Otevřené kvantové systémy
–
02OKS

18. září 2021

Obsah

1 Přehled značení **2**

2 Úvod **3**

2.1 Vývoj v uzavřeném kvantovém systému 4

3 Operátor hustoty **5**

3.1 Evoluce operátoru hustoty 7

3.2 Popis složeného systému 7

3.3 Schmidtův rozklad 8

3.4 Klasifikace stavů podle korelací 10

4 Matematický aparát **12**

4.1 Izomorfizmy 12

4.2 Kleinova nerovnost 16

4.3 Peierlova nerovnost 17

5 von Neumannova entropie **18**

5.1 Relativní entropie 20

6 Kvantové měření **23**

6.1 von Neumannovo měření 23

6.2 Zobecněné měření 24

7 Kvantové operace **28**

7.1 Vlastnosti kvantových operací 30

7.2 Kvantové operace teleportací 34

7.3 Krausova reprezentace 35

7.4 Stinespringova reprezentace 38

7.5 Neumarkova reprezentace 41

8 Změny kvantového systému **43**

8.1 Časová spojitost 45

8.1.1 Homogenní Markovovské procesy 49

8.2 Spektrální vlastnosti 50

1 Přehled značení

A^*	komplexní sdružení operátoru A
A^T	transponovaná matice k matici A
$A^\dagger$	hermitovské sdružení operátoru A
$\mathscr{H}$	Hilbertův stavový prostor
$\mathcal{B}(\mathscr{H})$	Hilbertův prostor všech omezených operátorů definovaných na stavovém prostoru $\mathscr{H}$
$\mathcal{S}(\mathscr{H})$	prostor všech operátorů hustoty definovaných na prostoru $\mathscr{H}$
ρ	operátor hustoty
$\otimes$	tenzorový součin
$\operatorname{Ker} A$	jádro operátoru A
$\operatorname{Ran} A$	obor hodnot operátoru A
$\operatorname{supp} A$	nosič operátoru A
$\sup M$	supremum množiny M
$\operatorname{Tr} A$	stopa operátoru A
$\operatorname{Tr}_{(\mathscr{H})}$ A	stopa operátoru A s explicitním vyjádřením prostoru $\mathscr{H}$, na kterém je operátor definován
$\operatorname{Tr}_{\mathscr{H}_B} A$	částečná stopa operátoru $A \in \mathcal{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$ přes prostor $\mathscr{H}_B$

2 Úvod

V běžných kurzech kvantové fyziky jsme se dosud setkali se systémy jako jsou volné částice, jejich shluky či částice podléhající vlivu okolního silového pole. Celý systém částice spolu s působícím polem šlo přitom považovat za izolovaný, nevyměňující si hmotu či energii s nějakým jiným systémem. Ve skutečnosti samozřejmě žádný takový, dokonale izolovaný, systém neexistuje. Pojem izolovaného systému slouží spíše jako idealizace skutečnosti, se kterou lze rozumně počítat a ke které se reálně můžeme pouze více či méně přiblížit. U dostatečně izolovaných systémů bude tato aproximace použitelná. Pro vývoj takovýchto systémů se v úvodních kurzech odvozovali různé rovnice – Schrödingerova rovnice, Klein-Gordonova rovnice, Diracova rovnice atd. Například v případě Schrödingerovy rovnice jsme mohli vývoj systému popsat pomocí evolučního operátoru, unitárního operátoru působícího na stav systému. Skutečnost, že daný operátor je unitární, zapříčiňuje časovou reverzibilitu vývoje daného systému. Během evoluce se tedy informace o stavu systému neztrácí a mezi každými dvěma časovými okamžiky existuje invertibilní operátor převádějící stav systému v jednom okamžiku na stav v okamžiku druhém.

Co ale když vývoj zkoumaného systému nelze popsat bez současného vlivu okolí? Pod *okolím* daného systému rozumíme nějaký jiný systém, jehož vývoj nejsme schopni plně zachytit a jeví se nám jako narušitel, se kterým zkoumaný systém nevyhnutelně interaguje. V reálném světě může jít například o zbytkové magnetické pole, které nevhodně působí na zkoumaný spin a jehož vliv přitom není experimentátor s to potlačit ani nijak kontrolovaně ovládat. Podobným narušitelem mohou být i částice, které se uvolňují z měřící aparatury a interagují se zkoumanou částicí. Příkladů by šlo samozřejmě najít mnoho a to nejen těch z laboratorního prostředí. Vývoj takovéhoto systému vystaveného vlivům prostředí již nelze popsat jednoduše pomocí evolučního operátoru. Časový vývoj již není obecně reverzibilní, část informace o počátečním stavu se vytrácí do okolí. Pokud máme na začátku například vzorek částic se spinem mířícím ve stejném směru, po dostatečně dlouhé době budou tyto spiny vlivem okolních polí a okolních interagujících částic namířeny zcela nahodile. Informace uložená na počátku, spiny namířené stejným směrem, byla vlivem okolí odnešena ze zkoumaného systému. Tato informace o počátečním rozložení spinů je sice stále přítomna, je ale ukryta ve stavu okolí, s nímž nelze dobře manipulovat a jenž nelze dobře měřit.

Právě popsaným systémům, které jsou vystaveny všetečným a neodstranitelným vlivům okolí, budeme říkat *otevřené (kvantové) systémy*. Jejich časový vývoj budeme označovat jako *vývoj otevřeného systému*, *otevřený vývoj*, *otevřená evoluce* či *otevřená dynamika*. Pokud budeme uvažovat složený systém skládající se ze studovaného systému a jeho okolí, nazveme tento *složený systém*, *celý systém* či prostě jen *systém*. *Studovaný systém* budeme nazývat též *zkoumaný systém* a konečně *okolí* budeme označovat též jako *prostředí*. Vedle okolí se při studiu kvantových systémů uvažují i pomocné systémy, které nelze označit za okolí a které jsou do úlohy zavedeny více méně uměle, aby zjednodušili manipulaci se zkoumaným systémem. Pro systém takto přidaný budeme užívat buď název *pomocný systém* či anglický název *ancilla*.

Na rozdíl od tradičních kurzů o kvantové fyzice provedeme ještě jednu změnu. Zatímco dosud se pracovalo s kvantovými systémy o nekonečněrozměrných stavových prostorech, jakým byl například prostor vlnových funkcí volné částice, zde se omezíme na Hilbertovy prostory stavů, které mají dimenzi *konečnou*. Operátory řídící vývoj otevřených systémů tak lze reprezentovat pomocí matic, což budeme i v mnoha důkazech využívat. Nejtypičtějším příkladem kvantového systému s konečněrozměrným stavovým prostorem je právě částice se spinem, kde studujeme pouze spinové stupně volnosti. Dalším příkladem může být polarizace fotonů, jejíž stavový prostor je dvourozměrný. Konečněrozměrné Hilbertovy prostory můžeme obdržet i v případě, kdy uvažujeme elektrony vázané v orbitalech atomů. Pokud předpokládáme, že excitace elektronu na příliš vysoké energetické hladiny jsou prakticky nemožné, je stavový prostor takovýchto elektronů, alespoň co se jejich energie týče, též konečněrozměrný.

2.1 Vývoj v uzavřeném kvantovém systému

Jak již bylo předesláno v úvodu, vývoj otevřených systémů se od vývoje těch uzavřených liší. Připomeňme si v krátkosti některé z výsledků kvantové teorie pro uzavřené systémy. Tyto výsledky pak budeme moci konfrontovat s výsledky získanými pro otevřené systémy. Vývoj v uzavřeném systému je generován odpovídajícím Hamiltoniánem H prostřednictvím Schrödingerovy rovnice

$$\mathrm{i}\,\frac{\mathrm{d}\,|\psi(t)\rangle}{\mathrm{d}t} = H|\psi(t)\rangle \quad (\hbar = 1). \tag{1}$$

Předpokládáme-li nezávislost Hamiltoniánu na čase, můžeme zavést evoluční operátor ve tvaru $U(t_2, t_1) = U(t_2 - t_1)$. Časový vývoj systému, jehož stav v čase t označíme $|\psi(t)\rangle$, pak můžeme vyjádřit pomocí evolučního operátoru v kompaktním tvaru $|\psi(t_2)\rangle = U(t_2, t_1)|\psi(t_1)\rangle$. Norma stavového vektoru přitom zůstává zachována, $\frac{\mathrm{d}}{\mathrm{d}t}\langle\psi(t)|\psi(t)\rangle = 0$, jak se lze snadno přesvědčit z rovnice výše. Žádná informace o stavu systému tedy neproudí pryč. Z čistého stavu dostaneme opět čistý stav (pro podrobnosti viz později). Navíc evoluční operátory $U(t)$ tvořící jednoparametrickou grupu transformací popisují časově reverzibilní vývoj. Jak uvidíme, u otevřených systémů žádná z těchto věcí už nebude pravda.

Protože $HH^\dagger = H^\dagger H$, je Hamiltonián diagonalizovatelný v ortonormální bázi svých vlastních vektorů. Opět, v případě otevřených kvantových systémů už generátor časového vývoje obecně diagonalizovat nepůjde.

V následující kapitole probereme ze všeho nejdřív způsob, jakým popisovat stav kvantového systému. Jednou z dalších odlišností je totiž fakt, že při popisu otevřeného systému se již nelze spolehnout na vektory z Hilbertova prostoru coby nositele informací o daném stavu.

3 Operátor hustoty

Popisujeme-li vývoj *uzavřeného* kvantového systému, vystačíme si většinou s pojmem *čistého stavu*. Jedná se o vektor v Hilbertově prostoru $\mathscr{H}$, který je danému kvantovému systému přidružen. Na daném Hilbertově prostoru je definován skalární součin, my si tento budeme značit v souhlase s Diracovou notací jako $\langle\cdot|\cdot\rangle$. Spolu s vektory Hilbertova prostoru uvažujeme i zobrazení, která na těchto vektorech působí. Neboť se omezujeme pouze na konečněrozměrné Hilbertovy prostory, jsou všechny operátory definované na daném Hilbertově prostoru h omezené, a tedy $\mathcal{B}(\mathscr{H})$ představuje množinu všech operátorů. Omezené operátory samotné tvoří další Hilbertův prostor, zavedeme-li na něm *Hilbert-Schmidtův skalární součin* následujícím způsobem. Mějme dva operátory $A, B \in \mathcal{B}(\mathscr{H})$, pak jejich skalární součin je definován vztahem

$$(A, B) \equiv \mathrm{Tr}(A^\dagger B), \tag{2}$$

kde $A^\dagger$ je operátor hermitovsky sdružený k operátoru A a $\mathrm{Tr}(cdot)$ značí stopu operátoru, viz sekci 1. V prostoru operátorů můžeme dále vydělit množinu všech *pozorovatelných* $\{A \in \mathcal{B}(\mathscr{H}) | A^\dagger = A\}$ *na prostoru* $\mathscr{H}$ tvořenou hermitovskými operátory. Jak bylo předesláno, dosud se pracovalo především s čistými stavy, vektory. Operátory představující vývoj systému či měření vzaly vektor a vrátili jiný vektor. Když jsme měli jistou pozorovatelnou A, dostali jsme jejím změřením na daném čistém stavu $|\psi\rangle$ číslo, které bylo vlastním číslem operátoru A a které jsme interpretovali jako výsledek měření. Pokud přitom nebyl vektor $|\psi\rangle$ vlastním vektorem pro A, obdrželi jsme různá čísla s různou pravděpodobností výskytu.

Důležité bylo si uvědomit, že vše, co o daném stavu kvantového systému jsme schopni zjistit, jsou průměrné hodnoty nejrůznějších veličin. Výsledek jediného měření na daném stavu neměl valné hodnoty. Rozlišujme nyní na chvíli důsledně dva pojmy, stav systému ψ a jemu příslušný vektor $|\psi\rangle$. Stavem systému máme na mysli soubor všech jeho vlastností. Pro popis stavu kvantového systému tak je nezbytné uvést střední hodnoty $\langle A\rangle_\psi$ všech pozorovatelných A na daném stavu působících. V případě stavů uzavřených systémů byla situace jednodušší v tom, že místo vypisování všech těchto středních hodnot jsme měli prostředek, jak je snadno spočítat. Tímto prostředkem byl vektor $|\psi\rangle$, z něhož jsme odpovídající střední hodnotu pozorovatelné A obdrželi vypočtením výrazu $\langle\psi|A|\psi\rangle$, který jsme prohlásili za střední hodnotu $\langle A\rangle_\psi$. Pokud se dal stav systému takto popsat pomocí vektoru, nazvali jsme ho čistým stavem.

Použijme analogický postup v širším kontextu. Opusťme zažitou představu čistých stavů a definujme si stav jako zobrazení, které každé pozorovatelné přiřazuje reálné číslo, na které naklademe pár podmínek. Máme tedy přesně to, co chceme. Dané zobrazení vezme pozorovatelnou A a vrátí odpovídající střední hodnotu $\langle A\rangle$. Korektní definice zní následovně.

Definice 3.1. Stavem systému nazveme lineární funkcionál $S : \mathcal{B}(\mathscr{H}) \to \mathbb{R}$ splňující dodatečné podmínky:

1. Normalizace: $S(\mathbb{I}) = 1$. (To jest, na identitu vrátí jedničku.)

2. Pozitivita: $S(A^\dagger A) \geq 0$, $\forall A \in \mathcal{B}(\mathscr{H})$. (To jest, na každý pozitivní operátor vrátí nezáporné číslo.)

Rieszova věta říká, že pro každý lineární funkcionál S najdeme operátor $\rho \in \mathcal{B}(\mathscr{H})$ tak, že $S(A) = (\rho, A) = \mathrm{Tr}(\rho^\dagger A)$ pro každý $A \in \mathcal{B}(\mathscr{H})$. O tomto operátoru si ukážeme, že je hermitovský a má jednotkovou stopu. Pro důkaz $\rho = \rho^\dagger$ ukážeme, že $(\rho, A) = (\rho^\dagger, A)$ pro každý operátor $A \in \mathcal{B}(\mathscr{H})$. Rovnost však stačí ukázat pro A hermitovkské, jelikož skalární součin je bilineární a každý operátor $A \in \mathcal{B}(\mathscr{H})$ je možné napsat jako součet dvou hermitovských operátorů $A = A_1 + iA_2 = (A + A^\dagger)/2 + i\left(i(-A + A^\dagger)/2\right)$. Nyní využijeme toho, že $S(\cdot)$ je reálné číslo, a tedy $S(\cdot) = S(\cdot)^*$. Pak dostáváme $(\rho, A) = \mathrm{Tr}(\rho^\dagger A) = S(A) = S(A)^* = \mathrm{Tr}(\rho^\dagger A)^* = \mathrm{Tr}(\rho^T A^*) = \mathrm{Tr}((\rho^T A^*)^T) = \mathrm{Tr}(A^\dagger \rho) = \mathrm{Tr}(\rho A^\dagger) = \mathrm{Tr}(\rho A) = (\rho^\dagger, A)$. Z normalizační podmínky navíc vyplývá $1 = S(\mathbb{I}) = \mathrm{Tr}(\rho^\dagger \mathbb{I}) = \mathrm{Tr}(\rho)$. Druhá definiční vlastnost nám přitom zajišťuje $0 \le S(C) = \mathrm{Tr}(\rho C)$ pro všechny pozitivní operátory C. Pokud zvolíme $C = |\psi\rangle\langle\psi|$, tak $\mathrm{Tr}(\rho C) = \mathrm{Tr}(\rho|\psi\rangle\langle\psi|) = \langle\psi|\rho|\psi\rangle \ge 0$ pro všechny $|\psi\rangle \in \mathscr{H}$. Operátor ρ je tedy dokonce pozitivní.

Definice 3.2. Operátor z úvah výše se nazývá **operátor hustoty**, popř. **matice hustoty**. Neboť pozitivita již vynucuje hermitovost, tak lze operátor hustoty charakterizovat jako *pozitivní operátor s jednotkovou stopou*, tj. $\rho \ge 0$ a $\mathrm{Tr}(\rho) = 1$.

Z definičních vlastností plyne, že obecný operátor hustoty lze vyjádřit ve tvaru $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$, kde $\lambda_i \ge 0$, $\sum_i \lambda_i = 1$ a $\{\psi_i\}_i$ je ortonormální báze tvořená jeho vlastními vektory. Vidíme, že ač jsme si stav definovali jako jistý lineární funkcionál, veškerou práci se stavem daného systému lze redukovat na počítání s jemu odpovídající maticí hustoty. V následujícím budeme pojmy *operátor hustoty* a *stav* volně zaměňovat.

Množinu všech stavů na daném Hilbertově prostoru $\mathscr{H}$ označíme $\mathcal{S}(\mathscr{H})$. Jedná se o konvexní množinu, neboť konvexní kombinace operátorů hustoty je opět operátor hustoty. Extremálními body této množiny jsou přitom *čisté stavy*, tj. stavy, jejichž operátor hustoty je projektor $\rho = |\psi\rangle\langle\psi|$ pro nějaké $|\psi\rangle \in \mathscr{H}$. Máme-li zadán operátor hustoty, jak snadno zjistit, zda popisuje čistý stav? Nutnou a postačující podmínku uvádí následující tvrzení.

Věta 3.1. *Operátor hustoty $\rho \in \mathcal{S}(\mathscr{H})$ popisuje čistý stav právě tehdy, když $\mathrm{Tr}(\rho^2) = 1$.*

Důkaz. Pro důkaz implikace zleva si stačí uvědomit, že když je operátor hustoty ρ čistý stav, tak existuje vektor $|\psi\rangle \in \mathscr{H}$ takový, že $\rho = |\psi\rangle\langle\psi|$ je projektor. Platí tedy $\rho^2 = \rho$ a z normalizace operátoru hustoty ihned $\mathrm{Tr}(\rho^2) = \mathrm{Tr}(\rho) = 1$. Pro důkaz opačné implikace uvažujme obecný tvar operátoru hustoty, $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$, kde $\{|\psi_i\rangle\}_i$ je ortonormální báze a $\{\lambda_i\}_i$ tvoří pravděpodobnostní rozdělení. Jednoduchými výpočty zjistíme, že $\rho^2 = \sum_i \lambda_i^2 |\psi_i\rangle\langle\psi_i|$, jehož stopa je $\mathrm{Tr}(\rho^2) = \sum_i \lambda_i^2$. Neboť je $\lambda_i \ge 0$ a $\sum_i \lambda_i = 1$, z podmínky $\mathrm{Tr}(\rho^2) = 1$ už rovnou plyne, že právě jedno vlastní číslo λ_{i_0} je jednička a ostatní jsou nuly. Kdyby tomu tak nebylo, tak by všechna nenulová vlastní čísla splňovala $\lambda_i < 1$, což implikuje $\lambda_i^2 < \lambda_i$. Máme tedy $1 = \sum_i \lambda_i > \sum_i \lambda_i^2$, což je spor s předpoklady dokazované implikace. Celkem tak máme $\rho = \lambda_{i_0} |\psi_{i_0}\rangle\langle\psi_{i_0}| = |\psi_{i_0}\rangle\langle\psi_{i_0}|$ a ρ je tak čistý stav. □

V případě dvourozměrného Hilbertova prostoru lze operátory hustoty vyjádřit pomocí Pauliho matic. **Pauliho matice** jsou tři 2×2 matice tvaru

$$\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3}$$

Operátory hustoty jsou pak tvaru $\rho = \frac{1}{2}(\mathbb{I} + \tau_1\sigma_X + \tau_2\sigma_Y + \tau_3\sigma_Z)$, kde $\vec{\tau} = (\tau_1, \tau_2, \tau_3) \in \mathbb{R}^3$ je vektor, jehož velikost je $\|\vec{\tau}\| \leq 1$, jinak by ρ nebyl pozitivní operátor. Pro $\|\vec{\tau}\| = 1$ popisuje ρ čistý stav.

3.1 Evoluce operátoru hustoty v uzavřeném systému

Výše jsme uvedli, že se budeme zabývat otevřenými systémy. Udělejme na chvíli krok zpět a koukněme se, jak se operátor hustoty ρ chová v případě uzavřeného systému. Uvažujme $\rho(t) = \sum_i \lambda_i |\psi_i(t)\rangle\langle\psi_i(t)|$ coby funkci času, kde jednotlivé bazické vektory $|\psi_i(t)\rangle$ podléhají Schrödingerově rovnici

$$\mathrm{i}\,\frac{\mathrm{d}\,|\psi_i(t)\rangle}{\mathrm{d}t} = H|\psi_i(t)\rangle, \tag{4}$$

Zderivujeme-li operátor hustoty $\rho(t)$ podle času a dosadíme-li za vzniklé výrazy ze Schrödingerovy rovnice, dospíváme k rovnici tvaru

$$\frac{\mathrm{d}\,\rho(t)}{\mathrm{d}t} = -\mathrm{i}\,[H, \rho(t)] \equiv L(\rho(t)), \tag{5}$$

kde jsme si definovali zobrazení $L : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$, jež se nazývá **Liouvilleův operátor**. Jedná se o antihermitovský lineární superoperátor zachovávající stopu (viz později). Právě uvedenou rovnici budeme moci porovnat s evoluční rovnicí obecného operátoru hustoty, až budeme studovat vývoj otevřených systémů.

Časový vývoj operátoru hustoty lze explicitně v případě uzavřeného systému vyjádřit ve tvaru

$$\rho(t) = U(t)\,\rho(0)\,U^\dagger(t), \tag{6}$$

kde $U(t)$ je jednoparametrický systém jistých unitárních operátorů. Stále platí, že časovým vývojem přejde čistý stav opět na čistý stav. U otevřených systémů už vývoj stavu nepůjde popsat pomocí unitárního operátoru tímto způsobem.

3.2 Popis složeného systému

Velmi důležitým konceptem v kvantové teorii je pojem složeného systému. Každému kvantovému systému je přidružen Hilbertův stavový prostor $\mathscr{H}$. V axiomatickém přístupu kvantové teorie se postuluje, že Hilbertův prostor systému složeného ze systémů A a B je roven tenzorovému součinu $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B$ Hilbertova prostoru $\mathscr{H}_A$ systému A a Hilbertova prostoru $\mathscr{H}_B$ systému B. Množina všech omezených operátorů na prostoru složeného systému je přitom rovna $\mathcal{B}(\mathscr{H}) = \mathcal{B}(\mathscr{H}_A \otimes \mathscr{H}_B) = \mathcal{B}(\mathscr{H}_A) \otimes \mathcal{B}(\mathscr{H}_B)$. Víme tedy, jak ze dvou systémů udělat systém jeden, jakým postupem ale postupovat v opačném směru? Mějme operátor hustoty ρ popisující společný stav podsystémů A a B. Jak vypadá stav podsystému A samotného?

Kdybychom jako ρ_A označili stav samotného podsystému A, platila by pro libovolnou pozorovatelnou M_A působící pouze na podsystému A samozřejmá rovnost $\langle M_A \rangle_{\rho_A} = \mathrm{Tr}(\rho_A\, M_A)$. Neboť pozorovatelná M_A nijak neovlivňuje podsystém B, měla by platit i rovnost vztažená k celému systému $\langle M_A \rangle_{\rho_A} = \mathrm{Tr}(\rho M)$, kde ρ je stav celého systému a M je pozorovatelná M_A

chápaná jako operátor na celém systému. Dohromady tedy $\mathrm{Tr}(\rho M) = \mathrm{Tr}(\rho_A M_A)$. Pokud je celkový stav faktorizovaného tvaru $\rho = \rho_A \otimes \rho_B$, je zřejmě $M = M_A \otimes \mathbb{I}$. Rovnost středních hodnot je pak splněna, neboť $\mathrm{Tr}(\rho M) = \mathrm{Tr}((\rho_A \otimes \rho_B)(M_A \otimes \mathbb{I})) = \mathrm{Tr}(\rho_A M_A)\,\mathrm{Tr}(\rho_B) = \mathrm{Tr}(\rho_A M_A)$. Existuje i jiný tvar vyjma $M = M_A \otimes \mathbb{I}$? Pro všechny ρ_A a ρ_B musí být splněno $\mathrm{Tr}((\rho_A \otimes \rho_B)\,M) = \mathrm{Tr}((\rho_A \otimes \rho_B)\,(M_A \otimes \mathbb{I}))$, to znamená $\mathrm{Tr}((\rho_A \otimes \rho_B)\,(M - M_A \otimes \mathbb{I})) = 0$. Žádný jiný tvar operátoru M již tedy neexistuje. Pro faktorizovaný stav systému $\rho = \rho_A \otimes \rho_B$, kde M_A je pozorovatelná na podsystému A, je odpovídající pozorovatelná M působící na celém systému tvaru $M = M_A \otimes \mathbb{I}$. Neboť je množina faktorizovaných stavů totální v prostoru operátorů, platí získaný výsledek pro všechny stavy ρ.

Musí tedy platit $\mathrm{Tr}(\rho_A\, M_A) = \mathrm{Tr}(\rho(M_A \otimes \mathbb{I}))$. Rozepíšeme-li si stopu explicitně v ortonormální bázi $\{|i^{(A)}\rangle|j^{(B)}\rangle\}_{ij}$, dostáváme $\mathrm{Tr}(\rho(M_A \otimes \mathbb{I})) = \sum_{ij}\langle i^{(A)}|\langle j^{(B)}|(\rho(M_A \otimes \mathbb{I}))|i^{(A)}\rangle|j^{(B)}\rangle = \sum_i \langle i^{(A)}|(\sum_j \langle j^{(B)}|\rho|j^{(B)}\rangle)M_A|i^{(A)}\rangle$. Když si označíme $\rho_A = \sum_j \langle j^{(B)}|\rho|j^{(B)}\rangle$, je poslední výraz roven $\sum_i \langle i^{(A)}|\rho_A M_A|i^{(A)}\rangle = \mathrm{Tr}(\rho_A M_A)$, kde nyní jde stopa již jen přes podsystém A.

Definice 3.3. Vzorec $\sum_j \langle j^{(B)}|\rho|j^{(B)}\rangle$, kterým jsme v předchozím odstavci zavedli operátor ρ_A, nazýváme **částečná stopa** operátoru ρ přes podsystém B (angl. *partial trace over subsystem B*) a značíme $\mathrm{Tr}_B(\rho)$. Neboli

$$\rho_A = \sum_j \langle j^{(B)}|\rho|j^{(B)}\rangle = \mathrm{Tr}_B(\rho). \tag{7}$$

Dobrá, máme zavedený operátor ρ_A, který splňuje požadovanou rovnost středních hodnot, jaký vztah má ale tento operátor ke skutečnému systému A? Ukážeme, že je tento operátor určen jednoznačně. K danému podsystému tedy existuje právě jeden operátor schopný konzistentně popisovat střední hodnoty libovolných pozorovatelných na tomto podsystému. Pro spor nechť existuje nějaký jiný operátor $\tilde{\rho}_A$, pro nějž $\mathrm{Tr}(M_A \tilde{\rho}_A) = \mathrm{Tr}(M\rho)$. Tento operátor lze rozložit do báze prostoru $\mathcal{B}(\mathscr{H}_A)$ tvořené hermitovskými operátory $\{B_i\}_i$. Dostáváme tak rozvoj do Fourierových koeficientů způsobem

$$\tilde{\rho}_A = \sum_i B_i(B_i, \tilde{\rho}_A) = \sum_i B_i \,\mathrm{Tr}(B_i \tilde{\rho}_A) = \sum_i B_i \,\mathrm{Tr}((B_i \otimes \mathbb{I})\rho) = \sum_i B_i \,\mathrm{Tr}(B_i \rho_A) = \rho_A, \tag{8}$$

což je spor. Operátor ρ_A je tedy určen jednoznačně a můžeme ho interpretovat jako stav podsystému A. Poznamenejme ještě důležitou věc, že informace obsažená ve stavech jednotlivých podsystémů *není* schopna v obecném případě reprodukovat stav celého systému. Pokud mezi oběma podsystémy existují korelace, provedením částečné stopy tyto korelace z popisu systému vypadnou.

3.3 Schmidtův rozklad

Při práci se stavy i při důkazech nejrůznějších tvrzení je velmi užitečné následující tvrzení, díky kterému lze každý čistý stav vyjádřit v jistém pěkném tvaru. Tomuto vyjádření se říká **Schmidtův rozklad** (angl. *Schmidt decomposition*).

Věta 3.2. Schmidtův rozklad. *Nechť* $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ *je čistý stav. Pak existuje ortonormální báze* $\{|e_j^{(A)}\rangle\}_j$ *prostoru* $\mathscr{H}_A$ *a ortonormální báze* $\{|f_j^{(B)}\rangle\}_j$ *prostoru* $\mathscr{H}_B$ *takové, že*

$$|\psi\rangle = \sum_{j=1}^{d} \alpha_j |e_j^{(A)}\rangle \otimes |f_j^{(B)}\rangle, \tag{9}$$

kde $d = \min\{\dim \mathscr{H}_A, \dim \mathscr{H}_B\}$. *Koeficienty* $\vec{\alpha} = (\alpha_1, \ldots, \alpha_d)$ *lze navíc vždy volit jako nezáporná čísla splňující rovnost* $\|\vec{\alpha}\| = \||\psi\rangle\|$.

