Uniwersytet im. Adama Mickiewicza
w Poznaniu

Wydział Fizyki

Praca Doktorska

Destylacja splątania ze stanów mieszanych o niepełnym rzędzie macierzy gęstości

Mikołaj Czechlewski

Promotor pracy

Prof. UAM dr hab. Andrzej Grudka

Zakład Elektroniki Kwantowej, Wydział Fizyki UAM

Poznań 2012

Oświadczenie

Ja niżej podpisany **Mikołaj Czechlewski** uczestnik studiów doktoranckich na Wydziale Fizyki Uniwersytetu im. Adama Mickiewicza w Poznaniu oświadczam, że przekładaną pracę doktorską pt. *Destylacja splątania ze stanów mieszanych o niepełnym rzędzie macierzy gęstości* napisałem samodzielnie. Oznacza to, że przy pisaniu pracy, poza niezbędnymi konsultacjami, nie korzystałem z pomocy innych osób, a w szczególności nie zlecałem opracowania rozprawy lub jej istotnych części innym osobom, ani nie odpisywałem tej rozprawy lub jej istotnych części od innych osób.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Równocześnie wyrażam zgodę na to, że gdyby powyższe oświadczenie okazało się nieprawdziwe, decyzja o wydaniu mi dyplomu zostanie cofnięta.

Podziękowania

Na powstanie i ostateczny kształt mojej pracy doktorskiej miało wpływ wiele osób, którym chciałbym w tym miejscu podziękować.

Jako pierwszemu dziękuję mojemu promotorowi Prof. UAM dr. hab. Andrzejowi Grudce za całą przekazaną mi przez te lata wiedzę oraz wszelką pomoc. Składają się na nią między innymi: niezliczone godziny konsultacji, setki zapisanych czerwonym długopisem stron kolejnych wersji tej pracy, megabajty klasycznej informacji przesyłanej pomiędzy nami za pomocą Internetu oraz wiele minut rozmów telefonicznych.

Chciałbym również podziękować Prof. UG dr. hab. Michałowi Horodeckiemu i Mgr. Michałowi Studzińskiemu z Uniwersytetu Gdańskiego, za zainteresowanie się problematyką mojej pracy doktorskiej, które z czasem przerodziło się w owocną współpracę. Dzięki niej nie tylko znacząco rozwinąłem moją pracę, lecz również poznałem i zachwyciłem się pięknem teorii grup.

Prof. UAM dr. hab. Antoniemu Wójcikowi chcę podziękować za współpracę i całą udzieloną mi pomoc podczas narodzin tematyki mojej pracy doktorskiej. Dziękuję Jemu również za jej pierwszą recenzję.

Osobne, równie ważne, podziękowania składam na ręce mojej żony Iwony, na którą zawsze mogłem liczyć, która mnie wspierała i niejednokrotnie odciążała mnie w moich obowiązkach domowych oraz rodzicielskich. Słowa podziękowania należą się także moim rodzicom i teściom, którzy także mnie wspierali duchowo i materialnie.

Adulescentia est tempus discendi, sed nulla aetas sera est ad discendum.

Mojej Rodzinie

Streszczenie

W niniejszej pracy doktorskiej przedstawiono nowy protokół destylacji splątania. Jest on oparty na metodzie bisekcji i w niektórych przypadkach wykorzystuje jednokierunkowy protokół haszujący. Protokół ten zastosowano do następujących dwuqubitowych stanów splątanych: a) stanu mieszanego składającego się z czystego stanu splątanego i ortogonalnego do niego czystego stanu produktowego; b) stanu mieszanego składającego się z dwóch czystych stanów splątanych różniących się fazą i ortogonalnego do nich czystego stanu produktowego; c) stanu mieszanego składającego się z czystego stanu splątanego i dwóch czystych stanów produktowych (wszystkie stany są wzajemnie ortogonalne). Pokazano, że w przypadku stanów z punktów a) i b) protokół ten zawsze pozwala wydestylować splątanie, a w przypadku stanów z punktu c) protokół ten pozwala wydestylować splątanie dla pewnego zakresu parametrów charakteryzujących stany. Protokół ten porównano z innymi szeroko stosowanymi protokołami i pokazano, że w zastosowaniu do wymienionych stanów jest on od nich na ogół efektywniejszy. Wykorzystując zaproponowany protokół, znaleziono dolne ograniczenie na asystowaną klasyczną komunikacją w dwie strony kwantową pojemność następujących kanałów kwantowych: a) kanału tłumiącego amplitudę; b) kanału tłumiącego amplitudę i zmieniającego fazę; c) uogólnionego kanału tłumiącego amplitudę.

Abstract

In this thesis we presented new entanglement distillation protocol. It is based on bisection method and in some cases it uses one-way hashing protocol. The protocol was applied to the following two-qubit entangled states: a) mixed state which consists of pure entangled state and orthogonal pure product state; b) mixed state which consists of two pure entangled states with different phases and orthogonal pure product state; c) mixed state which consists of pure entangled state and two pure product states (all states are mutually orthogonal). It was shown that in the case of states from points a) and b) the protocol always enables to distill entanglement and in the case of states from point c) it enables to distill entanglement for certain range of parameters characterising those states. The protocol was compared with other widely used protocols and it was shown that in the case of mentioned states it is usually more effective. Using the proposed protocol, we found lower bound on quantum capacity assisted by two-way classical communication of the following quantum channels: a) amplitude damping channel; b) amplitude damping and phase-flip channel; c) generalised amplitude damping channel.

Spis treści

ROZDZIAŁ 1

Wstęp

Podstawowym zasobem w komunikacji kwantowej jest splątanie [1]. Ma ono zastosowanie między innymi w tak ważnych protokołach jak protokół teleportacji kwantowej [2], protokół gęstego kodowania [3], czy protokół kryptograficzny Ekerta [4]. Wszystkie one wykorzystują stany maksymalnie splątane dzielone przez parę użytkowników. Niestety uzyskanie stanów maksymalnie splątanych (lub stanów im bliskich) jest w warunkach laboratoryjnych zadaniem trudnym. Na skutek nieuniknionego oddziaływania ze środowiskiem, stan kwantowy – a w szczególności zawarte w nim splątanie – dekoheruje. W efekcie para użytkowników zamiast czystych stanów maksymalnie splątanych (nawet jeśli zostały one początkowo przygotowane) otrzymuje mieszane stany splątane lub stany separowalne. Rodzi się więc potrzeba ochrony splątania przed dekoherencją. Jedną z możliwych metod jest zakodowanie stanów maksymalnie splątanych za pomocą kwantowego kodu korekcji błędów [5, 6]. Istnieje jednak druga, bardziej efektywna metoda, którą jest destylacja splątania [7, 8, 9]. W tym celu dwoje użytkowników, którzy współdzielą wiele kopii mieszanych stanów splątanych, przekształca je za pomocą lokalnych operacji kwantowych w mniejszą liczbę kopii stanów maksymalnie splątanych (lub stanów im bliskich). Użytkownicy ci mogą dodatkowo komunikować się klasycznie w celu skorelowania operacji, które wykonują. Niestety nie jest znany uniwersalny protokół destylacji splątania, który byłby optymalny dla wszystkich stanów (to znaczy pozwalałby wydestylować z nich maksymalną ilość splątania). Praktycznie dla różnych klas stanów różne protokoły okazują się efektywne. Co więcej, tylko w pojedynczych przypadkach udowodniono, że dany protokół jest optymalny.

W niniejszej pracy doktorskiej przedstawimy nowy protokół destylacji splątania. Jest

on oparty na metodzie bisekcji i w niektórych przypadkach wykorzystuje jednokierunkowy protokół haszujący. Protokół ten zastosujemy do następujących dwuqubitowych stanów splątanych:

a) stanu mieszanego składającego się z czystego stanu splątanego i ortogonalnego do niego czystego stanu produktowego,

b) stanu mieszanego składającego się z dwóch czystych stanów splątanych różniących się fazą i ortogonalnego do nich czystego stanu produktowego,

c) stanu mieszanego składającego się z czystego stanu splątanego i dwóch czystych stanów produktowych (wszystkie stany są wzajemnie ortogonalne).

Pokażemy, że w przypadku stanów z punktów a) i b) protokół ten zawsze pozwala wydestylować splątanie, a w przypadku stanów z punktu c) protokół ten pozwala wydestylować splątanie dla pewnego zakresu parametrów charakteryzujących te stany. Dodajmy jednak, że dla stanów z punktu c) istnieje również zakres parametrów, dla których protokół ma zerową wydajność mimo, że stany te zawierają destylowalne splątanie. Protokół ten porównamy z innymi szeroko stosowanymi protokołami destylacji splątania, takimi jak jednokierunkowy protokół haszujący czy protokół rekurencyjny. Pokażemy, że w zastosowaniu do wymienionych stanów jest on od nich na ogół efektywniejszy.

Wykorzystamy również zaproponowany protokół do znalezienia dolnego ograniczenia na asystowaną klasyczną komunikacją w dwie strony kwantową pojemność następujących kanałów kwantowych:

a) kanału tłumiącego amplitudę,

b) kanału tłumiącego amplitudę i zmieniającego fazę,

c) uogólnionego kanału tłumiącego amplitudę.

Na koniec dodajmy, że prawie wszystkie wyniki otrzymamy w sposób analityczny, wykorzystując wiedzę z rachunku prawdopodobieństwa, kombinatoryki i teorii grup.

ROZDZIAŁ 2

Podstawowe wiadomości teoretyczne

2.1 Kanały kwantowe

Kanałem kwantowym nazywamy liniowe, kompletnie dodatnie odwzorowanie zachowujące ślad, które odwzorowuje operator gęstości w operator gęstości. Oznaczmy przez ρ stan wejściowy kanału, przez $\mathcal{N}(\rho)$ stan wyjściowy, natomiast przez ρ_E stan środowiska (rysunek 2.1). Zakładamy, że stan wejściowy i stan środowiska są początkowo w stanie produktowym $\rho \otimes \rho_E$. Niech U oznacza operację unitarną działającą na przestrzeni zawierającej stan wejściowy i stan środowiska. Wtedy działanie kanału możemy wyrazić następująco

$$\mathcal{N}(\rho) \;=\; \mathrm{Tr}_E(U(\rho \otimes \rho_E)U^\dagger)\ . \tag{2.1}$$

Oznaczmy przez $|e_k\rangle$ ortonormalną bazę w przestrzeni Hilberta opisującą środowisko [10]. Dodatkowo, bez straty ogólności załóżmy, że wejściowy stan środowiska jest stanem czystym postaci

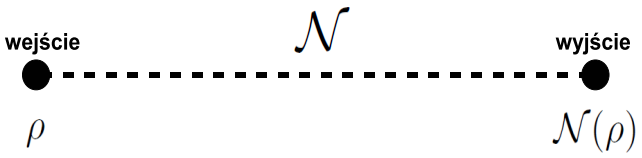
$$\rho_E \;=\; |e_0\rangle\langle e_0|\ , \tag{2.2}$$

wtedy wzór 2.1 możemy zapisać

$$\mathcal{N}(\rho) \;=\; \sum_k \langle e_k|\,(U(\rho \otimes |e_0\rangle\langle e_0|)U^\dagger)\,|e_k\rangle = \tag{2.3}$$

$$= \sum_k E_k \rho E_k^\dagger\ , \tag{2.4}$$

gdzie operatory $E_k = \langle e_k|\,U\,|e_0\rangle$ nazywamy operatorami Krausa. Działają one tylko na przestrzeni stanu wejściowego. Co więcej, ponieważ kanał kwantowy musi zachowywać



Rysunek 2.1: Kanał kwantowy.

ślad, mamy

$$1 \;=\; \mathrm{Tr}(\mathcal{N}(\rho)) = \mathrm{Tr}(\sum_k E_k \rho E_k^\dagger) = \mathrm{Tr}(\sum_k E_k^\dagger E_k \rho) \;. \tag{2.5}$$

Powyższy wzór musi być prawdziwy dla każdego ρ. Stąd operatory E_k spełniają warunek

$$\sum_k E_k^\dagger E_k \;=\; I \;. \tag{2.6}$$

Wyróżniamy kilka klas kanałów kwantowych. Najważniejszymi z nich są:

- kanały niszczące splątanie (ang. *entanglement breaking channels*) [11],
- kanały wiążące splątanie (ang. *entanglement binding channels*) [12],
- kanały degradowalne (ang. *degradable channels*) [13].

Jeżeli przez kanał niszczący splątanie prześlemy jedną cząstkę z dowolnego dwucząstkowego stanu splątanego to stan końcowy dwóch cząstek będzie stanem separowalnym. Bardziej złożona sytuacja nastąpi, gdy tę samą czynność wykonamy za pomocą kanału wiążącego splątanie. Wtedy stan końcowy dwóch cząstek będzie stanem o związanym splątaniu lub stanem separowalnym, przy czym dla pewnych wyborów stanów początkowych musi to być stan o związanym splątaniu (w przeciwnym wypadku kanał ten byłby kanałem łamiącym splątanie). Stan o związanym splątaniu to taki, który zawiera w sobie splątanie, którego nie możemy z niego wydestylować. Destylowalne splątanie dla takich stanów jest więc równe zero.

Zatrzymajmy się dłużej przy kanałach degradowalnych. Są one z naszego punktu widzenia najbardziej interesujące, gdyż do tej klasy kanałów należy rozważany przez nas

w dalszej części pracy kanał tłumiący amplitudę. W celu dokładnego podania definicji kanału degradowalnego wprowadźmy następujące oznaczenia: przez H_A oznaczmy przestrzeń Hilberta stanów wejściowych, przez H_B przestrzeń Hilberta stanów wyjściowych, a przez H_E przestrzeń środowiska. Kanał $\mathcal{N}$ jest odwzorowaniem przestrzeni Hilberta H_A w przestrzeń Hilberta H_B, którego działanie na stan ρ jest dane wzorem 2.1

$$\mathcal{N}(\rho) \quad : \quad H_A \rightarrow H_B \ . \tag{2.7}$$

Zdefiniujmy teraz kanał dualny, który jest odwzorowaniem z przestrzeni Hilberta H_A do przestrzeni Hilberta H_E

$$\mathcal{N}^c(\rho) : H_A \rightarrow H_E, \tag{2.8}$$

którego działanie na stan ρ jest dane wyrażeniem

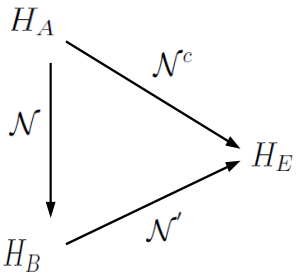
$$\mathcal{N}^c(\rho) = \mathrm{Tr}_B(U(\rho \otimes \rho_E)U^\dagger) \ . \tag{2.9}$$

Teraz możemy podać definicję kanału degradowalnego. Kanał $\mathcal{N}$ nazywamy degradowalnym, jeżeli istnieje taki kanał

$$\mathcal{N}^{'}(\rho) \quad : \quad H_B \rightarrow H_E, \tag{2.10}$$

że spełniony jest warunek (rysunek 2.2)

$$\mathcal{N}^c(\rho) = (\mathcal{N}^{'} \circ \mathcal{N})(\rho) \ . \tag{2.11}$$



Rysunek 2.2: Schemat przejścia pomiędzy przestrzeniami Hilberta H_A, H_B oraz H_E na skutek działania kanałów $\mathcal{N}$, $\mathcal{N}^{'}$ i $\mathcal{N}^c$.

W kolejnych pięciu podrozdziałach opiszemy interesujące nas kanały kwantowe. Oprócz podania dla każdego z nich formalnej postaci operatorów Krausa, przedstawimy ich działanie na qubit ze sfery Blocha.

2.1.1 Kanał tłumiący amplitudę

Kanał tłumiący amplitudę (ang. *amplitude damping channel*) jest jednym z podstawowych kanałów kwantowych, którego laboratoryjnym przykładem jest światłowód. Jego parametrem jest stopień tłumienia, który oznaczymy przez γ. Brak fotonu w światłowodzie jest reprezentowany stanem $|0\rangle$, a obecność fotonu stanem $|1\rangle$. Działanie kanału tłumiącego amplitudę możemy wyjaśnić w taki sposób: z prawdopodobieństwem γ foton emitowany jest do środowiska, natomiast z prawdopodobieństwem $1-\gamma$ foton pozostaje w światłowodzie. Formalny zapis tego kanału w postaci operatorów Krausa jest następujący

$$E_0^{\mathsf{ad}} = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1| \ , \tag{2.12}$$

$$E_1^{\mathsf{ad}} = \sqrt{\gamma}\,|0\rangle\langle 1| \ . \tag{2.13}$$

Poniżej zilustrowano zmianę stanu pojedynczego qubitu ze sfery Blocha (zapisanego w postaci macierzy gęstości)

$$\begin{aligned} |\lambda\rangle\langle\lambda| &= \cos^2\frac{\theta}{2}\,|0\rangle\langle 0| + \sin^2\frac{\theta}{2}\,|1\rangle\langle 1| + \\ &+ e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|0\rangle\langle 1| + e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|1\rangle\langle 0| \ , \end{aligned} \tag{2.14}$$

po przejściu przez opisywany kanał. Na wyjściu stan kanału będzie miał postać

$$\begin{aligned} \rho_{\mathsf{ad}} &= (\cos^2\frac{\theta}{2} + \gamma\sin^2\frac{\theta}{2})\,|0\rangle\langle 0| + (1-\gamma)\sin^2\frac{\theta}{2}\,|1\rangle\langle 1| + \\ &+ (\sqrt{1-\gamma})e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|0\rangle\langle 1| + \\ &+ (\sqrt{1-\gamma})e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|1\rangle\langle 0| \ . \end{aligned} \tag{2.15}$$

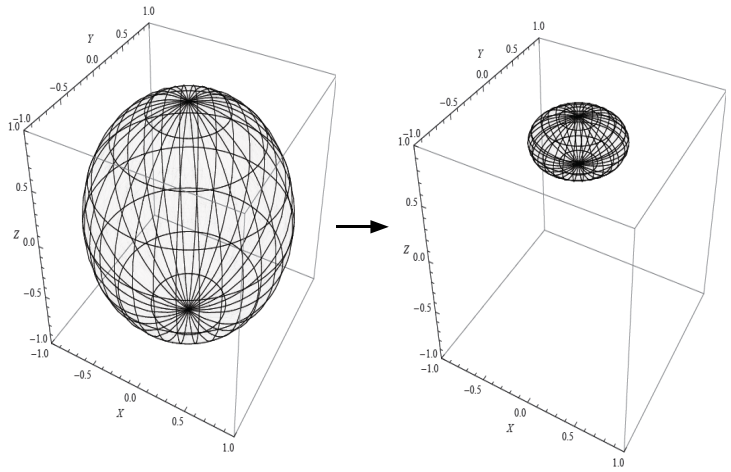
Ze wzoru 2.15 otrzymujemy, że współrzędne sfery Blocha transformują się następująco

$$\begin{aligned} r_x &\to r_x\sqrt{1-\gamma} \ , \\ r_y &\to r_y\sqrt{1-\gamma} \ , \\ r_z &\to \gamma + r_z(1-\gamma) \ , \end{aligned} \tag{2.16}$$

gdzie

$$\begin{aligned} r_x &= \sin(\theta)\cos(\varphi) \ , \\ r_y &= \sin(\theta)\sin(\varphi) \ , \\ r_z &= \cos(\theta) \ . \end{aligned} \tag{2.17}$$

Wizualizacja powyższej transformacji dla parametru tłumienia $\gamma = 0,8$ została przedstawiona na rysunku 2.3. Widać na nim, że sfera Blocha zostaje ściśnięta, a jej środek przesunięty w kierunku górnej części osi Z.



Rysunek 2.3: Działanie kanału tłumiącego amplitudę na sferę Blocha dla parametru $\gamma = 0,8$.

2.1.2 Uogólniony kanał tłumiący amplitudę

Działanie uogólnionego kanału tłumiącego amplitudę (ang. *generalized amplitude damping channel*) charakteryzują dwa parametry tłumienia γ oraz ξ. Dla tego kanału wyróżniamy trzy operatory Krausa, które mają postać

$$E_0^{\mathsf{gad}} = \sqrt{1-\xi}\,|0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1| \ , \tag{2.18}$$

$$E_1^{\mathsf{gad}} = \sqrt{\xi}\,|1\rangle\langle 0| \ , \tag{2.19}$$

$$E_2^{\mathsf{gad}} = \sqrt{\gamma}\,|0\rangle\langle 1| \ . \tag{2.20}$$

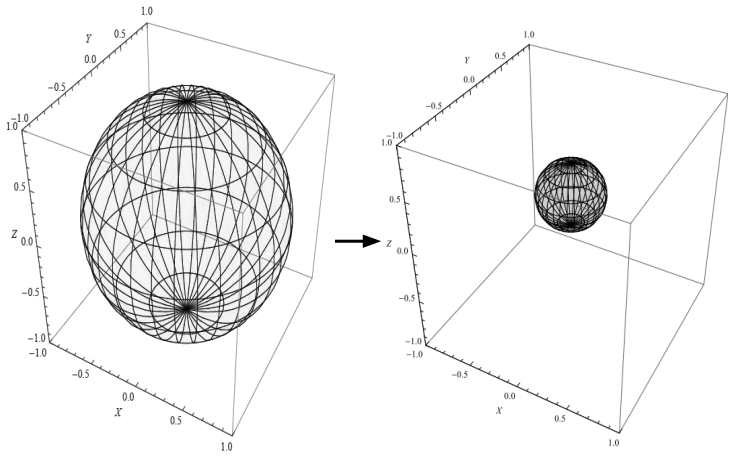
Przykład działania uogólnionego kanału tłumiącego amplitudę przedstawiony został dla stanu 2.14. W takim przypadku na wyjściu otrzymamy stan

$$\begin{aligned} \rho_{\mathsf{gad}} &= ((1-\xi)\cos^2\frac{\theta}{2} + \gamma\sin^2\frac{\theta}{2})\,|0\rangle\langle 0| + \\ &+ (\xi\cos^2\frac{\theta}{2} + (1-\gamma)\sin^2\frac{\theta}{2})\,|1\rangle\langle 1| + \\ &+ \sqrt{1-\xi}\sqrt{1-\gamma}e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|0\rangle\langle 1| + \\ &+ \sqrt{1-\xi}\sqrt{1-\gamma}e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|1\rangle\langle 0| \ . \end{aligned} \tag{2.21}$$

Natomiast współrzędne Blocha transformują się następująco

$$\begin{aligned} r_x &\to r_x\sqrt{1-\gamma}\sqrt{1-\xi}\ , \\ r_y &\to r_y\sqrt{1-\gamma}\sqrt{1-\xi}\ , \\ r_z &\to r_z(1-\xi-\gamma)+\gamma-\xi\ , \end{aligned} \tag{2.22}$$

co zostało przedstawione na rysunku 2.4. Podobnie jak w przypadku kanału tłumiącego amplitudę sfera Blocha zostaje ściśnięta i przesunięta.



Rysunek 2.4: Działanie uogólnionego kanału tłumiącego amplitudę na sferę Blocha dla parametrów $\xi = 0,5$ oraz $\gamma = 0,8$.

