = 7$ (plná čára), $N = 5$ (čárkovaná čára), $N = 3$ (tečkovaná čára).

Entropie matice hustoty ρ_{out} je rovna nule, a výsledný stav je tedy čistý, pouze v případě $s = 0$ a $N = 3$. Tento stav se někdy nazývá Slaterův a hraje důležitou roli v mnoha aplikacích kvantové informace, např. kvantové sdílení a distribuce šifrovacího klíče nebo porovnávání kvantových stavů [19]. Pro všechny ostatní konfigurace získáváme stavy smíšené, viz. obrázek 4.2. Hodnota parametru s , pro kterou univerzální proces (4.8) realizuje maximálně smíšené stavy, je dána algebraicko-logaritmickou rovnicí, jejíž řešení obecně nelze vyjádřit v analytickém tvaru, a jsme proto odkázáni na numerické metody. Závislost polohy maxima na dimenzi N znázorňuje obrázek 4.3. Limitní hodnota s_{max} pro N jdoucí do nekonečna je rovna jedné polovině.

Stejným způsobem můžeme analyzovat dvoučásticové redukované matice hustoty $\rho_{out}^{(ij)}$. Von Neumannova entropie těchto stavů je nemonotonní, viz obrázek 4.4, a nabývá minima v bodě $s = 0$ pro $N \in \{3, 4\}$ a pro $N \geq 5$



Obrázek 4.3: Hodnota parametru s , pro kterou je entropie stavu ρ_{out} maximální, v závislosti na dimenzi N .

je minimální entropie dosažena při $s = 1$. Všechny výstupní dvoučásticové stavy jsou smíšené, neboť platí

$$\forall s \in \langle 0, 1 \rangle, \quad \forall N \geq 3 \quad S(\rho_{out}^{(ij)}) > 0. \quad (4.13)$$

Entropie jednočásticových redukovaných stavů, obrázek 4.5, je pro každé N klesající, ale vždy nenulová funkce, a proto i všechny jednočásticové redukované výstupní stavy v této třídě budou smíšené.

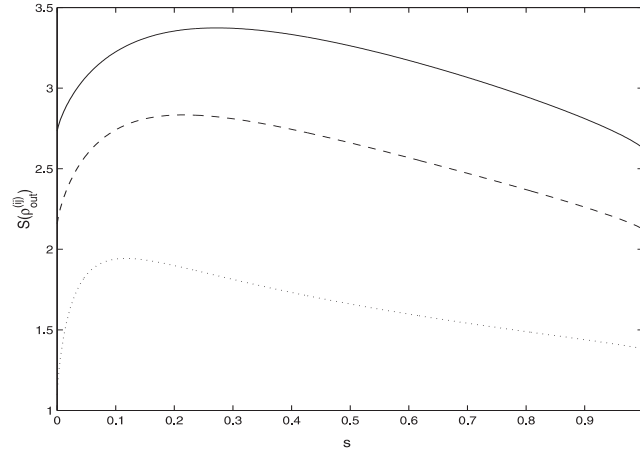
Pomocí entropie stavů ρ_{out} , $\rho_{out}^{(ij)}$ a $\rho_{out}^{(i)}$ můžeme spočítat index korelace, který vyjadřuje míru korelací mezi jednotlivými podsystémy [20]. Tato veličina je definována následovně