Důkaz. Uvažujme stav podsystému A, $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. Tento lze jistě rozložit do ortonormální báze vlastních vektorů, $\rho_A = \sum_i \alpha_i^2 |e_i^{(A)}\rangle\langle e_i^{(A)}|$. Vlastní čísla operátoru ρ_A lze psát ve tvaru kvadrátu, neboť jsou díky pozitivitě operátoru nezáporná. Dále určitě můžeme vyjádřit vektor $|\psi\rangle$ ve tvaru $|\psi\rangle = \sum_i |e_i^{(A)}\rangle \otimes |\varphi_i^{(B)}\rangle$, kde $|\varphi_i^{(B)}\rangle$ jsou nějaké vhodné vektory z prostoru $\mathscr{H}_B$. Pak platí $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \mathrm{Tr}_B(\sum_{ij} |e_i^{(A)}\rangle\langle e_j^{(A)}| \otimes |\varphi_i^{(B)}\rangle\langle\varphi_j^{(B)}|) = \sum_{ij} |e_i^{(A)}\rangle\langle e_j^{(A)}| \,\mathrm{Tr}(|\varphi_i^{(B)}\rangle\langle\varphi_j^{(B)}|)$. Využijeme-li vztahu $\mathrm{Tr}(|a\rangle\langle b|) = \langle b|a\rangle$, redukuje se poslední výraz na $\sum_{ij} |e_i^{(A)}\rangle\langle e_j^{(A)}| \langle\varphi_j^{(B)}|\varphi_i^{(B)}\rangle$. Tento výsledek můžeme porovnat s prvním vyjádřením operátoru ρ_A uvedeným výše, abychom shrnuli $\langle\varphi_j^{(B)}|\varphi_i^{(B)}\rangle = \alpha_i^2 \delta_{ij}$. Vektory $\{|\varphi_i^{(B)}\rangle\}_i$ jsou tedy navzájem kolmé a po vhodném přeškálování z nich můžeme vytvořit ortonormální bázi $|f_i^{(B)}\rangle \coloneqq \frac{1}{\alpha_i}|\varphi_i^{(B)}\rangle$. Vektor $|\psi\rangle$ lze tak psát ve tvaru $|\psi\rangle = \sum_i \alpha_i |e_i^{(A)}\rangle \otimes |f_i^{(B)}\rangle$, což bylo dokázati. □

Definice 3.4. Koeficientům $\alpha_1, \ldots, \alpha_d$ v rozkladu (9) se říká **Schmidtovy koeficienty**. Počet nenulových Schmidtových koeficientů ve Schmidtově rozkladu se nazývá **Schmidtovo číslo** či **Schmidtova hodnost** (angl. *Schmidt number* či *Schmidt rank*). Schmidtovu hodnost stavu ρ budeme označovat symbolem $\mathrm{rank}\,\rho$.

Největším rozdílem mezi obecným rozkladem operátoru a jeho Schmidtovým rozkladem je v tom, že ve druhém jmenovaném sčítáme jen přes jeden index, ke každému bazickému vektoru prostoru $\mathscr{H}_A$ přísluší právě jeden bazický vektor prostoru $\mathscr{H}_B$. Ze Schmidtova rozkladu lze však vyčíst daleko více. Například vezmeme-li si vektor $|\psi\rangle$ ve vyjádření (9), jeho redukované stavy jsou tvarů $\rho_A = \sum_i \alpha_i^2 |e_i^{(A)}\rangle\langle e_i^{(A)}|$ a $\rho_B = \sum_i \alpha_i^2 |f_i^{(B)}\rangle\langle f_i^{(B)}|$. Operátory hustoty obou podsystémů mají tedy *stejné spektrum*! V souvislosti se Schmidtovým rozkladem je užitečné uvést následující proceduru.

Poznámka 3.1. Uvažujme nějaký systém A s operátorem hustoty $\rho_A = \sum_i \alpha_i^2 |e_i\rangle\langle e_i| \in \mathscr{H}_A$, který není obecně čistý. Potom ke studovanému systému A lze uměle přidat pomocný systém B o Hilbertově prostoru $\mathscr{H}_B$ tak, že existuje čistý stav $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$ splňující $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$. Jinými slovy, ke každému operátoru hustoty ρ_A z prostoru $\mathscr{H}_A$ lze najít čistý stav $|\psi\rangle$ v prostoru $\mathscr{H}_A \otimes \mathscr{H}_B$ tak, že ρ_A lze interpretovat jako stav podsystému A, kdy se přitom celý systém $A + B$ nachází v čistém stavu $|\psi\rangle$. Prostoru $\mathscr{H}_B$ se v angličtině říká *ancilla* a jeho dimenzi lze položit rovnou Schmidtově číslu operátoru ρ_A, tj. $\dim \mathscr{H}_B = \mathrm{rank}\,\rho_A$. Využívajíce postupu při důkazu předchozí věty lze zjevně položit $|\psi\rangle = \sum_i \alpha_i |e_i\rangle|f_i\rangle$, kde $\{|f_i\rangle\}_i$ je nějaká ortonormální báze prostoru $\mathscr{H}_B$.

Právě popsané matematické hříčce vhodně přidávající pomocný systém k původní úloze se říká **purifikace** či **vyčišťování** (angl. *purification*). Pro znalé připomínáme, že právě uvedená purifikace (stavů) nemá nic společného s *purifikací provázání.*

Poznámka 3.2. *„Monogamie stavů": Čisté stavy nemohou být korelovány s jiným systémem.* Mějme složený systém $A + B$ ve stavu $\rho \in \mathcal{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$, přičemž stav podsystému A nechť je čistý, $\mathrm{Tr}_B(\rho) = \rho_A = |\psi\rangle\langle\psi|$ pro jisté $|\psi\rangle \in \mathscr{H}_A$. Pak stav tohoto podsystému nevykazuje žádné korelace se stavem systému B. Důvod je následující. Vzhledem k předchozí poznámce můžeme vždy zavést pomocný systém C a najít vektor $|\omega\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ tak, že $\mathrm{Tr}_C(|\omega\rangle\langle\omega|) = \rho$. Tento vektor je tedy purifikací stavu ρ, současně je ale i purifikací stavu $|\psi\rangle$. To lze jen tak, že $|\omega\rangle = |\psi\rangle \otimes |\varphi_{BC}\rangle$ pro jisté $|\varphi_{BC}\rangle \in \mathscr{H}_B \otimes \mathscr{H}_C$. Celkem tedy $\rho = \mathrm{Tr}_C(|\omega\rangle\langle\omega|) = |\psi\rangle\langle\psi| \otimes \mathrm{Tr}_C(|\varphi_{BC}\rangle\langle\varphi_{BC}|)$. Vidíme tedy explicitně, že stav složeného systému $A + B$ je ve faktorizovaném tvaru, jenž nepřipouští žádné korelace mezi oběma podsystémy.

3.4 Klasifikace stavů podle korelací

Uvažujme dva Hilbertovy prostory $\mathscr{H}_1$ a $\mathscr{H}_2$ a množinu stavů definovaných na jejich tenzorovém součinu, $\mathcal{S}(\mathscr{H}_1 \otimes \mathscr{H}_2)$. Tuto množinu lze rozdělit na podmnožiny tvořené vždy stavy, jejichž tvar je podobný co do jejich přípravy a kvantových vlastností. Základní dělení na čisté a smíšené stavy jsme již nastínili v předchozích sekcích, následující seznam uvádí další podpřípady.

- **Smíšené stavy** – Odpovídající operátor hustoty není projektor.
  - **Faktorizované stavy** – Stav ρ je faktorizovaný, pokud lze zapsat ve tvaru tenzorového součinu $\rho = \rho_1 \otimes \rho_2$, kde $\rho_i \in \mathcal{S}(\mathscr{H}_i)$. Tyto stavy zřejmě tvoří podmnožinu separabilních stavů.
  - **Separabilní stavy** – Stav ρ je separabilní, pokud lze zapsat ve tvaru sumy faktorizovaných stavů $\rho = \sum_i \alpha_i \rho_1^{(i)} \otimes \rho_2^{(i)}$, kde $\rho_1^{(i)} \in \mathcal{S}(\mathscr{H}_1)$, $\rho_2^{(i)} \in \mathcal{S}(\mathscr{H}_2)$ a $\{\alpha_i\}_i$ tvoří pravděpodobnostní rozdělení, tj. $\alpha_i > 0$ a $\sum_i \alpha_i = 1$. Takovýmto stavům se také říká *statistické směsi* či *klasicky korelované stavy.* Korelace v měřeních na takovýchto stavech lze totiž popsat čistě klasicky, žádné kvantové efekty není třeba uvažovat. V tom se tato rodina stavů zásadně liší od té následující tvořené provázanými stavy. Obecný tvar separabilního stavu se zdá být dost obecný. Naprosto libovolný operátor lze rozložit do tvaru $A = \sum_i \alpha_i E_i \otimes F_i$, kde $\{E_i\}_i$ je ortonormální báze v $\mathcal{B}(\mathscr{H}_1)$ a podobně $\{F_i\}_i$ je ortonormální báze v $\mathcal{B}(\mathscr{H}_2)$. Nejdůležitější rozdíl tohoto obecného případu od případu separabilních stavů je v tom, že nyní operátory E_i a F_i samotné musejí být operátory hustoty.
  - **Provázané stavy** – Všechny stavy, které nejsou separabilní, se nazývají provázané. Tyto stavy vykazují čistě kvantové korelace, které lze využít při kvantovém počítání. Kvantové korelace se silně využívají například v případě kvantové teleportace.
- **Čisté stavy** – Odpovídající operátor hustoty je projektor.

- **Neprovázané stavy** – Čistý stav $|\psi\rangle$ je neprovázaný, pokud lze zapsat ve tvaru $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. Vidíme, že se jedná o analogii faktorizovaných stavů ve smíšeném případě. Na druhou stranu, vektor, který bychom vyjádřili analogicky případu separabilních smíšených stavů, již nebude čistý. Zbývají nám tak již pouze provázané stavy.
- **Provázané stavy** – Čistý stav $|\psi\rangle$ je provázaný, pokud není neprovázaný. Obecně je tedy tvaru $|\psi\rangle = \sum_i \alpha_i |e_i\rangle \otimes |f_i\rangle$, viz (9). Stav $|\psi\rangle$ je přitom provázaný právě tehdy, když má alespoň dva nenulové koeficienty α_i, tj. $\operatorname{rank}|\psi\rangle \geq 2$. Z množiny provázaných stavů se vydělují **maximálně provázané stavy** $|\Omega\rangle$. Jedná se o stavy, pro něž jsou stavy podsystémů *maximálně smíšené*. Jinými slovy, čistý stav $|\Omega\rangle$ je maximálně provázaný právě tehdy, když $\rho_1 \equiv \mathrm{Tr}_2(|\Omega\rangle\langle\Omega|) = \frac{1}{d_1}\mathbb{I}_1$ a $\rho_2 \equiv \mathrm{Tr}_1(|\Omega\rangle\langle\Omega|) = \frac{1}{d_2}\mathbb{I}_2$. Ze Schmidtova rozkladu plyne $d_1 = d_2 = d$, maximálně provázaný stav je tedy tvaru $|\Omega\rangle = \sum_i \frac{1}{\sqrt{d}}|e_i\rangle \otimes |f_i\rangle$.

4 Matematický aparát

Abychom si ulehčili práci s různými zobrazeními a především zefektivnili důkazy nejrůznějších tvrzení, zavedeme si v tomto matematickém intermezzu pár pomocných pojmů, jejichž význam je sice čistě matematický, jejich aplikací však budeme dostávat zajímavá fyzikálně interpretovatelná tvrzení. Kromě předeslaných pojmů budeme užívat i jistou notaci a názvosloví, které si nyní letem světem představíme.

Se stopou operátoru $A \in \mathscr{H}$, značenou $\operatorname{Tr} A$, jsme se již seznámili. Připomeňme si, že se jedná o lineární zobrazení s vlastností cykličnosti $\operatorname{Tr}(ABC) = \operatorname{Tr}(CAB)$, $\forall A, B, C \in \mathcal{B}(\mathscr{H})$ (a tedy samozřejmě také $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$), splňující též $\operatorname{Tr}(A \otimes B) = \operatorname{Tr} A \cdot \operatorname{Tr} B$. Pokud budeme počítat se složitými výrazy, je užitečné si explicitně vyjádřit, na jakém prostoru vlastně stopu počítáme. V takovém případě budeme daný prostor psát v závorkách do spodního indexu způsobem $\operatorname{Tr}_{(\mathscr{H})} A$. Naproti tomu jsme si už zavedli i částečnou stopu operátoru definovaného na složeném systému $C \in \mathcal{B}(\mathscr{H}_A \otimes \mathscr{H}_B)$. Částečnou stopu přes podsystém B značíme s dolním indexem $\operatorname{Tr}_B C$, který vyjadřuje, přes jaký prostor se stopuje. V tomto případě ale nepíšeme závorky, takže záměna stopy a částečné stopy není pro trénované oko možná. Tato a další notace je shrnuta na počátku skript v sekci 1. Pokud budeme hovořit o *superoperátorech*, nemáme tím na mysli nic jiného, než lineární zobrazení definovaná na vektorovém prostoru operátorů. Konečně, občas využijeme vlastností podobnostní transformace. Dva operátory A a B jsou *podobné*, existuje-li regulární operátor C takový, že $A = CBC^{-1}$.

4.1 Izomorfizmy

V následujícím uvažujme dva Hilbertovy prostory $\mathscr{H}_1$ a $\mathscr{H}_2$, kde $\{|\mu\rangle\}_{\mu=1}^{M}$ je ortonormální báze prostoru $\mathscr{H}_1$ a podobně $\{|m\rangle\}_{m=1}^{N}$ je ortonormální báze v prostoru $\mathscr{H}_2$. V této sekci si zadefinujeme tři izomorfní zobrazení, která úspěšně využijeme v důkazech tvrzení nadcházejících sekcí.

1. Nechť $A \in \mathcal{B}(\mathscr{H}_1, \mathscr{H}_2)$ je omezené lineární zobrazení z prostoru $\mathscr{H}_1$ do prostoru $\mathscr{H}_2$. První izomorfizmus, který si uvedeme, vzájemně jednoznačně přiřazuje takovémuto zobrazení A vektor $|A\rangle$ z prostoru $\mathscr{H}_1 \otimes \mathscr{H}_2$ způsobem

$$\langle m|A|\mu\rangle \equiv \langle m\mu|A\rangle. \tag{10}$$

   Zobrazení A lze zřejmě vyjádřit jako $A = \sum_{m\mu} A_{m\mu}|m\rangle\langle\mu|$. Odpovídající vektor $|A\rangle$ je pak tvaru $|A\rangle = \sum_{m\mu} A_{m\mu}|m\rangle|\mu\rangle$. Ukažme si ještě, že přiřazení zobrazení a vektoru zachovává skalární součin. Pro libovolná dvě zobrazení $A, B \in \mathcal{B}(\mathscr{H}_1, \mathscr{H}_2)$ platí $(A, B) = \operatorname{Tr}(A^\dagger B) = \operatorname{Tr}((\sum_{m\mu} A^*_{m\mu}|\mu\rangle\langle m|)(\sum_{n\nu} B_{n\nu}|n\rangle\langle\nu|)) = \operatorname{Tr}(\sum_{m\mu\nu} A^*_{m\mu}B_{m\nu}|\mu\rangle\langle\nu|) = \sum_{m\mu\nu\alpha} A^*_{m\mu}B_{m\nu}\langle\alpha|\mu\rangle\langle\nu|\alpha\rangle = \sum_{m\alpha} A^*_{m\alpha}B_{m\alpha} = \langle A|B\rangle$. Zobrazení (10) je tedy izomorfizmus. Z definice (10) není hned patrné, jak si takové přiřazení představit, má přitom názorný význam. Představme si operátor A jako matici (A_{ij}). Pak právě uvedený izomorfizmus vezme první řádek této matice a udělá z něho sloupcový vektor. Pak vezme druhý řádek, udělá z něho podobně sloupcový vektor a ten připojí pod sloupcový vektor vytvořený z prvního řádku. Takto pokračuje dále až celou matici přemění na sloupcový vektor tím, že její řádky vyskládá za sebe. Graficky lze tento izomorfizmus znázornit jako vztah

$$\begin{pmatrix} A_{11} & A_{12} & \dots & A_{1M} \\ A_{21} & A_{22} & \dots & A_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ A_{N1} & A_{N2} & \dots & A_{NM} \end{pmatrix} \quad \leftrightarrow \quad \begin{pmatrix} A_{11} \\ A_{12} \\ \vdots \\ A_{1M} \\ A_{21} \\ A_{22} \\ \vdots \\ A_{2M} \\ \vdots \\ A_{NM} \end{pmatrix}. \tag{11}$$

2. Mějme nyní superoperátor $C : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ a nechť $\{A^{(k)}\}_{k=1}^{M^2}$ je ortonormální báze prostoru $\mathcal{B}(\mathscr{H}_2)$ a $\{B^{(l)}\}_{l=1}^{N^2}$ je ortonormální báze prostoru $\mathcal{B}(\mathscr{H}_1)$. Analogicky prvnímu izomorfizmu si definujme přiřazení
$$C = \sum_{kl} C_{kl} |A^{(k)}\rangle\langle B^{(l)}| \quad \leftrightarrow \quad |C\rangle = \sum_{kl} C_{kl} |A^{(k)}\rangle |B^{(l)}\rangle. \tag{12}$$
Podobně jako u prvního izomorfizmu, i zde by se analogickým způsobem ověřilo, že toto přiřazení zachovává skalární součin. Zavolíme-li ortonormální báze prostorů operátorů v jednoduchém tvaru $A^{(k)} = A^{mn} \equiv |m\rangle\langle n|$ a $B^{(l)} = B^{\mu\nu} \equiv |\mu\rangle\langle\nu|$, lze definiční vztah přepsat na
$$C = \sum_{mn\mu\nu} C_{\substack{mn\\ \mu\nu}} |A^{mn}\rangle\langle B^{\mu\nu}| \quad \leftrightarrow \quad |C\rangle = \sum_{mn\mu\nu} C_{\substack{mn\\ \mu\nu}} |A^{mn}\rangle |B^{\mu\nu}\rangle. \tag{13}$$
Neboť $|A^{mn}\rangle \in \mathscr{H}_2^{\otimes 2}$ a $|B^{\mu\nu}\rangle \in \mathscr{H}_1^{\otimes 2}$ je vektor $|C\rangle$ prvkem prostoru $\mathscr{H}_2^{\otimes 2} \otimes \mathscr{H}_1^{\otimes 2}$.

3. Využijme nyní notace pro bazické vektory zavedené v předchozím bodě a uvažujme operátor $X_C \in \mathcal{B}(\mathscr{H}_1 \otimes \mathscr{H}_2)$ tvaru $X_C = \sum_{mn\mu\nu} C_{\substack{mn\\ \mu\nu}} A^{mn} \otimes B^{\mu\nu} = \sum_{mn\mu\nu} C_{\substack{mn\\ \mu\nu}} |m\mu\rangle\langle n\nu|$. Porovnáme-li tento výraz s obecným tvarem operátoru $X_C = \sum_{mn\mu\nu} (X_C)_{\substack{m\mu\\ n\nu}} |m\mu\rangle\langle n\nu|$, dostáváme rovnost
$$(X_C)_{\substack{m\mu\\ n\nu}} = C_{\substack{mn\\ \mu\nu}}, \tag{14}$$
která nám definuje třetí a poslední izomorfizmus. Ověřme ještě, že toto přiřazení zachovává skalární součin. Mějme dva superoperátory, C a D. Potom platí $(X_C, X_D) = \mathrm{Tr}(X_C^\dagger X_D) = \mathrm{Tr}((\sum_{mn\mu\nu} (X_C)^*_{\substack{m\mu\\ n\nu}} |n\nu\rangle\langle m\mu|)(\sum_{ab\alpha\beta} (X_D)_{\substack{a\alpha\\ b\beta}} |a\alpha\rangle\langle b\beta|))$. Tento výraz se redukuje na $\sum_{mn\mu\nu} (X_C)^*_{\substack{m\mu\\ n\nu}} (X_D)_{\substack{m\mu\\ n\nu}} = \sum_{mn\mu\nu} C^*_{\substack{mn\\ \mu\nu}} D_{\substack{mn\\ \mu\nu}} = \langle C|D\rangle = (C, D)$, což jsme chtěli dokázat. Anglicky se přiřazení (14) říká *reshuffling operation*.

Jako velmi důležitý případ použití výše zmíněných izomorfizmů je následující situace. Mějme superoperátor $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$, který na vstupní operátory X působí způsobem
$$\phi(X) = A\, X\, B, \tag{15}$$

kde $A \in \mathcal{B}(\mathscr{H}_1, \mathscr{H}_2)$ a $B \in \mathcal{B}(\mathscr{H}_2, \mathscr{H}_1)$. Za použití izomorfizmů, které superoperátoru a operátoru přiřadí vektory, lze dokázat vztah

$$|\phi(X)\rangle = \phi_M |X\rangle, \quad \text{kde} \quad \phi_M = A \otimes B^T. \tag{16}$$

Počítáme-li se superoperátory působícími na nějaké operátory, lze manipulaci s nimi převést na jednodušší úlohu, kde počítáme s maticemi. Místo superoperátoru ϕ stačí tedy pracovat s maticí ϕ_M. Dokažme si nyní výše uvedený vztah, kde vyjádříme operátory A a B v lokálních bázích jednotlivých prostorů, $A = \sum_{m\mu} A_{m\mu} |m\rangle\langle\mu|$ a $B = \sum_{n\nu} B_{\nu n} |\nu\rangle\langle n|$. Pak dostáváme $\phi_M |X\rangle = (A \otimes B^T)|X\rangle = (\sum_{m\mu} A_{m\mu}|m\rangle\langle\mu|) \otimes (\sum_{n\nu} B_{\nu n}|n\rangle\langle\nu|) \sum_{\alpha\beta} X_{\alpha\beta}|\alpha\rangle|\beta\rangle = \sum_{m\mu n\nu} A_{m\mu} B_{\nu n} X_{\mu\nu} |m\rangle|n\rangle = \sum_{mn} (AXB)_{mn} |m\rangle|n\rangle = |AXB\rangle = |\phi(X)\rangle$.

Příklad 4.1. Připomeňme si Liouvilleův operátor $L(\rho(t)) = -\mathrm{i}\,(H(t)\rho(t) - \rho(t)H(t))$ zavedený v rovnici (5). S využitím vztahu (16) tento superoperátor zřejmě odpovídá matici $L_M(t) = -\mathrm{i}\, H(t) \otimes \mathbb{I} + \mathrm{i}\, \mathbb{I} \otimes H^T(t)$. Z tohoto vyjádření je ihned patrné, že L je antihermitovský. Navíc jsme se zbavili explicitní závislosti na vstupní stavu $\rho(t)$ a vlastnosti operátoru L lze tak přímo studovat pomocí odpovídající matice L_M.

Dále jsme si uváděli, že řídí-li se operátor hustoty $\rho(t)$ rovnicí (5), lze jeho vývoj reprezentovat jistým unitárním operátorem U takovým, aby $\rho(t) = U(t)\,\rho(0)\,U^\dagger(t)$. Máme tak přímo výraz tvaru (16), který lze převézt na násobení vektoru maticí, $|\rho(t)\rangle = U_M(t)|\rho(0)\rangle$. Příslušná matice $U_M(t) = U(t) \otimes U^*(t)$ je přitom unitární.

Zajímavý je izomorfní obraz maximálně provázaného stavu $|\Omega\rangle$. Mějme $|\Omega\rangle \in \mathscr{H}_1 \otimes \mathscr{H}_1$, jehož vyjádření zní $|\Omega\rangle = \frac{1}{\sqrt{d_1}} \sum_{i=1}^{d_1} |e_i\rangle \otimes |e_i\rangle$, kde $d_1 = \dim \mathscr{H}_1$. Pak je tento přidružený s násobkem identity

$$|\Omega\rangle \quad \leftrightarrow \quad \frac{1}{\sqrt{d_1}} \mathbb{I} \ \in \mathcal{B}(\mathscr{H}_1). \tag{17}$$

Uvažujeme-li tedy dvě zobrazení $A \in \mathcal{B}(\mathscr{H}_1, \mathscr{H}_2)$ a $B \in \mathcal{B}(\mathscr{H}_2, \mathscr{H}_1)$, tak platí důležitý vztah

$$(A \otimes B^T)|\Omega\rangle \quad \leftrightarrow \quad \frac{1}{\sqrt{d_1}} AB. \tag{18}$$

Nyní využijeme tohoto vztahu, abychom odvodili některé jednoduché, avšak užitečné, vlastnosti maximálně provázaného stavu. Předpokládáme přitom rovnost $\mathscr{H}_1 = \mathscr{H}_2$.

1. Díky vztahu (18) platí $(A \otimes \mathbb{I})|\Omega\rangle \leftrightarrow \frac{1}{\sqrt{d_1}} A$ a $(\mathbb{I} \otimes A^T)|\Omega\rangle \leftrightarrow \frac{1}{\sqrt{d_1}} A$ pro libovolný operátor A. Celkem tedy
$$(A \otimes \mathbb{I})|\Omega\rangle = (\mathbb{I} \otimes A^T)|\Omega\rangle. \tag{19}$$

2. Pro libovolný unitární operátor U máme $(U \otimes U^*)|\Omega\rangle \leftrightarrow \frac{1}{\sqrt{d_1}} UU^\dagger = \frac{1}{\sqrt{d_1}} \mathbb{I} \leftrightarrow |\Omega\rangle$. Neboli
$$(U \otimes U^*)|\Omega\rangle = |\Omega\rangle. \tag{20}$$

3. *Z maximálně provázaného stavu lze vyrobit lokálně libovolný stav.* Maximálně provázaný stav je stav dvou provázaných podsystémů, pod pojmem *lokálně* máme na mysli, že

používáme pouze ty operátory, které působí jen na jednom z podsystémů a s druhým podsystémem neudělají nic. Přesněji tedy pro každý čistý stav $|\phi\rangle \in \mathscr{H}_1 \otimes \mathscr{H}_1$ existuje nějaký operátor $A_\phi \in \mathcal{B}(\mathscr{H}_1)$ tak, že

$$|\phi\rangle = (A_\phi \otimes \mathbb{I})|\Omega\rangle. \tag{21}$$

Důkaz tohoto tvrzení je jednoduchý. K vektoru $|\phi\rangle$ je přidružen operátor ϕ, jež lze rozložit následovně $\phi = \sqrt{d_1}\phi(\frac{1}{\sqrt{d_1}}\mathbb{I})\mathbb{I} = A_\phi(\frac{1}{\sqrt{d_1}}\mathbb{I})\mathbb{I}$, kde jsme si označili $A_\phi = \sqrt{d_1}\phi$. Platí dále $\phi = A_\phi(\frac{1}{\sqrt{d_1}}\mathbb{I})\mathbb{I} \leftrightarrow (A_\phi \otimes \mathbb{I})|\Omega\rangle$, viz (18). Neboť jsme pracovali s izomorfizmy, tj. bijekcemi, dospíváme ke kýžené rovnosti.

Z důkazu též vidíme, že operátor A_ϕ je určen jednoznačně. Jako vedlejší produkt lze navíc odvodit i tyto vztahy pro skalární součin

$$\langle\phi|\psi\rangle = \mathrm{Tr}(\phi^\dagger\psi) = \frac{1}{d_1}\mathrm{Tr}(A_\phi^\dagger A_\psi^\dagger). \tag{22}$$

a pro tvar matic hustoty jednotlivých podsystémů

$$\begin{aligned} \rho_1 &= \mathrm{Tr}_2(|\phi\rangle\langle\phi|) = \frac{1}{d_1}A_\phi A_\phi^\dagger = \phi\phi^\dagger, \\ \rho_2 &= \mathrm{Tr}_1(|\phi\rangle\langle\phi|) = \frac{1}{d_1}A_\phi^T A_\phi^* = \phi^T\phi^*. \end{aligned}$$

Dokažme si rovnost pro matici hustoty prvního podsystému ρ_1. S využitím identity (21) máme $\rho_1 = \mathrm{Tr}_2(|\phi\rangle\langle\phi|) = \frac{1}{d_1}\sum_i\langle i|(A_\phi \otimes \mathbb{I})(\sum_{jk}|jj\rangle\langle kk|)(A_\phi^\dagger \otimes \mathbb{I})|i\rangle = \frac{1}{d_1}A_\phi(\sum_j|j\rangle\langle j|)A_\phi^\dagger = \frac{1}{d_1}A_\phi A_\phi^\dagger$. Ostatní vztahy by se dokázali obdobně.

Význačnost vztahu (21) si uvědomíme tehdy, představíme-li si jeho důsledky fyzikálně. Mějme dva systémy A a B nacházející se v maximálně provázaném stavu $|\Omega\rangle$. Nechť podsystém A vlastní Alice a podsystém B drží ve svých spárech Bob. Alice si chtěla udělat hezkou dovolenou a tak se svým podsystémem A odjela na Havaj, bez Boba. Bob se svým podsystémem B mezitím trčí doma v Praze a rozmýšlí si, jak Alici její dovolenou znepříjemnit. Díky vzorečku (21) je však vše snadné, Bob může provést libovolnou operaci A_ϕ pouze se *svým* podsystémem, aby *libovolně* změnil celkový stav systému $A + B$. Bob tak může na dálku ovlivňovat i stav Aliciina systému. Abychom však Bobovi nekřivdili, Alice si může počínat stejně zákeřně. Vzorec (19) nám totiž říká, že pro změnu stavu celého systému $A + B$ je jedno, zda to bude Bob či Alice, kdo provede úpravu na svém podsystému.

Příklad 4.2. Nechť $|\varphi\rangle = \frac{1}{5}(3|01\rangle + 4|10\rangle)$ je vektor popisující stav dvou provázaných podsystémů. Tento čistý stav je přidružen operátoru

$$\phi_M = \frac{1}{5}\begin{pmatrix} 0 & 3 \\ 4 & 0 \end{pmatrix}. \tag{23}$$

S jeho pomocí již snadno spočteme stav prvního podsystému

$$\rho_1 = \phi_M\phi_M^\dagger = \frac{1}{25}\begin{pmatrix} 9 & 0 \\ 0 & 16 \end{pmatrix}. \tag{24}$$

Než přikročíme ke studiu otevřených systémů je vhodné si uvést dvě nerovnosti dávající do souvislosti stopy jistých operátorů. Těmto dvěma nerovnostem jsou po řadě věnovány následující dvě kapitolky.

