Zbiory wypukłe

Podzbiór przestrzeni afinicznej nazywamy wypukłym, jeżeli dowolny odcinek o końcach w tym zbiorze, w całości się w nim zawiera. Punktami ekstremalnymi zbioru wypukłego nazywamy punkty, które nie mogą być przedstawione jako punkty wewnętrzne pewnego odcinka o końcach w zbiorze.

Zwarty zbiór wypukły jest otoczką wypukłą zbioru swoich punktów ekstremalnych (tw. Kreina Milamana), tzn. każdy jego punkt da się wyrazić jako kombinacja wypukła punktów ekstremalnych. Tw. Caratheodory'ego mówi, że maksymalna liczba składników rozkładu jest o jeden większa od wymiaru przestrzeni afinicznej zawierającej zbiór.

Zbióry stanów kwantowych i klasycznych

Klasycznie, jeżeli mamy skończoną σ algebrę zbiorów, to dowolną miarę probabilistyczną możemy przestawić jako wektor $|p\rangle$ jej wartości na zdarzeniach elementarnych, o dodatnich składowych sumujących się do 1. Zbiorem stanów jest $n-1$ wymiarowy sympleks $\Delta^{n-1} = \{(p_1, \ldots, p_n) \in \mathbb{R}^n_+ : \sum_i p_i = 1\}$. Punktami ekstremalnymi zbioru stanów są stany czyste, przyjmujące dla pewnego zdarzenia elementarnego wartość 1.

W mechanice kwantowej stany są reprezentowane przez macierze dodatnio półokreślone o śladzie równym 1 (*macierze gęstości*). Punktami ekstremalnymi zbioru stanów są stany o rzędzie jeden, czyli projektory na wektory w przestrzeni Hilberta (precyzyjniej - na jednowymiarowe podprzestrzenie). Jednemu stanowi czystemu odpowiada zbiór wektorów w przestrzeni Hilberta różniących się o fazę. Zbiór stanów czystych jest zatem zespoloną przestrzenią rzutową $\mathbb{C}P^{d-1}$.

Każdy maksymalny komutujący podzbiór stanów kwantowych jest liniowo izomorficzny ze zbiorem stanów klasycznych.

Zbiór stanów qbitu

Stany kwantowe układu dwupoziomowego reprezentowane są przez półdodatnio określone macierze hermitowskie 2×2 o śladzie równym 1. Każdą taką macierz można zapisać jako:

$$\rho = \frac{1}{2} \begin{bmatrix} 1+z & x-iy \\ x+iy & 1-z \end{bmatrix}. \tag{1}$$

Warunek półdodatniej określoności wyraża się jako $x^2 + y^2 + z^2 \leqslant 1$ - dostajemy równanie kuli. Kula ta nazywa się kulą Blocha. Na brzegu kuli (na sferze Blocha) leżą stany o rzędzie 1 - stany czyste. Operator hermitowski o śladzie 1 i o rzędzie 1 jest projektorem na 1-wymiarową podprzestrzeń napinaną przez pewien wektor ψ. Jeżeli wektor ψ jest unormowany, można zapisać projektor jako $|\psi\rangle\langle\psi|$. Wektor ten nazywany wektorem stanu, jest określony z dokładnością do fazy.

Zbiorem wektorów stanu jest sfera S^3. Zbiorem stanów czystych jest sfera S^2. Każdemu stanowi czystemu odpowiada zbiór wektorów stanu różniących się o fazę - sfera S^1. Sfera S^3 jest zatem wiązką nad przestrzenią bazową S^2 z włóknem S^1:

$$S^3 \xrightarrow{S^1} S^2 \tag{2}$$

Nazywa się ona *pierwszym rozwłóknieniem Hopfa*. Nie jest to wiązka trywialna ($S^3 \neq S^1 \times S^2$). Udowadniamy to, pokazując że nie istnieje globalne rzutowanie na S^1, czyli nie da się w sposób ciągły na całej sferze Blocha każdemu punktowi przypisać "wektora o kanonicznej fazie" i "odchylenia od kanonicznej fazy".

Ćwiczenie 1 *Wprowadź na sferze Blocha układ współrzędnych sferycznych θ, ϕ. Pokaż, że punktowi na sferze Blocha nie można w sposób ciągły przypisać wektora stanu.*

Ćwiczenie 2 *Udowodnij własność cykliczności śladu*

Przestrzeń macierzy nad $\mathbb{C}$ jest wyposażona w naturalny iloczyn skalarny (Hilberta-Schmidta):

$$\langle A|B\rangle_{HS} = \mathrm{Tr} A^\dagger B \tag{3}$$

Ćwiczenie 3 *Pokaż, że iloczyn HS jest niezmienniczy na działanie grupy unitarnej.*

Wniosek: Norma HS macierzy hermitowskiej jest normą euklidesową na jej spektrum.

Ćwiczenie 4 *Pokaż, że iloczyn HS dwóch macierzy gęstości o współrzędnych w kuli Blocha $\vec{r}_1 = [x_1, y_1, z_1], \vec{r}_2 = [x_2, y_2, z_2]$ wynosi $\frac{1}{2} + \frac{1}{2}\vec{r}_1 \cdot \vec{r}_2$.*

Ćwiczenie 5 *Pokaż, że para projektorów na ortogonalne podprzestrzenie odpowiada parze antypodycznych punktów na sferze Blocha.*

Rozkład spektralny macierzy hermitowskiej polega na znalezieniu jej rozkładu na kombinację liniową projektorów na ortogonalne podprzestrzenie. W przypadku macierzy półdodatnio określonej o śladzie jednostkowym będzie to kombinacja wypukła. Graficznie, rozkład spektralny w kuli Blocha oznacza znalezienie średnicy przechodzącej przez dany punkt, jej punktów wspólnych ze sferą Blocha, oraz współczynników kombinacji. Rozkład jest jednoznaczny dla wszystkich punktów z wyjątkiem punktu w środku, który jest proporcjonalny do identyczności i ma taką samą postać w każdej bazie ortonormalnej.

Zauważmy, że jeżeli zrezygnujemy z warunku ortogonalności projektorów w rozkładzie, dowolna macierz gęstości może być przedstawiona na nieskończenie wiele sposobów jako kombinacje dwóch projektorów - przez punkt w kuli można przeprowadzić nieskończenie wiele cięciw. Ogólniej:

Ćwiczenie 6 *Pokaż, że jeżeli macierz gęstości ma dwa przedstawienia: $\rho = \sum_i \alpha_i |\phi_i\rangle\langle\phi_i| = \sum_i \beta_i |\psi_i\rangle\langle\psi_i|$, to $\sqrt{\beta_i}\psi_i = \sum_j a_{ji}\sqrt{\alpha_i}\phi_j$, a wyrazy a_{ji} tworzą macierz prostokątną A o własności $A \cdot A^\dagger = I$.*

Ćwiczenie 7 *Pokaż, że w wyższych wymiarach przestrzeni Hilberta, kula opisana na zbiorze stanów ma promień $\sqrt{(d-1)/d}$, a kula wpisana ma promień $1/\sqrt{d(d-1)}$.*

Jeżeli H jest macierzą diagonalną, rozwiązaniem równania Schrödingera

$$i\hbar\partial_t\Psi = H\Psi \tag{4}$$

jest

$$\Psi(t) = \exp(-\frac{i}{\hbar}Ht)\Psi(0) = \begin{bmatrix} \exp(-\frac{i}{\hbar}E_0 t)\Psi_0(0) \\ \exp(-\frac{i}{\hbar}E_1 t)\Psi_1(0) \end{bmatrix}. \tag{5}$$

Odpowiada to jednostajnemu obracaniu się kuli Blocha wokół osi z. W przypadku ogólnego H, będzie to obrót wokół średnicy kuli Blocha napinanej przez projektory na wektory własne H.

Układy złożone

Łączna σ-algebra dwóch zdarzeń jest iloczynem kartezjańskim σ-algebr, spośród wszystkich rozkładów łącznych wyróżniamy rozkłady niezależne dane przez iloczyn $p_1 \times p_2$ rozkładów brzegowych: $p_1 = \sum_j p_{ij}, p_2 = \sum_i p_{ij}$.

Przestrzeń Hilberta układu złożonego jest iloczynem tensorowym przestrzeni Hilberta podukładów.

Rozkłady brzegowe (stany podukładów) uzyskujemy biorąc ślady częściowe:

$$[\rho_A]_{ij} = \sum_k \rho_{ik,jk} \qquad \text{macierz śladów bloków} \tag{6}$$

$$[\rho_B]_{ij} = \sum_k \rho_{ki,kj} \qquad \text{suma bloków diagonalnych.} \tag{7}$$

Jeżeli układy są od siebie niezależne, stanem całości jest iloczyn tensorowy stanów podukładów: $\rho = \rho_A \otimes \rho_B$.

Rozkład Schmidta Przeprowadźmy operację odwrotną do stogowania. Wektor Ψ w $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ można zapisać jako macierz A rozmiaru $d_2 \times d_1$ Do tej macierzy możemy zastosować twierdzenie o rozkładzie singularnym:

$$A = U \Lambda V^\dagger, \tag{8}$$

gdzie U i V są unitarne, a Λ jest dodatnia i diagonalna (w ogólności prostokątna). Innymi słowy:

$$A = \sum_i \lambda_i \left|u_i\right\rangle \left\langle v_i\right|, \tag{9}$$

dla ortonormalnych zbiorów $\{u_i\} \in \mathbb{C}^{d_2}$ i $\{v_i\} \in \mathbb{C}^{d_1}$. Zatem wektor Ψ można zapisać jako $\sum_i \lambda_i v_i \otimes u_i$. Udowodniliśmy w ten sposób twierdzenie o rozkładzie Schmidta. Liczby λ_i nazywamy współczynnikami Schmidta wektora Ψ.

Uwaga: Nie istnieje prosty odpowiednik rozkładu Schmidta dla stanu układu złożonego z więcej niż dwóch podukładów.

Stany separowalne i splątane Jeżeli wektor Ψ jest wektorem produktowym, to stan $\left|\Psi\right\rangle \left\langle\Psi\right|$ nazywamy *stanem czystym separowalnym*. Stan czysty, który nie jest separowalny nazywamy stanem splątanym. W przypadku stanów mieszanych, stan jest separowalny jeżeli da się rozłożyć na kombinacje wypukłą stanów czystych separowalnych. Jeżeli jest to niemożliwe, stan jest stanem splątanym. Definicja stosuje się do dowolnej liczby podukładów. Zagadnienie stwierdzenia separowalności stanu jest zadaniem trudnym, poświęcimy mu trochę uwagi w dalszych częściach wykładu.

Ślad częściowy stanu czystego Biorąc ślady częściowe wektora Ψ o rozkładzie Schmidta $\sum_i \lambda_i v_i \otimes u_i$ dostaniemy: $\rho_1 = \sum_i \lambda_i^2 \left|v_i\right\rangle \left\langle v_i\right|$ i $\rho_1 = \lambda_i^2 \sum_i \left|u_i\right\rangle \left\langle u_i\right|$. Mimo że mamy maksymalną informację o stanie całości (stan czysty), nie mamy pełnej informacji o podukładach (są w stanach mieszanych). Tego zjawiska nie ma w teorii komutatywnej.