2.1.3 Kanał zmieniający bit

Kolejnym ważnym kanałem kwantowym, który omówimy, jest kanał zmieniający bit (ang. *bit flip channel*). Działanie tego kanału należy interpretować następująco: z prawdopodobieństwem $1 - \delta$ qubit pozostanie niezmieniony, natomiast z prawdopodobieństwem δ do qubitu zostanie zastosowana operacja Pauliego X. Wobec tego operatory Krausa dla tego kanału mają postać

$$E_0^{\mathsf{bf}} = \sqrt{1-\delta}(|0\rangle\langle 0| + |1\rangle\langle 1|)\ , \tag{2.23}$$

$$E_1^{\mathsf{bf}} = \sqrt{\delta}(|0\rangle\langle 1| + |1\rangle\langle 0|). \tag{2.24}$$

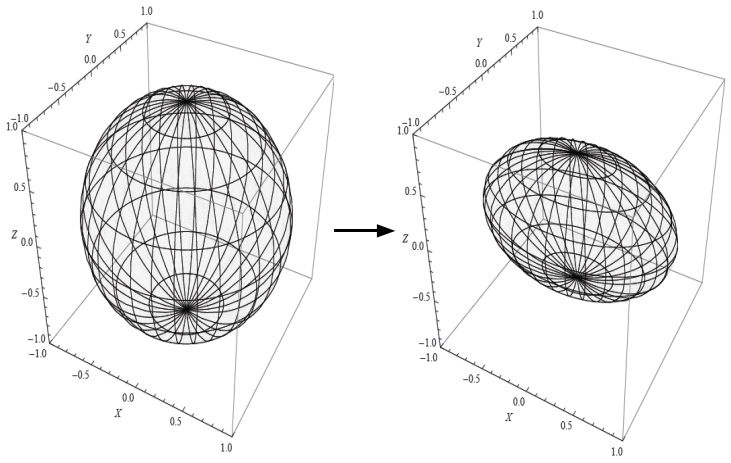
Qubit, który na wejściu tego kanału jest w stanie 2.14, na wyjściu tego kanału będzie znajdował się w stanie

$$\begin{aligned}\rho_{\mathsf{bf}} &= (1-\delta)\Big(\cos^2\frac{\theta}{2}|0\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| + \\ &+ e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|0\rangle\langle 1| + e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|1\rangle\langle 0|\Big) + \\ &+ \delta\Big(\cos^2\frac{\theta}{2}|1\rangle\langle 1| + \sin^2\frac{\theta}{2}|0\rangle\langle 0| + \\ &+ e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|1\rangle\langle 0| + e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|0\rangle\langle 1|\Big)\ .\end{aligned} \tag{2.25}$$

Natomiast poniższe wzory przedstawiają, jak transformują współrzędne sfery Blocha

$$\begin{aligned} r_x &\rightarrow r_x \ , \\ r_y &\rightarrow r_y(1-2\delta) \ , \\ r_z &\rightarrow r_z(1-2\delta) \ . \end{aligned} \tag{2.26}$$

Kanał zmieniający bit powoduje ściśnięcie sfery Blocha wzdłuż osi Y i Z o czynnik $1-2\delta$ (rysunek 2.5).



Rysunek 2.5: Działanie kanału zmieniającego bit na sferę Blocha dla parametru $\delta = 0,2$.

2.1.4 Kanał zmieniający fazę

Kanał zmieniający fazę (ang. *phase flip channel*) jest podobny do kanału zmieniającego bit. Różnica pomiędzy tymi kanałami polega na tym, że w przypadku kanału zmieniającego fazę z prawdopodobieństwem $1-\eta$ qubit pozostaje niezmieniony, a z prawdopodobieństwem η do qubitu zostaje zastosowana operacja Pauliego Z. Poniżej przedstawiono operatory Krausa opisujące ten kanał

$$E_0^{\mathsf{pf}} = \sqrt{1-\eta}(|0\rangle\langle 0| + |1\rangle\langle 1|) \ , \tag{2.27}$$

$$E_1^{\mathsf{pf}} = \sqrt{\eta}(|0\rangle\langle 0| - |1\rangle\langle 1|) \ . \tag{2.28}$$

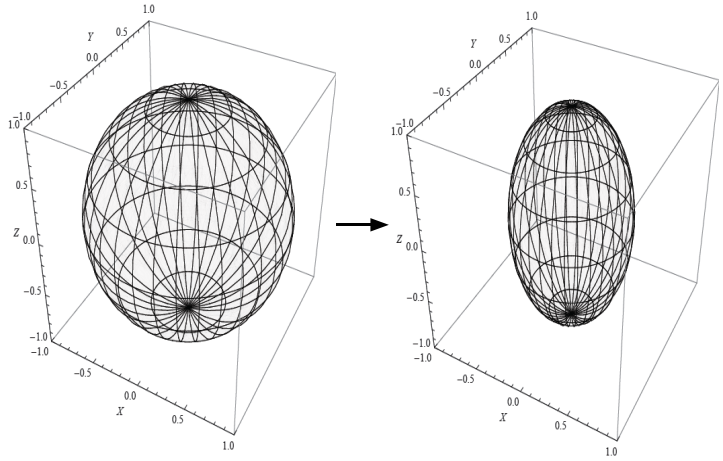
Przedstawmy działanie kanału zmieniającego fazę na qubit w stanie 2.14. Na wyjściu kanału w tym przypadku otrzymujemy następujący stan

$$\begin{aligned} \rho_{\mathsf{pf}} &= \cos^2\frac{\theta}{2}|0\rangle\langle 0| + \sin^2\frac{\theta}{2}|1\rangle\langle 1| + \\ &+ (1-2\eta)\Big(e^{-i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|0\rangle\langle 1| + e^{i\varphi}\sin\frac{\theta}{2}\cos\frac{\theta}{2}|1\rangle\langle 0|\Big) \ . \end{aligned} \tag{2.29}$$

Wobec tego współrzędne sfery Blocha transformują się następująco

$$\begin{aligned} r_x &\rightarrow r_x(2\eta - 1) \ , \\ r_y &\rightarrow r_y(2\eta - 1) \ , \\ r_z &\rightarrow r_z \ . \end{aligned} \tag{2.30}$$

Interpretacja graficzna powyższej transformacji przedstawiona jest na rysunku 2.6. Widać na nim, że kanał zmieniający fazę powoduje ściśnięcie sfery Blocha wzdłuż osi X i Y o czynnik $1 - 2\eta$.



Rysunek 2.6: Działanie kanału zmieniającego fazę na sferę Blocha dla parametru $\eta = 0, 2$.

2.1.5 Kanał będący złożeniem kanału tłumiącego amplitudę i zmieniającego fazę

Oprócz kanałów kwantowych opisanych powyżej istnieją również kanały złożone. Należy do nich kanał będący złożeniem kanału tłumiącego amplitudę i zmieniającego fazę (ang. *amplitude damping and phase flip channel*). Operatory Krausa opisujące działanie tego kanału mają postać

$$E_0^{\mathsf{adpf}} = \sqrt{1-\eta}(|0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|) \ , \tag{2.31}$$

$$E_1^{\mathsf{adpf}} = \sqrt{\eta}(|0\rangle\langle 0| - \sqrt{1-\gamma}\,|1\rangle\langle 1|) \ , \tag{2.32}$$

$$E_2^{\mathsf{adpf}} = \sqrt{\gamma}\,|0\rangle\langle 1| \ . \tag{2.33}$$

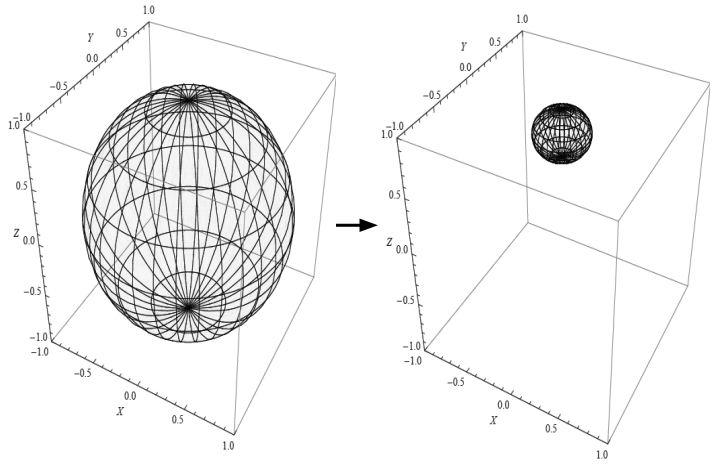
Analogicznie jak w poprzednich punktach przedstawimy działanie takiego kanału na qubit w stanie 2.14. Stan, jaki powstaje na wyjściu, ma postać

$$\begin{aligned}\rho_{\text{adpf}} &= (\cos^2\frac{\theta}{2} + \gamma\sin^2\frac{\theta}{2})\,|0\rangle\langle 0| + \\ &+ (1-\gamma)\sin^2\frac{\theta}{2}\,|1\rangle\langle 1| + \\ &+ e^{-i\varphi}\sqrt{1-\gamma}(2\eta-1)\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|0\rangle\langle 1| + \\ &+ e^{i\varphi}\sqrt{1-\gamma}(2\eta-1)\sin\frac{\theta}{2}\cos\frac{\theta}{2}\,|1\rangle\langle 0| \ .\end{aligned} \tag{2.34}$$

Natomiast współrzędne sfery Blocha transformuje się następująco

$$\begin{aligned} r_x &\to r_x(2\eta-1)\sqrt{1-\gamma}\ , \\ r_y &\to r_y(2\eta-1)\sqrt{1-\gamma}\ , \\ r_z &\to r_z(1-\gamma)+\gamma\ . \end{aligned} \tag{2.35}$$

Na rysunku 2.7 pokazano działanie kanału na sferę Blocha. Widzimy, że na skutek działania kanału została ona ściśnięta, a jej środek został przesunięty w kierunku górnej części osi Z.



Rysunek 2.7: Działanie kanału tłumiącego amplitudę i zmieniającego fazę na sferę Blocha dla parametrów $\eta = 0,2$ i $\gamma = 0,8$.

2.2 Pojemności kanałów kwantowych

Istnieje klika rodzajów pojemności kanału kwantowego. Różnorodność ta wynika z rodzaju informacji, jaką chcemy przesłać przez kanał oraz z dodatkowych zasobów jakimi mogą dysponować użytkownicy kanału kwantowego. O maksymalnej ilości informacji

klasycznej przesyłanej przez kanał kwantowy informuje nas pojemność klasyczna. Podobnie, o maksymalnej ilości informacji kwantowej, jaką możemy przesłać przez kanał kwantowy, informuje nas pojemność kwantowa.

Wprowadźmy najpierw pojęcie wierności. Jest to miara podobieństwa dwóch stanów kwantowych. Formalna definicja ma następującą postać

$$F = (\mathrm{Tr}(\sqrt{\rho}\sigma\sqrt{\rho}))^2 , \tag{2.36}$$

gdzie ρ i σ są macierzami gęstości. Z powyższego wzoru wynika, że gdy $\sigma = \rho$, to $F = 1$, natomiast gdy stany σ i ρ mają nośniki na wzajemnie ortogonalnych podprzestrzeniach, wtedy $F = 0$.

Pojemność klasyczna kanału kwantowego $\mathcal{N}$ dana jest wyrażeniem

$$C = \lim_{\epsilon\to 0}\lim_{n\to\infty}\sup\left\{\frac{m}{n} : \exists_K \exists_D \forall_{\psi\in\Gamma_m} F(\psi, K, D, \mathcal{N}) > 1-\epsilon\right\} , \tag{2.37}$$

gdzie ψ oznacza stan ze zbioru stanów ortogonalnych $\Gamma_m = \{|0\rangle, |1\rangle\}^{\otimes m}$, który chcemy przesłać przez kanał $\mathcal{N}$. Stan ψ zostaje zakodowany w n qubitów za pomocą protokołu kodowania K, n qubitów zostaje przesłanych przez kanał $\mathcal{N}$, a następnie stan ψ zostaje zdekodowany za pomocą protokołu dekodowania D. $F(\psi, K, D, \mathcal{N})$ oznacza wierność stanu końcowego ze stanem początkowym.

W analogiczny sposób definiujemy pojemność kwantową kanału kwantowego $\mathcal{N}$, czyli

$$Q = \lim_{\epsilon\to 0}\lim_{n\to\infty}\sup\left\{\frac{m}{n} : \exists_K \exists_D \forall_{\rho\in\mathcal{H}_2^{\otimes m}} F(\rho, K, D, \mathcal{N}) > 1-\epsilon\right\} , \tag{2.38}$$

gdzie ρ oznacza dowolny stan kwantowy z przestrzeni $\mathcal{H}_2^{\otimes m}$, który chcemy przesłać przez kanał $\mathcal{N}$.

Niestety, definicje 2.37 i 2.38 nie mówią, jak obliczyć pojemności klasyczną czy kwantową konkretnego kanału. Można tego dokonać, korzystając z przedstawionych poniżej wzorów.

Udowodniono, że pojemność klasyczna dana jest wzorem [14, 15]

$$C = \lim_{n\to\infty}\frac{1}{n}C_H(\mathcal{N}^{\otimes n}(\rho)) , \tag{2.39}$$

gdzie

$$C_H = \max_{\{p_i,\rho_i\}}\chi(\mathcal{N}(\rho)) , \tag{2.40}$$

oznacza pojemność klasyczną Holevo, natomiast χ jest funkcją Holevo

$$\chi(\mathcal{N}(\rho)) = S(\mathcal{N}(p_i\rho_i)) - \sum_i p_i S(\mathcal{N}(\rho_i)) . \tag{2.41}$$

$S(\rho)$ jest entropią von Neumanna stanu ρ. Jak widać funkcja Holevo jest różnicą pomiędzy entropią średniego stanu wyjściowego i średnią entropią stanów wyjściowych.

Niestety pojemność klasyczna Holevo nie jest addytywną funkcją kanału, co w ogólności nie pozwala na proste obliczenie pojemności [16]. Pokazano jednak, że dla kanałów depolaryzujących lub łamiących splątanie C_H jest addytywna [17, 18].

Znany jest również wzór na pojemność kwantową kanału kwantowego

$$Q \;=\; \lim_{n\to\infty}\frac{1}{n}\max_{\Phi_{AB}} I_c(I_A\otimes(\mathcal{N}^{\otimes n})_B(\Phi_{AB}))\;, \tag{2.42}$$

gdzie

$$I_c(I_A\otimes\mathcal{N}_B(\Phi_{AB})) \;=\; S(\mathcal{N}_B(\rho_B)) - S(I_A\otimes\mathcal{N}_B(\Phi_{AB}))\;, \tag{2.43}$$

oznacza koherentną informację obliczoną na stanie, który powstaje w wyniku przesłania przez kanał $\mathcal{N}$ podukładu B dowolnego czystego stanu splątanego Φ_{AB} [19, 20, 21]. Stan podukładu B we wzorze 2.43 oznaczony został przez $\rho_B = \mathrm{Tr}_B\Phi_{AB}$. Zoptymalizowana koherentna informacja podobnie jak pojemność klasyczna Holevo nie jest w ogólności addytywną funkcją kanału [22, 23, 24]. Natomiast jest ona addytywna dla kanałów degradowalnych i PPT [13, 25, 26].

Jeżeli użytkownicy oprócz kanału kwantowego posiadają dodatkowe zasoby, to mogą oni w pewnych przypadkach zwiększyć pojemność danego kanału kwantowego. Mówimy wtedy o asystowanych pojemnościach. Jeżeli dodatkowym zasobem jest komunikacja klasyczna od odbiorcy do nadawcy, to pojemność klasyczną (kwantową) kanału kwantowego oznaczamy przez $C_F(Q_F)$. Jeśli dodatkowym zasobem jest komunikacja klasyczna zarówno od odbiorcy do nadawcy jak i od nadawcy do odbiorcy, to pojemność klasyczną (kwantową) kanału kwantowego oznaczamy przez $C_2(Q_2)$. Należy zaznaczyć, że w przypadku pojemności C_2 klasyczna komunikacja nie może zależeć od przesyłanej wiadomości. Natomiast, gdy dodatkowym zasobem są czyste stany splątane między nadawcą a odbiorcą, to pojemność klasyczną (kwantową) kanału kwantowego oznaczamy przez $C_E(Q_E)$ [27, 28]. Pojemności te oraz odpowiadające im zasoby zebrano w tabeli 2.1. Relacje pomiędzy powyższymi pojemnościami zostały opisane w pracy [29] i są one następujące:

a) Pojemności klasyczne

$$C \leqslant C_F \leqslant C_2 \leqslant C_E\;, \tag{2.44}$$

b) Pojemności kwantowe

$$Q \leqslant Q_F \leqslant Q_2 \leqslant Q_E\;, \tag{2.45}$$

Tabela 2.1: Rodzaje asystowanych klasycznych i kwantowych pojemności kanału kwantowego.

Pojemność klasyczna	Pojemność kwantowa	Rodzaj dodatkowego zasobu
C_F	Q_F	Klasyczna komunikacja od odbiorcy do nadawcy
C_2	Q_2	Klasyczna komunikacja w obie strony to jest od nadawcy do odbiorcy jak i od odbiorcy do nadawcy
C_E	Q_E	Czyste stany splątane między nadawcą i odbiorcą

c) Pojemności klasyczne i kwantowe

$$Q \leqslant C \ , \tag{2.46}$$
$$Q_F \leqslant C_F \ , \tag{2.47}$$
$$Q_2 \leqslant C_2 \ , \tag{2.48}$$
$$Q_E = \frac{1}{2} C_E \ . \tag{2.49}$$

Należy też podkreślić, że dla niektórych kanałów nierówności z wzorów 2.44-2.48 przechodzą w nierówności ostre lub równości [29, 30, 31]. Znany jest wzór na asystowaną splątaniem pojemność klasyczną C_E [27, 28]

$$C_E = \max_{\rho}(S(\rho_B) + S(\mathcal{N}(\rho_B)) - S((\mathcal{N} \otimes I)\Phi_{AB}) \tag{2.50}$$

i – co za tym idzie – wzór na asystowaną splątaniem pojemność kwantową (porównaj 2.49). Zauważmy, że pojemność ta jest addytywna.

Poza klasyczną i kwantową pojemnością kanału kwantowego, istnieje również prywatna pojemność kanału kwantowego, która ma zastosowanie w kryptografii kwantowej [21, 32]. Podobnie jak pojemność klasyczna Holevo i zoptymalizowana koherentna informacja nie jest ona addytywną funkcją kanału [33, 34, 35, 36].

2.3 Protokoły destylacji splątania

W tym podrozdziale omówimy protokoły destylacji splątania. Zaczniemy jednak od wprowadzenia dwóch istotnych miar splątania: kosztu splątania i destylowalnego splątania [8, 37].

Definicja 2.1 (Koszt splątania)**.** *Niech ϱ_{AB} oznacza dowolny stan dwuqubitowy, natomiast n liczbę jego kopii. Niech P będzie protokołem wykorzystującym jedynie zachowujące ślad lokalne operacje (operacje unitarne lub pomiar), wspomagane przez klasyczną komunikację. Protokół ten przekształca czyste stany maksymalnie splątane w stany bliskie stanom ϱ_{AB}. Dalej, niech $\Phi(d)_{AB}$ symbolizuje macierz gęstości dwuquditowego, czystego stanu maksymalnie splątanego o wymiarze d. Koszt splątania $E_C(\varrho_{AB})$ definiujemy jako zminimalizowaną po wszystkich możliwych protokołach P wydajność r danego protokołu P, obliczaną w granicy n dążącego do nieskończoności. Formalnie, zapisujemy to następująco*

$$E_C(\varrho_{AB}) \;=\; \inf\left\{ r : \lim_{n\to\infty} \left[\inf_P \mathit{Tr}|\varrho_{AB}^{\otimes n} - P(\Phi(2^{rn})_{AB})| \right] = 0 \right\} . \tag{2.51}$$

Dualną miarą splatania jest destylowalne splątanie.

Definicja 2.2 (Destylowalne splątanie)**.** *Destylowalne splątanie $E_D(\varrho_{AB})$ definiujemy jako zmaksymalizowaną po wszystkich możliwych protokołach P wydajność r danego protokołu P, obliczaną w granicy n dążącego do nieskończoności. Zapisujemy to następująco*

$$E_D(\varrho_{AB}) \;=\; \sup\left\{ r : \lim_{n\to\infty} \left[\inf_P \mathit{Tr}|P(\varrho_{AB}^{\otimes n}) - \Phi(2^{rn})_{AB}| \right] = 0 \right\} , \tag{2.52}$$

przy czym P oznacza w tym przypadku protokół wykorzystujący jedynie zachowujące ślad lokalne operacje (operacje unitarne lub pomiar), wspomagane przez klasyczną komunikację, który przekształca stany ϱ_{AB} w stany bliskie czystym stanom maksymalnie splątanym. Protokół P nazywamy protokołem destylacji splątania.

Niestety obie z tych miar splątania są trudne do obliczenia. Dla kosztu splątania górnym ograniczeniem jest splątanie tworzenia, na które jest znany wzór analityczny dla dwóch qubitów [38]. Dodajmy, że splątanie tworzenia nie jest addytywne i może być ściśle większe od kosztu splątania [16, 39]. Dla destylowalnego splątania wyznaczono ograniczenie górne, którym jest względna entropia splątania [40, 41] oraz obliczono jego wartość dla konkretnych stanów kwantowych [42, 43, 44, 45, 46, 47, 48]. Dla pozostałych stanów możemy znaleźć ograniczenie dolne na destylowalne splątanie, opracowując dla nich protokoły destylacji splątania i obliczając ich wydajność. W informatyce kwantowej znanych jest wiele protokołów destylacji splątania. Dla stanów dwucząstkowych są to protokoły rekurencyjne [7, 9], protokoły wykorzystujące efekt pompowania splątania [49, 50, 51], protokoły typu $N \to M$ [52, 53, 54], protokoły haszujące [8, 55, 56, 57, 58] i inne [59, 60, 61]. Istnieją również protokoły destylacji splątania ze stanów wielocząstkowych [51, 53, 62, 63, 64, 65]. My omówimy dwa z tych protokołów, które zostały wykorzystane w tej pracy doktorskiej i porównane z zaproponowanymi protokołami.

2.3.1 Protokół rekurencyjny

Przedstawiony poniżej protokół rekurencyjny podany został w pracy [9]. Alternatywny protokół rekurencyjny podano w pracy [7]. Jest on jednak mniej efektywny, dlatego go pominiemy. Załóżmy, że Alicja i Bob posiadają dwie kopie mieszanego stanu splątanego ρ_{AB}, który w bazie Bella ma postać diagonalną

$$\rho_{AB} = \begin{pmatrix} a_1 & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 \\ 0 & 0 & a_3 & 0 \\ 0 & 0 & 0 & a_4 \end{pmatrix} . \tag{2.53}$$

Parametry $a_1 \geqslant a_2 \geqslant a_3 \geqslant a_4$ są prawdopodobieństwami wystąpienia stanów $|\psi^+\rangle_{AB}$, $|\phi^-\rangle_{AB}$,$|\phi^+\rangle_{AB}$, $|\psi^-\rangle_{AB}$, gdzie

$$|\psi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}) , \tag{2.54}$$

$$|\phi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}) . \tag{2.55}$$

Przebieg protokołu rekurencyjnego jest następujący:

1. Alicja stosuje na każdej kopii stanu ρ_{AB} operację unitarną U zdefiniowaną przez równania

$$U|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) , \tag{2.56}$$

$$U|1\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|0\rangle) , \tag{2.57}$$

natomiast Bob operację odwrotną $U^{\dagger}$

$$U^{\dagger}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) , \tag{2.58}$$

$$U^{\dagger}|1\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|0\rangle) . \tag{2.59}$$

2. Zarówno Alicja jak i Bob wykonują operację $CNOT$, zdefiniowaną następująco

$$CNOT|a\rangle|b\rangle = |a\rangle|b \oplus a\rangle , \tag{2.60}$$

gdzie $a, b \in \{0, 1\}$, a symbol $\oplus$ oznacza sumę modulo 2. Dalej, Alicja i Bob mierzą qubity docelowe w bazie obliczeniowej $\{|0\rangle, |1\rangle\}$. Jeżeli w wyniku pomiaru otrzymali koincydencję (oboje zmierzyli $|0\rangle$ lub oboje zmierzyli $|1\rangle$), to odrzucają qubity docelowe. Natomiast jeśli wynik zwrócił brak koincydencji oba qubity zostają odrzucone. W przypadku koincydencji wartość współczynnika a_1 określającego prawdopodobieństwo występowania stanu $|\psi^+\rangle_{AB}$ w stanie ρ'_{AB} po pomiarze zostaje zwiększona. Transformacje współczynników opisują poniższe wzory

$$a_1^{'} = \frac{a_1^2 + a_2^2}{N} , \tag{2.61}$$

$$a_2^{'} = \frac{2a_3a_4}{N} , \tag{2.62}$$

$$a_3^{'} = \frac{a_3^2 + a_4^2}{N} , \tag{2.63}$$

$$a_4^{'} = \frac{2a_1a_2}{N} , \tag{2.64}$$

gdzie N jest czynnikiem normalizacyjnym

$$N = (a_1 + a_2)^2 + (a_3 + a_4)^2 . \tag{2.65}$$

Mając n kopii stanu ρ_{AB}, Alicja i Bob mogą bardziej zwiększyć wartość współczynnika a_1. W tym celu dzielą posiadane kopie stanu na bloki, składające się z dwóch kopii i stosują opisany powyżej protokół na każdym z bloków. W ten sposób otrzymują $p_s\frac{n}{2}$ kopii stanu $\rho_{AB}^{'}$, gdzie p_s jest prawdopodobieństwem sukcesu. Następnie powtarzają rekurencyjnie przebieg protokołu na coraz to mniejszej liczby bloków. W granicy n dążącego do nieskończoności, prawdopodobieństwo a_1 będzie dążyło do jedności. Współczynnik przy stanie $|\psi^+\rangle_{AB}$ obliczamy rekurencyjnie podstawiając za a_1 współczynnik $a_1^{'}$ we wzorze 2.61 i tak dalej. Ważny podkreślenia jest fakt, że protokół rekurencyjny może być zastosowany tylko do stanów o współczynniku $a_1 > \frac{1}{2}$ (stany o współczynniku $a_1 \leqslant \frac{1}{2}$ są separowalne). Niestety wydajność protokołu rekurencyjnego jest zerowa. Chcąc osiągnąć niezerową wydajność, postępuje się następująco: najpierw za pomocą protokołu rekurencyjnego sprowadza się współczynnik a_1 do wartości, dla której inny protokół destylacji splątania ma niezerową wydajność (na przykład protokół haszujący), a następnie stosuje się ten protokół.

