

Przyczynowe więzy na strukturę korelacji w formalizmie kwantowym

Piotr Krasuń

21 marca 2017

Streszczenie

W pracy został zaprezentowany formalizm macierzy procesu, który opisuje regułę obliczania prawdopodobieństw otrzymania danych wyników w lokalnych laboratoriach przy wykorzystaniu potencjalnie nieprzyczynowych zasobów. Następnie przedstawiono zadanie komunikacyjne, w którym zasób o nieokreślonej przyczynowości może osiągać lepsze wyniki niż zasób klasyczny. Pokazano klasę procesów, która ilustruje fakt, że niewystarczająca jest nieseparowalność do złamania nierówności przyczynowych. Dalej zaprezentowano tak zwanego świadka przyczynowości (*causal witness*), który służy do stwierdzenia, czy dany zasób można rozłożyć na probabilistyczną kombinację zasobów o ściśle określonej przyczynowości. Za ich pomocą zostało pokazane w literaturze, że występowanie nieokreślonego porządku przyczynowego w naturze ma podstawy empiryczne. Zaprezentowano również miarę nieseparowalności. Następnie przedstawiono postulat, który ma wskazywać jakie procesy mogą być implementowalne fizycznie.

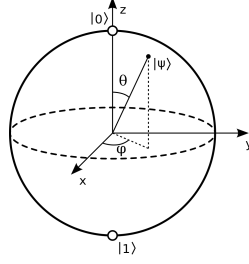
Abstract

In this work process matrix formalism is presented. It can be considered a way to calculate probabilities of obtaining certain results in local laboratories using possibly not causal resources. Next a communication task is shown. In this task a resource that is not causal can do better than a classic one. Following it a tool that can discriminate processes with indefinite causal order is described. A class of inseparable processes unable to violate any causal inequality was also illustrated. The so called causal witness was used to experimentally show that indefinite causal order is, in fact, a naturally occurring phenomena. An inseparability measure was also shown. Following it a purification postulate is characterized. It is a tool that is theorized to imply whether a following resource may be implemented physically.

1 Wstęp

1.1 Historia

Mechanika kwantowa od samego początku jej badania budziła wiele kontrowersji. Wielu badaczy miało trudności z zaakceptowaniem faktu, iż na fundamentalnym poziomie rzeczywistość nie jest deterministyczna, jak nam się wydawało. Zarówno losowa natura tej teorii, jak i wiele zadziwiających cech mechaniki kwantowej była początkowo źródłem wielu zaciekle dyskusji. Rok po opublikowaniu pracy Schrödingera, Einstein w swojej pracy zamieścił zdanie, które częściowo wyznaczało nurt badań w tamtym czasie, zaś dziś jest wraz z innymi popularnymi powiedzeniami kwantowymi zakorzenione w kulturze, a mianowicie, że "Bóg nie gra w kości". Ta teza później okazała się być nieprawdziwa - przynajmniej nie w takim stopniu, w jakim autor by sobie życzył. Sam formalizm doczekał się wielu interpretacji, często z wieloma elementami filozoficznymi. Dzisiaj najpopularniejszymi są interpretacja kopenhaska, teoria wielu światów, czy idea inkorporująca kwantową grawitację w mechanizm pomiaru. Ostatnia przytoczona pozycja wciąż oczekuje na sformułowanie, które jest zgodne z eksperymentami. Mimo tego pozostaje ideą ciekawą dla wielu badaczy. Mechanika kwantowa jest matematycznie bardzo elegancką teorią, którą można nazwać jednym z największych osiągnięć współczesnej fizyki. Wielokrotnie jej zaskakujące przewidywania zostały potwierdzone eksperymentalnie z niemal idealną dokładnością (w przeciwieństwie do np. stałej kosmologicznej, której niedokładność przekracza wiele dziesiątek rzędów wielkości).



Rysunek 1: Sfera Blocha. Punkty na tej sferze opisują wszystkie możliwe stany z dokładnością do czynnika fazowego. $|\psi\rangle$.

1.2 Podstawowe informacje

Stany systemów w mechanice kwantowej opisuje się jako elementy przestrzeni Hilberta $\psi \in \mathcal{H}$, a tak zwane obserwabla - samosprężone¹ operatory $A \in \mathcal{L}(\mathcal{H})$, które opisują fizyczne wielkości obserwowalne, jakie można zmierzyć na danym systemie. W przypadku skończonego wymiarowego bądź policzalnego można powiedzieć, że $\mathcal{H}^A = \mathcal{C}^N$ i obserwabla są po prostu macierzami hermitowskimi odpowiedniego wymiaru. Przez znak równości skrótowo określono, że jest to przestrzeń wektorowa nad ciałem tych liczb z iloczynem skalarnym wynikającym z mnożenia macierzy. Dosyć standardowym i wygodnym jest wykorzystywanie tak zwanej notacji Diraca, a mianowicie przedstawianie $\psi = |\psi\rangle$ i $\psi^\dagger = \langle\psi|$. Przykładowo w elementy $\psi \in \mathcal{C}^3$:

$$\psi = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} := |\psi\rangle \quad \psi^\dagger = (a_1^* \ a_2^* \ a_3^*) := \langle\psi| \quad (1)$$

Szeroko stosowanym zapisem w celu opisanego wektorów bazowych tzw. bazy obliczeniowej (*computational basis*, CB), czyli wektorów posiadającym jedyny niezerowy element o wartości jeden na i -tej pozycji, jest $|i\rangle$. Przykładowo w \mathcal{C}^3

$$|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \quad (2)$$

Sposób iterowania często różni się między pozycjami w literaturze. Tutaj przyjęto iterowanie od zera. Wygodnie narzucić warunek normalizacji stanów, a mianowicie $\langle\psi||\psi\rangle := \langle\psi|\psi\rangle = 1$, wtedy wartość oczekiwaną obserwabli w danym stanie $|\psi\rangle$ oblicza się tak: $\langle A \rangle := \langle\psi|A|\psi\rangle$. Warto zauważyć, że skoro obserwabla opisywane są przez macierze hermitowskie, można skorzystać z twierdzenia spektralnego i zapisać $A = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$, gdzie λ_i opisuje i -tą wartość własną zaś $|\lambda_i\rangle$ to i -ty wektor własny, który dobrano tak, że $\langle\lambda_i|\lambda_j\rangle = \delta_{ij}$. Wektory $\{|\lambda_i\rangle\}$ tworzą ortonormalną bazę w \mathcal{H} . Jednym z postulatów mechaniki kwantowej jest tzw. postulat pomiaru von Neumanna. Mówi on, że wykonując pomiar obserwabli A na systemie w stanie $|\psi\rangle$ i otrzymując wartość λ_i odpowiadającą wektorowi własnemu $|\lambda_i\rangle$ powoduje się przejście w stan $|\lambda_i\rangle$. Można, zakładając brak zdegenerowania niezerowych wartości własnych, zapisać w następujący sposób opisujący warunkową ewolucję po pomiarze

$$|\psi\rangle \mapsto \frac{\Pi_i |\psi\rangle}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}}, \quad (3)$$

¹Operatorem sprzężonym do ograniczonego liniowego operatora $T : \mathcal{H}^A \mapsto \mathcal{H}^B$ jest taki operator $T^* : \mathcal{H}^B \mapsto \mathcal{H}^A$, który spełnia następujący warunek $\langle Tx, y \rangle = \langle x, T^*y \rangle$, gdzie przez $\langle \cdot, \cdot \rangle$ rozumie się iloczyn skalarny, zaś $x \in \mathcal{H}^A, y \in \mathcal{H}^B$. Operatorem samosprężonym jest taki operator, gdzie $T^* = T$. W przypadku macierzy kwadratowych i iloczynu skalarnego wynikającego z mnożenia macierzy jest to warunek, że $A^\dagger = A$, gdzie $A^\dagger = (A^*)^T$. Takie macierze nazywa się hermitowskimi.

gdzie Π_i jest projektorem² odpowiadającym $|\lambda_i\rangle\langle\lambda_i|$. Zapisując $|\psi\rangle = \sum_i^N a_i|\lambda_i\rangle$, $\sum_i^N |a_i|^2 = 1$, prawdopodobieństwo zaobserwowania wyniku λ_i jest równe $|a_i|^2$, lub równoważnie

$$\Pr(\lambda_i) = \langle\psi|\Pi_i|\psi\rangle, \quad (4)$$

co znane jest jako reguła Borna. Fakt, że obserwabla są opisywane przez macierze hermitowskie zapewnia, że $\sum_i^N |\lambda_i\rangle\langle\lambda_i| = \mathbb{1}$, co dalej implikuje, że $\sum_i^N \Pr(\lambda_i) = \sum_i^N \langle\psi|\Pi_i|\psi\rangle = \langle\psi|\sum_i^N \Pi_i|\psi\rangle = \langle\psi|\psi\rangle = 1$ Stan całego systemu składającego się z pewnej ilości systemów opisuje element z

$$\mathcal{H}^{AB\dots Z} = \mathcal{H}^A \otimes \mathcal{H}^B \otimes \dots \mathcal{H}^Z, \quad (5)$$

gdzie \otimes to iloczyn tensorowy. Wraz ze wzrostem podsystemów składających się na system liczba wektorów bazowych rośnie eksponencjalnie, co jest fundamentem tzw. "kwantowego przyspieszenia", które pozwala heurystycznie/przybliżenie rozwiązać na komputerach kwantowych niektóre klasyczne problemy z eksponencjalnym przyspieszeniem, np. faktoryzacja liczb [25], rozwiązywanie układów liniowych [11] czy odpowiednio sformułowane problemy uczenia maszynowego [23, 16]. Ważną rzeczą do zaobserwowania jest fakt, że istnieją takie systemy, których nie można zapisać jako iloczyn stanów w poszczególnych podsystemach. Klasycznym przykładem tego jest

$$\begin{aligned} \mathcal{H}^{AB} &= \mathcal{C}^2 \otimes \mathcal{C}^2 \\ |\psi\rangle &= |1\rangle_A \otimes |1\rangle_B + |0\rangle_A \otimes |0\rangle_B := |1\rangle|1\rangle + |0\rangle|0\rangle := |11\rangle + |00\rangle \\ a_0|0\rangle + a_1|1\rangle \otimes b_0|0\rangle + b_1|1\rangle &= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle \\ a_0b_1 &= 0 \implies a_0 = 0 \vee b_1 = 0 \\ a_1b_0 &= 0 \implies a_1 = 0 \vee b_0 = 0 \end{aligned}$$

Powyższe implikuje, że $a_0b_0 \neq 1 \vee a_1b_1 \neq 1$.

Takie systemy, których nie da się zapisać w postaci $|\psi\rangle = |\psi\rangle_A \otimes |\phi\rangle_B$, nazywa się splątanymi. Splątanie kwantowe jest zasobem, który znalazł zastosowanie w wielu nowatorskich aplikacjach, jak np. kryptografia kwantowa [10], certyfikowana losowość [22], teleportacja kwantowa [21] czy wcześniej przytoczone "kwantowe przyspieszenie". Często w rozważaniach ogranicza się do skończonych przestrzeni Hilberta o wybranych rozmiarach. Najmniejszą i niepodzielną jednostką informacji jest kubit ($\mathcal{H} = \mathcal{C}^2$), fizycznie reprezentujący np. cząstkę ze spinem- $\frac{1}{2}$ (elektron), lub polaryzację fotonu. W wielu dziedzinach informatyki kwantowej ogranicza się praktycznie wyłącznie do analizy systemów złożonych z kubitów ze względu na pewną prostotę i wygodę badania takich systemów. Ciekawą interpretacją kubitów prezentuje Sfera Blocha (rysunek 1). Punkty na tej sferze opisują wszystkie prawidłowe znormalizowane $|\psi\rangle \in \mathcal{C}^2$. Okazuje się jednak, że formalizm stanów jest niewystarczający do opisu zespołów statystycznych (system znajduje się w jakimś z stanów z pewnym prawdopodobieństwem) wynikających z braku pełnej wiedzy o systemie bądź sposobie jego przygotowania. Do opisu takich sytuacji używa się macierzy gęstości. Macierz gęstości odpowiadająca systemie w pewnym stanie $|\psi\rangle$ to $\rho = |\psi\rangle\langle\psi|$. W przypadku, gdy stan znajduje się w jakimś stanie $|\psi_i\rangle$ z prawdopodobieństwem p_i macierz gęstości to

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \quad (6)$$

²Przez projektor rozumie się taką macierz A , że $A^2 = A$. W przypadku obserwabli projektory z twierdzenia spektralnego sumują się do identyczności i spełniają własność $\Pi_i\Pi_j = 0$. Założenie, że wartości własne są niezdegenerowane, które skutkuje tym, że projektory są niezdegenerowane nie jest konieczne. Projektory nie muszą być jednowymiarowe, sumując n liniowo niezależnych projektorów jednowymiarowych otrzymuje się projektor n -wymiarowy, który spełnia poprzednie relacje względem pozostałych macierzy co łatwo sprawdzić. Wielowymiarowe projektory mogą odpowiadać pomiarowi, który przypisuje taki sam wynik wielu ortogonalnym stanom, czy pomiar, który jest wykonywana na pewnej części systemu złożonego.

Powyższa rozkład nie jest unikatowy, dana macierz gęstości reprezentuje wiele różnych zespołów statystycznych, które generują jednakowe prawdopodobieństwa. W celu narzucenia generowania prawidłowego prawdopodobieństwa reguła opisaną dalej narzuca się na macierz ρ następujące warunki

$$\rho \geq 0^3 \quad (7)$$

$$\text{Tr } \rho = 1 \quad (8)$$

Wielkości i działania, analogiczne do tych opisanych w stosunku do stanów, w przypadku macierzy gęstości wyglądają następująco:

$$\langle A \rangle = \text{Tr}(A\rho) \quad (9)$$

$$\text{Pr}(\lambda_i) = \text{Tr}(\Pi_i \rho) \quad (10)$$

$$\rho \mapsto \frac{\Pi_i \rho \Pi_i}{\text{Tr}(\Pi_i \rho)} \quad (11)$$

Prócz warunkowej ewolucji podczas pomiaru, systemy kwantowe podlegają również ewolucji czasowej. W obrazie Schrödingera ewoluują stany. Wygląda to następująco:

$$U(t)|\psi(0)\rangle = |\psi(t)\rangle \quad (12)$$

$$U(t)^\dagger |\psi(t)\rangle = |\psi(0)\rangle \quad (13)$$

W obrazie Heisenberga ewoluują zaś obserwable

$$A(t) = U^\dagger A(0) U, \quad (14)$$

gdzie $U(t)$ jest pewnym unitarnym operatorem ($U^\dagger U = U U^\dagger = \mathbb{1}$) działającym na \mathcal{H} . Pomiar rzutujący nie jest jedynym pomiarem, który można wykonać. Najogólniejszym pomiarem, który można wykonać w mechanice kwantowej jest *positive valued measurement* (POVM). Opisywany jest on przez zbiór takich operatorów $\{E_i\}$, że $E_i > 0$, $\sum_i E_i = \mathbb{1}$. Poprzednie reguły przechodzą w

$$\text{Pr}(x_i) = \langle \psi | E_i | \psi \rangle \quad (15)$$

$$\text{Pr}(x_i) = \text{Tr}(E_i \rho) \quad (16)$$

$$E_i = \sum_j A_{ij}^\dagger A_{ij} \quad (17)$$

$$\rho \mapsto \frac{\sum_j A_{ij} \rho A_{ij}^\dagger}{\text{Tr}(\sum_j A_{ij} \rho A_{ij}^\dagger)}. \quad (18)$$

Pomiary takie realizuje się korzystając z pomocniczego systemu (*ancilli*), ewoluując złożony system odpowiednio dobranym operatorem unitarnym, następnie dokonując pomiaru rzutującego na *ancilli* i po odnotowaniu wyniku odrzuceniu jej. Ważnym narzędziem w formalizmie kwantowym są tak zwane kanały kwantowe (*quantum channel*), opisujące fizyczne połączenia, ich działania na fizyczny system. Kłasyycznym analogiem może być np. linia telefoniczna czy światłowód transmitujący internet. Przykładem fizycznej implementacji może znów być światłowód, który transmituje fotony, opisywane jako kubity. Kanały kwantowe opisują odwzorowania $\mathcal{M} : \mathcal{L}(\mathcal{H}^A) \rightarrow \mathcal{L}(\mathcal{H}^B)$, gdzie $\mathcal{L}(\mathcal{H}^A)$ jest przestrzenią macierzy na \mathcal{H}^A w przypadku skończenie wymiarowym, odwzorowujące liniowe operatory w przestrzeni wejściowej na liniowe operatory w przestrzeni wyjściowej, gdzie \mathcal{M} jest całkowicie dodatnią (*completely positive*, CP)⁴, $\mathcal{M}(\mathbb{1}) = \mathbb{1}$. Najogólniej kanały idealne, czyli takie, z których możemy otrzymać pełną informację o przechodzącym systemie, opisuje się $\mathcal{M}(\rho) = U^\dagger \rho U$, gdzie U jest pewną macierzą unitarną. W rzeczywistych

⁴Odwzorowanie jest CP, gdy $\phi \otimes \mathcal{I}_n$ również jest dodatnie $\forall n \in \mathcal{N}$. W przypadku odwzorowań o skończonych wymiarach każde dodatnie jest CP.

sytuacjach jednakże nie da się uniknąć oddziaływania z otoczeniem, który posiada dodatkowe niemierzalne stopnie swobody. Takie zaszumione kanały opisuje ogólnie $\mathcal{M}(\rho) = \text{Tr}_{\text{otoczenie}}(U^\dagger \rho \otimes \rho_0 U)$, gdzie $\text{Tr}_{\text{otoczenie}}$ opisuje operację śladu częściowego⁵, po stopniach swobody otoczenia, zaś operator unitarny U opisuje ewolucję czasową systemu i otoczenia, a ρ_0 jest stanem początkowym otoczenia [14]. Jasnym jest, że posiadając wyłącznie wiedzę na temat systemu ρ nie jest możliwe w ogólności odtworzenie informacji wysłanych. Typowym przykładem takiego zaszumionego kanału może być kanał depolaryzujący, który z prawdopodobieństwem η idealnie transmituje system, zaś z prawdopodobieństwem $1 - \eta$ depolaryzuje system, $\mathcal{M}(\rho) = \eta\rho + (1 - \eta)\mathbb{1}$. Najogólniejszym modelem kanałów kwantowych jest tzw. *quantum channel with memory* (kwantowy kanał z pamięcią) opisany np. w [15].

2 Macierz Procesu

Jednym z podejść do szukania korelacji nie zachowujących przyczynowego porządku jest rozwinięty w [18] formalizm macierzy procesu. Ewidentną zaletą tego podejścia jest zgodność z mechaniką kwantową na poziomie lokalnych eksperymentów. Jest to niejaki rozszerzenie łączące ideę POVM i regułę Borna. Podejście to porzuca założenie globalnej struktury czasoprzestrzeni. Opisuje się następująca sytuację: dwa odległe zamknięte laboratoria (tradycyjnie nazywane Alicja i Bob) wykonują pewne pomiary na zasobie kwantowym i otrzymują pewne wyniki. W przypadku tego formalizmu starano się zbudować taką strukturę, która przewiduje prawdopodobieństwa otrzymania danych wyników przy wykorzystaniu zasobu, który może nie mieć ściśle określonego porządku w czasie. W celu zachowania zgodności z mechaniką kwantową na poziomie lokalnym formalizm opiera się na następującym założeniu: operacje wykonywane przez poszczególną stronę są opisywane przez mechanikę kwantową w standardowym przyczynowym sformułowaniu, które można opisywać przy pomocy zbioru instrumentów kwantowych (*quantum instruments*) [8] z wejściową przestrzenią Hilberta \mathcal{H}^{A_1} i przestrzenią wyjściową \mathcal{H}^{A_2} . Najogólniej można je realizować poprzez zadziałanie unitarną transformacją na system wejściowy i system pomocniczy (*ancilla*), następnie wykonanie rzutującego pomiaru na części systemu pozostawiając pozostałą część systemu jako wyjście. Alicja wykorzystując dany instrument otrzymuje jeden z możliwych wyników x_i , który indukuje transformację \mathcal{M}_i^A z wejścia na wyjście. Odwzorowanie te odpowiada odwzorowaniu w pełni dodatnim (*completely positive*, CP)

$$\mathcal{M}_i^A : \mathcal{L}(\mathcal{H}^{A_1}) \mapsto \mathcal{L}(\mathcal{H}^{A_2}), \quad (19)$$

gdzie $\mathcal{L}(\mathcal{H}^X)$ jest przestrzenią macierzy na \mathcal{H}^X , której wymiar to d_X . Jej działanie na macierz gęstości ρ opisuje następująca formuła:

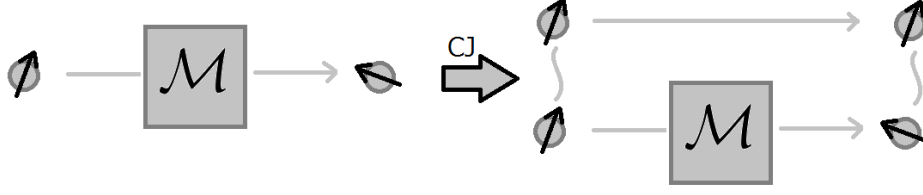
$$\mathcal{M}_i^A(\rho) = \sum_{j=1}^m E_{ij}^\dagger \rho E_{ij}, \quad (20)$$

gdzie macierze E_{ij} spełniają następujące własności:

$$\sum_{j=0}^m E_{ij}^\dagger E_{ij} \leq \mathbb{1}^{A_1} \quad (21)$$

$$\sum_{i=0}^n \sum_{j=0}^m E_{ij}^\dagger E_{ij} = \mathbb{1}^{A_1} \quad (22)$$

⁵Operację śladu pewnej macierzy A definiuje się następująco $\text{Tr } A = \sum_i \langle e_i | A | e_i \rangle$, gdzie $\{e_i\}$ to dowolna ortonormalna baza. W przypadku systemów złożonych można zdefiniować operację śladu częściowego. Zapisując pewną macierz $C = \sum_i \alpha_i A_i \otimes B_i$ ślad częściowy (po systemie B) oblicza się następująco $\text{Tr}_B C = \sum_i \alpha_i A_i \otimes \text{Tr}(B_i) = \sum_{ij} \alpha_i A_i \otimes \langle e_j | B_i | e_j \rangle = \sum_j (\mathbb{1} \otimes \langle e_j |) C (\mathbb{1} \otimes | e_j \rangle)$.



