POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Imię i nazwisko studenta: Wojciech Wantka
Nr albumu: 126689
Studia drugiego stopnia
Forma studiów: stacjonarne
Kierunek studiów: Informatyka
Specjalność: Algorytmy i technologie internetowe

# PRACA DYPLOMOWA MAGISTERSKA

Tytuł pracy w języku polskim: Optymalizacja półokreślona w wykrywaniu splątania kwantowego

Tytuł pracy w języku angielskim: Semidefinite programming for entanglement detection

| Potwierdzenie przyjęcia pracy | |
|---|---|
| Opiekun pracy<br><br>podpis | Kierownik Katedry/Zakładu (pozostawić właściwe)<br><br>podpis |
| dr inż. Piotr Mironowicz | |

Data oddania pracy do dziekanatu:

POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

**OŚWIADCZENIE dotyczące pracy dyplomowej zatytułowanej: Optymalizacja półokreślona w wykrywaniu splątania kwantowego**

Imię i nazwisko studenta: Wojciech Wantka
Data i miejsce urodzenia: 27.09.1990, Kartuzy
Nr albumu: 126689
Wydział: Wydział Elektroniki, Telekomunikacji i Informatyki
Kierunek: informatyka
Poziom kształcenia: drugi
Forma studiów: stacjonarne

Świadomy(a) odpowiedzialności karnej z tytułu naruszenia przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 2017 poz. 880 z późn. zm.) i konsekwencji dyscyplinarnych określonych w ustawie Prawo o szkolnictwie wyższym (Dz.U. 2017 poz. 2183 z późn. zm.),[1] a także odpowiedzialności cywilnoprawnej oświadczam, że przedkładana praca dyplomowa została opracowana przeze mnie samodzielnie.

Niniejsza praca dyplomowa nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadaniem tytułu zawodowego.

Wszystkie informacje umieszczone w ww. pracy dyplomowej, uzyskane ze źródeł pisanych i elektronicznych, zostały udokumentowane w wykazie literatury odpowiednimi odnośnikami zgodnie z art. 34 ustawy o prawie autorskim i prawach pokrewnych.

Potwierdzam zgodność niniejszej wersji pracy dyplomowej z załączoną wersją elektroniczną.

Gdańsk, dnia .....  .....
*podpis studenta*

[1] Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym:
Art. 214 ustęp 4. W razie podejrzenia popełnienia przez studenta czynu podlegającego na przypisaniu sobie autorstwa istotnego fragmentu lub innych elementów cudzego utworu rektor niezwłocznie poleca przeprowadzenie postępowania wyjaśniającego.
Art. 214 ustęp 6. Jeżeli w wyniku postępowania wyjaśniającego zebrany materiał potwierdza popełnienie czynu, o którym mowa w ust. 4, rektor wstrzymuje postępowanie o nadanie tytułu zawodowego do czasu wydania orzeczenia przez komisję dyscyplinarną oraz składa zawiadomienie o popełnieniu przestępstwa.

## STRESZCZENIE

W pracy przedstawiono podstawy programowania półokreślonego oraz problematykę separowalności macierzy gęstości, wraz z podaniem niezbędnej wiedzy z algebry liniowej. Praca objęła implementację potrzebnych narzędzi do formułowania warunków separowalności macierzy w oparciu o framework (np. pakiety SeDuMi i YALMIP w środowisku MATLAB/OCTAVE) oraz zilustrowanie zastosowań tych narzędzi na zaproponowanych przykładach.

Wykonane zadania:

1. Przegląd literatury odnośnie programowania półokreślonego
2. Wprowadzenie do metod informatyki kwantowej
3. Implementacja narzędzia w postaci skryptów w języku MATLAB
4. Sporządzenie dokumentacji skryptów oraz przykładów

**Słowa kluczowe:** informatyka kwantowa
**Dziedzina nauki:** Nauki o komputerach i informatyka

## ABSTRACT

In the thesis presented the methods of semidefinite programming and the problem of separability of density matrices, with presenting fundamental knowledge on linear algebra. The thesis includes the implementation of necessary tools formulating conditions for matrix separation based on available frameworks (e.g. SeDuMi and YALMIP packages in MATLAB/OCTAVE) and illustrated the use of these tools with proposed examples.

Tasks done:

1. Overview of the literature on semidefinite programming
2. Introduction to quantum information
3. Implementation of tools as scripts in MATLAB
4. Documentation of scripts and examples of their applications

**Keywords:** quantum information
**Field of science and keywords:** Computer and information sciences

## SPIS TREŚCI

## WYKAZ WAŻNIEJSZYCH OZNACZEŃ I SKRÓTÓW

$[n]$ – dla liczby naturalnej $n$ oznacza zbiór $\{0, 1, \ldots, n-1\}$

# 1. PODSTAWY ALGEBRAICZNE

## *1.1. Przestrzeń Hilberta*

Weźmy przestrzeń liniową wymiaru $n$ nad $\mathbb{C}$ i wyposażmy ją w iloczyn skalarny. Tak powstałą strukturę nazwiemy *przestrzenią Hilberta* (ogólnie, tzn. nie skonkretyzowaną w żaden sposób przestrzeń Hilberta oznaczać będziemy $\mathcal{H}$). Element (wektor) tej przestrzeni oznaczamy $|\psi\rangle$, natomiast iloczyn skalarny pomiędzy dwoma wektorami $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ oznaczymy $\langle\psi|\phi\rangle$ (taka konwencja określana jest mianem *notacji Diraca*). Przypomnijmy jeszcze, że na przestrzeni Hilberta indukowana jest za pomocą iloczynu skalarnego *norma* wektora, standardowo $||\psi|| \equiv \sqrt{\langle\psi|\psi\rangle}$.

### *1.1.1. Baza kanoniczna*

Jako $\mathcal{B} \equiv \{|i\rangle\}_{i\in I}$ oznaczmy bazę przestrzeni $\mathcal{H}$. Zakładamy też, że $\mathcal{B}$ stanowi ortonormalny układ wektorów – w przestrzeniach o skończonym wymiarze jesteśmy bowiem w stanie zastosować procedurę Grama-Schmidta. Dla ustalenia uwagi przyjmijmy $I \equiv \{0, 1, \ldots, n-1\}$ – przy takich oznaczeniach bazę $\mathcal{B}$ nazywamy bazą *kanoniczną*. Przyjmuje się, że wektory bazy kanonicznej oznaczamy

$$|i\rangle \equiv \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

gdzie nad współczynnikiem $1$ znajduje się $i$ zer.

Dowolny wektor $|\psi\rangle \in \mathcal{H}$ zapiszemy teraz jako

$$|\psi\rangle = \sum_{i\in I} \psi_i |i\rangle .$$

Założenie o skończonym wymiarze przestrzeni skutkuje wygodną reprezentacją w bazie $\mathcal{B}$ abstrakcyjnego wektora z przestrzeni Hilberta jako kolumny jego współczynników:

$$|\psi\rangle \equiv \begin{pmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{n-1} \end{pmatrix}.$$

### 1.1.2. *Współczynniki wektora w bazie ortonormalnej*

Przypomnimy obecnie wzór na współczynniki wektora w rozwinięciu w bazie $\mathcal{B}$, która zgodnie z założeniem stanowi układ ortonormalny, tzn.

$$\langle i|j\rangle = \delta_{ij},$$

gdzie dwuargumentowa funkcja $\delta_{ij}$, zwana *deltą Kroneckera*:

$$\delta_{ij} \equiv \begin{cases} 1, \text{dla } i = j \\ 0, \text{dla } i \neq j \end{cases}$$

Niech więc dowolnie ustalony wektor bazowy $|\alpha\rangle$ zostanie przemnożony skalarnie przez wektor $|\psi\rangle$. Pamiętając o własnościach iloczynu skalarnego (liniowość w drugim składniku) napiszemy

$$\langle\alpha|\psi\rangle = \langle\alpha| \left( \sum_i \psi_i |i\rangle \right) = \sum_i \psi_i \langle\alpha|i\rangle = \sum_i \psi_i \delta_{\alpha i} = \psi_\alpha$$

tzn.

