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, 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.

Rachunek prawdopodobieństwa, kanały informacyjne i pomiary

W rachunku prawdopodobieństwa podstawową rolę odgrywa trójka: $(X, \mathcal{F}, \mu)$ - przestrzeń probabilistyczna, σ-algebra jej podzbiorów i miara - funkcja przeliczalnie addytywna na rozłącznych podzbiorach t.że $\mu(X) = 1$ (unormowana). Funkcja mierzalna pomiędzy przestrzeniami probabilistycznymi $f : (X, \mathcal{F}_X) \to (Y, \mathcal{F}_Y)$ to funkcja dla której $\forall A \in \mathbb{F}_Y \ f^{-1}(A) \in \mathcal{F}_X$. Dalej będziemy skupiać się na przypadku $\#X = n < \infty$ i $\mathcal{F} = 2^X$.

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.

Każda funkcja $f : X \to \mathbb{R}$ jest teraz mierzalna i można ją przedstawić jako kowektor $\langle f|$ jej wartości.

Wartość oczekiwaną obliczamy jako $\mathbb{E}_p(f) = \langle f|p\rangle$. 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: $p_1 = \sum_j p_{ij}, p_2 = \sum_i p_{ij}$.

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.

Pomiar projektywny obserwabli 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. Prawdopodobieństwo otrzymania i-tego wyniku wynosi $p_i = \langle \mathbb{1}|\chi_{A_i}|p\rangle$. Stanem po pomiarze jest $\chi_{A_i}p\rangle / \langle \mathbb{1}|\chi_{A_i}|p\rangle$.

Pomiar uogólniony obserwabli f to odwzorowanie wyników pomiaru w zbiór funkcji nieujemnych $\{\langle m_i|\}$, mierzalnych względem $\sigma(f)$, sumujących się do $\langle \mathbb{1}|$ (wiersze 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 $\langle m_i| = \langle \mathbb{1}|K_i$.

Macierzowa reprezentacja rachunku prawdopodobieństwa

Zamieńmy teraz wektory prawdopodobieństwa $\vec{p}$ na macierze diagonalne i podobnie wektory reprezentujące funkcje mierzalne. Mamy wtedy

$$\mathbb{E}_p(f) = p \cdot f = \mathrm{Tr}\left(\begin{bmatrix} p_1 & & \\ & \ddots & \\ & & p_n \end{bmatrix}\begin{bmatrix} f_1 & & \\ & \ddots & \\ & & f_n \end{bmatrix}\right) \tag{1}$$

Stanem układu złożonego jest wektor z $\mathbb{R}_+^{n_1 \times n_2} = \mathbb{R}_+^{n_1} \otimes \mathbb{R}_+^{n_2}$. W zapisie macierzowym, będzie to macierz diagonalna z $\mathcal{B}(\mathbb{R}^{n_1 \times n_2}) = \mathcal{B}(\mathbb{R}_+^{n_1}) \otimes \mathcal{B}(\mathbb{R}_+^{n_2})$. Dwa podukłady są niezależne (nieskorelowane), gdy stan układu jest iloczynem tensorowym stanów podukładów.

Rozkłady brzegowe uzyskujemy biorąc ślady częściowe:

$$[\rho_A]_{ij} = \sum_k \rho_{ik,jk} \qquad \text{macierz śladów bloków} \tag{2}$$

$$[\rho_B]_{ij} = \sum_k \rho_{ki,kj} \qquad \text{suma bloków diagonalnych.} \tag{3}$$

Ślady częściowe macierzy diagonalnych są diagonalne i odtwarzamy klasyczne wzory na rozkłady brzegowe.

Działanie kanału informacyjnego $A\vec{p}$ w nowej reprezentacji wyraża wzór:

$$\begin{bmatrix} \sqrt{a_{11}} & & & \\ & \sqrt{a_{22}} & & \\ & & \ddots & \\ & & & \sqrt{a_{nn}} \end{bmatrix}\begin{bmatrix} p_1 & & & \\ & p_2 & & \\ & & \ddots & \\ & & & p_n \end{bmatrix}\begin{bmatrix} \sqrt{a_{11}} & & & \\ & \sqrt{a_{22}} & & \\ & & \vdots & \\ & & & \sqrt{a_{nn}} \end{bmatrix}^\dagger$$
$$+ \begin{bmatrix} & \sqrt{a_{12}} & & \\ & & \sqrt{a_{23}} & \\ & & & \ddots \\ \sqrt{a_{n1}} & & & \end{bmatrix}\begin{bmatrix} p_1 & & & \\ & p_2 & & \\ & & \ddots & \\ & & & p_n \end{bmatrix}\begin{bmatrix} & \sqrt{a_{12}} & & \\ & & \sqrt{a_{23}} & \\ & & & \ddots \\ \sqrt{a_{n1}} & & & \end{bmatrix}^\dagger$$
$$+ \cdots + \begin{bmatrix} & & & \sqrt{a_{1n}} \\ \sqrt{a_{21}} & & & \\ & \sqrt{a_{32}} & & \\ & & \ddots & \end{bmatrix}\begin{bmatrix} p_1 & & & \\ & p_2 & & \\ & & \ddots & \\ & & & p_n \end{bmatrix}\begin{bmatrix} & & & \sqrt{a_{1n}} \\ \sqrt{a_{21}} & & & \\ & \sqrt{a_{32}} & & \\ & & \ddots & \end{bmatrix}^\dagger$$
$$= \sum_i A_i p A_i^\dagger$$

Ćwiczenie 1 *Pokaż, że warunek stochastyczności macierzy A tłumaczy się jako $\sum_i A_i^\dagger A_i = I$*

Pomiar projektywny (PVM - *projective valued measure*) obserwabli F jest dany przez rozbicie przestrzeni probabilistycznej na rozłączne podzbiory, mierzalne względem σ_F (nie mogą rozróżniać punktów dla których F ma tę samą wartość). W zapisie macierzowym będzie to zbiór projektorów sumujących się do I. Podprzestrzenie, na które rzutują projektory muszą być sumami podprzestrzeni niezmienniczych F (przeformułowanie warunku σ_F mierzalności). Prawdopodobieństwo otrzymania i-tego wyniku wynosi $\mathrm{Tr}(\rho P_i)$, a stan po pomiarze: $P_i \rho P_i / \mathrm{Tr}(\rho P_i)$.

Pomiar uogólniony (POVM - *positive operator valued measure*) jest dany przez zbiór $\{\Lambda_i\}$ podkanałów sumujących się do kanału. Prawdopodobieństwo otrzymania i-tego wyniku wynosi $\mathrm{Tr}(\Lambda_i(\rho))$. Stanem po pomiarze jest: $\Lambda_i(\rho)/\mathrm{Tr}(\Lambda_i(\rho))$.

Ćwiczenie 2 *Udowodnij własność cykliczności śladu*

Jeżeli interesuje nas tylko prawdopodobieństwo wyniku, to wykorzystując własności cykliczności i liniowości śladu mamy:

$$\mathrm{Tr}(\Lambda_i(\rho)) = \mathrm{Tr}(\sum_j A_j^{(i)} \rho A_j^{(i)\dagger}) = \sum_j \mathrm{Tr}(A_j^{(i)} \rho A_j^{(i)\dagger}) = \sum_j \mathrm{Tr}(A_j^{(i)\dagger} A_j^{(i)} \rho) = \mathrm{Tr}(\sum_j A_j^{(i)\dagger} A_j^{(i)} \rho) = \mathrm{Tr}(M_i \rho),$$

gdzie M_i są operatorami dodatnimi sumującymi się do I.

Kwantowy rachunek prawdopodobieństwa

Uogólnienie rachunku prawdopodobieństwa do przypadku kwantowego uzyskujemy uwalniając bazy macierzy do tej pory diagonalnych. Stanami są macierze półdodatniokreślone o śladzie równym 1, obserwablami dowolne macierze hermitowskie. Stany czyste to projektory rzędu 1.

Kanały kwantowe to odwzorowania postaci $\rho \mapsto \sum_i A_i \rho A_i^\dagger$, gdzie $A_i^\dagger A_i = I$.

Postulaty Mechaniki Kwantowej

Tak jak z każdym układem klasycznym wiążemy pewną przestrzeń fazową X, tak z każdym układem kwantowym wiążemy pewną zespoloną przestrzeń Hilberta $\mathcal{H}$. Mechanika kwantowa jest niekomutatywnym uogólnieniem klasycznej mechaniki statystycznej i jako taka jest teorią liniową

	Postulat mechaniki kwantowej	Odpowiednik klasyczny
Algebra obserwabli i przestrzeń stanów		
1.1 algebra obserwabli	$\mathcal{B}(\mathcal{H})$	$L_\infty(X)$
1.2 przestrzeń stanów	$\mathcal{B}_T(\mathcal{H})$	$L_\infty(X)^*$
1.3 stany czyste	$\rho = \lvert\psi\rangle\langle\psi\rvert$	$\rho = \delta(x, x_0)$
1.4 przestrzeń stanów układu złożonego	$\mathcal{B}(\mathcal{H}_1) \otimes \mathcal{B}(\mathcal{H}_2) \cong \mathcal{B}(\mathcal{H}_1 \otimes \mathcal{H}_2)$	$L_\infty(X_1)^* \otimes L_\infty(X_2)^* \cong L_\infty(X_1 \times X_2)^*$
1.5 stany podukładów	$\rho_1 = \mathrm{Tr}_2\rho$	$\rho_1 = \int_{X_2} d\rho$
Pomiar projektywny (idealny) obserwabli A		
2.1 instrument pomiarowy	odwzorowanie zbioru wyników w w rozkład I na skończoną sumę ortogonalnych projektorów $a_i \to P_i$ P_i "zachowuje podprzestrzenie własne"	odwzorowanie zbioru wyników w w skończone rozbicie X na rozłączne podzbiory $a_i \to A_i$ każda poziomica leży w dokładnie jednym A_i
2.2 prawdopodobieństwo otrzymania wyniku a_i	$\mathrm{Tr}(\rho P_i)$	$\rho(A_i)$
2.3 stan po pomiarze z wynikiem a_i	$P_i\rho P_i/\mathrm{Tr}\rho P_i$	$\rho\lvert_{A_i}/\rho(A_i)$
Dynamika układu zamkniętego (zachowująca stany czyste)		
3.1 generator ewolucji	dowolna obserwabla H	dowolna obserwabla H
3.2 równanie ewolucji	$i\hbar\partial_t\rho = [H, \rho]$	$\partial_t\rho = \{H, \rho\}$
3.3 grupa dynamiczna	przekształcenia unitarne	symplektomorfizmy

Zauważmy, że ewolucja przeprowadza stany czyste w stany czyste. Jeżeli zapiszemy $\rho(t) = \lvert\psi(t)\rangle\langle\psi(t)\rvert$, to wektor $\psi(t)$ (zwany wektorem stanu) podlega równaniu:

$$i\hbar\partial_t\psi = H\psi$$

znanemu jako równanie Schrödingera. Klasycznie: równanie Hamiltona.

