Politechnika Gdańska
Wydział Fizyki Technicznej i Matematyki Stosowanej
Katedra Fizyki Teoretycznej i Informatyki Kwantowej

Rozprawa doktorska

O komunikacji klasycznej przez kanały kwantowe z wieloma nadawcami

Łukasz Czekaj

Rozprawa przygotowana pod kierunkiem
prof. dr. hab. Pawła Horodeckiego
Gdańsk, grudzień 2011

Publikacje

Praca ta zawiera rezultaty pochodzące z następujących publikacji:

- L. Czekaj, J.K. Korbicz, R.W. Chhajlany, P. Horodecki,
  Schemes of transmission of classical information via quantum channels with many senders: discrete and continuous variables cases,
  arXiv:1110.2594v1 [quant-ph], 2011,
  praca przyjęta do druku w Phys. Rev. A

- L. Czekaj,
  Subadditivity of the minimum output entropy and superactivation of the classical capacity of quantum multiple access channels,
  Physical Review A 83, (042304), 2011

- L. Czekaj, J.K. Korbicz, R.W. Chhajlany, P. Horodecki,
  Quantum superadditivity in linear optics networks: Sending bits via multiple-access Gaussian channels,
  Physical Review A 82, (020302(R)), 2010

- L. Czekaj, P. Horodecki,
  Purely Quantum Superadditivity of Classical Capacities of Quantum Multiple Access Channels,
  Physical Review Letters 102, (110505), 2009

Podziękowania

Niniejsza praca nie powstałaby bez wsparcia wielu osób. W tym miejscu chciałbym podziękować mojemu promotorowi, prof. dr hab. Pawłowi Horodeckiemu, za liczne i inspirujące rozmowy oraz wiele krytycznych uwag, które pomogły w przygotowaniu tej pracy. Chciałbym także podziękować Karolinie Paluszyńskiej, mojemu bratu — Mateuszowi Czekajowi oraz moim rodzicom za cierpliwość i wyrozumiałość, jaką obdarzyli mnie w trakcie pisania tej pracy.

Podczas prowadzenia badań, autor korzystał ze wsparcia następujących instytucji:

- Ministerstwo Nauki i Szkolnictwa Wyższego

  Grant NN200627013

- Unia europejska

  QESSENCE Integrating Project
  SCALA Integrating Project

Spis treści

Spis symboli i oznaczeń

$\log \equiv \log_2$ — logarytm przy podstawie 2

ln — logarytm naturalny

i — jednostka urojona

$\mathbb{R}$ — zbiór liczb rzeczywistych

$Sp(2n, \mathbb{R})$ — zbiór macierzy symplektycznych rozmiaru $2n \times 2n$ o elementach rzeczywistych

$f \circ g$ — złożenie funkcji $(f \circ g)(x) = f(g(x))$

$[M]_{i,j}$ — element macierzy M znajdujący się na przecięciu i-tego wiersza z j-tą kolumną

X — zmienna losowa

$p_X, p_{X,Y}, p_{X|Y}$ — rozkłady prawdopodobieństwa, prawdopodobieństwa łącznego i prawdopodobieństwa warunkowego dyskretnych zmiennych losowych X, Y lub odpowiednie gęstości rozkładów prawdopodobieństwa dla zmiennych ciągłych

$p_x = P(X = x)$ — prawdopodobieństwo zdarzenia, że zmienna losowa X przyjmie wartość x

$\mathrm{E}(X)$ — wartość średnia zmiennej losowej X

$\sigma^2(X) = E(X^2)$ — wariancja zmiennej losowej X

F_n — n-elementowy rozkład jednorodny

$\binom{n}{m} = \frac{n!}{m!(n-m)!}$ — symbol Newtona

$\binom{n}{m_1,\ldots,m_w} = \frac{n!}{\prod_{i=1}^{w} m_i!}$ — uogólniony symbol Newtona;
zakłada się, że $\prod_{i=1}^{w} m_i = n, m_i \in \mathbb{N}^+$

$\Gamma_A, \Gamma_B, \Lambda$ — kanały komunikacyjne

S_i — nadawca o numerze i

$E = \{S_i\}_{i=1}^{n}$ — zbiór wszystkich nadawców; gdzie n to liczba nadawców

R — odbiorca

X_i^A — wejście kanału Γ_A kontrolowane przez i-tego nadawcę

x_i^A — symbol przesyłany przez nadawcę i przez kanał Γ_A

$X_S = \{X_i\}_{S_i \in S}$ — wejścia kanału kontrolowane przez nadawców należących do zbioru S

$x_S = \{x_i\}_{S_i \in S}$ — symbole przesyłane przez kanał przez nadawców należących do zbioru S

W_{j_i} — komunikat j od nadawcy i

Y^A - wyjście kanału Γ_A

$\mathcal{A}_{W_i}$ — zbiór komunikatów przesyłanych przez nadawcę i

$\mathcal{A}_{X_i}$ — alfabet symboli wejściowych kanału dostępnych dla nadawcy i

$\mathcal{A}_Y$ — alfabet symboli na wyjściu kanału

$H(X), H(X,Y), H(X|Y)$ — entropia klasyczna (Shannona), entropia łączna oraz entropia warunkowa

$S(\rho)$ — entropia kwantowa (von Neumana)

$g(\rho)$ — entropia stanu Gassowskiego

$I(X:Y)$ — informacja wzajemna

χ — pojemność Holevo

$\mathcal{C}$ — pojemność klasyczna

$\mathcal{C}^{(n)} = \frac{1}{n}\mathcal{C}$ — regularyzowana pojemność klasyczna

$\mathcal{R}$ — obszar pojemności klasycznej

$\mathcal{R}^{(n)} = \frac{1}{n}\mathcal{C}$ — regularyzowany obszar pojemności klasycznej

$\tilde{\mathcal{R}}$ — obszar pojemności klasycznej uzyskany dla zadanego rozkładu prawdopodobieństwa symboli wejściowych

R — prędkość transmisji osiągana w danym protokole

R_i — indywidualna prędkość transmisji osiągana w danym protokole przez nadawcę S_i

$R_S = \sum_{i \in S} R_i$ — konwencja sumacyjna; $S \subseteq E$ oznacza tu podzbiór nadawców

$R_T = \sum_{i \in E} R_i$ — łączna prędkość transmisji; E to zbiór wszystkich nadawców

$\mathcal{Q}$ — pojemność kwantowa

$\mathcal{P}$ — ograniczenia na średnią energię symboli wejściowych przypadającą na jedno użycie kanału (ograniczenie na średnią moc na wejściu kanału)

$\mathcal{H}$ — przestrzeń Hilberta

$\otimes$ — iloczyn tensorowy

$|\psi\rangle$ — wektor z przestrzeni Hilberta

$\langle\psi|$ — wektor sprzężony do $|\psi\rangle$

$\langle\psi|\phi\rangle$ — iloczyn skalarny wektorów $|\psi\rangle$ i $|\phi\rangle$

$\{|0\rangle, |1\rangle, \ldots, |n\rangle\}$ — baza standardowa w n wymiarowej przestrzeni Hilberta

$|e_i\rangle$, $|f_j\rangle$ — wektory z bazy standardowej

X, Y, Z, A, B — operatory w przestrzeni Hilberta

$X^\dagger$ — sprzężenie Hermitowskie operatora X

$\mathrm{tr}X$ — ślad operatora X

$\mathrm{tr}_A X$ — ślad częściowy operatora X po podsystemie A

U — operacja unitarna

$\mathcal{W}$ — operator przesunięcia (operator Weyla)

I — identyczność (operator identyczności)

$\{\sigma_X, \sigma_Y, \sigma_Z\}, \{X, Y, Z\}$ — macierze Pauliego

$\sigma_i \in \{I, \sigma_X, \sigma_Y, \sigma_Z\}$

E_i — elementy reprezentacji Kraussa

$|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle, |\phi^-\rangle$ — stany Bella

ρ — stan mieszany

ψ, e_i — projektory na stan $|\psi\rangle, |e_i\rangle$

$\{p_i, |\psi_i\rangle\}$ — mieszanina stanów czystych

$a^\dagger, a, N = a^\dagger a$ — operatory kreacji, anihilacji oraz liczby fotonów

$|\alpha\rangle$ — stan spójny

$|\xi\rangle$ — stany ściśnięty

$|\psi_r\rangle$ — stan ściśnięty wzdłuż zadanej kwadratury

γ — macierz kowariancji stanu Gaussowskiego

d — przesunięcie stanu Gaussowskiego

X — transformacja wektora przesunięcia wykonywana przez kanał Gaussowski

Y — szum wprowadzany przez kwantowy kanał Gaussowski

nat — jednostka ilości informacji mierzona przy użyciu logarytmu naturalnego; 1 [nat] $= \log_2 e$ [bitów]

Wprowadzenie

Tematyka podjętych w tej rozprawie rozważań wpisuje się w zapoczątkowany w latach '60 nurt badań, dotyczący wykorzystania układów kwantowych jako nośnika informacji klasycznej. Najważniejsze pytania stawiane w tej dziedzinie dotyczą ilości informacji, jaką zakodować można w stany układu kwantowego [65]; efektywnych sposobów kodowania i odzyskiwania tej informacji [51, 53, 75] oraz pojemności klasycznej $\mathcal{C}$ kanału kwantowego, czyli maksymalnej prędkości, z jaką można przesyłać informację przez ten kanał. Źródła wymienionych wyżej pytań znaleźć można w zagadnieniach odnoszących się niemalże bezpośrednio do zastosowań przemysłowych jak np. kodowanie informacji klasycznej w stany spójne światła emitowane przez laser [46, 78] oraz transmisja informacji przez optyczne kanały komunikacyjne [61]. Bogaty przegląd zagadnień oraz rezultatów z zakresu kwantowej komunikacji znaleźć można w pracy [90].

Rozwój kwantowej torii komunikacji przyczynił się do sformułowania nowych wielkości: pojemność prywatna $\mathcal{P}$ [21, 34], określająca maksymalną prędkość transmisji przez kanał w przypadku, gdy komunikat jest ukryty przed otoczeniem oraz pojemność kwantowa $\mathcal{Q}$ [15] związana z rozmiarem przestrzeni Hilberta stanów, które można przesyłać spójnie przez kanał. Dostęp do nowych zasobów w postaci stanów nieklasycznych, jak np. stany ściśnięte światła czy stany splątane, stał się impulsem dla rozważań nad tym, czy możliwe jest przekroczenie fundamentalnych ograniczeń dla zadań komunikacyjnych sformułowanych na bazie klasycznej teorii informacji [91, 12, 55]. Do szczególnie intrygujących osiągnięć na tym polu należą m.in. procedura gęstego kodowania [16] oraz odkryte niedawno tzw. kwantowe efekty aktywacji.

Terminem kwantowy efekt aktywacji określa się zjawisko synergii związane ze wzrostem przydatności dwóch zasobów w zadaniach komunikacyjnych na skutek ich równoczesnego wykorzystania lub oddziaływania ze sobą.

Historycznie efekt ten wiąże się z aktywacją splątania związanego (ang. bound entanglement) [59] i superaddytywnością splątania destylowalnego (ang. distillable entanglement) [82].

W kontekście kanałów komunikacyjnych, znane obecnie kwantowe efekty aktywacji to: (i) superaddytywność pojemności kwantowej w scenariuszach z wieloma nadawcami i z dodatkowymi zasobami [36], (ii) superaddytywność $\mathcal{Q}$ w podstawowym scenariuszu 1-do-1 [92], (iii) superaddytywność pojemności prywatnej [66] oraz (iv) superaddytywność pojemności klasycznej w scenariuszach z jednym [49] i z wieloma nadawcami [28].

W pracy tej zajmować się będziemy ostatnim z wymienionych wyżej kwantowych efektów aktywacji — aktywacją obszarów pojemności klasycznej w wielodostępnych kanałach kwantowych.

Dwa podstawowe pojęcia, wokół których obracają się przedstawione dalej dociekania to *kanał kwantowy* oraz *pojemność Holevo*.

Kanał kwantowy to fizycznie realizowalne odwzorowanie operatorów gęstości w operatory gęstości. Operator gęstości opisuje w tym przypadku stan układu kwantowego, będącego nośnikiem informacji klasycznej. Kanał kwantowy, w kontekście kwantowej teorii informacji, jest rozszerzeniem pojęcia klasycznego kanału komunikacyjnego. Pozwala on na modelowanie oddziaływania układu kwantowego z otoczeniem oraz modelowaniem wprowadzanego przez to oddziaływanie szumu [72, 20, 42]. Kanał kwantowy może być używany do spójnej transmisji stanów kwantowych (transmisja informacji kwantowej) [9, 8] oraz transmisji informacji klasycznej zakodowanej w odpowiednie stany kwantowe [53].

Wielodostępowe kanały kwantowe to kanały kwantowe, w których występuje jeden odbiorca i co najmniej 2 nadawców. Istotne w tym przypadku jest to, że nadawcy działają niezależnie od siebie i nie mogą się ze sobą komunikować.

Pojemność Holevo χ odnosi się do górnego ograniczenia na ilość informacji klasycznej, którą można przekazać w schematach komunikacyjnych opartych o układy kwantowe [52]. Kodowanie Holevo - Schumacher - Westmoreland [53, 75] pokazało, jak można osiągnąć pojemność Holevo χ realizując zadanie bezbłędnej transmisji informacji klasycznej przez kanały kwantowe. Kodowanie HSW pozwoliło uznać pojemność Holevo za podstawową miarę użyteczności kanału kwantowego w transmisji informacji klasycznej oraz związać ją z maksymalną prędkością transmisji informacji klasycznej — pojemnością klasyczną $\mathcal{C}$ kanału. Pojemność Holevo oraz twierdzenie HSW stanowią w kontekście kanałów kwantowych analog twierdzenia Shannona [77] o kodowaniu

dla kanałów z szumem. W przypadku kanałów wielodostępowych wprowadza się, w oparciu o pojemność Holevo, pojęcie obszaru osiągalnych prędkości transmisji $\mathcal{R}$. W skrócie obszar ten będzie nazywany obszarem pojemności.

Punktem wyjścia dla opisanych w tej pracy badań było pytanie o rolę splątania w zadaniach związanych z komunikacją klasyczną przez kanały kwantowe oraz hipoteza o addytywności pojemności Holevo χ [12, 13, 54]. Dla dwóch pracujących równolegle kanałów kwantowych Φ oraz Γ zachodzi zawsze $\chi(\Phi) + \chi(\Gamma) \leq \chi(\Phi \otimes \Gamma)$, przy czym zapis $\Phi \otimes \Gamma$ oznacza równoległe połączenie kanałów. Addytywność pojemności Holevo χ ma miejsce jeżeli:

$$\chi(\Phi) + \chi(\Gamma) = \chi(\Phi \otimes \Gamma). \tag{1}$$

Hipoteza o addytywności pojemności Holevo mówi, że wzór (1) jest prawdziwy dla dowolnej pary kanałów kwantowych. W analogiczny sposób formułuje się hipotezę o addytywności regularyzowanej pojemności klasycznej:

$$\mathcal{C}^{(\infty)}(\Phi) + \mathcal{C}^{(\infty)} = \mathcal{C}^{(\infty)}(\Phi \otimes \Gamma). \tag{2}$$

Na rzecz hipotezy o addytywności pojemności χ przemawiało wiele wyników cząstkowych pokazujących, że addytywność zachodzi w przypadkach gdy jeden z kanałów to: kanał łamiący splątanie [79], kanał depolaryzujący [63], kanał identycznościowy [76], qubitowy kanał unitalny [62]. Argumentem w dyskusji była również addytywność pojemności dla klasycznych kanałów informacyjnych. W momencie podjęcia przedstawionych w tej pracy badań, pomimo dużego wysiłku środowiska naukowego, pytanie o addytywność pojemności Holevo χ dla dowolnej pary kanałów pozostawało trudnym, otwartym problem [81].

Pytanie o addytywność pojemności Holevo χ ma podstawowe znaczenie w zagadnieniach dotyczących oceny przydatności kanału kwantowego do komunikacji klasycznej. Addytywność pojemności Holevo oznacza istnienie formuł jednowyrazowych opisujących pojemność klasyczną $\mathcal{C}$ kanału, co wiąże się z istotną redukcją złożoności obliczeniowej problemu wyznaczania $\mathcal{C}$. Skutkiem addytywności jest także zasadnicze ograniczenie zbioru stanów kodowych osiągających pojemność klasyczną do stanów produktowych. Z drugiej strony, łamanie addytywności χ, czyli tzw. superaddywność χ, wskazuje na splątanie jako podstawę nowych technik radzenia sobie z szumem oraz na możliwość kwantowej aktywacji kanałów bezużytecznych do celów komunikacyjnych.

Głównym celem badań prowadzonych przeze mnie w ramach pracy doktorskiej była analiza komunikacji klasycznej przez kwantowe kanały wielodostępne ze szczególnym uwzględnieniem problematyki kwantowego efektu aktywacji. Tak zarysowany program badawczy wiązał się z:

- uogólnieniem pytania o addytywność pojemności Holevo χ na przypadek kwantowych kanałów wielodostępnych oraz wyrażeniem tego pytania w terminach obszarów pojemności klasycznej;
- konstrukcją przykładów wielodostępnych kanałów kwantowych, dla których występuje kwantowy efekt aktywacji obszarów pojemności klasycznej;
- wskazaniem źródeł oraz rodzajów aktywacji w tychże kanałach;
- propozycją schematu doświadczalnego obrazującego efekt aktywacji.

Przedstawione w tej pracy sprawozdanie z uzyskanych wyników ma następujący układ: w rozdziale 1 przedstawione zostały podstawowe zagadnienia z zakresu klasycznej i kwantowej torii informacji, wprowadzony również został formalizm macierzy kowariancji wykorzystywany w kontekście transmisji informacji klasycznej przez kanały Gaussowskie.

Rozdział 2 dotyczy efektów aktywacji w kanałach kwantowych działających w przestrzeniach o skończonym wymiarze. W części 2.1 prezentowane jest twierdzenie o addytywności obszarów pojemności dla kanałów klasycznych z wieloma nadawcami. W części 2.3.1 pojawia się pierwszy przykład aktywacji. Jest to aktywacja typu (i) polegająca na superaddytywności maksymalnej indywidualnej prędkości transmisji R_i przy zachowaniu addytywności łącznej prędkości transmisji R_T. Przykład został skonstruowany w oparciu o schemat gęstego kodowania. Następnie, w części 2.3.2, analizowany jest przykład aktywacji dla pracujących równolegle dwóch kopii tego samego kanału. Jest to przypadek, w którym pojemność klasyczna kanału nie może być wyrażona w postaci jednowyrazowej formuły Holevo. Analiza tego zagadnienia jest kontynuowana w części 2.3.3, gdzie badany jest wpływ splątania wielocząstkowego na obszar pojemności klasycznej. Część 2.3.4 zawiera przykłady efektów aktywacji dla regularyzowanych obszarów pojemności, których nie można wyrazić w postaci jednowyrazowych formuł Holevo. Występowanie efektu superaddytywności dla wielkości asymptotycznych wskazuje na kwantowy efekt aktywacji jako immanentną cechę wielodostępnych kanałów

kwantowych a nie tylko odbicie pewnych własności pojemności Holevo. Na koniec, w części 2.3.5 przedstawione zostaną przykłady kanałów pokazujące aktywację typu (ii) — aktywację łącznej prędkości transmisji R_T.

Rozdział 3 zawiera propozycje eksperymentów z obszaru optyki kwantowej obrazujących efekt aktywacji w kanałach Gaussowskich. W części 3.1 wprowadzone zostaje uogólnienie twierdzenia o addytywności obszarów pojemności klasycznej — tzw. zasada lokalności. Części 3.5.1 oraz 3.5.3 dostarczają dwa przykłady kanałów Gaussowskich wykazujących efekt aktywacji przy współpracy z idealnym kanałem jednomodowym. Pierwszy z przykładów to kanał zbudowany w oparciu o dzielnik wiązki, drugi to kanał składający się z niedestruktywnych bramek sumujących. W części 3.5.2 analizowany jest wpływ wyboru stanów kodowych na efekt aktywacji pod kątem zapotrzebowania na poziom ściśnięcia w transmitowanych jedno- i dwumodowych stanach ściśniętych. Rozważania te mogą być interesujące ze względu na konsekwencje efektu aktywacji dla światłowodowych sieci komunikacyjnych. Propozycje eksperymentów opisane w częściach 3.5.1 oraz 3.5.3 konfrontowane są w części 3.5.4 z ograniczeniami wynikającymi ze stanu współczesnej techniki eksperymentalnej w zakresie optyki kwantowej. Wyniki analiz przedstawionych w części 3.5.4 wydają się być optymistyczne sugerując, że przy obecnym poziomie techniki efekt aktywacji można uzyskać bez konieczności uciekania się do postselekcji wyników.

Rozdziały 2 oraz 3 zawierają część „Wyniki”, w której zebrany został nowy materiał uzyskany w trakcie prowadzonych przez Autora badań. Część „Otwarte pytania” omawia problemy, których niestety nie udało się rozwiązać w trakcie tych badań, a które wydają się być istotne dla dalszego zrozumienia problematyki kwantowej aktywacji obszarów pojemności klasycznej.

Rozdział 1

Preliminaria

Celem tego rozdziału jest zapoznanie czytelnika z używanym dalej aparatem pojęciowym. Został tutaj zebrany oraz usystematyzowany materiał z zakresu klasycznej i kwantowej teorii informacji, przy czym szczególną uwagę zwrócono na klasyczne źródła koncepcji takich jak kodowanie czy pojemność, zaadaptowanych później przez kwantową teorię informacji. Czytelnik znajdzie tu również opis technik służących do analizy stanów oraz kanałów Gaussowskich w kontekście transmisji informacji klasycznej. Starano się podkreślić naturalny związek tych technik z eksperymentami z zakresu optyki kwantowej.

Większość definicji i twierdzeń dotyczących klasycznej teorii informacji przytoczone jest za [25], z kolei opis formalizmu macierzy kowariancji oparty został na pracy [88].

1.1 Klasyczna teoria informacji

1.1.1 Entropia, entropia warunkowa i informacja wzajemna

Entropia Shannona to podstawowe pojęcie klasycznej teorii informacji. Rozumie się ją jako średnią *niepewność* odnośnie wartości zmiennej losowej X, zanim wartość ta zostanie poznana, lub komplementarnie jako średnią ilość informacji otrzymanej wraz z poznaniem wartości X.

Definicja 1.1 *Niech X będzie dyskretną zmienną losową nad alfabetem $\mathcal{A}_X$ z rozkładem prawdopodobieństwa $p_X = P(X = x)$. Entropia Shannona zmien-*

nej losowej X określona jest wzorem:

$$H(X) = -\sum_{x \in \mathcal{A}_X} p_X \log p_X \tag{1.1}$$

przy czym przyjmuje się, że $0 \log 0 = 0$.

Entropia zmiennej losowej X o rozkładzie jednorodnym nad zbiorem m-elementowym wynosi $H(X) = m \log m$.

Pojęcie entropii Shannona można rozszerzyć na dowolną liczbę zmiennych losowych:

Definicja 1.2 *Niech $X, Y, \ldots$ będą dyskretnymi zmiennymi losowymi o łącznym rozkładzie prawdopodobieństwa $p_{X,Y,\ldots}$. Wówczas entropia łączna wyraża się jako:*

$$H(X, Y, \ldots) = -\sum_{x \in \mathcal{A}_X, y \in \mathcal{A}_Y, \ldots} p_{X,Y,\ldots} \log p_{X,Y,\ldots}. \tag{1.2}$$

Entropia łączna osiąga wartość maksymalną, gdy zmienne losowe $X, Y, \ldots$ są niezależne. Własność ta to subaddytywność entropii. Wyraża się ona formułą:

$$H(X, Y, \ldots) \leq H(X) + H(Y) + \ldots. \tag{1.3}$$

Ponadto entropia posiada również własność silnej subaddytywności. Dla dowolnych trzech zmiennych losowych X, Y, Z zachodzi:

$$H(X, Y, Z) + H(Z) \leq H(X, Y) + H(Y, Z). \tag{1.4}$$

Skupmy się teraz na przypadku dwóch zmiennych losowych X, Y. Entropia łączna $H(X, Y)$ mierzy całkowitą niepewność odnośnie wartości zmiennych losowych X, Y. Entropia zmiennej losowej Y, jeśli znana jest wartość zmiennej losowej $X = x$, wynosi $H(Y|X = x) = \sum_y -p_{Y|X=x} \log p_{Y|X=x}$. Stosując to pojęcie można wprowadzić entropię warunkową, która mierzy średnią niepewność zmiennej losowej Y przy znanej wartości zmiennej losowej X.

Definicja 1.3 *Entropia warunkowa zdefiniowana jest wzorem:*

$$H(Y|X) = \sum_{x \in \mathcal{A}_X} p_x H(Y|X = x) \tag{1.5}$$

$$= -\sum_{x \in \mathcal{A}_X, y \in \mathcal{A}_Y} p_{x,y} \log p_{y|x}, \tag{1.6}$$

gdzie p_x jest brzegowym rozkładem prawdopodobieństwa zmiennej losowej X.

Wartości zmiennej losowej X dostarcza $H(X)$ bitów informacji o parze zmiennych losowych (X, Y). Entropia warunkowa $H(Y|X)$ wyraża, ile informacji brakuje jeszcze do pełnego określenia wartości pary (X, Y). Fakt ten można zapisać wzorem:

$$H(X, Y) = H(X) + H(Y|X). \tag{1.7}$$

Dostęp do nowych informacji zmniejsza naszą niepewność odnośnie zmiennej losowej, co formalnie wyraża się w postaci:

$$H(X|YZ) \leq H(X|Y), \tag{1.8}$$

gdzie X, Y, Z to zmienne losowe o łącznym rozkładzie prawdopodobieństwa $p_{x,y,z}$.

Ilość informacji, jaką niesie wartość zmiennej losowej X o wartości Y, dana jest przez informację wzajemną[1].

Definicja 1.4 *Informacja wzajemna między zmiennymi losowymi X i Y wyraża się wzorem:*

$$I(X : Y) = \sum_{x \in \mathcal{A}_X, y \in \mathcal{A}_Y} p_{x,y} \log \frac{p_{x,y}}{p_x p_y}. \tag{1.9}$$

Informacja wzajemna określa redukcję niepewności zmiennej losowej Y dzięki znajomości wartości zmiennej losowej X, tzn.:

$$I(X : Y) = H(Y) - H(Y|X). \tag{1.10}$$

Informacja wzajemna spełnia następującą regułę łańcuchową:

$$I(X, Y : Z) = I(X : Z|Y) + I(Y : Z), \tag{1.11}$$

gdzie $I(X : Z|Y) = H(Z|Y) - H(Z|XY)$ to warunkowa informacja wzajemna.

Analogiem pojęcia entropii dla ciągłych zmiennych losowych jest entropia różnicowa:

Definicja 1.5 *Entropia różnicowa ciągłej zmiennej losowej X o gęstości rozkładu prawdopodobieństwa p_x nad zbiorem $\mathcal{A}_X$ ma postać:*

$$h(X) = -\int_{\mathcal{A}_X} p_x \ln p_x dx. \tag{1.12}$$

[1] Informacja wzajemna jest wielkością symetryczną, tzn. określa ona również ilość informacji jaką wartość zmiennej losowej Y o wartości X

Entropia różnicowa dla m wymiarowej zmiennej losowej o rozkładzie normalnym z macierzą kowariancji γ wynosi:

$$h(X) = -\int_{-\infty}^{+\infty} d^m\bar{x} p_{\bar{x}} \ln p_{\bar{x}} = \frac{1}{2} \ln 2\pi e \det \gamma \tag{1.13}$$

Pojęcia różnicowej entropii łącznej, różnicowej entropii warunkowej oraz informacji wzajemnej można zdefiniować dla ciągłych zmiennych losowych w sposób analogiczny, jak ma to miejsce w przypadku zmiennych dyskretnych.

1.1.2 Kanał komunikacyjny

W tym podrozdziale przyjrzymy się procesowi komunikacji pomiędzy nadawcą (Alicją) a odbiorcą (Bobem). Celem tego procesu jest bezbłędne przekazanie komunikatu od nadawcy do odbiorcy i może on składać się z kilku etapów. Każdy z etapów rozpoczyna się od zakodowania komunikatu w wybraną wielkość fizyczną X (np. natężenie pola elektromagnetycznego). Po zakodowaniu następuje przekazywanie sygnału od nadawcy do odbiorcy, co wiąże się z określonym zjawiskiem fizycznym (np. propagacją fal elektromagnetycznych), które decyduje o formie odwzorowania pomiędzy X a otrzymaną przez Boba wielkością Y. Na podstawie wartości Y, Bob stara się określić jaki komunikat nadała Alicja. Proces fizyczny stojący za przekazaniem sygnału może wprowadzać niekontrolowane i losowe zakłócenia (np. zakłócenia wynikające z promieniowania tła, rozpraszanie fali elektromagnetycznej na przeszkodach) co prowadzi do zniekształcenia komunikatu odebranego przez Boba. Jeśli Alicja i Bob zgadzają się odnośnie do tego jaki komunikat został nadany, wówczas komunikacja kończy się sukcesem.

Kanał komunikacyjny jest matematycznym modelem niedeterministycznego procesu przekazywania sygnału fizycznego od Alicji do Boba. Wybrany przez Alicję zbiór sygnałów stanowi alfabet wejściowy $\mathcal{A}_X$ natomiast wyniki, które może otrzymać Bob to alfabet wyjściowy $\mathcal{A}_Y$. Wartość sygnału x przesyłanego przez Alicję to *symbol wejściowy*, wartość y otrzymana przez Boba to *symbol wyjściowy*. W pracy rozważane są tylko przypadki komunikacji w czasie dyskretnym, tzn. takie w których liczba użyć kanału w całym procesie komunikacji jest skończona.

Definicja 1.6 *Kanał komunikacyjny* $\Gamma : \mathcal{A}_X \mapsto \mathcal{A}_Y$ *to odwzorowanie stochastyczne opisane przez trójkę:* $(\mathcal{A}_X, \mathcal{A}_Y, p_{y|x})$ *gdzie* $\mathcal{A}_X$ *jest alfabetem wejściowym,* $\mathcal{A}_Y$ *jest alfabetem wyjściowym a* $p_{y|x}$ *określa prawdopodobieństwo otrzy-*

mania symbolu y, jeśli nadany został symbol x. $p_{Y|X}$ nazywać będziemy prawdopodobieństwem przejścia. Kanał nazywamy bezpamięciowym, jeżeli prawdopodobieństwo otrzymania na wyjściu symbolu y nie zależy od tego, jakie symbole były przesyłane podczas poprzednich użyć kanału. Jeśli $\mathcal{A}_X$ oraz $\mathcal{A}_Y$ są zbiorami skończonymi, to kanał nazywamy kanałem dyskretnym (kanałem w zmiennych dyskretnych), jeśli natomiast $\mathcal{A}_X$ oraz $\mathcal{A}_Y$ są izomorficzne ze zbiorem liczb rzeczywistych $\mathbb{R}$, to kanał nazywamy kanałem ciągłym (kanałem w zmiennych ciągłych).

Definicja 1.7 *Niech Γ_A, Γ_B będą kanałami bezpamięciowymi. $\mathcal{A}_{X^A}$, $\mathcal{A}_{X^B}$ to alfabety wejściowe, $\mathcal{A}_{Y^A}$, $\mathcal{A}_{Y^B}$ to alfabety wyjściowe a $p_{Y^A|X^A}, p_{Y^B|X^A}$ to prawdopodobieństwa otrzymania określonego symbolu wyjściowego przy zadanym symbolu wejściowym dla każdego z kanałów. Połączenie równoległe $\Gamma_A \otimes \Gamma_B$ kanałów bezpamięciowych to kanał w postaci:*

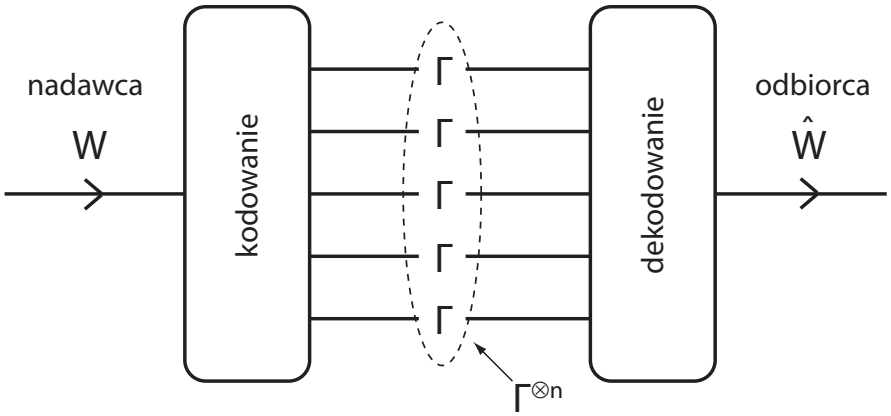
$$\Gamma_{AB} = (\mathcal{A}_{X^{AB}} = \mathcal{A}_{X^A} \times \mathcal{A}_{X^B}, \mathcal{A}_{Y^{AB}} = \mathcal{A}_{Y^A} \times \mathcal{A}_{Y^B}, p_{Y^{AB}|X^{AB}} = p_{Y^A|X^A} p_{Y^B|X^B}). \tag{1.14}$$

Wejście i wyjście kanału Γ_{AB} stanowią pary złożone odpowiednio z symboli wejściowych i wyjściowych kanałów Γ_A oraz Γ_B. W definicji zakładamy, że podczas procesu komunikacji nadawca nie dostaje żadnej informacji zwrotnej od odbiorcy. Połączenie równoległe n kopii tego samego kanału Γ będzie oznaczane przez $\Gamma^{\otimes} n$.

Przykład 1.1 *Wprowadzone przed chwilą pojęcia użyjemy do opisu transmisji sygnału binarnego przez światłowód jednomodowy. Układ taki można modelować za pomocą kanału binarnego [25]. Alfabet wejściowy i wyjściowy ma w tym przypadku postać $\mathcal{A}_X = \mathcal{A}_Y = \{0, 1\}$. Kanał jest symetryczny: z prawdopodobieństwem $1 - p$ transmisja przebiega bezbłędnie i kanał realizuje odwzorowanie $y = x$, natomiast z prawdopodobieństwem p kanał zamienia symbol na przeciwny $y = 1 - x$. W przypadku transmisji z prędkością $10[Gbit/s]$ na odcinku $100[km]$ obecnie osiąga się prawdopodobieństwo błędu p na poziomie 10^{-20}, natomiast na odcinku $160[km]$ prawdopodobieństwo błędu wzrasta do 10^{-2} [18].*

1.1.3 Pojemność dyskretnego kanału komunikacyjnego oraz twierdzenie o kodowaniu

Transmisja przez niedeterministyczny kanał komunikacyjny może zakończyć się sukcesem — odbiorca (Bob) oraz nadawca (Alicja) zgadzają się co do tego



Rysunek 1.1: Schemat transmisji zakodowanego komunikatu W przy użyciu n kopi kanału Γ. Komunikat zdekodowany przez odbiorcę to $\hat{W}$. Strzałki pokazują kierunek transmisji.

jaki komunikat został przesłany przez kanał — lub niepowodzeniem — na podstawie odebranego sygnału Bob sądzi, że Alicja wysłała inny komunikat niż miało to miejsce w rzeczywistości. Celem Alicji i Boba jest minimalizacja prawdopodobieństwa takiego zdarzenia. Osiągają to poprzez zastosowanie procedury nazywanej kodowaniem (porównaj [25]).

Niech $\mathcal{A}_W = \{W_i\}$ będzie zbiorem komunikatów, które może przesyłać nadawca. Rozmiar zbioru $\mathcal{A}_W$ wynosi M. Zakładamy, że każdy z komunikatów jest przesyłany z równym prawdopodobieństwem. Transmisja zakodowanego komunikatu odbywa się poprzez n kopi kanał Γ i składa się z następujących etapów (patrz Rys. 1.1):

1. Odwzorowanie za pomocą funkcji kodującej $f : \mathcal{A}_W \mapsto \mathcal{A}_{X^{\otimes n}}$ komunikatu nadawcy w n elementową sekwencję symboli wejściowych kanału Γ. Sekwencja $f(W_i)$ to *słowo kodowe*. Zbiór wszystkich słów kodowych używanych podczas transmisji tworzy *słownik kodowy* o rozmiarze M.

2. Transmisja słowa kodowego przez kanał $\Gamma^{\otimes n}$.

3. Dekodowanie na podstawie sekwencji symboli wyjściowych komunikatu wejściowego za pomocą funkcji $g : \mathcal{A}_{Y^{\otimes n}} \mapsto \mathcal{A}_W$.

Przed przystąpieniem do transmisji, obie strony ustalają postać funkcji f, g oraz zbioru komunikatów $\mathcal{A}_W$.

Definicja 1.8 *Kodem (M, n) dla kanału Γ nazywamy trójkę złożoną z $(f, g, \mathcal{A}_W)$.*

Słownik kodowy określa warunkowy rozkład prawdopodobieństwa symboli uzyskanych na wyjściu $\Gamma^{\otimes n}$ w przypadku, gdy nadano komunikat W. Celem kodowanie jest minimalizacja prawdopodobieństwa, że w wyniku transmisji dwóch różnych komunikatów otrzymamy taką samą sekwencję symboli ma wyjściu $\Gamma^{\otimes n}$. Cel ten osiągany jest dzięki nadmiarowości informacyjnej kodu: rozmiar słownika kodowego jest mniejszy od liczby wszystkich sekwencji, które można przesłać przez kanał $\Gamma^{\otimes n}$, a słowa kodowe są od siebie na tyle odległe, że prawdopodobieństwo, iż podczas transmisji dwa słowa kodowe zostaną przekształcone w taki sam ciąg symboli jest małe.

Definicja 1.9 *Prędkość transmisji R dla kodu (M, n) dana jest wzorem:*

$$R = \frac{\log M}{n} \text{ [bitów / pojedyńcze użycie kanału].} \tag{1.15}$$

Definicja 1.10 *Maksymalne prawdopodobieństwo błędu $\lambda^{(n)}$ dla kodu (M, n) i kanału Γ określa formuła:*

$$\lambda^{(n)} = \max_W P(g(\Gamma^{\otimes n}(f(W))) \neq W), \tag{1.16}$$

gdzie maksymalizacja odbywa się po całym zbiorze komunikatów.

$\lambda^{(n)}$ to maksymalne prawdopodobieństwo zdarzenia, że odbiorca i nadawca nie zgadzają się co do tego, jaki komunikat został przesłany.

Definicja 1.11 *Prędkość transmisji R jest osiągalna jeżeli istnieje ciąg kodów $(2^{nR}, n)$ takich, że maksymalne prawdopodobieństwo błędów $\lambda^{(n)} \to 0$ wraz z $n \to \infty$.*

Wielkością charakteryzującą kanał komunikacyjny jest jego *pojemność informacyjna* $\mathcal{C}$.

Definicja 1.12 *Pojemność dyskretnego bezpamięciowego kanału komunikacyjnego dana jest wzorem:*

$$\mathcal{C}(\Gamma) = \max_{p_X} I(X : Y). \tag{1.17}$$

Informacja wzajemna $I(X : Y)$ liczona jest dla rozkładu prawdopodobieństwa $p_{X,Y} = p_{Y|X} p_X$, gdzie $p_{Y|X}$ pochodzi z definicji kanału. Maksymalizacja odbywa się po wszystkich rozkładach prawdopodobieństwa p_X nad $\mathcal{A}_X$.

Rozmiar alfabetów $\mathcal{A}_X, \mathcal{A}_Y$ wprowadza ograniczenie na pojemność kanału:

$$\mathcal{C}(\Gamma) \leq \log |\mathcal{A}_X|, \mathcal{C}(\Gamma) \leq \log |\mathcal{A}_Y|. \tag{1.18}$$

Twierdzenie 1.1 *(Shannona o kodowaniu dla kanału komunikacyjnego): Dla kanału komunikacyjnego* Γ *osiągalne są te prędkości transmisji* R*, dla których zachodzi:*

$$R < \mathcal{C}(\Gamma). \tag{1.19}$$

Nie można osiągnąć prędkości transmisji $R > \mathcal{C}(\Gamma)$*.*

Dowód twierdzenia 1.1 zawiera konstrukcję kodów losowych osiągających zadaną prędkość transmisji.

1.1.4 Kanał Gaussowski

Kanał Gaussowski modeluje sytuację, w której do sygnału dodawany jest biały szum. Jest to przykład kanału w zmiennych ciągłych. Opisuje on dobrze komunikację satelitarną oraz przypadki, w których sygnał transmitowany jest przy użyciu pojedynczej wiązki. Źródłem zakłóceń mogą być tu: szum śrutowy, szum termiczny w nadajnikach i odbiornikach, promieniowanie elektromagnetyczne tła itp. Kanały Gaussowskie nie pozwalają na opis takich efektów jak interferencja, zjawiska nieliniowe czy echo, pomimo to stanowią podstawowe narzędzie w analizie pojemności, w przypadku gdy sygnał może przyjmować wartości z pewnego przedziału liczb rzeczywistych.

Definicja 1.13 *Kanał Gaussowski* $\Gamma : \mathcal{A}_X \mapsto \mathcal{A}_Y$*, gdzie* $\mathcal{A}_X = \mathcal{A}_Y = \mathbb{R}$*, to odwzorowanie stochastyczne, dla którego zależność między wejściem a wyjściem dana jest formułą:*

$$Y = X + Z. \tag{1.20}$$

Z *jest zmienną losową o rozkładzie normalnym ze średnią równą* 0 *i wariancją* σ^2_{szum}*.*

W przypadku komunikacji przez kanał Gaussowski mamy do czynienia ze schematem analogicznym do tego, z którym spotkaliśmy się w kontekście kanałów dyskretnych (porównaj Rys. 1.1). W obu przypadkach zbiór przesyłanych komunikatów jest skończony. Tym razem jednak komunikaty kodowane są w sekwencje liczb rzeczywistych.

Gdy $\mathcal{A}_Y = \mathbb{R}$, nadawca może wybrać dowolnie duży alfabet symboli wejściowych odsuniętych od siebie dowolnie daleko. Przy skończonym poziomie szumu σ^2_{szum}, prawdopodobieństwo błędnej interpretacji symbolu na wyjściu kanału maleje do zera, czego rezultatem jest nieskończona pojemność kanału (patrz Rw. (1.17)). Aby nadać fizyczne znaczenie pojemności kanału Gaussowskiego, muszą zatem zostać nałożone pewne ograniczenia na rozkład prawdopodobieństwa symboli wejściowych. Powszechnie stosuje się ograniczenie $\mathcal{P}$ na średnią moc (średnią energię przypadającą na użycie kanału) [25]:

$$\mathcal{P} : \sigma^2(X) \leq \sigma^2_{we}. \tag{1.21}$$

Ograniczenie to można rozumieć jako średnią ilość energii, którą nadawca może wykorzystać w procesie komunikacji (ilość energii dostarczanej przez elektrownię) lub jako wytrzymałość kanału (przekroczenie ograniczenia na średnią energię może prowadzić do zniszczenia kanału). Pojemność kanału Γ w zmiennych ciągłych będziemy więc rozumieli jako:

$$\mathcal{C}(\Gamma) = \max_{p_X : \sigma^2(X) \leq \sigma^2_{we}} I(X:Y). \tag{1.22}$$

Twierdzenie 1.2 *Pojemność kanału Gaussowskiego Γ ze średnim natężeniem szumu σ^2_{szum} oraz ograniczeniem na moc $\mathcal{P} : \sigma^2_{we}$ wynosi:*

$$\mathcal{C}(\Gamma) = \frac{1}{2} \ln \left(1 + \frac{\sigma^2_{we}}{\sigma^2_{szum}} \right) \textit{[natów/pojedyńcze użycie kanału]}. \tag{1.23}$$

Pojemność ta jest osiągana przez X o rozkładzie Gaussa z $\sigma^2(X) = \sigma^2_{we}$ i $\mathrm{E}(X) = 0$.

Iloraz $SNR = \sigma^2_{we}/\sigma^2_{szum}$ określa stosunek poziomu sygnału do szumu.

Dla kanałów Gaussowskich można zdefiniować, analogicznie jak w przypadku kanałów dyskretnych: kodowanie (M, n), szybkość transmisji R dla kodowania (M, n) oraz osiągalność R. Kodowanie musi spełniać warunek (1.21).

Twierdzenie 1.3 *(Twierdzenie o kodowaniu dla kanału Gaussowskiego): Dla kanału Gaussowskiego ze średnim natężeniem szumu σ^2_{szum} oraz ograniczeniem na moc $\mathcal{P} : \sigma^2_{we}$, prędkość transmisji R jest osiągalna jeśli:*

$$R < \mathcal{C}(\Gamma). \tag{1.24}$$

Nie można osiągnąć prędkość transmisji $R > \mathcal{C}(\Gamma)$. $\mathcal{C}(\Gamma)$ dane jest wzorem (1.23) (porównaj twierdzenie 1.1).

1.1.5 Kanał wielodostępny

Kanał wielodostępny pozwala opisać sytuację, w której występuje co najmniej dwóch nadawców i jeden odbiorca. Tak jak w przypadku kanałów 1-do-1, aby wysłać komunikat nadawcy kodują go w sekwencje symboli przekazywanych przez kanał. Za każdym razem, gdy kanał jest używany, przekazywana jest sekwencja zawierająca po jednym symbolu od każdego z nadawców, tzn. kanał pracuje w trybie synchronicznym[2]. Przed przystąpieniem do transmisji wszystkie strony zgadzają się na używanie określonego kodu. Podczas transmisji nie mogą już jednak współpracować - nadawcy przesyłają komunikaty niezależnie od siebie, żaden nadawca nie wie, jakie symbole przesyłają w danej chwili pozostali nadawcy[3]. Odbiorca, na podstawie odebranych symboli, stara się określić jaki komunikat wysłał każdy z nadawców. Transmisja kończy się niepowodzeniem, jeśli komunikat od któregokolwiek z nadawców został źle odczytany. Kodowanie w przypadku kanałów wielodostępnych musi radzić sobie nie tylko z szumem wprowadzanym przez kanał, ale również z interferencją sygnałów pochodzących od różnych nadawców. Pojęcie kanału wielodostępnego pojawia się w naturalny sposób w wielu rzeczywistych systemach, jak np. satelitarne systemy łączności czy sieci mobilne, szczególnie w kontekście transmisji uplink tj. od telefonu komórkowego do stacji bazowej.

Definicja 1.14 *Kanał wielodostępny z k nadawcami to odwzorowanie stochastyczne $\Gamma : \mathcal{A}_{X_1} \times \ldots \otimes \mathcal{A}_{X_n} \mapsto \mathcal{A}_Y$, gdzie $\mathcal{A}_{X_i}$ jest alfabetem symboli związanym z wejściem X_i, kontrolowanym przez nadawcę S_i. Relacja między wyjściem kanału a jego wejściami określona jest rozkładem prawdopodobieństwa $p_{Y|X_1,\ldots,X_k}$.*

Definicja 1.15 *Kod $(\{M_i\}, n)$ dla kanału wielodostępnego Γ jest trójką złożoną z $(\{f_i\}, g, \{\mathcal{A}_{W_i}\})$. f_i to funkcja kodująca nadawcy S_i a $\mathcal{A}_{W_i}$ to zbiór jego komunikatów. Rozmiar zbioru komunikatów $\mathcal{A}_{W_i}$ wynosi M_i. g oznacza funkcję dekodującą. Podczas każdej transmisji przesyłana jest sekwencja $(f_1(W_1), \ldots, f_k(W_k))$, gdzie W_i jest komunikatem od nadawcy S_i.*

[2]Wiadomości na temat asynchronicznej transmisji przez kanały wielodostępne można znaleźć w pracy [24]. Scenariusz, w którym równoczesna transmisja przez kanał kończy się zawsze utratą komunikatu (kanał kolizyjny), badany jest m.in. w pracy [69]. Wzbogacenie kanału kolizyjnego o informację zwrotną dla nadawców o wystąpieniu kolizji prowadzi bezpośrednio do modeli wczesnych lokalnych sieci komputerowych (ALOHA, Ethernet).