$$\psi_\alpha = \langle\alpha|\psi\rangle .$$

### 1.1.3. *Iloczyn skalarny – równoważne podejście*

Iloczyn skalarny wektorów $|\psi\rangle , |\phi\rangle \in \mathcal{H}$ można wyznaczyć wprost z definicji funkcji $\langle\psi|\phi\rangle$, a także za pomocą sumy współczynników tych wektorów. Dla

$$|\psi\rangle = \sum_{i\in I} \psi_i |i\rangle$$

oraz

$$|\phi\rangle = \sum_{i\in I} \phi_i |i\rangle$$

mamy bowiem

$$\langle\psi|\phi\rangle = \left( \sum_{i\in I} \psi_i \langle i| \right) \left( \sum_{j\in I} \phi_j |j\rangle \right) = \sum_{i,j\in I} \psi_i^* \phi_j \langle i|j\rangle = \sum_{i\in I} \psi_i^* \phi_i$$

### 1.1.4. *Przestrzeń sprzężona*

Samo wyrażenie $\langle\psi|\phi\rangle$ także w konwencji Diraca traktować można dwojako – formalnie bowiem w drugim składniku iloczynu skalarnego występują wektory postaci $|\cdot\rangle$ rozpatrywanej przestrzeni Hilberta $\mathcal{H}$, nazywane *ketami*, natomiast w pierwszym – wektory zapisywane jako $\langle\cdot|$,

nazywane *bra* (oba te pojęcia pochodzą od słowa *bracket*). Wektory *bra* definiuje się ściśle jako elementy *przestrzeni sprzężonej* do przestrzeni $\mathcal{H}$.

**Definicja 1.** *Przestrzenią sprzężoną do przestrzeni Hilberta $\mathcal{H}$ nazywamy przestrzeń $\mathcal{H}^*$ liniowych funkcjonałów $\langle\cdot| : \mathcal{H} \to \mathbb{C}$.*

**Uwaga 2.** *Funkcjonały z przestrzeni sprzężonej są liniowe, ponieważ iloczyn skalarny jest liniowy w drugim argumencie.*

Okazuje się, że w przestrzeniach Hilberta o wymiarze skończonym występuje wzajemna jednoznaczność bra i ketów, tzn. wektor $|\psi\rangle \in \mathcal{H}$ można rozpatrywać równoważnie jako wektor $\langle\psi| \in \mathcal{H}^*$ powstały z $|\psi\rangle$ na drodze przekształcenia, które w przestrzeniach o skończonym wymiarze wygląda następująco: z reprezentacji wektora jako kolumny współczynników i z formuły na iloczyn skalarny w bazie ortonormalnej mamy, że dla danego keta

$$|\psi\rangle = \begin{pmatrix} \psi_0 \\ \psi_1 \\ \vdots \\ \psi_{n-1} \end{pmatrix}$$

odpowiadający mu funkcjonał $\langle\psi| \in \mathcal{H}^*$ można zapisać jako

$$\langle\psi| = \begin{pmatrix} \psi_0^* & \psi_1^* & \dots & \psi_{n-1}^* \end{pmatrix}.$$

Wobec tego, bra powstaje z keta na skutek transpozycji i sprzężenia zespolonego. Teraz iloczyn skalarny $\langle\psi|\phi\rangle$ wektorów $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ uzyskuje dodatkowy sens zwykłego mnożenia wiersza przez kolumnę.

### *1.1.5. Podstawowe bazy*

Podamy definicje podstawowych baz pojawiających się w kwantowej informatyce.

**Definicja 3** (Baza Hadamarda)**.**

$$|0'\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|1'\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

**Definicja 4** (Baza Bella)**.**

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |3\rangle)$$

$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |3\rangle)$$

$$\left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$$

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle)$$

### *1.2. Przestrzeń Hilberta-Schmidta*

Dla danej przestrzeni Hilberta $\mathcal{H}$ z bazą $\mathcal{B}$ wprowadzamy przestrzeń operatorów liniowych $A : \mathcal{H} \to \mathcal{H}$ z działaniem standardowego dodawania dwóch operatorów i działaniem mnożenia operatora przez liczbę zespoloną. Przestrzeń taka jest przestrzenią liniową. Wyposażamy ją w działanie dwuargumentowe postaci

$$\langle A|B\rangle \equiv \mathbf{Tr}[A^{\dagger}B].$$

Łatwo pokazać, że tak zdefiniowana funkcja jest iloczynem skalarnym (nazywamy ją iloczynem skalarnym Hilberta–Schmidta) – przestrzeń operatorów rozszerzyliśmy wobec tego do przestrzeni Hilberta. Nazywamy ją przestrzenią Hilberta-Schmidta sprzężoną z przestrzenią $\mathcal{H}$ i oznaczamy $\mathcal{HS}$.

#### *1.2.1. Elementy macierzowe, ślad, komutator*

Przedstawimy podstawowe definicje i własności operatorów.

**Definicja 5.** *Elementem macierzowym w bazie $\mathcal{B}$ operatora liniowego $A$ nazywamy liczbę*

$$A_{ij} \equiv \langle i| A |j\rangle ,$$

*gdzie $|i\rangle , |j\rangle \in \mathcal{B}$. Ponadto, elementy macierzowe postaci $A_{ii}$ nazywamy elementami diagonalnymi operatora $A$.*

Operator $A$ można zapisać w następujący sposób:

$$A = \sum_{i,j \in I} A_{ij} |i\rangle \langle j| .$$

**Uwaga 6.** *Zapis postaci $\langle \cdot | \cdot | \cdot \rangle$ stosujemy w celach mnemotechnicznych – obowiązuje tutaj ogólna konwencja notacyjna:*

- $|A\psi\rangle \equiv A |\psi\rangle$
- $\langle A\psi| \equiv \langle \psi| A^{\dagger}$

**Definicja 7** (Ślad operatora)**.** *Śladem operatora liniowego $A$ nazywamy sumę jego elementów diagonalnych:*

$$\boldsymbol{Tr}[A] \equiv \sum_{i \in I} A_{ii}.$$

**Twierdzenie 8** (Ślad operatora jest cykliczny)**.** *Zachodzi*

$$\boldsymbol{Tr}[AB] = \boldsymbol{Tr}[BA]$$

Wprowadzimy teraz pojęcie *komutatora* operatorów liniowych.

**Definicja 9** (Komutator)**.** *Dla operatorów liniowych $A$ oraz $B$ działających na przestrzeni Hilberta $\mathcal{H}$ ich komutator definiujemy jako operator liniowy*

$$[A, B] \equiv A \circ B - B \circ A,$$

*gdzie działanie $\circ$ oznacza złożenie operatorów (w przypadku skończenie wymiarowym i reprezentacji macierzowej operatora jest to mnożenie macierzy). Ponadto, jeżeli $[A, B] = \hat{0}$ (gdzie $\hat{0}$ jest operatorem zerowym) to mówimy, że operatory $A$ i $B$ komutują.*

### *1.2.2. Operatory hermitowskie*

Wprowadzimy pojęcie operatora hermitowskiego i podamy jego podstawowe własności.

**Definicja 10** (Sprzężenie hermitowskie)**.** *Niech $|\psi\rangle, |\phi\rangle \in \mathcal{H}$, natomiast $A$ niech jest operatorem liniowym z $\mathcal{H}$ do $\mathcal{H}$. Operatorem sprzężonym hermitowsko do $A$ nazywamy operator*

$$A^\dagger \equiv (A^*)^T = (A^T)^*.$$

**Definicja 11** (Operator hermitowski)**.** *Operator liniowy $A$ nazywamy hermitowskim (samosprzężonym), gdy*

$$A = A^\dagger$$

**Twierdzenie 12.** *Wartości własne operatora hermitowskiego są rzeczywiste.*

### *1.2.3. Operatory dodatnio określone*

Wprowadzimy pojęcie i podamy podstawowe własności operatorów dodatnio określonych.

