České vysoké učení technické v Praze
Fakulta elektrotechnická

Katedra kybernetiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: Jáchym Barvinek

Studijní program: Otevřená informatika (bakalářský)

Obor: Informatika a počítačové vědy

Název tématu: Kvantová entropie a její zachování

Pokyny pro vypracování:

Student shrne základní vlastnosti kvantových automorfismů a Jordanových izomorfismů mezi maticovými algebrami, včetně příslušného pozadí kvantové teorie a základu maticové analýzy. Bude prezentovat Wignerovu větu o kvantových symetriích v případě algebry komplexních matic. Prostuduje její geometrické i numerické aspekty. Pokusí se o co nejjednodušší a originální důkaz tohoto základního principu kvantové mechaniky.

Ve druhé části bude studovat základní vlastnosti von Neumannovy entropie a vzájemné kvantové entropie dvou veličin v konečné dimenzi. Rozebere nedávný výsledek L.Molnara charakterizující lineární zobrazení maticových algeber, které zachovávají vzájemnou entropii pomocí aplikace Wignerovy věty.

Výsledkem bude přehledné pojednání obsahující detailní analýzu uvedeného výsledku a jeho důsledků, které může sloužit i jako učební materiál pro studenty.

Seznam odborné literatury:

[1] J. Hamhalter: Quantum Measure Theory. Kluwer Academic, Dordrecht, Boston, (2003).
[2] M. Bohata: Technique of Operator Algebras in Quantum Structures. Doctoral Thesis, 2012).
[3] L. Molnar: Maps on states preserving the relative entropy. J. Math. Phys., 49, 032114(2008)
[4] L. Molnar, P. Szokol: Maps on states preserving the relative entropy II. Linear Algebra and its Applications, 432, (2010), 3343-3350.
[5] M. A. Nielsen and I. Chuang: Quantum Computation and Quantum Information. Cambridge University Press, 2001.

Vedoucí bakalářské práce: prof. RNDr. Jan Hamhalter, CSc.

Platnost zadání: do konce zimního semestru 2013/2014

prof. Ing. Vladimír Mařík, DrSc.
vedoucí katedry

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 10. 1. 2013

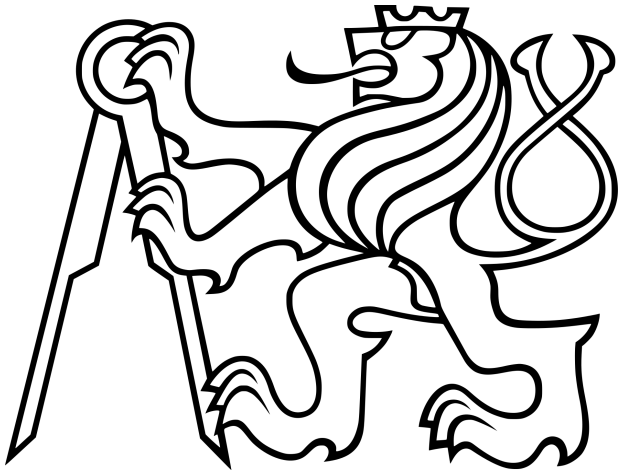
Prohlášení autora práce

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informač
zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských
závěrečných prací.

V Praze dne 23. 5. 2013 ..... Jaroslava Bankeová .....

Podpis autora práce

České vysoké učení technické
Fakulta elektrotechnická
Katedra kybernetiky



Bakalářská práce

Kvantová entropie a její zachování

Autor:
Jáchym Barvínek

Vedoucí:
prof. RNDr. Jan Hamhalter, CSc.

18. května 2013

Anotace Práce je úvodem do problematiky kvantové entropie, zejména vzájemné kvantové entropie. Je koncipována tak, aby byla přístupná čtenáři, který má pouze základní znalosti z lineární algebry a teorie pravděpodobnosti. V první polovině práce je podrobně rozebrán matematický aparát, důležitý pro tento aspekt kvantové teorie informace, včetně původního důkazu charakterizace Jordanových izomorfismů, jíž je dále využito pro důkaz Wignerovy věty. Tyto výsledky jsou pak aplikovány v důkazu charakterizace zobrazení zachovávajících vzájemnou kvantovou entropii. Navíc, pro lepší pochopení, je vysvětlena provázanost těchto matematických prostředků s formulací fyzikálních problémů.

Abstract This bachelor's thesis is an introductory text to quantum entropy, especially quantum relative entropy. It's suited to any reader, who has basic knowledge of linear algebra and probability theory. In the first half of this report, the mathematical apparatus important for this aspect of quantum information theory is thoroughly discussed. It includes an original proof of the characterization of Jordan isomorphisms, which is later used to prove Wigner's theorem. These results are then applied to characterization of quantum relative entropy preservers. Besides that, the connections between these mathematical tools and formulation of physical problems is explained for better understanding.

Prohlášení autora práce Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

.....	.....
V Praze dne	Podpis autora práce

Poděkování Děkuji prof. RNDr. Janu Hamhalterovi, CSc., který mou práci vedl a bez jehož četných konzultací by nemohla vzniknout. Dále děkuji svojí matce, která mi pomohla s jazykovou stránkou práce a všem dalším z řad své rodiny a přátel, kteří mě při studiu podporovali.

Obsah

Úvod

V této práci podrobně rozebíráme základy problematiky vzájemné kvantové entropie, jednoho ze základních pojmů kvantové teorie informace. Práce je tedy střípkem do mozaiky této stále se rozvíjející teorie, která snad jednou povede ke zrodu reálně použitelné kvantové výpočetní techniky, jež je zatím omezena na oblast výzkumu. Text je sestaven tak, aby byl přístupný i čtenáři, který má pouze základní znalosti lineární algebry, matematické analýzy a teorie pravděpodobnosti – lze ho tedy použít i jako studijní materiál. V první kapitole budujeme matematický aparát používaný v jisté části kvantové teorie, jedná se především o teorii Hilbertových prostorů konečné dimenze a operátorů mezi nimi. Druhá kapitola se zabývá Jordanovými $*$-izomorfismy. Po objasnění jejich základních vlastností je rozpracován důkaz jejich charakterizace. Tento důkaz je původní, vznikl nově jako součást této práce, a je elementární, tedy využívá jen zde uvedených matematických nástrojů. Věta charakterizující Jordanovy $*$-izomorfismy je obvykle dokazována obecněji (zejména se dokazuje pro nekonečnou dimenzi), ale je k tomu potřeba mnohem pokročilejšího aparátu. V další kapitole shrneme ty části matematické formulace kvantové teorie, které jsou užitečné pro hlubší pochopení problematiky kvantové entropie. Dokážeme dále Wignerovu větu o symetriích, jeden ze základních principů kvantové teorie, jakožto poměrně snadný důsledek výsledků z druhé kapitoly. Nejsme sami, kdo se o elementární důkaz Wignerovy věty pokouší. Původně jsme namísto charakterizace Jordanových $*$-izomorfismů zvažovali zařadit podrobné rozpracování důkazu uvedeného v článku [10]. Ovšem jeho podrobnou analýzou jsme došli k závěru, že obsahuje chybu. Ve čtvrté kapitole se konečně věnujeme kvantové entropii a zejména vzájemné kvantové entropii. Uvedeme jejich analogie v klasické teorii informace. Ty jsou speciálním případem těch kvantových, ale zavedeme je i pomocí kvantového formalismu. Přechod od klasické teorie informace ke kvantové je pak hladký. Rozebereme vlastnosti vzájemné kvantové entropie a za použití Wignerovy věty charakterizujeme zobrazení, která tuto veličinu zachovají jako unitární či antiunitární transformace – dobrat se tohoto výsledku elementárními metodami je cílem této práce. V závěru zmíníme některé důsledky a nastíníme další možnosti zkoumání v této oblasti.

Kapitola 1

Základní matematický aparát

V této úvodní kapitole zformulujeme základní pojmy a věty především z teorie Hilbertových prostorů a teorie operátorů, se kterými budeme dále pracovat. U čtenáře předpokládáme základní znalosti lineární algebry. V případech, kdy používáme zde nedefinované pojmy, se odvoláváme na standardní učebnice, jakou je například [8]. Ve stručnosti jsou důležité aspekty lineární algebry shrnuty i v publikaci [7], která tématicky více souvisí s touto prací. Relevantní matematická témata jsou též rozebírána v [12].

1.1 Značení

Přehled použitých značek, které nejsou v textu definovány.

$\mathbb{Z}, \mathbb{R}, \mathbb{C}$	Množina celých, resp. reálných resp. komplexních čísel.
$\mathbb{R}^n, \mathbb{C}^n$	Množina n-tic reálných resp. komplexních čísel.
$\mathbb{C}^{n\times m}$	Množina matic komplexních čísel rozměrů $n \times m$.
0	Podle kontextu číslo nula nebo nulový vektor.
$\mathbf{1}$	Identita – jednotková matice.
$\mathbf{0}$	lineární zobrazení na $\{0\}$ – nulová matice.
$\operatorname{Span} A$	Lineární obal množiny A.
$\operatorname{Ker} A$	Jádro lineárního zobrazení A.
$\operatorname{Range} A$	Obraz lineárního zobrazení A.
$\dim \mathcal{M}$	Dimenze lineárního prostoru $\mathcal{M}$.
$\imath$	Imaginární jednotka.
$\overline{x}$	Komplexně sdružené číslo k x, příp. vektor či matice (po složkách).
$\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$	Diagonální matice: pro $\operatorname{diag}(\lambda_1, \ldots, \lambda_n) = (a_{ij})$ je $(a_{ii}) = \lambda_i$, 0 jinak.
δ_{ij}	Kroneckerovo delta. $\delta_{ij} = 1$ když $i = j$, 0 jinak.
2^Ω	Potenční množina množiny Ω.
χ_M	Charakteristická funkce množiny M: $\chi_M(x) = 1$ když $x \in M$, 0 jinak.

1.2 Hilbertovy prostory

Při sestavování této sekce bylo čerpáno z [4]. Obsáhlejší výklad teorie Hilbertových prostorů je možné nalézt například v učebnici [9].

Definice 1.2.1. *Skalárním součinem* na vektorovém prostoru $\mathcal{V}$ nad tělesem $\mathbb{C}$ nazveme takové zobrazení $\langle \cdot, \cdot \rangle : \mathcal{V} \times \mathcal{V} \to \mathbb{C}$, které splňuje následující požadavky pro všechny vektory $x, y, z \in \mathcal{V}$ a skalár $\alpha \in \mathbb{C}$:

(a) $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$.

(b) $\langle \alpha x, y \rangle = \alpha \langle x, y \rangle$.

(c) $\langle x, y \rangle = \overline{\langle y, x \rangle}$.

(d) $\langle x, x \rangle \geq 0$ a rovnost nastává právě když $x = 0$.

O vektorech x, y říkáme, že jsou *ortogonální*, jestliže $\langle x, y \rangle = 0$, značeno $x \perp y$. *Norma indukovaná skalárním součinem* je definována takto: $\|x\| = \sqrt{\langle x, x \rangle}$. Vektor s normou 1 nazýváme *jednotkovým*.

Poznámka 1.2.2. Zbrazení $\|\cdot\| : x \mapsto \sqrt{\langle x, x \rangle}$ skutečně splňuje axiomy normy. Nezápornost, tedy to, že $\|x\| \geq 0$ pro všechna $x \in \mathcal{V}$ s rovností nastávající právě pro $x = 0$, snadno plyne z vlastnosti skalárního součinu (d). Homogenita, tedy že $\|\alpha x\| = |\alpha| \cdot \|x\|$ pro všechna $x \in \mathcal{V}, \alpha \in \mathbb{C}$ plyne z vlastností (b),(c). Trojúhelníková nerovnost též platí, ale nebudeme ji potřebovat, takže důkaz vynecháme.

Definice 1.2.3. *Komplexní Hilbertův prostor* (dále jen *Hilbertův prostor*) je vektorový prostor nad tělesem $\mathbb{C}$ se skalárním součinem, který je *úplný*. Úplností rozumíme to, že každá cauchyovská posloupnost má limitu v tomto prostoru (v normě indukovanou jeho skalárním součinem). *Podprostor* Hilbertova prostoru je nějaká jeho podmnožina, která je sama Hilbertovým prostorem.

Věta 1.2.4 (Pythagorova)**.** *Jsou-li vektory x, y z téhož Hilbertova prostoru ortogonální, pak:*

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2.$$

Důkaz.

$$\|x + y\|^2 = \langle x + y, x + y \rangle = \langle x, x \rangle + \underbrace{\langle y, x \rangle}_{=0} + \underbrace{\langle x, y \rangle}_{=0} + \langle y, y \rangle = \|x\|^2 + \|y\|^2. \qquad \square$$

Věta 1.2.5 (Cauchyho-Schwarzova nerovnost)**.** *Pro každé dva vektory x, y z téhož Hilbertova prostoru platí:*

$$|\langle x, y \rangle| \leq \|x\| \cdot \|y\|,$$

navíc rovnost nastává právě když x a y jsou lineárně závislé.

Důkaz. Pro $y = 0$ platí triviálně, nechť tedy dále $y \neq 0$. Označme:

$$z \ = x - \frac{\langle x, y\rangle}{\langle y, y\rangle} y. \tag{1.1}$$

Ukážeme, že $z \perp y$:

$$\langle z, y\rangle = \left\langle x - \frac{\langle x, y\rangle}{\langle y, y\rangle} y, y \right\rangle = \langle x, y\rangle - \frac{\langle x, y\rangle}{\langle y, y\rangle} \langle y, y\rangle = \langle x, y\rangle - \langle x, y\rangle = 0.$$

Snadnou úpravou (1.1) dostaneme rozklad x na ortogonální složky:

$$x = \frac{\langle x, y\rangle}{\langle y, y\rangle} y + z, \tag{1.2}$$

na nějž aplikujeme Pythagorovu větu 1.2.4:

$$\|x\|^2 = \left|\frac{\langle x, y\rangle}{\langle y, y\rangle}\right|^2 \|y\|^2 + \|z\|^2 = \frac{|\langle x, y\rangle|^2}{\|y\|^2} + \|z\|^2 \geq \frac{|\langle x, y\rangle|^2}{\|y\|^2}.$$

Vynásobíme-li tuto nerovnici výrazem $\|y\|^2$, obdržíme požadovanou nerovnost. Rovnost navíc může být splněna pouze když $\|z\|^2 = 0$, tedy $z = 0$. Ze vztahu (1.2) je pak snadno vidět, že $z = 0$ implikuje lineární závislost x, y. □

Tvrzení 1.2.6 (Polarizační identita)**.** *Jestliže zobrazení $T : \mathcal{V} \times \mathcal{V} \to \mathbb{C}$ splňuje pro všechna $x, y, z \in \mathcal{V}, \alpha \in \mathbb{C}$:*

- $T(x + y, z) = T(x, z) + T(y, z)$ *a také* $T(x, y + z) = T(x, y) + T(x, z)$.
- $T(\alpha x, y) = \alpha T(x, y)$ *a také* $T(x, \alpha y) = \overline{\alpha} T(x, y)$

pak pro všechna $x, y \in \mathcal{V}$ platí:

$$4T(x, y) = T(x + y, x + y) - T(x - y, x - y) + \imath(T(x + \imath y, x + \imath y) - T(x - \imath y, x - \imath y)).$$

Důkaz. Výrazy na pravé straně podle pravidel v předpokladech přepíšeme na takovou kombinaci, která v parametrech T obsahuje pouze samotné vektory x a y. Její součet dá požadovaný výsledek. □

Poznámka 1.2.7. Toto tvrzení obecně neplatí v reálném prostoru!

Definice 1.2.8. Nechť je $\mathcal{M}$ podprostor $\mathcal{H}$. Pak označíme $\mathcal{M}^\perp = \{x \in \mathcal{H} | y \perp m \ \forall m \in \mathcal{M}\}$.

Definice 1.2.9. Nechť je $\mathcal{H}$ Hilbertův prostor a $M \subseteq \mathcal{H}$. Bod $x_0 \in M$ je *nejbližším bodem* bodu $x \in \mathcal{H}$ z množiny M, jestliže:

$$\|x - x_0\| = \inf\{\|x - y\| | y \in M\}.$$

Poznámka 1.2.10. Nejbližší bod obecně nemusí existovat, může být právě jeden, nebo jich může být více, a to i nekonečně mnoho.

Věta 1.2.11. *Nechť je K uzavřená konvexní množina v Hilbertově prostoru $\mathcal{H}$. Ke každému bodu $h \in \mathcal{H}$ existuje jediný nejbližší bod z množiny K.*

Bez důkazu. Viz [4].