$$I_c^{(AB)} = S(\rho_A) + S(\rho_B) - S(\rho_{AB}), \quad (4.14)$$

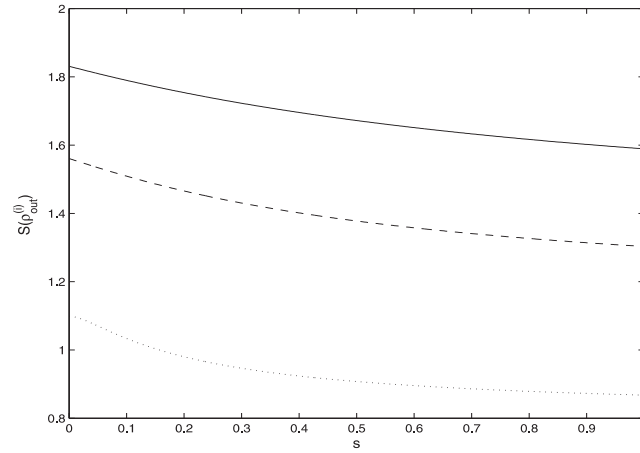
kde ρ_{AB} je matice hustoty složeného systému, ρ_A , resp. ρ_B je redukovaný stav na podsystému A , resp. B . Průběh míry korelací mezi jednočásticovým a dvoučásticovým redukovaným stavem $I_c^{(ij)(k)}$ v závislosti na parametru s demonstruje obrázek 4.6. Univerzální proces, který realizuje v této podtřídě maximálně korelované stavy jedno a dvoučásticového podsystému odpovídá pro všechny dimenze parametru $s = 0$. Index korelace je pro všechna N klesající funkce, ale se zvětšující se dimenzí vliv parametru s na míru korelací klesá a limitně platí

$$\forall s \in \langle 0, 1 \rangle \quad \lim_{N \rightarrow \infty} I_c^{(ij)(k)} = 2 \ln\left(\frac{3}{\sqrt[3]{2}}\right). \quad (4.15)$$

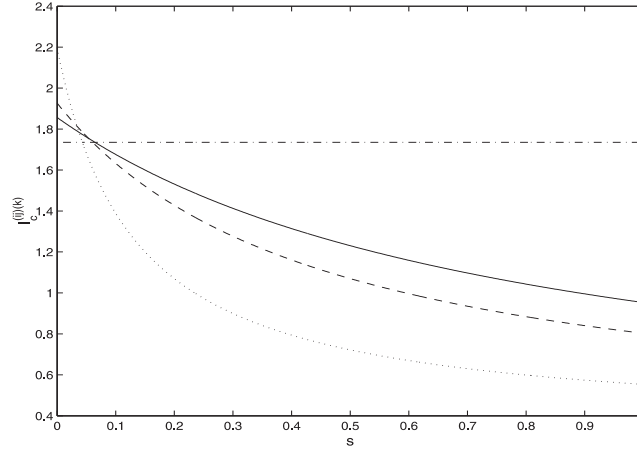
Korelace mezi jednočásticovými redukovanými stavy, obrázek 4.7, vykazuje



Obrázek 4.4: Průběh von Neumannovy entropie dvoučásticového redukovaného stavu $\rho_{out}^{(ij)}$ v závislosti na parametru s pro $N = 7$ (plná čára), $N = 5$ (čárkovaná čára), $N = 3$ (tečkovaná čára).



Obrázek 4.5: Průběh von Neumannovy entropie jednočásticového redukovaného stavu $\rho_{out}^{(i)}$ v závislosti na parametru s pro $N = 7$ (plná čára), $N = 5$ (čárkovaná čára), $N = 3$ (tečkovaná čára).

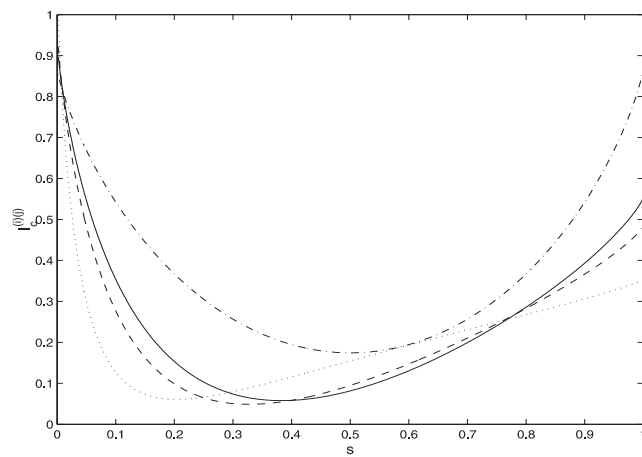


Obrázek 4.6: Průběh indexu korelace mezi redukovanými stavy $\rho_{out}^{(ij)}$ a $\rho_{out}^{(k)}$ v závislosti na parametru s pro $N = 7$ (plná čára), $N = 5$ (čárkovaná čára), $N = 3$ (tečkovaná čára) a $N \rightarrow \infty$ (čerchovaná čára).