4.2 Kleinova nerovnost

Věta 4.1. Kleinova nerovnost. *Nechť $f : I \to \mathbb{R}$ je konvexní a diferencovatelná funkce na intervalu $I = [a,b]$. Dále nechť A a B jsou hermitovské operátory takové, že jejich spektra leží v intervalu I, tj. $\sigma(A) \subset I$ a $\sigma(B) \subset I$. Pak platí*

$$\mathrm{Tr}(f(A) - f(B)) \geq \mathrm{Tr}((A-B)f'(B)). \tag{25}$$

Pokud je funkce f ostře konvexní, tak se rovnosti nabývá právě tehdy, když $A = B$.

Důkaz. Označme si $A = \sum_i a_i |e_i\rangle\langle e_i|$ a $B = \sum_i b_i |f_i\rangle\langle f_i|$. Potom $f(A) = \sum_i f(a_i)|e_i\rangle\langle e_i|$ a $f(B) = \sum_i f(b_i)|f_i\rangle\langle f_i|$. Neboť pracujeme s ortonormálními bázemi $\{|e_i\rangle\}_i$ a $\{|f_j\rangle\}_j$, plynou z Parsevalovy rovnosti vztahy $\sum_i |c_{ij}|^2 = 1$ a $\sum_j |c_{ij}|^2 = 1$, kde jsme si definovali $c_{ij} = \langle e_i|f_j\rangle$. Pro každý bazický vektor $|e_i\rangle$ dále dostáváme, že výraz $\langle e_i|(f(A) - f(B) - (A-B)f'(B))|e_i\rangle$ je roven

$$\begin{aligned}
& f(a_i) - \langle e_i| \sum_j f(b_j)|f_j\rangle\langle f_j||e_i\rangle - \langle e_i|\left(\sum_j a_j|e_j\rangle\langle e_j| - \sum_j b_j|f_j\rangle\langle f_j|\right)\sum_k f'(b_k)|f_k\rangle\langle f_k||e_i\rangle \\
= \quad & f(a_i) - \sum_j f(b_j)|c_{ij}|^2 - a_i \sum_j f'(b_j)|c_{ij}|^2 + \sum_j b_j |c_{ij}|^2 f'(b_j) \\
= \quad & f(a_i)\sum_j |c_{ij}|^2 - \sum_j |c_{ij}|^2 (f(b_j) + a_i f'(b_j) - b_j f'(b_j)) \\
= \quad & \sum_j |c_{ij}|^2 (f(a_i) - f(b_j) - (a_i - b_j)f'(b_j)).
\end{aligned}$$

Z věty o přírůstku funkce aplikovanou na interval $[c,d]$ platí $f(d) - f(c) = (d-c)f'(\xi)$ pro jisté $\xi \in (c,d)$. Neboť je funkce f konvexní, je její derivace kdekoli uvnitř intervalku $[c,d]$ větší než derivace v levém krajním bodě c a současně menší než derivace v pravém krajním bodě d, tj. $f'(\xi) \geq f'(c)$ a $f'(\xi) \leq f'(d)$. Celkem tedy $(d-c)f'(d) \geq f(d) - f(c) \geq (d-c)f'(c)$. Z těchto dvou nerovností již plyne, že výraz $f(a_i) - f(b_j) - (a_i - b_j)f'(b_j)$ je vždy nezáporný a tedy i $\langle e_i|(f(A) - f(B) - (A-B)f'(B))|e_i\rangle \geq 0$. První tvrzení věty již plyne přímo z definice stopy. Ukažme si ještě, že pro ostře konvexní funkce se rovnosti nabývá právě, když $A = B$. Vidíme, že rozdíl zkoumaný ve výrazech výše je nulový právě tehdy, když pro všechna i a j platí $a_i = b_j$ nebo $c_{ij} = 0$. Pro Hilbert-Schmidtovu normu rozdílu operátorů tedy dostáváme $\|A-B\|^2 = \mathrm{Tr}(A-B)^2 = \mathrm{Tr}(\sum_i a_i|e_i\rangle\langle e_i| - \sum_j b_j|f_j\rangle\langle f_j|)^2 = \mathrm{Tr}(\sum_i a_i^2|e_i\rangle\langle e_i| + \sum_j b_j^2|f_j\rangle\langle f_j| - 2\sum_{ij} a_i b_j c_{ij}|e_i\rangle\langle f_j|) = \sum_i a_i^2 + \sum_j b_j^2 - 2\sum_{ij} a_i b_j |c_{ij}|^2 = \sum_{ij}|c_{ij}|^2(a_i - b_j)^2 = 0$. Z toho již plyne $A = B$. Druhá implikace je zřejmá. □

Příklad 4.3. Uvažme funkci f definovanou na nezáporných číslech způsobem

$$f = \begin{cases} x \ln x & x > 0, \\ 0 & x = 0. \end{cases} \tag{26}$$

Její první a druhá derivace zní po řadě $f'(x) = 1 + \ln x$ a $f''(x) = 1/x$. Funkce f je tedy ostře konvexní pro $x > 0$. Pak pro libovolné pozitivní operátory A a B platí díky předchozí větě nerovnost $\mathrm{Tr}(A \ln A - B \ln B) \geq \mathrm{Tr}((A - B)(\mathbb{I} + \ln B))$, kterou můžeme upravit do tvaru

$$\mathrm{Tr}(A \ln A) - \mathrm{Tr}(A \ln B) \geq \mathrm{Tr}(A - B). \tag{27}$$

Tento vztah využijeme při studiu entropie v následující kapitole.

4.3 Peierlova nerovnost

Věta 4.2. Peierlova nerovnost. *Nechť f je konvexní funkce na intervalu $I \subset \mathbb{R}$ a $A \in \mathcal{B}(\mathscr{H})$ je hermitovský operátor, jehož spektrum leží v I, tj. $\sigma(A) \subset I$. Označme si libovolnou ortonormální bázi prostoru $\mathscr{H}$ jako $\{|f_i\rangle\}_i$. Pak platí*

$$\mathrm{Tr}(f(A)) \geq \sum_i f(\langle f_i|A|f_i\rangle). \tag{28}$$

Důkaz. S využitím notace použité při důkazu Kleinovy nerovnosti můžeme vyjádřit operátor A ve tvaru $A = \sum_j a_j |e_j\rangle\langle e_j|$ a $\langle f_i|f(A)|f_i\rangle = \sum_j f(a_j)|c_{ij}|^2 \geq f(\sum_j |c_{ij}|^2 a_j) = f(\sum_j |\langle f_i|e_j\rangle|^2 a_j) = f(\langle f_i|A|f_i\rangle)$, kde nerovnost plyne z konvexnosti funkce f. □

Důsledek 4.1. *Pro libovolné číslo $p \in (0,1)$, konvexní funkci f na intervalu I a operátory A a B splňující předpoklady předchozí věty platí*

$$\mathrm{Tr}\, f(pA + (1-p)B) \leq p \,\mathrm{Tr}\, f(A) + (1-p)\,\mathrm{Tr}\, f(B). \tag{29}$$

Důkaz. Označme si symbolem $\{|e_i\rangle\}_i$ ortonormální bázi tvořenou vlastními vektory operátoru $pA + (1-p)B$. Pak $\mathrm{Tr}\, f(pA + (1-p)B) = \sum_i \langle e_i|f(pA + (1-p)B)|e_i\rangle$. Díky vhodné volbě naší báze je tento výraz roven $\sum_i f(\langle e_i|(pA + (1-p)B)|e_i\rangle) = \sum_i f(p\langle e_i|A|e_i\rangle + (1-p)\langle e_i|B|e_i\rangle)$. Z konvexnosti je tento výraz menší nebo roven výrazu $p\sum_i f(\langle e_i|A|e_i\rangle) + (1-p)\sum_i f(\langle e_i|B|e_i\rangle)$, což je dále díky předchozí větě menší nebo rovno výrazu $p \,\mathrm{Tr}\, f(A) + (1-p)\,\mathrm{Tr}\, f(B)$. □

5 von Neumannova entropie

V informatice se zavádí veličina H popisující, jak moc je dané pravděpodobnostní rozdělení „neočekávatelné“. Pokud jsou všechny hodnoty rozdělení $\{p_i\}_i$ stejné, tak je tato veličina maximální. Nelze totiž preferovat jednu událost s pravděpodobností p_1 před druhou událostí s pravděpodobností p_2, neboť každá může nastat stejně často. Takovéto rozdělení bychom mohli označit za „nejvíce neočekávatelné“. Naopak, pokud je rozdělení $\{p_i\}_i$ tvořeno samými nulami vyjma jedné jedničky $p_{i_0} = 1$, je tato veličina nulová. V takovém případě totiž jev spjatý s pravděpodobností p_{i_0} nastává vždy a žádný jiný jev nenastává. Toto rozdělení je tedy „nejméně neočekávatelné“. Zmíněné veličině se říká *Shannonova entropie* a její definiční předpis pro pravděpodobnostní rozdělení $\{p_i\}_i$ zní $H(p_i) = -\sum_i p_i \ln p_i$.

Jak jsme si uváděli v kapitolce o operátorech hustoty, operátor hustoty ρ lze chápat jako vážený průměr čistých stavů, kde váhami je jisté pravděpodobnostní rozdělení tvořené vlastními hodnotami, $\rho = \sum_i \lambda_i |i\rangle\langle i|$. Tento zápis pak zhruba řečeno vyjadřuje, že se daný systém nachází v čistém stavu $|i\rangle$ s pravděpodobností λ_i. Pokud jsou všechna vlastní čísla vyjma jednoho nulová, je ρ samotné čistým stavem. Žádná neurčitost týkající se „výběru“ čistého stavu $|i\rangle$ z rozkladu výše tedy nevzniká. Naproti tomu, jsou-li všechna vlastní čísla stejná, může se stav daného systému nacházet v libovolném z čistých stavů $|i\rangle$ stejně pravděpodobně. Neurčitost „výběru“ čistého stavu je maximální.

Právě naznačená analogie mezi pravděpodobnostními rozděleními a operátory hustoty nás vede na myšlenku definovat entropii i pro tyto operátory. Jak se lze snadno přesvědčit v diagonální bázi operátoru ρ, výraz $-\operatorname{Tr}(\rho \ln \rho)$ je roven Shannonově entropii pro rozdělení $\{\lambda_i\}_i$. Tato úvaha nás motivuje pro zavedení následujícího pojmu.

Definice 5.1. Nechť $\rho \in \mathcal{S}(\mathscr{H})$ je nějaký operátor hustoty, pak **von Neumannova entropie** pro tento operátor je veličina definovaná vztahem

$$S(\rho) := -\operatorname{Tr}(\rho \ln \rho). \tag{30}$$

Entropie kvantových stavů je důležitá veličina s mnoha zajímavými a intuitivními vlastnostmi. Některé z nich si právě uvedeme.

- Platí $S(\rho) \geq 0$, kde se rovnosti nabývá právě, když ρ je čistý stav, tj. $\rho = |\psi\rangle\langle\psi|$ pro nějaké $|\psi\rangle \in \mathscr{H}$. Tuto vlastnost lze intuitivně chápat podobně jako v případě Shannonovy entropie. Chápeme-li operátor hustoty jako vážený průměr čistých stavů, pak zřejmě nejméně neočekávatelný výsledek měření na takovémto stavu bude tehdy, když bude tento stav čistý a při vhodné volbě projekčních operátorů (viz později) budeme dostávat stále tentýž výsledek.

- Je-li systém $A+B$ v čistém stavu $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B$, pak entropie stavů jeho podsystémů se rovnají, tj. $S(\rho_A) = S(\rho_B)$. Je-li navíc stav $|\psi\rangle$ maximálně provázaný, jsou tyto entropie rovny $S(\rho_A) = S(\rho_B) = \ln d > 0$, kde $d = \dim \mathscr{H}_A = \dim \mathscr{H}_B$. Z prvního bodu přitom $S(|\psi\rangle\langle\psi|) = 0$. Vidíme tak, že ač je stav celého systému plně určen, oba jeho podsystémy vykazují neurčitost.

- $S(U\rho U^\dagger) = S(\rho)$ pro libovolný unitární operátor $U \in \mathcal{B}(\mathscr{H})$. Při uzavřeném vývoji se tedy entropie stavu systému zachovává.

Pár dalších vlastností si vyslovíme a dokážeme ve formě lemmat níže.

Lemma 5.1. Konkávnost. *Nechť $\rho, \sigma \in \mathcal{S}(\mathscr{H})$ jsou dva stavy a $p \in [0,1]$. Pak platí*

$$S(p\rho + (1-p)\sigma) \geq pS(\rho) + (1-p)S(\sigma), \tag{31}$$

kde se rovnosti nabývá právě tehdy, když $\rho = \sigma$.

Důkaz. Označme si $\omega = p\rho + (1-p)\sigma$. Pak z nerovnosti (27) plyne $-\operatorname{Tr}(\omega \ln \omega) = -p\operatorname{Tr}(\rho \ln \omega) - (1-p)\operatorname{Tr}(\sigma \ln \omega) \geq -p(\operatorname{Tr}(\rho \ln \rho) + \operatorname{Tr}(\omega - \rho)) - (1-p)(\operatorname{Tr}(\sigma \ln \sigma) + \operatorname{Tr}(\omega - \sigma))$. Tento výraz lze dále upravit na $p(-\operatorname{Tr}(\rho \ln \rho)) + (1-p)(-\operatorname{Tr}(\sigma \ln \sigma)) - \operatorname{Tr}(p\omega - p\rho + (1-p)\omega - (1-p)\sigma) = pS(\rho) + (1-p)S(\sigma) - \operatorname{Tr}(\omega - (p\rho + (1-p)\sigma)) = S(\rho) + (1-p)S(\sigma)$. Tvrzení lze dokázat i aplikací nerovnosti (29), kde položíme $f(A) \coloneqq A \ln A$. Výsledek dostáváme ihned. □

Lemma 5.2. Subaditivita. *Nechť $\rho \in \mathcal{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$ je stav systému, $\rho_A = \operatorname{Tr}_B \rho$ a $\rho_B = \operatorname{Tr}_A \rho$ nechť jsou jemu odpovídající stavy podsystémů. Pak*

$$S(\rho) \leq S(\rho_A) + S(\rho_B), \tag{32}$$

přičemž rovnost nastává právě tehdy, když je ρ faktorizovaného tvaru $\rho = \rho_A \otimes \rho_B$.

Důkaz. Označíme-li $A = \rho$ a $B = \rho_A \otimes \rho_B$, plyne po dosazení do (27) z Kleinovy nerovnosti $\operatorname{Tr}(\rho \ln \rho) \geq \operatorname{Tr}(\rho \ln(\rho_A \otimes \rho_B)) + \operatorname{Tr}(\rho - \rho_A \otimes \rho_B) = \operatorname{Tr}(\rho \ln((\rho_A \otimes \mathbb{I})(\mathbb{I} \otimes \rho_B)) + \operatorname{Tr}(\rho) - \operatorname{Tr}(\rho_A \otimes \rho_B)$. Neboť $\operatorname{Tr}\rho = 1 = \operatorname{Tr}(\rho_A \otimes \rho_B)$, dostáváme $\operatorname{Tr}(\rho \ln \rho) \geq \operatorname{Tr}(\rho \ln(\rho_A \otimes \mathbb{I})) + \operatorname{Tr}(\rho \ln(\mathbb{I} \otimes \rho_B))$. Dále platí $\operatorname{Tr}(\rho \ln(\rho_A \otimes \mathbb{I})) = \operatorname{Tr}(\rho((\ln \rho_A) \otimes \mathbb{I})) = \operatorname{Tr}\rho_A \ln \rho_A$ a obdobně pro systém B. Celkem tedy $\operatorname{Tr}(\rho \ln \rho) \geq \operatorname{Tr}(\rho_A \ln \rho_A) + \operatorname{Tr}(\rho_B \ln \rho_B)$, z čehož již plyne dokazované tvrzení. □

Lemma 5.3. Arakiho-Liebova nerovnost. *Nechť $\rho \in \mathcal{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$ je operátor hustoty složeného systému, $\rho_A = \operatorname{Tr}_B \rho$ a $\rho_B = \operatorname{Tr}_A \rho$ nechť jsou jemu odpovídající stavy podsystémů. Pak*

$$S(\rho) \geq |S(\rho_A) - S(\rho_B)|. \tag{33}$$

Důkaz. Stav celého systému $\rho \in \mathcal{S}(\mathscr{H}_A \otimes \mathscr{H}_B)$ lze purifikovat na čistý stav $|\psi\rangle \in \mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ splňující $\rho = \operatorname{Tr}_C(|\psi\rangle\langle\psi|)$. Označíme si $S_i = S(\rho_i)$. Neboť $|\psi\rangle$ je čistý, platí z vlastností entropie zmíněných výše, že $S_{AB} = S_C$, $S_{AC} = S_B$ a $S_{BC} = S_A$. Dále ze subaditivity plyne $S_A + S_C \geq S_{AC}$ atd. Přeuspořádáním získaných nerovností dospíváme ke vztahům $S_{AB} = S_C \geq S_B - S_A$ a $S_{AB} \geq S_A - S_B$, ze kterých plyne dokazované tvrzení. □

Definice 5.2. Jako **index korelace** I_C kvantových stavů dvou podsystémů A a B označíme veličinu $I_C = S_A + S_B - S_{AB}$, kde $S_i = S(\rho_i)$ jsou entropie stavů jednotlivých podsystémů a S_{AB} je entropie stavu ρ celého systému.

Index korelace kvantifikuje míru klasických i kvantových korelací mezi dvěma systémy. Neboť mezi čistými stavy nevyvstávají žádné klasické korelace, můžeme říci, že pro čisté stavy veličina I_C přímo kvantifikuje míru provázání. Index korelace nabývá maximální hodnoty právě tehdy, když je stav ρ celého systému maximálně provázaný. Navíc platí zřejmé nerovnosti $0 \le I_C \le 2\min\{S_A, S_B\}$.

Pro entropii smíšeného stavu platí následující vztahy, které si vzápětí dokážeme.

Věta 5.1. *Nechť $\{p_i\}_i$ je pravděpodobnostní rozdělení, $\{\rho_i\}_i$ je sada operátorů hustoty z prostoru $\mathcal{B}(\mathscr{H})$ a $H(\{p_i\}_i) = -\sum_i p_i \ln p_i$ je Shannonova entropie. Pak platí*

$$\sum_i p_i S(\rho_i) \;\le\; S\left(\sum_i p_i\rho_i\right) \;\le\; \sum_i p_i S(\rho_i) + H(\{p_i\}_i). \tag{34}$$

Důkaz. První nerovnost lze dokázat matematickou indukcí, kde tvrzení pro $i = 2$ bylo dokázáno výše. Přikročme tedy k důkazu druhé nerovnosti. Tu nejprve dokážeme pro případ, kdy jsou $\rho_i \in \mathcal{S}(\mathscr{H})$ čisté stavy, $\rho_i = |\psi_i\rangle\langle\psi_i|$. Označme si $\mathscr{H} \equiv \mathscr{H}_A$ a připomeňme, že $\{|\psi_i\rangle\}_{i=1}^N$ nejsou obecně ortonormální. Definujme si pomocné vektory $|\psi^{AB}\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$ ležící v prostoru $\mathscr{H}_A \otimes \mathscr{H}_B$, kde $\{|i\rangle\}_i$ je ortonormální báze prostoru $\mathscr{H}_B$ dimenze $\dim \mathscr{H}_B = N$. Vidíme, že platí $\sum_i p_i\rho_i = \rho_A \equiv \mathrm{Tr}_B(|\psi^{AB}\rangle\langle\psi^{AB}|)$ a $\rho_B \equiv \mathrm{Tr}_A(|\psi^{AB}\rangle\langle\psi^{AB}|) = \sum_{ijk} \sqrt{p_i p_j}\langle e_k|\psi_i\rangle\langle\psi_j|e_k\rangle|i\rangle\langle j|$, kde $\{e_k\}_k$ je ortonormální báze prostoru $\mathscr{H}_A$. Pak $S(\sum_i p_i\rho_i) = S(\rho_A) = S(\rho_B)$, což plyne z obecných vlastností entropie. Z nerovnosti (27) dále $-\mathrm{Tr}(\rho\ln\rho) \le -\mathrm{Tr}(\rho\ln\rho')$ pro libovolné $\rho, \rho' \in \mathcal{S}(\mathscr{H}_B)$. Můžeme tedy vzít $\rho'_B = \sum_i p_i|i\rangle\langle i|$ a aplikovat nerovnost, abychom obdrželi $S(\rho_B) = -\mathrm{Tr}(\rho_B\ln\rho_B) \le -\mathrm{Tr}(\rho_B\ln\rho'_B)$. Nyní si uvědomíme, že stopa přes celý prostor je tvaru $\mathrm{Tr}(\cdot) = \sum_{ik}\langle e_k|\langle i|(\cdot)|e_k\rangle|i\rangle$. Explicitním výpočtem lze snadno zjistit, že poslední výraz, ke kterému jsme zatím dospěli, je roven $-\sum_i \mathrm{Tr}(\sum_k p_i|\langle e_k|\psi_i\rangle|^2|i\rangle\langle i|\ln\rho'_B)$. S pomocí Parsevalovy rovnosti lze tento výraz upravit na tvar $-\sum_i \mathrm{Tr}(p_i|i\rangle\langle i|\ln\rho'_B) = -\mathrm{Tr}(\rho'_B\ln\rho'_B) = -\sum_i p_i\ln p_i = H(\{p_i\}_i)$. Pro čisté stavy ρ_i jsme tedy dokázali nerovnost $S(\sum_i p_i\rho_i) \le H(\{p_i\}_i)$.

Pro obecné stavy máme $\rho_i = \sum_j p_j^{(i)}|e_j^{(i)}\rangle\langle e_j^{(i)}|$ a tedy $\rho = \sum_i p_i\rho_i = \sum_{ij} p_i p_j^{(i)}|e_j^{(i)}\rangle\langle e_j^{(i)}|$. Tento operátor můžu chápat jako soubor čistých stavů $\{|e_j^{(i)}\rangle\}_{ij}$ s pravděpodobnostním rozdělením $\{p_i p_j^{(i)}\}_{ij}$, na které mohu aplikovat výsledek obdržený výše. Dostáváme tudíž zřejmé vztahy $S(\rho) \le H(\{p_i p_j^{(i)}\}_{ij}) = -\sum_{ij} p_i p_j^{(i)} \ln p_i p_j^{(i)} = -\sum_{ij} p_i p_j^{(i)} \ln p_i - \sum_{ij} p_i p_j^{(i)} \ln p_j^{(i)}$. Tento výraz lze zjevně upravit dále na $-\sum_i(\sum_j p_j^{(i)})p_i\ln p_i + \sum_i p_i(-\sum_j p_j^{(i)}\ln p_j^{(i)}) = H(\{p_i\}_i) + \sum_i p_i S(\rho_i)$, což bylo dokázati. □

5.1 Relativní entropie

Kromě obyčejné entropie je vhodné si zavést další podobné pojmy, jakým je například relativní entropie. Než přikročíme k definici kvantové relativní entropie, je názorné si připomenout definici klasické relativní entropie. Ta je pro dvě pravděpodobnostní rozdělení $\vec{p} \equiv \{p_i\}_i$ a $\vec{q} \equiv \{q_i\}_i$ definována vztahem $S(\vec{q}\|\vec{p}) = \sum_i(q_i\ln q_i - q_i\ln p_i)$.

Příklad 5.1. *Nesouměrná mince.* Házejme si mincí a zjišťujme, s jakou pravděpodobností nám padne panna či orel. Chceme přitom zjistit, jaké pravděpodobnostní rozdělení sledují výsledky hodů této mince. Nechť $\{p, 1-p\}$ je pravděpodobnostní rozdělení, které mince skutečně sleduje a nechť $\{q, 1-q\}$ je nějaké jiné rozdělení. Dále nechť p, resp. q, odpovídá situaci, kdy nám padne panna, a podobně nechť $1-p$, resp. $1-q$, odpovídá situaci, kdy nám padne orel. Zajímá nás tedy, jaká je pravděpodobnost, že zaměníme rozdělení $\vec{p}$ a $\vec{q}$.

Při provedení N nezávislých pokusů je pravděpodobnost, že právě n-krát padne panna, rovna $p(n,N) = \binom{N}{n} p^n (1-p)^{N-n}$. Využijeme-li Stirlingovy formule pro aproximaci faktoriálu, obdržíme

$$
\begin{aligned}
\ln p(n,N) &= \ln \frac{N!}{n!(N-n)!} p^n (1-p)^{N-n} \sim \ln \frac{\left(\frac{N}{e}\right)^N}{\left(\frac{n}{e}\right)^n \left(\frac{N-n}{e}\right)^{N-n}} p^n (1-p)^{N-n} \\
&= N \ln N - n \ln n - (N-n)\ln(N-n) + n \ln p + (N-n)\ln(1-p) \\
&= -N\left(-\ln N + \frac{n}{N}\ln n + \left(1-\frac{n}{N}\right)\ln(N-n) - \frac{n}{N}\ln p - \left(1-\frac{n}{N}\right)\ln(1-p)\right) \\
&= -N\left(\frac{n}{N}\ln\frac{n}{N} + \left(1-\frac{n}{N}\right)\ln\left(1-\frac{n}{N}\right) - \frac{n}{N}\ln p - \left(1-\frac{n}{N}\right)\ln(1-p)\right).
\end{aligned}
$$

Označme si nyní $q = n/N$, předchozí výraz se tak redukuje do tvaru, v němž rozpoznáváme relativní entropii $-N(q\ln q + (1-q)\ln(1-q) - q\ln p - (1-q)\ln(1-p)) = -NS(\vec{q}\|\vec{p})$. Obdrželi jsme tak vzorec, kterému se říká *Sanovova věta*

$$p(\vec{q}\|\vec{p}) = e^{-NS(\vec{q}\|\vec{p})}, \tag{35}$$

kde $p(\vec{q}\|\vec{p})$ označuje pravděpodobnost záměny rozdělení $\vec{p}$ a $\vec{q}$. Z tohoto vzorce je patrné, že pravděpodobnost záměny se zmenšuje se zvětšující se relativní entropií. Relativní entropii lze chápat jako míru rozlišitelnosti rozdělení $\vec{p}$ a $\vec{q}$.

Relativní entropie *není* obecně symetrická, tj. obecně $S(\vec{p}\|\vec{q}) \neq S(\vec{q}\|\vec{p})$. Například pro rozdělení $\vec{p} = (1,0)$ a $\vec{q} = (1/2, 1/2)$ dostáváme $S(\vec{p}\|\vec{q}) = 1\ln 1 + 0\ln 0 - 1\ln 1/2 - 0\ln 1/2 = \ln 2$, zatímco $S(\vec{q}\|\vec{p}) = 1/2\ln 1/2 + 1/2\ln 1/2 - 1/2\ln 1 - 1/2\ln 0 = +\infty$. Přejděme nyní k definici *kvantové* relativní entropie.

Definice 5.3. Mějme dva operátory hustoty $\rho, \sigma \in \mathcal{S}(\mathscr{H})$. Pak **kvantová relativní entropie** pro tyto dva stavy je definována vztahem

$$S(\rho\|\sigma) = \mathrm{Tr}(\rho\ln\rho - \rho\ln\sigma). \tag{36}$$

Kvantovou relativní entropii dvou stavů lze chápat jako míru rozlišitelnosti (či nezaměnitelnosti) těchto dvou stavů. Uvažujme nyní stav ρ systému složeného ze dvou podsystémů A a B. Stavy jednotlivých podsystémů jsou zřejmě rovny $\rho_A = \mathrm{Tr}_B\,\rho$ a $\rho_B = \mathrm{Tr}_A\,\rho$. Jak už jsme si dříve řekli, stav podsystému A společně se stavem podsystému B *nejsou* schopny reprodukovat všechny vlastnosti obsažené ve stavu ρ složeného systému. Důvodem je to, že jednotlivé stavy podsystémů neobsahují informaci o jejich vzájemném provázání. Podívejme se, o kolik informace přijdeme, omezíme-li se pouze na stavy ρ_A a ρ_B namísto stavu ρ. Dostáváme $S(\rho\|\rho_A\otimes\rho_B) = \mathrm{Tr}(\rho\ln\rho) - \mathrm{Tr}(\rho\ln(\rho_A\otimes\rho_B)) = \mathrm{Tr}(\rho\ln\rho) - \mathrm{Tr}(\rho\ln(\mathbb{I}\otimes\rho_B)) - \mathrm{Tr}(\rho\ln(\rho_A\otimes\mathbb{I})) =$

$-S + S_A + S_B = I_C$. Vidíme tedy, že míra rozlišitelnosti provázaného stavu ρ od toho neprovázaného $\rho_A \otimes \rho_B$ je rovna indexu korelace I_C zavedenému výše.

Kvantová relativní entropie má dále následující vlastnosti, kde $\rho, \sigma \in \mathcal{S}(\mathscr{H})$ jsou libovolné operátory hustoty.

- $S(\rho\|\sigma) = +\infty$ právě tehdy, když $\operatorname{supp}\sigma \subset \operatorname{supp}\rho$,
- $S(\rho\|\sigma) \geq 0$, což plyne z Kleinovy nerovnosti; rovnost se přitom nabývá právě tehdy, když $\rho = \sigma$,
- $S(U\rho U^\dagger \| U\sigma U^\dagger) = S(\rho\|\sigma)$ pro všechny unitární operátory $U \in \mathcal{B}(\mathscr{H})$.

6 Kvantové měření

V základním kurzu kvantové mechaniky jsme se seznámili se způsobem, jakým se popisuje kvantové měření. Na rozdíl od měření v klasické fyzice, kvantové měření se přímo účastní vývoje systému. Po změření je stav systému obecně jiný, než před ním. To může být na jednu stranu nevýhodou, na druhou stranu lze však takovéto měření využít k přípravě stavů v přesně daném tvaru. Mějme úplný soubor pozorovatelných $M_1, \ldots, M_k$ odpovídajících nějakým fyzikálním veličinám $V_1, \ldots, V_k$. Po měření na daném stavu obdržíme soubor hodnot, neboli výsledků měření, $m_1, \ldots, m_k$ příslušný pozorovatelným $M_1, \ldots, M_k$. Z úplnosti množiny pozorovatelných pak máme zajištěno, že se změřený systém bude nacházet ve stavu, který je vlastním vektorem všech daných pozorovatelných s vlastními čísly $m_1, \ldots, m_k$. Můžeme si tedy připravit mnoho těchže systémů v libovolných stavech, na nich provádět měření a vybrat vždy jen ty systémy, pro které byly naměřené hodnoty totožné a rovné $m_1, \ldots, m_k$. Takto lze vyrábět stejné stavy o daném tvaru.