Ćwiczenie 3 *Udowodnij, że dla macierzy hermitowskiej H macierz* $\exp\left(-\frac{i}{\hbar}Ht\right)$ *jest unitarna.*

Kula Blocha

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

$$\rho = \frac{1}{2} \begin{bmatrix} 1+z & x-iy \\ x+iy & 1-z \end{bmatrix}. \tag{4}$$

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:

$$S^3 \xrightarrow{S^1} S^2 \tag{5}$$

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

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

$$\langle A|B\rangle_{HS} = \mathrm{Tr} A^\dagger B \tag{6}$$

Ćwiczenie 5 *Pokaż, że iloczyn HS jest niezmienniczy na działanie grupy unitarnej.*

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

Ćwiczenie 6 *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 7 *Pokaż, że para projektorów na ortogonalne podprzestrzenie odpowiada parze antypodycznych punktów na sferze Blocha.*

Ćwiczenie 8 *Jaka jest topologia zbioru wszystkich rozkładów $\mathbb{C}^2$ na sumę prostą dwóch ortogonalnych podprzestrzeni?*

Ćwiczenie 9 *Ogólniej, pokaż, że kąt pomiędzy wektorami na sferze Blocha jest równy dwukrotności kąta pomiędzy wektorami w p. Hilberta (co to znaczy kąt w przestrzeniach nad $\mathbb{C}$?)*

Rozkład spektralny macierzy hermitowskiej polega na znalezieniu jej rozkładu na kombinację liniową projektorów na ortogonalne podprzestrzenie. W przypadku macierzy półdodatnio określonej 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 10 *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* $A \cdot A^\dagger = I$*.*

Jeżeli H jest macierzą diagonalną, rozwiązaniem równania Schrödingera

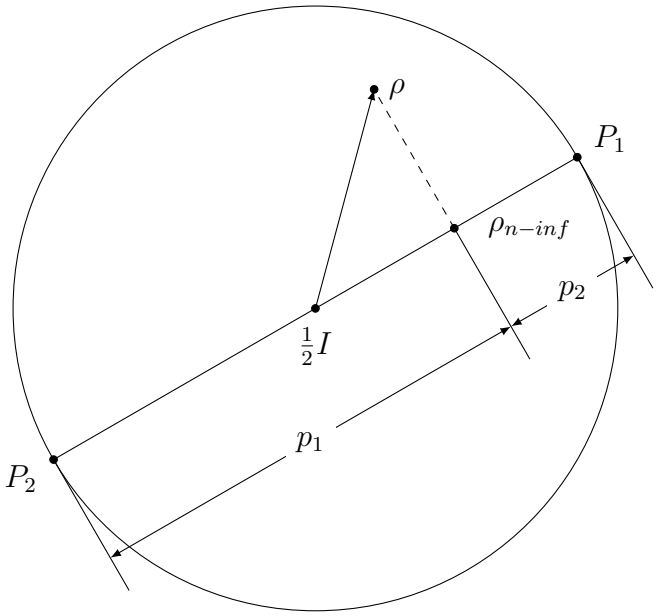
$$i\hbar\partial_t\Psi = H\Psi \tag{7}$$

jest

$$\Psi(t) = \exp(-\frac{i}{\hbar}Ht)\Psi(0) = \begin{bmatrix} \exp(-\frac{i}{\hbar}E_0t)\Psi_0(0) \\ \exp(-\frac{i}{\hbar}E_1t)\Psi_1(0) \end{bmatrix}. \tag{8}$$

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.

Pomiar nieinformujący obserwabli o projektorach Q_1, Q_2 w rozkładzie spektralnym odpowiada rzutowi stanu na średnicę napinaną przez Q_1 i Q_2. Jeżeli pomiar jest informujący, następuje kolaps do Q_1 albo Q_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 jej stan własny. Dla każdej innej obserwabli, która z nią nie komutuje, nie będzie to stan własny i nieoznaczoność nie będzie wynosiła 0.

Ćwiczenie 11 *W jakim stanie qubitu suma nieoznaczoności (wariancji) dwóch obserwabli będzie minimalna? Pokaż, że bez starty ogólności obserwable mogą być postaci*

$$A_1 = k_1 \begin{bmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{bmatrix}, \quad A_2 = k_2 \begin{bmatrix} \cos\beta & -\sin\beta \\ -\sin\beta & -\cos\beta \end{bmatrix}$$

Następnie znajdź sumę nieoznaczoności i pokaż, że osiąga ona minimum dla stanu

$$\rho_{min} = \frac{1}{2} \begin{bmatrix} 1+\cos\alpha & \sin\alpha \\ \sin\alpha & 1-\cos\alpha \end{bmatrix},$$

gdzie $\operatorname{tg} 2\alpha = \frac{k_1^2-k_2^2}{k_1^2+k_2^2} \operatorname{tg} 2\beta$. *Pokaż, że minimalna wartość sumy wariancji obserwabli wynosi*

$$\frac{1}{2}\left(k_1^2 + k_2^2 - \sqrt{(k_1^2+k_2^2)^2 - 4k_1^2k_2^2\sin^2(2\beta)}\right)$$

Wynik poprzedniego zadania chcielibyśmy wyrazić poprzez wielkości niezależne od przedstawienia macierzy. W tym celu:

Ćwiczenie 12 *Pokaż, że:*

$$\begin{aligned} k_1^2 &= \frac{1}{2}\mathrm{Tr}\widetilde{A}_1^2 \\ k_2^2 &= \frac{1}{2}\mathrm{Tr}\widetilde{A}_2^2 \\ 4k_1^2k_2^2\sin(2\beta) &= -\frac{1}{2}\mathrm{Tr}[\widetilde{A}_1, \widetilde{A}_2]^2 = -\frac{1}{2}\mathrm{Tr}[A_1, A_2]^2 \end{aligned}$$

gdzie $\widetilde{A}_i = A_i - \frac{1}{2}I\mathrm{Tr}A_i$.

Dostajemy ostatecznie, że:

$$\begin{aligned} \min_\rho \left(\sigma_\rho^2(A_1) + \sigma_\rho^2(A_2)\right) = \frac{1}{2}\Big(&\mathrm{Tr}A_1^2 - \frac{1}{2}(\mathrm{Tr}A_1)^2 + \mathrm{Tr}A_2^2 - \frac{1}{2}(\mathrm{Tr}A_2)^2\Big) \\ &\left(1 - \sqrt{1 - \frac{-\mathrm{Tr}[A_1,A_2]^2}{\mathrm{Tr}A_1^2 - \frac{1}{2}(\mathrm{Tr}A_1)^2 + \mathrm{Tr}A_2^2 - \frac{1}{2}(\mathrm{Tr}A_2)^2}}\right) \end{aligned}$$

Wielkość (dodatnia) $-\mathrm{Tr}[A_1, A_2]^2/(\mathrm{Tr}A_1^2 - \frac{1}{2}(\mathrm{Tr}A_1)^2 + \mathrm{Tr}A_2^2 - \frac{1}{2}(\mathrm{Tr}A_2)^2)$ jest unormowaną miarą niekomutowania macierzy. Dla obserwabli komutujących minimalna suma nieoznaczoności jest 0.

W teorio-informacyjnym podejściu nieoznaczoność pomiaru dla pary obserwabli A,B wyrażamy jako sumę entropii rozkładów wyników pomiarów obu obserwabli w danym stanie. Jest ona ograniczona z dołu przez:

$$H(A) + H(B) \geqslant -\log \max_{j,k} |\langle a_j|b_k\rangle|^2, \tag{9}$$

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.

Kanały kwantowe

Odwzorowania, które przeprowadzają na siebie macierze dodatnie w macierze dodatnie nazywane są odwzorowaniami dodatnimi (P). Poszukując ogólnej postaci odwzorowania przekształcającego stany w stany, powinniśmy postawić ostrzejszy warunek: Odwzorowanie $I \otimes \Lambda$ w oddziaływaniu na stan $\eta \otimes \rho$ powinno też być dodatnie dla wszystkich wymiarów dodatkowego podukładu. W ten sposób formułujemy warunek kompletnej dodatniości, który jest łatwiejszy do rozwiązania. Twierdzenie Choi mówi, że każde odwzorowanie kompletnie dodatnie jest postaci (postać Kraussa):

$$\rho \mapsto \sum_i A_i \rho A_i^\dagger \tag{10}$$

Postać tą spotkaliśmy już jako zapis kanału klasycznego dla stanów w reprezentacji macierzowej. Wtedy *fazy* (w rozkładzie polarnym) macierzy A_i różniły się od siebie cykliczną permutację. Uwolnienie baz da odwzorowanie kompletnie dodatnie, zachowujące ślad. Okazuje się, że jest to już najogólniejsza postać kanału kwantowego.