Poznámka 1.2.12. Každý Hilbertův prostor dimenze n je izomorfní s vektorovým prostorem $\mathbb{C}^n$, v němž jsou požadavky úplnosti a separability automaticky splněny. Standardní skalární součin je:

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_i}, \text{ kde } x, y \in \mathbb{C}^n.$$

Poznámka 1.2.13. Uvedená definice Hilbertova prostoru i výše zmíněné výsledky jsou obecné a vztahují se například i na různé prostory funkcí. V tomto textu se ale dále budeme zabývat jen Hilbertovými prostory konečné dimenze, tedy $\mathbb{C}^n$. Pokud to ale nebude zbytečnou komplikací, budeme se snažit držet obecného formalismu.

Věta 1.2.14. *Nechť $\mathcal{M}$ je podprostor Hilbertova prostoru $\mathbb{C}^n$ a $x \in \mathbb{C}^n$. Bod $x_0 \in \mathcal{M}$ je nejbližším bodem z množiny $\mathcal{M}$ k bodu x právě když $x - x_0 \in \mathcal{M}^\perp$.*

Bez důkazu. Viz [4].

Definice 1.2.15. Řekneme, že podprostory $\mathcal{H}_1, \mathcal{H}_2$ Hilbertova prostoru $\mathbb{C}^n$ tvoří *ortogonální rozklad*, což značíme $\mathbb{C}^n = \mathcal{H}_1 \oplus \mathcal{H}_2$, když:

(a) $\mathcal{H}_1$ a $\mathcal{H}_2$ jsou vzájemně ortogonální.

(b) $\mathbb{C}^n = \mathrm{Span}(\mathcal{H}_1 \cup \mathcal{H}_2)$.

Věta 1.2.16 (Projekční věta)**.** *Je-li $\mathcal{M}$ podprostor Hilbertova prostoru $\mathbb{C}^n$, pak:*

$$\mathbb{C}^n = \mathcal{M} \oplus \mathcal{M}^\perp.$$

Důkaz. Vyjádřeme $x \in \mathbb{C}^n$ takto: $x = x_0 + (x - x_0)$, kde $x_0 \in \mathcal{M}$ je nejbližším bodem k x z množiny $\mathcal{M}$. Podle věty 1.2.14 je ale $(x - x_0) \in \mathcal{M}^\perp$. Můžeme tedy každý vektor z $\mathbb{C}^n$ vyjádřit jako součet vektoru z $\mathcal{M}$ s vektorem z $\mathcal{M}^\perp$. □

Definice 1.2.17. *Ortonormální báze* Hilbertova prostoru $\mathcal{H}$ je množina $\{e_1, \ldots, e_n\}$, která splňuje:

(a) $\langle e_i, e_i \rangle = 1$, pro všechna $i = 1, \ldots, n$. Tzn. vektory báze jsou normalizované.

(b) $\langle e_i, e_j \rangle = 0$, pro všechna $i \neq j$. Tzn. vektory báze jsou vzájemně ortogonální.

To můžeme celé úsporně zapisovat pomocí Kroneckerova delta jako: $\langle e_i, e_j \rangle = \delta_{ij}$.

Standardní báze $\mathbb{C}^n$ je (ortonormální) množina:

$$\{\underbrace{(1, 0, 0, \ldots, 0)}_{n}, (0, 1, 0, \ldots, 0), (0, 0, 1, \ldots, 0), \ldots, (0, 0, 0, \ldots, 1)\}.$$

Tvrzení 1.2.18. *Nechť je $M = \{e_1, \ldots, e_n\}$ ortonormální báze Hilbertova prostoru $\mathcal{H}$. Pak pro každé $x \in \mathcal{H}$ platí:*

$$x = \sum_{i=1}^{n} \langle x, e_i \rangle \, e_i.$$

A navíc:

$$\|x\|^2 = \sum_{i=1}^{n} |\, \langle x, e_i \rangle \,|^2. \tag{1.3}$$

Důkaz. Nechť $y = \sum_{i=1}^{n} \langle x, e_i \rangle \, e_i$ pro nějaký vektor $x \in \mathcal{H}$. Výpočet

$$\langle x - y, e_i \rangle = \langle x, e_i \rangle - \left\langle \sum_{j=1}^{n} \langle x, e_j \rangle \, e_j, e_i \right\rangle = \langle x, e_i \rangle - \langle x, e_i \rangle = 0$$

ukazuje, že $(x - y) \perp e_i$ pro všechna $e_i \in M$ a tedy $(x - y) \perp \operatorname{Span} M = \mathcal{H}$. Proto musí být $x - y = 0$, tzn. $x = y$. Rovnost (1.3) pak plyne přímo z toho, jak jsme zavedli normu. □

1.3 Teorie operátorů

Definice 1.3.1. Zobrazení $A : \mathcal{H} \to \mathcal{K}$ mezi Hilbertovými prostory $\mathcal{H}, \mathcal{K}$ nazýváme *operátorem*, když je lineární, tzn. pro všechna $x, y \in \mathcal{H}, \alpha, \beta \in \mathbb{C}$ platí:

$$A(\alpha x + \beta y) = \alpha A(x) + \beta A(y).$$

Zobrazení A nazýváme *antilineárním operátorem*, když pro všechna $x, y \in \mathcal{H}, \alpha, \beta \in \mathbb{C}$ platí:

$$A(\alpha x + \beta y) = \overline{\alpha} A(x) + \overline{\beta} A(y).$$

V obou případech značíme zkráceně $A(x) = Ax$, pro $x \in \mathcal{H}$. Operátory (lineární) budeme ztotožňovat s maticemi, jež je reprezentují vůči standardní bázi.

Tvrzení 1.3.2. *Nechť $A, B : \mathcal{H} \to \mathcal{H}$ jsou operátory. Platí:*

(a) Jestliže $\langle Ax, x \rangle = 0$ pro všechna $x \in \mathcal{H}$, pak $A = \mathbf{0}$.

(b) Jestliže $\langle Ax, x \rangle = \langle Bx, x \rangle$ pro všechna $x \in \mathcal{H}$, pak $A = B$.

Důkaz.

(a) Z definice skalárního součinu plyne, že zobrazení $T : (x, y) \mapsto \langle Ax, y \rangle$ splňuje předpoklady polarizační identity 1.2.6. Podle něj je tedy $4T(x, y) = 0$ pro všechna $x, y \in \mathcal{H}$, tedy i $\langle Ax, y \rangle = 0$ pro všechna $x, y \in \mathcal{H}$, to implikuje $A = \mathbf{0}$. (Můžeme totiž volit $y = Ax$, z čehož $Ax = 0$ pro všechna x.)

(b) Danou rovnici můžeme přepsat jako $\langle (A - B)x, x \rangle = 0$. Důsledkem (a) je $A - B = \mathbf{0}$, tedy $A = B$.

□

Poznámka 1.3.3. Stejně jako polarizační identita 1.2.6 i tento jeho důsledek, Tvrzení 1.3.2, obecně platí jen v komplexním prostoru.

Tvrzení 1.3.4. *Je-li $A : \mathbb{C}^n \to \mathbb{C}^m$ operátor, pak existuje jediný operátor $B : \mathbb{C}^m \to \mathbb{C}^n$ takový, že pro všechna $x \in \mathbb{C}^n, y \in \mathbb{C}^m$ platí:*

$$\langle Ax, y\rangle = \langle x, By\rangle . \tag{1.4}$$

Důkaz. Existence: Je-li matice $A = (a_{ij})$, stačí volit $B = (\overline{a_{ji}})$ a přesvědčit se snadným výpočtem, že (1.4) platí. Jednoznačnost: Nechť existují B_1, B_2 takové, že je:

$$\langle Ax, y\rangle = \langle x, B_1 y\rangle = \langle x, B_2, y\rangle$$

pro všechna $x \in \mathbb{C}^n$. Potom ale:

$$\langle x, B_1 y - B_2 y\rangle = 0 \ \forall x \in \mathbb{C}^n \implies B_1 y - B_2 y = 0 \ \forall y \in \mathbb{C}^n \implies B_1 = B_2.$$

□

Definice 1.3.5. Jsou-li $A : \mathbb{C}^n \to \mathbb{C}^m, B : \mathbb{C}^m \to \mathbb{C}^n$ operátory splňující $\langle Ax, y\rangle = \langle x, By\rangle$ pro všechna $x \in \mathbb{C}^n, y \in \mathbb{C}^m$, pak nazveme B *adjungovaným operátorem* k A, značíme: $B = A^*$.

Poznámka 1.3.6. Všimněme si, že důkaz tvrzení je konstruktivní. Víme tedy jak matice A^* bude vypadat: Je to transponovaná, po prvcích komplexně sdružená, matice. Kvůli jednoznačnosti je tato vlastnost nutnou a postačující podmínkou pro adjungovaný operátor.

Tvrzení 1.3.7 (Základní vlastnosti adjunkce)**.** *Mějme operátory $A, B : \mathcal{H} \to \mathcal{H}$, skalár $\alpha \in \mathbb{C}$. Pak platí:*

(a) $(A^*)^* = A$,

(b) $(A + B)^* = A^* + B^*$,

(c) $(\alpha A)^* = \overline{\alpha} A^*$,

(d) $(AB)^* = B^* A^*$.

Důkaz. Snadno ověřitelné přímo z definice adjunkce. □

Definice 1.3.8. Operátor $A : \mathcal{H} \to \mathcal{H}$ nazýváme:

- *Samoadjungovaným*, když platí $A = A^*$.
- *Pozitivním* resp. *pozitivně definitním*, když platí $\langle x, Ax\rangle > 0$ pro každé $x \in \mathcal{H}, x \neq 0$. V případě neostré nerovnosti ho nazveme *pozitivně semidefinitním*.

- *Unitárním*, když platí $A^* = A^{-1}$.
- *Antiunitárním*, když je antilineární, bijektivní a platí $\langle Ax, Ay\rangle = \overline{\langle x, y\rangle}$ pro všechna $x, y \in \mathcal{H}$.

Poznámka 1.3.9. Je dobré si uvědomit, že výraz typu $\langle x, Ax\rangle$ je v konečné dimenzi vlastně kvadratickou formou proměnné x.

Definice 1.3.10. Platí-li pro operátor $A : \mathcal{H} \to \mathcal{H}$, vektor $x \in \mathcal{H}, x \neq 0$ a skalár $\lambda \in \mathbb{C}$ rovnost

$$Ax = \lambda x, \tag{1.5}$$

pak říkáme, že λ je *vlastní číslo* operátoru A a x jemu příslušný *vlastní vektor*. Množinu vlastních čísel operátoru A nazýváme jeho *spektrem*.

Poznámka 1.3.11. Uvedenou rovnici (1.5) můžeme přepsat jako $(\lambda\mathbf{1} - A)x = 0$. Ta má netriviální řešení pro x, právě když $\lambda\mathbf{1} - A$ je singulární, tj. $\det(\lambda\mathbf{1} - A) = 0$. Výraz $\det(\lambda\mathbf{1} - A)$ je polynomem proměnné λ. Hledání vlastních čísel tedy vede na úlohu hledání kořenů tohoto polynomu. U vlastních čísel tak mluvíme o *(algebraické) násobnosti* ve stejném smyslu jako u kořenů polynomu.

Tvrzení 1.3.12. *Nenulová lineární kombinace vlastních vektorů operátoru A příslušných témuž vlastnímu číslu λ, je též vlastním vektorem příslušným tomuto vlastnímu číslu.*

Důkaz. Nechť je λ vlastní číslo A a x, y vlastní vektory jemu příslušné. Pak pro $\alpha, \beta \in \mathbb{C}$ platí:

$$A(\alpha x + \beta y) = \alpha Ax + \beta Ay = \alpha\lambda x + \beta\lambda y = \lambda(\alpha x + \beta y).$$

□

Poznámka 1.3.13. Vlastní vektory příslušné témuž vlastnímu číslu tedy tvoří spolu s nulovým vektorem lineární podprostor prostoru obrazů daného operátoru.

Definice 1.3.14. *Geometrická násobnost* vlastního čísla je velikost báze podprostoru vlastních vektorů jemu příslušných.

Tvrzení 1.3.15 (Vlastnosti samoadjungovaných operátorů)**.**

(a) Množina samoadjungovaných operátorů definovaných na témže prostoru je uzavřená na lineární kombinace s reálnými koeficienty.

(b) Operátor je samoadjungovaný, právě když $\langle x, Ax\rangle \in \mathbb{R}\ \forall x \in \mathcal{H}$.

(c) Vlastní čísla samoadjungovaného operátoru jsou reálná.

Důkaz.

(a) Plyne z tvrzení 1.3.7, (b), (c).

(b) Nechť je $x \in \mathcal{H}$ libovolné. Na základě Tvrzení 1.3.2 platí:

$$A = A^* \iff \langle Ax, x\rangle = \langle x, Ax\rangle = \overline{\langle Ax, x\rangle} \iff \langle Ax, x\rangle \in \mathbb{R}.$$

(c) Nechť $A : \mathcal{H} \to \mathcal{H}$ je samoadjungovaný operátor, x je vlastní vektor A a λ jemu příslušné vlastní číslo. Z (b) plyne:

$$\underbrace{\langle Ax, x\rangle}_{\in\mathbb{R}} = \langle \lambda x, x\rangle = \lambda \underbrace{\langle x, x\rangle}_{\in\mathbb{R}}.$$

Takže λ musí být také z $\mathbb{R}$. □

Důsledek 1.3.16. *Množina pozitivních (resp. pozitivně semidefinitních) operátorů je podmnožinu samoadjungovaných operátorů na tomtéž prostoru.*

Tvrzení 1.3.17 (Vlastnosti pozitivních operátorů)**.**

(a) Vlastní čísla pozitivních (resp. pozitivně semidefinitních) operátorů jsou kladná (resp. nezáporná).

(b) Jsou-li $A, B : \mathcal{H} \to \mathcal{H}$ pozitivní operátory, pak ABA je pozitivní operátor.

Důkaz.

(a) Stejným způsobem jako pro samoadjungované (viz důkaz 1.3.15 (c)), jen místo $\mathbb{R}$ volíme interval $(0, \infty)$ resp. $\langle 0, \infty)$.

(b) Označme $y = Ax$. S využitím 1.3.16 pro všechna $x \in \mathcal{H}$ platí:

$$\langle x, ABAx\rangle = \langle A^*x, BAx\rangle = \langle Ax, BAx\rangle = \langle y, By\rangle > 0.$$ □

Tvrzení 1.3.18 (Vlastnosti unitárních operátorů)**.** *Následující tvrzení jsou ekvivalentní:*

(a) Operátor $U : \mathcal{H} \to \mathcal{H}$ je unitární.

(b) U je bijektivní a platí $\langle Ux, Uy\rangle = \langle x, y\rangle$ pro všechna $x, y \in \mathcal{H}$.

(c) Sloupce matice U tvoří ortonormální bázi $\mathcal{H}$.

Důkaz.

- (a) $\implies$ (b): U je unitární, tedy $U^*Ux = x$ pro všechna $x \in \mathcal{H}$. Tedy:

$$\langle x, y\rangle = \langle U^*Ux, y\rangle = \langle Ux, Uy\rangle.$$

- (b) $\implies$ (c): Nechť je $\{e_1, \ldots, e_n\}$ standardní báze. Vyjádřeme i-tý sloupec s_i matice U jako $s_i = Ue_i$. Protože je U bijektivní, jsou všechna s_i různá. A jelikož podle předpokladu (b) musí U zachovat vzájemnou ortogonalitu i normu, bude $\{s_1, \ldots, s_n\}$ ortonormální báze.

- (c) $\implies$ (a): Označme s_i i-tý sloupec matice U.

  Protože sloupce tvoří ortonormální bázi, je $\langle s_i, s_j \rangle = \delta_{ij}$. Tedy můžeme pro všechny sloupce zároveň zapsat jako: $U^*U = \mathbf{1}$. Protože jsou sloupce lineárně nezávislé, je U invertibilní a po vynásobení poslední rovnice U^{-1} zprava obdržíme $U^* = U^{-1}$.

□

Tvrzení 1.3.19. *Složení unitárního operátoru s unitárním, resp. antiunitárním operátorem je unitární, resp. antiunitární operátor.*

Důkaz. Snadno ověřitelné přímo z definice antiunitárního operátoru a předchozí charkterizace unitárních operátorů 1.3.18(b). □

Definice 1.3.20. *Stopa* čtvercové matice $(a_{ij}) = A \in \mathbb{C}^{n\times n}$, značeno $\operatorname{Tr} A$, je součet prvků na její diagonále. Formálně: $\operatorname{Tr} A = \sum_{i=1}^{n} a_{ii}$.