stejně jako v předchozím případě maximum pro $s = 0$. S rostoucím N se poloha parametru s , při kterém je dosaženo minimálních korelací, monotonně zvyšuje a konverguje k jedné polovině. V limitě platí

$$\forall s \in \langle 0, 1 \rangle \quad \lim_{N \rightarrow \infty} I_c^{(i)(j)} = (1 - s) \ln(1 - s) + s \ln s + \ln \frac{3}{\sqrt[3]{2}}. \quad (4.16)$$

Konstrukce univerzálních procesů na třech částicích pomocí vztahu (4.1) dovoluje realizovat širokou třídu kovariantních zobrazení. Jejich unitární evoluční operátor lze získat stejnou kanonickou konstrukcí, která byla popsána v sekci 3.4. Zůstává však otázkou, zda jsme schopni tímto způsobem realizovat všechny úplně pozitivní tříčásticové univerzální procesy, neboť jejich klasifikace není dosud zcela kompletní.



Obrázek 4.7: Průběh indexu korelace mezi redukovanými stavy $\rho_{out}^{(i)}$ a $\rho_{out}^{(j)}$ v závislosti na parametru s pro $N = 7$ (plná čára), $N = 5$ (čárkovaná čára), $N = 3$ (tečkovaná čára) a $N \rightarrow \infty$ (čerchovaná čára).

Závěr

V této diplomové práci jsme se zabývali implementací univerzálních procesů z jedné částice na M . Předpokládali jsme částice stejné, konečné dimenze N . Zaměřili jsme se speciálně na možnosti konstrukce Krausových operátorů univerzálních procesů pomocí projektorů a odvozené postupy jsme demonstrovali na podtřídách dvou a tříčásticových procesů.

Nejprve jsme věnovali pozornost procesům na dvou částicích realizovaných koherentní kombinací projektorů na symetrický a antisymetrický podprostor dvoučásticového Hilbertova prostoru. Odvodili jsme obecný parametrický tvar výsledné matice hustoty, (3.8), a dokázali, že takto získaný proces splňuje podmínku kovariance, a proto je univerzální. Výsledná matice hustoty je efektivně závislá na jednom komplexním parametru. Ukázali jsme, jak tyto procesy souvisí s klasifikací univerzálních procesů na dvou částicích provedené v [4], a nekoherentní superpozicí dvou vhodně zvolených procesů tohoto typu jsme zkonstruovali Krausovy operátory pro všechny procesy, pro které v této klasifikaci platí $p_3 = p_4 = 0$, viz. (2.19).

Postup realizace univerzálních procesů projektory jsme pomocí Schurova lemmantu zobecnili a uvedli ansatz (3.25), ve kterém je univerzální proces na M částicích konstruován pomocí koherentní kombinace projektorů na invariantní podprostory $(M + L)$ -částicové reducibilní reprezentace jednočásticové unitární grupy $U(N)$ a L -násobnou aplikací operace částečné stopy.

Ansatz (3.25) spolu s nekoherentní superpozicí takto získaných procesů dovoluje konstrukci široké podtřídy univerzálních procesů na libovolném počtu částic. Nevýhodou tohoto postupu je, že pokud nemáme k dispozici úplnou klasifikaci univerzálních procesů na daném počtu částic, neumíme zatím říci, o jak velkou podtřídu se jedná. Proto jsme se v dalším zkoumání omezili na dvou a tříčásticové procesy, kde je alespoň částečná klasifikace známa. Naopak výhodou uvedené konstrukce je možnost jejího přímočarého zobecnění na realizaci univerzálních procesů z L na M částic.