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:

$$\rho = \sum_{ij} \rho_{ij} |e_i\rangle \langle e_j| \xrightarrow{\text{stogowanie}} \vec{\rho} = \sum_{ij} \rho_{ij} |e_j\rangle \otimes |e_i\rangle \tag{11}$$

Obłożenie ρ przez A i B odpowiada następującemu odwzorowaniu wektora ρ:

$$A\rho B \longrightarrow B^T \otimes A \ \vec{\rho} \tag{12}$$

W tej reprezentacji działanie kanału zapisuje się jako

$$\vec{\rho} \mapsto \sum_i A_i^* \otimes A_i \vec{\rho} \tag{13}$$

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

Ćwiczenie 13 *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 $AXB = (B^T \otimes A)\vec{X}$).*

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 14 *Uzasadnij, że kanał kwantowo-klasyczny ma postać:*

$$\rho \mapsto \sum_j \mathrm{Tr}(\rho M_j) \left|j\right\rangle \left\langle j\right|, \quad dla \quad \sum_j M_j = I. \tag{14}$$

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

Kanał, który przekształca macierz diagonalną w macierz gęstości nazywamy kanałem klasyczno-kwantowym:

$$\rho \mapsto \sum_i \left\langle i\right| \rho \left|i\right\rangle \rho_i \tag{15}$$

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 sferę 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 15 *Jakie klasyczne kanały są odwracalne?*

Kolejną klasą kanałów, już nieodwracanych są kanały *random unitary*, gdy z pewnym prawdopodobieństwem zachodzi jeden lub drugi obrót unitarny

Ćwiczenie 16 *Znaleźć obraz kanału (bit flip channel):*

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

Ćwiczenie 17 *Jaka jest reprezentacja kanału który dokonuje skalowania macierzy Blocha w kierunkach x, y, pozostawiając niezmieniony kierunek z (phase flip channel)?*

Ćwiczenie 18 *Jaka jest reprezentacja kanału, który jednostajnie skaluje sferę Blocha (depolarising channel)?*

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

Kanał *amplitude damping* w sferze Blocha ilustruje izotropowe kurczenie się sfery 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 19 *Znajdź reprezentację Kraussa kanału amplitude damping. Znajdź przypadek ogólny opadania na stan Gibbsa.*

Ćwiczenie 20 *Jak można sparametryzować i scharakteryzować wszystkie kanały bitowe?*

Ćwiczenie 21 *Pokaż, że zbiór kanałów jednoqubitowych jest 12 wymiarowy. Czemu odpowiadają te wymiary? Ile wymiarów ma zbiór kanałów unitalnych?*

Układy złożone

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:

$$A = U\Lambda V^\dagger, \tag{16}$$

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

$$A = \sum_i \lambda_i \left|u_i\right\rangle \left\langle v_i\right|, \tag{17}$$

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 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 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.

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.

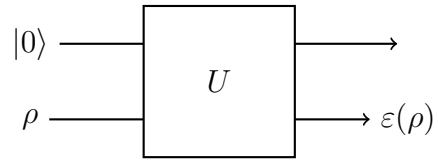
Ćwiczenie 22 *Jaką mamy swobodę wyboru stanów układu złożonego, odpowiadających danemu stanowi podukładu?*

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

Dowód: Weźmy $\eta = \left|e_1\right\rangle \left\langle e_1\right|$ 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 23 *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:

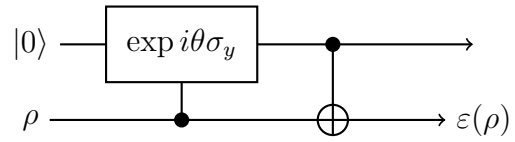


Dla tego samego U możemy zamienić podukłady rolami. Wtedy otrzymamy tzw. *kanał komplementarny* do ε.

Ćwiczenie 24 *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 (14), jeżeli interesuje nas tylko rozkład prawdopodobieństwa na wyjściu. Jeżeli natomiast interesuje nas również to, co dzieje się z układem po pomiarze, mamy:

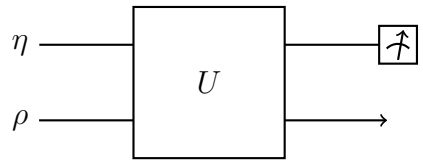
$$\rho \xrightarrow{p_i=\mathrm{Tr}\left(\rho\sum_j X_j^{(i)\dagger}X_j^{(i)}\right)} \frac{\sum_j X_j^{(i)}\rho X_j^{(i)\dagger}}{\mathrm{Tr}\left(\rho\sum_j X_j^{(i)\dagger}X_j^{(i)}\right)}, \quad \sum_{ij} X_j^{(i)\dagger}X_j^{(i)} = I \tag{18}$$

Jeżeli interesują nas tylko prawdopodobieństwa, przechodzimy do wzoru (14) 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

Rozróżnianie stanów kwantowych - teoria Helstroma 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 wektorom własnym.

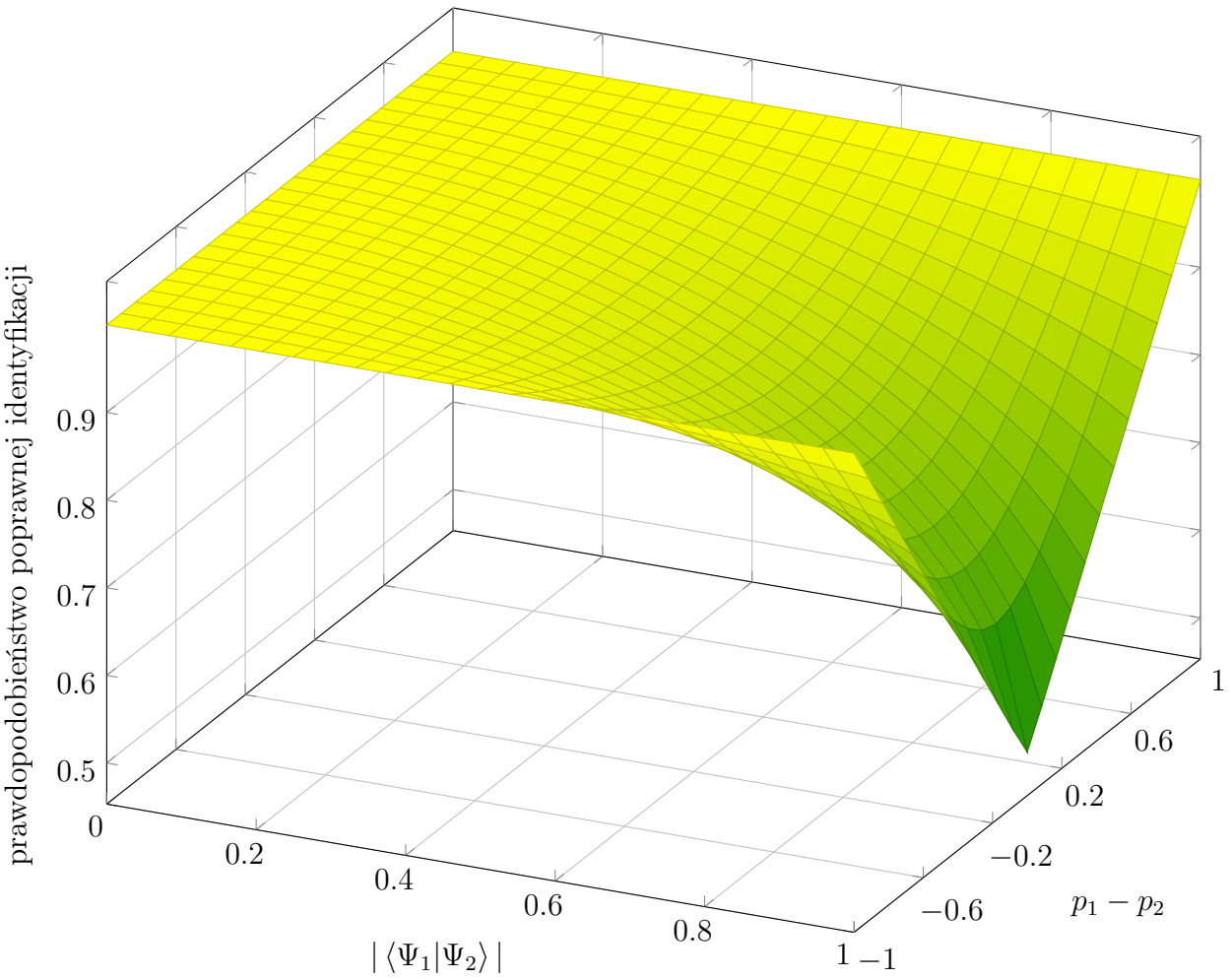
Jeżeli $p_1\rho_1 \geqslant p_2\rho_2$, to $A = I$ - optymalnie jest po prostu obstawiać 1 bez wykonywania żadnego pomiaru.