Tvrzení 1.3.21 (Vlastnosti stopy)**.**

(a) $\operatorname{Tr}(\alpha A + \beta B) = \alpha \operatorname{Tr} A + \beta \operatorname{Tr} B$*, pro všechny* $A, B \in \mathbb{C}^{n\times n}, \alpha, \beta \in \mathbb{C}$. *(Linearita)*

(b) $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$*, pro všechny* $A \in \mathbb{C}^{m\times n}, B \in \mathbb{C}^{n\times m}$. *(Cykličnost)*

Důkaz. Budiž $A = (a_{ij}), B = (b_{ij})$ matice uvedených rozměrů.

(a) $\operatorname{Tr}(\alpha A + \beta B) = \sum_{i=1}^{n} \alpha a_{ii} + \beta b_{ii} = (\alpha \sum_{i=1}^{n} a_{ii}) + (\beta \sum_{i=1}^{n} b_{ii}) = \alpha \operatorname{Tr} A + \beta \operatorname{Tr} B$.

(b) $\operatorname{Tr}(AB) = \sum_{i=1}^{n} \sum_{k=1}^{n} a_{ik} b_{ki} = \sum_{k=1}^{n} \sum_{i=1}^{n} b_{ik} a_{ki} = \operatorname{Tr}(BA)$. □

Tvrzení 1.3.22. *Stopa operátoru je součtem jeho vlastních čísel (každé je započteno tolikrát, jaká je jeho násobnost).*

Důkaz. Vlastní čísla $A \in \mathbb{C}^{n\times n}$ jsou kořeny polynomu $\det(\lambda\mathbf{1} - A) = 0$. Determinant je součet jistých součinů. Podívejme se na koeficient u λ^{n-1}, ten lze najít jedině v součinu prvků na diagonále: $(\lambda - a_{11})(\lambda - a_{22}) \dots (\lambda - a_{nn})$. Po roznásobení zjistíme, že to bude $a_{11} + a_{22} + \cdots + a_{nn} = \operatorname{Tr} A$. (Koeficient u λ^n je 1.) Rozklad charakteristického polynomu na kořenové činitele zapíšeme jako: $(\lambda - \lambda_1)(\lambda - \lambda_2) \dots (\lambda - \lambda_n)$. Koeficient u λ^{n-1} zde bude $\lambda_1 + \lambda_2 + \cdots + \lambda_n$. Odtud máme $\operatorname{Tr} A = \lambda_1 + \lambda_2 + \cdots + \lambda_n$. □

Věta 1.3.23 (O spektrálním rozkladu)**.** *Pokud operátor* $A : \mathcal{H} \to \mathcal{H}$ *komutuje se svou adjunkcí, tj. platí pro něj* $AA^* = A^*A$ *(je tzv.* normální*), pak lze sestavit ortonormální bázi* $\mathcal{H}$ *z jeho vlastních vektorů.*

Bez důkazu. Viz [12].

Důsledek 1.3.24. *Každý normální operátor* $A : \mathbb{C}^n \to \mathbb{C}^n$ *s vlastními čísly* $\lambda_1, \dots, \lambda_k$ *(každé tolikrát, kolik je jeho násobnost) lze psát ve tvaru:*

$$A = UDU^{-1}, \text{ kde } D = \operatorname{diag}(\lambda_1, \dots, \lambda_k), U \text{ je unitární.}$$

Důkaz. Volme za sloupce matice U prvky ortonormální báze $\mathbb{C}^n$ složené z vlastních vektorů matice A. Ověříme, že taková matice U je právě ona požadovaná. U je unitární díky Tvrzení 1.3.18. Rovnost $A = UDU^{-1}$ je ekvivalentní $AU = DU$. Z linearity stačí ověřit, že platí $AUe_i = DUe_i$ pro všechna e_i ze standardní báze $\mathbb{C}^n$. Označme s_i i-tý sloupec U a λ_i vlastní číslo A příslušné s_i. Je $Ue_i = s_i$ a $AUe_i = As_i = \lambda_i s_i$, protože s_i je vlastní vektor A. Dále snadno vidíme, že $De_i = \lambda e_i$ a tedy $UDe_i = \lambda_i Ue_i = \lambda_i s_i$, což jsme chtěli. □

Poznámka 1.3.25. Důležitou skupinou normálních operátorů, pro které budeme spektrální věty využívat, jsou operátory samoadjungované. (Platí $AA^* = AA = A^*A$.) Normální jsou též operátory unitární. (Platí $UU^* = UU^{-1} = \mathbf{1} = U^{-1}U = U^*U$.)

Definice 1.3.26. *Ortogonální projekce*, též *projektor* na podprostor $\mathcal{M}$ Hilbertova prostoru $\mathcal{H}$ je zobrazení $P_\mathcal{M} : \mathcal{H} \to \mathcal{M}$, které každému bodu z $\mathcal{H}$ přiřadí nejbližší bod v $\mathcal{M}$. Důležitý speciální případ, kdy je $\mathcal{M} = \mathrm{Span}\{e\}$ značíme stručně P_e. Říkáme, že projektory $P_\mathcal{M}, P_\mathcal{N}$ jsou vzájemně ortogonální, pokud $\mathcal{M} \perp \mathcal{N}$. Množinu všech projektorů na podprostor dimenze k v Hilbertově prostoru $\mathbb{C}^n$ značíme: $\mathcal{P}_k(\mathbb{C}^n)$.

Tvrzení 1.3.27. *Projektory jsou lineární operátory.*

Důkaz. Budiž $x, y \in \mathcal{H}$ a $P_\mathcal{M} : \mathcal{H} \to \mathcal{M}$ projektor. Označme $x = x_\mathcal{M} + x_{\mathcal{M}^\perp}, y = y_\mathcal{M} + y_{\mathcal{M}^\perp}$, kde $x_\mathcal{M}, y_\mathcal{M} \in \mathcal{M}, x_{\mathcal{M}^\perp}, y_{\mathcal{M}^\perp} \in \mathcal{M}^\perp$. Z věty 1.2.14 plyne:

$$P_\mathcal{M}(x + y) = x_\mathcal{M} + y_\mathcal{M} = P_\mathcal{M}(x) + P_\mathcal{M}(y).$$

A při vynásobení x nebo y komplexním číslem se nic nezmění. □

Důsledek 1.3.28. *Hodnost projektoru $P_\mathcal{M}$ je* $\dim \mathcal{M}$.

Tvrzení 1.3.29. *Je-li $\{e_1, \ldots, e_k\}$ ortonormální báze $\mathcal{M}$ a $P_\mathcal{M} : \mathcal{H} \to \mathcal{M}$ projektor, pak platí:*

$$P_\mathcal{M}(x) = \sum_{i=1}^{k} \langle x, e_i \rangle \, e_i. \tag{1.6}$$

Důkaz. Pro $x \in \mathcal{H}$ označme $\sum_{i=1}^{k} \langle x, e_i \rangle \, e_i = y$. Podle věty 1.2.14 nám stačí ověřit, zda $x - y \perp \mathcal{M}$. To platí, právě když $x - y \perp e_i$ pro každé e_i. Je:

$$\langle x - y, e_i \rangle = \langle x, e_i \rangle - \langle y, e_i \rangle = \langle x, e_i \rangle - \left\langle \sum_{j=1}^{k} \langle x, e_j \rangle \, e_j, e_i \right\rangle = \langle x, e_i \rangle - \sum_{j=1}^{k} \langle x, e_j \rangle \underbrace{\langle e_j, e_i \rangle}_{=\delta ji} =$$

$$= \langle x, e_i \rangle - \langle x, e_i \rangle = 0.$$

□

Poznámka 1.3.30. Odvodíme maticovou reprezentaci projektorů. Nejprve jen pro projektor $P_e : \mathbb{C}^n \to \mathbb{C}^n$ na podprostor dimenze 1, daný jednotkovým vektorem $e = (e_1, ..., e_n)$. Pro vektor $x = (x_1, \ldots, x_n)$ bude:

$$P_e x = \langle x, e \rangle \, e = \left(\sum_{i=1}^{n} x_i \overline{e_i} \right) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} (\sum_{i=1}^{n} x_i \overline{e_i}) \, e_1 \\ \vdots \\ (\sum_{i=1}^{n} x_i \overline{e_i}) \, e_n \end{pmatrix} = \sum_{i=1}^{n} \begin{pmatrix} \overline{e_i} e_1 \\ \vdots \\ \overline{e_i} e_n \end{pmatrix} x_i =$$

$$= \begin{pmatrix} e_1\overline{e_1} & \cdots & e_1\overline{e_n} \\ \vdots & \ddots & \vdots \\ e_n\overline{e_1} & \cdots & e_n\overline{e_n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Je tedy P_e reprezentován maticí $(e_i\overline{e_j})$. Projektor na podprostor $\mathcal{M}$ pak napíšeme jednoduše jako sumu projektorů na jednodimenzionální podprostory dané prvky nějaké ortonormální báze $\mathcal{M}$.

Tvrzení 1.3.31 (Vlastnosti projektorů)**.** *Nechť je $P_\mathcal{M} : \mathbb{C}^n \to \mathcal{M}$.*

(a) Prvky $\mathcal{M}$ jsou vlastní vektory $P_\mathcal{M}$ příslušné vlastnímu číslu 1 násobnosti k. Prvky $\mathcal{M}^\perp$ jsou vlastní vektory $P_\mathcal{M}$ příslušné vlastnímu číslu 0 násobnosti $n - k$. Jiné vlastní vektory $P_\mathcal{M}$ nemá.

(b) Nechť jsou P_e, P_f projektory na jednodimenzionální podprostory. Pak bude platit, že: $\mathrm{Tr}(P_e P_f) = |\langle e, f \rangle|^2$.

Důkaz. Nechť je $M = \{e_1, \ldots, e_k\}$ ortonormální báze $\mathcal{M}$ a $P_\mathcal{M} : \mathbb{C}^n \to \mathcal{M}$ projektor.

(a) Pro všechna $e_j \in M$ platí:

$$P_\mathcal{M} e_j = \sum_{i=1}^{k} \langle e_j, e_i \rangle \, e_i = \sum_{i=1}^{k} \delta_{ji} e_j = 1 e_j.$$

e_j je tedy vlastní vektor s vlastním číslem 1. Podle tvrzení 1.3.12 jsou pak vlastními vektory všechny prvky $\mathcal{M}$.

Pro $f \in M^\perp$ je výraz $\langle f, e_i \rangle$ vždy nulový, tedy: $P_\mathcal{M} f = 0 = 0f$, proto je f vlastní vektor příslušný nule. Podle projekční věty 1.2.16 žádné jiné vlastní vektory nejsou.

Z toho ihned plyne, že geometrická násobnost vlastního čísla 1 resp. 0 je k resp. $n-k$. To platí i pro algebraickou násobnost, což ukážeme sporem: Nechť algebraická násobnost vlastního čísla 1 je $c \neq k$. Uvažujme dle 1.3.24 diagonalizaci $P = UDU^{-1}$. D má na diagonále c jedniček a všude jinde nuly; U, U^{-1} jsou regulární. Hodnost celého součinu je tedy c. Ale z definice projektoru vyplývá, že jeho hodnost musí být $\dim \mathcal{M} = k$, což je spor.

(b) Ověříme výpočtem:

$$\begin{aligned}\operatorname{Tr}(P_e P_f) &= \sum_{i=1}^{n} \underbrace{\sum_{j=1}^{n} e_i \overline{e_j} f_j \overline{f_i}}_{=(P_e P_f)_{ii}} = \sum_{i=1}^{n} e_i \overline{f_i} \sum_{j=1}^{n} \overline{e_j} f_j = \sum_{i=1}^{n} e_i \overline{f_i} \langle e, f \rangle = \\ &= \langle f, e \rangle \langle e, f \rangle = |\langle e, f \rangle|^2.\end{aligned}$$

□

Tvrzení 1.3.32. *Operátor P je projektor právě když platí $P = P^* = P^2$.*

Důkaz. Nechť je nejprve P projektor. Skutečnost, že P je samoadjungovaný, tedy $P = P^*$, vidíme z jeho maticové reprezentace. $P = P^2$ protože každý prvek z oboru hodnot je vlastním vektorem příslušným vlastnímu číslu 1, tzn.: $P^2 x = P(Px) = 1(Px) = Px$.

Nechť nyní $P : \mathcal{H} \to \mathcal{H}$ je operátor a platí: $P = P^* = P^2$. Potřebujeme ukázat, že $(x - Px) \perp \operatorname{Range} P$ pro všechna $x \in \mathcal{H}$, neboli že $\langle x - Px, Py \rangle = 0$ pro všechna $x, y \in \mathcal{H}$. Za daných předpokladů platí:

$$\begin{aligned}\langle x - Px, Py \rangle &= \langle P^*(x - Px), y \rangle = \langle P(x - Px), y \rangle = \left\langle Px - P^2 x, y \right\rangle = \\ &= \langle Px - Px, y \rangle = \langle 0, y \rangle = 0.\end{aligned}$$

□

Důsledek 1.3.33. *Projektory jsou pozitivně semidefinitní operátory.*

Důkaz. Pro projektor P platí:

$$\langle x, Px \rangle = \left\langle x, P^2 x \right\rangle = \langle x, P^* Px \rangle = \langle Px, Px \rangle \geq 0.$$

□

Věta 1.3.34. *Je-li $A : \mathcal{H} \to \mathcal{H}$ normální operátor a $P_1, \ldots, P_k$ projektory na podprostory jeho vlastních vektorů příslušných (ve stejném pořadí) jeho vlastním číslům $\lambda_1, \ldots, \lambda_k$, pak platí:*

$$\mathbf{1} = P_1 + \cdots + P_k \tag{1.7}$$

a zároveň

$$A = \lambda_1 P_1 + \cdots + \lambda_k P_k. \tag{1.8}$$

Důkaz. Označme D_i diagonální matici, která má na diagonále jedničku tolikrát, kolik je násobnost λ_i, jinde nuly. (Je to vlastně projektor na nějaký lineární obal prvků standardní báze.) Podle 1.3.24 uvažujme rozklad $A = UDU^{-1}$. Zřejmě existují vhodná D_i (taková, že různá D_i, D_j nemají jedničku na stejné pozici diagonály), aby bylo:

$$A = UDU^{-1} = A = U(\lambda_1 D_1 + \cdots + \lambda_k D_k)U^{-1} = \lambda_1 U D_1 U^{-1} + \cdots + \lambda_k U D_k U^{-1}.$$

Lehce se dle 1.3.32 přesvědčíme, že UD_iU^{-1} je projektor:

$$\begin{aligned}(UD_iU^{-1})^* =&(U^{-1})^*D_i^*U^* = UD_iU^{-1}\\ (UD_iU^{-1})^2 =&UD_iU^{-1}UD_iU^{-1} = UD_i^2U^{-1} = UD_iU^{-1}.\end{aligned}$$

Vztah (1.7) dostaneme navíc z toho, že $\sum_{i=1}^{k} D_i = \mathbf{1}$. □

Tvrzení 1.3.35. *Pro operátor $A : \mathbb{C}^n \to \mathbb{C}^n$ platí:* $\operatorname{Range} A^* = (\operatorname{Ker} A)^\perp$.

Důkaz. Dokážeme že $(\operatorname{Range} A^*)^\perp = \operatorname{Ker} A$, což je ekvivalentní. Platí:

$$\begin{aligned}x \perp \operatorname{Range} A^* &\iff \langle x, A^*y\rangle = 0 \ \forall y \in \mathbb{C}^n\\ &\iff \langle Ax, y\rangle = 0 \ \forall y \in \mathbb{C}^n\\ &\iff Ax = 0 \iff x \in \operatorname{Ker} A.\end{aligned}$$

□

Definice 1.3.36. *Nosič* operátoru $A : \mathcal{H} \to \mathcal{H}$, značen $\operatorname{Supp} A$ je definován takto:

$$\operatorname{Supp} A \ = \operatorname{Range} A^* = (\operatorname{Ker} A)^\perp.$$

Poznámka 1.3.37. Nosič budeme používat pro pozitivně semidefinitní operátory. Pro pozitivní operátor A platí $\operatorname{Supp} A = \operatorname{Range} A$. Nemuseli bychom pojem nosiče ani zavádět, ale v tomto odvětví matematiky se tradičně používá, budeme se toho tedy držet. Podstatné je vědět, že obraz pozitivně semidefinitního operátoru je ortogonální k jeho jádru.