Ćwiczenie 8 *Znajdź operator iloczynu skalarnego dwóch spinów:* $S^{(1)} \cdot S^{(2)} = S_x^{(1)} \otimes S_x^{(2)} + S_y^{(1)} \otimes S_y^{(2)} + S_z^{(1)} \otimes S_z^{(2)}$

Ćwiczenie 9 *Znajdź propagator dla układu dwóch spinów* $\frac{1}{2}$ *pod działaniem Hamiltonianu* $gB \cdot S_z^{(1)} + gB \cdot S_z^{(2)} + JS^{(1)} \cdot S^{(2)}$. *Znajdź równanie na ewolucję macierzy gęstości jednego spinu.*

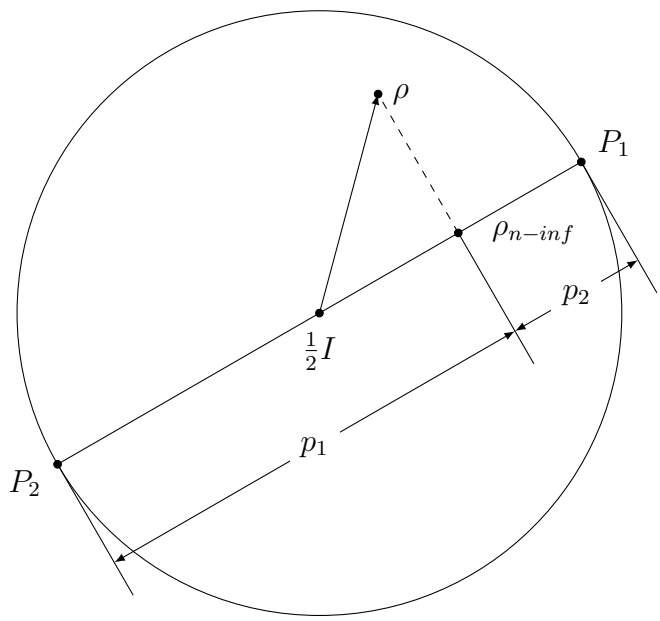
Pomiary projektywne

Pomiar projektywny funkcji mierzalnej f to odwzorowanie zbioru wyników pomiaru w zbiór projektorów (funkcji charakterystycznych) $\{\chi_{A_i}\}$ dla pewnego rozkładu przestrzeni probabilistycznej na rozłączne podzbiory należące do σ-algebry generowanej przez f (f-mierzalne). Prawdopodobieństwo otrzymania i-tego wyniku wynosi $p_i = \langle \mathbb{1}|\chi_{A_i}|p\rangle$. Stanem po pomiarze jest $\chi_{A_i}p\rangle/\langle \mathbb{1}|\chi_{A_i}|p\rangle$.

Kwantowo, pomiar projektywny obserwabli F to odwzorowanie zbioru wyników pomiaru w rozkład operatora identycznościowego $\mathbb{I}_{\mathcal{H}}$ w zbiór projektorów $\{P_i\}$ komutujących z F. Podprzestrzenie, na które rzutują projektory muszą być sumami podprzestrzeni niezmienniczych F (warunek F-mierzalności projektorów, w ogólności są to całki rozłącznych podzbiorów rozbicia widma operatora po jego mierze spektralnej). Prawdopodobieństwo otrzymania i-tego wyniku wynosi $\mathrm{Tr}(\rho P_i)$, a stan po pomiarze: $P_i\rho P_i/\mathrm{Tr}(\rho P_i)$.

Kwantowy pomiar projektywny składa się z dwóch etapów: pomiaru nieinformującego i klasycznego pomiaru informującego.

W przypadku qbitu, Pomiar nieinformujący obserwabli o projektorach P_1, P_2 w rozkładzie spektralnym odpowiada rzutowi stanu na średnicę napinaną przez P_1 i P_2. Jeżeli pomiar jest informujący, następuje kolaps do P_1 albo P_2 z prawdopodobieństwami proporcjonalnymi do długości odcinków w rozkładzie.



Rysunek 1: Pomiar projektywny nieinformujący (rzutowanie na średnicę) i informujący (kolaps) w sferze Blocha. Płaszczyznę rysunku wyznaczają projektory pomiaru i mierzony stan.

Zasada nieoznaczoności

Konsekwencją niekomutowania obserwabli jest zasada nieoznaczoności. Jeżeli nieoznaczoność pewnej obserwabli w pewnym stanie jest 0, musi to być kombinacja jej stanów własnych. Dla każdej innej obserwabli, która z nią nie komutuje, nie będzie to stan własny i nieoznaczoność nie będzie wynosiła 0.

W teorio-informacyjnym podejściu nieoznaczoność pomiaru dla pary obserwabli A,B wyrażamy jako sumę entropii rozkładów wyników pomiarów obu obserwabli w danym stanie. Może ona zależeć tylko od relacji między bazami własnymi obserwabli. Mamy następujące:

Twierdzenie (Maasen - Uffink): Niech p i q będą rozkładami prawdopodobieństwa wyników pomiarów obserwabli A i B w pewnym stanie ρ. Suma ich entropii jest ograniczona z dołu przez wielkość niezależną od stanu:

$$H(p) + H(q) \geqslant -\log \max_{j,k} |\langle a_j | b_k \rangle|^2, \tag{10}$$

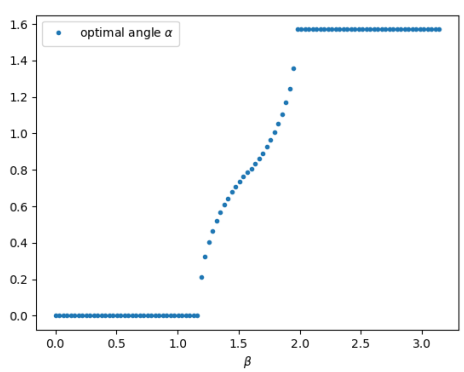
gdzie $\{a_k\}$, $\{b_k\}$ są wektorami własnymi odpowiednio obserwabli A i B.

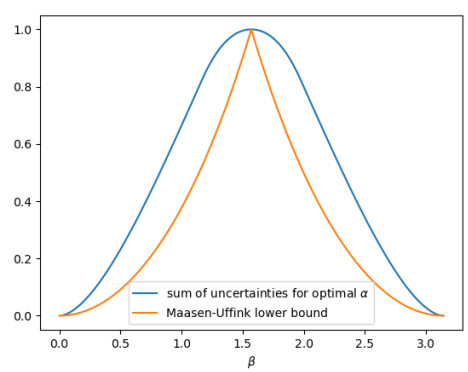
Zauważmy, że wystarczy jeden wspólny wektor własny by można było być pewnym wyniku obu obserwabli na raz.

Ćwiczenie 10 *Niech A i B będą obserwablami w $\mathbb{C}^2$, a β niech będzie kątem pomiędzy średnicami kuli Blocha reprezentującymi ich rozkłady spektralne.*

- *Znajdź ograniczenie dolne sumy entropii rozkładów prawdopodobieństwa wyników pomiarów obserwabli.*
- *Znajdź sumę entropii rozkładów prawdopodobieństwa wyników pomiarów obserwabli dla danego stanu i znajdź jej miminum.*
- *Pokaż, że minimum jest większe od ograniczenia dolnego.*

```python
import numpy as np
from scipy.optimize import minimize

def H(p):
        """binary Shannon entropy of prob. distr. {p,1-p}"""
        res = -(p*np.log(p)+(1-p)*np.log(1-p))/np.log(2)
        res = res * (p < 1) * (p > 0) + 0 * (p == 0) + 0 * (p == 1)      # to handle 0log0
        return res

def sum_of_uncertainties(beta,alpha):
        """For two projective measurements of Bloch coordinates:
{[sin(beta/2),0,cos(beta/2)], [-sin(beta/2),0,-cos(beta/2)]}
{[-sin(beta/2),0,cos(beta/2)], [sin(beta/2),0,-cos(beta/2)]}
and state: [sin(alpha),0,cos(alpha)]
calculates H(p) + H(q), where p and q are prob. distr. of first and second PM respectively
"""
        return H((1+np.cos(beta/2-alpha))/2) + H((1+np.cos(beta/2+alpha))/2)

@np.vectorize
def alpha_opt(beta):
        """For given beta (parameter describing non-commutativity of PMs), returns value of alpha
(state parameter) minimising the function sum_of_uncertainties"""
        f = lambda alpha: sum_of_uncertainties(beta, alpha)
        res = min((minimize(f, np.random.rand()*np.pi/2) for _ in range(5)), key = lambda res: res.fun)
        res = np.abs(res.x) % np.pi
        if res > np.pi/2: res = np.pi - res
        return res


import matplotlib.pyplot as plt
beta = np.linspace(0,np.pi,101)                          # range of beta
aa = alpha_opt(beta)                                     # corresponding optimal alphas
# plot optimal alpha in function of beta
plt.plot(beta,aa,'.', label = r'optimal angle $\alpha$')
plt.legend()
plt.xlabel(r'$\beta$')
plt.show()
# plot minimal sum_of_uncertainties in comparison to Maasen-Uffink bound.
plt.plot(beta,sum_of_uncertainties(beta,aa),label=r'sum of uncertainties for optimal $\alpha$')
plt.plot(beta,-np.log(np.maximum(np.cos(beta/2)**2,np.sin(beta/2)**2))/np.log(2),
                label='Maasen-Uffink lower bound')
plt.legend()
plt.xlabel(r'$\beta$')
plt.show()
```





MUBs

Dwie bazy $\{e_i\}$ i $\{f_i\}$ przestrzeni $\mathbb{C}^d$ nazywamy *unbiased*, jeżeli $\forall i,j|\langle i|j\rangle|^2 = \frac{1}{d}$. Zbiór baz parami *unbiased* nazywamy *mutually unbiased bases*. Zbiór ten może zawierać maksymalnie $d+1$ baz. Potrafimy skonstruować takie zbiory gdy d jest potęgą liczby pierwszej.

W przypadku, gdy d jest liczbą pierwszą, konstrukcja przebiega następująco: Za pomocą macierzy:

$$X = \begin{bmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & & & \\ & \omega & & \\ & & \ddots & \\ & & & \omega^{d-1} \end{bmatrix}$$

wyznaczamy macierze $X^\alpha Z^\beta$ reprezentacji projektywnej grupy Weyla. Jest ich d^2, a wśród nich jest oczywiście I_d. Dla pozostałych d^2-1 macierzy wyznaczamy bazy własne. Okazuje się, że jest $(d+1)$ baz, a każda jest bazą własną dla $(d-1)$ macierzy. (I_d) jest diagonalne w każdej z nich.

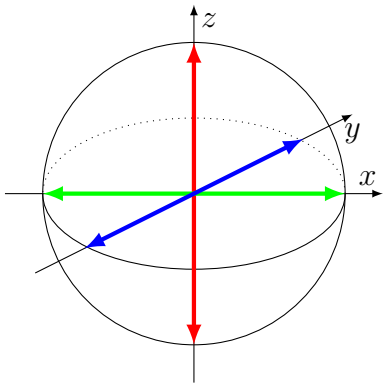
W $d=3$ konstrukcja ta przebiega następująco:

	$\beta=0$	$\beta=1$	$\beta=2$
$\alpha=0$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^* \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega^* & 0 \\ 0 & 0 & \omega \end{bmatrix}$
$\alpha=1$	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega \\ \omega^* & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega^* \\ \omega & 0 & 0 \end{bmatrix}$
$\alpha=2$	$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 \\ \omega & 0 & 0 \\ 0 & \omega^* & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 1 \\ \omega^* & 0 & 0 \\ 0 & \omega & 0 \end{bmatrix}$

- baza: $\left\{ \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$
- baza: $\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega \\ \omega^* \end{bmatrix}, \begin{bmatrix} 1 \\ \omega^* \\ \omega \end{bmatrix} \right\}$
- baza: $\left\{ \begin{bmatrix} \omega^* \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega^* \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \omega^* \end{bmatrix} \right\}$
- baza: $\left\{ \begin{bmatrix} \omega \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \omega \end{bmatrix} \right\}$

Ponieważ d jest liczbą pierwszą, projektywną reprezentację macierzową grupy Weyla możemy traktować jako dwuwymiarową przestrzeń liniową nad ciałem $\mathbb{Z}_d$, czyli $\mathbb{Z}_d^2$. Okazuje się, że elementy $X^{\alpha_1}Z^{\beta_1}$ i $X^{\alpha_2}Z^{\beta_2}$ komutują (z dokładnością do fazy), wtedy i tylko wtedy, gdy $\alpha_1\beta_2 - \alpha_2\beta_1 = 0 \mod d$ tzn. gdy leżą na jednej prostej. Zbiór baz własnych elementów jest izomorficzny ze zbiorem prostych w $\mathbb{Z}_d^2$, czyli z przestrzenią $\mathbb{Z}_d P^1$.