Existuje několik způsobů, jak formalizovat měření v kvantové mechanice. O nich lze ukázat, že jsou ekvivalentní, pokud vezmeme v úvahu i další postuláty kvantové mechaniky, nejen postulát o měření. V následujícím si představíme dvě koncepce, von Neumannovo měření a zobecněné měření.

6.1 von Neumannovo měření

Často používaným formalizmem je ten von Neumannům. Zde je každé vlastnosti B přidružen ortogonální projektor $E(B)$. Platí tedy $E(B) = E^\dagger(B) = E^2(B)$. Je-li na systému ve stavu ρ zjištěn výskyt veličiny B, tak se systém po změření nachází ve stavu

$$\rho' = \frac{E(B)\rho E(B)}{\mathrm{Tr}(E(B)\rho E(B))}. \tag{37}$$

Vlastnost B je přitom naměřena s pravděpodobností

$$p(B) \equiv \mathrm{Tr}(E(B)\rho E(B)) = \mathrm{Tr}(E(B)\rho). \tag{38}$$

Jak víme ze základního kurzu, každé veličině přísluší nějaká pozorovatelná R, tj. hermitovský operátor působící na Hilbertově prostoru daného kvantového systému. Ukažme si nyní, jak je toto pojetí v souladu s formalizmem von Neumannova měření. Mějme samosdružený operátor R definovaný obecně na podmnožině $D(R)$ Hilbertova prostoru $\mathscr{H}$, tedy $R : D(R) \to \mathscr{H}$, $R = R^\dagger$. Z funkcionální analýzy plyne, že tento operátor lze spektrálně rozložit způsobem

$$R = \int_{-\infty}^{\infty} r \,\mathrm{d}E_r, \tag{39}$$

kde E_r je spektrální třída projektorů splňující následující tři vlastnosti

1. $E_{r'} \geq E_r \quad \text{pro} \quad r' \geq r$,
2. $\lim_{\varepsilon \to 0} E_{r+\varepsilon} = E_r$,

3. $\lim_{r\to-\infty} E_r = 0, \quad \lim_{r\to+\infty} E_r = \mathbb{I}$.

Označme si nyní $\Delta r_i = (r_{i-1}, r_i]$ a $\Delta E_i = E_{r_i} - E_{r_{i-1}}$. Platí tedy zřejmé vztahy $\bigcup_i \Delta r_i = \mathbb{R}$ a $\sum_i \Delta E_i = \mathbb{I}$, $\Delta E_i \Delta E_j = \delta_{ij} \Delta E_i$. Množině $\{\Delta E_i\}$ se říká *ortogonální rozklad jednotky*. Měřme nyní fyzikální veličinu reprezentovanou pomocí pozorovatelné R na systému o stavu ρ. Při každém měření můžeme dostat obecně různé číselné výsledky $r \in \mathbb{R}$. Ptejme se dále, s jakou pravděpodobností obdržíme po změření hodnotu r ležící v intervalu Δr_i. Intervalu odpovídá projektor ΔE_i, tato pravděpodobnost je tedy podle von Neumanna rovna $p(\Delta r_i) = \mathrm{Tr}(\Delta E_i\, \rho)$. Podobně výsledný stav po takovém měření zní

$$\rho' = \frac{\Delta E_i\, \rho\, \Delta E_i}{\mathrm{Tr}(\Delta E_i\, \rho)}. \tag{40}$$

Z těchto výrazů a vztahů pro ortogonální rozklad jednotky ihned plynou rovnosti $\sum_i p(\Delta r_i) = 1$ a $\rho'_i \rho'_j = \delta_{ij} \rho'_i$. Veličinu $p_i \equiv p(\Delta r_i)$ lze tedy skutečně interpretovat jako pravděpodobnost, neboť je správně normalizovaná na jedničku a navíc je pro každý interval Δr_i nezáporná, což plyne z pozitivity operátorů ΔE_i.

Jak vidno, měřením vzniknou podmíněné soubory operátorů hustoty $\{(p_i, \rho'_i)\}_i$. Po měření máme s pravděpodobností p_i výsledný stav tvaru ρ'_i. Lze rozlišovat mezi dvěma způsoby, jakým měření provádíme. Buď daný počáteční stav změříme a koukneme se na výsledek měření. Tak zjistíme, že systém je v některém ze stavů tvaru (40). Této variantě se říká **selektivní měření**. Naproti tomu můžeme však systém změřit a na výsledek měření se nepodívat. Neboť nyní nevíme, v jakém stavu se systém přesně nachází, musíme středovat přes všechny možnosti s příslušnými pravděpodobnostmi. Na konci měření máme tak systém popsán stavem

$$\rho' = \sum_i p_i \rho'_i = \sum_i \mathrm{Tr}(\Delta E_i\, \rho) \frac{\Delta E_i\, \rho\, \Delta E_i}{\mathrm{Tr}(\Delta E_i\, \rho)} = \sum_i \Delta E_i\, \rho\, \Delta E_i. \tag{41}$$

Tato varianta se nazývá **neselektivní měření**.

6.2 Zobecněné měření

Ukažme si nyní obecnější přístup k zachycení kvantového měření. Po změření daného systému v daném stavu ρ dostáváme výsledek měření, nějakou číselnou hodnotu m. Označme si množinu všech takovýchto možných výstupů měření symbolem $\mathcal{M}$ a zkoumejme s jakou pravděpodobností naměříme hodnotu $m \in \mathcal{M}$. Od počátku uvažujeme, že tato pravděpodobnost bude záviset jednak na hodnotě m, jednak na vstupním stavu ρ. Je to tedy jistá funkce $p(m) = f_m(\rho)$. Vezmeme-li v úvahu rozklad $\rho = \sum_i p_i \rho_i$ a základní pravidla pro počítání s podmíněnými pravděpodobnostmi $p(\cdot|\cdot)$, docházíme ke vztahům

$$f_m(\rho) = p(m) = \left(\sum_i p(i|m)\right) p(m) = \sum_i p(i|m) p(m) = \sum_i p(m|i) p_i = \sum_i p_i f_m(\rho_i). \tag{42}$$

Vidíme tedy, že funkce f_m by měla být lineární na konvexních kombinacích stavů. Bez újmy na obecnosti ji tedy můžeme chápat jako lineární zobrazení na celém prostoru omezených operátorů $\mathcal{B}(\mathscr{H})$. Toto zobrazení navíc na vstupní stav vrátí číslo. Jedná se tedy o lineární funkcionál a z Rieszovy věty existuje jednoznačně daný operátor $F_m \in \mathcal{B}(\mathscr{H})$ tak, že lze f_m vyjádřit pomocí skalárního součinu $f_m(\rho) = (\rho, F_m)$. Připomeňme, že Hilbert-Schmidtův skalární součin je definován vztahem $(A, B) = \mathrm{Tr}(A^\dagger B)$. Celkem jsme tedy dostali operátor F_m tak, že $p(m) = \mathrm{Tr}(F_m \rho)$. Aby výraz $p(m)$ mohl představovat pravděpodobnostní rozdělení, musíme ještě požadovat nezápornost $p(m) \geq 0$ a normalizaci na jedničku. Tyto podmínky jsou zajištěny, splňují-li operátory F_m pro hodnoty $m \in \mathcal{M}$ vztah $\sum_{m\in\mathcal{M}} F_m = \mathbb{I}$ a jsou-li všechny pozitivní, $F_m \geq 0$. Právě uvedená úvaha byla motivací pro zavedení pravděpodobnosti ve tvaru

$$p(m) = \mathrm{Tr}(F_m\,\rho), \tag{43}$$

kde F_m jsou pozitivní operátory splňující $\sum_{m\in\mathcal{M}} F_m = \mathbb{I}$. Těmto operátorům se říká **efekty**. Dosud jsme popisovali zobecněné kvantové měření pouze z pohledu jeho výstupních hodnot $m \in \mathcal{M}$ a jejich pravděpodobností $p(m)$. Nezajímali jsme se o tvar výsledného stavu ρ'_m. Této koncepci se říká **POVM měření**, což pochází z anglického *Positive-Operator-Valued Measurement*. POVM operátory F_m nejsou schopny zachytit tvar výsledného stavu, ale hodí se pro popis pravděpodobností s jakými dostaneme jednotlivé výsledky.

Abychom mohli popsat i výsledný stav po měření ρ'_m, musíme formalizmus zobecněného měření rozšířit o další prvek. Tím jsou zobrazení $\phi_m : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$, která se nazývají **kvantové operace**, popřípadě **instrumenty**. Máme-li systém ve stavu ρ, po změření hodnoty $m \in \mathcal{M}$ přejde tento stav do tvaru

$$\rho'_m = \frac{1}{p(m)}\phi_m(\rho). \tag{44}$$

O zobrazeních ρ_m lze ukázat, že to jsou lineární a pozitivní superoperátory (viz později). Neboť výsledné stavy musejí být normalizovány na jednotkovou stopu, $1 = \mathrm{Tr}(\rho'_m) = \mathrm{Tr}(\phi_m(\rho))/p(m)$, dostáváme

$$\mathrm{Tr}(\phi_m(\rho)) = p(m) = \mathrm{Tr}(F_m\,\rho). \tag{45}$$

Při selektivním měření tedy obdržíme stav (44) s pravděpodobností (45). Při neselektivním pak máme

$$\rho' = \sum_{m\in\mathcal{M}} p(m)\,\rho'_m = \sum_{m\in\mathcal{M}} \phi_m(\rho). \tag{46}$$

Snadno nahlédneme, že při položení $F_m = \Delta E_m$ a $\phi_m(\rho) = \Delta E_m\,\rho\,\Delta E_m$ se zobecněné měření redukuje na von Neumannovo měření. Lze však ukázat i opačnou implikaci. Pokud se neomezíme jen na měření samotné a v úvahu vezmeme i unitární vývoj celého systému, jde zobecněné měření popsat pomocí měření von Neumannova a tohoto unitárního vývoje.

Vraťme se ještě k POVM měření popsanému výše, kdy se nestaráme o výsledný stav ρ'_m. Uvažujme obecnou situaci, kdy máme pro dané měření k dispozici instrumenty ϕ_m. Z rovnice (45) je vidět, že pokud provedeme pouze POVM měření, máme ve volbě instrumentů ϕ_m jistou volnost. Skutečně, soubor tvořený instrumenty $\phi_m(\rho) = \sqrt{F_m}\,\rho\,\sqrt{F_m}$ dává stejné pravděpodobnosti jako soubor tvořený instumenty $\phi_m(\rho) = U\sqrt{F_m}\,\rho\,\sqrt{F_m}U^\dagger$, kde U je nějaký unitární operátor.

Příklad 6.1. *Diskriminace stavů.* V tomto příkladu si připomeneme měření čistých stavů. Vzhledem k měřením popsaným výše se toto měření redukuje pouze na projekci čistých stavů coby vektorů na vektory nějaké ortonormální báze daného Hilbertova prostoru. Z dřívějška víme, že čisté stavy, které jsou navzájem ortogonální, lze s jistotou vždy rozlišit, měříme-li je ve vhodné ortonormální bázi. Pro konkrétnost mějme dva stavy $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ a $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Lze se snadno přesvědčit, že tyto stavy jsou správně znormalizované a navzájem kolmé. Měříme-li je ve výpočetní bázi $\{|0\rangle, |1\rangle\}$ dostáváme pro oba z nich s pravděpodobností $1/2$ vektor $|0\rangle$ a se stejnou pravděpodobností i vektor $|1\rangle$. Ve výpočetní bázi tedy tyto stavy odlišit nelze. Pootočíme-li však výpočetní bázi do báze tvořené samotnými vektory $\{|+\rangle, |-\rangle\}$, jejich rozlišení je zjevně dokonalé. Pro stav $|+\rangle$ obdržíme po projekci s pravděpodobností 1 tentýž stav $|+\rangle$ a podobně pro $|-\rangle$.

Uvažme nyní situaci, kdy máme dva různé vektory $|\psi_1\rangle$ a $|\psi_2\rangle$, které na sebe *nejsou* kolmé. I v tomto případě lze zkonstruovat měření, které je schopné tyto stavy odlišit. Avšak za cenu toho, že toto odlišení nebude možné při každém měření. Jako možnou konstrukci uvažujme dva ortogonální projektory, $P_1 = |\psi_1\rangle\langle\psi_1|$ a $P_2 = \mathbb{I} - |\psi_1\rangle\langle\psi_1|$. Snadno si rozmyslíme, že když zařízení odpovídající projektoru P_2 zaznamená vzruch, tak do něm vletěl stav $|\psi_2\rangle$. Pokud ale činnost zaznamenalo zařízení sdružené s operátorem P_1, nemůžeme o vlétajícím stavu nic říct, neboť oba stavy $|\psi_1\rangle$ i $|\psi_2\rangle$ mají nenulovou složku ve směru vektoru $|\psi_1\rangle$. Kdyby tomu tak nebylo, tak by $\langle\psi_1|\psi_2\rangle = 0$, což je ve sporu s předpoklady. Víme tedy alespoň, při kterém měření jsme *nedostali* stav $|\psi_1\rangle$. Obecně lze tento postup implementovat pomocí POVM operátorů

$$E_1 = a_1|\psi_2^\perp\rangle\langle\psi_2^\perp|, \quad E_2 = a_2|\psi_1^\perp\rangle\langle\psi_1^\perp|, \quad E_0 = \mathbb{I} - E_1 - E_2, \tag{47}$$

které nejsou projekcemi(!) Čísla a_i jsou zatím nespecifikovaná. V následujícím určíme jejich hodnotu tak, aby pravděpodobnost správného rozlišení stavů $|\psi_i\rangle$ byla největší. Označme si pravděpodobnost úspěchu, že zjistíme stav $|\psi_i\rangle$ jako p_i. Pak dostáváme $p_1 = \langle\psi_1|E_1|\psi_1\rangle = a_1\langle\psi_1|(\mathbb{I} - |\psi_2\rangle\langle\psi_2|)|\psi_1\rangle = a_1(1 - |d|^2)$, kde $d = \langle\psi_1|\psi_2\rangle$. Obdobně bychom obdrželi i vztah $p_2 = a_2(1 - |d|^2)$. Dále zjevně platí $\langle\psi_2|E_1|\psi_2\rangle = 0 = \langle\psi_1|E_2|\psi_1\rangle$. Pravděpodobnosti neúspěchu jsou rovny $q_i = \langle\psi_i|E_0|\psi_i\rangle = 1 - p_i$. Z těchto výsledků snadno nahlédneme explicitní tvar matice E_0. Protože tento operátor musí být pozitivní, platí

$$\begin{pmatrix} q_1 & d \\ d^* & q_2 \end{pmatrix} \geq 0, \tag{48}$$

neboli $q_1 q_2 \geq |d|^2$. Symbolem η_i dále označme pravděpodobnost, s jakou je stav $|\psi_i\rangle$ posílán do měřícího přístroje. Průměrná pravděpodobnost správného určení stavu tak zní zřejmě $P = p_1\eta_1 + p_2\eta_2$ a podobně průměrná pravděpodobnost nesprávného určení je $Q = q_1\eta_1 + q_2\eta_2 = 1 - P$. Jak vidno, maximum veličiny P odpovídá minimu pro Q. Snažíme-li se maximalizovat pravděpodobnost správného určení stavů, musíme minimalizovat výraz $q_1\eta_1 + q_2\eta_2$, kde q_i vystupují jako parametry. Z pozitivity operátoru E_0 vidíme, že tento operátor je nulový pro $q_2 = |d|^2/q_1$. (Tehdy máme ve hře jen operátory E_1 a E_2.) Dosadíme-li tuto hodnotu do minimalizovaného výrazu, dostáváme rovnost

$$\min Q = q_1\eta_1 + \frac{|d|^2}{q_1}\eta_2, \tag{49}$$

kde q_1 vystupuje jako parametr. Pomocí derivace určíme minimum tohoto výrazu. Zjišťujeme, že minima se nabývá pro $q_1 = |d|\sqrt{\eta_2/\eta_1}$ a $q_2 = |d|\sqrt{\eta_1/\eta_2}$, kdy je $Q_{\min} = 2\sqrt{\eta_1\eta_2}|d|$. Můžeme nyní zpětně dopočítat hodnoty a_i

$$a_1 = \frac{1 - |d|\sqrt{\frac{\eta_2}{\eta_1}}}{1 - |d|^2}, \quad a_2 = \frac{1 - |d|\sqrt{\frac{\eta_1}{\eta_2}}}{1 - |d|^2}. \tag{50}$$

Celkem tedy, POVM soubor operátorů tvaru (47), pro nějž je pravděpodobnost správného rozlišení stavů $|\psi_1\rangle$ a $|\psi_2\rangle$ největší, má prefaktory a_i rovny (50).

Příklad 6.2. NECHAPU UCEL PRIKLADU, ANI JEHO ZNENI Uvažujme dva operátory hustoty $\rho, \sigma \in \mathcal{S}(\mathscr{H})$. Nechť σ je stav, který dostávám. Jaká je pravděpodobnost, že tento stav zaměním se stavem ρ, provádím-li na něm měření? Míru, s jakou se dva stavy navzájem odlišují, lze kvantifikovat pomocí relativní entropie $S(\sigma\|\rho) = \mathrm{Tr}(\sigma \ln \sigma) - \mathrm{Tr}(\sigma \ln \rho)$. Veškerou informaci, kterou jsme schopni získat o tvaru obou stavů a jejich případné odlišnosti, pochází z kvantového měření a odpovídajících pravděpodobností nalezení daných výsledků. Různost dvou stavů lze tedy popsat i skrze klasickou entropii aplikovanou na pravděpodobnostní rozdělení příslušná jednotlivým stavům. Pro nějaký POVM soubor $\{A_i\}_i$ dostáváme pravděpodobnosti $p_i = \mathrm{Tr}(A_i \sigma)$ a $q_i = \mathrm{Tr}(A_i \rho)$. Hledáme nyní tedy takové POVM $\{A_i\}_i$, aby (klasická) relativní entropie S_1^{klas} byla nejvyšší, totiž aby

$$S_1^{\mathrm{klas}}(\sigma\|\rho) = \sup_{\{A_i\}} \left(\sum_i (\mathrm{Tr}(A_i \sigma) \ln \mathrm{Tr}(A_i \sigma) - \mathrm{Tr}(A_i \sigma) \ln \mathrm{Tr}(A_i \rho)) \right). \tag{51}$$

Tato hodnota nám bude říkat, jak moc lze stavy σ a ρ od sebe odlišit. Počítání hrůzného výrazu výše pro klasickou entropii lze zjednodušit, vezmeme-li N kopií $\sigma^N \coloneqq \sigma^{\otimes N}$ a $\rho^N \coloneqq \rho^{\otimes N}$ původních stavů a zvolíme-li POVM následujícím způsobem. Při volbě $A_i \in \mathcal{B}(\mathscr{H}^{\otimes N})$ (tj. operátory A_i působí na celých σ^N, resp. ρ^N), kde $\sum_i A_i = \mathbb{I}$, je nejvyšší možná relativní entropie tvaru

$$S_N(\sigma\|\rho) = \sup_{\{A_i\}} \frac{1}{N} \left(\sum_i (\mathrm{Tr}(A_i \sigma^N) \ln \mathrm{Tr}(A_i \sigma^N) - \mathrm{Tr}(A_i \sigma^N) \ln \mathrm{Tr}(A_i \rho^N)) \right). \tag{52}$$

Dále lze ukázat, že obecně $S(\sigma\|\rho) \geq S_N(\sigma\|\rho)$, kde se rovnosti nabývá právě tehdy, když $[\rho, \sigma] = 0$. Navíc, v limitě platí rovnost vždy, $S(\sigma\|\rho) = \lim_{N\to\infty} S_N(\sigma\|\rho)$. Když počítáme relativní entropii dvou stavů, stačí tedy uvažovat výrazy tvaru (52), které nám poskytnou spodní odhad, a popřípadě provést limitu $N \to \infty$.

7 Kvantové operace

V předchozích statích jsme se seznámili s kvantovým měřením. V případě zobecněného kvantového měření jsme si navíc zavedli jistá zobrazení, která popisovala výsledek takového měření a pravděpodobnost jeho výskytu. Tato zobrazení jsme nazvali kvantové operace. Konkrétně pro počáteční stav popsaný operátorem hustoty ρ jsme koncový stav zapisovali ve tvaru $\frac{1}{p_m}\phi_m(\rho)$. Tento stav se přitom mohl vyskytovat s pravděpodobností $p_m = \operatorname{Tr}\phi_m(\rho)$. Zde $\phi_m : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ jsou právě kvantové operace. Jejich použití se však neomezuje na popis kvantového měření. Nacházejí velmi široké uplatnění a pro studium otevřených kvantových systémů jsou klíčové. Proto se s nimi v této kapitole seznámíme podrobněji.

Formálně lze kvantové operace zavádět různými způsoby. My si nyní představíme axiomatický přístup. Na základě tří axiomů, které mají fyzikální opodstatnění, odvodíme tvar obecné kvantové operace. Mějme tedy nějaké zobrazení $\phi_m : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$. Pak toto zobrazení nazveme *kvantová operace*, splňuje-li následující tři axiomy.

Axiom 1. *Zobrazení ϕ_m je konvexně lineární vůči stavům. Neboli pro každý konečný soubor operátorů hustoty $\{\rho_i\}_i$ s pravděpodobnostním rozdělením $\{p_i\}_i$ platí*

$$\phi_m\left(\sum_i p_i\rho_i\right) = \sum_i p_i\,\phi_m(\rho_i). \tag{53}$$

Rozumnost tohoto požadavku nahlédneme v následující úloze. Mějme operátor hustoty tvaru $\rho = \sum_i p_i\rho_i$ a předpokládejme, že jsme na tomto stavu provedli měření s výsledkem m. Po změření dané fyzikální veličiny popsané operacemi $\{\phi_m\}_m$ se tak počáteční stav ρ zredukoval na $\frac{\phi_m(\rho)}{\operatorname{Tr}\phi_m(\rho)}$. Současně ale můžeme výsledek měření chápat jako kdybychom ho prováděli přímo na souboru $\{\rho_i\}_i$. Protože se každé ρ_i vyskytuje v ρ s jistou pravděpodobností, bude i výsledek měření záviset na těchto pravděpodobnostech. Pokud bychom změřili jeden daný ρ_i, vypadal by koncový stav jako $\frac{\phi_m(\rho_i)}{\operatorname{Tr}\phi_m(\rho_i)}$. My jsme ale změřili celý soubor $\{\rho_i\}_i$ najednou s výsledkem m. Situace, kdy změříme konkrétní ρ_i, tak přitom může nastat s pravděpodobností $p(i|m)$, což je pravděpodobnost změření operátoru ρ_i za předpokladu, že hodnota měření byla m. Celkem je tedy výsledek měření možno popsat jako vážený průměr $\sum_i p(i|m)\frac{\phi_m(\rho_i)}{\operatorname{Tr}\phi_m(\rho_i)}$. Ztotožníme-li oba přístupy, jak ten pomocí operátoru ρ, tak ten pomocí souboru $\{\rho_i\}_i$, dospíváme k rovnosti

$$\frac{\phi_m(\rho)}{\operatorname{Tr}\phi_m(\rho)} = \sum_i p(i|m)\frac{\phi_m(\rho_i)}{\operatorname{Tr}\phi_m(\rho_i)}. \tag{54}$$

Nyní můžeme využít Bayesova pravidla, podle něhož $p(i|m)p(m) = p(m|i)\,p_i$. Současně víme, že $p(m) = \operatorname{Tr}\phi_m(\rho)$ a $p(m|i) = \operatorname{Tr}\phi_m(\rho_i)$. Z předchozího vzorce si můžeme vyjádřit pravděpodobnost $p(i|m)$ a tu dosadit do vztahu (54) dostávajíce

$$\phi_m(\rho) = \sum_i p_i\,\phi_m(\rho_i). \tag{55}$$

Axiom výše hovoří pouze o linearitě na konvexní množině stavů. Z této konvexní podmnožiny lze ale kvantovou operaci lineárně dodefinovat na celý prostor.

Axiom 2. *Pro každý operátor hustoty ρ musí stopa zobrazení ϕ_m splňovat nerovnosti*

$$0 \leq \operatorname{Tr} \phi_m(\rho) \leq 1. \tag{56}$$

Opodstatnělost tohoto axiomu přímo plyne ze skutečnosti, že chceme, aby stopa $\operatorname{Tr} \phi_m(\rho)$ vyjadřovala pravděpodobnost. Musí být tedy nezáporná a menší nebo rovna jedné. Ostatně to jsme také předpokládali výše, když jsme chtěli nastínit rozumnost prvního axiomu. Pravděpodobnosti se musejí sčítat na jedničku, neboli

$$1 = \sum_m p_m = \sum_m \operatorname{Tr} \phi_m(\rho) = \operatorname{Tr}\left(\sum_m \phi_m(\rho)\right). \tag{57}$$

Označme si $\phi = \sum_m \phi_m$. Pak rovnost výše znamená $\operatorname{Tr} \phi(\rho) = 1$. Dále platí vztah $\operatorname{Tr}(\phi(\rho)) = \operatorname{Tr}(\phi^\dagger(\mathbb{I})\rho)$, který lze odvodit z vlastností Hilbert-Schmidtova skalárního součinu. Neboť je ρ stav, je splněno $\operatorname{Tr} \rho = 1$. Poskládáme-li předchozí výrazy dohromady, dostáváme

$$\operatorname{Tr}(\phi^\dagger(\mathbb{I})\rho) = \operatorname{Tr} \rho, \quad \forall \rho \in \mathcal{S}(\mathscr{H}). \tag{58}$$

To je splněno právě tehdy, když $\phi^\dagger(\mathbb{I}) = \mathbb{I}$. V této souvislosti si uveďme pár definic.

Definice 7.1. Řekneme, že obecné zobrazení ϕ **zachovává stopu** právě, když $\operatorname{Tr} \phi(\rho) = 1$ pro všechny stavy ρ. Podobně řekneme, že zobrazení ϕ **nezvyšuje stopu** právě, když platí $\operatorname{Tr} \phi^\dagger(\rho) \leq 1$. (Anglicky se zobrazení, které zachovává stopu, říká *trace-preserving mapping.* Podobně zobrazení, které stopu nezvyšuje, se nazývá *trace-non-increasing mapping.*)

Uveďme si konečně závěrečný axiom z definice kvantových operací. K jeho vyřčení bude nutná ještě jedna definice.

Definice 7.2. Zobrazení ϕ_m je **úplně pozitivní** právě tehdy, když je pozitivní každé zobrazení tvaru $\phi_m \otimes \mathbb{I}_{\tilde{\mathscr{H}}}$, kde $\tilde{\mathscr{H}}$ označuje libovolný dodatečný Hilbertův prostor, který jsme ke sledovanému prostoru přidali, a $\mathbb{I}_{\tilde{\mathscr{H}}}$ značí identitu na prostoru $\mathcal{B}(\tilde{\mathscr{H}})$. (Anglicky se úplně pozitivní řekne *completely positive* a zkracuje se na *CP*.)

Axiom 3. *Zobrazení ϕ_m je úplně pozitivní.*

Na první, ani druhý, pohled není zcela jasné, co tento axiom představuje. Tento požadavek souvisí s tím, že chceme, abychom aplikací zobrazení ϕ_m dostávali vždy *stavy* a nemohli tak dostat něco, co v kvantové mechanice nelze použít pro popis fyzikálního systému. Mějme zkoumaný systém A s prostorem $\mathscr{H}_A$, na nějž aplikujeme operaci ϕ_m. Představme si navíc, že tento systém tvoří jen část nějakého většího systému $A + B$, jehož prostor zní $\mathscr{H}_A \otimes \mathscr{H}_B$. Takovouto situaci je rozumné uvažovat, dost často nás v danou chvíli nezajímá stav celého systému, ale pouze jeho podsystému. Aplikaci operace ϕ_m lze tedy ekvivalentně popsat pomocí operátoru $\phi_m \otimes \mathbb{I}$, který působí na stav celého systému $A + B$. Nyní začíná být požadavek na úplnou pozitivitu jasnější. Aby původní (libovolný) stav celého systému $A + B$ přešel opět na *stav*, je nutné, aby operátor $\phi_m \otimes \mathbb{I}$ byl pozitivní. Neboť může být zkoumaný systém A podsystémem různě velkého systému, kde se prostor $\mathscr{H}_B$ mění, je nutné, aby operace $\phi_m \otimes \mathbb{I}$ byla pozitivní pro různé $\mathscr{H}_B$.

7.1 Vlastnosti kvantových operací

Působení superoperátoru $\phi_m \otimes \mathbb{I}_{\tilde{\mathscr{H}}}$ na libovolný prvek $X = \sum_i A_i \otimes B_i \in \mathcal{B}(\mathscr{H} \otimes \tilde{\mathscr{H}})$ vypadá následovně

$$(\phi_m \otimes \mathbb{I}_{\tilde{\mathscr{H}}})(X) = \sum_i (\phi_m \otimes \mathbb{I}_{\tilde{\mathscr{H}}})(A_i \otimes B_i) = \sum_i \phi_m(A_i) \otimes B_i. \tag{59}$$

Mohlo by se zdát, že ověřit úplnou pozitivitu nějakého zobrazení je těžký úkol, vždyť v definici požadujeme pozitivitu zobrazení $\phi_m \otimes \mathbb{I}_{\tilde{\mathscr{H}}}$ pro každý Hilbertův prostor $\tilde{\mathscr{H}}$. Ukazuje se však, že situace je mnohem jednodušší, než by se zdálo, a to hlavně díky následující větě.