Definice 1.3.38. Nechť je A pozitivní matice a $A = U \operatorname{diag}(\lambda_1, \ldots, \lambda_k)U^{-1}$ její rozklad podle 1.3.24. Pak definujeme logaritmus A takto:

$$\log A \ = U \operatorname{diag}(\log \lambda_1, \ldots, \log \lambda_k)U^{-1},$$

což je totéž jako:

$$\log A \ = \log(\lambda_i)P_i + \cdots + \log(\lambda_k)P_k, \tag{1.9}$$

kde P_i je projektor na podprostor vlastních vektorů A příslušných vlastnímu číslu λ_i.

Obdobně definujeme odmocninu pozitivně semidefinitní matice A takto:

$$A^{\frac{1}{2}} \ = U \operatorname{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_k})U^{-1},$$

což je totéž jako:

$$A^{\frac{1}{2}} \ = \sqrt{\lambda_i}P_i + \cdots + \sqrt{\lambda_k}P_k.$$

Poznámka 1.3.39. Je-li A pozitivně semidefinitní, pak logaritmus nemá smysl (nelze zlogaritmovat nulové vlastní číslo). V takovém případě ale můžeme zúžit definiční obor A na $\operatorname{Supp} A$. Na tomto prostoru bude $\log A$ definován.

Kapitola 2

Jordanovy izomorfismy mezi maticovými algebrami

V této kapitole rozebíráme vlastnosti Jordanových izomorfismů, operací zachovávajících důležité vlastnosti maticových algeber: algebraických struktur s operací mocnění (zde ve smyslu běžného násobení matic) a involutivní operace (uvažujeme adjunkci). V závěru kapitoly tyto izomorfismy jednoznačně charakterizujeme. Toho později využijeme i pro charakterizaci dalších typů zobrazení.

2.1 Základní pojmy

Definice 2.1.1. *Komutátor* dvou operátorů $A, B : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ je výraz: $AB - BA$, značíme: $AB - BA = [A, B]$.

Tvrzení 2.1.2 (Vlastnosti komutátoru)**.**

(a) Operátory A, B komutují právě když $[A, B] = \mathbf{0}$.

(b) $[A, B] = -[B, A]$.

(c) $[[A, B], C] + [[B, C], A] + [[C, A], B] = \mathbf{0}$. *(Jacobiho identita)*

Důkaz. Ověřitelné přímo z definice. □

Definice 2.1.3. Zobrazení $\varphi : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ nazveme *Jordanovým $*$-izomorfismem* pokud:

(a) φ je izomorfismus (lineární bijektivní zobrazení) mezi lineárními prostory operátorů.

(b) $\varphi(A^2) = \varphi(A)^2$ pro všechna $A \in \mathbb{C}^{n\times n}$. *(Zachování mocniny)*

(c) $\varphi(A^*) = \varphi(A)^*$ pro všechna $A \in \mathbb{C}^{n\times n}$. *(Zachování adjunkce)*

Poznámka 2.1.4. Pozor, když říkáme pouze *izomorfismus*, míníme tím klasický izomorfismus (lineární bijekci) mezi lineárními prostory, nikoliv Jordanův $*$-izomorfismus.

Tvrzení 2.1.5 (Základní vlastnosti Jordanova $*$-izomorfismu)**.** *Nechť* $\varphi : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ *je Jordanův* $*$*-izomorfismus, pak platí:*

(a) $\varphi(AB + BA) = \varphi(A)\varphi(B) + \varphi(B)\varphi(A)$ *pro každé* $A, B \in \mathbb{C}^{n\times n}$.

(b) $\varphi(ABA) = \varphi(A)\varphi(B)\varphi(A)$ *pro každé* $A, B \in \mathbb{C}^{n\times n}$.

(c) $\varphi(ABC + CBA) = \varphi(A)\varphi(B)\varphi(C) + \varphi(C)\varphi(B)\varphi(A)$ *pro každé* $A, B, C \in \mathbb{C}^{n\times n}$.

(d) $\varphi([[A, B], C]) = [[\varphi(A), \varphi(B)], \varphi(C)]$ *pro všechna* $A, B, C \in \mathbb{C}^{n\times n}$.

(e) $\varphi([A, B]^2) = [\varphi(A), \varphi(B)]^2$ *pro všechna* $A, B \in \mathbb{C}^{n\times n}$.

(f) Když $A, B \in \mathbb{C}^{n\times n}$ *komutují, pak platí:* $\varphi(AB) = \varphi(A)\varphi(B) = \varphi(B)\varphi(A)$.

(g) $\varphi(A^k) = \varphi(A)^k$ *pro každé* $A \in \mathbb{C}^{n\times n}, k \in \mathbb{Z}$*, je-li výraz definován. (Tzn.:* $k \geq 1$ *nebo* A *je regulární.)*

Důkaz. (S jistými obměnami převzato z [1].)

(a) Uvědomíme si, že $AB + BA = (A + B)^2 - A^2 - B^2$. Z linearity φ pak dostaneme:

$$\begin{aligned}\varphi(AB + BA) =& \varphi(A + B)^2 - \varphi(A)^2 - \varphi(B)^2 = (\varphi(A) + \varphi(B))^2 - \varphi(A)^2 - \varphi(B)^2 \\ =& \varphi(A)\varphi(B) + \varphi(B)\varphi(A).\end{aligned}$$

(b) Plyne z (a) spolu s rovností:

$$2ABA = (AB + BA)A + A(AB + BA) - BA^2 - A^2B.$$

(c) Dostaneme z (b) a z toho, že platí:

$$ABC + CBA = (A + C)B(A + C) - ABA - CBC.$$

(d) Z definice komutátoru snadno získáme:

$$[[A, B], C] = ABC + CBA - (BAC + CAB).$$

Z (c) a z této rovnosti (d) přímo plyne.

(e) Rovnost

$$[A, B]^2 = A(BAB) + (BAB)A - AB^2A - BA^2B,$$

spolu s (a) a (b) implikuje (e).

(f) Jelikož $[A, B] = \mathbf{0}$, z (d) máme pro všechna C:

$$\mathbf{0} = \varphi([[A, B], C]) = [[\varphi(A), \varphi(B)], \varphi(C)].$$

Tedy, $[\varphi(A), \varphi(B)]$ komutuje se všemi prvky $\mathbb{C}^{n\times n}$, speciálně i se svou adjunkcí a je tedy normální a můžeme ho dle 1.3.24 unitárně rozložit jako:

$$[\varphi(A), \varphi(B)] = UDU^{-1},$$

navíc z (e) máme:

$$\varphi([A, B]^2) = [\varphi(A), \varphi(B)]^2 = \mathbf{0} = UD^2U^{-1},$$

ale pak už nutně musí být $\mathbf{0} = D^2 = D$ čili $[\varphi(A), \varphi(B)] = \mathbf{0}$, což znamená že: $\varphi(A)\varphi(B) = \varphi(B)\varphi(A)$. Navíc z předpokladu a (a) získáme:

$$\varphi(AB) = \frac{1}{2}(\varphi(A)\varphi(B) + \varphi(B)\varphi(A)) = \varphi(A)\varphi(B).$$

(g) Nejprve tvrzení dokážeme pro $k \geq 1$ indukcí podle k. Pro $k = 1$ platí triviálně. Předpokládejme nyní, že platí $\varphi(A^k) = \varphi(A)^k$. Ukážeme, že bude platit $\varphi(A^{k+1}) = \varphi(A)^{k+1}$. Z (a) a indukčního předpokladu dostaneme:

$$\varphi(A^{n+1}) = \frac{1}{2}\varphi(AA^n + A^nA) = \frac{1}{2}(\varphi(A)\varphi(A^n) + \varphi(A^n)\varphi(A) = \varphi(A)^{n+1}.$$

Nechť je dále A regulární. Ukážeme, že $A^0 = \varphi(A)^0$, což je totéž jako: $\mathbf{1} = \varphi(\mathbf{1})$. Protože jednotková matice komutuje se všemi maticemi, z (f) dostaneme:

$$\varphi(A) = \varphi(\mathbf{1}A) = \varphi(\mathbf{1})\varphi(A) = \varphi(A)\varphi(\mathbf{1})$$

Rovnost $\mathbf{1} = \varphi(\mathbf{1})$ je pak důsledkem surjektivity φ.

Jelikož A komutuje se svou inverzí, opět z (f) máme:

$$\varphi(AA^{-1}) = \varphi(A)\varphi(A^{-1}) = \varphi(\mathbf{1}) = \mathbf{1} = \varphi(A)\varphi(A)^{-1},$$

což implikuje $\varphi(A^{-1}) = \varphi(A)^{-1}$. A konečně pro $k \leq -1$ máme:

$$\varphi(A^k) = \varphi((A^{-k})^{-1}) = \varphi(A^{-k})^{-1} = \varphi(A)^k.$$

□

Tvrzení 2.1.6. *Jordanův $*$-izomorfismus zachová spektrum. Formálně: Je-li φ Jordanův $*$-izomorfismus a λ je ve spektru operátoru A, právě když je i ve spektru $\varphi(A)$.*

Důkaz. Nechť λ není ve spektru A. Číslo λ není ve spektru A právě když $(A - \lambda\mathbf{1})$ je regulární, což nastává právě když $(\varphi(A) - \lambda\mathbf{1})$ je regulární, což nastává právě když λ není ve spektru $\varphi(A)$. □

Tvrzení 2.1.7. *Jordanův $*$-izomorfismus zobrazí projektor na projektor stejné hodnosti. Navíc: Jsou-li obrazy dvou projektorů ortogonální, Jordanův $*$-izomorfismus vzájemnou ortogonalitu zachová.*

Důkaz. Nechť je $\varphi : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ Jordanův $*$-izomorfismus. Podle 1.3.32 víme, že množina projekčních operátorů je plně charakterizována takto: $\mathcal{P} = \{P \in \mathbb{C}^{n\times n} | P = P^* = P^2\}$. Ovšem pak:

$$\varphi(\mathcal{P}) = \varphi(\{P \in \mathbb{C}^{n\times n} \mid P = P^* = P^2\}) = \{\varphi(P) \in \mathbb{C}^{n\times n} \mid \varphi(P) = \varphi(P)^* = \varphi(P)^2\} = \mathcal{P},$$

takže se projektory zobrazí na projektory. Dále ukážeme, že se zachová hodnost. Projektor P má hodnost n právě tehdy, když $P = P_1 + \cdots + P_n$, kde P_i jsou různé projektory hodnosti 1. Z linearity izomorfismu stačí tedy ukázat, že se zachovají hodnost u projektorů hodnosti 1. To uděláme sporem. Kdyby se projektor P hodnosti 1 zobrazil na projektor hodnosti 2 (pro jakoukoliv vyšší hodnost analogicky) dostaneme:

$$\varphi(P) = Q_1 + Q_2,$$

kde Q_1, Q_2 mají hodnost 1 a $Q_1 \neq Q_2$. Když ale na obě strany rovnosti aplikujeme inverzní zobrazení, dostaneme:

$$P = \varphi^{-1}(Q_1) + \varphi^{-1}(Q_2).$$

Jelikož φ^{-1} je též Jordanův $*$-izomorfismus, máme na pravé straně rovnosti součet dvou různých projektorů hodnosti alespoň 1, který má výslednou hodnost větší než 1, což je spor. Zbývá dokázat dovětek o ortogonalitě. Nechť P, Q jsou projektory s ortogonálními obrazy, tj: $PQ = \mathbf{0}$. Ihned dostáváme: $\varphi(P)\varphi(Q) = \varphi(Q)\varphi(P) = \varphi(PQ) = \varphi(\mathbf{0}) = \mathbf{0}$. □

Poznámka 2.1.8. Pozorování: Unitární zobrazení podle 1.3.18 zachová normu i vzájemnou ortogonalitu. Zobrazíme-li tedy unitárně celou ortonormální bázi, výsledkem bude zase ortonormální báze.

Tvrzení 2.1.9. *Je-li U unitární operátor, pak platí:*

$$P_{Ue} = UP_eU^*.$$

Důkaz. Z maticové reprezentace projektoru máme:

$$(P_{Ue})_{ij} = (Ue)_i\overline{(Ue)_j} = U\ (e_i\overline{e_j})U^* = (UP_eU^*)_{ij}.$$

□

2.2 Charakterizace Jordanových $*$-izomorfismů

Tvrzení 2.2.1. *Je-li zobrazení φ v jednom ze tvarů:*

- *$\varphi(A) = V^{-1}AV$ pro všechna $A \in \mathbb{C}^{n\times n}$, kde V je unitární operátor.*
- *$\varphi(A) = V^{-1}A^*V$ pro všechna $A \in \mathbb{C}^{n\times n}$, kde V je antiunitární operátor.*

Pak se jedná o Jordanův $*$-izomorfismus.

Důkaz. Snadno ověřitelné přímo z definice Jordanova $*$-izomorfismu, spolu s faktem, že $(A^*)^2 = (A^2)^*$ dle 1.3.7 (d). □

Poznámka 2.2.2. Ve zbytku kapitoly budeme ukazovat, že když zobrazení φ má jednu z uvedených vlasností, není to jen postačující podmínkou, aby bylo Jordanovým $*$-izomorfismem, ale i podmínkou nutnou.

Tvrzení 2.2.3. *Nechť je S množina všech samoadjungovaných operátorů z $\mathbb{C}^{n\times n}$ a zobrazení $\varphi : S \to S$ je reálně-lineární (tj. nad tělesem $\mathbb{R}$) izomorfismus, zachovávající mocninu, tj. $\varphi(A^2) = \varphi(A)^2$. Pak existuje jednoznačné rozšíření φ na zobrazení $\tilde{\varphi} : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$, které je Jordanovým $*$-izomorfismem.*

Důkaz. Označme pro $A \in \mathbb{C}^{n\times n}$:

$$A \ = A_1 + \imath A_2, \text{ kde } A_1 = \frac{A \ + A^*}{2}, A_2 = \frac{A \ - A^*}{2\imath}.$$

(O korektnosti označení se snadno přesvědčíme dosazením.) Operátory A_1, A_2 jsou zřejmě samoadjungované. (Pozor, $\imath A_2$ už samoadjungovaný není.) Definujme:

$$\tilde{\varphi}(A) = \varphi(A_1) + \imath\varphi(A_2).$$

Ověříme, že:

$$\tilde{\varphi}(A^2) = \tilde{\varphi}(A_1^2 - A_2^2 + \imath(A_1A_2 + A_2A_1)) = \varphi(A_1)^2 - \varphi(A_2)^2 + \imath\varphi(A_1A_2 + A_2A_1) = \tilde{\varphi}(A)^2.$$

A podobně také:

$$\tilde{\varphi}(A^*) = \tilde{\varphi}((A_1 + \imath A_2)^*) = \tilde{\varphi}(A_1^* + \bar{\imath}A_2^*) = \varphi(A_1) + \bar{\imath}\varphi(A_2) = \tilde{\varphi}(A)^*.$$

□

Tvrzení 2.2.4. *Pro každý Jordanův $*$-izomorfismus $\varphi : \mathbb{C}^{2\times2} \to \mathbb{C}^{2\times2}$ platí jedna ze dvou následujících možností:*

- *$\varphi(A) = V^{-1}AV$ pro všechna $A \in \mathbb{C}^{2\times2}$, kde V je unitární operátor.*
- *$\varphi(A) = V^{-1}A^*V$ pro všechna $A \in \mathbb{C}^{2\times2}$, kde V je antiunitární operátor.*

Důkaz. Mějme $e_1 = (1, 0), e_2 = (0, 1)$ standardní (ortonormální) bázi $\mathbb{C}^2$. Projektory na její prvky jsou: $P_{e_1} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right), P_{e_2} = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Podle Tvrzení 2.1.7 jsou $\varphi(P_{e_1}), \varphi(P_{e_2})$ nějaké projektory na ortogonální podprostory dimenze 1. Jednotkové vektory z těchto podprostorů nám vytvoří nějakou ortonormální bázi $\mathbb{C}^2$, množinu $\{f_1, f_2\}$. Přechod od původní standardní báze je dán vhodným unitárním zobrazením U takovým, že: $Ue_1 = f_1, Ue_2 = f_2$. (V maticové reprezentaci bude mít U jako sloupce vektory f_1, f_2.) Pak pro $e \in \{e_1, e_2\}$ máme dle 2.1.9:

$$\varphi(P_e)x = P_{Ue}x = U^{-1}P_eU \ x, \text{pro libovolné } x \in \mathbb{C}^2.$$

Díky tomu ale můžeme bez újmy na obecnosti předpokládat, že φ má vlastnost:

$$\varphi(P_e) = P_e,$$

jelikož složení unitárního zobrazení U s unitárním resp. antiunitárním bude výsledné hledané unitární resp. antiunitární zobrazení. Dále tedy budeme hledat V za tohoto předpokladu, totiž že φ zachová projektory na standardní bázi.