W przypadku qubitu konstrukcja ta prowadzi do baz własnych macierzy σ_z, σ_x i $\sigma_y \sim \sigma_x\sigma_z$. W kuli Blocha bazy te to pary projektorów leżących na osiach układu współrzędnych:

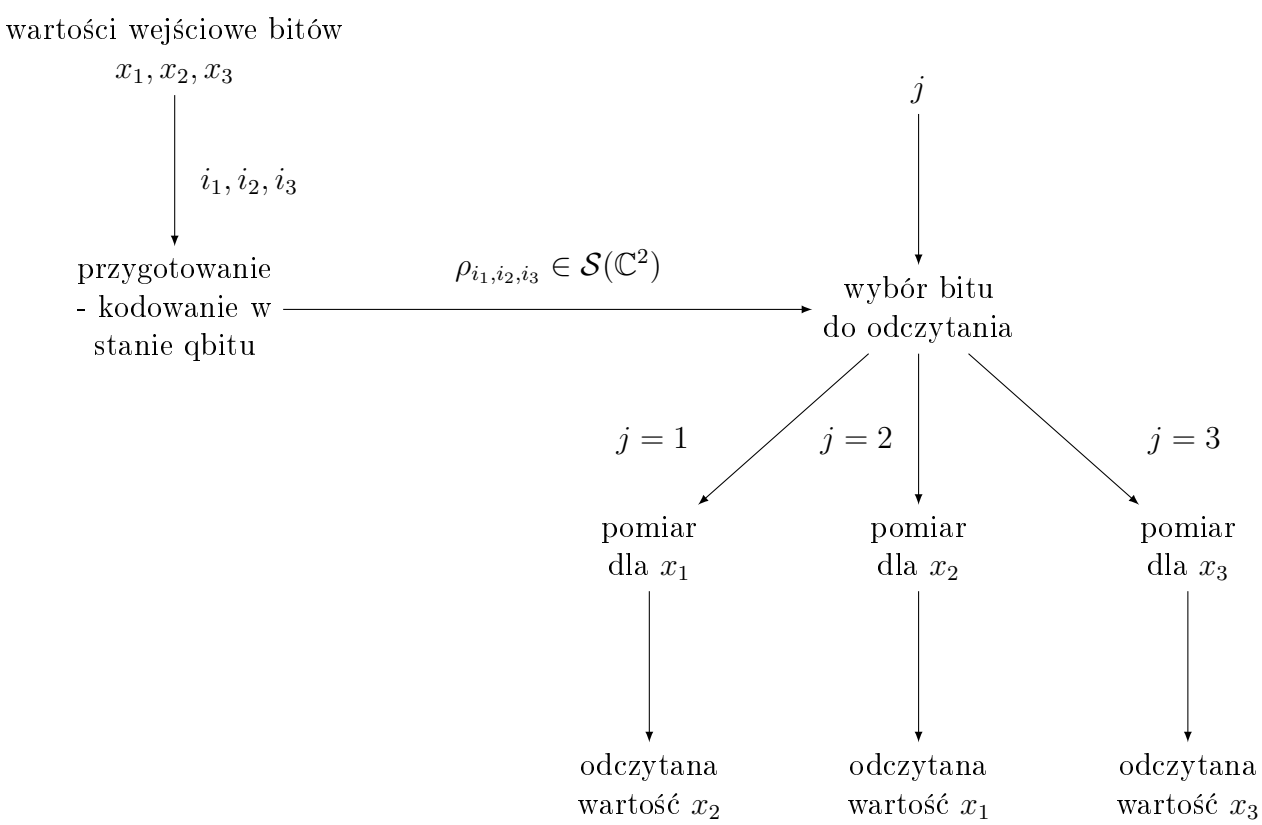


W $d = 2$, mierząc obserwable, których bazami własnymi są kolejne bazy ze zbioru MUB, otrzymujemy trzy wartości oczekiwane, które są równe współrzędnym x, y, i z w kuli Blocha mierzonego stanu.

W wyższych wymiarach jest podobnie - podprzestrzenie operatorów diagonalnych w bazach z MUB są wzajemnie do siebie ortogonalne, więc każdy stan rzutuje się ortogonalnie na te $(d + 1)$ podprzestrzeni. Prawodpodobieństwa różnych wyników pomiaru projektywnego w danej bazie pozwala zrekonstruować wartość rzutu na daną podprzestrzeń.

Random access codes

Niech naszym zadaniem będzie zakodowanie wartości trzech bitów w jednym qubicie, maksymalizujące prawdopodobieństwo prawidłowego odgadnięcia wartości jednego z bitów, wybieranych losowo z równymi prawdopodobieństwami.



Klasycznie, maksymalne prawdopodobieństwo poprawnego odgadnięcia wynosi 2/3 (jeden bit kodowany, dwa pozostałe odgadywane losowo). W przypadku kwantowym kodujemy stan trzech bitów w

osiem stanóœ qubitu o współrzędnych w kuli Blocha: $[\pm 1/\sqrt{3}, \pm 1/\sqrt{3}, \pm 1/\sqrt{3}]$. Zależnie od j (numer qubitu którego wartość odgadujemy) dokonujemy pomiaru projektywnego w jednej z baz MUB. Prawdopodobieństwo poprawnego odczytania wybranego bitu wynosi $(1 + 1/\sqrt{3})/2 \approx 0.7887$. Używając zasobów kwantowych obserwujemy polepszenie wyniku w porównaniu do przepadku klasycznego.

Kanały kwantowe

Odwzorowania pomiędzy rozkładami prawdopodobieństwa nazywają się *kanałami informacyjnymi* i są (w przypadku skończonych σ-algebr) reprezentowane przez macierze stochastyczne, tzn. o wyrazach nieujemnych i o kolumnach sumujących się do 1.

Kanałami kwantowymi są odwzorowania liniowe, zachowujące dodatniość (P). Powinien być spełniony ostrzejszy warunek: Odwzorowanie $I \otimes \Lambda$ powinno też być dodatnie dla wszystkich wymiarów dodatkowego podukładu. W ten sposób formułujemy warunek kompletnej dodatniości (CP), który jest łatwiejszy do rozwiązania. Twierdzenie Choi mówi, że każde odwzorowanie kompletnie dodatnie jest postaci (postać Kraussa):

$$\rho \mapsto \sum_i A_i \rho A_i^\dagger \tag{11}$$

Dodatkowo, kanał powinien zachowywać ślad (CPTP). Odpowiada to następującemu warunkowi na operatory Kraussa:

$$\sum_i A_i^\dagger A_i = I \tag{12}$$

Możemy zapytać, kiedy dwa kanały w postaci Kraussa reprezentują ten sam kanał. Przydatna okazuje się tutaj technika *stogowania*, czyli zapisania macierzy $n \times n$ jako wektor o n^2 współrzędnych, powstały z ustawienia kolumn macierzy n jedna pod drugą:

$$\rho = \sum_{ij} \rho_{ij} \left|e_i\right\rangle \left\langle e_j\right| \xrightarrow{\text{stogowanie}} \vec{\rho} = \sum_{ij} \rho_{ij} \left|e_i\right\rangle \otimes \left|e_j\right\rangle \tag{13}$$

Obłożenie ρ przez A i B odpowiada następującemu odwzorowaniu wektora $\vec{\rho}$:

$$A\rho B \longrightarrow A \otimes B^T \ \vec{\rho} \tag{14}$$

W tej reprezentacji działanie kanału zapisuje się jako

$$\vec{\rho} \mapsto \sum_i A_i \otimes A_i^* \vec{\rho} \tag{15}$$

Kanał jest jednoznacznie wyznaczony przez macierz $\sum_i A_i \otimes A_i^*$, żeby sprawdzić czy dwie reprezentacje Kraussa odpowiadają temu samemu kanałowi, trzeba porównać tak skonstruowane macierze.

Ćwiczenie 11 *Pokazać, że dwie reprezentacje kanału $\sum_i A_i \rho A_i^\dagger$ oraz $\sum_i B_i \rho B_i^\dagger$ są sobie równoważne $\iff$ $B_i = \sum_j U_{ij} A_j$, gdzie U jest macierzą unitarną (wykorzystać fakt, że $AXB = (A \otimes B^T)\vec{X}$).*

Macierz $\sum_i A_i \otimes A_i^*$ możemy przepisać jako $\sum_i \vec{A}_i \otimes \vec{A}_i^*$, co daje wektor o n^4 współrzędnych. Możemy też położyć pierwszy składnik iloczynu, by dostać macierz: $\sum_i \vec{A}_i^\dagger \otimes \vec{A}_i = \sum_i \left|\vec{A}_i\right\rangle \left\langle \vec{A}_i\right|$. Minimalną długością reprezentacji kanału jest rząd macierzy $\sum_i \left|\vec{A}_i\right\rangle \left\langle \vec{A}_i\right|$. Widać też, że jeżeli za $\vec{A}_i$ wybierzemy wektory własne $\sum_i \left|\vec{A}_i\right\rangle \left\langle \vec{A}_i\right|$, to dostaniemy reprezentację kanału ze wszystkimi macierzami A_i ortogonalnymi w iloczynie HS.

Kanały CQ i QC

Kanał, który przekształca dowolną macierz gęstości w macierz diagonalną w pewnej ustalonej bazie (redukujący przypadek niekomutatywny do komutatywnego) nazywamy kanałem kwantowo-klasycznym.

Ćwiczenie 12 *Uzasadnij, że kanał kwantowo-klasyczny ma postać:*

$$\rho \mapsto \sum_j \mathrm{Tr}(\rho M_j) \left|j\right\rangle \left\langle j\right|, \quad dla \quad \sum_j M_j = I. \tag{16}$$

Zauważmy, że jest to pomiar POVM - najbardziej ogólne liniowe odwzorowanie przypisujące macierzy gęstości rozkład prawdopodobieństwa.

Kanał, który przekształca macierz diagonalną w macierz gęstości (obcięcie kanału kwantowego do komutującej podalgebry) nazywamy kanałem klasyczno-kwantowym:

$$\rho \mapsto \sum_i \left\langle i\right| \rho \left|i\right\rangle \rho_i \tag{17}$$

taki kanał nazywamy *przygotowaniem.*

Jeżeli $\{M_j\}$ komutują, lub jeżeli $\{\rho_i\}$ komutują, to otrzymujemy kanał klasyczno-klasyczny.

Kanały qubitowe

Kanały dla jednego qbitu są reprezentowane przez odwzorowania liniowe przekształcające kulę Blocha w samą siebie. Jedynymi kanałami surjektywnymi, czyli odwracalnymi są obroty wokół pewnej osi - są one reprezentowane przez obłożenie macierzy ρ przez transformacje unitarne. Obrazem każdego kanału będzie pewna elipsoida zawarta w kuli Blocha.

Ćwiczenie 13 *Jakie klasyczne kanały są odwracalne?*

Kolejną klasą kanałów, już nieodwracanych są kanały *random unitary*, gdy obroty unitarne z pewnego zbioru są stosowane do stanu zgodnie z pewnym rozkładem prawdopodobieństwa.

