České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

Výzkumný úkol

Vojtěch Košťák

České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

Univerzální procesy v kvantové informaci

Vojtěch Košťák

Katedra fyziky
Akademický rok: 2003/2004
Školitel: Prof. Doc. Ing. Igor Jex, DrSc.

V Praze dne 15. listopadu 2004

Obsah

Úvod

Současně s vývojem teorie a experimentální praxe kvantové fyziky vznikl i zcela nový obor kvantové informatiky. Možnost superpozice a provázání kvantových stavů, které jsou přímými důsledky linearity kvantové mechaniky, dovoluje vyvinout algoritmy, které řeší některé problémy, jejichž složitost v klasické informatice vyžaduje exponenciální nároky na prostředky nebo čas, pouze v polynomiálním čase. Mezi takové problémy patří například faktorizace velkých čísel na prvočísla. Exponenciální časová náročnost řešení této úlohy v klasickém světě využívá například kryptografie a téměř každému z nás dnes tento fakt chrání informace či soukromí. V roce 1996 publikoval P. Shor algoritmus [1], který s využitím principů kvantové teorie řeší faktorizaci s polynomiální složitostí.

Linearita, stejný prvek, který obohacuje možnosti kvantové informatiky, na ní uvaluje i přísná omezení, která znemožňují realizaci některých, klasické informatice naprosto vlastních, procesů. Jedním z nich je například vytvoření přesné kopie libovolného kvantového stavu [2]. Musíme se proto spokojit s procesy produkující nedokonalé kopie, popsané např. Wernerem v [3]. Jeho klonovací proces patří do třídy tzv. univerzálních procesů, které lze charakterizovat vlastností, že působí na každý stav v jistém smyslu stejně. Pro procesy tohoto typu, přenášející čistý stav jedné částice na M-částicový stav, lze přeformulovat tuto vlastnost pomocí kovariantní podmínky. Mimo to musí univerzální proces splňovat i další podmínky kladené na realizovatelný kvantový proces. Souhrnná klasifikace univerzálních kvantových procesů na dvou částicích byla podána v práci [4], kde bylo mimo jiné ukázáno, že každý takový proces je charakterizován pěti reálnými parametry.

Cílem této práce je seznámit s klasifikací třídy univerzálních procesů provedené v [4], formalismem a teorií kvantových operací a literaturou související s realizací univerzálních procesů. Speciálně je přihlédnuto k procesům klonování jedné částice na dvě a univerzální provázání dvou částic, pro které je popsána unitární realizace a odvozena její dekompozice na rotace ve dvourozměrných podprostorech. Chceme-li experimentálně realizovat určitou operaci je třeba nejprve najít kvantový proces, který ji realizuje, poté zkon-

struovat jeho unitární realizaci a nakonec najít experimentální uspořádání odpovídající danému unitárnímu operátoru. Právě poslední bod je motivací k hledání dekompozice tohoto typu.

Text je uspořádán následovně: V první kapitole je popsán formalismus kvantových operací [5], jakožto nejobecnějších procesů, které lze v rámci kvantové teorie realizovat, a jejich Krausova reprezentace, která je užitečná mimo jiné k tomu, že s její znalostí lze pro danou kvantovou operaci zkonstruovat její unitární realizace. V druhé kapitole je stručně popsána klasifikace univerzálních procesů na dvou částicích, jak byla podána v práci [4]. Ve třetí kapitole je nejprve popsán optimální proces kopírování z jedné částice na dvě a následně odvozena dekompozice jeho realizace. Dále je na základě [4] odvozena unitární realizace a její dekompozice jednoho z univerzálních procesů provázání dvou částic.

Kapitola 1

Kvantové operace a Krausova representace

V této kapitole definujeme třídu nejobecnějších zobrazení mezi maticemi hustoty, které jsou v rámci kvantové mechaniky přípustné. Zavedeme pojem kvantové operace a popíšeme její tvar v tzv. Krausově reprezentaci. Na konci kapitoly uvedeme několik základních kvantových operací na jednom qubitu a jejich znázornění na Blochově sféře.

1.1 Kvantové operace

Časový vývoj operátoru hustoty uzavřeného kvantového systému je popsán Liouvillovou rovnicí

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

Vývoj na časovém intervalu J, kdy se systém volně vyvíjel, je pak ekvivalentní působení unitárního propagátoru $U(t, s)$ na matici hustoty ρ, tedy platí

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

Unitární vývoj kvantových systémů je ale z několika důvodů pro kvantovou informatiku nedostačující. Za prvé v praxi lze jen těžko najít systém, který se svým okolím vůbec neinteraguje. Pokud chceme 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 okolním prostředím a jeho vývoj, chápeme-li ho jako vývoj podsystému celého systému okolí-nosič, již nemusí být unitární. Za druhé, pokud bychom se omezili v kvantových algoritmech pouze na unitární vývoj, třída úloh, která

by byla tímto způsobem realizovatelná, by se velmi zúžila. Lze totiž využít nevýhody prvního případu v náš prospěch. Náš systém můžeme rozšířit o další, tzv. ancillu, a na rozšířeném systému realizovat vhodnou unitární transformaci. Pokud výsledný stav zprůměrujeme přes ancillu, tj. provedeme operaci částečné stopy přes podsystém příslušející ancille, transformace realizovaná na našem původním systému již nemusí být unitární. Za třetí, v realizaci kvantových algoritmů se velmi často vyskytuje proces projektivního měření, které zcela jistě není unitární.

Chceme najít nejobecnější tvar zobrazení $\mathcal{E}$, kvantové operace, která převede vstupní stav ρ_{in} na výstupní $\rho_{out} = \mathcal{E}(\rho_{in})$, přičemž netrváme na rovnosti dimenzí Hilbertových prostorů vstupního a výstupního systému. Fakt, že $\mathcal{E}$ má zobrazit matici hustoty na jinou matici hustoty implikuje podmínky

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

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

Pokud připustíme i nedeterministickou dynamiku systému, kterou je například proces měření, lze podmínku zeslabit na

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

Výsledek můžeme interpretovat tak, že proces $\mathcal{E}$ nastane s pravděpodobností $\mathrm{Tr}\mathcal{E}(\rho_{in})$ a konečný stav je $\rho_{out} = \frac{\mathcal{E}(\rho_{in})}{\mathrm{Tr}\mathcal{E}(\rho_{in})}$.

Pokud má být definice kvantová operace konzistentní se statistickou interpretací matice hustoty, měla by být další podmínkou na kvantovou operaci linearita vůči vstupnímu stavu. Je-li vstupní stav ρ_{in}^0 s pravděpodobností p a ρ_{in}^1 s pravděpodobností $(1-p)$, měl by výstupní stav být kombinací $\mathcal{E}(\rho_{in}^0)$ a $\mathcal{E}(\rho_{in}^1)$ se stejnými pravděpodobnostmi. Shrňme tedy

$$\mathcal{E} \text{ lineární vůči vstupu: } \mathcal{E}(\sum_i p_i \rho_i) = \mathcal{E}(\rho_{in}) = \sum_i p_i \mathcal{E}(\rho_i). \tag{1.6}$$

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

$$\mathcal{E} \text{ úplně pozitivní: } \rho_{AB} \geq 0 \Rightarrow (I \otimes \mathcal{E})\rho_{AB} \geq 0, , \tag{1.7}$$

kde ρ_{AB} je matice hustoty na libovolném rozšířeném systému AB a I je identická operace na podsystému B. Tato podmínka plyne z přirozeného požadavku, že pokud je námi zkoumaný systém A součástí nějakého většího AB, nesmí kvantová operace $\mathcal{E}$ převést fyzikální stav celého systému AB na stav nefyzikální.

Nyní se podívejme na vývoj neuzavřeného kvantového systému. Přirozenou cestou, jak zahrnout do modelu interakci sledovaného systému (hlavní systém) s okolím, je nahlížet na otevřený systém spolu s okolím jako na jeden systém uzavřený, podléhající unitární interakci U. Předpokládejme, prozatím, že celkový systém je na vstupu ve faktorizovaném stavu $\rho_S \otimes \rho_E$. Po transformaci je stav hlavního systému dán rovnicí

$$\mathcal{E}(\rho_S) = \mathrm{Tr}_E \left[U(\rho_S \otimes \rho_E) U^\dagger \right]. \tag{1.8}$$

Úpravou rovnice (1.8) lze dojít k jiné, elegantní formě vyjádření operace $\mathcal{E}$ známé jako Krausova reprezentace [5], [7].

Nechť $|e_k\rangle$ je ortonormální báze konečněrozměrného Hilbertova prostoru okolí a $\rho_E = |e_0\rangle\langle e_0|$ je jeho počáteční stav. Předpoklad čistoty stavu nijak neubírá postupu na obecnosti, neboť vždy lze Hilbertův prostor prostředí rozšířit tak, aby počáteční smíšený stav byl v rozšířeném systému čistý. Rovnici (1.8) lze přepsat do tvaru

$$\mathcal{E}(\rho_S) = \sum_k \langle e_k | U \left[\rho_S \otimes |e_0\rangle\langle e_0| \right] U^\dagger | e_k \rangle = \sum_k E_k \rho_S E_k^\dagger, \tag{1.9}$$

kde $E_k = \langle e_k | U | e_0 \rangle$ je již operátor na Hilbertově prostoru hlavního systému. Operátory E_k se nazývají operačními či Krausovy elementy nebo též Krausovy operátory operace $\mathcal{E}$. Z rovnice (1.9) plyne $\sum E E^\dagger = I$ a připustíme-li nedeterministickou dynamiku, lze tuto podmínku rozšířit na

$$\sum_k E_k^\dagger E_k \leq I \tag{1.10}$$

Popis kvantových procesů Krausovou reprezentací je natolik obecný, že lze vyslovit tzv. větu o Krausově reprezentaci (důkaz viz [5]), která říká, že kvantový proces $\mathcal{E}$ splňuje podmínky (1.3), (1.5), (1.6) a (1.7) právě tehdy, když existuje její Krausova reprezentace. Kvantovou operaci, jako nejobecnější kvantově-mechanicky realizovatelný proces, lze tedy definovat rovnicí (1.9) a podmínkou (1.10). Pokud má kvantová operace pouze jeden Krausův operátor, nazýváme jí čistou.