**Definicja 13** (Operator dodatnio określony)**.** *Operator liniowy $A$ nazywamy dodatnio określonym, gdy*

$$\forall_{|\psi\rangle \in \mathcal{H}} \langle\psi| A |\psi\rangle \geqslant 0.$$

*Piszemy wtedy $A \geqslant 0$.*

**Twierdzenie 14.** *Operator dodatnio określony jest hermitowski.*

**Twierdzenie 15.** *Wartości własne operatora dodatnio określonego są nieujemnymi liczbami rzeczywistymi.*

**Twierdzenie 16.** *Jeżeli $A$ jest operatorem liniowym, to operator $A^\dagger A$ jest dodatnio określony.*

*Dowód.* Niech $|\psi\rangle \in \mathcal{H}$ będzie dowolnym wektorem. Wtedy

$$\langle\psi| A^\dagger A |\psi\rangle = \langle A\psi|A\psi\rangle = \|A|\psi\rangle\|^2 \geqslant 0,$$

więc $A^\dagger A$ jest operatorem dodatnio określonym. □

**Twierdzenie 17.** *Jeżeli $A$, $B$ są operatorami na $\mathcal{H}$ dodatnio określonymi, to ich suma $A + B$ jest operatorem dodatnio określonym.*

*Dowód.* Niech $|\psi\rangle \in \mathcal{H}$. Wtedy

$$\langle\psi| (A + B) |\psi\rangle = \langle\psi| A |\psi\rangle + \langle\psi| B |\psi\rangle \geqslant 0.$$

□

Jako definicję operatora dodatnio określonego równoważną definicji 13 można przyjąć poniższą definicję *operatora dodatniego* (nazwa została przyjęta jedynie po to, aby odróżnić od siebie dokładne treści obu definicji):

**Definicja 18** (Operator dodatni)**.** *Operator liniowy $A$ nazywamy dodatnim, gdy jest hermitowski i ma nieujemne spektrum.*

Okazuje się bowiem, że z twierdzeń 14 oraz 15 wynika

**Wniosek 19.** *Operator liniowy $A$ jest dodatnio określony $\iff$ jest dodatni.*

### *1.3. Iloczyn tensorowy*

#### *1.3.1. Definicja ogólna*

W niniejszym paragrafie postaramy się przedstawić w możliwie najogólniejszy sposób definicję iloczynu tensorowego, podając następnie praktyczną jego realizację w przestrzeniach o wymiarze skończonym.

Weźmy dwie przestrzenie Hilberta $\mathcal{H}_A$ i $\mathcal{H}_B$. Dla wektorów $|A\rangle \in \mathcal{H}_A$ oraz $|B\rangle \in \mathcal{H}_B$ wektor będący ich *iloczynem tensorowym* (oznaczany $|A\rangle \otimes |B\rangle$) formalnie jest elementem przestrzeni będącej *iloczynem tensorowym przestrzeni* $\mathcal{H}_A$ i $\mathcal{H}_B$. Najpierw wprowadzimy więc pojęcie iloczynu tensorowego przestrzeni, a następnie – definicję działania mnożenia tensorowego wektorów.

**Definicja 20** (Iloczyn tensorowy przestrzeni)**.** *Iloczynem tensorowym przestrzeni Hilberta $\mathcal{H}_A$ (z ortonormalną bazą $\left|i^A\right\rangle$) i $\mathcal{H}_B$ (z ortonormalną bazą $\left|j^B\right\rangle$) nazywamy przestrzeń*

$$\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B,$$

*której elementy stanowią wszystkie wektory postaci*

$$|C\rangle \equiv |A\rangle \otimes |B\rangle \,, dla \;\; |A\rangle \in \mathcal{H}_A, |B\rangle \in \mathcal{H}_B. \tag{1}$$

*Dodatkowo, wektory tej przestrzeni stanowią z definicji wszystkie kombinacje liniowe układu wektorów $\left|i^A\right\rangle \otimes \left|j^B\right\rangle$, tzn. zbiór wektorów postaci*

$$|C\rangle = \sum_{ij} c_{ij} \left|i^A\right\rangle \otimes \left|j^B\right\rangle . \tag{2}$$

**Definicja 21** (Iloczyn tensorowy wektorów)**.** *Dla danych przestrzeni Hilberta $\mathcal{H}_A$ oraz $\mathcal{H}_B$ działanie mnożenia tensorowego wektorów z $\mathcal{H}_A$ z wektorami z $\mathcal{H}_B$ definiuje się jako funkcję $\otimes : \mathcal{H}_A \times \mathcal{H}_B \to \mathcal{H}_{AB}$, mającą własność liniowości w obu swoich składnikach, tzn.*

1. ***Jednorodność w obu składnikach.*** *Dla każdego skalara $z \in \mathbb{C}$ i dla każdych wektorów $A \in \mathcal{H}_A$ oraz $B \in \mathcal{H}_B$*

$$z(|A\rangle \otimes |B\rangle) = (z\,|A\rangle) \otimes |B\rangle = |A\rangle \otimes (z\,|B\rangle)$$

2. ***Addytywność w pierwszym składniku.*** *Dla każdych wektorów $|A_1\rangle , |A_2\rangle \in \mathcal{H}_A$ oraz $|B\rangle \in \mathcal{H}_B$*

$$(|A_1\rangle + |A_2\rangle) \otimes |B\rangle = |A_1\rangle \otimes |B\rangle + |A_2\rangle \otimes |B\rangle$$

3. ***Addytywność w drugim składniku.*** *Dla każdych wektorów $|A\rangle \in \mathcal{H}_A$ oraz $|B_1\rangle , |B_2\rangle \in \mathcal{H}_B$*

$$|A\rangle \otimes (|B_1\rangle + |B_2\rangle) = |A\rangle \otimes |B_1\rangle + |A\rangle \otimes |B_2\rangle$$

**Uwaga 22** (Oznaczenia)**.** *Dla $|A\rangle \in \mathcal{H}_A$ i $|B\rangle \in \mathcal{H}_B$ oznaczać będziemy*

$$|A\rangle \otimes |B\rangle \equiv |A\rangle\,|B\rangle .$$

*Czasem piszemy nawet $|A\rangle \otimes |B\rangle \equiv |AB\rangle$.*

**Uwaga 23.** *Z liniowości iloczynu tensorowego wynika, że każdy wektor z $\mathcal{H}_{AB}$ postaci (1) można zapisać w postaci (2). Dla*

$$|A\rangle = \sum_i c_i^{(A)} \left|i^{(A)}\right\rangle$$

*oraz*

$$|B\rangle = \sum_j c_j^{(B)} \left|j^{(B)}\right\rangle$$

*mamy bowiem*

$$|A\rangle\,|B\rangle = \left(\sum_i c_i^{(A)} \left|i^{(A)}\right\rangle\right) \left(\sum_j c_j^{(B)} \left|j^{(B)}\right\rangle\right)$$

$$= \sum_{ij} c_i^{(A)} c_j^{(B)} \left| i^{(A)} \right\rangle \left| j^{(B)} \right\rangle = \sum_{ij} c_{ij} \left| i^{(A)} \right\rangle \left| j^{(B)} \right\rangle ,$$

*jeżeli tylko* $c_{ij} \equiv c_i^{(A)} c_j^{(B)}$.

*Implikacja odwrotna jednak nie zachodzi: nie każdy wektor dany w postaci (2) da się zapisać w postaci (1) (podamy później przykład takiego wektora). Ta własność zdefiniowanej przez nas struktury iloczynu tensorowego będzie miała wielkie znaczenie przy wprowadzaniu pojęcia splątania.*

**Uwaga 24.** *O tych wektorach przestrzeni* $\mathcal{H}_{AB}$*, które można zapisać w postaci (1) mówimy, że są wektorami produktowymi.*

### *1.3.2. Iloczyn tensorowy w przestrzeniach o skończonym wymiarze*

Podamy teraz definicję iloczynu tensorowego w przestrzeniach Hilberta o wymiarze skończonym określonych nad $\mathbb{C}$.

Wprowadzimy najpierw pewne działanie wykonywane na macierzach – rozważane ogólnie nie ma ono nic wspólnego z teorią kwantów.

**Definicja 25** (Iloczyn Kroneckera macierzy)**.** *Dla macierzy*

$$A \in M_{p\times q}(\mathbb{C})$$

*i*

$$B \in M_{r\times s}(\mathbb{C})$$

*ich iloczyn Kroneckera zdefiniowany jest jako macierz*

$$C \in M_{pr\times qs}(\mathbb{C})$$

*dana wzorem*

$$C \equiv A \otimes B = \begin{pmatrix} A_{00}B & A_{01}B & \dots & A_{0,q-1}B \\ A_{10}B & A_{11}B & \dots & A_{1,q-1}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{p-1,0}B & A_{p-1,1}B & \dots & A_{p-1,q-1}B \end{pmatrix}. \tag{3}$$

**Przykład 26** (Iloczyn Kroneckera)**.** *Dla danych macierzy*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

$$B = \begin{pmatrix} e & f & g \\ h & i & j \end{pmatrix}$$

*ich iloczyn Kroneckera przyjmuje wartość*

$$C = \begin{pmatrix} aB & bB \\ cB & dB \end{pmatrix} = \begin{pmatrix} ae & af & ag & be & bf & bg \\ ah & ai & aj & bh & bi & bj \\ ce & cf & cg & de & df & dg \\ ch & ci & cj & dh & di & dj \end{pmatrix}$$

Podamy podstawowe własności iloczynu Kroneckera.