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

$$p_{sukces} = \frac{1}{2}\left(1 + ||p_1\rho_1 - p_2\rho_2||_1\right), \tag{19}$$

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

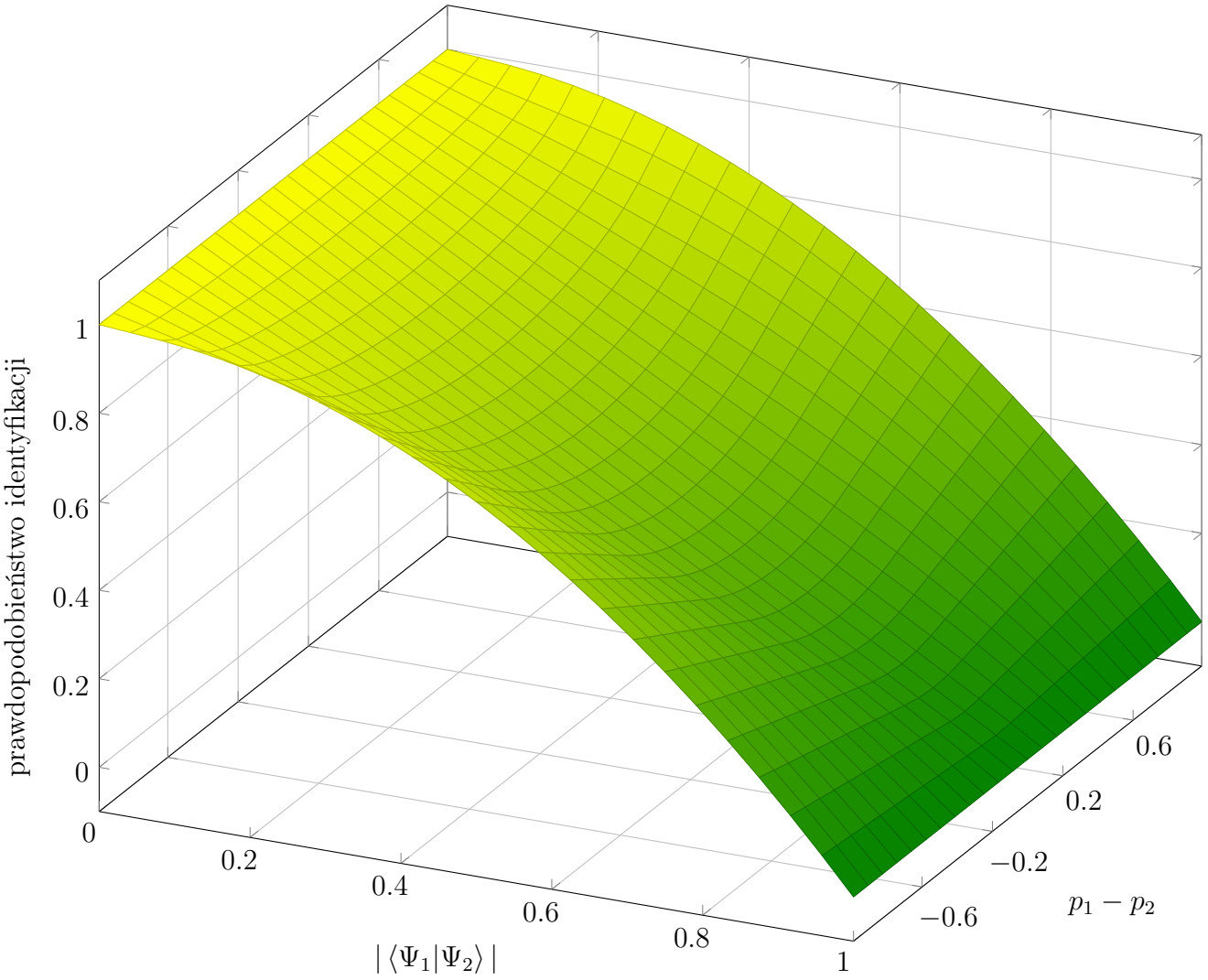
Ćwiczenie 25 *Wyprowadź wzór na prawdopodobieństwo sukcesu rozróżnienia dwóch stanów czystych wysyłanych z dowolnymi prawdopodobieństwami, zależne od* $p_1 - p_2$ *i* $|\langle\Psi_1|\Psi_2\rangle|^2$.



Ćwiczenie 26 *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.

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



Działania na polaryzacji fotonu

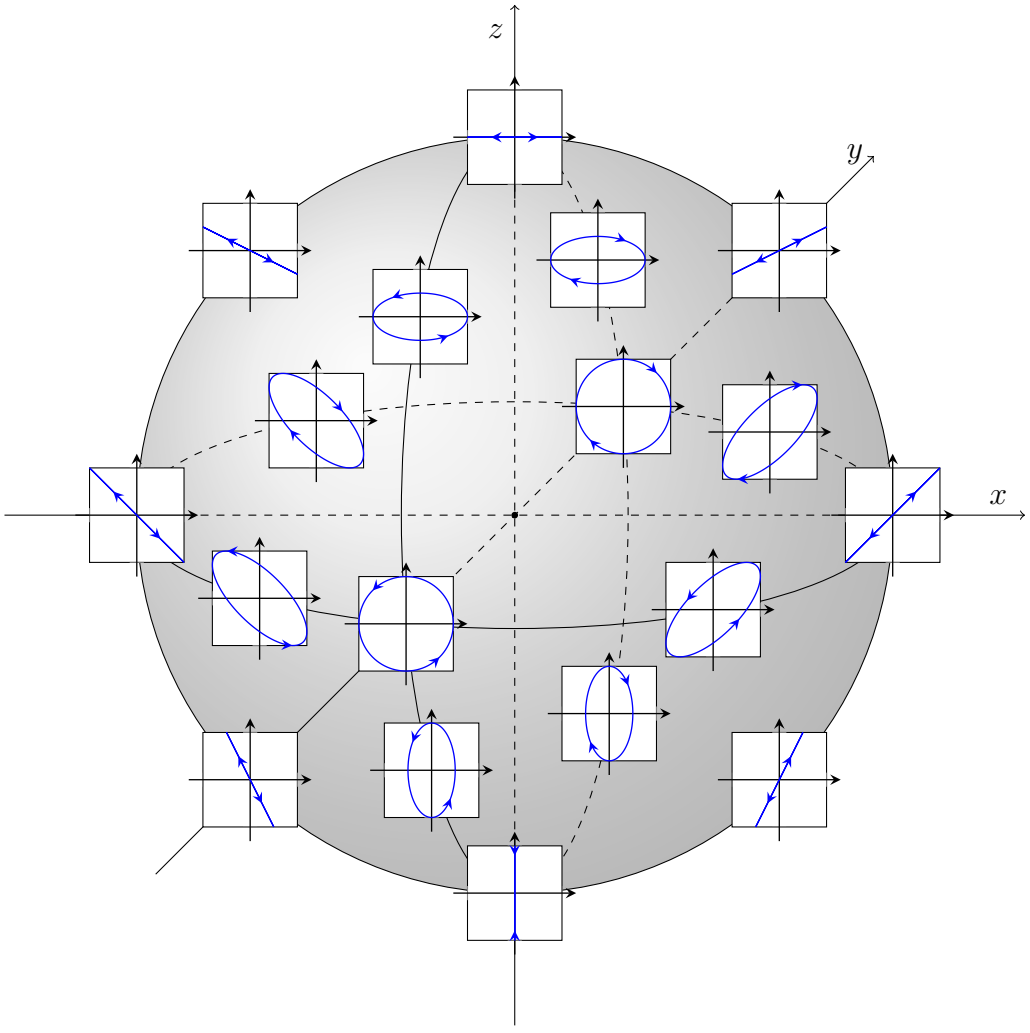
Fala elektromagnetyczna propagująca wzdłuż osi z może mieć 2 polaryzacje - poziomą i pionową, a także być kombinacją fal podstawowych:

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

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

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

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



Energia fotonu to kwadrat normy wektora pola elektrycznego w bazie polaryzacji. Z zasady zachowania energii wynika, że każdy element optyczny, który przekształca stan fotonu zachowując jego energię musi być macierzą unitarną w bazie polaryzacji. Podobnie operator działający na stanie dwufotonowym 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 $e^{i\alpha\sigma_y}$):

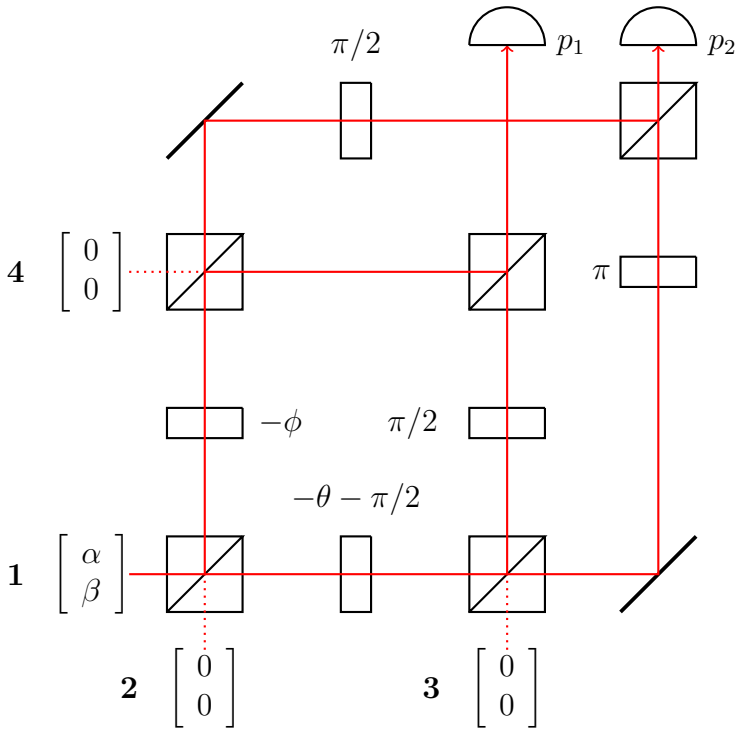
$$\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix} \tag{20}$$

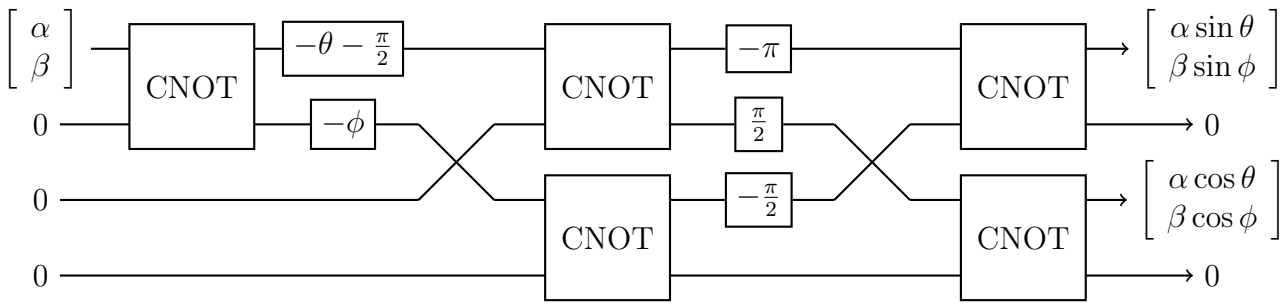
Polaryzujący dzielnik wiązki, przepuszcza polaryzację poziomą, a odbija polaryzację pionową. Macierz w bazie xh, xv, yh, yv

$$\begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \\ \cdot & 1 & \cdot & \cdot \end{bmatrix} \tag{21}$$

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 27 *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 28 *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

$$\begin{bmatrix} e^{i\delta/2} & 0 \\ 0 & e^{-i\delta/2} \end{bmatrix} \tag{22}$$

Ćwiczenie 29 *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 30 *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

$$-2 \leqslant \mathbb{E}(A_1B_1) + \mathbb{E}(A_1B_2) + \mathbb{E}(A_2B_1) - \mathbb{E}(A_2B_2) \leqslant 2 \tag{23}$$

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 (23). 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 31 *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:

$$\forall B \ \sum_b P(a, b|A, B) = P(a|A) \tag{24}$$

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 32 *Załóżmy, że*

$$p(ab|AB) = \left[\begin{array}{c|c|c|c} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & 0 \end{array}\right] \tag{25}$$

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?