Ćwiczenie 14 *Znaleźć obraz kanału (bit flip channel):*

$$\rho \mapsto p\rho + (1-p)\sigma_x \rho \sigma_x^\dagger$$

Ćwiczenie 15 *Jaka jest reprezentacja kanału który dokonuje skalowania kuli Blocha w kierunkach x, y, pozostawiając niezmieniony kierunek z (phase flip channel)?*

Ćwiczenie 16 *Jaka jest reprezentacja kanału, który jednostajnie skaluje kulę Blocha (depolarising channel)?*

Ćwiczenie 17 *Niech Φ będzie odwzorowaniem skalującym kulę Blocha w kierunkach x, y, z o czynniki α, β, γ. Jakie ograniczenia na czynniki wprowadza warunek dodatniości, a jakie warunek kompletnej dodatniości?*

Wszystkie kanały *random unitary* są unitalne (bistochastyczne). Implikacja przeciwna zachodzi tylko dla qubitu.

Kanał *amplitude damping* jest reprezentowany przez izotropowe kurczenie się kuli Blocha do bieguna północnego. Jeżeli układem jest atom dwupoziomowy z pewnym prawdopodobieństwem emisji fotonu na jednostkę czasu, to zmiana stanu tego układu w pewnym okresie czasu będzie dana właśnie kanałem *amplitude damping*.

Ćwiczenie 18 *Znajdź reprezentację Kraussa kanału amplitude damping. Znajdź przypadek ogólny opadania na stan Gibbsa.*

Ćwiczenie 19 *Jak można sparametryzować i scharakteryzować wszystkie kanały bitowe?*

Ćwiczenie 20 *Pokaż, że zbiór kanałów jednoqubitowych jest 12 wymiarowy. Czemu odpowiadają te wymiary? Ile wymiarów ma zbiór kanałów unitalnych?*

Pomiary uogólnione

Pomiar uogólniony funkcji mierzalnej f to odwzorowanie wyników pomiaru w zbiór funkcji nieujemnych $\{\langle m_i|\}$, f-mierzalnych, sumujących się do $\langle \mathbb{1}|$ (czyli takie funkcje mogą być interpretowane jako wiersze pewnej macierzy stochastycznej). Pomiar uogólniony uwzględnia błąd pomiarowy - nośniki funkcji $\langle m_i|$ nakładają się na siebie. Prawdopodobieństwo otrzymania i-tego wyniku wynosi $p_i = \langle m_i|p\rangle$.

Działanie pomiaru uogólnionego na stany jest reprezentowane przez macierze substochastyczne K_i sumujące się do macierzy stochastycznej. Stanem po pomiarze jest $K_i|p\rangle/\langle \mathbb{1}|K_i|p\rangle$. Zachodzi zależność $\langle m_i| = \langle \mathbb{1}|K_i$.

Twierdzenia o podnoszeniu

Twierdzenie: Każdą macierz gęstości układu d-poziomowego można przedstawić jako ślad częściowy stanu czystego układu złożonego. Taki stan czysty nazywa się *puryfikacją* stanu ρ.

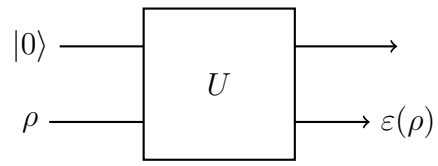
Ćwiczenie 21 *Jaką mamy swobodę wyboru stanów układu złożonego, odpowiadających danemu stanowi podukładu?*

Twierdzenie: Każdy kanał kwantowy da się zapisać jako $\rho \mapsto \mathrm{Tr}_1(U\eta \otimes \rho U^\dagger)$.

Dowód: Weźmy $\eta = |e_1\rangle\langle e_1|$ i niech U_{ij} oznacza ij-ty blok macierzy U. Wtedy $\mathrm{Tr}_1(U\eta \otimes \rho U^\dagger) = \sum_i U_{i1}\rho U_{i1}^\dagger$, zatem ma postać Kraussa. By przeprowadzić dowód w drugą stronę, trzeba udowodnić, że macierz, której pierwsza kolumna bloków jest zadana, może zostać przy pewnym założeniu rozszerzona do macierzy unitarnej.

Ćwiczenie 22 *Załóżmy, że mamy dane pierwszą kolumnę bloków pewnej macierzy. Kiedy da się dobudować brakującą część tak, by była ona unitarna?*

Rysunkowo, możemy przedstawić to następująco:

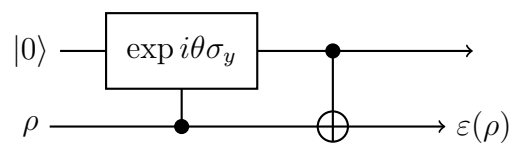


Dla tego samego U możemy zamienić podukłady rolami. Wtedy otrzymamy tzw. *kanał komplementarny* do ε.

Ćwiczenie 23 *Pokaż, że kanał amplitude damping:*

$$A_1 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}, A_2 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}$$

można zrealizować jako:



gdzie $\gamma = \sin^2\theta$.

Pomiar uogólniony (POVM) jest dany wzorem (16), jeżeli interesuje nas tylko rozkład prawdopodobieństwa na wyjściu. Jeżeli natomiast interesuje nas również to, co dzieje się z układem po pomiarze, mamy:

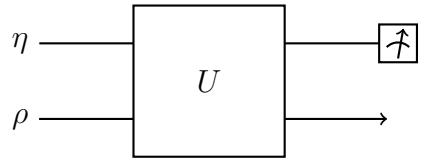
$$\rho \xrightarrow{p_i = \mathrm{Tr}\left(\rho \sum_j X_j^{(i)\dagger} X_j^{(i)}\right)} \frac{\sum_j X_j^{(i)} \rho X_j^{(i)\dagger}}{\mathrm{Tr}\left(\rho \sum_j X_j^{(i)\dagger} X_j^{(i)}\right)}, \quad \sum_{ij} X_j^{(i)\dagger} X_j^{(i)} = I \tag{18}$$

Jeżeli interesują nas tylko prawdopodobieństwa, przechodzimy do wzoru (16) poprzez: $M_i = \sum_j X_j^{(i)\dagger} X_j^{(i)}$

Twierdzenie: Każdy pomiar uogólniony na ρ da się przedstawić jako pomiar układu z dołączonym pewnym innym układem, po pewnym czasie wspólnej ewolucji.

Dowód: Podobnie jak w dowodzie poprzedniego twierdzenia startujemy ze stanu $|e_1\rangle\langle e_1| \otimes \rho$, ale baza dołączonego układu jest indeksowana wszystkimi parami ij. Bazę pomiarową stanowią projektory $|e_{ij}\rangle\langle e_{ij}|$, ale po pomiarze następuje "sklejenie" wyników o tym samym i.

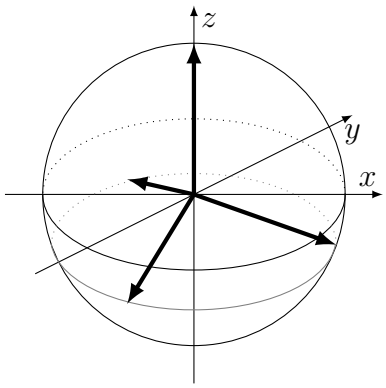
Rysunkowo, możemy przedstawić to następująco:



Teoria POVM

SIC POVMs Istnieje d^2 prostych w $\mathbb{C}^d$ o takim samym kącie pomiędzy prostymi w każdej parze. Jest to maksymalna liczność zbioru takich linii i przypuszcza się (*Zauner conjecture*), że zbiór ten istnieje dla każdego d. Można wskazać konstrukcję aż do wymiaru 21 i kilku wyższych, numerycznie do 151 i kilku wyższych.

Projektory na takie wektory sumują się do operatora dI_d, a iloczyn HS parami różnych projektorów jest zawsze taki sam. Dla qubitu, projektory te są wierzchołkami czworościanu foremnego na sferze Blocha:



Ćwiczenie 24 *Wyznacz macierze powyższych projektorów*

Odp. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ $\quad \frac{1}{3}\begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & 2 \end{bmatrix}$ $\quad \frac{1}{3}\begin{bmatrix} 1 & \sqrt{2}e^{i\frac{2\pi}{3}} \\ \sqrt{2}e^{i\frac{-2\pi}{3}} & 2 \end{bmatrix}$ $\quad \frac{1}{3}\begin{bmatrix} 1 & \sqrt{2}e^{-i\frac{2\pi}{3}} \\ \sqrt{2}e^{i\frac{2\pi}{3}} & 2 \end{bmatrix}$

Projektory takie sumują się do $2I_2$ (dI_d w przypadku ogólnym). Skalując je przez czynnik $\frac{1}{2}$, dostaniemy POVM nazywany SIC POVM (*symmetric, informationally complete*).

POVM daje cztery rezultaty, oznaczmy je jako $0, \ldots, 3$. Przy pomiarze macierzy gęstości $\rho = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z)$ otrzymamy następujące częstości zliczeń wyników:

$$\begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} = \frac{1}{4}\mathbb{1} + \frac{1}{12}\begin{bmatrix} 0 & 0 & 3 \\ 2\sqrt{2} & 0 & -1 \\ -\sqrt{2} & \sqrt{6} & -1 \\ -\sqrt{2} & -\sqrt{6} & -1 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} \tag{19}$$

Zauważmy, że kolumny macierzy są do siebie ortogonalne. Wzór ten jest izometrycznym zanurzeniem kuli Blocha w podprzestrzeń afiniczną czterowymiarowych rozkładów prawdopodobieństwa.

Ćwiczenie 25 *Wyznacz wzory na x, y, z.*

Rozróżnianie stanów kwantowych - teoria Helstrøma Załóżmy, że źródło produkuje dwa stany ρ_1 i ρ_2 z prawdopodobieństwami odpowiednio p_1 i p_2. Naszym zadaniem jest skonstruować dwuwartościowy POVM, dla którego prawdopodobieństwo poprawnej odpowiedzi będzie maksymalne.

Dwuwartościowy POVM jest postaci $\{A, I - A\}$, dla $0 \leqslant A \leqslant I$. Szukamy maksimum wyrażenia $\mathrm{Tr}(Ap_1\rho_1) + \mathrm{Tr}((I - A)p_2\rho_2) = p_2 + \mathrm{Tr}(A(p_1\rho_1 - p_2\rho_2))$. Widzimy, że A powinno być projektorem na sumę prostą podprzestrzeni własnych $p_1\rho_1 - p_2\rho_2$ odpowiadających dodatnim wartościom własnym.