Obecnou matici $B = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ můžeme vyjádřit takto:

$$B = \underbrace{(P_{e_1} + P_{e_2})}_{=\mathbf{1}} B \underbrace{(P_{e_1} + P_{e_2})}_{=\mathbf{1}} = \underbrace{P_{e_1} B P_{e_1}}_{=\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)} + \underbrace{P_{e_1} B P_{e_2}}_{=\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right)} + \underbrace{P_{e_2} B P_{e_1}}_{=\left(\begin{smallmatrix} 0 & 0 \\ c & 0 \end{smallmatrix}\right)} + \underbrace{P_{e_2} B P_{e_2}}_{=\left(\begin{smallmatrix} 0 & 0 \\ 0 & d \end{smallmatrix}\right)} =$$
$$= a P_{e_1} + P_{e_1} B P_{e_2} + P_{e_2} B P_{e_1} + d P_{e_2}.$$

Ze zachování projekcí, linearity a vlastnosti 2.1.5 (c) Jordanova $*$-izomorfismu φ pak plyne, že:

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & x \\ y & d \end{pmatrix},$$

tj. φ zachová diagonálu. Uvažujme matici $A = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$, pro tu platí:

$$\varphi(A) = \begin{pmatrix} 0 & y \\ x & 0 \end{pmatrix},\ A^2 = \mathbf{0}.$$

Zároveň kvůli podmínce $\varphi(A^2) = \varphi(A)^2$ musí platit buď $x = 0$ nebo $y = 0$. Nechť nejprve platí první případ, tj. $y = 0$. Dostáváme:

$$\varphi \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ \alpha & 0 \end{pmatrix},\ \alpha \in \mathbb{C},$$

a z toho zároveň:

$$\varphi \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \varphi \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^* = \begin{pmatrix} 0 & 0 \\ \alpha & 0 \end{pmatrix}^* = \begin{pmatrix} 0 & \overline{\alpha} \\ 0 & 0 \end{pmatrix}.$$

Z linearity φ tak plyne pro libovolnou matici vztah:

$$\varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & \overline{\alpha} b \\ \alpha c & d \end{pmatrix} \tag{2.1}$$

Hledejme nyní omezení na α. Jordanův $*$-izomorfismus zachová spektrum. Spektrum matice $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ je $\{-1, 1\}$. Spektrum jejího obrazu, $\left(\begin{smallmatrix} 0 & \overline{\alpha} \\ \alpha & 0 \end{smallmatrix}\right)$, pak $\{-|\alpha|, |\alpha|\}$. Musí tedy být $|\alpha| = 1$. Zvolme unitární zobrazení $V : (z_1, z_2) \in \mathbb{C}^2 \mapsto (\alpha z_1, z_2)$. V maticové reprezentaci je $V = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$, a tedy je $V^{-1} = \left(\begin{smallmatrix} \overline{\alpha} & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Snadno se spočte, že:

$$\begin{pmatrix} \overline{\alpha} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \overline{\alpha} b \\ \alpha c & d \end{pmatrix} = \varphi \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Vrat'me se nyní k druhému případu, kdy je $x = 0$. Podobnou úvahou dojdeme k tomu, že platí vztah:

$$\varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & \alpha c \\ \overline{\alpha} b & d \end{pmatrix} \tag{2.2}$$

Testováním spektra matice $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ opět získáme omezení $|\alpha| = 1$. Definujme nyní antiunitární operátor $V : (z_1, z_2) \in \mathbb{C}^2 \mapsto (\alpha\overline{z_1}, \overline{z_2})$, máme $V^{-1} = V$. Nechť $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Podívejme se, jak působí $V^{-1}A^*V$ na obecný vektor (z_1, z_2).

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \overset{V}{\mapsto} \begin{pmatrix} \alpha\overline{z_1} \\ \overline{z_2} \end{pmatrix} \overset{A^*}{\mapsto} \begin{pmatrix} \overline{a}\alpha\overline{z_1} + \overline{cz_2} \\ \overline{b}\alpha\overline{z_1} + \overline{dz_2} \end{pmatrix} \overset{V^{-1}}{\longmapsto} \begin{pmatrix} az_1 + \alpha c z_2 \\ \overline{\alpha} b z_1 + d z_2 \end{pmatrix}.$$

Přitom ale:

$$\begin{pmatrix} a & \alpha c \\ \overline{\alpha} b & d \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} az_1 + \alpha c z_2 \\ \overline{\alpha} b z_1 + d z_2 \end{pmatrix}.$$

Tedy $V^{-1}A^*V$ působí na všechny vektory stejně jako zobrazení φ, a proto je mu rovno. □

Poznámka 2.2.5. Důležité pozorování, kterého dále využijeme: Díky předpokladu, že projektory na standardní bázi se zachovají, jsme v průběhu důkazu došli k tomu, že až na pronásobení komplexní jednotkou $\alpha, \overline{\alpha}$ je izomorfismus φ pro matice 2×2 dán buď identitou (rovnost (2.1), unitární případ) nebo transpozicí (rovnost (2.2), antiunitární případ). Protože jsou ale $\alpha, \overline{\alpha}$ komplexní jednotky, můžeme za daných předpokladů nalézt v obou případech unitární operátor W, pro nějž platí buď $\varphi(A) = W^{-1}AW$ nebo $\varphi(A) = W^{-1}A^TW$. Říkáme, že φ je *unitárně ekvivalentní* identitě nebo transpozici.

Předchozí tvrzení lze zobecnit pro čtvercové matice libovolné dimenze, což říká následující věta.

Věta 2.2.6. *Pro každý Jordanův $*$-izomorfismus $\varphi : \mathbb{C}^{n\times n} \to \mathbb{C}^{n\times n}$ platí jedna ze dvou následujících možností:*

- $\varphi(A) = V^{-1}AV$ *pro všechna* $A \in \mathbb{C}^{n\times n}$*, kde* V *je unitární operátor.*
- $\varphi(A) = V^{-1}A^*V$ *pro všechna* $A \in \mathbb{C}^{n\times n}$*, kde* V *je antiunitární operátor.*

Důkaz. Úplně na začátku ověříme speciální případ, kdy $n = 1$, což je triviální: Například vzhledem k tomu, že φ zachová spektrum, musí pro $A \in \mathbb{C}^{1\times 1}$ být $\varphi(A) = A = \mathbf{1}^{-1}A\mathbf{1}$. Případ, kdy $n = 2$ řeší předchozí tvrzení 2.2.4. Dále se budeme zabývat případem, kdy $n \geq 3$.

Komentář úvodem. O matici vzniklé z matice A vynulováním nějakých sloupců a řádků se stejným indexem v rámci tohoto důkazu říkáme, že je *podmaticí* A. V následujícím textu několikrát použijeme následující úvahu: Množina všech podmatic matic $\mathbb{C}^{n\times n}$ u kterých nulujeme vždy stejných k řádků a sloupců, tvoří prostor izomorfní s $\mathbb{C}^{(n-k)\times(n-k)}$, tzn. že existuje bijekce mezi touto množinou a $\mathbb{C}^{(n-k)\times(n-k)}$, zachovávající lineární kombinace, adjunkce a maticové součiny. Speciálně pak má obraz z $\mathbb{C}^{(n-k)\times(n-k)}$ diagonálu vytvořenou z diagonály vzoru s vypuštěnými prvky ve vynulovaných sloupcích. Zřejmě cokoliv platí o Jordanově $*$-izomorfismu v jednom prostoru, musí platit i v prostoru izomorfním.

Budiž $\{e_1, \ldots, e_n\}$ standardní ortonormální báze $\mathbb{C}^n$. Podobně jako v předchozím důkazu můžeme bez újmy na obecnosti předpokládat, že projektory na standardní bázi se zachovají, tzn. $\varphi(P_{e_i}) = P_{e_i}$. Dále mějme zadáno $A = (a_{ij}) \in \mathbb{C}^{n\times n}$ a označme jako $D = \operatorname{diag}(a_{ii})_{i=1}^n$, diagonální matici se shodnou diagonálou. Uvědomme si, že $P_{e_i}AP_{e_j}$ je matice, která má na pozici i, j stejnou hodnotu jako A a všude jinde nuly. Teď můžeme A vyjádřit následujícím způsobem:

$$A = \sum_{i=1}^{n}\sum_{j=1}^{n} P_{e_i}AP_{e_j} = \left(\sum_{\substack{i,j\\ i=1,\ldots,n\\ j\leq i}} (P_{e_i}AP_{e_j} + P_{e_j}AP_{e_i})\right) - D.$$

Je důležité pochopit význam sčítance sumy v poslední části rovnosti. Jedná se o matici, která má na dvou pozicích, osově symetrických podle diagonály, stejné prvky jako A, jinde nuly. Pro nás bude významné především to, že pro pevné hodnoty i, j tvoří množina matic $\{P_{e_i}AP_{e_i} + P_{e_i}AP_{e_j} + P_{e_j}AP_{e_i} + P_{e_j}AP_{e_j} | A \in \mathbb{C}^{n\times n}, n > 2\}$ prostor, který je izomorfní s $\mathbb{C}^{2\times 2}$. Prvky na diagonále můžeme chápat jako symetrické samy se sebou a počítají se tak dvakrát, proto na konci odečteme D.

Tvrzení 2.1.5 (c) spolu s linearitou a tím, že je φ identické pro diagonální matice, nám dá:

$$\varphi(A) = \left(\sum_{\substack{i,j\\ i=1,\ldots,n\\ j\leq i}} (P_{e_i}\varphi(A)P_{e_j} + P_{e_j}\varphi(A)P_{e_i})\right) - D.$$

Protože je ale každý sčítanec sumy z prostoru izomorfního s $\mathbb{C}^{2\times 2}$, je na nich φ unitárně ekvivalentní buď s identitou nebo transpozicí. Na základě toho můžeme říci, že uvedený výraz bude (míněno v obrazu tohoto izomorfismu) buď ve tvaru (2.1) nebo (2.2). Naším cílem teď bude ukázat, že volba tohoto tvaru musí být vždy stejná. Tedy že se nemůže stát, aby na jedné podmatici byla unitární ekvivalenci s identirou a na jiné s transpozicí. Nejprve to ověříme pro matice typu 3×3. Stačí nám nalézt nějaký příklad matice, na které když nebudou všechny volby stejné, dojdeme ke sporu, že $\varphi(A)^2 \neq \varphi(A^2)$. Nechť je:

$$A = \begin{pmatrix} 0 & 0 & 0\\ 1 & 0 & 0\\ 1 & 1 & 0 \end{pmatrix}, \text{ z čehož dostáváme: } A^2 = \begin{pmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 1 & 0 & 0 \end{pmatrix}.$$

V následující tabulce jsou shrnuty všechny možnosti, jak může tuto matici za našich předpokladů φ zobrazit tak, aby nebyly všechny volby stejné. (V druhém řádku mocníme první a ve třetím aplikujeme φ stejným způsobem jako v prvním na matici A^2.) α, β, γ jsou nějaké komplexní jednotky.

$\varphi(A)$	$\begin{pmatrix}0&\alpha&0\\0&0&0\\\overline{\beta}&\overline{\gamma}&0\end{pmatrix}$	$\begin{pmatrix}0&\alpha&\beta\\0&0&0\\0&\overline{\gamma}&0\end{pmatrix}$	$\begin{pmatrix}0&\alpha&0\\0&0&\gamma\\\overline{\beta}&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&\beta\\\overline{\alpha}&0&0\\0&\overline{\gamma}&0\end{pmatrix}$	$\begin{pmatrix}0&0&\beta\\\overline{\alpha}&0&\gamma\\0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0\\\overline{\alpha}&0&\gamma\\\overline{\beta}&0&0\end{pmatrix}$
$\varphi(A)^2$	$\begin{pmatrix}0&0&0\\0&0&0\\0&\alpha\overline{\beta}&0\end{pmatrix}$	$\begin{pmatrix}0&\beta\overline{\gamma}&0\\0&0&0\\0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&\alpha\gamma\\\gamma\overline{\beta}&0&0\\0&\alpha\overline{\gamma}&0\end{pmatrix}$	$\begin{pmatrix}0&\beta\overline{\gamma}&0\\0&0&\beta\overline{\alpha}\\\overline{\alpha\gamma}&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0\\0&0&\beta\overline{\alpha}\\0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0\\\gamma\overline{\beta}&0&0\\0&0&0\end{pmatrix}$
$\varphi(A^2)$	$\begin{pmatrix}0&0&0\\0&0&0\\\overline{\beta}&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&\beta\\0&0&0\\0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0\\0&0&0\\\overline{\beta}&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&\beta\\0&0&0\\0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&\beta\\0&0&0\\0&0&0\end{pmatrix}$	$\begin{pmatrix}0&0&0\\0&0&0\\\overline{\beta}&0&0\end{pmatrix}$

Protože se třetí řádek nikde nerovná druhému a vyčerpali jsme všechny možnosti, v maticích typu 3×3 musí být volba stejná pro všechny prvky. Teď už větu snadno zobecníme i pro $n > 3$. Formálně například indukcí: nechť je volba, zda se prvky symetrické podle diagonály zobrazí unitárně nebo antiunitárně, vždy stejná pro matice z $\mathbb{C}^{m\times m}, m < n$ a nechť $A \in \mathbb{C}^{n\times n}$. Podobně jako jsme si v počátku důkazu rozložili matici na součet matic z prostoru izomorfního s $\mathbb{C}^{2\times 2}$, můžeme si teď obdobně rozložit A na součet matic z prostorů izomorfních s $\mathbb{C}^{m\times m}, m < n$. Konkrétně když označíme A_i matici vzniklou z A vynulováním i-tého řádku a i-tého sloupce a C matici vzniklou z A vynulováním prvního řádku a sloupce i posledního řádku a sloupce dostaneme:

$$\begin{aligned} A \ =&A_n + A_1 - C + (P_{e_1}AP_{e_n} + P_{e_n}AP_{e_1}) = \\ =& \underbrace{A_n}_{(n-1)\times(n-1)} + \underbrace{A_1}_{(n-1)\times(n-1)} - \underbrace{C}_{(n-2)\times(n-2)} + \underbrace{(P_{e_1}AP_{e_n} + P_{e_n}AP_{e_1} + P_{e_1}AP_{e_2} + P_{e_2}AP_{e_1})}_{3\times 3} - \\ &- \underbrace{(P_{e_1}AP_{e_2} + P_{e_2}AP_{e_1})}_{2\times 2}. \end{aligned}$$

A jsme tedy rozložili na součet jejích podmatic. Ve svorce je vždy uveden typ prostoru matic, s nímž je prostor obsahující daný sčítanec izomorfní. O všech těchto prostorech předpokládáme, že na nich tvrzení platí. Poslední sčítanec je podmaticí prvního i předposledního, proto na nich musí být volba vždy stejná. Sčítanec C má rozměry alespoň 2×2 a je společnou podmaticí A_n, A_1. Vidíme, že na všech členech musí být volba vždy stejná, tím je důkaz hotov. □

Kapitola 3

Formalismus kvantové teorie

V této kapitole zavádíme některé základní pojmy z kvantové teorie. Kvantová teorie je velmi rozsáhlá, zde uvádíme jen minimum relevantní k tématu této práce. Více o aspektech kvantové teorie souvisejících s touto prací je možno nalézt v [7]. U čtenáře předpokládáme základní znalosti teorie pravděpodobnosti.

3.1 Axiomatika kvantové teorie

Poznámka 3.1.1. V této práci se zabýváme pouze systémy kvantových veličin, u kterých je možné naměřit jen konečně mnoho různých hodnot. (Např. spin elektronu, polarizace fotonu atd.) V klasickém případě je pravděpodobnostní struktura takového systému dána konečnou množinou elementárních jevů Ω, která spolu s pravděpodobnostní mírou P tvoří pravděpodobnostní prostor $(\Omega, \mathcal{A}, P), \mathcal{A} = 2^{\Omega}$. Stav systému je pak popsán právě pravděpodobnostní mírou, což je funkce $P : \mathcal{A} \to \langle 0, 1\rangle$ (zde $\langle 0, 1\rangle$ značí uzavřený interval), vyhovující následujícím axiomům:

(a) $P(\Omega) = 1$,

(b) $P(\emptyset) = 0$,

(c) $P(M \cup N) = P(M) + P(N)$, jestliže $M \cap N = \emptyset$.