[3]Wpływ współpracy-korelacji między nadawcami na pojemność kanału wielodostępnego analizowany był m.in w pracy [83].

Definicja 1.16 *Maksymalne prawdopodobieństwo błędu* $\lambda^{(n)}$ *dla kodu* $(\{M_i\}, n)$ *określa wzór:*

$$\lambda^{(n)} = \max_{(W_1,\ldots,W_k)} P(g(\Gamma^{\otimes n}(f(W_1),\ldots,f(W_k))) \neq (W_1,\ldots,W_k)), \qquad (1.25)$$

przy czym maksimum liczymy po wszystkich sekwencjach $(W_1,\ldots,W_k) \in \mathcal{A}_{X_1} \times \mathcal{A}_{X_1}$*. Zwróćmy uwagę, że błąd podczas transmisji występuje wtedy, gdy przynajmniej jeden komunikat zostanie odkodowany niepoprawnie.*

Z kodem $(\{M_i\}, n)$ wiąże się wektor prędkości transmisji $(R_1,\ldots,R_k)$, gdzie $R_i = \log M_i/n$. Jego osiągalność definiuje się analogicznie, jak w przypadku kanałów z jednym nadawcą.

Definicja 1.17 *Obszar pojemności* $\mathcal{R}(\Gamma)$ *dla kanału* Γ *to zbiór wszystkich osiągalnych wektorów prędkości transmisji.*

Definicja 1.18 *(Procedura dzielenie czasu [25] (ang. time sharing)): Niech dane będą dwa kody:* $(\{2^{nR_1}, 2^{nR_2}\}, n)$ *oraz* $(\{2^{nR'_1}, 2^{nR'_2}\}, n)$*. Procedura dzielenia czasu oznacza umowę między nadawcami* S_1 *i* S_2*, że podczas pierwszych* t_1 *użyć kanału będą korzystali z kodu pierwszego, przez następne* t_2 *z kodu drugiego potem znowu na* t_1 *użyć wrócą do kodu pierwszego itd.*

Niech $\alpha = \frac{t_1}{t_1+t_2}$. W wyniku procedury dzielenia czasu nadawcy przesyłają (w sensie asymptotycznym $n \to \infty$) ze średnimi prędkościami $(\alpha R_1 + (1-\alpha)R'_1, \alpha R_2 + (1-\alpha)R'_2)$.

Obszar pojemności dyskretnego kanału wielodostępnego został po raz pierwszy podany w pracach [2, 67]. Poniżej, dla wektora $R \in \mathbb{R}^k$ stosujemy skrótową notację $R_S = \sum_{i\in S} R_i$, gdzie R_i to element wektora R a $S \subseteq \{1,\ldots,k\}$.

Twierdzenie 1.4 *(O kodowaniu dla dyskretnych kanałów wielodostępnych) Obszar pojemności* $\mathcal{R}(\Gamma)$ *stanowi wypukłą otoczkę wszystkich wektorów prędkości transmisji* R*, dla których istnieje rozkład prawdopodobieństwa symboli wejściowych* $p_{X_1,\ldots,X_k} = p_{X_1} \cdot \ldots \cdot p_{X_k}$ *taki, że dla każdego podzbioru nadawców* S *zachodzi:*

$$R_S \leq I(X_S, Y | X_{S^C}), \qquad (1.26)$$

gdzie: S^C *jest dopełnieniem podzbioru nadawców,* X_S *to zbiór wejść kanałów odpowiadający* S*.*

Równoważnie, obszar pojemności to domknięcie zbioru wektorów prędkości transmisji R, dla których istnieją rozkłady prawdopodobieństwa w postaci $p_{X_1,\ldots,X_k,Q} = p_Q p_{X_1|Q} \ldots p_{X_k|Q}$ takie, że dla każdego podzbioru nadawców S spełnione są nierówności [25]:

$$R_S \leq I(X_S, Y | X_{S^C}, Q). \tag{1.27}$$

Na mocy twierdzenia Caratheodoriego, zmienna losowa Q przyjmuje wartości $q \in \{1, \ldots, k+1\}$. Zmienną losową Q można interpretować jako wynik zastosowania procedury dzielenia czasu. Wielkość $R_T = \sum_{i=1}^{k} R_i$ nazywana jest całkowitą prędkością transmisji.

Dla przypadku kanału z dwoma nadawcami, nierówności (1.26) redukują sie do postaci:

$$\begin{aligned} R_1 &\leq I(X_1 : Y | X_2) && (1.28)\\ R_2 &\leq I(X_2 : Y | X_1) && (1.29)\\ R_1 + R_2 &\leq I(X_1, X_2 : Y). && (1.30) \end{aligned}$$

Przykład 1.2 *Binarny kanał Γ_{XOR} z dwoma nadawcami.*

Kanał Γ_{XOR} posiada dwa wejścia, przez które można przesyłać stany z alfabetu $\mathcal{A}_{X_1} = \mathcal{A}_{X_2} = \{0, 1\}$. Wejścia i wyjścia kanału wiąże relacja: $Y = X_1 \oplus X_2$, gdzie $\oplus$ oznacza dodawanie modulo 2. Warto zauważyć, że kanał ten działa w sposób deterministyczny natomiast ewentualne błędy transmisji występują na skutek interferencji symboli przesyłanych przez nadawców. Na podstawie ograniczenia (1.18) łatwo zauważyć, że obszar pojemności $\mathcal{R}(\Gamma_{XOR})$ zawiera się w obszarze $\mathcal{O}$:

$$\mathcal{O} : R_1 \leq 1, R_2 \leq 1, R_1 + R_2 \leq 1. \tag{1.31}$$

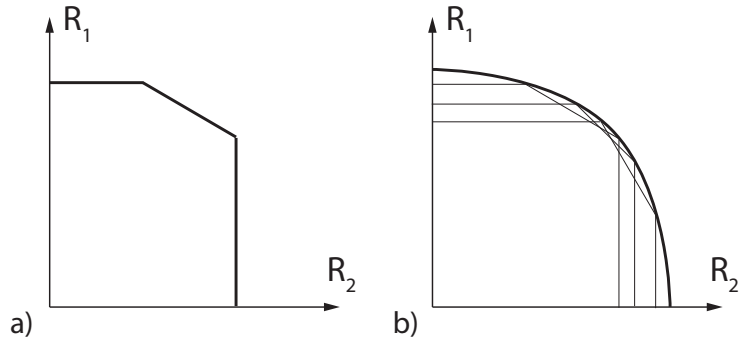
Przekonamy się teraz, że obszary te pokrywają się. Punkty $(R_1^{max}, 0) = (1, 0)$ i $(0, R_2^{max}) = (0, 1)$ są osiągane odpowiednio przez rozkłady $P(X_1 = 1, X_2 = 0) = 0.5, P(X_1 = 0, X_2 = 0) = 0.5, P(X_1, X_2 = 1) = 0$ oraz $P(X_1 = 0, X_2 = 0) = 0.5, P(X_1 = 0, X_2 = 1) = 0.5, P(X_1 = 1, X_2) = 0$. Punkt $(0, 0)$ jest osiągany w oczywisty sposób w sytuacji, gdy każdy z nadawców przesyła tylko jeden ustalony symbol. $\mathcal{O}$ jest otoczką wypukłą rozpiętą na punktach: $(1, 0), (0, 1), (0, 0)$. Stąd, na mocy Tw. 1.4 otrzymujemy natychmiast $\mathcal{R}(\Gamma_{XOR}) = \mathcal{O}$.

Nierówności (1.27) wyznaczają obszar pojemności $\tilde{\mathcal{R}}_Q = \mathcal{R}_{p_{X_1,\ldots,X_k,Q}}(\Gamma)$ dla ustalonego rozkładu prawdopodobieństwa $p_{X_1,\ldots,X_k,Q}$. Dla $p_Q = \delta(Q = 1)$,

obszar ten odpowiada nierównościom (1.26) i będzie w skrócie oznaczany przez $\tilde{\mathcal{R}}$. Obszar $\tilde{\mathcal{R}}_Q$ ma postać:

$$\tilde{\mathcal{R}}_Q = \{R \in \mathbb{R}^n : \forall_{S \subseteq E}\ R_S \leq I(X_S : Y|X_{S^C}, Q), \forall_{i \in E}\ R_i \geq 0\} \tag{1.32}$$

Relacje pomiędzy obszarami pojemności $\mathcal{R}$ i $\tilde{\mathcal{R}}$ przedstawia Rys. 1.2.



Rysunek 1.2: a) Obszar pojemności $\tilde{\mathcal{R}} = \mathcal{R}_{p_{X_1,\ldots,X_k}}$ wyznaczony dla rozkładu rozkładu prawdopodobieństwa symboli wejściowych $p_{X_1,\ldots,X_k}$, b) $\mathcal{R}$ jako otoczka wypukła obszarów pojemności $\mathcal{R}_{p_{X_1,\ldots,X_k}}$.

Przyjrzymy się teraz pewnym geometrycznym własnościom obszaru $\tilde{\mathcal{R}}_Q$.

Definicja 1.19 *Niech $E = \{1, \ldots, k\}$ oraz $f : 2^E \mapsto \mathbb{R}_+ \cup \{0\}$ będzie funkcją podzbiorów E. Wielościan:*

$$\mathcal{B}(f) = \{x \in \mathbb{R}^k : \forall_{S \subseteq E}\ x_S \leq f(S), \forall_{i \in E}\ x_i \geq 0\} \tag{1.33}$$

jest polimatroidem wtedy i tylko wtedy, gdy funkcja f spełnia: (i) $f\{\emptyset) = 0$, (ii) $S \subseteq T \Rightarrow f(S) \leq f(T)$, (iii) $f(S) + f(T) \geq f(S \cup T) + f(S \cap T)$.

Twierdzenie 1.5 *Obszar pojemności $\tilde{\mathcal{R}}_Q$ dla ustalonego rozkładu prawdopodobieństwa symboli wejściowych jest polimatroidem [48].*

Dowód:

Podstawiając $f(S) = I(X_S : Y|X_{S^C}, Q)$ do wzoru (1.33) otrzymujemy natychmiast definicję obszaru pojemności $\tilde{\mathcal{R}}_Q$. Aby udowodnić twierdzenie należy zatem sprawdzić, czy tak zadana funkcja $f(S)$ spełnia warunki (i)-(iii).

Warunek (i) oznacza, że informacja wzajemna w przypadku braku nadawców wynosi 0, co zachodzi w oczywisty sposób.

Prawdziwość warunku (ii) można pokazać w następujący sposób:

$$\begin{aligned} f(T) &= I(X_T : Y|X_{T^C}, Q) && (1.34)\\ &= H(Y|X_{T^C}, Q) - H(Y|X_T, X_{T^C}, Q) && (1.35)\\ &\geq H(Y|X_{S^C}, Q) - H(Y|X_S, X_{S^C}, Q) && (1.36)\\ &= I(X_S : Y|X_{S^C}, Q) && (1.37)\\ &= f(S). && (1.38) \end{aligned}$$

Nierówność (1.36) otrzymujemy korzystamy z $S \cup S^C = T \cup T^C = E$ oraz z faktu, że dodatkowa informacja może co najwyżej zmniejszyć entropię zmiennej losowej ($S \subseteq T \Rightarrow T^C \subseteq T^C$, patrz Rw. (1.8)).

Pokażemy teraz, że warunek (*iii*) również jest spełniony. W tym celu zaczniemy od wyrażenia informacji wzajemnej przez odpowiednie entropie:

$$\begin{aligned} f(S) + f(T) &= I(X_S : Y|X_{S^C}, Q) + I(X_T : Y|X_{T^C}, Q)\\ &= H(Y|X_{S^C}, Q) - H(Y|X_S, X_{S^C}, Q) +\\ &\quad H(Y|X_{T^C}, Q) - H(Y|X_T, X_{T^C}, Q)\\ &= H(Y, X_{S^C}, Q) - H(X_{S^C}, Q) - H(Y|X_S, X_{S^C}, Q) +\\ &\quad H(Y, X_{T^C}, Q) - H(X_{T^C}, Q) - H(Y|X_T, X_{T^C}, Q). \end{aligned}$$

Korzystając z reguły łańcuchowej dla entropii[4] oraz z niezależności nadawców pod warunkiem Q[5] możemy przekształcić poprzednie wyrażenie do postaci:

$$\begin{aligned} f(S) + f(T) &= H(Y, X_{S^C}, Q) - \sum_{i_\in S^C} H(X_i|Q) - H(Q) - H(Y|X_E, Q)\\ &\quad H(Y, X_{T^C}, Q) - \sum_{i_\in T^C} H(X_i|Q) - H(Q) - H(Y|X_E, Q). \end{aligned}$$

[4] $H(X_1, X_2, X_3, Q) = H(X_1|X_2, X_3, Q) + H(X_2|X_3, Q) + H(X_3|Q) + H(Q)$

[5] $H(X_1|X_2, X_3, Q) = H(X_1|Q)$

Po odpowiednim przegrupowaniu wyrazów widzimy, że możemy skorzystać tutaj z silnej subaddytywności entropii[6]:

$$\begin{aligned}
f(S)+f(T) &= H(Y,X_{S^C},Q)+H(Y,X_{T^C},Q) \\
&\quad -\sum_{i\in S}H(X_i|Q)-H(Q)-\sum_{i\in T^C}H(X_i|Q)-H(Q) \\
&\quad -2H(Y|X_E,Q) \\
&\geq H(Y,X_{S^C\cup T^C},Q)+H(Y,X_{S^C\cap T^C},Q) \\
&\quad -\sum_{i\in S^C}H(X_i|Q)-H(Q)-\sum_{i\in T^C}H(X_i|Q)-H(Q) \\
&\quad -2H(Y|X_E,Q) \\
&= H(Y,X_{S^C\cup T^C},Q)+H(Y,X_{S^C\cap T^C},Q) \\
&\quad -\sum_{i\in S^C\cap T^C}H(X_i|Q)-H(Q)-\sum_{i\in S^C\cup T^C}H(X_i|Q)-H(Q) \\
&\quad -2H(Y|X_E,Q)
\end{aligned}$$

Ponownie robiąc użytek z reguły łańcuchowej oraz niezależności nadawców pod warunkiem Q, na podstawie ostatniej formuły otrzymujemy:

$$\begin{aligned}
f(S)+f(T) &\geq H(Y,X_{S^C\cup T^C},Q)+H(Y,X_{S^C\cap T^C},Q) \\
&\quad -H(X_{S\cap T},Q)-H(X_{S^C\cup T^C},Q) \\
&\quad -2H(Y|X_E,Q) \\
&= I(X_{S\cap T}:Y|X_{(S\cap T)^C},Q)+I(X_{S\cup T}:Y|X_{(S\cup T)^C},Q) \\
&= f(S\cap T)+f(S\cup T),
\end{aligned}$$

co kończy dowód.

□

Zbiór wierzchołków k wymiarowego polimatroidu (tj. takiego, że $E=\{1,\ldots,k\}$) posiada bardzo użyteczną własność. Otóż wszystkie jego elementy można wyznaczyć przy użyciu wariacji bez powtórzeń ze zbioru $\{1,\ldots,k\}$ [38]. Niech π będzie pewną wariacją bez powtórzeń. Odpowiada jej wierzchołek v o współrzędnych: $v_{\pi_1}=f(\{\pi_1\})$, $v_{\pi_i}=f(\{\pi_1,\ldots,\pi_i\})-f(\{1,\ldots,\pi_{i-1}\})$

[6] patrz Rw. (1.4) $H(A,B)+H(B,C)\geq H(A,B,C)+H(B)$, gdzie $A=X_{S^C\setminus(S^C\cap T^C)}; B=Y,X_{S^C\cap T^C},Q; C=X_{T^C\setminus(S^C\cap T^C)}$

oraz $\forall_{i \notin \pi} v_i = 0$. Stosując regułę łańcuchową (patrz Rw. (1.11)) można pokazać, że prędkości transmisji osiągane w wierzchołku v wynoszą:

$$R_{\pi_i} = I(X_{\pi_i} : Y | X_{\pi_{i+1}}, \ldots, X_{\pi_n}, Q). \tag{1.39}$$

Zwróćmy uwagę, że dwie różne wariacje mogą prowadzić do wierzchołków z takimi samymi wektorami prędkości transmisji.

W przypadku kanału 2-do-1 lista wariancji bez powtórzeń z przynależnymi doń wektorami prędkości transmisji to (patrz Rys. 1.3):

$$\pi = \emptyset : \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$
$$\pi = \{1\} : \begin{pmatrix} I(X_1 : Y | X_2, Q) \\ 0 \end{pmatrix}, \ \pi = \{2\} : \begin{pmatrix} 0 \\ I(X_2 : Y | X_1, Q) \end{pmatrix},$$
$$\pi = \{1,2\} : \begin{pmatrix} I(X_1 : Y | X_2, Q) \\ I(X_2 : Y | Q) \end{pmatrix}, \pi = \{2,1\} : \begin{pmatrix} I(X_1 : Y | Q) \\ I(X_2 : Y | X_1, Q) \end{pmatrix}.$$

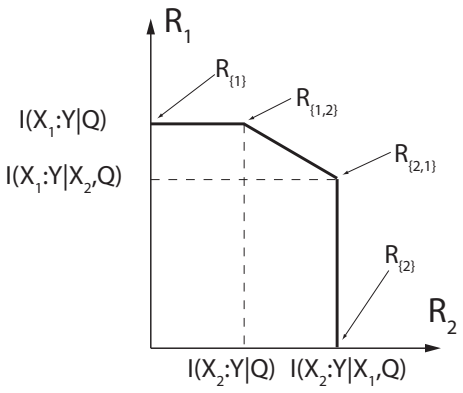
Formuła (1.39) na prędkości transmisji osiągane w wierzchołku v sugeruje iteracyjną procedurę dekodowania (ang. successive cancellation decoding). Niech π będzie wariacją bez powtórzeń, która odpowiada wierzchołkowi v. Zakładamy, że π zawiera k elementów. Na podstawie odebranego ciągu symboli wyjściowych, odbiorca dekoduje komunikat pochodzący od nadawcy S_{π_k}. Odkodowany komunikat oznaczymy przez m_{π_k}. Znając m_{π_k} odbiorca przystępuje do dekodowania komunikatu pochodzącego od nadawcy $S_{\pi_{k-1}}$. Następnie przy założeniu, że nadawcy S_{π_k} oraz $S_{\pi_{k-1}}$ wysłali odpowiednio komunikaty m_{π_k} i $m_{\pi_{k-1}}$, stara się określić komunikat od nadawcy $S_{\pi_{k-2}}$ itd. Można pokazać, że procedura taka jest optymalna [2].

Definicja 1.20 *Kanał Gaussowski, który posiada $k \geq 2$ nadawców, a jego wejścia i wyjście wiąże relacja:*

$$Y = \sum_{i=1}^{k} X_i + Z, \tag{1.40}$$

nazywać będziemy Gaussowskim kanałem wielodostępnym. Y to zmienne losowa związana z wyjściem kanału, natomiast X_i z wejściem kanału należącym do nadawcy S_i, Z modeluje szum o rozkładzie Gaussa z $\mathrm{E}(Z) = 0$ oraz $\sigma^2(Z) = \sigma^2_{szum}$. Na średnią energię przesyłaną przez kanał nakłada się zbiór ograniczeń:

$$\mathcal{P} : \{S_i : \sigma^2(X_i) \leq \sigma^2_{we}(S_i)\}, \tag{1.41}$$



Rysunek 1.3: Obszar pojemności $\tilde{\mathcal{R}}_Q$ dla ustalonego rozkładu prawdopodobieństwa symboli wejściowych z zaznaczonymi wierzchołkami R_{π_i}.

gdzie $\sigma^2_{we}(S_i)$ odnosi się do wejścia kontrolowanego przez nadawcę S_i.

Twierdzenie 1.6 *Wektor prędkości transmisji $(R_1, \ldots, R_k)$ należy do obszaru pojemności $\mathcal{R}(\Gamma)$ kanału Gaussowskiego Γ wtedy i tylko wtedy, gdy dla każdego podzbioru nadawców S zachodzi:*

$$R_S \leq \frac{1}{2} \log \left(1 + \frac{\sigma^2_{we}(S)}{\sigma^2_{szum}} \right), \tag{1.42}$$

gdzie: $R_S = \sum_{S_i \in S} R_i, \sigma^2_{we}(S) = \sum_{S_i \in S} \sigma^2_{we}(S_i)$.

1.2 Kwantowa teoria informacji

Systemy kwantowe rozpatrywane w pracy będziemy dzielić na dwie kategorie: systemy w zmiennych dyskretnych oraz systemy w zmiennych ciągłych. Do pierwszej z kategorii należą te układy kwantowe, których przestrzeń Hilberta ma wymiar skończony. Przykładem jest tu wizytówka kwantowej teorii informacji - bit kwantowy (qbit) - który opisuje przestrzeń Hilberta izomorficzna z $\mathbb{C}^2$. Fizyczne realizacje qbitu to między innymi: spin elektronu, polaryzacja fotonu. Drugą kategorię stanowią układy, których przestrzeń Hilberta nie ma skończonego wymiaru. Ilustracją jest tu n-modowe pole elektromagnetyczne. W przypadku systemów w zmiennych ciągłych zakres pracy ogranicza się

jedynie do systemów bozonowych i transmisji informacji klasycznej przez kanały Gaussowskie[7]. W dalszej części rozdziału zostanie wprowadzony odpowiedni formalizm, pozwalający w efektywny sposób opisać ten rodzaj transmisji. Omawiając stany Gaussowskie będziemy często odnosić się do optyki kwantowej, gdzie stany te pojawiają się w sposób naturalny.

1.2.1 Stany kwantowe

Stan czysty systemu kwantowego S (t.j. stan reprezentujący pełną wiedzę o systemie S) opisany jest przez znormalizowany wektor $|\psi\rangle$, należący do przestrzeni Hilberta $\mathcal{H}_S$. Wektor dualny do $|\psi\rangle$ jest oznaczany jako $\langle\psi|$. Iloczyn skalarny wektorów stanów $|\psi\rangle$ oraz $|\phi\rangle$ to $\langle\psi|\phi\rangle$. Dla oznaczenia operatora rzutu (projektora) na stan $|\psi\rangle$ przyjęto konwencję $\psi = |\psi\rangle\langle\psi|$. Zależność między stanem początkowym $|\psi_0\rangle$ a stanem końcowym $|\psi_T\rangle$ ewoluującego w czasie, izolowanego systemu fizycznego dana jest równaniem $|\psi_T\rangle = U|\psi_0\rangle$, gdzie U jest operatorem unitarnym: $UU^\dagger = U^\dagger U = \mathrm{I}$.

Ustalona baza ortonormalna w przestrzeni Hilberta $\mathcal{H}$ stanowi *bazę standardową* tej przestrzeni. W przypadku przestrzeni n wymiarowej ma ona postać: $\{|0\rangle, |1\rangle, \ldots, |n\rangle\}$. Czasem, dla oznaczenia elementów tej bazy stosowana będzie notacja: $|e_i\rangle, |f_i\rangle$. Baza standardowa qbitu składa się z wektorów:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.43}$$

W odniesieniu do elementów bazy standardowej będziemy używać określenia *etykieta* aby podkreślić fakt, że mamy do czynienia z obiektami w pełni odróżnialnymi od siebie. Termin etykieta będzie również stosowany przy opisie stanu układu klasycznego w ramach formalizmu mechaniki kwantowej.

Stan mieszany modeluje sytuację, gdy brak jest pełnej wiedzy o stanie systemu kwantowego. Do przedstawienia stanu mieszanego używa się *operatora (macierzy) gęstości* $\rho : \mathcal{H} \mapsto \mathcal{H}$. Operator gęstości jest to nie ujemny operator Hermitowski o śladzie 1. Dla stanu czystego $|\psi\rangle$ ma on postać projektora $|\psi\rangle\langle\psi|$. Zbiór wartości własnych operatora gęstości stanowi rozkład prawdopodobieństwa.

Mieszanina stanów czystych $\{p_i, |\psi_i\rangle\}$ opisuje system, który z prawdopodobieństwem p_i znajduje w jednym ze stanów czystych z ustalonego zbioru

[7] Wykorzystanie fermionów oraz obdarzonych masą bozonów jako nośników informacji klasycznej i kwantowej analizowane jest m.in. w pracach [32, 33].

$\{|\psi_i\rangle\}$. Należy podkreślić, że układ przyjmuje tylko stany ze zbioru $\{|\psi_i\rangle\}$. Istnienie zbioru $\{|\psi_i\rangle\}$ odróżnia mieszaninę stanów od stanu mieszanego. Operator gęstości mieszaniny stanów czystych $\{p_i, |\psi_i\rangle\}$ ma postać $\rho = \sum_i p_i \psi_i$, gdzie ψ_i to projektor $\psi_i = |\psi_i\rangle\langle\psi_i|$. Różne mieszaniny stanów mogą posiadać taki sam operator gęstości.

System, w którym można wyróżnić co najmniej dwie fizycznie oddzielne części, nazywany jest *systemem złożonym*. Przykładem systemu złożonego jest atom wodoru oddziaływający z jednomodowym polem elektromagnetycznym. Niech system złożony S składa się z podsystemów $S_1, S_2, \ldots, S_n$. Przestrzeń Hilberta $\mathcal{H}_S$ skojarzona z systemem S jest produktem tensorowym przestrzeni Hilberta jego podsystemów: $\mathcal{H}_S = \bigotimes_{i=1}^{n} \mathcal{H}_{S_i}$. Jeśli podsystemy S_i są przygotowane w stanach czystych $|\psi_i\rangle$, wówczas stan systemu S nazywany jest *czystym stanem produktowym* i ma postać: $|\psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$. Dla zwięzłości, w dalszej części pracy, znak iloczynu tensorowego będzie opuszczany przy zapisie czystych stanów produktowych. Czasem stan produktowy systemu składającego się z qbitów będzie zapisywany w postaci: $|010\rangle$. Stany czyste, których nie da się przedstawić jako stany produktowe nazywane są *czystymi stanami splątanymi*.

Dla stanów mieszanych wprowadza się pojęcie separowalności stanów.

Definicja 1.21 *Stan mieszany ρ_S układu S nad przestrzenią $\mathcal{H}_S = \bigotimes_{i=1}^{n} \mathcal{H}_{S_i}$ nazywany jest stanem separowalnym jeśli można go przedstawić w postaci:*

$$\rho_S = \sum_j p_j \rho_1^j \otimes \ldots \rho_n^j, \tag{1.44}$$

gdzie p_j to rozkład prawdopodobieństwa.

Stany produktowe są stanami separowalnymi natomiast stany splątane nie są separowalne. Ponieważ w tej pracy zajmujemy się zasadniczo transmisją stanów czystych, czytelnika zainteresowanego ogólną teorią splątania odsyłamy do pracy [60].

Twierdzenie 1.7 *(O rozkładzie Schmidta): Niech system AB składa się z podsystemów A i B. Wówczas dla każdego stanu czystego $|\psi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ systemu AB istnieją takie zbiory stanów ortogonalnych $\{|a_i\rangle\}, \{|b_i\rangle\}$ należące odpowiednio do przestrzeni $\mathcal{H}_A$ i $\mathcal{H}_B$, że stan $|\psi_{AB}\rangle$ da się przedstawić w postaci:*

$$|\psi_{AB}\rangle = \sum_{i=1}^{r} \lambda_i |a_i\rangle |b_i\rangle, \tag{1.45}$$

gdzie $\{\lambda_i\}$ *to zbiór rzeczywistych dodatnich współczynników, przy czym zachodzi:* $\sum_i \lambda_i^2 = 1$. r *to liczba Schmidta stanu* $|\psi_{AB}\rangle$.

Twierdzenie 1.8 *Stan czysty układu dwuczęściowego jest stanem produktowym jeśli liczba Schmidta tego stanu wynosi* $r = 1$. *W przypadku gdy* $r > 1$, *stan jest stanem splątanym.*

Jeśli stan czysty $|\psi_{AB}\rangle$ jest stanem produktowym, to zawsze istnieje para stanów $|\psi_A\rangle \in \mathcal{H}_A, |\psi_B\rangle \in \mathcal{H}_B$ takich, że $|\psi_{AB}\rangle = |\psi_A\rangle|\psi_B\rangle$.

Definicja 1.22 *Stan czysty* $|\psi_{AB}\rangle$ *jest stanem maksymalnie splątanym, jeśli jego liczba Schmidta spełnia*

$$r = \min(\dim \mathcal{H}_A, \dim \mathcal{H}_B). \tag{1.46}$$

Przestrzeń stanów układu dwu qbitowego można rozpiąć na wektorach w postaci:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{1.47}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1.48}$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{1.49}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1.50}$$

Powyższe stany to stany Bella (nazywane również stanami EPR). Są one maksymalnie splątane i stanowią zbiór stanów ortogonalnych, który nazywany jest bazą Bella.

Definicja 1.23 *(Ślad częściowy:) Niech* AB *będzie systemem złożonym z podsystemów* A *i* B *oraz niech* $\{a_i\}, \{b_j\}$ *stanowią bazy ortogonalne odpowiednio w przestrzeni* $\mathcal{H}_A$ *i* $\mathcal{H}_B$. *Ślad częściowy operatora gęstości* ρ_{AB} *po podsystemie* B *to odwzorowanie liniowe w postaci:*

$$tr_B[\rho_{AB}] = \sum_{i,j,k} \Big(\langle b_k|\langle a_i|\rho_{AB}|a_j\rangle|b_k\rangle \Big) |a_i\rangle\langle a_j|. \tag{1.51}$$

Operator gęstości ρ_{AB} systemu AB zredukowany do podsystemu A dany jest wzorem: $\rho_A = \mathrm{tr}_B[\rho_{AB}]$.

Pomiar uogólniony (ang. POVM) składa się ze zbioru nieujemnych operatorów Hermitowskich $\{M_m\}$ spełniających relację $\sum_m M_m = \mathrm{I}$. Prawdopodobieństwo uzyskania wyniku m podczas wykonywania pomiaru POV na operatorze gęstości ρ dane jest wzorem $p_m = \mathrm{tr}[M_m\rho]$. Pomiar von Neumana w bazie $\{|e_m\rangle\}$ jest szczególnym przypadkiem pomiaru POV, w którym M_m jest projektorem na wektor stanu $|e_m\rangle$.

Entropia klasyczna mierzy niepewność co do wartości realizacji zmiennej losowej X. Uogólnieniem tego pojęcia pozwalającym mierzyć niepewność odnośnie stanu systemu kwantowego ρ jest *entropia von Neumana* $S(\rho)$ zdefiniowana wzorem:

$$S(\rho) = -\mathrm{tr}[\rho \log \rho] \tag{1.52}$$

Entropia von Neumana operatora gęstości ρ o wartościach własnych $\{\lambda_i\}$ wynosi: $S(\rho) = H(\{\lambda_i\})$. Niektóre z istotnych własności entropii von Neumana to (poniżej zakładamy że ρ, ρ_i to operatory gęstości, natomiast p_i to rozkład prawdopodobieństwa):

- Dodatniość: $S(\rho) \geq 0$, równość zachodzi dla stanów czystych.
- Ograniczenie górne: $S(\rho) \leq \log d$ gdzie d jest wymiarem przestrzeni Hilberta, na której zdefiniowane jest ρ. W przypadku zmiennych dyskretnych równość zachodzi dla stanów zupełni zmieszanych, t.j. stanów w postaci $\frac{1}{d}\mathrm{I}$.
- Wklęsłość: $S(\sum_i p_i\rho_i) \geq \sum_i p_i S(\rho_i)$
- Subaddytywność: $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$, równość zachodzi dla stanów produktowych $\rho_{AB} = \rho_A \otimes \rho_B$.
- Nierówność trójkąta (nierówność Araki-Lieba): $S(\rho_{AB}) \geq |S(\rho_A) - S(\rho_B)|$.
- Dla stanu czystego ρ_{AB} zachodzi: $S(\rho_A) = S(\rho_B)$.
- Dla systemów w zmiennych dyskretnych entropia jest funkcją ciągłą.
- $S(\sum_i p_i\rho_i) \leq \sum_i p_i S(\rho_i) + H(\{p_i\})$, równość zachodzi gdy stany ρ_i mają nośniki na podprzestrzeniach wzajemnie ortogonalnych.

- Unitarna niezmienniczość entropii: dla każdego operatora unitarnego U zachodzi $S(U\rho U^\dagger) = S(\rho)$.
- Silna subaddytywność entropii: $S(\rho_{ABC}) + S(\rho_B) \leq S(\rho_{AB}) + S(\rho_{BC})$.

1.2.2 Stany Gaussowskie oraz formalizm macierzy kowariancji

Niech S będzie n-modowym systemem bozonowym (w pracy rozważane są tylko układy o skończonej liczbie modów), którego przestrzeń Hilberta ma strukturę: $\mathcal{H}_S = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n$. $\mathcal{H}_i$ to przestrzeń Hilberta opisującą i-ty mod układu. $\{|n_i\rangle\}$ oznacza bazę Focka (bazę stanów n-fotonowych) w przestrzeni $\mathcal{H}_i$, natomiast $a_i^\dagger, a_i$ to operatory kreacji i anihilacji w tej przestrzeni. Stan próżni, czyli stan podstawowy układu bozonowego, oznaczany jest przez $|0\rangle$. *Kanoniczne operatory położenia i pędu* dla modu i zdefiniowane są jako:

$$X_i = \frac{1}{\sqrt{2}}\left(a_i + a_i^\dagger\right),\ P_i = -\frac{\mathrm{i}}{\sqrt{2}}\left(a_i - a_i^\dagger\right). \tag{1.53}$$

Ponieważ operatory kanoniczne są Hermitowskie, będziemy się do nich odnosić używając również sformułowania *obserwable kanoniczne*. Definicja 1.53 prowadzi do relacji komutacji: $[X_i, X_j] = [P_i, P_j] = 0$ oraz $[X_i, P_j] = \mathrm{i}\delta_{i,j}$. W dalszej części pracy operatory kanoniczne będą zwykle grupowane w wektor $R = (R_1, R_2, \ldots, R_{2n})^T = (X_1, P_1, \ldots, X_n, P_n)^T$. Relacje komutacji mogą być zapisane przy użyciu wektora R w postaci: $[R_i, R_j] = \mathrm{i}J^{(n)}_{ij}$, gdzie:

$$J^{(n)} = \bigoplus_{i=1}^{n} J,\ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1.54}$$

Każdy stan ρ systemu bozonowego S można przedstawić w postaci [88, 43]:

$$\rho = \frac{1}{(2\pi)^n}\int_{\mathbb{R}^{2n}} d\xi^{2n}\chi_\rho\left(J^{(n)}\xi\right)\mathcal{W}\left(-J^{(n)}\xi\right). \tag{1.55}$$

$\mathcal{W}(\xi) = \exp\left(\mathrm{i}\xi^T R\right)$ to operator Weyla a χ_ρ to funkcja charakterystyczna stanu ρ. Stanowi ona reprezentację stanu ρ w przestrzeni fazowej danej przez operatory kanoniczne. Jej postać można obliczyć używając formuły:

$$\chi_\rho(\xi) = \mathrm{tr}\left[\rho\mathcal{W}(\xi)\right] \tag{1.56}$$

Definicja 1.24 *Stany Gaussowskie to stany, których funkcja charakterystyczna ma postać funkcji Gaussa:*

$$\chi(\xi) = \exp\left[-\frac{1}{4}\xi^T\gamma\xi + \mathrm{i}\xi^T d - c\right], \tag{1.57}$$

gdzie $\gamma > 0$ jest symetryczną macierzą rzeczywistą, $d \in \mathbb{R}^n$, $c > 0$ jest liczbą rzeczywistą i odgrywa rolę czynnika normalizującego. Stany takie będą oznaczane przez $\rho_{\gamma,d}$.

Wektor $d_i = \mathrm{tr}[\rho R_i]$ interpretuje się jako przesunięcie stanu ρ w przestrzeni fazowej a γ jako macierzą kowariancji stanu:

$$\gamma_{ij} = 2\mathrm{tr}\left[\rho(R_i - d_i)(R_j - d_j)\right] - \mathrm{i}J^{(n)}. \tag{1.58}$$

Poniższe twierdzenie charakteryzuje macierze kowariancji stanów fizycznych oraz pozwala określić, czy dla danej macierzy kowariancji istnieje stan Gaussowski. Twierdzenie to jest przepisaniem zasady nieoznaczoności na język macierzy kowariancji.

Twierdzenie 1.9 *Macierzy kowariancji γ opisuje układ fizyczny wtedy i tylko wtedy, gdy zachodzi warunek: $\gamma + \mathrm{i}J^{(n)} \geq 0$.*

Stan ρ może być reprezentowany w przestrzeni fazowej przez funkcję Wignera [89] W_ρ. Użycie funkcji Wignera pozwala mówić o stanie ρ w kategoriach rozkładu quasi-prawdopodobieństwa w przestrzeni fazowej. Funkcja Wignera W_ρ dana jest przez transformatę Fouriera funkcji charakterystycznej χ_ρ:

$$W_\rho(\xi) = \frac{1}{(2\pi)^{2n}} \int_{-\infty}^{+\infty} d^{2n}\eta e^{-\mathrm{i}\xi^T\eta}\chi_\rho(\eta) \tag{1.59}$$

Dla stanu Gaussowskigo $\rho_{\gamma,d}$ funkcja Wignera ma postać:

$$W(\xi) = \frac{1}{\pi^n\sqrt{\det\gamma}} \exp\left[-(\xi - d)^T\gamma^{-1}(\xi - d)\right]. \tag{1.60}$$

Rozkład gęstości prawdopodobieństwa wyników pomiaru na stanie ρ obserwabli kanonicznej R_j można określić poprzez całkę funkcji Wignera W_ρ po współrzędnych fazowych ξ_i dla $i \neq j$. Np. dla układu jednomodowego w stanie ρ, rozkład gęstości prawdopodobieństwa wyników pomiaru obserwabli kanonicznej X wynosi $p_X = \int_{-\infty}^{\infty} W_\rho(x,p)dx$.

Niech ρ_{AB} opisuje stan układu złożonego z części A i B. Funkcję charakterystyczną ξ_A stanu układu zredukowanego $\rho_A = \mathrm{tr}_B[\rho_{AB}]$ otrzymuje się kładąc w funkcji charakterystycznej χ_{AB} stanu ρ_{AB} wartość $\xi_B = 0$, gdzie ξ_B oznacza zmienne odnoszące się do podsystemu B. W przypadku układu dwumodowego wygląda to następująco: $\chi_A(\xi_A) = \chi_{AB}(\xi_A, \xi_B = 0)$. Łatwo zauważyć, że operacja śladu częściowego zachowuje Gaussowski charakter stanu.

Niech $\gamma^{(i)}, d^{(i)}$ oznaczają odpowiednio macierz kowariancji oraz przesunięcie układu n modowego zredukowanego do modu i. Jeżeli $d^{(i)} = 0$ wówczas średnia liczba fotonów w modzie i wynosi:

$$\langle N_i \rangle = \frac{1}{4}\left(\gamma^{(i)}_{1,1} + \gamma^{(i)}_{2,2} - 2\right) \tag{1.61}$$

Operacja unitarna $U = \exp[\mathrm{i}H]$ zachowuje Gaussowski charakter dowolnego stanu, jeśli generujący ją hamiltonian H jest co najwyżej formą kwadratową operatorów kreacji i anihilacji [88]. W formalizmie macierzy kowariancji, działanie operacji unitarnej na stan $\rho_{\gamma,d}$ określa przekształcenie:

$$\gamma \mapsto S\gamma S^T \tag{1.62}$$

$$d \mapsto Sd + \tilde{d}, \tag{1.63}$$

gdzie $\tilde{d} \in \mathbb{R}^{2n}, S \in Sp(2n, \mathbb{R})$. Operacja unitarna wiąże się tutaj ściśle z pojęciem macierzy symplektycznej S, czyli takiej, która zachowują formę symplektyczną $SJ^{(n)}S^T = J^{(n)}$. W interpretacji fizycznej, macierz symplektyczna cechuje się tym, że w działaniu na macierz kowariancji zachowuje relację nieoznaczoności: $\gamma + \mathrm{i}J^{(n)} \geq 0$.

1.2.3 Przegląd podstawowych elementów optycznych

Poniżej zamieszczony został opis elementów optycznych, z którymi czytelnik spotka się w dalszej części pracy. Działanie każdego z elementów przedstawiono w terminach operacji unitarnych oraz w formalizmie macierzy kowariancji. Więcej informacji można znaleźć w pracach [88, 43].

Dzielnik wiązki

Dzielnik wiązki to jedno z najczęściej spotykanych urządzeń w optyce kwantowej. Znajduje zastosowanie w różnego typu interferometrach, detekcji stanów Bella oraz przy wytwarzania splątania. Wejście i wyjście dzielnika wiązki

składa się z dwóch modów. Każda z wiązek padających na dzielnik wiązki zostaje z określonym współczynnikiem przepuszczona lub odbita. Współczynnik charakteryzujące te procesy będą oznaczane odpowiednio przez: $T = \sin^2\phi$, $R = 1 - T = \cos^2\phi$. Dzielnik wiązki 50:50 (t.j. taki, który w równych proporcjach przepuszcza i odbija wiązki wejściowe) reprezentowany jest operacją unitarną:

$$U_{DW} = \exp\left[\frac{\pi}{4}(a_1 a_2^\dagger - a_1^\dagger a_2)\right]. \tag{1.64}$$

W formalizmie przestrzeni fazowej bardziej ogólna postać dzielnika wiązki dana jest przez:

$$S = \begin{pmatrix} \sqrt{R} & 0 & -\sqrt{T} & 0 \\ 0 & \sqrt{R} & 0 & -\sqrt{T} \\ \sqrt{T} & 0 & \sqrt{R} & 0 \\ 0 & \sqrt{T} & 0 & \sqrt{R} \end{pmatrix}, \; \tilde{d} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{1.65}$$

W przypadku dzielnika wiązki 50:50 mamy $R = T = 1/2$. Dzielnik wiązki jest elementem pasywnym, tzn. energia wiązek padających na wyjścia jest równa energii wiązek opuszczających ten element.

Przesunięcie

Przesunięcie $D(\alpha)$ to operacja unitarna w postaci:

$$D(\alpha) = \exp(\alpha a^\dagger - \alpha^* a). \tag{1.66}$$

Często będzie używana notacja $D(d_x, d_p) = D(\alpha/\sqrt{2})$. W działaniu na stan Gaussowski, przesunięcie opisana jest przez:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; \tilde{d} = \begin{pmatrix} d_x \\ d_y \end{pmatrix}. \tag{1.67}$$

Zauważmy, że przesunięcie nie zmienia macierzy kowariancji stanu. Operator przesunięcia wiąże z operatorem Weyla relacja: $D(\xi) = \mathcal{W}(J\xi)$. Przesunięcie jest operacją aktywną, tzn. w działaniu na stan zmienia jego średnią liczbę fotonów. Operację przesunięcia realizuje się mieszając przy użyciu bardzo niesymetrycznego dzielnika wiązki (99:1) [94] (porównaj część 3.5.1) dany stan wejściowy z wiązką pochodzącą od silnego źródła światła spójnego (laser).

Ściskanie jednomodowe

Operacja ściskania jednomodowego powoduje zmniejszenie wariancji jednego z operatorów kanonicznych za cenę wzrostu wariancji drugiego. Wiąże się z tym następująca operacja unitarna:

$$S(\zeta) = \exp\left[\frac{1}{2}(\zeta^* a^2 - \zeta a^{\dagger 2})\right], \tag{1.68}$$

W formalizmie macierzy gęstości, ściskanie jednomodowe dla przypadku $\zeta = r \in \mathbb{R}$ opisują:

$$S = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}, \; \tilde{d} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \tag{1.69}$$

Ściskanie, tak samo jak przesunięcie jest operacją aktywną. Ściskanie dowolnego stanu można wykonać przy użyciu medium Kerra [5]. Jednak w praktyce w laboratoriach wytwarza się zasadniczo tylko ściśnięte stany próżni, o czym więcej będzie powiedziane w dalszej części pracy.

1.2.4 Przegląd podstawowych klas stanów Gaussowskich

Poniżej zamieszczony został przegląd wybranych klas stanów Gaussowskich. Każda z wymienionych tu klas cechuje się specyficzną formą macierzy kowariancji należących do niej stanów.

Stany spójne (koherentne)

Stany spójne $|\alpha\rangle$ to, obok stanów termicznych, najbardziej "klasyczneśtany pola elektromagnetycznego. Zdefiniowane są jako prawe stany własne operatora anihilacji: $a|\alpha\rangle = \alpha|\alpha\rangle$, gdzie α to parametr zespolony. Stany spójne należą do grupy stanów o minimalnej nieoznaczoności (tzn. takich, dla których zachodzi równość w zasadzie nieoznaczoności). Ponadto cechują się tym, że mają takie same wariancje obu zmiennych kanonicznych. Stany spójne otrzymuje sie poprzez działanie operatorem przesunięcia na stan próżni: $|\alpha\rangle = D(\alpha)|0\rangle$. W praktyce źródłem stanów spójnych jest laser współpracujący z odpowiednim układem redukującym szum do poziomu kwantowego [5]. Stan spójny w reprezentacji stanów Focka, przedstawia się następująco:

$$|\alpha\rangle = \exp\left(-\frac{1}{2}|\alpha|^2\right) \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |\alpha\rangle. \tag{1.70}$$

Związana z nim macierz kowariancji ma specyficzną postać:

$$\gamma_{SP} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.71}$$

Wektor przesunięcia stanu $|\alpha\rangle$ opisuje zależność:

$$d = \begin{pmatrix} d_x \\ d_y \end{pmatrix} = \begin{pmatrix} \mathrm{re}\,\sqrt{2}\alpha \\ \mathrm{im}\,\sqrt{2}\alpha \end{pmatrix} \tag{1.72}$$

Stany spójne tworzą bazę nadmiarową w przestrzeni Hilberta $\int d^2\alpha |\alpha\rangle\langle\alpha| = \mathrm{I}$. Średnia liczba fotonów stanu spójnego $|\alpha\rangle$ wynosi $N = |\alpha|^2$.

Stany termiczne

Stan termiczny opisuje pole elektromagnetyczne pochodzące z ciała doskonale czarnego o temperaturze T. W tej pracy, zamiast temperatury, stan termiczny określać będzie jego średnia liczba fotonów N. Ponownie zaczniemy od reprezentacji Focka, gdzie N fotonowy stan termiczny opisuje formuła:

$$\rho_{term} = \frac{1}{1+N} \sum_{n=0}^{\infty} \left(\frac{N}{1+N} \right)^n |n\rangle\langle n|. \tag{1.73}$$

Macierz kowariancji oraz wektor przesunięcia stanu termicznego mają postać:

$$\gamma = \begin{pmatrix} 1+2N & 0 \\ 0 & 1+2N \end{pmatrix}, \; d = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{1.74}$$

Stan termiczny z $N = 0$ to stan próżni. Dla ustalonego N, stan termiczny posiada maksymalną entropię. Wynosi ona $S(\rho_{term}) = g(N)$, gdzie $g(x) = (1+x)\ln(1+x) - x\ln x$.