Věta 7.1. *Lineární zobrazení $\phi : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ je úplně pozitivní právě tehdy, když*

$$(\phi \otimes \mathbb{I}_d)(|\Omega\rangle\langle\Omega|) \geq 0, \tag{60}$$

kde $d = \dim \mathscr{H}$ a $|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_\mu |\mu\mu\rangle$ je maximálně provázaný stav na $\mathscr{H} \otimes \mathscr{H}$.

Stačí tedy ověřovat pozitivitu jednoho konkrétního operátoru, který vznikne tak, že na maximálně provázaný stav aplikujeme zobrazení $\phi \otimes \mathbb{I}_d$, které se skládá z ϕ a identity na dodatečném prostoru. Za tento dodatečný prostor stačí přitom volit pouze jeden konkrétní prostor a to prostor $\mathscr{H}$ samotný. Ukažme si nyní důkaz předchozí věty.

Důkaz. DIVNE, NEUVAZUJE RUZNE DIMENZE A ODKUD PLATI, ZE OPERATOR A_k JE UNITARNI? Implikace zleva doprava je jasná. Z obecného tvrzení určitě plyne jeho konkrétní případ. Dokažme si tedy opačnou implikaci. Mějme pozitivní operátor působící na celém Hilbertově prostoru $\rho \in \mathcal{B}(\mathscr{H} \otimes \mathscr{H})$, kde $\dim \mathscr{H} = d$. Pak $(\phi \otimes \mathbb{I}_d)(\rho) \geq 0$ je ekvivalentní podmínce $(\phi \otimes \mathbb{I}_d)(|\psi_k\rangle\langle\psi_k|) \geq 0$ pro všechna k, kde $\rho = \sum_k \lambda_k |\psi_k\rangle\langle\psi_k|$. Neboť $|\psi_k\rangle$ je čistý stav, lze ho vyjádřit ve tvaru $|\psi_k\rangle = (\mathbb{I} \otimes A_k)|\Omega\rangle$ pro nějaký operátor $A_k : \mathscr{H} \to \mathscr{H}$, viz dříve. Takže $(\phi \otimes \mathbb{I}_d)(|\psi_k\rangle\langle\psi_k|) = (\phi \otimes \mathbb{I}_d)(\mathbb{I} \otimes A_k)|\Omega\rangle\langle\Omega|(\mathbb{I} \otimes A_k^\dagger) = (\mathbb{I} \otimes A_k)(\phi \otimes \mathbb{I}_d)(|\Omega\rangle\langle\Omega|)(\mathbb{I} \otimes A_k^\dagger)$. Poslední výraz je podobnostní transformací spjat s operátorem $(\phi \otimes \mathbb{I}_d)(|\Omega\rangle\langle\Omega|)$. Podobnost zachovává pozitivitu, je-li tedy $(\phi \otimes \mathbb{I}_d)(|\Omega\rangle\langle\Omega|)$ pozitivní, je takové i $(\phi \otimes \mathbb{I}_d)(|\psi_k\rangle\langle\psi_k|)$. □

V právě uvedené větě byl použit operátor, jehož význam doceníme především v následujících kapitolách. Je jím **Jamiolkowského stav** τ_ϕ definovaný pro každou operaci ϕ jako

$$\tau_\phi = (\phi \otimes \mathbb{I}_d)(|\Omega\rangle\langle\Omega|). \tag{61}$$

S využitím izomorfizmů, které jsme si zavedli na počátku, lze ukázat pěknou identitu

$$\tau_\phi = \frac{1}{d} X_\phi, \tag{62}$$

kde X_ϕ je operátor zavedený pomocí rovnice (14). Než přikročíme k důkazu této rovnosti, připomeňme si značení. Mějme zobrazení $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$, $\{|\mu\rangle\}_\mu$ nechť je ortonormální báze prostoru $\mathscr{H}_1$ a podobně nechť $\{|\nu\rangle\}_\nu$ je ortonormální báze prostoru $\mathscr{H}_2$. Dále nechť $\{|B^{\mu\nu}\rangle\}_{\mu\nu}$ a $\{|A^{mn}\rangle\}_{mn}$ jsou po řadě ortonormální báze prostorů $\mathcal{B}(\mathscr{H}_1)$ a $\mathcal{B}(\mathscr{H}_2)$, kde jsme si označili $|B^{\mu\nu}\rangle = |\mu\rangle\langle\nu|$ a $|A^{mn}\rangle = |m\rangle\langle n|$.

Jak jsme si již dříve uvedli, pro operaci ϕ, kterou si lze vyjádřit ve tvaru $\phi = \sum \phi_{\substack{mn\\ \mu\nu}} |A^{mn}\rangle\langle B^{\mu\nu}|$, platí následující vztah (14)

$$\phi = \sum_{mn\mu\nu} \phi_{\substack{mn\\ \mu\nu}} |A^{mn}\rangle\langle B^{\mu\nu}| \quad \leftrightarrow \quad X_\phi = \sum_{mn\mu\nu} \phi_{\substack{mn\\ \mu\nu}} A^{mn} \otimes B^{\mu\nu} = \sum_{mn\mu\nu} \phi_{\substack{mn\\ \mu\nu}} |m\mu\rangle\langle n\nu|, \tag{63}$$

tedy $X_\phi = \phi^R$. Rozepíšeme-li si maximálně provázaný stav v dané ortonormální bázi, je důkaz výše uvedené rovnosti triviální, neboť

$$\begin{aligned} \tau &= \frac{1}{d}(\phi \otimes \mathbb{I}_d)\left(\sum_{\mu\nu} |\mu\mu\rangle\langle\nu\nu|\right) = \frac{1}{d}\sum_{\mu\nu} \phi(|\mu\rangle\langle\nu|) \otimes |\mu\rangle\langle\nu| = \frac{1}{d}\sum_{\mu\nu} \phi(|B^{\mu\nu}\rangle) \otimes |\mu\rangle\langle\nu| \\ &= \frac{1}{d}\sum_{mn\mu\nu} \phi_{\substack{mn\\ \mu\nu}} |m\rangle\langle n| \otimes |\mu\rangle\langle\nu| = \frac{1}{d}\sum_{mn\mu\nu} \phi_{\substack{mn\\ \mu\nu}} |m\mu\rangle\langle n\nu| = \frac{1}{d} X_\phi. \end{aligned}$$

Pro praktické počítání si uveďme ještě jednu rovnost mezi stopami různých reprezentací těchže operátorů na daném prostoru s využitím Jamiolkowského stavu odpovídající dané operaci.

Lemma 7.1. *Nechť $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ je jisté zobrazení, dále nechť τ_ϕ je jemu odpovídající Jamiolkowského stav a X_ϕ operátor zavedený vztahem* (14)*. Pak pro každou dvojici operátorů $A \in \mathcal{B}(\mathscr{H}_2)$ a $B \in \mathcal{B}(\mathscr{H}_1)$ platí následující rovnosti*

$$\mathrm{Tr}(A\,\phi(B)) = \mathrm{Tr}(X_\phi\,(A \otimes B^T)) = d\ \mathrm{Tr}(\tau_\phi\,(A \otimes B^T)). \tag{64}$$

Důkaz. Druhá rovnost plyne ze vztahu (62), dokažme si tedy rovnost první. Opět začněme výčtem značení: $A = \sum_{mn} A_{mn}|m\rangle\langle n|$, $B = \sum_{\mu\nu} B_{\mu\nu}|\mu\rangle\langle\nu|$, $X_\phi = \sum_{m\mu n\nu} \phi_{\substack{mn\\ \mu\nu}} |m\mu\rangle\langle n\nu|$, z čehož plyne $A \otimes B^T = \sum_{m\mu n\nu} A_{mn}B_{\mu\nu}|m\nu\rangle\langle n\mu|$ a $\phi(B) = \phi(\sum_{\mu\nu} B_{\mu\nu}|\mu\rangle\langle\nu|) = \sum_{ab\mu\nu} B_{\mu\nu}\phi_{\substack{ab\\ \mu\nu}}|a\rangle\langle b|$. Pro levou stranu rovnosti tedy platí

$$\begin{aligned} \mathrm{Tr}(A\,\phi(B)) &= \mathrm{Tr}\left(\sum_{mn} A_{mn}|m\rangle\langle n| \sum_{ab\mu\nu} B_{\mu\nu}\phi_{\substack{ab\\ \mu\nu}}|a\rangle\langle b|\right) = \mathrm{Tr}\left(\sum_{abm\mu n\nu} A_{mn}B_{\mu\nu}\phi_{\substack{ab\\ \mu\nu}}|m\rangle\langle n||a\rangle\langle b|\right) \\ &= \sum_{m\mu n\nu} A_{mn}B_{\mu\nu}\phi_{\substack{nm\\ \mu\nu}}. \end{aligned}$$

Přitom pro pravou stranu téže dokazované rovnosti dostáváme

$$\mathrm{Tr}(X_\phi\,(A \otimes B^T)) = \mathrm{Tr}\left(\sum_{m\mu n\nu} \phi_{\substack{mn\\ \mu\nu}}|m\mu\rangle\langle n\nu| \sum_{a\alpha b\beta} A_{ab}B_{\alpha\beta}|a\beta\rangle\langle b\alpha|\right) = \sum_{m\mu n\nu} A_{nm}B_{\mu\nu}\phi_{\substack{mn\\ \mu\nu}}.$$

Porovnáním odpovídajících si indexů tak vidíme, že obě strany si jsou skutečně rovny. □

Výhodnost zavedení operátoru X_ϕ lze ilustrovat i na příkladu následující věty podávající vztah mezi tímto operátorem a některými vlastnostmi operace ϕ.

Věta 7.2. *Nechť $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$. Pak platí následující ekvivalence mezi zobrazením ϕ a operátorem X_ϕ, resp. τ_ϕ, kde $B \in \mathcal{B}(\mathscr{H}_1)$ je libovolný.*

1. *Hermitovost:* $\phi(B^\dagger) = \phi(B)^\dagger \Leftrightarrow X_\phi = X_\phi{}^\dagger$,
2. *úplná pozitivita:* ϕ *je CP* $\Leftrightarrow X_\phi \geq 0$,
3. *zachování stopy:* $\operatorname{Tr}\phi(B) = \operatorname{Tr}B \Leftrightarrow \operatorname{Tr}_{\mathscr{H}_2}(X_\phi) = \mathbb{I}_{\mathscr{H}_1}$,
4. *unitalita:* $\phi(\mathbb{I}) = \mathbb{I} \Leftrightarrow \operatorname{Tr}_{\mathscr{H}_1}(X_\phi) = \mathbb{I}_{\mathscr{H}_2}$.

Důkaz. Abychom dokázali první bod, uvažme předchozí větu, podle níž $\operatorname{Tr}(X_\phi\,(A\otimes B^*)) = \operatorname{Tr}(A\,\phi(B^\dagger))$. Předpokládejme nyní rovnost $\phi(B^\dagger) = \phi(B)^\dagger$ pro důkaz implikace zleva. Pak $\operatorname{Tr}(A\,\phi(B^\dagger)) = \operatorname{Tr}(A\,\phi(B)^\dagger) = \operatorname{Tr}((\phi(B)\,A^\dagger)^\dagger) = \operatorname{Tr}(\phi(B)\,A^\dagger)^*$. Opět s využitím předchozí věty je poslední výraz roven $\operatorname{Tr}(X_\phi\,(A^\dagger\otimes B^T))^* = \operatorname{Tr}(X_\phi{}^\dagger\,(A\otimes B^*))$. Porovnáním prvního výrazu výše a právě získaného posledního výrazu, kterážto rovnost musí platit pro všechna $A\in\mathcal{B}(\mathscr{H}_2)$ a $B\in\mathcal{B}(\mathscr{H}_1)$, dospíváme k identitě $X_\phi = X_\phi{}^\dagger$. Opačná implikace by se dokázala stejně, pouze v opačném pořadí. Pro důkaz druhého bodu si stačí připomenout, že ϕ je úplně pozitivní právě tehdy, když Jamiolkowského stav τ_ϕ je pozitivní a z identity (62) již plyne tvrzení. K dokázání třetího bodu vyjděme z předchozí věty: $\operatorname{Tr}(\phi(B)) = \operatorname{Tr}(X_\phi\,(\mathbb{I}\otimes B^T)) = \operatorname{Tr}_{(\mathscr{H}_1)}((\operatorname{Tr}_{\mathscr{H}_2}(X_\phi))B^T)$. Současně již z dřívějška víme, že zachování stopy je ekvivalentní s tvrzením $\phi^\dagger(\mathbb{I}) = \mathbb{I}$. S využitím vlastností skalárního součinu tedy $\operatorname{Tr}(\phi(B)) = (\mathbb{I},\phi(B)) = (\phi^\dagger(\mathbb{I}),B) = (\mathbb{I},B) = \operatorname{Tr}(B) = \operatorname{Tr}(B^T)$. Porovnáním obou výpočtů, které si jsou rovny pro všechny operátory B, dostáváme $\operatorname{Tr}_{\mathscr{H}_2}(X_\phi) = \mathbb{I}_{\mathscr{H}_1}$, což jsme chtěli dokázat. Čtvrtý bod by se dokázal podobně jako bod třetí. □

Poznámka 7.1. Uvědomme si důležitý vztah: *Jamiolkowský stav τ_ϕ úplně pozitivního zobrazení ϕ zachovávajícího stopu je operátorem hustoty.* Ačkoli se τ_ϕ nazývá slovem *stav*, skutečným stavem, tj. operátorem hustoty, je jen, když zobrazení ϕ splňuje podmínky uvedené v předchozí větě.

Příklad 7.1. Nyní si udáme příklad jednoduchého zobrazení, které je sice pozitivní, není ale úplně pozitivní. Tím zobrazením je superoperátor transponování $\phi:\mathcal{B}(\mathscr{H})\to\mathcal{B}(\mathscr{H})$, $\phi(A) = A^T$ (transponování v bázi $\{|\mu\rangle\}_{\mu=1}^d$). Neboť transpozicí nezměníme spektrum operátoru, je-li tento pozitivní, je pozitivní i jeho transpozice. Je ϕ úplně pozitivní? Využijme věty 7.1. Máme tak $\tau_\phi = (\phi\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) = \frac{1}{d}(\phi\otimes\mathbb{I})\sum_{\mu\nu}|\mu\mu\rangle\langle\nu\nu| = \frac{1}{d}\sum_{\mu\nu}\phi(|\mu\rangle\langle\nu|)\otimes|\mu\rangle\langle\nu| = \frac{1}{d}\sum_{\mu\nu}|\nu\rangle\langle\mu|\otimes|\mu\rangle\langle\nu| = \frac{1}{d}\sum_{\mu\nu}|\nu\mu\rangle\langle\mu\nu|$. Abychom viděli, že operátor τ_ϕ není pozitivní, uvažme případ $d=2$ a bázi $\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$, pro něž dostáváme

$$\tau_\phi = \begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}. \tag{65}$$

Tato matice má za vlastní čísla 1 a -1, není tedy pozitivní a my tak můžeme shrnout, že zobrazení ϕ není úplně pozitivní.

Z výše uvedené věty o úplné pozitivitě superoperátoru plynou následující dva užitečné důsledky. Jeden hovoří o rozkladu zobrazení na úplně pozitivní zobrazení. Druhý se pak vztahuje ke kvantovému měření.

Důsledek 7.1. Rozklad na úplně pozitivní zobrazení. *Nechť* $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ *je lineární zobrazení. Pak:*

1. *Zobrazení* ϕ *lze zapsat jako komplexní lineární kombinaci čtyř úplně pozitivních zobrazení.*
2. *Pokud je* ϕ *navíc hermitovské, tj.* $\phi(B^\dagger) = \phi^\dagger(B)$, *tak jej lze zapsat jako reálnou lineární kombinaci dvou úplně pozitivních zobrazení.*

Důkaz. Zobrazení ϕ je izomorfně svázané s operátorem $X_\phi = d\,\tau_\phi$, jež lze rozložit způsobem $X_\phi = (X_\phi + X_\phi^\dagger)/2 + \mathrm{i}\,(X_\phi - X_\phi^\dagger)/(2\mathrm{i}\,)$. Označíme-li nyní symbolem Pos pozitivní část operátoru a jako Neg jeho „negativní" část, tak

$$X_\phi = \mathrm{Pos}\left(\frac{X_\phi + X_\phi^\dagger}{2}\right) - \mathrm{Neg}\left(\frac{X_\phi + X_\phi^\dagger}{2}\right) + \mathrm{i}\ \mathrm{Pos}\left(\frac{X_\phi - X_\phi^\dagger}{2\mathrm{i}}\right) - \mathrm{i}\ \mathrm{Neg}\left(\frac{X_\phi - X_\phi^\dagger}{2\mathrm{i}}\right). \tag{66}$$

Všechny výrazy tvaru $\mathrm{Pos}(\cdot)$ či $\mathrm{Neg}(\cdot)$ jsou pozitivní operátory, po řadě izomorfně sdružené se zobrazeními ϕ_1 až ϕ_4, která jsou tak úplně pozitivní. Máme tak rozklad zobrazení na úplně pozitivní zobrazení ve tvaru

$$\phi = \phi_1 - \phi_2 + \mathrm{i}\,\phi_3 - \mathrm{i}\,\phi_4. \tag{67}$$

Druhé tvrzení se dokáže naprosto analogicky. Hermiticita zobrazení ϕ zaručuje $X_\phi = X_\phi^\dagger$, které je tak tvaru $X_\phi = \mathrm{Pos}(X_\phi) - \mathrm{Neg}(X_\phi)$. Z toho již rovnou plyne $\phi = \phi_1 - \phi_2$. □

Důsledek 7.2. „Žádná informace bez narušení." – "No information without disturbance." *Nechť* $T_\alpha : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ *jsou instrumenty (kvantové operace). Pokud neselektivní měření nezmění stav (tedy* $T = \sum_\alpha T_\alpha = \mathbb{I}$*), tak* $T_\alpha \propto \mathbb{I}$ *pro všechna* α *a pravděpodobnost získání výstupu* α *je nezávislá na vstupním stavu.*

Důkaz. Máme $(T \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) = |\Omega\rangle\langle\Omega|$ a $(T \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) = \sum_\alpha (T_\alpha \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) = \sum_\alpha \tau_\alpha$, kde $\tau_\alpha \geq 0$ a $|\Omega\rangle\langle\Omega|$ je čistý stav. Pak tedy

$$|\Omega\rangle\langle\Omega| = \sum_\alpha \mathrm{Tr}(\tau_\alpha)\left(\frac{\tau_\alpha}{\mathrm{Tr}(\tau_\alpha)}\right), \tag{68}$$

což je konvexní lineární kombinace stavů, která dává čistý stav. Z toho již plyne existence konstant A_α takových, že $\tau_\phi = A_\alpha |\Omega\rangle\langle\Omega|$ pro všechna α, a tedy $T_\alpha = A_\alpha \mathbb{I}$. Pro pravděpodobnosti navíc platí $p_\alpha = \mathrm{Tr}(T_\alpha(\rho)) = A_\alpha$. □

Z předchozího důsledku plyne, že při měření stavu, kdy se nekoukneme na výsledek tohoto měření a toto měření navíc nijak nezmění stav, nejsme schopni zjistit jakoukoli informaci o tvaru měřeného stavu.

7.2 Implementace kvantové operace teleportací

V předchozích kurzech jsme se seznámili s kvantovou teleportací částic. Nyní tento koncept využijeme při implementaci kvantové operace ϕ zachovávající stopu. Jinými slovy, zobrazení $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ je nyní *kvantový kanál.* Konkrétně uvažme Alici, která má ve vlastnictví kvantový kanál ϕ a navíc pár maximálně provázaných částic $|\Omega\rangle$. Na druhé straně zeměkoule nechť čeká trpělivý Bob, jehož jediným majetkem je částice ve stavu $\rho \in \mathcal{S}(\mathscr{H}_1)$. Chamtivé Alici se z rozmaru zachtělo získat stav $\phi(\rho)$, svízel však tkví v tom, že vstupní stav ρ leží kdesi u Boba. Zdánlivě bezvýchodnou situaci lze vyřešit s lehkou pomocí altruistického Boba následujícím kvantovým algoritmem.

1. Alice aplikuje svoji kvantovou operaci ϕ na první ze svých částic. Jestliže byl stav jejího páru částic na počátku $|\Omega\rangle\langle\Omega|$, po aplikaci tento přechází na stav $(\phi\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) = \tau_\phi \equiv \tau$. Bob nedělá se svou částicí ve stavu ρ zhola nic. Stav celého systému tří částic je tak $\tau \otimes \rho$.

2. Ač nerada, pošle Alice svou druhou částici Bobovi. Trpělivý Bob se však na přijatou částici nepodívá. Kdyby to udělal, porušil by kvantové provázání a nedozvěděl by se nic. Jeho stav τ_B by totiž vypadal jako $\tau_B = \mathrm{Tr}_A(\tau_\phi) = \mathrm{Tr}_A((\phi \otimes \mathbb{I})|\Omega\rangle\langle\Omega|) = \frac{1}{d}\mathbb{I}_B$, kde $d = \dim \mathscr{H}_1$ a poslední rovnost vyplývá z faktu, že zobrazení ϕ zachovává stopu. Stav τ_B je tedy maximálně smíšený a nenese tak žádnou informaci.

3. Jako poslední krok provede Bob měření pomocí sady dvou ortogonálních projektorů $P_1 = |\Omega\rangle\langle\Omega|$, $P_2 = \mathbb{I} - |\Omega\rangle\langle\Omega|$. Měření probíhá na obou částicích, které má v tuto chvíli Bob k dispozici, jednu ve stavu ρ a druhou, kterou získal od Alice. Zajímá nás přitom, kdy výsledek měření odpovídá projekci P_1. Po takovém měření se předchozí stav tří částic $\tau \otimes \rho$ změní na stav

$$\rho' = \frac{1}{p'}((\mathbb{I} \otimes |\Omega\rangle\langle\Omega|)(\tau \otimes \rho)(\mathbb{I} \otimes |\Omega\rangle\langle\Omega|)^\dagger), \quad \text{kde} \quad p' = \mathrm{Tr}((\mathbb{I} \otimes |\Omega\rangle\langle\Omega|)(\tau \otimes \rho)) \tag{69}$$

   je pravděpodobnost naměření stavu ρ'. V tuto chvíli má Alice v držení pouze jednu částici, jejíž stav je přitom $\rho_A = \mathrm{Tr}_B(\rho')$. Ale světe div se, tento stav je přitom její vysněný stav $\rho_A = \phi(\rho)$! Tento obdrží s pravděpodobností p'.

Důkaz. Dokažme si výše uvedený vztah $\rho_A = \phi(\rho)$. Z definice stavu podsystému a tvaru stavu ρ' dostáváme pro libovolný operátor M vztahy $\mathrm{Tr}(\rho_A M) = \mathrm{Tr}(\rho' (M \otimes \mathbb{I})) = \frac{1}{p'}\mathrm{Tr}((\mathbb{I} \otimes |\Omega\rangle\langle\Omega|)(\tau\otimes\rho)(\mathbb{I}\otimes|\Omega\rangle\langle\Omega|)(M\otimes I)) = \frac{1}{p'}\mathrm{Tr}((\tau\otimes\rho)(M\otimes|\Omega\rangle\langle\Omega|))$. Platí tedy $p'\,\mathrm{Tr}(\rho_A M) = \mathrm{Tr}((\tau\otimes\rho)(M\otimes|\Omega\rangle\langle\Omega|)) = \frac{1}{d}\mathrm{Tr}((\tau\otimes\rho)(M\otimes(\sum_{\mu\nu}|\mu\rangle\langle\nu|\otimes|\mu\rangle\langle\nu|))) = \frac{1}{d}\sum_{\mu\nu}\mathrm{Tr}(\tau(M\otimes|\mu\rangle\langle\nu|))\,\mathrm{Tr}(\rho|\mu\rangle\langle\nu|)$. Nyní využijeme rovnosti (64) a vztahu $\rho_{\mu\nu} = \mathrm{Tr}(\rho|\mu\rangle\langle\nu|)$ k tomu, abychom upravili poslední výraz do tvaru $\frac{1}{d^2}\sum_{\mu\nu}\mathrm{Tr}(M\phi(|\nu\rangle\langle\mu|))\rho_{\mu\nu} = \frac{1}{d^2}\mathrm{Tr}(M\phi(\rho))$. Pokud položíme $M = \mathbb{I}$ a vzpomeneme si na vzorec pro pravděpodobnost p', tak vidíme, že $p' = \frac{1}{d^2}\mathrm{Tr}(\phi(\rho)) = \frac{1}{d^2}\mathrm{Tr}(\rho) = \frac{1}{d^2}$. Porovnáme-li tak výraz, ze kterého jsme vycházeli, s tím, ke kterému jsme po úpravách dospěli, obdržíme rovnost $\mathrm{Tr}(\rho_A M) = \mathrm{Tr}(M\phi(\rho))$, která musí platit pro všechna M. Tím je vztah $\rho_A = \phi(\rho)$ dokázán. □

Příklad 7.2. *Kvantová teleportace.* Nechť $\phi = \mathbb{I}$, pak výše uvedený postup odpovídá již dříve popsané teleportaci stavů s tím rozdílem, že stav je teleportován od Boba k Alici! Pro případ $d = 2$ dostáváme $|\psi\rangle_{\text{Bob}} = \alpha|0\rangle + \beta|1\rangle$. Alice tedy získá stav $|\psi\rangle_{\text{Bob}}$ s pravděpodobností $1/d^2 = 1/4$.

Příklad 7.3. *Depolarizační kanál.* Nechť $\phi(\rho) = p\,\rho + \frac{1-p}{d}\mathbb{I}$. Je toto zobrazení úplně pozitivní? Platí $\tau_\phi = (\phi\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) = \frac{1}{d}\sum_{\mu\nu}(\phi\otimes\mathbb{I})(|\mu\rangle\langle\nu|\otimes|\mu\rangle\langle\nu|) = \frac{1}{d}\sum_{\mu\nu}(p|\mu\rangle\langle\nu| + (1-p)\mathbb{I}/d)\otimes|\mu\rangle\langle\nu| = p|\Omega\rangle\langle\Omega| + (1-p)\frac{1}{d^2}\mathbb{I}\otimes\sum_{\mu\nu}|\mu\rangle\langle\nu| = p|\Omega\rangle\langle\Omega| + \frac{1-p}{d}\mathbb{I}\otimes|\varphi\rangle\langle\varphi|$, kde $|\varphi\rangle = \frac{1}{\sqrt{d}}\sum_\mu|\mu\rangle$. Poslední výraz je zjevně pozitivní zobrazení a my tak můžeme uzavřít, že depolarizační kanál ϕ je vskutku úplně pozitivní zobrazení.

7.3 Krausova reprezentace

Kvantové operace jsou natolik důležitá zobrazení, že pro ně bylo nalezeno a zavedeno hned několik reprezentací. Tedy způsobů, jak tyto operace zapisovat a vyjadřovat jejich působení na vstupní operátory. My si představíme několik z nich s tím, že jako první si představíme patrně nejrozšířenější reprezentaci, **Krausovu reprezentaci**. Konkrétní vyjádření kvantové operace stejně jako některé její základní vlastnosti jsou shrnuty v následující větě.

Věta 7.3. *Lineární zobrazení $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ je úplně pozitivní právě tehdy, když ho lze pro každý operátor $A \in \mathcal{B}(\mathscr{H}_1)$ zapsat ve tvaru*

$$\phi(A) = \sum_{j=1}^{r} K_j\,A\,K_j^\dagger, \tag{70}$$

*kde K_j jsou tak zvané **Krausovy operátory**. Pro toto zobrazení dále platí následující tvrzení.*

1. *Zobrazení ϕ zachovává stopu právě tehdy, když $\sum_j K_j^\dagger K_j = \mathbb{I} \in \mathcal{B}(\mathscr{H}_1)$.*
2. *Zobrazení ϕ je unitální právě tehdy, když $\sum_j K_j K_j^\dagger = \mathbb{I} \in \mathcal{B}(\mathscr{H}_2)$.*
3. *Nechť r označuje minimální počet Krausových operátorů nutných k reprezentování zobrazení ϕ. Pak platí $r = \operatorname{rank}(\tau_\phi) \leq d_1 \cdot d_2$, kde $d_i = \dim\mathscr{H}_i$.*
4. *Ortogonalita: Pro dané zobrazení ϕ vždy existuje taková Krausova reprezentace, která má r ortogonálních Krausových operátorů, kde r je definováno výše.*
5. *Ekvivalentní reprezentace: Dvě množiny Krausových operátorů $\{K_j\}_{j=1}^m$ a $\{K'_j\}_{j=1}^n$ reprezentují tutéž kvantovou operaci ϕ právě tehdy, když existuje unitární matice U, pro níž $K_j = \sum_l U_{jl} K'_l$. (Pokud $m \neq n$, tak menší množinu operátorů doplníme nulovými operátory.)*

Důkaz. Z dřívějška víme, že ϕ je úplně pozitivní právě, když $\tau = (\phi\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) \geq 0$, kde $\tau \in \mathcal{B}(\mathscr{H}_2\otimes\mathscr{H}_1)$ je nějaký stav. Lze ho tedy zapsat pomocí čistých stavů $|\psi_i\rangle \in \mathscr{H}_2\otimes\mathscr{H}_1$ ve tvaru $\tau = \sum_i|\psi_i\rangle\langle\psi_i| = \sum_i(K_i\otimes\mathbb{I})|\Omega\rangle\langle\Omega|(K_i^\dagger\otimes\mathbb{I}) = (\sum_i K_i\,(\cdot)\,K_i^\dagger\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)$. V druhé rovnosti jsme využili již dokázané existence jistého operátoru K_i takového, že pro daný stav $|\psi_i\rangle$ platí $|\psi_i\rangle = (K_i \otimes \mathbb{I})(|\Omega\rangle)$. Porovnáním výrazů, které jsme právě odvodili, dostáváme žádanou rovnost $\phi = \sum_i K_i\,(\cdot) K_i^\dagger$.