**Twierdzenie 27.** *Jeżeli $A$, $B$, $C$, $D$ są macierzami takimi, że wyrażenia $AC$ i $BD$ mają sens jako mnożenie algebraiczne macierzy, to*

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD), \tag{4}$$

*gdzie $\otimes$ jest iloczynem Kroneckera macierzy.*

Można też udowodnić twierdzenie ogólniejsze:

**Twierdzenie 28.** *Niech $|a_1\rangle, |a_2\rangle \in \mathcal{H}_A$, $|b_1\rangle, |b_2\rangle \in \mathcal{H}_B$. Wówczas*

$$(|a_1\rangle |b_1\rangle)(\langle a_2| \langle b_2|) = |a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|. \tag{5}$$

Ponadto mamy

**Twierdzenie 29.** *Jeżeli $A$, $B$ są macierzami, to*

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger. \tag{6}$$

**Wniosek 30.** *Iloczyn Kroneckera zachowuje hermitowskość, tzn. jeżeli macierze $A$ i $B$ są hermitowskie, to macierz $A \otimes B$ również.*

Można też pokazać, że w odniesieniu do operatora **Tr** mamy następujące

**Twierdzenie 31.** *Jeżeli $A$ i $B$ są dowolnymi macierzami kwadratowymi, to*

$$\boldsymbol{Tr}[A \otimes B] = \boldsymbol{Tr}[A] \cdot \boldsymbol{Tr}[B]. \tag{7}$$

Należy podkreślić, że działanie (3) *spełnia własności iloczynu tensorowego*. Pokażemy później, że w kwantowej teorii informacji interesującymi nas przestrzeniami Hilberta są zwykłe $n$-wymiarowe przestrzenie kolumn liczb zespolonych $V^n(\mathbb{C})$ i sprzężone z nimi przestrzenie Hilberta–Schmidta, tzn. przestrzenie macierzy kwadratowych wymiaru $n$: $M_{n\times n}(\mathbb{C})$. Naturalnym rozwiązaniem jest przyjęcie w tych przestrzeniach iloczynu tensorowego według reguły (3). Wobec tego, w kwantowej teorii informacji iloczyn tensorowy oznacza po prostu iloczyn Kroneckera.

Uogólnimy obecnie rozważania podane w definicji 5.

Niech dane są skończenie wymiarowe przestrzenie Hilberta $\mathcal{H}_A$ oraz $\mathcal{H}_B$ z bazami odpowiednio

$$\{|a_i\rangle\}_{i\in[n_A]}$$

oraz

$$\{|b_j\rangle\}_{j\in[n_B]}.$$

Niech dany jest też operator liniowy $A$ działający na przestrzeni $\mathcal{H}_A \otimes \mathcal{H}_B$. Dla

$$i,k \in [n_A],$$

$$j,l \in [n_B]$$

elementem macierzowym tego operatora w bazie $\{|a_i\rangle |b_j\rangle\}_{i\in[n_A],j\in[n_B]}$ przestrzeni złożonej nazywamy liczbę

$$A_{\substack{ij\\kl}} \equiv \langle a_i| \langle b_j| A |a_k\rangle |b_l\rangle .$$

Operator $A$ zapiszemy wtedy w rozważanej bazie jako

$$A = \sum_{i,k\in[n_A];j,l\in[n_B]} A_{\substack{ij\\kl}} (|a_i\rangle |b_j\rangle)(\langle a_k| \langle b_l|)$$

$$\overset{Tw.28}{=} \sum_{i,k\in[n_A];j,l\in[n_B]} A_{\substack{ij\\kl}} |a_i\rangle \langle a_k| \otimes |b_j\rangle \langle b_l| . \tag{8}$$

### *1.4. Twierdzenie spektralne*

#### *1.4.1. Projektory*

**Definicja 32.** *Niech $\mathcal{H}_A$, $\mathcal{H}_B$ będą skończenie wymiarowymi przestrzeniami Hilberta. Dla $|A\rangle \in \mathcal{H}_A$ i $|B\rangle \in \mathcal{H}_B$ wyrażenie $|A\rangle \langle B|$ wyznaczone według reguły (3) i będące wektorem z przestrzeni $\mathcal{H}_A \otimes \mathcal{H}_B^*$, gdzie $\mathcal{H}_B^*$ jest przestrzenią sprzężoną do przestrzeni $\mathcal{H}_B$, nazywamy iloczynem zewnętrznym wektorów $|A\rangle$ i $|B\rangle$.*

Niech dana jest przestrzeń Hilberta $\mathcal{H}$ wymiaru $n$ z bazą ortonormalną $\{|i\rangle\}_{i=0}^{n-1}$. Wtedy (zob. 1.1.2) dowolny wektor $|\psi\rangle \in \mathcal{H}$ można zapisać jako

$$|\psi\rangle = \sum_{i=0}^{n-1} |i\rangle \underbrace{\langle i|\psi\rangle}_{\psi_i}.$$

Każdemu wektorowi $|i\rangle$ z bazy przypiszmy teraz operator liniowy $|i\rangle \langle i| : \mathcal{H} \to \mathcal{H}$, którego działanie zdefiniujemy następująco:

$$(|i\rangle \langle i|) |\psi\rangle \equiv |i\rangle \langle i|\psi\rangle .$$

Wtedy

$$|\psi\rangle = \left(\sum_{i=0}^{n-1} |i\rangle\langle i|\right)|\psi\rangle,$$

tzn.

$$\sum_{i=0}^{n-1} |i\rangle\langle i| = I. \tag{9}$$

Oznaczmy

$$\Pi_i \equiv |i\rangle\langle i|, i = 0, 1, \ldots, n-1.$$

**Definicja 33.** *Niech dana jest przestrzeń liniowa i jej podprzestrzeń $V$. Niech bazą podprzestrzeni $V$ jest $\mathcal{B}_V$. Projektorem rzutującym na podprzestrzeń $V$ nazywamy operator*

$$\Pi_V \equiv \sum_{|i\rangle \in \mathcal{B}_V} |i\rangle\langle i|.$$

*Ponadto, jeżeli baza $\mathcal{B}_V$ jest układem ortonormalnym, to projektor $\Pi_V$ nazywamy ortonormalnym.*

Własność (9) układu ortonormalnych projektorów $\{|i\rangle\langle i|\}_{i=0}^{n-1}$ nazywamy *rozkładem identyczności*. Ponadto, złożenie dwóch projektorów z tego układu spełnia

$$\Pi_i \Pi_j = \delta_{ij} \Pi_i.$$

Mamy bowiem dla dowolnego wektora $|\psi\rangle \in \mathcal{H}$

$$\Pi_i \Pi_j |\psi\rangle = \Pi_i |j\rangle\langle j|\psi\rangle = |i\rangle\langle i|j\rangle\langle j|\psi\rangle = \delta_{ij}\Pi_i|\psi\rangle.$$

Latwo też pokazać, że konstrukcja skończenie wymiarowych projektorów ortonormalnych za pomocą iloczynu Kroneckera implikuje ich hermitowskość.

**Fakt 34.** *Projektory ortonormalne są operatorami dodatnio określonymi.*

*Dowód.* Jeżeli $\Pi$ jest projektorem ortonormalnym, to

$$\Pi^\dagger \Pi = \Pi^2 = \Pi.$$

Z drugiej strony, z twierdzenia 16 wynika, że operator $\Pi^\dagger\Pi$ jest dodatnio określony. □

### *1.4.2. Rozkład spektralny*

Przedstawimy tutaj ideę *rozkładu spektralnego* operatora. Samo pojęcie zdefiniujemy rozważając przypadek, gdy działa on w pewnej przestrzeni Hilberta $\mathcal{H}$. Konstrukcję uogólnimy następnie do przestrzeni $\mathcal{H}_{AB} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$.