Stany ściśnięte jednomodowe

Prezentację „nieklasycznych" stanów Gaussowskich zaczniemy od jednomodowego stanu ściśniętego. Tak jak stan spójny, jest on stanem o minimalnej nieoznaczoności. Jednak w tym przypadku wariancje zmiennych kanonicznych różnią się od siebie: wariancja jednej z obserwabli kanonicznych – obsewabli ściśniętej – jest tu mniejsza niż w stanie spójnym. W obszarze teorii informacji, bezpośrednią konsekwencją tego faktu jest większa wartość ilorazu poziomu sygnału do szumu (SNR) w przypadku kodowania sygnału w

przesunięcie obserwabli ściśniętej w porównaniu z kodowaniem sygnału w przesunięcie stanów spójnych [91, 23].

Dalej skupimy się na ściśniętych stanach próżni: $|\zeta;0\rangle = S(\zeta)|0\rangle$, gdzie $\zeta = re^{\mathrm{i}\phi}$ jest parametrem zespolonym. Mają one następującą reprezentację w bazie Focka:

$$|\zeta;0\rangle = \sqrt{\operatorname{sech} r}\sum_{n=0}^{\infty}\frac{\sqrt{(2n)!}}{n!}\left[-\frac{1}{2}e^{\mathrm{i}\phi}\operatorname{tgh} r\right]|2n\rangle, \tag{1.75}$$

r oznacza tu parametr ściśnięcia a ϕ określa kierunek na płaszczyźnie fazowej $X-P$, w którym stan jest ściskany: $\phi = 0$ oznacza ściskanie obserwabli X, natomiast $\phi = \pi$ obserwabli P. Macierz kowariancji dla $\phi = 0$ przyjmuje postać:

$$\gamma = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}. \tag{1.76}$$

Średnia liczba fotonów w stanie ściśniętym wynosi $N = \sinh^2 r$. Ściśnięte stany próżni można przesuwać; otrzymuje się wtedy przesunięte ściśnięte stany próżni: $|\zeta;\alpha\rangle = D(\alpha)|\zeta;0\rangle$.

Eksperymenty związane z wytwarzaniem ściśniętych stanów próżni wykorzystują różnego rodzaju nieliniowe procesy optyczne. Pierwsze eksperymenty opierały się na zdegenerowanym mieszaniu czterech fal [5]. Obecnie wysoki poziom ściśnięcia rzędu $r = 1.15$ uzyskuje się zwykle bazując na zdegenerowanym parametrycznym obniżaniu częstotliwości [86].

Stany ściśnięte dwumodowe

Stany ściśnięte dwumodowe są przykładem splątanych stanów Gaussowskich. W stanach takich obserwujemy ściśnięcie kombinacji liniowych zmiennych kanonicznych należących do różnych modów, w szczególności: $X_1 - X_2$ oraz $P_1 + P_2$ co odpowiada kierunkowi ściskania $\phi = 0$. Wielkość ściśnięcia określa, podobnie jak w przypadku stanów jednomodych, parametr r. Ogólna postać dwumodowego stanu ściśniętego próżni to:

$$|\zeta\rangle = \operatorname{sech} r\sum_{n=0}^{\infty}\left[e^{\mathrm{i}\phi}\operatorname{tgh} r\right]^n|n\rangle|n\rangle, \tag{1.77}$$

gdzie $\zeta = re^{\mathrm{i}\phi}$ jest parametrem zespolonym. W dalszej części pracy używane będą tylko stany, dla których $\phi = 0$. Macierz kowariancji takiego stanu ma

postać:

$$\gamma_{SPL} = \begin{pmatrix} \cosh 2r & 0 & \sinh 2r & 0 \\ 0 & \cosh 2r & 0 & -\sinh 2r \\ \sinh 2r & 0 & \cosh 2r & 0 \\ 0 & -\sinh 2r & 0 & -\cosh 2r \end{pmatrix} \tag{1.78}$$

Nieformalnie, w granicy $r \to \infty$, dwumodowy ściśnięty stan próżni może być zapisany w reprezentacji położenia lub reprezentacji pędu jako:

$$\int_{\mathbb{R}} dx|x\rangle|x\rangle, \int_{\mathbb{R}} dp|p\rangle|-p\rangle, \tag{1.79}$$

co uświadamia nam charakter korelacji między odpowiednimi obserwabliami w obu modach.

Średnia liczba fotonów w dwumodowym stanie ściśniętym próżni wynosi $N = 2\sinh^2 r$. Ślad częściowy po jednym z modów prowadzi do stanu termicznego o średniej liczbie fotonów $N = \sinh^2 r$.

Stany dwumodowe można uzyskać przy użyciu niezdegenerowanej wersji procesów używanych do otrzymywania ściśniętych stanów jednomodowych. Ponadto do otrzymywania dwumodowych stanów ściśniętych wykorzystuje się również mieszanie dwóch jednomodowych stanów ściśniętych na dzielniku wiązki $50:50$ [88].

Twierdzenie 1.10 *(O postaci standardowej stanu dwumodowego [17]): Dowolny dwumodowy stan Gaussowski może być opisany, z dokładnością do lokalnych operacji unitarnych, za pomocą 4 parametrów, t.j. macierz kowariancji:*

$$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix} \tag{1.80}$$

można sprowadzić, używając macierzy symplektycznych S_1 i S_2 działających odpowiednio na modach 1 i 2, do postaci:

$$\gamma \mapsto (S_1 \oplus S_2)\gamma(S_1 \oplus S_2)^T = \begin{pmatrix} a & 0 & c_+ & 0 \\ 0 & a & 0 & c_- \\ c_+ & 0 & b & 0 \\ 0 & c_- & 0 & b \end{pmatrix}. \tag{1.81}$$

Powyżej, macierze A, B, C są macierzami rzeczywistymi 2×2, $A = A^T, A > 0, B = B^T, B > 0$. Współczynniki a, b, c_+, c_- dane są przez relacje: $\det\gamma = (ab - c_-^2)(ab - c_+^2), \det A = a^2, \det B = b^2, \det C = c_+c_-$.

Twierdzenie to można rozumieć jako Gaussowski odpowiednik twierdzenia Schmidta o dekompozycji. Stan Guassowski jest stanem splątanym, jeśli zachodzi:

$$\det \gamma + 1 < \det A + \det B - 2 \det C. \tag{1.82}$$

Twierdzenie 1.11 *(O diagonalizacji [1]): Macierz kowariancji γ stanu Gaussowskiego może być sprowadzona, przy użyciu operacji symplektycznych, do postaci:*

$$\gamma \mapsto S\gamma S^T = \bigoplus_{i=1}^{n} \nu_i \mathrm{I}_2, \tag{1.83}$$

gdzie S oznacza operację symplektyczną a $\nu_i \in [1, \infty)$ to symplektyczne wartości własne.

Symplektyczne wartości własne dane są przez pierwiastki kwadratowe wartości własnych macierzy $-J^{(n)}\gamma J^{(n)}\gamma$. W zbiorze wartości własnych macierzy $-J^{(n)}\gamma J^{(n)}\gamma$ każda z liczb występuje dwukrotnie. Symplektyczne wartości własne oblicza się biorąc po jednej wartości z pary. Symplektyczną wartość własną można utożsamić ze średnią liczbą fotonów w stanie termicznym $\nu_i = 2N_i + 1$, a ponieważ S odpowiada operacji unitarnej na układzie, entropia stanu Gaussowskiego ma postać:

$$S(\rho) = \sum_{i=1}^{n} g\left(\frac{\nu_i - 1}{2}\right). \tag{1.84}$$

Czasami, dla zwiększenia zwięzłości, w dalszej części pracy będzie stosowana notacja: $S(\gamma) = S(\rho_{\gamma,d})$.

1.2.5 Kanał kwantowy

Kluczową koncepcją w modelowaniu ewolucji układu kwantowego Q w obecności szumu jest *kanał kwantowy*[8]. Kanał kwantowy stanowi pewnego rodzaju uogólnienie klasycznego kanału informacyjnego. Nadawca wykorzystuje kanał kwantowy aby przesłać do odbiorcy układ kwantowy Q. Kanał kwantowy może być rozumiany jako czarna skrzynka w tym sensie, że nie interesują nas

[8]Inne metody opisu ewolucji układów otwartych takie jak ang. quantum master equation oraz ich relacje z kanałem kwantowym można znaleźć między innymi w pracach [72, 20, 42]

szczegóły fizycznego procesu leżącego u podstaw ewolucji układu oraz sposób oddziaływania układu z otoczeniem a jedynie relacja między stanami wejściowymi i wyjściowymi układu podlegającego ewolucji. Kanał kwantowy opisuje procesy markowskie tzn. takie, w których stan układu opuszczającego kanał zależy tylko od stanu tego układu przed wejściem do kanału, nie zależy natomiast od tego jakie stany były wcześniej transmitowane przez kanał – kanał kwantowy jest bezpamięciowy. O układzie Q zakłada się, że jest on początkowo odizolowany od otoczenia, tj. układ Q oraz środowisko występują w stanie produktowym: $\rho_{we} \otimes \rho_{sr}$, gdzie ρ_{we} to stan wejściowy układu Q a ρ_{sr} to stan środowiska. Oddziaływanie systemu Q z otoczeniem następuje dopiero podczas transmisji przez kanał. System Q oraz otoczenie tworzą w tym momencie układ izolowany tak więc ich ewolucję opisuje operator unitarny U. Przyjmuje się, że żadna ze stron procesu komunikacji nie ma dostępu do otoczenia i nie wie w jakim stanie aktualnie się ono znajduje. Odbiorca otrzymuje w wyniku opisanego wyżej procesu stan wyjściowy ρ_{wy}, który wiąże się ze stanem wejściowym ρ_{we} równaniem:

$$\rho_{wy} = \mathrm{tr}_{sr}\left[U(\rho_{we} \otimes \rho_{sr})U^{\dagger}\right] \tag{1.85}$$

Zakłada się, że środowisko jest na tyle duże, że zmiana jego stanu na skutek oddziaływania z systemem Q jest pomijalnie mała. Konsekwencją tego jest wspomniana wyżej bezpamięciowość kanału. Kanał kwantowy opisany wzorem (1.85) formalnie definiuje się jako:

Definicja 1.25 *Kanał kwantowy to liniowe, kompletnie dodatnie i zachowujące ślad odwzorowanie w postaci:* $\Phi : B(\mathcal{H}_{we}) \mapsto B(\mathcal{H}_{wy})$.

Definicja ta mówi, że kanał kwantowy przekształca operatory gęstości w operatory gęstości. W przypadku zmiennych dyskretnych, każdy kanał kwantowy można przedstawić przy użyciu reprezentacji Krausa o czym mówi poniższe twierdzenie:

Twierdzenie 1.12 *Kanał kwantowy* Φ *w zmiennych dyskretnych można przedstawić w postaci sumy operatorów [50]:*

$$\Phi(\rho) = \sum_i E_i \rho E_i^{\dagger}, \tag{1.86}$$

przy czym zachodzi: $\sum_i E_i^{\dagger} E_i = \mathrm{I}$.

Reprezentacja taka nie jest jednoznaczna, tzn. dla danego kanału może istnieć wiele równoważnych reprezentacji.

Reprezentacja dana Tw. 1.12 prowadzi do bardzo intuicyjnej interpretacji działania kanału: stan wejściowy ρ jest przekształcany z prawdopodobieństwem $p_i = \mathrm{tr}[E_i \rho E_i^\dagger]$ w stan wyjściowy

$$\rho \mapsto \frac{E_i \rho E_i^\dagger}{\mathrm{tr}[E_i \rho E_i^\dagger]}, \tag{1.87}$$

co bardzo blisko wiąże się z działaniem klasycznego kanału komunikacyjnego.

Równoległe połączenie kanałów kwantowych definiuje się analogicznie, jak w przypadku kanałów klasycznych.

Definicja 1.26 *Minimalna entropia wyjścia* $H_{min}(\Phi)$ *kanału* Φ *dana jest wzorem:*

$$H_{min}(\Phi) = \inf_{\rho} S(\Phi(\rho)). \tag{1.88}$$

Minimalna entropia wyjścia H_{min} stanowi dolne ograniczenie na ilość szumu wprowadzanego przez kanał podczas transmisji.

Przedstawione poniżej przykłady ilustrują koncepcję kanału kwantowego oraz reprezentacji kanału w postaci sumy operatorów. Warto zwrócić uwagę na analogię pomiędzy kanałem depolaryzującym a klasycznym kanałem symetrycznym. Wszystkie opisane poniżej kanały to odwzorowania w postaci: $\Phi : B(\mathbb{C}^n) \mapsto B(\mathbb{C}^n)$

- Kanał identycznościowy

  Kanał identycznościowy $\mathcal{I}$ nie zmienia postaci stanu wejściowego: $\mathcal{I}(\rho) = \rho$. Kanał ten można przedstawić przy użycia pojedynczego operatora:

  $$E_0 = \mathrm{I}. \tag{1.89}$$

- Pomiar projektorowy (pomiar von Neumana)

  Kanał wykonuje na stanie wejściowym pomiar projektorowy w wybranej bazie ortogonalnej $\{|i\rangle\}$ nad przestrzenią wejściową $\mathbb{C}^n$. Stany ortogonalne, stanowiące wyjście kanału, są w pełni rozróżnialne i mogą być traktowane jako klasyczne etykiety. Można więc powiedzieć, że kanał przekształca układ kwantowy w układ klasyczny. Kanały realizujące

tego typu operacje nazywa się kanałami $q - c$. Reprezentacja kanału dana jest przez zbiór projektorów:

$$E_i = |i\rangle\langle i|. \tag{1.90}$$

- Przygotowanie stanu

  Przygotowanie stanu to operacja komplementarna do pomiaru. Polega ona na przekształceniu układu klasycznego w stan kwantowy. Dla danej etykiety $|i\rangle$ na wejściu, kanał produkuje stan $|v_i\rangle$. Zbiór stanów $\{|v_i\rangle\}$ nie musi być ani ortogonalny ani zupełny. Kanały realizujące preparację stanu zalicza się do grupy kanałów $c - q$.

  Operatory opisujące kanał to:

$$E_i = |\phi_i\rangle\langle i|. \tag{1.91}$$

- Kanał łamiący splątanie

  Cechą charakterystyczną kanałów łamiących splątanie jest to, że nie można ich użyć do wytworzenia stanu splątanego pomiędzy uczestnikami procesu komunikacji. Reprezentacja takiego kanału w postaci [58]:

$$E_i = |\phi_i\rangle\langle\psi_i|, \sum_i |\psi_i\rangle\langle\psi_i| = \mathrm{I} \tag{1.92}$$

  pozwala interpretować go jako szeregowe połączenie kanałów wykonującego pomiar oraz preparacji stanu. Cechą charakterystyczną kanału łamiącego splątanie jest to, że wszystkie operatory E_i są rzędu 1.

- Kanały zmieniające bit, fazę oraz bit-fazę

  Wszystkie omawiane poniżej kanały działają na układ 1-qbitowy. W tym miejscu wygodnie jest myśleć o qbicie, jako o cząstce ze spinem 1/2, przy czym baza standardowa związana jest z pomiarem spinu wzdłuż osi Z. Cząstka taka, przechodząc przez kanał, z prawdopodobieństwem p nie zmienia swego stanu, natomiast z prawdopodobieństwem $1 - p$ ulega obrotowi o π radianów wzdłuż odpowiedniej osi. W przypadku kanału zmieniającego bit jest to oś X, co odpowiada transformacji $|0\rangle \leftrightarrow |1\rangle$. Dla kanału zmieniającego fazę jest to oś Z, prowadzi to do zmiany fazy na przeciwną dla cząstki w stanie $|1\rangle$. Kanał zmieniający bit-fazę wykonuje obrót wzdłuż osi Y i jest złożeniem dwóch poprzednich przypadków.

Kanały reprezentowane są przez następujące pary operatorów:

$$E_0^{bit} = \sqrt{p}\mathrm{I},\ E_1^{bit} = \sqrt{1-p}X \tag{1.93}$$

$$E_0^{faza} = \sqrt{p}\mathrm{I},\ E_1^{faza} = \sqrt{1-p}Z \tag{1.94}$$

$$E_0^{bit-faza} = \sqrt{p}\mathrm{I},\ E_1^{bit-faza} = \sqrt{1-p}Y, \tag{1.95}$$

gdzie X, Y, Z to macierze Pauliego. Dla $p = 1/2$ kanał zmieniający fazę sprowadza się do kanału wykonującego pomiar projektorowy w bazie $\{|0\rangle, |1\rangle\}$.

- Kanał depolaryzujący

  Kanał depolaryzujący z prawdopodobieństwem $1-p$ pozostawia stan układu bez zmian, zaś z prawdopodobieństwem p zamienia stan układu w stan maksymalnie wymieszany. Działanie kanału depolaryzującego opisuje równanie:

  $$\Phi(\rho) = \frac{p}{n}\mathrm{I} + (1-p)\rho. \tag{1.96}$$

  W przypadku kanału qbitowego, kanał depolaryzujący reprezentują operatory:

  $$E_0 = \sqrt{1-\frac{3p}{4}}\mathrm{I},\ E_1 = \frac{\sqrt{p}}{2}X,\ E_2 = \frac{\sqrt{p}}{2}Y,\ E_3 = \frac{\sqrt{p}}{2}Z \tag{1.97}$$

  Kanał depolaryzujący wykonuje z równym prawdopodobieństwem obrót wzdłuż każdej z osi.

Definicja 1.27 *n modowy kanał Gaussowski Φ to kanał kwantowy, który przekształca stany Gaussowskie w stany Gassowskie. Kanał taki w następujący sposób transformuje operator Weyla [88]:*

$$\mathcal{W}(\xi) \mapsto \mathcal{W}(X\xi) \exp\left(-\frac{1}{2}\xi^T Y \xi\right) \exp\left(\mathrm{i}\xi^T d'\right), \tag{1.98}$$

gdzie X, Y są macierzami rzeczywistymi o rozmiarze $2n \times 2n$, ponadto Y jest macierzą symetryczną oraz dodatnią, d' to wektor liczb rzeczywistych o rozmiarze $2n$.

Warunek kompletnej dodatniości wymaga, aby spełniona była nierówność:

$$Y + iJ^{(n)} - iX^T J^{(n)} X \geq 0. \tag{1.99}$$

W powyższej definicji macierz Y można interpretować jako klasyczny szum dodawany przez kanał do zmiennych kanonicznych. Działanie kanału Φ w terminach macierzy kowariancji przedstawia się następująco (będzie ono oznaczane małą literą alfabetu greckiego):

$$\phi(\gamma) \mapsto X^T \gamma X + Y,\ \phi(d) \mapsto X^T d + d' \tag{1.100}$$

Kanał Gaussowski jest w pełni opisany przez macierze X,Y oraz przesunięcie d'. Dowolne przesunięcie stanu Gaussowskiego można osiągnąć stosując lokalne operacje unitarne, a ponieważ te nie wpływają na przepustowość kanału, w dalszej części pracy przyjmujemy dla uproszczenia $d' = 0$.

Ważne przykłady Gaussowskich kanałów kwantowych:

- Kanał wprowadzający szum klasycznym

  Kanał w losowy sposób przesuwa stan wejściowy ($X = \mathrm{I}$). Wprowadzane przesunięcie ma rozkład Gaussowski opisany macierzą kowariancji Y. Działanie kanału przedstawia formuła:

  $$\phi(\gamma) = \gamma + Y. \tag{1.101}$$

  Przy użyciu szumu klasycznego można modelować między innymi szum elektroniczny w urządzeniach pomiarowych lub w urządzeniach służących do modulacji wiązki światła.

- Kanał termiczny

  Kanał termiczny opisuje oddziaływanie układu n modowego z otoczeniem w stanie równowagi termicznej. Mod wejściowy i sprzężony jest z modem w stanie termicznym o średniej liczbie fotonów N_i. Sprzężenie modeluje się przy użyciu dzielnika wiązki o transmitancji T_i. Działanie kanału dane jest przez macierze:

  $$X = \bigoplus_i \sqrt{T_i}\mathrm{I}_2,\ Y = \bigoplus_i (1 - T_i)(1 + 2N_i)\mathrm{I}_2, \tag{1.102}$$

- Kanał tłumiący

  Szczególnym przypadkiem kanału termicznego jest kanał tłumiący. Odnosi się on do sytuacji, gdy otocznie jest w stanie próżni: $N_i = 0$. Używając pojęcia kanału tłumiącego, można opisać m.in. straty na elementach optycznych.

Kwantowe kanały wielodostępne definiuje się analogicznie do kanałów kwantowych z jednym nadawcą. Różnicę stanowi tutaj ograniczenie na strukturę stanów wejściowych wynikające z założenia, że tak jak w przypadku klasycznym, nadawcy nadają niezależnie od siebie a każdy z nich kontroluje odrębne wejście kanału. Dla prostoty, podane niżej definicje i twierdzenia odnosić się będą tylko do przypadku kanałów z dwoma nadawcami. Można je jednak łatwo rozszerzyć na kanały z wieloma nadawcami.

Definicja 1.28 *Kwantowy kanał wielodostępny z dwoma nadawcami to liniowe, zachowujące ślad, zupełnie dodatnie odwzorowanie w postaci:*

$$\Phi : B(\mathcal{H}_1) \otimes B(\mathcal{H}_2) \mapsto B(\mathcal{H}_{wy}), \tag{1.103}$$

gdzie $\mathcal{H}_1$, $\mathcal{H}_2$ to przestrzenie Hilberta opisujące wejście kontrolowane odpowiednio przez nadawcę S_1 i S_2. Przestrzeń Hilberta $\mathcal{H}_{wy}$ opisuje wyjście kanału.

O ile nadawcy S_1 i S_2 nie dzielą stanu splątanego, nadają oni niezależnie od siebie stany ρ_1 i ρ_2 a odbiorca otrzymuje stan $\Phi(\rho_1 \otimes \rho_2)$.

Pojęcie kanału wielodostępnego w analogiczny sposób uogólnia się dla dowolnej liczby nadawców.

Definicja 1.29 *Minimalna entropia wyjścia $H_{min}(\Phi)$ kanału wielodostępnego Φ dana jest wzorem:*

$$H_{min}(\Phi) = \inf_{\rho_1,\rho_2} S(\Phi(\rho_1 \otimes \rho_2)), \tag{1.104}$$

przy czym stany ρ_1 i ρ_2 należą do przestrzeni opisującej wejście kanału kontrolowane odpowiednio przez S_1 i S_2.

1.2.6 Przesyłanie informacji klasycznej kanałem kwantowym

W pracy będziemy rozpatrywać następujący schemat komunikacji: Alicja chce przesłać do Boba, za pośrednictwem kanału kwantowego Φ, komunikat $x \in \mathcal{A}_X$. W tym celu koduje komunikat x w *stan wejściowy* ρ_x, który następnie przesyła przez kanał Φ. Stan odebrany przez Boba to $\Phi(\rho_x)$. Bob

wykonuje pomiar POV $\{M_y\}$, przy użyciu którego stara się określić, jaki komunikat nadała Alicja. Wynik pomiaru to zmienna losowa o rozkładzie prawdopodobieństwa $p_{y|x} = \mathrm{tr}[\Phi(\rho_x)M_y]$. Przedstawiony powyżej proces można schematycznie zapisać jako:

$$x \mapsto \rho_x \mapsto \Phi(\rho_x) \mapsto p_{y|x} = \mathrm{tr}[\Phi(\rho_x)M_y] \mapsto y. \tag{1.105}$$

Informacja wzajemna $I(X : Y)$ zależy od wyboru *mieszaniny stanów wejściowych* $\{p_x, \rho_x\}$ oraz pomiaru POV. Podobnie jak w przypadku klasycznym, gdzie odbiorca zna rozkład prawdopodobieństwa oraz alfabet symboli wejściowych, w przypadku kwantowym zna on mieszaninę stanów wejściowych $\{p_x, \rho_x\}$ i na tej podstawie może dobrać optymalny pomiar. Cechą charakterystyczną transmisji informacji klasycznej przez kanał kwantowy jest swoboda wyboru mieszaniny nadawanych stanów. Ma to istotny wpływ na parametry transmisji, o czym możemy się przekonać na przykładzie kanału zmieniającego bit z $p = 1/2$: jeśli nadawca wybierze stany kodowe w postaci $|0\rangle, |1\rangle$, wówczas odbiorca zawsze otrzymuje stan maksymalnie wymieszany, niezależnie od tego który stan kodowy przesłano, w związku z czym nie jest w stanie określić co chciał zakomunikować nadawca. Prędkość transmisji w tym przypadku wynosi 0 bitów/użycie kanału. Z drugiej strony, wybierając stany kodowe $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, niezmiennicze ze względu na działanie kanału, nadawca i odbiorca są w stanie komunikować się z prędkością 1 bit/użycie kanału.

Górne ograniczenie na $I(X : Y)$ przy zadanej mieszaninie stanów wejściowych $\{p_x, \rho_x\}$ podaje twierdzenie Holevo [52]:

Twierdzenie 1.13 *(Ograniczenie Holevo:) Załóżmy, że Alicja przesyła do Boba przez kanał Φ stany z mieszaniny $\{p_x, \rho_x\}$. Wówczas, niezależnie od pomiaru jaki Bob używa do dekodowania odebranego stanu $\Phi(\rho_x)$, informacja wzajemna między Alicją i Bobem ograniczona jest przez:*

$$I(X : Y) \leq S(\Phi(\rho)) - \sum_x p_x S(\Phi(\rho_x)), \tag{1.106}$$

gdzie $\rho = \sum_x p_x \rho_x$.

Wyrażenie $S(\Phi(\rho))$ podaje średnią entropię na wyjściu kanału, natomiast $S(\Phi(\rho_x))$ mierzy produkcję entropii w przypadku transmisji stanu ρ_x. Dalej stosowane będzie oznaczenie: $\chi_{\{p_x,\rho_x\}}(\Phi) = S(\Phi(\rho)) - \sum_x p_x S(\Phi(\rho_x))$.

Prawa strona wyrażenia (1.106) zależy jedynie od mieszaniny stanów wejściowych, supremum na ich zbiorze prowadzi do pojemności Holevo:

Definicja 1.30 *Pojemność Holevo kanału* Φ *to:*

$$\chi(\Phi) = \sup_{\{p_x,\rho_x\}} \left[S\Big(\Phi(\rho)\Big) - \sum_x p_x S\Big(\Phi(\rho_x)\Big) \right]. \tag{1.107}$$

Zwróćmy uwagę, że maksimum we wzorze (1.107) osiągane jest przez stany czyste.

Podobnie jak ma to miejsce w przypadku klasycznym, aby zapobiec błędom w podczas komunikacji przy użyciu kanału $\Phi : B(\mathbb{C}^n) \mapsto B(\mathbb{C}^n)$, nadawca i odbiorca używają kodu (M, n). Tym razem jednak funkcja kodująca f odwzorowuje komunikaty z $\mathcal{A}_W$ na odpowiednie stany kodowe z $B(\mathcal{H}_{we}^{\otimes n})$, natomiast funkcja dekodująca to pomiar łączny przeprowadzony na stanach z przestrzeni $B(\mathcal{H}_{wy}^{\otimes n})$. Kolejne części stanu kodowego przesyłane są podczas kolejnych użyć kanału Φ. W przypadku gdy stany kodowe mają postać iloczynów tensorowych stanów należących do $B(\mathcal{H}_{we})$, kod nazywamy kodem produktowym. Przez $\mathcal{C}^{(1)}(\Phi)$ oznaczana będzie pojemność klasyczna kanału kwantowego, gdy nadawca ogranicza się do kodów produktowych. Pojemność $\mathcal{C}^{(1)}$ nazywać będziemy formułą jednowyrazową.

Twierdzenie 1.14 *(Holevo-Schumacher-Westmoreland [53, 75]) Dla kanału* Φ *istnieje ciąg kodów produktowych* $(2^{nR}, n)$ *osiągających w granicy* $n \to \infty$ *prędkość transmisji:*

$$R = \chi(\Phi). \tag{1.108}$$

Ponieważ $\mathcal{C}^{(1)}(\Phi) \leq \chi(\Phi)$, na mocy powyższego twierdzenia otrzymujemy:

$$\mathcal{C}^{(1)}(\Phi) = \chi(\Phi) \tag{1.109}$$

Gdy stany kodowe są w postaci iloczynu tensorowego stanów należących do $B(\mathcal{H}_{we}^{\otimes m})$, pojemność klasyczna kanału Φ oznaczana będzie przez $\mathcal{C}^{(m)}(\Phi)$. Przypadek ten obejmuje transmisję m cząstkowych stanów splątanych, przy czym splątanie występuje pomiędzy częściami stanu kodowego przesyłanymi podczas kolejnych użyć kanału Φ. Naturalne uogólnienie Tw. 1.14 prowadzi do: $\mathcal{C}^{(m)}(\Phi) = \frac{1}{m}\chi(\Phi^{\otimes m})$. Pojemność Holewo (patrz Rw. (1.107)) liczona jest tu jako maksimum po zbiorze wszystkich mieszanin określonych na przestrzeni $\mathcal{H}_{we}^{\otimes m}$. Pozwala to uwzględnić wpływ co najwyżej m cząstkowego splątania na pojemność kanału Φ. Łatwo zauważyć, że obowiązuje relacja: $\mathcal{C}^{(m+1)}(\Phi) \geq \mathcal{C}^{(m)}(\Phi)$. Przez $\mathcal{C}^{(\infty)}(\Phi) = \lim_{m\to\infty} \mathcal{C}^{(m)}(\Phi)$ oznaczać będziemy

pojemność w sytuacji, gdy nadawca ma całkowitą swobodę w doborze stanów kodowych. $\mathcal{C}^{(\infty)}$ uwzględnia wpływ splątania dowolnego rozmiaru i jest maksymalną wartością pojemności, jaką można uzyskać dla kanału Φ.

Pojemność klasyczna kanałów kwantowych, o których była mowa powyżej przedstawia się następująco[9]:

- Kanał identycznościowy

  Optymalna mieszanina stanów dla kanału identycznościowego to $\{\frac{1}{n}, |e_i\rangle\}$, gdzie $|e_i\rangle$ są wektorami z dowolnej bazy ortonormalnej na przestrzeni $\mathcal{H}_{we}$. Indeks i przebiega po wszystkich wektorach z bazy.

  $$\mathcal{C}^{(1)} = \log n \tag{1.110}$$

- Pomiar projektorowy

  Pomiar projektorowy ma taką samą pojemność jak kanał identycznościowy:

  $$\mathcal{C}^{(1)} = \log n, \tag{1.111}$$

  jednak w tym przypadku istnieje tylko jedna optymalna mieszanina w postaci: $\{\frac{1}{n}, |i\rangle\}$. Stany $|i\rangle$ są zdeterminowane przez projektory definiujące kanał.

- Przygotowanie stanu

  Kanał osiąga maksymalną pojemność na mieszaninie stanów: $\{p_i, |i\rangle\}$. Rozkład prawdopodobieństwa p_i wyznacza się maksymalizując wartość średniej entropii wyjścia $S(\sum_i p_i |v_i\rangle\langle v_i|)$. Ze względu na wklęsłość entropii, zadanie to można łatwo wykonać za pomocą maksymalizacji numerycznej, np. metodą gradientową.

- Kanał zmieniający bit, fazę oraz bit-fazę

  Jak już wcześniej wspomniano, dla każdego z kanałów istnieje para stanów ortogonalnych $|v\rangle, |v^{\perp}\rangle$[10] niezmienniczych ze względu na działanie odpowiedniego operatora obrotu. Optymalna mieszanina składa się ze stanów niezmienniczych występujących w równych proporcjach co prowadzi do pojemności:

  $$\mathcal{C}^{(1)} = 1. \tag{1.112}$$

[9] Tak jak poprzednio zakładamy że kanał są w postaci $\Phi : B(\mathbb{C}^n) \mapsto B(\mathbb{C}^n))$.

[10] Są to unormowane wektory własne operatora obrotu.

- Kanał depolaryzujący

  Pojemność kanału depolaryzującego wynosi [63]:

  $$\mathcal{C}^{(1)} = \log n + (\frac{p}{n} + 1 - p) \log \left(\frac{p}{n} + 1 - p \right) + (n-1) \frac{p}{n} \log \left(\frac{p}{n} \right) . \quad (1.113)$$

  W zależności od parametru p zmienia się ona w zakresie od: 0 dla $p = 1$ do $\log n$ dla $p = 0$.

W omówionych powyżej przypadkach można pokazać, że zachodzi: $\mathcal{C}^{(\infty)} = \mathcal{C}^{(1)}$ [76, 79, 62, 63].

Zajmiemy się teraz pojemnością klasyczną kanałów Gaussowskich. Temat ten przyciągał zainteresowanie już w latach '60. Szczególną uwagę skupiano wówczas nad problemem kodowania informacji w impulsy światła emitowane przez laser oraz nad fizycznymi ograniczeniami takiej transmisji. W pracy [85] pojawia się pomysł wykorzystania nieklasycznych stanów światła w celu zwiększenia prędkości transmisji. Obszerny przegląd zagadnień związanych z kwantowymi ograniczeniami na transmisję informacji przez szeroko i wąsko pasmowe kanały Gaussowskie można znaleźć w pracach [91, 23]. Podstawowe schematy komunikacji rozważane w kontekście idealnego jednomodowego kanału Gaussowskiego oraz uzyskiwane w nich prędkości transmisji to (N oznacza średnią liczbę fotonów na wejściu kanału):

- kodowanie informacji w stany Focka oraz detekcja liczby fotonów:

  $$R_{Fock} = g(N); \quad (1.114)$$

- kodowanie informacji w przesunięcie jednej kwadratury $(d_x, 0)$ stanu spójnego oraz detekcja homodynowa X:

  $$R_{HM} = \log \left[\sqrt{1 + 4N} \right] ; \quad (1.115)$$

- kodowanie informacji w przesunięcie obu kwadratur (d_x, d_p) stanu spójnego oraz detekcja heterodynowa X, P [46, 78]:

  $$R_{SP} = \log \left[1 + N \right] ; \quad (1.116)$$

- kodowanie informacji w przesunięcie jednej kwadratury jednomodowego stanu ściśniętego $(d_x, 0)$ oraz detekcja homodynowa X [91]:

  $$C_{SC} = \log \left[1 + 2N \right] . \quad (1.117)$$

Przegląd eksperymentów związanych z wykorzystaniem stanów Gassowskich w komunikacji klasycznej można znaleźć w pracy [5].

Formuła Holevo (1.107), w przypadku kanałów Gaussowskich, obowiązuje w nieznacznie zmienionej postaci:

$$\chi(\Phi) = \sup_{\{p_x,\rho_x\},\mathrm{tr}[H\rho]\leq E} \left[S(\Phi(\rho)) - \int dx p_x S(\Phi(\rho_x)) \right], \tag{1.118}$$

gdzie $\rho = \int dx \rho_x$. Podobnie jak w przypadku klasycznych kanałów Gaussowskich, zbieżność formuły (1.118) zapewnia ograniczenie na średnią energię stanów wejściowych $\mathcal{P} : \mathrm{tr}[H\rho] \leq E$, które zwykle przyjmuje postać ograniczenia na średnią liczbę fotonów.

Obecnie znana jest tylko pojemność kanału idealnego $\mathcal{I}$:

$$\mathcal{C}^{(\infty)} = g(N) \tag{1.119}$$

oraz n modowego kanału tłumiącego [45]:

$$\mathcal{C}^{(\infty)} = \max_{N_i:\sum_i N_i = N} g(T_i N_i), \tag{1.120}$$

gdzie T_i określa transmitancję kanału dla modu i a N_i to ograniczenie na średnią liczbę fotonów w tym modzie. Zauważmy, że pojemność kanału zależy od właściwej alokacji całkowitej liczby fotonów N dostępnej dla nadawcy. Dla obu kanałów zachodzi $\mathcal{C}^{(\infty)} = \mathcal{C}^{(1)}$.

Przypuszcza się, że pojemność kanałów Gaussowskich osiągana jest przez Gaussowskie mieszaniny stanów Gaussowskich [56]. Pojemność Holevo (tzw. Gaussowska pojemność Holevo χ_G) w tym kontekście wynosi [54]:

$$\chi_G(\Phi) = \sup_{Y\geq 0} S(\phi(\gamma + Y)) - S(\phi(\gamma)), \tag{1.121}$$

gdzie γ oznacza macierz kowariancji stanu minimalizującego $S(\phi(\gamma))$. Optymalna mieszanina stanów wejściowych w tym przypadku to $\{p_d, \rho_{\gamma,d}\}$. Wszystkie stany z mieszaniny posiadają taką samą macierz kowariancji γ. Informacja kodowana jest w przesunięcie d stanów wejściowych, którego rozkład prawdopodobieństwa wyraża formuła:

$$p_d = \frac{1}{\pi^n \sqrt{\det Y}} \exp\left(-d^T Y^{-1} d\right). \tag{1.122}$$

Średni stan na wejściu kanału ma postać $\rho_{Y+\gamma,0}$. $\{p_d, \rho_{\gamma,d}\}$ jest przykładem *alfabetu modulacyjnego* (ang. modulation alphabet), gdzie modulacji podlega przesunięcie stanu wejściowego ρ_γ. Korzystając ze wzoru (1.61), ograniczenie na średnią energię stanów na wejściu kanału $\mathcal{P} : \mathrm{tr}[H\rho_{Y+\gamma,0}] \leq E$ można wyrazić w kategoriach średniej liczby fotonów przypadających na stan wejściowy:

$$\sum_{i=1}^{n} \frac{1}{4}\big((Y+\gamma)_{2i-1,2i-1} + (Y+\gamma)_{2i,2i} - 2\big) \leq N, \tag{1.123}$$

gdzie i indeksuje mody wejściowe kanału. Zauważmy, że warunek (1.123) obejmuje zarówno energię potrzebną na wytworzenie stanu ρ_γ jak i tą zużytą na jego modulację (przesunięcie).

Ostatnie twierdzenie prezentowane w tej części to odpowiednik Tw. 1.14 dla kanałów kwantowych z wieloma nadawcami.

Twierdzenie 1.15 *Niech $\{p_{x_1}, \rho_{x_1}\}, \{p_{x_2}, \rho_{x_2}\}$ oznaczają odpowiednio mieszaniny stanów wejściowych dla nadawców S_1 i S_2, z kolei ρ_1 i ρ_2 to stany średnie dla tych mieszanin. Obszar pojemności klasycznej $\mathcal{R}^{(1)}(\Phi)$ dla kanału Φ stanowi wypukłą otoczkę zbioru wszystkich wektorów (R_1, R_2), dla których istnieją mieszaniny stanów wejściowych $\{p_{x_1}, \rho_{x_1}\}, \{p_{x_2}, \rho_{x_2}\}$ takie, że [3]:*

$$R_1 \leq I(X_1 : Y|X_2) \tag{1.124}$$

$$R_2 \leq I(X_2 : Y|X_1) \tag{1.125}$$

$$R_1 + R_2 \leq I(X_1, X_2 : Y). \tag{1.126}$$

Formuła na informację wzajemną przyjmuje tu postać: $I(X_1, X_2 : Y) = S(\Phi(\rho_1 \otimes \rho_2)) - \sum_{x_1,x_2} p_{x_1} p_{x_2} S(\Phi(\rho_{x_1} \otimes \rho_{x_2})$, zaś warunkowa informacja wzajemna dana jest wzorem: $I(X_1 : Y|X_2) = \sum_{x_2} p_{x_2} I(X_1 : Y|X_2 = x_2)$, gdzie $I(S_1 : Y|S_2 = x_1) = S(\Phi(\rho_1 \otimes \rho_{x_2}) - \sum_{x_1} p_{x_1} S(\Phi(\rho_{x_1} \otimes \rho_{x_2}))$.

Twierdzenie to w naturalny sposób uogólnia się dla większej liczby nadawców. Zwróćmy uwagę na podobieństwo twierdzeń określających obszar pojemności klasycznej w przypadku wielodostępowego kanału kwantowego (Tw. 1.15) oraz wielodostępowego kanału klasycznego (Tw. 1.4).

Tak jak w przypadku kanałów z jednym nadawcą, tutaj również wprowadza się obszar pojemności $\mathcal{R}(\Phi)^{(m)}$ dla oznaczenia sytuacji, gdy nadawcy mogą wykorzystywać podczas transmisji m cząstkowe stany splątane. Regularyzowany obszar pojemności klasycznej definiuje się jako $\mathcal{R}(\Phi)^{(\infty)} = \lim_{m\to\infty} \mathcal{R}^{(m)}(\Phi)$.

Rozdział 2

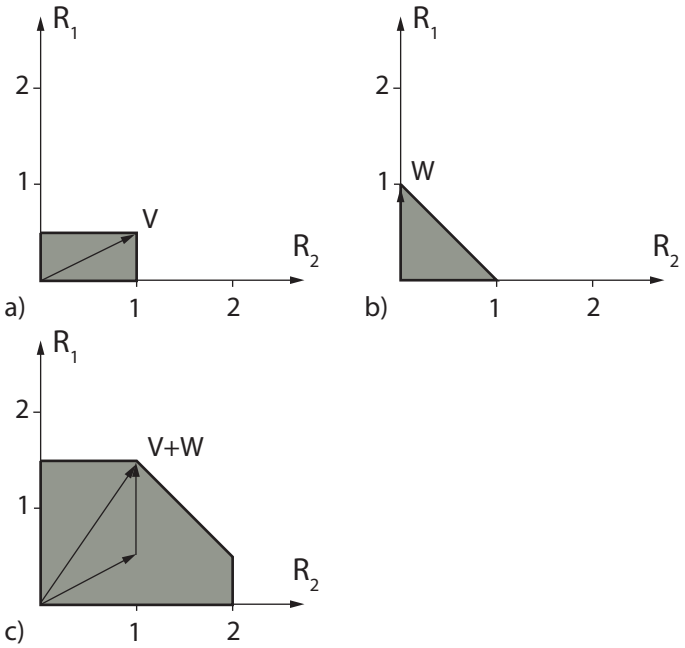
Aktywacja pojemności klasycznej w kanałach dyskretnych

Przegląd wyników, dotyczących roli splątania w transmisji informacji klasycznej oraz aktywacji pojemności klasycznej, zaczniemy od wielodostępnych kanałów kwantowych działających w obszarze zmiennych dyskretnych. Zagadnienie aktywacji przybiera tutaj postać superaddytywności obszarów pojemności klasycznej, co czyni je szczególnie czytelnym. Przedstawione wyniki wskazują na dwie zasadniczo różne formy superaddytywności obszarów pojemności: (i) wzrost prędkości transmisji poszczególnych nadawców przy zachowaniu łącznej prędkości transmisji R_T, co w analizowanych przypadkach, wiąże się ze schematem gęstego kodowania oraz wzrostem zróżnicowania stanów na wyjściu kanału kwantowego; (ii) wzrost łącznej prędkości transmisji R_T, będący konsekwencją subaddytywności minimalnej entropii wyjścia H_{min}. Superaddytywność typu (i) analizowana będzie między innymi w kontekście przekraczania obszaru danego formułami jednowyrazowymi (w kanałach, dla których $\mathcal{R}^{(\infty)}(\Phi) = \mathcal{R}^{(1)}(\Phi)$) oraz wpływu splątania na osiąganie regularyzowanego obszaru pojemności klasycznej, w szczególności wpływu splątania wielocząstkowego (w kanałach, dla których $\mathcal{R}^{(\infty)}(\Phi) \subsetneq \mathcal{R}^{(2)}(\Phi) \subsetneq \mathcal{R}^{(1)}(\Phi)$). Pokazany zostanie również przykład superaddytywności regularyzowanych obszarów pojemność klasycznej.

Badanie efektów aktywacji oraz superaddytywności jest w przypadku zmiennych dyskretnych szczególnie wdzięczne ze względu na prosty aparat matematyczny i pojęciowy. Pozwala to ominąć niepotrzebną komplikację prowadzonych wywodów a skupić się na istocie prezentowanych zagadnień. Zalety te trzeba jednak okupić problemami natury technicznej, dającymi o so-

bie znać przy próbie eksperymentalnej weryfikacji omawianych tu koncepcji. Więcej szczegółów na ten temat czytelnik znajdzie w części 2.3.

2.1 Addytywność obszarów pojemności i minimalnej entropii wyjścia w kanałach klasycznych



Rysunek 2.1: Addytywność obszarów pojemności kanałów klasycznych: a) dwóch nadawców przekazuje komunikaty do tego samego odbiorcy przez niezależne binarne kanały symetryczne z $H(p) = 0.5$ i $H(p) = 0$; b) obszar pojemności binarnego kanału XOR; c) obszar pojemności równoległego połączenia przedstawionych wcześniej kanałów jest równy sumie Minkowskiego obszarów pojemności a) i b).

W pracy zajmujemy się transmisją informacji klasycznej w sytuacji, gdy uczestnicy procesu komunikacji mogą korzystać równocześnie z kilku kanałów wielodostępnych. Kluczową cechą tego scenariusza jest, w przypadku klasycznych kanałów dyskretnych, addytywność obszarów pojemności, tzn. obszar

pojemności uzyskany dla równoległego połączenia kanałów jest sumą geometryczną obszarów pojemności kanałów składowych. Właściwość tą, której łamanie pozwala mówić o kwantowym efekcie aktywacji, ujmuje następujące twierdzenie:

Twierdzenie 2.1 *Obszar pojemności dyskretnych wielodostępnych kanałów klasycznych n-do-1 jest addytywny:*

$$\mathcal{R}(\Phi_A \otimes \Phi_B) = \mathcal{R}(\Phi_A) + \mathcal{R}(\Phi_B), \tag{2.1}$$

gdzie + oznacza sumę geometryczną: $\mathcal{R}(\Phi_A) + \mathcal{R}(\Phi_B) = \{u_A + u_B : u_A \in \mathcal{R}(\Phi_A), u_B \in \mathcal{R}(\Phi_B)\}$.

Powyżej zakładamy, że obydwa kanały mają taką samą liczbę nadawców. Można to osiągnąć przez formalne rozszerzenie zbioru nadawców danego kanału do odpowiedniej wielkości, przy czym komunikat od dodatkowych nadawców jest zawsze tracony[1]. Szczególnym przypadkiem tego twierdzenia jest addytywność pojemności kanałów 1-do-1. Twierdzenie jest zilustrowane na Rys. 2.1.