Pro podtřídu univerzálních procesů na dvou částicích, které lze realizovat projektory na tříčásticové stavy a jednou operací částečné stopy, jsme odvodili obecné tvary výstupních matic hustoty (A.3) a (A.4), které jsou

efektivně závislé na třech komplexních parametrech. V této třídě jsme identifikovali proces optimálního kopírování z jedné částice na dvě a ukázali, že zde leží část jednoparametrické třídy univerzálních provazovacích procesů pro hodnoty parametru p_4 z intervalu $\langle 0, \frac{N}{2(N+1)} \rangle$. Pro tyto procesy jsme blíže analyzovaly množinu přípustných koeficientů, které parametrizují koherentní kombinaci projektorů, a našli jejich hodnoty, pro které je pravděpodobnost realizace procesu při kanonické konstrukci unitární evoluce maximální.

Nakonec jsme se věnovali podtřídě univerzálních procesů na třech částicích, které lze realizovat pomocí (3.25) pouze projektory na tříčásticové stavy. Odvodili jsme obecný tvar výstupní matice hustoty, která je efektivně závislá na třech komplexních parametrech, její vlastní čísla a vlastní čísla jedno a dvoučásticových redukovaných stavů. Se znalostí spekter těchto matic jsme se zaměřili blíže na vlastnosti podtřídy realizované kombinací projektorů na symetrický a antisymetrický tříčásticový podprostor. V tomto případě jsou všechny dvoučásticové, resp. jednočásticové redukované stavy stejné a jejich spektra závisí pouze na absolutních velikostech parametrů, nikoli na jejich fázích. Analyzovali jsme chování entropie výsledných redukovaných a neredukovaných stavů a indexu korelace mezi jednotlivými podsystémy.

Univerzální procesy hrají v kvantové teorii informace důležitou roli, neboť dovolují optimálně aproximovat mnoho procesů, které jsou kvantové fyzice zapovězené. Studium jejich vlastností a možností realizace má tedy velký význam pro budoucí aplikaci kvantových algoritmů.

Závěrem bych chtěl velmi poděkovat svému školiteli Prof. Ing. Igoru Jexovi, DrSc. za pečlivé vedení této diplomové práce. Můj dík patří také Ing. Jaroslavu Novotnému za mnoho inspirativních diskusí.

Dodatek A

Výstupní stavy univerzálního procesu na třech částicích realizovaného projektory

A.1 Tříčásticová matice hustoty

Výstupní matici hustoty ρ_{out}^3 univerzálního procesu na třech částicích realizovanou projektory na invariantní podprostory tříčásticové reprezentace jednočásticové unitární grupy získáme dosazením (3.39) až (3.41) do (3.38) a její obecný tvar je

$$\begin{aligned}\rho_{out}^3 &= \frac{1}{\mathcal{N}} |\sigma|^2 |111\rangle\langle 111| + \frac{1}{\mathcal{N}} \sum_{a \neq 1} \left\{ \left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 |1aa\rangle\langle 1aa| \right. \\ &+ \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 |aa1\rangle\langle aa1| + \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) |1aa\rangle\langle aa1| \\ &+ \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{2} \right) \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) |aa1\rangle\langle 1aa| + \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 |a1a\rangle\langle a1a| \\ &+ \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{2} \right) |1aa\rangle\langle a1a| + \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{2} \right) \times \\ &\times \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) |a1a\rangle\langle 1aa| + \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{2} \right) |aa1\rangle\langle a1a| \\ &+ \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) |a1a\rangle\langle aa1| + \left[\left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right] \times \\ &\times |11a\rangle\langle 11a| + \left[\left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 \right] |1a1\rangle\langle 1a1|\end{aligned}$$