Každá náhodná veličina X, tedy funkce $X : \Omega \to \mathbb{R}$, nabývá různých hodnot $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ pro $k \leq |\Omega|$ a dá se tedy napsat jako kombinace charakteristických funkcí:

$$X = \lambda_1 \chi_{M_1} + \cdots + \lambda_k \chi_{M_k} \tag{3.1}$$

kde $M_1, \ldots, M_k$ je disjunktní rozklad množiny Ω. Pravděpodobnost, že X nabude hodnoty λ_i je pak $P(M_i)$. Střední hodnota je dána výrazem:

$$\mathrm{E}\, X = \lambda_1 P(M_1) + \cdots + \lambda_k P(M_k).$$

V kvantovém případě je diskrétní pravděpodobnostní prostor nahrazen svou kvantovou analogií následujícím způsobem:

- Nosná množina Ω pro $|\Omega| = n$ je nahrazena Hilbertovým prostorem $\mathbb{C}^n$.
- Struktura náhodných jevů $\mathcal{A}$ je nahrazena strukturou podprostorů $\mathcal{L}(\mathbb{C}^n)$ Hilbertova prostoru $\mathbb{C}^n$, přičemž disjunktnost (nezávislost) jevů odpovídá ortogonalitě podprostorů.
- Stav systému je dán pravděpodobnostní funkcí $P : \mathcal{L}(\mathbb{C}^n) \to \langle 0, 1\rangle$, která definitoricky splňuje následující podmínky:
  (a) $P(\mathbb{C}^n) = 1$,
  (b) $P(\{0\}) = 0$,
  (c) $P(\mathrm{Span}(\mathcal{M} \cup \mathcal{N})) = P(\mathcal{M}) + P(\mathcal{N})$, jestliže $\mathcal{M} \perp \mathcal{N}$.

Stavy systému nejsou tak obecné, jak by se mohlo zdát. Existuje jejich popis na základě Gleasonovy věty.

Věta 3.1.2 (Gleasonova)**.** *Mějme Hilbertův prostor $\mathbb{C}^n, n \geq 3$. Pro každý stav P na $\mathcal{L}(\mathbb{C}^n)$ existuje právě jeden pozitivně semidefinitní operátor $\sigma : \mathbb{C}^n \to \mathbb{C}^n$ se stopou 1, tak, že pro každé $\mathcal{M} \in \mathcal{L}(\mathbb{C}^n)$ platí:*

$$P(\mathcal{M}) = \mathrm{Tr}(\sigma P_{\mathcal{M}}). \tag{3.2}$$

Bez důkazu. Viz [3] nebo původní článek [2].

Definice 3.1.3. Operátor σ v předchozí větě se nazývá *operátor hustoty*. Množinu všech operátorů hustoty na Hilbertově prostoru $\mathcal{H}$ značíme $\mathcal{S}(\mathcal{H})$.

Poznámka 3.1.4. V prostoru dimenze 2 Gleasonova věta neplatí, přesto se fyzikálně přijímají jen stavy dané formulí (3.2). Dostáváme tak vzájemně jednoznačné zobrazení mezi operátory hustoty a stavy. Můžeme je tedy zaměňovat.

Poznámka 3.1.5. Kvantová veličina je obecně popsána samoadjungovaným operátorem $X : \mathbb{C}^n \to \mathbb{C}^n$. Tento operátor má spektrální rozklad (dle 1.3.34):

$$X = \lambda_1 P_{\mathcal{M}_1} + \cdots + \lambda_k P_{\mathcal{M}_k}, \tag{3.3}$$

kde λ_i jsou navzájem různá vlastní čísla operátoru X a $\mathcal{M}_i$ jim odpovídající podprostory vlastních vektorů. Systém podprostorů $(\mathcal{M}_i)$ tvoří ortogonální rozklad $\mathbb{C}^n$. Rozklad (3.3) je analogií rozkladu (3.1). Ve shodě s klasickým případem může veličina (výsledek jejího měření) nabývat hodnot $\lambda_1, \ldots, \lambda_k$. Je-li stav systému dán pravděpodobnostní funkcí P na $\mathbb{C}^n$, pak pravděpodobnost, že veličina X nabude hodnoty λ_i je $P(\mathcal{M}_i)$. Nechť σ je operátor hustoty odpovídající P. Pak bude střední hodnota takto popsané kvantové veličiny X:

$$\mathrm{E}_\sigma X = \lambda_1 P(\mathcal{M}_1) + \cdots + \lambda_k P(\mathcal{M}_k) = \lambda_1 \mathrm{Tr}(\sigma P_{\mathcal{M}_1}) + \cdots + \lambda_k \mathrm{Tr}(\sigma P_{\mathcal{M}_k}) = \mathrm{Tr}(\sigma X).$$

Speciálně uvažujme jednotkový vektor $e \in \mathbb{C}^n$ a projektor P_e. Díváme-li se na P_e jako na operátor hustoty, pak určuje stav systému, který nazýváme *čistý*. Současně se můžeme na

P_e dívat jako na kvantovou veličinu nabývající hodnot z $\{0,1\}$. Její střední hodnota (tedy pravděpodobnost, že nabude hodnoty 1) je v daném čistém stavu popsaném operátorem hustoty P_f, pro nějaký jednotkový vektor f, rovna (poslední rovnost platí podle Tvrzení 1.3.31 (c)):

$$\mathrm{E}_{P_f}(P_e) = \mathrm{Tr}(P_f P_e) = |\langle f, e\rangle|^2. \tag{3.4}$$

Obecněji, je-li systém v čistém stavu P_f, $f = (f_1, \ldots, f_n)$, a X je obecný samoadjungovaný operátor, bude platit:

$$E_{P_f}(X) = \mathrm{Tr}(P_f X) = \langle Xf, f\rangle, \tag{3.5}$$

což odvodíme pro $X = (x)_{ij}$ takto:

$$\mathrm{Tr}(P_f X) = \sum_{i=1}^{n} (P_f X)_{ii} = \sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij} f_j \overline{f_i} = \sum_{i=1}^{n} (Xf)_i \overline{f_i} = \langle Xf, f\rangle.$$

3.2 Kvantové symetrie a Wignerova věta

Poznámka 3.2.1. Dynamika kvantového systému je dána buď to vhodnou transformací množiny fyzikálních veličin (Heisenbergův přístup) nebo vhodnou transformací množiny stavů (operátorů hustoty), což je Shrödingerův přístup. Přirozené je přitom například předpokládat, že daná transformace zachová vnitřní pravděpodobnostní strukturu systému, tedy přechodové pravděpodobnosti mezi čistými stavy. Zásadní Wignerova věta, dokázaná v této sekci, říká, že takové transformace, nazývané symetriemi, jsou vždy generovány unitárním nebo antiunitárním zobrazením.

Více o dynamice kvantových systémů, relevantní pro kvantovou teorii informace, lze nalézt v publikaci [7].

Definice 3.2.2. *Symetrií* kvantového systému nazýváme bijektivní zobrazení, které zachová střední hodnoty (3.4). Formálně jde tedy o bijekci $\varphi : \mathcal{P}_1(\mathbb{C}^n) \to \mathcal{P}_1(\mathbb{C}^n)$, která splňuje:

$$\mathrm{Tr}(\varphi(P_e)\varphi(P_f)) = \mathrm{Tr}(P_e P_f)$$

pro všechna $P_e, P_f \in \mathcal{P}_1(\mathbb{C}^n)$.

Věta 3.2.3 (Wignerova)**.** *Každou symetrii $\varphi : \mathcal{P}_1(\mathbb{C}^n) \to \mathcal{P}_1(\mathbb{C}^n)$ lze zapsat ve tvaru:*

$$\varphi(P) = V^{-1} P V,$$

kde V je nějaký unitární nebo antiunitární operátor.

Důkaz. Uvádíme zjednodušenou verzi důkazu podle [5]. V původní publikaci je důkaz složitější, protože se uvádí silnější znění věty. Základní struktura důkazu je následující: Danou symetrii rozšíříme jednoznačně na lineární operátor definovaný na prostoru samoadjungovaných operátorů a posléze na prostoru všech operátorů (definovaných na témže Hilbertově prostoru). Následně ukážeme, že vzniklé zobrazení je Jordanovým $*$-izomorfismem a důkaz uzavřeme aplikací předcházející Věty 2.2.6.

Nechť je φ daná symetrie a A samoadjungovaný operátor vyjádřený takto:

$$A = \sum_{i=1}^{n} \lambda_i P_i,\ \lambda_i \in \mathbb{R}, P_i \in \mathcal{P}_1(\mathbb{C}^n). \tag{3.6}$$

Definujme zobrazení $\hat{\varphi}$, rozšíření φ na samoadjungované operátory, takto:

$$\hat{\varphi}(A) = \sum_{i=1}^{n} \lambda_i \varphi(P_i).$$

Protože vyjádření A ve tvaru (3.6) není jednoznačné, musíme ukázat, že tato definice je korektní, tj. nezávislá na volbě vyjádření. Nechť je tedy další vyjádření:

$$A = \sum_{i=1}^{n} \mu_i Q_i,\ \mu_i \in \mathbb{R}, Q_i \in \mathcal{P}_1(\mathbb{C}^n).$$

Pro libovolné $R \in \mathcal{P}_1(\mathbb{C}^n)$ pak spočteme:

$$\operatorname{Tr}\left(\sum_{i=1}^{n} \lambda_i \varphi(P_i)\varphi(R)\right) = \sum_{i=1}^{n} \lambda_i \operatorname{Tr}\left(\varphi(P_i)\varphi(R)\right) = \sum_{i=1}^{n} \lambda_i \operatorname{Tr}\left(P_i R\right) = \operatorname{Tr}\left(\sum_{i=1}^{n} \lambda_i P_i R\right) =$$
$$= \operatorname{Tr}\left(\sum_{i=1}^{n} \mu_i Q_i R\right) = \sum_{i=1}^{n} \mu_i \operatorname{Tr}\left(Q_i R\right) = \sum_{i=1}^{n} \mu_i \operatorname{Tr}\left(\varphi(Q_i)\varphi(R)\right) = \operatorname{Tr}\left(\sum_{i=1}^{n} \mu_i \varphi(Q_i)\varphi(R)\right).$$

Tudíž je pro všechna $R \in \mathcal{P}_1(\mathbb{C}^n)$:

$$\operatorname{Tr}\left(\left(\sum_{i=1}^{n} \lambda_i \varphi(P_i) - \sum_{i=1}^{n} \mu_i \varphi(Q_i)\right) \varphi(R)\right) = 0.$$

Díky linearitě stopy bychom dostali podobnou rovnost, pokud bychom nahradili $\varphi(R)$ nějakou lineární kombinací obrazů projektorů zobrazení φ. To nám dovoluje říci, že:

$$\operatorname{Tr}\left(\left(\sum_{i=1}^{n} \lambda_i \varphi(P_i) - \sum_{i=1}^{n} \mu_i \varphi(Q_i)\right)\left(\sum_{i=1}^{n} \lambda_i \varphi(P_i) - \sum_{i=1}^{n} \mu_i \varphi(Q_i)\right)\right) =$$
$$= \operatorname{Tr}\left(\left(\sum_{i=1}^{n} \lambda_i \varphi(P_i) - \sum_{i=1}^{n} \mu_i \varphi(Q_i)\right)^2\right) = 0.$$

Operátor $\left(\sum_{i=1}^{n} \lambda_i \varphi(P_i) - \sum_{i=1}^{n} \mu_i \varphi(Q_i)\right)^2$ je mocninou samoadjungovaného operátoru a je tedy pozitivně-semidefinitní. Protože má nulovou stopu, tedy i jediné vlastní číslo 0, musí sám být nulový. Z toho snadno dostaneme:

$$\sum_{i=1}^{n} \lambda_i \varphi(P_i) - \sum_{i=1}^{n} \mu_i \varphi(Q_i) = 0.$$

Tudíž je $\hat{\varphi}$ definováno korektně. Z toho jak bylo $\hat{\varphi}$ zavedeno, je teď zřejmé, že je reálně-lineární a tak platí:

$$\hat{\varphi}(A^2) = \hat{\varphi}\left(\sum_{i=1}^{n} \lambda_i^2 P_{e_i}\right) = \sum_{i=1}^{n} \lambda_i^2 \varphi(P_{e_i}) = \hat{\varphi}(A)^2.$$

Aplikací tvrzení 2.2.3 rozšiřme $\hat{\varphi}$ na Jordanův $*$-izomorfismus $\tilde{\varphi}$. Wignerova věta je teď důsledkem věty 2.2.6. □

Kapitola 4

Kvantová entropie

4.1 Kvantová entropie

Poznámka 4.1.1. Přestože ji nebudeme dále potřebovat, pro větší názornost uvedeme něco málo o Shannonově entropii. Uvažujme konečný pravděpodobností prostor $(\Omega, \mathcal{A}, P), \Omega = \{1, \ldots, n\}, \mathcal{A} = 2^{\Omega}$. Můžeme ztotožnit pravděpodobnostní rozdělení s n-ticí pravděpodobností jednotlivých elementárních jevů. Budeme tedy mít $P \equiv (p_1, \ldots, p_n)$, kde $p_i \geq 0$ pro všechna $i = 1, \ldots, n$ a $\sum_{i=1}^{n} p_i = 1$.

Naší motivací je nejprve nějakým způsobem vyjádřit míru neurčitosti tohoto pravděpodobnostního rozdělení, neboli střední množství informace, jenž nám přinese zjištění, který jev nastal. Intuitivně: Příliš nás nepřekvapí informace o tom, že nastal jev s vysokou pravděpodobností. Proto by se množství informace $I(A) : \mathcal{A} \to \mathbb{R}$ obsažené ve zjištění že nastal jev A mělo blížit k nule s tím, jak se pravděpodobnost jevu A blíží jedné. Naopak informace o tom, že se stalo něco velice nepravděpodobného, je v tomto smyslu mnohem hodnotnější, a tak by se $I(A)$ mělo blížit k nekonečnu s tím, jak se pravděpodobnost jevu A blíží nule. Požadujeme funkci I spojitou vzhledem k pravděpodobnosti daného jevu. Dále je přirozený požadavek, aby pro nezávislé jevy $M, N \in \mathcal{A}$ bylo $I(M \cap N) = I(M) + I(N)$. Dá se formálně ukázat, že to nám stačí k určení funkce I – je to (až na násobek konstantou):

$$I(M) = -\log P(M) \text{ s konvencí: } I(\emptyset) = \infty,$$

což není překvapivé, vzhledem k tomu, že pravděpodobnost průniku nezávislých jevů je součinem jejich pravděpodobnostní a logaritmus zobrazuje součin na součet. Pro elementární jevy funkci zjednodušíme na $\hat{I} : \Omega \to \mathbb{R}$, kde:

$$\hat{I}(i) = -\log p_i \text{ s konvencí: } -\log 0 = \infty.$$

Na volbě základu logaritmu příliš nezáleží, určuje jen jednotky ve kterých množství informace měříme. Typicky se používá dvojkový (jednotka *bit*) nebo přirozený (jednotka *nat*). Dohodněme se na používání dvojkového logaritmu. Funkce $\hat{I}$ je náhodnou veličinou, můžeme tedy určit její střední hodnotu a to je právě Shannonova entropie, značená $H(P)$.

Takže když pro diskrétní náhodou veličinu označíme $\rho = \operatorname{diag}(p_1, \ldots, p_n)$, bude:

$$H(P) = \mathrm{E}\,\hat{I}(\Omega) = \sum_{i\in\Omega} p_i(-\log p_i) = \operatorname{Tr}(\rho(-\log\rho)) = -\operatorname{Tr}(\rho\log\rho),$$

s konvencí $0 \cdot \log 0 = 0$.

Dalším pojmem, jehož zobecněním se budeme zabývat, je *(klasická) vzájemná entropie*. Ta by měla charakterizovat odlišnost dvou pravděpodobnostních rozdělení nebo chybu, které se dopustíme použitím jiné distribuce pravděpodobnosti. Uvažujme tedy druhé pravděpodobnostní rozdělení $Q \equiv \{q_1, \ldots, q_n\}$. Vzájemnou entropii $H(P\|Q)$ pak definujeme takto:

$$H(P\|Q) = \sum_{i\in\Omega} p_i \left(-\log\frac{q_i}{p_i}\right) = \sum_{i\in\Omega} p_i \log p_i - \sum_{i\in\Omega} p_i \log q_i = \operatorname{Tr}(\rho\log\rho) - \operatorname{Tr}(\rho\log\sigma),$$

pro $\sigma = \operatorname{diag}(q_1, \ldots, q_n)$. Ve speciálním případě, kdy by pro nějaká i bylo $p_i \neq 0, q_i = 0$ definujeme vzájemnou entropii jako nekonečnou.

Stojí za povšimnutí, že $H(P\|P) = 0$, což lze interpretovat tak, že při použití správné veličiny se nedopouštíme žádné chyby.

Nyní můžeme plynule přejít k definici Von Neumannovy entropie, která je zobecněním Shannonovy entropie pro kvantové systémy.