Lemat 2.1 *Suma geometryczna* $\tilde{\mathcal{R}}_Q(\Phi_A)+\tilde{\mathcal{R}}_Q(\Phi_B)$ *obszarów pojemności dla ustalonych rozkładów prawdopodobieństwa ma postać:*

$$\begin{aligned} \mathcal{O} \;=\; & \big\{R \in \mathbb{R}^n : \forall_{S\subseteq E}\, \forall_{i\in E} R_i \geq 0, \\ & R_S \leq I(X_S^A, Y^A | X_{S^C}^A, Q^A) + I(X_S^B, Y^B | X_{S^C}^B, Q^B)\big\}. \end{aligned} \tag{2.2}$$

gdzie E to zbiór nadawców, $R_S = \sum_{i\in S} R_i$ *(patrz Rw. (1.27)).*

Dowód:

Wykonując sumowanie po współrzędnych, łatwo pokazać, że $\mathcal{O}$ zawiera obszar $\tilde{\mathcal{R}}_Q(\Phi_A)+\tilde{\mathcal{R}}_Q(\Phi_B)$. Udowodnimy teraz, że każdy wektor prędkości transmisji należący do $\mathcal{O}$ da się przedstawić jako sumę wektorów należących odpowiednio do $\tilde{\mathcal{R}}_Q(\Phi_A)$ oraz $\tilde{\mathcal{R}}_Q(\Phi_B)$. Ze względu na wypukłość $\mathcal{O}$, wszystkie punkty należące do tego obszaru można przedstawić jako kombinację liniową jego wierzchołków [97]. Zatem wystarczy pokazać, że odpowiednie przedstawienie

[1] Rozkład prawdopodobieństwa przejścia dla tak rozszerzonego kanału ma postać $p_{Y|X_1,\ldots,X_{N_A}} = p_{Y|X_1,\ldots,X_{N_B}}$ przy czym przyjmujemy, że $N_A \geq N_B$

istnieje dla wierzchołków $\mathcal{O}$. W dalszej argumentacji kluczową rolę odgrywać będzie fakt, że zarówno $\mathcal{O}$ jak i $\tilde{\mathcal{R}}_Q(\Phi_A), \tilde{\mathcal{R}}_Q(\Phi_B)$ to polimatroidy (patrz Tw. 1.5).

Niech π będzie pewną wariacją bez powtórzeń ze zbioru $\{1,\ldots,n\}$ a $v \in \mathcal{O}$ to odnoszący się do niej wierzchołek. Zgodnie ze wzorem (1.39) wierzchołek ten ma współrzędne:

$$v_i = I(X^A_{\pi_i} : Y^A | X^A_{\pi_{i+1}}, \ldots, X^A_{\pi_n}, Q_A) + I(X^B_{\pi_i} : Y^B | X^B_{\pi_{i+1}}, \ldots, X^B_{\pi_n}, Q_B) \quad (2.3)$$

i można go przedstawić jako sumę wektorów v_A, v_B o współrzędnych odpowiednio:

$$v^A_i = I(X^A_{\pi_i} : Y^A | X^A_{\pi_{i+1}}, \ldots, X^A_{\pi_n}, Q_A), \quad (2.4)$$

$$v^B_i = I(X^B_{\pi_i} : Y^B | X^B_{\pi_{i+1}}, \ldots, X^B_{\pi_n}, Q_B). \quad (2.5)$$

Zauważmy jednak, że wektory te to wierzchołki należące odpowiednio do $\tilde{\mathcal{R}}_Q(\Phi_A), \tilde{\mathcal{R}}_Q(\Phi_B)$ i odpowiadające wariacji π.

□

Wstawiając $p_Q = \delta(Q = 1)$, można sprawdzić, że analogiczne twierdzenie zachodzi również dla obszarów pojemności $\tilde{\mathcal{R}}$.

Dowód (Twierdzenie 2.1):

($\supseteq$) Niech $u_A \in \mathcal{R}(\Phi_A), u_B \in \mathcal{R}(\Phi_B)$. Istnieją zatem rozkłady prawdopodobieństwa symboli wejściowych $p_A = p_{X^A_E, Q^A}$, $p_B = p_{X^B_E, Q^B}$ oraz odpowiadające im obszary pojemności $\tilde{\mathcal{R}}_Q(\Phi_A)$, $\tilde{\mathcal{R}}_Q(\Phi_B)$ takie, że $u_A \in \tilde{\mathcal{R}}_Q(\Phi_A)$, $u_B \in \tilde{\mathcal{R}}_Q(\Phi_B)$. Niech $\tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B)$ to obszar pojemności uzyskany dla rozkładu prawdopodobieństwa $p_{AB} = p_{X^A_E, X^B_E, Q^A, Q^B} = p_A p_B$. Przypomnijmy, że obszar pojemności dla ustalonego rozkładu prawdopodobieństwa symboli wejściowych ma postać (porównaj (1.27) oraz (1.32)):

$$\tilde{\mathcal{R}}_Q = \{R \in \mathbb{R}^n : \forall_{S \subseteq E}\, R_S \leq I(X_S : Y | X_{S^C}, Q), \forall_{i \in E}\, R_i \geq 0\} \quad (2.6)$$

Podstawiając p_{AB} do powyższej formuły otrzymujemy $\tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B) = \mathcal{O}$. Zatem, na mocy Lem. 2.1 widzimy, że $u_A + u_B \in \tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B)$. Na podstawie definicji obszaru pojemności zachodzi $\tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B) \subseteq \mathcal{R}(\Phi_A \otimes \Phi_B)$. Wnioskujemy zatem, że: $u_A + u_B \in \mathcal{R}(\Phi_A \otimes \Phi_B)$ co kończy dowód.

($\subseteq$) Niech $u \in \mathcal{R}(\Phi_A \otimes \Phi_B)$. Ponownie skorzystamy z faktu, że dla wektora prędkości transmisji u istnieje rozkład prawdopodobieństwa symboli wejściowych $p_{AB} = p_{X_E^A, X_E^B, Q^A, Q^B}$ oraz odpowiadający mu obszar pojemności $\tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B)$ taki, że $u \in \tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B)$. Pokażemy teraz, że $u \in \tilde{\mathcal{R}}_Q(\Phi_A) + \tilde{\mathcal{R}}_Q(\Phi_B)$, przy czym obszary $\tilde{\mathcal{R}}_Q(\Phi_A)$ oraz $\tilde{\mathcal{R}}_Q(\Phi_B)$ zostały wyznaczone dla rozkładów prawdopodobieństwa p_A, p_B będących wynikiem śladowania rozkładu wyjściowego p_{AB} po odpowiednich podsystemach[2].

Zaczniemy od kilku obserwacji, które ułatwią dalsze obliczenia. Poniżej używać będziemy zapisu $x_S^A, x_S^B, x_S = \{x_S^A, x_S^B\}$ do oznaczenia wektora symboli wejściowych transmitowanych odpowiednio przez Φ_A, Φ_B, $\Phi_A \otimes \Phi_B$ przez nadawców należących do zbioru S.

Zauważmy najpierw, że dla dowolnego podzbioru nadawców $S \subseteq E$, średnia entropia na wyjściu kanału produktowego $\Phi_A \otimes \Phi_B$ jest nie większa niż suma średnich entropii na wyjściu każdego z kanałów składowych.

$$
\begin{aligned}
H(Y|X_S, Q) &= \sum_{x_S, q} p_{x_S} H(Y|X_S = x_S, Q = q) && (2.7)\\
&\leq \sum_{x_S^A, x_S^B, q^A, q^B} p_{x_S^A, x_S^B, q^A, q^B} \Big(H(Y^A|X_S^A = x_S^A, Q^A = q^A) && (2.8)\\
&\quad + H(Y^B|X_S^B = x_S^B, Q^B = q^B) \Big) \\
&= \sum_{x_S^A, q^A} p_{x_S^A, q^A} H(Y^A|X_S^A = x_S^A, Q^A = q^A) && (2.9)\\
&\quad + \sum_{x_S^B, q^B} p_{x_S^B, q^B} H(Y^B|X_S^B = x_S^B, Q^B = q^B) \\
&= H(Y^A|X_S^A, Q^A) + H(Y^B|X_S^B, Q^B), && (2.10)
\end{aligned}
$$

gdzie w kroku (2.8) skorzystaliśmy z subaddytywności entropii.

Teraz pokażemy, że produkcja entropii przez kanał produktowy $\Phi_A \otimes \Phi_B$ jest równa sumie entropii produkowanych przez kanały składowe. W dowodzie skorzystamy z faktoryzacji prawdopodobieństwa przejścia $p_{Y|X_E} =$

[2] $p_A = P(X_E^A = \{x_1^A, \ldots, x_n^A\}, Q^A = q^A) = \sum_{x_E^B, q^B} p_{x_E^A, x_E^B, q^A, q^B}$, analogicznie definiujemy p_B.

$p_{Y^A|X_E^A} p_{Y^B|X_E^B}$ (patrz Def. 1.7) dla $\Phi_A \otimes \Phi_B$:

$$\begin{aligned} H(Y|X_E) &= -\sum_{x_E,y} p_{x_E,y} \log p_{y|x_E} && (2.11)\\ &= -\sum_{x_E^A,y^A} \sum_{x_E^B,y^B} p_{x_E^A,y^A,x_E^B,x_E^B,y^B} \log p_{y^A|x_E^A} p_{y^B|x_E^B} && (2.12)\\ &= -\sum_{x_E^A,y^A} p_{x_E^A,y^A} \log p_{y^A|x_E^A} && (2.13)\\ &\quad -\sum_{x_E^B,y^B} p_{x_E^B,y^B} \log py^B|x_E^B \\ &= H(Y^A|X_E^A) + H(Y^B|X_E^B). && (2.14) \end{aligned}$$

Korzystać będziemy również z faktu, że wyjście kanału zależy tylko od jego wejścia — żadna dodatkowa informacja nie wpływa na średnią entropię na wyjściu kanału:

$$\begin{aligned} H(Y|X_E,Q) &= -\sum_{x_E,y,q} p_{x_E,y,q} \log p_{y|x_E,q} && (2.15)\\ &= -\sum_{x_E,y,q} p_{x_E,y,q} \log p_{y|x_E} && (2.16)\\ &= -\sum_{x_E,y} p_{x_E,y} \log p_{y|x_E} && (2.17)\\ &= H(Y|X_E). && (2.18) \end{aligned}$$

Powyższe równanie jest prawdziwe zarówno dla kanałów składowych Φ_A, Φ_B jak i połączenia równoległego $\Phi_A \otimes \Phi_B$.

Wróćmy do głównej części dowodu. Korzystając z przedstawionych obserwacji, możemy podać górne ograniczenie na informację wzajemną $I(X_S : Y|X_{S^C}, Q)$ występującą w definicji obszaru pojemności $\tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B)$ (patrz Rw. 2.6):

$$
\begin{aligned}
I(X_S : Y|X_{S^C}, Q) &= H(Y|X_{S^C}, Q) - H(Y|X_S, X_{S^C}, Q) && (2.19)\\
&= H(Y|X_{S^C}, Q) && (2.20)\\
&\quad -H(Y^A|X_S^A, X_{S^C}^A, Q^A) - H(Y^B|X_S^B, X_{S^C}^B, Q^A)\\
&\leq H(Y^A|X_{S^C}^A, Q^A) + H(Y^B|X_{S^C}^B, Q^B) && (2.21)\\
&\quad -H(Y^A|X_S^A, X_{S^C}^A, Q^A) - H(Y^B|X_S^B, X_{S^C}^B, Q^B)\\
&= I(X_S^A : Y^A|X_{S^C}^A, Q^A) + I(X_S^B : Y^B|X_{S^C}^B, Q^B), && (2.22)
\end{aligned}
$$

gdzie wzór (2.20) wynika z własności faktoryzacji (patrz Rw. (2.14)) natomiast wzór (2.21) z subaddytywności entropii warunkowej (patrz Rw. (2.9)).

Porównując uzyskane ograniczenie z obszarem $\mathcal{O}$ zadanym przez (2.2) widzimy, że $\tilde{\mathcal{R}}_Q(\Phi_A \otimes \Phi_B) \subseteq \tilde{\mathcal{R}}_Q(\Phi_A) + \tilde{\mathcal{R}}_Q(\Phi_B)$, a zatem $u \in \tilde{\mathcal{R}}_Q(\Phi_A) + \tilde{\mathcal{R}}_Q(\Phi_B)$.

□

Ponieważ kanał $\Phi_A \otimes \Phi_B$ jest również kanałem wielodostępnym, Tw. 1.4 można stosować rekurencyjnie, pokazując w ten sposób że dla dowolnego zbioru dyskretnych kanałów wielodostępnych zachodzi:

$$\mathcal{R}\left(\bigotimes_i \Phi_i\right) = \sum_i \mathcal{R}\left(\Phi_i\right). \tag{2.23}$$

Przedstawione twierdzenie przede wszystkim pokazuje, że regularyzowany obszar pojemności kanałów wielodostępnych wyraża się formułami jednowyrazowymi: $\mathcal{R}^{(\infty)} = \mathcal{R}^{(1)}$. Ponadto odnosząc twierdzenie o kodowaniu (patrz Tw. 1.4) do przypadku $\Phi_A \otimes \Phi_B$, wystarczy dla każdego z nadawców S_i rozpatrywać rozkłady prawdopodobieństwa w postaci $p_{X_i^A, X_i^B} = p_{X_i^A} p_{X_i^B}$. Bardziej ogólne rozkłady prawdopodobieństwa zdefiniowane na $\mathcal{A}_{S_i^A} \times \mathcal{A}_{S_i^B}$ nie prowadzą do wzrostu obszaru pojemności. Kody konkatenacyjne[3] są zatem optymalne dla $\Phi_A \otimes \Phi_B$.

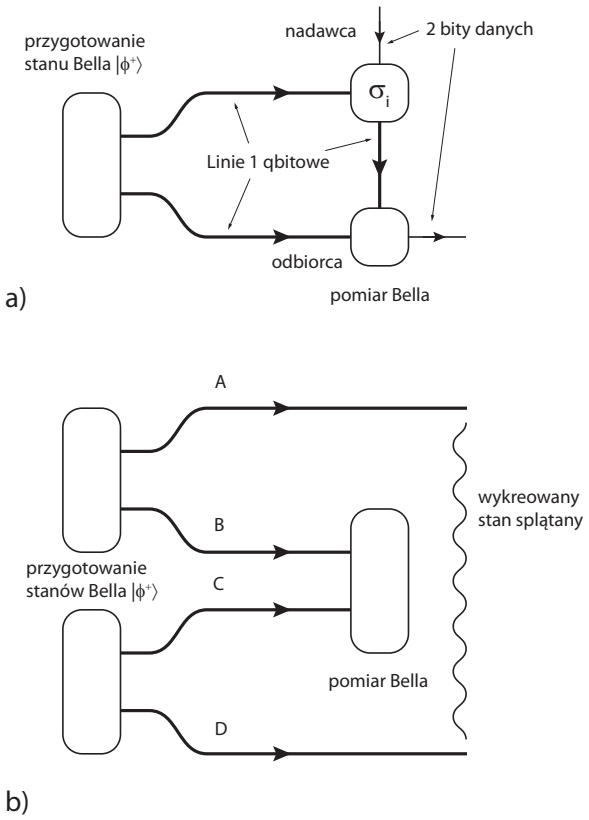
[3]Kod konkatenacyjny kodów $(\{f_i^A\}, g^A, \{\mathcal{A}_{W_i^A}\})$, $(\{f_i^B\}, g^B, \{\mathcal{A}_{W_i^B}\})$ ma postać $(\{f_i^A \times f_i^B\}, g^A \times g^B, \{\mathcal{A}_{W_i^A} \times \mathcal{A}_{W_i^B}\})$. Słowa kodowe kodu konkatenacyjnego to pary (s_i^A, s_i^B) gdzie słowa kodowe s_i^A i s_i^B należące odpowiednio do pierwszego i drugiego kodu i są transmitowane przez wejście kanałów Φ_A i Φ_B należące do S_i.

Z addytywnością obszarów pojemności jest blisko związana addytywność minimalnej entropii wyjścia H_{min}:

$$H_{min}(\Phi_A \otimes \Phi_B) = H_{min}(\Phi_A) + H_{min}(\Phi_B). \tag{2.24}$$

Dowód tego faktu wynika natychmiast z faktoryzacji prawdopodobieństwa przejścia $p_{Y|X_E}$ dla $\Phi_A \otimes \Phi_B$.

2.2 Gęste kodowanie oraz wymiana splątania



Rysunek 2.2: a) schemat gęstego kodowania; b) schemat wymiany splątania; opis obrazków znajduje się w tekście.

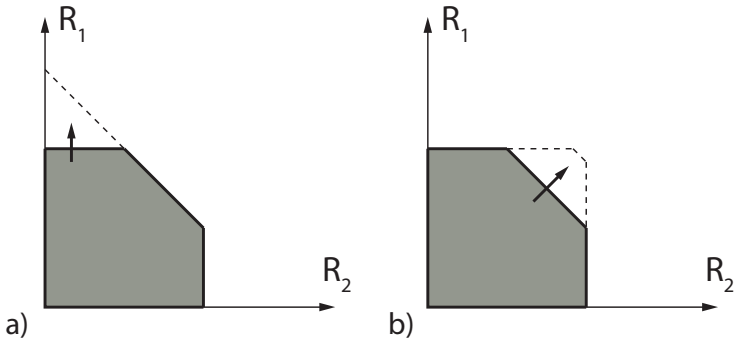
Poniżej opisane zostaną dwa schematy pełniące kluczową funkcję w prezentowanych dalej wynikach. Zaczniemy od schematu gęstego kodowania [16].

Odnosi się on do sytuacji, w której nadawca i odbiorca w momencie transmisji współdzielą stan splątany. Dostęp do tego dodatkowego zasobu ma wpływ na prędkość transmisji informacji klasycznej. Osiągana w tym przypadku wartość nazywa się pojemnością klasyczną wspomaganą splątaniem [14]. W najprostszym przypadku, gdy nadawca i odbiorca współdzielą stan Bella: $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (patrz Rw. (1.47)), schemat gęstego kodowania wygląda następująco (patrz Rys. 2.2.a): nadawca wykonuje na swoim qbicie operację unitarną $\sigma_i \in \{\mathrm{I}, \sigma_x, \sigma_y, \sigma_z\}$, — w ten sposób koduje swój komunikat klasyczny — następnie przesyła qbit do odbiorcy. Teraz odbiorca posiada cały stan dwuqbitowy. Zauważmy, że w wyniku operacji unitarnej współdzielony stan $|\phi^+\rangle$ przechodzi w jeden z czterech ortogonalnych stanów Bella. Odbiorca, wykonując pomiar projektorowy w bazie Bella, może dokładnie określić, jaka operacja została wykonana i jaki komunikat został nadany. Podsumowując, transmisja jednego qbitu pozwoliła, dzięki współdzieleniu splątania, przekazać dwa bity informacji klasycznej. Jest to efekt czysto kwantowy.

Wymiana splątania to procedura, która prowadzi do powstania splątania pomiędzy cząstkami które nie miały okazji oddziaływać ze sobą w przeszłości [11, 95, 96]. Tu również opiszemy jedynie najprostszy przypadek bazujący na stanach Bella (patrz Rys. 2.2.a). W wymianie splątania biorą udział cztery strony: A, B, C i D. Początkowo, stany splątane współdzielą A i B oraz C i D: $|\phi^+\rangle_{AB} \otimes |\phi^+\rangle_{CD}$. Na podsystemach należących do B i C przeprowadzany jest łączny pomiar w bazie Bella, którego wynik (2 bity informacji klasycznej) komunikowany jest A i D. A i D mogą teraz wykonać lokalne operacje unitarne i w ten sposób uzyskać stan $|\phi^+\rangle_{AD}$. Łączny pomiar wykonany na podsystemach B i C wykreował splątanie pomiędzy A i D, mimo iż podsystemy te cały czas były od siebie odseparowane. Zauważmy jeszcze, że w opisanej konfiguracji, pomiędzy A i D powstaje taki sam stan Bella, jaki został zmierzony na podsystemach B i C.

2.3 Wyniki

Jak wspomniano we wstępie do rozdziału, w przypadku wielodostępnych kanałów kwantowych możemy wyróżnić dwie formy superaddytywności: (i) wzrost prędkości transmisji poszczególnych nadawców przy zachowaniu łącznej prędkości transmisji R_T; (ii) wzrost łącznej prędkości transmisji R_T. Rys. 2.3 ilustruje różnice między przedstawionymi typami superaddytyw-



Rysunek 2.3: Superaddytywność obszarów pojemności klasycznej: a) wzrost prędkości transmisji nadawcy S_1 przy zachowaniu łącznej prędkości transmisji R_T — superaddytywność typu (i); b) wzrost łącznej prędkości transmisji R_T (nie musi wiązać się ze wzrostem R_i) — superaddytywność typu (ii). Szarym kolorem zaznaczono obszar uzyskany podczas transmisji stanów produktowych; linią przerywaną zysk wynikający z użycia stanów splątanych; strzałki wskazują kierunek, w którym przesunął się obszar pojemności.

ności.

Superaddytywność typu (i) nie ma odniesienia do kanałów 1-do-1. W tym przypadku splątanie umożliwia zapełnienie luki między maksymalną prędkością transmisji R_i nadawcy S_i, a ograniczeniem wynikającym z łącznej prędkości transmisji R_T (porównaj Tw. 1.15 — kształt obszaru pojemności). Ilustrację stanowią tu kanały, które można znaleźć w częściach: 2.3.1-2.3.4. Opisane tam konstrukcje opierają się na schemacie gęstego kodowania który, robiąc użytek ze splątania, prowadzi do wzrostu zróżnicowania stanów na wyjściu kanału a tym samym entropii stanu średniego.

Efekt superaddytywności będący konsekwencją zastosowania schematu gęstego kodowania jest najlepiej widoczny w skrajnie asymetrycznych przykładach kanałów. Można w nich wyróżnić jednego nadawcę właściwego — to on czerpie korzyści związane z użyciem stanów splątanych. Pozostali nadawcy pełnią funkcję pomocników. Ich jedynym zadaniem jest dostarczanie określonych stanów splątanych. Zastosowanie splątania w niczym im nie pomaga a w opisanych protokołach nie przesyłają oni żadnych komunikatów — ich prędkość transmisji wynosi 0. Symetryzacja kanału, chociaż możliwa, prowadzi do rozmycia efektu superaddytywności, o czym można przeczytać pod koniec części 2.3.1.

Superaddytywność typu (ii) jest efektem analogiczny do efektu aktywacji uzyskanego dla przypadku kanałów 1-do-1 [49]. Tutaj podział zadań jest bardziej sprawiedliwy i wszyscy nadawcy grają równorzędne role.

Problem superaddytywności typu (ii) jest globalnie równoważny z zagadnieniem subaddytywności H_{min} — istnienie pary kanałów, dla której zachodzi jeden z wymienionych tu efektów pozwala na konstrukcję takiej pary kanałów, dla której zachodzi drugi z wymienionych efektów [81]. Związek lokalny tych dwóch efektów, t.j. równoczesne występowanie superaddytywności typu (ii) oraz subaddytywności H_{min} dla danej pary kanałów, można pokazać m.in. dla kanałów, dla których zachodzi $\Phi(\bar{\rho}) = \frac{1}{d}\mathrm{I}$, gdzie $\bar{\rho}$ to stan średni odpowiadający optymalnej mieszaninie stanów wejściowych a d to wymiar przestrzeni wyjścia kanału Φ [76]. W pracy [31] analizowane są inne przypadki kanałów, dla których również ma miejsce taki lokalny związek. Znane obecnie przykłady kanałów, dla których występuje efekt superaddytywności typu (ii) (patrz [27] oraz [49]), poprzez konstrukcję zaczerpniętą z pracy [81], bazują na efekcie subaddytywność H_{min}. Pytanie o to, czy lokalny związek superaddytywności typu (ii) oraz subaddytywności H_{min} zachodzi dla wszystkich kanałów pozostaje problemem otwartym.

Struktura kanałów z wieloma nadawcami jest bogatsza niż struktura kanałów 1-do-1, co pozwala szukać innych źródeł subaddytywności H_{min} niż te, z którymi mamy do czynienia w przypadku kanałów 1-do-1. Wyniki prezentowane w części 2.3.5 odnoszą się do tego zagadnienia.

Pytania, na które starano się odpowiedzieć w tym rozdziale to:

- Czy efekt superaddytywności $\mathcal{R}(\Phi_A) + \mathcal{R}(\Phi_B) \subsetneq \mathcal{R}(\Phi_A \otimes \Phi_B)$ w ogóle zachodzi?

  Rozważania na ten temat oraz pozytywna odpowiedź na pytanie pojawiają się w części 2.3.1. Pochodzą one z pracy [28] i są pierwszymi tego typu wynikami, z jakimi można spotkać się w literaturze.

- Czy dla pojedynczego kanału splątanie ma wpływ na $\mathcal{R}^{(n)}(\Phi)$?

  Przykład pokazujący, że $\mathcal{R}^{(1)}(\Phi) \subsetneq \mathcal{R}^{(2)}(\Phi)$ znajduje się w części 2.3.2 również i pochodzi z pracy [28].

- Czy do uzyskania $\mathcal{R}^{(\infty)}(\Phi)$ wystarcza splątanie dwucząstkowe?

  W części 2.3.3 analizowany jest przykład kanału kwantowego Φ, dla którego $\mathcal{R}^{(2)} \subsetneq \mathcal{R}^{(\infty)}$. Stany splątane pozwalające osiągnąć $\mathcal{R}^{(n)}(\Phi)$

dla $n > 2$, ze względu na wymagane symetrie, nie dają się zredukować do iloczynu tensorowego stanów Bella, a przez to do klasycznego schematu gęstego kodowania. Prowadzone w części 2.3.3 rozważania wiążą się również z ważnym ze względów praktycznym zagadnieniem rzędu splątania n wystarczającego, aby dla danego kanału Φ uzyskać zadowalające przybliżenie $\mathcal{R}^{(n)}(\Phi) \approx \mathcal{R}^{(\infty)}(\Phi)$. Prezentowane wyniki pochodzą z pracy [30].

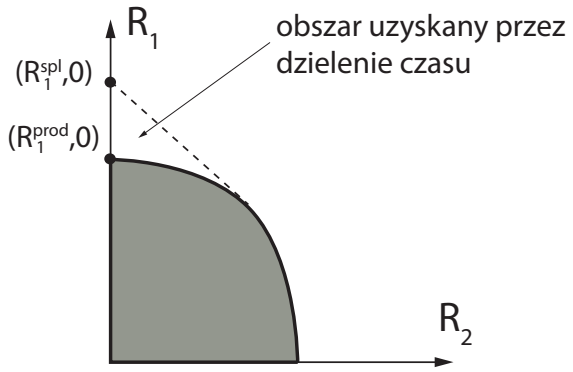
- Czy możliwa jest superaddytywność regularyzowanych obszarów pojemności klasycznej $\mathcal{R}^{(\infty)}(\Phi) + \mathcal{R}^{(\infty)}(\Psi) \subsetneq \mathcal{R}^{(\infty)}(\Phi \otimes \Psi)$?

  Przykład pokazujący, że superaddytywność $\mathcal{R}^{(\infty)}$ faktycznie ma miejsce, znajduje się w części 2.3.4 i pochodzi z pracy [30]. Przedstawiona jest tam superaddytywność typu (i). Superaddytywność typu (ii) wyrażona w terminach $\mathcal{R}^{(\infty)}$ ciągle pozostaje nieuchwytna.

- Czy możliwa jest superaddytywność typu (ii)? Czy możliwa jest subaddytywność minimalnej entropii wyjścia H_{min}?

  Pozytywna odpowiedź na oba pytania znajduje się w części 2.3.5 i została zaczerpnięta z pracy [27]. Pokazany tu efekt opiera się na fundamentalnej własności kanałów wielodostępnych jaką jest niezależność nadawców, przez co różni się on zasadniczo od wyniku Hastingsa [49] i nie daje się do niego sprowadzić. Zaletą prezentowanego podejścia jest istnienie algorytmu pozwalającego wyznaczyć jawną postać analizowanych tu kanałów, co powinno pomóc w lepszym zrozumieniu mechanizmów stojących za efektem subaddytywności H_{min} oraz superaddytywności $\mathcal{R}$.

Warto jeszcze nadmienić, w odniesieniu do wyników prezentowanych w części 2.3.5, że efekt superaddytywności $\mathcal{R}$ został pokazany na przykładzie kanałów wielodostępowych łamiących splątanie [58]. Ponieważ superaddytywność pojemności klasycznej nie zachodzi dla łamiących splątanie kanałów z jednym nadawcą i jednym odbiorcą, pokazany efekt sugeruje jakościową różnicę pomiędzy kanałami z jednym i wieloma nadawcami. Zostało to po raz pierwszy zauważone w pracy [47] gdzie za przykład posłużył wielodostępowy kanał łamiący splątanie współpracujący z kanałem identycznościowym. Przedstawiony wynik idzie o krok dalej demonstrując, że bardzo silna superaddytywność ma miejsce również w przypadku, gdy komunikacja zachodzi *wyłącznie* poprzez kanały łamiące splątanie.



Rysunek 2.4: Schemat dowodzenia superaddytywności obszarów pojemności klasycznej.

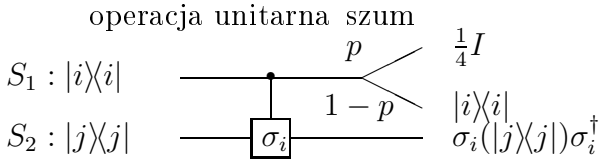
Przeglądając wyniki, czytelnik często będzie spotykał się z opisaną niżej strategią dowodzenia superaddytywności $\mathcal{R}$. Załóżmy, że chcemy pokazać superaddytywność obszarów pojemności wielodostępowych kanałów Φ_A, Φ_B (może oczywiście zachodzić sytuacja $\Phi_A = \Phi_B$). Dla uproszczenia przyjmijmy, że kanały te posiadają po dwóch nadawców. Niech $\mathcal{R}_{prod}(\Phi_A \otimes \Phi_B)$ będzie obszarem pojemności uzyskanym przez protokoły korzystające tylko ze stanów produktowych natomiast, aby otrzymać obszar $\mathcal{R}_{spl}(\Phi_A \otimes \Phi_B)$, trzeba posiłkować się stanami splątanymi. Niech R_1^{prod}, R_2^{prod} to maksymalne wartości prędkości transmisji osiągane przez nadawców S_1, S_2 w obszarze $\mathcal{R}_{prod}$. Chcemy udowodnić, że: $\mathcal{R}_{prod}(\Phi_A \otimes \Phi_B) \subsetneq \mathcal{R}_{spl}(\Phi_A \otimes \Phi_B)$. W tym celu wystarczy pokazać, że korzystając ze stanów splątanych, jeden z nadawców, powiedzmy S_1, osiąga prędkość transmisji $R_1^{spl} > R_1^{prod}$ (porównaj punkty $(R_1^{spl}, 0), (R_1^{prod}, 0)$ na Rys. 2.4). Innymi słowy, musimy znaleźć ograniczenie górne na R_1^{prod} oraz odpowiedni protokół. Mając punkt $(R_1^{spl}, 0) \notin \mathcal{R}_{prod}(\Phi_A \otimes \Phi_B)$, ograniczenie dolne na $\mathcal{R}_{spl}(\Phi_A \otimes \Phi_B)$ otrzymuje się poprzez procedurę dzielenia czasu między protokołem osiągającym $(R_1^{spl}, 0)$ a protokołami osiągającymi punkty z $\mathcal{R}_{prod}(\Phi_A \otimes \Phi_B)$. Oczywiście procedura dzielenia czasu pozwala uzyskać również wszystkie punkty z $\mathcal{R}_{prod}(\Phi_A \otimes \Phi_B)$, co kończy dowód. Opisaną technikę ilustruje Rys. 2.4.

Doświadczenia z zakresu optyki kwantowej wydają się być najbardziej naturalnym obszarem do weryfikacji koncepcji kwantowej komunikacji. W praktyce obecnie napotyka się tu jednak na liczne problemy natury technicznej: (i) liniowe elementy optyczne nie pozwalają przeprowadzić pomiaru w pełnej bazie Bella [87, 68, 22, 44]; (ii) nie dysponujemy wystarczająco silnym

medium Kerra, pozwalającym realizować bramki dwuqbitowe z zadowalającą dokładnością; (iii) schemat KLM [64] oraz jednokierunkowe obliczenia kwantowe [74], wydające się najbardziej obiecującą alternatywą dla bramek opartych o medium Kerra, wprowadzają zbyt wysoki poziom szumu [5] oraz wymagają postselekcja otrzymanych wyników, co może zostać uznane za lukę logiczną w ewentualnych eksperymentach.

2.3.1 Zaczynamy: kwantowa aktywacja w elementarnych przykładach kanałów

Pierwszy przykład superaddytywności obszarów pojemności klasycznej zademonstrowany zostanie przy użyciu prostego kanału Φ^p z dwoma nadawcami: S_1, S_2 współpracującego z kanałem identycznościowym $\mathcal{I}$. Podczas jednego użycia, przez kanał $\mathcal{I}$ każdy z nadawców może przesłać bezbłędnie 1 qubit. Transmisja stanów splątanych pomiędzy kanałem Φ^p, a $\mathcal{I}$ pozwala obserwować efekt superaddytywności dla nadawcy S_1.



Rysunek 2.5: Schemat kanału Φ^p. Opis kanału zamieszczono w tekście.

Nadawca S_1 przesyła układy 4 poziomowe ($\mathcal{H}_{S_1} = \mathbb{C}^4$) a nadawca S_2 qbity ($\mathcal{H}_{S_2} = \mathbb{C}^2$). Schemat kanału przedstawiony jest na Rys. 2.5. Można na nim wyróżnić dwa bloki. Pierwszy z nich to operacja unitarna:

$$U = \sum_{i=1}^{4} e_i \otimes \sigma_i, \tag{2.25}$$

gdzie $e_i = |i\rangle\langle i|$ natomiast $\sigma_i \in \{I, \sigma_x, \sigma_y, \sigma_z\}$. W zależności od stanu, w jakim znajduje się podukład od nadawcy S_1, podukład od nadawcy S_2 jest modyfikowany przez działanie odpowiedniej macierzy Pauliego. Drugi blok wiąże się z szumem wprowadzanym przez kanał na linię S_1. Stan tej linii, z prawdopodobieństwem p, jest zastępowany przez stan maksymalnie wymieszanym, natomiast z prawdopodobieństwem $1-p$ pozostawiany bez zmian.

Blok ten można przedstawić jako $\Lambda_p \otimes \mathcal{I}$, gdzie Λ_p to 2 qbitowy kanał depolaryzacyjny. Odbiorca ma dostęp zarówno do linii S_1 jak i S_2. Podsumowując, działanie kanału wyraża się formułą:

$$\Phi^p(\rho) = (\Lambda_p \otimes \mathcal{I})(\rho) = (1-p)U\rho U^\dagger + p\frac{1}{4}\mathrm{I} \otimes \mathrm{tr}_{S_1}\left[U\rho U^\dagger\right]. \tag{2.26}$$

Poniżej analizowany będzie scenariusz, w którym występuje $\Phi^{p=1}$. W tym przypadku stan wyjściowy na linii S_1 jest zawsze maksymalnie wymieszany i nie niesie żadnej informacji o wejściach kanału. Dla uproszczenia rachunków można zatem przyjąć, że odbiorca ma dostęp tylko do stanu wyjściowego na linii S_2. Odpowiada to operacji częściowego śladu.

Poszukamy teraz górnego ograniczenia dla obszarów pojemności $\mathcal{R}^{(\infty)}(\Phi^{p=1})$ oraz $\mathcal{R}^{(\infty)}(\mathcal{I})$. Wyjście kanału $\Phi^{\otimes n}$ ma rozmiar n qbitów. Na mocy ograniczenia Holevo, układ n qbitowy może nieść co najwyżej n bitów informacji klasycznej. To oznacza, że regularyzowany obszar pojemności musi spełniać:

$$R_1 + R_2 \leq 1. \tag{2.27}$$

Podobna argumentacja prowadzi do ograniczenia dla obszaru pojemności kanału identycznościowego $\mathcal{I}$:

$$R_1 \leq 1,\ R_2 \leq 1. \tag{2.28}$$

Poniżej zobaczymy, że wyznaczone przed chwilą ograniczenia obszarów pojemności są osiągane przy użyciu stanów produktowych. W przypadku gdy nadawca S_1 przesyła tylko jeden ustalony stan, powiedzmy $|0\rangle$, stan przesyłany przez S_2 trafia do odbiorcy w niezmienionej postaci, co prowadzi do wektora prędkości transmisji: $(R_1, R_2) = (0, 1)$. Natomiast gdy S_2 nadaje ciągle stan $|0\rangle$, nadawca S_2 może pozostawić go bez zmian przesyłając stan $|0\rangle$ lub przekształcić w $\sigma_X|0\rangle = |1\rangle$ przesyłając $|1\rangle$. Odbiorca za każdym razem otrzymuje stan czysty, produkcja entropii przez kanał ma wartość 0, prędkość transmisji zależy zatem tylko od entropii średniego stanu wyjściowego. Stąd, dla opisanego protokółu, otrzymujemy wektor prędkości transmisji: $(R_1, R_2) = (1, 0)$. W przypadku $\mathcal{I}$ ograniczenie (2.28) jest osiągane przez mieszaniny składające się w równych proporcjach ze stanów $|0\rangle, |1\rangle$. Pokazuje to, że obszary pojemności $\mathcal{R}^{(\infty)}(\Phi^{p=1})$ oraz $\mathcal{R}^{(\infty)}(\mathcal{I})$ wyznaczane są przez formuły jednowyrazowe, tj. $\mathcal{R}^{(\infty)} = \mathcal{R}^{(1)}$. Transmisja splątania pomiędzy kopiami tego kanału nie zwiększa obszaru pojemności.

Znajdziemy teraz regularyzowany obszar pojemności $\mathcal{R}^{(\infty)}(\Phi^{p=1} \otimes \mathcal{I})$ dla pracujących równolegle kanałów $\Phi^{p=1}$ i $\mathcal{I}$. Posługując się ograniczeniem Holevo odpowiednio dla wejść i wyjścia $(\Phi^{p=1} \otimes \mathcal{I})^{\otimes n}$ uzyskujemy ograniczenie górne regularyzowanego obszaru pojemności w postaci:

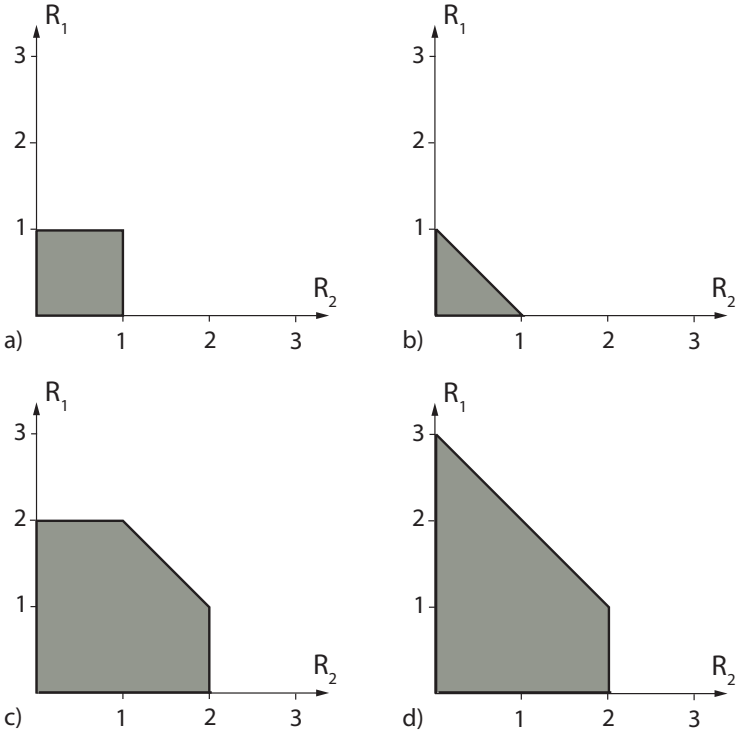
$$R_1 \leq 3,\ R_2 \leq 2,\ R_1 + R_2 \leq 3. \tag{2.29}$$

Aby pokazać, że ograniczenie to jest osiągalne, odwołamy się do koncepcji gęstego kodowania. Niech nadawca S_2 przesyła zawsze stan $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Pierwsza część stanu transmitowana jest przez kanał $\Phi^{p=1}$, natomiast drugą przez kanał $\mathcal{I}$. Wysyłając jeden z czterech stanów $|0\rangle, \ldots, |3\rangle$, nadawca S_1 wpływa na stan pochodzący od S_2 i decyduje o tym, który z czterech stanów Bella otrzyma odbiorca. Ponieważ stany Bella są wzajemnie ortogonalne, nadawca S_1 może za jednym użyciem kanału przekazać bezbłędnie dowolny z czterech komunikatów. Nadawca S_1 może również przesłać 1 bit informacji przez swoje wejście kanału $\mathcal{I}$. W sumie prowadzi to do wektora prędkości transmisji: $(R_{S_1}, R_{S_2}) = (3, 0)$. Pozostałe punkty obszaru pojemności danego nierównościami (2.29) można otrzymać poprzez procedurę dzielenie czasu tak, jak to opisano we wstępie. Regularyzowany obszar pojemności $\mathcal{R}^{(\infty)}(\Phi^{p=1} \otimes \mathcal{I})$ ponownie dany jest formułami jednowyrazowymi. Obszar $\mathcal{R}^{(\infty)}(\Phi^{p=1} \otimes \mathcal{I})$ został pokazany na Rys. 2.6.d). Porównując go z obszarem pojemności osiąganym w przypadku transmisji stanów produktowych $\mathcal{R}^{(\infty)}(\Phi^{p=1}) + \mathcal{R}^{(\infty)}(\mathcal{I})$ — Rys. 2.6.c) — widzimy zysk prędkości jaki doświadcza, dzięki wykorzystaniu splątania, nadawca S_1.

Zwróćmy uwagę na występującą tu asymetrię między nadawcami S_1 i S_2. Nadawca S_2 pełni funkcję pomocnika - nie przesyła żadnej informacji a jego zadanie polega na dostarczaniu zasobu jakim jest splątanie. W ten sposób umożliwia nadawcy S_1 osiągnięcie większej prędkość transmisji. Widzimy tutaj pewien rodzaj zdalnego gęstego kodowania, które S_1 wykonuje na podukładzie dostarczonym przez S_2. Zarówno przy transmisji stanów produktowych jak i splątanych, odbiorca otrzymuje stany czyste. Ponieważ produkcja entropii wynosi 0, wzrost prędkości transmisji wywołany jest przez wzrost różnorodności stanów, które otrzymuje odbiorca.

Na koniec tej części zobaczymy jeszcze, jak można przekształcić kanał $\Phi^{p=1}$ w kanał Ψ symetryczny ze względu na zamianę nadawców. W tym przypadku superaddytywność maksymalnej prędkości transmisji będzie można obserwować dla każdego z nadawców.

Kanał Ψ (patrz Rys. 2.7) posiada dwóch nadawców: S_A i S_B. Każdy z nich kontroluje po dwie 1 qbitowe linie. Kanał może pracować w dwóch trybach.



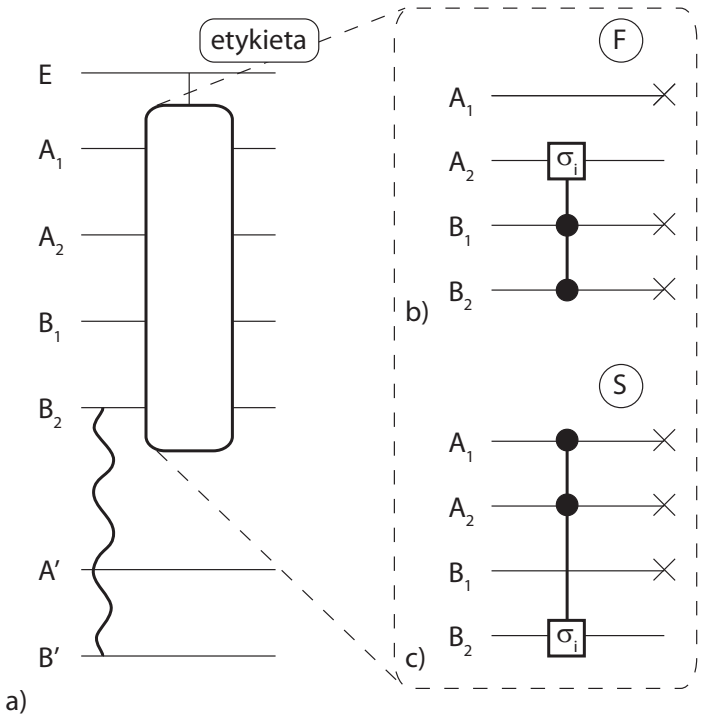
Rysunek 2.6: Łamanie addytywności obszarów pojemności: a) obszar pojemności kanału $\Phi^{p=1}$, b) obszar pojemności kanału identycznościowego, c) suma Minkowskiego obszarów a) i b), d) obszar pojemności pracujących równolegle kanałów z punków a) i b), obszar ten jest większy od obszaru c).

Aktualny tryb wybierany jest losowo przy każdej transmisji. Odbywa się to przez pomiar na środowisku E będącym w stanie maksymalnie wymieszanym. Każdy z trybów ma równe szanse realizacji. Odbiorca jest informowany o wyniku pomiaru na środowisku, a zatem i o trybie pracy kanału przy użyciu etykiety $|F\rangle$ lub $|S\rangle$.

Ze względu na rozmiar przestrzeni wyjścia, obszar pojemności kanału Ψ ograniczony jest przez:

$$R_A \leq 1,\ R_B \leq 1,\ R_A + R_B \leq 1 \tag{2.30}$$

Wierzchołek $(1, 0)$ jest osiągany, gdy nadawca S_A przesyła z równym prawdopodobieństwem stany $|00\rangle, |01\rangle$ natomiast nadawca S_B tylko stan $|00\rangle$. Wierzchołek $(0, 1)$ można otrzymać w sposób analogiczny. Pozostałe punkty obszaru dane są poprzez procedurę dzielenia czasu.



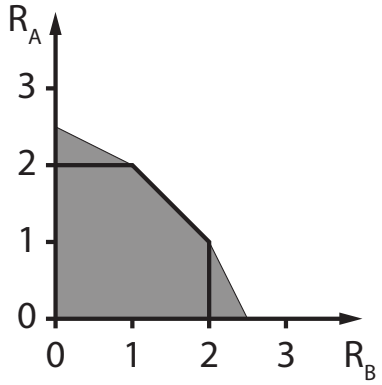
Rysunek 2.7: a) kanał Ψ współpracuje z kanałem identycznościowym, linia falowana oznacza splątanie, b), c) dwa tryby pracy kanału Ψ, w kółku wartość etykiety odnosząca się do danego trybu. Krzyżyk na końcu linii oznacza, że odbiorca otrzymuje stan maksymalnie wymieszany. Kontrolowana bramka σ_i realizuje operację unitarną: $|00\rangle\langle 00|\otimes \mathrm{I} + |10\rangle\langle 10|\otimes\sigma_x + |01\rangle\langle 01|\otimes\sigma_z + |11\rangle\langle 11|\otimes \sigma_y$.

Aby zademonstrować efekt superaddytywności, ponownie skorzystamy z kanału identycznościowego: $\mathcal{I}$. Obszar pojemności dla stanów produktowych $\mathcal{R}(\Psi) + \mathcal{R}(\mathcal{I})$ dany jest w tym przypadku przez:

$$R_A \leq 2,\ R_B \leq 2,\ R_A + R_B \leq 3. \tag{2.31}$$

Teraz zobaczymy jak na obszar pojemności wpływa transmisja stanów splątanych. Dolne ograniczenie dla tego obszaru zostało przedstawione na Rys. 2.8. Wierzchołki $(1, 2)$ oraz $(2, 1)$ można otrzymać przesyłając stany produktowe, dlatego poniżej zostanie opisany jedynie scenariusz, który pozwala osiągnąć wierzchołek $(2.5, 0)$ [4].

[4]Wierzchołek $(0, 2.5)$ otrzymuje się analogicznie ze względu na symetrię kanału



Rysunek 2.8: Dolne ograniczenie na $\mathcal{R}(\Psi \otimes \mathcal{I})$. Pogrubionymi liniami został zaznaczony obszar $\mathcal{R}(\Psi) + \mathcal{R}(\mathcal{I})$.