2.3.2 Jednokierunkowy protokół haszujący

Jednokierunkowy protokół haszujący został szczegółowo przedstawiony w pracach [8, 55, 56]. Protokół ten wymaga komunikacji klasycznej w jednym kierunku i ma zatosowanie do:

- destylacji klucza szyfrującego,
- destylacji splątania,
- generacji klucza szyfrującego,
- generacji splątania.

W tej pracy doktorskiej interesuje nas wydajność tego protokołu, o której informuje nas poniższe twierdzenie.

Twierdzenie 2.1 (Wydajność jednokierunkowego protokołu haszującego w przypadku destylacji splątania)**.** *Niech ρ_{AB} oznacza stan mieszany współdzielony przez dwóch użytkowników Alicję i Boba. Jeśli zastosują oni na stanie jednokierunkowy protokół haszujący z komunikacją klasyczną od Alicji do Boba, to jego wydajność będzie spełniała nierówność*

$$R_{\rightarrow} \geqslant S(\rho_B) - S(\rho_{AB}) \ , \tag{2.66}$$

gdzie $S(\rho_B)$ to entropia von Neumana stanu podukładu odbiorcy, natomiast $S(\rho_{AB})$ to entropia stanu całego układu. Wielkość po prawej stronie nierówności nazywamy koherentną informacją (patrz wzór 2.43)

Warto dodać, że w niektórych przypadkach wydajność protokołu haszującego można poprawić jeśli dopuścimy komunikację klasyczną w obydwu kierunkach [57, 58]. Istnieje również protokół destylacji splątania oparty na kodach polarnych, który dla stanów dwuqubitowych diagonalnych w bazie stanów maksymalnie splątanych, osiąga taką samą wydajność jak protokół haszujący. Niestety, obecnie nie wiadomo czy taką samą wydajność protokół ten osiąga dla dowolnego stanu splątanego [66].

2.4 Teoria grup

W tym punkcie przedstawimy aparat matematyczny, który zostanie wykorzystany w rozdziale 4, dotyczącym destylacji splątania z mieszanego stanu splątanego dwóch qubitów o macierzy gęstości rzędu 3. Więcej wiadomości oraz dowody przedstawionych w tym podrozdziale twierdzeń czytelnik znajdzie w [67].

2.4.1 Niezbędne pojęcia

Definicja 2.3 (Waga Hamminga)**.** *W ciągu bitów o długości n wagą Hamminga nazywamy liczbę bitów o wartości 1.*

Przykład 2.1. *Waga Hamminga ciągu bitów $x = 11101100$ o długości $n = 8$ jest równa $k = 5$.*

Definicja 2.4 (Dystans Hamminga)**.** *Dystans Hamminga pomiędzy dwoma ciągami bitów x oraz y o długości n definiujemy jako liczbę pozycji, na których ciągi te różnią się.*

Przykład 2.2. *Ciągi o długości $n = 8$ postaci*

$$\begin{aligned} \textit{numer pozycji} \quad & 12345678\ , \\ x &= 00011101\ , \\ y &= 00101101\ , \end{aligned}$$

różnią się na dwóch pozycjach (3 i 4), stąd dystans Hamminga pomiędzy nimi jest równy 2.

Definicja 2.5 (Grupa)**.** *Grupą nazywamy zbiór G z działaniem mnożenia $\cdot : G \times G \to G$, spełniający następujące warunki:*

1. *Dla dowolnych elementów $a, b, c \in G$ zachodzi prawo łączności $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
2. *W zbiorze G istnieje element neutralny e dla działania $\cdot$, taki, że dla każdego $a \in G$ prawdziwe jest $e \cdot a = a \cdot e = a$.*
3. *Dla każdego $a \in G$ istnieje element odwrotny do niego, który oznaczymy a^{-1}, taki, że $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

Ponadto jeżli dla dowolnych $a, b \in G$ zachodzi $a \cdot b = b \cdot a$, to grupę nazywamy przemienną lub abelową.

2.4.2 Permutacje, podziały liczb naturalnych i diagramy Younga

Wprowadźmy najpierw kilka definicji dotyczących permutacji [68, 69].

Definicja 2.6 (Permutacja)**.** *Niech $X_n = \{1, 2, \ldots, n\}$ oznacza zbiór liczb naturalnych. Permutacją $\pi(i)$, gdzie $i \in X_n$ nazywamy każdą bijekcję zbioru X_n w ten sam zbiór. Oznaczmy przez S_n zbiór wszystkich bijekcji zbioru X_n.*

Zbiór S_n składa się z $n!$ elementów (permutacji). Dowolną permutację $\pi \in S_n$ możemy przedstawić za pomocą macierzy $M_{2,n}$ lub w postaci macierzy zerojedynkowej $M_{n,n}$. Zilustrujmy to poniższym przykładem.

Przykład 2.3. *Dla $n = 3$ zbiór S_3 składa się z $3! = 6$ elementów. Przedstawmy jeden z nich*

$$\begin{aligned} \pi(1) &= 2\ , \\ \pi(2) &= 3\ , \\ \pi(3) &= 1\ , \end{aligned} \tag{2.67}$$

w postaci macierzy $M_{2,3}$

$$M_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} . \tag{2.68}$$

Przedstawmy wartości 1, 2 *i* 3 *za pomocą wektorów*

$$1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} , \tag{2.69}$$

$$2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} ,$$

$$3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} ,$$

wtedy macierz zerojedynkowa $M_{3,3}$ *ma postać*

$$M_{3,3} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} . \tag{2.70}$$

Definicja 2.7 (Cykl)**.** *Niech* $x_1, x_2, \ldots, x_k$ *oznaczają różne liczby ze zbioru* X_n*. Jeśli permutacja* π *zachowuje pozostałe* $n - k$ *liczb ze zbioru* X_n *oraz*

$$\begin{aligned} \pi(x_1) &= \pi(x_2) , \\ \pi(x_2) &= \pi(x_3) , \\ &\cdots , \\ \pi(x_k) &= \pi(x_1) , \end{aligned} \tag{2.71}$$

wtedy π *nazywamy cyklem o długości* k *i oznaczamy* $(x_1, x_2, \ldots, x_k)$*. Cykl długości jeden jest identycznością. Natomiast cykl o długości dwa, nazywamy transpozycją i oznaczamy* τ*.*

Przykład 2.4 (Cykl)**.** *Permutacja*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \tag{2.72}$$

ma następujący cykl o długości 4

$$\begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} . \tag{2.73}$$

Definicja 2.8 (Cykle rozłączne)**.** *Dwa cykle* $\pi_1 = (x_1, x_2, \ldots, x_k)$ *oraz* $\pi_2 = (y_1, y_2, \ldots, y_l)$ *ze zbioru* S_n *są rozłączne, gdy zbiory* $(x_1, x_2, \ldots, x_k)$ *i* $(y_1, y_2, \ldots, y_l)$ *są rozłączne. Dwa cykle rozłączne są przemienne.*

Twierdzenie 2.2. *Każda permutacja* $\pi \in S$ *jest złożeniem pewnej liczby cykli rozłącznych. Przedstawienie permutacji* π *w postaci złożenia rozłącznych cykli jest jednoznaczne z dokładnością do porządku czynników. Ponadto każda z permutacji z* S_n *jest złożeniem pewnej liczby transpozycji.*

Przykład 2.5. *Permutację*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \tag{2.74}$$

możemy rozłożyć na następujący iloczyn transpozycji

$$\begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} . \tag{2.75}$$

Definicja 2.9 (Znak permutacji)**.** *Niech* $\pi = \tau_1 \tau_2 \ldots \tau_k$ *jest jednym z rozkładów permutacji* $\pi \in S_n$ *na iloczyn transpozycji. Liczbę* $\mathrm{sgn}\pi = (-1)^k$ *nazywamy znakiem permutacji. Znak permutacji zależy jednie od samej permutacji* π*, a nie od jej rozkładu. Permutację nazywamy parzystą, gdy* $\mathrm{sgn}\pi = 1$*, natomiast nieparzystą, kiedy* $\mathrm{sgn}\pi = -1$*.*

Z powyższej definicji możemy wywnioskować, że permutacja, która ma rozkład na iloczyn składający się z parzystej liczby transpozycji, jest permutacją parzystą, a permutacja składająca się z nieparzystej liczby transpozycji, jest permutacją nieparzystą.

Przykład 2.6. *Permutacja* π *ze zbioru* S_6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix} \tag{2.76}$$

ma rozkład na transpozycję postaci

$$\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 5 & 6 \end{pmatrix} . \tag{2.77}$$

Znak tej permutacji $\mathrm{sgn}\pi = (-1)^3 = -1$*, więc jest to permutacja nieparzysta.*

Wprowadzimy teraz pojęcie podziału liczby oraz diagramów Younga.

Definicja 2.10 (Podział λ)**.** *Podziałem* λ *liczby* n*, należącej do zbioru liczb naturalnych (*0 *nie zaliczamy do zbioru liczb naturalnych), nazywamy nierosnący ciąg postaci*

$$\lambda \;=\; (\lambda_1, \lambda_2, \ldots, \lambda_r, \ldots) , \tag{2.78}$$

gdzie λ_i *również należą do zbioru liczb naturalnych. Dla każdego podziału wyróżniamy trzy pojęcia:*

1. *Długość, czyli liczbę jego elementów, którą oznaczamy przez* $l(\lambda)$.

2. *Wagę, czyli sumę wszystkich jego elementów, którą oznaczamy przez*

$$|\lambda| \;=\; \sum_i \lambda_i \;. \tag{2.79}$$

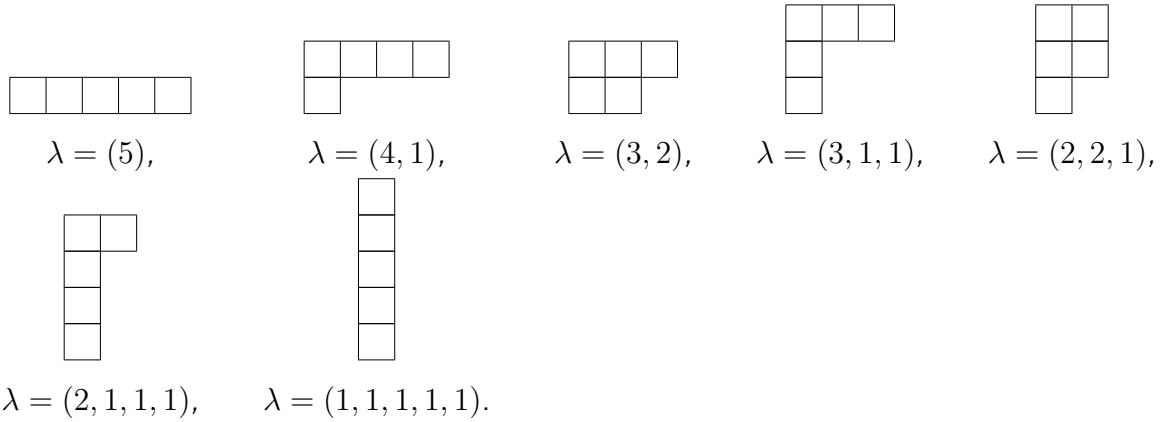
3. *Krotność* m_i *i-tego elementu, którą oznaczamy przez* $\lambda_i^{m_i}$.

Przykład 2.7. *Dla liczby* $n = 5$ *mamy następujące podziały*

$$\left(\begin{array}{c} 5 \end{array}\right)\left(\begin{array}{cc} 4 & 1 \end{array}\right)\left(\begin{array}{cc} 3 & 2 \end{array}\right)\left(\begin{array}{cc} 3 & 1^2 \end{array}\right)\left(\begin{array}{cc} 2^2 & 1 \end{array}\right)\left(\begin{array}{cc} 2 & 1^3 \end{array}\right)\left(\begin{array}{c} 1^5 \end{array}\right) \;. \tag{2.80}$$

Rozkład λ można przedstawić graficznie za pomocą diagramów Younga. Diagram Younga składa się z rzędów pustych kwadratów. Każdy i-ty rząd składa się z λ_i kwadratów.

Przykład 2.8. *Rozkłady dla* $n = 5$ *z przykładu 2.7 odpowiadają diagramom Younga*



$\lambda = (5)$, $\lambda = (4,1)$, $\lambda = (3,2)$, $\lambda = (3,1,1)$, $\lambda = (2,2,1)$,

$\lambda = (2,1,1,1)$, $\lambda = (1,1,1,1,1)$.

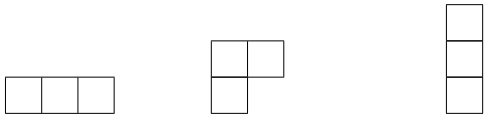
Wyobraźmy sobie, że dla danego rozkładu liczby n, w puste kwadraty reprezentującego go diagramu Younga, wpiszemy bez powtórzeń liczby naturalne $m \in \{1, 2, \ldots, n\}$. Jeśli rozkład tych liczb spełnia warunek, że w każdym wierszu od lewej do prawej strony i w każdej kolumnie od góry do dołu tworzą one ciąg rosnący, to taki diagram nazywamy standardowym diagramem Younga. W naszych dalszych rozważaniach pojawi się również pojęcie semi-standardowego diagramu Younga. Semi-standardowym diagramem Younga nazywamy diagram Younga wypełniony liczbami naturalnymi, które w każdym wierszu od lewej do prawej strony tworzą ciąg niemalejący, natomiast w każdej kolumnie od góry do dołu tworzą ciąg rosnący. W takim diagramie elementy λ_i rozkładu λ mogą się powtarzać.

Przykład 2.9 (Semi-standardowe diagramy Younga)**.** *Dla* $n = 3$ *mamy poniższe semi-standardowe diagramy Younga*

$$\begin{array}{|c|c|}\hline 1&1\\\hline 2\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 1&1\\\hline 3\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 2&2\\\hline 3\\\cline{1-1}\end{array}$$

Dalsze przykłady dotyczyć będą diagramów Younga i standardowych diagramów Younga.

Przykład 2.10 (Diagramy Younga i standardowe diagramy Younga)**.** *Dla $n = 3$ mamy następujące diagramy Younga*



$\lambda = (3), \qquad \lambda = (2,1), \qquad \lambda = (1,1,1).$

Natomiast standardowe diagramy Younga mają postać

$$\begin{array}{|c|c|c|}\hline 1&2&3\\\cline{1-3}\end{array} \qquad \begin{array}{|c|c|}\hline 1&2\\\hline 3\\\cline{1-1}\end{array} \qquad \begin{array}{|c|c|}\hline 1&3\\\hline 2\\\cline{1-1}\end{array} \qquad \begin{array}{|c|}\hline 1\\\hline 2\\\hline 3\\\cline{1-1}\end{array}$$

$\lambda = (3), \qquad \lambda = (2,1), \qquad \lambda = (2,1), \qquad \lambda = (1,1,1).$

Liczbę standardowych diagramów Younga dla danego rozkładu λ, możemy obliczyć ze wzoru

$$f^{\lambda} \;=\; n!\frac{\Delta(\nu_1,\nu_2,\ldots,\nu_r)}{\nu_1!\nu_2!\ldots\nu_r!}\;, \tag{2.81}$$

gdzie indeks $r = l(\lambda)$ jest długością podziału λ, $\nu_i(\lambda) = \lambda_i + l(\lambda) - i$ dla $i = 1, 2, \ldots l(\lambda)$, natomiast $\Delta(x_1, x_2, \ldots, x_r)$ oznacza następujące wyrażenie

$$\Delta(x_1,x_2,\ldots,x_r) \;=\; \prod_{i<j}(x_i - x_j)\;, \tag{2.82}$$

przy czym dla $r = 1$ wyrażenie $\Delta(x_1) = 1$.

Przykład 2.11. *W przykładzie 2.10 widać, że dla $n = 3$ mamy trzy możliwe przypadki rozkładu. I tak, rozkładowi $\lambda = (3)$ odpowiada jeden standardowy diagram Younga, rozkładowi $\lambda = (2,1)$ – dwa, zaś rozkładowi $\lambda = (1,1,1)$ – jeden standardowy diagram Younga. Teraz uzyskajmy ten wynik korzystając ze wzoru 2.81.*

1. *Rozkład $\lambda = (3)$*

$$\begin{aligned} l(\lambda) &= 1\;, \\ \nu_1 &= 3\;, \\ \Delta(\nu_1) &= 1\;, \\ f^{(3)} &= 1\;. \end{aligned} \tag{2.83}$$

2. *Rozkład* $\lambda = (2,1)$

$$\begin{aligned} l(\lambda) &= 2 \,, \\ \nu_1 &= 3 \,, \\ \nu_2 &= 1 \,, \\ \Delta(\nu_1,\nu_2) &= 2 \,, \\ f^{(2,1)} &= 2 \,. \end{aligned} \tag{2.84}$$

3. *Rozkład* $\lambda = (1,1,1)$

$$\begin{aligned} l(\lambda) &= 3 \,, \\ \nu_1 &= 3 \,, \\ \nu_2 &= 2 \,, \\ \nu_3 &= 1 \,, \\ \Delta(\nu_1,\nu_2,\nu_3) &= 2 \,, \\ f^{(1,1,1)} &= 1 \,. \end{aligned} \tag{2.85}$$

2.4.3 Metoda symetryzacji Younga i dekompozycji Schura-Weyla

W tym punkcie przedstawimy metodę symetryzacji Younga i dekompozycji Schura-Weyla. Niech grupa permutacji S_n będzie zdefiniowana na przestrzeni $(\mathbb{C}^d)^{\otimes n}$. Wtedy n-krotny iloczyn tensorowy tej przestrzeni możemy przedstawić jako

$$(\mathbb{C}^d)^{\otimes n} = \oplus_\lambda \mathcal{H}_\lambda^U \otimes \mathcal{H}_\lambda^S \,, \tag{2.86}$$

gdzie $\mathcal{H}_\lambda^S$ jest przestrzenią reprezentacji nieprzywiedlnych grupy S_n dla rozkładu λ, natomiast $\mathcal{H}_\lambda^U$ jest przestrzenią krotności danej reprezentacji. Na przestrzeni $(\mathbb{C}^d)^{\otimes k}$ możemy zdefiniować symetryzatory Younga $P^{\lambda,a}$, które związane są z danym rozkładem λ

$$P^{\lambda,a} = \frac{f^\lambda}{n!} \prod_{k \in \text{kolumna}(\lambda,a)} \mathcal{A}_k \prod_{k \in \text{wiersz}(\lambda,a)} \mathcal{S}_k \,, \tag{2.87}$$

gdzie f^λ to czynnik zdefiniowany we wzorze 2.81, zaś

$$\mathcal{S}_k = \sum_{\pi \in S_n} V_\pi \,, \tag{2.88}$$

$$\mathcal{A}_k = \sum_{\pi \in S_n} \text{sgn}(\pi) V_\pi \,. \tag{2.89}$$

W powyższym wzorze V_π jest operatorem permutacji, działającym następująco

$$V_\pi |i_1\rangle \otimes \cdots \otimes |i_n\rangle = |i_{\pi(1)}\rangle \otimes \cdots \otimes |i_{\pi(n)}\rangle \,, \tag{2.90}$$

gdzie $|i_1\rangle \ldots |i_n\rangle$ są wektorami bazowymi z przestrzeni $(\mathbb{C}^d)^{\otimes n}$. Operatory we wzorach 2.88 i 2.89 rzutują odpowiednio na podprzestrzeń symetryczną i antysymetryczną przestrzeni $(\mathbb{C}^d)^{\otimes k}$. Wyznaczamy je korzystając z danego standardowego diagramu Younga (oznaczonego przez a) dla rozkładu λ. I tak operator $\mathcal{S}_k$ powstaje z permutacji elementów znajdujących się w k-tym wierszu diagramu, natomiast operator $\mathcal{A}_k$ powstaje z permutacji elementów znajdujących się w k-tej kolumnie diagramu. Należy zaznaczyć, że symetryzatory $P^{\lambda,a}$ są idempotentne, czyli spełniają równość

$$(P^{\lambda,a})^2 \;=\; P^{\lambda,a}\;, \tag{2.91}$$

lecz w ogólności nie są one wzajemnie ortogonalne i hermitowskie. Na koniec przedstawimy jak symetryzatory Younga wiążą się z dekompozycją Schura-Weyla. Mianowicie symetryzator Younga można zapisać następująco

$$P^{\lambda,a} \;=\; I^U_\lambda \otimes |u\rangle\langle v|\;, \tag{2.92}$$

gdzie I^U_λ jest operatorem identycznościowym działającym na przestrzeni krotności reprezentacji $\mathcal{H}^U_\lambda$, a wektory $|u\rangle$ i $|v\rangle$ należą do przestrzeni $\mathcal{H}^S_\lambda$.

ROZDZIAŁ 3

Destylacja splątania ze stanów mieszanych składających się z czystego stanu splątanego i czystego stanu produktowego

3.1 Bisekcyjny protokół destylacji

W tym rozdziale przedstawimy bisekcyjny protokół destylacji, który pierwotnie został opisany w pracy [70]. Ma on zastosowanie do destylacji splątania ze stanu mieszanego składającego się z czystego stanu splątanego i czystego stanu produktowego ortogonalnego do niego. W pracy [71] rozszerzono jego zastosowanie pokazując, że protokół ten w połączeniu z jednokierunkowym protokołem haszującym może zostać użyty do destylacji splątania ze stanu mieszanego składającego się z dwóch czystych stanów splątanych różniących się fazą i stanu produktowego ortogonalnego do nich.

3.1.1 Dwuqubitowe stany mieszane

Załóżmy, że Alicja i Bob współdzielą $n = 2^m$ kopii stanu ρ_{AB}, gdzie $m \in \mathbb{N}$. Stan ρ_{AB} jest stanem mieszanym, składającym się z czystego stanu splątanego i stanu produktowego ortogonalnego do niego. Jego postać jest następująca

$$\rho_{AB} \;=\; p|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB} + (1-p)\,|01\rangle\,\langle 01|_{AB} \;, \tag{3.1}$$

gdzie

$$|\phi^+(\alpha)\rangle_{AB} \;=\; \alpha\,|00\rangle_{AB} + \sqrt{1-\alpha^2}\,|11\rangle_{AB} \;. \tag{3.2}$$

Bez straty ogólności zakładamy, że parametr α należy do zbioru liczb rzeczywistych. Zadaniem Alicji i Boba będzie wydestylowanie stanów maksymalnie splątanych z n kopii stanu 3.1. Użytkownicy mogą wykonywać lokalne operacje kwantowe i komunikować się ze sobą w klasyczny sposób. W celu wydestylowania splątania stosują oni następujący protokół:

1. Każdy z użytkowników dokonuje pomiaru na n qubitach ze współdzielonych n kopii stanu ρ_{AB}. Pomiar ten jest dany przez operatory rzutowe

$$P_k = \sum_{\text{permutacje}} \bar{P}_1^{\otimes k} \otimes \bar{P}_0^{\otimes(n-k)} , \tag{3.3}$$

gdzie

$$\begin{aligned} \bar{P}_1 &= |1\rangle\langle 1| , \\ \bar{P}_0 &= |0\rangle\langle 0| . \end{aligned} \tag{3.4}$$

We wzorze 3.3 przez *permutacje* rozumiemy sumę po permutacjach bez powtórzeń iloczynów tensorowych n operatorów rzutowych 3.4. W iloczynach tych k operatorów ma postać $\bar{P}_1$, a $n-k$ ma postać $\bar{P}_0$. Oznacza to, że każdy z użytkowników mierzy, ile qubitów znajduje się w stanie $|0\rangle$, a ile w stanie $|1\rangle$ bez mierzenia, które qubity znajdują się w tych stanach.