1.2 Příklady kvantových operací

V této sekci uvedeme několik konkrétních příkladů operací a jejich Krausových reprezentací, jako jsou bit-flip, phase-flip a depolarizační kanál, které hrají při přenosu kvantové informace důležitou roli. Prvním z nich je popis operace částečné stopy přes podsystém nějakého většího systému. Nechť $\mathcal{H}_{AB}$

je Hilbertův prostor složeného systému AB, $|i\rangle_A$ je báze podsystému A a $|j\rangle_B$ báze podsystému B. Potom

$$\begin{aligned} \mathrm{Tr}_B \rho_{AB} &= \sum_{k=1}^{d_B} \langle k|_B \left(\sum_{i,l=1}^{d_A} \sum_{j,m=1}^{d_B} \lambda_{ijlm} |i\rangle_A |j\rangle_B \langle l|_A \langle m|_B \right) |k\rangle_B = \\ &= \sum_{k=1}^{d_B} \sum_{i,l=1}^{d_A} \lambda_{iklk} |i\rangle_A \langle l|_A = \sum_{k=1}^{d_B} E_k \rho_{AB} E_k^\dagger = \mathcal{E}(\rho_{AB}), \end{aligned} \tag{1.11}$$

kde definujme $E_k : H_{AB} \to H_A$

$$E_k \left(|i\rangle_A |j\rangle_B \right) = \delta_{jk} |i\rangle_A. \tag{1.12}$$

Předchozí rovnice tedy definuje Krausovy operátory pro operaci částečná stopy.

Modifikací předchozího případu můžeme pomocí Krausovy reprezentace vyjádřit stopu. Nechť $\mathcal{H}_A$ je Hilbertův prostor měřeného systému určený bází $|i\rangle_A$. Potom, když tento systém rozšíříme o jednorozměrný výstupní Hilbertův prostor $\mathbb{C}$ s bází $|0\rangle_B$ a provedeme na rozšířeném systému kvantovou operaci (1.11) přes podsystém A, bude výsledkem stav

$$\mathcal{E}(\rho) = |0\rangle_B \langle 0|_B \mathrm{Tr}\rho. \tag{1.13}$$

Než přejdeme k dalším příkladům uveďme ještě názorný způsob geometrické interpretace působení kvantové operace na qubit (dvourozměrný kvantový systém), jako působení určité akce na tzv. Blochovu sféru. Každý stav ρ qubitu lze zapsat v bázi[1] $I, \overrightarrow{\sigma}$, kde σ_i jsou Pauliho matice, jako

$$\rho = \frac{I + \overrightarrow{r}\,\overrightarrow{\sigma}}{2} = \frac{1}{2} \begin{pmatrix} 1 + r_z & r_x - i r_y \\ r_x + i r_y & 1 - r_z \end{pmatrix}, \tag{1.14}$$

kde $\overrightarrow{r}$ je jednotkový vektor v $\mathbb{R}^3$. Lze ukázat, že v této (Blochově) reprezentaci platí pro každou operaci zachovávající stopu

$$\overrightarrow{r} \xrightarrow{\mathcal{E}} r' = M \overrightarrow{r} + \overrightarrow{c}, \tag{1.15}$$

kde $M = OS$, S je reálná symetrická matice, O je reálná ortogonální matice. Na operaci $\mathcal{E}$ můžeme proto nahlížet jako na deformaci Blochovy sféry ve směrech vlastních vektorů S, následovanou rotací O a posunutím ve směru $\overrightarrow{c}$.

[1] Obecně lze každý stav n-rozměrného kvantového systému reprezentovat lineární kombinací matice I a báze algebry bezestopých matic $\mathfrak{su}(N)$.

Uvažujme následující operaci $\mathcal{E}$, tzv. bit-flip kanál, na qubitu: stav $|0\rangle$ resp. $|1\rangle$ transformuje s pravděpodobností $(1-p)$ na $|1\rangle$ resp. $|0\rangle$. Krausovy elementy této operace jsou

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad E_1 = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{1.16}$$

a tedy

$$\mathcal{E}(\rho) = E_0\rho E_0^\dagger + E_1\rho E_1^\dagger = \frac{1}{2}\begin{pmatrix} 1+(2p-1)r_z & r_x - i(2p-1)r_y \\ r_x + i(2p-1)r_y & 1-(2p-1)r_z \end{pmatrix}, \tag{1.17}$$

což odpovídá transformaci Blochova vektoru

$$\overrightarrow{r}' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2p-1 & 0 \\ 0 & 0 & 2p-1 \end{pmatrix}\overrightarrow{r}. \tag{1.18}$$

Z tvaru matice M je patrné, že bit flip kanál působí na Blochově sféře jako kontrakce roviny y-z faktorem $2p-1$ a složka r_x zůstává beze změn.

Další důležitou operací je tzv. phase-flip kanál, který s pravděpodobností $1-p$ mění relativní fázi qubitu o π. Tedy, je-li transformován qubit ve stavu např. $\alpha|0\rangle + \beta|1\rangle$ vystoupí s pravděpodobností $1-p$ ve stavu $\alpha|0\rangle - \beta|1\rangle$. Operační elementy phase-flip kanálu jsou

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad E_1 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.19}$$

Jednoduchým výpočtem lze stejně jako v předchozím příkladu vyjádřit matici M,

$$M = \begin{pmatrix} 2p-1 & 0 & 0 \\ 0 & 2p-1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{1.20}$$

Narozdíl od bit-flip kanálu se při této operaci kontrahuje v Blochově reprezentaci rovina x-y, zatímco osa z zůstává zachována.

Velmi důležitým příkladem kvantového šumu je tzv. depolarizační kanál, který působí tak, že pro libovolný vstupní stav je výstupní s pravděpodobností p zcela depolarizován. Pro jeden qubit má tato transformace tvar

$$\mathcal{E}(\rho) = \frac{1}{2}pI + (1-p)\rho. \tag{1.21}$$

Operace (1.21) není vyjádřena v Krausově reprezentaci. Pokud využijeme vztahu

$$\forall\rho: \quad \frac{I}{2} = \frac{\rho + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z}{4}, \tag{1.22}$$

který lze ověřit s využitím komutačních relací pro σ_i a Blochovy reprezentace pro ρ, lze vztah (1.21) přepsat na tvar

$$\mathcal{E}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z). \tag{1.23}$$

Při vizualizaci na Blochově sféře se jedná o kontrakci s faktorem $1 - p$ ve všech hlavních osách.

Důležitou aplikací kvantových operací je popis disipace energie kvantového systému. Takový proces lze charakterizovat kvantovou operací zvanou amplitudové tlumení. Pomocí formalismu kvantových operací odvodíme jednoduchý model disipace energie pro jeden optický mód.

Uvažujme mód ve stavu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, kde $|i\rangle$ jsou vlastní stavy operátoru počtu fotonů. Do cesty fotonů přidáme dělič paprsků, který v interakčním obraze působí jako unitární transformace $B = \exp[\theta(a^\dagger b - ab^\dagger)]$, kde θ je parametr vyjadřující sílu interakce, $a, a^\dagger$ resp. $b, b^\dagger$ jsou anihilační a kreační operátory uvažovaného módu, resp. módu na druhém vstupu děliče paprsků. Pomocí rozvoje operátoru B do mocninné řady lze spočíst stav systému po průchodu děličem. Předpokládejme ještě, že mód odpovídající operátoru b, tedy prostředí, které disipovanou energii přijímá, je před interakcí na děliči ve vakuovém stavu $|0\rangle$. Potom

$$\begin{aligned} B|0\rangle_b(\alpha|0\rangle_a + \beta|1\rangle_a) &= \beta\left[\sum_{n=0}^{\infty}\frac{(-1)^n\theta^{2n}}{(2n)!}|0_b1_a\rangle + \sum_{n=0}^{\infty}\frac{(-1)^n\theta^{2n+1}}{(2n+1)!}|1_b0_a\rangle\right] \\ &+ \alpha|0_b0_a\rangle \qquad (1.24) \\ &= \alpha|0_b0_a\rangle + \beta(\cos\theta|0_b1_a\rangle + \sin\theta|1_b0_a\rangle), \qquad (1.25) \end{aligned}$$

neboť

$$(a^\dagger b - ab^\dagger)|0\rangle_b|1\rangle_a = -|1\rangle_b|0\rangle_a, \quad (a^\dagger b - ab^\dagger)|1\rangle_b|0\rangle_a = |0\rangle_b|1\rangle_a. \tag{1.26}$$

Provedeme-li nyní na výsledný stav stopu přes prostředí, získáme následující vyjádření kvantové operace

$$\mathcal{E}(\rho) = E_0\rho{E_0}^\dagger + E_1\rho{E_1}^\dagger, \tag{1.27}$$

kde $E_k = \langle k|B|0\rangle$ jsou

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \cos\theta \end{pmatrix} \tag{1.28}$$

$$E_1 = \begin{pmatrix} 0 & \sin\theta \\ 0 & 0 \end{pmatrix} \tag{1.29}$$

a speciálně pro $\rho = |\psi\rangle\langle\psi|$

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \begin{pmatrix} |\alpha|^2 + |\beta|^2 \sin^2\theta & \alpha\beta^* \cos\theta \\ \alpha^*\beta\cos\theta & |\beta|^2\cos^2\theta \end{pmatrix} \tag{1.30}$$

Tento výsledek lze interpretovat následujícím způsobem. Element E_0 nechá stav $|0\rangle$ nezměněn, ale stavu $|1\rangle$ zmenší amplitudu, a element E_1 změní stav $|1\rangle$ na $|0\rangle$, což fyzikálně odpovídá ztrátě fotonu. Veličinu $\sin^2\theta$ lze interpretovat jako pravděpodobnost oné ztráty, jak plyne z (1.30).