Niech nadawca S_A przesyła z prawdopodobieństwem 1/8 stany w postaci $|i\rangle|i'\rangle$. Stan $|i\rangle \in \{|00\rangle, \ldots, |11\rangle\}$ podawany jest na wejście A_1, A_2 kanału Ψ a stan $|i'\rangle \in \{|0\rangle, |1\rangle\}$ na wejście A' kanału $\mathcal{I}$. Nadawca S_B przesyła cały czas stan $\frac{1}{\sqrt{2}}|0\rangle(|00\rangle + |11\rangle)$, gdzie stan Bell jest nadawany przez kanał $\mathcal{I}$ oraz linię B_2 kanału Ψ. Dla danego wejścia (i, i') odbiorca otrzymuje stan:

$$\begin{aligned} \rho_{i,i'} &= \frac{1}{2}|F\rangle\langle F| \otimes \frac{1}{2}\mathrm{I} \otimes |i_{A_2}\rangle\langle i_{A_2}| \otimes \frac{1}{8}\mathrm{I}^{\otimes 3} \otimes |i'\rangle\langle i'| \qquad (2.32) \\ &+ \frac{1}{2}|S\rangle\langle S| \otimes \frac{1}{8}\mathrm{I}^{\otimes 3} \otimes |\psi_i\rangle\langle\psi_i| \otimes |i'\rangle\langle i'| \end{aligned}$$

Stan wyjściowy składa sie z etykiety informującej o trybie pracy kanału oraz 6 qbitów. Pierwsze 4 qbity to linie A_1, A_2, B_1, B_2 kanału Ψ. Qbity 5 i 6 qbit to linie A' i B' kanału $\mathcal{I}$. Jeśli kanał pracuje w trybie F, na linii S_2 wykonywana jest losowo, z równym prawdopodobieństwem, operacja I lub σ_Y. Ponieważ operacje te nie zmieniają wektorów $|0\rangle, |1\rangle$, odbiorca jest w stanie odczytać komunikat przesyłany linią A_2. Natomiast, gdy kanał pracuje w trybie S, operacja σ_i kontrolowana przez stan podukładu pochodzącego od nadawcy S_A jest wykonywana na stanie Bella dostarczonym przez S_B. Wynik tej operacji to stan ψ_i. Średni stan na wyjściu kanału $\bar{\rho} = \frac{1}{8}\sum_{i,i'} \rho_{i,i'}$ ma postać:

$$\begin{aligned} \bar{\rho} &= \frac{1}{2}\left(|F\rangle\langle F|\frac{1}{64}\mathrm{I}^{\otimes 6} + |S\rangle\langle S|\frac{1}{64}\mathrm{I}^{\otimes 6}\right) \qquad (2.33) \\ &= \frac{1}{128}\mathrm{I}^{\otimes 7} \qquad (2.34) \end{aligned}$$

Entropie opisanych stanów wynoszą odpowiednio $S(\rho_{i,i'}) = 4.5$ [5] i $S(\bar{\rho}) = 7$. Na podstawie Tw. 1.14, prędkość transmisji $R_A = 2.5$. Nadawca S_B przesyła tylko jeden stan, osiągana przez niego prędkość transmisji wynosi zatem $R_B = 0$.

W pokazanych wierzchołkach wykraczających poza obszar pojemności dla stanów produktowych jeden z nadawców dalej pełni funkcję pomocnika. Opisana wyżej symetryzacja skutkuje zmniejszeniem wielkości efektu aktywacji.

2.3.2 Obecność nietrywialnego szumu: kiedy formuła jednowyrazowa zawodzi

Zajmować się teraz będziemy efektem superaddytywności występującym podczas wielokrotnego użycia tego samego kanału. W rozważaniach ponownie posłużymy się wprowadzonym wcześniej kanałem Φ^p, na którego przykładzie zobaczymy:

$$\mathcal{R}^{(1)}(\Phi^p) \subsetneq \mathcal{R}^{(2)}(\Phi^p). \tag{2.35}$$

Parametr p należy tym razem do przedziału $(0, 1)$, w którym to zakresie kanał wprowadza nietrywialny szum. Przez nietrywialny rozumiemy tutaj sytuację, gdy nie można, tak jak poprzednio, odrzucić zaszumionego fragmentu stanu wyjściowego kanału ze względu na niesioną przezeń informację o stanie wejściowym.

Wyznaczenie całego obszaru pojemności, nawet w przypadku formuły jednowyrazowej, jest trudnym zadaniem. Aby pokazać efekt superaddytywności wystarczy jednak ograniczyć się do analizy prędkości transmisji R_1 uzyskiwanych przez nadawcę S_1. Poniżej także będziemy mieli do czynienia z sytuacją, gdy nadawca S_2 pełni funkcję pomocnika i przesyła za każdym razem ten sam ustalony stan. Korzystając z ograniczenia Holevo, maksymalną prędkość transmisji uzyskaną przez S_1 przy użyciu stanów produktowych można oszacować przez:

$$R_1^{(1)} \leq \max_{v,\{p_i,u_i\}} \left[S\left(\Phi^p(\rho \otimes v)\right) - \sum_i p_i S\left(\Phi^p(u_i \otimes v)\right) \right], \tag{2.36}$$

gdzie $\rho = \sum_i p_i u_i$, $|u_i\rangle \in \mathbb{C}^4$, $|v\rangle \in \mathbb{C}^2$.

[5] Obliczając entropię korzystamy z relacji $S(\sum_i p_i \rho_i) = \sum_i p_i \rho_i + H(\{p_i\})$ zachodzącej dla operatorów gęstości ρ_i rozpiętych na podprzestrzeniach wzajemnie ortogonalnych oraz z ortogonalności $|F\rangle$ i $|S\rangle$.

Następujące lematy pomogą pokazać, że ograniczenie (2.36) jest ciasne oraz ułatwią obliczenie maksymalnej wartości $R_1^{(1)}$.

Lemat 2.2 *Entropia średniego stanu wyjścia* $S\left(\Phi^p(\rho \otimes v)\right)$ *osiąga wartość maksymalną dla stanu maksymalnie wymieszanego* $\rho = \frac{1}{4}\mathrm{I}$.

Dowód:

Dla ustalonego stanu v definiujemy kanał $\tilde{\Phi}^p(\varrho) = \Phi^p(\varrho \otimes v)$. Ze względu na liniowość kanału $\tilde{\Phi}^p$ i własności entropii, $S\left(\tilde{\Phi}^p(\varrho)\right)$ jest wklęsłą funkcją stanu ϱ. Funkcja taka posiada swoje maksimum w punkcie ekstremum — wystarczy zatem dowieść, że przypada on w $\varrho = \frac{1}{4}\mathrm{I}$. W tym celu pokażemy, że pochodna entropii wzdłuż dowolnego kierunku Δ [6] znika dla ϱ:

$$\forall_\Delta \quad \left.\frac{\partial S\left(\tilde{\Phi}^p(\varrho + \alpha\Delta\right)}{\partial\alpha}\right|_{\alpha=0} = 0. \tag{2.37}$$

Pochodna entropii wyraża się formułą [80]:

$$\left.\frac{\partial S(\rho + \alpha\delta)}{\partial\alpha}\right|_{\alpha=0} = -\mathrm{tr}\left[\delta \log \rho\right], \tag{2.38}$$

gdzie δ jest macierzą kierunku o śladzie równym 0. Dla kanału Φ^p, stan ρ oraz kierunek δ w punkcie $\varrho = \frac{1}{4}\mathrm{I}$ mają postać (patrz Rw. (2.26)):

$$\begin{aligned}
\rho &= \tilde{\Phi}^p\left(\frac{1}{4}\mathrm{I}\right) \\
&= (1-p)U\left(\frac{1}{4}\mathrm{I} \otimes |v\rangle\langle v|\right)U^\dagger + p\frac{1}{8}\mathrm{I} \otimes \mathrm{I}, \qquad (2.39)\\
\delta &= \tilde{\Phi}^p(\Delta) \\
&= (1-p)U(\Delta \otimes v)U^\dagger + p\frac{1}{4}\mathrm{I} \otimes \mathrm{tr}_{S_1}\left[U(\Delta \otimes v)U^\dagger\right], \qquad (2.40)
\end{aligned}$$

gdzie $U = \sum_i e_i \otimes \sigma_i$. Ponieważ kanał kwantowy zachowuje ślad, zachodzi $\mathrm{tr}\left[\delta\right] = 0$, można więc stosować formułę (2.38). Przepiszmy operator $\log\rho$

[6] Δ jest macierzą 4×4 o śladzie równym 0.

używając projektora $P = U(\mathrm{I} \otimes v)U^\dagger$:

$$\begin{aligned} \log \rho &= \log \left[\frac{p}{8}(\mathrm{I} \otimes \mathrm{I} - P) + \frac{2+p}{4} P \right] && (2.41) \\ &= (\mathrm{I} \otimes \mathrm{I} - P) \log \left(\frac{p}{8} \right) + P \log \left(\frac{2+p}{4} \right). && (2.42) \end{aligned}$$

W kroku (2.42) korzystamy z faktu, że $\mathrm{I} \otimes \mathrm{I} - P$ jest również projektorem oraz że funkcja log w działaniu na projektor nie zmienia go.

Biorąc postać δ oraz $\log \rho$ ze wzoru (2.40), równanie (2.42) oraz korzystając z liniowości operacji śladu, formułę (2.38) można rozbić na sumę czterech wyrazów:

$$\begin{aligned} \mathrm{tr}\left[\delta \log \rho\right] &= \frac{p}{4} \log \left(\frac{2+p}{4} \right) \mathrm{tr}\left[\left(\mathrm{I} \otimes \mathrm{tr}_{S_1} \left[U(\Delta \otimes v)U^\dagger \right] \right) \cdot P \right] + && (2.43) \\ & (1-p) \log \left(\frac{2+p}{4} \right) \mathrm{tr}\left[U(\Delta \otimes v)U^\dagger \cdot P \right] + \\ & \frac{p}{4} \log \left(\frac{p}{8} \right) \mathrm{tr}\left[\mathrm{I} \otimes \mathrm{tr}_{S_1} \left[U(\Delta \otimes v)U^\dagger \cdot \mathrm{I} \otimes \mathrm{I} \right] \right] + \\ & (1-p) \log \left(\frac{p}{8} \right) \mathrm{tr}\left[U(\Delta \otimes v)U^\dagger \cdot \mathrm{I} \otimes \mathrm{I} \right] \end{aligned}$$

Poniżej przekonamy się, że każdy z tych wyrazów znika, co ostatecznie dowodzi, iż dla każdego kierunku Δ i każdego stanu v, formuła (2.38) wynosi 0.

Korzystając ze znanej własności operacji śladu $\mathrm{tr}\left[A \otimes B\right] = \mathrm{tr}\left[A\right] \mathrm{tr}\left[B\right]$ oraz z $\mathrm{tr}\left[\Delta\right] = 0$ otrzymujemy od razu:

$$\begin{aligned} \mathrm{tr}\left[U(\Delta \otimes v)U^\dagger \right] &= \mathrm{tr}\left[\Delta \otimes v\right] \\ &= 0. && (2.44) \end{aligned}$$

Ponadto posiłkując się cyklicznością śladu oraz wykonując mnożenie widzimy, że:

$$\begin{aligned} \mathrm{tr}\left[U(\Delta \otimes v)U^\dagger \cdot P \right] &= \mathrm{tr}\left[U(\Delta \otimes v)U^\dagger \cdot U(\mathrm{I} \otimes v)U^\dagger \right] \\ &= \mathrm{tr}\left[\Delta \otimes v\right] \\ &= 0 && (2.45) \end{aligned}$$

Zanim przejdziemy do dyskusji kolejnego wyrazu zauważmy, że:

$$\begin{aligned}
\mathrm{tr}_{S_1}\left[U(\Delta\otimes v)U^\dagger\right] &= \mathrm{tr}_{S_1}\left[\sum_{i,j}(e_i\Delta e_j)\otimes(\sigma_i v\sigma_j)\right] && (2.46)\\
&= \sum_{i,j}\mathrm{tr}_{S_1}\left[e_i\Delta e_j\right]\otimes(\sigma_i v\sigma_j) && (2.47)\\
&= \sum_{i}\mathrm{tr}_{S_1}\left[e_i\Delta\right]\otimes(\sigma_i v\sigma_i), && (2.48)
\end{aligned}$$

gdzie wzór (2.48) otrzymaliśmy dzięki ortogonalności e_i. Wykonując proste przekształcenia otrzymujemy:

$$\begin{aligned}
&\mathrm{tr}\left[\left(\mathrm{I}\otimes\mathrm{tr}_{S_1}\left[U(\Delta\otimes v)U^\dagger\right]\right)\cdot P\right]\\
&= \mathrm{tr}\left[\left(\mathrm{I}\otimes\sum_i\mathrm{tr}_{S_1}\left[e_i\Delta\right]\sigma_i v\sigma_i\right)\cdot P\right]\\
&= \mathrm{tr}\left[U^\dagger\cdot\left(\mathrm{I}\otimes\sum_i\mathrm{tr}_{S_1}\left[e_i\Delta\right]\sigma_i v\sigma_i\right)\cdot U\cdot(\mathrm{I}\otimes v)\right]\\
&= \sum_{k,l}\mathrm{tr}\left[e_k e_l\right]\mathrm{tr}\left[\left(\sum_i\mathrm{tr}_{S_1}\left[e_i\Delta\right]\sigma_k\sigma_i v\sigma_i\sigma_l v\right)\right]\\
&= \sum_{k,l}\delta_{k,l}\mathrm{tr}\left[\left(\sum_i\mathrm{tr}_{S_1}\left[e_i\Delta\right]\sigma_k\sigma_i v\sigma_i\sigma_l v\right)\right]\\
&= \sum_{k}\mathrm{tr}\left[\sum_i\mathrm{tr}_{S_1}\left[e_i\Delta\right]\sigma_k\sigma_i v\sigma_i\sigma_k v\right]\\
&= \sum_{k,i}\mathrm{tr}_{S_1}\left[e_i\Delta\right]\mathrm{tr}\left[\sigma_k\sigma_i v\sigma_i\sigma_k v\right]\\
&= \sum_{i}\mathrm{tr}_{S_1}\left[e_i\Delta\right]\mathrm{tr}\left[\sum_k\sigma_k\sigma_i v\sigma_i\sigma_k v\right]\\
&= \sum_{i}\mathrm{tr}_{S_1}\left[e_i\Delta\right]\mathrm{tr}\left[\mathrm{I}v\right] && (2.49)\\
&= \mathrm{tr}\left[\Delta\right] && (2.50)\\
&= 0, && (2.51)
\end{aligned}$$

gdzie formuła (2.49) wynika z $\forall_{w\in\mathbb{C}^2}\sum_i \sigma_i w\sigma_i = \mathrm{I}$ a (2.50) z zupełności zbioru projektorów $\{e_i\}$. W podobny sposób możemy pokazać:

$$\begin{aligned}\mathrm{tr}\left[\mathrm{I}\otimes \mathrm{tr}_{S_1}\left[U(\Delta\otimes v)U^\dagger\right]\right] &= \mathrm{tr}\left[\mathrm{I}\otimes\sum_i \mathrm{tr}_{S_1}\left[e_i\Delta\right]\sigma_i v\sigma_i\right]\\ &= 4\sum_i \mathrm{tr}\left[e_i\Delta\right]\mathrm{tr}\left[\sigma_i v\sigma_i\right]\\ &= 4\mathrm{tr}\left[\Delta\right]\\ &= 0 \qquad (2.52)\end{aligned}$$

□

Lemat 2.3 *Entropia wyjścia* $S\big(\Phi^p(u\otimes v)\big)$ *kanału* Φ^p *osiąga minimum dla stanów* $|u\rangle\in\{|0\rangle,\ldots,|3\rangle\}$ *i wynosi* $H(1-\frac{3p}{4},\frac{p}{4},\frac{p}{4},\frac{p}{4})$.

Dowód:

Minimalna entropia wyjścia kanału depolaryzującego Λ_p pracującego równolegle z dowolnym kanałem Γ spełnia:

$$H_{min}(\Lambda_p\otimes\Gamma) = H_{min}(\Lambda_p) + H_{min}(\Gamma) \qquad (2.53)$$

i jest osiągana przez stany produktowe [63]. W takim razie $H_{min}(\Phi^p)$ możemy oszacować przez (patrz Rw. (2.26)):

$$\begin{aligned}H_{min}(\Phi^p) &= \min_{|u\rangle,|v\rangle} S\Big(\Phi^p[|u\rangle\langle u|\otimes|v\rangle\langle v|]\Big) &(2.54)\\ &= \min_{|u\rangle,|v\rangle} S\Big((\Lambda_p\otimes\mathcal{I})\left[U\left(|u\rangle\langle u|\otimes|v\rangle\langle v|\right)U^\dagger\right]\Big) &(2.55)\\ &\geq \min_{|u\rangle,|v\rangle} S\Big((\Lambda_p\otimes\mathcal{I})\left[|u\rangle\langle u|\otimes|v\rangle\langle v|\right]\Big) &(2.56)\\ &= H_{min}(\Lambda_p\otimes\mathcal{I}) &(2.57)\\ &= H_{min}(\Lambda_p) + H_{min}(\mathcal{I}). &(2.58)\end{aligned}$$

W przypadku kanału Φ^p, kanał depolaryzujący Λ_p działa na przestrzeni $\mathbb{C}^4$, zatem $H_{min}(\Lambda_p) = H(1-\frac{3p}{4},\frac{p}{4},\frac{p}{4},\frac{p}{4})$. Ponieważ stany w postaci $U|i\rangle|v\rangle$ dla $|i\rangle\in\{|0\rangle,\ldots,|3\rangle\}$ są produktowe, łatwo sprawdzić, że osiągają one powyższe oszacowanie, co oznacza, że $H_{min}(\Phi^p) = H(1-\frac{3p}{4},\frac{p}{4},\frac{p}{4},\frac{p}{4})$.

□

Wracając do szacowania R_1, niech nadawca S_1 przesyła z równym prawdopodobieństwem stan z bazy standardowej, natomiast nadawca S_2 stan $|0\rangle$. Średni stan transmitowany przez S_1 ma postać $\rho = \frac{1}{4}\mathrm{I}$ i na mocy Lem. 2.2 maksymalizuje on $S\left(\Phi^p(\rho \otimes v)\right)$. Stany w postaci $|i\rangle|0\rangle$ spełniają założenia lematu 2.3, stąd minimalizują entropię wyjścia kanału Φ^p. Łącząc oba fakty, przedstawiony protokół pozwala osiągnąć ograniczenie (2.36). Osiągana prędkość transmisji wynosi:

$$R_1^{(1)} = H\left(\frac{2-p}{8}, \frac{2-p}{8}, \frac{2-p}{8}, \frac{2-p}{8}, \frac{p}{8}, \frac{p}{8}, \frac{p}{8}, \frac{p}{8}\right) - H\left(1 - \frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4}\right). \tag{2.59}$$

Zajmiemy się teraz scenariuszem, w którym przesyłane są stany splątane. Analizować będziemy prędkość transmisji nadawcy S_1 w układzie $\Phi^p \otimes \Phi^p$ dla następującego protokołu: mieszanina stanów wejściowych nadawcy S_1 ma postać $\{\frac{1}{16}, e_i \otimes e_j\}$, nadawca S_2 przesyła zawsze stan $|\Psi^+\rangle$. Na podstawie ograniczenia Holevo otrzymujemy:

$$\begin{aligned} R_1^{(2)} = &- \left(\frac{3}{8}(2-p)p \log\left[\frac{1}{64}(2-p)p\right] + \frac{1}{8}(4-6p+3p^2)\log\left[\frac{1}{64}(4-6p+3p^2)\right]\right) \\ &- H\left(1-\frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4}\right). \end{aligned} \tag{2.60}$$

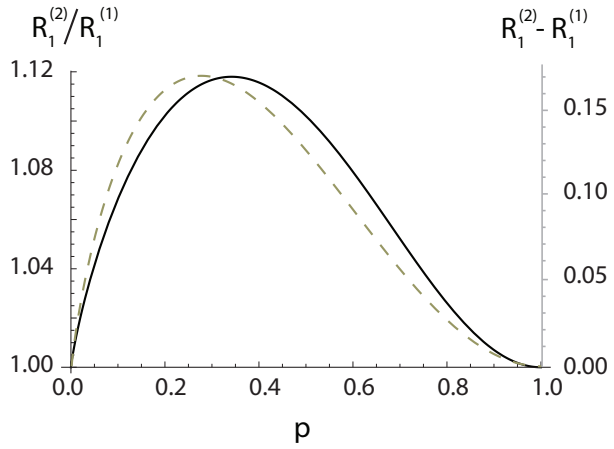
Wartość ta nie musi być maksymalną wartością prędkości transmisji. Stan Ψ^+ został wybrany arbitralnie z pominięciem procedury optymalizacji po mieszaninach stanów wejściowych.

Zwróćmy uwagę, że dla kodów produktowych i kodów wykorzystujących splątanie kanał produkuje taką samą ilość entropii $H\left(1 - \frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4}\right)$. Zysk prędkości, podobnie jak w części 2.3.1, zawdzięczamy procedurze gęstego kodowania, która prowadzi do wzrostu zróżnicowania stanów wyjściowych. Różnica pojemności $R_{S_1}^{(2)} - R_{S_1}^{(1)}$ oraz iloraz $R_{S_1}^{(2)}/R_{S_1}^{(1)}$ przedstawione zostały na Rys. 2.9. Kształt krzywych na rysunku można interpretować w następujący sposób:

- Dla $p = 0$ żaden z egzemplarzy kanału Φ^p nie wprowadza szumu. Gęste kodowanie nie odgrywa tutaj żadnej roli, gdyż odbiorca ma bezpośredni dostęp, poprzez górną linię kanału, do stanu transmitowanego przez S_1.

- Gdy $p = 1$, komunikat niesie jedynie dolna linia kanału Φ^p. W przypadku gęstego kodowania oba kanały konkurują o współdzielony stan splątany, przez co transmitowane przez nie komunikaty nawzajem się zakłócają.

- W przedziale $0 < p < 1$, z niezerowym prawdopodobieństwem $2p(1-p)$ ma miejsce sytuacja, gdy tylko jeden z kanałów składowych wprowadza szum. Ustalmy, że jest to kanał pierwszy. Odbiorca, dzięki górnej linii drugiego kanału, zna dokładną postać stanu transmitowanego tym kanałem. Dzięki tej wiedzy oraz w oparciu o stan splątany, może odczytać komunikat wysłany przez kanał pierwszy. Właśnie ta sytuacja ma wpływ na wzrost prędkości transmisji nadawcy S_1.



Rysunek 2.9: Iloraz (linia ciągła, lewa oś Y) oraz różnica (linia przerywana, prawa oś Y) prędkości transmisji przez kanał Φ^p dla nadawcy S_1 w przypadku użycia produktowych słów kodowych $R_1^{(1)}$ oraz stanów Bella $R_1^{(2)}$. Wielkości są pokazane w funkcji poziomu szumu p.

2.3.3 Poza klasycznym schematem gęstego kodowania: wpływ splątania wielocząstkowego

Zajmiemy się teraz przykładem kanału $\Phi_{n,n'}$, którego regularyzowany obszar pojemności $\mathcal{R}^{(\infty)}(\Phi_{n,n'})$ nie może zostać osiągnięty przy użyciu splątania 2-

cząstkowego[7]. Przedstawiona poniżej analiza pokazuje, że w ogólnej sytuacji zadanie wyznaczenia obszaru $\mathcal{R}^{(\infty)}$ wymaga optymalizacji z wykorzystaniem wielocząstkowych stanów splątanych.

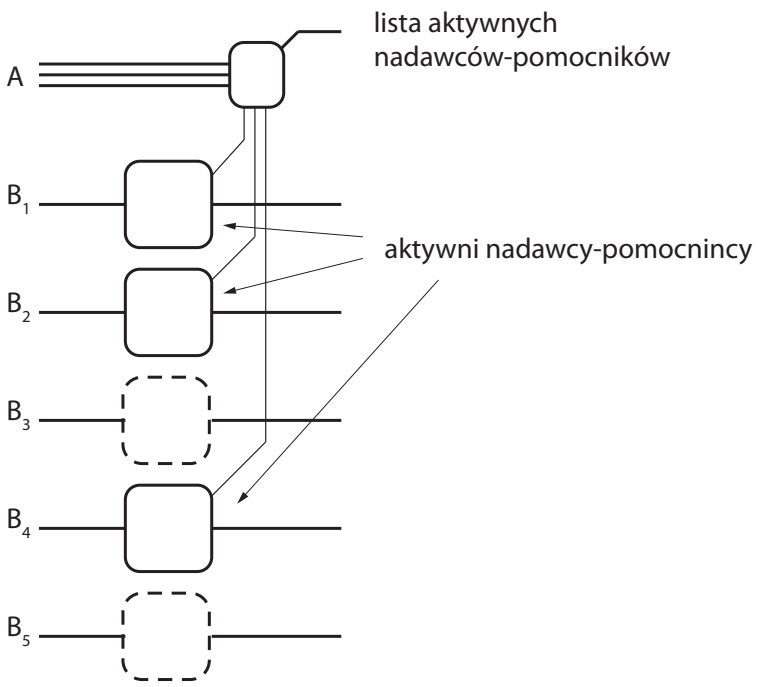
Kanał $\Phi_{n,n'}$, o którym będzie dalej mowa posiada wyróżnionego nadawcę A oraz n nadawców-pomocników B_i. Wejście nadawcy A składa się z n' klasycznych linii 2-bitowych [8], nadawcy B_i mogą przesyłać po jednym qbicie. Podczas każdego użycia kanału losowana jest n' elementowa wariacja bez powtórzeń w, ze zbioru nadawców pomocników. Wylosowani nadawcy stają się aktywnymi nadawcami-pomocnikami. Następnie do każdej linii wejściowej i nadawcy A przypisywany jest aktywny nadawca-pomocnik B_{w_i}. Oznacza to, że w zależności od stanu linii i nadawcy A, stan pochodzący od nadawcy B_{w_i} jest modyfikowany przez jedną z operacji unitarnych $\{\mathrm{I}, \sigma_x, \sigma_y, \sigma_z\}$. Wszystkie wariacje losowane są z równym prawdopodobieństwem. W przypadku gdy nadawca B_i nie jest aktywny, wykonywana jest operacja I, tzn. stan od tego nadawcy pozostaje bez zmian. Odbiorca ma dostęp do linii pochodzących od nadawców B_i oraz etykiety $|w\rangle$, mówiącej o wylosowanej wariacji. Na Rys. 2.10 przedstawiono schemat kanału $\Phi_{n,n'}$ dla $n' = 3, n = 5$. Odnosi się on do konfiguracji, w której linie $1, 2$ i 3 zostały przypisane odpowiednio do nadawców B_1, B_2, B_4. Etykieta opisująca taką konfigurację ma postać wektora $w = (1, 2, 4)$.

Dalsza analiza dotyczy scenariuszy, w których komunikacja odbywa się poprzez m kopi kanału $\Phi_{n,n'=1}$. Kanał $\Phi_{n,n'=1}$, który dla zwięzłości oznaczać będziemy przez Φ, posiada tylko jedną linię wejściową. Prawdopodobieństwo, że nadawca B_i zostanie przypisany do tej linii w danym przypadku użycia kanału wynosi $p = 1/n$. Φ_w oznaczać będzie kanał, w którym aktywny jest nadawca B_w. Analogicznie $\Phi_{\tilde{w}}^{\otimes m} = \Phi_{w_1} \otimes \ldots \otimes \Phi_{w_m}$, gdzie $|\tilde{w}\rangle = |w_1, \ldots, w_m\rangle = |w_1\rangle \otimes \ldots \otimes |w_m\rangle$. Prawdopodobieństwo aktywacji dowolnego z pomocników jest takie samo co znaczy, że $p_{\tilde{w}} = p^m$. Zwróćmy uwagę, że produkcja entropii w kanale $\Phi_{n,n'=1}$ pod warunkiem w wynosi 0, tj. znając etykietę w oraz stan czysty na wejściu kanału można dokładnie określić stan czysty na wyjściu kanału. Stąd otrzymujemy:

$$\forall_{|e\rangle \in \mathcal{H}_A^{\otimes m}, |\phi_i\rangle \in \mathcal{H}_{B_i}^{\otimes m}} S\big(\Phi_{\tilde{w}}^{\otimes m}(e \otimes \phi_1 \otimes \ldots \otimes \phi_n)\big) = 0. \tag{2.61}$$

[7]Porównaj z częścią 2.3.1, gdzie splątanie dwucząstkowe wystarczało, aby otrzymać regularyzowany obszar pojemności.

[8]Równoważnie można powiedzieć, że są to linie 2-qbitowe na których wykonywany jest pomiar w bazie standardowej.



Rysunek 2.10: Schemat kanału $\Phi_{n,n'}$ dla $n = 5$ nadawców pomocników B_i i $n' = 3$ linii należących do nadawcy A.

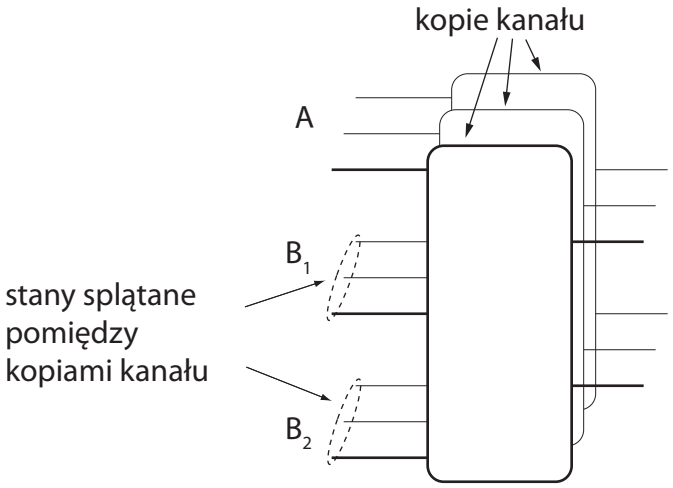
Ponownie interesować nas będzie tylko prędkość transmisji $R_A^{(m)}(\Phi_{n,n'=1})$ dla nadawcy A. Nadawcy B_i wspierają nadawcę A przesyłając zawsze jeden i ten sam ustalony m-cząstkowy stan splątany. Ich prędkość transmisji wynosi 0. Rys. 2.11 pokazuje którymi liniami, w opisanej konfiguracji, przesyłane są stany splątane.

Lemat 2.4 *Niech kanał kwantowy* $\Psi(\rho) = \sum_w p_w \Psi_w(\rho) \otimes |w\rangle\langle w|$ *działa z prawdopodobieństwem* p_w *jak kanał* Ψ_w*, przy czym odbiorca otrzymuje etykietę* $|w\rangle$ *z informacją, z którym kanałem ma aktualnie do czynienia. Pojemność Holevo kanału* Ψ *jest ograniczona przez:*

$$\chi(\Psi) \leq \sum_w p_w \chi(\Psi_w) \tag{2.62}$$

Równość zachodzi w przypadku, gdy ta sama mieszanina stanów jest optymalna dla wszystkich Ψ_w*.*

Dowód:



Rysunek 2.11: Równoległe połączenie $m = 3$ kopi kanału $\Phi_{n=2,n'=1}$. Kreskowane elipsy wskazują linie współdzielące stan splątany.

Dowód lematu sprowadza się do prostych rachunków:

$$\begin{aligned}
\chi(\Psi) &= \max_{\{p_x,\rho_x\}} S\left(\Psi\left(\sum p_x\rho_x\right)\right) - \sum_x p_x S\left(\Psi\left(\rho_x\right)\right) && (2.63)\\
&= \max_{\{p_x,\rho_x\}} S\left(\sum_w p_w \Psi_w\left(\sum p_x\rho_x\right)|w\rangle\langle w|\right) && (2.64)\\
&\quad - \sum_x p_x S\left(\sum_w p_w \Psi_w\left(\rho_x\right)|w\rangle\langle w|\right)\\
&= \max_{\{p_x,\rho_x\}} \sum_w p_w \left\{ S\left(\Psi_w\left(\sum p_x\rho_x\right)\right) + H(\{p_w\}) \right. && (2.65)\\
&\quad \left. - \sum_x p_x S\left(\Psi_w\left(\rho_x\right)\right) - H(\{p_w\}) \right\}\\
&\leq \sum_w p_w \max_{\{p_x,\rho_x\}} S\left(\Psi_w\left(\sum p_x\rho_x\right)\right) - \sum_x p_x S\left(\Psi_w\left(\rho_x\right)\right) && (2.66)\\
&= \sum_w p_w \chi(\Psi_w), && (2.67)
\end{aligned}$$

gdzie w kroku (2.65) korzystamy z ortogonalności etykiet $|w\rangle$. Zwróćmy jesz-

cze uwagę, że dla ustalonej mieszaniny stanów wejściowych $\{p_i, \rho_i\}$ mamy:

$$\chi_{\{p_i,\rho_i\}}(\Psi) = \sum_w p_w \chi_{\{p_i,\rho_i\}}(\Psi_w) \tag{2.68}$$

□

Lemat 2.5 *Pojemność Holevo χ dla kanałów kwantowych* 1*-do-*1 *z wejściem klasycznym jest addytywna.*

Dowód:

W przypadku kanałów kwantowych z wejściem klasycznym, zbiór stanów wejściowych jest ustalony, optymalizacji podlega jedynie rozkład prawdopodobieństwa transmisji poszczególnych stanów wejściowych. Niech e_{x_1} i e_{x_2} oznaczają etykiety klasyczne wysyłane odpowiednio przez kanały Γ_1 oraz Γ_2 natomiast p_{x_1,x_2} oznacza łączne prawdopodobieństwo transmisji pary $\{e_{x_1}, e_{x_2}\}$, które osiąga $\chi(\Gamma_1 \otimes \Gamma_2)$, t.j.:

$$\begin{aligned} \chi(\Gamma_1 \otimes \Gamma_2) &= \chi_{\{p_{x_1,x_2}, e_{x_1}\otimes e_{x_2}\}}(\Gamma_1 \otimes \Gamma_2) && (2.69)\\ &= S(\Gamma_1 \otimes \Gamma_2(\rho)) - \sum_{x_1,x_2} p_{x_1,x_2} S(\Gamma_1 \otimes \Gamma_2(e_{x_1} \otimes e_{x_2})). && (2.70) \end{aligned}$$

Zauważmy, że:

$$\begin{aligned} S\left(\Gamma_1 \otimes \Gamma_2(e_{x_1} \otimes e_{x_2})\right) &= S\left(\Gamma_1(e_{x_1}) \otimes \Gamma_2(e_{x_2})\right) && (2.71)\\ &= S\left(\Gamma_1(e_{x_1})\right) + S\left(\Gamma_2(e_{x_2})\right), && (2.72) \end{aligned}$$

jak również:

$$S(\Gamma_1 \otimes \Gamma_2(\bar{\rho})) \leq S(\Gamma_1(\bar{\rho}_1)) + S(\Gamma_2(\bar{\rho}_2)), \tag{2.73}$$

gdzie $\bar{\rho}$, $\bar{\rho_1}$, $\bar{\rho_2}$ to odpowiednie średnie stany wejścia. Wstawiając powyższe obserwacje do wzoru (2.70) otrzymujemy:

$$\begin{aligned} \chi(\Gamma_1 \otimes \Gamma_2) &\leq S(\Gamma_1(\bar{\rho_1})) + S(\Gamma_2(\bar{\rho_2})) && (2.74)\\ &\quad - \sum_{x_1,x_2} p_{x_1,x_2}(S(\Gamma_1(e_{x_1})) + S(\Gamma_2(e_{x_2}))) \\ &= S(\Gamma_1(\bar{\rho}_1)) - \sum_{x_1} p_{x_1} S(\Gamma_1(e_{x_1})) + && (2.75)\\ &\quad S(\Gamma_2(\bar{\rho}_2)) - \sum_{x_2} p_{x_2} S(\Gamma_2(e_{x_2})) \\ &\leq \chi(\Gamma_1) + \chi(\Gamma_2). && (2.76) \end{aligned}$$

Relacja $\chi(\Gamma_1 \otimes \Gamma_2) \geq \chi(\Gamma_1) + \chi(\Gamma_2)$ także zachodzi, co łatwo sprawdzić biorąc $p_{x_1,x_2} = p_{x_1} p_{x_2}$, gdzie rozkłady p_{x_1}, p_{x_2} osiągają odpowiednio $\chi(\Gamma_1)$ oraz $\chi(\Gamma_2)$.

□

Twierdzenie 2.2 *Górne ograniczenie dla prędkości transmisji $R_A^{(m)}(\Phi_{n,n'=1})$ nadawcy A ma postać:*

$$R_A^{(m)}(\Phi_{n,n'=1}) \leq \frac{n}{m} \sum_{i=0}^{m} p^i (1-p)^{m-i} \binom{m}{i} \min(2i, m), \tag{2.77}$$

gdzie n jest liczbą nadawców-pomocników, m jest liczbą kopii kanału $\Phi_{n,n'=1}$, $p = 1/n$. Liczba m określa również, ilu cząstkowe stany splątane przesyłane są przez każdego z nadawców.

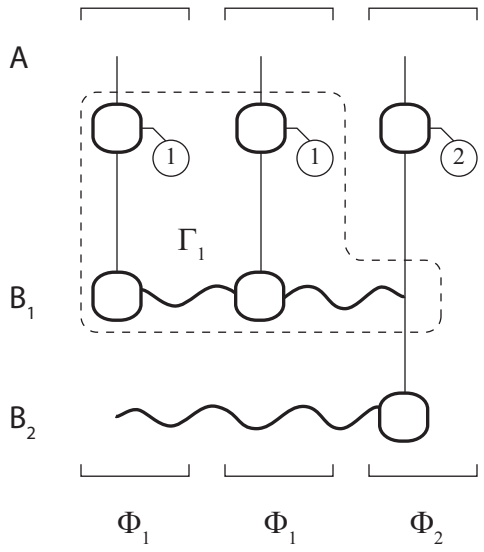
Dowód:

Plan dowodu przedstawia się następująco. Najpierw znajdziemy ograniczenie górne na prędkość transmisji $R_A(\Phi_{\tilde{w}}^{\otimes m})$ dla ustalonego $\tilde{w}$. Okaże się, że wartość ta zależy jedynie od tego, ile razy nadawca B_i stał się nadawcą aktywnym. Liczbę aktywacji l_i danego nadawcy łatwo określić znając etykietę $\tilde{w}$. Na podstawie ograniczenia dla $R_A(\Phi_{\tilde{w}}^{\otimes m})$ podamy ograniczenie górne na $R_A^{(m)}(\Phi_{n,n'=1}) = \frac{1}{m} R_A(\Phi_{n,n'=1})$.

Aby wyznaczyć $R(\Phi_w^{\otimes m})$, zrobimy mały formalny wybieg. Otóż zamiast rozważać m kopii kanału Φ, będziemy przez chwilę zajmować się n kanałami Γ_i, przy czym zachodzi równoważność:

$$\Phi_w^{\otimes m} \equiv \bigotimes_{i=1}^{n} \Gamma_i \tag{2.78}$$

w sensie odwzorowania stanów wejściowych na stan wyjściowy. Wejście kanału Γ_i składa się ze wszystkich wejść kontrolowanych przez nadawcę B_i oraz tych wejść należących do A, które mają wpływ na podsystem od nadawcy B_i. Ponieważ stan przesyłany przez B_i jest ustalony, na kanał Γ_i można patrzeć jak na kanał 1-do-1 z wejściem klasycznym. Wejście to jest kontrolowane przez nadawcę A. Wejście kanału ma rozmiar $2l_i$ bitów. Wyjście kanału Γ_i ma rozmiar m qbitów. Kanały Γ_i, Γ_j różniące się indeksem ($i \neq j$) nie dzielą



Rysunek 2.12: Równoważność $\Phi_w^{\otimes m} \equiv \bigotimes_{i=1}^{n} \Gamma_i$ na przykładzie kanałów $\Phi_{1,1,2}^{\otimes 3}$ i $\Gamma_1 \otimes \Gamma_2$. Pionowe bloki na rysunku oznaczają kolejne kopie kanału Φ, linią przerywaną zaznaczono kanał Γ_1, pogrubiona linia falowana oznacza stany splątane przesyłane przez nadawców B_1 i B_2, w kółku przedstawiono etykietę klasyczną odpowiadającą danej realizacji kanału Φ.

linii wejściowych. Wprowadzenie kanałów $\{\Gamma_i\}$ to jedynie odpowiednie przegrupowanie linii wejściowych i wyjściowych. Stąd wynika równoważność obu przedstawień. Rys. 2.12 ilustruje opisany tutaj zabieg.

Wymiary przestrzeni wejścia i wyjścia kanału Γ_i stanowią górne ograniczenia na jego pojemność klasyczną:

$$\chi\left(\Gamma_i\right) \leq \min(2l_i, m). \tag{2.79}$$

Na podstawie Lem. 2.5 otrzymujemy

$$\chi\left(\bigotimes_{i=1}^{n} \Gamma_i\right) = \sum_{i=1}^{n} \chi(\Gamma_i). \tag{2.80}$$

Podstawiając oszacowanie (2.79) do równania (2.80) oraz korzystając z równoważności kanałów (2.78) otrzymujemy:

$$R_A\left(\Phi_w^{\otimes m}\right) \leq \left(\sum_{i=1}^{n} \min(2l_i, m)\right). \tag{2.81}$$

Skorzystamy teraz z Lem. 2.4. Podstawienia $\Psi_w = \Phi_w^{\otimes m}$, $p_w = p^m$, $\chi(\Psi_w) = R\,(\Phi_w^{\otimes m})$ wraz z ograniczeniem (2.81) prowadzą do:

$$\begin{aligned} R_A(\Phi^{\otimes m}) \;&\leq\; p^m \sum_w \big(\min(2l_1(w), m) + \ldots + \min(2l_n(w), m)\big) && (2.82)\\ &= \sum_{l_1+\ldots+l_n=m} \frac{m!}{l_1!\cdot\ldots\cdot l_n!} p^m \big(\min(2l_1, m)+\ldots+\min(2l_n, m)\big) && (2.83)\\ &= n \sum_{l=0}^{m} \binom{m}{l} p^m \min(2l, m)\alpha_l && (2.84) \end{aligned}$$

Etykiety w, które prowadzą do takiej samej konfiguracji $\{l_1, \ldots, l_n\}$, zostały zebrane we wzorze (2.83) w jeden wyraz. Przechodząc do (2.84) korzystamy z symetrii względem nadawców B_i oraz podstawienia $\alpha_l = \sum_{l_2+\ldots+l_n=m-l} \binom{m-l}{l_2,\ldots,l_n}$. Przypomnijmy, że

$$\sum_{k_1+\ldots+k_n\leq m} \binom{m}{k_1, \ldots, k_n} = n^m, \tag{2.85}$$

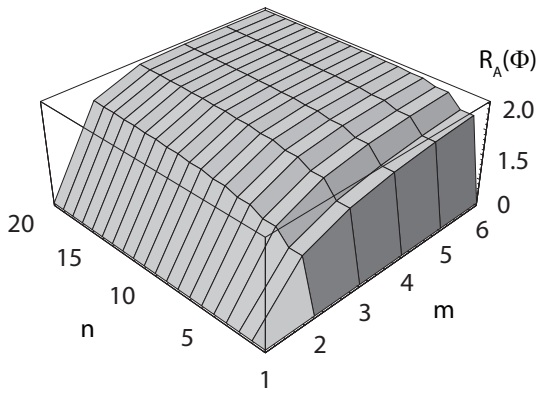
co prowadzi do $\alpha_l = (n-1)^{m-l}$ oraz:

$$\begin{aligned} R_A(\Phi^{\otimes m}) \;&\leq\; n \sum_{l=0}^{m} \binom{m}{l} \min(2l, m) p^m (n-1)^{m-l} && (2.86)\\ &=\; n \sum_{l=0}^{m} p^l (1-p)^{m-l} \binom{m}{l} \min(2l, m), && (2.87) \end{aligned}$$

gdzie w równaniu (2.86) korzystamy z faktu, że dla $p = 1/n$ otrzymujemy $(n-1)p = (n-1)/n = 1-p$. Podstawienie $R_A^{(m)}(\Phi) = \frac{1}{m} R_A(\Phi^{\otimes m})$ kończy dowód.

□

Ograniczenie górne na $R_A^{(m)}(\Phi_{n,n'=1})$ przedstawione w Tw. 2.2 jest osiągane dla $m \in \{1, 2, 5\}$ przez następujące protokoły: nadawca A przesyła z równym prawdopodobieństwem wszystkie elementy z kontrolowanej przez niego $2m$ bitowej przestrzeni wejścia $\Phi^{\otimes m}$, podczas gdy nadawcy B_i przesy-



Rysunek 2.13: Górne ograniczenie na prędkość transmisji $R_A^{(m)}(\Phi)$ w funkcji m-liczby kopii kanału Φ, oraz liczby nadawców-pomocników n.

łają za każdym razem odpowiednio:

$$m = 1 \quad : \quad |0\rangle \tag{2.88}$$

$$m = 2 \quad : \quad |\phi^+\rangle \tag{2.89}$$

$$\begin{aligned} m = 5 \quad : \quad |0_L\rangle = \frac{1}{4}\big[&|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle \\ &+|01010\rangle - |11011\rangle - |00110\rangle - |11000\rangle \\ &-|11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle \\ &-|10001\rangle - |01100\rangle - |10111\rangle + |00101\rangle\big], \end{aligned} \tag{2.90}$$

gdzie $|0_L\rangle$ to słowo kodowe z 5-qbitowego kodu korekcyjnego [72].

Aby dowieść, że omawiane tu ograniczenie jest faktycznie osiągane w przedstawionych scenariuszach wystarczy pokazać, że każdy z nich prowadzi do równości w formule (2.79). Produkcja entropia przez kanał Γ_i wynosi 0 co znaczy, że jego przepustowość zależy tylko od entropii średniego stanu wyjścia. Należy zatem sprawdzić, czy rzeczywiście wynosi ona $\min(2l_i, 2)$. Dla $m = 1$ sprawa jest oczywista. Uzasadnienie dla $m = 2$ znajduje się poniżej:

1. $l = 0$: transmitowany stan Bella pozostaje bez zmian, entropia stanu czystego wynosi 0.

2. $l = 1$: operacje unitarne należące do zbioru $\{\mathrm{I}, \sigma_x, \sigma_y, \sigma_z\}$, wykonane na dowolnym qbicie stanu Bella, pozwalają otrzymać wszystkie 4 stany

Bella. Ponieważ prawdopodobieństwo wykonania każdej z operacji unitarnych jest takie samo, entropia średniego stanu wynosi 2.

3. $l = 2$: sytuacja ta sprowadza się do rekurencyjnego zastosowania argumentu użytego dla $l = 1$, ostatecznie stan średni składa się w równych proporcjach ze wszystkich stanów Bella a jego entropia znowu wynosi 2.