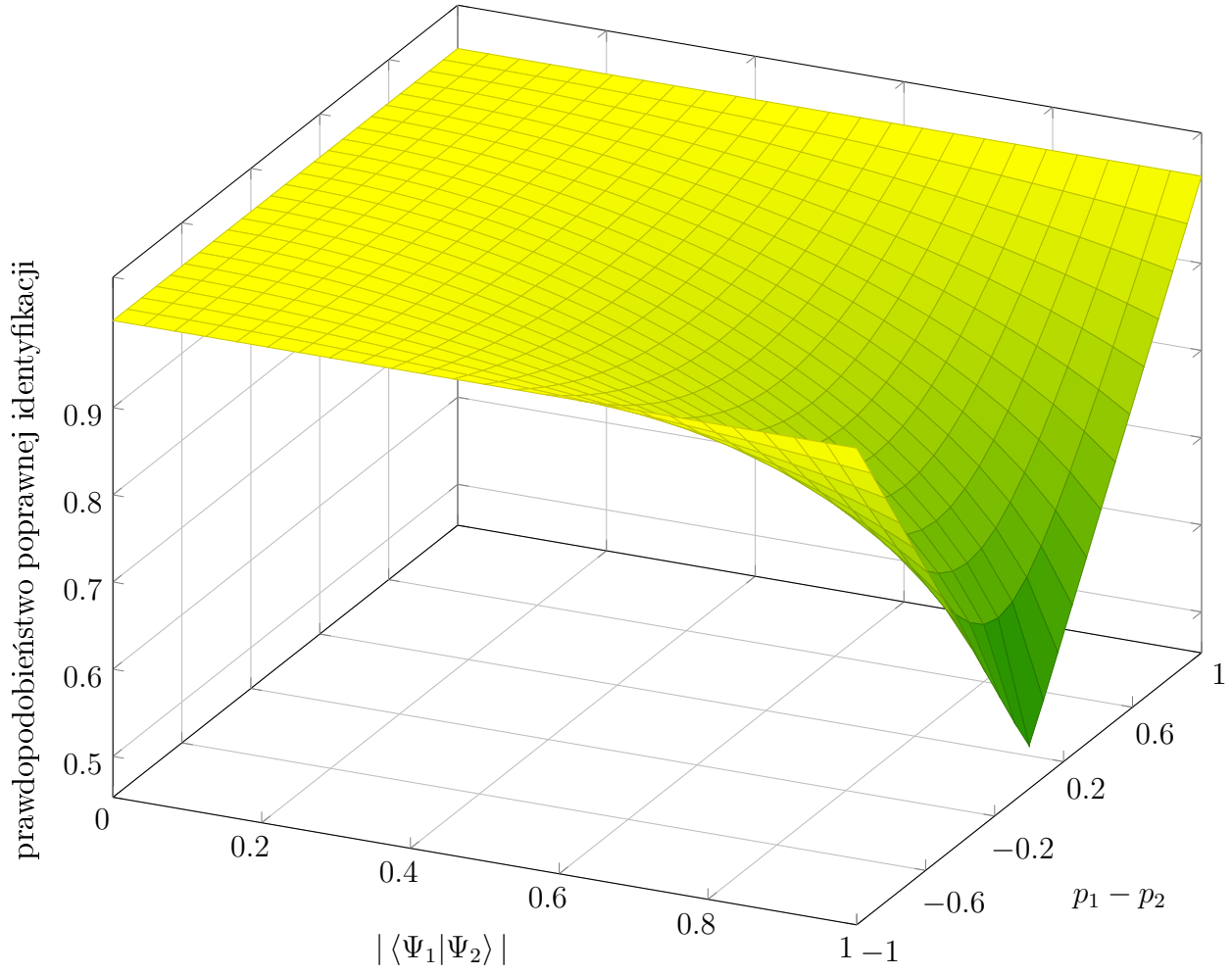
Jeżeli $p_1\rho_1 \geqslant p_2\rho_2$, to $A = I$ - optymalnie jest po prostu obstawiać 1 bez wykonywania żadnego pomiaru.

Macierz $p_1\rho_1 - p_2\rho_2$ nosi nazwę macierzy Helstrøma. Prawdopodobieństwo otrzymania poprawnego wyniku:

$$p_{sukces} = \frac{1}{2}\left(1 + ||p_1\rho_1 - p_2\rho_2||_1\right), \tag{20}$$

gdzie $||\cdot||_1$ jest normą śladową - sumą wartości bezwzględnych wartości własnych.

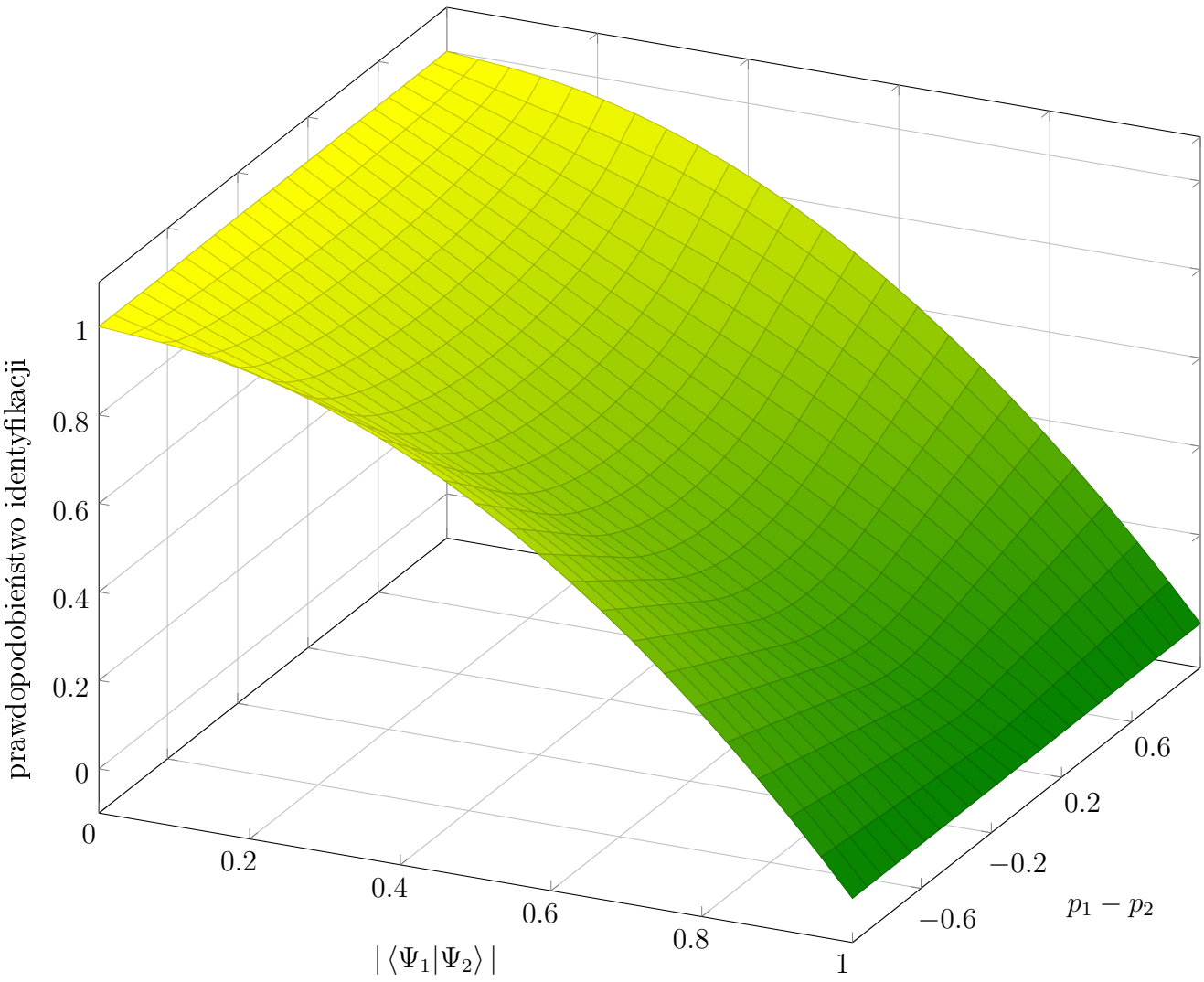
Ćwiczenie 26 *Wyprowadź wzór na prawdopodobieństwo sukcesu rozróżnienia dwóch stanów czystych wysyłanych z dowolnymi prawdopodobieństwami, zależne od $p_1 - p_2$ i $|\langle\Psi_1|\Psi_2\rangle|^2$.*



Ćwiczenie 27 *Znajdź POVM o trzech elementach: 1,2,? który wykrywa nieortogonalne stany (pojawiające się z prawdopodobieństwami p_1 i p_2) bez błędu (tzn. jeżeli wyszła 1 lub 2, możemy być pewni, że to zostało nadane) minimalizującego prawdopodobieństwo "?". Wyprowadź wzór na minimalne $p_?$.*

Odp.

$$p_? = \begin{cases} p_1 + |\langle\Psi_1|\Psi_2\rangle|^2 p_2 & \text{gdy } p_2|\langle\Psi_1|\Psi_2\rangle|^2 \geqslant p_1 \\ p_2 + |\langle\Psi_1|\Psi_2\rangle|^2 p_1 & \text{gdy } p_1|\langle\Psi_1|\Psi_2\rangle|^2 \geqslant p_2 \\ 2|\langle\Psi_1|\Psi_2\rangle|\sqrt{p_1 p_2} & \text{w przeciwnym wypadku} \end{cases}$$


prawdopodobieństwo identyfikacji
1
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1
$|\langle\Psi_1|\Psi_2\rangle|$
−0.6
−0.2
0.2
0.6
$p_1 - p_2$

Działania na polaryzacji fotonu

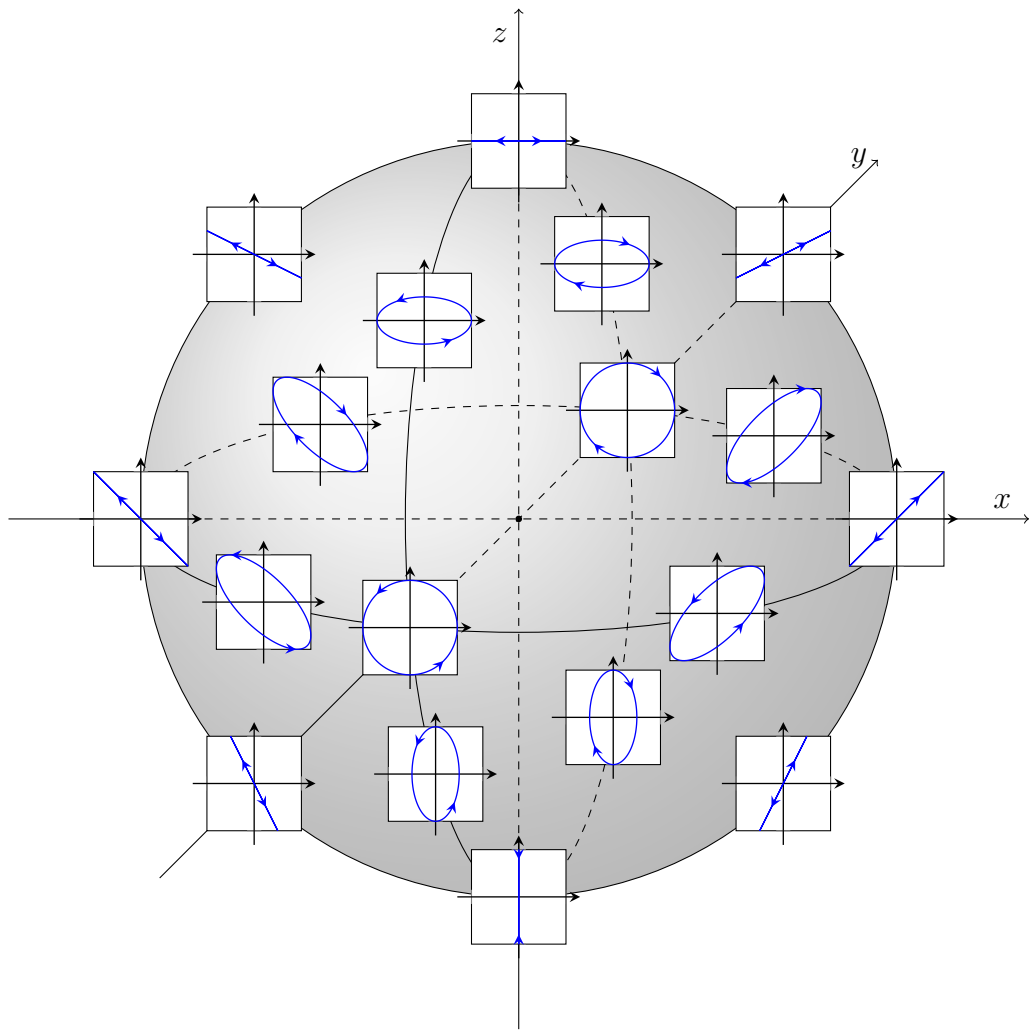
Fala elektromagnetyczna propagująca wzdłuż osi z może mieć 2 polaryzacje - poziomą i pionową, a także być kombinacją fal podstawowych:

$$e^{i\omega t}\begin{bmatrix}1\\0\end{bmatrix} - \text{polaryzacja pozioma} \qquad e^{i\omega t}\begin{bmatrix}0\\1\end{bmatrix} - \text{polaryzacja pionowa}$$

$$e^{i\omega t}\begin{bmatrix}1\\1\end{bmatrix} - \text{polaryzacja } 45^\circ \qquad e^{i\omega t}\begin{bmatrix}1\\-1\end{bmatrix} - \text{polaryzacja - } 45^\circ$$

$$e^{i\omega t}\begin{bmatrix}1\\i\end{bmatrix} - \text{polaryzacja prawoskrętna} \qquad e^{i\omega t}\begin{bmatrix}1\\-i\end{bmatrix} - \text{polaryzacja lewoskrętna}$$

Dla polaryzacji fali nie gra roli ani amplituda fali ani jej faza globalna, zatem zbiorem możliwych polaryzacji jest również sfera (tzw. *sfera Poincaré*).