$$\begin{aligned}
& + \left[\left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 \right] |a11\rangle\langle a11| + \left[\left(\frac{\sigma}{3} + \frac{2\mu}{3} \right) \times \right. \\
& \times \left. \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) + \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{2} \right) \right] |11a\rangle\langle 1a1| \\
& + \left[\left(\frac{\bar{\sigma}}{3} + \frac{2\bar{\mu}}{3} \right) \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) + \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) \right] |1a1\rangle\langle 11a| \\
& + \left[\left(\frac{\sigma}{3} + \frac{2\mu}{3} \right) \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) + \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{2} \right) \right] |11a\rangle\langle a11| \\
& + \left[\left(\frac{\bar{\sigma}}{3} + \frac{2\bar{\mu}}{3} \right) \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) + \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) \right] |a11\rangle\langle 11a| \\
& + \left[\left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{2} \right) \right] |1a1\rangle\langle a11| \\
& + \left[\left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{2} \right) \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) \right] |a11\rangle\langle 1a1| \Big\} \\
& + \frac{1}{\mathcal{N}} \sum_{1 \neq a \neq b \neq 1} \left\{ [|1ab\rangle \left(\frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right) + |1ba\rangle \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \right. \\
& + |ab1\rangle \left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) + |a1b\rangle \left(\frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right) \\
& + |b1a\rangle \left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) + |ba1\rangle \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \Big] \times \\
& \times \left[\langle 1ab| \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} + \frac{\bar{\mu}}{3} + \frac{\bar{\nu}}{3} \right) + \langle 1ba| \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{6} \right) \right. \\
& + \langle ab1| \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{6} \right) + \langle a1b| \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} + \frac{\bar{\mu}}{3} - \frac{\bar{\nu}}{3} \right) \\
& + \left. \left. \langle b1a| \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{6} \right) + \langle ba1| \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{6} \right) \right] \right\}, \quad (\text{A.1})
\end{aligned}$$

kde \mathcal{N} má tvar

$$\begin{aligned}
\mathcal{N} & = \frac{1}{6} |\sigma|^2 (N+1)(N+2) + \frac{1}{3} (|\mu|^2 + |\nu|^2) (N^2 - 1) \\
& + \frac{1}{6} |\alpha|^2 (N-1)(N-2). \quad (\text{A.2})
\end{aligned}$$

A.2 Dvoučasticové redukováná matice hustoty

Provedením operace částečné stopy přes jednu ze tří částic výstupní matice hustoty ρ_{out}^3 , danou vztahem (A.1), získáme tři třídy výstupních matic hustoty univerzálních procesů na dvou částicích. Vyloučení druhé, resp. třetí

částice vede na matice hustoty $\rho_{out}^{(2)}$, resp. $\rho_{out}^{(3)}$. Vyloučením první částice dostaneme stejnou matici jako $\rho_{out}^{(2)}$ jen s tím rozdílem, že parametry α a ν změni znaménko.