1. Dokažme nyní první bod z výčtu výše. Zobrazení ϕ zachovává stopu právě, když platí $\mathrm{Tr}\,\phi(A) = \mathrm{Tr}\,A \Leftrightarrow (\mathbb{I}, \phi(A)) = (\phi^\dagger(\mathbb{I}), A) = (\mathbb{I}, A) \Leftrightarrow \phi^\dagger(\mathbb{I}) = \mathbb{I}$. Abychom dokončili důkaz prvního bodu, odvoďme si explicitní tvar sdruženého zobrazení $\phi^\dagger$. Obecně platí $(B, \phi(A)) = (\phi^\dagger(B), A)$ neboli $\sum_i \mathrm{Tr}(B^\dagger K_i A K_i^\dagger) = \sum_i \mathrm{Tr}(K_i^\dagger B^\dagger K_i A)$, což lze dále upravit na $\mathrm{Tr}(\sum_i (K_i^\dagger B K_i)^\dagger A) = (\sum_i (K_i^\dagger B K_i), A)$. Porovnáním výrazů tedy obdržíme vztah $\phi^\dagger(A) = \sum_i K_i^\dagger A K_i$. Položíme-li nyní $A = \mathbb{I}$, dostáváme tvrzení prvního bodu. Podobně bychom postupovali při důkazu unitality v bodu druhém.

2. Třetí a čtvrtý bod dokážeme současně. Mějme stav $\tau = \sum_{i=1}^r \alpha_i |\tilde{e}_i\rangle\langle\tilde{e}_i|$, kde $\{|\tilde{e}_i\rangle\}_{i=1}^r$ je ortonormální báze daného Hilbertova prostoru. Označme si $|e_i\rangle = \sqrt{\alpha_i}|\tilde{e}_i\rangle$, potom $\tau = \sum |e_i\rangle\langle e_i|$. Poznamenejme ještě, že počet vektorů r nutných pro rozklad stavu τ je nejmenší, jsou-li $|e_i\rangle$ vlastní vektory. Nejmenší rozklad tedy odpovídá (nenormalizovaným) vlastním stavům k τ, z čehož již plyne $r = \mathrm{rank}(\tau) \leq d_1 \cdot d_2$. Jak je to s ortogonalitou? Pro $i \neq j$ máme $0 = \langle e_i|e_j\rangle = \langle\Omega|(K_i^\dagger \otimes \mathbb{I})(K_j \otimes \mathbb{I})|\Omega\rangle = \sum_{\mu\nu} \frac{1}{d_1}\langle\mu\mu|(K_i^\dagger \otimes \mathbb{I})(K_j \otimes \mathbb{I})|\nu\nu\rangle = \sum_\mu \frac{1}{d_1}\langle\mu|K_i^\dagger K_j|\mu\rangle = \frac{1}{d_1}\mathrm{Tr}(K_i^\dagger K_j) = \frac{1}{d_1}(K_i, K_j)$.

3. Pro důkaz pátého bodu nejdříve ukážeme, že platí tvrzení: Mějme libovolný stav ρ takový, že $\rho = \sum_{j=1}^M |\psi_j\rangle\langle\psi_j|$ a současně $\rho = \sum_{l=1}^N |\psi'_l\rangle\langle\psi'_l|$. Pak nutnou a postačující podmínkou pro takovýto dvojitý zápis je existence unitární matice U takové, že $|\psi_j\rangle = \sum_l U_{jl}|\psi'_l\rangle$. Dokažme si toto lemmátečko. Vezměme ortonormální bázi $\{|j\rangle\}_{j=1}^{\max}$, kde $\max \equiv \max\{M, N\}$, a definujme $|\psi\rangle = \sum_{j=1}^{\max} |\psi_j\rangle|j\rangle$ a $|\psi'\rangle = \sum_{j=1}^{\max} |\psi'_j\rangle|j\rangle$. Oba dva právě zavedené čisté stavy jsou purifikacemi stavu ρ na stejném prostoru. Z toho plyne $\rho = \mathrm{Tr}_2\,|\psi\rangle\langle\psi| = \mathrm{Tr}_2\,|\psi'\rangle\langle\psi'|$. Neboť současně obecně $\rho = \sum_i \lambda_i^2 |e_i\rangle\langle e_i|$, dostáváme $|\psi\rangle = \sum_i \lambda_i |e_i\rangle|f_i\rangle$ a $|\psi'\rangle = \sum_i \lambda_i |e_i\rangle|f'_i\rangle$. Ze Schmidtova rozkladu víme, že existuje unitární transformace U, pro níž $|f_i\rangle = U|f'_i\rangle$, $U = \sum_{jl} U_{jl}|j\rangle\langle l|$. Z toho již $|\psi\rangle = (\mathbb{I} \otimes U)|\psi'\rangle$. Dosadíme-li tento výraz zpět, dospíváme ke vztahům $\sum_j |\psi_j\rangle|j\rangle = (\mathbb{I} \otimes U)\sum_k |\psi'_k\rangle|k\rangle = \sum_k |\psi'_k\rangle \sum_{jl} U_{jl}|j\rangle\langle l||k\rangle = \sum_{jk} |\psi'_k\rangle U_{jk}|j\rangle = \sum_j (\sum_k U_{jk}|\psi'_k\rangle)|j\rangle$. Porovnáním tedy máme $|\psi_j\rangle = \sum_k U_{jk}|\psi'_k\rangle$. Tímto jsme dokázali lemmátečko. Aplikujme nyní toto dokázané tvrzení na pátý bod věty. Stav $|\psi_j\rangle = (K_j \otimes \mathbb{I})|\Omega\rangle$ je izomorfně sdružený se zobrazením $\frac{1}{\sqrt{d_1}}K_j$ a podobně stav $|\psi'_k\rangle = (K'_k \otimes \mathbb{I})|\Omega\rangle$ je přitom izomorfně sdružený se zobrazením $\frac{1}{\sqrt{d_1}}K'_k$. Zapůsobíme-li izomorfizmem na rovnost $(K_j \otimes \mathbb{I})|\Omega\rangle = \sum_{jk} U_{jk}(K'_k \otimes \mathbb{I})|\Omega\rangle$, dostáváme ihned $K_j = \sum_k U_{jk}K'_k$. Tím je důkaz věty dokončen.

□

Definice 7.3. Číslo r z třetího bodu výše uvedené věty nazveme **Krausova hodnost** (angl. *Kraus rank*) zobrazení ϕ.

Inu dobrá, již víme, co to je Krausova reprezentace, jak ji ale pro konkrétní zobrazení ϕ najít? Lze postupovat například následujícím postupem. Vyjděme z Jamiolkowského stavu

τ_ϕ, ten si rozložme do vlastní báze a na bazické vektory aplikujme izomorfizmus. Konkrétně $\tau_\phi = (\phi \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) = \sum_i |\psi_i\rangle\langle\psi_i| = \frac{1}{\sqrt{d_1}} X_\phi = \frac{1}{\sqrt{d_1}}(\sum_i |\varphi_i\rangle\langle\varphi_i|)$. Z předchozích úvah v důkazu tedy $|\psi_i\rangle = (K_i \otimes \mathbb{I})|\Omega\rangle \in \mathscr{H}_2 \otimes \mathscr{H}_1$. Tento stav je izomorfně sdružen s jistým operátorem $\Psi_i \in \mathcal{B}(\mathscr{H}_1, \mathscr{H}_2)$. Platí tedy $\Psi_i = \frac{1}{\sqrt{d_1}} K_i$ a tak $K_i = \sqrt{d_1}\Psi_i = \Phi_i$.

Příklad 7.4. *"No-go theorem" pro NOT operaci.* Existuje taková kvantová operace, aby prováděla transponování $|\varphi\rangle \to |\varphi^T\rangle \equiv |\varphi\rangle^T$? Kdyby taková operace, jíž si označíme ε, existovala, tak by muselo platit $\varepsilon(|\varphi\rangle\langle\varphi|) = \sum_j K_j(|\varphi\rangle\langle\varphi|)K_j^\dagger = |\varphi^T\rangle\langle\varphi^T|$ pro libovolné $|\varphi\rangle$. Pak tedy $0 = \langle\varphi|(\varepsilon(|\varphi\rangle\langle\varphi|))|\varphi\rangle = \sum_j \langle\varphi|K_j|\varphi\rangle\langle\varphi|K_j^\dagger|\varphi\rangle = \sum_j |\langle\varphi|K_j|\varphi\rangle|^2$, z čehož plyne $\langle\varphi|K_j|\varphi\rangle = 0$ pro všechna $|\varphi\rangle$. Položíme-li nyní $|\varphi\rangle = \alpha|\varphi_1\rangle + \beta|\varphi_2\rangle$, posledně jmenovaný nulový výraz zní $|\alpha|^2\langle\varphi_1|K_j|\varphi_1\rangle + |\beta|^2\langle\varphi_2|K_j|\varphi_2\rangle + \alpha^\star\beta\langle\varphi_1|K_j|\varphi_2\rangle + \alpha\beta^\star\langle\varphi_2|K_j|\varphi_1\rangle$. První dva sčítance jsou zjevně nulové. Když dosadíme $\alpha = 1 = \beta$ přejde předchozí výraz do tvaru $\langle\varphi_1|K_j|\varphi_2\rangle + \langle\varphi_2|K_j|\varphi_1\rangle = 0$. Pokud položíme $\alpha = \mathrm{i} = \beta$, obdržíme $-\mathrm{i}\langle\varphi_1|K_j|\varphi_2\rangle + \mathrm{i}\langle\varphi_2|K_j|\varphi_1\rangle = 0$. Z těchto dvou rovností již plyne $\langle\varphi_2|K_j|\varphi_1\rangle = 0$ a tedy $K_j = 0$ pro všechna j. Taková operace ε tedy neexistuje.

Příklad 7.5. *Depolarizační kanál podruhé.* Na příkladu depolarizačního kanálu si názorně ukažme některé jeho Krausovy reprezentace. Pro obecný operátor A je depolarizační kanál definovaný vzorcem

$$\phi(A) = p \cdot A + \operatorname{Tr} A \cdot \frac{1-p}{d} \cdot \mathbb{I}. \tag{71}$$

Jeho působení v prostoru dimenze dvě, $d = 2$, lze ilustrovat na Blochově sféře jako její „scvrknutí“. Aby mělo hledání Krausových operátorů vůbec smysl, je nutné, v souladu s větou 7.3, ukázat, že je depolarizační kanál ϕ úplně pozitivní zobrazení. To ale vskutku je, neboť $\tau_\phi = (\phi \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) = \frac{1}{d}\sum_{\mu\nu}(\phi \otimes \mathbb{I})|\mu\mu\rangle\langle\nu\nu| = \frac{1}{d}\sum_{\mu\nu}\phi(|\mu\rangle\langle\nu|) \otimes |\mu\rangle\langle\nu| = \frac{1}{d}\sum_{\mu\nu}(p|\mu\rangle\langle\nu| + \frac{1-p}{d}\mathbb{I}\operatorname{Tr}(|\mu\rangle\langle\nu|)) \otimes |\mu\rangle\langle\nu| = p|\Omega\rangle\langle\Omega| + \frac{1-p}{d^2}\mathbb{I} \otimes \mathbb{I}$, což je zjevně pozitivní operátor.

V případě dvourozměrného prostoru $d = 2$ můžeme Krausovu reprezentaci depolarizačního kanálu volit takto:

$$\begin{array}{rclrcl} |\psi_0\rangle & = & \sqrt{p}|\Omega\rangle, & & & \\ |\psi_1\rangle & = & \frac{\sqrt{1-p}}{d}|00\rangle, & |\psi_2\rangle & = & \frac{\sqrt{1-p}}{d}|01\rangle, \\ |\psi_3\rangle & = & \frac{\sqrt{1-p}}{d}|10\rangle, & |\psi_4\rangle & = & \frac{\sqrt{1-p}}{d}|11\rangle. \end{array} \tag{72}$$

Odpovídající Krausovy operátory pak vypadají následovně:

$$\begin{array}{rclrcl} K_0 & = & \sqrt{p}\,\mathbb{I}, & & & \\ K_1 & = & \sqrt{\frac{1-p}{d}}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & K_2 & = & \sqrt{\frac{1-p}{d}}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \\ K_3 & = & \sqrt{\frac{1-p}{d}}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, & K_4 & = & \sqrt{\frac{1-p}{d}}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \end{array} \tag{73}$$

Lze ale brát i jiné rozklady jako třeba $|\Omega_0\rangle = |\Omega\rangle$, $|\Omega_i\rangle = (\sigma_i \otimes \mathbb{I})|\Omega\rangle$, kde σ_i jsou Pauliho matice. Z konstrukce jsou všechny $\{|\Omega_i\rangle\}_{i=0}^3$ maximálně provázané stavy, které jsou navzájem kolmé. Platí pak $\tau_\phi = p|\Omega_0\rangle\langle\Omega_0| + \frac{1-p}{4}\sum_{i=0}^4 |\Omega_i\rangle\langle\Omega_i| = \frac{1+3p}{4}|\Omega_0\rangle\langle\Omega_0| + \frac{1-p}{4}\sum_{i=1}^4 |\Omega_i\rangle\langle\Omega_i|$. Navíc z tvaru $|\Omega_i\rangle$ plyne $K_0 = \frac{\sqrt{1+3p}}{2}\mathbb{I}$, $K_i = \frac{\sqrt{1-p}}{2}\sigma_i$.

Definice 7.4. Jedním ze speciálních příkladů kvantové operace je zobrazení nazvané **náhodná unitární operace** (angl. *random unitary operation*). V jejím případě mají Krausovy operátory tvar $K_i = \sqrt{p_i}\,U_i$, kde U_i je nějaké unitární zobrazení a p_i je pravděpodobnostní rozdělení. Celkově tedy

$$\phi(A) = \sum_{i=1}^{n} p_i U_i\, A\, U_i^\dagger, \tag{74}$$

kde $p_i \geq 0$ pro všechny $i \in \{1, \dots, n\}$ a navíc $\sum_i p_i = 1$. Náhodnou unitární operaci lze chápat jako vážený průměr různých unitárních vývojů systému.

Pro uzavřený vývoj systému ve stavu ρ platí, že po určitém čase se tento systém bude nacházet ve stavu $U\rho U^\dagger$, kde U je odpovídající evoluční operátor. V otevřeném vývoji už toto však neplatí. Na náhodnou unitární operaci tak lze nahlížet jako na zobecnění uzavřeného unitárního vývoje, neboť při volbě $n = 1$ dostáváme z této operace opět uzavřený vývoj. Před představením další reprezentace si ještě uveďme následující větu, kterou nebudeme dokazovat.

Věta 7.4. *Pro $d = 2$ platí, že každý kanál ϕ lze zapsat jako náhodně unitární operaci.*

7.4 Stinespringova reprezentace

Jak již bylo řečeno, kromě Krausovy reprezentace kvantových operací existují i další způsoby jejího vyjádření. Jedním z nich je Stinespringova reprezentace, kterou si představíme v následující větě.

Věta 7.5. Stinespringova reprezentace v Heisenbergově obraze. *Nechť $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ je úplně pozitivní zobrazení. Potom pro všechna čísla $r \geq \operatorname{rank}(\tau)$ existuje zobrazení V takové, že $V : \mathscr{H}_1 \to \mathbb{C}^r \otimes \mathscr{H}_2$ a platí*

$$\phi^\dagger(A) = V^\dagger(\mathbb{I}_{\mathbb{C}^r} \otimes A)V, \tag{75}$$

kde V je izometrií právě tehdy, když ϕ zachovává stopu.

Důkaz. Vyjděme z Krausovy reprezentace zobrazení ϕ: $\phi(A) = \sum_{j=1}^r K_j A K_j^\dagger$ a tedy $\phi^\dagger(A) = \sum_{j=1}^r K_j^\dagger A K_j$, $K_j : \mathscr{H}_1 \to \mathscr{H}_2$. Definujme $V = \sum_{j=1}^r |j\rangle \otimes K_j$, kde $\{|j\rangle\}_{j=1}^r$ je ortonormální báze prostoru $\mathbb{C}^r$, tj. $V|\varphi\rangle = \sum_{j=1}^r |j\rangle \otimes K_j|\varphi\rangle$. Potom $\phi^\dagger(A) = \sum_{j=1}^r (\langle j| \otimes K_j^\dagger)(\mathbb{I} \otimes A)(\sum_{l=1}^r |l\rangle \otimes K_l) = V^\dagger(\mathbb{I} \otimes A)V$. Navíc ϕ zachovává stopu právě tehdy, když $\sum_{j=1}^r K_j^\dagger K_j = \mathbb{I}$, což je ekvivalentní s podmínkou $V^\dagger V = \mathbb{I}_{\mathscr{H}_1}$. □

Poznámka 7.2. Když V je izometrie, tak ji lze přidáním vhodné ancilly rozšířit na unitární operátor. Pro pomocný prostor $\mathbb{C}^r$ se v angličtině používá pojem *dilation space*. Věta výše platí i pro zobrazení ϕ samotné, pak $V : \mathscr{H}_2 \to \mathbb{C}^r \otimes \mathscr{H}_1$. Hlavní důvod pro používání jeho sdružení $\phi^\dagger$ je snazší dokazování, že dané ϕ zachovává stopu. Nakonec si ještě osvětleme, proč je v předchozí větě zmínka o Heisenbergově obrazu. Pro libovolnou pozorovatelnou A máme $\langle A\rangle_{\rho(t)} = \operatorname{Tr}(A\,\rho(t)) = \operatorname{Tr}(A\,\phi_t(\rho(0))) = (A^\dagger, \phi_t(\rho(0))) = (\phi_t^\dagger(A^\dagger), \rho(0)) = \operatorname{Tr}(\phi_t^\dagger(A)\rho(0)) = \langle A(t)\rangle_{\rho(0)}$, kde jsme v poslední rovnosti definovali $A(t) = \phi_t^\dagger(A)$. Operace ϕ je tedy schopna popsat časový vývoj pozorovatelných v Heisenbergově obraze.

Poznámka 7.3. *Částečné uspořádání úplně pozitivních zobrazení.* Na množině úplně pozitivních zobrazení lze zavést částečné uspořádání následujícím způsobem. Mějme dvě taková zobrazení ϕ_i a jim odpovídající $\tau_i = (\phi_i \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|)$, pak definujeme

$$\phi_1 \geq \phi_2 \quad \Leftrightarrow \quad \tau_2 \geq \tau_1. \tag{76}$$

Operátory τ_i odpovídající úplně pozitivním ϕ_i jsou samy pozitivní a je na nich tak přirozeně zavedeno uspořádání. Výraz výše má tedy smysl. V souvislosti s částečným uspořádáním úplně pozitivních zobrazení si dokažme následující větu.

Věta 7.6. *Nechť $\phi_i : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ jsou dvě úplně pozitivní zobrazení taková, že $\phi_2 \geq \phi_1$. Nechť dále $V_i : \mathscr{H}_2 \to \mathbb{C}^{r_i} \otimes \mathscr{H}_1$ jsou jejich Stinespringovy reprezentace (ve Schrödingerově obraze). Potom existuje kontrakce $C : \mathbb{C}^{r_2} \to \mathbb{C}^{r_1}$ taková, že $V_1 = (C \otimes \mathbb{I}_{\mathscr{H}_1})V_2$. Pod kontrakcí přitom chápeme zobrazení C splňující $C^\dagger C \leq \mathbb{I}$, tj. $\|C\| \leq 1$.*

Důkaz. Definujme si zobrazení $W_i = (\mathbb{I}_{\mathbb{C}_{r_i}} \otimes \langle\Omega|)(V_i \otimes \mathbb{I}_{\mathscr{H}_1})$, $W_i \in \mathcal{B}(\mathscr{H}_2 \otimes \mathscr{H}_1, \mathbb{C}^{r_i})$. Pro ně platí

$$\begin{aligned}
W_i^\dagger W_i &= (V_i^\dagger \otimes \mathbb{I}_{\mathscr{H}_1})(\mathbb{I}_{\mathbb{C}_{r_i}} \otimes |\Omega\rangle)(\mathbb{I}_{\mathbb{C}_{r_i}} \otimes \langle\Omega|)(V_i \otimes \mathbb{I}_{\mathscr{H}_1}) \;=\; (V_i^\dagger \otimes \mathbb{I})(\mathbb{I} \otimes |\Omega\rangle\langle\Omega|)(V_i \otimes \mathbb{I}) \\
&= \frac{1}{d}\sum_{\mu\nu}(V_i^\dagger \otimes \mathbb{I})(\mathbb{I} \otimes |\mu\rangle\langle\nu| \otimes |\mu\rangle\langle\nu|)(V_i \otimes \mathbb{I}) \;=\; \frac{1}{d}\sum_{\mu\nu}(V_i^\dagger(\mathbb{I} \otimes |\mu\rangle\langle\nu|)V_i) \otimes |\mu\rangle\langle\nu| \\
&= \frac{1}{d}\sum_{\mu\nu}\phi_i(|\mu\rangle\langle\nu|) \otimes |\mu\rangle\langle\nu| \;=\; \frac{1}{d}(\phi_i \otimes \mathbb{I})\Big(\sum_{\mu\nu}|\mu\mu\rangle\langle\nu\nu|\Big) \;=\; \frac{1}{d}(\phi_i \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) \\
&= \tau_i,
\end{aligned}$$

kde $d = \dim \mathscr{H}_1$. Tento výsledek implikuje, že normy zobrazení W_1 splňují jednoduchou nerovnost $\|W_1|\varphi\rangle\|^2 = \langle\varphi|W_1^\dagger W_1|\varphi\rangle = \langle\varphi|\tau_1|\varphi\rangle \leq \langle\varphi|\tau_2|\varphi\rangle = \|W_2|\varphi\rangle\|^2$. Následkem tohoto platí $\operatorname{Ker} W_2 \subset \operatorname{Ker} W_1$ a tedy $\operatorname{Ran} W_1 \subset \operatorname{Ran} W_2$. Z toho plyne, že existuje lineární zobrazení $C : \mathbb{C}^{r_2} \to \mathbb{C}^{r_1}$, pro nějž $W_1 = C W_2$. Z již dokázané nerovnosti norem máme $W_1^\dagger W_1 \leq W_2^\dagger W_2$, neboli $W_2^\dagger C^\dagger C W_2 \leq W_2^\dagger W_2$. Úpravou získáváme $W_2^\dagger(\mathbb{I} - C^\dagger C)W_2 \geq 0$ a C je tak kontrakce, $\mathbb{I} - C^\dagger C \geq 0$. Ukažme ještě, že vztah zobrazení V_i a W_i je jednoznačný. Platí

$$\begin{aligned}
d(W_i \otimes \mathbb{I})(\mathbb{I} \otimes |\Omega\rangle) &= d((\mathbb{I} \otimes \langle\Omega|)(V_i \otimes \mathbb{I}) \otimes \mathbb{I})(\mathbb{I} \otimes |\Omega\rangle) && (77)\\
&= \sum_{\mu\nu}((\mathbb{I} \otimes \langle\mu| \otimes \langle\mu|)(V_i \otimes \mathbb{I}) \otimes \mathbb{I})(\mathbb{I} \otimes |\nu\rangle \otimes |\nu\rangle) && (78)\\
&= \sum_{\mu\nu}((\mathbb{I} \otimes \langle\mu|)V_i) \otimes |\nu\rangle\langle\mu|\nu\rangle && (79)\\
&= \sum_{\mu}((\mathbb{I} \otimes \langle\mu|)V_i) \otimes |\mu\rangle. && (80)
\end{aligned}$$

Připomeňme si nyní vztah $V_i = \sum_{j\nu n} V^{(i)}_{j\nu,n}|j\nu\rangle\langle n|$. Dosadíme-li tento do posledního výrazu našeho výpočtu, obdržíme rovnosti $\sum_\mu(\mathbb{I} \otimes \langle\mu|)V_i \otimes |\mu\rangle = \sum_\mu \sum_{j\nu n} V^{(i)}_{j\nu,n}|j\rangle\langle\mu|\nu\rangle\langle n| \otimes |\mu\rangle = \sum_{\mu jn} V^{(i)}_{j\mu,n}|j\rangle\langle n| \otimes |\mu\rangle = \sum_{\mu jn} V^{(i)}_{j\mu,n}|j\mu\rangle\langle n| = V_i$. Celkově tedy $V_1 = d(W_1 \otimes \mathbb{I}_{\mathscr{H}_1})(\mathbb{I}_{\mathscr{H}_2} \otimes |\Omega\rangle) = d(CW_2 \otimes \mathbb{I}_{\mathscr{H}_1})(\mathbb{I}_{\mathscr{H}_2} \otimes |\Omega\rangle) = (C \otimes \mathbb{I}_{\mathscr{H}_1})V_2$. □

Stinespringovu reprezentaci lze rozšířit i na případ kvantových instrumentů. Společně se Stinespringovou reprezentací lze kvantovou operaci zapisovat v podobném tvaru k (75), kde však navíc využijeme částečné stopy. Blíže se těmto otázkám věnují následující dvě tvrzení.

Věta 7.7. Radonova-Nikodymova reprezentace kvantových instrumentů. *Nechť* $\{\phi_i\}_i$ *je množina úplně pozitivních zobrazení* $\phi_i : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ *takových, že* $\sum_i \phi_i = \phi$*. Nechť Stinespringova reprezentace zobrazení* ϕ *je* $V : \mathscr{H}_2 \to \mathbb{C}^r \otimes \mathscr{H}_1$*, tj.* $\phi(A) = V^\dagger(\mathbb{I}_{\mathbb{C}^r} \otimes A)V$*. Potom existuje množina pozitivních operátorů* $Q_i \in \mathcal{B}(\mathbb{C}^r)$ *takových, že* $\sum_i Q_i = \mathbb{I}_{\mathbb{C}^r}$ *a současně* $\phi_i(A) = V^\dagger(Q_i \otimes A)V$*.*

Důkaz. Určitě platí $\phi_i \leq \phi$. Z předchozí věty tedy existují kontrakce C_i a zobrazení V_i splňující $V_i = (C_i \otimes \mathbb{I}_{\mathscr{H}_1})V$ a $\phi_i(A) = V_i^\dagger(\mathbb{I}_{\mathbb{C}^{r_i}} \otimes A)V_i$. Celkem tedy $\phi_i(A) = V^\dagger(C_i^\dagger \otimes \mathbb{I}_{\mathscr{H}_1})(\mathbb{I}_{\mathbb{C}^{r_i}} \otimes A)(C_i \otimes \mathbb{I}_{\mathscr{H}_1})V = V^\dagger(C_i^\dagger C_i \otimes A)V$. Zobrazení $Q_i \coloneqq C_i^\dagger C_i$ jsou zjevně pozitivní a díky vlastnosti $\sum_i \phi_i = \phi$ splňují rovnost $\sum_i Q_i = \mathbb{I}$. □

Věta 7.8. *Nechť* $\phi : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ *je úplně pozitivní zobrazení zachovávající stopu. Potom existuje unitární zobrazení* $U : \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \mathscr{H}_2 \to \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \mathscr{H}_2$ *a normalizovaný čistý stav* $|\varphi\rangle \in \mathscr{H}_2 \otimes \mathscr{H}_2$ *tak, že*

$$\phi(\rho) = \mathrm{Tr}_{\mathscr{H}_1 \otimes \mathscr{H}_2}\left(U(\rho \otimes |\varphi\rangle\langle\varphi|)U^\dagger\right). \tag{81}$$

Způsobu, jakým lze zobrazení ϕ zapsat v právě uvedené větě, se anglicky říká *open-system representation.* Ukažme si nyní její důkaz.