Jako poslední příklad kvantových operací zde uvedeme ještě ztrátu kvantové informace, při níž nedochází k disipaci energie. Jedná se o tzv. disipaci fáze. Fyzikálně popisuje takový proces např. rozptyl fotonu při průchodu vlnovodem.

Jednoduchým modelem představující disipaci fáze může být následující případ kvantového šumu. Předpokládejme opět jeden qubit ve stavu $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, na který působí operátor $R_z(\theta)$ s náhodným parametrem θ, kde

$$R_z(\theta) = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix} \tag{1.31}$$

Předpokládejme dále, že úhel θ lze popsat náhodnou veličinou s Gaussovým rozdělením s nulovou střední hodnotou a kvadratickou odchylkou 2λ. Potom výstupní matice hustoty je dána vztahem

$$\rho = \frac{1}{\sqrt{4\pi\lambda}} \int_{\infty}^{-\infty} R_z(\theta)|\psi\rangle\langle\psi|R_z^\dagger(\theta) \exp\left(\frac{-\theta^2}{4\lambda}\right) d\theta \tag{1.32}$$

$$= \begin{pmatrix} |\alpha|^2 & ab^* e^{-\lambda} \\ a^* b e^{-\lambda} & |b|^2 \end{pmatrix}. \tag{1.33}$$

Odpovídající operační elementy mohou odpovídat např.

$$E_0 = \sqrt{\delta}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad E_1 = \sqrt{1-\delta}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{1.34}$$

kde $\delta = \frac{1}{2}(1 + e^{-\lambda})$. Je tedy patrné, že fázová disipace představuje stejnou kvantovou operaci jako phase-flip kanál.

Kapitola 2

Univerzální kvantové procesy

V této kapitole definujeme pojem univerzálního kvantového procesu a na jednoduchém příkladu demonstrujeme tzv. podmínku kovariance. Dále dle práce [4] parametrizujeme třídu všech univerzálních procesů na dvou částicích libovolné, ale stejné dimenze.

2.1 Definice univerzálního kvantového procesu

Děje kvantové fyziky podléhají, vzhledem k její lineární povaze, jistým omezením a proto ne každý proces je realizovatelný. Příkladem takového omezení je proces klonování kvantového stavu. Předpokládejme lineární transformaci T na dvoučásticovém Hilbertově prostoru, která kopíruje naprosto přesně dva ortogonální stavy prvního částice, pro jednoduchost řekněme qubitu; tedy

$$\begin{aligned} T|0\rangle|0\rangle &\rightarrow |0\rangle|0\rangle \\ T|1\rangle|0\rangle &\rightarrow |1\rangle|1\rangle. \end{aligned} \tag{2.1}$$

Potom vzhledem k požadované linearitě transformace T 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 zcela neodpovídá naší představě kopie, tedy vstupního stavu, tedy $\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)$. Při popisu maticemi hustoty je rozdíl mezi ideální kopií a výsledným jednočásticovým stavem po transformaci T ještě názornější,

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

Obrazem matice hustoty odpovídající stavu $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ je zcela depolarizovaný stav. Můžeme se proto ptát, zda existuje lineární transformace, která

sice nekopíruje žádný stav přesně, ale odchylka od ideální kopie je pro všechny vstupní stavy stejná. Univerzální kvantový proces můžeme vágně definovat jako kvantově mechanicky realizovatelnou transformaci, která se, vzhledem k nějakému kvantitativnímu kritériu, chová ke všem stavům stejně. V případě klonování taková transformace skutečně existuje a budeme se jí podrobněji zabývat v odstavci 3.1.

Před formálním zavedením pojmu univerzálního kvantového procesu uveďme ještě jeden příklad, kterým bude definice motivována. Nejprve připravíme systém dvou rozlišitelných částic se spinem $\frac{1}{2}$ v následujícím stavu

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

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

$$\rho_2(\mathbf{m}) = \frac{\mathbf{P}_J \rho_1(\mathbf{m}) \mathbf{P}_J}{\mathrm{Tr}\left(\mathbf{P}_J \rho_1(\mathbf{m}) \mathbf{P}_J\right)}, \tag{2.4}$$

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

$$\rho_2(\mathbf{m}) = p_1 |1,1\rangle\langle 1,1| + (1-p_1)|1,0\rangle\langle 1,0|, \qquad p_1 = \frac{2}{3} \tag{2.5}$$

nebo

$$\rho_2(\mathbf{m}) = |0,0\rangle\langle 0,0| \tag{2.6}$$

Oba tyto kvantové procesy jsou univerzální v tom smyslu, že pravděpodobnost p_1 vystupující ve výrazech (2.5) není 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

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

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

> Kvantový proces P na dvou částicích nazvu univerzální, právě když pro každý čistý stav $|m\rangle_0$ a každou unitární transformaci U platí podmínka kovariance (2.7).

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 informatiky, ale navíc demonstrují symetrie Hilbertova prostoru.

2.2 Dvoučásticové univerzální procesy

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

$$\mathcal{P} : \rho_{in}(\mathbf{p}) \otimes \rho_{ref} \longrightarrow \rho_{out}(\mathbf{p}). \tag{2.8}$$

Operátor ρ_{ref} je libovolná pevně zvolená jednočásticová referenční matice hustoty, $\rho_{in}(\mathbf{p})$ je projektor na čistý stav charakterizovaný zobecněným Blochovým vektorem $\mathbf{p}$, tedy $\rho_{in}(\mathbf{p}) = |\mathbf{p}\rangle\langle\mathbf{p}|$.

Každou matici hustoty systému dimenze N lze zapsat ve tvaru

$$\rho_{in} = \frac{1}{N}\left(I + \sum_{i,j=1}^{N} p_{ij}\mathbf{A}_{ij}\right), \tag{2.9}$$

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

$$(\mathbf{A}_{ij})^{kl} = \delta_{ik}\delta_{jl} - \frac{1}{N}\delta_{ij}\delta_{kl}. \tag{2.10}$$

Z (2.10) a ze samosdruženosti matice hustoty plyne $\mathbf{A}_{ij}^{\dagger} = \mathbf{A}_{ji}$ a $p_{ij}^{*} = p_{ji}$ (aby rovnice (2.9) 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]

$$\begin{aligned}\rho_{out}(\mathbf{p}) &= \frac{1}{N^2}I\otimes I + \alpha_{ij}^{(1)}(\mathbf{p})\mathbf{A}_{ij}\otimes\mathbf{I} + \alpha_{ij}^{(2)}(\mathbf{p})\mathbf{I}\otimes\mathbf{A}_{ij} \\ &\quad + K_{ijkl}(\mathbf{p})\mathbf{A}_{ij}\otimes\mathbf{A}_{kl}.\end{aligned} \tag{2.11}$$

Aplikujeme-li na předchozí vztah podmínku linearity vůči $\mathbf{p}$, dojdeme k závěru, že koeficienty $\alpha_{ij}^{(1,2)}(\mathbf{p})$ a $K_{ijkl}(\mathbf{p})$ musí být lineárními funkcemi v p_{ij}. 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 (2.11) získáme sadu rovnic, které musí být splněny, aby proces $\mathcal{P}$ splňoval podmínku kovariance (2.7):

$$\alpha_{ij}^{(1,2)}(\mathbf{p})\mathbf{A}_{ij}\otimes\mathbf{I} = \alpha_{ij}^{(1,2)}(\mathbf{p}_0)U(\mathbf{p})\mathbf{A}_{ij}U^{\dagger}(\mathbf{p})\otimes\mathbf{I} \tag{2.12}$$

$$K_{ijkl}(\mathbf{p})\mathbf{A}_{ij}\otimes\mathbf{A}_{kl} = K_{ijkl}(\mathbf{p}_0)\left(U(\mathbf{p})\otimes U(\mathbf{p})\right)\left(\mathbf{A}_{ij}\otimes\mathbf{A}_{kl}\right)\left(U^{\dagger}(\mathbf{p})\otimes U^{\dagger}(\mathbf{p})\right) \tag{2.13}$$

[1]Ke zjednodušení zápisu užíváme v dalším Einsteinovo sumační pravidlo

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

$$\begin{aligned} \alpha_{ij}^{(1,2)}(\mathbf{p}) &= \alpha^{(1,2)} p_{ij} && (2.14) \\ K_{ijkl}(\mathbf{p}) &= C\delta_{il}\delta_{jk} + \beta p_{il}\delta_{jk} + \beta^* p_{jk}\delta_{il}, && (2.15) \end{aligned}$$

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

$$\begin{aligned} \rho_{out}(\mathbf{p}) &= \frac{1}{N^2} I \otimes I + \alpha^{(1)} p_{ij} \mathbf{A}_{ij} \otimes \mathbf{I} + \alpha^{(2)} p_{ij} \mathbf{I} \otimes \mathbf{A}_{ij} + C\mathbf{A}_{ij} \otimes \mathbf{A}_{ji} \\ &\quad + \beta p_{il} \mathbf{A}_{ij} \otimes \mathbf{A}_{jl} + \beta^* p_{il} \mathbf{A}_{ji} \otimes \mathbf{A}_{lj}. \qquad (2.16) \end{aligned}$$