Podobne rozumowanie można przeprowadzić dla stanu $|0_L\rangle$ z 5 qbitowego kodu korekcyjnego ($m = 5$). Rozpatrzmy sytuację, w której kanał Γ_i działa na stan $|0_L\rangle$, na pozycjach opisanych przez wektor π (wektor ma l elementów). Niech $\Lambda^{(j)}_{p=1}(\rho)$ oznacza kanał depolaryzujący działający na j-ty qbit stanu ρ. Kanał $\Lambda^{(j)}_{p=1}(\rho)$ wprowadza szum z prawdopodobieństwem $p = 1$. Ponieważ nadawca A z równym prawdopodobieństwem przesyła wszystkie stany wejściowe, średni stan na wyjściu Γ_i dla danego π ma postać:

$$\rho_\pi = \left(\bigotimes_{i=1}^{l} \Lambda^{(\pi_i)}_{p=1} \right) \left[|0_L\rangle\langle 0_L| \right], \tag{2.91}$$

gdzie π_i oznacza wartość i tego elementu wektora π. Aby pokazać, że dla każdego l w formule (2.79) zachodzi równość, musimy sprawdzić, czy dla wszystkich π zachodzi $S(\rho_\pi) = \min(2l, 5)$. Zadanie to wymaga rozpatrzenia wielu przypadków, dlatego do jego wykonania został użyty program komputerowy napisany dla systemu obliczeniowego Mathematica. Kod programu zamieszczony został w dodatku A. Dla każdego $l \in \{1, \ldots, 5\}$ program generuje listę wszystkich l elementowych kombinacji ze zbioru $\{1, \ldots, 5\}$. Każda z tych kombinacji to inny wektor pozycji π. Następnie program sprawdza, czy dla wszystkich π zachodzi warunek $S(\rho_\pi) = \min(2l, 5)$.

Na podstawie przedstawionych argumentów łatwo wyciągnąć wniosek, że dla dowolnego w przedstawione kodowanie wysyca formułę (2.81). Ponieważ protokół jest optymalny dla wszystkich możliwych w, w Lem. 2.4 zachodzi równość, która przekłada się na równość w wyrażeniu (2.82). To pokazuje, że opisany protokoły osiągają prędkość transmisji:

$$R^{(m)}_A(\Phi_{n,n'=1}) = \frac{n}{m} \sum_{i=0}^{m} p^i (1-p)^{m-i} \binom{m}{i} \min(2i, m). \tag{2.92}$$

Pokazany tutaj efekt superaddytywności bazuje na pewnym rozszerzeniu schematu gęstego kodowania na przypadek n-cząstkowy. Cechą wyróżniającą

analizowany przypadek jest to, że w przeciwieństwie do klasycznego schematu gęstego kodowania, nie mamy tutaj do czynienia z wyodrębnioną częścią stanu splątanego, na którą działa operacja unitarna. Z definicji kanału, operacje unitarne wykonywane są na losowych fragmentach stanu splątanego. Niezależnie od tego, gdzie zostanie wykonana operacja unitarna, oczekujemy że za każdym razem stan będzie transformowany w równie duży zbiór stanów ortogonalnych. Taką własność posiadają stany kodowe z 5 qbitowego kodu korekcyjnego: liczba stanów, które można osiągnąć poprzez unitarną transformację wybranego stanu kodowego, zależy tylko od liczby qbitów, których ta transformacja dotyczy, nie zależy natomiast od ich położenia. Użyteczność stanu splątanego do optymalizacji prędkości transmisji pociąga za sobą wymaganie aby stan wykazywał odpowiednio dużą symetrię względem zamiany miejscami jego części składowych.

Schemat gęstego kodowania nie może przekroczyć ograniczenia m bitów entropii na m-qbitowy stan splątany od nadawcy B_i. Zatem im bliżej l_i do m, tym mniejszy wzrost entropii stanu wyjściowego i tym mniejszy wzrost prędkości transmisji. W przypadku, gdy liczba nadawców-pomocników $n = 1$ lub m jest małe, stan splątany dość często niesie mniej niż $2l_i$ bitów informacji. Jednak gdy $n > 1$ z pomocą przychodzi asymptotyczna zasada ekwipartycji mówiąca, że wraz ze wzrostem m wartości l_i koncentrują się w okolicach m/n. Gdy m i n rosną zachowując odpowiednią proporcję, szansa że stan splątany od nadawcy B_i niesie mniej niż $2l_i$ bitów informacji maleje.

2.3.4 Kanały z wieloma nadawcami: superaddytywność regularyzowanego obszaru pojemności

Zebrane w tej części wyniki dotyczą efektu aktywacji dla regularyzowanych obszarów pojemności $\mathcal{R}^{(\infty)}(\Phi_I) + \mathcal{R}^{(\infty)}(\Phi_{II}) \subsetneq \mathcal{R}^{(\infty)}(\Phi_I \otimes \Phi_{II})$. Należy tutaj podkreślić, że w analizowanym przypadku obszarów $\mathcal{R}^{(\infty)}$ nie można przedstawić przy użyciu formuł jednowyrazowych, tj. $\mathcal{R}^{(1)}(\Phi_i) \subsetneq \mathcal{R}^{(\infty)}(\Phi_i)$ dla $i \in \{I, II\}$. Dalej posługiwać się będziemy kanałami $\Phi_I = \Phi_{n=10,n'=9}$ i $\Phi_{II} = \Phi_{n=10,n'=1}$, których struktura została opisana w części 2.3.3.

Zaczniemy od sprawdzenia, czy dla kanałów Φ_I i Φ_{II}, obszary pojemności faktycznie spełniają $\mathcal{R}^{(1)} \subsetneq \mathcal{R}^{(\infty)}$, tzn. czy aby na pewno omawiany tu przypadek nie daje się sprowadzić do sytuacji opisanej w części 2.3.1. Tym razem również wystarczy, gdy ograniczymy się do prędkość transmisji dla nadawcy A (nadawcy B_i pełnią rolę pomocników).

Biorąc pod uwagę wymiar łącznej przestrzeni wyjścia nadawców B_i aktywnych w danym momencie, łatwo zauważyć, że maksymalna prędkość osiągana podczas transmisji stanów produktowych wynosi $R_A^{(1)} = n'$.

Przyjrzymy się teraz prędkości transmisji $R_A^{(2)}$ w układach $\Phi_I^{\otimes 2}$ oraz $\Phi_{II}^{\otimes 2}$, gdy nadawcy B_i przesyłają jeden i ten sam stan Bella. W takiej sytuacji na układy $\Phi_I^{\otimes 2}$ oraz $\Phi_{II}^{\otimes 2}$ możemy patrzeć formalnie jak na kanały 1-do-1. Entropia wyjścia w obu układach, przy znajomości etykiety wyjściowej w, wynosi 0 (patrz formuła (2.68)). Zatem prędkość transmisji jest równa entropii średniego stanu na wyjściu pod warunkiem w, tj. entropii średniego stanu linii pochodzących od nadawców B_i. Podobnie jak robiliśmy to wcześniej przyjmujemy, że nadawca A przesyła z równym prawdopodobieństwem wszystkie elementy bazy standardowej kontrolowanej przez siebie przestrzeni wejścia. Prawdopodobieństwo, że podczas kolejnych transmisji dany zbiór aktywnych nadawców B_i zostanie wybrany dwukrotnie, wynosi $p = 1/\binom{n}{n'}$. Z prawdopodobieństwem $1-p$ zbiory aktywnych nadawców różnią się w obu przypadkach transmisji o co najmniej dwa elementy. Nadawca A czerpie w takiej sytuacji korzyść z gęstego kodowania i może przesyłać co najmniej 2 dodatkowe bity informacji. Ponownie biorąc pod uwagę wymiar łącznej przestrzeni wyjścia aktywnych w danym momencie nadawców B_i oraz schemat gęstego kodowania otrzymujemy, że z prawdopodobieństwem p nadawca A przesyła z prędkością $2n'$ natomiast z prawdopodobieństwem $1-p$ nadaje z prędkością co najmniej $2(n'-1)+2\cdot 2$. Na podstawie wzoru 2.68 otrzymujemy następujące ograniczenie na prędkość transmisji w rozważanym protokole: $R_A \geq p2n' + (1-p)\big(2(n'-1)+2\cdot 2\big)$. Zatem, dla maksymalnych regularyzowanych prędkości transmisji zachodzi:

$$R_A^{(1)} = n' < n' + (1-p) \leq \frac{1}{2} R_A \leq R_A^{(2)} \leq R_A^{(\infty)}, \tag{2.93}$$

co przekłada się na $\mathcal{R}^{(1)} \subsetneq \mathcal{R}^{(\infty)}$.

Pokażemy teraz, że $\mathcal{R}^{(\infty)}(\Phi_I) + \mathcal{R}^{(\infty)}(\Phi_{II}) \subsetneq \mathcal{R}^{(\infty)}(\Phi_I \otimes \Phi_{II})$. W tym celu udowodnimy relację $R_A^{(\infty)}(\Phi_I) + R_A^{(\infty)}(\Phi_{II}) < R_A^{(\infty)}(\Phi_I \otimes \Phi_{II})$.

Zaczniemy od oszacowania z góry wartości $R_A^{(\infty)}(\Phi_I) + R_A^{(\infty)}(\Phi_{II})$. Przypomnijmy, że prędkość transmisji przez kanał jest ograniczona z góry przez logarytm rozmiaru przestrzeni wejścia i przestrzeni wyjścia kanału. Stąd, dla nadawcy A i kanału $\Phi_{n,n'}$, mamy:

$$R_A^{(m)} \leq \frac{1}{m} \min(2n'm, nm) = \min(2n', m). \tag{2.94}$$

Stosując powyższy wzór do kanałów Φ_I oraz Φ_{II} otrzymujemy $R_A^{(\infty)}(\Phi_I) \leq \min(2 \cdot 9, 10) = 10$ oraz $R_A^{(\infty)}(\Phi_{II}) \leq \min(2 \cdot 1, 10) = 2$, co prowadzi do $R_A^{(\infty)}(\Phi_I) + R_A^{(\infty)}(\Phi_{II}) \leq 12$.

Do wyznaczenia ograniczenia dolnego dla $R_A^{(\infty)}(\Phi_I \otimes \Phi_{II})$ użyjemy następujący protokół: niech nadawca A używa tylko linii należących do kanału Φ_I, tzn. przez linie należące do kanału Φ_I przesyła z równym prawdopodobieństwem wektory z bazy standardowej, natomiast przez linię należącą do kanału Φ_{II} zawsze stan $|0\rangle$. Nadawcy B_i przesyłają zawsze jeden i ten sam stan Bella. Pierwsza część stanu idzie linią należącą do kanału Φ_I natomiast druga linią należącą do kanału Φ_{II}. Łatwo zauważyć, że niezależnie od tego którzy nadawcy są aktywni, każda z linii kanału Φ_I nadawcy A modyfikuje stan innego podukładu. Stąd, na podstawie schematu gęstego kodowania, prędkość transmisji uzyskana przez A związana jest z wymiarem kontrolowanej przez niego przestrzeni wejścia kanały Φ_I (przypomnijmy, że kanał Φ_{II} jest pasywny) i wynosi 18. Otrzymujemy zatem:

$$R_A^{(\infty)}(\Phi_I) + R_A^{(\infty)}(\Phi_{II}) \leq 12 < 18 \leq R_A^{(\infty)}(\Phi_I \otimes \Phi_{II}). \tag{2.95}$$

W ten sposób wykazaliśmy efekt superaddytywności dla regularyzowanych obszarów pojemności.

Wartość pojemność Holevo jest silnie związana ze zbiorem stanów, na którym prowadzona jest procedura optymalizacji mieszaniny stanów kodowych. Występowanie efektu superaddytywności dla wielkości asymptotycznych $\mathcal{R}^{(\infty)}$ sugeruje, że kwantowy efekt aktywacji jest cechą wielodostępnych kanałów kwantowych a nie jedynie odbiciem własności pojemności Holevo wynikających z rozszerzenia zbioru dopuszczalnych stanów kodowych.

2.3.5 ϵ - superaktywacja: $\epsilon \otimes \epsilon \gg \epsilon$.

W przedstawionych dotychczas przykładach, efekt superaddytywności związany był zasadniczo ze schematem gęstego kodowania. Wykorzystanie stanów splątanych prowadziło do takiej samej produkcji entropii, jak w przypadku transmisji stanów produktowych. W żadnym z przedstawionych wyników nie udało się zaobserwować wzrostu łącznej prędkości transmisji R_T. Ostatni rezultat, który zostanie przedstawiony czytelnikowi w tym rozdziale, dotyczy subaddytywności minimalnej entropii wyjścia H_{min} i ma wypełnić opisaną wyżej lukę. Czytelnik zobaczy tutaj między innymi, jak splątanie pozwala zmniejszyć produkcję entropii, czego bezpośrednią konsekwencją będzie

wzrost R_T. W opisanym protokole wszyscy nadawcy są równorzędnymi beneficjentami zysków płynących z wykorzystania splątania. Interesujący jest również fakt, że będziemy mieli tutaj do czynienia z efektem ϵ-superaktywacji — dzięki wykorzystaniu splątania, łączna prędkość transmisji przez kanały, praktycznie nie nadające się do komunikacji ($R_T = \epsilon \approx 0$), osiągnie poziom $R_T \approx 1$.

Przedrostek ϵ został użyty w tytule dla podkreślenia, że przez analizowane w tej części kanały można transmitować informację klasyczną z niewielką, jednakże różną od zera prędkością. W tym sensie, opisana tu ϵ-superaktywacja jest słabsza od przedstawionej w pracy [92] superaktywacji pojemności kwantowej typu $0 \otimes 0 > 0$, gdzie kanały składowe rzeczywiście mają zerowe pojemności kwantowe (porównaj [36] dla scenariuszy z wieloma uczestnikami).

Na początek kilka pojęć związanych z koncepcją klasycznego ekstraktora entropii, który to stanowi trzon przytoczonej dalej argumentacji.

Dla dwóch zmiennych losowych X, Y o takim samym nośniku, odległość statystyczna zdefiniowana jest jako:

$$\mathrm{dist}(X, Y) = \frac{1}{2} \sum_{e \in \sup(X)} |P(X = e) - P(Y = e)| \,. \tag{2.96}$$

F_m oznacza zmienną losową o rozkładzie równomiernym na zbiorze 2^m elementowym.

Lemat 2.6 *Dla binarnej zmiennej losowej X, relacja:* $\mathrm{dist}(X, F_2) = \epsilon$ *pociąga za sobą:* $1 - H(X) = (2/\ln 2)\epsilon^2 + O(\epsilon^4)$. *Dla* $\epsilon \in (0, 0.5)$ *zachodzi* $1 - H(X) \leq 4\epsilon^2$.

Dowód:

Dowód lematu wynika natychmiast z rozwinięcia w szereg Taylora.

□

Klasyczny *wielo*źródłowy *ekstraktor losowości* jest funkcją, która destyluje entropię z niezależnych „słabych źródeł losowości". Słowo „klasyczne" ma odróżnić opisaną sytuację od przypadków, gdzie losowość otrzymuje się na skutek efektów kwantowych. Użyteczność zmiennej losowej jako źródła losowości w procesie ekstrakcji mierzy *minimalna entropii* H_∞ [4, 98] zdefiniowana jako:

$$H_\infty(X) = \min_{x \in \sup X} -\log p(x) \tag{2.97}$$

Definicja 2.1 *Wielośródłowy ekstraktor losowości [7] to funkcja* $f_{\text{ext}} : \{0,1\}^{n\times l} \mapsto \{0,1\}^m$, *która dla* l *niezależnych* n*-bitowych źródeł* $X_1, \ldots, X_l$ *z* $H^\infty(X_i) \geq k$ *spełnia:*

$$\text{dist}\left(f_{\text{ext}}\left(X_1, \ldots, X_l\right), F_m\right) \leq \epsilon. \tag{2.98}$$

Funkcja f_{ext} *nazywana jest* l*-źródłowym ekstraktorem z wymaganiami na minimalną entropię rzędu* k*,* n*-bitowym wejściem,* m*-bitowym wyjściem i odległością statystyczną rzędu* ϵ*.*

Twierdzenie 2.3 *(O istnieniu ekstraktora [7]:) Niech* $m < k < n$ *będą liczbami naturalnymi oraz* $\epsilon > 0$*. Jeśli zachodzi* $k > \log n + 2m + 2\log(1/\epsilon) + 1$*, wówczas istnieje 2-źródłowy ekstraktor* $f_{\text{opt}} : \{0,1\}^{n\times 2} \to \{0,1\}^m$ *z* k*-bitowymi wymaganiami na minimalną entropię* H_∞ *oraz odległością statystyczną* ϵ*. Postać ekstraktora może być wyznaczona w czasie proporcjonalnym do:* $2^{5n^2 2^{2k}}$*.*

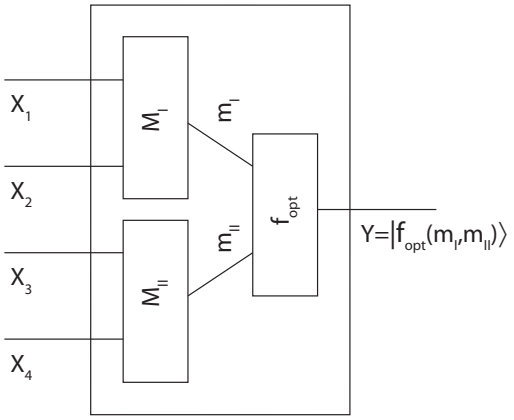
Poniżej będą używane uogólnienie stany Bella [11] postaci:

$$|\psi_{\alpha,\beta}\rangle = \frac{1}{\sqrt{D}} \sum_{l=0}^{D-1} \exp\left(\frac{2\pi \mathrm{i}}{D}\alpha l\right) |l\rangle|l+\beta\rangle, \tag{2.99}$$

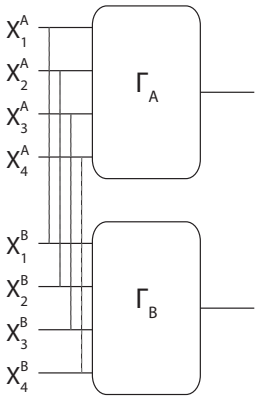
gdzie $\alpha, \beta \in \{0, D-1\}$ są indeksami. Stany należą do przestrzeni $\mathbb{C}^D \otimes \mathbb{C}^D$.

Dla stanu $|\mu\rangle = \sum_i \mu_i |i\rangle$, gdzie $\{|i\rangle\}$ jest bazą standardową, będzie stosowana notacja $|\mu^*\rangle = \sum_i \mu_i^* |i\rangle$ i $D = 2^d$.

Punktem wyjścia dla dalszych analiz będą dwie rodziny kanałów $\{\Gamma_A^{(\delta)}\}$ i $\{\Gamma_B^{(\delta)}\}$ indeksowanych przez δ. Kanały $\{\Gamma_A^{(\delta)}\}$ i $\{\Gamma_B^{(\delta)}\}$ posiadają 4 nadawców, z których każdy kontroluje jedno d-qbitowe wejście: $X_1^A, \ldots, X_4^A$ $(X_1^B, \ldots, X_4^B)$. Ich wyjścia mają rozmiar 1 qbita i są oznaczane przez: Y^A, Y^B. Wejścia X_i^A i X_i^B są kontrolowane przez nadawcę S_i. Rozmiar wejść kanałów zależy od parametru δ w następujący sposób: $d = \lceil 2\log(1/\delta) + 12 \rceil$. Obydwa kanały opierają się na podobnym schemacie (patrz Rys. 2.14). Z tego powodu zostanie opisany tylko kanał Γ_A z zaznaczeniem miejsca, w którym kanały różnią się. W pierwszym kroku kanał wykonuje pomiary projektorowe M_I oraz M_{II}. M_I jest pomiarem łącznym na wejściach X_1, X_2, natomiast M_{II} na wejściach X_3, X_4. W przypadku kanału Γ_A pomiary wykonywane są w bazie $\{|\psi_{\alpha,\beta}\rangle\}$, natomiast w przypadku kanału Γ_B w bazie $\{|\psi_{\alpha,\beta}^*\rangle\}$. Wyniki pomiarów oznaczone są odpowiednio przez m_I i m_{II}. Przyjmujemy, że mają



Rysunek 2.14: Ogólny schemat dla wielodostępowych kanałów kwantowych Γ_A i Γ_B. X_i to d-qubitowe wejścia, M_I oraz M_{II} reprezentują wykonywane przez kanał pomiary projektorowe których wynik to m_I i m_{II}. f_{opt} jest klasycznym ekstraktorem losowości o właściwościach opisanych Tw. 2.3.



Rysunek 2.15: Kanały Γ_A i Γ_B pracujące równolegle. Linie kreskowane oznaczają stany splątane $|\psi_{0,0}\rangle$ przesyłane przez $\Gamma_A \otimes \Gamma_B$.

one postać pary $m = (\alpha, \beta)$. Zmienne losowe związane z wynikami pomiarów stanowią $2d$-bitowe wejście dla ekstraktora losowości f_{opt}. Wyjście f_{opt} ma rozmiar jednego bitu. W zależności wartości $f_{\text{opt}}(m_I, m_{II})$, kanał produkuje stan wyjściowy $|0\rangle$ lub $|1\rangle$. Istnienie ekstraktora f_{opt} o odpowiednich własnościach zostanie pokazane później.

Wróćmy do głównego tematu niniejszej części, czyli subaddytywności minimalnej entropii wyjścia. Zaczniemy od pokazania, że dla $\delta > 0$ minimalna

entropia wyjścia $H_{min}(\Gamma_A^{(\delta)})$ oraz $H_{min}(\Gamma_B^{(\delta)})$ jest nie mniejsza niż $1-\delta$. Następnie, analizując przypadek gdy wszyscy nadawcy S_i przesyłają stany $|\psi_{0,0}\rangle$ (patrz Rys. 2.15), znajdziemy górne ograniczenie na $H_{min}(\Gamma_A^{(\delta)} \otimes \Gamma_B^{(\delta)})$ w postaci $\Gamma_A^{(\delta)} \otimes \Gamma_B^{(\delta)} = 1$. Będzie to prowadzić do wniosku, że dla $\delta < 1/2$ zachodzi subaddytywność minimalnej entropii wyjścia: $H_{min}(\Gamma_A^{(\delta)}) + H_{min}(\Gamma_B^{(\delta)}) > H_{min}(\Gamma_A^{(\delta)} \otimes \Gamma_B^{(\delta)})$.

Lemat 2.7 *Niech przez kanał $\Gamma_A^{(\delta)}$ będą nadawane stany produktowe w postaci: $|\mu_1^A\rangle \otimes |\mu_2^A\rangle \otimes |\mu_3^A\rangle \otimes |\mu_4^A\rangle$, gdzie $|\mu_i^A\rangle$ to stan nadawany przez S_i. Analogicznie dla $\Gamma_B^{(\delta)}$. Wówczas dla zmiennych losowych, związanych z wynikami wykonywanych przez kanał pomiarów, zachodzi: $H^\infty(M_I^A) = H^\infty(M_{II}^A) = H^\infty(M_I^B) = H^\infty(M_{II}^B) \geq d$, gdzie d oznacza rozmiar wejścia kanału.*

Analogiczny lemat można pokazać również w dla kanału $\Gamma_B^{(\delta)}$

Dowód:

Zajmiemy się przypadkiem $H^\infty(M_I^A) = d$. Pozostałe można udowodnić w ten sam sposób. Niech pomiar projektorowy M_I^A będzie wykonywany na stanie produktowym $|\mu\rangle|\nu\rangle$, gdzie $|\mu\rangle = \sum_{j=0}^{D-1} \mu_j |j\rangle$, $|\nu\rangle = \sum_{k=0}^{D-1} \nu_k |k\rangle$ są d-qbitowymi stanami dostarczonymi odpowiednio przez nadawcę S_1 i S_2. Poniżej zostanie pokazane, że rozkład prawdopodobieństwa $P(m_I^A = (\alpha,\beta)) = |\langle\psi_{\alpha,\beta}|\mu|\nu\rangle\rangle|^2$ otrzymania w wyniku pomiaru M_I^A pary wartości $m_I^A = (\alpha,\beta)$ spełnia $p_{\alpha,\beta} \leq \frac{1}{D}$. Prostą konsekwencją tego faktu jest: $H_\infty(M_I^A) \geq d$. Zauważmy, że:

$$
\begin{aligned}
p(\alpha,\beta) &= |\langle\psi_{\alpha,\beta}|\mu\rangle|\nu\rangle|^2 && (2.100)\\
&= \frac{1}{D}\left|\sum_{l=0}^{D-1} \exp\left(\frac{2\pi\mathrm{i}}{D}\alpha l\right) \langle l|\langle l+\beta| \sum_{j=0}^{D-1} \mu_j |j\rangle \sum_{k=0}^{D-1} \nu_k |k\rangle\right|^2 \\
&= \frac{1}{D}\left|\sum_{j=0,k=0,l=0}^{D-1} \exp\left(\frac{2\pi\mathrm{i}}{D}\alpha l\right) \mu_j \nu_k \langle l|j\rangle\langle l+\beta|k\rangle\right|^2 && (2.101)\\
&= \frac{1}{D}\left|\sum_{l=0}^{D-1} \exp\left(\frac{2\pi\mathrm{i}}{D}\alpha l\right) \mu_l \nu_{l+\beta}\right|^2 && (2.102)\\
&= \frac{1}{D}\left|\langle\mu^*|U_\beta^\alpha|\nu\rangle\right|^2, && (2.103)
\end{aligned}
$$

gdzie $U_\beta^\alpha = \sum_{l=0}^{D-1} |l+\beta\rangle\langle l| \exp\left(\frac{2\pi i}{D}\alpha l\right)$ jest operacją unitarną. Ostatecznie, na podstawie własności iloczynu skalarnego otrzymujemy: $p_{\alpha,\beta} = \frac{1}{D}|\langle\mu^*|U_\beta^\alpha|\nu\rangle|^2 \leq \frac{1}{D}$.

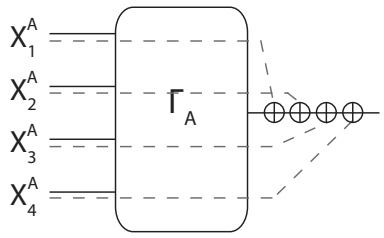
□

W oparciu o Lem. 2.7 można stwierdzić, że ekstraktor losowości f_{opt} pracuje w oparciu o zmienne losowe spełniające wymaganie $H_\infty \geq d$. Zauważmy jeszcze, że dla $d > 4$ zachodzi $d/2 > \log d$. Stąd otrzymujemy $d = \lceil 2\log 1/\delta + 12\rceil$ spełniające dla $\epsilon = \sqrt{\delta}/2$ założenia Tw. 2.3. W ten sposób przekonaliśmy się, że istnieje ekstraktor losowości f_{opt}, którego wyjście leży w statystycznej odległości $\epsilon = \sqrt{\delta}/2$ od rozkładu jednorodnego F_1. Na podstawie Lem. 2.6 minimalna entropia wyjścia kanału ograniczona jest przez: $H_{min} \geq 1 - \epsilon$.

Przejdźmy teraz do entropii wyjścia $\Gamma_A^{(\delta)} \otimes \Gamma_B^{(\delta)}$. Jak już zostało wspomniane, rozważać będziemy przypadek, w którym wszyscy nadawcy S_i przesyłają stany $|\psi_{0,0}\rangle$. Pierwsza część $2d$-qbitowego stanu jest nadawana przez kanał $\Gamma_A^{(\delta)}$, natomiast druga przez kanał $\Gamma_B^{(\delta)}$. Sytuacja ta została przedstawiona na Rys. 2.15. Poniżej zobaczymy, że entropia wyjścia układu $(\Gamma_A^{(\delta)} \otimes \Gamma_B^{(\delta)}$ dla tego protokołu nie może przekroczyć 1.

Ekstraktor losowości f_{opt} jest funkcją deterministyczną. Jeśli wyniki pomiarów dla kanałów $\Gamma_A^{(\delta)}$ i $\Gamma_B^{(\delta)}$ są sobie równe: $m_I^A = m_I^B$ oraz $m_{II}^A = m_{II}^B$, to $f_{\text{opt}}(m_I^A, m_{II}^A) = f_{\text{opt}}(m_I^B, m_{II}^B)$ a stąd również i stany otrzymane na wyjściach kanałów. W przypadku transmisji stanów splątanych, rzeczywiście zachodzi: $m_I^A = m_I^B$ oraz $m_{II}^A = m_{II}^B$, co pokazują poniższe rachunki:

$$
\begin{aligned}
p(m_I^A, m_I^B) &= p(\alpha_A, \beta_A, \alpha_B, \beta_B) && (2.104)\\
&= \frac{1}{D^2}\left|\langle\psi_{0,0}^*|U_{\beta_A}^{\alpha_A} \otimes U_{\beta_B}^{\alpha_B\dagger}|\psi_{0,0}\rangle\right|^2 && (2.105)\\
&= \frac{1}{D^2}\left|\frac{1}{D}\sum_{k,l=0}^{D-1}\langle k|\langle k|\exp\left[\mathrm{i}\frac{2\pi}{D}(\alpha_A - \alpha_B)l\right]\right. && (2.106)\\
&\quad \left.\times\, |l+\beta_A\rangle|l+\beta_B\rangle\right|^2 && (2.107)\\
&= \frac{1}{D^4}\left|\sum_{l}^{D-1}\exp\left[\mathrm{i}\frac{2\pi}{D}(\alpha_A - \alpha_B)l\right]\delta_{\beta_A,\beta_B}\right|^2 && (2.108)\\
&= \frac{1}{D^2}\delta_{\alpha_A,\alpha_B}\delta_{\beta_A,\beta_B}. && (2.109)
\end{aligned}
$$



Rysunek 2.16: Konstrukcja kanału $\tilde{\Gamma}$. Linie ciągłe odpowiadają liniom kwantowym, natomiast kreskowane klasycznym. Linie klasyczne kontrolują operacje CNOT wykonywane na wyjściu kanału.

Formułę (2.105) otrzymuje się w ten sam sposób jak formułę (2.103). Powyższy wynik można interpretować jako uogólnienie wymiany splątania [11, 95, 96]. Splątanie pomiędzy użyciami kanałów $\Gamma_A^{(\delta)}$ i $\Gamma_B^{(\delta)}$ poprzez pomiar M_I^A jest zamieniane na splątanie pomiędzy wejściami kanału $\Gamma_B^{(\delta)}$ należącymi do nadawców S_1 i S_2. Analogiczne rozumowanie można przeprowadzić dla pomiarów M_{II}^A i M_{II}^B.

Skoro wyjścia kanałów $\Gamma_A^{(\delta)}$ i $\Gamma_B^{(\delta)}$ są sobie równe, to stan wyjściowy $\Gamma_A^{(\delta)} \otimes \Gamma_B^{(\delta)}$ można zapisać w postaci $p|00\rangle\langle 00| + (1-p)|11\rangle\langle 11|$. Oczywiste jest, że entropia tego stanu nie może przekraczać 1 bitu.

Zajmiemy się teraz zagadnieniem superaddytywności obszarów pojemności klasycznej. Posłużymy się tu przykładem kanałów $\tilde{\Gamma}_A^{(\delta)}, \tilde{\Gamma}_B^{(\delta)}$ będących drobną modyfikacją odpowiednio kanałów $\Gamma_A^{(\delta)}$ i $\Gamma_B^{(\delta)}$. Podobnie jak wyżej, omówiony zostanie tylko kanał $\tilde{\Gamma}_A^{(\delta)}$, gdyż kanał $\Gamma_B^{(\delta)}$ zachowuje się analogicznie. Kanał $\tilde{\Gamma}_A^{(\delta)}$ przedstawiony jest na Rys. 2.16. Posiada on cztery wejścia i jedno wyjście. Każde wejście składa się z linii d-qbitowej i linii 1-bitowej. Kanał ten definiujemy w następujący sposób:

$$\tilde{\Gamma}_A^{(\delta)}\Big(\rho_1 \otimes e_1^{(i)} \otimes \ldots \otimes \rho_4 \otimes e_4^{(l)}\Big) = \mathrm{CNOT}_i \circ \ldots \circ \mathrm{CNOT}_l\Big(\Gamma_A^{(\delta)}(\rho_1 \otimes \ldots \otimes \rho_4)\Big). \tag{2.110}$$

ρ oznacza stany przesyłane liniami kwantowymi, natomiast $e^{(\cdot)}$ bity przesyłane liniami klasycznymi. $\mathrm{CNOT}_0(\rho) = \rho$ oraz $\mathrm{CNOT}_1(\rho) = X\rho X^\dagger$. Zobaczymy teraz, że w przypadku transmisji stanów produktowych, klasyczny obszar pojemności $\mathcal{R}_{prod} = \mathcal{R}^{(1)}(\tilde{\Gamma}_A^{(\delta)}) + \mathcal{R}^{(1)}(\tilde{\Gamma}_B^{(\delta)})$ ograniczony jest nierównościami $R_S = \sum_{i\in S} R_i \leq 2\delta$, zachodzącymi dla każdego podzbioru nadawców S. Obszar ten porównamy z obszarem pojemności uzyskanym przez protokół transmisji, który wykorzystuje stany splątane: $\mathcal{R}_{spl} = \mathcal{R}^{(1)}(\tilde{\Gamma}_A^{(\delta)} \otimes \tilde{\Gamma}_B^{(\delta)})$.

Zauważmy, że $R_S \leq I(X_S : Y|X_{S^C}) \leq H_{max} - H_{min}$ gdzie H_{max} to maksymalna entropia wyjścia kanału. Na podstawie wymiaru przestrzeni wyjścia kanałów $\tilde{\Gamma}_A^{(\delta)}$ oraz $\tilde{\Gamma}_B^{(\delta)}$, w obu przypadkach mamy $H_{max} \leq 1$. Biorąc pod uwagę wyniki dotyczące minimalnej entropii wyjścia kanałów Γ_A i Γ_B otrzymujemy $H_{min} \geq 1 - \delta$, co prowadzi do $R_S(\tilde{\Gamma}_A^{(\delta)}) \leq \delta$, $R_S(\tilde{\Gamma}_B^{(\delta)}) \leq \delta$ oraz $R_S(\tilde{\Gamma}_A^{(\delta)}) + R_S(\tilde{\Gamma}_B^{(\delta)}) \leq 2\delta$.

Sprawdźmy co się stanie, gdy do gry włączą się stany splątane. W tym celu posłużymy się następującym protokołem: każdy z nadawców, podobnie jak wyżej, przesyła liniami kwantowymi kanałów $\tilde{\Gamma}_A^{(\delta)}$, $\tilde{\Gamma}_A^{(\delta)}$ stan $\Psi_{0,0}$. Przez linię klasyczną kanału $\tilde{\Gamma}_A^{(\delta)}$ przesyłana jest cały czas etykieta 0. Linia klasyczna kanału $\tilde{\Gamma}_B^{(\delta)}$ używana jest w zależności od potrzeb i mogą nią być przesyłane etykiety 0 oraz 1. Jak mieliśmy już okazję zauważyć, wyjścia kanałów $\Gamma_A^{(\delta)}$ i $\Gamma_B^{(\delta)}$, w przypadku transmisji stanów splątanych, są takie same. Jeśli odbiorca wykona na wyjściu kanału $\tilde{\Gamma}_B^{(\delta)}$ operację CNOT kontrolowaną przez wyjście kanału $\tilde{\Gamma}_A^{(\delta)}$, cała sytuacja sprowadzi się do transmisji przez klasyczny binarny kanał XOR. Klasyczne linie kanału $\tilde{\Gamma}_B$ odpowiadają wejściom kanału XOR, natomiast wynik operacji CNOT mierzony w bazie standardowej wyjściu kanału XOR. Obszar pojemności kanału XOR jest opisany dobrze znaną z klasycznej teorii informacji formułą $R_1 + R_2 + R_3 + R_4 \leq 1$ [70].

2.4 Otwarte pytania

Przedstawione wyżej wyniki nasuwają nowe pytania oraz sugerują dalsze kierunki badań nad efektem aktywacji obszarów pojemności klasycznej. Rozważania poniżej stanowią odniesienie do części z tych problemów.

- Czy zachodzi superaddytywność regularyzowanych obszarów pojemności wyrażona w terminach R_T?

- Wykorzystanie schematu gęstego kodowania oraz wymiany splątania pozwala łamać addytywność $\mathcal{R}$. Czy można podać jakąś strukturalną charakterystykę wielodostępowych kanałów kwantowych, dla których ten efekt zachodzi?

- Mieliśmy okazję przekonać się, że twierdzenia o addytywności pojemności klasycznej dla pewnych klas kanałów kwantowych (kanałów łamiących splątanie, kanałów identycznościowych) nie przenoszą się na

obszar kanałów z wieloma nadawcami. Jakie klasy kanałów wielodostępowych zachowują addytywność $\mathcal{R}$?

- Czy istnieje zwięzła formuła na ciasne (ang. tight) ograniczenie górne $\mathcal{R}^{\infty}$? Ograniczenie takie pozwalałoby zatrzymać procedurę optymalizacji dla zadowalającego przybliżenia $\mathcal{R}^{(n)} \approx \mathcal{R}^{(\infty)}$.

- Jakie stany kwantowe są użyteczne w optymalizacji $\mathcal{R}^{(n)}$: słowa kodowe z kwantowych kodów korekcyjnych, stany klastrowe, stany Dicka [35]?

- Jak duży wpływ na efekt superaddytywności ma obecność szumu?

- Czy efekt superaddytywności typu (ii) zawsze występuje w parze z efektem subaddytywności H_{min}?

Rozdział 3

W stronę eksperymentu - efekt aktywacji w kanałach Gaussowskich

Rozdział ten jest próbą pokazania, że efekt kwantowej aktywacji obszarów pojemności klasycznej, analogiczny do rozważanego w przypadku zmiennych dyskretnych, można zaobserwować w laboratorium już dziś, przy obecnym stanie techniki[1].

Przełożeniu opisanych w poprzednim rozdziale koncepcji na język stanów Gaussowskich pozwala ominąć ograniczenia oraz trudności implementacyjne opisane w części 2.3. Z drugiej strony, proponowana tu zmiana podejścia, wprowadza pewne trudności formalne oraz sprawia, że sam efekt aktywacji staje się mniej czytelny. W przypadku kanałów Gaussowskich nie można utrzymać w mocy twierdzenia o addytywności obszarów pojemności (patrz Tw. 2.1), dlatego poniżej wprowadzona zostanie zasada lokalności. Jest ona uogólnieniem Tw. 2.1 w tym sensie, że obejmuje szerszą klasę kanałów wielodostępnych, tj. wielodostępne kanały dyskretne i Gaussowskie. Wiąże się to jednak z rezygnacją z pełnej charakteryzacji obszaru pojemności pracujących równolegle kanałów wielodostępnych. Aktywacja pojemności klasycznej Gaussowskich wielodostępnych kanałów kwantowych będzie analizowana w tym rozdziale właśnie w kontekście łamania zasady lokalności.

[1] Obszerne wprowadzenie do najnowszych osiągnięć w obszarze eksperymentalnej optyki kwantowej można znaleźć w pracy [5].

3.1 Zasada lokalności w klasycznych wielodostępnych kanałach Gaussowskich

Zasada lokalności jest uogólnieniem twierdzenia o addytywności pojemności klasycznej (Tw. 2.1), obowiązującego dla kanałów dyskretnych. Zanim przejdziemy do jej szczegółowego przedstawienia, spójrzmy na przykład pokazujący dlaczego twierdzenie o addytwności nie przenosi się na kanały Gaussowskie nawet w najprostszym przypadku kanałów 1-do-1. Rozpatrzmy dwa kanały Gaussowskie 1-do-1: Φ_1 i Φ_2, dla których poziom szumu wynosi odpowiednio $\sigma^2_{szum}(\Phi_1)$ i $\sigma^2_{szum}(\Phi_2)$. Zakładamy, że $\sigma^2_{szum}(\Phi_1) < \sigma^2_{szum}(\Phi_2)$. Ponadto, w przypadku obu kanałów nadawca podlega takiemu samemu ograniczeniu σ^2_{we} na średnią dostępną moc. Pojemności uzyskiwane w tym momencie przez niego to $C_1 = \frac{1}{2}\log\left[1+\frac{\sigma^2_{we}}{\sigma^2_{szum}(\Phi_1)}\right]$ i $C_2 = \frac{1}{2}\log\left[1+\frac{\sigma^2_{we}}{\sigma^2_{szum}(\Phi_2)}\right]$ (patrz Rw. (1.23)). Co się stanie, gdy nadawca ma dostęp do obu kanałów jednocześnie? Średnia moc, z której może korzystać nadawca, wynosi wówczas $\tilde{\sigma}^2_{we} = 2\sigma^2_{we}$. Ponieważ poziom szumów wprowadzanych przez kanały Φ_1 i Φ_2 jest różny, nadawca może zoptymalizować alokację mocy, wykorzystując większą jej część do kodowania komunikatów przesyłanych przez kanał o mniejszym poziomie szumu. W przypadku gdy $\sigma^2_{szum}(\Phi_1)+2\sigma^2_{we} \leq \sigma^2_{szum}(\Phi_2)$, najlepszym posunięciem jest wykorzystanie całej dostępnej mocy do komunikacji przez kanał Φ_1, w pozostałych przypadkach optimum uzyskuje się spełniając formułę $\sigma^2_{szum}(\Phi_1)+\tilde{\sigma}^2_{we}(\Phi_1) = \sigma^2_{szum}(\Phi_2)+\tilde{\sigma}^2_{we}(\Phi_2)$, gdzie: $\tilde{\sigma}^2_{we}(\Phi_i)$ to moc przydzielona na komunikację przez kanał Φ_i (porównaj ang. "water filling algorithm"[25]). Za każdym razem nadawca osiąga pojemność $\tilde{C} > C_1 + C_2$. Widzimy zatem, że optymalizując alokację średniej mocy na wejściu kanału Φ_i, nadawca ma wpływ na łączną pojemność układu $\Phi_1 \otimes \Phi_2$, dzięki czemu łamie w opisanym przypadku addytywność pojemności klasycznej.

Wróćmy teraz do formuł opisujących obszar pojemności wielodostępnego kanału Gaussowskiego. Na podstawie równania (1.42) możemy zauważyć, że prędkość transmisji R_S dla grupy nadawców S zależy jedynie od lokalnego ograniczenia na średnią dostępną moc $\mathcal{P}$. Prowadzi to do wniosku, że dodatkowe zasoby (moc, kanał) dostępne dla jednego z nadawców nie mogą, w przypadku klasycznych kanałów komunikacyjnych, zwiększyć maksymalnej prędkości transmisji osiąganej przez innego nadawcę [29]. Fakt ten, prawdziwy zarówno w przypadku kanałów dyskretnych jak i kanałów Gaussowskich, będziemy nazywać zasadą lokalności.

3.2 Prędkość transmisji dla alfabetów modulacyjnych

Na wstępie przedstawmy schemat komunikacji, który wielokrotnie będzie pojawiał się w kontekście wspomaganego splątaniem łamania zasady lokalności: (i) nadawca koduje komunikat klasyczny w przesunięcie d ustalonego stanu Gassowskiego $\rho_{\gamma,d=0}$, tzn. podczas transmisji posługuje się alfabetem modulacyjnym $\{p_d, \rho_{\gamma,d}\}$, gdzie p_d dane jest wzorem (1.122); (ii) stan $\rho_{\gamma,d}$ przesyłany jest przez kanał komunikacyjny Φ; (iii) odbiorca dekoduje komunikat poprzez pomiar odpowiednich obserwabli na wyjściu kanału $\Phi(\rho_{\gamma,d})$. W analizowanych w tym rozdziale przypadkach, pomiar wykonywany przez odbiorcę można zawsze sprowadzić, przy użyciu elementów optyki liniowej, do pomiaru odpowiedniego zbioru Ω_M komutujących kwadratur.

Poniżej rozpatrywać będziemy n-modowy stan Gaussowski $\rho_{\gamma,d}$ oraz m-elementowy zbiór komutujących obserwabli kanonicznych Ω_M. Ω_M stanowi podzbiór zbioru wszystkich obserwabli kanonicznych Ω, zdefiniowanych na przestrzeni, do której należy ρ. Będziemy stosować oznaczenie $\Omega_D = \Omega \backslash \Omega_M$. Zobaczymy teraz, jak przy użyciu macierzy kowariancji γ oraz wektora przesunięcia d stanu $\rho_{\gamma,d}$ można wyrazić rozkładu gęstości prawdopodobieństwa wyników ξ_M równoczesnego pomiaru wszystkich obserwabli z Ω_M. W tym celu zapiszmy p_{ξ_M} jako całkę funkcji Wignera $W_\rho(\xi)$ po zmiennych ξ_D odnoszących się do obserwabli ze zbioru Ω_D:

$$p_{\xi_M} = \int_{-\infty}^{+\infty} d^{2n-m}\xi_D W_\rho(\xi). \tag{3.1}$$

Rozwijając powyższą formułę zgodnie ze wzorem (1.59) otrzymujemy:

$$\begin{aligned}
p_{\xi_M} &= \int_{-\infty}^{+\infty} d^{2n-m}\xi_D \frac{1}{(2\pi)^{2n}} \int_{-\infty}^{+\infty} d^{2n}\eta e^{-\mathrm{i}\xi^T\eta}\chi_\rho(\eta) && (3.2)\\
&= \frac{1}{(2\pi)^{2n}} \int_{-\infty}^{+\infty} d^{2n}\eta e^{-\mathrm{i}\xi_M^T\eta_M}\chi_\rho(\eta) \int_{-\infty}^{+\infty} d^{2n-m}\xi_D e^{-\mathrm{i}\xi_D^T\eta_D} && (3.3)\\
&= \frac{1}{(2\pi)^{2n}} \int_{-\infty}^{+\infty} d^{2n}\eta e^{-\mathrm{i}\xi_M^T\eta_M}\chi_\rho(\eta)(2\pi)^{2n-m}\delta^{(2n-m)}(\eta_D) && (3.4)\\
&= \frac{1}{(2\pi)^{m}} \int_{-\infty}^{+\infty} d^{m}\eta_M e^{-\mathrm{i}\xi_M^T\eta_M}\chi_\rho(\eta_M, \eta_D = 0). && (3.5)
\end{aligned}$$

Zmienne pomocnicze η_M, η_D odnoszą się do tych samych obserwabli kanonicznych co ξ_D, ξ_M. Powyżej skorzystaliśmy z $\delta(x) = \frac{1}{\pi}\int_{-\infty}^{+\infty} dy \exp(-\mathrm{i}xy)$.

Odwołując się do postaci funkcji charakterystycznej χ stanu Gaussowskiego $\rho_{\gamma,d}$ (patrz Rw. (1.57)) otrzymujemy:

$$\chi_\rho(\eta_M, 0) = \exp\left[-\frac{1}{4}\eta_M^T\tilde{\gamma}\eta_M + \mathrm{i}\eta_M^T\tilde{d} - \tilde{c}\right], \tag{3.6}$$

gdzie $\tilde{\gamma}$ oraz $\tilde{d}$ powstaje z γ i d poprzez usunięcie odpowiednich kolumn i wierszy związanych z obserwablami kanonicznymi należącymi do Ω_D. Stosując transformatę Fouriera, wyznaczamy gęstość prawdopodobieństwa wyników ξ_M pomiaru obserwabli Ω_M:

$$p_{\xi_M} = \frac{1}{\pi^m\sqrt{\det\tilde{\gamma}}}\exp\left[-(\xi_M - \tilde{d})^T\tilde{\gamma}^{-1}(\xi_M - \tilde{d})\right]. \tag{3.7}$$

Podstawiając do wzoru (3.7) $\gamma \mapsto \gamma_\Phi = \phi(\gamma)$, $d \mapsto d_\Phi = \phi(d)$, otrzymamy gęstość prawdopodobieństwa wyników pomiaru obserwabli Ω_M na wyjściu kanału Φ.