2. Jeśli zarówno Alicja jak i Bob otrzymają wynik pomiaru k, to stan po pomiarze przyjmuje postać

$$\rho_{kAB}^n = \frac{P_{kA}P_{kB}\rho_{AB}^{\otimes n}P_{kA}P_{kB}}{\text{Tr}(P_{kA}P_{kB}\rho_{AB}^{\otimes n}P_{kA}P_{kB})} . \tag{3.5}$$

Zapiszmy stan $\rho_{AB}^{\otimes n}$ w następującej postaci

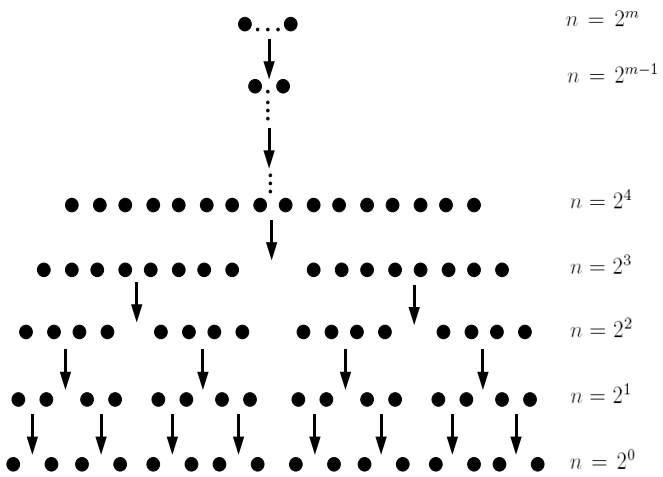
$$\begin{aligned} \rho_{AB}^{\otimes n} &= p^n|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB}^{\otimes n} + \\ &+ p^{(n-1)}(1-p)[|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB}^{\otimes(n-1)} \otimes |01\rangle\langle 01|_{AB} + \\ &+ \text{permutacje}] + \\ &+ p^{(n-2)}(1-p)^2[|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB}^{\otimes(n-2)} \otimes |01\rangle\langle 01|_{AB}^{\otimes 2} + \\ &+ \text{permutacje}] + \\ &+ \cdots + (1-p)^n[|01\rangle\langle 01|_{AB}^{\otimes n}] . \end{aligned} \tag{3.6}$$

Analizując wzory 3.3, 3.4, 3.5 i 3.6 można zauważyć, że operatory P_{kA} i P_{kB} anihilują wszystkie człony po prawej stronie znaku równości we wzorze 3.6 z wyjątkiem pierwszego. Stąd stan ρ_{kAB}^n jest stanem maksymalnie splątanym o rzędzie

Schmidta rankP_{kA} = rankP_{kB} = $\binom{n}{k}$ [72]. Warto zaznaczyć, że w przypadkach, gdy $k = 0$ lub $k = n$, splątanie jest całkowicie niszczone.

Jeśli Alicja otrzyma inny wynik pomiaru niż Bob, to dzielą oni pary qubitów na dwie równe grupy i wykonują analogiczny pomiar jak w pierwszym kroku niezależnie na każdej grupie. Schemat bisekcji przedstawia rysunek 3.1.

3. Alicja i Bob przerywają bisekcję na danej grupie par qubitów, gdy otrzymają na niej te same wyniki pomiaru. Natomiast kontynuują bisekcję na tej grupie par qubitów, dla której otrzymali różne wyniki pomiarów. Schemat blokowy protokołu znajduje się na rysunku 3.2



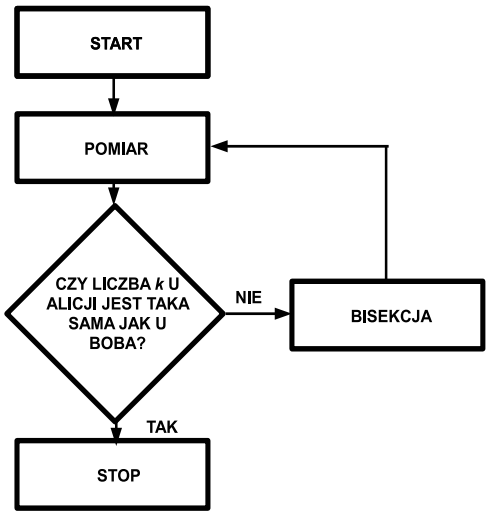
Rysunek 3.1: Schemat bisekcji w protokole destylacji. Czarna kropka oznacza pojedynczą parę qubitów dzieloną przez Alicję i Boba.

Wyprowadzimy teraz wzór na wydajność protokołu. W tym celu oznaczymy przez i numer kroku protokołu, natomiast przez R_i splątanie wydestylowane z grupy $2^{m-(i-1)}$ par qubitów pod warunkiem, że Alicja i Bob otrzymają te same wyniki pomiarów. Przez $p(S_i)$ oznaczymy prawdopodobieństwo sukcesu w i-tym kroku (to znaczy otrzymania przez Alicję i Boba tych samych wyników pomiarów), a przez $p(F_i)$ prawdopodobieństwo porażki w i-tym kroku. Wprowadźmy również na podstawie wzoru 3.6 prawdopodobieństwa

$$p(s_i) \;=\; p^{2^{m-(i-1)}} \tag{3.7}$$

oraz

$$p(f_i) \;=\; 1 - p^{2^{m-(i-1)}} \;. \tag{3.8}$$



Rysunek 3.2: Schemat blokowy protokołu bisekcyjnego.

Określają one odpowiednio, że w grupie składającej się z $2^{m-(i-1)}$ stanów ρ_{AB} jest $2^{m-(i-1)}$ stanów $|\phi^+(\alpha)\rangle \langle\phi^+(\alpha)|_{AB}$ oraz, że w grupie składającej się z $2^{m-(i-1)}$ stanów ρ_{AB} nie ma $2^{m-(i-1)}$ stanów $|\phi^+(\alpha)\rangle \langle\phi^+(\alpha)|_{AB}$. Zauważmy, że

$$p(S_i) \;=\; p(s_i) \tag{3.9}$$

oraz

$$p(F_i) \;=\; p(f_i). \tag{3.10}$$

Zgodnie z protokołem sukces w i-tym kroku na danej grupie par qubitów skutkuje przerwaniem na niej pomiarów, natomiast porażka powoduje przejście do bisekcji i kolejnego pomiaru na 2^{m-i} parach qubitów. Przez $p(S_i, F_{i-1})$ oznaczymy łączne prawdopodobieństwo sukcesu w i-tym kroku dla jednej z dwóch grup par qubitów i porażki w $i-1$-ym kroku dla grupy par qubitów składającej się z wymienionych wyżej grup. Zauważmy, że prawdopodobieństwo to spełnia równanie

$$p(S_i, F_{i-1}) = 2p(s_i)p(f_i)\ . \tag{3.11}$$

Czynnik 2 we wzorze 3.11 pojawia się, ponieważ po porażce w $i-1$-szym kroku Alicja i Bob mogą osiągnąć sukces w i-tym kroku najwyżej dla jednej z dwóch grup. Ponadto zauważmy, że jeżeli Alicja i Bob odnieśli porażkę dla jednej grupy par qubitów w $i-1$-szym kroku, to musieli również odnieść porażkę we wszystkich krokach poprzednich dla każdej grupy qubitów zawierającej tę grupę. Ponadto zauważmy, że w $i-1$-szym kroku możemy mieć 2^{i-2} grup par qubitów, dla których Alicja i Bob odnieśli porażkę. Wobec

tego dostaniemy następujący wzór na wydajność protokołu

$$R = \frac{1}{2^m}\Big(p(S_1)R_1 + p(S_2,F_1)R_2 + \cdots + 2^{i-2}p(S_i,F_{i-1})R_i + \ldots\Big) . \quad (3.12)$$

Korzystając z wzorów 3.7, 3.8, 3.9, 3.10 i 3.11 wyrażenie to możemy zapisać w postaci

$$\begin{aligned} R &= \frac{1}{2^m}\Big(p^{2^m}R_1 + 2p^{2^{m-1}}(1-p^{2^{m-1}})R_2 + \quad (3.13)\\ &+ 2^{i-2}2p^{2^{m-(i-1)}}(1-p^{2^{m-(i-1)}})R_i + \ldots\Big) = \\ &= \frac{1}{2^m}\Big(p^{2^m}R_1 + \sum_{i=2}^{m-1} 2^{i-2}p^{2^{m-(i-1)}}(1-p^{2^{m-(i-1)}})R_i\Big) . \end{aligned}$$

Po przekształceniach dostajemy

$$R = \frac{1}{2^m}\sum_{i=1}^{m} p^{2^{m-(i-1)}}(2^{i-1}R_i - 2^i R_{i+1}) , \quad (3.14)$$

gdzie założyliśmy, że $R_{m+1} = 0$.

Przejdźmy do wyznaczenia wzoru na R_i. Zacznijmy od obliczenia prawdopodobieństwa tego, że zarówno Alicja jak i Bob otrzymają wyniki k pod warunkiem, że oboje otrzymają takie same wyniki wykonując pomiar na $2^{m-(i-1)}$ parach qubitów. Jest ono równe

$$p(k|S_i) = \alpha^{2(2^{m-(i-1)}-k)}(\sqrt{1-\alpha^2})^{2k}\binom{2^{m-(i-1)}}{k} . \quad (3.15)$$

Natomiast stan po pomiarze współdzielony przez Alicję i Boba jest stanem maksymalnie splątanym o rzędzie Schmidta $\binom{2^{m-(i-1)}}{k}$. Wobec tego splątanie wydestylowane z grupy $2^{m-(i-1)}$ par qubitów pod warunkiem, że Alicja i Bob otrzymają te same wyniki pomiarów, jest równe uśrednionemu rzędowi Schmidta stanu maksymalnie splątanego otrzymanego przez Alicję i Boba. Jest ono dane wyrażeniem

$$\begin{aligned} R_i = &\sum_{k=0}^{2^{m-(i-1)}} \alpha^{2(2^{m-(i-1)}-k)}(\sqrt{1-\alpha^2})^{2k}\binom{2^{m-(i-1)}}{k} \times \quad (3.16)\\ &\log_2\binom{2^{m-(i-1)}}{k} . \end{aligned}$$

Wzór 3.16 jest wzorem ogólnym dla dwuqubitowych stanów mieszanych, składających się z czystego stanu splątanego i stanu produktowego ortogonalnego do niego. Przyjmijmy teraz, że czysty stan splątany jest stanem maksymalnie splątanym

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) . \quad (3.17)$$

Wobec tego stan 3.1 przyjmuje postać

$$\rho_{AB} = p|\phi^+\rangle\langle\phi^+|_{AB} + (1-p)\,|01\rangle\,\langle 01|_{AB} . \quad (3.18)$$

Wzór na splątanie wydestylowane z grupy $2^{m-(i-1)}$ par qubitów pod warunkiem, że Alicja i Bob otrzymają te same wyniki pomiarów, dostajemy podstawiając za α we wzorze 3.16 wartość $\frac{1}{\sqrt{2}}$. Po uproszczeniach otrzymujemy wzór

$$R_i = \sum_{k=0}^{2^{m-(i-1)}} \frac{1}{2^{2^{m-(i-1)}}} \binom{2^{m-(i-1)}}{k} \log_2 \binom{2^{m-(i-1)}}{k} . \tag{3.19}$$

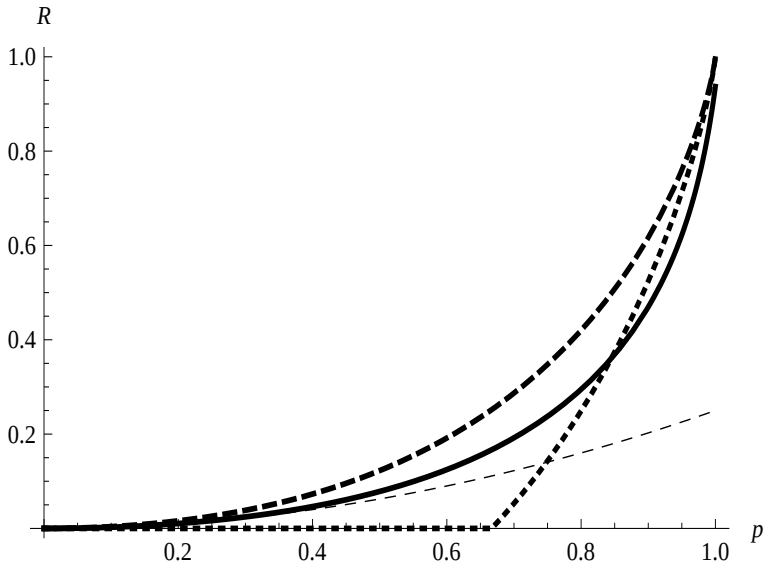
Podstawiając formułę 3.19 do wyrażenia 3.14 możemy obliczyć wydajność naszego protokołu dla stanu splątanego, składającego się ze stanu maksymalnie splątanego i stanu produktowego ortogonalnego do niego.

Na rysunku 3.3 przedstawiono zależność wydajności protokołu bisekcyjnego od parametru p. Ponadto porównano ją ze względną entropią splątania oraz z wydajnościami innych protokołów destylacji splątania, a mianowicie protokołem Bennetta i innych z pracy [7] oraz protokołem haszującym. Liczba kopii stanu 3.18, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$. Zauważmy, że wydajność protokołu bisekcyjnego jest zawsze większa (z wyjątkiem $p = 0$) od wydajności protokołu Bennetta i innych, oraz że w szerokim zakresie parametru p jest ona większa od wydajności protokołu haszującego. Zwróćmy również uwagę, że wydajność protokołu bisekcyjnego jest mniejsza od względnej entropii splątania. Przypomnijmy, że względna entropia splątania jest górnym ograniczeniem na destylowalne splątanie [41].

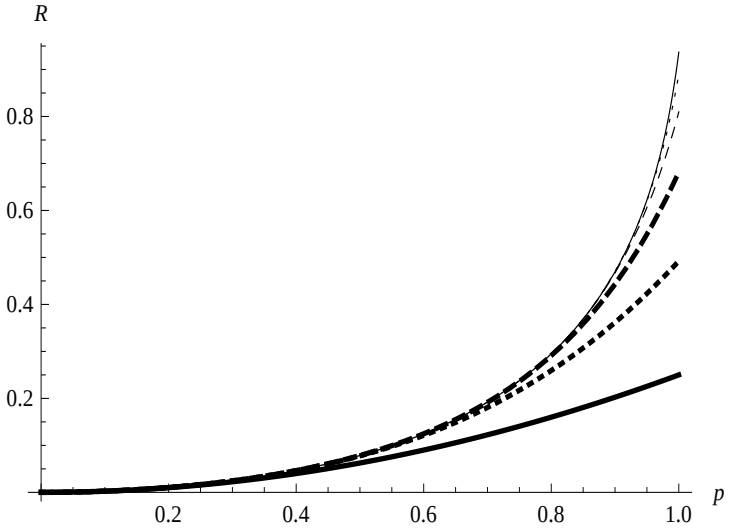
Na rysunku 3.4 przedstawiono zależność wydajności R protokołu bisekcyjnego od parametru p dla różnej liczby kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar. Natomiast w tabeli 3.1 przedstawiono przykładowe wyniki liczbowe dla $p = \frac{2}{3}$. Zauważmy, że wykresy dla $n = 32$ i $n = 64$ praktycznie się pokrywają, a przykładowe wyniki liczbowe są identyczne z dokładnością do sześciu cyfr znaczących. Oznacza to, że protokół jest szybko zbieżny wraz ze wzrostem liczby n.

Tabela 3.1: Wartości wydajności R protokołu bisekcyjnego w zależności od liczby kopii n stanów ρ_{AB}, na których wykonywany jest pierwszy pomiar dla parametru $p = \frac{2}{3}$. Źródło: [70].

n	R
2	$0,111111$
4	$0,158981$
8	$0,16638$
16	$0,166574$
32	$0,166575$
64	$0,166575$



Rysunek 3.3: Zależność wydajności R różnych protokołów destylacji splątania od parametru p: protokół bisekcyjny – linia gruba ciągła, protokół Bennetta i innych z pracy [7] – linia cienka kreskowana, protokół haszujący – linia gruba kropkowana. Linia gruba kreskowana przedstawia względną entropię splątania. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$. Źródło: [70].



Rysunek 3.4: Zależność wydajności R protokołu bisekcyjnego od parametru p dla różnej liczby kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar: $n = 2$ – linia ciągła gruba, $n = 4$ – linia kropkowana gruba, $n = 8$ – linia kreskowana gruba, $n = 16$ – linia kreskowana cienka, $n = 32$ – linia kropkowana cienka, $n = 64$ – linia ciągła cienka. Wykresy dla $n = 32$ i $n = 64$ praktycznie się pokrywają.

3.1.2 Wieloqubitowe stany mieszane

Zastosowanie protokołu destylacji splątania opisanego w punkcie 3.1.1 można rozszerzyć do wielocząstkowych stanów qubitów. Oznaczmy przez t liczbę użytkowników współdzielących $n = 2^m$ kopii stanu $\rho_{ABC...}$ postaci

$$\rho_{ABC...} = p\,|\phi(\alpha)\rangle\,\langle\phi(\alpha)|_{ABC...} + (1-p)\sigma_{ABC...}\ , \tag{3.20}$$

gdzie

$$|\phi(\alpha)\rangle_{ABC...} = \alpha|\underbrace{0\ldots0}_{t}\rangle_{ABC...} + \sqrt{1-\alpha^2}|\underbrace{1\ldots1}_{t}\rangle_{ABC...}\ , \tag{3.21}$$

$$\sigma = \sum_{\text{permutacje}}\sum_{t_0=1}^{t-1} q_{t_0,\text{permutacje}} \left(|1\underbrace{0\ldots0}_{t_0}\underbrace{1\ldots1}_{t-t_0-1}\rangle\langle 1\underbrace{0\ldots0}_{t_0}\underbrace{1\ldots1}_{t-t_0-1}|_{ABC...}\right)\ . \tag{3.22}$$

W stanie opisanym wzorem 3.22 występują ciągi o długości t, zawierające t_0 stanów $|0\rangle$ oraz $t-t_0$ stanów $|1\rangle$. Ciągi takie sumujemy po wartościach t_0 i permutacjach. Protokół przebiega analogicznie jak w przypadku stanów dwuqubitowych. Wszyscy użytkownicy wykonują pomiar dany operatorami rzutowymi 3.3. Przerywają oni protokół na danej grupie qubitów, gdy każdy z nich otrzyma taką samą wartość k. Brak koincydencji między wszystkimi użytkownikami skutkuje bisekcją. Wydajność w takim protokole przedstawiają wzory 3.14 i 3.16. Należy jednak podkreślić, że destylowane są tutaj wieloqubitowe stany splątane typu GHZ, a nie – jak w poprzednim punkcie – dwuqubitowe stany maksymalnie splątane.

3.1.3 Dwucząstkowe mieszane stany quditów

W tym punkcie uogólnimy bisekcyjny protokół destylacji na przypadek pewnych dwucząstkowych stanów quditów [71]. Przez d oznaczymy wymiar quditu. Rozważymy przypadek dwóch stanów różniących się złożonością zawartego w nich stanu separowalnego.

W pierwszym przypadku stan ρ_{AB} ma postać

$$\rho_{AB} = p\,|\phi_d\rangle\,\langle\phi_d|_{AB} + (1-p)\,|01\rangle\,\langle 01|_{AB}\ , \tag{3.23}$$

gdzie

$$|\phi_d\rangle_{AB} = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle_{AB}\ . \tag{3.24}$$

Stan 3.23 jest stanem mieszanym, składającym się ze stanu maksymalnie splątanego dwóch quditów i stanu produktowego ortogonalnego do niego. Aby wydestylować splątanie z n kopii tego stanu, Alicja i Bob stosują opisany wcześniej protokół bisekcyjny,

ale z innymi operatorami rzutowymi. Operatory te są dane wzorem

$$P_k = \sum_{\text{permutacje}} \bar{P}_1^{\otimes k} \otimes \bar{P}_0^{\otimes(n-k)} , \tag{3.25}$$

gdzie

$$\begin{aligned} \bar{P}_1 &= |1\rangle\langle 1| , \\ \bar{P}_0 &= \sum_{\substack{i=0,\\ i\neq 1}}^{d-1} |i\rangle\langle i| . \end{aligned} \tag{3.26}$$

Splątanie wydestylowane z grupy $2^{m-(i-1)}$ stanów ρ_{AB} pod warunkiem, że Alicja i Bob otrzymają te same wyniki pomiarów, wynosi

$$\begin{aligned} R_i = {} & \frac{1}{d^{2^{m-(i-1)}}} \sum_k \binom{2^{m-(i-1)}}{k} (d-1)^{2^{m-(i-1)}-k} \times \\ & \log_2 \binom{2^{m-(i-1)}}{k} (d-1)^{2^{m-(i-1)}-k} . \end{aligned} \tag{3.27}$$

Czynnik $\binom{2^{m-(i-1)}}{k}(d-1)^{2^{m-(i-1)}-k}$ we wzorze 3.27 jest rzędem Schmidta stanu maksymalnie splątanego, który Alicja i Bob dostaną, jeżeli w wyniku pomiaru oboje otrzymają rezultat k. Aby otrzymać całkowitą wydajność protokołu, należy podstawić R_i dane wyrażeniem 3.27, do wzoru 3.14.

Zależność wydajności protokołu bisekcyjnego od parametru p dla stanu 3.23 dla różnych wymiarów quditów d przedstawiono na rysunku 3.5. Widzimy, że wraz ze wzrostem wymiaru d i parametru p wzrasta wydajność protokołu. Nie jest to zaskakujące, ponieważ dla $p = 1$ stany te zawierają $\log d$ e-bitów.