Volné parametry stále nemohou být libovolné, neboť aby byl operátor definovaný (2.16) maticí hustoty, musí být navíc pozitivní. Tuto podmínku lze splnit, pokud nalezeme vlastní čísla této matice a určíme podmínky na $\alpha^{(1,2)}$, C a β tak, aby byla vždy nezáporná. Z podmínky kovariance (2.7) plyne, že pokud je λ vlastní číslo $\rho(\mathbf{p}_0)$, pak je i vlastním číslem 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 (2.16) v tomto případě lze zapsat ve tvaru

$$\rho_{out}(p_{ij} = N\delta_{1i}\delta_{1j}) = \sum_{i=1}^{4} \oplus p_i \rho_i, \qquad (2.17)$$

kde operátory hustoty ρ_i jsou

$$\begin{aligned} \rho_1 &= |11\rangle\langle 11| \\ \rho_2 &= \sum_{j=2}^{N} \Bigg[|1j\rangle\langle 1j| \left(\frac{1}{2(N-1)} + N\frac{\alpha^{(1)} - \alpha^{(2)}}{2p_2} \right) + \\ &\quad + |j1\rangle\langle j1| \left(\frac{1}{2(N-1)} + N\frac{\alpha^{(2)} - \alpha^{(1)}}{2p_2} \right) + \\ &\quad + |1j\rangle\langle j1| \frac{C + N\beta}{p_2} + |j1\rangle\langle 1j| \frac{C + N\beta^*}{p_2} \Bigg] \end{aligned}$$

$$
\begin{aligned}
\rho_3 &= \frac{1}{N-1}\sum_{j=2}^{N}|jj\rangle\langle jj| \\
\rho_4 &= \sum_{2=i<j}^{N}\Big[|ij\rangle\langle ij|\frac{1}{(N-1)(N-2)} + \\
&\quad +|ji\rangle\langle ji|\frac{1}{(N-1)(N-2)} + \\
&\quad +(|ij\rangle\langle ji| + |ji\rangle\langle ij|)\frac{C}{p_4}\Big]
\end{aligned}
\tag{2.18}
$$

a pravděpodobnosti p_i jsou

$$
\begin{aligned}
p_1 &= \frac{1}{N^2} + (N-1)(\alpha^{(1)}+\alpha^{(2)}) + C(1-\frac{1}{N}) + (\beta+\beta^*)\frac{(N-1)^2}{N} \\
p_2 &= (N-1)(\frac{2}{N^2} + (N-2)(\alpha^{(1)}+\alpha^{(2)}) - \frac{2C}{N} - 2\frac{N-1}{N}(\beta+\beta^*)) \\
p_3 &= (N-1)(\frac{1}{N^2} - (\alpha^{(1)}+\alpha^{(2)}) + C(1-\frac{1}{N}) + \frac{(\beta+\beta^*)}{N}) \\
p_4 &= (N-1)(N-2)(\frac{1}{N^2} - (\alpha^{(1)}+\alpha^{(2)}) + \frac{C}{N} + \frac{(\beta+\beta^*)}{N}).
\end{aligned}
\tag{2.19}
$$

Z podmínky $\mathrm{Tr}\rho_{out} = 1$ a výrazu (2.17) plyne, že p_i splňují

$$
p_1 + p_2 + p_3 + p_4 = 1. \tag{2.20}
$$

Z rovnic (2.18) a (2.19) spočítáme vlastní čísla matice hustoty $\rho_{out}(p_{ij} = N\delta_{1i}\delta_{1j})$;

$$
\begin{aligned}
\lambda_1 &= p_1 \\
\lambda_{2\pm} &= \frac{p_2}{2(N-1)} \pm \sqrt{\frac{N^2}{4}\left(\alpha^{(1)}-\alpha^{(2)}\right)^2 + |C+\beta N|^2} \\
\lambda_3 &= \frac{p_3}{N-1} \\
\lambda_{4\pm} &= \frac{p_4}{(N-1)(N-2)} \pm |C|.
\end{aligned}
\tag{2.21}
$$

Aby tedy byla matice ρ_{out} operátorem hustoty, musí mít všechna vlastní čísla nezáporná.

V případě $N \geq 3$ lze tři nezávislé reálné parametry $(\alpha^{(1)}+\alpha^{(2)})$, $(\beta+\beta^*)$ a C vyjádřit z rovnic (2.19) a (2.20) pomocí, řekněme, p_1, p_3, p_4. Tyto vztahy

mají tvar

$$\begin{aligned}
\beta + \beta^* &= -\frac{1}{N(N-1)} + \frac{p_4}{(N-1)(N-2)} + \frac{p_1}{(N-1)} \\
\alpha^{(1)} + \alpha^{(2)} &= \frac{N-2}{N^2(N-1)} - \frac{p_4 - p_1 + p_3}{N(N-1)} \\
C &= \frac{p_3}{N-1} - \frac{p_4}{(N-1)(N-2)}.
\end{aligned} \tag{2.22}$$

K jednoznačné specifikaci dvoučásticového univerzálního procesu je třeba specifikovat navíc parametry $\alpha^{(1)} - \alpha^{(2)}$ a $\beta - \beta^*$. V následující kapitole uvidíme několik příkladů univerzálních procesů na dvou částicích.

Kapitola 3

Realizace univerzálních kvantových procesů

V této kapitole nejprve ukážeme, jak vypadá optimální univerzální proces klonování jedné konečněrozměrné částice na dvě, odvozený v [3], a jaký může mít tvar unitární transformace, která ho realizuje [6]. Ve volbě takové transformace zůstává velká volnost a cílem první části této kapitoly je konstrukce konkrétní unitární matice realizující klonování, která je vhodná k dekompozici na součin rotací ve dvourozměrných podprostorech. Dále bychom chtěli zkonstruovat unitární realizaci univerzálního provazovacího procesu odvozeného v [4] a její rozklad v součin unitárních rotací ve dvourozměrných podprostorech.

Motivací k takovému rozkladu je možnost dekomponovat rotace ve dvourozměrných podprostorech generovaných dvěma vektory výpočetní báze na součin jedno a dvoučásticových unitárních transformací, což je z experimentálního hlediska velmi pozitivní fakt. Tento postup využívá tzv. Greyova kódování a je podrobněji popsán v [5].

3.1 Operace klonování částice

Jak již bylo v 2.1 ukázáno, vzhledem k linearitě nelze kvantově realizovat klonovací proces na Hilbertově prostoru, který kopíruje dva ortogonální stavy přesně. 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 podstavy výsledné matice hustoty byly shodné, a aby kvalita výstupu, tedy jistá míra vzdálenosti od ideální kopie, byla pro všechny vstupní stavy,

v našem případě pro čisté stavy, stejná[1].

V článku [3] definoval R. F. Werner klonovací zobrazení kopírující stav L identických částic dimenze N na M,

$$T(\rho^{\otimes L}) = \frac{d[L]}{d[M]} S_M (\rho^{\otimes L} \otimes I^{\otimes M-L}) S_M, \tag{3.1}$$

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

$$d[M] = \left(\begin{array}{c} N+M-1 \\ M \end{array} \right). \tag{3.2}$$

O tomto zobrazení ukázal, že je optimální a jediné, nabývající maximální jednočásticové fidelity

$$\mathcal{F} = \frac{L}{M} \frac{M+N}{L+N}. \tag{3.3}$$

Pro $L = 1$, $M = 2$ tento proces splňuje podmínku kovariance (2.7) a ve formalizmu ukázaném v přechozí kapitole lze charakterizovat parametry

$$\begin{aligned} \alpha^{(1)} &= \alpha^{(2)} = \frac{N+2}{2N^2(N+1)}, \\ \beta &= \beta^* = \frac{1}{2N(N+1)}, \\ C &= 0 \end{aligned} \tag{3.4}$$

a pravděpodobnosti odpovídající jednotlivým ρ_i jsou

$$\begin{aligned} p_1 &= \frac{2}{N+1}, \\ p_2 &= \frac{N-1}{N+1}, \\ p_3 &= p_4 = 0. \end{aligned} \tag{3.5}$$

Chceme-li zobrazení (3.1) pro $L = 1$, $M = 2$ fyzikálně realizovat, je nutné Hilbertův prostor originálu a budoucí kopie rozšířit o ancillu a na rozšířeném systému nalézt unitární transformaci U pro kterou platí

$$T(\rho^{\otimes L}) = \mathrm{Tr}_a \left(U \rho_{in} \otimes \rho_{ref} U^\dagger \right), \tag{3.6}$$

[1]Tyto podmínky lze různým způsobem zeslabovat, například nepožadujeme symetrii jednočásticových stavů [8], [9]. Takovými zobecněními se zde zabývat nebudeme.

kde Tr_a značí stopu přes ancillu a ρ_{ref} je pevně zvolený počáteční stav referenčního systému a ancilly. Je zřejmé, že pokud taková unitární transformace existuje, zůstává v její volbě volnost ve výběru právě počátečního stavu ρ_{ref}.

V práci [6] je takové unitární zobrazení definováno působením na bazické stavy

$$U|i\rangle|X\rangle = \alpha|ii\rangle|X_i\rangle + \beta \sum_{j\neq i} \big(|ij\rangle + |ji\rangle\big)|X_j\rangle, \tag{3.7}$$

$$\alpha = \sqrt{\frac{2}{N+1}}, \qquad \beta = \sqrt{\frac{1}{2(N+1)}}, \tag{3.8}$$

kde $|i\rangle$ je ortonormální báze jednočásticového Hilbertova prostoru, $|X\rangle$ reprezentuje normovaný počáteční stav kopírovacího stroje, tedy prázdné kopie a ancilly a stavy $|X_i\rangle$ jsou ortonormální vektory z Hilbertova prostoru ancilly. Pokud zvolíme za $\rho_{in} = |1\rangle\langle 1|$ a vyjádříme explicitně pravou stranu rovnice (3.6) dojdeme k vyjádření

$$\rho_{out}^{(clone)} = \frac{2}{N+1}|11\rangle\langle 11| + \frac{1}{2(N+1)} \sum_{j\neq 1} (|1j\rangle + |j1\rangle)(\langle 1j| + \langle j1|). \tag{3.9}$$

To však není nic jiného, než proces popsaný (2.17) s pravděpodobnostmi (3.5), a tedy Wernerův $1 \to 2$ optimální klonovací proces (3.1).

3.2 Dekompozice operace klonování

Nyní se dostáváme k úkolu dekomponovat unitární zobrazení U definované rovnicí (3.7). V této sekci budeme dimenzi jednočásticového Hilbertova prostoru vždy značit N.