Definice 4.1.2. *Von Neumannova entropie* S, dále jen *entropie* stavu popsaného operátorem hustoty $\rho = \sum_{i=1}^{k} p_i P_{e_i}, p_i \neq 0$, pro ortonormální bázi $\{e_1, \ldots, e_k\}$ je:

$$S(\rho) = \mathrm{E}_\rho(-\log\rho) = -\operatorname{Tr}(\rho\log\rho) = -\sum_{i=1}^{k} p_i \log p_i,$$

kde definiční obor operátoru ρ omezíme na množinu $\operatorname{Supp}\rho$.

Poznámka 4.1.3. Omezením definičního oboru ρ v definici ošetřujeme případ, kdy bychom měli dělat logaritmus z operátoru, který je jen pozitivně semidefinitní, nikoliv pozitivní. V maticové reprezentaci se toto omezení projeví takto: Nechť $U^{-1}DU$ podle 1.3.24 je maticová reprezentace operátoru ρ definovaného na $\mathbb{C}^n$. Reprezentace ρ definovaného na $\operatorname{Supp}\rho$ pak bude následující: Z matice D vypustíme nulové řádky a sloupce a z matic U^{-1}, U vypustíme řádky a sloupce na stejných pozicích. Tím dojde k jakési „regularizaci“, takže $\log\rho$ bude dávat smysl. Z formalismu kvantové teorie víme, že podprostor vlastních vektorů příslušný vlastnímu číslu 0 odpovídá jevu s pravděpodobností 0, takže toto opatření je analogií toho, kdybychom v klasické entropii neuvažovali jevy s nulovou pravděpodobností, což je ekvivalentní s konvencí $0 \cdot \log 0 = 0$. Algebraicky to můžeme chápat tak, že do stopy, jakožto součtu vlastních čísel, nezapočítáme nulová vlastní čísla, což výsledek nezmění.

Poznámka 4.1.4. Všimněme si, že pro čistý stav, tj. takový, že jediné vlastní číslo ρ je jednička a ostatní nuly, bude Von Neumannova entropie $S(\rho)$ nulová. Von Neumannova entropie tedy kvantifikuje cosi jako vzdálenost od čistého stavu.

Definice 4.1.5. *Vzájemná (kvantová) entropie* dvou kvantových stavů popsaných operátory hustoty $\rho, \sigma \in \mathcal{S}(\mathbb{C}^n)$, značena $S(\rho\|\sigma)$ je:

$$S(\rho\|\sigma) = \begin{cases} \mathrm{Tr}(\rho \log \rho) - \mathrm{Tr}(\rho \log \sigma) = -S(\rho) - \mathrm{Tr}(\rho \log \sigma), \text{ pro } \mathrm{Supp}\,\rho \subseteq \mathrm{Supp}\,\sigma, \\ \infty \text{ jinak.} \end{cases}$$

Kde definiční obor operátoru ρ ve výrazu $\mathrm{Tr}(\rho \log \rho)$ omezíme na množinu $\mathrm{Supp}\,\rho$ a definiční obor operátorů ρ, σ ve výrazu $\mathrm{Tr}(\rho \log \sigma)$ omezíme na množinu $\mathrm{Supp}\,\sigma$.

Poznámka 4.1.6. Omezení definičního oboru ve výrazu $\mathrm{Tr}(\rho \log \rho) = -S(\rho)$ je zřejmě ze stejného důvodu jako v případě Von Neumannovy entropie. Omezení ve výrazu $\mathrm{Tr}(\rho \log \sigma)$ je ale potenciálně problematické. Mohlo by se stát, že omezíme operátor ρ natolik, že by po tomto omezení jeho nový obor hodnot byl vlastní podmnožinou původního? Pak by se jednalo o analogii situace u klasické vzájemné entropie, kdy můžeme narazit na nevlastní výraz $c \cdot \log 0$ pro $c > 0$. Ukážeme, že taková situace může nastat pouze když $\mathrm{Supp}\,\rho \nsubseteq \mathrm{Supp}\,\sigma$ a zároveň zdůvodníme, proč i zde pak vzájemnou entropii definujeme jako nekonečnou.

Nechť $\lambda_1, \ldots, \lambda_k$ jsou navzájem různá vlastní čísla operátoru σ a $P_1, \ldots, P_k$ projektory na jim příslušné podprostory (ve stejném pořadí). Pokud platí $\mathrm{Supp}\,\rho \subseteq \mathrm{Supp}\,\sigma$, má při konvenci $0 \cdot \log 0 = 0$ smysl výraz:

$$\mathrm{Tr}(\rho \log \sigma) = \mathrm{Tr}\left(\rho \sum_{i=1}^{k} \log(\lambda_i) P_i\right) = \sum_{i=1}^{k} \mathrm{Tr}(\rho P_i) \log \lambda_i.$$

Nemůže se totiž stát, že by bylo λ_i nulové a zároveň $\mathrm{Tr}(\rho P_i)$ nenulové. Pro $\lambda_i = 0$ totiž platí:

$$\mathrm{Supp}\,P_i = \mathrm{Ker}\,\sigma \perp \mathrm{Supp}\,\sigma,$$

z čehož plyne $\mathrm{Supp}\,P_i \perp \mathrm{Supp}\,\rho$, a tedy:

$$\mathrm{Tr}(\rho P_i) = \mathrm{Tr}(P_i \rho) = \mathrm{Tr}(\mathbf{0}) = 0.$$

Předpokládejme nyní, že platí $\mathrm{Supp}\,\rho \nsubseteq \mathrm{Supp}\,\sigma$ a podíváme se, co z toho lze vysoudit. Přechodem k ortogonálním doplňkům (viz. Věta 1.2.16) dostaneme: $\mathrm{Ker}\,\sigma \nsubseteq \mathrm{Ker}\,\rho$, tedy σ je nenulové na prostoru $\mathrm{Ker}\,\rho$. Pak musí existovat i, že P_i je nenulové na prostoru $\mathrm{Ker}\,\rho$, tedy:

$$\rho P_i \neq \mathbf{0}. \tag{4.1}$$

Sporem dokážeme, že:

$$P_i \rho P_i \neq \mathbf{0}. \tag{4.2}$$

Nechť tedy platí opak: $P_i \rho P_i = \mathbf{0}$. Pro každý vektor $x \in \mathcal{H}$ je: $\langle P_i \rho P_i x, x \rangle = 0$. To dá:

$$0 = \left\langle P_i \rho^{\frac{1}{2}} \rho^{\frac{1}{2}} P_i x, x \right\rangle = \left\langle P_i \rho^{\frac{1}{2}} x, P_i \rho^{\frac{1}{2}} x \right\rangle = \|\rho^{\frac{1}{2}} P_i x\|^2.$$

Takže $\rho^{\frac{1}{2}} P_i = \mathbf{0}$. To implikuje $\rho P_i = \mathbf{0}$, což je spor s (4.1), takže (4.2) platí. Zároveň postupnou aplikací vlasností vlastností 1.3.32, 1.3.21 (b), 1.3.17, dostáváme:

$$\mathrm{Tr}(\rho P_i) = \mathrm{Tr}(\rho P_i^2) = \mathrm{Tr}(P_i \rho P_i) > 0.$$

Při označení $\mathrm{Tr}(\rho P_i) = a$ dostaneme dosazením formálně:

$$\mathrm{Tr}(\rho P_i) \cdot \log \lambda_i = a \cdot \log 0 = a \cdot (-\infty) = -\infty.$$

Jelikož se výraz $\mathrm{Tr}(\rho P_i)$ v definici vyskytuje se záporným znaménkem, definujeme v takovémto případě vzájemnou entropii jako nekonečnou.

Tvrzení 4.1.7 (Jensenova nerovnost)**.** *Nechť je X konvexní podmnožina lineárního prostoru. Každá* striktně konvexní *funkce $f : X \to \mathbb{R}$ (tj. taková, že pro pro každé a, kde $0 < a < 1$, pro každá $x, y \in X$ platí: $f(ax + (1-a)y) < af(x) + (1-a)f(y)$.) splňuje pro $x_i \in X, 0 \leq a_i \leq 1, \sum_{i=1}^n a_i = 1$:*

$$f\left(\sum_{i=1}^n a_i x_i\right) \leq \sum_{i=1}^n a_i f(x_i).$$

Navíc rovnost nastává právě když existuje $a_i = 1$.

Tvrzení 4.1.8. *Záporně vzatý logaritmus, $-\log$, je striktně konvexní funkce na celém svém definičním oboru.*

Dobře známá tvrzení z matematické analýzy. Zde bez důkazu.

Tvrzení 4.1.9. *Pro všechna $x \geq 0$ platí (při konvenci $\log 0 = -\infty$):*

$$\log(x) \ln(2) = \ln(x) \leq x - 1, \tag{4.3}$$

kde rovnost nastává pouze pro $x = 1$.

Důkaz. Plyne ze striktní konkávnosti funkce ln. (Funkce $x - 1$ je její tečnou v bodě $x = 1$.) □

Tvrzení 4.1.10 (Kleinova nerovnost)**.** *Kvantová vzájemná entropie je nezáporná, tj.:*

$$S(\rho \| \sigma) \geq 0,$$

pro všechny operátory hustoty $\rho, \sigma \in \mathcal{S}(\mathbb{C}^n)$. Navíc, rovnost nastává právě když $\rho = \sigma$.

Důkaz. Hlavní myšlenku tohoto důkazu čerpáme z publikace [7].

Nejprve dokážeme, že klasická vzájemná entropie je nezáporná. Mějme pravděpodobnostní rozdělení $P \equiv (p_1, \ldots, p_n)$,$Q \equiv (q_1, \ldots, q_n)$. Buď je vzájemná entropie nekonečná (a

tedy nezáporná) nebo postupujeme následovně: Přepíšeme rovnost (4.3) do tvaru $-\log x \geq \frac{1-x}{\ln 2}$ a na základě toho si uvědomíme, že:

$$H(P\|Q) = \sum_{i=1}^{n} p_i \log p_i - \sum_{i=1}^{n} p_i \log q_i = \sum_{i=1}^{n} p_i \log \frac{p_i}{q_i} \geq$$
$$\geq \frac{1}{\ln 2} \sum_{i=1}^{n} p_i \left(1 - \frac{q_i}{p_i}\right) = \frac{1}{\ln 2} \underbrace{\sum_{i=1}^{n} (p_i - q_i)}_{=1-1=0} = 0.$$

Rovnost nastává právě když $\frac{p_i}{q_i} = 1$ pro všechna i, tzn. právě když $P = Q$.

Nyní přejdeme k samotnému důkazu nezápornosti kvantové vzájemné entropie. Předpokládejme, že $\operatorname{Supp}\rho \subseteq \operatorname{Supp}\sigma$, jinak tvrzení platí triválně přímo z definice. Nechť P, Q jsou i nadále pravděpodobnostní rozdělení a označme $\rho = \sum_{i=1}^{n} p_i P_{e_i}, \sigma = \sum_{i=1}^{n} q_i P_{f_i}$, kde $\{e_1 \ldots, e_n\}$ i $\{f_1, \ldots, f_n\}$ jsou ortonormální báze $\operatorname{Supp}\sigma$. K tomuto nás opravňuje předpoklad $\operatorname{Supp}\rho \subseteq \operatorname{Supp}\sigma$ a Tvrzení 1.3.34, kde projektory na vícedimenzionální podprostory rozepíšeme jako součet projektorů na jednodimenzionální podprostory dané prvky jejich ortonormálních bazí. Protože je

$$\operatorname{Tr}(\rho \log \rho) = \sum_{i=1}^{n} p_i \log p_i,$$

dostaneme:

$$\operatorname{Tr}(\rho \log \sigma) = \operatorname{Tr}\left(\left(\sum_{i=1}^{n} p_i P_{e_i}\right)\left(\sum_{j=1}^{n} \log(q_j) P_{f_j}\right)\right) = \operatorname{Tr}\left(\sum_{i,j=1}^{n} p_i \log(q_j) P_{e_i} P_{f_j}\right) =$$
$$= \sum_{i,j=1}^{n} p_i \log(q_j) |\langle e_i, f_j \rangle|^2,$$

kde jsme v posledním kroku využili Tvrzení 1.3.31 (b) spolu s linearitou stopy. Označíme $|\langle e_i, f_j \rangle|^2 = a_{ij}$. Všimněme si, že sloupce i řádky matice (a_{ij}) se sčítají do jedničky, což plyne z tvrzení 1.2.18. Vzájemnou entropii nyní můžeme zapsat jako:

$$S(\rho\|\sigma) = \operatorname{Tr}(\rho \log \rho) - \operatorname{Tr}(\rho \log \sigma) = \sum_{i=1}^{n} p_i \log p_i - \sum_{i,j=1}^{n} p_i \log(q_j) a_{ij} =$$
$$= \sum_{i=1}^{n} p_i \left(\log(p_i) - \sum_{j=1}^{n} \log(q_j) a_{ij}\right).$$

Protože $-\log$ je konvexní funkce, použitím Jensenovy nerovnosti dostaneme:

$$\sum_{i=1}^{n} p_i \left(\log(p_i) - \sum_{j=1}^{n} \log(q_j) a_{ij}\right) \geq \sum_{i=1}^{n} p_i \left(\log(p_i) - \log\left(\sum_{j=1}^{n} q_j a_{ij}\right)\right). \qquad (4.4)$$

Dále označíme $r_i = \sum_{j=1}^n q_j a_{ij}$. Zřejmě je $r_i \geq 0$, ale navíc také:

$$\sum_{i=1}^n r_i = \sum_{i=1}^n \sum_{j=1}^n q_j |\langle e_i, f_j\rangle|^2 = \sum_{j=1}^n q_j \underbrace{\sum_{i=1}^n |\langle e_i, f_j\rangle|^2}_{=1} = 1.$$

$R \equiv (r_1, \ldots, r_n)$ je tedy náhodné rozdělení. Můžeme tedy udělat závěr, že:

$$S(\rho\|\sigma) \geq \sum_{i=1}^n p_i(\log(p_i) - \log(r_i)) = H(P\|R) \geq 0.$$

Rovnost v (4.4) podle dovětku Jensenovy nerovnosti nastává právě když matice (a_{ij}) je permutační (tzn. má v každém řádku i sloupci právě jednu jedničku, jinde nuly), z čehož plyne, že $\rho = \sigma$. (Možná jsou jen jinak očíslovány vlastní prvky bazí $(e_i), (f_i)$). □

Poznámka 4.1.11. Vzájemná entropie není metrikou. Obecně $S(\rho\|\sigma) \neq S(\sigma\|\rho)$.

4.2 Molnárova věta

Věta 4.2.1. *Nechť $\varphi : \mathcal{S}(\mathbb{C}^n) \to \mathcal{S}(\mathbb{C}^n)$ je bijektivní zobrazení zachovávající vzájemnou kvantovou entropii, tj. takové, že platí:*

$$S(\varphi(\rho)\|\varphi(\sigma)) = S(\rho\|\sigma)$$

pro všechna $\rho, \sigma \in \mathcal{S}(\mathbb{C}^n)$. Pak φ lze zapsat ve tvaru:

$$\varphi(\rho) = V^{-1}\rho V \quad (\rho \in \mathcal{S}(\mathbb{C}^n)), \tag{4.5}$$

kde V je unitární nebo antiunitární operátor.

Poznámka 4.2.2. Uvedený výsledek byl teprve poměrně nedávno (2008) dokázán L. Molnárem. Zde uvádíme podrobněji rozpracovanou variantu právě jeho důkazu podle [6].