Důkaz. Věta 7.5 nám zaručuje existenci izometrie $V : \mathscr{H}_1 \to \mathbb{C}^r \otimes \mathscr{H}_2$ takové, že $\phi^\dagger(A) = V^\dagger(\mathbb{I}_{\mathbb{C}^r} \otimes A)V$ a $r \geq \mathrm{rank}(\tau)$. Zvolme si $\mathbb{C}^r \coloneqq \mathscr{H}_1 \otimes \mathscr{H}_2$ a ptejme se, jak vypadá v této reprezentaci zobrazení $\phi(\rho)$. Pro každou pozorovatelnou A dostáváme rovnosti $\mathrm{Tr}_{(\mathscr{H}_2)}(A\phi(\rho)) = \mathrm{Tr}_{(\mathscr{H}_1)}(\phi^\dagger(A)\,\rho) = \mathrm{Tr}_{(\mathscr{H}_1)}(V^\dagger(\mathbb{I}_{\mathscr{H}_1 \otimes \mathscr{H}_2} \otimes A)V\,\rho) = \mathrm{Tr}_{(\mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \mathscr{H}_2)}((\mathbb{I}_{\mathscr{H}_1 \otimes \mathscr{H}_2} \otimes A)V\,\rho\,V^\dagger)$. Pokud u stop vyznačujeme prostor, přes který se stopuje, v závorkách, znamená to, že se nejedná o částečnou stopu, ale pouze explicitně uvádíme, na jakém prostoru je stopa prováděna. Poslední výraz je přitom roven $\mathrm{Tr}_{(\mathscr{H}_2)}(A\,\mathrm{Tr}_{\mathscr{H}_1 \otimes \mathscr{H}_2}(V\rho V^\dagger))$. Předchozí úpravy jsme prováděli pro libovolnou pozorovatelnou $A = A^\dagger$, není těžké nahlédnout, že však musí platit i pro nehermitovské operátory. Dostáváme tak celkem $\phi(\rho) = \mathrm{Tr}_{\mathscr{H}_1 \otimes \mathscr{H}_2}(V\rho V^\dagger)$. Zmíněné zobrazení $V = \sum_{\mu m n \nu} V_{\mu mn,\nu}|\mu mn\rangle\langle\nu|$ je obecně izomorfie, dodefinujme ho na unitární operátor U. To lze vždy. Položme $|\varphi\rangle = |11\rangle$. Operátor U definujme tak, aby platil vztah

$$\langle\mu mn|U|\nu\rangle|\varphi\rangle \equiv \langle\mu mn|U|\nu 11\rangle = V_{\mu mn,\nu}. \tag{82}$$

Maticově to neznamená nic jiného, než že matici U vytvoříme z matice V tím, že připojíme zprava vhodný blok W tak, aby U bylo unitární. Matice V tak tvoří první blok v matici U, který odpovídá bazickým vektorům $\{|1\rangle|11\rangle, \ldots, |\dim\mathscr{H}_1\rangle|11\rangle\}$. Blok W tedy odpovídá zbývajícím bazickým vektorům $|1\rangle|12\rangle, \ldots, |\dim\mathscr{H}_1\rangle|12\rangle, |1\rangle|13\rangle, \ldots, |\dim\mathscr{H}_1\rangle|13\rangle$ a tak dále, až $|1\rangle|\dim\mathscr{H}_2 \dim\mathscr{H}_2\rangle, \ldots, |\dim\mathscr{H}_1\rangle|\dim\mathscr{H}_2 \dim\mathscr{H}_2\rangle$. Neboli

$$U = \left(\begin{array}{|c|c|}\hline V & \quad W \quad \\ \hline\end{array}\right). \tag{83}$$

Ze vzorce (82) plyne $V = U(\mathbb{I}_{\mathscr{H}_1} \otimes |\varphi\rangle)$. Tudíž $\phi(\rho) = \mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}(U(\mathbb{I} \otimes |\varphi\rangle)\rho(\mathbb{I} \otimes \langle\varphi|)U^\dagger) = \mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}(U(\rho \otimes |\varphi\rangle\langle\varphi|)U^\dagger)$. □

Poznámka 7.4. V předchozí větě stopujeme přes množinu $\mathscr{H}_1 \otimes \mathscr{H}_2$ obsahující původní prostor $\mathscr{H}_1$, na němž jsou definovány operátory tvořící vstupy do zobrazení ϕ. Co, když $\mathscr{H}_1 = \mathscr{H}_2 = \mathscr{H}$, tj. $\phi : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$? Lze vzorec v tvrzení výše uvedené věty zjednodušit? Mějme unitární zobrazení $U_1 : \mathscr{H}^{\otimes 3} \to \mathscr{H}^{\otimes 3}$, které provádí transpozici $|mno\rangle \to |nom\rangle$ v lokální bázi $\{|m\rangle\}_m$ prostoru $\mathscr{H}$. Pak dostáváme

$$\phi(\rho) = \mathrm{Tr}_{\mathscr{H}\otimes\mathscr{H}}\left(UU_1(\rho \otimes |\varphi\rangle\langle\varphi|)U_1{}^\dagger U^\dagger\right). \tag{84}$$

Hlavním rozdílem oproti předchozí větě je to, že nyní již stopujeme pouze přes prostředí, které jsme si na počátku uměle přidali. Tento zápis je tedy názornější: vezmi vstupní stav ρ, k němu něco přidej (stav $|\varphi\rangle\langle\varphi|$), tento celek nech unitárně vyvíjet (podle operátoru UU_1) a na konci vývoje se podívej na svůj původní prostor $\mathscr{H}$ tím, že vystopuješ přes prostředí, které jsi si na počátku zavedl přidání stavu $|\varphi\rangle\langle\varphi|$.

V otevřené dynamice je největším problémem provázanost zkoumaného systému s prostředím. Vývoj zkoumaného systému lze tak studovat způsobem, že si k němu dočasně připojíme prostředí, celek necháme unitárně vyvíjet (zkoumaný systém spolu s prostředím již tvoří uzavřený systém) a na konci vývoje se podíváme jen na tu část výsledného stavu, která odpovídá zkoumanému systému. Tento postup přesně odpovídá postupu popsanému v předchozím odstavci, kde jsme slovně osvětlovali význam vzorce (84). Proto se tomuto vzorci a jeho obecnější variantě (81) říká právě open-system representation.

Věta 7.9. Implementace kvantových instrumentů pomocí POVM. *Nechť $\phi_i : \mathcal{B}(\mathscr{H}_1) \to \mathcal{B}(\mathscr{H}_2)$ jsou úplně pozitivní zobrazení, pro něž $\sum_i \phi_i = \phi$, kde ϕ přitom zachovává stopu. Pak existuje POVM $\{Q_i : \mathscr{H}_1 \otimes \mathscr{H}_2 \to \mathscr{H}_1 \otimes \mathscr{H}_2\}_i$ tak, že platí*

$$\phi_i(\rho) = \mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}\left((Q_i \otimes \mathbb{I}_{\mathscr{H}_2})U(\rho \otimes |\varphi\rangle\langle\varphi|)U^\dagger\right). \tag{85}$$

Důkaz. S využitím věty (7.7) víme, že najdeme Q_i a V tak, aby $\phi_i^\dagger(A) = V^\dagger(Q_i \otimes A)V$, $V : \mathscr{H}_1 \to \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes \mathscr{H}_2$, kde přitom $V^\dagger V = \mathbb{I}_{\mathscr{H}_1}$. Pak $\mathrm{Tr}_{(\mathscr{H}_2)}(A\,\phi_i(\rho)) = \mathrm{Tr}_{(\mathscr{H}_1)}(\phi_i^\dagger(A)\,\rho) = \mathrm{Tr}_{(\mathscr{H}_1)}(V^\dagger(Q_i \otimes A)V\,\rho) = \mathrm{Tr}_{(\mathscr{H}_1\otimes\mathscr{H}_2\otimes\mathscr{H}_2)}((Q_i \otimes A)V\rho V^\dagger) = \mathrm{Tr}_{(\mathscr{H}_1\otimes\mathscr{H}_2\otimes\mathscr{H}_2)}((\mathbb{I}\otimes A)(Q_i\otimes\mathbb{I})V\rho V^\dagger)$, kde opět v závorkách vyznačujeme prostor, přes který se stopuje. Pokud u stopy žádná závorka není, jedná o částečnou stopu. Poslední výraz je roven $\mathrm{Tr}_{(\mathscr{H}_2)}(A\,\mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}((Q_i \otimes \mathbb{I})V\,\rho\,V^\dagger))$. Porovnáním prvního a posledního členu v rovnostech výše pro zobrazení $\phi_i(\rho)$ dostáváme $\phi_i(\rho) = \mathrm{Tr}_{\mathscr{H}_1\otimes\mathscr{H}_2}((Q_i \otimes \mathbb{I}_{\mathscr{H}_2})V\,\rho\,V^\dagger)$. Analogicky postupu v předchozí větě bychom doplnili izometrii V na unitární operátor U a nalezli čistý stav $|\varphi\rangle$ tak, abychom obdrželi vzorec v tvrzení této věty. □

7.5 Neumarkova reprezentace

Jako poslední reprezentaci si uveďme tu Neumarkovu. Zde se budeme zabývat POVM měřeními, tedy měřeními, kde nás nezajímají výsledné stavy systému, ale pouze pravděpodobnosti, se kterými danou hodnotu pozorovatelné naměříme. Blíže viz následující věta.

Věta 7.10. *Každé POVM měření lze realizovat jako von Neumannovo měření na větším Hilbertově prostoru. Konkrétně mějme sadu POVM operátorů* $\{F_i\}_{i=1}^m$, $F_i \geq 0$, $\sum_i F_i = \mathbb{I}$, *působících na prostoru* $\mathscr{H}$. *Pak měření popsané touto sadou lze realizovat i pomocí sady* $\{\Pi_i\}_{i=1}^m$, *kde* $\Pi_i : \mathscr{H} \otimes \mathbb{C}^{M-d} \to \mathscr{H} \otimes \mathbb{C}^{M-d}$ *jsou ortogonální projektory, přičemž* $d = \dim \mathscr{H}$ *a* $M = \sum_{i=1}^m \operatorname{rank} F_i$. *Pravděpodobnosti naměření jednotlivých hodnot jsou pak rovny*

$$p_i \equiv \operatorname{Tr}_{(\mathscr{H})}(F_i\,\rho) = \operatorname{Tr}_{(\mathscr{H}\otimes C^{M-d})}(\Pi_i(\rho \oplus 0)). \tag{86}$$

Důkaz. Uvažujme nejprve případ, kdy $\operatorname{rank} F_i = 1$, $\forall i \in \{1, \ldots, m\}$. Operátory F_i jsou tedy projektory $F_i = |\psi_i\rangle\langle\psi_i|$, které nemusejí být ortogonální. Platí tedy, že lineární obal vektorů $|\psi_i\rangle$ tvoří celý prostor $\mathscr{H}$, jehož dimenze je d, tj. $\operatorname{span}_i\{|\psi_i\rangle\} = \mathscr{H}$, $\dim \mathscr{H} = d$. Nechť $\{|j\rangle\}_{j=1}^d$ je jeho ortonormální báze. Tu doplňme na ortonormální bázi prostoru $\mathscr{H} \oplus \mathbb{C}^{m-d}$, $\{|j\rangle\}_{j=1}^m$. (V právě uvažovaném případě je $M = m$.) Dále definujme zobrazení $Z = \sum_{i=1}^m \sum_{j=1}^d \langle j|\psi_i\rangle |i\rangle\langle j|$, jehož sdružení zní $Z^\dagger = \sum_{i=1}^m \sum_{j=1}^d \langle j|\psi_i\rangle^* |j\rangle\langle i|$. Pak

$$\begin{aligned} Z^\dagger Z &= \sum_{i,l=1}^m \sum_{j,k=1}^d \langle j|\psi_i\rangle^* \langle k|\psi_l\rangle |j\rangle\langle i||l\rangle\langle k| = \sum_{i=1}^m \sum_{j,k=1}^d \langle \psi_i|j\rangle\langle k|\psi_i\rangle |j\rangle\langle k| & (87)\\ &= \sum_{j,k=1}^d \langle k| \left(\sum_{i=1}^m |\psi_i\rangle\langle\psi_i|\right) |j\rangle |j\rangle\langle k| = \sum_{j,k=1}^d \langle k| \left(\sum_{i=1}^m F_i\right) |j\rangle |j\rangle\langle k| & (88)\\ &= \sum_{j,k=1}^d \langle k||j\rangle |j\rangle\langle k| = \sum_{j=1}^d |j\rangle\langle j| = \mathbb{I}. & (89) \end{aligned}$$

Platí tedy, že Z je izometrie. Porovnáním obecného tvaru zobrazení $Z = \sum_{ij} Z_{ij}|i\rangle\langle j|$ s tím, jak jsme si ho definovali, vidíme, že $V_{ij} = \langle j|\psi_i\rangle$. Podobně jako v předchozích větách můžeme k matici (V_{ij}), která je rozměrů $m \times d$, připojit vhodný blok tak, aby vzniklá matice (U_{ij}) byla unitární, rozměrů $m \times m$, viz (83). Existují tak vektory $|\psi_i^\perp\rangle \in \mathbb{C}^{m-d}$ takové, že pro vektory $|\varphi_i\rangle = |\psi_i\rangle + |\psi_i^\perp\rangle \in \mathscr{H} \oplus \mathbb{C}^{m-d}$ platí $U_{ij} = \langle j|\varphi_i\rangle$, $i, j \in \{1, \ldots, m\}$. Speciálně pak $V_{ij} = \langle j|\varphi_i\rangle$, $i \in \{1, \ldots, m\}$, $j \in \{1, \ldots, d\}$. Definujme si nyní $\Pi_i = |\varphi_i\rangle\langle\varphi_i|$. Pro tyto operátory platí $\operatorname{Tr}_{(\mathscr{H}\oplus\mathbb{C}^{m-d})}(\Pi_i(\rho \oplus 0)) = \operatorname{Tr}_{(\mathscr{H}\oplus\mathbb{C}^{m-d})}(|\varphi_i\rangle\langle\varphi_i|(\rho \oplus 0)) = \langle\varphi_i|\rho \oplus 0|\varphi_i\rangle = \langle\psi_i|\rho|\psi_i\rangle + \langle\psi_i^\perp|0|\psi_i^\perp\rangle = \langle\psi_i|\rho|\psi_i\rangle = \operatorname{Tr}_{(\mathscr{H})}(F_i\,\rho)$.

Uvažujme nyní obecný případ. Tehdy lze operátory F_i rozložit do vlastní báze zjevným způsobem $F_i = \sum_j |\psi_j^{(i)}\rangle\langle\psi_j^{(i)}|$, kde lineární obal vektorů $|\psi_j^{(i)}\rangle$ je opět prostor $\mathscr{H}$ dimenze d, tj. $\operatorname{span}_{ij}\{|\psi_j^{(i)}\rangle\} = \mathscr{H}$, $\dim \mathscr{H} = d$. Můžeme tak postupovat analogicky k případu výše, kdy budeme mít ortonormální bází $\{|\varphi_j^{(i)}\rangle\}_{ij}$ prostoru $\mathscr{H} \oplus \mathbb{C}^{M-d}$, kde $|\varphi_j^{(i)}\rangle = |\psi_j^{(i)}\rangle + |\psi_j^{(i)\perp}\rangle$. Z těchto vektorů pak definujeme operátory $\Pi_i = \sum_j |\varphi_j^{(i)}\rangle\langle\varphi_j^{(i)}|$ splňující vztahy $\operatorname{Tr}_{(\mathscr{H}\oplus\mathbb{C}^{M-d})}(\Pi_i(\rho\oplus 0)) = \operatorname{Tr}_{(\mathscr{H}\oplus\mathbb{C}^{M-d})}(\sum_j |\varphi_j^{(i)}\rangle\langle\varphi_j^{(i)}|(\rho \oplus 0)) = \sum_j \langle\varphi_j^{(i)}|\rho \oplus 0|\varphi_j^{(i)}\rangle = \sum_j \langle\psi_j^{(i)}|\rho|\psi_j^{(i)}\rangle + \sum_j \langle\psi_j^{(i)\perp}|0|\psi_j^{(i)\perp}\rangle = \operatorname{Tr}_{(\mathscr{H})}(F_i\,\rho)$. Dokázali jsme tak větu. □

8 Změny kvantového systému

V předchozí sekci jsem si zevrubně představili kvantové operace, nástroj, jehož prostřednictvím lze studovat vývoj otevřených kvantových systémů. Uvedli jsme si některé vlastnosti těchto zobrazení a různé způsoby jejich vyjádření, různé reprezentace. V této sekci se již konečně podíváme na celou věc více fyzikálně a místo kvantových operací samotných bude v centru našeho zájmu stát vývoj kvantového systému.

Přesto si napřed uveďme jisté požadavky či omezení, která budeme nyní na kvantové operace klást. Již od počátku budeme v definicích kvantových operací brát $\mathscr{H}_1 = \mathscr{H}_2 = \mathscr{H}$. Dále budeme uvažovat jen deterministické změny, jinými slovy budou naše kvantové operace zachovávat stopu. Konkrétně mějme zobrazení $\phi_{(t_1,t_0)}$, které vezme stav $\rho_A(t_0) \in \mathcal{S}(\mathscr{H})$ a vrátí obecně jiný stav $\rho_A(t_1) \in \mathcal{S}(\mathscr{H})$. O tomto zobrazení předpokládáme, že má za definiční obor celou množinu stavů $\mathcal{S}(\mathscr{H})$, je lineární a úplně pozitivní. Platí tedy $\rho_A(t_1) = \phi_{(t_1,t_0)}\rho_A(t_0) = \sum_i K_i\, \rho_A(t_0)\, K_i^\dagger = \mathrm{Tr}_B(U(\rho_A(t_0) \otimes |\varphi\rangle\langle\varphi|)U^\dagger)$. Druhá rovnost představuje Krausovu reprezentaci, třetí rovnost pak reprezentaci á la otevřený systém (81), kde jsme stavem $|\varphi\rangle\langle\varphi|$ popsali okolí systému.

Na tomto místě může vzniknout námitka, proč pro okolí bereme jen čistý stav a ne stav obecný, smíšený. Uvažme tedy obecnější tvar stavu okolí popsaný operátorem hustoty $\sigma = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$, kde $|\psi_i\rangle$ tvoří ortonormální bázi Hilbertova prostoru okolí. Pak dostáváme

$$\begin{aligned} \rho_A(t_1) &= \phi_{(t_1,t_0)}\rho_A(t_0) = \mathrm{Tr}_B(U(\rho_A(t_0) \otimes \sigma)U^\dagger) && (90)\\ &= \sum_{il} \lambda_i \langle\psi_l|(U(\rho_A(t_0) \otimes |\psi_i\rangle\langle\psi_i|)U^\dagger)|\psi_l\rangle && (91)\\ &= \sum_{il} \left(\sqrt{\lambda_i}\langle\psi_l|U|\psi_i\rangle\right)\rho_A(t_0)\left(\sqrt{\lambda_i}\langle\psi_i|U^\dagger|\psi_l\rangle\right). && (92) \end{aligned}$$

Označíme-li si $K_{il} = \sqrt{\lambda_i}\langle\psi_l|U|\psi_i\rangle$, přejde předchozí rovnost na tvar $\rho_A(t_1) = \sum_{il} K_{il}\rho_A(t_0)K_{il}^\dagger$, což není nic jiného, než vyjádření v Krausově reprezentaci. (Připomeňme, že operátor U působí na celém prostoru a tak výraz K_{il} není číslo, ale operátor na prostoru zkoumaného systému.) Opět tak máme zajištěnu existenci vhodného operátoru $\tilde{U}$ a čistého stavu $|\tilde{\varphi}\rangle$ tak, že $\rho_A(t_1) = \mathrm{Tr}_B(\tilde{U}(\rho_A(t_0) \otimes |\tilde{\varphi}\rangle\langle\tilde{\varphi}|)\tilde{U}^\dagger)$. Jak vidno, uvažováním obecného stavu σ namísto čistého $|\varphi\rangle$ pro popis okolí nepřináší žádné zobecnění.

Uvažujme dále obecnější změny ve tvaru $\rho_A(t_1) = \mathrm{Tr}_B(U\rho(t_0)U^\dagger)$, kde $\rho(t_0)$ je nyní stav celého systému, jak našeho zkoumaného podsystému, tak i jeho okolí. Oproti předchozímu případu je situace nyní obecnější v tom, že operátor hustoty $\rho(t_0)$ může obsahovat i korelace (provázání) mezi zkoumaným systémem a okolím. Formálně lze psát $\rho(t_0) = \rho_A(t_0) \otimes \rho_B(t_0) + \rho_{\mathrm{corr}}$, kde $\mathrm{Tr}\,\rho_{\mathrm{corr}} = 0$ a nejedná se o stav, ale o pomocný operátor. Potom máme

$$\rho_A(t_1) = \mathrm{Tr}_B(U(\rho_A(t_0) \otimes \rho_B(t_0))U^\dagger) + \mathrm{Tr}_B(U\rho_{\mathrm{corr}}U^\dagger) = \sum_{il} K_{il}\rho_A(t_0)K_{il}^\dagger + \delta_U\rho(t_1,t_0). \quad (93)$$

Formálně tedy můžeme výsledný stav popsat pomocí Krausovy reprezentace a „něčeho navíc“, veličiny $\delta_U\rho(t_1,t_0)$. Tato veličina obecně závisí na stavu ρ_A. Dále je dobré mít na paměti, že operátor ρ_{corr} omezuje třídu vstupních stavů. Například nemůže dojít k situaci, kdy je stav $\rho_A(t_0)$ čistý a přitom je operátor ρ_{corr} nenulový. Pokud je ρ_{corr} nenulový, existují mezi zkoumaným systémem a okolím korelace, které nelze popsat pomocí čistých stavů podsystémů. V této souvislosti je též vhodné si uvést následující větu, která má spíše symbolický význam.

Věta 8.1. *Jakýkoliv časový vývoj kvantového stavu ρ_A lze vždy zapsat ve tvaru*

$$\rho_A(t_1) = \sum_\alpha K_\alpha(t_1, t_0, \rho_A)\rho_A(t_0)K_\alpha^\dagger(t_1, t_0, \rho_A). \tag{94}$$

Důkaz. Nechť $\rho_A(t_1) = \sum_i \lambda_i(t_1)|\psi_i(t_1)\rangle\langle\psi_i(t_1)|$ a U_1 je zobrazení přehazující operátory v tenzorovém součinu, $U_1(A\otimes B)U_1^\dagger = B\otimes A$. Každý operátor A lze psát komplikovaným způsobem $A = \mathrm{Tr}_2(U_1(B\otimes A)U_1^\dagger)$. Aplikujeme-li tuto identitu na stav $\rho_A(t_1)$ výše a provedeme-li výpočet obdobný výpočtům v předchozích odstavcích, dospíváme k vyjádření ve tvaru Krausovy reprezentace $\rho_A(t_1) = \sum_{il} K_{il}\rho_A(t_0)K_{il}^\dagger$, kde $K_{il} = \sqrt{\lambda_i(t_1)}\langle\psi_l(t_1)|U|\psi_i(t_1)\rangle$. □

Hlavní rozdíl mezi Krausovou reprezentací, tak jak jsme si ji definovali výše, a předchozí větou tkví ve tvaru operátorů K. Zatímco v Krausově reprezentaci byly operátory plně určeny nezávisle na vstupním stavu, operátory K_α v předchozím tvrzení závisejí nejen na časech, ale i na vstupních stavech ρ_A. Pro každý vstupní stav je tedy K_α obecně různý.

Poznámka 8.1. O kvantové mechanice se hovoří jako o lineární teorii. Toto tvrzení však není zcela správně. Například v purifikačních protokolech se lze setkat se vzorci tvaru

$$\rho_2 = \mathrm{Tr}_2(U(\rho_1\otimes\rho_1)U^\dagger). \tag{95}$$

Jak vidno, takovýto výraz je *kvadratický* v proměnných specifikujících stav ρ_1.

Poznámka 8.2. V předchozí sekci jsme podrobně studovali kvantové operace a jejich vlastnosti. Na počátku této sekce jsme dále ukazovali, do jaké míry jsou tato zobrazení schopna zachytit vývoj otevřeného kvantového systému. Kvantové operace lze studovat z čistě matematického hlediska, v kontextu fyzikálního vývoje systému však budeme těmto operacím

$$\phi_{(t_1,t_0)}(\cdot) = \sum_\alpha K_\alpha(t_1,t_0)(\cdot)K_\alpha^\dagger(t_1,t_0) \tag{96}$$

říkat **univerzální dynamická zobrazení** (angl. *universal dynamical maps, UDM*). Platí zjevně $\phi_{(t_1,t_0)} : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$. Tento superoperátor vyjadřuje vývoj otevřeného systému. Jak je to však s reverzibilitou takového vývoje, existuje UDM $\phi_{(t_0,t_1)}$ popisující vývoj v opačném směru? Jednoduchým příkladem toho, že takový superoperátor obecně neexistuje, je následující zobrazení. Nechť $\{|\varphi_i\rangle\}_i$ je ortonormální báze prostoru $\mathscr{H}$ a $|\varphi\rangle$ je nějaký vektor z $\mathscr{H}$. Definujme $\phi(\rho) = \sum_i E_i\rho E_i^\dagger = \sum_i |\varphi\rangle\langle\varphi_i|\rho|\varphi_i\rangle\langle\varphi| = (\mathrm{Tr}\,\rho)|\varphi\rangle\langle\varphi|$. Toto zobrazení sice je UDM, ale nelze ho invertovat. Pro obecný případ lze dokázat následující větu, kterou si my však dokazovat nebudeme.

Věta 8.2. *Pro dané univerzální dynamické zobrazení $\phi_{(t_1,t_0)}$ je jeho inverze též UDM právě tehdy, když existuje unitární operátor U takový, že $\phi_{(t_1,t_0)}(\cdot) = U(\cdot)U^\dagger$.*

Vývoj kvantového systému popsaného UDM zobrazením je tedy reverzibilní právě tehdy, když je uzavřený, unitární.

8.1 Časová spojitost – Markovovská evoluce

Dosud jsme k popisu časového vývoje otevřeného systému využívali kvantové operace alias univerzální dynamická zobrazení. Tato zobrazení udávají, jak se změní stav studovaného systému mezi dvěma danými časy. Konkrétně nechť $\phi_{(t_1,t_0)}$ popisuje časový vývoj systému od času t_0 k času t_1. Jedná se tedy o *diskrétní* popis vývoje studovaného systému, nevíme nic o stavech systému v časech $t_0 < t < t_1$. Zkusme nyní přistoupit k vývoji otevřeného systému z jiné strany. Nyní budeme chtít studovat *spojité* časové vývoje, stav systému tedy budeme chtít znát v každém čase. Uvažujme proto následující rovnici, kde $\rho \in \mathcal{S}(\mathscr{H})$, s počáteční podmínkou $\rho(0) = \rho_0$, jejíž zápis zní

$$\frac{\mathrm{d}\,\rho(t)}{\mathrm{d}t} = L(t)(\rho(t)). \tag{97}$$

Zobrazení L zatím zůstává nespecifikované, jeho účelem je však zjevně popisovat vývoj daného systému. Zmíněné rovnici se říká **evoluční rovnice**. Její řešení můžeme formálně vyjádřit ve tvaru $\rho(t) = T(t,t_0)\rho_0$, kde je T lineární zobrazení, kterážto vlastnost plyne z linearity samotné evoluční rovnice. Kvůli konzistenci časového vývoje musejí tato zobrazení splňovat následující dvě podmínky:

$$T(t,t) = \mathbb{I}, \qquad T(t_2,t_0) = T(t_2,t_1)\,T(t_1,t_0), \tag{98}$$

pro všechna t a všechny časy t_0, t_1, t_2 splňující $t_2 \geq t_1 \geq t_0$. Každá sada operátorů vyhovující těmto podmínkám se nazývá **evoluční třída**.

Věta 8.3. *Diferencovatelná evoluční třída $T(t,s)$ je jediným řešením soustavy rovnic*

$$\frac{\mathrm{d}\,T(t,s)}{\mathrm{d}t} = L(t)T(t,s), \quad \frac{\mathrm{d}\,T(t,s)}{\mathrm{d}s} = -T(t,s)\,L(s), \quad T(s,s) = \mathbb{I}, \tag{99}$$

kde L je nějaký jednoparametrický systém operátorů.

Důkaz. Nechť $t \geq s$. Nejdříve ukažme, že evoluční třída T skutečně řeší dané rovnice pro nějaký systém operátorů L. Platí

$$\frac{\mathrm{d}\,T(t,s)}{\mathrm{d}t} = \lim_{h\to 0}\frac{T(t+h,s)-T(t,s)}{h} = \lim_{h\to 0}\frac{T(t+h,t)T(t,s)-T(t,s)}{h} = \lim_{h\to 0}\frac{T(t+h,t)-\mathbb{I}}{h}T(t,s). \tag{100}$$

Definujeme-li si $L(t) = \lim_{h\to 0}\frac{T(t+h,t)-\mathbb{I}}{h}$, je rovnost dokázána. Dokažme si ještě jednoznačnost. Pro spor mějme dvě řešení $T(t,s)$ a $S(t,s)$, z nichž si sestrojíme systém operátorů Q, kde $Q(r) \coloneqq T(t,r)S(r,s)$ pro $t \geq r \geq s$. Pro derivaci následně platí

$$\frac{\mathrm{d}\,Q(r)}{\mathrm{d}r} = \frac{\mathrm{d}\,T(t,r)}{\mathrm{d}r}S(r,s) + T(t,r)\frac{\mathrm{d}\,S(r,s)}{\mathrm{d}r}. \tag{101}$$

Když dosadíme za derivace z rovnic výše, tak zjišťujeme, že derivace $\frac{\mathrm{d}\,Q(r)}{\mathrm{d}r}$ je nulová a $Q(r)$ je tedy stejný pro všechny časy r. Položíme-li $r = s$, redukuje se nám tvar tohoto operátoru na $Q(s) = T(t,s)$. Podobně při dosazení $r = t$ obdržíme $Q(t) = S(t,s)$. Dokázali jsme tak jednoznačnost řešení. □

V případě uzavřených systémů, jejichž vývoj se řídí Schrödingerovou rovnicí, je stav systému tvaru $\rho(t) = U(t,t_0)\rho_0$, kde $U(t,t_0)$ jsou unitární operátory zjevně tvořící evoluční třídu. Vraťme se nyní zpět k našemu popisu pomocí kvantových operací a pokusme se tento přístup propojit s právě naznačeným spojitým popisem vývoje. Jak lze snadno nahlédnout z reprezentace á la otevřený systém (81), k operaci $\phi_{(t_1,t_0)}$ zmíněné výše přísluší jistý unitární operátor $U(t_1,t_0)$ popisující vývoj studovaného systému spolu s jeho okolím

$$\phi_{(t_1,t_0)}(\rho_A(t_0)) = \mathrm{Tr}_B\left(U(t_1,t_0)(\rho_A(t_0)\otimes\rho_B(t_0))U^\dagger(t_1,t_0)\right). \tag{102}$$

Mějme dále kvantovou operaci $\phi_{(t_2,t_0)}$ popisující vývoj systému od času t_0 k času $t_2 > t_1$, jemuž je příslušný unitární operátor $U(t_2,t_0)$. Unitární operátory popisují vývoj celého, uzavřeného, systému, splňují tedy vztah $U(t_2,t_0) = U(t_2,t_1)\,U(t_1,t_0)$, kde $U(t_2,t_1)$ popisuje vývoj celého systému od času t_1 k času t_2. Kdybychom chtěli podobnou rovnost najít i pro odpovídající kvantové operace, tj.

$$\phi_{(t_2,t_0)} = \phi_{(t_2,t_1)}\circ\phi_{(t_1,t_0)}, \tag{103}$$

tak narazíme na problém. Necháme-li počáteční stav $\rho_A(t_0)$ vyvíjet do času t_1, může se tento provázat se stavem okolí ρ_B. Provedeme-li ale poté v (102) částečnou stopu, připravíme se o znalost těchto kvantových korelací. Kvantová operace $\phi_{(t_2,t_1)}$ tak obecně nemá dostatek informací pro správný popis vývoje systému od času t_1 k času t_2. Obecně bychom museli psát

$$\phi_{(t_2,t_1)}(\rho_A(t_0)) = \mathrm{Tr}_B(U(t_2,t_1)\,\rho(t_1)\,U^\dagger(t_2,t_1)), \tag{104}$$

kde $\rho(t_1)$ je stav zkoumaného systému spolu s okolím. Výše jsme viděli, že vývoj provázaného stavu nelze zcela zachytit pomocí Krausových operátorů a zobrazení $\phi_{(t_2,t_1)}$ tak obecně nemusí být kvantovou operací, viz (93). Nicméně, níže si vydělíme takovou podtřídu otevřených vývojů, pro níž bude vlastnost (103) splněna.