Nejprve naznačíme postup, který užijeme k dekompozici matice U. Předpokládejme obecnou (později unitární) matici $A \in \mathcal{C}^{m,m}$ a matici rotace $R_{1m}(\theta)$ působící pouze na první a poslední vektor báze prostoru $\mathcal{C}^m$, v níž je vyjádřena matice operátoru A,

$$A = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix}$$

$$R_{1m}(\theta) = \begin{pmatrix} \cos\theta & 0 & \dots & 0 & \sin\theta \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \\ -\sin\theta & 0 & \dots & 0 & \cos\theta \end{pmatrix}. \tag{3.10}$$

Po vynásobení A z leva maticí $R_{1,m}(\theta)$ dostaneme matici $A^{(1)}$, která se od A bude lišit pouze v prvním a posledním řádku, navíc prvek $a^{(1)}_{m,1}$ je roven

$$a^{(1)}_{m,1} = a_{1,1}\cos\theta + a_{m,1}\sin\theta \tag{3.11}$$

a vhodnou volbou θ můžeme zaručit, že $a^{(1)}_{m,1} = 0$. Zde jsme předpokládali, že prvky $a_{1,1}$ a $a_{1,m}$ jsou reálné. Pokud by tomu tak nebylo, vynásobili bychom matici A nejprve vhodnou diagonální unitární maticí, která by tyto prvky upravila na reálné. Tím jsme na místě původního a_{m1} vyrobili nulu. Obdobně bychom pokračovali dál s rotací působící na dvourozměrný podprostor příslušející prvnímu a $(m-1)$-nímu bazickému vektoru, pak prvnímu a $(m-2)$-tému, atd., až prvnímu a druhému bazickému vektoru. Žádná z rotací už neohrozí nulu vytvořenou předchozími úpravami, neboť každá ovlivní pouze první a jistý l-tý řádek. Po těchto úpravách dospějeme k matici

$$A^{(m-1)} = R_{2,1}(\theta_{2,1})\ldots R_{m,1}(\theta_{m,1})A, \tag{3.12}$$

která má v prvním sloupci, kromě diagonálního prvku, samé nuly. Pokud je A unitární, potom, vzhledem k tomu, že rotace i případné fázové posuny jsou také unitární, i v prvním řádku jsou, kromě prvku $a^{m-1}_{1,1}$, samé nuly. Matici A lze potom vyjádřit jako

$$A = R_1^{-1}A^{(m-1)} = R^{-1}_{m,1}(\theta_{m,1})\ldots R^{-1}_{2,1}(\theta_{2,1})A^{(m-1)}. \tag{3.13}$$

Stejným postupem bychom mohli postupovat při diagonalizaci dalších sloupců. I zde je patrné, že vytvoření nuly v určitém sloupci nenaruší nuly ve sloupcích předchozích. V těchto sloupcích jsou totiž na řádcích, které se kombinují, již vždy samé nuly. Touto procedurou dojdeme až k diagonální matici, kterou můžeme vynásobením maticí komplexně sdruženou převést na identitu. V našem případě můžeme bez újmy na obecnosti předpokládat, že výsledná matice je již jednotková. Potom lze A vyjádřit jako

$$A = R_1^{-1}\ldots R^{-1}_{m-1}I, \tag{3.14}$$

kde matice R_j je

$$R_j = R_{m,j}(\theta_{m,j})\ldots R_{j-1,j}(\theta_{j-1,j}). \tag{3.15}$$

Předchozí postup nám říká, že každý, v našem případě reálný, unitární operátor na Hilbertově prostoru dimenze m lze rozložit do součinu $\frac{1}{2}m(m-1)$ rotací působících vždy pouze na dvourozměrném podprostoru. Toto schéma užijeme pro dekompozici unitární transformace (3.7), která realizuje optimální proces klonování z jedné částice na dvě. Je zřejmé, že toto zobrazení

není předpisem (3.7) definováno zcela, neboť lineární zobrazení je jednoznačně definováno pomocí obrazů na všechny bazické vektory prostoru, na kterém působí. Operátor U působí na Hilbertově prostoru $\mathcal{H} = \mathcal{H}_O \otimes \mathcal{H}_B \otimes \mathcal{H}_A$, tedy na tenzorovém součinu Hilbertových prostorů originálu (O), budoucí kopie (B) a ancilly (A), který má dimenzi N^3. Zbývá tedy dodefinovat obrazy vždy $N(N^2-1)$ zbývajících bazických vektorů.

V experimentální realizaci kvantových algoritmů je důležitým parametrem složitost aparatury, tedy počet transformací a hradel na systému prováděných. Rozklad unitární realizace nějakého kvantového procesu do součinu jednodušších unitárních operátorů odpovídá sekvenci experimentálních uspořádání kladených za sebou. Proto je pro realizaci každého procesu důležité nejen najít příslušnou sekvenci unitární operátorů, ale i vhodně optimalizovat počet a pestrost druhů použitých transformací. Z tohoto hlediska není množství $\frac{1}{2}N^3(N^3-1)$ rotací[2] zcela uspokojivé, zvláště pokud je operace (3.7) určená pouze obrazem N bazických vektorů. V následujícím ukážeme, že k realizaci procesu klonování, postačí $2N(N-1)$ rotací.

Z důvodů jednoduššího zápisu ještě přepišme vztah (3.7) tak, že působí na prostoru $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_O$, počáteční stav kopírovacího stroje $|X\rangle$ zvolme $|00\rangle$ a $|X_i\rangle = |i\rangle$,

$$U|00i\rangle = \alpha|iii\rangle + \beta \sum_{j\neq i} |j\rangle\big(|ij\rangle + |ji\rangle\big). \tag{3.16}$$

Tím docílíme toho, že, pokud zvolíme ve výpočetní bázi pořadí vektorů přirozeným způsobem podle hodnoty v N-ární soustavě, bude prvních N sloupců matice operátoru U určeno právě předpisem (3.16) a ostatních $N^3 - N$ zbývá libovolně doplnit tak, aby U byla unitární. Obecné doplnění na unitární transformaci by ale nebylo nijak optimální co do počtu rotací potřebných k dekompozici. V tomto ohledu se nabízí jako optimální najít takovou realizaci, která po diagonalizaci prvních N sloupců již přejde v jednotkovou matici. Toto bude motivující myšlenkou v dalším postupu.

Nejprve spočtěme celkový počet poddiagonálních nenulových prvků prvních N sloupců matice operátoru (3.16). Je užitečné si všimnout, že v těchto sloupcích je na každém řádku nejvýše jedna nenulová hodnota, a proto se při diagonalizaci jednoho sloupce ostatní z N prvních nemění (ostatní sloupce se obecně samozřejmě mění). Proto počet nenulových poddiagonálních prvků prvních N sloupců odpovídá počtu rotací potřebných k jejich diagonalizaci. Poddiagonalita nenulového klm-tého prvku v i-tém sloupci ($i = 0, \ldots, N-1$) odpovídá v našem uspořádání a v N-ární soustavě podmínce $00i < klm$, a vzhledem k (3.16), je první nenulový prvek každého tohoto sloupce typu $00i$,

[2] viz předchozí odstavec

a tedy v matici U jde o prvek diagonální. V každém z těchto sloupců je tedy $2(N-1)$ poddiagonálních nenulových prvků, a proto pro jejich diagonalizaci je třeba celkem $2N(N-1)$.

Výše zmíněnou vlastnost prvních N sloupců, která zaručuje, že se při diagonalizaci jednoho z těchto sloupců ostatních $N-1$ nemění, můžeme dále využít k tomu, že problém dekompozice matice U, rozdělíme do N nezávislých diagonalizací jednotlivých sloupců. Navíc je vidět, že některé bazické vektory $\mathcal{H}$ se v (3.16) nevyskytují vůbec. Působení U na takové vektory můžeme tedy volit jako identitu, a odpovídající sloupce (z podmínky unitarity i řádky) jsou diagonální s jedničkou na diagonále. V rovnici (3.16) se vyskytuje celkem $N(2N-1)$ bazických vektorů, a U jsme tedy dodefinovali jako identitu na podprostoru generovaném $N^3 - N(2N-1)$ bazických vektorů.

Zavedeme značení, které nám dovolí využít předchozích vlastností a elegantně zapsat matici operátoru optimální operace klonování, přičemž bude patrné, jak je možné ji snadno a efektivně dekomponovat. Označme

$$\mathcal{X}_i = \mathrm{span}\{|iii\rangle, |jji\rangle, |jij\rangle; j \neq i\} \tag{3.17}$$

$$\hat{\mathcal{X}} = \mathrm{span}\{|klm\rangle; m \neq k \neq l\} \tag{3.18}$$

a identické operátory na těchto podprostorech označme Id_i, resp. $\hat{\mathrm{Id}}$ a na podprostorech $\mathcal{X}_i^{\perp}$ je označme $\hat{\mathrm{Id}}_i$. Hilbertův prostor $\mathcal{H}$ lze psát jako direktní součet podprostorů $\mathcal{X}_i$ a $\hat{\mathcal{X}}$, tedy $\mathcal{H} = \hat{\mathcal{X}} \bigoplus_{i=0}^{N-1} \mathcal{X}_i$. Matici U lze potom bez újmy na obecnosti zapsat ve tvaru

$$U = \hat{\mathrm{Id}} \bigoplus_{i=0}^{N-1} U_i = \prod_{i=0}^{N-1} (\hat{\mathrm{Id}}_i \oplus U_i), \tag{3.19}$$

kde operátory U_i jsou unitární a působí pouze na podprostorech $\mathcal{X}_i$. Problém dekompozice matice U se tedy zúží na dekompozici menších matic U_i. Navíc v matici U_i je rovnicí (3.16) určen vždy právě jeden, a při dodržení přirozeného uspořádání bazických vektorů právě první, sloupec. Potom, pokud dopočítáme ostatní sloupce tak, že po diagonalizaci prvního přejde matice U_i v identický operátor lze s užitím předchozího diagonalizačního postupu psát

$$\begin{aligned} U &= \prod_{i=0}^{N-1} (\hat{\mathrm{Id}}_i \oplus U_i) = \prod_{i=0}^{N-1} \left(\hat{\mathrm{Id}}_i \oplus \prod_{j=2}^{2N-1} R_{ij} \right) \\ &= \prod_{i=0}^{N-1} \prod_{j=2}^{2N-1} \left(\hat{\mathrm{Id}}_i \oplus R_{ij} \right), \end{aligned} \tag{3.20}$$

kde R_{ij} jsou rotace ve dvourozměrných podprostorech podprostoru $\mathcal{X}_i$, a tedy $\hat{\mathrm{Id}}_i \oplus R_{ij}$ jsou rotace stejného typu na $\mathcal{H}$. Je užitečné si uvědomit, že vnější produkt je komutativní, neboť $\hat{\mathrm{Id}}_i \oplus U_i$ jsou komutující operátory, zatímco vnitřní produkt není.