Nierówność Bella jest wyprowadzana 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 ostatniego qubitu 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 33 *Pokaż, że stany z bazy magicznej dwóch qubitów można przekształcać na siebie za pomocą lokalnej transformacji unitarnej.*

Ćwiczenie 34 *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 35 *Jak teleportować stan qutritu za pomocą dwóch par splątanych qubitów?*

Ćwiczenie 36 *Niech nadawca i odbiorca dzielą parę w stanie czystym $\alpha|00\rangle + \beta|11\rangle$, 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: $(\gamma|00\rangle + \delta|11\rangle)/sqrt2$. Ile wynosi te prawdopodobieństwo? Wykonaj to samo dla pozostałych stanów po pomiarze. Jakie jest prawdopodobieństwo całkowite poprawnej teleportacji?*

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

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:

$$\rho^{\otimes N} \underset{Formation}{\overset{Distilation}{\rightleftarrows}} \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes M} \otimes ... \tag{26}$$

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 wyjściowego, 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 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:

$$\frac{1 + \sqrt{1 - C(\rho)^2}}{2}, \quad \frac{1 - \sqrt{1 - C(\rho)^2}}{2} \tag{27}$$

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

$$EOF = \frac{1 + \sqrt{1 - C(\rho)^2}}{2} \log_2 \frac{1 + \sqrt{1 - C(\rho)^2}}{2} + \frac{1 - \sqrt{1 - C(\rho)^2}}{2} \log_2 \frac{1 - \sqrt{1 - C(\rho)^2}}{2}. \tag{28}$$

Inną miarą splątania jest *negativity*: $\mathcal{N}(\rho) = \frac{1}{2}(||\rho^\Gamma||_1 - 1)$ (norma śladowa — suma wartości bezwzględnych wartości własnych macierzy, 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 transpose).

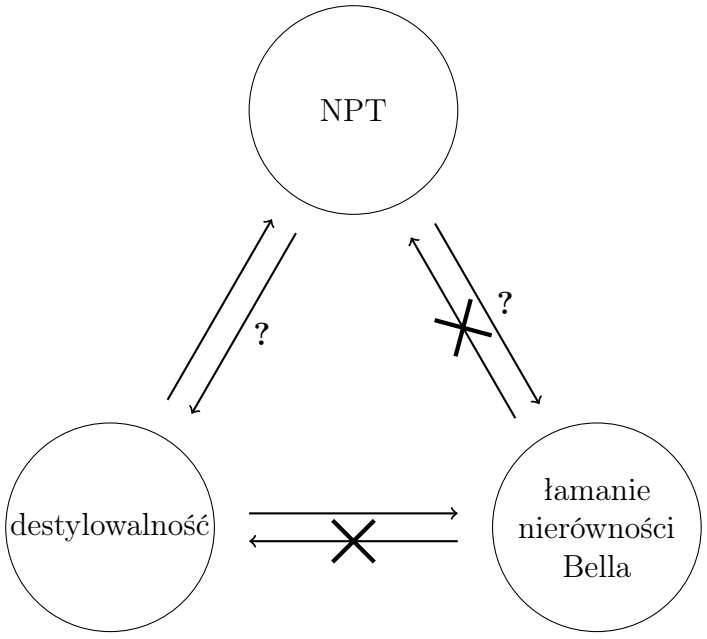
Ćwiczenie 37 *Pokaż, że kryterium częściowej transpozycji wykrywa wszystkie czyste stany splątane.*

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 38 *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 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:

$$\Phi : \mathcal{B}(\mathbb{C}^{d_1}) \to \mathcal{B}(\mathbb{C}^{d_1}). \qquad d_1 d_2 \leqslant 6 \Rightarrow \left(\Phi \in \mathcal{P} \iff \Phi(\rho) = \sum_i A_i \rho^T A_i^\dagger + \sum_i B_i \rho B_i^\dagger \right) \tag{29}$$

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

$$\begin{aligned} CH(|e_i\rangle \langle e_i|) &= |e_i\rangle \langle e_i| + |e_{i+1}\rangle \langle e_{i+1}| \\ CH(|e_i\rangle \langle e_j|) &= -|e_i\rangle \langle e_j|, \text{ dla } i \neq j \end{aligned} \tag{30}$$

Odwzorowanie to jest w stanie wykrywać stany splątane PPT.

Ćwiczenie 39 *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 40 *Dla dwuparametrowej rodziny operatorów o śladzie równym* 1*:*

$$\rho = \frac{1}{3(1+a+b)} \left[\begin{array}{ccc|ccc|ccc} 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & a & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & b & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot & \cdot \\ \hline \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & a & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & b & \cdot \\ 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 \end{array}\right] \tag{31}$$

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:

$$D = \begin{bmatrix} e^{i\phi_0} & \cdot & \cdot \\ \cdot & e^{i\phi_1} & \cdot \\ \cdot & \cdot & e^{i\phi_2} \end{bmatrix} \tag{32}$$

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

$$\Phi(\rho) = \int D \otimes D^* \rho (D \otimes D^*)^\dagger \mathrm{d}\phi_0 \mathrm{d}\phi_1 \mathrm{d}\phi_2 \tag{33}$$

Odwzorowanie takie zachowuje bez zmian wartości na diagonali i wyrazy pozadiagonalne w miejscach gdzie we wzorze (31) znajdują się 1, a pozostałe wartości zeruje (jest zatem projektorem). Co więcej, dla separowalnego ρ, $\Phi(\rho)$ będzie separowalne. Zauważmy, że stan (31) 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:

$$W = (I_{d_1} \otimes \Lambda) \left|\Psi\right\rangle \left\langle\Psi\right|, \tag{34}$$

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

Ćwiczenie 42 *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 $(I \otimes \Phi)\rho \not\geqslant 0$, 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 43 *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.

Algorytmy kwantowe

Klasyczny algorytm Shora

Rozważmy funkcję wykładniczą a^x z $\mathbb{Z}$ do ciała $\mathbb{Z}_N$. Rzędem elementu a nazywamy okres tej funkcji, czyli najmniejszą dodatnią liczbę r taką, że:

$$a^r \mod N = 1$$

Może zajść jedna z trzech możliwości:

- $2 \not| r$
- $2 | r \ \wedge \ a^{r/2} \mod N = -1$
- $2 | r \ \wedge \ a^{r/2} \mod N \neq -1$

Interesuje nas ostatni przypadek. Wprowadzamy oznaczenie $x = a^{r/2}$. Ponieważ $x^2 \mod N = 1$, zatem $x^2 - 1 = (x+1)(x-1) \mod N = 0$, oznacza to że iloczyn jest podzielny przez N. Żaden ze składników nie jest podzielny przez N - pierwszy ponieważ rzędem a jest r a nie $r/2$, drugi z założenia że zachodzi trzeci z powyższych przypadków. Zatem N jest liczbą złożoną, a jej rozkład znajdziemy licząc $NWD(x+1, N)$ (efektywny algorytm)

Sukces zależy od wyboru a. Okazuje się, że prawdopodobieństwo trafienia takiego a (trzecia możliwość alternatywy) wynosi $1 - 2^{-m} \geqslant 3/4$, gdzie m jest liczbą czynników pierwszych w rozkładzie. Prawdopodobieństwo nieznalezienia maleje wykładniczo z liczbą prób. Jest to algorytm probabilistyczny. Podsumowując, jego kroki przebiegają następująco:

1. Wybierz a losowo z przedziału $\{1, N-1\}$. Jeżeli $NWD(a, N) \neq 1$, mamy znaleziony czynnik rozkładu, w przeciwym wypadku idziemy dalej.
2. Wyznacz rząd a
3. Jeżeli r jest nieparzyste lub $a^{r/2} \mod N = -1$, wróć do punktu 2, w przeciwnym wypadku przejdź dalej
4. czynnikem rozkładu będzie $NWD(a^{r/2}, N)$.

Kwantowy algorytm Shora

Klasyczny algorytm Shora, mimo prostej implikacji i szybko malejącego prawdopodobieństwa niepowodzenia, nie ma praktycznego znaczenia. Trudność jest ukryta w czasochłonności wyznaczenia rzędu elementu. Ten krok algorytmu poprawiamy obliczając go przy pomocy komputera kwantowego.

Potrzebujemy rejestru kwantowego, w którym jesteśmy w stanie zapisać naszą liczbę N^2, czyli który ma długość K, gdzie $N^2 < Q = 2^K$. Przestrzeń Hilberta rejestru wyjściowego musi być przynajmniej N-wymiarowa (rejestr długości $\lceil \log_2 N \rceil$). Stanem dwóch rejestrów jest początkowo $|0\rangle \otimes |0\rangle$.