W drugim przypadku stan ρ_{AB} ma postać

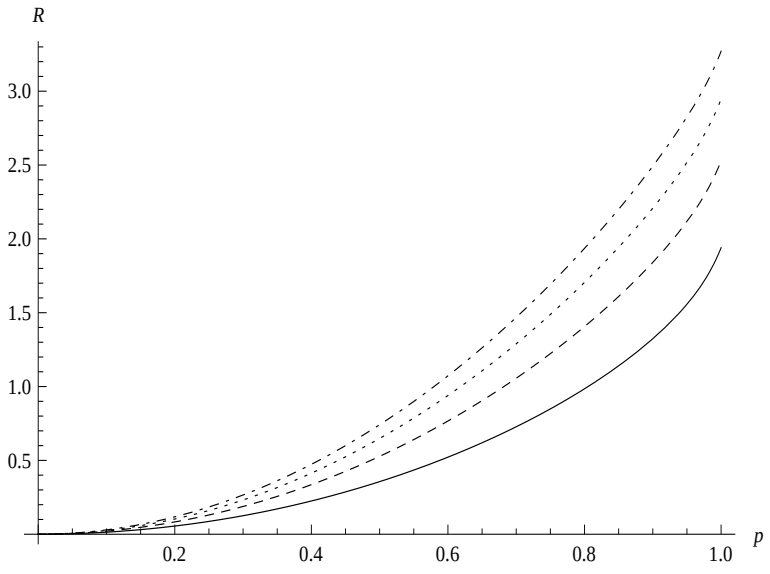
$$\rho_{AB} = p\,|\phi_d\rangle\langle\phi_d|_{AB} + (1-p) \sum_{\substack{i=0,\\ i \text{ parzyste}}}^{d-1} q_i\,|i(i+1)\rangle\langle i(i+1)|_{AB} . \tag{3.28}$$

W tej sytuacji stan separowalny jest bardziej złożony i składa się z $\frac{d}{2}$ stanów produktowych. Bardziej złożone są również operatory rzutowe, jakich muszą użyć Alicja i Bob, aby wydestylować splątanie

$$P_k = \sum_{\text{permutacje}} \bar{P}_1^{\otimes k} \otimes \bar{P}_0^{\otimes(n-k)} , \tag{3.29}$$

gdzie

$$\begin{aligned} \bar{P}_1 &= \sum_{i=1,\ i \text{ nieparzyste}}^{d-1} |i\rangle\langle i| , \\ \bar{P}_0 &= \sum_{i=0,\ i \text{ parzyste}}^{d-1} |i\rangle\langle i| . \end{aligned} \tag{3.30}$$



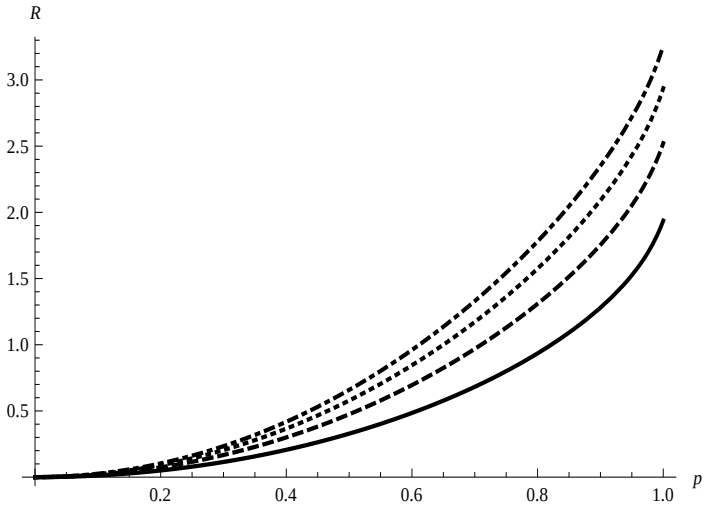
Rysunek 3.5: Zależność wydajności protokołu bisekcyjnego R od parametru p dla stanu 3.23 dla różnych wymiarów quditów d: $d = 4$ – linia ciągła, $d = 6$ – linia kreskowana, $d = 8$ – linia kropkowana, $d = 10$ – linia kreskowano-kropkowana. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$.

Splątanie wydestylowane z grupy $2^{m-(i-1)}$ stanów ρ_{AB} pod warunkiem, że Alicja i Bob otrzymają te sam wyniki pomiarów jest dane wyrażeniem

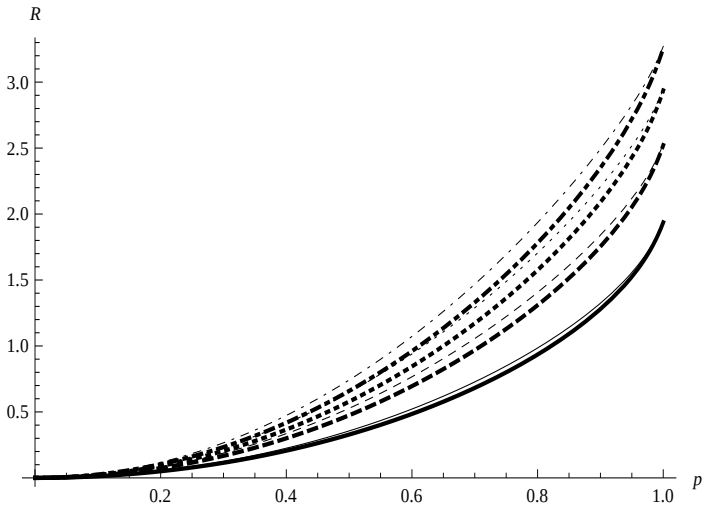
$$R_i = \frac{1}{d^{2^{m-(i-1)}}} \sum_{k}^{2^{m-(i-1)}} \binom{2^{m-(i-1)}}{k} \left(\frac{d}{2}\right)^{2^{m-(i-1)}} \times \log_2 \binom{2^{m-(i-1)}}{k} \left(\frac{d}{2}\right)^{2^{m-(i-1)}} . \tag{3.31}$$

Czynnik $\binom{2^{m-(i-1)}}{k}(\frac{d}{2})^{2^{m-(i-1)}}$ jest rzędem Schmidta stanu maksymalnie splątanego, który Alicja i Bob otrzymają, jeżeli oboje uzyskają w wyniku pomiaru rezultat k. Podobnie jak w poprzednim przypadku, całkowitą wydajność protokołu otrzymamy podstawiając R_i dane wyrażeniem 3.31, do wzoru 3.14.

Zależność wydajności protokołu bisekcyjnego od parametru p dla liczby kopii stanu 3.28 $n = 64$ dla różnych wartości d przedstawiono na rysunku 3.6. Widzimy, że podobnie jak dla stanu 3.23, wraz ze wzrostem wymiaru d i parametru p wzrasta wydajność protokołu. Na rysunku 3.7 porównano wydajność R protokołu bisekcyjnego dla obydwu przypadków.



Rysunek 3.6: Zależność wydajności protokołu bisekcyjnego R od parametru p dla stanu 3.28 dla różnych wymiarów quditów d: $d = 4$ – linia ciągła, $d = 6$ – linia kreskowana, $d = 8$ – linia kropkowana, $d = 10$ – linia kreskowano-kropkowana. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$.



Rysunek 3.7: Porównanie zależności wydajności protokołu bisekcyjnego R od parametru p dla stanów 3.23 i 3.28 dla różnych wymiarów quditów d. Dla stanu 3.23: $d = 4$ – linia ciągła, $d = 6$ – linia kreskowana, $d = 8$ – linia kropkowana, $d = 10$ – linia kreskowano-kropkowana. Dla stanu 3.28: $d = 4$ – linia gruba ciągła, $d = 6$ – linia gruba kreskowana, $d = 8$ – linia gruba kropkowana, $d = 10$ – linia gruba kreskowano-kropkowana. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$.

3.2 Ulepszenie protokołu bisekcyjnego

W pracy [70] przedstawiono protokół destylacji splątania dla stanu 3.17, który osiąga większą wydajność niż oryginalny protokół bisekcyjny. Protokół ten łączy ze sobą protokół bisekcyjny i protokół haszujący. Jego kroki są następujące:

1. Alicja i Bob dokonują na n parach stanu 3.17 pomiaru danego przez operatory rzutowe 3.3.

2. Jeżeli Alicja i Bob otrzymają te sam wyniki pomiarów, to znaczy $k_A = k_B$, wtedy dostaną stan maksymalnie splątany o rzędzie Schmidta $\binom{n}{k_A}$ i przerywają protokół.

Jeżeli Alicja i Bob otrzymają różne wyniki pomiarów, to znaczy $k_A \neq k_B$, to wykonują jedną z dwóch czynności:

a) Stosują na otrzymanym stanie protokół haszujący.

b) Dzielą n par qubitów na dwie równe grupy i na każdej grupie powtarzają czynności z punktów 1 i 2 (z n zastąpionym przez $n/2$).

Alicja i Bob wybierają tę czynność, która daje większą wydajność protokołu.

Obecnie wyprowadzimy wzór rekurencyjny na wydajność tego protokołu. Załóżmy, że Alicja i Bob otrzymali w pierwszym kroku wyniki pomiarów k_A i k_B. Zauważmy, że możliwe są tylko wyniki pomiarów dla których $k_B \geqslant k_A$. W takim przypadku Alicja i Bob otrzymają po pomiarze następujący stan

$$\begin{aligned} \rho(n,k_A,k_B)_{AB} &= \frac{1}{p(n,k_A,k_B)} P^n_{k_A} P^n_{k_B} [|\phi^+\rangle\langle\phi^+|^{\otimes(n-(k_B-k_A))}_{AB} \otimes \\ &\quad |01\rangle\langle 01|^{\otimes k_B-k_A}_{AB} + \text{permutacje}] P^n_{k_A} P^n_{k_B}, \end{aligned} \tag{3.32}$$

gdzie

$$p(n,k_A,k_B) = \binom{n}{n-(k_B-k_A)} \binom{n-(k_B-k_A)}{k_A} 2^{-(n-(k_B-k_A))} . \tag{3.33}$$

Prawdopodobieństwo tego, że Alicja i Bob otrzymają w pierwszym kroku rezultaty k_A i k_B jest dane przez iloczyn prawdopodobieństwa, że wśród n kopii stanu 3.32 znajduje się $n-(k_B-k_A)$ stanów maksymalnie splątanych $|\phi^+\rangle$ i (k_B-k_A) stanów produktowych $|01\rangle$ oraz prawdopodobieństwa, że w wyniku pomiaru na $n-(k_B-k_A)$ kopiach stanów maksymalnie splątanych otrzymają rezultat k_A. Pierwsze z tych prawdopodobieństw wynosi

$$p(n,k_A,k_B) = p^{n-(k_B-k_A)}(1-p)^{k_B-k_A} \binom{n}{n-(k_B-k_A)} . \tag{3.34}$$

Drugie z tych prawdopodobieństw jest równe

$$\binom{n-(k_B-k_A)}{k_A} 2^{-(n-(k_B-k_A))} \ . \tag{3.35}$$

Wobec tego prawdopodobieństwo tego, że Alicja i Bob otrzymają w pierwszym kroku wyniki pomiarów k_A i k_B, wynosi

$$P(n,k_A,k_B) \ = \ p^{n-(k_B-k_A)}(1-p)^{k_B-k_A}p(n,k_A,k_B) \ . \tag{3.36}$$

Załóżmy, że w i-tym kroku Alicja i Bob otrzymali rezultaty k_A i k_B, i zdecydowali się zastosować protokół haszujący. Zauważmy, że stan po pomiarze będzie dany wyrażeniem analogicznym do 3.32

$$\begin{aligned}\rho(m,k_A,k_B)_{AB} \ &= \ \frac{1}{p(m,k_A,k_B)} P^m_{k_A}P^m_{k_B}[|\phi^+\rangle\langle\phi^+|^{\otimes(m-(k_B-k_A))}_{AB} \otimes \\ &\quad |01\rangle\langle 01|^{\otimes(k_B-k_A)}_{AB} + \text{permutacje}]P^m_{k_A}P^m_{k_B},\end{aligned} \tag{3.37}$$

gdzie

$$p(m,k_A,k_B) \ = \ \binom{m}{m-(k_B-k_A)}\binom{m-(k_B-k_A)}{k_A}2^{-(m-(k_B-k_A))} \tag{3.38}$$

i $m=\frac{n}{2^{(i-1)}}$. Wynika to z faktu, że operatory rzutowe spełniają równanie

$$(P^{n/2}_{x'}\otimes P^{n/2}_{x''})P^n_x = (P^{n/2}_{x'}\otimes P^{n/2}_{x''})\delta_{x'+x'',x}. \tag{3.39}$$

Wydajność protokołu haszującego jest dana przez jedną z dwóch koherentnych informacji, to znaczy

$$I_{c,A\to B}(\rho_{AB}) \ = \ S(\rho_B)-S(\rho_{AB}), \tag{3.40}$$

gdy komunikacja klasyczna przebiega od Alicji do Boba, lub

$$I_{c,B\to A}(\rho_{AB}) \ = \ S(\rho_A)-S(\rho_{AB}), \tag{3.41}$$

gdy komunikacja klasyczna przebiega od Boba do Alicji. Entropia podukładu Alicji jest równa

$$S(m,k_A,k_B) \ = \ \log_2\binom{m}{k_A} \ , \tag{3.42}$$

gdzie $\binom{m}{k_A}$ jest liczbą ciągów m-bitowych o wadze Hamminga k_A. Natomiast entropia podukładu Boba wynosi

$$S(m,k_A,k_B) \ = \ \log_2\binom{m}{k_B} \ , \tag{3.43}$$

gdzie $\binom{m}{k_B}$ jest liczbą ciągów m-bitowych o wadze Hamminga k_B. Ponieważ stan całego układu Alicji i Boba po pomiarze jest stanem mieszanym, składającym się z $\binom{m}{m-(k_B-k_A)}$ czystych stanów ortogonalnych, które występują z równymi wagami, więc

$$S(m,k_A,k_B) \;=\; \log_2 \binom{m}{m-(k_B-k_A)}. \tag{3.44}$$

Ostatecznie wydajność protokołu haszującego dana jest wyrażeniem

$$I_c(m,k_A,k_B) \;=\; \log_2 \left[\max\left\{ \binom{m}{k_A}, \binom{m}{k_B} \right\} \right] - \log_2 \binom{m}{m-(k_B-k_A)}. \tag{3.45}$$

Maksimum w powyższym wzorze występuje, ponieważ Alicja i Bob będą destylować splątanie za pomocą protokołu haszującego, który daje większą wydajność.

Załóżmy teraz, że w k-tym kroku Alicja i Bob zdecydowali się podzielić m par qubitów na dwie równe grupy i na każdej grupie dokonali pomiaru danego przez operatory rzutowe 3.3. Obliczmy prawdopodobieństwo i stan po pomiarze w przypadku, gdy Alicja i Bob otrzymają w wyniku pomiaru rezultaty k'_A i k'_B na pierwszej grupie par qubitów i rezultaty k''_A i k''_B na drugiej grupie par qubitów pod warunkiem, że w k-tym kroku uzyskali rezultaty k_A i k_B. Ponieważ Alicja i Bob dokonują pomiarów na stanie 3.37, ich wyniki spełniają następujące zależności

$$k'_A + k''_A \;=\; k_A \;, \tag{3.46}$$

$$k'_B + k''_B \;=\; k_B \;, \tag{3.47}$$

a prawdopodobieństwo ich otrzymania wynosi

$$p(k'_A,k'_B,k''_A,k''_B|m,k_A,k_B) \;=\; \frac{p(m/2,k'_A,k'_B)p(m/2,k''_A,k''_B)}{p(m,k_A,k_B)} \;. \tag{3.48}$$

Z kolei stan po pomiarze przyjmuje postać

$$\rho(m/2,k'_A,k'_B)_{AB} \;\otimes\; \rho(m/2,k''_A,k''_B)_{AB} \;. \tag{3.49}$$

Wobec tego wydajność protokołu będzie dana następującym wzorem rekurencyjnym

$$\begin{aligned} R(m,k_A,k_B) \;=\; & \sum_{k'_A=k'_{A\,\mathsf{min}}}^{k'_{A\,\mathsf{max}}} \sum_{k'_B=k'_{B\,\mathsf{min}}}^{k'_{B\,\mathsf{max}}} \\ & p(k'_A,k'_B,k_A-k'_A,k_B-k'_B|m,k_A,k_B) \\ & [R(m/2,k'_A,k'_B)+R(m/2,k_A-k'_A,k_B-k'_B)] \;, \end{aligned} \tag{3.50}$$

gdzie

$$k_{A\,\mathsf{min}} \;=\; \max\{0,k_A-\frac{m}{2}\} \;, \tag{3.51}$$

$$k_{A\,\mathsf{max}} \;=\; \min\{k_A,\frac{m}{2}\} \;, \tag{3.52}$$

$$k_{B\,\mathsf{min}} \;=\; \max\{0,k_B-\frac{m}{2}\} \;, \tag{3.53}$$

$$k_{B\,\mathsf{max}} \;=\; \min\{k_B,\frac{m}{2}\} \;. \tag{3.54}$$

Alicja i Bob wybiorą optymalny protokół, to znaczy albo zastosują protokół haszujący, albo podzielą m par qubitów na dwie równe grupy i na każdej grupie dokonają pomiaru danego przez operatory rzutowe 3.3. Ich wybór zależy od tego, w którym przypadku uzyskają większą wydajność. Wobec tego zmodyfikujemy wzór 3.50 w następujący sposób

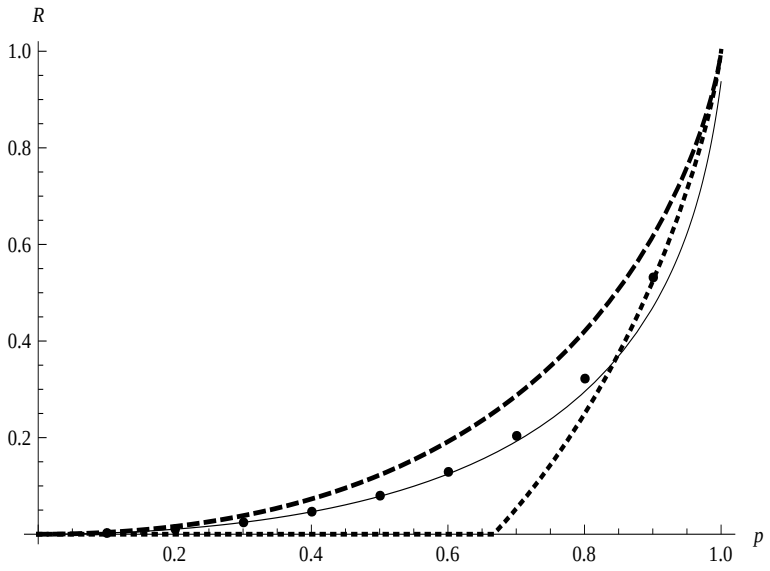
$$\begin{aligned} R(m,k_A,k_B) \;=\; \max\Big\{ & I_c(m,k_A,k_B), \\ & \sum_{k_A^{'}=k_{A\,\min}^{'}}^{k_{A\,\max}^{'}} \sum_{k_B^{'}=k_{B\,\min}^{'}}^{k_{B\,\max}^{'}} \\ & p(k_A^{'},k_B^{'},k_A-k_A^{'},k_B-k_B^{'}|m,k_A,k_B) \\ & [R(m/2,k_A^{'},k_B^{'})+R(m/2,k_A-k_A^{'},k_B-k_B^{'})]\Big\}\ . \end{aligned} \tag{3.55}$$

Należy podkreślić, że ostateczne wyrażenie należy uśrednić po wynikach pomiarów otrzymanych przez Alicję i Boba w pierwszym kroku.

Z konstrukcji protokołu wynika, że ma on wydajność nie mniejszą zarówno od protokołu bisekcyjnego jak i od protokołu haszującego. Porównanie wydajności protokołu bisekcyjno-haszującego z wydajnością innych protokołów w zastosowaniu do destylacji splątania ze stanu 3.17 przedstawiono na rysunku 3.8. Ponadto w tabeli 3.2 przedstawiono zależność wydajności protokołu bisekcyjno-haszującego od liczby kopii stanu 3.17, na których wykonywany jest pierwszy pomiar dla parametru $p=\frac{2}{3}$. Dla porównania podano analogiczne wyniki dla protokołu bisekcyjnego. Można zauważyć, że dla $n \geqslant 8$ wydajność protokołu bisekcyjno-haszującego jest większa od wydajności protokołu bisekcyjnego.

Tabela 3.2: Wartości wydajności R_{bh} dla protokołu bisekcyjno-haszującego i R_b dla protokołu bisekcyjnego w zależności od liczby kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar dla parametru $p=\frac{2}{3}$. Źródło: [70].

n	R_{bh}	R_b
2	$0,111111$	$0,111111$
4	$0,158981$	$0,158981$
8	$0,173419$	$0,16638$
16	$0,175076$	$0,166574$
32	$0,175129$	$0,166575$
64	$0,175129$	$0,166575$



Rysunek 3.8: Zależność wydajności R różnych protokołów destylacji splątania od parametru p: protokół bisekcyjny – linia cienka ciągła, protokół bisekcyjno-haszujący – kropki, protokół haszujący – linia gruba kropkowana. Linia gruba kreskowana przedstawia względną entropię splątania. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$. Źródło: [70].

3.3 Protokół filtrująco-haszujący

W tym punkcie porównamy protokół bisekcyjny z protokołem będącym połączeniem protokołu filtrującego [73, 74, 75, 76, 77] i protokołu haszującego. Nasze rozważania będą dotyczyć stanu mieszanego, składającego się ze stanu maksymalnie splątanego i stanu produktowego ortogonalnego do niego, to znaczy

$$\rho_{AB} = p|\phi^+\rangle\langle\phi^+|_{AB} + (1-p)\,|01\rangle\,\langle 01|_{AB} \ , \tag{3.56}$$

gdzie

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \ . \tag{3.57}$$

Przeanalizujemy następujący scenariusz protokołu filtrującego. Alicja dokonuje lokalnego pomiaru na swoim qubicie danego przez operatory Krausa

$$\begin{aligned} P_S &= \sqrt{\epsilon}\,|0\rangle\,\langle 0|_A + |1\rangle\,\langle 1|_A \ , \\ P_F &= \sqrt{1-\epsilon}\,|0\rangle\,\langle 0|_A \ , \end{aligned} \tag{3.58}$$

natomiast Bob nie mierzy swojego qubitu. Parametr ϵ przyjmuje wartości z zakresu od 0 do 1. Postać nieunormowanego stanu po pomiarze w przypadku, gdy Alicja otrzyma rezultat S, można obliczyć z następującego wzoru

$$\rho^{'}_{AB} = P_S \otimes I \rho_{AB} P_S \otimes I \ . \tag{3.59}$$

Jego jawna postać wygląda następująco

$$\rho_{AB}^{'} = p|\phi^{+}(\epsilon)\rangle\langle\phi^{+}(\epsilon)|_{AB} + (1-p)\epsilon\,|01\rangle\,\langle 01|_{AB}\ , \tag{3.60}$$

gdzie

$$|\phi^{+}(\epsilon)\rangle_{AB} = \frac{1}{\sqrt{2}}(\sqrt{\epsilon}\,|00\rangle_{AB} + |11\rangle_{AB})\ . \tag{3.61}$$

Natomiast unormowany stan jest dany wyrażeniem

$$\rho_{AB}^{''} = \frac{1}{p_S}\rho_{AB}^{'}\ , \tag{3.62}$$

gdzie $p_S = \mathrm{Tr}(\rho_{AB}^{'})$ jest prawdopodobieństwem otrzymania przez Alicję rezultatu S. Jeżeli Alicja i Bob posiadają wiele kopii takich stanów, wtedy mogą zastosować protokół haszujący i wydestylować splątanie z wydajnością równą koherentnej informacji $I_{c,A\rightarrow B}(\rho_{AB}^{''})$ unormowanego stanu $\rho_{AB}^{''}$ w przypadku, gdy Alicja przesyła klasyczną informację do Boba. Żeby otrzymać wydajność całego protokołu musimy pomnożyć koherentną informację przez prawdopodobieństwo p_S otrzymania rezultatu S. Obliczmy tę wydajność

$$\begin{aligned}
R_f &= p_S I_{c,A\rightarrow B}(\rho_{AB}^{''}) = p_S(S(\rho_B^{''}) - S(\rho_{AB}^{''})) = \\
&= p_S(-\mathrm{Tr}(\rho_B^{''}\log_2\rho_B^{''}) + \mathrm{Tr}(\rho_{AB}^{''}\log_2\rho_{AB}^{''})) = \\
&= -\mathrm{Tr}(\rho_B^{'}\log_2\rho_B^{'}) + \mathrm{Tr}(\rho_B^{'}\log_2 p_S) + \mathrm{Tr}(\rho_{AB}^{'}\log_2\rho_{AB}^{'}) - \mathrm{Tr}(\rho_{AB}^{'}\log_2 p_S) = \\
&= -\mathrm{Tr}(\rho_B^{'}\log_2\rho_B^{'}) + \mathrm{Tr}(\rho_{AB}^{'}\log_2\rho_{AB}^{'}) = \\
&= S(\rho_B^{'}) - S(\rho_{AB}^{'}) = I_{c,A\rightarrow B}(\rho_{AB}^{'})\ .
\end{aligned} \tag{3.63}$$

Wobec tego wydajność całego protokołu jest równa koherentnej informacji $I_{c,A\rightarrow B}(\rho_{AB}^{'})$ nieunormowanego stanu $\rho_{AB}^{'}$. Podobnie, gdy Bob przesyła klasyczną informację do Alicji, wydajność całego protokołu jest równa koherentnej informacji $I_{c,B\rightarrow A}(\rho_{AB}^{'})$ nieunormowanego stanu $\rho_{AB}^{'}$. Ponieważ chcemy uzyskać jak największą wydajność, zoptymalizujemy obydwie koherentne informacje nieunormowanego stanu $\rho_{AB}^{'}$ ze względu na parametr ϵ, a następnie weźmiemy większą z nich. Ostatecznie maksymalna wydajność, jaką możemy otrzymać wynosi

$$R_f = \max\{\max_{\epsilon} I_{c,A\rightarrow B}(\rho_{AB}^{'}), \max_{\epsilon} I_{c,B\rightarrow A}(\rho_{AB}^{'}), 0\}\ . \tag{3.64}$$

Wyniki porównujące wydajność protokołu filtrująco-haszującego (R_f) z wydajnością protokołu bisekcyjno-haszującego (R_{bh}) i protokołu bisekcyjnego (R_b) dla konkretnych wartości p przedstawiono w tabeli 3.3. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w przypadku protokołu bisekcyjno-haszującego i bisekcyjnego, wynosi $n = 64$. Widzimy, że wydajność protokołu bisekcyjno-haszującego jest większa od wydajności protokołu filtrująco-haszującego dla wszystkich przedstawionych wartości

parametru p. Natomiast wydajność protokołu bisekcyjnego jest większa od wydajności protokołu filtrująco-haszującego dla wszystkich przedstawionych wartości parametru p oprócz $p = 0,9$.