Energia fotonu to kwadrat normy wektora pola elektrycznego. Z zasady zachowania energii wynika, że każdy element optyczny, który przekształca stan fotonu zachowując jego energię musi być operatorem unitarnym. Podobnie operator działający na stanach dwufotonowych musi być operacją z

$U(4)$. Operacje unitarne na przestrzeni Hilberta n qubitów nazywane są *bramkami*, w analogii do klasycznych bramek n-bitowych.

Rozważać będziemy następujące elementy optyczne:

Skręcenie płaszczyzny polaryzacji o kąt α (bramka $e^{i\alpha\sigma_y}$):

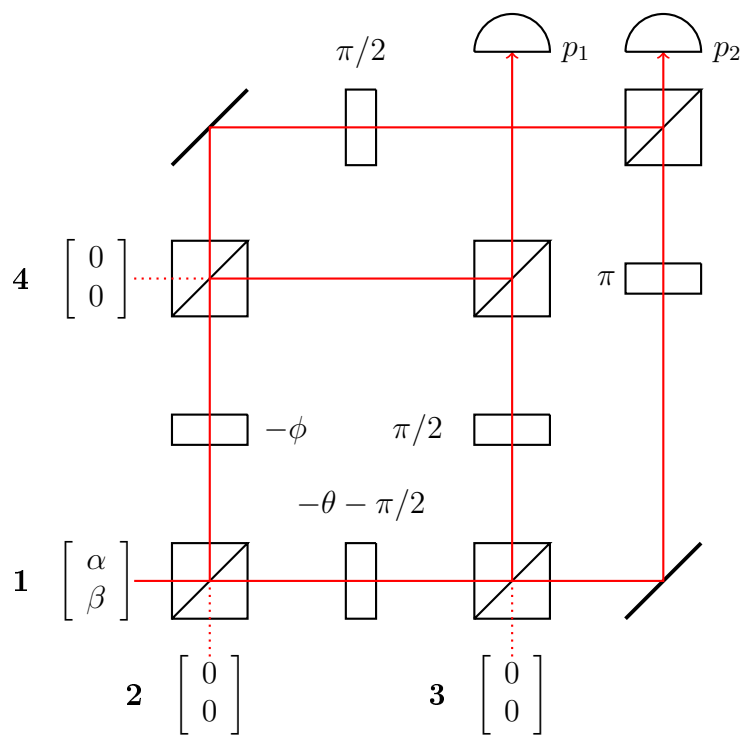
$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \tag{21}$$

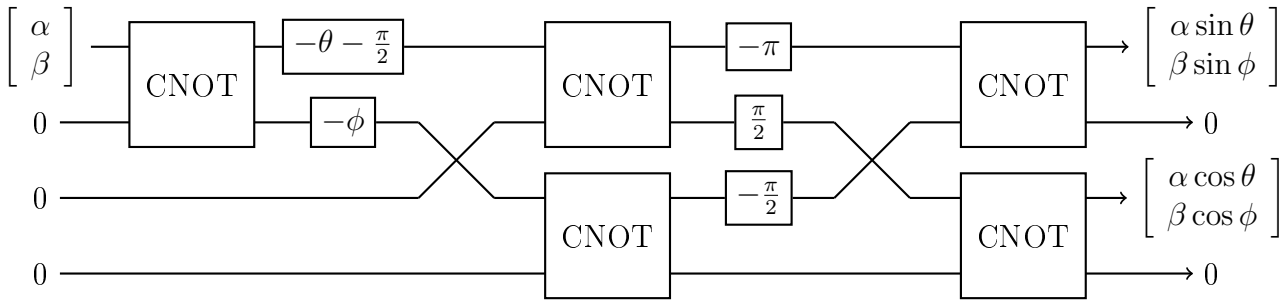
Polaryzujący dzielnik wiązki, przepuszcza polaryzację poziomą, a odbija polaryzację pionową. Macierz w bazie xh, xv, yh, yv

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \end{bmatrix} \tag{22}$$

Jest to dwuqubitowa bramka CNOT (*controlled NOT*). Qubit polaryzacji jest qubitem kontrolnym, a qubitem kontrolowanym jest qubit drogi.

Przeanalizuj działanie układu z rysunku:





$$\begin{bmatrix}\alpha\\ \beta\\ \hline 0\\ 0\\ \hline 0\\ 0\\ \hline 0\\ 0\end{bmatrix} \longmapsto \begin{bmatrix}\alpha\\ 0\\ \hline 0\\ \beta\\ \hline 0\\ 0\\ \hline 0\\ 0\end{bmatrix} \longmapsto \begin{bmatrix}-\alpha\sin\theta\\ \alpha\cos\theta\\ \hline -\beta\sin\phi\\ \beta\cos\phi\\ \hline 0\\ 0\\ \hline 0\\ 0\end{bmatrix} \longmapsto \begin{bmatrix}-\alpha\sin\theta\\ 0\\ \hline -\beta\sin\phi\\ 0\\ \hline 0\\ \alpha\cos\theta\\ \hline 0\\ \beta\cos\phi\end{bmatrix} \longmapsto \begin{bmatrix}\alpha\sin\theta\\ 0\\ \hline 0\\ \beta\sin\phi\\ \hline -\alpha\cos\theta\\ 0\\ \hline 0\\ \beta\cos\phi\end{bmatrix} \longmapsto \begin{bmatrix}\alpha\sin\theta\\ \beta\sin\phi\\ \hline 0\\ 0\\ \hline -\alpha\cos\theta\\ \beta\cos\phi\\ \hline 0\\ 0\end{bmatrix}$$

$$\Psi = \begin{bmatrix}\alpha\\ \beta\end{bmatrix}, \qquad p_1 = \mathrm{Tr}\left(\begin{bmatrix}\cos^2\theta & 0\\ 0 & \cos^2\phi\end{bmatrix}|\Psi\rangle\langle\Psi|\right) \qquad p_2 = \mathrm{Tr}\left(\begin{bmatrix}\sin^2\theta & 0\\ 0 & \sin^2\phi\end{bmatrix}|\Psi\rangle\langle\Psi|\right),$$

Ćwiczenie 28 *Powyższy układ realizuje dwuelementowy POVM dla qubitu o diagonalnych elementach. Jak przy pomocy tego układu i jednoqubitowych branek unitarnych skonstruować dowolny POVM dla qubitu?*

Bramki jednoqubitowe

Twierdzenie: Dowolną d-arną bramkę logiczną można zrealizować jako złożenie bramek NAND.

Twierdzenie: Dowolną operację $U(n)$ można zrealizować przy pomocy bramek jednoqubitowych i bramki CNOT.

Ćwiczenie 29 *Pokaż, że nie istnieje uniwersalna bramka NOT dla qubitu.*

Płytka opóźniająca zorientowana w bazie standartowej h, v (lub ściśnięcie światłowodu w kierunku poziomym) wprowadzająca różnicę faz δ dana jest macierzą

$$\begin{bmatrix} e^{i\delta/2} & 0\\ 0 & e^{-i\delta/2}\end{bmatrix} \tag{23}$$

Ćwiczenie 30 *Pokaż, że dowolną bramkę qubitową w polaryzacjach fotonu można zrealizować jako trzy ściśnięcia światłowodu w kierunkach* $0°, 45°, 0°$.

No cloning, broadcasting, BB84

Spróbujmy skonstruować operację, która dostaje na wejściu ustalony wektor stanu pustego rejestru ψ i wektor stanu ϕ na wejściu i produkuje na wyjściu wektor $\phi \otimes \phi$. Załóżmy, że operacja ta działa dla dwóch stanów:

$$U(\phi_1 \otimes \psi) = \phi_1 \otimes \phi_1$$
$$U(\phi_2 \otimes \psi) = \phi_2 \otimes \phi_2.$$

Operacja powinna być unitarna, a stąd widać, że wektory stanów ϕ_1, ϕ_2 muszą być ortogonalne. Urządzenie klonujące jest możliwe tylko dla zbioru ortogonalnych stanów czystych. Zbiór stanów czystych, na których klonowanie działa determinuje całkowicie urządzenie klonujące. Ma ono postać: *zmierz w bazie ortonornalnej i na podstawie wyniku przygotuj dwie kopie.* Kombinacje wypukłe stanów klonowanych nie są klonowane, ale *rozgłaszane* - otrzymujemy stan mieszany wielu kopii o poprawnych rozkładach brzegowych, ale skorelowanych ze sobą. Struktury beoadcastowe pojawiają się w mechaniźmie "kwantowego darwinizmu" - wyłaniania się obiektywnej rzeczywistości dla obiektu kwantowego.

Ćwiczenie 31 *Czy może pomóc rozważenie maszyny klonującej z dodatkową przestrzenią Hilberta:* $U : |i\rangle \otimes |0\rangle \otimes |0\rangle \to |i\rangle \otimes |i\rangle \otimes |X_i\rangle$ *?*

To samo ograniczenie dotyczy stanów klasycznych - wszystkie stany czyste mogą być klonowane (ponieważ są do siebie ortogonalne), natomiast stany mieszane nie mogą być klonowane, a tylko rozgłaszane.

Możemy natomiast spróbować znaleźć maszynę klonującą, która wykonuje zadanie w sposób przybliżony i zminimalizować błąd klonowania (maksymalny lub średni).

Obserwację powyższą możemy wyrazić również tak: załóżmy że mamy kanał o jednym wejściu i dwóch wyjściach $\Phi_{1,2} : \mathcal{B}(\mathcal{H}_{in}) \to \mathcal{B}(\mathcal{H}_{out1}) \otimes \mathcal{B}(\mathcal{H}_{out1})$. Zawsze możemy wyśladować jedno z wyjść i otrzymać kanały brzegowe Φ_1 i Φ_2. Nie istnienie maszyny klonującej oznacza, że nie istnieje taki kanał, którego oboma kanałami brzegowymi są kanały identycznościowe.

BB84 W protokole BB84 strony A i B chcą ustalić wspólny klucz bitowy, nieznany osobom trzecim. Protokół pozwala na znalezienie wspólnego klucza i mieć pewność że nikt inny nie ma o nim informacji.

Strona A losuje ciąg wartości bitów: 0,1 i ciąg baz ze zbioru

$$\{|0\rangle, |1\rangle\}, \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}.$$

Koduje i-ty bit w i-tej bazie i wysyła do B. Strona B losuje dla każdego bitu jedną z baz z powyższego zbioru i dokonuje pomiaru. Po przesłaniu wszystkich bitów, Strona A informuje publicznie o ciągu użytych baz. Strona B odpowiada, które z baz wybranych przez niego były zgodne. Bity, dla których bazy się nie zgadzały (połowa wszystkich) są usuwane i obie strony mają ten sam ciąg bitów.