Na rejestrze wejściowym wykonujemy dyskretną transformatę Fouriera

$$U_F : |q\rangle \mapsto \frac{1}{\sqrt{Q}} \sum_{q'=0}^{Q-1} \exp(2\pi i q' q / Q) \, |q'\rangle \, . \tag{35}$$

Rejestr wejściowy zawiera teraz równą superpozycję wszystkich stanów bazowych, a rejestr wyjściowy jest niezmieniony: $\frac{1}{\sqrt{Q}}\sum_{q=0}^{Q-1}|q\rangle\otimes|0\rangle$. Teraz wykonujemy na rejestrach funkcję $|q\rangle\otimes|0\rangle\rightarrow|q\rangle\otimes|a^q \mod N\rangle$ i otrzymujemy w wyniku $\frac{1}{\sqrt{Q}}\sum_{q=0}^{Q-1}|q\rangle\otimes|a^q \mod N\rangle$.

Następnie wykonujemy transformatę Fouriera na rejestrze wejściowym:
$Q^{-1}\sum_{q=0}^{Q-1}\sum_{q'=0}^{Q-1}\exp(2\pi iqq'/Q)|q\rangle\otimes\left|a^{q'} \mod N\right\rangle$ i wykonujemy pomiar w bazie standartowej (obliczeniowej). Prawdopodobieństwo otrzymania wyniku q_0 wynosi:

$$p(q_0)=\frac{1}{Q^2}\sum_q\sum_{q'}\exp(2\pi iq_0q'/Q)\exp(-2\pi iq_0q/Q)\langle f(q)|f(q')\rangle \tag{36}$$

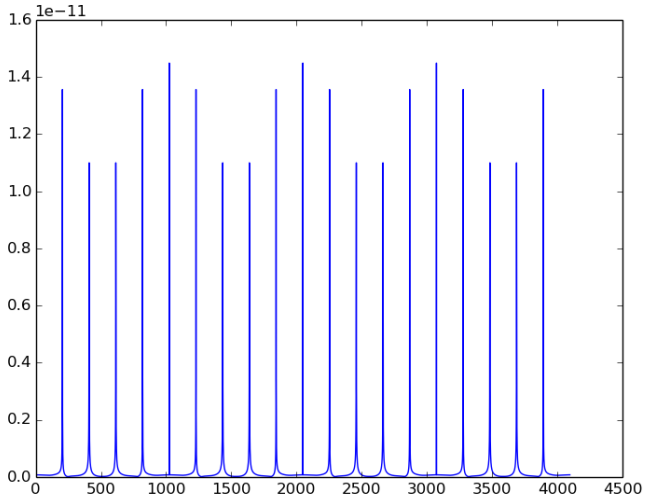
Iloczyn skalarny jest równy 1 gdy $q-q'$ jest wielokrotnością r i 0 w przeciwnym wypadku. Mamy zatem:

$$p(q_0)=\frac{1}{Q^2}\sum_{j=0}^{r-1}\sum_{\mu=0}^{\lfloor\frac{Q-1-j}{r}\rfloor}\sum_{\nu=0}^{\lfloor\frac{Q-1-j}{r}\rfloor}\exp(2\pi iq_0(\mu r+j)/Q)\exp(-2\pi iq_0(\nu r+j)/Q)$$

$$=\frac{1}{Q^2}\sum_{j=0}^{r-1}\left|\sum_{\mu=0}^{\lfloor\frac{Q-1-j}{r}\rfloor}\exp(2\pi iq_0\mu r/Q)\right|^2=$$

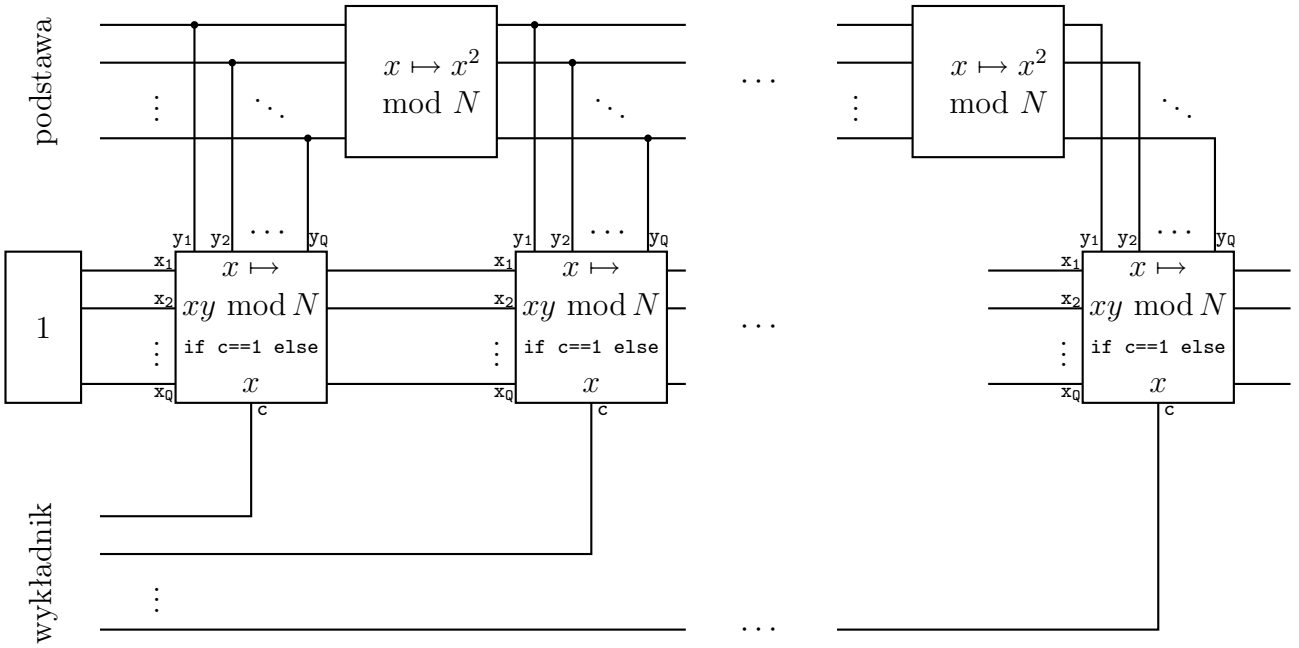
$$\frac{(Q \mod r)\sin^2\left(\pi q_0r\left(\lfloor\frac{Q-1}{r}\rfloor+1\right)/Q\right)+(r-Q \mod r)\sin^2\left(\pi q_0r\lfloor\frac{Q-1}{r}\rfloor/Q\right)}{Q^2\sin\left(\pi q_0r/Q\right)}$$

Funkcja ta ma pik gdy $q_0r/Q\in\mathbb{Z}$:



Pomiar pierwszego rejestru da (z dużym prawdopodobieństwem) pewną liczbę y, taką że y/Q jest bliskie wielokrotności $1/r$. Istnieje metoda ułamków łańcuchowych, która pozwala z wyniku jednego pomiaru odzyskać r.

Funkcja potęgowa Funkcję potęgową realizujemy poprzez algorytm szybkiego potęgowania:



Obwód składa się z dwóch typów bramek. Górne bramki realizują podnoszenie do kwadratu modulo N. Dolne bramki mnożą modulo N oba rejestry wejściowe (lewy i górny) jeżeli bit kontrolny (na dole) jest ustawiony na 1, w przeciwnym wypadku przepuszczają na wyjście wartość lewego rejestru. Zauważmy, że bramek jest $2Q-1$, czyli ilość operacji rośnie liniowo z rozmiarem wykładnika w bitach (logarytmicznie z jego wartością).

Transformata Fouriera Wykonanie transformaty Fouriera jest mnożeniem wektora wejściowego przez macierz o wyrazach $\exp(2\pi i \cdot kl/Q)/Q$. Zauważmy, że obliczając współrzędną y_k:

$$y_k = \frac{1}{Q}\sum_{l=0}^{Q-1} \exp(2\pi i \cdot kl/Q)\, x_l = \frac{1}{2}\frac{1}{Q/2}\sum_{k=0}^{Q/2-1} \exp(2\pi i \cdot kl/(Q/2))\, x_{2k} + \frac{1}{2}\frac{1}{Q/2}\exp(2\pi i \cdot k/Q)\sum_{k=0}^{Q/2-1} \exp(2\pi i \cdot kl/(Q/2))\, x_{2k+1} \tag{37}$$

wykonujemy jedno mnożenie i redukujemy problem do obliczenia dwóch tranformat Fouriera w wymiarze $Q/2$. (pamiętamy, że $Q = 2^K$, czyli powyższy krok będziemy mogli wykonać aż do momentu gdy $Q = 1$). W każdym kroku wykonujemy Q mnożeń, opierając się na wynikach transformat Fouriera połówek z poprzedniego kroku. Kroków jest $K = \log_2 Q$. Cała tranformata Fouriera wymaga wykonania $Q \log_2 Q$ mnożeń, a nie Q^2, jak w wypadku ogólnej macierzy.