Tabela 3.3: Porównanie wydajności protokołu filtrująco-haszującego (R_f), protokołu bisekcyjno-haszującego (R_{bh}) i protokołu bisekcyjnego (R_b) dla różnych wartości parametru p. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar wynosi $n = 64$.

p	R_f	R_{bh}	R_b
$0,1$	$0,00128807$	$0,00252427$	$0,00252424$
$0,2$	$0,00608361$	$0,01039192$	$0,0103882$
$0,3$	$0,01598048$	$0,0245307$	$0,0244754$
$0,4$	$0,0310459$	$0,04668578$	$0,0463282$
$0,5$	$0,0495459$	$0,07984542$	$0,078389$
$0,6$	$0,0976421$	$0,12910356$	$0,124628$
$0,7$	$0,160549$	$0,20363273$	$0,192043$
$0,8$	$0,280058$	$0,32225551$	$0,294733$
$0,9$	$0,520997$	$0,53181998$	$0,469567$

ROZDZIAŁ 4

Destylacja splątania ze stanów mieszanych składających się z dwóch czystych stanów splątanych i czystego stanu produktowego

W tym rozdziale opiszemy protokół destylacji splątania dla mieszanego stanu splątanego o rzędzie macierzy gęstości równym trzy.

4.1 Opis protokołu

W pracy [71] przedstawiono zastosowanie protokołu bisekcyjnego w połączeniu z jednokierunkowym protokłem haszującym do destylacji splątania z mieszanego stanu splątanego rzędu 3. Stan ten składa się z dwóch czystych stanów splątanych różniących się fazą i stanu produktowego ortogonalnego do nich, to jest

$$\rho_{AB} = p\rho^{'}_{AB} + (1-p)\left|01\right\rangle\left\langle 01\right|_{AB} , \tag{4.1}$$

gdzie

$$\rho^{'}_{AB} = q|\phi^{+}(\alpha)\rangle\langle\phi^{+}(\alpha)|_{AB} + (1-q)|\phi^{-}(\alpha)\rangle\langle\phi^{-}(\alpha)|_{AB}, \tag{4.2}$$

natomiast

$$|\phi^{+}(\alpha)\rangle_{AB} = \alpha\left|00\right\rangle_{AB} + \sqrt{1-\alpha^2}\left|11\right\rangle_{AB} , \tag{4.3}$$

$$|\phi^{-}(\alpha)\rangle_{AB} = \alpha\left|00\right\rangle_{AB} - \sqrt{1-\alpha^2}\left|11\right\rangle_{AB} . \tag{4.4}$$

Wyobraźmy sobie, że Alicja i Bob posiadają $n = 2^m$ kopii stanu 4.1. Wobec tego całkowity stan ma postać

$$\begin{aligned}
\rho_{AB}^{\otimes n} &= p^n \rho_{AB}^{'\otimes n} + \\
&+ p^{(n-1)}(1-p)[\rho_{AB}^{'\otimes(n-1)} \otimes |01\rangle\langle 01|_{AB} + \\
&+ \text{permutacje}] + \\
&+ p^{(n-2)}(1-p)^2[\rho_{AB}^{'\otimes(n-2)} \otimes |01\rangle\langle 01|_{AB}^{\otimes 2} + \\
&+ \text{permutacje}] + \\
&+ \cdots + (1-p)^n[|01\rangle\langle 01|_{AB}^{\otimes n}] \; .
\end{aligned} \tag{4.5}$$

W powyższym wzorze słowo *permutacje* oznacza wszystkie możliwe permutacje iloczynu tensorowego $n-k$ stanów $\rho_{AB}^{'}$ i k stanów $|01\rangle\langle 01|$. Alicja i Bob destylują splątanie, stosując do $n = 2^m$ kopii stanu ρ_{AB} protokół bisekcyjny przedstawiony w podrozdziale 3.1. Istnieje jednak różnica pomiędzy obydwoma przypadkami. O ile w przypadku destylacji splątania ze stanów 3.1 i otrzymania zarówno przez Alicję i Boba wyniku pomiaru k, stan po pomiarze jest stanem maksymalnie splątanym, to w przypadku destylacji splątania ze stanu 4.5 i otrzymania zarówno przez Alicję jak i Boba wyniku pomiaru k, stan po pomiarze, który oznaczymy przez ρ_{kAB}^n, jest nadal stanem mieszanym. Jak się okaże w następnym podrozdziale, jest to stan o dodatniej koherentnej informacji. Wobec tego, Alicja i Bob po otrzymaniu wielu kopii takiego stanu mogą wydestylować z niego splątanie za pomocą protokołu haszującego z wydajnością $I_c(\rho_{kAB}^n)$. Powtarzając rozumowanie z podrozdziału 3.1.1 i zastępując logarytm z rzędu Schmidta we wzorze 3.16 przez koherentną informację 2.43, dostajemy następujące wyrażenie na wydajność całego protokołu

$$R = \frac{1}{2^m}\sum_{i=1}^{m} p^{2^{m-(i-1)}}(2^{i-1}R_i - 2^i R_{i+1}) \; , \tag{4.6}$$

gdzie

$$R_i = \sum_{k=0}^{2^{m-(i-1)}} \alpha^{2(2^{m-(i-1)}-k)}(\sqrt{1-\alpha^2})^{2k}\binom{2^{m-(i-1)}}{k} I_c(\rho_{kAB}^{2^{m-(i-1)}}) \; , \tag{4.7}$$

oznacza splątanie wydestylowane z grupy $2^{m-(i-1)}$ stanów ρ_{AB} pod warunkiem, że Alicja i Bob otrzymali ten sam wynik pomiaru i $R_{m+1} = 0$.

W dalszych punktach tego rozdziału skupimy się na znalezieniu wzoru na koherentną informację występującą w powyższym wzorze. W tym celu sięgniemy do opisanych w punkcie 2.4 metod matematycznych.

4.2 Obliczenie koherentnej informacji dla stanu po pomiarze

Jeżeli zarówno Alicja jak i Bob w i-tym kroku otrzymają w wyniku pomiaru ten sam wynik k, wtedy stan po pomiarze będzie dany wzorem

$$\rho_{kAB}^{n} = \frac{P_{kA}P_{kB}\rho_{AB}^{\otimes n}P_{kA}P_{kB}}{\mathsf{Tr}(P_{kA}P_{kB}\rho_{AB}^{\otimes n}P_{kA}P_{kB})} , \tag{4.8}$$

gdzie $n = 2^{m-(i-1)}$. Zgodnie z definicją podaną we wzorze 2.43 koherentna informacja dla stanu po pomiarze ρ_{kAB}^{n} będzie miała postać

$$I_c(\rho_{kAB}^{n}) = S(\rho_{kB}^{n}) - S(\rho_{kAB}^{n}) . \tag{4.9}$$

Entropia podukładu Boba jest równa rzędowi operatora rzutowego P_k i wynosi

$$S(\rho_{kB}^{n}) = \log_2 \binom{n}{k} . \tag{4.10}$$

Chcąc obliczyć entropię całego układu, musimy znaleźć wartości własne stanu ρ_{kAB}^{n}. Zauważmy, że stan ten ma takie same wartości własne jak stan

$$\rho_{k}^{n} = \frac{P_k\rho^{\otimes n}P_k}{\mathsf{Tr}(P_k\rho^{\otimes n}P_k)} . \tag{4.11}$$

W powyższym wzorze ρ jest stanem postaci

$$\rho = x\,|+\rangle\langle+| + (1-x)\frac{I}{2} , \tag{4.12}$$

gdzie $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $x = 2q - 1$, natomiast I oznacza dwuwymiarową macierz jednostkową. Wynika to z faktu, że stan ρ_{kAB}^{n} można przekształcić w stan ρ_{k}^{n} za pomocą operacji unitarnej. Wystarczy, że na każdej parze qubitów AB zastosujemy operację unitarną C-NOT, gdzie qubit A jest qubitem kontrolnym, a qubit B jest qubitem docelowym. Wobec powyższego wzór na koherentną informację sprowadza się do następującego wyrażenia

$$I_c(\rho_{kAB}^{n}) = \log_2 \binom{n}{k} - S(\rho_{k}^{n}) . \tag{4.13}$$

Znalezieniu wartości własnych stanu ρ_{k}^{n} poświęcimy kolejny podrozdział. Alternatywne wyprowadzenie wzoru na wartości własne przedstawimy w Dodatku.

4.2.1 Wartości własne stanu ρ_{k}^{n}

Bez straty ogólności, w celu uproszczenia obliczeń, wszelkie rozważania dotyczyć będą stanu nieunormowanego postaci

$$\widetilde{\rho}_{k}^{n} = P_k\rho^{\otimes n}P_k . \tag{4.14}$$

Zauważmy, że powyższy stan możemy zapisać następująco

$$\widetilde{\rho}_k^n = \frac{1}{2^n}\sum_{l=0}^{k} x^{2l} D_l^k \ , \tag{4.15}$$

gdzie

$$D_l^k = \sum_{x,y;d(x,y)=2l} |x\rangle \langle y| \ . \tag{4.16}$$

Niech $\mathcal{H}_k^n$ oznacza przestrzeń Hilberta rozpiętą na wektorach składających się z n qubitów i wadze Hamminga równej k w bazie standardowej. We wzorze 4.16 $|x\rangle$ i $|y\rangle$ są wektorami bazowymi z tej przestrzeni (to jest iloczynami tensorowymi k wektorów $|1\rangle$ i $n-k$ wektorów $|0\rangle$), natomiast $d(x,y)$ oznacza odległość Hamminga pomiędzy ciągami bitowymi x oraz y.

W celu pokazania, że stan $\widetilde{\rho}_k^{\otimes n}$ ma postać 4.15, zapiszemy go następująco

$$\widetilde{\rho}_k^n = P_k\Big[\frac{x}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) + \frac{1-x}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)\Big]^{\otimes n} P_k \ , \tag{4.17}$$

oraz podstawimy

$$\begin{aligned} |0\rangle\langle 0| &= P_{00} \ , \\ |1\rangle\langle 1| &= P_{11} \ , \\ |0\rangle\langle 1| &= P_{01} \ , \\ |1\rangle\langle 0| &= P_{10} \ . \end{aligned} \tag{4.18}$$

Wobec tego wzór 4.17 przyjmie postać

$$\begin{aligned} \widetilde{\rho}_k^n = P_k\Big[\frac{x}{2}(P_{01}+P_{10}) \ + \ \frac{1}{2}(P_{11}+P_{00})\Big]^{\otimes n} P_k = \\ = \Big(\frac{1}{2}\Big)^n \sum_{l=0}^{n} x^l P_k \hat{\mathcal{S}}\Big[(P_{01}+P_{10})^{\otimes l} \ \otimes \ (P_{00}+P_{11})^{\otimes(n-l)}\Big] P_k \ , \end{aligned} \tag{4.19}$$

gdzie symbol $\hat{\mathcal{S}}$ oznacza operator symetryzacji, czyli sumę po wszystkich możliwych permutacjach bez powtórzeń elementów ciągu, który w naszym przypadku składa się z l elementów $P_{01}+P_{10}$ oraz $n-l$ elementów $P_{11}+P_{00}$, na przykład

$$\begin{aligned} \hat{\mathcal{S}}[(P_{01}+P_{10})^{\otimes 2} \ \otimes \ (P_{00}+P_{11})] = \\ = (P_{01}+P_{10}) \ \otimes \ (P_{01}+P_{10})\otimes(P_{00}+P_{11}) + \\ +(P_{01}+P_{10}) \ \otimes \ (P_{00}+P_{11})\otimes(P_{01}+P_{10}) + \\ +(P_{00}+P_{11}) \ \otimes \ (P_{01}+P_{10})\otimes(P_{01}+P_{10}) \ . \end{aligned} \tag{4.20}$$

Zapiszmy operator, który stoi przy x^l w postaci

$$\begin{aligned} P_k\hat{\mathcal{S}}\Big[(P_{01}+P_{10})^{\otimes l} \ \otimes \ (P_{11}+P_{00})^{\otimes(n-l)}\Big] P_k = \\ = \sum_{i=0}^{l}\sum_{j=0}^{n-l} P_k\hat{\mathcal{S}}\Big[P_{01}^i \otimes P_{10}^{l-i} \ \otimes \ P_{11}^j \otimes P_{00}^{n-l-j}\Big] P_k \ . \end{aligned} \tag{4.21}$$

Ponieważ operatory rzutowe P_k rzutują na podprzestrzeń rozpiętą przez wektory o wadze Hamminga równej k, wobec tego wyrażenie $P_k\Big[P_{01}^i \otimes P_{10}^{l-i} \otimes P_{11}^j \otimes P_{00}^{n-l-j}\Big]P_k$ nie zeruje się tylko dla $i+j=k$ i $l-i+j=k$. Stąd otrzymujemy zależność $l=2i$.

Wyprowadzimy teraz kilka własności macierzy D_l^k oraz wektorów $|x\rangle$ i $|y\rangle$.

Własność 4.1. *Dystans Hamminga $d(x,y)$ pomiędzy wektorami $|x\rangle$ i $|y\rangle$ o wadze Hamminga równej k spełnia nierówność*

$$d(x,y) \leqslant \min\{k, n-k\} \ . \tag{4.22}$$

Udowodnimy to w następujący sposób. Podzielmy ciąg x na dwie części. W pierwszej części wartości bitów na odpowiednich pozycjach są zgodne z wartościami bitów w ciągu y, a w drugiej części wartości te są przeciwne. Dystans Hamminga będzie równy liczbie bitów w drugiej części. Ponieważ wagi Hamminga ciągów x oraz y są równe, stąd wagi Hamminga w pierwszej i w drugiej części również są równe. Wobec tego liczba bitów w drugiej części ciągu musi być parzysta i – co więcej – nie może być ona większa niż liczba jedynek k oraz liczba zer $n-k$ w całym ciągu x. W szczególności otrzymujemy, że dystans Hamminga $d(x,y)$ jest liczbą parzystą.

Własność 4.2. *Dla dwóch różnych par ciągów (x,y) oraz (x',y') o równych dystansach Hamminga $d(x,y)=d(x',y')$ istnieje permutacja π, taka, że*

$$(\pi(x),\pi(y)) \ = \ (x',y') \ . \tag{4.23}$$

Własność tę udowodnimy następująco. Niech permutacja π_{xy} działa na ciągi x i y tak, że przesuwa bity z pozycji zgodnych na lewą stronę, a bity z pozycji niezgodnych na prawą stronę. Dalej wszystkie bity o wartości 1 z ciągu x przesuwa na ostatnie pozycje w każdej części, automatycznie przenosząc odpowiadające im bity w ciągu y. Taka transformacja sprowadza ciągi x i y do tak zwanej postaci kanonicznej x^0 i y^0

$$\begin{aligned} x^0 &= \underbrace{0\ldots0}_{n-k-l}\underbrace{1\ldots1}_{k-l}\underbrace{0\ldots0}_{l}\underbrace{1\ldots1}_{l} \ , \\ y^0 &= \underbrace{0\ldots0}_{n-k-l}\underbrace{1\ldots1}_{k-l}\underbrace{1\ldots1}_{l}\underbrace{0\ldots0}_{l} \ , \end{aligned} \tag{4.24}$$

które zależne są jedynie od n, k i $l=\frac{d(x,y)}{2}$. Rozważmy teraz dwie różne permutacje π_{xy} i $\pi_{x'y'}$. Ich działanie możemy zapisać następująco

$$\begin{aligned} \pi_{xy}xy &= x^0y^0 \ , \\ \pi_{x'y'}x'y' &= x^0y^0 \ . \end{aligned} \tag{4.25}$$

Z powyższych wzorów otrzymujemy

$$\pi_{xy}xy \ = \ \pi_{x'y'}x'y' \ . \tag{4.26}$$

Mnożąc obustronnie wyrażenie 4.26 przez permutację odwrotną $\pi^{-1}_{x^{'}y^{'}}$, dostajemy

$$\pi^{-1}_{x^{'}y^{'}}\pi_{xy}xy \;=\; x^{'}y^{'}\ . \tag{4.27}$$

Stąd permutacja $\pi = \pi^{-1}_{x^{'}y^{'}}\pi_{xy}$.

Własność 4.3. *Macierze D^k_l i $D^k_{l'}$ wzajemnie komutują.*

Przedstawmy macierze D^k_l oraz $D^k_{l'}$ na dwa sposoby

$$\begin{aligned} D^k_l &= \sum_{\substack{x,y\\ d(x,y)=2l}} |x\rangle\langle y|\ , \qquad (4.28)\\ D^k_{l'} &= \sum_{\substack{x,y\\ d(y^{'},z)=2l^{'}}} |y^{'}\rangle\langle z| \end{aligned}$$

i

$$\begin{aligned} D^k_l &= \sum_{\substack{y,z\\ d(y,z)=2l}} |y\rangle\langle z|\ , \qquad (4.29)\\ D^k_{l'} &= \sum_{\substack{x,y^{'}\\ d(x,y^{'})=2l^{'}}} |x\rangle\langle y^{'}|\ . \end{aligned}$$

Ze wzoru 4.28 otrzymujemy

$$\begin{aligned} D^k_l D^k_{l'} &= \sum_{\substack{x,y,y^{'},z\\ d(x,y)=2l\\ d(y^{'},z)=2l^{'}}} |x\rangle\langle y|y^{'}\rangle\langle z| = \qquad (4.30)\\ &= \sum_{\substack{x,y,z\\ d(x,y)=2l\\ d(y,z)=2l^{'}}} |x\rangle\langle z| = \sum_{x,z} f_{ll'}(x,z)\,|x\rangle\langle z|\ , \end{aligned}$$

natomiast ze wzoru 4.29 dostajemy

$$\begin{aligned} D^k_{l'} D^k_l &= \sum_{\substack{x,y^{'},y,z\\ d(x,y^{'})=2l^{'}\\ d(y,z)=2l}} |x\rangle\langle y^{'}|y\rangle\langle z| = \qquad (4.31)\\ &= \sum_{\substack{x,y,z\\ d(x,y)=2l^{'}\\ d(y,z)=2l}} |x\rangle\langle z| = \sum_{x,z} f_{l'l}(x,z)\,|x\rangle\langle z|\ , \end{aligned}$$

gdzie

$$\begin{aligned} f_{ll'}(x,z) &= |y : d(x,y)=2l, d(y,z)=2l^{'}|\ , \qquad (4.32)\\ f_{l'l}(x,z) &= |y : d(x,y)=2l^{'}, d(y,z)=2l|\ . \qquad (4.33) \end{aligned}$$

Wobec tego

$$[D^k_l, D^k_{l'}] = \sum_{x,z}(f_{ll'}(x,z) - f_{l'l}(x,z))\,|x\rangle\langle z|\ . \tag{4.34}$$

Stąd naszym celem jest pokazanie, że

$$f_{ll'}(x,z) = f_{l'l}(x,z) \ . \tag{4.35}$$

Wprowadźmy bijekcję g, która dokonuje na ciągach x oraz z operacji negacji na różniących je bitach. Funkcja ta działa więc następująco

$$g(x) \ = \ z \ , \tag{4.36}$$
$$g(z) \ = \ x \ . \tag{4.37}$$

Zauważmy, że funkcja g nie zmienia dystansu Hamminga pomiędzy ciągami bitów. Wobec tego

$$d(x,y^{'}) \ = \ d(g(x),g(y^{'})) = d(z,y) = d(y,z) \ , \tag{4.38}$$
$$d(y^{'},z) \ = \ d(g(y^{'}),g(z)) = d(y,x) = d(x,y) \ , \tag{4.39}$$

gdzie $y^{'} = g(y)$ oraz $y = g(y^{'})$. Wnioskujemy, że bijekcja g odwzorowuje zbiór $\{y : d(x,y) = 2l, d(y,z) = 2l^{'}\}$ na zbiór $\{y^{'} : d(x,y^{'}) = 2l^{'}, d(y^{'},z) = 2l\}$, a to oznacza, że te dwa zbiory mają taką samą liczbę elementów.

Własność 4.4. *Każdy operator działający w przestrzeni $\mathcal{H}_k^{\otimes n}$ niezmienniczy względem permutacji qubitów σ jest liniową kombinacją operatorów D_l^k.*

Weźmy dowolny operator z przestrzeni $\mathcal{H}_k^{\otimes n}$ postaci

$$A \ = \ \sum_{x,y} a_{x,y} \left|x\right\rangle \left\langle y\right| \ , \tag{4.40}$$

posiadający własność

$$A \ = \ V_\sigma A V_\sigma^\dagger \ , \tag{4.41}$$

gdzie operator V_σ reprezentuje permutację σ. Z własności 4.2 wiemy, że dla dwóch par ciągów (x,y) i $(x^{'},y^{'})$, o tych samych wagach i dystansach Hamminga, istnieje permutacja π, która odwzorowuje x w $x^{'}$ i y w $y^{'}$. Rozważmy permutację π o tej własności. Z jednej strony

$$V_{\pi^{-1}} A V_{\pi^{-1}}^\dagger \ = \ \sum_{x,y} a_{x,y} |\pi^{-1}(x)\rangle\langle\pi^{-1}(y)| = \sum_{x,y} a_{\pi(x),\pi(y)} \left|x\right\rangle \left\langle y\right| \ , \tag{4.42}$$

a z drugiej strony

$$V_{\pi^{-1}} A V_{\pi^{-1}}^\dagger \ = \ A = \sum_{x,y} a_{x,y} \left|x\right\rangle \left\langle y\right| \ . \tag{4.43}$$

Stąd otrzymujemy zależność

$$a_{x,y} \ = \ a_{\pi(x),\pi(y)} = a_{x',y'} \ . \tag{4.44}$$

Wnioskujemy więc, że dla dwóch par ciągów o równych dystansach i wagach Hamminga współczynniki a_{xy} i $a_{x'y'}$ są identyczne. A to oznacza, że operator A jest liniową kombinacją operatorów D_l^k.

Pokażemy teraz, w jaki sposób podprzestrzeń $\mathcal{H}_k^{\otimes n}$ rozkłada się na reprezentacje nieprzywiedlne grupy permutacji S_n.