**Przestrzeń $\mathcal{H}$** Rozważmy operator liniowy $A$ działający w przestrzeni Hilberta $\mathcal{H}$.

**Definicja 35.** *Mówimy, że operator liniowy $A$ ma rozkład spektralny, gdy da się go przedstawić w postaci*

$$A = \sum_{\lambda \in \sigma(A)} \lambda \Pi_\lambda,$$

*gdzie $\sigma(A)$ jest zbiorem różnych wartości własnych operatora $A$, natomiast $\Pi_\lambda$ jest projektorem ortonormalnym rzutującym na podprzestrzeń własną odpowiadającą wartości własnej $\lambda$.*

**Definicja 36** (Operator normalny)**.** *Operator liniowy $A$ nazywamy normalnym gdy*

$$A^\dagger A = A A^\dagger$$

**Twierdzenie 37** (Twierdzenie Spektralne)**.** *Operator liniowy ma rozkład spektralny $\Leftrightarrow$ jest normalny.*

Ponieważ operator hermitowski jest normalny:

$$A = A^\dagger \Longrightarrow A^\dagger A = A A^\dagger = A^2,$$

to z twierdzenia 37 mamy

**Wniosek 38.** *Operator hermitowski ma rozkład spektralny.*

Zapiszmy jeszcze prosty fakt.

**Fakt 39.** *Jeżeli operatory liniowe $A$ oraz $B$ działające na przestrzeni Hilberta $\mathcal{H}$ wymiaru $n$ posiadają rozkład spektralny we wspólnej bazie ortonormalnych projektorów $\{\Pi_i\}_{i=0}^{n-1}$ postaci*

$$A = \sum_{i=0}^{n-1} a_i \Pi_i,$$

$$B = \sum_{i=0}^{n-1} b_i \Pi_i,$$

*to operatory $A$ i $B$ komutują.*

*Dowód.* Zachodzi

$$AB = \left( \sum_{i=0}^{n-1} a_i \Pi_i \right) \left( \sum_{j=0}^{n-1} b_j \Pi_j \right) = \sum_{i,j=0}^{n-1} a_i b_j \Pi_i \Pi_j = \sum_{i=0}^{n-1} a_i b_i \Pi_i.$$

Podobnie

$$BA = \sum_{i=0}^{n-1} b_i a_i \Pi_i.$$

Wobec tego $AB = BA$. □

**Przestrzeń $\mathcal{H}_{AB}$** Rozważmy teraz przestrzenie Hilberta $\mathcal{H}_A$ oraz $\mathcal{H}_B$, odpowiednio wymiaru $n_A$ i $n_B$ i z bazami ortonormalnych projektorów

$$\left\{\Pi_i^{(A)}\right\}_{i=0}^{n_A-1},$$

$$\left\{\Pi_j^{(B)}\right\}_{j=0}^{n_B-1}.$$

Uogólnienia dokonamy dla operatorów produktowych działających w $\mathcal{H}_{AB}$, tzn. dla takich operatorów $E^{(AB)}$, które w przestrzeni Hilberta–Schmidta $\mathcal{HS}_{AB} \equiv \mathcal{HS}_A \otimes \mathcal{HS}_B$ sprzężonej z przestrzenią Hilberta $\mathcal{H}_{AB}$, są wektorami produktowymi (1), tzn.

$$E^{(AB)} = E^{(A)} \otimes E^{(A)},$$

gdzie pewne operatory $E^{(A)}$, $E^{(B)}$ działające na przestrzeni $\mathcal{H}_A$ oraz $\mathcal{H}_B$ same mają rozkłady spektralne

$$E^{(A)} = \sum_i \lambda_i^{(A)} \Pi_i^{(A)},$$

$$E^{(B)} = \sum_j \lambda_j^{(B)} \Pi_j^{(B)}.$$

Wtedy

$$E^{(AB)} = \left(\sum_i \lambda_i^{(A)} \Pi_i^{(A)}\right) \otimes \left(\sum_j \lambda_j^{(B)} \Pi_j^{(B)}\right)$$

$$= \sum_{ij} \lambda_i^{(A)} \lambda_j^{(B)} \Pi_i^{(A)} \otimes \Pi_j^{(B)}.$$

Definiując $\lambda_{ij}^{(AB)} \equiv \lambda_i^{(A)} \lambda_j^{(B)}$, $\Pi_{ij}^{(AB)} \equiv \Pi_i^{(A)} \otimes \Pi_j^{(B)}$, otrzymujemy rozkład spektralny operatora $E^{(AB)}$ na projektory działające w przestrzeni $\mathcal{H}_{AB}$ postaci

$$E^{(AB)} = \sum_{ij} \lambda_{ij}^{(AB)} \Pi_{ij}^{(AB)},$$

gdzie bazą ortonormalnych projektorów jest zbiór

$$\left\{\Pi_{ij}^{(AB)}\right\}_{i\in[n_A], j\in[n_B]}.$$

**Uwaga 40.** *Zauważmy jednak, że niekoniecznie wszystkie tak określone wartości własne są różne.*

### 1.5. Operatory binarne i operatory von Neumanna

Opiszemy tutaj pewną klasę operatorów hermitowskich.

#### 1.5.1. Operatory binarne

**Definicja 41** (Operator binarny)**.** *Operator liniowy $A$ nazywamy binarnym, gdy $A$ jest hermitowski i $A^2 = I$.*

**Fakt 42.** *Jeżeli $A$ jest operatorem hermitowskim, to*

$$A^2 = I \iff \sigma(A) \subseteq \{+1, -1\}.$$

#### 1.5.2. Macierze Pauliego

**Definicja 43** (Macierze Pauliego)**.** *Macierzami Pauliego nazywamy następujące macierze:*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

#### 1.5.3. Operatory von Neumanna

**Definicja 44** (Operator von Neumanna)**.** *Jeżeli $\hat{v} \in \mathbb{R}^3$ jest wektorem jednostkowym, to operatorem von Neumanna (operatorem pomiaru spinu wzdłuż osi $\hat{v}$) nazywamy operator działający na przestrzeni $V^2(\mathbb{C})$ dany wzorem*

$$\hat{v} \cdot \vec{\sigma} \equiv \sum_{i=1}^{3} v_i \sigma_i = \begin{pmatrix} v_3 & v_1 - iv_2 \\ v_1 + iv_2 & -v_3 \end{pmatrix}.$$

Przytoczymy poniżej kilka podstawowych własności operatorów von Neumana.

**Twierdzenie 45.** *Jeżeli $\hat{a} \cdot \vec{\sigma}, \hat{b} \cdot \vec{\sigma}$ są operatorami von Neumanna, to*

$$(\hat{a} \cdot \vec{\sigma})(\hat{b} \cdot \vec{\sigma}) = \left(\hat{a} \cdot \hat{b}\right) I + i \left(\hat{a} \times \hat{b}\right) \cdot \vec{\sigma}.$$

**Fakt 46.** *Operator von Neumanna $\hat{v} \cdot \vec{\sigma}$ jest operatorem hermitowskim. Ponadto łatwo sprawdzić, że $(\hat{v} \cdot \vec{\sigma})^2 = I$. Wobec tego, $\hat{v} \cdot \vec{\sigma}$ jest operatorem binarnym.*

**Fakt 47.** *Spektrum operatora von Neumanna $\hat{v} \cdot \vec{\sigma}$ to zbiór $\{+1, -1\}$. Ponadto*

$$\hat{v} \cdot \vec{\sigma} = \Pi_+ - \Pi_-,$$

*gdzie* $\Pi_{\pm} = \frac{1}{2}(I \pm \hat{v}\cdot\vec{\sigma})$ *jest projektorem rzutującym na odpowiednią podprzestrzeń własną.*

# 2. WPROWADZENIE DO KWANTOWEJ TEORII INFORMACJI

Podamy tutaj najważniejsze elementy mechaniki kwantowej – te, które interesować nas będą z perspektywy zastosowań mechaniki kwantowej w teorii informacji.