Rysunek 2: Rysunek ilustruje działanie izomorfizmu CJ. Zamiast działać odwzorowaniem na pewien stan izomorfizm CJ pokazuje działanie na maksymalnie splątane cząstki. Z powodu izomorfizmu w drugą stronę, konwencjonalnie interpretuje się izomorfizm CJ jako teleportację bramek kwantowych.

Takie odwzorowania, które spełniają (21) z równością zachowuje ślad (*trace preserving*, TP). Prawdopodobieństwo zaobserwowania wyniku realizowanego przez odwzorowanie \mathcal{M}_i^A to

$$\Pr(\mathcal{M}_i^A) = \text{Tr}(\mathcal{M}_i^A(\rho)) \quad (23)$$

Widać od razu, że równanie (22) narzuca, by możliwość zaobserwowania dowolnego wyniku była równa 1. Co łatwo pokazać w następujący sposób:

$$\begin{aligned} \sum_i \Pr(\mathcal{M}_i^A) &= \sum_i \text{Tr}(\mathcal{M}_i^A(\rho)) = \sum_{ij} \text{Tr} [E_{ij}^\dagger \rho E_{ij}] \\ &= \sum_{ij} \text{Tr} [\rho E_{ij}^\dagger E_{ij}] = \text{Tr} \left[\rho \sum_{ij} E_{ij}^\dagger E_{ij} \right] = \text{Tr} [\rho] = 1 \end{aligned} \quad (24)$$

W przypadku, gdy mamy do czynienia z więcej niż jedną stroną, *procesem* nazywa się listę $\Pr(\mathcal{M}_i^A, \mathcal{M}_j^B, \dots)$ dla wszystkich możliwych lokalnych wyników. Dalej w tym rozdziale będzie opisywany wyłącznie przypadek dwustronny, jednakże rozszerzenie formalizmu na przypadek wielostronny jest trywialne. Wygodnym sposobem przedstawiania odwzorowań \mathcal{M}_i^A jest izomorfizm Choi-Jamiołkowski (CJ) [13, 7], który pozwala przedstawiać transformacje liniowe przy pomocy macierzy. Macierz CJ $M_i^{A_1 A_2} \in \mathcal{L}(\mathcal{H}^{A_1} \otimes \mathcal{H}^{A_2}) \geq 0$ jest zdefiniowana jako

$$\mathfrak{C}(\mathcal{M}_i^A) = M_i^{A_1 A_2} := [\mathcal{I} \otimes \mathcal{M}_i^A(|\mathbb{1}\rangle)\langle\mathbb{1}|]^T = \left[\sum_{i,j=0}^{d_{A_1}-1} |i\rangle\langle j| \otimes \mathcal{M}_i^A(|i\rangle\langle j|) \right]^T, \quad (25)$$

$$|\mathbb{1}\rangle = \sum_{i=0}^{d_{A_1}-1} |ii\rangle, \quad (26)$$

gdzie $\{|j\rangle\}^{d_{A_1}}$ tworzy ortonormalną bazę w \mathcal{H}^{A_1} . Często wygodnie korzystać z odpowiednika (21) i (22) dla postaci CJ odwzorowań, który wygląda następująco:

$$\text{Tr}_{A_2} [M_i^{A_1 A_2}] \leq \mathbb{1}^{A_1}, \quad \forall i \quad (27)$$

$$\sum_i \text{Tr}_{A_2} [M_i^{A_1 A_2}] = \mathbb{1}^{A_1} \quad (28)$$

Drugi izomorfizm CJ pozwala przedstawiać macierze przy pomocy wektorów, tzw. "podwójnych ketów",

$$|A\rangle\rangle := \mathbb{1} \otimes A|\mathbb{1}\rangle = \sum_{i=0}^{d_{A_1}-1} |i\rangle A|i\rangle \quad (29)$$

Korzystając z tego przejścia można zapisać prawdopodobieństwo dwóch rezultatów jako

$$\Pr(\mathcal{M}_i^A, \mathcal{M}_j^B) = \text{Tr}(W^{A_1 A_2 B_1 B_2} (M_i^{A_1 A_2} \otimes M_j^{B_1 B_2})). \quad (30)$$

Macierz W w $\mathcal{L}(\mathcal{H}^{A_1} \otimes \mathcal{H}^{A_2} \otimes \mathcal{H}^{B_1} \otimes \mathcal{H}^{B_2})$ nazywa się macierzą procesu (*process matrix*). W celu generowania prawidłowego prawdopodobieństwa narzuca się dodatkowe warunki na W

$$W^{A_1 A_2 B_1 B_2} \geq 0. \quad (31)$$

$$\text{Tr } W^{A_1 A_2 B_1 B_2} = d_{A_2 B_2} \quad (32)$$

$$\text{Tr} [W^{A_1 A_2 B_1 B_2} (M^{A_1 A_2} \otimes M^{B_1 B_2})] = 1. \quad (33)$$

$$\forall M^{A_1 A_2}, M^{B_1 B_2} \geq 0, \text{Tr}_{A_2} M^{A_1 A_2} = \mathbb{1}^{A_1}, \text{Tr}_{B_2} M^{B_1 B_2} = \mathbb{1}^{B_1}, \quad (34)$$

gdzie $M^{A_1 A_2} = \sum_i M_i^{A_1 A_2}$. Warunek (31) zapewnia, że prawdopodobieństwa nie będą ujemne, a (33) i (34) - pewność zaobserwowania dowolnej pary odwzorowań.

Baza Hilberta-Schmidta dla $\mathcal{L}(\mathcal{H}^X)$ dane jest przez zbiór macierzy $\{\sigma_\mu^X\}_{\mu=0}^{d_X^2-1}$, gdzie $\sigma_0^X = \mathbb{1}$, $\text{Tr}(\sigma_\mu^X \sigma_\nu^X) = d_X \delta_{\mu\nu}$, $\text{Tr}(\sigma_{\mu>0}^X) = 0$. Ogólny element przestrzeni $\mathcal{L}(\mathcal{H}^{A_1} \otimes \mathcal{H}^{A_2} \otimes \mathcal{H}^{B_1} \otimes \mathcal{H}^{B_2})$ można zapisać, jako

$$W^{A_1 A_2 B_1 B_2} = \sum_{\mu\nu\lambda\gamma} w_{\mu\nu\lambda\gamma} \sigma_\mu^{A_1} \otimes \sigma_\nu^{A_2} \otimes \sigma_\lambda^{B_1} \otimes \sigma_\gamma^{B_2} \quad (35)$$

$$w_{\mu\nu\lambda\gamma} \in \mathbb{C}.$$

Wyrażenia zawierające wyłącznie wyrazy $\sigma_i^{A_1} \otimes \mathbb{1}^{reszta}$, ($i > 0$) nazywa się wyrażeniami typu A_1 , wyrażenia zawierające $\sigma_i^{A_1} \otimes \sigma_j^{A_2} \otimes \mathbb{1}^{reszta}$, ($i, j > 0$) nazywa się wyrażeniami typu $A_1 A_2$ etc. Najogólniejsza macierz procesu generująca prawidłowe prawdopodobieństwa, tak długo jak jest dodatnia, dla odwzorowań zgodnych z (31) i (33) to:

$$W^{A_1 A_2 B_1 B_2} = \frac{1}{d_{A_1} d_{B_1}} (\mathbb{1} + \sigma^{B \preceq A} + \sigma^{A \preceq B} + \sigma^{A \not\preceq B}) \quad (36)$$

$$\sigma^{A \preceq B} := \sum_{ij>0} a_{ij} \sigma_i^{A_1} \sigma_j^{B_2} + \sum_{ijk>0} b_{ijk} \sigma_i^{A_1} \sigma_j^{B_1} \sigma_k^{B_2} \quad (37)$$

$$\sigma^{B \preceq A} := \sum_{ij>0} c_{ij} \sigma_i^{A_2} \sigma_j^{B_1} + \sum_{ijk>0} d_{ijk} \sigma_i^{A_1} \sigma_j^{A_2} \sigma_k^{B_1} \quad (38)$$

$$\sigma^{A \not\preceq B} := \sum_{i>0} e_i \sigma_i^{A_1} + \sum_{i>0} f_i \sigma_i^{B_1} + \sum_{ij>0} h_{ij} \sigma_i^{A_1} \sigma_j^{B_1} \quad (39)$$

$$\forall_{ij} a_{ij}, b_{ij}, c_{ij}, d_{ij}, e_{ij}, f_{ij}, g_{ij}, h_{ij} \in \mathbb{R},$$

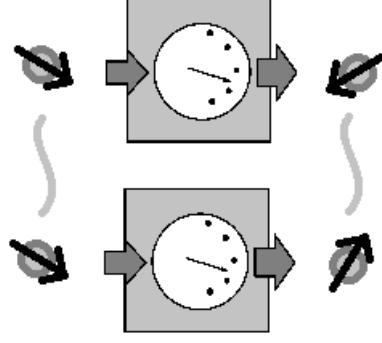
gdzie $\sigma^{A \preceq B}$ można uznać za zasób, w którym Alicja znajduje się w przeszłości Boba, $\sigma^{B \preceq A}$ za zasób, w którym Bob jest w przeszłości Alicji, zaś $\sigma^{A \not\preceq B}$ za zasób, w którym Alicja i Bob nie komunikują się ze sobą. Słuszność takiej interpretacji utwierdzają interpretacje poszczególnych wyrazów, które składają się na poszczególne zasoby. Zostały one opisane dalej. Wyróżnia się trzy rodzaje wyrażeń należących do rodziny macierzy przedstawionych powyżej.

2.1 Stany

Prawidłowe macierze procesu zawierające wyłącznie wyrazy typu $A_1 B_1$, A_1 , B_1 produkują takie same statystyki jak macierze gęstości wraz z regułą Borna. Można więc intuicyjnie wiązać wyrazy typu $A_1 B_1$, A_1 , B_1 z sposobem na opis stanów. Zaobserwować to można w następujący sposób. Okazuje się, że macierz CJ, która opisuje zaobserwowanie pewnego stanu $|\psi\rangle\langle\psi|$ i przygotowanie innego stanu $|\phi\rangle\langle\phi|$ wygląda następująco:

$$\mathfrak{C}(\mathcal{M}) = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi|^T. \quad (40)$$

W celu wyprowadzenia powyższego równania zacząć można od przeanalizowania w jaki sposób wygląda postać mapy, która opisuje pomiar danego stanu $|\psi\rangle$. Dobierając wektory $\{|\psi_i\rangle\}$ tak, by tworzyły bazę



Rysunek 3: Schematyczne przedstawienie stanów. Laboratoria wykonują pewne wybrane pomiary na systemach po czym wysyłają je ze swoich laboratoriów. Każde z laboratoriów otrzymuje różne, potencjalnie splątane, systemy.

ortonormalną i $|\psi_0\rangle = |\psi\rangle$ z wcześniej podanej definicji działania mapy można zapisać:

$$\begin{aligned}\mathcal{M}(\rho) &= \mathcal{M}\left(\sum_{ij} \alpha_{ij} |\psi_i\rangle\langle\psi_j|\right) = \sum_{ijm} [\alpha_{ij} E_m^\dagger |\psi_i\rangle\langle\psi_j| E_m] \\ &= \sum_{ijklef m} (e_{lkm} e_{efm}^* \alpha_{ij} |\psi_k\rangle\langle\psi_l| |\psi_i\rangle\langle\psi_j| |\psi_e\rangle\langle\psi_f|) .\end{aligned}\quad (41)$$

Biorąc pod uwagę fakt, że stan po otrzymaniu macierz po zadziałaniu mapą powinna być wielokrotnością $|\psi\rangle$ (stan obserwowany jest z pewnym prawdopodobieństwem). Narzuca to warunek, że $k = 0$. Następnie zapisując regułę prawdopodobieństwa:

$$\text{Tr}[\mathcal{M}(\rho)] = \sum_{ijlk} \text{Tr}[e_{0lm} e_{0km}^* \alpha_{ij} |\psi\rangle\langle\psi_l| |\psi_i\rangle\langle\psi_j| |\psi_k\rangle\langle\psi|] = \sum_{ijlkm} \text{Tr}[e_{0lm} e_{0km}^* \alpha_{ij} \delta_{jk} \delta_{jl} |\psi\rangle\langle\psi|] = \sum_{im} |e_{0im}| \alpha_{ii} .\quad (42)$$

Powyższy wynik musi się zgadzać z prawdopodobieństwem wynikającym z standardowej reguły prawdopodobieństwa, czyli:

$$\sum_{ij} \text{Tr}[\alpha_{ij} |\psi\rangle\langle\psi| |\psi_i\rangle\langle\psi_j|] = \sum_j \text{Tr}[\alpha_{0j} |\psi\rangle\langle\psi_j|] = \alpha_{00} .\quad (43)$$

Co narzuca warunek, że $e_{ijm} = 0$ dla $i \neq 0 \wedge j \neq 0$. Jako, że pozostał wyłącznie wyraz typu $|\psi\rangle\langle\psi|$ można dokonać sumowania po m co daje:

$$\sum_{im} |e_{00m}| \alpha_{ii} = \sum_m |e_{00m}| \alpha_{ii} = e_{00} \alpha_{ii} .\quad (44)$$

Korzystając ponownie z (43) widać, że $|e_{00}| = 1$. Korzystając z definicji, postać CJ tego odwzorowania to:

$$\begin{aligned}\mathfrak{C}(\mathcal{M}) &= \sum_{ij} |i\rangle\langle j| \otimes (|\psi\rangle\langle\psi|^\dagger |j\rangle\langle i| |\psi\rangle\langle\psi|)^T = \sum_{ij} |i\rangle\langle j| \otimes (|\psi\rangle \left(\sum_l \beta_l^* \langle l||j\rangle\right) \left(\sum_k \beta_k \langle i||k\rangle\right) \langle\psi|)^T \\ &= \sum_{ij} \beta_i \beta_j^* |i\rangle\langle i| \otimes |\psi\rangle\langle\psi|^T = |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|^T .\end{aligned}\quad (45)$$

Dalej zauważając, ewolucja unitarna jest już zapisana w odpowiedniej formie oraz wybierając macierz unitarną jako $U = \sum_i |\phi_i\rangle\langle\psi_i|$, gdzie wektory $\{|\phi_i\rangle\}$ tworzą bazę ortonormalną, a $|\phi_0\rangle$ jest wybranym stanem, który chce się przygotować, złożenie poprzedniej z poprzednią transformacją ma postać:

$$|\psi\rangle\langle\psi| \otimes U |\psi\rangle\langle\psi| U^\dagger = |\psi\rangle\langle\psi| \otimes |\phi\rangle\langle\phi| .\quad (46)$$

Co pokazuje, że rzeczywiście tak wygląda odwzorowanie CJ dla pomiaru i przygotowania stanu. Przyjmując teraz następująco postać macierzy procesu:

$$W = \rho^{A_1 B_1} \otimes \mathbb{1}^{A_2} \otimes \mathbb{1}^{B_2}, \quad (47)$$

która opisuje każdą macierz procesu zawierającą wyłącznie wybrane w tym rozdziale wyrazy. Zapisując regułę prawdopodobieństwa otrzymuje się

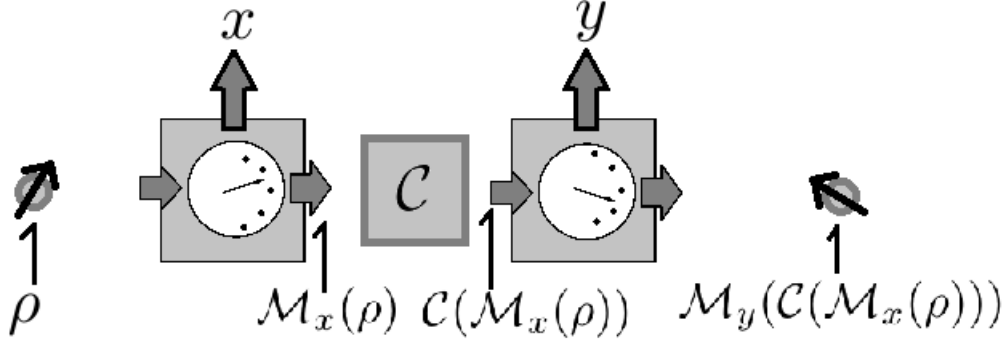
$$\begin{aligned} \Pr(x, y) &= \text{Tr} [(\rho^{A_1 B_1} \otimes \mathbb{1}^{A_2} \otimes \mathbb{1}^{B_2})(|\psi_x\rangle\langle\psi_x|^{A_1} \otimes |\psi_y\rangle\langle\psi_y|^{B_1} \otimes |\phi_x\rangle\langle\phi_x|^{A_2} \otimes |\phi_y\rangle\langle\phi_y|^{B_2})] \\ &= \text{Tr} [\rho|\psi_x\rangle\langle\psi_x| \otimes |\psi_y\rangle\langle\psi_y| \otimes |\phi_x\rangle\langle\phi_x| \otimes |\phi_y\rangle\langle\phi_y|] \\ &= \text{Tr} [\rho|\psi_x\rangle\langle\psi_x| \otimes |\psi_y\rangle\langle\psi_y|] \text{Tr} [|\phi_x\rangle\langle\phi_x|] \text{Tr} [|\phi_y\rangle\langle\phi_y|] \\ &= \text{Tr} [\rho|\psi_x\rangle\langle\psi_x| \otimes |\psi_y\rangle\langle\psi_y|]. \end{aligned} \quad (48)$$

Powyższe wyprowadzenie pokazuje, że dla pomiarów von Neumanna, tak zdefiniowana macierz procesu generuje takie same statystyki jak formalizm macierzy gęstości. Warto jeszcze zaznaczyć, że iloczynowa postać tej macierzy procesu zapewnia, że $\rho^{A_1 B_1}$ również jest dodatnie, czyli spełnia wszystkie warunki narzucone przez formalizm macierzy gęstości. Jednym ze sposobów na pokazanie, że generowane są identyczne statystyki dla dowolnych POVM jest wykonanie jawnego rachunku:

$$\begin{aligned} \Pr(x, y) &= \text{Tr} [\rho^{A_1 B_1} \otimes \mathbb{1}^{A_2 B_2} (M_x^{A_1 A_2} \otimes M_y^{B_1 B_2})] \\ &= \sum_{ijkl} \text{Tr} [(\alpha_{ijkl}|i\rangle\langle j|^{A_1} \otimes \mathbb{1}^{A_2} \otimes |k\rangle\langle l|^{B_1} \otimes \mathbb{1}^{B_2}) M_x^{A_1 A_2} \otimes M_y^{B_1 B_2}] \\ &= \sum_{ijklmnef} \text{Tr} [\alpha_{ijkl}|i\rangle\langle j| \otimes \mathbb{1} \otimes |k\rangle\langle l| \otimes \mathbb{1} (|m\rangle\langle n| \otimes \mathcal{M}_x(|n\rangle\langle m|)^T \otimes |e\rangle\langle f| \otimes \mathcal{M}_y(|f\rangle\langle e|)^T)] \\ &= \sum_{ijklmnef} \text{Tr} [\alpha_{ijkl}|i\rangle\langle j||m\rangle\langle n|^{A_1} \otimes |k\rangle\langle l||e\rangle\langle f|^{B_1}] \text{Tr} [\mathcal{M}_x(|n\rangle\langle m|)^{A_2 T} \otimes \mathcal{M}_y(|f\rangle\langle e|)^{B_2 T}] \\ &= \sum_{mnef} \text{Tr} [\alpha_{ijkl}\langle n||i\rangle\langle j||m\rangle \otimes \langle f||k\rangle\langle l||e\rangle] \text{Tr} [\mathcal{M}_x(|n\rangle\langle m|)^{A_2 T} \otimes \mathcal{M}_y(|f\rangle\langle e|)^{B_2 T}] \\ &= \sum_{mnef} \text{Tr} [\alpha_{nmfe}] \text{Tr} [\mathcal{M}_x(|n\rangle\langle m|)^{A_2 T} \otimes \mathcal{M}_y(|f\rangle\langle e|)^{B_2 T}] \\ &= \sum_{mnef} \text{Tr} [\alpha_{nmfe} \mathcal{M}_x(|n\rangle\langle m|)^{A_2 T} \otimes \mathcal{M}_y(|f\rangle\langle e|)^{B_2 T}] \\ &= \text{Tr} \left[\mathcal{M}_x \otimes \mathcal{M}_y \left(\sum_{nmfe} \alpha_{nmfe} |n\rangle\langle m| \otimes |f\rangle\langle e| \right)^T \right] \\ &= \text{Tr} [\mathcal{M}_x \otimes \mathcal{M}_y(\rho)^T] \\ &= \text{Tr} [\mathcal{M}_x \otimes \mathcal{M}_y(\rho)]. \end{aligned} \quad (49)$$

Ostateczna postać po przekształceniach zgadza się z tą, która opisuje statystyki pomiarów na systemie złożonym opisywanym przez równanie (23). Przykładowo macierz procesu, która opisuje sytuację, gdzie laboratoria dzielą maksymalnie splątane ⁶ cząsteczki zapisuje się następująco:

$$W = |\mathbb{1}\rangle\langle\mathbb{1}|^{A_1 B_1} \otimes \mathbb{1}^{A_2} \otimes \mathbb{1}^{B_2}. \quad (50)$$



Rysunek 4: Schematyczna reprezentacja kanału CPTP. Alicja wykonuje wybrane operacje na systemie po czym wysyła go do Boba. W trakcie przesyłania systemu zostaje zaaplikowana unitarna transformacja U .