Lemat 4.1. *Podprzestrzeń $\mathcal{H}_k^{\otimes n}$ ma następujący rozkład na reprezentacje nieprzywiedlne grupy permutacji S_n*

$$\mathcal{H}_k^{\otimes n} \;=\; \oplus_{j=0}^{\min\{k,n-k\}} N_j^k \;, \tag{4.45}$$

gdzie N_j^k jest wyznaczone przez rozkład $\lambda = (n-j,j)$. Ponadto operatory D_l^k mają następującą postać

$$D_l^k \;=\; \sum_{j=0}^{\min\{k,n-k\}} \alpha_l^k(j) P_j^k \;, \tag{4.46}$$

gdzie P_j^k jest operatorem rzutowym na reprezentację nieprzywiedlną N_j^k. W podprzestrzeni $\mathcal{H}_k^{\otimes n}$ każda z reprezentacji wyznaczona przez rozkład λ występuje tylko raz, co zapisujemy następująco

$$\mathcal{H}_\lambda^U \otimes \mathcal{H}_\lambda^S \cap \mathcal{H}_k^{\otimes n} \;=\; \mathbb{C} \otimes \mathcal{H}_\lambda^S \;. \tag{4.47}$$

Dowód. Zależność 4.47 wynika z następujących faktów. Ponieważ wszystkie operatory działające w przestrzeni $\mathcal{H}_k^{\otimes n}$ niezmiennicze względem permutacji wzajemnie komutują, w rozkładzie przestrzeni $\mathcal{H}_k^{\otimes n}$ na reprezentacje nieprzywiedlne, wymiar przestrzeni krotności $\mathcal{H}_\lambda^U$ musi być równy jeden. Z faktu, że j nie jest większe od k oraz $n-k$, wnioskujemy, że symetryzator Younga odpowiadający rozkładowi $\lambda = (n-j,j)$ anihiluje wektory o wadze Hamminga mniejszej niż j (oraz analogicznie wektory, w których liczba zer jest mniejsza niż j). ■

Możemy teraz wyprowadzić wzór na wartości własne operatorów D_l^k. Weźmy dowolny wektor $|\phi\rangle$ z przestrzeni reprezentacji nieprzywiedlnej N_j^k i korzystając z równania 4.46, wyraźmy wartość własną $\alpha_l^k(j)$ w postaci

$$\alpha_l^k(j) \;=\; \frac{\langle\phi|\, D_l^k \,|\phi\rangle}{\langle\phi|\phi\rangle} \;, \tag{4.48}$$

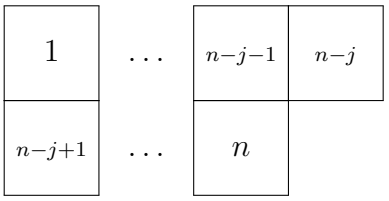
Pokażemy teraz, że wektor $|\phi\rangle$ możemy wybrać w następujący sposób

$$|\phi\rangle \;=\; \hat{P}_j |x^0\rangle \;, \tag{4.49}$$

gdzie $|x^0\rangle$ jest wektorem kanonicznym z przestrzeni $\mathcal{H}_k^{\otimes n}$

$$|x^0\rangle \;=\; |\underbrace{0\ldots0}_{n-k}\underbrace{1\ldots1}_{k}\rangle \;, \tag{4.50}$$

natomiast $\hat{P}_j$ oznacza symetryzator odpowiadający diagramowi Younga



. (4.51)

A więc operator $\hat{P}_j$ jest równy operatorowi $P^{\lambda,a}$ zdefiniowanemu we wzorze 2.87.

Wystarczy teraz pokazać, że wektor $\hat{P}_j|x^0\rangle$ jest niezerowy i należy do podprzestrzeni $\mathcal{H}_\lambda^U \otimes \mathcal{H}_\lambda^S \cap \mathcal{H}_k^{\otimes n}$. To, że jest on niezerowy, wynika z definicji symetryzatora Younga 2.87. Zawieranie się wektora $\hat{P}_j|x^0\rangle$ w podprzestrzeni $\mathcal{H}_k^{\otimes n}$, wynika z dwóch faktów: po pierwsze wektor $|x^0\rangle$ należy z definicji do tej podprzestrzeni, po drugie symetryzatory Younga są kombinacją liniową operatorów permutacji, a te nie zmieniają wagi Hamminga (to znaczy podprzestrzeń $\mathcal{H}_k^{\otimes n}$ jest niezmiennicza ze względu na ich działanie). Natomiast to, że wektor $\hat{P}_j|x^0\rangle$ należy do podprzestrzeni $\mathcal{H}_\lambda^U \otimes \mathcal{H}_\lambda^S$, wynika z definicji symetryzatora Younga 2.87.

Możemy więc wektor 4.49 utożsamiać z wektorem $|\phi\rangle$ ze wzoru 4.48. Korzystając z powyższych własności, możemy napisać

$$\alpha_l^k(j) \;=\; \frac{\langle x^0|\mathcal{S}\mathcal{A}D_l^k\mathcal{A}\mathcal{S}|x^0\rangle}{\langle x^0|\mathcal{S}\mathcal{A}^2\mathcal{S}|x^0\rangle}\;, \tag{4.52}$$

gdzie $\mathcal{S}$ i $\mathcal{A}$ są odpowiednio symetryzatorem i antysymetryzatorem znanym ze wzoru 2.88 i 2.89 dla rozkładu $\lambda = (n-j, j)$.

Naszym celem jest znalezienie jawnej postaci wartości własnych $\alpha_l^k(j)$. Przeanalizujmy najpierw licznik oraz mianownik we wzorze 4.52. Ponieważ operator D_l^k komutuje z operatorami $\mathcal{S}$ i $\mathcal{A}$, oraz $\mathcal{A}$ jest proporcjonalny do operatora rzutowego, możemy napisać, że

$$\begin{aligned}\langle x^0|\mathcal{S}\mathcal{A}D_l^k\mathcal{A}\mathcal{S}|x^0\rangle \;&=\; \langle x^0|\mathcal{S}\mathcal{A}^2\mathcal{S}D_l^k|x^0\rangle = \\ &=\; c\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}D_l^k|x^0\rangle = \\ &=\; c\sum_{y\in Y_{|x^0\rangle}}\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|y\rangle\;,\end{aligned} \tag{4.53}$$

$$\langle x^0|\mathcal{S}\mathcal{A}^2\mathcal{S}|x^0\rangle \;=\; c\sum_{y\in Y_{|x^0\rangle}}\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|x^0\rangle\;, \tag{4.54}$$

gdzie c jest pewną stałą, a $Y_{|x^0\rangle}$ jest zbiorem stanów $|y\rangle$, które są oddalone od stanu $|x^0\rangle$ o dystans Hamminga równy $2l$

$$Y_{|x^0\rangle} \;=\; \{|y\rangle \in \mathcal{H}_k^{\otimes n} : d(x_0, y) = 2l\}\;. \tag{4.55}$$

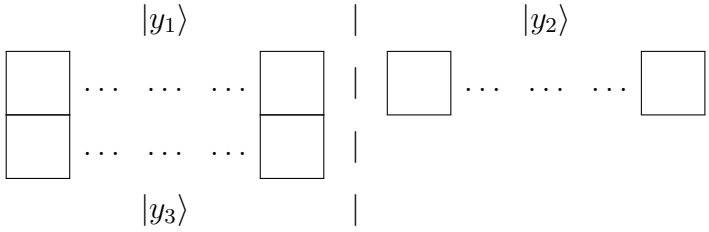
Korzystając z wzorów 4.53 i 4.54 możemy wzór 4.52 zapisać następująco

$$\alpha_l^k(j) \;=\; \sum_{y\in Y_{|x^0\rangle}}\frac{c\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|y\rangle}{c\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|x^0\rangle} = \sum_{y\in Y_{|x^0\rangle}}\frac{\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|y\rangle}{\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|x^0\rangle}\;. \tag{4.56}$$

Dokonajmy teraz następującego podziału wektora $|y\rangle$

$$|y\rangle \;=\; |y_1\rangle_1\,|y_2\rangle_2\,|y_3\rangle_3\ , \tag{4.57}$$

który wpiszemy w diagram Younga w następujący sposób



, (4.58)

gdzie wektory y_1 i y_3 wypełniają j kwadratów, a wektor y_2 pozostałe $n-2j$ kwadratów. Podzielmy zbiór $Y_{|x^0\rangle}$ na podzbiory, które są określone przez wagę Hamminga wektorów $|y_1\rangle\,|y_2\rangle$

$$Y^m_{|x^0\rangle} \;=\; \{|y\rangle \in \mathcal{H}_k^{\otimes n} : d(x_0,y) = 2l, w(y_1y_2) = m\}\ . \tag{4.59}$$

W dalszej części pokażemy, że elementy sumy 4.56 zależą tylko od zbioru $Y^m_{|x^0\rangle}$, do którego należy wektor $|y\rangle$. W ten sposób możemy przedstawić wzór 4.56 w postaci

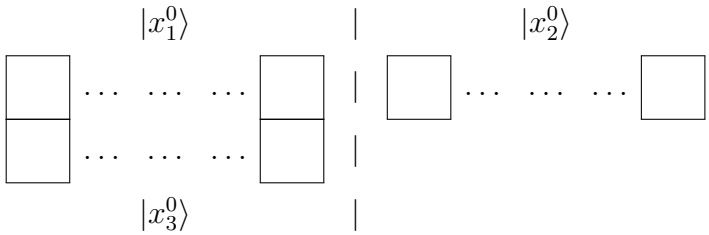
$$\begin{aligned}\alpha^k_l(j) \;&=\; \sum_{m=\max\{l,k-j\}}^{\min\{k,k-j\}} \sum_{y\in Y^m_{|x^0\rangle}} \frac{\langle x^0|\mathcal{SAS}|y\rangle}{\langle x^0|\mathcal{SAS}|x^0\rangle} = \\ &=\; \sum_{m=\max\{l,k-j\}}^{\min\{k,k-j\}} |Y^m_{|x^0\rangle}|\frac{\langle x^0|\mathcal{SAS}|y\rangle}{\langle x^0|\mathcal{SAS}|x^0\rangle}.\end{aligned} \tag{4.60}$$

Pozostaje nam do obliczenia moc zbioru $Y^m_{|x^0\rangle}$ oraz czynnik $\frac{\langle x^0|\mathcal{SAS}|y\rangle}{\langle x^0|\mathcal{SAS}|x^0\rangle}$.

Zacznijmy od policzenia mocy zbioru $Y^m_{|x^0\rangle}$. W tym celu podzielmy wektor $|x^0\rangle$ podobnie, jak podzieliliśmy wektor $|y\rangle$:

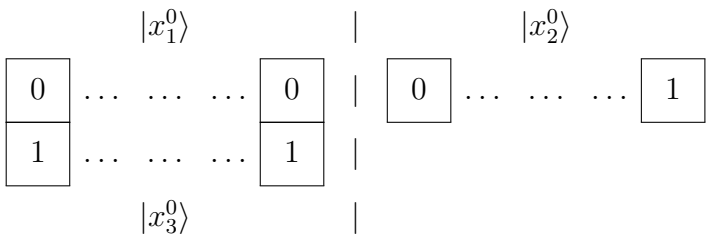
$$|x^0\rangle \;=\; |x^0_1\rangle_1|x^0_2\rangle_2|x^0_3\rangle_3 = |0^{\otimes j}\rangle_1|x_2\rangle_2|1^{\otimes j}\rangle_3\ , \tag{4.61}$$

i wpiszmy go w diagram Younga w podobny sposób jak wektor $|y\rangle$, to znaczy



, (4.62)

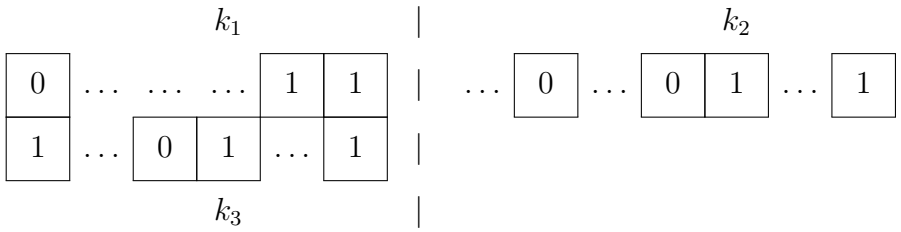
który jawnie wygląda następująco



. (4.63)

Pierwszy wiersz w diagramie 4.63 jest podzielony na dwie części. Lewa część składa się z j kwadratów wypełnionych bitami o wartości 0, natomiast prawa część składa się z $n-2j$ kwadratów wypełnionych bitami o wartości 0 i 1. Drugi wiersz składa się z j kwadratów, z których każdy jest wypełniony bitem o wartości 1.

Dla stanu $|y\rangle$ diagram Younga będzie następujący



. (4.64)

Przez k_1 oznaczyliśmy liczbę jedynek w pierwszym wierszu wektora $|y\rangle$, która przekrywa się z zerami w pierwszym wierszu wektora $|x^0\rangle$, przez k_2 – liczbę jedynek w pierwszym wierszu wektora $|y\rangle$, która przekrywa się z jedynkami w pierwszym wierszu wektora $|x^0\rangle$ i przez k_3 – liczbę jedynek w drugim wierszu wektora $|y\rangle$. Ponieważ waga Hamminga wektora $|y\rangle$ wynosi k, musi być spełniona relacja

$$k_1 + k_2 + k_3 = k \ . \tag{4.65}$$

Z kolei z faktu, że liczba jedynek w pierwszym wierszu wektora $|y\rangle$ jest równa m, mamy

$$m = k_1 + k_2 \ . \tag{4.66}$$

Dystans Hamminga $2l$ pomiędzy wektorami $|x^0\rangle$ i $|y\rangle$ jest sumą dwóch dystansów l_1 i l_2. Pierwszy z nich jest dystansem pomiędzy ciągami z pierwszych wierszy w diagramach 4.63 i 4.64, natomiast drugi z nich jest dystansem pomiędzy ciągami z drugich wierszy w tych diagramach. Dystanse te spełnią następującą zależność

$$l_1 \ = \ k_1 + (k - j - k_2) \ , \tag{4.67}$$

$$l_2 \ = \ j - k_3 \ . \tag{4.68}$$

Dodając stronami powyższe równania otrzymujemy

$$2l = l_1 + l_2 = k + k_1 - k_2 - k_3 \ = \ k + 2k_1 - \underbrace{(k_1 + k_2 + k_3)}_{k} = 2k_1 \ . \tag{4.69}$$

Spójrzmy teraz na diagram 4.64. Permutacje ciągów w obu wierszach muszą zachowywać dystanse l_1 i l_2. I tak, liczba permutacji zachowujących dystans l_1 od pierwszego wiersza wektora $|y\rangle$ do pierwszego wiersza wektora $|x^0\rangle$, wynosi

$$\binom{n-k}{k_1}\binom{l-j}{k_2} \ , \tag{4.70}$$

natomiast liczba permutacji zachowujących dystans l_2 od drugiego wiersza wektora $|y\rangle$ do drugiego wiersza wektora $|x^0\rangle$ jest równa

$$\binom{j}{k_3} . \tag{4.71}$$

Z równań 4.65, 4.66 oraz 4.69 dostajemy

$$\begin{aligned} k_1 &= l , \\ k_2 &= m - l , \\ k_3 &= k - m . \end{aligned} \tag{4.72}$$

Mnożąc przez siebie 4.70, 4.71 oraz korzystając z 4.72 otrzymujemy ostateczny wzór na moc zbioru $Y^m_{|x^0\rangle}$

$$|Y^m_{|x^0\rangle}| = \binom{n-k}{l}\binom{k-j}{m-l}\binom{j}{k-m} . \tag{4.73}$$

Przejdźmy teraz do obliczenia czynnika $\frac{\langle x^0|\mathcal{SAS}|y\rangle}{\langle x^0|\mathcal{SAS}|x^0\rangle}$. Dokonajmy podziału wektorów $|x^0\rangle$ oraz $|y\rangle$ zgodnie z diagramami 4.63 i 4.64. Ze wzoru 2.87 widzimy, że antysymetryzator działa tylko na częściach 1 i 3, co zapisujemy następująco

$$\mathcal{A} = \mathcal{A}_{13} . \tag{4.74}$$

Natomiast symetryzator działa na częściach 1 i 2 oraz niezależnie na części 3, czyli

$$\mathcal{S} = \mathcal{S}_{12}\mathcal{S}_3 . \tag{4.75}$$

Wyprowadzimy obecnie pewną relację, którą spełniają operatory $\mathcal{S}_{12}$, $\mathcal{S}_3$ i $\mathcal{A}_{13}$. W tym celu wprowadzimy następujący operator permutacji

$$\mathcal{X} = \sum_{\sigma\in S_n} V^{(1)}_\sigma \otimes V^{(3)}_\sigma , \tag{4.76}$$

gdzie $V^{(i)}_\sigma$ jest operatorem permutacji znanym ze wzoru 2.90, działającym na i-tej części wektora $|x^0\rangle$ z podziału 4.62. Natomiast suma rozciąga się po wszystkich permutacjach σ należących do grupy S_n. Zauważmy, że operator ten komutuje zarówno z $\mathcal{S}_{12}$, jak i z $\mathcal{A}_{13}$

$$\mathcal{X}\mathcal{S}_{12} = \mathcal{S}_{12}\mathcal{X} , \tag{4.77}$$

$$\mathcal{X}\mathcal{A}_{13} = \mathcal{A}_{13}\mathcal{X} \tag{4.78}$$

oraz, że zachodzą tożsamości

$$\mathcal{S}_3\mathcal{S}_{12} = \mathcal{X}\mathcal{S}_{12} , \tag{4.79}$$

$$\mathcal{S}_{12}\mathcal{S}_3 = \mathcal{S}_{12}\mathcal{X} . \tag{4.80}$$

Korzystając z tych własności, otrzymujemy

$$\begin{aligned}\mathcal{S}_{12}\mathcal{S}_3\mathcal{A}_{13}\mathcal{S}_3\mathcal{S}_{12} &= \mathcal{S}_{12}\mathcal{S}_3\mathcal{A}_{13}\mathcal{X}\mathcal{S}_{12} = \\ &= \mathcal{S}_3\mathcal{S}_{12}\mathcal{X}\mathcal{A}_{13}\mathcal{S}_{12} = \\ &= \mathcal{S}_3\mathcal{X}\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{S}_{12} = \\ &= \mathcal{S}_3^2\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{S}_{12}\ .\end{aligned} \tag{4.81}$$

Działając operatorem $\mathcal{S}_3^2$ z prawej strony na wektor $\langle x^0|$, dostajemy

$$\begin{aligned}\langle x^0|\mathcal{S}_3^2 &= \langle x_1^0|_1\langle x_2^0|_2\langle x_3^0|_3|\mathcal{S}_3^2 = \langle x_1^0|_1\langle x_2^0|_2\langle x_3^0|_3\mathcal{S}_3^2 = \\ &= \langle x_1^0|_1\langle x_2^0|_2\langle x_3^0|_3 j!j! = (j!)^2\langle x_1^0|_1\langle x_2^0|_2\langle x_3^0|_3\ .\end{aligned} \tag{4.82}$$

Korzystając ze wzorów 4.81 oraz 4.82 otrzymujemy

$$\langle x^0|\mathcal{S}_{12}\mathcal{S}_3\mathcal{A}_{13}\mathcal{S}_3\mathcal{S}_{12} = (j!)^2\langle x^0|\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{S}_{12}\ . \tag{4.83}$$

Działając operatorami $\mathcal{A}_{13}$ i $\mathcal{S}_{12}$ na wektory $|x^0\rangle$ i $|y\rangle$, dostajemy odpowiednio

$$\begin{aligned}\mathcal{A}_{13}\mathcal{S}_{12}|x^0\rangle &= \mathcal{A}_{13}|x_3^0\rangle_3\mathcal{S}_{12}|x_1^0\rangle_1|x_2^0\rangle_2 = \\ &= f(x_{12}^0)\mathcal{A}_{13}|x_3^0\rangle_3|(x_{12}^0)^{\mathcal{S}}\rangle_{12}\ ,\end{aligned} \tag{4.84}$$

$$\begin{aligned}\mathcal{A}_{13}\mathcal{S}_{12}|y\rangle &= \mathcal{A}_{13}|y_3\rangle_3\mathcal{S}_{12}|y_1\rangle_1|y_2\rangle_2 = \\ &= f(y_{12})\mathcal{A}_{13}|y_3\rangle_3|(y_{12})^{\mathcal{S}}\rangle_{12}\ ,\end{aligned} \tag{4.85}$$

gdzie $f(x_{12}^0)$ ($f(y_{12})$) jest liczbą permutacji, które nie zmieniają wektora $|x_{12}^0\rangle_{12}$ ($|y_{12}\rangle_{12}$), natomiast $|(x_{12}^0)^{\mathcal{S}}\rangle_{12}$ ($|(y_{12})^{\mathcal{S}}\rangle_{12}$) oznacza zsymetryzowany wektor $|(x_{12}^0)\rangle_{12}$ ($|(y_{12})\rangle_{12}$). Korzystając z wzorów 4.82, 4.84 i 4.85, możemy obliczyć licznik ze wzoru 4.60

$$\begin{aligned}(j!)^2\langle x^0|\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{A}_{13}\mathcal{S}_{12}|y\rangle &= c^2(j!)^2\langle x^0|\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{A}_{13}\mathcal{S}_{12}|y\rangle = \\ &= c^2(j!)^2 f(y_{12})\langle x_3^0|_1\langle\bar{x}_3^0|_3\mathcal{A}_{13}|\bar{y}_3\rangle_1|y_3\rangle_3\langle(x_2^0)^{\mathcal{S}}|(x_2^0)^{\mathcal{S}}\rangle_2 = \\ &= (-1)^{j-k+m}c^2(j!)^2 f(y_{12})\langle x_3^0|_1\langle\bar{x}_3^0|_3\mathcal{A}_{13}|x_3\rangle_1|\bar{x}_3\rangle_3\langle(x_2^0)^{\mathcal{S}}|(x_2^0)^{\mathcal{S}}\rangle_2\end{aligned} \tag{4.86}$$

oraz mianownik z tego wzoru

$$\begin{aligned}(j!)^2\langle x^0|\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{A}_{13}\mathcal{S}_{12}|x^0\rangle &= c^2(j!)^2\langle x^0|\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{A}_{13}\mathcal{S}_{12}|x^0\rangle\langle(x_2^0)^{\mathcal{S}}|(x_2^0)^{\mathcal{S}}\rangle_2 = \\ &= c^2(j!)^2 f(x_{12}^0)\langle x_3^0|_1\langle\bar{x}_3^0|_3\mathcal{A}_{13}|x_3\rangle_1|\bar{x}_3\rangle_3\langle(x_2^0)^{\mathcal{S}}|(x_2^0)^{\mathcal{S}}\rangle_2\ .\end{aligned} \tag{4.87}$$

Symbol c w powyższych wzorach oznacza stałą normalizacyjną, natomiast $\bar{x}$ oznacza negację wszystkich bitów w ciągu x. Stąd po uproszczeniach dostajemy

$$\frac{\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|y\rangle}{\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|x^0\rangle} = \frac{\langle x^0|\mathcal{S}_{12}\mathcal{A}_{13}\mathcal{S}_{12}|y\rangle}{\langle x^0|\mathcal{S}\mathcal{A}\mathcal{S}|x^0\rangle} = (-1)^{j-k+m}\frac{f(y_{12})}{f(x_{12}^0)}\ . \tag{4.88}$$

Pozostało nam teraz wyznaczenie wzorów na $f(y_{12})$ oraz $f(x^0_{12})$. Wiemy, że w wektorze $|y_{12}\rangle$ jest $n-j$ bitów, więc liczba jego możliwych permutacji wynosi $(n-j)!$. Jednak $\binom{n-j}{m}$ permutacji zmienia wektor $|y_{12}\rangle$. Stąd permutacji nie zmieniających wektora $|y_{12}\rangle$ pozostaje

$$f(y_{12}) \;=\; \frac{(n-j)!}{\binom{n-j}{m}} \;. \tag{4.89}$$

Identyczne rozważanie dotyczy funkcji $f(x^0_{12})$. Tutaj jednak liczba permutacji zmieniających wektor $|x^0_{12}\rangle$ jest równa $\binom{n-j}{n-k}$. Mamy więc

$$f(x^0_{12}) \;=\; \frac{(n-j)!}{\binom{n-j}{n-k}} \;. \tag{4.90}$$

Podstawiając wyrażenia 4.89 i 4.90 do wzoru 4.88, otrzymujemy

$$\frac{\langle x^0|\mathcal{SAS}|y\rangle}{\langle x^0|\mathcal{SAS}|x^0\rangle} \;=\; (-1)^{j-k+m}\frac{\binom{n-j}{n-k}}{\binom{n-j}{m}} \;, \tag{4.91}$$

co jest ostatecznym wzorem na drugą część wyrażenia 4.60. Łącząc ze sobą obie części wzoru 4.60 to jest 4.73 i 4.91 dostajemy wzór na wartości własne macierzy D^k_l

$$\alpha^k_l(j) \;=\; \sum_{m=\max\{l,k-j\}}^{\min\{k,k-j\}} (-1)^{j-k+m}\frac{\binom{n-j}{n-k}}{\binom{n-j}{m}}\binom{n-k}{l}\binom{k-j}{m-l}\binom{j}{k-m}. \tag{4.92}$$

Dokonując podstawienia

$$m \;=\; k-j+l-r \;, \tag{4.93}$$

otrzymujemy następującą postać wzoru 4.92

$$\alpha^k_l(j) \;=\; \sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}} (-1)^{l-r}\binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r} \;. \tag{4.94}$$

Korzystając z zależności 4.15, możemy przedstawić wartości własne stanu $\widetilde{\rho}^n_k$ w postaci

$$\lambda^n_k(j) \;=\; \frac{1}{2^n}\sum_{l=0}^{k} x^{2l}\alpha^k_l(j) \;, \tag{4.95}$$

co po podstawieniu za $\alpha^k_l(j)$ wyrażenia 4.94 daje nam

$$\begin{aligned}\lambda^n_k(j) \;=\; & \frac{1}{2^n}\sum_{l=0}^{k} x^{2l}\sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}} (-1)^{l-r} \\ & \binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r} \;.\end{aligned} \tag{4.96}$$

Pozostaje nam wyznaczenie wzoru na krotności poszczególnych wartości własnych. Krotność wartości własnej dla danego j jest równa liczbie standardowych diagramów Younga dla rozkładu $\lambda = (n-j, j)$. Podstawiając więc odpowiednie wartości do wzoru 2.81, otrzymujemy następującą krotność

$$g^n_j \;=\; \binom{n}{j}\frac{n-2j+1}{n-j+1} \;. \tag{4.97}$$

4.3 Przykład: pomiar na czterech kopiach stanu ρ_{AB}

Powyższe rozważania teoretyczne zilustrujmy przykładem. Na podstawie wyprowadzonych w poprzednim punkcie wzorów wyznaczymy wartości własne stanu otrzymanego w wyniku pomiaru czterech kopii stanu ρ_{AB}. Rozważymy te przypadki, w których zarówno Alicja jak i Bob otrzymają te same wyniki pomiarów k. Są to: $k = 0$, $k = 1$, $k = 2$, $k = 3$ i $k = 4$. Z tych pięciu przypadków przeanalizujemy dokładnie jedynie dwa: $k = 1$ oraz $k = 2$. Pominięcie pozostałych przypadków motywujemy w następujący sposób: wyniki dla $k = 0$ i $k = 4$ są trywialne, natomiast rezultat dla $k = 1$ jest równoważny rezultatowi dla $k = 3$.