Przepiszmy wzór (35) wykorzystując rozwnięcie binarne $k = \sum_l k_l 2^l$ liczby q':

$$\begin{aligned}
|j\rangle \mapsto & 2^{-K/2}\sum_{k_1=0}^{1}\cdots\sum_{k_K=0}^{1}\exp\left(\frac{2\pi i}{2^K} j\sum_{l=0}^{K-1} k_l 2^l\right)|k_{K-1}\ldots k_0\rangle \\
= & 2^{-K/2}\sum_{k_1=0}^{1}\cdots\sum_{k_K=0}^{1}\bigotimes_{l=0}^{K-1}\exp\left(2\pi i 2^{l-K} j k_l\right)|k_l\rangle \\
= & 2^{-K/2}\bigotimes_{l=0}^{K-1}\left(\sum_{k_l=0}^{1}\exp\left(2\pi i 2^{l-K} j k_l\right)|k_l\rangle\right) = 2^{-K/2}\bigotimes_{l=0}^{K-1}\left(|0\rangle + \exp\left(2\pi i 2^{l-K} j\right)|1\rangle\right)
\end{aligned} \tag{38}$$

Występująca w eksponencie liczba $2^{l-K}j$ jest liczbą wymierną, wykorzystując rozwinięcie binarne $j = \sum_{\nu=0}^{K-1} j_\nu 2^\nu$ liczby j możemy jej część ułamkową (tylko ona liczy się do fazy) zapisać jako $0.j_{K-l-1}\dots j_1$ i ostatecznie mamy:

$$|j\rangle \mapsto \frac{|0\rangle + \exp\left(2\pi i 0.j_{K-1}\dots j_0\right)|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + \exp\left(2\pi i 0.j_{K-2}\dots j_0\right)|1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{|0\rangle + \exp\left(2\pi i 0.j_0\right)|1\rangle}{\sqrt{2}} \tag{39}$$

Zdefiniujmy bramkę qbitową R_k jako

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i 2^{-k}} \end{bmatrix} \tag{40}$$

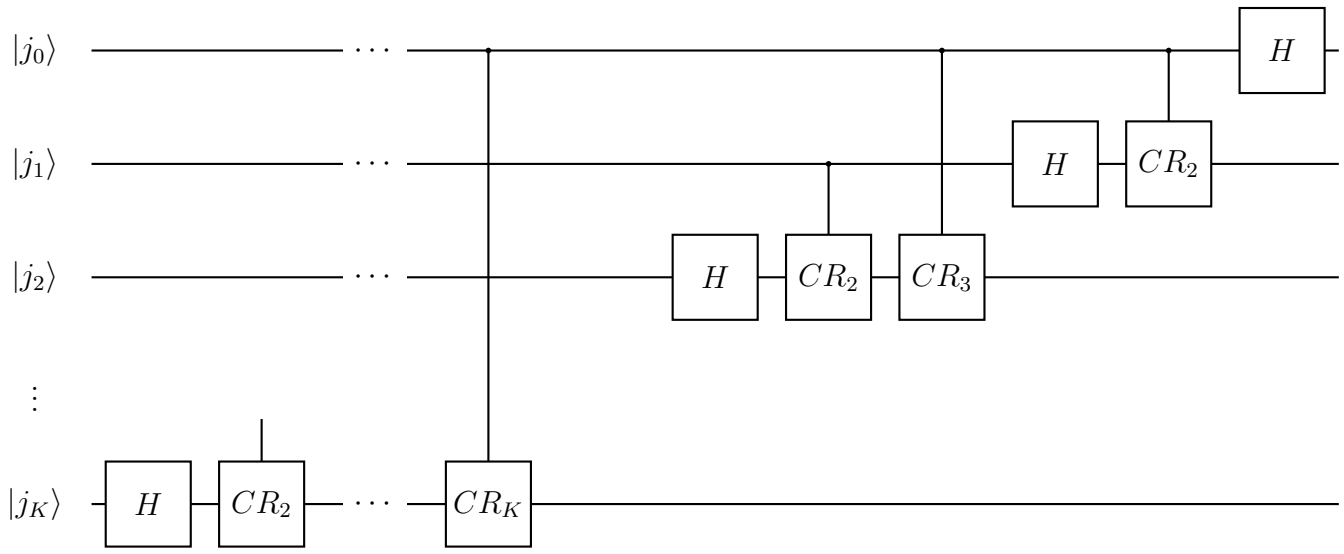
Możemy zdefiniować jej wersję CR_k - bramkę dwuqubitową:

$$CR_k = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{2\pi i 2^{-k}} \end{bmatrix} \tag{41}$$

Zauważmy, że wektor $(|0\rangle + \exp\left(\pi i j_{K-1}\right)|1\rangle)/\sqrt{2}$ powstaje poprzez działanie na wektor $|j_{K-1}\rangle$ bramką Hadamarda:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{42}$$

Przesunięcie o czynnik fazowy $\exp\left(2\pi i \cdot 0.j_{K-1}j_{K-2}\dots j_0\right)$ można zapisać jako działanie na wektor $(|0\rangle + \exp\left(\pi i j_{K-1}\right)|1\rangle)/\sqrt{2}$ ciągu bramek $CR_2 \cdot CR_3 \dots CR_K$ sterowanych bitami od $K-2$-ego do 0-wego.



Komputer NMR

Jedną z implementacji komputera komputera operującego na $\lesssim 10$ qubitach jest komputer NMR. Qubitami są spiny połówkowe jąder w cząsteczce. Operacje są wykonywane na makroskopowej próbce $\sim 10^{20}$ cząsteczek. Przez to pomiary które wykonujemy dają nam od razu wartość średnią obserwabli w stanie mieszanym. Pomiar ten nie niszczy stanu, a niekomutujące obserwable mogą być mierzone jednocześnie.

Próbka umieszczona jest w silnym stałym polu magnetycznym $\sim 10T$ wzdłuż osi z, które orientuje spiny jądrowe. Dla każdego jądra równanie $\hbar\gamma B_0 = \hbar\omega_0$ definiuje *częstość Larmora*, zależną od współczynnika gyromagnetycznego γ, który jest różny dla różnych jąder:

jądro	H	C	F	P	N
γ [MHz/T]	42.6	10.7	40.0	17.4	3.1

W cząsteczce częstości Larmora jąder mogą mieć dodatkowy wkład od przesunięć chemicznych - oddziaływania spinów jąder z momentem pędu elektronów (jeżeli dwa atomy przechodzą na siebie pod działaniem grupy symetrii cząsteczki, będą miały tę samą wartość przesumięcia chemicznego). Dla $B_0 \sim 10T$, energia drgań termicznych jest 4-5 rzędów wielkości większa od energii spinu w polu magnetycznym.

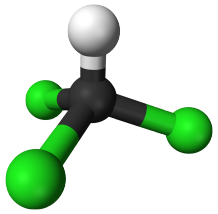
Do próbki przykładamy również w kierunku x zmienne pole magnetyczne i przy pomocy niego operujemy na stanach jąder. Druga cewka w tym samym kierunku służy do odczytu.

W cząsteczce za qubity możemy brać te jądra, które będziemy mogli oddzielnie adresować za pomocą impulsów pola magnetycznego, tzn. te które mają częstości rezonansowe oddzielone od innych cząsteczek (im bardziej, tym w krótszym czasie τ możemy wykonać operację). W ten sposób konstruujemy operacje jednoqubitowe. Operacjami wieloqubitowymi są operacje generowane przez Hamiltonian ewolucji swobodnej, który zależy od siły sprzężeń J pomiędzy jądrami. Czas ten musi być na tyle długi, by w czasie operacji jednoqubitowych efekty sprzęgania się jąder były pomijalne. Prowadzi to do warunku:

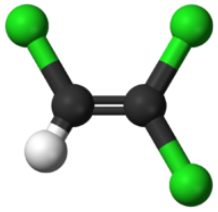
$$\delta\omega_0 \gg \frac{1}{\tau} \gg J/\hbar \tag{43}$$

Skala dekoherencji musi być większa niż $J/\hbar$. Daje to wskazówki które cząsteczki nadają się do obliczeń i ile atomów możemy wykorzystać. Cząsteczki wykorzystywane w obliczeniach to m.in:

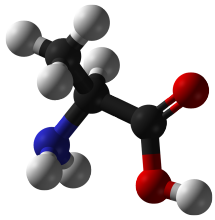
- 2 qubity: chloroform (qubity: H i C)



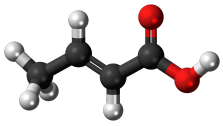
- 3 qubity: trichloroeten (qubity: H i C)



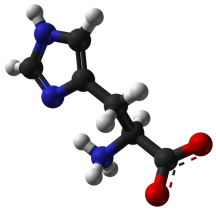
- 4 qubity: alanina (qubity: 1 × H i 3 × C)



- 7 qubitów: kwas krotonowy (qubity: 2 × H, 4 × C, 1 × H_3)



- 12 qubitów + qutrit: histydyna (qubity: 3 × H, 3 × N, 6 × C, dwa nierozróżnialne wodory tworzą singlet i qutrit)



(węgiel ^{12}C ma zerowy spin jądra, we wszystkich powyższych cząsteczkach trzeba mieć węgle ^{13}C).

Hamiltonian spinów jądrowych cząsteczki to

$$H = \frac{\hbar}{2}\sum_i \omega_i \sigma_z^{(i)} + \sum_{i<j} J_{ij} \sum_k \sigma_k^{(i)} \otimes \sigma_k^{(j)}, \tag{44}$$

gdzie $\sigma_k^{(i)}$ oznacza $\bigotimes_{i=1}^n I$ z I na k-tym miejscu zamienioną na σ_k.

W czasie trwania τ impulsu sterującego o częstości ω_{rf} adresowany jest jeden qubit, a w tym czasie sprzęganie jąder jest pomijalnie małe. Hamiltonian pojedyńczego spinu ma postać:

$$H(t) = -\hbar\omega_z \frac{1}{2}\sigma_z + \hbar\omega_x \cos(\omega_{rf}t - \phi)\frac{1}{2}\sigma_x \tag{45}$$

Przechodzimy do obrazu oddziaływania $\rho(t) \to \rho_R(t) = U_R^\dagger(t)\rho(t)U_R(t)$, gdzie $U_R(t) = \exp(i\omega_z t\frac{1}{2}\sigma_z)$:

$$H_R(t) = U_R^\dagger H U_R - i\hbar U_R^\dagger \dot{U}_R = \hbar/2 \begin{bmatrix} 0 & \omega_x e^{-i\omega_0 t}\cos(\phi - \omega_{rf}t) \\ \omega_x e^{i\omega_0 t}\cos(\phi - \omega_{rf}t) & 0 \end{bmatrix} \tag{46}$$

Jeżeli częstość sygnału sterującego jest równa częstości Larmora, to Hamiltonian w obrazie oddziaływania ma postać:

$$H_R = \frac{1}{2}\hbar\omega_x(\cos\phi\sigma_x + \sin\phi\sigma_y) \tag{47}$$

Człony oscylujące z częstością $2\omega_0$ pominęliśmy, ponieważ w czasie trwania impulsu uśrednią się do 0 (RWA).