2.2 Kanały

Wyrazy typu $A_1 A_2 B_1$, $B_1 B_2 A_1$ można przyjąć za sposób opisywania kanałów. O ile łatwo zauważyć słuszność, że formuła

$$\text{Tr} [\mathcal{M}_y^B \circ \mathcal{C} \circ \mathcal{M}_x^A(\rho)] \quad (51)$$

opisuje statystyki pomiarowe eksperymentu, w którym Alicja wykonuje pewne pomiary przesyła system kanałem CPTP \mathcal{C} po czym Bob wykonuje swoje pomiary na otrzymanym systemie to nie oczywista jest jej równoważność z

$$\text{Tr} \left[\left(\rho^{A_1} \otimes C^{A_2 B_1 T} \otimes \mathbb{1}^{B_2} \right) (M_x^{A_1 A_2} \otimes M_y^{B_1 B_2}) \right]. \quad (52)$$

Można to pokazać następująco:

$$\begin{aligned} & \text{Tr} \left[\left(\rho^{A_1} \otimes C^{A_2 B_1} \otimes \mathbb{1} \right) (M_x^{A_1 A_2} \otimes M_y^{B_1 B_2}) \right] \\ &= \sum_{ijklmn} \text{Tr} \left[(\rho \otimes |i\rangle\langle j| \otimes \mathcal{C}(|i\rangle\langle j|) \otimes \mathbb{1}) (|k\rangle\langle l| \otimes \mathcal{M}_x(|l\rangle\langle k|)^T \otimes |m\rangle\langle n| \otimes \mathcal{M}_y(|n\rangle\langle m|)^T) \right] \\ &= \sum_{ijklmn} \text{Tr} \left[\rho |k\rangle\langle l| \otimes |i\rangle\langle j| \mathcal{M}_x(|l\rangle\langle k|)^T \otimes \mathcal{C}(|i\rangle\langle j|) |m\rangle\langle n| \otimes \mathcal{M}_y(|n\rangle\langle m|)^T \right] \\ &= \text{Tr} [\rho |k\rangle\langle l|] \text{Tr} [|i\rangle\langle j| \mathcal{M}_x(|l\rangle\langle k|)] \text{Tr} [\mathcal{C}(|i\rangle\langle j|) |m\rangle\langle n|] \text{Tr} [\mathcal{M}_y(|m\rangle\langle n|)] \\ &= \sum_{ijmn} \text{Tr} \left[|i\rangle\langle j| \mathcal{M}_x \left(\sum_{lk} \rho_{lk} |l\rangle\langle k| \right)^T \right] \text{Tr} [\mathcal{C}(|i\rangle\langle j|) |m\rangle\langle n|] \text{Tr} [\mathcal{M}_y(|n\rangle\langle m|)^T] \\ &= \sum_{ijmn} \text{Tr} [|i\rangle\langle j| \mathcal{M}_x(\rho)^T] \text{Tr} [\mathcal{C}(|i\rangle\langle j|) |m\rangle\langle n|] \text{Tr} [\mathcal{M}_y(|n\rangle\langle m|)^T] \\ &= \sum_{mn} \text{Tr} [\mathcal{C}(\mathcal{M}_x(\rho)) |m\rangle\langle n|] \text{Tr} [\mathcal{M}_y(|n\rangle\langle m|)^T] \\ &= \text{Tr} [\mathcal{M}_y(\mathcal{C}(\mathcal{M}_x(\rho)))^T] = \text{Tr} [\mathcal{M}_y(\mathcal{C}(\mathcal{M}_x(\rho)))] \\ &= \text{Tr} [\mathcal{M}_y^B \circ \mathcal{C} \circ \mathcal{M}_x^A(\rho)] \end{aligned} \quad (53)$$

Przykładowo macierz opisująca odwracalny kanał, który wysyła cząstkę z A_2 do B_1 i wykonuje pewną operację unitarną U to $|U\rangle\rangle\langle\langle U|^{A_2 B_1}$. Korzystając z wcześniej opisanej detekcji stanu i przygotowania

⁶Do sprecyzowania co rozumiane jest pod pojęciem maksymalnego splątania konieczne jest wprowadzenie miary splątania. Przez miarę splątania rozumie się taką funkcję, która jest monotoniczna, gdy laboratoria mogą wykonywać lokalne operacje i komunikować się klasycznie (np. telefonem). Konieczne również jest, by zbiegała do zera dla stanów niesplątanych. Przykładem takiej miary jest entropia von Neumanna definiowana przez $S(\rho) = -\text{Tr}[\rho \log \rho]$. Okazuje się, że jest ona maksymalna dla $\frac{1}{d}|\mathbb{1}\rangle\rangle\langle\langle \mathbb{1}|$ [12].

innego stanu eksperyment, w którym Alicja wysyła system zakodowany w bazie z , a Bob wykonują pomiar w bazie z następnie Alicja przesyła dalej swój system, a Bob przesyła stan maksymalnie zmieszany stan $(\frac{1}{2}\mathbb{1})$ można opisać następującymi odwzorowaniami

$$\xi(i) = |i\rangle\langle i| \otimes |i\rangle\langle i| \quad (54)$$

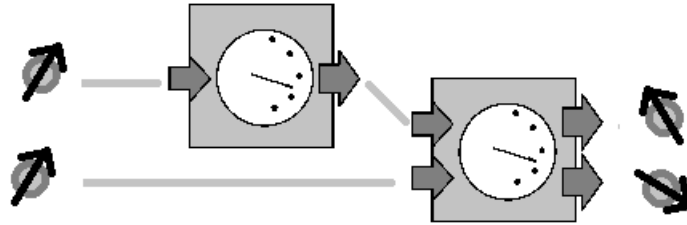
$$\eta(j) = |j\rangle\langle j| \otimes \frac{1}{2}\mathbb{1}. \quad (55)$$

W celu skrócenia zapisu pominięto indeksy górne, które pozostaną dalej niejawne, gdy ich brak nie będzie wprowadzał niejasności. Można się spodziewać, że gdy laboratorium będzie łączył kanał z A_2 do B_1 , który zamienia $|i\rangle \mapsto |i \oplus 1\rangle$, kanał ten opisuje postać CJ macierzy unitarnej $\sum_i |i\rangle\langle i \oplus 1|$, a Alicja na wejściu dostaje stan maksymalnie zmieszany, to prawdopodobieństwo zaobserwowania stanu $|j\rangle$ u Boba będzie równe 1, gdy Alicja wyśle mu stan $|j \oplus 1\rangle$ i zerowe w przeciwnym wypadku. Podejrzenia te potwierdza jawny rachunek:

$$\begin{aligned} W &= \sum_{ijkl} \mathbb{1} \otimes |i\rangle\langle j| \otimes |k \oplus 1\rangle\langle k| |i\rangle\langle j| |l\rangle\langle l \oplus 1| \otimes \mathbb{1} \\ \Pr(i, j) &= \frac{4}{\text{Tr } W} \text{Tr}[W(\xi(i) \otimes \eta(j))] \\ &= C \sum_{efkl} \text{Tr}[\mathbb{1} \otimes |e\rangle\langle f| \otimes |k \oplus 1\rangle\langle k| |e\rangle\langle f| |l\rangle\langle l \oplus 1| \otimes \mathbb{1}] (|i\rangle\langle i| \otimes |i\rangle\langle i| \otimes |j\rangle\langle j| \otimes \mathbb{1}) \\ &= \frac{2}{8} \sum_{efkl} \delta_{if} \delta_{j(l \oplus 1)} \text{Tr}[|i\rangle\langle i| \otimes |e\rangle\langle i| \otimes |k \oplus 1\rangle\langle k| |e\rangle\langle f| |l\rangle\langle j| \otimes \mathbb{1}] \\ &= \frac{2}{8} \sum_{efkl} \delta_{if} \delta_{ke} \delta_{fl} \delta_{j(l \oplus 1)} \text{Tr}[|i\rangle\langle i| \otimes |e\rangle\langle i| \otimes |k \oplus 1\rangle\langle j| \otimes \mathbb{1}] \\ &= \frac{2}{8} \sum_k \delta_{i(j \oplus 1)} \text{Tr}[|i\rangle\langle i| \otimes |k\rangle\langle i| \otimes |k \oplus 1\rangle\langle j| \otimes \mathbb{1}] \\ &= \frac{2}{8} \sum_k \delta_{i(j \oplus 1)} \text{Tr}[|i\rangle\langle i| \otimes |k\rangle\langle i| \otimes |k \oplus 1\rangle\langle i \oplus 1| \otimes \mathbb{1}] \\ &= \frac{1}{2} \delta_{i(j \oplus 1)}. \end{aligned} \quad (57)$$

Co potwierdza podejrzenia, że powyższy zasób jest kanałem od Alicji do Boba.

2.3 Kanały z pamięcią



Rysunek 5: Schematyczna reprezentacja kanału z pamięcią na przykładzie zasobu wykorzystywanego do implementacji kodowania supergęstego. Alicja z Bobem dzielą maksymalnie splątane cząstki. Alicja wykonuje pewną unitarną transformację i wysyła swój system dalej do Boba.

Do opisywania kanałów z pamięcią wykorzystuje się wyrazy typu $B_1 B_2 A_1$, $A_1 A_2 B_1$. Są one najogólniejszym wyrazem zgodnym wymaganiami narzuconymi na macierze procesu. Ciekawym przykładem

kanalu z pamięcią może być zasób wykorzystywany przy implementacji kodowania supergęstego (*superdense coding*). Jest to protokół, który wykorzystuje się do przesłania dwóch bitów informacji od Alicji do Boba. Początkowo produkowana jest para maksymalnie splątanych cząsteczek jedna jest wysłana do Alicji druga do Boba. Następnie Alicja wykonuje jedną z czterech lokalnych unitarnych transformacji na swoim systemie po czym wysyła swój system do Boba. Macierze, którymi działa Alicja to $\{U_i\} = \{\mathbb{1}, \mathbb{X}, \mathbb{Z}, -i\mathbb{Y}\}$, gdzie $\mathbb{X}, \mathbb{Y}, \mathbb{Z}$ to macierze Pauliego:

$$\mathbb{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \mathbb{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \mathbb{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (58)$$

Okazuje się, że po wykonaniu lokalnej transformacji system złożony znajduje się w jednym z czterech ortogonalnych stanów, co pozwala Bobowi, po otrzymaniu systemu od Alicji, określić jaką transformację wykonała Alicja, czyli otrzymać wiadomość od Alicji zakodowaną w wykonanej przez nią transformacji. Wyjątkowość tego protokołu polega na fakcie, że Bob może otrzymać pierwszą cząstkę arbitralnie wcześniej, niż cząstkę, którą otrzyma od Alicji, co więcej może on otrzymać tę cząstkę zanim Alicja zdecyduje jakie 2 bity chce mu przesłać. Co może błędnie sugerować, że Alicja wysłała dwa klasyczne bity przy pomocy jednego kubitu. Sytuacja taka jest zabroniona przez granicę Holevo (*Holevo bound*). Mimo wszystko dwa kubity są wysyłane w celu przesłania dwóch klasycznych bitów co nie wprowadza sprzeczności. W celu wykonania tego protokołu potrzebne są dwie maksymalnie splątane cząsteczki i kanał od Alicji do Boba. Korzystając z wiedzy z poprzednich dwóch podrozdziałów zapisuje się ten zasób następująco:

$$W = |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{A_1 B_{11}}|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{A_2 B_{12}}\mathbb{1}^{B_{21} B_{22}}, \quad (59)$$

gdzie w tym przypadku Bob operuje na dwóch cząstkach. W przypadku Boba pierwsza cyfra indeksów dolnych systemów Boba wskazuje, czy dany system jest wejściowy czy wyjściowy, zaś druga cyfra jest porządkowa. Stany po wykonaniu kolejnych unitarnych transformacji z dokładnością do stałej to $\{|\psi_i\rangle\} = \{\mathbb{1} \otimes U_i |\psi_i\rangle\} = \{|00\rangle + |11\rangle, |10\rangle + |01\rangle, |00\rangle - |11\rangle, |10\rangle - |01\rangle\}$. Postać CJ operacji wykonywanych przez poszczególne strony to:

$$\xi(i) = \frac{1}{4} \sum_{ef} |e\rangle\langle f| \otimes U_i |e\rangle\langle f| U_i^\dagger \quad (60)$$

$$\eta(j) = \frac{1}{4} |e\rangle\langle e| \sum_{ef} U_j |e\rangle\langle f| U_j^\dagger |f\rangle\langle f| \otimes \mathbb{1}. \quad (61)$$

Korzystając z reguły prawdopodobieństwa i zapisując systemy w kolejności $A_1 A_2 B_{11} B_{12} B_{21} B_{22}$ wykonuje się następujące obliczenia:

$$\begin{aligned} \Pr(j|i) &= \frac{1}{2} \text{Tr} [W(\xi(i) \otimes \eta(j))] \\ &= \frac{1}{32} \sum_{efklmnqp} \text{Tr} \left[|e\rangle\langle f| \otimes |k\rangle\langle l| \otimes |e\rangle\langle f| \otimes |k\rangle\langle l| \otimes \mathbb{1} \otimes \mathbb{1} \left(|m\rangle\langle n| \otimes U_i |m\rangle\langle n| U_i^\dagger \otimes |q\rangle\langle p| \otimes U_j |q\rangle\langle p| U_j^\dagger \otimes \mathbb{1} \otimes \mathbb{1} \right) \right] \\ &= C \sum_{efklmnqp} \delta_{fm} \delta_{l(m+(i\oplus 1)\oplus 1)} \delta_{fq} \delta_{l(q+(j\oplus 1)\oplus 1)} \text{Tr} \left[|e\rangle\langle n| \otimes |k\rangle\langle n| U_i^\dagger \otimes |e\rangle\langle p| \otimes |k\rangle\langle p| U_j^\dagger \otimes \mathbb{1} \otimes \mathbb{1} \right] \\ &= 4C \sum_{efklmnqp} \delta_{(m+(i\oplus 1)\oplus 1)(q+(j\oplus 1)\oplus 1)} \delta_{fm} \delta_{fq} \text{Tr} \left[|e\rangle\langle n| \otimes |k\rangle\langle n| U_i^\dagger \otimes |e\rangle\langle p| \otimes |k\rangle\langle p| U_j^\dagger \right] \\ &= 4C \sum_{ekmnp} \delta_{(i\oplus 1)(j\oplus 1)} \text{Tr} \left[|e\rangle\langle n| \otimes |k\rangle\langle n| U_i^\dagger \otimes |e\rangle\langle p| \otimes |k\rangle\langle p| U_j^\dagger \right] \\ &= \delta_{ij} \\ C &= \frac{-1^{(i\div 2 + j\div 2)}}{32} \end{aligned} \quad (62)$$

gdzie powyżej $x \oplus y$ traktowano jako $x + y \bmod 2$, zaś \div to dzielenie bez reszty. Powyższe obliczenia pokazują, że rzeczywiście opisywany jest tutaj protokół supergęstego kodowania.

3 Przyczynowa separowalność i przyczynowe nierówności

Macierzami procesu *causally separable* (przyczynowo separowalnymi) nazywa się takie macierze, które można zapisać jako wypukłą kombinację procesów o implementowalnych przy założeniu określonej struktury przyczynowej. Definiując:

$$W^{B \not\prec A} := \frac{1}{d_{A_1} d_{B_1}} \mathbb{1} + \sigma^{A \preceq B} + \sigma^{A \not\prec B} \quad (63)$$

$$W^{A \not\prec B} := \frac{1}{d_{A_1} d_{B_1}} \mathbb{1} + \sigma^{B \preceq A} + \sigma^{A \not\prec B} \quad (64)$$

$$W^{A \not\prec B} := \frac{1}{d_{A_1} d_{B_1}} \mathbb{1} + \sigma^{A \not\prec B}, \quad (65)$$

gdzie pierwszy proces można interpretować jako zasób, w którym Bob nie jest przed Alicją, a drugi jako ten, w którym Alicja nie jest przed Bobem.

$$W^{A_1 A_2 B_1 B_2} = q W^{B \not\prec A} + (1 - q) W^{A \not\prec B}, \quad 0 \leq q \leq 1. \quad (66)$$

Powyższa dekompozycja nie musi być jednoznaczna, jako że wyrazy typu $W^{A \not\prec B}$ można włączyć do wybranego wyrazu. Przed wprowadzeniem przyczynowej nierówności (*causal inequality*) warto wspomnieć o tzw. nierówności Bella. Jest to nieskończona rodzina nierówności, których żaden niesplątany system nie może złamać. Jest to niezależny od implementacji pomiarów (*device independent*) sposób weryfikacji splątania kwantowego. Dla każdego zadanie, które wykonują pewne strony można wprowadzić nierówność, która ogranicza (np. z góry) wyniki jakie mogą zostać osiągnięte przy wykorzystaniu zasobów o określonej przyczynowości. Jeżeli taka nierówność zostałaby złamana można wnioskować, że zasób wykorzystany w zadaniu nie ma określonej przyczynowości.

Przyjmuje się następujące założenia na temat natury rzeczywistości uporządkowanej przyczynowo:

Przyczynowa struktura (*causal structure*, CS) Wydarzenia obdarzone są częściowym porządkiem w strukturze czasoprzestrzeni, można wyznaczyć kolejność wydarzeń $A \prec B$, która wyznacza kierunek przesyłania informacji; jeżeli $A \prec B$, to możliwe jest sygnalizowanie ⁷ z A do B, lecz nie na odwrót.

Wolny wybór (*Free choice*, FC) W przypadku wyboru liczb losowych, możliwe korelacje występują wyłącznie z wynikami z przyszłości.

Zamknięte laboratoria (*Closed laboratories*, CL) Liczba odgadnięta przez Alicję może być skorelowana z liczbą losową Boba wyłącznie, jeżeli system wysłany do Alicji jest przed (w sensie przyczynowości) generacją liczby Boba, analogicznie w przypadku odwrotnym.