## *2.1. Stany kwantowe*

W ujęciu ogólnym stan układu kwantowego dany jest *funkcją falową*, tzn. funkcją zespoloną zależną od parametru czasu i biorącą również wartości z *przestrzeni konfiguracyjnej* badanego układu (ma ona spełniać odpowiednie równanie różniczkowe – w przypadku nierelatywistycznej mechaniki kwantowej jest to równanie Schrödingera). Nie będziemy się tym ogólnym podejściem zajmować (jednak dla wygody także w skończonym wymiarze używać będziemy pojęcia "funkcja falowa" w odniesieniu do obiektu opisującego stan układu). W przypadku skończenie wymiarowym odpowiednikiem funkcji falowej jest wektor z przestrzeni $V^n(\mathbb{C})$ lub macierz (operator liniowy) z przestrzeni $M_{n\times n}(\mathbb{C})$. Oba przypadki rozważamy poniżej. Przyjmijmy też pewną umowę:

**Umowa 48.** *W dalszych rozważaniach mówiąc "przestrzeń Hilberta" mamy na myśli przestrzeń*

$$\mathcal{H} \equiv V^n(\mathbb{C}). \tag{10}$$

*Wtedy sprzężona z nią przestrzeń Hilberta–Schmidta*

$$\mathcal{HS} \equiv M_{n\times n}(\mathbb{C}). \tag{11}$$

Opis przeprowadzimy dokonując podziału na układy kwantowe *pojedyncze* i *złożone* – podamy matematyczną strukturę tych ostatnich. Uprzedzając jednak fakty (wynikające z tej struktury) powiedzmy najpierw, że to, czy dany obiekt matematyczny mający opisać pewien rzeczywisty układ kwantowy potraktujemy jako pojedynczy bądź złożony (w sensie poniższych definicji) można niekiedy przyjąć jako sprawę umowy (i wygody w obliczeniach). Bywa jednak też tak, że rozróżnienia dokonują same prawa fizyki i nie ma możliwości nagiąć do nich opisywanego przez nas formalizmu.

### *2.1.1. Układy pojedyncze*

#### Stany czyste układów pojedynczych

**Definicja 49** (Stany czyste)**.**

1. *Stanem czystym pojedynczego układu kwantowego nazywamy unormowany wektor*

$$|\psi\rangle = \sum_i \psi_i |i\rangle$$

*z przestrzeni $\mathcal{H}$ z bazą ortonormalną*

$$\mathcal{B} = \{|i\rangle\}_{i\in I}, I = \{0, 1, \ldots, n-1\},$$

*której elementy nazywamy stanami bazowymi*

2. *Ponadto, prawdopodobieństwo tego, że stan $|\psi\rangle$ występuje w stanie $|i\rangle$ definiuje się jako*

$$p(|i\rangle \,||\psi\rangle) \equiv |\psi_i|^2. \tag{12}$$

**Uwaga 50.** *Druga część powyższej definicji zostanie wyjaśniona w pełni po wprowadzeniu pomiaru von Neumanna.*

**Stany mieszane układów pojedynczych – operator gęstości**

**Definicja 51** (Stany mieszane)**.** *Jeżeli pojedynczy układ kwantowy z prawdopodobieństwem $p_i$ znajduje się w stanie czystym $|\psi_i\rangle$, to jego stan opisuje operator liniowy na $\mathcal{H}$, nazywany operatorem gęstości. Jest on postaci*

$$\rho \equiv \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|, 0 \leqslant p_i \leqslant 1, \sum_i p_i = 1.$$

**Uwaga 52.** *Jeżeli stan kwantowy opisywany operatorem gęstości z prawdopodobieństwem $1$ znajduje się w pewnym stanie czystym $|\psi\rangle$ (wtedy $\rho = |\psi\rangle \langle\psi|$), to taki stan również nazywamy czystym.*

**Uwaga 53.** *Oznaczamy też $p_i = p(|\psi_i\rangle)$.*

**Uwaga 54.** *W mechanice kwantowej rozważa się też takie stany mieszane, które same są mieszanką innych stanów mieszanych, tzn. jeżeli układ z prawdopodobieństwem $p(\rho_i)$ opisany jest przez stan $\rho_i$, to całkowity operator gęstości ma postać*

$$\rho_\Sigma \equiv \sum_i p(\rho_i)\rho_i.$$

*W naszych rozważaniach przyjmujemy jednak, że wprowadzając stan mieszany $\rho$ nie traktujemy go jako część takiej mieszanki, tzn. wystąpienie stanu $\rho$ jest zdarzeniem pewnym:*

$$p(\rho) = 1.$$

**Twierdzenie 55** (Charakteryzacja operatorów gęstości)**.** *Operator $\rho$ działający na przestrzeni Hilberta $\mathcal{H}$ jest operatorem gęstości wtedy i tylko wtedy, gdy*

1. ***Tr***$[\rho] = 1$
2. *$\rho$ jest operatorem dodatnio określonym*

*Dowód.* "$\Longrightarrow$" Niech $\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|$. Wtedy

$$\mathbf{Tr}[\rho] = \sum_i p_i \mathbf{Tr}[\left|\psi_i\right\rangle \left\langle\psi_i\right|] = \sum_i p_i = 1.$$

Niech teraz $|\psi\rangle \in \mathcal{H}$ będzie dowolnym wektorem. Wtedy

$$\langle\psi|\,\rho\,|\psi\rangle = \langle\psi|\left(\sum_i p_i\,|\psi_i\rangle\,\langle\psi_i|\right)|\psi\rangle$$

$$= \sum_i p_i\,\langle\psi|\psi_i\rangle\,\langle\psi_i|\psi\rangle = \sum_i p_i|\,\langle\psi|\psi_i\rangle\,|^2 \geqslant 0.$$

"$\Longleftarrow$" Ponieważ $\rho$ jest operatorem dodatnio określonym, to ma rozkład spektralny (zob. twierdzenie 14 i wniosek 38) postaci

$$\rho = \sum_j \lambda_j\,|j\rangle\,\langle j|\,,$$

gdzie $\lambda_j$ są nieujemnymi (zob. twierdzenie 15) wartościami własnymi operatora $\rho$. Dodatkowo, ponieważ $\mathbf{Tr}[\rho] = 1$, to $\sum_j \lambda_j = 1$. Oznacza to, że $\rho$ jest operatorem gęstości. □

Widać z powyższych definicji, że podstawowym obiektem opisującym w przestrzeniach o skończonym wymiarze układy kwantowe jest w najprostszy sposób rozumiany wektor z $V^n(\mathbb{C})$. Konstrukcja funkcji falowej w oparciu o tę przestrzeń jest też konstrukcją w pełni ogólną (w skończonym wymiarze) – pojęcie operatora gęstości wywodzi się bowiem z pojęcia stanu czystego (pokażemy później, że z definicji pomiaru kwantowego na stanie czystym jako odpowiedniego zbioru trójek *(wartość, prawdopodobieństwo, kolaps)* wynika postać tego zbioru w scenariuszu pomiaru na stanie mieszanym). Ponadto każdy operator gęstości staje się kolumną liczb w bazie złożonej z operatorów gęstości. Widać wobec tego jeszcze wyraźniej umowność tego, co nazwiemy "początkową" przestrzenią Hilberta, w której zanurzone będą funkcje falowe układu. Można powiedzieć, że za obiekt opisujący układ kwantowy przyjmuje się to, czym w odniesieniu do tego układu najwygodniej się posługiwać – wszystko zależy od stopnia abstrakcji koniecznej do opisu (a także od tego, jaka część pełnej informacji o układzie jest potrzebna). Powtarzamy naszą umowę 48 stanowiącą, że w całych niniejszych rozważaniach stoimy w punkcie "zerowym" w hierarchii abstrakcji opisu układu kwantowego, tzn. za "początkową" przestrzeń Hilberta uznajemy przestrzeń (10). W oparciu o nią budujemy przestrzeń (11) operatorów gęstości.

### *2.1.2. Układy złożone*

Punktem wyjściowym do rozważań z niniejszego paragrafu jest – jak już o tym wspominaliśmy – potrzeba traktowania niektórych układów kwantowych jako złożonych z wielu mniejszych części. Warto w tym miejscu nieco uściślić sam formalizm dotyczący pojêcia *układu kwantowego* – będziemy przez niego rozumieć abstrakcyjny obiekt (wciąż mający jednak przedstawiać rzeczywiste zjawisko) oznaczany np. $A$ i mający właściwość polegającą na możliwości jego *opisu* rozumianego przez wygenerowanie z niego teorii według procedury przedstawionej w poprzednim paragrafie (z całą jej dowolnością – tzn. przyjętą przestrzenią Hilberta).