Definice 8.1. Říkáme, že kvantový systém podstupuje **Markovovský vývoj** (respektive **Markovovskou evoluci**) právě tehdy, když je jeho vývoj popsán evoluční třídou tvořenou univerzálními dynamickými zobrazeními.

Jinými slovy se systém řídí Markovovskou evolucí právě, když je jeho vývoj popsán evoluční třídou a tato třída je navíc tvořena kvantovými operacemi. Tyto předpoklady na vývoj systému jsou velmi omezující. Leč, v teoretických spisech se lze s tímto modelem setkat poměrně často.

Odvoďme si nyní diferenciální tvar Markovovského vývoje. Najdeme tedy tvar příslušného zobrazení L v rovnici (97). Postupem obdobným tomu v důkazu věty (8.3) upravíme tvar časové derivace operátoru hustoty následovně

$$\frac{\mathrm{d}\,\rho(t)}{\mathrm{d}t} = \lim_{h\to 0}\frac{\rho(t+h)-\rho(t)}{h} = \lim_{h\to 0}\frac{T(t+h,t)-\mathbb{I}}{h}\rho(t) = L(t)\rho(t), \tag{105}$$

kde jsme položili $L(t) = \lim_{h\to 0}\frac{T(t+h,t)-\mathbb{I}}{h}$. Dospěli jsme tak k evoluční rovnici, které se v tomto kontextu též říká **řídící rovnice** (angl. *master equation*). Zobrazení L lze přitom vyjádřit v hezčím tvaru tak, jak je ukázáno v následujícím lemmatu. Uveďme si nejprve však pomocnou definici.

Definice 8.2. Zobrazení $L : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ je **podmíněně úplně pozitivní** právě tehdy, když

$$P(L \otimes \mathbb{I}_{\mathscr{H}})(|\Omega\rangle\langle\Omega|)P \geq 0, \tag{106}$$

kde P je ortogonální projekce na $(\mathrm{span}(|\Omega\rangle\langle\Omega|))^{\perp}$, tj. $P = \mathbb{I} - |\Omega\rangle\langle\Omega|$.

Lemma 8.1. *Nechť $L : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ je nějaké zobrazení. Pak následující tvrzení jsou ekvivalentní.*

1. *Zobrazení L je hermitovské (tj. obrazy hermitovských operátorů jsou opět hermitovské) a podmíněně úplně pozitivní.*
2. *Existuje úplně pozitivní zobrazení $\phi : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ a matice $K \in \mathcal{B}(\mathscr{H})$ tak, že $L(\rho) = \phi(\rho) - K\rho - \rho K^{\dagger}$.*

Důkaz. Nejprve ukážeme, že podmíněná úplná pozitivita nezávisí na volbě maximálně provázaného stavu $|\Omega\rangle$. Uvažujme tedy $|\Omega'\rangle = (\mathbb{I} \otimes U)|\Omega\rangle$. Pak výraz $P'(L \otimes \mathbb{I})(|\Omega'\rangle\langle\Omega'|)P'$ je roven

$$\begin{aligned}
&(\mathbb{I} - |\Omega'\rangle\langle\Omega'|)(L \otimes \mathbb{I})((\mathbb{I} \otimes U)|\Omega\rangle\langle\Omega|(\mathbb{I} \otimes U^{\dagger}))(\mathbb{I} - |\Omega'\rangle\langle\Omega'|) \\
=\ &((\mathbb{I} \otimes U) - |\Omega'\rangle\langle\Omega'|(\mathbb{I} \otimes U))(L \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|)((\mathbb{I} \otimes U^{\dagger}) - (\mathbb{I} \otimes U^{\dagger})|\Omega'\rangle\langle\Omega'|) \\
=\ &(\mathbb{I} \otimes U)(\mathbb{I} - |\Omega\rangle\langle\Omega|)(L \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|)(\mathbb{I} - |\Omega\rangle\langle\Omega|)(\mathbb{I} \otimes U^{\dagger}) \\
=\ &(\mathbb{I} \otimes U)P(L \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|)P(\mathbb{I} \otimes U^{\dagger}).
\end{aligned}$$

Obdrželi jsme tak výraz, který je podobnostní transformací spjat s výrazem $P(L\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)P$. Když je jeden výraz pozitivní, je pozitivní i druhý. Pozitivita tedy skutečně nezávisí na volbě stavu $|\Omega\rangle$.

Přejděme nyní k důkazům jednotlivých implikací, začněme s implikací z prvního do druhého bodu. Zobrazení L nechť je tedy hermitovské. Pak $\tau = (L \otimes \mathbb{I}_{\mathscr{H}})(|\Omega\rangle\langle\Omega|)$ je též hermitovský. Jako další krok doplníme vektor $|\Omega\rangle$ na ortonormální bázi $\{|\Omega\rangle, |\Omega_1\rangle, \ldots, |\Omega_k\rangle\}$. V této bázi můžeme τ vyjádřit způsobem $\tau = \tau_0|\Omega\rangle\langle\Omega| + \sum_i(\tau_i|\Omega_i\rangle\langle\Omega| + \tau_i^*|\Omega\rangle\langle\Omega_i|) + Q$, kde $Q = \sum_{ij}\tau_{ij}|\Omega_i\rangle\langle\Omega_j|$ je hermitovská matice. Zavedeme-li vektor $|\psi\rangle = (\tau_0/2)|\Omega\rangle + \sum_i \tau_i|\Omega_i\rangle$, můžeme přepsat τ jako $\tau = Q + |\psi\rangle\langle\Omega| + |\Omega\rangle\langle\psi|$. Jak vidno, Q žije na ortogonálním doplňku k $|\Omega\rangle$. Dále $P\tau P = Q$, takže $Q \geq 0$. Existuje tedy úplně pozitivní ϕ tak, že $Q = (\phi \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|)$ a navíc existuje matice K taková, že $-|\psi\rangle = (K \otimes \mathbb{I})|\Omega\rangle$. (Znaménko mínus je voleno tímto způsobem z historických důvodů.) Celkem máme $\tau = (\phi\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) - (K\otimes\mathbb{I})|\Omega\rangle - |\Omega\rangle(K^{\dagger}\otimes\mathbb{I})$. Tento vzorec můžeme dále upravit použitím vztahu $ABC \sim (A\otimes C^T)|B\rangle$ na tvar $(\phi\otimes\mathbb{I} - (K(\cdot)\mathbb{I})\otimes\mathbb{I} - (\mathbb{I}(\cdot)K^{\dagger})\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)$. Porovnáním tohoto výrazu s původním tvarem pro τ získáváme $L(A) = \phi(A) - KA - AK^{\dagger}$.

Pro důkaz opačné implikace nechť $L(\rho) = \phi(\rho) - K\rho - \rho K^{\dagger}$. Z tohoto plyne $(L \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) = (\phi \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) - (K \otimes \mathbb{I})(|\Omega\rangle\langle\Omega|) - (|\Omega\rangle\langle\Omega|)(K^{\dagger} \otimes \mathbb{I})$. Uvědomíme-li si, že $P|\Omega\rangle = 0 = \langle\Omega|P$, tak ihned dostáváme $P(L\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)P = P(\phi\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)P$. Neboť je poslední výraz pozitivní, je zobrazení L podmíněně úplně pozitivní. K dokončení důkazu ještě ověřme, že je L hermitovské. Skutečně, platí $L(\rho^{\dagger}) = \phi(\rho^{\dagger}) - K\rho^{\dagger} - \rho^{\dagger}K^{\dagger} = (\phi(\rho) - \rho K^{\dagger} - K\rho)^{\dagger} = (L(\rho))^{\dagger}$, což bylo dokázati. □

Předešlé tvrzení udává specifičtější tvar zobrazení L na základě některých jeho obecných vlastností. O tom, zda má popisovat Markovovský vývoj či ne, jsme se dosud nezmínili. To uděláme až v tvrzení následujícím.

Věta 8.4. *Nechť $T(t,s) : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ je evoluční třída. Pak následující dvě tvrzení jsou ekvivalentní.*

1. *$T(t,s)$ je Markovovská evoluční třída.*
2. *Zobrazení $L(t) = \lim_{h\to 0} \frac{T(t+h,t)-\mathbb{I}}{h}$ je podmíněně úplně pozitivní.*

Důkaz. Pro důkaz implikace z jedničky do dvojky mějme $T(t,s)$, které je úplně pozitivní. Platí tedy $(T(t,s)\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) \geq 0$. Pro malá h mohu rozumně provést rozklad způsobem $T(t+h,s) = T(t,s) + \frac{\mathrm{d}T(t,s)}{\mathrm{d}t}h + \mathcal{O}(h^2)$ a tedy $T(t+h,t) = \mathbb{I} + L(t)h + \mathcal{O}(h^2)$. Z toho plyne $0 \leq (T(t+h,t)\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) = |\Omega\rangle\langle\Omega| + h(L(t)\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|) + \mathcal{O}(h^2)$. Celý výraz je pozitivní, tj. hermitovský. Pošleme-li h do nuly, tak zjišťujeme, že i $(L(t)\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)$ je hermitovský a tak $L(t)$ zachovává hermitovost. Navíc, obložíme-li celý výraz projektorem P a vydělíme-li číslem h, máme $0 \leq P(L(t)\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)P + P(\frac{1}{h}\mathcal{O}(h^2))P$. Druhý člen jde do nuly pro $h \to 0$ a tak $P(L(t)\otimes\mathbb{I})(|\Omega\rangle\langle\Omega|)P \geq 0$. Zobrazení $L(t)$ je tedy podmíněně úplně pozitivní. Důkaz opačné implikace z druhého do prvního bodu je nad rámec této přednášky. □

Z důkazu právě uvedené věty plyne, že pro Markovovský vývoj je odpovídající zobrazení L hermitovské a podmíněně úplně pozitivní. Podle lemmatu 8.1 lze takovéto zobrazení napsat ve tvaru $L(\rho) = \phi(\rho) - K\rho - \rho K^\dagger$ pro jistou matici K a kvantovou operaci ϕ. Neboť L může záviset na čase a kvantové operace ϕ_t lze vyjádřit v Krausově reprezentaci, platí

$$L(t)(A) = \phi_t(A) - K(t)A - AK^\dagger(t) = \sum_i V_i(t)AV_i^\dagger(t) - K(t)A - AK^\dagger(t) \tag{107}$$

pro vhodně zvolené jednoparametrické třídy matic V_i a K. Takovýto vývoj nezvyšuje stopu, platí tedy, že časová derivace stopy $\mathrm{Tr}(\rho(t))$ je nekladná. Neboli

$$0 \geq \frac{\mathrm{d}\,\mathrm{Tr}(\rho(t))}{\mathrm{d}t} = \mathrm{Tr}\left(\frac{\mathrm{d}\rho(t)}{\mathrm{d}t}\right) = \mathrm{Tr}(L(t)\rho(t)) = \mathrm{Tr}(L^\dagger(t)(\mathbb{I})\,\rho(t)), \tag{108}$$

kde první rovnost plyne z definice derivace a linearity stopy. Druhá rovnost plyne z evoluční rovnice a konečně třetí rovnost plyne z vlastností Hilbert-Schmidtova skalárního součinu. Neboť výše odvozený vztah musí platit pro všechny časy t a stavy $\rho(t)$, je jeho splnění ekvivalentní podmínce

$$L^\dagger(t)(\mathbb{I}) \leq 0, \quad \forall t. \tag{109}$$

Z toho již přímo vyplývá, že evoluční třída zachovává stopu právě tehdy, když $L^\dagger(t)(\mathbb{I}) = 0$, tj. $\phi_t^\dagger(\mathbb{I}) = K(t)+K^\dagger(t)$ pro všechny časy, viz (107). Tento vztah tedy ukazuje, že operátor $\phi_t^\dagger(\mathbb{I})$ je samosdružený. Navíc, obecnou matici K lze rozložit na součet hermitovské a antihermitovské matice způsobem

$$K = \frac{K+K^\dagger}{2} + \frac{K-K^\dagger}{2} = K_H + K_A, \tag{110}$$

kde $K_H = \frac{K+K^\dagger}{2} = K_H^\dagger$ a $K_A = \frac{K-K^\dagger}{2} = -K_A^\dagger$. Pro součet tedy máme $K+K^\dagger = 2K_H$. Porovnáme-li tento výraz s obdrženým vztahem $\phi_t^\dagger(\mathbb{I}) = K(t)+K^\dagger(t)$, můžeme psát $K(t) = \frac{1}{2}\phi_t^\dagger(\mathbb{I})+\mathrm{i}\,H(t)$, kde $H(t)$ je nějaký samosdružený operátor. Dosadíme-li toto vyjádření do vzorce pro zobrazení L, dostáváme

$$\begin{aligned}
L(t)(A) &= \sum_i V_i A V_i^\dagger - \frac{1}{2}\phi^\dagger(\mathbb{I})A - \frac{1}{2}A\phi^\dagger(\mathbb{I}) - \mathrm{i}\,HA + \mathrm{i}\,AH && (111)\\
&= \sum_i V_i A V_i^\dagger - \frac{1}{2}\{\phi^\dagger(\mathbb{I}), A\} + \mathrm{i}\,[A,H] && (112)\\
&= \mathrm{i}\,[A,H] + \sum_i (V_i A V_i^\dagger - \frac{1}{2}\{V_i^\dagger V_i, A\}) && (113)\\
&= \mathrm{i}\,[A,H] + \frac{1}{2}\sum_i (2V_i A V_i^\dagger - V_i^\dagger V_i A - A V_i^\dagger V_i) && (114)\\
&= \mathrm{i}\,[A,H] + \frac{1}{2}\sum_i \left(\left[V_i A, V_i^\dagger\right] + \left[V_i, A V_i^\dagger\right]\right), && (115)
\end{aligned}$$

kde $[\cdot,\cdot]$ značí komutátor a $\{\cdot,\cdot\}$ označuje antikomutátor. Výrazu $\sum_i (V_i(\cdot)V_i^\dagger - \frac{1}{2}\{V_i^\dagger V_i, (\cdot)\})$ ve třetím řádku se říká **Lindbladovská forma**, resp. **Lindbladův superoperátor**, a operátory V_i se nazývají **Lindbladovy operátory**. Řídící rovnici (97), kde za L dosadíme ten, který jsme v poslední rovnosti odvodili, se říká **Lindbladova rovnice**. Snadno nahlédneme, že pokud položíme všechny V_i rovné nule, tak se nám Lindbladova rovnice redukuje do tvaru

$$\frac{\mathrm{d}\,\rho(t)}{\mathrm{d}t} = \mathrm{i}\,[A,H], \tag{116}$$

což je *Liouvilleova rovnice*. Operátor H je hermitovský a lze ho tudíž interpretovat jako *Hamiltonián* daného systému.

8.1.1 Homogenní Markovovské procesy

Uvažujme nyní, že je zobrazení L konstantní, neboli jednoparametrická třída zobrazení $L(t)$ má všechny prvky stejné a rovné L. Z diskuze výše vidíme, že L je konstantní právě tehdy, když ϕ a K jsou konstantní. Zobrazení L lze chápat jako generátor evoluční třídy $T(t_2,t_1)$ (98). Z rovnice (97) totiž plyne

$$T(t_2,t_1) = e^{L(t_2-t_1)}. \tag{117}$$

Operátor $T(t_2,t_1)$ tedy závisí jen na rozdílu $\tau = t_2 - t_1$ počátečního t_1 a konečného času t_2. Označme si $T(t_2,t_1) = \phi_\tau$. Pak z vlastností evoluční třídy plyne

$$\phi_{\tau_1+\tau_2} = \phi_{\tau_2} \circ \phi_{\tau_1}. \tag{118}$$

Množina univerzálních dynamických zobrazení ϕ_τ tak zjevně tvoří pologrupu, této pologrupě se říká **(kvantová) Markovovská (dynamická) pologrupa**.

Příklad 8.1. *Defázování dvouhladinového kvantového systému.* Uvažujme dvouhladinový systém, tj. systém, který se může nacházet buď v základním, nebo v excitovaném stavu. Nechť je tento navíc v kontaktu s tepelnou lázní. Zajímá nás chování našeho dvouhladinového systému při defázování, kde zanedbáme změny v lázni, o níž předpokládáme, že je obrovská ve srovnání s naším zkoumaným systémem. Defázování je pak za takovýchto předpokladů popsáno Hamiltoniánem $H = \frac{\omega_0}{2}\sigma_Z$ a Lindbladovským operátorem $V = \sqrt{\gamma}\sigma_Z$. Neboť $\frac{1}{2}\{{\sigma_Z}^\dagger\sigma_Z, \rho\} = \frac{1}{2}\{\mathbb{I}, \rho\} = \rho$ je Lindbladova rovnice tvaru

$$\frac{\mathrm{d}\,\rho(t)}{\mathrm{d}t} = \mathrm{i}\left[\rho(t), \frac{\omega_0}{2}\sigma_Z\right] + \gamma(\sigma_Z\rho(t)\sigma_Z - \rho(t)), \tag{119}$$

kde $\rho(t)$ je matice hustoty dvouhladinového stavu. Lze ukázat, že časový vývoj popsaný touto rovnici vynucuje, že matice hustoty $\rho(t)$ vyjádřená ve výpočetní bázi přejde do diagonálního tvaru, pošleme-li čas do nekonečna. Neboli

$$\rho(0) = \begin{pmatrix} \rho_{11} & \rho_{12} \\ \rho_{21} & \rho_{22} \end{pmatrix} \xrightarrow{t\to\infty} \begin{pmatrix} \rho_{11} & 0 \\ 0 & \rho_{22} \end{pmatrix}. \tag{120}$$

8.2 Spektrální vlastnosti kvantových operací a generátorů Markovovské evoluční třídy

Mnoho zajímavých vlastností superoperátorů lze vyčíst ze znalosti jejich vlastních čísel. V této kapitolce se tedy budeme blíže věnovat právě spektru kvantových operací a podobných zobrazení. Na úvod si připomeňme definici a některé vlastnosti operátorové normy pro operátory $A \in \mathcal{B}(\mathscr{H})$. Její definice pro takové operátory zní

$$\|A\| = \sup_{\|x\|=1} \|Ax\|. \tag{121}$$

Uvedeme si čtyři vlastnosti, jež budeme v následujícím potřebovat. Pro každé dva operátory $A, B \in \mathcal{B}(\mathscr{H})$ platí

1. $\|AB\| \leq \|A\|\|B\|$,
2. $\|A\| = \|A^\dagger\|$,
3. $\|A^\dagger A\| = \|A\|^2$,
4. $\|A\| = \|UAV\|$ pro $U, V \in \mathcal{B}(\mathscr{H})$ unitární.

Kromě té poslední byly všechny vlastnosti dokázány již v kurzu funkcionální analýzy. Poslední rovnost si dokážeme pomocí rozkladu operátoru na singulární hodnoty. Z právě zmíněných vlastností normy mimo jiné plyne, že množina omezených operátorů tvoří $C^\star$-algebru.

Poznámka 8.3. Každý (obecně komplexní) operátor A lze rozložit do tvaru $A = UDV$, kde U a V jsou unitární operátory a D je diagonální matice, jejíž prvky d_i jsou všechny nezáporné. Těmto prvkům se říká **singulární vlastní hodnoty** operátoru A. Pro diagonalizovatelné operátory A navíc existuje unitární operátor U_1 takový, že $A = U_1 D_1 U_1{}^\dagger$, kde D_1 je diagonální matice tvořená vlastními čísly α_i. Součin $AA^\dagger$ pak splňuje rovnost $AA^\dagger = U_1|D_1|^2 U_1{}^\dagger = UD^2U^\dagger$. Máme tak dvojí vyjádření vlastních čísel operátoru $AA^\dagger$ – jednak pomocí matice $|D_1|^2$, jednak pomocí matice D^2. Platí tedy rovnost $|\alpha_i|^2 = d_i^2$, tj. $|\alpha_i| = d_i$. Lze dále ukázat, že norma operátoru A se spočte jako $\|A\| = s_1(d_i) = \max_i d_i$. S využitím tohoto vztahu již lze dokázat druhou vlastnost operátorové normy zmíněné ve výčtu výše.

Definice 8.3. Nechť $A \in \mathcal{B}(\mathscr{H})$ je operátor splňující $\|A\| \leq 1$. Pak A se nazývá **kontrakce**.

Věta 8.5. *Omezený operátor $A \in \mathcal{B}(\mathscr{H})$ je kontrakce právě, když*

$$\begin{pmatrix} \mathbb{I} & A \\ A^\dagger & \mathbb{I} \end{pmatrix} \geq 0. \tag{122}$$

Důkaz. Uvažujme nejprve jednorozměrný případ, tj. $\dim \mathscr{H} = 1$. Pak je ihned vidět, že matice

$$\begin{pmatrix} 1 & a \\ a^* & 1 \end{pmatrix} \tag{123}$$

je pozitivní právě tehdy, když $|a| \leq 1$. Pro vyšší dimenze vyjádřeme operátor A pomocí jeho singulárních hodnot ve tvaru $A = UDV$. Pak

$$\begin{pmatrix} \mathbb{I} & A \\ A^\dagger & \mathbb{I} \end{pmatrix} = \begin{pmatrix} \mathbb{I} & UDV \\ V^\dagger D U^\dagger & \mathbb{I} \end{pmatrix} = \begin{pmatrix} U & 0 \\ 0 & V^\dagger \end{pmatrix} \cdot \begin{pmatrix} \mathbb{I} & D \\ D & \mathbb{I} \end{pmatrix} \cdot \begin{pmatrix} U^\dagger & 0 \\ 0 & V \end{pmatrix}. \tag{124}$$

Poslední výraz je tvořen třemi maticemi, z nichž třetí je hermitovsky sdružená k první. Tento výraz je tedy sdružen podobnostní transformací s maticí

$$\begin{pmatrix} \mathbb{I} & D \\ D & \mathbb{I} \end{pmatrix}, \tag{125}$$

která je tvořena diagonálními maticemi D a $\mathbb{I}$. Lze ji tedy přepsat do tvaru

$$\begin{pmatrix} \mathbb{I} & D \\ D & \mathbb{I} \end{pmatrix} = P \left(\bigoplus_i \begin{pmatrix} 1 & d_i \\ d_i & 1 \end{pmatrix} \right) P^\dagger, \tag{126}$$

kde P je vhodná permutační matice a d_i jsou diagonální prvky matice D. Tento výraz je podobností transformací sdružen s direktním součtem matic 2×2, které jsou stejného tvaru, jaký jsme vyšetřovali v jednorozměrném případě na začátku důkazu. Protože podobnostní transformace zachovává pozitivitu, stačí nám vyšetřovat pozitivitu každé takovéto matice 2×2 zvlášť. Pro tyto matice jsme ale už důkaz pozitivity provedli na počátku důkazu. Můžeme tedy shrnout, že daná matice je pozitivní právě, když $d_i \leq 1$ pro všechny indexy i, což je ekvivalentní s tím, že operátor A je kontrakce. □

Věta 8.6. Russo-Dyeova věta. *Nechť $\phi : \mathcal{B}(\mathscr{H}) \to \mathcal{B}(\mathscr{H})$ je pozitivní a unitální lineární zobrazení. Pak jeho operátorová norma je rovna jedné, neboli*

$$\|\phi\| \equiv \sup_{\|A\|=1} \|\phi(A)\| = 1. \tag{127}$$

Důkaz. Nejprve ukážeme, že pro unitární U platí $\|\phi(U)\| \leq 1$. Uvažujme spektrální rozklad operátoru U ve tvaru $U = \sum_i \lambda_i P_i$, kde vlastní čísla tedy splňují $|\lambda_i| = 1$ a projektory na vlastní podprostory se sčítají na identitu, $\sum_i P_i = \mathbb{I}$. Zobrazení ϕ je unitální, tj. $\mathbb{I} = \phi(\mathbb{I}) = \phi(\sum_i P_i)$. S využitím této vlastnosti pak můžeme psát

$$\begin{pmatrix} \mathbb{I} & \phi(U) \\ \phi^\dagger(U) & \mathbb{I} \end{pmatrix} = \begin{pmatrix} \sum_i \phi(P_i) & \sum_i \lambda_i \phi(P_i) \\ \sum_i \lambda_i^* \phi(P_i) & \sum_i \phi(P_i) \end{pmatrix} = \sum_i \begin{pmatrix} \phi(P_i) & \lambda_i \phi(P_i) \\ \lambda_i^* \phi(P_i) & \phi(P_i) \end{pmatrix} \tag{128}$$

Sumu matic za poslední rovností lze vyjádřit jako tenzorový součin v následujícím tvaru

$$\sum_i \begin{pmatrix} 1 & \lambda_i \\ \lambda_i^* & 1 \end{pmatrix} \otimes \phi(P_i). \tag{129}$$

Neboť ϕ je z předpokladů pozitivní a $|\lambda_i| = 1$, tak suma matic výše je pozitivní operátor a z předchozí věty tak plyne, že $\|\phi(U)\| \leq 1$. Uvažujme dále libovolný operátor $A \in \mathcal{B}(\mathscr{H})$ o jednotkové normě. Ukážeme nyní, že lze tento vyjádřit jako $A = \frac{1}{2}(U + V)$, kde U a V jsou unitární operátory. Protože $\|A\| = 1$, tak všechny singulární hodnoty d_i leží v intervalu $[0, 1]$ a lze je tak napsat jako cosinus jistého úhlu φ_i. Rozklad A na singulární hodnoty tedy vypadá jako $A = U_1 D V_1$, kde $D = \mathrm{Diag}(\cos(\varphi_1), \ldots, \cos(\varphi_n)) = \frac{1}{2}(D_1 + {D_1}^\dagger)$. Matice D_1 je přitom diagonální matice tvaru $D_1 = \mathrm{Diag}(\exp(\mathrm{i}\,\varphi_1), \ldots, \exp(\mathrm{i}\,\varphi_n))$, neboť $\cos(\varphi_i) = \frac{1}{2}(\exp(\mathrm{i}\,\varphi) + \exp(-\mathrm{i}\,\varphi)$. Pak tedy $A = \frac{1}{2} U_1 (D_1 + {D_1}^\dagger) V_1 = \frac{1}{2}(U_1 D_1 V_1 + U_1 {D_1}^\dagger V_1)$.

Přikročme k závěrečné části důkazu. S využitím zápisu $A = \frac{1}{2}(U+V)$ a již dokázané nerovnosti pro unitární operátory dostáváme $\|\phi(A)\| = \frac{1}{2}\|\phi(U) + \phi(V)\| \leq 1$. Navíc $\phi(\mathbb{I}) = \mathbb{I}$, nerovnosti se tedy nabývá a platí tak $\|\phi\| = 1$. □

Tvrzení předchozí věty lze zobecnit v následujícím znění i pro neunitální operace ϕ.

Věta 8.7. *Nechť ϕ je pozitivní lineární superoperátor na $\mathcal{B}(\mathscr{H})$. Pak $\|\phi\| = \|\phi(\mathbb{I})\|$.*

Důkaz. Položme $R = \phi(\mathbb{I})$. Pokud je R invertovatelné, pak pro $\tilde{\phi}(A) = R^{-\frac{1}{2}} \phi(A) R^{-\frac{1}{2}}$ platí, že $\tilde{\phi}(A)$ je unitální a pozitivní. Z předchozí věty tedy vyplývá $\|\tilde{\phi}(A)\| = \|R^{-\frac{1}{2}} \phi(A) R^{-\frac{1}{2}}\| = 1$. Takže $\|\phi(A)\| = \|R^{\frac{1}{2}} \tilde{\phi}(A) R^{\frac{1}{2}}\| \leq \|R^{\frac{1}{2}}\|^2 \|\tilde{\phi(A)}\|$. Neboť pro obecné $B \in \mathcal{B}(\mathscr{H})$ platí $\|B^\dagger B\| = \|B\|^2$, tak $\|\phi(A)\| \leq \|R^{\frac{1}{2}} R^{\frac{1}{2}}\| \|\tilde{\phi}\| \|A\| = \|R\| \|A\|$. Z definice normy operátoru tedy $\|\phi\| \leq \|R\| = \|\phi(\mathbb{I})\|$. Navíc pro volbu $A = \mathbb{I}$ dostáváme $\|\phi(\mathbb{I})\| \leq \|R\| \|\mathbb{I}\| = \|R\|$. Neboť $R = \phi(\mathbb{I})$, tak se předchozí nerovnosti nabývá a celkem tedy platí $\|\phi\| = \|\phi(\mathbb{I})\|$. Pro neinvertibilní R můžeme definovat $\phi_\varepsilon(A) = \phi(A) + \varepsilon \mathbb{I}$, které je pro každé $\varepsilon > 0$ invertovatelné. Nyní bychom postupovali stejně jako v předchozím případě pro ϕ_ε a nakonec provedli limitní přechod $\varepsilon \to 0$. Neboť je norma spojité zobrazení, tak i pro neinvertovatelné R máme $\|\phi\| = \|\phi(\mathbb{I})\|$. □

Dovětek

Přepsal Jaroslav Kysela (kyseljar@fjfi.cvut.cz) na základě vlastnoručních poznámek z přednášek Ing. Jaroslav Novotného, Ph.D. konaných v letním semestru akademického roku 2014/2015. Z původního kurzu jsou vynechány poslední dvě přednášky jednak navazující na kapitolu Spektrální vlastnosti operátorů a jednak probírající nevratnost a produkci entropie v kvantovém systému. Naopak jsou přidány pasáže, jejichž účelem by mělo být snazší pochopení uváděných a dokazovaných matematických vzorců a alespoň částečné motivování zaváděných definic a postupů.