Rozważa się następującą dwustronną grę realizowaną wielokrotnie przez dwa odległe laboratoria (Alicję i Boba). W każdej iteracji rozgrywki Alicja i Bob otrzymują na wejściu pewien fizyczny system, wykonują na nim pewne operacje i wysyłają dalej system. Każda ze stron może otrzymać sygnał wyłącznie przez

⁷W przypadku, gdy $A \prec B$ oznacza to, że brzegowy rozkład prawdopodobieństwa otrzymania danego wyniku nie zależy od wejścia drugiej strony. $\Pr(a|x, y) = \Pr(a|x, y') \quad \forall a, x, y, y'$, $\Pr(a|x, y) = \sum_b \Pr(a, b|x, y)$, gdzie przez a, b oznaczamy wyniki otrzymane przez odpowiednie strony, zaś x, y ich wejścia.

system wchodzący do laboratorium, zaś wysłać wyłącznie przez system wychodzący z laboratorium. Widać więc, że jeżeli Alicja otrzyma system, który przeszedł pewną procedurę u Boba, to Bob może wysłać informacje, zaś Alicja może ją wyłącznie odebrać, co uniemożliwia dwustronna sygnalizację. Każdy z graczy otrzymując system losuje jeden bit wybraną metodą oznaczany a dla Alicji i b dla Boba. Dodatkowo Bob losuje bit b', który decyduje, czy Bob ma zgadywać bit a Alicji, czy Alicja ma zgadywać bit b Boba. Bez utraty ogólności można przyjąć, że obie strony zgadują bit drugiego gracza. W zależności od b' ich predykcja może się nie liczyć. Zakłada się, że bity losowane są z równym prawdopodobieństwem. Prawdopodobieństwo sukcesu w takiej grze zapisuje się następująco

$$\Pr_{\text{sukcesu}} := \frac{1}{2} [\Pr(x = b|b' = 0) + \Pr(y = a|b' = 1)] \quad (67)$$

Każda strategia w uporządkowanej strukturze czasu osiąga $\Pr_{\text{sukcesu}} \leq \frac{3}{4}$. Optymalna strategię opisuje się nierygorystycznie następująco: w przypadku $A \prec B$ Alicja może zakodować swój bit w pewien sposób w systemie, który wyśle do Boba, dlatego można wybrać taką strategię, że $\Pr(y = a) = 1$, Alicji pozostaje wtedy losowa predykcja co do wartości bitu Boba - $\Pr(x = b) = \frac{1}{2}$. Można również pokazać, że żadna probabilistyczna strategia nie może poprawić wyniku, co daje optymalną strategię. Okazuje się, że korzystając z korelacji opisywanych przez formalizm macierzy procesu $\Pr_{\text{sukces}} \leq \frac{2+\sqrt{2}}{4}$. Można rozważyć następującą macierz procesu

$$W^{A_1 A_2 B_1 B_2} = \frac{1}{4} \left[\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}}(\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + q\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z} + \frac{(1-q)}{2}\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{1}) \right], \quad 0 \leq q \leq 1. \quad (68)$$

Macierze $\mathbb{1}, \mathbb{X}, \mathbb{Y}, \mathbb{Z}$ tworzą bazę Hilberta-Schmidta. W powyższym zapisie pominięto iloczyn tensorowy, w celu skrócenia zapisu w miejscach, gdzie jego brak nie powinien wprowadzać nieporozumień - $\mathbb{1}^{A_1} \mathbb{X}^{A_2} \mathbb{Y}^{B_1} \mathbb{Z}^{B_2} =: \mathbb{1}\mathbb{X}\mathbb{Y}\mathbb{Z}$. Przedstawioną macierz z $q = 1$ wraz z dalej przedstawioną procedurą komunikacji wprowadzono w [18] jako zasób, który pozwala złamać przyczynową nierówność wynikającą z tej gry. W [6] pokazano, że przy odpowiednich założeniach o dozwolonych operacjach jest to maksymalne przekroczenie nierówności wynikającej z tego zadania. Z drugiej strony widać od razu, że przy $q = 0$ mamy $A \prec B$, zatem oczywistym jest, że taki zasób nie pozwala złamać przyczynowej nierówności. Sterując wartością q można zaobserwować odpowiednio przejścia macierzy z ustalonej przyczynowości poprzez separowalną do nieseparowalnej. Macierze separowalne nie mogą łamać żadnej nierówności przyczynowej, nieseparowalne zostaną dokładniej opisane dalej. Procedura komunikacji wygląda następująco. Za każdym razem Alicja mierzy swój system w bazie z i przypisuje $x = 0$ dla $|z_+\rangle$ zaś $x = 1$ dla $|z_-\rangle$, a następnie przygotowuje na nowo kubit i zakodowuje a w tej samej bazie. Odwzorowanie CP Alicji wygląda następująco:

$$\xi(x, a) = \frac{1}{4} [\mathbb{1} + (-1)^x \mathbb{Z}] \otimes [\mathbb{1} + (-1)^a \mathbb{Z}]. \quad (69)$$

Natomiast, gdy Bob jako posiadacz bitu b' chce odczytać bit Alicji, mierzy przychodzący kubit w bazie z i przypisuje wyniki tego pomiaru do y analogicznie jak Alicja. W tym przypadku nieistotne jest jaki stan przygotowuje Bob, więc przygotowuje dowolny stan ρ^{B_2} znormalizowany do $\text{Tr}(\rho^{B_2}) = 1$. W przypadku $b' = 0$, Bob chce wysłać swój bit do Alicji. Dokonuje pomiaru w bazie x , następnie w przypadku wyniku $y = |x_+\rangle$ zakodowuje swój bit następująco: $0 \rightarrow |z_+\rangle, 1 \rightarrow |z_-\rangle$ w drugim kodowanie wygląda odwrotnie $1 \rightarrow |z_+\rangle, 0 \rightarrow |z_-\rangle$. Jego odwzorowanie wygląda następująco

$$\eta(y, b, b') = \begin{cases} \frac{1}{2} [\mathbb{1} + (-1)^y \mathbb{Z}] \otimes \rho & b' = 1 \\ \frac{1}{4} [\mathbb{1} + (-1)^y \mathbb{X}] \otimes [\mathbb{1} + (-1)^{b+y} \mathbb{Z}] & \text{w przeciwnym wypadku.} \end{cases} \quad (70)$$

Przypominając, że prawdopodobieństwo sukcesu w tej grze dane jest jako

$$\Pr_{\text{sukcesu}} := \frac{1}{2} [\Pr(x = b|b' = 0) + \Pr(y = a|b' = 1)], \quad (71)$$

i przyjmując dla wygody obliczeń, że ρ w mapie Boba to $\frac{1}{2}\mathbb{1}$

$$\begin{aligned}
\Pr(x, y|a, b, 1)_q &= \frac{1}{4} (p_1 + p_2 + p_3 + p_4) \\
p_1 &= \frac{1}{16} \text{Tr} [(\mathbb{1} + (-1)^x \mathbb{Z}) \otimes (\mathbb{1} + (-1)^a \mathbb{Z}) \otimes (\mathbb{1} + (-1)^y \mathbb{Z}) \otimes \mathbb{1}] \\
&= 1 \\
p_2 &= \frac{1}{16\sqrt{2}} \text{Tr} [\mathbb{1} \mathbb{Z} \mathbb{1} (\mathbb{1} + (-1)^x \mathbb{Z}) \otimes (\mathbb{1} + (-1)^a \mathbb{Z}) \otimes (\mathbb{1} + (-1)^y \mathbb{Z}) \otimes (\mathbb{1} + (-1)^{b+y} \mathbb{Z})] \\
&= \frac{4}{16\sqrt{2}} \text{Tr} [(\mathbb{Z} + (-1)^a \mathbb{Z} \mathbb{Z}) \otimes (\mathbb{Z} + \mathbb{Z} \mathbb{Z} (-1)^y)] \\
&= \frac{1}{\sqrt{2}} (-1)^a (-1)^y \\
p_3 &= \frac{q}{8\sqrt{2}} \text{Tr} [(\mathbb{Z} + (-1)^x \mathbb{Z} \mathbb{Z}) \otimes (\mathbb{X} + (-1)^y \mathbb{X} \mathbb{Z}) \otimes \mathbb{Z}] \\
&= \frac{1}{4\sqrt{2}} (-1)^x \cdot 0 \cdot 0 \\
p_4 &= 0
\end{aligned} \tag{72}$$

Co po obliczeniu odpowiednich rozkładów brzegowych i wykonaniu analogicznych obliczeń dla $b' = 0$ daje:

$$\Pr(x = b|b' = 0)_q = \frac{\sqrt{2}q + 2}{4} \tag{73}$$

$$\Pr(y = a|b' = 1)_q = \frac{\sqrt{2} + 2}{4} \tag{74}$$

$$\Pr_{\text{sukcesu}_q} = \frac{\sqrt{2}q + \sqrt{2} + 4}{8}, \tag{75}$$

gdzie indeks odnotowuje zależność prawdopodobieństwa od q . Tak jak się spodziewano, prawdopodobieństwo sukcesu Alicji rośnie wraz ze zwiększaniem współczynnika przy członie $\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z}$ rozumianym jako reprezentacja kanału kwantowego z pamięcią, który odpowiada za sygnalizujące korelacje $A \preceq B$. Przy $q = 0$ Alicja ma dostęp wyłącznie do niesygnalizujących nietrywialnych zasobów (wyraz $\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{1}$), które nie mogą zwiększyć prawdopodobieństwa sukcesu w tej grze, gdyż wymaga ona zasobów sygnalizujących. Argument ten został rygorystycznie pokazany np. w [2]. Wraz ze zwiększaniem q Alicja ma dostęp do coraz większej ilości sygnalizujących zasobów, co pozwala jej częściej wygrywać w owej grze. Ważnym jest zauważyć, że macierz ta jest nieujemna $W^{A_1 A_2 B_1 B_2} \geq 0$ dla $0 \leq q \leq 1$, korzystając z tego protokołu łamie się przyczynową nierówność dla $q \geq \sqrt{2} - 1$, zaś proces jest nieseparowalny dla $q \geq q_0$, $q_0 \approx 0.365$. Separowalność przybliżono numerycznie. Wskazywać to może, że w tej grze i przy wykorzystaniu tej procedury niewystarczającym zasobem do złamania przyczynowych nierówności jest nieseparowalność (w tym przypadku może to być wina nieoptymalnej metody dla danego zasobu), lecz ilustruje fakt, iż niewystarczającym zasobem jest nieseparowalność, co zostanie rygorystycznie pokazane w następnym rozdziale.

3.1 Systemy n-wymiarowe

W celu rozważania systemów więcej wymiarowych konieczne jest wykorzystanie bazy dla systemów o odpowiednim wymiarze. Przykładowo bazą dla systemów 2^n poziomowych jest $\{\sigma_i\}^{\otimes n}$, gdzie σ_i to macierz Pauliego. W przypadku systemów o dowolnym wymiarze wygodnie jest skorzystać z bazy Hilberty-Schmidta dla macierzy n-wymiarowych. Przykładem takiej bazy są uogólnione macierze Gell-Manna, które między innymi zostały opisane w dodatku A. Przypadek, w którym ma się do czynienia

z systemami o m^n poziomach można traktować jako przypadek, w którym działa się na n systemach m poziomowych. Nierówność zaprezentowaną w poprzednim podrozdziale można próbować również badać przy pomocy procesów, w którym laboratoria otrzymują więcej, niż jeden kubit. Przykładowo biorąc macierz procesu jako:

$$W = \bigotimes_i^n \frac{1}{4} \left[\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}} (\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + \mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z}) \right], \quad (76)$$

który odpowiada n -krotnemu powieleniu skrajnego procesu opisanego w poprzednim podrozdziale. W takim procesie każde z laboratoriów otrzymuje n kubitów i wysyła je dalej po czym każdy kubit transportowany jest takim samym kanałem. Warto podkreślić, że założone jest, że laboratoria mogą wykonywać pomiary wyłącznie na poszczególnych kubitach i nie mają dostępu do korelacji wielosystemowych. Sfałszowana postać tego procesu zapewnia, że jest całkowicie dodatni przez co jest prawidłowym procesem. W celu zakodowania swojej wiadomości każde z laboratoriów wykonuje na każdym z kubitów operacje z poprzedniego rozdziału. Prawdopodobieństwo jest dane następująco:

$$\begin{aligned} \Pr(\mathbf{x}, \mathbf{y} | a, b, b') &= \frac{1}{4} \text{Tr} \left[\bigotimes_i^n \left[\left(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}} (\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + \mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z}) \right) \left(\xi(x_i, a) \otimes \eta(y_i, b, b') \right) \right] \right] \\ &= \frac{1}{4} \prod_i^n \text{Tr} \left[\left(\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}} (\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + \mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z}) \right) \left(\xi(x_i, a) \otimes \eta(y_i, b, b') \right) \right] \\ &= \prod_i^n \Pr(x_i, y_i | a, b, b'), \end{aligned} \quad (77)$$

gdzie $\mathbf{x} = (x_1, x_2, \dots, x_n)$, $\mathbf{y} = (y_1, y_2, \dots, y_n)$. Przypisując $x = 1$, gdy $\sum x_i \geq c_x$, $x = 0$,gdy $\sum x_i \leq d_x$ i $x = ?$ w przeciwnym wypadku (analogicznie dla y). Prawdopodobieństwo sukcesu można zapisać wtedy tak samo jak poprzednio, czyli:

$$\Pr_{\text{sukcesu}} = \frac{1}{2} [\Pr(x = b | b' = 0) + \Pr(y = a | b' = 1)]. \quad (78)$$

Można również sformułować prawdopodobieństwo sukcesu w przypadku, gdy strony mają możliwość zrezygnowania z zgadywania.

$$\Pr_{\text{sukces?}} = \frac{1}{2} [\Pr(x = b | b' = 0, x \neq ?) + \Pr(y = a | b' = 1, y \neq ?)]. \quad (79)$$

Przykładowo dla procesu, gdzie każde laboratorium otrzymuje trzy kubity i Alicja przypisuje $x = 1$, gdy $\sum_i^3 x_i \geq 2$, a $x = 0$ w przeciwnym wypadku (analogicznie dla Boba). Prawdopodobieństwo można wyliczyć jako:

$$\Pr_{\text{sukces}} = \Pr_{\text{sukces?}} \approx 0.941. \quad (80)$$

W przypadku przypisania, $x = ?$ dla $1 \leq \sum_{i=0}^2 x_i \leq 2$. Można otrzymać wynik:

$$\Pr_{\text{sukces?}} \approx 0.994. \quad (81)$$

W tym przypadku Alicja i Bob postanawiają zrezygnować ze zgadywania $\frac{11}{16}$ czasu. Powyższe wyniki są ewidentnie lepsze, niż przedstawione wcześniej. Sterując liczbą wysłanych systemów i porzucanych wyników można osiągnąć arbitralnie dobry wynik dla $\Pr_{\text{sukces?}}$, \Pr_{sukces} . Koniecznym jest podkreślenie faktu, że eksperyment, gdzie laboratoria mogą wybrać swój wynik na podstawie wielu pomiarów jest ograniczony inną wartością. W przypadku klasycznym również możliwe jest osiągnięcie dowolnych prawdopodobieństw sukcesu przy odpowiedniej dużej liczbie systemów.

3.2 Adnotacja

Sposób obliczenia:

$$\Pr_{\text{sukcesu}} = \frac{1}{2} \left(\frac{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'0} \delta_{xb}}{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'0}} + \frac{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'1} \delta_{ya}}{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'1}} \right) \quad (82)$$

$$\Pr_{\text{sukcesu}} = \frac{1}{2} \left(\frac{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'0} \delta_{xb} \delta_{x?0}}{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'0} \delta_{x?0}} + \frac{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'1} \delta_{ya} \delta_{x?0}}{\sum_{x_1 x_2 x_3 y_1 y_2 y_3 a b b' = 0} \Pr(x, y|a, b, b') \delta_{b'1} \delta_{x?0}} \right) \quad (83)$$

$$x? = \begin{cases} 0 & x \neq ? \\ 1 & x = ? \end{cases} \quad (84)$$

3.3 Procesy z przyczynowym modelem

Ważną klasę procesów pokazano w [9]. Jest to klasa procesów przyczynowo nieseparowalnych podlegająca przyczynowemu modelowi, czyli takie procesy, które są nieseparowalne, lecz produkują wyłącznie korelacje, które są zgodne z przyczynowym porządkiem. Procesy takie oczywiście nie mogą łamać przyczynowych nierówności niezależnie od przyjętej strategii. Przykładem takiego procesu jest

$$W^{A \prec B} := \mathbb{1}^\circ + \frac{1}{12}(\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + \mathbb{1}\mathbb{X}\mathbb{X}\mathbb{1} + \mathbb{1}\mathbb{Y}\mathbb{Y}\mathbb{1}) \quad (85)$$

$$W^{B \prec A} := \mathbb{1}^\circ + \frac{1}{4}(\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z}) \quad (86)$$

$$W := qW^{A \prec B} + (1 - q + \epsilon)W^{B \prec A} - \epsilon \mathbb{1}^\circ, \quad (87)$$

gdzie $\mathbb{1}^\circ = \frac{1}{d_{A_1} d_{B_1}} \mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}$. Zauważa się, że $W \geq 0$ dla $\epsilon \leq q - 1 + \sqrt{\frac{(1-q)(q+3)}{3}}$ i przyczynowo nieseparowalne dla $\epsilon \geq 0$. Dowód faktu, że ten proces nie może złamać żadnej przyczynowej nierówności niezależnie od strategii przebiega następująco. Pokazuje się najpierw, że proces ten produkuje te same korelacje co W^{T_B} , gdzie T_B oznacza częściową transpozycję systemów $\mathcal{H}^{B_1} \otimes \mathcal{H}^{B_2}$ względem CB. Natomiast W^{T_B} jest przyczynowo separowalna i nie może złamać przyczynowych nierówności. Co razem dowodzi tezę. Pierwsza część dowodu przebiega następująco

$$\begin{aligned} \Pr(x, y|a, b) &= \text{Tr} [W^{T_B} \xi(x, a) \otimes \eta(y, b)^T] \\ &= \sum_{\mu\nu\lambda\gamma} w_{\mu\nu\lambda\gamma} \text{Tr} [(\sigma_\mu^{A_1} \otimes \sigma_\nu^{A_2}) \otimes (\sigma_\lambda^{B_1} \otimes \sigma_\gamma^{B_2})^T \xi(x, a) \otimes \eta(y, b)^T] \\ &= \sum_{\mu\nu\lambda\gamma} w_{\mu\nu\lambda\gamma} \text{Tr} [(\sigma_\mu^{A_1} \otimes \sigma_\nu^{A_2}) \xi(x, a) \otimes (\sigma_\lambda^{B_1} \otimes \sigma_\gamma^{B_2})^T \eta(y, b)^T] \\ &= \sum_{\mu\nu\lambda\gamma} w_{\mu\nu\lambda\gamma} \text{Tr} [(\sigma_\mu^{A_1} \otimes \sigma_\nu^{A_2}) \xi(x, a)] \text{Tr} [(\sigma_\lambda^{B_1} \otimes \sigma_\gamma^{B_2})^T \eta(y, b)^T] \\ &= \sum_{\mu\nu\lambda\gamma} w_{\mu\nu\lambda\gamma} \text{Tr} [(\sigma_\mu^{A_1} \otimes \sigma_\nu^{A_2}) \xi(x, a)] \text{Tr} [(\sigma_\lambda^{B_1} \otimes \sigma_\gamma^{B_2}) \eta(y, b)] \\ &= \text{Tr} [W \xi(x, a) \otimes \eta(y, b)] \end{aligned} \quad (88)$$

Ta równość jest spełniona nawet wtedy, gdy $W^{T_B} \leq 0$, czyli opisuje niefizyczna macierz procesu, taki proces generuje dodatnie prawdopodobieństwo dla lokalnych pomiarów, lecz może generować ujemne prawdopodobieństwa, gdy laboratoria dzielą splątane cząsteczki, takie rozszerzenie jest istotne fizycznie. Trzeba zauważyć, że dla każdego kwantowego instrumentu $\{\eta(y, b)\}$, instrument $\{\eta(y, b)^T\}$ również jest

prawidłowy, jako że transpozycja transformuje odwzorowania CP do odwzorowań CP i mapy zachowujące ślad (*trace preserving*, TP) do map zachowujących ślad. Następnie pokazuje się w sposób jawny przyczynową separację W^{T_B} . Widać, że

$$\left[\mathbb{1}^\circ + \frac{1}{12} (\mathbb{1}ZZ\mathbb{1} + \mathbb{1}XX\mathbb{1} + \mathbb{1}YY\mathbb{1}) \right]^{T_B} = \mathbb{1}^\circ + \frac{1}{12} \mathbb{1}ZZ\mathbb{1} + \mathbb{1}XX\mathbb{1} - \mathbb{1}YY\mathbb{1}, \quad (89)$$

po prawej stronie nierówności można rozpoznać macierz procesu opisujący kanał depolaryzacyjny, krótko opisany we wstępie, z prawdopodobieństwem $\frac{2}{3}$ depolaryzacji oraz $\frac{1}{3}$ idealnej transmisji systemu. Z definicji procesu depolaryzacyjnego pisze się

$$D_{\frac{2}{3}}^{A \prec B} = \frac{2}{3} \mathbb{1}^\circ + \frac{1}{3} I^{A \prec B} \quad (90)$$

$$I^{A \prec B} = \frac{\mathbb{1}|I\rangle\rangle\langle\langle I|\mathbb{1}}{2}. \quad (91)$$

Dodając do tego $(W^{B \prec A})^{T_B} = W^{B \prec A}$ wynika, że

$$\begin{aligned} W^{T_B} &= \frac{2q}{3} \mathbb{1}^\circ + \frac{q}{3} I^{A \prec B} + (1 - q + \epsilon) W^{B \prec A} - \epsilon \mathbb{1}^\circ \\ &= \frac{q}{3} I^{A \prec B} + (1 - q + \epsilon) W^{B \prec A} - \left(\frac{2q}{3} - \epsilon \right) \mathbb{1}^\circ, \end{aligned} \quad (92)$$

co jest kombinacją wypukłą procesów uporządkowanych przyczynowo tak długo jak $\epsilon < \frac{2q}{3}$ można jednakże sprawdzić, że $q - 1 + \sqrt{\frac{(1-q)(3+q)}{3}} \leq \frac{2q}{3}$ więc poprzedni warunek jest zawsze spełniony, co kończy dowód, pokazano, że każdy prawidłowy proces (87) ma przyczynowy model. Autorzy [9] sugerują, żeby wziąć rozkład na kombinacje wypukłe W jako transpozycje względem systemu Boba równania (92). Można dalej zauważyć, że wyraz $\frac{q}{3} (I^{A \prec B})^{T_B}$ stanie się nieujemny, gdy doda się do niego $\frac{2q}{3}$ białego szumu, a ilość dostępnego szumu, który można zabrać z wyrazu $(\frac{2q}{3} - \epsilon) \mathbb{1}^\circ$ jest ostro mniejszy od wymaganego. Narzuca się interpretacja, że proces W jest kombinacją wypukłą niefizycznego kanału od Alicji do Boba i fizycznego kanału od Boba do Alicji, co może być wskazówką, że proces W jest nieimplementowalny fizycznie. Powyższy dowód opiera się na fakcie, że odwzorowania poddane częściowej transpozycji według odpowiedniego systemu są nadal poprawnymi odwzorowaniami CP. Może to być jednak nieprawdziwe, gdy systemy są poszerzone o splątane cząsteczki. Częściowa transpozycja nie jest wtedy pełną transpozycją względem danych systemów, czyli może transformować odwzorowania CP na odwzorowania nie CP. Procesy takie, które nie łamią przyczynowych nierówności, a łamią je gdy zostaną rozszerzone o splątany system w odpowiednich laboratoriach, nazywa się rozszerzenie nieprzyczynowymi (*not extensively causal*), o których można przeczytać więcej w [9].