Rozważać będziemy teraz $N$ takich układów kwantowych, z których każdy oznaczymy $A_1, A_2, \ldots, A_N$. Związane są z nimi przestrzenie Hilberta $\mathcal{H}_{A_i} = V^{n_i}(\mathbb{C})$, którym odpowiadają bazy ortonormalne $\left|j^{(A_i)}\right\rangle$.

**Definicja 56** (Układ złożony)**.** *Działaniem służącym połączeniu przestrzeni stanów $\mathcal{H}_{A_i}$ podukładów $A_i$ w nową przestrzeń stanów jest iloczyn tensorowy. Otrzymujemy więc przestrzeń*

$$\mathcal{H} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \ldots \otimes \mathcal{H}_{A_N}.$$

*Gdy zbiór funkcji falowych $\psi^{(A_i)}$ podukładów jest dany, to funkcja falowa układu złożonego wyraża się przez ich iloczyn tensorowy:*

$$\psi = \psi^{(A_1)} \otimes \psi^{(A_2)} \otimes \ldots \otimes \psi^{(A_N)}. \tag{13}$$

W poniższych szczegółowych rozważaniach wprowadzamy układ złożony z jedynie dwóch podukładów: $A$ i $B$, którym odpowiadają przestrzenie

$$(\mathcal{H}_A, \left|i^{(A)}\right\rangle)$$

oraz

$$(\mathcal{H}_B, \left|j^{(B)}\right\rangle).$$

Interesować nas będzie wobec tego przypadek układu *dwuczęściowego* (*bipartite*):

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B.$$

**Uwaga 57.** *Dla $\mathcal{H}_A = V^n(\mathbb{C})$ i $\mathcal{H}_B = V^m(\mathbb{C})$ pisze się w skrócie*

$$\mathcal{H}_{AB} = n \otimes m. \tag{14}$$

**Stany czyste układów złożonych** Ogólny wektor stanu w przestrzeni $\mathcal{H}_{AB}$ układu złożonego wyraża się w tym przypadku jako

$$\left|\psi^{(AB)}\right\rangle = \sum_{ij} c_{ij} \left|i^{(A)}\right\rangle \left|j^{(B)}\right\rangle. \tag{15}$$

Korzystając z (13), jeżeli stany podukładów $A$ i $B$ są dane i równe $\left|\psi^{(A)}\right\rangle$, $\left|\psi^{(B)}\right\rangle$ odpowiednio, to stan układu złożonego $AB$ dany jest jako

$$\left|\psi^{(AB)}\right\rangle = \left|\psi^{(A)}\right\rangle \otimes \left|\psi^{(B)}\right\rangle.$$

Ze względu na rozbicie przestrzeni $\mathcal{H}_{AB}$ na dwie klasy stanów czystych (zob. Uwaga 23) wprowadza się następującą definicję:

**Definicja 58.** *Jeżeli stan czysty $\left|\psi^{(AB)}\right\rangle \in \mathcal{H}_{AB}$ da się zapisać w postaci*

$$|\psi\rangle = \left|\psi^{(A)}\right\rangle \left|\psi^{(B)}\right\rangle$$

*dla pewnych stanów czystych $\left|\psi^{(A)}\right\rangle \in \mathcal{H}_A$ i $\left|\psi^{(B)}\right\rangle \in \mathcal{H}_B$, to stan $\left|\psi^{(AB)}\right\rangle$ nazywamy separowalnym. W przeciwnym razie nazywamy go stanem splątanym.*

**Przykład 59** (Stan splątany)**.** *Przykładem stanu splątanego w przestrzeni $\mathcal{H} = V^2(\mathbb{C}) \otimes V^2(\mathbb{C})$ jest jeden ze stanów Bella:*

$$\left|\Phi^+\right\rangle \equiv \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{16}$$

*Okazuje się, że nie da się go przedstawić w postaci iloczynu $|\psi\rangle |\phi\rangle$ dowolnych dwóch stanów czystych z przestrzeni $V^2(\mathbb{C})$. Niech bowiem*

$$|\psi\rangle \equiv \begin{pmatrix} a \\ b \end{pmatrix}$$

*i*

$$|\phi\rangle \equiv \begin{pmatrix} c \\ d \end{pmatrix}.$$

*Wtedy*

$$|\psi\rangle |\phi\rangle = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

*Otrzymujemy wobec tego układ warunków: $ac = \frac{1}{\sqrt{2}}$, $ad = 0$, $bc = 0$, $bd = \frac{1}{\sqrt{2}}$. Widać od razu, że jest on sprzeczny.*

**Stany mieszane układów złożonych** W przypadku stanów mieszanych stan układu złożonego definiuje się jako operator gęstości $\rho^{(AB)}$ działający na przestrzeni $\mathcal{H}_{AB}$. Nazywa się go wtedy *łącznym* operatorem gęstości. Niech na przestrzeniach Hilberta $\mathcal{H}_A$ i $\mathcal{H}_B$ dane są ortonormalne bazy $\{|a_i\rangle\}_{i\in[n_A]}$ oraz $\{|b_j\rangle\}_{j\in[n_B]}$. Wtedy (zob. (8)) łączny operator gęstości definiujemy ogólnie jako

$$\rho^{(AB)} \equiv \sum_{i,k\in[n_A];j,l\in[n_B]} \rho^{(AB)}_{\substack{ij \\ kl}} |a_i\rangle \langle a_k| \otimes |b_j\rangle \langle b_l|, \tag{17}$$

gdzie $\rho^{(AB)}_{\substack{ij \\ kl}}$ jest odpowiednim elementem macierzowym.

Podobnie jak dla stanów czystych, korzystając z Definicji 56 mamy, że jeżeli dane są operatory gęstości podukładów, to stan układu z nich złożonego wyznaczony jest przez stan produktowy (zob. Uwaga 24):

$$\rho^{(AB)} = \rho^{(A)} \otimes \rho^{(B)}. \tag{18}$$

Definicja stanu separowalnego zostaje jednak dla stanów mieszanych rozszerzona w stosunku do przypadku stanów czystych – za taki stan uważa się nie tylko produkt dwóch stanów, ale każdą wypukłą kombinację produktów.

**Definicja 60.** *Jeżeli operator gęstości $\rho^{(AB)}$ działający na przestrzeni $\mathcal{H}_A \otimes \mathcal{H}_B$ da się zapisać w postaci*

$$\rho^{(AB)} = \sum_i p_i \rho_i^{(A)} \otimes \rho_i^{(B)}, 0 \leqslant p_i \leqslant 1, \sum_i p_i = 1, \tag{19}$$

*gdzie $\rho_i^{(A)}$, $\rho_i^{(B)}$ są operatorami gęstości działającymi na przestrzeni $\mathcal{H}_A$, $\mathcal{H}_B$ odpowiednio, to stan mieszany $\rho^{(AB)}$ nazywamy separowalnym. W przeciwnym razie nazywamy go stanem splątanym.*

### *2.2. Separowalność macierzy gęstości*

Okazuje się, że dla układów dwuczęściowych (14) ogólnie sprawa rozstrzygnięcia, czy operator gęstości działający na przestrzeni $\mathcal{H}_{AB}$ jest separowalny, jest problemem algorytmicznie NP-trudnym (zob. [5]). Dla przypadku $n = m = 2$ istnieje jednak bardzo ważne kryterium. Najpierw podamy definicję:

**Definicja 61.** *Niech $\mathcal{H}_A = \mathcal{H}_B = V^d(\mathbb{C})$ są przestrzeniami Hilberta z ortonormalnymi bazami*

$$\{\left|i^{(A)}\right\rangle\}_{i\in\{0,1,\ldots,d-1\}}$$

*oraz*

$$\{\left|j^{(B)}\right\rangle\}_{j\in\{0,1,\ldots,d-1\}}.$$

*Niech $A$ jest operatorem liniowym działającym na przestrzeni $\mathcal{H}_{AB}$ i niech w bazie*

$$\mathcal{B}_{AB} \equiv \{\left|i^{(A)}\right\rangle \left|j^{(B)}\right\rangle\}_{i,j\in\{0,1,\ldots,d-1\}}$$

*jego elementy macierzowe są równe*

$$A \equiv \begin{pmatrix} A_{00} & A_{01} & \cdots & A_{0,d-1} \\ A_{10} & A_{11} & \cdots & A_{1,d-1} \\ \vdots & \vdots & \vdots & \vdots \\ A_{d-1,0} & A_{d-1,1} & \cdots & A_{d-1,d-1} \end{pmatrix},$$

*gdzie* $A_{ij} \in M_{d\times d}(\mathbb{C})$.