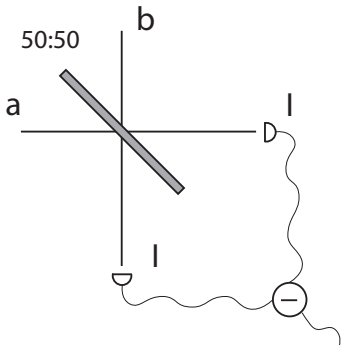
Zauważmy, że wzór (3.7) ma taką samą postać, jak formuła opisująca gęstość prawdopodobieństwa sygnału opuszczającego klasyczny kanał Gaussowski z szumem zadanym macierzą kowariancji $\tilde{\gamma}$. Obserwację tą wykorzystamy do wyznaczenia prędkości transmisji przez kanał Φ w rozpatrywanym schemacie. Niech Y oznacza macierz kowariancji sygnału użytego do modulacji stanu-nośnika $\rho_{\gamma,d=0}$. Zakładamy, że sygnał modulujący ma rozkład Gaussa. Po przejściu przez kanał Y transformuje się do postaci $Y_\Phi = \phi(Y)$. γ_Φ zawiera w sobie szum wprowadzany przez kanał Φ oraz szum związany z zasadą nieoznaczoności której podlega $\rho_{\gamma,d=0}$. Korzystając z liniowości odwzorowania $\phi(.)$ oraz ze wzoru (1.13) otrzymujemy:

$$R = \frac{1}{2}\log\left(\frac{\det\left[\tilde{Y}_\Phi + \tilde{\gamma}_\Phi\right]}{\det\tilde{\gamma}_\Phi}\right). \tag{3.8}$$

W przypadku kanału jednomodowego realizującego przekształcenie $\phi(\gamma) = X^T\gamma X + Z$, kodowanie w przesunięcie d_x prowadzi do prędkości transmisji:

$$R = \frac{1}{2}\log\left(1 + \frac{\sigma_{syg}^2}{\sigma_{szum}^2}\right), \tag{3.9}$$

gdzie $Y = \sigma_{we}^2\mathrm{I}$, $\sigma_{syg}^2 = [\tilde{Y}_\Phi]_{1,1} = X_{11}^2\sigma_{we}^2$ oraz $\sigma_{szum}^2 = [\tilde{\gamma}_\Phi]_{1,1} = [X^T\gamma X + Z]_{11}$. Ponownie spotykamy się tu z ilorazem poziomu sygnału do szumu $RSN = \sigma_{syg}^2/\sigma_{szum}^2$.



Rysunek 3.1: Różnicowy pomiar homodynowy. Pomiar kwadratury wykonywany jest na modzie a, mod b to silne pole w stanie spójnym, I oznacza detektor mierzący natężenia światła w danej wiązce.

3.3 Pomiar homodynowy

W tej części skupimy się na (iii) kroku opisanego powyżej schematu, a dokładniej na metodzie pomiaru dowolnej kwadratury przy użyciu różnicowego pomiaru homodynowego oraz związku pomiędzy rozkładem prawdopodobieństwa uzyskanej w ten sposób wartości, a funkcją charakterystyczną stanu, na którym był przeprowadzany pomiar. Zajmiemy się tu również prędkością transmisji informacji klasycznej we wspomnianym schemacie komunikacji.

Zajmować się będziemy tylko idealnym różnicowym pomiarem homodynowym. Dokładną analizę pomiaru można znaleźć w pracy [5], natomiast w części 3.5.4 opisany jest model szumu dla pomiaru homodynowego oraz jego wpływ na parametry transmisji. Schemat różnicowego pomiaru homodynowego przedstawiony został na Rys. 3.1. Różnicowy pomiar homodynowy zaczyna się od mieszania modów a i b na dzielniku wiązki 50:50. Mod a to system, na którym mierzona jest kwadratura Q; b to system w stanie spójnym $|\beta\rangle$, przy czym zakładamy, że β przyjmuje wartość wystarczająco dużą, aby traktować system b jako mod silnego pola klasycznego. W pomiarze homodynowym mod b pełni funkcję lokalnego oscylatora referencyjnego, ustalającego fazę mierzonej kwadratury Q. Operatory anihilacji wiązek opuszczających dzielnik mają postać:

$$\hat{c} = \frac{1}{\sqrt{2}}(\hat{a} + \mathrm{i}\hat{b}),\ \hat{d} = \frac{1}{\sqrt{2}}(\hat{b} + \mathrm{i}\hat{a}). \tag{3.10}$$

Pomiar natężenia światła $I_c = \hat{c}^\dagger\hat{c}, I_d = \hat{d}^\dagger\hat{d}$ na modach c i d wraz z odpo-

wiednim przetwarzaniem wyników pozwala na pomiar obserwabli:

$$I_d - I_c = \hat{c}^\dagger \hat{c} - \hat{d}^\dagger \hat{d} = \mathrm{i}\left(\hat{a}^\dagger \hat{b} - \hat{a}\hat{b}^\dagger\right). \tag{3.11}$$

Zgodnie z założeniem system b to mod silnego pola klasycznego, co prowadzi do:

$$I_d - I_c = |\beta|\left(\hat{a}e^{-\mathrm{i}\theta} + \hat{a}^\dagger e^{\mathrm{i}\theta}\right), \tag{3.12}$$

gdzie θ związane jest z fazą modu b. Widzimy zatem, że opisany schemat pozwala na pomiar dowolnej kwadratury:

$$Q(\theta) = \frac{1}{2}\left(\hat{a}e^{-\mathrm{i}\theta} + \hat{a}^\dagger e^{\mathrm{i}\theta}\right). \tag{3.13}$$

Pomiar Q można sprowadzić do zastosowania odpowiedniego przesunięcia fazowego na modzie a oraz pomiaru obserwabli kanonicznej X.

3.4 Gęste kodowanie w zmiennych ciągłych

Prezentowane w tym rozdziale wyniki, podobnie jak te przytoczone wcześniej dla kanałów w zmiennych dyskretnych, bazują na schemacie gęstego kodowania. Z tego względu, aby ułatwić dalszą lekturę, poniżej omówiona zostanie jego realizacja w oparciu o stany Gaussowskie [6, 19] oraz analog pomiaru Bella w zmiennych ciągłych [41].

Schemat gęstego kodowania przedstawia się następująco: (i) nadawca i odbiorca współdzielą dwumodowy stan ściśnięty $|\psi_r\rangle$ gdzie r oznacza parametr ściśnięcia; (ii) nadawca wykonuje na swoim podukładzie operację przesunięcia $D(d_x, d_p)$, po czym (iii) odsyła go odbiorcy przez idealny kanał jednomodowy; (iv) odbiorca przeprowadza równoczesny pomiar obserwabli $X_1 - X_2$ oraz $P_1 + P_2$, pomiar ten jest uogólnieniem pomiaru Bella na przypadek zmiennych ciągłych. Dla parametru ściśnięcia r oraz przesunięcia (d_x, d_p) wyniki pomiaru mają rozkład Gaussowski o wartości średniej: $\mathrm{E}(X_1 - X_2) = d_x$, $\mathrm{E}(P_1 + P_2) = d_p$ oraz wariancji $\sigma^2(X_1 - X_2) = \sigma^2(P_1 + P_2) = e^{-2r}$. Na podstawie wyniku pomiaru, nadawca może określić wartość przesunięcia (d_x, d_p), przy czym dokładność z jaką to zrobi rośnie wraz z parametrem ściśnięcia r. Prędkość transmisji, przy średniej mocy σ_{we}^2 zużytej na modulację stanu $|\psi_r\rangle$ wynosi:

$$R = \log\left(1 + \sigma_{we}^2 e^{2r}\right). \tag{3.14}$$

Aby porównać prędkości transmisji w opisanym wyżej schemacie z pojemnością idealnego kanału jednomodowego $C_{id} = g(N)$ (patrz Rw. (1.119)), musimy wprowadzić łączne ograniczenie $\mathcal{P}$ na średnią moc wykorzystywaną w procesie komunikacji, obejmujące moc zużytą na przygotowanie stanów ściśniętych oraz na ich modulację. Ograniczenie to, w terminach średniej liczby fotonów przypadających na jedno użycie kanału, wynosi:

$$\sigma_{we}^2 + \sinh^2 r \leq N. \tag{3.15}$$

Optymalizacja poziomu sygnału do szumu we wzorze (3.14) dla ustalonego N prowadzi do pojemności schematu gęstego kodowania w postaci:

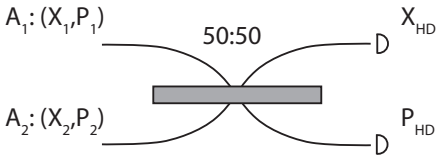
$$\mathcal{C}_{GK} = \log\left(1 + N + N^2\right). \tag{3.16}$$

Można pokazać, że w granicy $N \to \infty$ zachodzi $\mathcal{C}_{GK} = 2\mathcal{C}(\mathcal{I})$. Granica $N \to \infty$ odpowiada transmisji stanów maksymalnie splątanych. Podobnie jak w przypadku zmiennych dyskretnych, występuje tutaj charakterystyczne podwojenie pojemności klasycznej. Zysk pojemności w schemacie gęstego kodowania zaczyna być odczuwalny począwszy od $r = 0.7809$, co odpowiada ściśnięciu dwumodowemu na poziomie $6.78dB$. Stan ściśnięty niesie wówczas średnio $N = 1.884$ fotonów.

Na koniec porównamy jeszcze schemat gęstego kodowania z dwoma protokołami działającymi w oparciu o stany Gaussowskie (porównaj część 1.2.6 oraz część 3.5.2): kodowanie w przesunięcie (d_x, d_p) stanów spójnych i detekcja heterodynowa X, P oraz kodowanie w przesunięcie $(d_x, 0)$ ściśniętych stanów próżni i detekcja homodynowa X. Prędkość transmisji uzyskiwana w pierwszym przypadku wynosi $R_{SP} = \log(1 + N)$ [46, 78, 91] i jest ona zawsze mniejsza od $\mathcal{C}_{GK}$. Drugi z protokołów osiąga prędkość transmisji $R_{SC} = \log(1 + 2N)$ [91]. Wartość parametru ściśnięcia, powyżej której $\mathcal{C}_{GK}$ przewyższa R_{SC}, wynosi $r = 0.5493$ co odpowiada ściśnięciu dwumodowemu na poziomie $4.77dB$.

Typowa implementacja dwumodowego analogu pomiaru Bella w zmiennych ciągłych polega na mieszaniu modów wejściowych na dzielniku wiązki $50:50$ (patrz Rw. (1.65)). Wiąże się to z następującą transformacją obserwabli kanonicznych:

$$\begin{pmatrix} X_1 \\ P_1 \\ X_2 \\ P_2 \end{pmatrix} \mapsto \begin{pmatrix} X_1' \\ P_1' \\ X_2' \\ P_2' \end{pmatrix} = \begin{pmatrix} \frac{X_1 - X_2}{\sqrt{2}} \\ \frac{P_1 - P_2}{\sqrt{2}} \\ \frac{X_1 + X_2}{\sqrt{2}} \\ \frac{P_1 + P_2}{\sqrt{2}} \end{pmatrix}. \tag{3.17}$$



Rysunek 3.2: Realizacja analogu pomiaru Bella w zmiennych ciągłych poprzez mieszanie modów wejściowych na dzielniku wiązki 50:50 oraz pomiar homodynowy.

Na drodze wiązek opuszczających dzielnik umieszczane są detektory homodynowe wykonujące odpowiednio pomiar obserwabli kanonicznej $X = X_1'$ pierwszej wiązki i obserwabli kanonicznej $P = P_2'$ drugiej wiązki. W ten sposób realizowany jest równoczesny pomiar na modach wejściowych obserwabli $(X_1 - X_2)/\sqrt{2}$ oraz $(P_1 + P_2)/\sqrt{2}$. Współczynnik $1/\sqrt{2}$ usuwa się przez odpowiednie skalowanie wyników pomiaru.

3.5 Wyniki

Pytania, na które starano się odpowiedzieć w tym rozdziale, to:

- Czy istnieją kanały Gaussowskie pozwalające obserwować wspomaganą splątaniem aktywację pojemności klasycznej?

  Dwa przykłady takich kanałów, zbudowane w oparciu o (i) dzielnik wiązki oraz (ii) bramkę XP, czytelnik znajdzie odpowiednio w części 3.5.1 oraz części 3.5.3. Głównym ograniczeniem dla obserwacji efektu aktywacji jest problem z osiągnięciem wystarczająco wysokiego poziomu ściśnięcia. We wskazanych fragmentach została podana minimalna wartość r konieczna do uzyskania aktywacji.

- Jak przestawia się prędkość transmisji uzyskana dzięki zastosowaniu splątania na tle innych protokołów pracujących w oparciu o stany Gaussowskie?

  Należy tutaj zauważyć, że wykorzystanie splątania nie jest w przypadku kanałów Gaussowskich jedynym środkiem prowadzącym do łamania zasady lokalności. Jak pokazano w pracy [93], efekt taki można również uzyskać używając jednomodowych stanów ściśniętych. Oba podejścia

porównywane są w części 3.5.2 pod kątem poziomu ściśnięcia koniecznego do złamania zasady lokalności. Dodatkowo, prędkość osiągana przy transmisji wspomaganej stanami splątanymi zostaje tam zestawiona z prędkością transmisji w typowym protokole sieciowej komunikacji światłowodowej.

- Jak bardzo ograniczenia związane z dokładnością aparatury pomiarowej i sprzętu laboratoryjnego wpływają na występowania efekt aktywacji?

  W części 3.5.4, na przykładzie konkretnych wartości dotyczących efektywności aparatury pomiarowej, dokładności realizacji bramek XP[2] oraz strat podczas transmisji przez elementy optyczne, poddawany dyskusji jest wpływ szumu na efekt aktywacji. Omawiana jest również relacja między poziomem szumu, a wymaganym w danej implementacji poziomem ściśnięcia stanów splątanych. Wyniki wydają się być optymistyczne sugerując, że przy osiąganym obecnie poziomie ściśnięcia aparatura pomiarowa jest wystarczająco dokładna, aby obserwować efekt aktywacji bez konieczności uciekania się do postselekcji wyników.

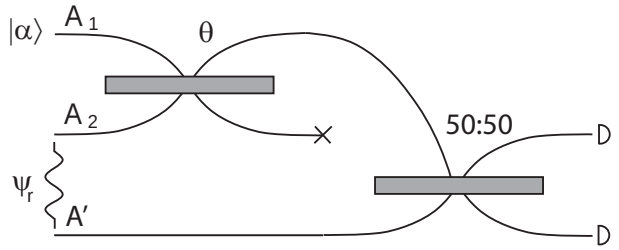
Podobnie jak rozdziale dotyczącym kanałów dyskretnych, w celu zademonstrowania łamania zasady lokalności, analizować będziemy jedynie prędkość transmisji uzyskiwaną przez jednego z nadawców, podczas gdy drugi pełnić będzie rolę pomocnika dostarczając za każdym razem ściśniętych stanów próżni.

3.5.1 Dzielnik wiązki: łamanie zasady lokalności w laboratorium.

W tej części zobaczymy, jak wykorzystując dzielnik wiązki — jeden z najpopularniejszych elementów optycznych — można zademonstrować w laboratorium wspomagane splątaniem łamanie zasady lokalności. Prezentowane tu zastosowanie dzielnika wiązki wiąże się bezpośrednio z technikami telekomunikacji światłowodowej i klasycznym sprzęganiem wiązek światłowodowych [39] oraz jest naturalnym podejściem do modelowania optycznych sieci telekomunikacyjnych [71, 37].

W proponowanym schemacie doświadczenia mamy dwóch nadawców (S_1 i S_2) komunikujących się z tym samym odbiorcą. Obaj nadawcy korzystają z

[2]Skupiamy się tu na podejściu: ang. measurment-induced XP gate.



Rysunek 3.3: Budowa kanału Φ_θ oraz konfiguracja pozwalająca obserwować wspomagane splątaniem łamanie zasady lokalności.

kanału wielodostępowego Φ_θ[3]. Ponadto nadawca S_2 ma dostęp do idealnego kanału jednomodowego $\mathcal{I}$. Łamanie zasady lokalności zostanie pokazane na podstawie prędkości transmisji informacji klasycznej osiąganej przez nadawcę S_1. Mówiąc ściśle zobaczymy, że dla ustalonych ograniczeń $\mathcal{P}$ na moc dostępną nadawcom zachodzi: $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I}) > R_1^{(\infty)}(\Phi_\theta) + R_1^{(\infty)}(\mathcal{I})$. Oznacza to, że dodatkowe zasoby dostępne dla S_2 jakimi sa splątanie i kanał komunikacyjny $\mathcal{I}$ pozwalają zwiększyć prędkość transmisji osiąganą przez S_1.

Schemat układu $\Phi_\theta \otimes \mathcal{I}$ znajduje się na Rys. 3.3. Kanał Φ_θ składa się z dzielnika wiązki o transmitancji $T = \cos^2\theta$, na którym mieszane są mody pochodzące od nadawców S_1 i S_2. Odbiorca ma dostęp do jednego z modów wyjściowych dzielnika wiązki. Drugi mod wyjściowy jest tracony. Kanał realizuje odwzorowanie: $\Phi_\theta(\rho_1 \otimes \rho_2) = \mathrm{tr}_{S_1}\left[U_{DW}(\rho_1 \otimes \rho_2)U_{DW}^\dagger\right]$, wyrażające się w terminach operatorów kanonicznych jako:

$$\begin{pmatrix} X_1 \\ P_1 \\ X_2 \\ P_2 \end{pmatrix} \mapsto \begin{pmatrix} X_{\Phi_\theta} \\ P_{\Phi_\theta} \end{pmatrix} = \begin{pmatrix} \sin\theta X_1 + \cos\theta X_2 \\ \sin\theta P_1 + \cos\theta P_2 \end{pmatrix}. \tag{3.18}$$

Zaczniemy od wyznaczenia prędkości transmisji $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})$ nadawcy S_1, gdy przesyła on stany spójne $\rho_{\gamma=\mathrm{I},d}$[4]. Nadawca S_2 za każdym razem przesyła dwumodowy stan ściśnięty $|\psi_r\rangle\langle\psi_r|$. Odbiorca wykonuje pomiar Bella obserwabli $X_{\Phi_\theta} - X_I, P_{\Phi_\theta} + P_I$ (patrz część 3.4) na wyjściu $\Phi \otimes \mathcal{I}$, określając w ten sposób komunikat od S_1. W granicy bardzo jasnych stanów $|d|^2 \to \infty$ oraz transmitancji $T \to 1$, przy zachowaniu proporcji $|d|^2(1-T) = const$, kanał

[3] $\theta \in [0, \pi)$ to parametr charakteryzujący kanał.

[4] Nadawca koduje swój komunikat koduje w przesunięcie (d_x, d_p) stanu próżni $\rho_{\gamma=\mathrm{I},0}$.

Φ_θ realizuje operację przesunięcia na modzie pochodzącym od nadawcy S_2 [73]: $\Phi(\rho_{\gamma=\mathrm{I},d} \otimes \rho_2) = D(d_x \sin\theta, d_y \sin\theta)\rho_1 D(d_x \sin\theta, d_y \sin\theta)^\dagger$. Przesunięcie to moduluje stan ściśnięty $|\psi_r\rangle\langle\psi_r|$, co w powiązaniu z wykonywanym przez odbiorcę pomiarem Bella daje bliską analogię schematem gęstego kodowania dla zmiennych ciągłych.

Ponieważ nadawca S_2 nie przesyła żadnych komunikatów, schemat $\Phi_\theta \otimes \mathcal{I}$ możemy traktować jak kanał 1-do-1 i skorzystać z podejścia przedstawionego w części 3.3. Przyjmujemy standardowo (porównaj Rw. (1.122)), że przesunięcie stanów nadawanych przez S_1 ma rozkład prawdopodobieństwa (porównaj Rw. (1.122)):

$$p_d = \frac{1}{2\pi\sigma_{we}^2} \exp\left(-\frac{|d|^2}{2\sigma_{we}^2}\right), \tag{3.19}$$

co prowadzi do wejściowych macierzy kowariancji sygnału oraz szumu w postać:

$$Y = \mathrm{diag}\left(\left\{2\sigma_{we}^2, 2\sigma_{we}^2\right\}\right) \oplus \mathrm{diag}\left(\{0,0,0,0\}\right) \tag{3.20}$$

$$\gamma = \gamma_{SP} \oplus \gamma_{SPL}, \tag{3.21}$$

gdzie γ_{SP} to macierz kowariancji stanu spójnego a γ_{SPL} dwumodowego stanu ściśniętego. Na podstawie wzoru (3.18), otrzymujemy macierze kowariancji szumu $\gamma_{\Phi_\theta\otimes\mathcal{I}}$ oraz sygnału $Y_{\Phi_\theta\otimes\mathcal{I}}$ na wyjściu układu $\Phi_\theta \otimes \mathcal{I}$ w postaci:

$$Y_{\Phi_\theta\otimes\mathcal{I}} = \mathrm{diag}\left(\left\{2\sin^2\theta\sigma_{we}^2, 2\sin^2\theta\sigma_{we}^2, 0, 0\right\}\right) \tag{3.22}$$

$$\gamma_{\Phi_\theta\otimes\mathcal{I}} = \begin{pmatrix} \cos^2\theta \mathrm{ch}2r + \sin^2\theta & 0 & \cos\theta \mathrm{sh}2r & 0 \\ 0 & \cos^2\theta \mathrm{ch}2r + \sin^2\theta & 0 & -\cos\theta \mathrm{sh}2r \\ \sin\theta \mathrm{sh}2r & 0 & \mathrm{ch}2r & 0 \\ 0 & -\sin\theta \mathrm{sh}2r & 0 & \mathrm{ch}2r \end{pmatrix}.$$

W wyniku pomiaru Bella otrzymujemy ostatecznie:

$$\tilde{Y}_{\Phi_\theta\otimes\mathcal{I}} = \mathrm{diag}\left(\left\{\sin^2\theta\sigma_{we}^2, \sin^2\theta\sigma_{we}^2\right\}\right) \tag{3.23}$$

$$\tilde{\gamma}_{\Phi_\theta\otimes\mathcal{I}} = \mathrm{diag}\left(\left\{\left(\cosh r - \cos\theta \sinh r\right)^2, \left(\cosh r - \cos\theta \sinh r\right)^2\right\}\right) \tag{3.24}$$

Podstawiając powyższe wyniki do wzoru (3.8) otrzymujemy prędkość transmisji:

$$R_1^{(1)}(\Phi_\theta \otimes \mathcal{I}) = \log\left[1 + \frac{\sin^2\theta\sigma_{we}^2}{(\mathrm{ch}r - \cos\theta \mathrm{sh}r)^2}\right]. \tag{3.25}$$

Prędkość transmisji $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})$, tak jak można było się spodziewać, dąży w granicy $T \to 1$,$\sigma_{we}^2 \to \infty$, $\sigma_{we}^2(1-T) = const$ do prędkości transmisji schematu gęstego kodowania $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I}) \to \log(1+e^{2r}\sigma_{we}^2 \sin^2\theta)$. Dalej będziemy zakładać ograniczenie $\mathcal{P}$ na średnią liczbę fotonów na użycie kanału:

$$\begin{cases} S_1 & : \quad \sigma_{we}^2 \leq N_1 \\ S_2 & : \quad 2\mathrm{sh}^2 r \leq 2N_2 \end{cases} \tag{3.26}$$

Ekstrema (3.25) przy braku ograniczeń leżą na krzywej:

$$T = \mathrm{th}^2 r. \tag{3.27}$$

Równanie to łączy ze sobą parametry kanału (transmitancja $T = \cos^2\theta$) z parametrami sygnału (ściśnięcie r). Gdy na równanie (3.25) nałożone są ograniczenia (3.26), w zależności od transmitancji T otrzymujemy dwa przypadki: $T > N_2/(N_2+1)$ oraz $T < N_2/(N_2+1)$. W pierwszym z nich maksimum osiągane jest w punkcie $\sigma_{we}^2 = N_1, \mathrm{sh}^2 r = N_2$, co prowadzi do prędkości transmisji: $R_1^{max} = \log\left[1 + RN_1/2(\sqrt{N_2+1} - \sqrt{TN_2})^2\right]$. Drugi przypadek jest bardziej interesujący. Tutaj maksimum leży na krzywej (3.27) i osiągane jest dla $\sigma_{we}^2 = N_1$. W tym przypadku mamy:

$$R_1^{max}(\Phi_\theta \otimes \mathcal{I}) = \log(1+N_1). \tag{3.28}$$

Ze względu na (3.27) powyższe wyrażenie nie zależy w sposób jawny od parametru ściśnięcia r oraz transmitancji zwierciadła T.

Mając w pamięci analogię do schematu gęstego kodowania, można by oczekiwać relacji typu $R_1^{max}(\Phi_\theta \otimes \mathcal{I}) \propto \log(1+N_1^2)$. Zwróćmy jednak uwagę, że maksymalna prędkość transmisji $R_1^{max}(\Phi_\theta \otimes \mathcal{I})$ osiągana jest w obszarze, gdzie większość energii pochodzącej od S_1 jest tracona, podczas gdy schemat gęstego kodowania zakłada komunikację przez kanał idealny.

Teraz wyznaczymy ograniczenie górne na regularyzowaną prędkość transmisji $R_1^{(\infty)}(\Phi_\theta)$. Zakładać będziemy takie same ograniczenia $\mathcal{P}$ jak w przypadku $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})$ (patrz Rw. (3.26)). Na podstawie ograniczenia Holevo, łączna prędkość transmisji dla obu nadawców spełnia:

$$R_1(\Phi_\theta) + R_2(\Phi_\theta) \leq \max_{\rho_1,\rho_2} S(\Phi_\theta(\rho_1 \otimes \rho_2)) \leq g(N_{wy}). \tag{3.29}$$

Stosując bilansu mocy dla dzielnika wiązki otrzymujemy:

$$N_{wy} = \sin^2\theta N_1 + 2\cos^2\theta N_2. \tag{3.30}$$

Ograniczenie to jest osiągalne w obszarze dużych mocy, gdy nadawca S_2 zużywa całą dostępną moc na wyprodukowanie jednomodowego, ściśniętego stanu próżni [93].

W przypadku n użyć kanału Φ_θ ograniczenia $\mathcal{P}$ przyjmują postać:

$$\begin{cases} S_1 & : & \sum_{k=1}^{n} N_1^{(k)} \leq nN_1 \\ S_2 & : & \sum_{k=1}^{n} N_2^{(k)} \leq nN_2 \end{cases} \tag{3.31}$$

Niech ρ_G będzie n-modowym stanem Gaussowskim o średniej liczbie fotonów N. Redukcja stanu ρ_G do modu k zawiera $N^{(k)}$ fotonów i będzie oznaczana przez $\rho_G^{(k)}$. Zachodzi wówczas [57]:

$$S(\rho_G) \leq \sum_{k=1}^{n} S(\rho_G^{(k)}). \tag{3.32}$$

Korzystając ze wzoru (3.30) oraz z faktu, że stan termiczny maksymalizuje entropię, otrzymujemy:

$$S(\rho_G) \leq \sum_{k=1}^{n} g\left(\sin^2\theta N_1^{(k)} + 2\cos^2\theta N_2^{(k)}\right). \tag{3.33}$$

Optymalizacja alokacji mocy przy ograniczeniach (3.31), prowadzi w szczególności do:

$$\max_{\rho_1^{(n)},\rho_2^{(n)}} S\left(\Phi_\theta^{(n)}\left(\rho_1^{(n)} \otimes \rho_2^{(n)}\right)\right) \leq n\, g\left(\sin^2\theta N_1 + 2\cos^\theta N_2\right) = n\, g\left(N_{wy}\right). \tag{3.34}$$

Ponieważ $R_1^{(n)}(\Phi_\theta) + R_2^{(n)}(\Phi_\theta) \leq \frac{1}{n}\max_{\rho_1^{(n)},\rho_2^{(n)}} S(\Phi_\theta^{(n)}(\rho_1^{(n)} \otimes \rho_2^{(n)}))$ wnioskujemy, że:

$$R_1^{(n)}(\Phi_\theta) \leq g(N_{wy}). \tag{3.35}$$

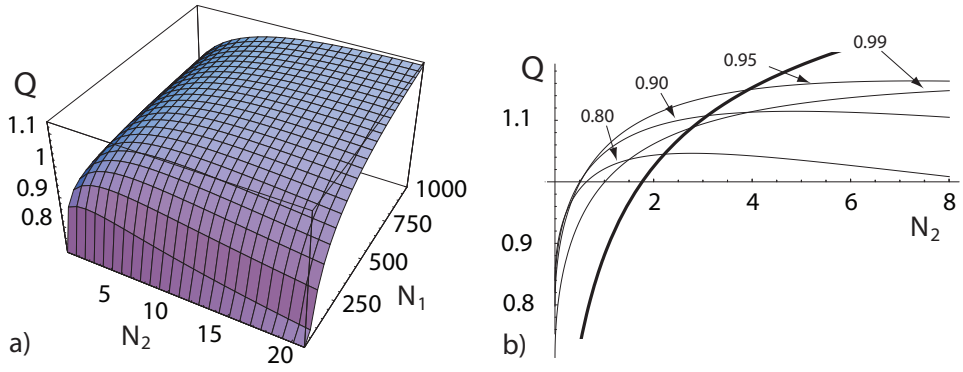
Mając $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})$ oraz $R_1^{(\infty)}(\Phi_\theta)$ możemy wrócić do zagadnienia aktywacji. Ponieważ $R_1^{(\infty)}(\Phi_\theta)$ uwzględnia wpływ splątania między kopiami kanału Φ_θ, możemy mówić tutaj o aktywacji pojemności. Nadawca S_1 nie ma dostępu do kanału $\mathcal{I}$, zatem $R_1^{(\infty)}(\mathcal{I}) = 0$. Wystarczy więc, że znajdziemy takie θ, N_1, N_2, dla których zachodzi: $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I}) > R_1^{(\infty)}(\Phi_\theta)$. Na początek ograniczymy się w poszukiwaniach do obszaru, gdzie efekt kwantowy występuje

najsilniej, tj. przyjmujemy, że nadawca S_2 w pełni wykorzystuje swoje zasoby ($\sinh^2 = N_2$) oraz poruszamy się po krzywej związanej z ekstremum $R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})$ (porównaj wzór (3.27)), która tu przyjmuje postać

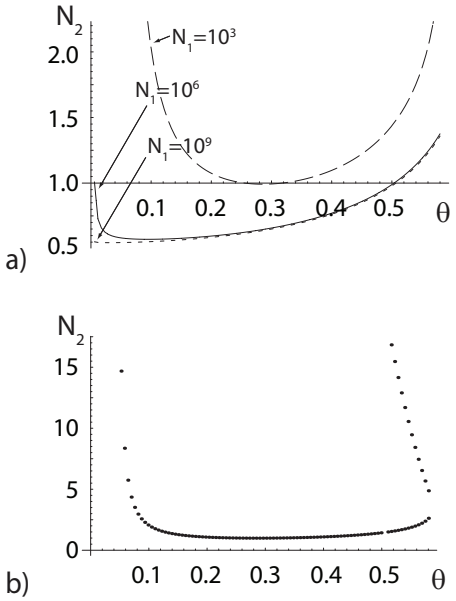
$$\cos^2\theta = N_2/(N_2+1). \tag{3.36}$$

Wstawiając (3.36) do wzoru (3.30) otrzymujemy ograniczenie górne na prędkość transmisji przez kanał Φ_θ (patrz wzór (3.35)) $R_1^{(\infty)}(\Phi_\theta) \leq g(N_{max})$, gdzie $N_{max} = (N_1 + 2N_2^2)/(N_2+1)$. Dalej przyjmujemy dla uproszczenia $R_1^{(\infty)}(\Phi_\theta) = g(N_{max})$. Z naszego punktu widzenia jest to najgorszy przypadek, gdyż oznacza największą prędkość transmisji $R_1^{(\infty)}(\Phi_\theta)$. Iloraz $Q = R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})/R_1^{(\infty)}(\Phi_\theta)$ osiąga maksimum w punkcie $N_1 = 2N_2(N_2+2)$, gdzie przyjmuje postać $Q = \log(1+2N_2(N_2+2))/g(4N_2)$. Dla $N_2 \to \infty$ mamy $Q \to 2$. Widzimy tu jasno łamanie zasady lokalności oraz efekt aktywacji. Iloraz Q dla $N_1 = 2N_2(N_2+2)$ został przedstawiony linią pogrubioną na Rys. 3.4.b). Należy zwrócić uwagę, że dla każdej wartości N_2 mamy do czynienia z innym parametrem θ a tym samym z inną realizacją kanału Φ_θ. Aktywację można obserwować począwszy od $N_2 = 1.73$, co odpowiada ściśnięciu dwumodowemu rzędu $9.46dB$. Z praktycznego punktu widzenia interesujące jest zachowanie ilorazu Q dla ustalonego parametru θ. Na Rys. 3.4.b) przedstawiony został przebieg Q dla kilku skończonych wartości transmitancji $T = \cos^2\theta$ dla $N_1 = 1000$. Aktywacja osiągana jest tu wcześniej niż w przypadku, gdy trzymamy się krzywej (3.36). Ściśnięcie rzędu $5.7-7.7dB$, dla których pojawia się efekt, leży w zakresie realizowanym przy użyciu obecnych technik eksperymentalnych.

Rys. 3.5 stara się odpowiedzieć na pytanie, w jak dużym obszarze parametrów N_1, N_2, θ ma miejsce łamania zasady lokalności. Znajomość tego obszaru pozwala na optymalny wybór parametrów układu doświadczalnego. Na rysunku przedstawione zostały krzywe demarkacyjne $Q = 1$ dla różnych wartości N_1. Startując od $N_2 = 0$ i poruszając się kierunku $N_2 = \infty$ wkraczamy w obszar $R_{SPL} > R_{S_1}^{\Phi_\theta}$. Ze względów praktycznych interesuje nas zakres małych N_2. Wraz z $N_1 \to \infty, \theta \to 0$ zbliżamy się do schematu gęstego kodowania, czego odbiciem jest przesuwanie się minimalnej wartości θ, dla której pojawia się efekt w kierunku $\theta = 0$.



Rysunek 3.4: Wpływ splątania na prędkość transmisji informacji klasycznej. a) zachowanie $Q = R_1^{(1)}(\Phi_\theta \otimes \mathcal{I})/R_1^{(\infty)}(\Phi_\theta)$ w zależności od ograniczenia $\mathcal{P}$ na średnią ilość fotonów na użycie kanału dla nadawców S_1 i S_2 ($\cos^2\theta = \mathrm{th}^2 r$), b) cięcie wykresu a) dla $N_1 = 1000$.



Rysunek 3.5: Dolne ograniczenie dla obszaru $R_{SPL} > R_{S_1}^{\Phi_\theta}$. a) różnymi rodzajami linii przedstawione zostały krzywe $Q = 1$ dla $N_1 = 10^3, 10^6, 10^9$; b) ograniczenie obszaru $Q > 1$ dla $N_1 = 10^3$ widziane w większej skali.

3.5.2 Mieszanina stanów kodowych a prędkość transmisji: poszukiwanie najkrótszej drogi do łamania zasady lokalności

Wybór mieszaniny stanów kodowych w znaczący sposób wpływa na prędkość transmisji poszczególnych nadawców. Korzystając ponownie ze schematu wprowadzonego w części 3.5.1, będziemy drążyli to zagadnienie, szczególnie zwracając uwagę na sytuacje, w których łamana jest zasada lokalności. Skupimy się tylko na transmisji stanów Gaussowskich z alfabetu modulacyjnego oraz prędkości transmisji nadawcy S_1. Nadawca S_2 nie przesyła żadnej informacji i zawsze nadaje tylko jeden ustalony stan. We wszystkich omawianych przypadkach zakładamy ograniczenia $\mathcal{P}$ na średnią moc dostępną dla nadawców w postaci:

$$\begin{cases} S_1 & : & N_1 \\ S_2 & : & N_2 \end{cases} \tag{3.37}$$

Porównywać będziemy następujące protokoły:

- Nadawcy S_1 i S_2 przesyłają stany spójne. S_1 koduje komunikat w przesunięcie (d_x, d_y) nadawanego stanu. Wartości przesunięcia mają rozkład Gaussa (patrz Rw. (1.122)) z macierzą kowariancji $Y = \mathrm{diag}\left(\{2\sigma_{we}^2, 2\sigma_{we}^2\}\right)$, gdzie $\sigma_{we}^2 = N_1$. Nadawca S_2 przez cały czas wysyła tylko jeden wybrany stan spójny. Odbiorca wykonuje pomiar heterodynowy otrzymując w ten sposób średnią wartość obserwabli kanonicznych X_{Φ_θ} i P_{Φ_θ} dla wiązki opuszczającej kanał Φ_θ. Prędkość transmisji wynosi [46, 78, 91]:

  $$R_{SP} = \log(1 + \sin^2\theta N_1). \tag{3.38}$$

  Analogiczny wynik można otrzymać dla kanału tłumiącego o transmitancji $T = \sin^2\theta$ [45]. R_{SP} zależy tylko od lokalnych ograniczeń dla S_1, zatem zachowuje zasadę lokalności.

- Nadawcy S_1 i S_2 przesyłają jednomodowe ściśnięte stany próżni. W obu przypadkach ściskanie zachodzi wzdłuż tej samej kwadratury, powiedzmy X. Parametry ściśnięcia nie zmieniają się podczas procesu komunikacji. S_1 koduje komunikat w przesunięcie d_x, natomiast odbiorca wykonuje pomiar homodynowy obserwabli X_{Φ_θ}. Wartości przesunięcia przyjmują rozkład Gaussa, macierz kowariancji sygnału wejściowego ma postać $Y = \mathrm{diag}\left(\{2\sigma_x^2, 0\}\right)$. Prędkość transmisji wynosi [93]:

  $$R_{SC} = \frac{1}{2}\log\left[1 + \frac{\sigma_x^2 \sin^2\theta}{\sin^2\theta\, e^{-2R} + \cos^2\theta\, e^{-2r}}\right], \tag{3.39}$$

gdzie R i r oznaczają ściśnięcie stanów pochodzących odpowiednio od S_1 i S_2. Poziom szumu w R_{SC} zależy od parametru ściśnięcia r nadawcy S_2 co oznacza, że łamana jest zasada lokalności. Ograniczenia $\mathcal{P}$ wymuszają $\sigma_x^2/2 + \sinh^2 R \leq N_1$ oraz $\sinh^2 r \leq N_2$. Gdy użytkownik S_1 wykonuje optymalizację poziomu sygnału do szumu, w granicy $N_1 \to \infty, N_2 \to \infty$ prędkość transmisji dąży do $R_{SC} \to \log(1 + N_1)$. Wykorzystanie ściśnięcia pozwala poradzić sobie ze stratami energii wynikającymi z transmisji przez Φ_θ.

- Nadawca S_1 przesyła stany spójne kodując komunikat w przesunięcie (d_x, d_y), nadawca S_2 przesyła dwumodowy stan ściśnięty, odbiorca wykonuje pomiar Bella w zmiennych ciągłych. Protokół ten został dokładnie opisany w części 3.5.1. Tutaj przytoczymy tylko uzyskaną prędkość transmisji:

$$R_{SPL} = \log\left[1 + \frac{\sin^2\theta\sigma_{we}^2}{(\cosh r - \cos\theta\sinh^2 r)}\right], \tag{3.40}$$

  gdzie r to parametr ściśnięcia stanu transmitowanego przez S_2, który ze względu na ograniczenia $\mathcal{P}$ spełnia $2\sinh^2 r = N_2$. W przypadku odpowiednio dużego N_2 optymalizacja R_{SPL} pozwala zbliżyć się do $R_{SPL}^{opt} = \log(1 + N_1)$. Wartość ta jest równa pojemności idealnego kanału jednomodowego. Wykorzystanie splątania pozwala poradzić sobie, podobnie jak w poprzednim punkcie, ze stratami w kanale. Tu również obserwujemy łamanie zasady lokalności.

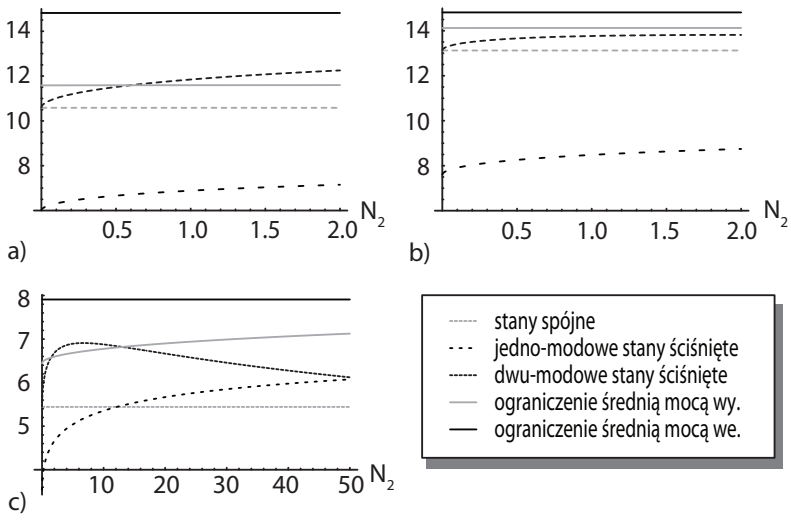
We wszystkich opisanych wyżej przypadkach nadawca S_2 może komunikować się z odbiorcą poprzez kanał identycznościowy, jednakże tylko w przypadku transmisji stanów splątanych użycie tego kanału zwiększa prędkość transmisji dla nadawcy S_1.

Odwoływać się będziemy także do następujących ograniczeń na prędkość transmisji dla S_1:

- Ograniczenie związane ze średnią liczbą fotonów stanów wejściowych od nadawcy S_1.

$$R_1^{max} = g(N_1). \tag{3.41}$$

  Wyznacza ono maksymalną prędkość transmisji uzyskiwaną przez S_1 w przypadku, gdy komunikuje się on z odbiorcą przez idealny kanał jednomodowy. Nie może ono zostać przekroczone przez żaden protokół. Interesuje nas, jak bardzo dany protokół zbliża się do tego ograniczenia.



Rysunek 3.6: Zastawienie prędkości transmisji osiąganych przez protokoły opisane w części 3.5.2 w układzie $\Phi_\theta \otimes \mathcal{I}$ w zależności od średniej liczby fotonów na użycie kanału dla nadawcy N_2: a)$\theta = \pi/4$, $N_1 = 10^6$; b) $\theta = 0.2$, $N_1 = 10^6$; c) $\theta = 0.5$, $N_1 = 10^3$.

- Ograniczenie związane ze średnią liczbą fotonów na wyjściu kanału Φ_θ.

$$R_1^{\Phi_\theta} = g(\sin^2\theta N_1 + \cos^2\theta N_2). \tag{3.42}$$

  Odnosi się ono do sytuacji gdy nadawca S_2 nie może korzystać ze splątania pomiędzy wejściami kanałów Φ_θ oraz $\mathcal{I}$. Uwzględnia regularyzację prędkości transmisji.

W przypadku transmisji stanów produktowych muszą być spełnione oba ograniczenia, zachodzi więc $R_1 \leq \min(R_1^{max}, R_1^{\Phi_\theta})$.

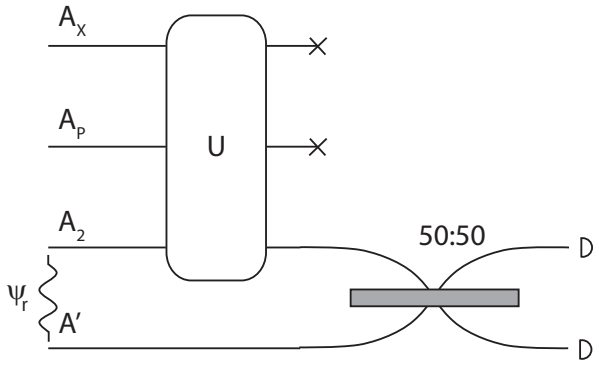
Na Rys. 3.6 analizowane jest zachowanie prędkości transmisji osiąganej przez nadawcę S_1 w zależności od ograniczeń N_2 na moc dostępną dla nadawcy S_2, dla różnych parametrów kanału Φ_θ. Rys. 3.6.a) pokazuje, że koszt splątania, jaki należy ponieść, aby zademonstrować łamanie zasady lokalności, jest dość mały. Występowanie efektu zależy silnie od ograniczeń na moc $\mathcal{P}$ oraz parametrów kanału, co widać na Rys. 3.6.b). Zmiana parametru θ prowadzi do sytuacji, gdy przy danych ograniczeniach $\mathcal{P}$ efekt nie występuje. Rys. 3.6.c) przedstawia zachowanie prędkości transmisji w większym zakresie N_2. Widzimy na nim, że dla małych N_2 najbardziej efektywne

spośród prezentowanych podejść związane jest z transmisją dwumodowych stanów ściśniętych. Obserwujemy tutaj jednak zjawisko wysycenia - wartość R_{SPL} osiąga maksimum dla pewnego poziomu splątania. Dalszy wzrost ilości splątania wiąże się ze wzrostem wymiany splątania ze środowiskiem podczas transmisji przez Φ_θ, a co za tym idzie, stan wyjściowy staje się coraz bardziej splątany ze stanem modu, do którego odbiorca nie ma dostępu. Prowadzi to do wzrostu szumu i spadku prędkości transmisji. W przypadku transmisji jednomodowych stanów ściśniętych sytuacja prezentuje się inaczej. Tutaj, w granicy $N_1 \to \infty$, $N_2 \to \infty$, prędkość transmisji R_{SC} zbliża się do granicy R_1^{max}, jak zostało to pokazane w pracy [93]. Zauważmy, że to podejście wymaga pewnego minimalnego poziomu ściśnięcia, aby przekroczyć prędkość osiąganą dla transmisji stanów spójnych a nakład ściśnięcia potrzebny żeby zbliżyć się do R_1^{max}, w porównaniu z protokołem wykorzystującym stany splątane jest duży.

Jak wspomniano we wstępie do części 3.5.1, kanał Φ_θ koresponduje z klasycznym podejściem do telekomunikacji światłowodowej, gdzie możemy spotkać się z następującym scenariuszem: pewna grupa nadawców współdzieli wiązkę światłowodową, do której przyłączają swoje lokalne generatory stanów spójnych [26, 37]; nadawcy pracują na tym samym modzie; współdzielona wiązka wykorzystywana jest do jednokierunkowej transmisji do wspólnego odbiorcy. Protokoły oparte o stany ściśnięte jedno i dwumodowe mogą inspirować nowe kierunki rozwoju w telekomunikacji światłowodowej przy czym, ze względu na koszt ściśnięcia, łatwiejsze wydaje się podejście wykorzystujące dwumodowe stany ściśnięte.