$$\begin{aligned}
\rho_{out}^{(2)} &= \frac{1}{\mathcal{N}} \text{Tr}_2 P_3 \rho_{in} \otimes I_2 P_3^\dagger \\
&= \frac{1}{\mathcal{N}} \left\{ \left[|\sigma|^2 + (N-1) \left(\left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + \left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right| \right) \right] |11\rangle\langle 11| \right. \\
&+ \sum_{a \neq 1} \left\{ \left[\left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + (N-2) \times \right. \right. \\
&\times \left. \left. \left(\left| \frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right|^2 \right) \right] |1a\rangle\langle 1a| \right. \\
&+ \left. \left[\left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 + 2 \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + (N-2) \left(\left| \frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right|^2 \right. \right. \\
&+ \left. \left. \left| \frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right|^2 \right) \right] |a1\rangle\langle a1| + \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 |aa\rangle\langle aa| \\
&+ \left[\left(\frac{2\sigma}{3} + \frac{5\mu}{6} + \frac{\nu}{2} \right) \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) + \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{2} \right) \right. \\
&+ (N-2) \left(\left(\frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right) \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{6} \right) \right. \\
&+ \left. \left. \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{6} \right) \right) \right] |1a\rangle\langle a1| \\
&+ \left[\left(\frac{2\bar{\sigma}}{3} + \frac{5\bar{\mu}}{6} + \frac{\bar{\nu}}{2} \right) \left(\frac{\sigma}{3} - \frac{\mu}{3} \right) + \left(\frac{\bar{\sigma}}{3} - \frac{\bar{\mu}}{3} \right) \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) \right. \\
&+ (N-2) \left(\left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} + \frac{\bar{\mu}}{3} + \frac{\bar{\nu}}{3} \right) \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \right. \\
&+ \left. \left. \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{6} \right) \right) \right] |a1\rangle\langle 1a| \\
&+ \sum_{1 \neq a \neq b \neq 1} \left\{ \left[\left| \frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right|^2 \right] |ab\rangle\langle ab| \right. \\
&+ \left. 2\text{Re} \left[\left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} + \frac{\bar{\mu}}{3} - \frac{\bar{\nu}}{3} \right) \right] |ab\rangle\langle ba| \right\}, \quad (\text{A.3})
\end{aligned}$$

$$\begin{aligned}
\rho_{out}^{(3)} &= \frac{1}{\mathcal{N}} \text{Tr}_3 P_3 \rho_{in} \otimes I_2 P_3^\dagger \\
&= \frac{1}{\mathcal{N}} \left\{ \left[|\sigma|^2 + (N-1) \left(\left| \frac{\sigma}{3} + \frac{2\mu}{3} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right) \right] |11\rangle\langle 11| \right. \\
&+ \sum_{a \neq 1} \left\{ \left[2 \left| \frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 + (N-2) \left(\left| \frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right|^2 \right. \right. \\
&+ \left. \left. \left| \frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right|^2 \right) \right] |1a\rangle\langle 1a| + \left[2 \left| \frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right|^2 + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right. \right. \\
&+ \left. \left. (N-2) \left(\left| \frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right|^2 \right) \right] |a1\rangle\langle a1| \right. \\
&+ \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 |aa\rangle\langle aa| + \left[2 \left(\frac{\sigma}{3} + \frac{\mu}{6} + \frac{\nu}{2} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{2} \right) + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right. \\
&+ \left. (N-2) \left(\left(\frac{\sigma}{6} + \frac{\alpha}{6} + \frac{\mu}{3} + \frac{\nu}{3} \right) \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} + \frac{\bar{\mu}}{3} - \frac{\bar{\nu}}{3} \right) \right. \right. \\
&+ \left. \left. \left(\frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right) \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} - \frac{\bar{\nu}}{6} \right) \right) \right] |1a\rangle\langle a1| \\
&+ \left[2 \left(\frac{\sigma}{3} + \frac{\mu}{6} - \frac{\nu}{2} \right) \left(\frac{\bar{\sigma}}{3} + \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{2} \right) + \left| \frac{\sigma}{3} - \frac{\mu}{3} \right|^2 \right. \\
&+ \left. (N-2) \left(\left(\frac{\sigma}{6} - \frac{\alpha}{6} + \frac{\mu}{3} - \frac{\nu}{3} \right) \left(\frac{\bar{\sigma}}{6} + \frac{\bar{\alpha}}{6} + \frac{\bar{\mu}}{3} + \frac{\bar{\nu}}{3} \right) \right. \right. \\
&+ \left. \left. \left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{6} \right) \right) \right] |a1\rangle\langle 1a| \Big\} \\
&+ \sum_{1 \neq a \neq b \neq 1} \left\{ \left[\left| \frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right|^2 + \left| \frac{\sigma}{6} - \frac{\alpha}{6} - \frac{\mu}{6} + \frac{\nu}{6} \right|^2 \right] |ab\rangle\langle ab| \right. \\
&+ \left. 2\text{Re} \left[\left(\frac{\sigma}{6} + \frac{\alpha}{6} - \frac{\mu}{6} - \frac{\nu}{6} \right) \left(\frac{\bar{\sigma}}{6} - \frac{\bar{\alpha}}{6} - \frac{\bar{\mu}}{6} + \frac{\bar{\nu}}{6} \right) \right] |ab\rangle\langle ba| \right\}, \quad (\text{A.4})
\end{aligned}$$