*Częściową transpozycją operatora* $A$ *ze względu na podukład* $B$ *nazywamy operator* $A^\Gamma$*, którego elementy macierzowe w bazie* $\mathcal{B}_{AB}$ *dane są przez:*

$$A^\Gamma \equiv \begin{pmatrix} A_{00}^T & A_{01}^T & \cdots & A_{0,d-1}^T \\ A_{10}^T & A_{11}^T & \cdots & A_{1,d-1}^T \\ \vdots & \vdots & \vdots & \vdots \\ A_{d-1,0}^T & A_{d-1,1}^T & \cdots & A_{d-1,d-1}^T \end{pmatrix}.$$

**Fakt 62.** *Częściowa transpozycja ze względu na podukład* $B$*:*

1. *Zachowuje hermitowskość operatora*
2. *Zachowuje ślad operatora*

**Twierdzenie 63** (Kryterium Częściowej Transpozycji, zob. [5])**.** *Operator gęstości* $\rho$ *działający w przestrzeni* $2 \otimes 2$ *jest stanem separowalnym* $\iff$ *operator* $\rho^\Gamma$ *jest operatorem gęstości w sensie podanym w charakteryzacji z Twierdzenia 55.*

**Fakt 64.** *Z Wniosku 19 i Faktu 62 wynika, że aby sprawdzić, że operator* $\rho^\Gamma$ *jest operatorem gęstości, wystarczy pokazać, że jego spektrum jest nieujemne.*

W przypadku operatorów gęstości na układach złożonych wprowadza się też pojęcie *operatora zredukowanego do podukładu*, analogiczne do pojęcia brzegowej gęstości prawdopodobieństwa łącznej zmiennej losowej (klasycznej).

**Definicja 65.** *Dla danego łącznego operatora gęstości* $\rho^{(AB)}$ *jego śladem częściowym ze względu na podukład B nazywa się operator (okazuje się, że jest on operatorem gęstości)*

$$\rho^{(A)} \equiv \textbf{\textit{Tr}}_B[\rho^{(AB)}], \tag{20}$$

*gdzie działanie* $\textbf{\textit{Tr}}_B$ *nazywamy śladowaniem częściowym ze względu na podukład B i dla układów dwuczęściowych oraz operatora gęstości postaci (17) definiuje się je następująco:*

$$\begin{aligned} \textbf{\textit{Tr}}_B[\rho^{(AB)}] &\equiv \sum_{i,k\in[n_A];j,l\in[n_B]} \rho_{\substack{ij\\kl}}^{(AB)} |a_i\rangle \langle a_k| \, \textbf{\textit{Tr}}[|b_j\rangle \langle b_l|] \\ &= \sum_{i,k\in[n_A];j,l\in[n_B]} \rho_{\substack{ij\\kl}}^{(AB)} |a_i\rangle \langle a_k| \langle b_l|b_j\rangle . \end{aligned} \tag{21}$$

Operator $\rho^{(A)}$ powstały z $\rho^{(AB)}$ w wyniku śladowania ze względu na podukład $B$ opisuje podukład $A$, tzn. jest jego operatorem gęstości.

**Fakt 66.** *Jeżeli stan* $\rho^{(AB)}$ *jest stanem produktowym (18), to*

$$\textbf{\textit{Tr}}_B[\rho^{(A)} \otimes \rho^{(B)}] = \rho^{(A)}. \tag{22}$$

*Dowód.* Niech

$$\rho^{(A)} = \sum_i p_i \left|\psi_i^{(A)}\right\rangle \left\langle\psi_i^{(A)}\right|$$

oraz

$$\rho^{(B)} = \sum_j q_j \left|\psi_j^{(B)}\right\rangle \left\langle\psi_j^{(B)}\right|.$$

Wtedy

$$\begin{aligned}
&\mathbf{Tr}_B \left[ \left( \sum_i p_i \left|\psi_i^{(A)}\right\rangle \left\langle\psi_i^{(A)}\right| \right) \otimes \left( \sum_j q_j \left|\psi_j^{(B)}\right\rangle \left\langle\psi_j^{(B)}\right| \right) \right] \\
&= \mathbf{Tr}_B \left[ \sum_{ij} p_i q_j \left|\psi_i^{(A)}\right\rangle \left\langle\psi_i^{(A)}\right| \otimes \left|\psi_j^{(B)}\right\rangle \left\langle\psi_j^{(B)}\right| \right] \\
&= \sum_{ij} p_i q_j \left|\psi_i^{(A)}\right\rangle \left\langle\psi_i^{(A)}\right| \underbrace{\left\langle\psi_j^{(B)}\middle|\psi_j^{(B)}\right\rangle}_{1} \\
&= \left( \sum_i p_i \left|\psi_i^{(A)}\right\rangle \left\langle\psi_i^{(A)}\right| \right) \underbrace{\left( \sum_j q_j \right)}_{1} = \rho^{(A)}.
\end{aligned}$$

□

## 3. WPROWADZENIE DO PROGRAMOWANIA PÓŁOKREŚLONEGO

**Definicja 67** (Programowanie półokreślone)**.** *Ogólne zagadnienie programowania półokreślonego w postaci pierwotnej definiuje się jako*

$$\begin{cases} \max \textbf{\textit{Tr}}[CX] \\ \textit{ze względu na:} \\ \bullet \textbf{\textit{Tr}}[A_i X] = b_i, i = 1, \ldots, p \\ \bullet X \geqslant 0 \end{cases}$$

*gdzie*

- $X \in M_{n\times n}(\mathbb{R})$ *jest macierzą symetryczną traktowaną jako zmienna*
- $C, A_i \in M_{n\times n}(\mathbb{R}), i = 1, \ldots, p$ *są danymi macierzami symetrycznymi*
- $b_i \in \mathbb{R}, i = 1, \ldots, p$ *są danymi liczbami*

## WYKAZ LITERATURY


[1] R. A. Bertlmann. “Theoretical Physics T2, Quantum Mechanics”. W: (). URL: https://www.univie.ac.at/physikwiki/images/a/a0/T2_Skript_final.pdf.

[2] L. Vandenberghe; S. Boyd. “Semidefinite Programming”. W: *SIAM Review, 38 (1): 49-95, March 1996* (). URL: http://stanford.edu/~boyd/papers/sdp.html.

[3] M. A. Nielsen; I. L. Chuang. “Quantum Computation and Quantum Information, Cambridge University Press, Cambridge (2000)”. W: ().

[4] M. Hirvensalo. *Algorytmy kwantowe, Wydawnictwa Szkolne i Pedagogiczne Spółka Akcyjna, Warszawa (2004)*.

[5] R. Horodecki; P. Horodecki; M. Horodecki; K. Horodecki. *Quantum entanglement*. URL: arXiv:quant-ph/0702225v2.

[6] S. Kryszewski. “Mechanika kwantowa – skrypt dla studentów III roku fizyki”. W:

[7] Wu-Sheng Lu. *Use SeDuMi to Solve LP, SDP and SCOP Problems: Remarks and Examples*. URL: http://www.ece.uvic.ca/~wslu/Talk.html.

[8] R. Shankar. “Mechanika kwantowa, Wydawnictwo Naukowe PWN, Warszawa (2007)”. W: ().

[9] A. Doherty; P. Parrilo; F. Spedalieri. “A complete family of separability criteria”. W: *Phys. Rev. A 69, 022308 (2004)* (). URL: https://arxiv.org/abs/quant-ph/0308032.

[10] A. Doherty; P. Parrilo; F. Spedalieri. “Distinguishing separable and entangled states”. W: *Physical Review Letters, Vol. 88, No. 18, 187904 (2002)* (). URL: https://arxiv.org/abs/quant-ph/0112007.

[11] S. Szpikowski. *Podstawy Mechaniki Kwantowej, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin (2011)*.

[12] S. Boyd; L. Vandenberghe. *Convex Optimization, Cambridge University Press, Cambridge (2004)*.

## WYKAZ RYSUNKÓW

## WYKAZ TABEL