Důkaz. Nejprve ukážeme, že zobrazení ve tvaru (4.5) skutečně entropii zachová. Ve výpočtech v tomto odstavci uvažujeme zúžené definiční obory operátorů ve smyslu definice vzájemné entropie. Podle definice logaritmu pro unitární nebo antiunitární operátor V a operátor hustoty ρ platí: $V^{-1}\log(\rho)V = \log(V^{-1}\rho V)$. Tak spočteme:

$$\begin{aligned} V^{-1}\rho V(\log(V^{-1}\rho V) - \log(V^{-1}\sigma V)) =& V^{-1}\rho V(V^{-1}\log(\rho)V - V^{-1}\log(\sigma)V) = \\ =& V^{-1}\rho(\log(\rho) - \log(\sigma))V. \end{aligned}$$

Pro

$$\operatorname{Supp} V^{-1}\rho V \subseteq \operatorname{Supp} V^{-1}\sigma V \iff \operatorname{Supp}\rho \subseteq \operatorname{Supp}\sigma,$$

pak dostaneme:

$$S(V^{-1}\rho V\|V^{-1}\sigma V) = \mathrm{Tr}(V^{-1}\rho(\log(\rho)-\log(\sigma))V) = \mathrm{Tr}(VV^{-1}\rho(\log(\rho)-\log(\sigma))) = \\ = \mathrm{Tr}(\rho(\log(\rho)-\log(\sigma))) = S(\rho\|\sigma).$$

V případě antiunitárního operátoru nás k tomuto kroku opravňuje fakt, že antiunitární operátor je složením unitárního operátoru a komplexního sdružení. Totiž, je-li $V = UK$, kde U je unitární operátor a dále $K : x \in \mathbb{C}^n \mapsto \overline{x}$ operace komplexního sdružení, bude $V^{-1}AV = KU^{-1}AUK$. Rozepsáním působení tohoto operátoru na obecný vektor snadno nahlédneme, že $KU^{-1}AUK = \overline{U^{-1}AU}$, což má stále stejnou stopu jako A. Tedy:

$$S(V^{-1}\rho V\|V^{-1}\sigma V) = S(\rho\|\sigma).$$

Dále budeme dokazovat opačnou implikaci, tedy že každé zobrazení zachovávající vzájemnou entropii už nutně musí být v tomto tvaru.

Případ, kdy $n = 1$, platí triviálně, neboť v jedné dimenzi existuje jediný operátor hustoty: číslo 1. φ tedy bude identita a V můžeme též volit jako identitu. Dále v důkazu předpokládáme $n \geq 2$.

Protože je vzájemná entropie $S(\rho\|\sigma)$ konečná, právě když $\mathrm{Supp}\,\rho \subseteq \mathrm{Supp}\,\sigma$, musí mít φ vlastnost:

$$\mathrm{Supp}\,\rho \subseteq \mathrm{Supp}\,\sigma \iff \mathrm{Supp}\,\varphi(\rho) \subseteq \mathrm{Supp}\,\varphi(\sigma) \tag{4.6}$$

pro všechna $\rho, \sigma \in \mathcal{S}(\mathbb{C}^n)$. Speciálně pak:

$$\mathrm{Supp}\,\rho = \mathrm{Supp}\,\sigma \iff \mathrm{Supp}\,\varphi(\rho) = \mathrm{Supp}\,\varphi(\sigma)$$

a ekvivalentně tedy:

$$\mathrm{Supp}\,\rho \subsetneq \mathrm{Supp}\,\sigma \iff \mathrm{Supp}\,\varphi(\rho) \subsetneq \mathrm{Supp}\,\varphi(\sigma) \tag{4.7}$$

pro všechna $\rho, \sigma \in \mathcal{S}(\mathbb{C}^n)$. Připomeňme, že operátory hustoty jsou pozitivně semidefinitní, a tedy zde Supp = Range. Hodnost operátoru ρ je k, právě když k je maximální takové, že existuje posloupnost $\rho_1, \ldots, \rho_k$ operátorů hustoty na $\mathbb{C}^n$ splňující:

$$\mathrm{Supp}\,\rho_1 \subsetneq \cdots \subsetneq \mathrm{Supp}\,\rho_k \subseteq \mathrm{Supp}\,\rho$$

Takovou posloupnost můžeme zkonstruovat například volbou: $\rho_i = \frac{1}{i}P_{\mathcal{M}_i}$, kde $\mathcal{M}_i$ je lineární obal prvních i prvků seřazené ortonormální báze složené z vlastních vektorů ρ příslušných nenulovým vlastním číslům. Nyní tedy podle vlastností (4.6), (4.7) musí φ zachovat hodnost prvků $\mathcal{S}(\mathbb{C}^n)$. Speciálně je tedy $\rho \in \mathcal{S}(\mathbb{C}^n)$ projektor hodnosti 1 (čili čistý stav), právě když $\varphi(\rho)$ je projektor hodnosti 1. Dále nechť je $\sigma \in \mathcal{S}(\mathbb{C}^n)$ operátor hodnosti 2 ve tvaru: $\sigma = \lambda P + \mu Q$, kde $P, Q \in \mathcal{P}_1(\mathbb{C}^n)$ jsou vzájemně ortogonální a $0 < \lambda < \mu = 1 - \lambda < 1$ a nechť $R \in \mathcal{P}_1(\mathbb{C}^n)$ je libovolný. Na operátoru σ nás bude zajímat pouze jeho chování jakožto druhého parametru vzájemné entropie, proto bez újmy

na obecnosti jeho definiční obor omezme na $\operatorname{Supp}\sigma$. Díky tomu podle (1.9) můžeme napsat $\log(\sigma) = \log(\lambda)P + \log(\mu)Q$. Také je $-S(R) = 0$ (viz 4.1.4). Následně můžeme díky linearitě stopy zapsat:

$$S(R\|\sigma) = \begin{cases} -(\log(\lambda)\operatorname{Tr}(RP) + \log(\mu)\operatorname{Tr}(RQ)), \text{ pro } \operatorname{Supp} R \subseteq \operatorname{Supp}\sigma, \\ \infty \text{ jinak.} \end{cases} \tag{4.8}$$

V případě, kdy je vzájemná entropie konečná, můžeme, vzhledem k tomu, že platí inkluze $\operatorname{Supp} R \subseteq \operatorname{Supp}\sigma = \operatorname{Supp}(P+Q)$ a tedy $R(P+Q) = R$, snadno spočítat:

$$\operatorname{Tr}(RP) + \operatorname{Tr}(RQ) = \operatorname{Tr}(R(P+Q)) = \operatorname{Tr}(R) = 1.$$

Jednotkový vektor $r \in \operatorname{Supp} R$ lze vyjádřit jako kombinaci jednotkových vektorů p, q, kde $p \in \operatorname{Supp} P, q \in \operatorname{Supp} Q$, tedy: $r = \alpha p + \beta q$. Pythagorova věta 1.2.4 s homogenitou normy navíc dá: $1 = \|r\| = |\alpha|^2 + |\beta|^2$. Parametr α tedy jistě můžeme volit z intervalu $\langle 0, 1\rangle$. To znamená, že:

$$\operatorname{Tr}(RP) = \operatorname{Tr}(P_r P_p) = |\langle r, p\rangle|^2 = |\langle \alpha p + \beta q, p\rangle|^2 = |\alpha \underbrace{\langle p, p\rangle}_{=1} + \beta \underbrace{\langle q, p\rangle}_{=0}|^2 = |\alpha|^2 = \alpha^2.$$

Protože R bylo libovolné, můžeme i parametr α v zadaném rozsahu libovolně měnit a tedy výraz $\operatorname{Tr}(RP)$ může nabýt libovolné hodnoty z intervalu $\langle 0, 1\rangle$. Spolu s tím, že $\operatorname{Tr}(RP) + \operatorname{Tr}(RQ) = 1$, z toho plyne, že vzájemná entropie $S(R\|\sigma)$ nabývá všech hodnot z intervalu $\langle -\log\mu, -\log\lambda\rangle$ sjednoceného s $\{\infty\}$. Z tohoto oboru hodnot tedy můžeme získat původní vlastní čísla operátoru σ. Vzhledem k tomuto pozorování, předpokladu, že φ zachová vzájemnou entropii a tomu, že $\varphi(R)$ může nabýt libovolné hodnoty z $\mathcal{P}_1(\mathbb{C}^n)$ (φ je bijekce), musí být operátor $\varphi(\sigma)$ ve tvaru:

$$\varphi(\sigma) = \lambda P' + \mu Q',$$

kde $P', Q' \in \mathcal{P}_1(\mathbb{C}^n)$ jsou vzájemně ortogonální. S ohledem na to, že je každý bod intervalu $\langle -\log\mu, -\log\lambda\rangle$ jednoznačně dán jako konvexní kombinace jeho koncových bodů, bude $S(R\|\sigma) = -\log\lambda$ právě když $\operatorname{Tr}(RP) = 1$. Navíc však v takovém případě bude:

$$\operatorname{Tr}(RP) = |\langle r, p\rangle|^2 = \|r\| \cdot \|p\| = 1,$$

což podle dovětku Caucho-Schwarzovy nerovnosti 1.2.5 nastává pouze když r, p jsou lineárně závislé, ale pak $R = P$. (r a p jsou stejné až na násobek komplexní jednotkou.) Dostáváme tak následující sadu ekvivalencí:

$$\begin{aligned} R = P &\iff S(R\|\sigma) = -\log\lambda \\ &\iff S(\varphi(R)\|\varphi(\sigma)) = -\log\lambda \\ &\iff S(\varphi(R)\|\lambda P' + \mu Q') = -\log\lambda \\ &\iff \varphi(R) = P', \end{aligned}$$

což dává $\varphi(P) = P'$. Analogicky bychom dostali $\varphi(Q) = Q'$. Dohromady tedy máme:

$$\varphi(\lambda P + \mu Q) = \lambda\varphi(P) + \mu\varphi(Q) \tag{4.9}$$

Speciálně, φ zachová vzájemnou ortogonalitu P, Q.

Nechť jsou teď P, R jiné projektory hodnosti 1, které nejsou vzájemně ortogonální. Dále nechť je teď Q projektor hodnosti 1 ortogonální na P a nechť platí inkluze podprostorů $\operatorname{Supp} R \subseteq \operatorname{Supp} P \oplus \operatorname{Supp} Q$. Zvolme $\lambda, \mu, 0 < \lambda < \mu = 1 - \lambda < 1$ jako výše. Z (4.8) a (4.9) dostaneme:

$$\begin{aligned} -(\log(\lambda)\operatorname{Tr}(RP) + \log(\mu)\operatorname{Tr}(RQ)) &= S(R\|\lambda P + \mu Q) = S(\varphi(R)\|\lambda\varphi(P) + \mu\varphi(Q)) = \\ &= -(\log(\lambda)\operatorname{Tr}(\varphi(R)\varphi(P)) + \log(\mu)\operatorname{Tr}(\varphi(R)\varphi(P))). \end{aligned} \tag{4.10}$$

Víme, že $\varphi(P), \varphi(Q)$ jsou vzájemně ortogonální a že:

$$\operatorname{Supp}\varphi(R) \subseteq \operatorname{Supp}\varphi(\lambda P + \mu Q) = \operatorname{Supp}(\lambda\varphi(P) + \mu\varphi(Q)) = \operatorname{Supp}\varphi(P) \oplus \operatorname{Supp}\varphi(Q).$$

Dvojice $\operatorname{Tr}(\varphi(R)\varphi(P)), \operatorname{Tr}(\varphi(R)\varphi(Q))$ tak opět bude mít jednotkový součet a nezáporné hodnoty. S ohledem na (4.10) a fakt, že prvek kompaktního intervalu lze jednoznačně určit koeficienty konvexní kombinace jeho krajních bodů, vyvodíme že:

$$\operatorname{Tr}(\varphi(R)\varphi(P)) = \operatorname{Tr}(RP).$$

Na $\mathcal{P}_1(\mathbb{C}^n)$ se tedy φ chová jako symetrie a podle Wignerovy věty 3.2.3 musí existovat unitární nebo antiunitární operátor V takový, že $\varphi(P) = V^{-1}PV$ pro každé $P \in \mathcal{P}_1(\mathbb{C}^n)$. Zbývá nám tedy rozšířit tento výsledek na $\mathcal{S}(\mathbb{C}^n)$. Uvažujme zobrazení $\psi : \rho \mapsto V^{-1}\varphi(\rho)V$. Ukážeme, že platí $\psi(\rho) = \rho$ pro všechna $\rho \in \mathcal{S}(\mathbb{C}^n)$. ψ je zřejmě bijektivní, navíc zachová vzájemnou entropii, neboť je složením zobrazení, zachovávajících vzájemnou entropii. (Viz první odstavec důkazu.) Podobně jako v (4.6) pro $P \in \mathcal{P}_1(\mathbb{C}^n)$ máme:

$$\operatorname{Supp} P \subseteq \operatorname{Supp}\rho \iff \operatorname{Supp} P = \operatorname{Supp}\psi(P) \subseteq \operatorname{Supp}\psi(\rho),$$

což dá $\operatorname{Supp}\rho = \operatorname{Supp}\psi(\rho)$. Navíc, pro každé takové P máme:

$$\operatorname{Tr}(P\log\rho) = -S(P\|\rho) = -S(\psi(P)\|\psi(\rho)) = -S(P\|\psi(\rho)) = \operatorname{Tr}(P\log\psi(\rho)).$$

Tuto rovnici můžeme pro jednotkový vektor $x \in \operatorname{Supp} P$ podle (3.5) přepsat na:

$$\langle\log(\rho)x, x\rangle = \langle\log(\psi(\rho))x, x\rangle,$$

z čehož dle 1.3.2 (b) plyne $\log(\rho) = \log(\psi(\rho))$ a tedy $\rho = \psi(\rho) = V^{-1}\varphi(\rho)V$, což uzavírá důkaz, jelikož $\varphi(\rho) = V^{-1}\rho V$ pro všechny operátory hustoty ρ. □

Poznámka 4.2.3. Ukazuje se, že znění věty lze zajímavě zobecnit – předpoklad bijektivity zobrazení φ je možné vypustit a závěr bude stále platit. Důkaz je pak pochopitelně ještě delší. Zde ho neuvádíme, je možné jej nalézt v článku [11].

Závěr

V této práci jsme studovali některé aspekty teorie operátorů a pomocí aparátu Jordanových $*$-izomorfismů též Wignerovu větu. Tyto matematické nástroje jsme využili v důkazu Molnárovy věty, charakterizující zobrazení zachovávající vzájemnou kvantovou entropii, kterou lze považovat za završení této práce. Výsledek, že zobrazení zachovávající vzájemnou kvantovou entropii jsou wignerovského typu, není na první pohled vůbec zřejmý: Vzájemná entropie je jasně nelineární funkcí, přesto zobrazení která jí zachovávají, lineární být musí. Při své analýze úlohy Wignerovy věty v kvantové teorii informace jsme s úspěchem použili lineárně algebraický, potažmo maticový přístup k popisu kvantových automorfismů. Zdá se nám, že tento originální důkaz by mohl přispět k obsáhlé literatuře existující v této oblasti.

Vzájemná kvantová entropie je jedním ze základních pojmů v kvantové teorii informace, potažmo ve vývoji kvantové výpočetní techniky. Je proto důležité vědět, jaké druhy operací můžeme se systémem provádět, aby se tato veličina nezměnila. K tomu nám dává návod právě Molnárova věta.

V tomto tématu vidíme několik možností dalšího zkoumání. První co se nabízí je pokusit se výsledek zobecnit i do Hilbertových prostorů nekonečné dimenze, které mají ve fyzice významnou roli. Jinou možností je studovat jak mohou vypadat unitární/antiunitární zobrazení vyskytující se v Molnárově větě (nejsou totiž dána jednoznačně) a vyvinout metody jak tato zobrazení určit například podle působení φ na nějakou bázi. Z více inženýrského hlediska by mohla být zajímavá nějaká studie, pojednávající o aplikaci, či možnostech aplikace, těchto výsledků v technice.

Tento text je psán v rámci možností co nejpřístupnějším způsobem a snad jako takový bude užitečnou pomůckou novým zájemcům o toto téma.

Literatura

[1] BOHATA, M.: *Technique of operator algebras in quantum structures*. Dizertační práce, FEL ČVUT, 2013.

[2] GLEASON, A. M.: Measures on the closed subspaces of a Hilbert space. *Journal of Mathematics and Mechanics*, 1957.

[3] HAMHALTER, J.: *Quantum Measure Theory*. Springer, 2003.

[4] HAMHALTER, J.: Pokročilá analýza - poznámky k přednáškám, 2012.

[5] MOLNÁR, L.: *Selected Preserver Problems on Algebraic Structures of Linear Operators and on Function Spaces*. Springer, 2007.

[6] MOLNÁR, L.: Maps on states preserving the relative entropy. *Journal of Mathematical Physics*, 2008.

[7] NIELSEN, M. A.; CHUANG, I. L.: *Quantum Computation and Quantum Information*. Cambridge University Press, 2001.

[8] OLŠÁK, P.: *Úvod do algebry, zejména lineární*. FEL ČVUT, 2007.

[9] RUDIN, W.: *Analýza v reálném a komplexním oboru*. Academia, 1977.

[10] SIMON, R.; MUKUNDA, N.; CHATURVEDI, S.; aj.: Two elementary proofs of the Wigner theorem on symmetry in quantum mechanics. *Physics Letters A*, 2008.

[11] SZOKOL, P.; MOLNÁR, L.: Maps on states preserving the relative entropy II. *Linear Algebra and it's Applications*, 2010.

[12] ZAHRADNÍK, M.; MOTL, L.: *Pěstujeme lineární algebru*. Karolinum, 1995.