Załóżmy teraz, że w tor włącza się podsłuchiwacz , który dokonuje pomiaru w jednej z baz a następnie dokonuje przygotowania bitu w tej bazie zgodnie z otrzymanym wynikiem pomiaru. Podsłuchujący dla połowy bitów trafia z wyborem bazy, wtedy odczytuje prawidłową wartość bez zmieniania

jej. Jeżeli natomiast wybierze bazę niezgodną z nadawcą, wtedy z prawdopodobieństwem 1/2 podsłuchiwacz odczyta prawidłową wartość i niezależnie z prawdopodobieństwem 1/2 odbiorca odczyta niezmienioną wartość bitu. Oznacza to, że 1/4 wysłanych bitów zostanie podsłuchana nieprawidłowo, ale też 1/4 podłuchanych bitów będzie miałą u nadawcy inną wartość niż u odbiorcy. Poświęcenie części bitów klucza pozwala na wykrycie podsłuchu.

Jeżeli źródło fotonów A jest dalekie od jednofotonowego (koduje bit w wielu fotonach), to podsłuchujący może wstawić BS i będzie to trudne do stwierdzenia (strona B nie potrafi liczyć fotonów). BS puści część fotonów dalej, a część zapisze do pamięci (przetłumaczy np. na stan atomów dwupoziomowych). Następnie po ujawnieniu baz i informacji które bity są odrzucane a które nie, dokonuje ich pomiaru i ma klucz.

Nierówność CHSH

Rozważmy teraz czery zmienne losowe A_1, A_2, B_1, B_2 określone na przestrzeni probabilistycznej Ω i przyjmujące wartości ± 1. Zauważmy, że zachodzi ograniczenie $A_1B_1 + A_1B_2 + A_2B_1 - A_2B_2 \leqslant 2$ dla każdego punktu w Ω (w określonym punkcie x zachodzi $B_1(x) = B_2(x)$ **albo** $B_1(x) = -B_2(x)$). Biorąc średnią dostaniemy

$$-2 \leqslant \mathbb{E}(A_1B_1) + \mathbb{E}(A_1B_2) + \mathbb{E}(A_2B_1) - \mathbb{E}(A_2B_2) \leqslant 2 \tag{24}$$

Załóżmy że mamy źródło par cząstek o spinie 1/2 które rozbiegają się w przeciwnych kierunkach i następnie są mierzone jednocześnie (wzgl. źródła) w dwóch odległych laboratoriach. Każde laboratorium (A i B) wybiera losowo z równym prawdopodobieństwem jeden z dwóch kierunków spinu (1 lub 2) i dokonuje pomiaru. Wynik pomiaru spinu i w laboratorium C to zmienna losowa C_i. Zmienne A_1, A_2, B_1, B_2 powinny spełniać nierówność (24). Przyjrzyjmy się co się stanie, jeżeli mierzonymi wielkościami są są $\hat{A}_1 = \sigma_z, \hat{A}_2 = \sigma_x, \hat{B}_1 = (\sigma_x + \sigma_z)/\sqrt{2}, \hat{B}_2 = (\sigma_z - \sigma_x)/\sqrt{2}$, a źródło produkuje stan czysty reprezentowany przez wektor $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

Ćwiczenie 32 *Pokaż, że nierówność CHSH nie jest łamana w stanach separowalnych.*

W mechanice kwantowej lewa strona nierówności nie może przekroczyć wartości $2\sqrt{2}$ (Tsirelson's bound).

Wprowadźmy na korelacje jedynie ograniczenie, by nie mogły nieść informacji, to znaczy, że jeżeli jedna strona mierzy wielkość A, a strona druga mierzy jedną z dwóch wielkości B lub B', to rozkład brzegowy $p(a)$ nie może zależeć od wybranej obserwabli po drugiej stronie:

$$\forall B \ \sum_b P(a, b|A, B) = P(a|A) \tag{25}$$

W przeciwnym wypadku, byłoby możliwe natychmiastowe przenoszenie informacji pomiędzy stronami. Jeżeli nałożymy tylko warunek non-signaling na korelacje, to lewa strona nierówności CHSH może osiągnąć wartość 4.

Ćwiczenie 33 *Załóżmy, że*

$$p(ab|AB) = \left[\begin{array}{c|c|c|c} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \end{array}\right] \tag{26}$$

Pokaż, że jest taki układ prawdopobieństw warunkowych nie przenosi informacji. Ile wynosi lewa strona nierówność CHSH dla tego rozkładu? Jak należałoby zmodyfikować powyższą macierz, by dostać rozkład przenoszący informację?

Nierówności Bella są wyprowadzane przy założeniu istnienia wspólnej przestrzeni probabilistycznej dla zmiennych losowych, co jest jednym z aksjomatów klasycznej teorii prawdopodobieństwa (aksjomaty Kołmogorowa). Łamanie nierówności Bella w mechanice kwantowej pokazuje że teoria ta nie spełnia aksjomatów Kołmogorowa - jest niekołmogorowska.

Teleportacja

Załóżmy że strony A i B współdzielą stan czysty splątany dwóch qubitów reprezentowany przez wektor $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ i dodatkowo A posiada qubit w pewnym stanie $\alpha|0\rangle + \beta|1\rangle$. A wykonuje na posiadanych dwóch qubitach pomiar łaczny w *bazie magicznej*:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Z równymi prawdopodobieństwami, po pomiarze stanem qubitu posiadanego przez B będzie:

$$\alpha|0\rangle + \beta|1\rangle$$
$$\alpha|0\rangle - \beta|1\rangle$$
$$\alpha|1\rangle + \beta|0\rangle$$
$$\alpha|1\rangle - \beta|0\rangle$$

A informuje o swoim wyniku B (przesyłając 2 bity), który stosując stosowną operację unitarną przekształca stan swojego qubitu do stanu posiadanego początkowo przez A. Współdzielony stan splątany został zniszczony, a A posiada teraz dwa qubity w stanie czystym reprezentowanym przez jeden z wektorów bazy magicznej. Do przesłania jednego qubitu musimy zużyć dwa bity i jedną parę w stanie maksymalnie splątanym.

Ćwiczenie 34 *Pokaż, że stany z bazy magicznej dwóch qubitów można przekształcać na siebie za pomocą lokalnej transformacji unitarnej.*

Ćwiczenie 35 *Jak wyglądają wektory bazy magicznej dwóch qutritów? W jaki sposób teleportować stan qutritu przy pomocy stanu czystego o wektorze z bazy magicznej dwóch qutritów?*

Ćwiczenie 36 *Jak teleportować stan qutritu za pomocą dwóch par splątanych qubitów?*

Jeżeli spróbujemy teleportować stan używając pary w stanie czystym, niemaksymalnie splątanym, to dostaniemy niemożliwy do skorygowania błąd transmisji.

Ćwiczenie 37 *Niech nadawca i odbiorca dzielą parę w stanie czystym $\gamma|00\rangle + \delta|11\rangle$, gdzie $\alpha \geqslant \beta$. Skonstruuj POVM, który z maksymalnym prawdopodobieństwem doprowadzi stan (nieunormowany) po pomiarze $\alpha\gamma|00\rangle + \beta\delta|11\rangle$) do postaci stanu wyjściowego dla teleportacji idealnej: $(\alpha|00\rangle + \beta|11\rangle)/\sqrt{2}$. Ile wynosi te prawdopodobieństwo? Wykonaj to samo dla pozostałych stanów po pomiarze. Jakie jest prawdopodobieństwo całkowite poprawnej teleportacji?*

Miary i kryteria splątania

LOCC Klasa operacji LOCC to operacje na stanach układu złożonego, w których możemy używać operacji lokalnych i klasycznej komunikacji. Operację, którą wykonamy na lokalnym podukładzie możemy uzależniać od wyniku pomiaru wykonanego na drugim podukładzie, i na odwrót. Możemy w ten sposób sekwencyjnie przesyłać sobie wyniki lokalnych pomiarów i uzależniać od otrzymanych wartości operacje wykonywane przez nas na stanie. Jest trudna w charakteryzacji. Każda dobrze określona miara splątania powinna być monotoniczna ze względu na operacji LOCC, tzn. po wykonaniu dowolnej takiej operacji na stanie, miara splątania stanu nie może wzrosnąć.

Destylacja i tworzenie splątania Załóżmy, że istnieje protokół dystylacji (operacja LOCC), pozwalający z N kopii stanów niemaksymalnie splątanych stworzyć M kopii stanów maksymalnie splątanych:

$$\rho^{\otimes N} \underset{Formation}{\overset{Distilation}{\rightleftarrows}} \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes M} \otimes ... \tag{27}$$

Dla danego N zmaksymalizujmy stosunek M/N po wszystkich możliwych prokołach, a następnie przejdźmy z $N \to \infty$. Otrzymana liczba jest miarą „jakości“ (z punktu widzenia zastosowań) splątania stanu wejściowego, nazywaną *entanglement of distilation* (EOD).

Z drugiej strony możemy zapytać ile M par stanów maksymalnie splątanych be stworzyć N kopii stanu. Minimalizujemy stosunek M/N po wszystkich protokołach i przechodzimy z $N \to \infty$. Otrzymaną liczbę nazywamy *entanglement of formation* (EOF):

Dla dwucząstkowego stanu czystego, EOF jest równe EOD i obie miary są równe entropii von Neumanna (entropia Shannona na widmie macierzy gęstości) śladu częściowego stanu. Jest to jedyna poprawnie zdefiniowana miara splątania dla stanów czystych. Dla stanów mieszanych nie ma jednoznacznie zdefiniowanej miary splątania, a EOD $\leqslant$ EOF. Istnieją stany splątane, z których nie da się wydestylować stanów czystych maksymalnie splątanych. Takie slątanie nazywamy *splątaniem związanym* (*bound entanglement*).

W szczególnym przypadku dwóch qubitów istnieje wzór na EOF stanu. Zdefiniujmy dla stanu wielkość *concurrence* wzorem: $C(\rho) = \max\{0, 2\lambda_{max} - 1\}$, gdzie λ_{max} oznacza maksymalną wartość własną macierzy hermitowskiej: $\sqrt{\sqrt{\rho}(\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)\sqrt{\rho}}$. Liczba ta jest dla wszystkich stanów w przedziale $[0, 1]$. Oznacza to, że para liczb:

$$\frac{1 + \sqrt{1 - C(\rho)^2}}{2}, \quad \frac{1 - \sqrt{1 - C(\rho)^2}}{2} \tag{28}$$

jest rozkładem prawdopodobieństwa. EOF stanu ρ to entropia Shannona tego rozkładu:

$$EOF = \frac{1+\sqrt{1-C(\rho)^2}}{2}\log_2\frac{1+\sqrt{1-C(\rho)^2}}{2} + \frac{1-\sqrt{1-C(\rho)^2}}{2}\log_2\frac{1-\sqrt{1-C(\rho)^2}}{2}. \tag{29}$$

Inną miarą splątania jest *negativity*: $\mathcal{N}(\rho) = \frac{1}{2}(||\rho^\Gamma||_1 - 1)$ (gdzie $||\cdot||_1$ — norma śladowa i ρ^Γ — ρ po częściowej transpozycji) oraz *logarithmic negativity*: $EN(\rho) = \log_2 ||\rho^\Gamma||_1$. Ta ostatnia jest ograniczeniem dolnym na EOD.

Kryterium częściowej transpozycji Jeżeli stan jest separowalny, to jego częściowa transpozycja $(I \otimes T)\rho$ jest półdodatnio określona. Stany wykrywane przez częściową transpozycję nazywamy NPT (negative partial transposition).