4 Świadek przyczynowości

Poprzedni rozdział sugeruje, że istnieje klasa procesów, która nie może złamać żadnej przyczynowej nierówności, zaś jest nieseparowalna przyczynowo. Istnieje więc motywacja do poszukiwania metody, która sklasyfikuje, czy dany stan jest separowalny czy nie. Wprowadzony w [3] świadek przyczynowości (*causal witness*) jest analogiem do świadka splątania (*entanglement witness*), który pozwala klasyfikować splątanie danego układu niezależnie od jego zdolności do łamania nierówności Bella. Ściśle mówiąc świadek przyczynowości to taki operator S , że

$$\text{Tr}[SW^{sep}] \geq 0 \quad (93)$$

dla każdego przyczynowo separowalnego procesu W^{sep} . Taka definicja jest zmotywowana twierdzeniem o separującej hiperpłaszczyźnie, które mówi, że dla każdych dwóch wypukłych zbiorów albo ich przecięcie nie jest zbiorem pustym, albo istnieje taka hiperpłaszczyzna, że zbiory leżą po obu jej stronach,

nierygorystycznie mówiąc. Można to łatwo sobie zobrazować geometrycznie. Jako że zbiór macierzy separowalnych jest wypukły i zamknięty dla każdego nieseparowalnego procesu W^{nsep} , to istnieje taki świadek przyczynowości, że

$$\text{Tr} [S_{W^{nsep}} W^{nsep}] < 0. \quad (94)$$

4.1 Sformułowanie macierzy procesu niezależne od bazy

Przed dalszym charakteryzowaniem świadków przyczynowości wygodnie jest wprowadzić niezależne od wyboru bazy sformułowanie macierzy procesu. Definiuje się następującą operację:

$${}_X W = \frac{\mathbb{1}^X}{d_X} \otimes \text{Tr}_X W, \quad (95)$$

która opisuje operację wzięcia śladu i zastąpienia tego systemu znormalizowaną macierzą jednostkową. Warunki wprowadzone w rozdziale 2 są równoważne z następującymi

$$W \geq 0 \quad (96)$$

$$\text{Tr} W = d_O \quad (97)$$

$$W = L_V(W), \quad (98)$$

gdzie $d_0 = d_{A_2} d_{B_2} \dots$ jest iloczynem wymiaru wszystkich systemów wyjściowych, a L_V jest projektorem, zdefiniowanym w [3], na pewną podprzestrzeń $\mathcal{L}_V \subset \mathcal{H}^{A_1} \otimes \mathcal{H}^{A_2} \otimes \mathcal{H}^{B_1} \otimes \mathcal{H}^{B_2} \dots$. W sposób jawny projektor dla przypadku dwustronnego L_V wyraża się następująco:

$$L_V(W) = {}_{A_2} W + {}_{B_2} W - {}_{A_2 B_2} W - {}_{B_1 B_2} W + {}_{A_2 B_1 B_2} W - {}_{A_1 A_2} W + {}_{A_1 A_2 B_2} W. \quad (99)$$

Warto tutaj porównać powyższe równanie do poprzedniego sformułowania macierzy procesu. Zauważa się, że w przypadku wybranej bazy Hilberta-Schmidta operacja

$${}_X [\sigma_\mu^X \otimes \sigma_\nu^Y] = \delta_{\mu 0}. \quad (100)$$

Należy przypomnieć, że $\sigma_0 = \mathbb{1}$. Wynika to oczywiście z faktu, że reszta wyrazów jest bezśladowa i $\frac{\text{Tr} \mathbb{1}^X}{d_X} = 1$. Co daje następującą interpretację dla wyrazów występujących w (99): są to wyrazy zakazane w tym formalizmie, lub bardziej precyzyjnie dany projektor implikuje układ równań liniowych narzucających warunki na współczynniki występujące przy danych macierzach bazowych. Zważywszy na fakt, że jawna postać projektora dla n stron została wyprowadzona w oryginalnym artykule, łatwym zadaniem jest wyprowadzenie warunków na współczynniki przy owych bazach. Dla oswojenia się z powyższym projektorem można sprawdzić spełnianie $W = L_V(W)$ przez macierz procesu wprowadzoną w poprzednim

rozdziale:

$$W = \frac{1}{4} \left[\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}}(\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + q\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z} + \frac{(1-q)}{2}\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{1}) \right], \quad 0 \leq q \leq 1. \quad (101)$$

$$A_2 W = \frac{1}{4} \left[\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}}(q\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{Z} + \frac{(1-q)}{2}\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{1}) \right] \quad (102)$$

$$B_2 W = \frac{1}{4} \left[\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}}(\mathbb{1}\mathbb{Z}\mathbb{Z}\mathbb{1} + \frac{(1-q)}{2}\mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{1}) \right] \quad (103)$$

$$A_2 B_2 W = \frac{1}{4} \left[\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1} + \frac{1}{\sqrt{2}} \frac{(1-q)}{2} \mathbb{Z}\mathbb{1}\mathbb{X}\mathbb{1} \right] \quad (104)$$

$$B_1 B_2 W = \frac{1}{4} [\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}] \quad (105)$$

$$A_2 B_1 B_2 W = \frac{1}{4} [\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}] \quad (106)$$

$$A_1 A_2 W = \frac{1}{4} [\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}] \quad (107)$$

$$A_1 A_2 B_2 W = \frac{1}{4} [\mathbb{1}\mathbb{1}\mathbb{1}\mathbb{1}] \quad (108)$$

$$W = L_V(W). \quad (109)$$

W poprzednich obliczeniach korzystano z faktu, że wyłącznie $\mathbb{1}$ jest jedynym elementem bazy Hilberta-Schmidta o niezerowym śladzie, konsekwencją tego jest to, że operator X działający na macierz jednostkową na danej pozycji dokonuje trywialnej zmiany, zaś w przeciwnym wypadku usuwa dany wyraz.

4.2 Poszukiwanie świadka przyczynowości

Zauważa się, że warunek (93) jest równoważny z następującymi dwoma

$$\text{Tr} [W^{A \prec B} S] \geq 0 \quad (110)$$

$$\text{Tr} [W^{B \prec A} S] \geq 0. \quad (111)$$

Oczywiście powyższe równania wynikają z definicji stanów separowalnych, jako kombinacji wypukłej macierzy o określonej przyczynowości i liniowości śladu. Łatwo można zaobserwować, że pozbywając się wyrazów zawierających wyrazy typu $\dots B_2$ usuwamy korelacje wyjścia Boba z pomiarami Alicji co implikuje, że $A \prec B$. Piszę się, że:

$$B_2 W = W^{A \prec B}, \quad (112)$$

lub analogicznie

$$A_2 W = W^{B \prec A}. \quad (113)$$

Wykorzystując powyższą zależność, równanie (111) możemy zapisać następująco:

$$\text{Tr} [A_2 W S] \geq 0 \quad (114)$$

Traktując ślad jako iloczyn skalarny $\langle MS \rangle = \text{Tr} MS$ oraz zauważając, że X jest operatorem samosprężonym równoważne z powyższym równaniem jest:

$$\text{Tr} [W_{A_2} S] \geq 0. \quad (115)$$

Dla prawidłowych macierzy procesu wystarczającym dla S do bycia świadkiem przyczynowości jest

$$A_2 S \geq 0 \quad (116)$$

$$B_2 S \geq 0. \quad (117)$$

Zauważa się dodatkowo dowolność dodania dowolnego elementu S^\perp z przestrzeni ortogonalnej do \mathcal{L}_V , który nie zmieni wartości 93, a mianowicie

$$\text{Tr} [W (S + S^\perp)] = \text{Tr} [WS] \quad (118)$$

Okazuje się, że powyższe warunki charakteryzują wszystkich świadków przyczynowości. Co zbierając razem daje:

Macierz hermitowska S jest świadkiem przyczynowości wtedy i tylko wtedy, gdy da się ją zapisać jako

$$S = S_P + S^\perp \quad (120)$$

gdzie S_P i S^\perp są takimi macierzami hermitowskimi, że

$$A_2 S_P \geq 0, B_2 S_P \geq 0, L_V(S^\perp) = 0. \quad (122)$$

Pokazuje się, że zbiór tak zdefiniowanych świadków przyczynowości jest domkniętym stożkiem wypukłym. Można jednak ograniczyć się z S do przestrzeni \mathcal{L}_V . Wybierając $S^\perp = L_V(S_P) - S_P$, który może być dowolny. Mamy $L_V(S) = S$. Okazuje się, że taki ograniczony zbiór świadków przyczynowości: $\mathcal{S}_V = \mathcal{S} \cap \mathcal{L}_V$, również jest domkniętym wypukłym stożkiem. Jako, że wybrane elementy ortogonalne do \mathcal{L}_V nie zmieniają wartości $\text{Tr} WS$, nie zmieniają one też dlatego zdolności S do wykrywania separowalności. Dostając pewną macierz W i chcąc zbadać, czy jest ona separowalna, można spróbować znaleźć minimalną wartość $\text{Tr} WS$. W przypadku możliwości znalezienia minimum globalnego takiego wyrażenia widzimy, że jeżeli nie uda nam się znaleźć takiego S , że $\text{Tr} WS < 0$ oznacza to, że nie istnieje taka hiperpłaszczyzna oddzielająca procesy separowalne, więc ten proces też jest separowalny. W przeciwnym wypadku proces jest nieseparowalny. W celu ograniczenia od dołu skończoną wartością, by możliwe było rozwiązanie problemu numerycznie, na $\text{Tr} SW$ należy narzucić pewien dowolny warunek normujący. Autorzy oryginalnego artykułu proponują następujący:

$$\text{Tr} \Omega S \leq 1, \quad (123)$$

gdzie Ω jest znormalizowaną macierzą procesu. Poszerzając powyższy warunek do nieznormalizowanych macierzy procesu, dostaje się

$$\text{Tr} \Omega S \leq \frac{\text{Tr} \Omega}{d_O} \quad (124)$$

Co można przepisać, jako

$$\text{Tr} \left[\Omega \left(\frac{\mathbb{1}}{d_O} - S \right) \right] \geq 0 \quad (125)$$

Łatwo zauważyć, że powyższy warunek jest warunkiem, który muszą spełniać operatory $\frac{\mathbb{1}}{d_O} - S$, by należały do stożka dualnego macierzy procesu, czyli takiego, że ich iloczyn skalarny jest nieujemny z macierzami procesu. Co sprowadza problem optymalizacyjny do:

$$\min \text{Tr} [WS] \quad (126)$$

$$\text{tak, aby } S \in \mathcal{S}_V, \quad \frac{\mathbb{1}}{d_O} - S \in \mathcal{W}_V^*, \quad (127)$$

gdzie $\mathcal{W}_V^* := \mathcal{W}^* \cap \mathcal{L}_V$. \mathcal{W}^* jest wcześniej wspomnianym stożkiem dualnym do macierzy procesu, zaś człon \mathcal{L}_V wynika z wcześniej narzuconego warunku na $S \in \mathcal{L}_V$. Problem ten okazuje się być prawidłowym problemem programowania liniowego po stożku (*semidefinite programming*, SDP), którego numeryczne rozwiązanie jest zbieżne do optimum globalnego. Wynika z tego, że rozwiązanie takiego problemu optymalizacyjnego daje kryterium separowalności przyczynowej. Okazuje się dodatkowo, że wartość $-\text{Tr} [WS^*]$ odpowiada minimalnej wartości λ takiej, że

$$\frac{1}{1 + \lambda} (W + \lambda \tilde{\Omega}), \quad (128)$$

zoptymalizowanej po wszystkich znormalizowanych macierzach procesu $\tilde{\Omega}$. Wartość ta określa odporność danego procesu do pozostania nieseparowalnym podczas mieszania z "najgorszym" możliwym szumem. $-\text{Tr}[WS^*]$ nazywa się, analogicznie do podobnej wartości związanej ze splątaniem, uogólnioną wytrzymałością (*generalized robustness*), i oznacza się ją

$$R_g(W) = -\text{Tr}[S^*W] \quad (129)$$

Jest to miara nieseparowalności spełniająca standardowe wymagania, a mianowicie

Dyskryminacja $R_g(W) \geq 0$ dla każdej macierzy procesu, przyjmuje wartość 0 wyłącznie dla procesów należących do \mathcal{W}^{sep} .

Wypukłość $R_g(\sum_i p_i W_i) \leq \sum_i p_i R_g(W_i)$ dla dowolnych macierzy procesu i $p_i \geq 0$ takich, że $\sum_i p_i = 1$.

Monotoniczność ze względu na lokalne operacje $R_g(\$ (W)) \leq R_g(W)$, gdzie $\$(W)$ jest dowolnym procesem, który można otrzymać przez złożenie go z lokalnymi odwzorowaniami CPTP.

Można wprowadzić również problem, w którym poszukuje się minimalnej ilości białego szumu potrzebnego do spowodowania, by proces stał się separowalnym. Biały szum może się okazać bardziej adekwatnym modelem szumu niż przypadek pesymistyczny. Problem optymalizacyjny, który otrzymuje się jest następujący

$$\min \text{Tr}[WS] \quad (130)$$

$$\text{tak, by } S \in \mathcal{S}_{\mathcal{V}}, \text{Tr}[\mathbb{1}^\circ S] \leq 1. \quad (131)$$

Wprowadza się wtedy wielkość nazywaną losowa wytrzymałość (*random robustness*), która jest powiązana z S^* - optimum powyższego problemu - w następujący sposób.

$$R_r(W) = -\text{Tr}[S^*W] \quad (132)$$

W przeciwieństwie do uogólnionej wytrzymałości nie jest to miara nieseparowalności, w sensie poprzednio przytoczonych postulatów, jako że nie jest monotoniczna pod działaniem lokalnych odwzorowań CPTP.

4.3 Implementacja świadka przyczynowości

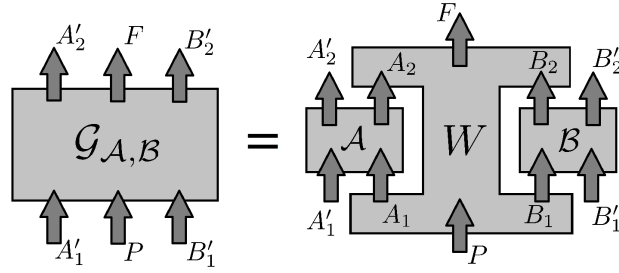
Korzystając chociażby z twierdzenia spektralnego wiadomym jest, że macierz hermitowską S można zapisać jako kombinację liniową następującej postaci

$$S = \sum_{i,j} \gamma_{i,j} \sigma_i^{A_1 A_2} \otimes \sigma_j^{B_1 B_2}, \quad (133)$$

gdzie macierze $\sigma \geq 0$. Dodatkowo w $\gamma_{i,j}$ można dodać stałą skalującą tak, aby $\text{Tr}_{A_2} \sigma_i \leq \mathbb{1}^{A_1}$, $\text{Tr}_{B_2} \sigma_j \leq \mathbb{1}^{B_1}$. Co więcej można dodać do S macierz $\sigma_0^{A_1 A_2} \otimes \sigma_0^{B_1 B_2}$ o zerowej stałej, która nie zmienia wartości S , tak aby $\sum_i \text{Tr}_{A_2} \sigma_i^{A_1 A_2} = \mathbb{1}^{A_1}$ i analogicznie dla strony Boba. Wtedy można traktować macierze $\sigma_i^{A_1 A_2}$, $\sigma_j^{B_1 B_2}$ jako reprezentacje CJ pewnego instrumentu kwantowego, więc wielkość

$$\text{Tr}[WS] = \sum_{i,j} \gamma_{i,j} \text{Tr}[W \sigma_i^{A_1 A_2} \otimes \sigma_j^{B_1 B_2}], \quad (134)$$

gdzie wartość po prawej stronie równania jest oczywiście prawdopodobieństwem zaobserwowania danych odwzorowań, wielkość tę można oszacować eksperymentalnie. Warto również przypomnieć, że do S można dodać dowolny element z przestrzeni ortogonalnej do przestrzeni $\mathcal{L}_{\mathcal{V}}$, co nie zmienia wartości oczekiwanej świadka, a może skutkować w łatwiejszego do implementacji fizycznie odwzorowania.



Rysunek 6: Rysunek symbolizuje działanie procesu W jako funkcje wyższego rzędu odwzorowań \mathcal{A} i \mathcal{B} , która dla danych odwzorowań zwraca odwzorowanie $\mathcal{G}_{\mathcal{A},\mathcal{B}}$ reprezentującą transformację, która przechodzi z globalnej przeszłości do globalnej przyszłości.