Dla dwóch oddziałujących spinów Hamiltonian ma postać:

$$\begin{aligned} H = &-\hbar\omega_{z1}\frac{1}{2}\sigma_z \otimes I - \hbar\omega_{z2}\frac{1}{2}I \otimes \sigma_z + J_{12}\sum_k \sigma_k \otimes \sigma_k \\ &+B_{x,1}\cos(\omega_{rf1}t - \phi_1)(\gamma_1\frac{1}{2}\sigma_x \otimes I + \gamma_2 I \otimes \frac{1}{2}\sigma_x) \\ &+B_{x,2}\cos(\omega_{rf2}t - \phi_2)(\gamma_1\frac{1}{2}\sigma_x \otimes I + \gamma_2 I \otimes \frac{1}{2}\sigma_x) \end{aligned} \tag{48}$$

przechodzimy do obrazu oddziaływania transformacją $U_R = \exp(i\omega_{z1}t\frac{1}{2}\sigma_z)\otimes\exp(i\omega_{z2}t\frac{1}{2}\sigma_z)$. W rozważanej skali czasowej ($\Delta\omega_x\tau \gg 1$) składniki oscylujące z częstością $\Delta\omega_x$ uśredniają się i Hamiltonian przyjmuje postać:

$$\begin{aligned} H_R = &\frac{1}{4}J_{12}\sigma_z \otimes \sigma_z + \frac{1}{2}\omega_{x,1}(\cos\phi_1\sigma_x \otimes I + \sin\phi_1\sigma_y \otimes I) \\ &+\frac{1}{2}\omega_{x,2}(\cos\phi_2 I \otimes \sigma_x + \sin\phi_2 I \otimes \sigma_y), \end{aligned}$$

gdzie $\omega_{x,i} = \frac{1}{2}\gamma_i B_{x,i}$. Dla wielu spinów Hamiltonian w obrazie oddziaływania ma postać:

$$H_R = \frac{1}{4}\sum_{i<j} J_{ij}\sigma_z^{(i)} \otimes \sigma_z^{(j)} + \frac{1}{2}\sum_i \omega_{x,i}(\cos\phi_i\sigma_x^{(i)} + \sin\phi_i\sigma_y^{(i)}) \tag{49}$$

Bramki jednoqubitowe Mamy dwuparametrową rodzinę operacji SU(2):

$$e^{\frac{i}{2}\theta(\cos\phi\sigma_x + \sin\phi\sigma_y)} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}e^{-i\phi} \\ -i\sin\frac{\theta}{2}e^{i\phi} & \cos\frac{\theta}{2} \end{bmatrix} \tag{50}$$

Nie możemy w ten sposób zaimplementować obrotu wokół osi z, ale można go otrzymać składając powyższe operacje:

$$e^{-i\alpha\sigma_z/2} = e^{-i\frac{\pi}{4}\sigma_x}e^{-i\alpha\frac{1}{2}\sigma_y}e^{i\frac{\pi}{4}\sigma_x} \tag{51}$$

Dobierając fazy i czasy trwania sekwencji impulsów sterujących, możemy wykonać każdą operację SU(2) na każdym z qubitów oddzielnie.

Bramki dwuqubitowe Dowolną operację na wielu qubitach zrealizujemy przy pomocy bramek CNOT. Do zrealizowania bramki CNOT potrzebujemy w swobodnej ewolucji wyłączyć sprzężenia pomiędzy wszystkimi parami qubitów innymi niż jedna którą jesteśmy zainteresowani. Dokonujemy tego za pomocą techniki *refocusingu*. Załóżmy odtąd, że mamy jedno sprzężenie $\sigma_z \otimes \sigma_z$.

Ćwiczenie 44 *Pokaż, że:*

$$\exp\left(-i\frac{\pi}{4}\sigma_z \otimes I\right)\exp\left(i\frac{\pi}{4}I \otimes \sigma_z\right)\exp\left(-i\frac{\pi}{4}I \otimes \sigma_x\right)$$

$$\exp\left(-i\frac{\pi}{4}\sigma_z \otimes \sigma_z\right)\exp\left(-i\frac{\pi}{4}I \otimes \sigma_y\right) = \exp\left(-i\frac{\pi}{4}\right)\left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{array}\right] \sim CNOT$$

Ćwiczenie 45 *Pokaż, że:*

$$I \otimes \exp(-i\frac{\pi}{4}\sigma_x) \cdot \exp\left(-i\frac{\pi}{4}\sigma_z \otimes I\right) \exp\left(i\frac{\pi}{4} I \otimes \sigma_z\right) \exp\left(-i\frac{\pi}{2^{k+1}} I \otimes \sigma_x\right) \exp\left(-i\frac{\pi}{4}\sigma_z \otimes \sigma_z\right)$$
$$\exp\left(-i\frac{\pi}{2^{k+1}} I \otimes \sigma_y\right) I \otimes \exp(i\frac{\pi}{4}\sigma_x) = \exp\left(-i\frac{\pi}{4}\right) \left[\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & e^{i\pi/2^k} & 0 \\ 0 & 0 & 0 & e^{-i\pi/2^k} \end{array}\right] \sim CR_k$$

Efektywne stany czyste Jak wspomnieliśmy, nawet dla bardzo silnych pól i umiarkowanie niskich temperatur, stan termiczny spinu jądra jest bliski stanowi maksymalnie mieszanemu. Nie zwiększamy jego czystości, ale doprowadzamy go do postaci $(1-\epsilon)\rho_{max} + \epsilon|\Psi\rangle\langle\Psi|$. Stan maksymalnie mieszany jest niezmienniczy na wszystkie operacje i daje równy poziom tła przy pomiarze.

Tomografia kwantowa i teoria estymacji

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.

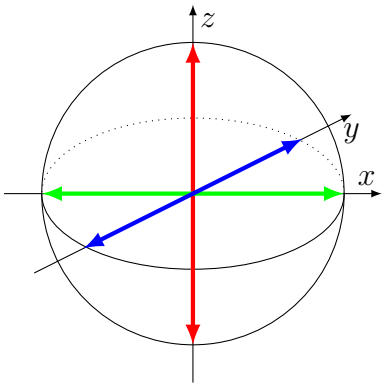
W $d=3$ konstrukcja ta przebiega następująco:

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

- 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 trkatować 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:



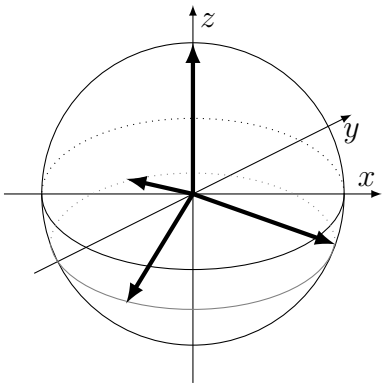
W $d = 2$, mierząc obserwable, których bazami własnymi są kolejne bazy ze zbioru MUB, otrzymujemy trzy wartości oczekiwane, które są równe współrzędnym x, y, i z w kuli Blocha mierzonego stanu.

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.

SIC POVMs

Istnienie 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, 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 46 *Wyznacz macierze powyższych projektorów*

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

Projektory takie sumują się do $2I_2$. skalując je przez czynnik $\frac{1}{2}$ ($\frac{1}{d}$ w przypadku ogólnym), dostaniemy POVM nazywany SIC POVM (*symmetric, informationaly 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:

$$\begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ p_3 \end{bmatrix} = \frac{1}{4}\mathbb{1} + \frac{1}{12}\begin{bmatrix} 0 & 0 & 3 \\ 2\sqrt{2} & 0 & -1 \\ -\sqrt{2} & \sqrt{6} & -1 \\ -\sqrt{2} & -\sqrt{6} & -1 \end{bmatrix}\begin{bmatrix} x \\ y \\ z \end{bmatrix} \tag{52}$$

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

Ćwiczenie 47 *Wyznacz wzory na x, y, z.*

Estymacja parametrów rozkładu

Wynikiem serii pomiaru długości n, o K możliwych rezultatach jest krotka K liczb, sumujących się do jedynki i oznaczających częstości otrzymywania kolejnych wyników. Są one estymatorami prawdziwych prawdopodobieństw - parametrów rozkładu. Chcielibyśmy wiedzieć, jak dokładnie te estymatory estymują parametry rozkładu.

Rozkład prawdopodobieństwa na sympleksie parametrów rozkładu, pod warunkiem że otrzymano daną serię pomiarową, w której liczności kolejnych wyników wynoszą n_i jest równy (z dokładnością do czynnika normującego wyrażonego przez funkcje Γ):

$$P(p_1, p_2, \ldots, p_K) \sim \prod_{i=1}^{K} p_i^{n_i} \tag{53}$$

Funkcja ta osiąga swoje maksimum, jak się spodziewamy, w punkcie $\vec{p}_{max} = \frac{1}{n}\vec{n}$, ale wartościami oczekiwanymi parametrów rozkładu są: $\mathbb{E}(p_i) = \frac{n_i+1}{n+K}$.

Elementami macierzy kowariancji są:

$$Var(p_i) = \frac{(n_i+1)(n+K-n_i-1)}{(n+K)^2(n+K+1)} \tag{54}$$

$$Cov(p_i, p_j) = -\frac{(n_i+1)(n_j+1)}{(n+K)^2(n+K+1)} \tag{55}$$

rozkład ten nazywa się *rozkładem Dirichleta*. Wykorzystując powyższe wzory możemy kontrolować macierz kowariancji parametrów stanu wyznaczonych w procesie tomografii.