přičemž \mathcal{N} lze vyjádřit

$$\begin{aligned}
\mathcal{N} &= \frac{1}{6} |\sigma|^2 (N+1)(N+2) + \frac{1}{3} (|\mu|^2 + |\nu|^2) (N^2 - 1) \\
&+ \frac{1}{6} |\alpha|^2 (N-1)(N-2). \quad (\text{A.5})
\end{aligned}$$

Literatura

- [1] P. W. Shor (1997), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing* 26, 1484.
- [2] W. K. Wootters, W. H. Zurek (1982), A Single Quantum Cannot Be Cloned, *Nature* 299, 802.
- [3] R. F. Werner, Optimal Cloning of Pure States (1998), *Phys. Rev. A* 58, 1827.
- [4] G. Alber, A. Delgado, I. Jex (2001), Optimal Two-Particle Entanglement by Universal Quantum Processes, *Quantum Information and Computation* 1, 33.
- [5] M. Štefaňák (2003), Many Particle Universal Processes, Diploma thesis, FJFI.
- [6] M. A. Nielsen, I. L. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge.
- [7] K. Kraus (1983), *States, Effects, Operations: Fundamental Notions of Quantum Theory*, Springer-Verlag, Berlin.
- [8] H. Bechmann-Pasquinucci, N. Gisin (1999), Incoherent and Coherent Eavesdropping in the Six-state Protocol of Quantum Cryptography, *Phys. Rev. A* 59, 4238.
- [9] V. Bužek, M. Hillery, R. F. Werner (1999), Optimal Manipulations with Qubits: Universal NOT Gate, *Phys. Rev. A* 60, R2626.
- [10] C. S. Niu, R. B. Griffiths (1998), Optimal Copying of One Quantum Bit, *Phys. Rev. A* 58, 4377.
- [11] N. Cerf (2000), Pauli Cloning of a Quantum Bit, *Phys. Rev. Lett.* 84, 4497.

- [12] M. Lewenstein, A. Sanpera (1998), Separability and Entanglement of Composite Quantum Systems, *Phys. Rev. Lett.* 80, 2261.
- [13] G. Vidal, R. F. Werner (2002), A Computable Measure of Entanglement, *Phys. Rev. A*, 65, 032314.
- [14] A. Peres (1996), Separability Criterion for Density Matrices, *Phys. Rev. Lett.* 77, 1413.
- [15] M. Horodecki, P. Horodecki, R. Horodecki (1996), Separability of Mixed States: Necessary and Sufficient Conditions, *Phys. Lett. A* 223, 1.
- [16] W. Fulton, J. Harris (1991), *Representation Theory, A First Course*, Springer, New York.
- [17] J. Q. Chen, J. Ping, F. Wang (2002), *Group Representation Theory for Physicist*, World Scientific, Singapore.
- [18] Z. Q. Ma, X. Y. Gu (2004), *Problems & Solutions in Group Theory for Physicist*, World Scientific, Singapore.
- [19] I. Jex, G. Alber, S. M. Barnett, A. Delgado (2003), Antisymmetric Multi-partite Quantum States and Their Applications, *Fortschritte der Physik*, 51, 172.
- [20] S. M. Barnett, S. J. D. Phoenix (1989), Entropy As a Measure of Optical Correlation, *Phys. Rev. A* 40, 2404.
- [21] A. Peres (1995), *Quantum Theory: Concepts and Methods*, Kluwer Academic Pub., Dordrecht.