5 Postulat puryfikacyjny

Ważnym aktualnie nierozwiązanym problemem występującym w tym formalizmie jest brak jasnego kryterium, które stwierdzałoby, które procesy są możliwe do zrealizowania fizycznie. Nie wiadomo, czy łamanie nierówności przyczynowych jest możliwe fizycznie, czy wyłącznie jest matematycznym artefaktem. Jasne jednakże jest, że występowanie nieseparowalności jest fizycznie występującym fenomenem, który został potwierdzony doświadczalnie przy realizacji tzw. kwantowego przełącznika (*quantum switch*)-zasobu, który nie może złamać przyczynowych nierówności - wykorzystując wcześniej opisanego świadka przyczynowości np. w [24]. Może to nasuwać postulat, że fizycznie niemożliwe jest naruszenie tych nierówności. Prawdziwość tego postulatu wciąż stoi pod znakiem zapytania. W [4] autorzy proponują postulat puryfikacyjny (*purification postulate*). Uznają za konieczne, że każda fundamentalna fizycznie poprawna teoria musi być odwracalna. Motywują się faktem, że każda znana fundamentalna teoria jest odwracalna - taka intuicja sprawdza się do tej pory. Warto jeszcze dodać, że we wstępie zostały opisany pomiar rzutu jako nieodwracalny rodzaj ewolucji, jednakże można modelować pomiar w sposób niewymagający takich pomiarów modelując układ pomiarowy, jako system kwantowy, który ewoluuje unitarnie wraz z mierzonym systemem, co pokazano np. w [20]. W celu dalszego opisu postulatu koniecznym jest opisanie, jak rozumiana jest odwracalność w kontekście procesów. W tym celu procesy są poszerzone o globalną przeszłość i globalną przyszłość. Rozumie się je jako operacje, które odwzorowują stany w globalnej przeszłości do stanów w globalnej przyszłości, które przechodzą przez region o nieokreślonej przyczynowości lokalnych laboratoriów opisywanych właśnie przez te macierze. Co sprowadza do definicji czystych procesów (*pure processes*), jako procesów, które w sposób unitarny transformują przyszłość do przeszłości, gdy w lokalnych laboratoriach zostaną zaaplikowane odpowiednie unitarne transformacje. Ta definicja sprowadza do ich postulatu, który mówi, że procesy są puryfikowalne wtedy i tylko wtedy, gdy da się zaprezentować je jako czyste procesy w większej przestrzeni i tylko takie procesy są implementowalne. Autorzy postulatu dodatkowo zauważają, że o ile żaden znany dwustronny proces łamiący nierówności przyczynowe nie okazał się być puryfikowalnym, to istnieje proces trzystronny, który jest puryfikowalny i może łamać przyczynowe nierówności, więc jeżeli niemożność łamania przyczynowych nierówności uznaliby się za prawo natury, a ten postulat za prawdziwy, to byłby on konieczny, a nie wystarczający. We wcześniejszych rozdziałach proces był definiowany jako zasób, który definiował wszystkie statystyki pomiarów dla danych instrumentów, lub równoważnie jako funkcja, która transformuje odwzorowania CP do prawdopodobieństw. Wprowadzenie pojęcia puryfikacji wymaga zmiany definicji na biliniową funkcję działającą trywialnie na *ancille*, która odwzoruje \mathcal{A} i \mathcal{B} do $\mathcal{G}_{\mathcal{A},\mathcal{B}}$, gdzie \mathcal{A} jest odwzorowanie CPTP z A_1, A'_1 do A_2, A'_2 , analogicznie \mathcal{B} jest mapą CPTP z B_1, B'_1 do B_2, B'_2 , zaś $\mathcal{G}_{\mathcal{A},\mathcal{B}}$ mapą CPTP z P, A'_1, A'_2

do F, B'_1, B'_2 . Primem oznaczono *ancille*. Ponownie przez A niepisane kaligraficznie oznaczać będzie się reprezentacje CJ odpowiednich map, podobnie dla innych map. Taka definicja nie jest w żaden sposób sprzeczna z tymi podanymi wcześniej, gdyż ma ona służyć jedynie jako droga do zbudowania narzędzia stwierdzającego, czy dany proces jest fizyczny bądź nie. Trzeba zaznaczyć, iż w tym rozdziale definicja izomorfizmu CJ jest zmieniona o transpozycję, która wcześniej została wprowadzona ze względu na wygodę, teraz jednakże może sprawiać, że pewne odwzorowania CP mogą zostać mapowane na macierze niedodatnie. Jako że żadna przestrzeń nie może sygnalizować P , a przestrzeń F nie może sygnalizować do żadnej innej, można je interpretować odpowiednio jako globalną przeszłość i globalną przyszłość. Oczywiście tak zdefiniowany proces ma swoją reprezentację jako macierz - pisze się

$$G_{A,B} = \text{Tr}_{A_1 A_2 B_1 B_2} [W^{T_{A_1 A_2 B_1 B_2}} (A \otimes B)] \quad (135)$$

gdzie $W \in A_1 \otimes A_2 \otimes A'_1 \otimes A'_2 \otimes B_1 \otimes B_2 \otimes B'_1 \otimes B'_2 \otimes F \otimes P$ jest oczywiście definiowaną macierzą procesu. W powyższym równaniu macierze jednostkowe na *ancillach*, globalnej przyszłości i przeszłości pozostały niejawne. Równanie (135) może być skrócone z wykorzystaniem iloczynu łączącego (*link product*). W celu zapisania postaci CJ złożenia pewnych dwóch funkcji można obliczyć jawną postać CJ $\mathfrak{C}(\mathcal{M} \circ \mathcal{N})$. Wygodniejszym jednak często okazuje się być wcześniej wspomniany iloczyn łączący definiowany jako następująca abstrakcyjna operacja na macierzach:

$$N * M = \text{Tr}_{I \cap J} \left[(\mathbb{1}^{J \setminus I} \otimes M^{T_{I \cap J}})(N \otimes \mathbb{1}^{I \setminus J}) \right], \quad (136)$$

gdzie $M \in \bigotimes_{i \in I} A^i$, $N \in \bigotimes_{j \in J} A^j$. W skrajnych przypadkach gdy $I \cap J = \emptyset$, $N * M$ to po prostu $N \otimes M$, a gdy $I \cap J = I = J$ to $N * M = \text{Tr} M^T N$. Ułatwić zaobserwowanie działania iloczynu łączącego w przypadkach bardziej skomplikowanych pozwala następujący przykład:

$$\begin{aligned} \mathbb{1} \mathbb{X} \mathbb{Y}^{ABC} * \mathbb{Y} \mathbb{Y} \mathbb{Z}^{BCD} &= \text{Tr}_{BC} \left[\left(\mathbb{1}^A \otimes \mathbb{Y} \mathbb{Y} \mathbb{Z}^{BCD T_{BC}} \right) (\mathbb{1} \mathbb{X} \mathbb{Y}^{ABC} \otimes \mathbb{1}^D) \right] \\ &= \text{Tr}_{BC} [\mathbb{1}^A \otimes (-Y X)^B \otimes -Y Y^C \otimes Z^D] \\ &= \mathbb{1}^A \otimes Z^D \text{Tr}_B [-Y X] \text{Tr}_C [-Y Y] \\ &= \mathbb{1}^A \otimes Z^D 0 \cdot -1 \\ &= 0 \end{aligned} \quad (137)$$

Znając iloczyn łączący w sposób bardzo elegancki można zdefiniować dwustronny proces jako

$$G_{A,B} = W * (A \otimes B). \quad (138)$$

W celu uniknięcia sprzeczności trzeba narzucić warunki na W tak, aby $G_{A,B}$ była odwzorowaniem CPTP dla wszystkich prawidłowych odwzorowań CPTP A i B , co implikuje analogiczne warunki do tych podanych we wcześniejszych rozdziałach

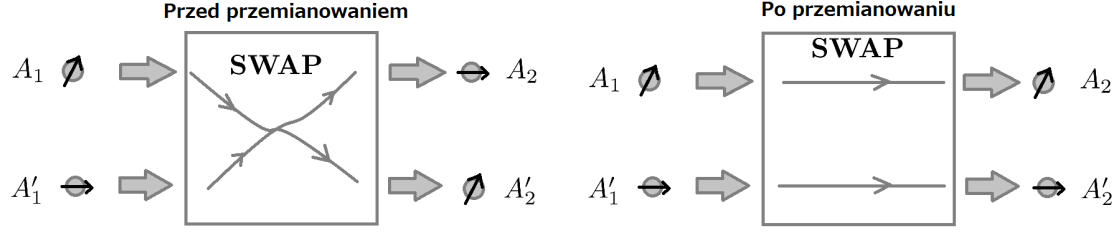
$$W \geq 0 \quad (139)$$

$$\text{Tr} W = d_{A_2} d_{B_2} d_P \quad (140)$$

$$W = L_V(W). \quad (141)$$

Jawna postać powyższego projektora jest następująca:

$$\begin{aligned} L_V(W) &= W - {}_F W + {}_{A_2 F} W + {}_{B_2} W - {}_{A_2 B_2 F} W \\ &\quad - {}_{A_1 A_2 F} W + {}_{A_1 A_2 B_2 F} W - {}_{B_1 B_2 F} W \\ &\quad + {}_{A_2 B_1 B_2 F} W - {}_{A_1 A_2 B_1 B_2 F} W + {}_{P A_1 A_2 B_1 B_2 F} W. \end{aligned} \quad (142)$$



Rysunek 7: Rysunek schematycznie przedstawia działanie operacji **SWAP**. Na wejściu Alicja otrzymuje system złożony np. w stanie $\rho^{A_1} \otimes \rho^{A'_1}$ następnie aplikuje unitarną macierz **SWAP** definiowaną następująco $\mathbf{SWAP} = \sum_{ij} |ij\rangle\langle ji|$, a na wyjściu otrzymuje system w stanie $\rho^{A_2} \otimes \rho^{A'_2}$. Postać CJ tej macierzy to: $|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{A_1 A'_2} \otimes |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{A'_1 A_2}$. Warto również zauważyć, że po przemianowaniu systemów wyjściowych $A_2 \rightarrow A'_2, A'_2 \rightarrow A_2$ operacja **SWAP** działa trywialnie.

Ważnym spostrzeżeniem jest fakt, który przekonuje do słuszności poprzedniej definicji macierzy procesu, definiując $W' = {}_P F W$ i korzystając z faktu, że ${}_X X W = {}_X W$, po elementarnych przekształceniach otrzymuje się, że

$$L_V(W') = {}_{A_2} W' + {}_{B_2} W' - {}_{A_2 B_2} W' - {}_{B_1 B_2} W' + {}_{A_2 B_1 B_2} W' - {}_{A_1 A_2} W' + {}_{A_1 A_2 B_2} W'. \quad (143)$$

Powyższy projektor ma takie same wyrazy, jak ten zdefiniowany w (99). Każdy dwustronny proces zdefiniowany w poprzednim sensie rozszerzony o odpowiednio znormalizowaną jednostkową przyszłość i przeszłość spełnia warunki narzucone powyżej, co pokazuje, że każdy proces dwustronny, definiowany jak poprzednio, jest zgodny z tą definicją.

5.1 Czysty proces

Proces czysty definiuje się jako macierz, którą można zapisać w następującej postaci

$$W_{\text{czysty}} = |U_W\rangle\rangle\langle\langle U_W|, \quad (144)$$

dla pewnej transformacji unitarnej U_W . Faktem jest, że czysty proces odwzorowuje unitarne odwzorowania A i B na macierz unitarną. Szkic dowodu przebiega następująco, wybierając \mathcal{A}, \mathcal{B} , jako operacje **SWAP** (rysunek 7), które odpowiednio zamieniają *ancille* z oryginalnymi systemami, to pisze się, że

$$G_{A,B} = W * \left(|\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{A'_1 A_2} |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{A_1 A'_2} \otimes |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{B'_1 B_2} |\mathbb{1}\rangle\rangle\langle\langle\mathbb{1}|^{B_1 B'_2} \right) = W, \quad (145)$$

gdzie po prawej stronie równania przemianowano nazwy odpowiednich przestrzeni. Przekształcenie te ilustrują istnienie odwzorowań, które są przekształcane w macierz unitarną. W ogólności:

$$W = |U_W\rangle\rangle\langle\langle U_W| \quad (146)$$

$$A = |U_A\rangle\rangle\langle\langle U_A| \quad (147)$$

$$B = |U_B\rangle\rangle\langle\langle U_B|. \quad (148)$$

Następnie

$$G_{A,B} = |U_W\rangle\rangle\langle\langle U_W| * (|U_A\rangle\rangle\langle\langle U_A| \otimes |U_B\rangle\rangle\langle\langle U_B|) = |U_G\rangle\rangle\langle\langle U_G|, \quad (149)$$

gdzie

$$U_G^{A'_1 B'_1 P} = \text{Tr}_{A_1 B_1} \left[\left(U_W^{P A_1 B_1} \otimes \mathbb{1}^{A'_1 B'_1} \right) \left(\mathbb{1}^P \otimes U_A^{A_1 A'_1} \otimes U_B^{B_1 B'_1} \right) \right] \quad (150)$$

Z założenia mamy, że $\mathcal{G}_{A,B}$ jest CPTP, więc $\text{Tr}_{A'_2 B'_2 F} G_{A,B} = \mathbb{1}^{A'_1 B'_1 P}$. Podstawiając tu $|U_G\rangle\rangle\langle\langle U_G|$ dostaje się

$$\text{Tr}_{A'_2 B'_2 F} |U_G\rangle\rangle\langle\langle U_G| = U_G^\dagger U_G = \mathbb{1}^{A'_1 B'_1 P}, \quad (151)$$

co kończy dowód.

5.2 Proces puryfikowalny

Proces puryfikowalny W definiuje się jako proces dla, którego można znaleźć proces czysty S spełniający następującą równość:

$$W^{A_1 A_2 A'_1 A'_2 B_1 B_2 B'_1 B'_2} = S^{A_1 A_2 A'_1 A'_2 B_1 B_2 B'_1 B'_2 P F} * (|0\rangle\langle 0|^P \otimes \mathbb{1}^F), \quad (152)$$

Definicja ta jest zgodna tylko z tymi macierzami procesu, które można odzyskać z procesu czystego, gdy w globalnej przeszłości umieści się ustalony stan i wykona się ślad częściowy po globalnej przeszłości. Odpowiada to sytuacji, w której nie obserwuje się globalnej przeszłości i przyszłości. Postuluje się, że wyłącznie procesy czyste można skonstruować fizycznie, gdyby było inaczej zachwiana byłaby zasada odwracalności, która jest uznawana za kluczową.

5.3 Warunki konieczne i wystarczające

Warunkami koniecznymi i wystarczającymi, by proces był czysty są:

$$\begin{aligned} \forall i, j \quad L_V^\perp (|w_i\rangle\langle w_j|) &= 0 \\ \langle w_i | |w_j\rangle &= d_{A_2} d_{B_2} \delta_{ij} \\ L_V^\perp &= \mathbb{1} - L_V \\ |w_\psi\rangle &:= \langle \psi^* |^P |U_S\rangle. \end{aligned} \quad (153)$$

W celu wyprowadzenia powyższych zależności na początku zauważa się, że:

$$|U_S\rangle\rangle\langle\langle U_S| * (|\psi\rangle\langle\psi|^P \otimes \mathbb{1}^F) = |w_\psi\rangle\langle w_\psi| * \mathbb{1}^F = \text{Tr}_F |w_\psi\rangle\langle w_\psi| \quad (154)$$

Równanie (??) zapisuje się

$$W = \text{Tr}_F |w_0\rangle\langle w_0|, \quad (155)$$

gdzie $|w_0\rangle$ oznacza $\langle 0|^P |U_S\rangle\rangle$. Wcześniej narzucano, by S mapowało A i B na inną prawidłowe odwzorowanie CPTP. Ten warunek można zreformułować w jawny sposób przy pomocy stanów $|\psi\rangle$. S jest prawidłowym procesem, kiedy $[S * (A \otimes B)] * |\psi\rangle\langle\psi|^P$ jest prawidłowym stanem kwantowym. Wynika to z faktu, że narzucony został warunek na macierz procesu, by przekształcała odwzorowania A i B na prawidłowe odwzorowania CPTP, które przekształcają każdy poprawny stan na inny poprawny stan. Wychodząc z drugiej strony można wywnioskować, że jeżeli wynik zadziałania macierzą procesu na odwzorowaniach przekształca wszystkie poprawne stany na inne poprawne stany to musi być to prawidłowy wynik. Ważnym jednakże jest zauważyć, że

$$[S * (A \otimes B)] * |\psi\rangle\langle\psi| = (S * |\psi\rangle\langle\psi|^P) * (A \otimes B). \quad (156)$$

Warunek, by prawa strona równania produkowała prawidłowe stany dla każdego stanu i każdych dwóch odwzorowań jest równoważny z warunkiem, by proces z trywialną przeszłością ($S * |\psi\rangle\langle\psi|^P$ produkował prawidłowe odwzorowania CPTP z trywialną przeszłością z prawidłowych odwzorowań CPTP. Zapisując jawnie ten warunek otrzymuje się

$$\begin{aligned} \forall |\psi\rangle \quad (S * |\psi\rangle\langle\psi|) &= |w_\psi\rangle\langle w_\psi| = L_V(|w_\psi\rangle\langle w_\psi|) \\ \text{Tr} |w_\psi\rangle\langle w_\psi| &= d_{A_2} d_{B_2}, \end{aligned} \quad (157)$$

gdzie L_V jest poprzednio zdefiniowanym projektorem z $d_P = 1$. Równanie (155) można zidentyfikować jako standardową puryfikację stanów mieszanych w przestrzeni mniej wymiarowej jako stanów czystych w przestrzeniach więcej wymiarowych. Dla macierzy o rozkładzie spektralnym danym

$$W = \sum_i^{r-1} \lambda_i |\lambda_i\rangle \langle \lambda_i|, \quad (158)$$

gdzie λ_i to niezerowe wartości własne, a $|\lambda_i\rangle$ to odpowiadające im wektory własne. Poprawną puryfikacją dla takiej macierzy jest

$$|w_0\rangle = \sum_i^{r-1} \sqrt{\lambda_i} |\lambda_i\rangle |i\rangle, \quad (159)$$

co można łatwo sprawdzić. Puryfikacja ta jest unikatowa z dokładnością do pewnej izometrii V na puryfikowanym systemie, lecz taka izometria nie zmienia poprawności stanów zwracanych przez proces, więc można ją wybrać jako identyczność bez utraty ogólności, jego przyszłość jako trywialną, więc rozmiar puryfikowanego systemu jako rząd W . Pozwala to wybrać r^2 wymiarową bazę dla puryfikowanych macierzy. Zapisać wtedy można wektory $|w_\psi\rangle$ w tej bazie, jako $\sum_i^{r-1} \alpha_i |w_i\rangle$. Korzystając teraz z liniowości operacji w warunkach (157) i cykliczności śladu przepisać je można jako

$$\begin{aligned} \forall i, j \quad L_V^\perp (|w_i\rangle \langle w_j|) &= 0 \\ \langle w_i | w_j \rangle &= d_{A_2} d_{B_2} \delta_{ij} \\ L_V^\perp &= \mathbb{1} - L_V, \end{aligned} \quad (160)$$

gdzie $|w_i\rangle := \langle i|^P |U_S\rangle$.

5.4 Warunek konieczny

Okazuje się jednakże, że znalezienie takiego zbioru wektorów $\{|v_i\rangle\}$ jest problemem trudnym, gdyż warunek $L_V^\perp (|v_i\rangle \langle v_j|) = 0$ jest kwadratowy. Dlatego w duchu artykułu, który wprowadził puryfikację zostanie tutaj opisany i wyprowadzony warunek konieczny, który jest łatwy do sprawdzenia. Procesy, które nie spełniają tego warunku będą więc niepuryfikowalne, zaś dla reszty będzie niekonkluzywny. Wektor $|v_0\rangle$ jest ściśle określony dla danej macierzy, jego postać jest znana, więc warunek $L_V^\perp (|v_i\rangle \langle v_0|) = 0$ jest liniowy co pozwala scharakteryzować przestrzeń V_W formowaną przez wektory, które je spełniają. W celu skonstruowania ortonormalnej bazy dla V_W wykorzystuje się $\Pi_{L_V^\perp}$ zdefiniowany następująco

$$\forall i, j \quad \Pi_{L_V^\perp} |i\rangle \langle j| = |L_V^\perp (|i\rangle \langle j|)\rangle \quad (161)$$

Otrzymuje się wtedy, że

$$L_V^\perp (|v\rangle \langle v_0|) = 0 \iff \Pi_{L_V^\perp} |v_0^*\rangle |v\rangle = 0 \quad (162)$$

Definiując dalej operator O_W dany następująco

$$O_W := (\langle w_0^* | \otimes \mathbb{1}) \Pi_{L_V^\perp} (|w_0^*\rangle \otimes \mathbb{1}) \quad (163)$$

i aplikując go na $|v\rangle$

$$O_W |v\rangle = 0 \iff \Pi_{L_V^\perp} |w_0^*\rangle |v\rangle = 0. \quad (164)$$

Jeżeli $|v\rangle$ ma spełniać powyższy warunek, niezerowe składowe może mieć wyłącznie przy tych wektorach bazowych, które odpowiadają wektorom własnym tego operatora, przy których stoją zerowe wartości własne, lub równoważnie wektory własne O_W o zerowych wartościach własnych rozpinają przestrzeń V_W .