Nyní zbývá odvodit obecný předpis pro příslušnou posloupnost matic rotací, což se redukuje na hledání posloupnosti úhlů, která diagonalizuje první sloupec matice U_k rozměru $(2N-1)\times(2N-1)$, a předpis pro ostatní sloupce tak, aby po diagonalizaci prvního tvořily jednotkovou matici. Pro tento účel stačí zabývat se nejprve působením matic rotace pouze na jeden obecný sloupcový vektor. Pro zpřehlednění zápisu budeme sloupec diagonalizovat v pořadí od druhého prvku k poslednímu. Matice rotací tedy budou kombinovat první složku vektoru, na který působí, s druhou, třetí až $(2N-1)$-ní. Označme

$$\sigma_i = \sin\varphi_i, \qquad \gamma_i = \cos\varphi_i, \quad i = 2,\ldots,2N-1 \tag{3.21}$$

prvky určující matici rotace R_{ki}, která kombinuje i-tou složku vektoru s první, u^i, resp. $u^{i'}$ složky původního, resp. výsledného vektoru, $u^1_{(i)}$ je první složka původního vektoru po působení matic R_{k2} až R_{ki-1}. Klademe tedy $u^1_{(2)} = u^1$ a $u^{1'} = u^1_{(2N)}$. Potom pro $i \geq 2$ platí

$$u^{i'} = -\sigma_i u^1_{(i)} + \gamma_i u^i \tag{3.22}$$

a pro první složku platí

$$\begin{aligned} u^1_{(i)} &= \gamma_{i-1}u^1_{(i-1)} + \sigma_{i-1}u^{i-1} = \gamma_{i-1}(\gamma_{i-2}u^1_{i-2} + \sigma_{i-2}u^{i-2}) + \sigma_{i-1}u^{i-1} \\ &= \left(\prod_{j=2}^{i-1}\gamma_j\right)u^1_{(2)} + \sum_{k=2}^{i-1}\left(\prod_{j=k+1}^{i-1}\gamma_j\right)\sigma_k u^k, \end{aligned} \tag{3.23}$$

a pokud zvolíme formálně $\sigma_1 = 1$ a $\gamma_1 = 0$ můžeme výsledek zapsat jako

$$u^1_{(i)} = \sum_{k=1}^{i-1}\left(\prod_{j=k+1}^{i-1}\gamma_j\right)\sigma_k u^k. \tag{3.24}$$

S využitím (3.24) upravíme podmínky na u^i na tvar

$$u^{1'} = u^1_{(2N)} = \sum_{k=1}^{2N-1}\left(\prod_{j=k+1}^{2N-1}\gamma_j\right)\sigma_k u^k \tag{3.25}$$

$$u^{i'} = -\sigma_i\sum_{k=1}^{i-1}\left(\prod_{j=k+1}^{i-1}\gamma_j\right)\sigma_k u^k + \gamma_i u^i, \quad i = 2,\ldots,2N-1. \tag{3.26}$$

Pro nalezení u^i pro l-tý sloupec matice U_k je třeba řešit soustavu rovnic (3.25) a (3.26) s levou stranou $u^{i'} = \delta_{li}$. Vzhledem k úloze, která k soustavě vedla je snadné ji explicitně vyřešit, neboť působením součinů matic rotací na U_k jsme získali jednotkovou matici, a proto matici U_k lze vyjádřit jako působení součinů těchto matic v opačném pořadí a s opačnými smysly rotace. Po výpočtu analogického k výše provedenému dojdeme k explicitnímu vyjádření složek matice U_k

$$\begin{aligned}(U_k)_{ab} &= \sigma_a \left[\left(\prod_{j=a+1}^{2N-1} \gamma_j \right) \delta_{1b} - \sum_{l=a+1}^{2N-1} \left(\prod_{j=a+1}^{l-1} \gamma_j \right) \sigma_l \delta_{lb} \right] \\ &+ \gamma_a \delta_{ab}, \qquad a, b = 1, \ldots, 2N-1. \end{aligned} \tag{3.27}$$

Nyní je třeba určit posloupnosti γ_i a σ_i. Ty jsou určeny podmínkou převedení prvního sloupce matice U_k, označme jeho složky β^i, který je určen (3.16), na sloupec o složkách $(1, 0, \ldots, 0)$. Z toho plyne podmínka

$$0 = -\sigma_i \beta^1_{(i)} + \gamma_i \beta^i, \quad i = 2, \ldots, 2N-1. \tag{3.28}$$

Po převedení prvního sčítance na levou stranu můžeme rovnici umocnit, neboť můžeme obě strany rovnice předpokládat za nezáporné, a využít, že σ_i a γ_i jsou vázány podmínkou $\sigma_i^2 + \gamma_i^2 = 1$. Z toho plyne, že

$$\gamma_i^2 = \frac{(\beta^1_{(i)})^2}{(\beta^1_{(i)})^2 + (\beta^i)^2} \tag{3.29}$$

$$\sigma_i^2 = \frac{(\beta^i)^2}{(\beta^1_{(i)})^2 + (\beta^i)^2} \tag{3.30}$$

Využitím první rovnosti ve výrazu (3.23) a po dosazení (3.29) a (3.30) dostaneme explicitní předpis pro $\beta^1_{(i)}$.

$$\beta^1_{(i)} = \gamma_{i-1}\beta^1_{i-1} + \sigma_{i-1}\beta^{i-1} = \sqrt{(\beta^1_{(i-1)})^2 + (\beta^{i-1})^2} = \sqrt{\sum_{j=1}^{i-1} (\beta^j)^2} \tag{3.31}$$

Vztahy (3.20), (3.27), (3.29), (3.30) a (3.31) je problém optimálního rozkladu procesu klonování (3.16) zcela vyřešen. Nyní uvedeme příklad pro $N = 2$. Podle (3.20) hledáme matice U_0, U_1 a jejich rozklady R_{0j} a R_{1j}, kde $j =$

2, 3. Podle výše zmíněných vztahů můžeme napsat

$$R_{02} = \begin{pmatrix} \frac{\sqrt{4}}{\sqrt{5}} & \frac{\sqrt{1}}{\sqrt{5}} & 0 \\ -\frac{\sqrt{1}}{\sqrt{5}} & \frac{\sqrt{4}}{\sqrt{5}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_{03} = \begin{pmatrix} \frac{\sqrt{5}}{\sqrt{6}} & 0 & \frac{\sqrt{1}}{\sqrt{6}} \\ 0 & 1 & 0 \\ -\frac{\sqrt{1}}{\sqrt{6}} & 0 & \frac{\sqrt{5}}{\sqrt{6}} \end{pmatrix} \tag{3.32}$$

$$R_{12} = \begin{pmatrix} \frac{\sqrt{1}}{\sqrt{2}} & \frac{\sqrt{1}}{\sqrt{2}} & 0 \\ -\frac{\sqrt{1}}{\sqrt{2}} & \frac{\sqrt{1}}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_{13} = \begin{pmatrix} \frac{\sqrt{1}}{\sqrt{3}} & 0 & \frac{\sqrt{2}}{\sqrt{3}} \\ 0 & 1 & 0 \\ -\frac{\sqrt{2}}{\sqrt{3}} & 0 & \frac{\sqrt{1}}{\sqrt{3}} \end{pmatrix} \tag{3.33}$$

$$U_0 = \begin{pmatrix} \frac{\sqrt{2}}{\sqrt{3}} & -\frac{\sqrt{1}}{\sqrt{5}} & -\frac{\sqrt{2}}{\sqrt{15}} \\ \frac{\sqrt{1}}{\sqrt{6}} & \frac{\sqrt{4}}{\sqrt{5}} & -\frac{\sqrt{1}}{\sqrt{30}} \\ \frac{\sqrt{1}}{\sqrt{6}} & 0 & \frac{\sqrt{5}}{\sqrt{6}} \end{pmatrix}, \quad U_1 = \begin{pmatrix} \frac{\sqrt{1}}{\sqrt{6}} & -\frac{\sqrt{1}}{\sqrt{2}} & -\frac{\sqrt{1}}{\sqrt{6}} \\ \frac{\sqrt{1}}{\sqrt{6}} & \frac{\sqrt{1}}{\sqrt{2}} & -\frac{\sqrt{1}}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} & 0 & \frac{\sqrt{1}}{\sqrt{3}} \end{pmatrix}. \tag{3.34}$$

U je tedy reprezentováno maticí 8×8, která má tvar

$$U = \begin{pmatrix} \frac{\sqrt{2}}{\sqrt{3}} & 0 & 0 & 0 & 0 & -\frac{\sqrt{1}}{\sqrt{5}} & -\frac{\sqrt{2}}{\sqrt{15}} & 0 \\ 0 & \frac{\sqrt{1}}{\sqrt{6}} & -\frac{\sqrt{1}}{\sqrt{2}} & 0 & 0 & 0 & 0 & -\frac{\sqrt{1}}{\sqrt{6}} \\ 0 & \frac{\sqrt{1}}{\sqrt{6}} & \frac{\sqrt{1}}{\sqrt{2}} & 0 & 0 & 0 & 0 & -\frac{\sqrt{1}}{\sqrt{3}} \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{\sqrt{1}}{\sqrt{6}} & 0 & 0 & 0 & 0 & \frac{\sqrt{4}}{\sqrt{5}} & -\frac{\sqrt{1}}{\sqrt{30}} & 0 \\ \frac{\sqrt{1}}{\sqrt{6}} & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{5}}{\sqrt{6}} & 0 \\ 0 & \frac{\sqrt{2}}{\sqrt{3}} & 0 & 0 & 0 & 0 & 0 & \frac{\sqrt{1}}{\sqrt{3}} \end{pmatrix} \tag{3.35}$$

3.3 Operace provázání dvou částic

V této sekci ukážeme, dle [4], třídu univerzálních procesů, které provazují dvě částice, což odpovídá podmínce, že výsledný stav procesu neobsahuje žádnou separabilní komponentu. V práci [10] je ukázáno, že každý stav dvoučásticového systému ρ lze dekomponovat na separabilní a neseparabilní část ρ_{sep} a ρ_{insep} tak, že platí $\rho = \lambda\rho_{sep} + (1-\lambda)\rho_{insep}$, kde $0 \leq \lambda \leq 1$. Ačkoli sama dekompozice není jednoznačná, maximální možná hodnota λ je. Je tedy zajímavé hledat parametry univerzálních procesů, jejichž výstupní stavy mají maximální λ rovno nule.