3.5.3 Schemat gęstego kodowania: niedestruktywna bramka sumacyjna

W tej części przedstawiony zostanie kanał Φ pozwalający obserwować wspomagane splątaniem łamanie zasady lokalności, którego istotną cechą jest, widoczna na pierwszy rzut oka, analogia do schematu gęstego kodowania w zmiennych ciągłych. Schemat kanału Φ znajduje się na Rys. 3.7. Kanał składa się z 3 wejść jednomodowych i jednego jednomodowego wyjścia. Wejścia A_X i A_P są kontrolowane przez nadawcę S_1, natomiast wejście A_2 przez nadawcę S_2. Kanał realizuje przekształcenie: $\Phi\left(\rho_{XP} \otimes \rho_2\right) = \mathrm{tr}_{X,P}\left[U(\rho_{XP} \otimes \rho_2)U^\dagger\right]$, gdzie: $U = \exp\left[-\mathrm{i}\left(x_X p_2 - p_P x_2\right)\right]$, które w terminach obserwabli kanonicz-



Rysunek 3.7: Budowa kanału Φ oraz konfiguracja pozwalająca obserwować wspomagane splątaniem łamanie zasady lokalności.

nych ma postać:

$$\begin{pmatrix} X_X \\ P_X \\ X_P \\ P_P \\ X_2 \\ P_2 \end{pmatrix} \mapsto \begin{pmatrix} X_2 + X_X \\ P_2 + P_P \end{pmatrix}. \tag{3.43}$$

Techniczna realizacja operatora U w kanale Φ bazuje na iloczynie trzech bramek XP (tj. bramek wykonujących przekształcenia: $(x_1, p_1, x_2, p_2) \mapsto (x_1, p_1 - p_2, x_1 + x_2, p_2)$) [10]:

$$U = \exp[-\mathrm{i}(x_X p_2 - p_P x_2)] \tag{3.44}$$

$$= \exp[\frac{\mathrm{i}}{2} x_X p_P] \exp[-\mathrm{i} x_X p_2] \exp[\mathrm{i} p_P x_2]. \tag{3.45}$$

Bramkę XP można aproksymować w oparciu o stany ściśnięte, detekcję homodynową i optykę liniową. Schemat aproksymacji (znany pod nazwą ang. measurement-induced XP gate) został podany w pracy [40], a wyniki eksperymentów odnoszących się do przedstawionego tam podejścia można znaleźć w pracy [94]. W tej części będziemy zakładać wierną realizację bramki XP odkładając do części 3.5.4 analizę wpływu na pojemność kanału zniekształceń związanych z rzeczywistą realizacją tej bramki.

Zajmować się będziemy jak zwykle scenariuszem, w którym nadawca S_2 ma dostęp do dodatkowego jednomodowego kanału identycznościowego $\mathcal{I}$,

przez który komunikuje się z odbiorcą. Interesuje nas tylko prędkości transmisji osiągane przez nadawcę S_1. Nadawca S_1 przesyła linią A_X i A_P jednomodowe stany próżni ściśnięte odpowiednio wzg. obserwabli kanonicznych X i P. Dla obu linie parametr ściśnięcia wynosi R. Nadawca S_2 przesyła liniami A_2 i A' dwumodowy stan ściśnięty $|\psi_r\rangle\langle\psi_r|$ o parametrze ściśnięcia r. S_1 koduje komunikat klasyczny w przesunięcie X i P stanów przesyłanych odpowiednio liniami A_X i A_P. Podobnie jak w części 3.5.1 mamy tutaj do czynienia z alfabetem modulacyjnym, zaczniemy więc od podania macierzy kowariancji sygnału Y oraz macierzy kowariancji γ modulowanego stanu wejściowego dla układu $\Phi \otimes \mathcal{I}$:

$$\begin{aligned} Y &= \operatorname{diag}\left(\left\{2\sigma_{we}^2, 0, 0, 2\sigma_{we}^2\right\}\right) \oplus \operatorname{diag}\left(\{0,0,0,0\}\right) && (3.46)\\ \gamma &= \gamma_{SC-X} \oplus \gamma_{SC-P} \oplus \gamma_{SPL}, && (3.47) \end{aligned}$$

gdzie $\gamma_{SC-X}, \gamma_{SC-P}$ to macierze kowariancji jednomodowych stanów próżni ściśniętych odpowiednio wzg. obserwabli X oraz P, γ_{SPL} to macierz kowariancji dwumodowego stanu ściśniętego a σ_{we}^2 określa wariancję przesunięcia transmitowanych stanów. Macierze kowariancji sygnału oraz szumu na wyjściu $\Phi \otimes \mathcal{I}$ mają postać:

$$\begin{aligned} Y_{\Phi\otimes\mathcal{I}} &= \operatorname{diag}\left(\left\{2\sigma_{we}^2, 2\sigma_{we}^2, 0, 0\right\}\right) && (3.48)\\ \gamma_{\Phi\otimes\mathcal{I}} &= \gamma_{SPL} + \operatorname{diag}\left(\left\{e^{-2R}, e^{-2R}, 0, 0\right\}\right). && (3.49) \end{aligned}$$

W wyniku pomiaru Bella otrzymujemy:

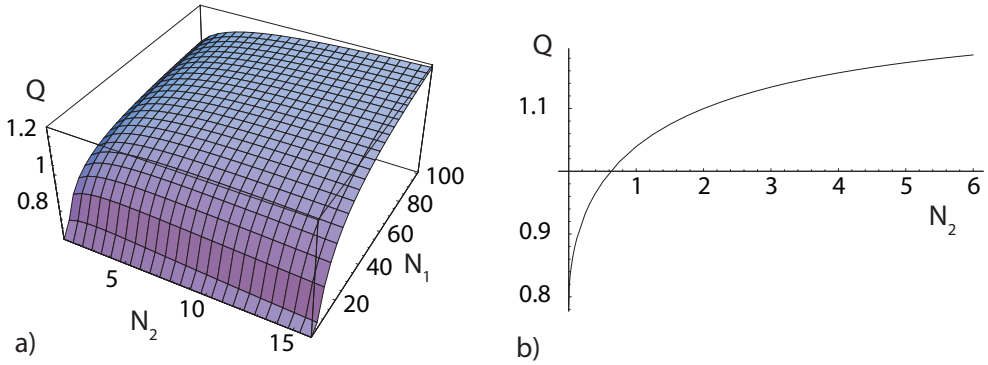
$$\begin{aligned} \tilde{Y}_{\Phi\otimes\mathcal{I}} &= \operatorname{diag}\left(\left\{\sigma_{we}^2, \sigma_{we}^2\right\}\right) && (3.50)\\ \tilde{\gamma}_{\Phi\otimes\mathcal{I}} &= \operatorname{diag}\left(\left\{e^{-2r} + e^{-2R}/2, e^{-2r} + e^{-2R}/2\right\}\right), && (3.51) \end{aligned}$$

co prowadzi do prędkości transmisji nadawcy S_1 w postaci:

$$R_1^{(1)}(\Phi \otimes \mathcal{I}) = \log\left[1 + \frac{\sigma_{we}^2}{e^{-2r} + e^{-2R}/2}\right]. \qquad (3.52)$$

Łatwo zauważyć, że dla $R \to \infty$ otrzymujemy formułę opisującą prędkość transmisji w schemacie gęstego kodowania. Ograniczenia $\mathcal{P}$ na średnią liczbę fotonów przypadających na użycie kanału przyjmujemy w postaci:

$$\begin{cases} S_1 \;:\; \sigma_{we}^2 + 2\sinh^2 R \le N_1 \\ S_2 \;:\; 2\sinh^2 r \le 2N_2 \end{cases} \qquad (3.53)$$



Rysunek 3.8: Wpływ splątania na prędkość transmisji informacji klasycznej. a) zachowanie $Q = R_1^{(1)}(\Phi \otimes \mathcal{I})/R_1^{(\infty)}(\Phi)$ w zależności od ograniczenia $\mathcal{P}$ na średnią liczbę fotonów na użycie kanału dla nadawców S_1 i S_2, b) cięcie wykresu a) dla $N_1 = 100$.

$R_1^{(1)}(\Phi \otimes \mathcal{I})$ osiąga maksimum przy ograniczeniach (3.53) dla: $2e^{2R} = -e^{2r} + \sqrt{e^{4r} + 4e^{2r}(N_1+1) + 4}$, przy czym zachodzi $\sinh^2 r \leq N_2$. Maksimum to będziemy oznaczać przez $R_1^{max}(\Phi \otimes \mathcal{I})$.

Porównamy teraz wartość $R_1^{max}(\Phi \otimes \mathcal{I})$, podobnie jak w części 3.5.1, z górnym ograniczeniem na prędkość transmisji $R_1^{(\infty)}(\Phi)$, danym przez maksymalną entropię $g(N_{max})$ stanu o średniej liczbie fotonów:

$$N_{max} = \left(\sqrt{2N_2 + \frac{1}{2}} + \sqrt{N_1 + 1}\right)^2 - \frac{1}{2}. \tag{3.54}$$

Wartość N_{max} jest maksymalną średnią liczbą fotonów opuszczającą kanał przy ograniczeniach (3.53) i wynika bezpośrednio z relacji (3.43). Rys. 3.8.a) przedstawia iloraz $R_1^{max}(\Phi \otimes \mathcal{I})/R_1^{(\infty)}(\Phi)$. Na Rys. 3.8.b) znajduje się cięcie obszaru z części a) dla $N = 100$. Możemy zauważyć, że efekt aktywacji pojawia się dla $N_2 > 0.63$, co odpowiada ściśnięciu stanu dwumodowego rzędu $6.33dB$. Na wytworzenie stanu ściśniętego o parametrze ściśnięcia $12.73dB$, nadawca S_1 wykorzystuje 4.21 fotonów w każdej linii. Na końcu przedziału, t.j. dla $N_2 = 6$ (ściśnięcie rzędu $14.15dB$) nadawca S_1 zużywa do przygotowania stanów ściśniętych 9.45 fotonów w każdej linii.

3.5.4 Wpływ szumu: jak daleko do eksperymentów?

Realistyczne modele układów eksperymentalnych, w których udział biorą Gaussowskie kanały wielodostępnych powinny uwzględniać techniczne ograniczenia zastosowanych tam elementów optycznych oraz pojawiające się podczas transmisji zakłócenia. Analizując osiągane w eksperymencie prędkości transmisji, należy zwrócić uwagę m.in. na takie zagadnienia jak: straty na elementach optycznych, ograniczoną dokładność realizacji bramek kwantowych (w naszym przypadku bramek XP), szum termiczny wprowadzany przez źródła stanów kodowych, straty i szum wynikające niedoskonałości fotodetektorów oraz szum powstający podczas transmisji światła do i z badanego kanału Gaussowskiego. W tej części będziemy analizować, jak wymienione wyżej czynniki wpływają na efekt aktywacji w scenariuszach opisanych w częściach 3.5.1 oraz 3.5.3. Pozwoli to nam określić wymagania dotyczące dokładności sprzętu potrzebnego do obserwacji efektu. Zaczniemy od dyskusji eksperymentalnej realizacji kanału Φ wprowadzonego w części 3.5.3. Zobaczymy tu, jak ograniczona dokładność realizacji bramki XP prowadzi to powstania zakłóceń. W dalszej części zajmiemy się bardziej ogólnym modelem szumu, związanym z kanałem termicznym (patrz Rw. (1.102)), w wyniku czego uzyskamy nowe formuły na prędkości transmisji nadawcy S_1 dla układów $\Phi \otimes \mathcal{I}$ oraz $\Phi_\theta \otimes \mathcal{I}$.

Problem pojemności klasycznej kwantowych kanałów Gaussowskich wprowadzających szum jest trudny. Nie są znane obecnie formuły na pojemność klasyczną nawet dla tak podstawowych przypadków, jak kanał termiczny. Nie wiadomo również, czy stany Gaussowskie są w tym przypadku optymalną mieszaniną stanów wejściowych. Z tego powodu konieczne będzie posługiwanie się dość grubym oszacowaniem na prędkość transmisji dla stanów produktowych związanym ze średnią liczbą fotonów na wyjściu kanału (porównaj Rw. (3.42)). W rzeczywistości może się okazać, że efekt aktywacji można obserwować również dla większego poziomu szumu i strat oraz przy mniejszym parametrze ściśnięcia.

Kanał Φ można zbudować w oparciu o 3 bramki XP (patrz Rw. (3.45)). Poniżej analizowana będzie aproksymacja bramki XP opisana w pracy [40] (ang. measurment-induced XP - XP_{MI}). Realizacja kanału Φ przy użyciu bramek XP_{MI} oznaczana będzie przez Φ_{MI}.

Transformacja obserwabli kanonicznych przez bramkę XP_{MI} opisana jest

formułami:

$$X_1^{wy} = X_1^{we} - \sqrt{\alpha}X_0 - \sqrt{\beta}X_A, \tag{3.55}$$

$$P_1^{wy} = P_1^{we} - \frac{1-T}{\sqrt{T}}P_2^{we} + \sqrt{\alpha/T}P_0 + \sqrt{T\beta}P_B, \tag{3.56}$$

$$X_2^{wy} = X_2^{we} + \frac{1-T}{\sqrt{T}}X_1^{we} - \sqrt{\alpha/T}\hat{p}_0 + \sqrt{T\beta}X_A, \tag{3.57}$$

$$P_2^{wy} = P_2^{we} - \sqrt{\alpha}P_0 + \sqrt{\beta}P_B, \tag{3.58}$$

gdzie $\alpha = (1-T)(1-\eta)/(1+T)\eta, \beta = (1-T)/(1+T)$, X_0, P_0 to obserwable kanoniczne mierzone na stanach pomocniczych będących ściśniętymi stanami próżni o parametrze ściśnięcia s, θ to efektywność detekcji homodynowej. Dla $T = \frac{1}{2}\left(3-\sqrt{5}\right)$ oraz $s \to \infty, \theta \to 1$ wzory (3.55)-(3.58) przechodzą w

$$\begin{pmatrix} X_1^{we} \\ P_1^{we} \\ X_2^{we} \\ P_2^{we} \end{pmatrix} \mapsto \begin{pmatrix} X_1^{we} \\ P_1^{we} - P_2^{we} \\ X_2^{we} + X_1^{we} \\ P_2^{we} \end{pmatrix}. \tag{3.59}$$

Dalej zakładać będziemy, że zakłócenia wprowadzane przez elementy optyki liniowej są pomijalnie małe w porównaniu z tymi, które są związane z efektywnością pomiaru homodynowego oraz skończonym ściśnięciem stanów pomocniczych.

Bramkę XP_{MI} można, w oparciu o (3.55)-(3.58), przedstawić jako kanał Gaussowski Γ_{XP} opisany macierzami:

$$X = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \; Y = \begin{pmatrix} \sigma_1^2 & 0 & 0 & 0 \\ 0 & \sigma_2^2 & 0 & 0 \\ 0 & 0 & \sigma_2^2 & 0 \\ 0 & 0 & 0 & \sigma_1^2 \end{pmatrix}. \tag{3.60}$$

Powyżej $\sigma_1^2 = \alpha + \beta e^{-2s}, \sigma_2^2 = \alpha/T + \beta T e^{-2s}$. Aproksymacja staje się idealna w granicy $\theta \to 1$ oraz $s \to \infty$. Dla uproszczenia będziemy przyjmować, że wszystkie bramki XP_{MI}, użyte do realizacji kanał Φ, działają w oparciu o ten sam zestaw parametrów θ i s.

Składając ze sobą kanały Γ_{XP} zgodnie ze schematem kanału Φ otrzymujemy:

$$\Phi_{MI}\left(\rho_{XP} \otimes \rho_2\right) = \mathrm{tr}_{A_X, A_P}\left[\Gamma_{X_X P_P} \circ \Gamma_{X_X P_2} \circ \Gamma_{P_P X_2}(\rho_{XP} \otimes \rho_2)\right]. \tag{3.61}$$

Indeks przy kanale Γ oznacza oddziaływanie realizowane przez bramkę XP_{MI}. Na tej podstawie widać, że działanie kanału Φ_{MI} wyrażone w terminach macierzy kowariancji to:

$$\phi_{MI}(\gamma) = \phi(\gamma) + \sigma^2_{XP}\mathrm{I}, \tag{3.62}$$

gdzie $\sigma^2_{XP} = \sigma_1 + \sigma_2$. σ^2_{XP} uwzględnia człony pochodzące od bramek realizujących oddziaływanie $x_X p_2$ oraz $p_P x_2$. Kanał Φ_{MI} można zatem przedstawić jako złożenie oryginalnego kanału Φ z kanałem Φ^{cl} wprowadzającym klasyczny szum Gaussowski o macierzy kowariancji $\sigma^2_{XP}\mathrm{I}$ (patrz Rw. (1.101)):

$$\Phi_{MI} = \Phi^{cl} \circ \Phi. \tag{3.63}$$

Postępując analogicznie jak w części 3.5.3, otrzymujemy formułę na prędkość transmisji dla nadawcy S_1 w postaci (porównaj Rw. (3.52)):

$$R_1^{(1)}(\Phi \otimes \mathcal{I}) = \log\left[1 + \frac{\sigma^2_{we}}{e^{-2r} + e^{-2R}/2 + \sigma^2_{XP}/2}\right], \tag{3.64}$$

gdzie R i r to parametry ściśnięcia modów należących odpowiednio do nadawców S_1 i S_2. σ^2_{we} odnosi się do średniej mocy zużytej na kodowanie.

Zajmiemy się teraz wpływem ograniczeń aparatury pomiarowej (efektywność detekcji homodynowej, szum ciemny) oraz strat na elementach optycznych. W tym celu skorzystamy ze standardowego podejścia (patrz [5]), które polega na tym, że przed każdy idealny detektor homodynowy, występujący w badanym układzie (patrz Rys. 3.7) wstawiamy kanały termiczne (patrz Rw. (1.102)) o transmitancji $T = \cos^2\omega$ oraz średniej liczbie fotonów w stanie termicznym N_T. Kanał taki wprowadza do układu średnio $N_T \sin^2\omega$ fotonów szumu. Zaznaczmy jeszcze, że zebranie szumu pojawiającego się w różnych miejscach badanego układu do kanału termicznego możliwe jest ze względu na liniowość kanału Φ oraz brak korelacji między szumem dodawanym w rożnych miejscach układu.

Wykonując obliczenia podobne do tych które już robiliśmy, dostajemy prędkość transmisji dla nadawcy S_1 w układzie $\Phi \otimes \mathcal{I}$ przy uwzględnieniu szumu:

$$R_1^{szum}(\Phi\otimes\mathcal{I}) = \log\left[1 + \frac{\sigma^2_{we}\cos^2\omega}{(e^{-2r} + e^{-2R}/2)\cos^2\omega + (1+2N_T)\sin^2\omega}\right], \tag{3.65}$$

gdzie R, r i σ^2_{we} mają znaczenie jak we wzorze (3.64) natomiast N_T oraz $T = \cos^2\omega$ to parametry kanału termicznego.

Przedstawiony tu model szumu w zastosowaniu do układu $\Phi_\theta \otimes \mathcal{I}$ prowadzi do:

$$R_1^{szum}(\Phi_\theta \otimes \mathcal{I}) = \log\left[1 + \frac{\sigma_{we}^2 \sin^2\theta \cos^2\omega}{(\cosh r - \cos\theta \sinh r)^2 \cos^2\omega + (1+2N_T)\sin^2\omega}\right], \tag{3.66}$$

gdzie θ jest parametrem kanału Φ_θ.

Rys. 3.9 pokazuje zachowanie $R_1^{szum}(\Phi_\theta \otimes \mathcal{I})$ dla $N_1 = 1000$ i $\theta = 0.25$ w zależności od liczby fotonów w dwumodowym stanie ściśniętym dla różnych parametrów N_T i ω. Wartości parametrów N_1 oraz θ dobrano tak, aby zminimalizować poziom ściśnięcia konieczny do uzyskania efektu superaddytywności (porównaj Rys. 3.5) Rys. 3.9.a) przedstawia przypadki $N_T = 0$ oraz $T_\omega = 1; 0.95; 0.9; 0.85$ — występuje tutaj tylko tłumienie. Prędkość transmisji $R_1^{szum}(\Phi_\theta \otimes \mathcal{I})$ została zestawiona z ograniczeniem związanym ze średnią liczbą fotonów na wyjściu kanału:

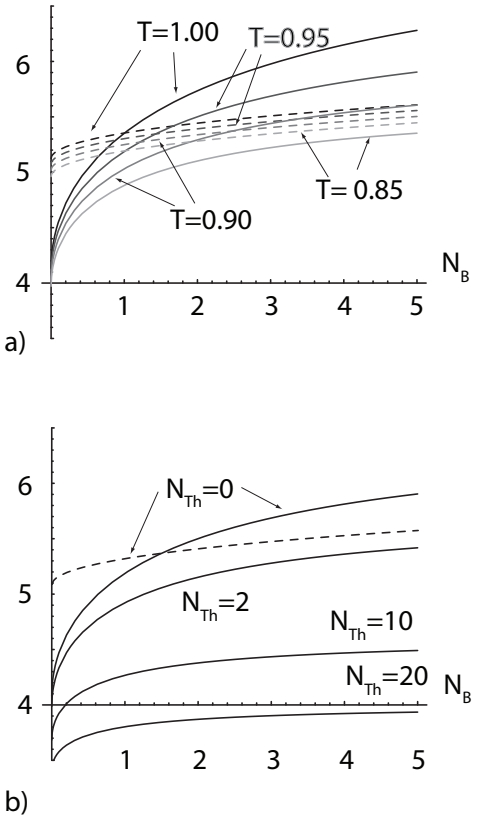
$$R_1^{\Phi_\theta} = g\big(\cos^2\omega(\sin^2\theta N_1 + \cos^2\theta N_2)\big). \tag{3.67}$$

Widzimy, że już straty rzędu 85% prowadzą do zaniku efektu superaddytywności. Rys. 3.9.b) przedstawia zachowanie funkcji $R_1^{szum}(\Phi_\theta \otimes \mathcal{I})$ dla $T_\omega = 0.95$ oraz $N_T = 0; 2; 10; 20$. Efektywnie do stanu splątanego dodawane jest $0; 0.1; 0.5; 1$ fotonów szumu. Prędkość transmisji jest bardzo wrażliwa na ten rodzaj zakłóceń.

Przedyskutujemy teraz możliwość eksperymentalnej weryfikacji efektu aktywacji w kontekście dostępnych obecnie środków technicznych [5, 86]. Dla pomiaru homodynowego przyjmować będziemy efektywność kwantową o wartości $\eta = 99\%$[5] oraz poziom szumu ciemnego o $20dB$ poniżej poziomu szumu śrutowego lokalnego oscylatora. Średnia liczba fotonów przypadająca na transmisję $N_1 = 1000$ pozwala na liniową aproksymację pomiaru homodynowego (średnia liczba fotonów w wiązce pochodzącej od oscylatora lokalnego wynosi zwykle $4{\cdot}10^6$). Największe notowane dotąd wartość ściśnięcie jednomodowego stanu próżni [86] jest rzędu 10 dB (odpowiada to średniej liczbie fotonów 2.025).

Zaczniemy od omówienia układu $\Phi_{MI} \otimes \mathcal{I}$ w świetle wyników raportowanych w pracy [94]. Do realizacji bramki XP_{MI} posłużono się tam stanami ściśniętymi o ściśnięciu rzędu $5.6dB$ oraz detektorami o efektywności kwantowej 98%. W ten sposób uzyskano wartość współczynnika $T_P =$

[5] Zwróćmy uwagę, że w przypadku detekcji homodynowej mamy do czynienia z pomiarem na stanach jasnych, gdzie nie potrzeba rozdzielczości jednofotonowej. Efektywność kwantowa na poziomie $\eta = 99\%$ uzyskuje się m.in. dla fotodiod PIN.



Rysunek 3.9: Prędkość transmisji $R_1^{szum}(\Phi_\theta \otimes \mathcal{I})$ dla $N_1 = 1000$ i $\theta = 0.25$. a) zależność prędkości transmisji od transmitancji T_ω kanału termicznego, prędkość transmisji porównujemy z ograniczeniem górnym na prędkość transmisji stanów produktowych $R_{S_1}^{\Phi_\theta} = g\big(\cos^2\omega(\sin^2\theta N_1 + \cos^2\theta N_2)\big)$; b) zależność prędkości transmisji od średniej liczby fotonów w stanie termicznym N_T dla $T = 0.95$.

$SNR_{wy}/SNR_{we} = 0.4$, gdzie $SNR_{we(wy)}$ jest ilorazem poziomu sygnału do szumu dla wejściowej wiązki sygnałowej (x_1^{we}, p_1^{we}) oraz wyjściowej wiązki wskaźnika (x_2^{wy}, p_2^{wy}). Poziom szumu wprowadzany przez bramkę wynosi $\sigma^2_{XP} = 5$. Wstawiając tą wartość do wzoru (3.64) oraz porównując uzyskany wynik z ograniczeniem związanym ze średnią liczbą fotonów na wyjściu kanału (patrz Rw. (3.54)) nie możemy stwierdzić występowania efektu aktywacji. Z drugiej strony, zastosowanie stanów ściśniętych o ściśnięciu $10dB$ teoretycznie pozwala uzyskać wartość $\sigma^2_{XP} = 0.098$. W tej sytuacji efekt aktywacji występuje.

Bardziej optymistyczne przedstawia się sytuacja dla układu $\Phi_\theta \otimes \mathcal{I}$. Przyjmując realistyczny poziom strat w układzie rzędu 5% oraz przytoczone wyżej parametry detektora homodynowego otrzymujmy $\cos^2\omega = 0.94, N_T = 0.09$. Dla układu z parametrem $\theta = 0.25$ efekt aktywacji pojawia się już dla ściśnięcia dwumodowego rzędu 7.8 dB (średnia liczba fotonów w stanie ściśniętym wynosi 2.1). Pozwala to przypuszczać, że istnieje obecnie możliwość eksperymentalnej weryfikacji łamania zasady lokalności przy użyciu układu $\Phi_\theta \otimes \mathcal{I}$. Ponieważ efekt jest widoczny nawet w przypadku niedoskonałych urządzeń pomiarowych, eksperyment powinien być pozbawiony luk logicznych oraz konieczności postselekcji wyników i statystycznego poprawiania ich jakości.

Na koniec zauważmy jeszcze, że wzory (3.64)-(3.66) pasują do schematu $R = \log(1 + \sigma^2_{sygnal}/\sigma^2_{szum})$. Dzięki zastosowaniu splątania, nadawcy są w stanie manipulować stosunkiem poziomu sygnału do szumu czego rezultatem jest efekt aktywacji. Pojawienie się szumu termicznego wprowadza dolne ograniczenie na wartość σ^2_{szum}.

3.6 Otwarte pytania

Kończąc rozdział dotyczący transmisji informacji klasycznej przez wielodostępne kanały Gaussowskie, warto zwrócić uwagę na kilka istotnych pytań dotyczących tego tematu, które jeszcze nie znalazły odpowiedzi:

- Jakie są formuły na pojemność klasyczną podstawowych kanałów Gaussowskich: kanału termicznego, kanału z szumem klasycznym etc?
- Czy stany Gaussowskie optymalizują pojemność kanałów Gaussowskich?

  Odpowiedź na te dwa pytania wydaje się być kluczowa w zrozumieniu transmisji informacji klasycznej przez kanały Gaussowskie. Pozwoli ona

poprawić jakość oszacowań na pojemność klasyczną przy transmisji stanów produktowych oraz obniżyć wymagania konieczne do spełnienia, aby uzyskać efekt aktywacji (np. ściśnięcie stanów dwumodowych).

- Czy istnieją bardziej naturalne przykłady kanałów, dla których występuje wspomagany splątaniem efekt aktywacji pojemności klasycznej? Na ile efekt ten jest powszechny w kanałach Gaussowskich?

  Odpowiedź na to pytanie może wiązać się z interesującymi aplikacjami w rzeczywistych systemach telekomunikacyjnych.

- Czy istnieją przykłady kanałów Gaussowskich 1-do-1 lub wielodostępnych, dla których występuje efekt aktywacji łącznej prędkości transmisji R_T?

  Warto tu wspomnieć, że w przypadku pojemności kwantowej Q znamy już tego typu wynik dla kanałów 1-do-1 [84].

- Jaki jest wpływ splątania wielocząstkowego na pojemność klasyczną kanałów Gaussowskich?

Dodatek A

Entropia stanu średniego na wyjściu kanału Γ

Poniżej zamieszczony został kod programu w Mathematice, który posłużył w części 2.3.3 do wyznaczenia entropii stanu średniego ρ_π na wyjściu kanału Γ oraz testowania warunku:

$$S(\rho_\pi) = \min(2l, 5), \tag{A.1}$$

gdzie π to lista qbitów stanu $|0_L\rangle$, na których kanał Γ wykonuje jedną z operacji Pauliego; liczba tych qbitów wynosi $l = |\pi|$. Z przeprowadzonych obliczeń wynika, że dla $l = 3$ średni stan ρ_π na wyjściu kanału jest maksymalnie wymieszany, nie ma więc potrzeby sprawdzania warunku dla $l \geq 4$.

Stan średni ρ_π obliczany jest na według formuły:

$$\rho_\pi = \left(\bigotimes_{i=1}^{l} \Lambda_{p=1}^{(\pi_i)} \right) \left[|0_L\rangle\langle 0_L| \right], \tag{A.2}$$

gdzie $\Lambda_{p=1}^{(\pi_i)}$ to 1-qbitowy kanał depolaryzujący wprowadzający szum z prawdopodobieństwem $p = 1$ — kanał ten działa na π_i-ty qbit stanu $|0_L\rangle$.

W przedstawionym programie, do kodowania pozycji wykorzystano rozkłady `cmp` liczby $5 - l$. Zachodzi tu następująca relacja $\pi_i = i + \sum_{l=1}^{i} \mathrm{cmp}_l$. Procedura `getRotatedState[cmp_List, i_,...]` zwraca stan $\rho_{cmp,i,\ldots} = U|0_L\rangle\langle 0_L|U^\dagger$, gdzie $U = \mathrm{I}^{\mathrm{cmp}_1} \otimes \sigma_i \otimes \mathrm{I}^{\mathrm{cmp}_2} \otimes \ldots$. Odpowiada to rotacji stanu $|0_L\rangle$ przez macierze Pauliego $\sigma_i, \sigma_j, \sigma_k$ działające na pozycjach zadanych przez wektor π.

Aby zachować czytelność, przedstawiony poniżej kod nie był optymalizowany. Program korzysta z pakietu „QuCalc" autorstwa Paula Dumais.

```
<< QuCalc‘
<< Combinatorica‘

(*macierze pauliego*)
operators = id[1], sigx, sigy, sigz;

(*slowo kodowe*)
baseState =
  ket[1/4 ( ket["00000"] + ket["10010"] + ket["01001"] +
            ket["10100"] + ket["01010"] - ket["11011"] -
            ket["00110"] - ket["11000"] - ket["11101"] -
            ket["00011"] - ket["11110"] - ket["01111"] -
            ket["10001"] - ket["01100"] - ket["10111"] +
            ket["00101"] )];

(*obracanie slowa kodowego na pozycjach
  okreslonych przez parametr cmp*)

getRotatedState[cmp_List, i_] := Module[{ U, currState},
   U = (id[cmp[[1]]] ⊗ operators[[i]] ⊗ id[cmp[[2]]]);
   currState = U.baseState;
   Return[currState.dag[currState]];
   ];

getRotatedState[cmp_List, i_, j_] := Module[{ U, currState},
   U = (id[cmp[[1]]]⊗ operators[[i]]⊗
        id[cmp[[2]]]⊗ operators[[j]]⊗
        id[cmp[[3]]]);
   currState = U.baseState;
   Return[currState.dag[currState]];
   ];

getRotatedState[cmp_List, i_, j_, k_] := Module[{ U, currState},
   U = (id[cmp[[1]]]⊗ operators[[i]]⊗
        id[cmp[[2]]]⊗ operators[[j]]⊗
```

```
        id[cmp[[3]]]⊗ operators[[k]]⊗
        id[cmp[[4]]]);
   currState = U.baseState;
   Return[currState.dag[currState]];
   ];

(* entropia stanu sredniego w przypadku gdy slowo
        kodowe jest modyfikowane na zadanej liczbie pozycji *)

(* 1 pozycja - 2 bity entropii *)

test = Module[{ cmps, ci, sumState, i},
   cmps = Compositions[4, 2];
   For[ci = 1, ci <= Length[cmps],
    sumState = Sum[ getRotatedState[cmps[[ci]], i],
                    { i, 1, 4 } ]/4;
    Print[cmps[[ci]], "=", entropy[state[sumState]]];
    ci++]
   ];

(* 2 pozycje - 4 bity entropii *)

test = Module[{ cmps, ci, sumState, i, j},
   cmps = Compositions[3, 3];
   For[ci = 1, ci <= Length[cmps],
    sumState = Sum[ getRotatedState[cmps[[ci]], i, j],
                    { i, 1, 4},{ j, 1, 4} ]/16;
    Print[cmps[[ci]], "=", entropy[state[sumState]]];
    ci++]
   ];

(* 3 pozycje - 5 bitow entropii *)

test = Module[{ cmps, ci, sumState, i, j, k},
   cmps = Compositions[2, 4];
   For[ci = 1, ci <= Length[cmps],
    sumState = Sum[ getRotatedState[cmps[[ci]], i, j, k],
                    { i, 1, 4}, { j, 1, 4},
```

```
                { k, 1, 4} ]/64;
 Print[cmps[[ci]], "=", entropy[state[sumState]]];
 ci++]
];
```

Podsumowanie

Omawiane w niniejszej rozprawie problemy skupiają się wokół roli, jaką odegrać może splątanie w transmisji informacji klasycznej przez kwantowe kanały wielodostępne oraz związanego z tym zagadnienia kwantowej aktywacji obszarów pojemności klasycznej.

W rozdziale 2 przedstawione zostały przykłady kanałów kwantowych pokazujące, że efekt aktywacji obszarów pojemności klasycznej faktycznie ma miejsce. Uzyskane wyniki wskazują na dwie zasadniczo różne formy efektu aktywacji w kanałach z wieloma nadawcami: aktywacja typu (i) polegająca na superaddytywności maksymalnej indywidualnej prędkości transmisji R_i dla wybranych nadawców przy zachowaniu addytywności łącznej prędkości transmisji R_T; aktywacja typu (ii) będąca superaddytywnością łącznej prędkości transmisji R_T. W analizowanych przypadkach aktywacja typu (i) wiązała się ze wzrostem zróżnicowania stanów na wyjściu kanału poprzez realizację pewnego rodzaju rozproszonego gęstego kodowania. Aktywacja typu (ii) była natomiast konsekwencją subaddytywności minimalnej entropii wyjścia H_{min}, co pozwala na interpretację tego efektu jako analogu aktywacji w kanałach 1-do-1. Efekt aktywacji wykazany został zarówno w kontekście superaddytywności pojemności Holevo χ jak i superaddywyności regularyzowanej pojemności klasycznej $C^{(\infty)}$. Ponadto pokazany został przykład kanału, w którym do osiągnięcia regularyzowango obszaru pojemności $C^{(\infty)}$ konieczne jest wykorzystanie splątania wielocząstkowego $n > 2$.

Rozdział 3 stanowi studium wykonalności eksperymentów obrazujących efekt aktywacji. Główne wyniki przedstawione w tym rozdziale to dwa przykłady kanałów Gaussowskich: (i) kanał zbudowany w oparciu o dzielnik wiązki oraz (ii) kanał składający się z niedestruktywnych bramek sumacyjnych, przy użyciu których można obserwować efekt aktywacji typu (i). Analiza tych kanałów, uwzględniająca aktualny stan techniki eksperymentalnej z zakresu optyki kwantowej, pozwala przypuszczać, że eksperymenty

pokazujące efekt aktywacji typu (i) są możliwe do przeprowadzania już dziś.

Jak każde badania, również te zostawiają po sobie więcej pytań niż uzyskanych odpowiedzi. Pomimo postępu w zrozumieniu efektu aktywacji obszarów pojemności klasycznej, wiele z omawianych tu zagadnień wymaga dalszej analizy. Na zakończenie chciałbym wskazać kilka otwartych problemów które wydają się najistotniejsze w dalszych badaniach nad efektem aktywacji obszarów pojemności klasycznej.

- Związek aktywacji typu (ii) z subaddytywnością H_{min} — czy te dwa efekty zawsze idą ze sobą w parze?
- Czy występuje aktywacja typu (ii) dla regularyzowanych obszarów pojemności $\mathcal{R}^{(\infty)}$?
- Czy efekt aktywacji typu (ii) ma miejsce dla kanałów Gaussowskich, a jeśli tak, to jak wygląda eksperyment obrazujący ten efekt?
- Czy istnieją naturalne przykłady kanałów optycznych, dla których zachodzi efekt aktywacji? Pytanie to ma szczególnie istotne znaczenie w kontekście światłowodowych sieci komunikacyjnych.

Bibliografia

[1] G. S. Agarwal. *Phys. Rev. A*, 828(3), 1971.

[2] R. Ahlswede. *in 2nd Int. Symp. Inf. Th., (Tsahkadsor, Armenia)*, 1971.

[3] A. E. Allahverdyan, D. B. Saakian. *Quantum computing and quantum communications*. Springer, Berlin, 1999.

[4] O. Goldreich B. Chor. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[5] H. A. Bachor, T. C. Ralph. *A Guide to Experiments in Quantum Optics*. WILEY-VCH, Weinheim, 2004.

[6] M. Ban. *J. Opt. B: Quantum Semiclass. Opt.*, L9(1), 1999.

[7] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, A. Wigderson. *In Proc. 37th STOC. ACM*, 2005.

[8] H. Barnum, E. Knill, M.A. Nielsen. *IEEE Trans. Inf. Th.*, 19(46), 2000.

[9] H. Barnum, M.A. Nielsen, B. Schumacher. *Phys. Rev. A*, 4153(57), 1998.

[10] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, K. Nemoto. *Phys. Rev. Lett.*, 097904(88), 2002.

[11] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. Wootters. *Phys. Rev. Lett.*, 70(1895), 1993.

[12] C. H. Bennett, C. A. Fuchs, J. A. Smolin. Entanglement enhanced classical communication on a noisy quantum channel. *Quantum Communication, Computing and Measurment, Proc. QCM96*, pages 79–88, 1997.

[13] C. H. Bennett, P. W. Shor. Quantum information theory. *IEEE Trans. Inf. Th.*, (44), 1999.

[14] C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal. *IEEE Trans. Inf. Th.*, 2637(48), 2002.

[15] C. H. Bennett, D. P. DiVincenzo J. A. Smolin, W. K. Wootters. *Phys. Rev. A*, 3824(54), 1996.

[16] C. H. Bennett, S. J. Wiesner. *Phys. Rev. Lett.*, 2881(69), 1997.

[17] A. Botero, B. Reznik. *Phys. Rev. A*, 052311(67), 2003.

[18] H. Bourdoucen, A. Alhabs. *International Journal of Electrical and Computer Engineering*, 13(4), 2009.

[19] S. L. Braunstein, H.J. Kimble. *Phys. Rev. A*, 61(042302), 2000.

[20] H-P Breuer, F. Petruccione. *THE THEORY OF OPEN QUANTUM SYSTEMS*. Oxford University Press, Oxford, 2003.

[21] N. Cai, A. Winter, R. W. Yeung. *Problems of Information Transmission*, 40(4), 2004.

[22] J. Calsamiglia, N. Lutkenhaus. *Appl. Phys. B*, 67(72), 2001.

[23] C. M. Caves, P. D. Drummond. *Rev. Mod. Phys.*, 66(2), 1994.

[24] T. Cover, R. J. McEliece, E. C. Posner. *IEEE Trans. Inf. Th.*, 27, 1981.

[25] T. M. Cover, J.M. Thomas. *Elements of Information Theory*. Wiley & Sons, New York, 1991.

[26] J. Crisp, B Elliott. *Introduction to Fiber Optics*. Elsevier, Oxford, 2005.

[27] L. Czekaj. *Phys. Rev. A*, 042304(83), 2011.

[28] L. Czekaj, P. Horodecki. *Phys. Rev. Lett.*, 110505(102), 2009.

[29] L. Czekaj, J. K. Korbicz, R. W. Chhajlany, P. Horodecki. *Phys. Rev. A*, 020302(R)(82), 2010.

[30] L. Czekaj, J. K. Korbicz, R. W. Chhajlany, P. Horodecki. *arXiv:quant-ph/1110.2594*, 2011.

[31] N. Datta, M. B. Ruskai. *J. Phys. A: Math. Gen.*, 3, 2005.

[32] A. Sen De, B. Gromek, D. Bruss, M. Lewenstein. *Phys. Rev. Lett.*, 260503(95), 2005.

[33] A. Sen De, B. Gromek, D. Bruss, M. Lewenstein. *Phys. Rev. A*, 022331(75), 2007.

[34] I. Devetak. *IEEE Trans. Inf. Th.*, 51(1), 2005.

[35] R. H. Dicke. *Phys. Rev.*, 99(93), 1954.

[36] W. Dur, J. I. Cirac, P. Horodecki. *Phys. Rev. Lett.*, 020503(93), 2004.

[37] H. J. R. Dutton. *Understanding Optical Communications.* IBM Corporation, International Technical Support Organization, http://www.redbooks.ibm.com, 1998.

[38] J. Edmonds. *in Proc. Calgary Int. Conf. on Combinatorial structures and appl., Calgart, Alberta*, 1969.

[39] A. A. Abou El-Fadl, G. E. Elabiad, SH. M. Eladl, M.S.I. Rageh. *16tb National Radio Science Conference, Ain Shams Uaiversity, Cairo, Egypt*, 1999.

[40] R. Filip, P. Marek, U.L. Andersen. *Phys. Rev. A*, 042308(71), 2005.

[41] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik. *Science*, 706(282), 1998.

[42] C. W. Gardiner, P. Zoller. *Quantum Noise, A Handbook of Markovian and Non-Markovian Quantum Stochastic Methods with Applications to Quantum Optics.* Springer, Berlin, 2000.

[43] C. C. Gerry, P. L. Knight. *Introductory Quantum Optics.* Cambridge University Press, Cambridge, 2005.

[44] S. Ghosh, G. Kar, A. Roy, A. Sen(De), U. Sen. *Phys. Rev. Lett.*, 277902(87), 2001.

[45] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, H. P. Yuen. *Phys. Rev. Lett.*, 92(027902), 2004.

[46] J. P. Gordon. *Proc. IRE*, 1898(50), 1962.

[47] A. Grudka, P. Horodecki. *Phys. Rev. A*, 060305(R)(81), 2010.

[48] S. Hanly, P. Whiting. *in Proc. IEEE Int. Symp. on Inf. Th., (Trondheim, Norway)*, 1994.

[49] M. B. Hastings. *Nature Physics*, 255(5), 2009.

[50] K. Hellwig, K. Kraus. *Comm. Math. Phys.*, 142(16), 1970.

[51] C. W. Helstrom. *Journal of Statistical Physics*, (1), 1969.

[52] A. S. Holevo. *Probl. Inf. Transm.*, 110(9), 1973.

[53] A. S. Holevo. *IEEE Trans. Inf. Th.*, 269(44), 1998.

[54] A. S. Holevo. *Russ. Math. Surveys*, 1295(53), 1998.

[55] A. S. Holevo. The additivity problem in quantum information theory. *Proceedings of the International Congress of Mathematicians, Madrid, Spain*, 2006.

[56] A. S. Holevo, M. E. Shirokov. pages arXiv:quant–ph/0408176, 2004.

[57] A. S. Holevo, M. Sohma, O. Hirota. *Phys. Rev. A*, 1820(59), 1999.

[58] M. Horodecki, P. W. Shor, M. B. Ruskai. *Rev. Math. Phys.*, 629(15), 2003.

[59] P. Horodecki, M. Horodecki, R. Horodecki. *Phys. Rev. Lett.*, 1056(82), 1999.

[60] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki. *Rev. Mod. Phys.*, (81), 2009.

[61] R. Jodoin, L. Mandel. *JOSA*, 61(2), 1971.

[62] C. King. *J. Math. Phys.*, 4641(43), 2002.

[63] C. King. The capacity of the quantum depolarizing channel. *arXiv:quant-ph/0204172*, 2002.

[64] E. Knill, R. Laflamme, G. J. Milburn. *Nature*, 46(409), 2001.

[65] L. B. Levitin. *in Proceedings of the Fourth All-Union Conference on Information Theory, Tashkent*, 1969.

[66] K. Li, A. Winter, X-B Zou, G-C Guo. *Phys. Rev. Lett.*, 120501(103), 2009.

[67] H. Liao. *Multiple access channels, PhD thesis.* University of Hawaii, Honolulu, 1972.

[68] N. Lutkenhaus, J. Calsamiglia, K.-A. Suominen. *Phys. Rev. A*, 3295(59), 1999.

[69] J. L. Massey, P. Mathys. *IEEE Trans. Inf. Th.*, 31, 1985.

[70] M. Mattas, P.R.J. Ostergard. *IEEE Trans. Inf. Th.*, 51(9), 2005.

[71] J. M. Myers. *arXiv:quant-ph/0411107; 0411108.*

[72] M. A. Nielsen, I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[73] M. G. A. Paris. *Phys. Lett. A*, 78(217), 1996.

[74] R. Raussendorf, H. J. Briegel. *Phys. Rev. Lett.*, 5188(86), 2001.

[75] B. Schumacher, M. Westmoreland. *Phys. Rev. A*, 131(56), 1997.

[76] B. Schumacher, M. D. Westmoreland. Relative entropy in quantum information theory. *in proc. AMS special session on Quantum Information and Computation*, 2000.

[77] C. E. Shannon. *Bell System Technical Journal*, (27), 1948.

[78] C. Y. She. *IEEE Trans. Inf. Th. IT*, 32(14), 1968.

[79] P. W. Shor. *J. Math. Phys.*, 43(4334).

[80] P. W. Shor. *arXiv:quant-ph/0304102*, 2003.

[81] P. W. Shor. *Comm. Math. Phys.*, (246), 2004.

[82] P. W. Shor, J. A. Smolin, B. M. Terhal. *Phys. Rev. Lett.*, 2681(86), 2001.

[83] D. Slepian, J. K. Wolf. *Bell System Technical Journal*, 52, 1973.

[84] G. Smith, J.A. Smolin, J. Yard. *arXiv:quant-ph/1102.4580*, 2011.

[85] H. Takahashi. Information theory of quantum-mechanical channels. In A.V. Balakrishnan, editor, *Advances in Communication Systems*, volume 227, Orlando FL, 1965. Academic Press.

[86] H. Vahlbruch, M. Mehmet, S. Chelkowski, B. Hage, A. Franzen, N. Lastzka, S. Gossler, K. Danzmann, R. Schnabel. *Phys. Rev. Lett.*, 033602(100), 2008.

[87] L. Vaidman, N. Yoran. *Phys. Rev. A*, 116(59), 1999.

[88] X-B Wang, T. Hiroshima, A. Tomita, M. Hayashi. *Phys. Rep.*, 448(1), 2007.

[89] E. P. Wigner. *Phys. Rev.*, 794(40), 1932.

[90] M. M. Wilde. *From Classical to Quantum Shannon Theory.* 2011.

[91] Y. Yamamoto, H.A. Haus. *Rev. Mod. Phys.*, 1001(58), 1986.

[92] G. Yard, J. Smith. *Science*, 182(321), 2008.

[93] B. J. Yen, J. H. Shapiro. *Phys. Rev. A*, 062312(72), 2005.

[94] J. Yoshikawa, Y. Miwa, A. Huck, U. L. Andersen, P. van Loock, A. Furusawa. *Phys. Rev. Lett.*, 250501(101), 2008.

[95] B. Yurke, D. Stoler. *Phys. Rev. Lett.*, 68(1251), 1992.

[96] M. Zukowski A. Zeilinger, M. A. Horne, A. Ekert. *Phys. Rev. Lett.*, 71(4287), 1993.

[97] G. M. Ziegler. *Lectures on polytopes.* Springer, New York, 1995.

[98] D. Zuckerman. *In Proc. 31st IEEE symposium on Foundations of Computer Science*, pages 534–543, 1990.