Niech teraz przez $\{|r_i\rangle\}$ dane będą właśnie te wektory tworzące ortonormalną bazę w V_W oraz niech $R = \sum_i |i\rangle\langle r_i|$. Ograniczyć można ten projektor do przestrzeni $V_W^* \otimes V_W$ w następujący sposób

$$\Pi_{L_V^\perp|V_W} = (R^* \otimes R) \Pi_{L_V^\perp} (R^{\dagger} \otimes R^{\dagger}) \quad (165)$$

Niech teraz $\{|m_k\rangle\}_{k=0}^{d_m-1}$ będzie zbiorem wektorów własnych $\Pi_{L_V^\perp|V_W}$ z niezerową wartością własną. Korzystając z argumentu analogicznego do tego powyżej

$$\Pi_{L_V^\perp|V_W} |v_j^*\rangle |v_i\rangle = 0 \iff \forall k \langle v_j^* | \langle v_i | |m_k\rangle = 0 \quad (166)$$

Można teraz spostrzec, że powyższy warunek wygodnie przepisać na

$$\langle v_j^* | \langle v_i | |m_k\rangle = \langle v_i | M_k | v_j \rangle \quad (167)$$

$$|M_k\rangle\rangle = |m_k\rangle. \quad (168)$$

W ogólności macierze M_k nie są hermitowskie, a konieczne są rzeczywiste wartości własne w celu skorzystania z twierdzenia, które zaraz zostanie przytoczone. Definiuje się

$$C_k = M_k + M_k^\dagger C_{k+d_m} = i(M_k - M_k^\dagger) \quad (169)$$

Widać oczywiście, że $\frac{C_k - iC_{k+d_m}}{2} = M_k$, a same macierze C_k zostały zdefiniowane jako hermitowskie. Daje to możliwość zapisania, że

$$\Pi_{L_V^\perp|V_W} |v_j^*\rangle |v_i\rangle = 0 \iff \forall k \langle v_i | C_k | v_j \rangle \quad (170)$$

Dalsze rozwijanie i badanie tego warunku wystarczającego jest otwarty problemem. Udowodniono jednak w opisywanym artykule, że wymiar przestrzeni, której wektory spełniają

$$\langle v' | C_k | v \rangle = 0 \quad (171)$$

równy jest

$$d_{C_k} = n_{k0} + \min(n_{k+}, n_{k-}), \quad (172)$$

gdzie n_0, n_{k+}, n_{k-} są odpowiednio liczbą zerowych, dodatnich i ujemnych wartości własnych k -tej macierzy. Intuicyjne uzasadnienie tego twierdzenia może być następujące: dostępnych jest n_0 składowych, które nie wpływają na ten wynik oraz $\min(n_{k+}, n_{k-})$, które trzeba wyzerować odpowiednio drugim znakiem. Wybierając znak, którego jest więcej, zabrakłoby po prostu składowych do ich wyzerowania. Toteż prostym ograniczeniem, które okazuje się być w wielu przypadkach nietrywialne jest wzięcie rozmiaru najmniejszej przestrzeni, jeżeli będzie ona mniejsza niż rząd W to macierz będzie niepurifikowalna, lub zwięźle

$$W \text{ jest purifikowalne} \implies d_{max}(W) \geq \text{rank}(W) \quad (173)$$

$$d_{max}(W) := \min_i d_{C_i} \quad (174)$$

6 Przykłady

W rozdziale trzecim podano przykład procesu, które może łamać przyczynowe nierówności. Okazuje się, że ten proces nie jest purifikowalny dla skrajnego $q = 1$, dla $q = 0$ jest purifikowalny, bo przyczynowy, zaś ze względu na złożoność obliczeniową i brak dostępnych wyników w literaturze nie jest wiadome, dla jakich q ten proces jest purifikowalny.

Kolejnymi interesującymi przykładami są kanały kwantowe. Wektor procesu dla kanału kwantowego jest następujący:

$$|w_{channel}\rangle^{A \prec B} = |\mathbb{1}\rangle^{PA_1} |\mathbb{1}\rangle^{A_2 B_1} |\mathbb{1}\rangle^{B_2 F}. \quad (175)$$

Reprezentuje on oczywiście zasób, które ma ściśle określoną przyczynowość, dlatego nie może złamać żadnych nierówności przyczynowych. Biorąc proces następujący

$$a|w_{channel}\rangle\langle w_{channel}|^{A \prec B} + b|w_{channel}\rangle\langle w_{channel}|^{B \prec A}, \quad (176)$$

warunek normujący daje, że $a + b = 1$, więc ewidentnie proces jest separowalny. Co za tym idzie on również nie może złamać nierówności przyczynowych. Taki zasób można interpretować jako probabilistyczny kanał, który z pewnym prawdopodobieństwem decyduje, kto jest przed kim. Eksplorując dalej procesy związane w prosty sposób z kanałami można zadać sobie pytanie, co w takim razie dzieje się z spójnym zmieszonym kanałem, niech wektor procesu będzie dany

$$|w_{procesu}\rangle = a|w_{channel}\rangle^{A \prec B} + b|w_{channel}\rangle^{B \prec A} \quad (177)$$

Okazuje się jednakże, że niestety proces dany tym wektorem nie należy do przestrzeni poprawnych procesów, gdy dwa współczynniki są różne od zera. W celu uratowania tego wyborczego pomysłu spróbowano wziąć

$$W' = CL_V(W). \quad (178)$$

C jest stałą normalizacyjną równą $\frac{d_O}{\text{Tr } W'}$. W celu prób złamania nierówności danej w trzecim rozdziale wykorzystano następujący protokół. Gdyby dany był idealny dwustronny kanał, można by otrzymać system w jednym laboratorium, zmierzyć $|i\rangle\langle i|$ i powiązać przesyłany bit z odebrany stanem, przypisać odpowiednio swój bit do stanu i wysłać go do drugiego laboratorium. Idąc za pomysłem, że proces powyższy reprezentuje pewnego rodzaju pozostałość z takiego idealnego dwustronnego kanału, przyjmuje się właśnie tę procedurę. Odpowiednie odwzorowania są więc dane

$$\eta(x, a) = |x\rangle\langle x| \otimes |a\rangle\langle a| \quad (179)$$

$$\xi(y, b, b') = \eta(y, b) \quad (180)$$

Pamiętając, że prawdopodobieństwo jest dane jak zwyczaj, czyli

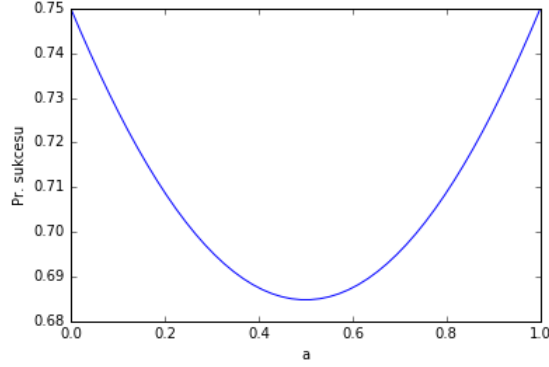
$$\text{Pr}(x, y|a, b, b') = \text{Tr} \{W [\eta(x, a) \otimes \xi(y, b, b')]\} \quad (181)$$

Okazuje się, że prawdopodobieństwo sukcesu w grze zdefiniowanej w rozdziale trzecim wynosi 0.8 dla $a = b$, który jest równym połączeniem dwóch kanałów. Niestety radość musi ukrócić fakt, że powyższa macierz okazuje się nie być nieujemna. Dodając najmniejszą ilość białego szumu takiego, że W' będzie nieujemne, czyli

$$W'' = W' + \lambda_{min} \mathbb{1}, \quad (182)$$

gdzie λ_{min} to najmniejsza wartość własna. Otrzymuje się prawdopodobieństwo równe około 0.68, co niestety ujmuje przydatności i wyjątkowości takiego zasobu. Co niestety zmusza do szukania innych ciekawych implementowalnych fizycznie procesów. W celu spełnienia warunku normalizacyjnego $a + b \leq C$, gdzie C jest pewną stałą, dlatego bez utraty ogólności można wybierać $a + b = 1$ i następnie dokonywać procesu renormalizacji. Na rysunku 8 pokazano prawdopodobieństwo sukcesu dla rodziny procesów generowanych powyżej opisaną metodą.

Bardzo ważnym przykładem, który został zaimplementowany fizycznie, który potwierdza występowanie w fizyce nieprzyczynowego porządku jest kwantowy przełącznik (*quantum switch*). Jest to proces,



Rysunek 8: Wykres pokazujący zależność między a a prawdopodobieństwem sukcesu

w którym kanały kwantowe są w superpozycji zależnej od stanów w przeszłości. Jego wektor wygląda następująco

$$|w_{switch}\rangle = |0\rangle^{P_1} |\mathbb{1}\rangle^{P_2 A_1} |\mathbb{1}\rangle^{A_2 B_1} |\mathbb{1}\rangle^{B_2 F_2} |0\rangle^{F_1} + |1\rangle^{P_1} |\mathbb{1}\rangle^{P_2 B_1} |\mathbb{1}\rangle^{B_2 A_1} |\mathbb{1}\rangle^{A_2 F_2} |1\rangle^{F_1}, \quad (183)$$

gdzie $F = F_1 \otimes F_2$, $P = P_1 \otimes P_2$. Proces ten jest ewidentnie reprezentacją wektorową CJ pewnego unitarnego operatora. Wystarczy zaobserwować, że działając na proces macierzą unitarną postaci

$$U = \mathbb{1}^{P_1 P_2 A_1 A_2 B_1 B_2 F_1} \otimes |0\rangle\langle 0|^{F_2} + \mathbb{1}^{P_1 P_2} \otimes \mathbf{SWAP}^{A_1 B_1} \otimes \mathbf{SWAP}^{A_2 B_2} \otimes |1\rangle\langle 1|^{F_2}, \quad (184)$$

otrzymuje się wektor CJ macierzy jednostkowej. Wynika więc z tego, że sam proces jest wektorem CJ macierzy unitarnej. Kubit kontrolny z P_1 pozostaje niezmienny zaś badając zmianę stanu z P_2 można dowiedzieć się, jaką "drogę" przebyły. Taki zasób nie jest w stanie złamać żadnych nierówności przyczynowych. Nie jest żaden znany puryfikowalny przykład w literaturze, który byłby w stanie złamać przyczynowe nierówności, jednakże znany jest proces trzystronny, wprowadzony w [26], który jest w stanie złamać przyczynowe nierówności.

$$W_{det} = \sum_{a,b,c} |a, b, c\rangle \langle a, b, c| \otimes |\neg b \wedge c, \neg c \wedge a \neg a \wedge b\rangle \langle \neg b \wedge c, \neg c \wedge a, \neg a \wedge b|, \quad (185)$$

systemy zostały zapisane w następującej kolejności $A_2 B_2 C_2 A_1 B_1 C_1$. Korzystając ze standardowej metody zamieniania nieodwracalnych logicznych funkcji w odwracalne pisze się zamienia się $|x\rangle \mapsto |f(x)\rangle$ na $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$ wykorzystując to powyższy proces można przepisać w postaci wektorowej na

$$|w\rangle = \sum_{a,b,c,e,f,g} |a, b, c\rangle |e, f, g\rangle \otimes |a, b, c\rangle |i \oplus \neg b \wedge c, f \oplus \neg c \wedge a, g \oplus \neg a \wedge b\rangle, \quad (186)$$

gdzie systemy zostały wypisane w kolejności $A_2 B_2 C_2 P F A_1 B_1 C_1$. Tutaj zarówno przeszłość jak i przyszłość mają po trzy kubity, co stanowi puryfikację powyższego procesu.

6.1 Wielostronne przykłady

Okazuje się, że generalizacja formalizmu macierzy procesu do większej liczby stron powoduje komplikowanie się części wprowadzonych pojęć. W celu zilustrowania powstających problemów można zacząć od pokazania przykładu trzystronnego kwantowego przełącznika. Tym razem rozszerzono postać przełącznika z artykułu [3]. W przypadku trzystronnym przełącznik kwantowy składa się z czterech laboratoriów: Alicji, Boba, Charliego i Dawida. Pierwszych troje otrzymuje kubit wykonuje na nim pewne

operacji i pomiary i wysyła system dalej. Laboratorium Dawida ma dostęp do dwóch podsystemów D_1^t kubit, który jest kubitem poddanym operacją Alicji, Boba i Charliego w pewnej kolejności oraz podsystemu kontrolnego D_1^c , który określa przyczynowy porządek wykonanych operacji. Zakłada się, że Dawid porzuca swój system po wykonaniu pomiarów na nim. Rozmiary poszczególnych podsystemów to:

$$d_{A_1} = d_{A_2} = d_{B_1} = d_{B_2} = d_{C_1} = d_{C_2} = 2, \quad d_{D_1} = 12 = 2 \cdot 6, \quad d_{D_2} = 1 \quad (187)$$

Wygodnie zdefiniować jest następujące wielkości:

$$|C(X, Y, Z, i)\rangle := |\psi\rangle^{X_1} |\mathbb{1}\rangle^{X_2 Y_1} |\mathbb{1}\rangle^{Y_2 Z_1} |\mathbb{1}\rangle^{Z_2 D_1^t} |i\rangle^{D_1^c} \quad (188)$$

$$|C(X, Y, Z)\rangle := |\psi\rangle^{X_1} |\mathbb{1}\rangle^{X_2 Y_1} |\mathbb{1}\rangle^{Y_2 Z_1} |\mathbb{1}\rangle^{Z_2 D_1^t} \quad (189)$$

Wektor trzystronnego przełącznika można zapisać jako:

$$\begin{aligned} |w\rangle = \frac{1}{\sqrt{6}} \sum_i |C(X_i, Y_i, Z_i, i)\rangle = \frac{1}{\sqrt{6}} & |C(A, B, C, 0)\rangle + |C(A, C, B, 1)\rangle + |C(B, A, C, 2)\rangle \\ & + |C(B, C, A, 3)\rangle + |C(C, A, B, 4)\rangle + |C(C, B, A, 5)\rangle. \end{aligned} \quad (190)$$

Okazuje się, że tak zdefiniowany wektora procesu generują poprawną macierz procesu. Analizę tego procesu można rozpocząć od zbadanie jak wygląda obserwowany proces, gdy podsystem kontrolny zostanie zignorowany. Standardowo jest to równoważne z wykonaniem śladu częściowego po ignorowanym podsystemie:

$$\begin{aligned} \text{Tr}_{D_1^c} |w\rangle\langle w| &= \frac{1}{6} \text{Tr}_{D_1^c} \left[\sum_{ij} |C(X_i, Y_i, Z_i, i)\rangle\langle C(X_j, Y_j, Z_j, j)| \right] \\ &= \frac{1}{6} \text{Tr}_{D_1^c} \left[\sum_{ij} |C(X_i, Y_i, Z_i)\rangle\langle C(X_j, Y_j, Z_j)| \right] \\ &= \frac{1}{6} |C(X_i, Y_i, Z_i)\rangle\langle C(X_i, Y_i, Z_i)|. \end{aligned} \quad (191)$$

Łatwo zidentyfikować wyraz typu $|C(A, B, C)\rangle\langle C(A, B, C)|$ ($|C(A, B, C, 0)\rangle\langle C(A, B, C, 0)|$) jako proces, w którym Alicja jest połączona idealnym kanałem z Bobem, Bob z Charliem, Charlie z Dawidem. Widać więc, że gdy nie jest posiadana wiedza na temat podsystemu kontrolnego obserwowany proces jest probabilistyczna kombinacją wszystkich możliwych porządków idealnych kanałów między A, B i C - analogicznie do przypadku przełącznika dwustronnego. Intuicyjnie można teraz wnioskować, że proces trzystronnego przełącznika jest nieseparowalny przyczynowo. Oczywiście jest, że zredukowany proces jest prawidłowym procesem, opisuje on zasób, który można zrealizować fizycznie. Jednakże proces kwantowego przełącznika posiada jeszcze wyrazy mieszane, które nie posiadają fizycznej interpretacji. Zarówno postać wektora procesu jako superpozycji wyrazów zgodnych z konkretnymi porządkami przyczynowymi jak i istnienie wyrazów mieszanych pozwala wnioskować, że proces ten jest nieseparowalny. Specjalna postać tego procesu pozwala na postulowanie, że zasób ten jest w pewien intuicyjny sposób nieseparowalny, lecz w ogólności posiadając proces lub dostęp do generowanych przez niego korelacji stwierdzenia czy jest on nieseparowalny jest nietrywialnym problemem. Można zapisać przyczynowe nierówności dla przypadku wielostronnego [1], jednakże już w przypadku trzystronnym okazuje się to być kłopotliwe. Biorąc pod uwagę fakt, że dwustronny przełącznik nie może generować korelacji łamiących przyczynowe nierówności zapewne jego trzystronny odpowiednik również ich nie łamie. Słuszność tego zdania jest problemem otwartym, lecz gdy w przypadku założenia jego prawdziwości nie można scharakteryzować separowalności przyczynowej przełącznika przy pomocy nierówności przyczynowych. Nietrywialne jest również rozszerzenie świadka przyczynowości dla większej liczby stron. Fakt, że przy pomocy operatorów x można określić,

w przypadku dwustronnym, przyczynowy porządek danego wyrazu zapewnia ładną postać świadka przyczynowości. Nie jest to prawdziwe w przypadku wielostronnym. Przykładowo można rozważyć te dwa procesy:

$$W_{ABC} = \rho^{A_1} \otimes |1\rangle\rangle\langle\langle 1|^{A_2 B_1} \otimes |1\rangle\rangle\langle\langle 1|^{B_2 C_1} \otimes 1^{C_2} \quad (192)$$

$$W_{BAC} = \rho^{B_1} \otimes |1\rangle\rangle\langle\langle 1|^{B_2 A_1} \otimes |1\rangle\rangle\langle\langle 1|^{A_2 C_1} \otimes 1^{C_2}. \quad (193)$$

Oba procesy zawierają wyrazy typu $A_1 A_2 B_1 B_2 C_1$, które ewidentnie mogą posiadać korelacje zgodne z pewnym porządkiem przyczynowym. Powyższy przykład ilustruje fakt, że istnieją takie wyrazy, których porządku przyczynowego nie można scharakteryzować przy pomocy projektorów X . Sformułowanie świadków przyczynowości dla przypadku wielostronnego jest wciąż problemem otwartym. Wiele wskazuje na to, że nawet jeżeli można sformułować świadków przyczynowości dla wielu stron to poszukiwanie świadków będzie problemem trudnym numerycznie. Mnogość problemów dalej pokazuje rozumowanie przeprowadzone w [19]. W tym artykule, zostało pokazane, że w przypadku wielostronnym laboratoria mogą wpływać swoimi operacjami na kolejność stron występujących po sobie. Fakt ten dodatkowo utrudnia sformułowanie przyczynowej separowalności i wprowadza pojęcie procesów o określonej przyczynowości i separowalnych do określonej przyczynowości. Pokazują, że pojęcia te są nierówne w przypadku wielostronnym. W celu poznania rygorystycznej definicji czytelnik jest zachęcany do zapoznania się z oryginalnym artykułem. Intuicyjnie można zilustrować następującym eksperymentem: Alicja otrzymuje kubit, dokonuje pomiar w pewnej bazie, w przypadku otrzymania jednego wyniku w klasyczny sposób powoduje, że Bob jest przed Charliem, gdy otrzyma drugi wynik Charlie jest przed Bobem. Za każdym razem eksperyment taki ma ściśle określony porządek przyczynowy, lecz próbując zapisać zasób ten przy pomocy macierzy procesu okazuje się, że niemożliwe jest zapisanie go w postaci separowalnej przyczynowo.

7 Wnioski

W pracy przedstawiono podstawy formalizmu macierzy procesu. Zaprezentowano przykładowe zadanie, w którym nieprzyczynowe zasoby mogą osiągać lepsze wyniki, niż zasoby o określonym porządku przyczynowym. Następnie pokazano narzędzie, które zostało wykorzystane do eksperymentalnego potwierdzenia braku ścisłego określenia przyczynowości w przyrodzie. Opisano następnie proponowany postulat, który miałby określać, czy dany proces jest implementowalny fizycznie. Podano parę oryginalnych przykładów. Poszukiwanie wektorów, które spełniałyby warunek wystarczający i konieczny okazuje się być trudnym problemem, więc zademonstrowano wyprowadzenie warunku koniecznego, który sprowadza się do działań algebry liniowej.

Badanie nieprzyczynowości wydaje się być popularnym nurtem w informatyce kwantowej, który niesie wiele nadziei na nowe ważne odkrycia, chociażby na połączenie mechaniki kwantowej z grawitacją. Istnieje wiele elementów, które wymagają rozwinięcia. Ewidentnym brakiem w prezentowanym na końcu postulatcie jest brak jakichkolwiek innych przesłanek na jego słuszność, niż intuicja fizyczna. Wymagane jest w celu utwierdzenia słuszności powyższego postulat wiele eksperymentów fizycznych, jednakże ze względu na pewien metafizyczny charakter tego postulatu będzie to trudne. Ważne są również badania nad skutecznymi metodami spełniania wystarczającego warunku, gdyż problematyczne będą procesy niewykłuczane przez warunek konieczny.