Začneme opět od rovnice (2.17). 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

$$p_1 = 0, \quad p_3 = 0. \tag{3.36}$$

V práci [4] je ukázáno, že jde o podmínku postačující k tomu, aby výsledný stav už žádnou separabilní komponentu neobsahoval. Při těchto parametrech plyne ze vztahů (2.21) $\lambda_{4-} = 0$ a z podmínky nezápornosti vlastních čísel matice hustoty a vztahu pro λ_{2-} dostaneme

$$\begin{aligned}
\alpha^{(1)} &= \alpha^{(2)}, \\
\beta &= \beta^*, \\
\rho_2^{(ent)} &= \frac{1}{2(N-1)} \sum_{j=2}^{N} \big(|1j\rangle\langle 1j| + |j1\rangle\langle j1| - \\
&\quad |1j\rangle\langle j1| - |j1\rangle\langle 1j| \big), \\
\rho_4^{(ent)} &= \frac{1}{(N-1)(N-2)} \sum_{2=i<j}^{N} \big(|ij\rangle\langle ij| + |ji\rangle\langle ji| - \\
&\quad |ij\rangle\langle ji| - |ji\rangle\langle ij| \big).
\end{aligned} \tag{3.37}$$

Společně s parametry (3.36) a vztahem (2.17) získáváme

$$\rho_{out}^{(ent)}(\mathbf{m}_0 = N\mathbf{A}_{11}) = (1-p_4)\rho_2^{(ent)} \oplus p_4\rho_4^{(ent)}. \tag{3.38}$$

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 [11]. Dle této práce je negativita $N(\rho)$ libovolné dvoučásticové matice hustoty mírou provázání, kde

$$N(\rho) = |\sum_i \mu_i| \tag{3.39}$$

a μ_i jsou záporná vlastní čísla částečné transpozice, viz [12],[13], ρ^T matice hustoty ρ. Z vlastností $N(\rho)$ a tvaru (3.38) plyne horní odhad

$$N(\rho_{out}(\mathbf{m}_0)) \leq \frac{1}{2\sqrt{N-1}} + p_4 \left(\frac{1}{N-1} - \frac{1}{2\sqrt{N-1}} \right), \tag{3.40}$$

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 pro $p_4 = 1$, a tedy $p_2 = 0$, a pro $N > 5$ je optimální provazovací proces určen podmínkou $p_4 = 0$, a tedy $p_2 = 1$. Právě tímto naposledy zmíněným procesem se budeme dále zabývat a směřovat k dekompozici jeho unitární realizace. Lze ukázat, že

pokud $\rho_{in} = \frac{1}{N}|\psi\rangle\langle\psi| \otimes I$, bude Krausovým operátorem tohoto procesu projektor na antisymetrický podprostor A dvoučásticového Hilbertova prostoru, tj.

$$\mathcal{E}(\rho) = \frac{2}{N-1} A(\rho \otimes I)A. \tag{3.41}$$

Inspirujeme-li se operací klonování částice, je dobrým kandidátem na unitární realizaci operátor

$$U|i\rangle|X\rangle = \beta \sum_{j \neq i} \big(|ij\rangle - |ji\rangle\big)|j\rangle \tag{3.42}$$

Vektory $U|i\rangle|X\rangle$ jsou jistě ortogonální a z normovací podmínky dostaneme

$$1 = \beta^2 \sum_{j,k \neq i} (\langle ij| - \langle ji|)(|ik\rangle - |ki\rangle)\delta_{kj} = 2\beta^2(N-1), \tag{3.43}$$

a tedy lze volit $\beta = \sqrt{\frac{1}{2(N-1)}}$. Je třeba ukázat, že takto, částečně, definovaná unitární transformace skutečně realizuje proces (3.41). Pro počáteční stav $|\psi\rangle = \sum_j \alpha_j |j\rangle$ platí

$$\begin{aligned} \mathcal{E}(|\psi\rangle\langle\psi|) &= \frac{2}{N-1} \sum_{i,j,k} \alpha_i \bar{\alpha}_j A|ik\rangle\langle jk|A \\ &= \frac{1}{2(N-1)} \sum_{i,j,k} \alpha_i \bar{\alpha}_j \big(|ik\rangle - |ki\rangle\big)\big(\langle jk| - \langle kj|\big). \end{aligned} \tag{3.44}$$

Pokud počáteční stav rozšíříme o referenční stav a ancilluna, získáme po aplikaci U a provedení stopy přes ancillu

$$\begin{aligned} \rho_{out} &= \mathrm{Tr}_A U|\psi\rangle\langle\psi| \otimes |X\rangle\langle X|U^\dagger = \mathrm{Tr}_A \sum_{i,j} \alpha_i \bar{\alpha}_j U|i\rangle|X\rangle\langle j|\langle X|U^\dagger \\ &= \frac{1}{2(N-1)} \mathrm{Tr}_A \sum_{i,j} \alpha_i \bar{\alpha}_j \sum_{k \neq i, l \neq j} \big(|ik\rangle - |ki\rangle\big)\big(\langle jl| - \langle lj|\big) \otimes |k\rangle\langle l| \\ &= \frac{1}{2(N-1)} \sum_{i,j} \alpha_i \bar{\alpha}_j \sum_{k \neq i,j} \big(|ik\rangle - |ki\rangle\big)\big(\langle jk| - \langle kj|\big) \end{aligned} \tag{3.45}$$

Vidíme, že předchozí výraz je roven pravé straně rovnice (3.44) a unitární operátor (3.42) tedy skutečně realizuje proces provázání dvou částic charakterizovaný $p_4 = 0$.

3.4 Dekompozice operace provázání

Stejně jako jsme ve 3.2 dekomponovali operátor realizující kopírování, rozložíme nyní operátor U provázání dvou částic dimenze N definovaný vztahem (3.42). Pro zpřehlednění zápisu přepíšeme operátor U tak, že působí na Hilbertově prostoru $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_O$, kde A, resp. B, resp. O značí Hilbertův prostor ancilly, resp. referenčního systému, resp. originálu. Počáteční stav ancilly i referenční stav zvolme $|0\rangle$. Potom

$$U|0\rangle|0\rangle|i\rangle = \beta \sum_{j\neq i} |j\rangle\big(|ji\rangle - |ij\rangle\big) \tag{3.46}$$

a je patrné, že lze postupovat obdobně jako u operace klonování, neboť lze U opět zapsat jako direktní součet operátorů působících na jistých podprostorech $\mathcal{H}$. Definujme

$$\begin{aligned}
\mathcal{X}_0 &= \mathrm{span}\{|000\rangle, |jj0\rangle, |j0j\rangle; j \neq 0\}, && (3.47)\\
\mathcal{X}_i &= \mathrm{span}\{|jji\rangle, |jij\rangle; j \neq i\}, \quad i \neq 0, && (3.48)\\
\hat{\mathcal{X}} &= \mathrm{span}\{|nnn\rangle, |klm\rangle; m \neq k \neq l, n \neq 0\} && (3.49)
\end{aligned}$$

a operátory identit Id_i, $\hat{\mathrm{Id}}$ a $\hat{\mathrm{Id}}_i$ zaveďme stejně jako v případě klonování. Označme $N_i = \dim\mathcal{X}_i$. Můžeme opět psát $\mathcal{H} = \hat{\mathrm{Id}} \oplus \sum_i \oplus \mathcal{X}_i$. Podprostor $\mathcal{X}_0$ se od ostatních $\mathcal{X}_i$ liší proto, aby bylo zaručeno, že diagonální prvek matice operátoru na podprostoru $\mathcal{X}_i$ ve výpočetní bázi byl zároveň diagonálním prvkem matice operátoru na $\mathcal{H}$.

Operátor U lze potom psát ve tvaru (3.19). V maticích U_i jsou vztahem (3.46) určeny vždy pouze první sloupce, a proto, pokud vhodně dopočítáme zbylé prvky matic, lze psát

$$\begin{aligned}
U &= \prod_{i=0}^{N-1} (\hat{\mathrm{Id}}_i \oplus U_i) = \prod_{i=0}^{N-1} \left(\hat{\mathrm{Id}}_i \oplus \prod_{j=1}^{N_i} R_{ij} \right)\\
&= \prod_{i=1}^{N-1} \prod_{j=1}^{N_i} \left(\hat{\mathrm{Id}}_i \oplus R_{ij} \right). && (3.50)
\end{aligned}$$

Úloha dekompozice U se i v tomto případě redukuje na dekompozici matic U_k a vzhledem k tvaru matice zůstávají v platnosti i vztahy (3.22) až (3.27), pouze je třeba pozměnit meze součinů tak, aby odpovídali dimenzím podprostorů. Získáváme tedy ihned tvar matice U_k

$$\begin{aligned}
(U_k)_{ab} &= \sigma_a \left[\left(\prod_{j=a+1}^{N_k} \gamma_j \right) \delta_{1b} - \sum_{l=a+1}^{N_k} \left(\prod_{j=a+1}^{l-1} \gamma_j \right) \sigma_l \delta_{lb} \right]\\
&+ \gamma_a \delta_{ab}, \qquad a, b = 1, \ldots, N_k. && (3.51)
\end{aligned}$$

a zbývá odvodit příslušné parametry rotací. V tomto smyslu je proces provázání obecnější, neboť kromě nezáporných prvků prvních sloupců matic U_i se zde objevují i prvky záporné.