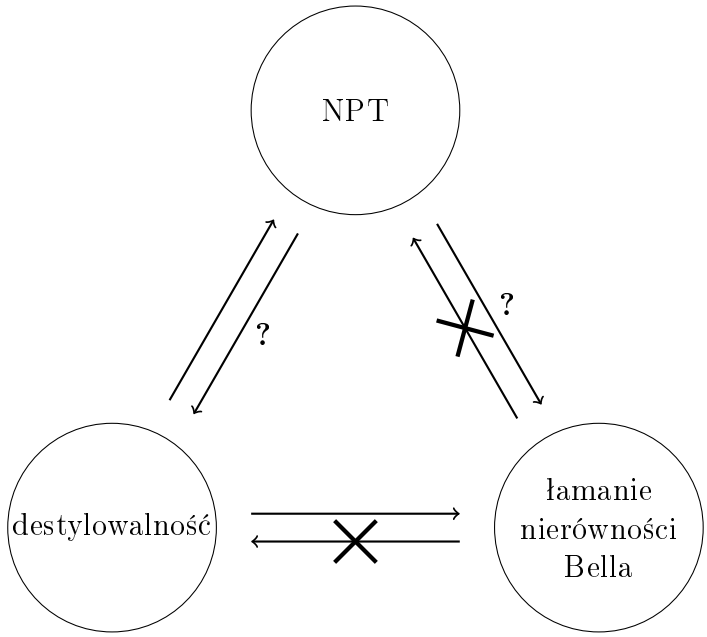
Ćwiczenie 38 *Pokaż, że kryterium częściowej transpozycji wykrywa wszystkie czyste stany splątane.*

W wymiarach 2×2, 2×3, 3×2 częściowa transpozycja wykrywa wszystkie stany splątane. W wyższych wymiarach istnieją stany splątane (mieszane) o dodatniej częściowej transpozycji (PPT).

Ćwiczenie 39 *Znajdź podzbiór stanów separowalnych w sympleksie stanów diagonalnych w bazie magicznej dwóch qbitów.*

Splątanie PPT Stany splątane PPT (o dodatniej częściowej traspozycji) spotkamy już dla dwóch qutritów. Można skonstruować przykład takiego stanu za pomocą nieroszerzalnych baz produktowych (UPB): Skonstruujmy na płaszczyźnie $\mathbb{R}^2$ pięciokąt foremny scentrowany w 0. Do wektorów wskazujących na jego wierzchołki dodajmy składową z o takiej wartości, by każde dwa wektory odpowiadające niesąsiednim wierzchołkom były ortogonalne. Dostajemy układ wektorów w $\mathbb{R}^3 \subset \mathbb{C}^3$. Teraz rozważmy układ 5 wektorów w $\mathbb{C}^2 \otimes \mathbb{C}^3 \supset \{\psi_i \otimes \psi_{2i}\}$. Zauważmy, że nie istnieje wektor produktowy do nich prostopadły, zatem dopełnienie ortogonalne podprzestrzeni przez nie napinanej jest 4-wymiarową podprzestrzenią nie zawierającą niezerowego wektora produktowego $\Rightarrow$ unormowany projektor na tę podprzestrzeń jest stanem splątanym. Stan ten nie zmienia się pod działaniem częściowej transpozycji, zatem jest stanem splątanym PPT.

Operacje LOCC zachowują dodatniość częściowej transpozycji. Wniosek - ze stanu splątanego PPT nie można wydestylować żadnych par maksymalnie splątanych. Splątanie stanu PPT jest *splątaniem związanym*. Zachodzą następujące związki:



Kryterium odwzorowań dodatnich Kryterium częściowej transpozycji jest ważnym, ale szczególnym przypadkiem kryterium odwzorowań dodatnich.

Jeżeli Λ jest odwzorowaniem dodatnim, to dla stanu produktowego $\rho \otimes \sigma$, $(I \otimes \Lambda)(\rho \otimes \sigma)$ też jest operatorem dodatnim. Własność ta zachodzi zatem dla wszystkich stanów separowalnych. Wiemy, że jeżeli Λ nie jest kompletnie dodatnie, to $(I \otimes \Lambda)$ nie jest dodatnie, czyli w działaniu na jakiś stan da operator niedodatni. W ten sposób wykrywa splątanie stanu. Twierdzenie Horodeckich mówi, że dla każdego stanu splątanego istnieje odwzorowanie dodatnie które go wykrywa.

Potrafimy stwierdzać splątanie stanu, jeżeli znamy wszystkie odwzorowania dodatnie. Jest to trudne zadanie. Przykładem takiego odwzorowania jest transpozycja. Dla wymiarów podukładów 2×2 i 2×3 transpozycja jest (z dokładnością do złożenia z odwzorowaniem kompletnie dodatnim i dodania odwzorowania kompletnie dodatniego) jedynym odwzorowaniem nie kompletnie dodatnim:

$$\Phi : \mathcal{B}(\mathbb{C}^{d_1}) \to \mathcal{B}(\mathbb{C}^{d_1}). \qquad d_1 d_2 \leqslant 6 \Rightarrow \left(\Phi \in \mathcal{P} \iff \Phi(\rho) = \sum_i A_i \rho^T A_i^\dagger + \sum_i B_i \rho B_i^\dagger \right) \tag{30}$$

Przykładem odwzorowania dodatniego, ale nie kopletnie dodatniego i nie powstającego z transpozycji, jest odwzorowanie Choi, które definiujemy w bazie standardowej:

$$\begin{aligned} CH(|e_i\rangle\langle e_i|) &= |e_i\rangle\langle e_i| + |e_{i+1}\rangle\langle e_{i+1}| \\ CH(|e_i\rangle\langle e_j|) &= -|e_i\rangle\langle e_j|, \text{ dla } i \neq j \end{aligned} \tag{31}$$

Odwzorowanie to jest w stanie wykrywać stany splątane PPT.

Ćwiczenie 40 *Dla odwzorowania Choi znajdź odwzorowanie dualne*

Kryterium realignmentu Innym ważnym kryterium wykrywania splątania jest kryterium realignemntu lub *normy krzyżowej (crossnorm)*. Kryterium to polega na skonstruowaniu nowej macierzy: $R(\rho)_{ij,kl} = \rho_{ik,jl}$. Obliczamy normę śladową tej macierzy (sumę jej wartości singularnych). Nie powinna ona przekroczyć 1 dla stanu separowalnego. Równoważnie, obliczamy sumę pierwiastków wartości własnych macierzy Gramma bloków macierzy gęstości.

Dowód: Łatwo sprawdzić, że dla stanu separowalnego czystego norma wynosi 1. Norma jest funkcjonałem wypukłym (nierówność trójkąta), zatem na stanie mieszanym separowalnym norma powinna być $\leqslant 1$ $\square$

Ćwiczenie 41 *Dla dwuparametrowej rodziny operatorów o śladzie równym* 1*:*

$$\rho = \frac{1}{3(1+a+b)} \left[\begin{array}{ccc|ccc|ccc} 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \end{array}\right] \tag{32}$$

Narysuj na płaszczyźnie ab obszary:

1. *stanów*
2. *stanów NPT*
3. *stanów wykrywanych przez odwzorowanie Choi*
4. *stanów wykrywanych przez odwzorowanie Choi dualne*
5. *stanów wykrywanych przez kryterium realignmentu*

Pokazaliśmy, że jeżeli $a < 1$ lub $b < 1$, to stan jest splątany. W tej rodzinie możemy pokazać, że pozostałe stany (gdy $a \geqslant 1$ i $b \geqslant 1$) są separowalne. Podziałajmy na stan ρ operacją $D \otimes D^*$, gdzie D jest macierzą unitarną diagonalną:

$$D = \begin{bmatrix} e^{i\phi_0} & \cdot & \cdot \\ \cdot & e^{i\phi_1} & \cdot \\ \cdot & \cdot & e^{i\phi_2} \end{bmatrix} \tag{33}$$

a następnie wycałkujmy to wyrażenie po kątach ϕ_0, ϕ_1, ϕ_2. Oznaczmy taka operację na stanie ρ jako Φ:

$$\Phi(\rho) = \int D \otimes D^* \rho (D \otimes D^*)^\dagger \mathrm{d}\phi_0 \mathrm{d}\phi_1 \mathrm{d}\phi_2 \tag{34}$$

Odwzorowanie takie zachowuje bez zmian wartości na diagonali i wyrazy pozadiagonalne w miejscach gdzie we wzorze (32) znajdują się 1, a pozostałe wartości zeruje (jest zatem projektorem). Co więcej, dla separowalnego ρ, $\Phi(\rho)$ będzie separowalne. Zauważmy, że stan (32) powstaje poprzez działanie odwzorowania Φ ze stanu, w którym w miejsce zer wstawimy jedynki, a taki stan (jako suma macierzy diagonalnej i projektora na wektor produktowy) jest separowalny.

Świadkowie splątania

Możemy przypisać odwzorowaniu $\Lambda : \mathcal{B}(\mathbb{C}^{d_1}) \to \mathcal{B}(\mathbb{C}^{d_2})$ obserwablę $W \in \mathcal{B}(\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2})$ za pomocą wzoru:

$$W = (I_{d_1} \otimes \Lambda) \left|\Psi\right\rangle \left\langle\Psi\right|, \tag{35}$$

gdzie $\Psi = \frac{1}{\sqrt{d_1}}\langle\sum_i |ii\rangle\rangle$). Odwzorowanie to przeprowadza odwzorowania kompletnie dodatnie w operatory dodatnie, a odwzorowania dodatnie w operatory dodatnie na wektorach produktowych. Odwzorowania dodatnie ale nie kompletnie dodatnie przechodzą na tzw. *świadków splątania* - obserwable których wartość średnia jest nieujemna na stanach separowalnych, ale ujemna w pewnych stanach splątanych. Do wykrycia wszystkich stanów wykrywanych przez Λ potrzebujemy całej orbity świadków pod działaniem grupy lokalnych operacji unitarnych.

Powyższe odwzorowanie jest odwracalne i nosi nazwę *izomorfizmu Jamiołkowskiego.*

Ćwiczenie 42 *Pokaż, że nierówność CHSH można zapisać jako wartość oczekiwaną pewnego świadka splątania.*

Ćwiczenie 43 *Znajdź świadków odpowiadających odwzorowaniom Choi i Choi dualne.*

Jeżeli odwzorowanie Φ wykrywa pewien stan ρ, to w ogólności świadek odpowiadający odwzorowaniu nie będzie wykrywał tego stanu. Świadka wykrywający stan znajdujemy w następujący sposób: jeżeli $(I \otimes \Phi)\rho \ngeq 0$, to macierz ta posiada ujemną wartość własną. Weźmy wektor ϕ z odpowiadającej jej podprzestrzeni własnej. Mamy: $\langle\phi|\,(I \otimes \Phi)\rho\,|\phi\rangle = \langle P_\phi|(I \otimes \Phi)\rho\rangle_{HS} < 0$. Za świadka należy wziąć $W = I \otimes \Phi^{\#} P_\phi$, gdzie $\Phi^{\#}$ oznacza sprzężenie w przestrzeni operatorów.

Świadek jest obserwablą w przestrzeni układu złożonego z dwóch odseparowanych przestrzennie podukładów. Żeby go zmierzyć, należo rozłożyć go na sumę iloczynów tensorowych obserwabli lokalnych. Pomiar świadka odbywa się tak jak pomiar nierówności CHSH (która jest szczególnym przypadkiem świadka splątania).

Ćwiczenie 44 *Dla świadka odpowiadającego odwzorowaniu Choi, znajdź rozkład na sumę iloczynów tensorowych obserwabli lokalnych.*

Zbiór stanów w wyższych wymiarach i kula Gurvitsa

Zbiór stanów qubitu jest kulą o promieniu $1/\sqrt{2}$ wokół stanu maksymalnie mieszanego. Kula opisana na zbiorze stanów ma promień $\sqrt{(d-1)/d}$, a kula wpisana ma promień $1/\sqrt{d(d-1)}$. W wymiarze 2 kule te się pokrywają i zbiór stanów jest kulą. W wyższych wymiarach jego brzeg przebiega pomiędzy sferami. Można udowodnić, że kula wpisana w zbiór stanów zawiera tylko stany separowalne. Kula ta nazywa się *kulą Gurvitsa.* Każda kula o większym promieniu wokół stanu maksymalnie splątanego będzie zawierać już stany splątane.