Spis treści

1	Wstęp	2
1.1	Historia	2
1.2	Podstawowe informacje	3
2	Macierz Procesu	6
2.1	Stany	8
2.2	Kanały	11
2.3	Kanały z pamięcią	12
3	Przyczynowa separowalność i przyczynowe nierówności	14
3.1	Systemy n-wymiarowe	16
3.2	Adnotacja	18
3.3	Procesy z przyczynowym modelem	18
4	Świadek przyczynowości	19
4.1	Sformułowanie macierzy procesu niezależne od bazy	20
4.2	Poszukiwanie świadka przyczynowości	21
4.3	Implementacja świadka przyczynowości	23
5	Postulat puryfikacyjny	24
5.1	Czysty proces	26
5.2	Proces puryfikowalny	27
5.3	Warunki konieczne i wystarczające	27
5.4	Warunek konieczny	28
6	Przykłady	29
6.1	Wielostronne przykłady	31
7	Wnioski	33
	Bibliografia	36
	Dodatek A Szybkie obliczanie L_V	37
	Dodatek B Jawna postać $\Pi_{L_V^\perp}$	40

Spis rysunków

1	Sfera Blocha. Punkty na tej sferze opisują wszystkie możliwe stany z dokładnością do czynnika fazowego. $ \psi\rangle$	3
2	Rysunek ilustruje działanie izomorfizmu CJ. Zamiast działać odwzorowaniem na pewien stan izomorfizm CJ pokazuje działanie na maksymalnie splątane cząstki. Z powodu izomorfizmu w drugą stronę, konwencjonalnie interpretuje się izomorfizm CJ jako teleportację bramek kwantowych.	7
3	Schematyczne przedstawienie stanów. Laboratoria wykonują pewne wybrane pomiary na systemach po czym wysyłają je ze swoich laboratoriów. Każde z laboratoriów otrzymuje różne, potencjalnie splątane, systemy.	9
4	Schematyczna reprezentacja kanału CPTP. Alicja wykonuje wybrane operacje na systemie po czym wysyła go do Boba. W trakcie przesyłania systemu zostaje zaaplikowana unitarna transformacja U	11
5	Schematyczna reprezentacja kanału z pamięcią na przykładzie zasobu wykorzystywanego do implementacji kodowania supergęstego. Alicja z Bobem dzielą maksymalnie splątane cząstki. Alicja wykonuje pewną unitarną transformację i wysyła swój system dalej do Boba.	12
6	Rysunek symbolizuje działanie procesu W jako funkcje wyższego rzędu odwzorowań \mathcal{A} i \mathcal{B} , która dla danych odwzorowań zwraca odwzorowanie $\mathcal{G}_{\mathcal{A},\mathcal{B}}$ reprezentującą transformację, która przechodzi z globalnej przeszłości do globalnej przyszłości.	24
7	Rysunek schematycznie przedstawia działanie operacji SWAP . Na wejściu Alicja otrzymuje system złożony np. w stanie $\rho^{A_1} \otimes \rho^{A'_1}$ następnie aplikuje unitarną macierz SWAP definiowaną następująco $\mathbf{SWAP} = \sum_{ij} ij\rangle\langle ji $, a na wyjściu otrzymuje system w stanie $\rho^{A_2} \otimes \rho^{A'_2}$. Postać CJ tej macierzy to: $ \mathbb{1}\rangle\langle\mathbb{1} ^{A_1 A'_2} \otimes \mathbb{1}\rangle\langle\mathbb{1} ^{A'_1 A_2}$. Warto również zauważyć, że po przemianowaniu systemów wyjściowych $A_2 \rightarrow A'_2$, $A'_2 \rightarrow A_2$ operacja SWAP działa trywialnie.	26
8	Wykres pokazujący zależność między a a prawdopodobieństwem sukcesu	31

Bibliografia

- [1] Alastair A. Abbott, Christina Giarmatzi, Fabio Costa, and Cyril Branciard. Multipartite causal correlations: Polytopes and inequalities. 2016.
- [2] M. L. Almeida, J. D. Bancal, N. Brunner, A. Acin, N. Gisin, and S. Pironio. Guess your neighbour's input: a multipartite non-local game with no quantum advantage. 2010.
- [3] Mateus Araújo, Cyril Branciard, Fabio Costa, Adrien Feix, Christina Giarmatzi, and Časlav Brukner. Witnessing causal nonseparability. 2015.
- [4] Mateus Araújo, Adrien Feix, Miguel Navascués, and Časlav Brukner. A purification postulate for quantum mechanics with indefinite causal order, 2016.
- [5] Reinhold A Bertlmann and Philipp Krammer. Bloch vectors for qudits. *Journal of Physics A: Mathematical and Theoretical*, 41(23):235303, 2008.
- [6] Časlav Brukner. Bounding quantum correlations with indefinite causal order. 2014.
- [7] Man-Duen Choi. Completely positive linear maps on complex matrices. *Linear Algebra and its Applications*, 10(3):285 – 290, 1975.
- [8] E. B. Davies and J. T. Lewis. An operational approach to quantum probability. *Comm. Math. Phys.*, 17(3):239–260, 1970.
- [9] Adrien Feix, Mateus Araújo, and Časlav Brukner. Causally nonseparable processes admitting a causal model. 2016.
- [10] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. 2001.
- [11] Aram W. Harrow, Avinandan Hassidim, and Seth Lloyd. Quantum algorithm for solving linear systems of equations. 2008.
- [12] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. 2007.
- [13] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Reports on Mathematical Physics*, 3(4):275–278, December 1972.
- [14] M. Keyl. Fundamentals of quantum information theory. 2002.
- [15] Dennis Kretschmann and Reinhard F. Werner. Quantum channels with memory. 2005.
- [16] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. Quantum principal component analysis. 2013.
- [17] Jonas Maziero. Computing partial traces and reduced density matrices. 2016.
- [18] Ognian Oreshkov, Fabio Costa, and Časlav Brukner. Quantum correlations with no causal order. 2011.
- [19] Ognian Oreshkov and Christina Giarmatzi. Causal and causally separable processes. 2015.
- [20] Asher Peres. Quantum measurements are reversible. *American Journal of Physics*, 42(10):886–891, 1974.

- [21] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L. Braunstein. Advances in quantum teleportation. 2015.
- [22] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bell's theorem. 2009.
- [23] Patrick Rebentrost, Masoud Mohseni, and Seth Lloyd. Quantum support vector machine for big data classification. 2013.
- [24] Giulia Rubino, Lee A. Rozema, Adrien Feix, Mateus Araújo, Jonas M. Zeuner, Lorenzo M. Procopio, Časlav Brukner, and Philip Walther. Experimental verification of an indefinite causal order, 2016.
- [25] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. 1995.
- [26] Āmin Baumeler and Stefan Wolf. The space of logically consistent classical processes without causal order. 2015.

Dodatek A Szybkie obliczanie L_V

W wielu przypadkach, gdy ma się do czynienia z dużymi macierzami konieczne jest skorzystanie z metod numerycznych. Problemатyczne ze względu na złożoność obliczeniową okazują się nawet takie pozornie proste operacje jak częściowy ślad. Licząc naiwnie go z następującej formuły, która jest łatwa do zaimplementowania

$$\text{Tr}_B A = \sum_i^{d_B} (\mathbb{1}^A \otimes \langle i|_B) A (\mathbb{1}^A \otimes |i\rangle_B). \quad (194)$$

Dla wybranego i wykonując pierwsze mnożenie otrzymuje się macierz o $d_A^2 d_B$ komórkach, gdzie obliczenie każdej komórki wymaga $d_A d_B$ operacji, następnie wykonuje się drugie mnożenie, które nie zwiększa złożoności. Wykonując tę procedurę dla wszystkich $|i\rangle$ otrzymuje się złożoność $O(d_A^3 d_B^3)$. Wykorzystując wiedzę o chociażby strukturze (praktycznie wszystkie komórki są zerami) można znacznie przyspieszyć te obliczenia. W [17] pokazano wydajną metodę obliczania częściowego śladu. Posiadając jawną postać pewnej macierzy A , w celu wyliczenia ${}_X A$ konieczne po wykonaniu śladu częściowego jest zastąpienie jedyneką odpowiedniego systemu. Jawnie iloczyn tensorowy dla macierzy reprezentuje się przy pomocy tzw. iloczynu Kroneckera. O ile jest pewna dowolność w zapisie matematycznym, gdzie postawi się znak iloczynu tensorowego tak długo jak odnotuje się jakiego podsystemu dotyczy macierz, w implementacji kolejność systemów jest niejawną, zakodowaną pozycyjnie. Korzystając z wydajnej metody na obliczanie śladu można łatwo w wydajny sposób obliczyć operacje ${}_X A$ skrajnych systemów następująco:

$${}_{A_1} A = \mathbb{1}^{A_1} \otimes \text{Tr}_{A_1} A, \quad (195)$$

$${}_{A_N} A = \text{Tr}_{A_N} A \otimes \mathbb{1}^{A_N}. \quad (196)$$

W innych przypadkach macierz jednostkowa będzie znajdowała się na niewłaściwym miejscu, co zmusza do wykorzystania tzw. macierzy komutacji, co pozwala zapisać

$${}_{A_n} A = Q (\text{Tr}_{A_n} A \otimes \mathbb{1}^{A_N}) Q \quad (197)$$

$$Q = \sum_{ijkl} |i\rangle_{A_1 \dots A_{n-1}} |j\rangle_{A_n} |k\rangle_{A_{n+1} \dots A_{N-1}} |l\rangle_{A_N} \langle i|_{A_1 \dots A_{n-1}} \langle l|_{A_n} \langle k|_{A_{n+1} \dots A_{N-1}} \langle j|_{A_N}, \quad (198)$$

gdzie A_N oznacza ostatni system, zaś $\mathbb{1}^{A_N}$ rozumie się, ako macierz jednostkowa o odpowiednim rozmiarze na ostatniej pozycji. Zauważa się, że macierz Q ma $d_{A_1 A_2 \dots A_N}$ jedynek, jest unitarna co razem daje, że w każdej kolumnie i każdym rzędzie jest dokładnie jedna jedynka i na innych miejscach zera. Wynika to z faktu, że gdyby było inaczej to obliczając wyznacznik macierzy Q metodą minorów rozwijając względem wiersza, w którym nie stoi jedynka wyszłoby, że wyznacznik tej macierzy byłby równy zero, co jest sprzeczne z faktem, że macierz ta jest odwracalna. Niemożliwa jest większa liczba jedynek, niż jeden w każdej kolumnie i wierszu, ponieważ jest ich dokładnie $d_{A_1 A_2 \dots A_N}$. Taka postać macierzy pozwala na obliczenie wartości danej komórki macierzy w czasie stałym co pozwala na wykonanie operacji ${}_X A$ w $O(d_{A_1 A_2 \dots A_N}^2)$. Problem można również rozwiązać w inny sposób, który może być uznawany za bardziej elegancki, a oferuje taką samą złożoność obliczeniową i jest bardziej przystępny implementacyjnie jest wykonywanie tej operacji na tzw. uogólnionym wektorze Blocha. W wcześniejszym rozdziale została wprowadzona baza Hilberta-Schmidta. Jest to zbiór macierzy, zawierających macierz jednostkową i $d_A^2 - 1$ bezśladowych macierzy ortoznormalizowanych w sensie iloczynu skalarnego Hilberta-Schmidta, czyli

$$\text{Tr}(\Gamma_i \Gamma_j) = C \delta_{ij}, \quad (199)$$

gdzie C jest pewną stałą normalizacyjną. Można rozpisać A jako:

$$A = \sum_{i=0}^{d_A^2-1} \sigma_i \Gamma_i = \sigma \Gamma \quad (200)$$

$$\sigma := \{\sigma_0, \sigma_1, \dots\} \quad (201)$$

$$\Gamma := \{\Gamma_0, \Gamma_1, \dots\}^T \quad (202)$$

$$\sigma_i = \frac{1}{C} \text{Tr}[A \Gamma_i]. \quad (203)$$

Standardowo, gdy mówi się o wektorze Blocha narzucony jest zwykle warunek normalizacji śladu $\text{Tr} A = 1$ co wyznacza $\sigma_0 = \frac{1}{d_{A_1 A_2 \dots}}$, który nie jest włączany do wektoru Blocha σ . Tutaj jednak można mieć do czynienia z nieznormalizowanymi macierzami więc wyraz σ_0 jest nieokreślony i wraz z macierzą jednostkową włączony do odpowiednich wektorów. Jako bazę w celu obliczania ${}_X A$ wybrano uogólnione macierze Gell-Manna (UMG) [5]; są uogólnieniem macierzy Pauliego na więcej wymiarów. Macierze te dzieli się na trzy grupy definiowane następująco:

- $\frac{d(d-1)}{2}$ Symetrycznych UMG

$$\Gamma_{ij}^S = |i\rangle\langle j| + |j\rangle\langle i|, \quad 1 \leq i < j \leq d. \quad (204)$$

- $\frac{d(d-1)}{2}$ Antysymetrycznych UMG

$$\Gamma_{ij}^A = -i|i\rangle\langle j| + i|j\rangle\langle i|, \quad 1 \leq i < j \leq d. \quad (205)$$

- $(d-1)$ Diagonalnych UMG

$$\Gamma_i = \sqrt{\frac{2}{i(i+1)}} \left(\sum_{j=1}^i |j\rangle\langle j| - i|i+1\rangle\langle i+1| \right), \quad 1 \leq i \leq d-1 \quad (206)$$

Przez pogrubione \mathbf{i} oznaczono jednostkę urojoną. UMG spełnia następującą relację ortoznormalizowania: $\text{Tr} \Gamma_i \Gamma_j = 2\delta_{ij}$. W [5] wyprowadzono następujące rozwinięcie standardowych macierzy ($|i\rangle\langle j|$) w bazie UMG:

$$|i\rangle\langle j| = \begin{cases} \frac{1}{2} (\Gamma_{ij}^S + i\Gamma_{ij}^A), & \text{dla } i < j \\ \frac{1}{2} (\Gamma_{ji}^S - i\Gamma_{ji}^A), & \text{dla } i > j \\ -\sqrt{\frac{j-1}{2j}} \Gamma_{j-1} + \sum_{n=0}^{d-j-1} \frac{1}{\sqrt{2(j+n)(j+n+1)}} \Gamma_{j+n} + \frac{1}{d} \mathbb{1}, & \text{dla } j = d. \end{cases} \quad (207)$$

Łatwo zauważyć, że posiadając ortogonalną bazę w systemie A $\{\Gamma_i^A\}$ i bazę w B $\{\Gamma_j^B\}$ macierze $\{\Gamma_i \otimes \Gamma_j\}$ tworzą bazę w $A \otimes B$, ponieważ:

$$\text{Tr}[(\Gamma_i^A \otimes \Gamma_j^B)(\Gamma_e^A \otimes \Gamma_f^B)] \quad (208)$$

$$= \text{Tr}[\Gamma_i^A \Gamma_e^A \otimes \Gamma_j^B \Gamma_f^B] \quad (209)$$

$$= \text{Tr}[\Gamma_i^A \Gamma_e^A] \text{Tr}[\Gamma_j^B \Gamma_f^B] \quad (210)$$

$$= CD\delta_{ie}\delta_{jf}. \quad (211)$$

Korzystając z tego wyniku jako bazę w $P \otimes A_1 \otimes A_2 \otimes B_1 \otimes B_2 \otimes F$ można wybrać $\{\Gamma_i \otimes \Gamma_j \otimes \Gamma_k \otimes \Gamma_l \otimes \Gamma_e \otimes \Gamma_f\}$, gdzie poszczególne macierze są UMG o odpowiednim wymiarze. Macierz ta skrótowo będzie nazywana $\Gamma_{ijkl ef}$. Można teraz zapisać:

$$W = \sum_{ijkl ef} \sigma_{ijkl ef} \Gamma_{ijkl ef} = \sigma \Gamma. \quad (212)$$

Rozpisując W w bazie $|i\rangle\langle j|$ otrzymuje się

$$W = \sum_{ij} \alpha_{ij} |i\rangle\langle j|. \quad (213)$$

Następnie zauważa się, że

$$|m\rangle^A |n\rangle^B \langle i|^A \langle j|^B = |d_A m + n\rangle^{AB} \langle d_A i + j|^{AB}. \quad (214)$$

Wnioskiem płynącym z łączności iloczynu tensorowego jest fakt, że baza CB w przestrzeni więcej wymiarowej jest iloczynem tensorowym baz CB w poszczególnych podsystemach. Rozważa się dalej, jak wygląda wektor Blocha macierzy typu $|i\rangle\langle j|$. Widać, że:

$$A \otimes B = (\sigma^A \Gamma^A) \otimes (\sigma^B \Gamma^B) = (\sigma^A \otimes \sigma^B)(\Gamma^A \otimes \Gamma^B). \quad (215)$$

Co przekładając na macierz $|i\rangle\langle j|$ daje:

$$|i\rangle\langle j| = |ijkl ef_1\rangle\langle ijkl ef_2| = \sigma_{ijkl ef} \Gamma = (\sigma_i \otimes \sigma_j \otimes \sigma_k \otimes \sigma_l \otimes \sigma_e \otimes \sigma_f) \Gamma. \quad (216)$$

Z równania (207) widać, że wyrazy typu $|i\rangle\langle j|$ dla $i \neq j$ mają stałą ($O(1)$) liczbę niezerowych współrzędnych σ_i i jest ich $O(d^2)$ dla ogólnej macierzy. Zaś wyrazy, gdzie $i = j$ mają $O(d)$ niezerowych wyrazów, ale jest ich tylko $O(d)$ więc policzenie ich wkładu dla dowolnej macierzy również zajmuje $O(d^2)$ czasu. Co pokazuje, że policzenie wektora Blocha dla bazy UMG zajmuje $O(d^2)$ czasu. Korzystając z analogicznego argumentu można pokazać, że odwrotna transformacja działa również w $O(d^2)$. Dalej zostanie pokazane, że obliczenia wektora Blocha dla baz składających się z $O(1)$ iloczynów tensorowych baz UMG również jest kwadratowy względem wymiaru systemu złożonego. Widać to od razu, gdy rozważy się ile czasu zajmuje obliczenie wektora Blocha następującej macierzy:

$$|i\rangle\langle i| \otimes |j\rangle\langle j| \otimes |k\rangle\langle l| \otimes |e\rangle\langle f|, \quad \text{gdzie } k \neq l, e \neq f. \quad (217)$$

Wyrazy typu zaprezentowanego powyżej mają $O(d_1 d_2)$ i jest ich w rozkładzie pewnej ogólnej macierzy $O(d_1 d_2 d_3^2 d_4^2)$. Widać, że wyrazy typu $|i\rangle\langle i|$ kontrybuują liniową liczbę wyrazów do wektora Blocha i jest ich liniowa liczba, zaś wyrazy typu $|i\rangle\langle j|$ dają stałą liczbę wyrazów, lecz jest ich kwadratowa liczba, a dla systemów złożonych złożoność widocznie się faktoryzuje. Sumując po wszystkich ustawieniach wyrazów diagonalnych i niediagonalnych otrzymuje się $O(1)$ wyrazów $O(d^2)$, czyli ostatecznie złożoność to obliczania rozkładu $O(d^2)$. Definiując operację

$$({}^X \sigma) \Gamma = {}_X(\sigma \Gamma), \quad (218)$$

jej jawne działanie jest bardzo proste a mianowicie, dla pewnego wektora Blocha opisującego stan systemu złożonego $A \otimes X \otimes B$ mapuje ona ijk-ty element wektora do

$$\sigma_{ijk} \mapsto \delta_{j0} \sigma_{ijk}. \quad (219)$$

Korzystając dalej z faktu, że ${}_XY A = {}_X({}_Y A)$. Zaaplikowanie projektora L_V sprowadza się do wykonania $O(1)$ operacji na $O(d^2)$ elementach wektory Blocha, czyli złożoność znów kwadratowa. Warto jeszcze podkreślić, że ze względu na rzadkość wektorów Blocha wskazanym jest trzymanie go w postaci par $\{(\sigma_{ijklef}, \Gamma_{ijklef})\}$, lub innym rzadkim formacie, w celu osiągnięcia odpowiedniej złożoności przy wykonywaniu wielu obliczeń projektorów macierzy standardowych.

Dodatek B Jawna postać $\Pi_{L_V^\perp}$

Operator $\Pi_{L_V^\perp}$ definiuje się następująco:

$$\forall i, j \quad \Pi_{L_V^\perp} |i\rangle\langle j| = |L_V^\perp(|i\rangle\langle j|)\rangle. \quad (220)$$

Dalej przytaczając argument z poprzedniego dodatku o CB zapisać można:

$$|i\rangle\langle j| = |i\rangle|j\rangle = |id_a + j\rangle = |e\rangle. \quad (221)$$

Widać z tego, że postać CJ macierzy standardowej to wektor CB w innej przestrzeni. Definiuje się wektor $|\pi_e\rangle = |L_V^\perp(|i\rangle\langle j|)\rangle$. Zauważa się teraz, że

$$\Pi_{L_V^\perp} |e\rangle = |\pi_e\rangle, \quad (222)$$

czyli macierz $\Pi_{L_V^\perp}$ mapuje wektory bazowe CB na pewne inne wektory co z definicji macierzy mówi, że e-ta kolumna macierzy $\Pi_{L_V^\perp}$ to wektor $|\pi_e\rangle$. Trzeba dalej zauważyć jednakże, że niewskazane jest trzymanie macierzy $\Pi_{L_V^\perp}$ w gęstej reprezentacji, gdzie każde pole macierzy ma swoją jawną reprezentację w pamięci. Niemożliwość tego może uświadomić następująca obserwacja: łatwo sprawdzić, że macierz ta ma $O(d^4)$ elementów. W przypadku projektora odpowiadającego macierzy przedstawionej w trzecim rozdziale zajmowałaby ona ok. 410TB pamięci w przypadku podwójnej precyzji. Przytaczając argument z dodatku A wiadome jest, że macierz ta ma $O(d^2)$ niezerowych elementów. Konieczna więc jest reprezentacja tej macierzy w rzadkim formacie np. skompresowanym formacie kolumnowym.