Vyjděme opět z podmínky, že první sloupec se diagonalizací převede na sloupec o složkách $(1, 0, \ldots, 0)$. Z toho plyne podmínka

$$0 = -\sigma_i \beta^1_{(i)} + \gamma_i \beta^i, \quad i = 2, \ldots, 2N-2, \text{ resp. } 2N-1. \tag{3.52}$$

Aby bylo možno rovnici umocnit a vyřešit je třeba přidat podmínku[3]

$$\mathrm{sign}\sigma_i = \mathrm{sign}\beta^1_{(i)}, \qquad \mathrm{sign}\gamma_i = \mathrm{sign}\beta^i. \tag{3.53}$$

Řešením jsou potom vztahy

$$\gamma_i = \frac{\mathrm{sign}\beta^i |\beta^1_{(i)}|}{\sqrt{(\beta^1_{(i)})^2 + (\beta^i)^2}} \tag{3.54}$$

$$\sigma_i = \frac{\mathrm{sign}\beta^1_{(i)} |\beta^i|}{\sqrt{(\beta^1_{(i)})^2 + (\beta^i)^2}} \tag{3.55}$$

Dosazením předchozích vztahů do první rovnosti v (3.23) ještě odvodíme explicitní předpis pro $\beta^1_{(i)}$

$$\begin{aligned} \beta^1_{(i)} &= \gamma_{i-1}\beta^1_{i-1} + \sigma_{i-1}\beta^{i-1} = \frac{\mathrm{sign}\beta^{i-1}|\beta^1_{(i-1)}|\beta^1_{(i-1)} + \mathrm{sign}\beta^1_{(i-1)}|\beta^{i-1}|\beta^{i-1}}{\sqrt{(\beta^1_{(i-1)})^2 + (\beta^{i-1})^2}} \\ &= \mathrm{sign}\beta^{i-1}\mathrm{sign}\beta^1_{(i-1)}\sqrt{(\beta^1_{(i-1)})^2 + (\beta^{i-1})^2} \\ &= \mathrm{sign}\beta^{i-1}\mathrm{sign}\beta^1_{(i-1)}\sqrt{\sum_{j=1}^{i-1}(\beta^j)^2}. \end{aligned} \tag{3.56}$$

a vztahy (3.54) a (3.55) lze přepsat do elegantní podoby

$$\gamma_i = \frac{\beta^1_{(i)}}{\beta^1_{(i+1)}} \tag{3.57}$$

$$\sigma_i = \frac{\beta^i}{\beta^1_{(i+1)}}. \tag{3.58}$$

[3] $\mathrm{sign}0 \equiv 1$

Pomocí vztahů (3.51), (3.57), (3.58) a (3.56) již můžeme dodefinovat unitární realizaci (3.42) a sestrojit její rozklad do dvoudimenzionálních podprostorů. Na závěr uveďme příklad pro $N = 3$ (příklad pro $N = 2$ není příliš demonstrativní, neboť antisymetrický podprostor $\mathcal{H}$ je jednorozměrný)

$$\gamma_{02} = 0, \quad \gamma_{03} = \frac{1}{\sqrt{2}}, \quad \gamma_{04} = -\frac{\sqrt{2}}{\sqrt{3}}, \quad \gamma_{05} = \frac{\sqrt{3}}{2} \tag{3.59}$$

$$\sigma_{02} = 1, \quad \sigma_{03} = -\frac{1}{\sqrt{2}}, \quad \sigma_{04} = -\frac{1}{\sqrt{3}}, \quad \sigma_{05} = \frac{1}{2}, \tag{3.60}$$

$$\gamma_{12} = -\frac{1}{\sqrt{2}}, \quad \gamma_{13} = -\frac{\sqrt{2}}{\sqrt{3}}, \quad \gamma_{14} = -\frac{\sqrt{3}}{2}, \tag{3.61}$$

$$\sigma_{12} = \frac{1}{\sqrt{2}}, \quad \sigma_{13} = -\frac{1}{\sqrt{3}}, \quad \sigma_{14} = \frac{1}{2}, \tag{3.62}$$

$$\gamma_{22} = -\frac{1}{\sqrt{2}}, \quad \gamma_{23} = \frac{\sqrt{2}}{\sqrt{3}}, \quad \gamma_{24} = -\frac{\sqrt{3}}{2}, \tag{3.63}$$

$$\sigma_{22} = \frac{1}{\sqrt{2}}, \quad \sigma_{23} = -\frac{1}{\sqrt{3}}, \quad \sigma_{24} = -\frac{1}{2}, \tag{3.64}$$

$$U_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ -\frac{1}{2} & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{12}} \\ \frac{1}{2} & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{12}} \\ -\frac{1}{2} & 0 & 0 & -\frac{\sqrt{2}}{\sqrt{3}} & \frac{1}{\sqrt{12}} \\ \frac{1}{2} & 0 & 0 & 0 & \frac{\sqrt{3}}{2} \end{pmatrix}, \tag{3.65}$$

$$U_1 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{12}} \\ -\frac{1}{2} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{12}} \\ -\frac{1}{2} & 0 & -\frac{\sqrt{2}}{\sqrt{3}} & \frac{1}{\sqrt{12}} \\ \frac{1}{2} & 0 & 0 & \frac{\sqrt{3}}{2} \end{pmatrix}, \tag{3.66}$$

$$U_2 = \begin{pmatrix} \frac{1}{2} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{6}} & -\frac{1}{\sqrt{12}} \\ -\frac{1}{2} & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{6}} & \frac{1}{\sqrt{12}} \\ \frac{1}{2} & 0 & \frac{\sqrt{2}}{\sqrt{3}} & -\frac{1}{\sqrt{12}} \\ -\frac{1}{2} & 0 & 0 & -\frac{\sqrt{3}}{2} \end{pmatrix}. \tag{3.67}$$

Celá matice U má rozměr 27×27, a proto ji zde nebudeme vypisovat. Kompozice U pomocí U_0, U_1 a U_2 se snadno provede použitím vztahu (3.50).

Závěr

V práci byly zkoumány možnosti realizace dvou univerzálních procesů, a to optimálního kopírování z jedné částice na dvě a jednoho zástupce jednoparametrické třídy univerzálních provazovacích procesů. Se znalostí unitární realizace klonování jsme odvodili unitární operátor realizující tento provazovací proces. Ukázali jsme, že oba tyto procesy lze rozložit na direktní součet operátorů U_k působících na menších podprostorech, a proto lze problém dekompozice na rotace ovlivňující pouze dva vektory výpočetní báze redukovat na hledání rozkladu těchto sčítanců. V obou případech se nám podařilo najít explicitní výraz pro tvar jejich matic daných (3.27), resp. (3.51) pro kopírování, resp. provázání, i posloupnosti argumentů matic rotací, které tvoří dekompozici operátorů U_k, (3.29), (3.30), (3.31), resp. (3.56), (3.57), (3.58) pro kopírování, resp. provázání. Navíc tento rozklad výrazně optimalizuje počet rotací potřebných k dekompozici operátorů.

Předmětem dalšího zkoumání je najít unitární realizace širší třídy univerzálních procesů a zkonstruovat jejich rozklady. Tento úkol není v obecné šíři nijak jednoduchý a možné cesty, které se nabízejí je hledání Krausových reprezentací těchto procesů nebo využití principu purifikace a hledání operátorů na nějakém rozšířeném systému.

Literatura

[1] P. W. Shor (1996), Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, quant-ph/9508027.

[2] W. K. Wooters (1982), W. H. Zurek, Nature 299, 802.

[3] R. F. Werner, Optimal cloning of pure states, quant-ph/9804001.

[4] G. Alber, A. Delgado, I. Jex (2001), Optimal Two-Particle Entanglement by Universal Quantum Processes, Quant. Inf. and Comp. 1(3), 33.

[5] M. A. Nielsen, I. L. Chuang (2000), Quantum Computation and Quantum Information, Cambridge University Press.

[6] V. Buzek, M. Hillery (1998), Universal Optimal Cloning of Arbitrary Quantum States: From Qubits to Quantum Registers , Phys. Rev. Lett. 81, 5003–5006.

[7] K.Kraus (1983), States, Effects, Operations: Fundamental Notions of Quantum Theory, Springer-Verlag, Berlin.

[8] C. S. Niu, R. B. Griffiths (1998), Optimal copying of one quantum bit, Phys. Rev. A 58, 4377.

[9] N. Cerf (2000), Pauli Cloning of a Quantum Bit, Phys. Rev. Lett. 84, 4497.

[10] M. Lewenstein, A. Sanpera (1998), Separability and Entanglement of Composite Quantum Systems, Phys. Rev. Lett. 80, 2261.

[11] G. Vidal, R.F. Werner (2002), A Computable Measure of Entanglement, quant-ph/0102117.

[12] Peres A. (1996), Separability Criterion for Density Matrices, Phys. Rev. Lett. 77, 1413.

[13] Horodecki M., Horodecki P., Horodecki R. (1996), Separability of Mixed States: Necessary and Sufficient Conditions, Phys. Lett. A 223, 1.

[14] V. Buzek, M. Hillery (1998), Universal Optimal Cloning of Qubits and Quantum Registers, quant-ph/9801009.

[15] N. Gisin, S. Massar (1997), Optimal Quantum Cloning Machines, Phys. Rev. Lett. 79 (11), 2153.

[16] M. Stefanak (2003), Many Particle Universal Processes, Diploma thesis.