4.3.1 Przypadek $n = 4$, $k = 1$

Postać stanu $\tilde{\rho}_1^4$ jest następująca

$$\tilde{\rho}_1^4 \;=\; \frac{1}{2^4}\Big(D_0^1 + x^2 D_1^1\Big)\,, \tag{4.98}$$

gdzie

$$D_0^1 \;=\; \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}\,, \tag{4.99}$$

$$D_1^1 \;=\; \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&1&0&0&1&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix} . \tag{4.100}$$

Dla takich wartości parametrów n i k parametr j przyjmuje dwie wartości: $j = 0$ oraz $j = 1$. Stąd stan $\tilde{\rho}_1^4$ ma dwie różne wartości własne. Wektor kanoniczny 4.24 ma postać

$$|x^0\rangle \;=\; |0001\rangle \;. \tag{4.101}$$

Przeanalizujmy najpierw przypadek dla $j = 0$. Diagram Younga $\lambda = (4, 0)$ ma postać następującą

0	0	0	1

Odpowiadający mu operator Younga przekształca wektor $|x^0\rangle$ w następujący sposób

$$P^{(4,0)}|x^0\rangle \;=\; \frac{1}{4}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \;. \tag{4.102}$$

Z powyższego wzoru dostajemy

$$\langle x^0|(P^{(4,0)})^\dagger P^{(4,0)}|x^0\rangle \;=\; \frac{1}{4} \;. \tag{4.103}$$

Obliczmy najpierw wartości własne macierzy D_0^1. Na początku wyznaczymy zbiór wektorów $|y\rangle$ oddalonych od wektora $|x^0\rangle$ o dystans Hamminga równy 0

$$Y_{|x^0\rangle} \;=\; \{|0001\rangle : d(x^0, y) = 0\} \;. \tag{4.104}$$

Jego moc wynosi $|Y_{|x^0\rangle}| = 1$. Operator Younga przekształca wektor $|y\rangle$ z tego zbioru następująco

$$P^{(4,0)}|y\rangle \;=\; \frac{1}{4}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle) \;. \tag{4.105}$$

Korzystając z 4.102 i 4.105, otrzymujemy

$$\langle x^0|(P^{(4,0)})^\dagger P^{(4,0)}|y\rangle \;=\; \frac{1}{4}\;. \tag{4.106}$$

Na podstawie wzoru 4.60, otrzymujemy następujący wynik na wartość własną macierzy D_0^1 dla $j=0$.

$$\alpha_0^1(0) \;=\; 1\;. \tag{4.107}$$

Powyższe wyniki zgadzają się z analogicznymi wynikami otrzymanymi ze wzoru 4.94

$$\alpha_0^1(0) \;=\; \sum_{m=1}^{1}(-1)^{-1+m}\frac{\binom{4}{3}}{\binom{4}{m}}\binom{3}{0}\binom{1}{m-0}\binom{0}{1-m}=1\;. \tag{4.108}$$

Obliczmy teraz wartości własne macierzy D_1^1. Związany z nią zbiór wektorów $|y\rangle$ oddalonych od wektora $|x^0\rangle$ o dystans Hamminga równy 2 ma postać

$$Y_{|x^0\rangle} \;=\; \{|0010\rangle,|0100\rangle,|1000\rangle : d(x^0,y)=2\}\;. \tag{4.109}$$

Moc tego zbioru wynosi $|Y^1_{|x^0\rangle}|=3$. Operator Younga przekształca wektor $|y\rangle$ z tego zbioru następująco

$$P^{(4,0)}|y\rangle \;=\; \frac{3}{4}(|0001\rangle+|0010\rangle+|0100\rangle+|1000\rangle)\;. \tag{4.110}$$

Z 4.102 i 4.110 otrzymujemy

$$\langle x^0|(P^{(4,0)})^\dagger P_1^{(4,0)}|y\rangle \;=\; \frac{3}{4}\;. \tag{4.111}$$

Na podstawie wzoru 4.60 wyznaczymy wartość własną macierzy D_1^1 dla $j=0$

$$\alpha_1^1(0) \;=\; 3\;, \tag{4.112}$$

która zgadza się z wartością własną otrzymaną ze wzoru 4.94

$$\alpha_1^1(0) \;=\; \sum_{m=1}^{1}(-1)^{-1+m}\frac{\binom{4}{3}}{\binom{4}{m}}\binom{3}{1}\binom{1}{m-1}\binom{0}{1-m}=3\;. \tag{4.113}$$

Znając $\alpha_0^1(0)$ oraz $\alpha_1^1(0)$, możemy wyznaczyć ze wzoru 4.95 wartość własną stanu $\tilde{\rho}_1^4$ dla $j=0$

$$\lambda_1^4(0) \;=\; 1x^0+3x^2=1+3x^2\;. \tag{4.114}$$

Krotność tej wartości własnej, obliczona ze wzoru 4.97, wynosi

$$g_0^4 \;=\; 1\;. \tag{4.115}$$

Przeanalizujmy teraz przypadek dla $j=1$. Diagram Younga $\lambda=(3,1)$ ma postać

0	0	0
1		

Wektor kanoniczny $|x^0\rangle$ jest przekształcany przez odpowiadający powyższemu diagramowi operator Younga następująco

$$P^{(3,1)}|x^0\rangle \;=\; \frac{1}{2}(|0001\rangle - |1000\rangle) \; . \tag{4.116}$$

Z powyższego wzoru dostajemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|x^0\rangle \;=\; \frac{1}{2} \; . \tag{4.117}$$

Operator Younga przekształca wektor $|y\rangle$ ze zbioru 4.104 następująco

$$P^{(3,1)}|y\rangle \;=\; \frac{1}{2}(|0001\rangle - |1000\rangle) \; , \tag{4.118}$$

Z 4.116 i 4.118 otrzymujemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|y\rangle \;=\; \frac{1}{2} \; . \tag{4.119}$$

Teraz na podstawie wzoru 4.60 obliczamy wartość własną macierzy D_0^1 dla $j = 1$

$$\alpha_0^1(1) \;=\; 1 \; . \tag{4.120}$$

Wynik ze wzoru 4.120 jest zgodny z wynikiem otrzymanym ze wzoru 4.94

$$\alpha_0^1(1) \;=\; \sum_{m=0}^{0}(-1)^{0+m}\frac{\binom{3}{3}}{\binom{3}{m}}\binom{3}{0}\binom{0}{m-0}\binom{1}{1-m} = 1 \; . \tag{4.121}$$

Pozostało nam obliczenie wartości własnej macierzy D_1^1. Dowolny wektor $|y\rangle$ ze zbioru 4.109 jest przekształcany następująco

$$P^{(3,1)}|y\rangle \;=\; \frac{1}{2}(|1000\rangle - |0001\rangle) \; . \tag{4.122}$$

Z 4.116 i 4.122 otrzymujemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|y\rangle \;=\; -\frac{1}{2} \; . \tag{4.123}$$

Podstawiając tę wartość do wzoru 4.60 otrzymujemy wartość własną macierzy D_1^1 dla $j = 1$

$$\alpha_1^1(1) \;=\; -1 \; . \tag{4.124}$$

Powyższe wyniki są takie same, jak otrzymane ze wzoru 4.94

$$\alpha_1^1(1) \;=\; \sum_{m=0}^{1}(-1)^{0+m}\frac{\binom{3}{3}}{\binom{3}{m}}\binom{3}{1}\binom{0}{m-1}\binom{1}{1-m} = -1 \; . \tag{4.125}$$

Teraz korzystając ze wzoru 4.95 możemy wyznaczyć wartość własną stanu $\tilde{\rho}_1^4$ dla $j = 1$

$$\lambda_1^4(1) \;=\; 1x^0 - 1x^2 = 1 - x^2 \; , \tag{4.126}$$

której krotność obliczona ze wzoru 4.97 wynosi

$$g_1^4 \;=\; 3 \; . \tag{4.127}$$

4.3.2 Przypadek $n = 4$, $k = 2$

Dla tego przypadku stan $\tilde{\rho}_2^4$ będzie miał postać

$$\tilde{\rho}_2^4 = \frac{1}{2^4}\Big(D_0^2 + x^2 D_1^2 + x^4 D_2^2\Big)\,, \tag{4.128}$$

gdzie

$$D_0^2 = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}, \tag{4.129}$$

$$D_1^2 = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0\\
0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0\\
0&0&0&1&0&0&1&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&1&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}, \tag{4.130}$$

$$D_2^2 = \begin{pmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{pmatrix} . \quad (4.131)$$

Wektor kanoniczny 4.24 ma postać

$$|x^0\rangle = |0011\rangle \ . \quad (4.132)$$

Dla takich wartości parametrów n i k parametr j przyjmuje trzy wartości $j = 0$, $j = 1$ oraz $j = 2$, więc stan $\tilde{\rho}_2^4$ będzie miał trzy różne wartości własne. Dla przypadku $j = 0$ diagram Younga ma postać

0	0	1	1

Odpowiadający mu operator Younga przekształca wektor $|x^0\rangle$ w następujący sposób

$$P^{(4,0)}|x^0\rangle = \frac{1}{6}(|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle) \ . \quad (4.133)$$

Z powyższego wzoru otrzymujemy

$$\langle x^0|(P^{4,0})^\dagger P^{(4,0)}|x^0\rangle = \frac{1}{6} \ . \quad (4.134)$$

Obliczmy najpierw wartości własne macierzy D_0^2. Zbiór wektorów $|y\rangle$ oddalonych od wektora $|x^0\rangle$ o dystans Hamminga równy 0 ma postać

$$Y_{|x^0\rangle} = \{|0011\rangle : d(x^0, y) = 0\} \ . \quad (4.135)$$

Jego moc wynosi $|Y_{|x^0\rangle}| = 1$. Wektor $|y\rangle$ z tego zbioru jest przekształcany przez operator Younga $P^{(4,0)}$ następująco

$$P^{(4,0)}|y\rangle = \frac{1}{6}(|0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle) \ . \quad (4.136)$$

Z 4.133 i 4.136 dostajemy

$$\langle x^0|(P^{(4,0)})^\dagger P^{(4,0)}|y\rangle \;=\; \frac{1}{6}\,. \tag{4.137}$$

Obliczona na podstawie wzoru 4.60 wartość własna macierzy D_0^2 dla $j=0$ wynosi

$$\alpha_0^2(0) \;=\; 1\,. \tag{4.138}$$

Jest ona zgodna z wartością własną obliczoną ze wzoru 4.94

$$\alpha_0^2(0) \;=\; \sum_{m=2}^{2}(-1)^{-2+m}\frac{\binom{4}{2}}{\binom{4}{m}}\binom{2}{0}\binom{2}{m-0}\binom{0}{2-m}=1\,. \tag{4.139}$$

Obliczmy teraz wartość własną macierzy D_1^2. Związany z tą macierzą zbiór wektorów $|y\rangle$ oddalonych od wektora $|x^0\rangle$ o dystans Hamminga równy 2, jest następujący

$$Y_{|x^0\rangle} \;=\; \{|0101\rangle,|0110\rangle,|1001\rangle,|1010\rangle : d(x^0,y)=2\}\,. \tag{4.140}$$

Jego moc wynosi $|Y_{|x^0\rangle}|=4$. Operator Younga przekształca dowolny wektor z tego zbioru w następujący sposób

$$P^{(4,0)}|y\rangle \;=\; \frac{4}{6}(|0011\rangle+|0101\rangle+|0110\rangle+|1001\rangle+|1010\rangle+|1100\rangle)\,. \tag{4.141}$$

Z 4.133 i 4.141 otrzymujemy

$$\langle x^0|(P^{(4,0)})^\dagger P^{(4,0)}|y\rangle \;=\; \frac{4}{6}\,. \tag{4.142}$$

Wartość własna macierzy D_1^2 dla $j=0$, obliczona na podstawie wzoru 4.60, wynosi

$$\alpha_1^2(0) \;=\; 4\,. \tag{4.143}$$

Identyczny wyniki dostajemy z 4.94

$$\alpha_1^2(0) \;=\; \sum_{m=2}^{2}(-1)^{-2+m}\frac{\binom{4}{2}}{\binom{4}{m}}\binom{2}{1}\binom{2}{m-1}\binom{0}{2-m}=4\,. \tag{4.144}$$

Przejdźmy do wyznaczenia wartości własnej macierzy D_2^2. Zbiór stanów oddalonych od wektora $|x^0\rangle$ o dystans Hamminga równy 4, ma postać

$$Y_{|x^0\rangle} \;=\; \{|1100\rangle : d(x^0,y)=4\}\,. \tag{4.145}$$

Jego moc jest równa$|Y_{|x^0\rangle}|=1$. Wektor $|y\rangle$ z tego zbioru jest przekształcany przez operator Younga $P^{(4,0)}$ następująco

$$P^{(4,0)}|y\rangle \;=\; \frac{1}{6}(|0011\rangle+|0101\rangle+|0110\rangle+|1001\rangle+|1010\rangle+|1100\rangle)\,. \tag{4.146}$$

Z 4.133 i 4.146 dostajemy

$$\langle x^0|(P^{(4,0)})^\dagger P^{(4,0)}|y\rangle \;=\; \frac{1}{6}\,. \tag{4.147}$$

Możemy teraz skorzystać ze wzoru 4.60 i obliczyć wartość własną macierzy D_2^2 dla $j = 0$

$$\alpha_2^2(0) \;=\; 1 \; . \tag{4.148}$$

Identyczny wynik otrzymamy korzystając ze wzoru 4.94

$$\alpha_2^2(0) \;=\; \sum_{m=2}^{2} (-1)^{-2+m} \frac{\binom{4}{2}}{\binom{4}{m}} \binom{2}{2} \binom{2}{m-2} \binom{0}{2-m} = 1 \; . \tag{4.149}$$

Podstawiając $\alpha_l^2(0)$ do wzoru 4.95, dostajemy wartość własną stanu $\tilde{\rho}_2^4$ dla $j = 0$

$$\lambda_2^4(0) \;=\; 1x^0 + 4x^2 + 1x^4 = 1 + 3x^2 + x^4 \; . \tag{4.150}$$

Jej krotność obliczona na podstawie wzoru 4.97 wynosi

$$g_0^4 \;=\; 1 \; . \tag{4.151}$$

Rozpatrzmy teraz przypadek parametru $j = 1$. Diagram Younga ma wtedy postać

0	0	1
1		

Utworzony na jego podstawie operator Younga działa na wektor $|x^0\rangle$ następująco

$$P^{(3,1)}|x^0\rangle \;=\; \frac{1}{2}(|0011\rangle + |1001\rangle - |1010\rangle - |1100\rangle) \; . \tag{4.152}$$

Z powyższego wzoru dostajemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|x^0\rangle \;=\; 1 \; . \tag{4.153}$$

Najpierw wyznaczymy wartości własne macierzy D_0^2. Operator Younga $P^{(3,1)}$ działa na wektor $|y\rangle$ ze zbioru 4.135 następująco

$$P^{(3,1)}|y\rangle \;=\; \frac{1}{2}(|0011\rangle + |1001\rangle - |1010\rangle - |1100\rangle) \; . \tag{4.154}$$

Z 4.152 i 4.154 otrzymujemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|y\rangle \;=\; 1 \; . \tag{4.155}$$

Obliczona ze wzoru 4.62 wartość własna macierzy D_0^2 dla $j = 1$ wynosi

$$\alpha_0^2(1) \;=\; 1 \; . \tag{4.156}$$

Wartość ta zgadza się z wartością własną obliczoną na podstawie wzoru 4.94

$$\alpha_0^2(1) \;=\; \sum_{m=1}^{1} (-1)^{-1+m} \frac{\binom{3}{2}}{\binom{3}{m}} \binom{2}{0} \binom{1}{m-0} \binom{1}{2-m} = 1 \; . \tag{4.157}$$

Obliczmy teraz wartości własne macierzy D_1^2. Operator Younga $P^{(3,1)}$ przekształca wektor $|y\rangle$ ze zbioru 4.140 następująco

$$P^{(3,1)}|y\rangle \;=\; 0. \tag{4.158}$$

Z 4.152 i 4.158 dostajemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|y\rangle \;=\; 0\ . \tag{4.159}$$

Obliczona na podstawie wzoru 4.62 wartość własna macierzy D_1^2 dla $j=1$ jest równa

$$\alpha_1^2(1) \;=\; 0\ . \tag{4.160}$$

Identyczny wynik otrzymujemy ze wzoru 4.94

$$\alpha_1^2(1) \;=\; \sum_{m=1}^{1}(-1)^{-1+m}\frac{\binom{3}{2}}{\binom{3}{m}}\binom{2}{1}\binom{1}{m-1}\binom{1}{2-m}=0\ . \tag{4.161}$$

Przejdźmy do obliczenia wartości własnej macierzy D_2^2. Operator Younga $P^{(3,1)}$ działa na wektor $|y\rangle$ ze zbioru 4.145 następująco

$$P^{(3,1)}|y\rangle \;=\; \frac{1}{2}(|1010\rangle+|1100\rangle-|0011\rangle-|1001\rangle)\ . \tag{4.162}$$

Z 4.152 i 4.162 dostajemy

$$\langle x^0|(P^{(3,1)})^\dagger P^{(3,1)}|y\rangle \;=\; -1\ . \tag{4.163}$$

Wartość własna macierzy D_2^2 dla $j=1$, obliczona ze wzoru 4.62, wynosi

$$\alpha_2^2(1) \;=\; -1\ . \tag{4.164}$$

Jest ona zgodna z wartością własną otrzymaną ze wzoru 4.94

$$\alpha_2^2(1) \;=\; \sum_{m=1}^{2}(-1)^{-1+m}\frac{\binom{3}{2}}{\binom{3}{m}}\binom{2}{2}\binom{1}{m-2}\binom{1}{2-m}=-1\ . \tag{4.165}$$

Korzystając ze wzoru 4.95 możemy wyznaczyć wartość własną stanu $\tilde{\rho}_2^4$ dla $j=1$

$$\lambda_2^4(1) \;=\; 1x^0+0x^2-1x^4=1-x^4\ . \tag{4.166}$$

Krotność wartości własnej 4.166, obliczona ze wzoru 4.97, wynosi

$$g_1^4 \;=\; 3\ . \tag{4.167}$$

Wreszcie rozpatrzmy przypadek parametru $j=2$. Diagram Younga ma wtedy postać

0	0
1	1

Odpowiadający mu operator Younga $P^{(2,2)}$ działa na wektor $|x^0\rangle$ następująco

$$P^{(2,2)}|x^0\rangle \;=\; \frac{2}{6}(|0011\rangle + |1100\rangle - |0110\rangle - |1001\rangle)\;. \tag{4.168}$$

Z powyższego wzoru otrzymujemy

$$\langle x^0|(P^{(2,2)})^\dagger P^{(2,2)}|x^0\rangle \;=\; \frac{4}{9}\;. \tag{4.169}$$

Najpierw obliczymy wartość własną macierzy D_0^2. Operator Younga $P^{(2,2)}$ przekształca wektor $|x^0\rangle$ ze zbioru 4.135 w następujący sposób

$$P^{(2,2)}|y\rangle \;=\; \frac{2}{6}(|0011\rangle + |1100\rangle - |0110\rangle - |1001\rangle)\;. \tag{4.170}$$

Z 4.168 i 4.174 dostajemy

$$\langle x^0|(P^{(2,2)})^\dagger P^{(2,2)}|y\rangle \;=\; \frac{4}{9}\;. \tag{4.171}$$

Wartość własna macierzy D_0^2 dla $j=2$ otrzymana na podstawie wzoru 4.97 wynosi

$$\alpha_0^2(2) \;=\; 1\;. \tag{4.172}$$

Identyczną wartość własną otrzymamy ze wzoru 4.94

$$\alpha_0^2(2) \;=\; \sum_{m=0}^{0}(-1)^{0+m}\frac{\binom{2}{2}}{\binom{2}{m}}\binom{2}{0}\binom{0}{m-0}\binom{2}{2-m} = 1\;. \tag{4.173}$$

Wyznaczmy teraz wartości własne macierzy D_1^2. Operator Younga $P^{(2,2)}$ działa na wektor $|y\rangle$ ze zbioru 4.140 następująco

$$P^{(2,2)}|y\rangle \;=\; \frac{4}{6}(|0110\rangle + |1001\rangle - |0011\rangle - |1100\rangle)\;. \tag{4.174}$$

Z 4.168 i 4.174 dostajemy

$$\langle x^0|(P^{2,2})^\dagger P^{(2,2)}|y\rangle \;=\; -\frac{8}{9}\;. \tag{4.175}$$

Wartość własna macierzy D_1^2 dla $j=2$ obliczona ze wzoru 4.97 wynosi

$$\alpha_1^2(2) \;=\; -2\;. \tag{4.176}$$

Identyczny wynik dostaniemy ze wzoru 4.94

$$\alpha_1^2(2) \;=\; \sum_{m=0}^{1}(-1)^{0+m}\frac{\binom{2}{2}}{\binom{2}{m}}\binom{2}{1}\binom{0}{m-1}\binom{2}{2-m} = -2\;. \tag{4.177}$$

Przejdźmy do obliczenia wartości własnej macierzy D_2^2. Operator Younga $P^{(2,2)}$ działa na wektor $|y\rangle$ ze zbioru 4.145 następująco

$$P^{(2,2)}|y\rangle \;=\; \frac{2}{6}(|0011\rangle + |1100\rangle - |0110\rangle - |1001\rangle)\;. \tag{4.178}$$

Z 4.168 i 4.178 otrzymujemy

$$\langle x^0|(P^{(2,2)})^\dagger P^{(2,2)}|y\rangle \;=\; \frac{4}{9}\,. \tag{4.179}$$

Obliczona ze wzoru 4.60 wartość własna macierzy D_2^2 dla $j=2$ wynosi

$$\alpha_2^2(2) \;=\; 1\,. \tag{4.180}$$

Jest ona zgodna z wartością własną obliczoną ze wzoru 4.94

$$\alpha_2^2(2) \;=\; \sum_{m=0}^{2}(-1)^{0+m}\frac{\binom{2}{2}}{\binom{2}{m}}\binom{2}{2}\binom{0}{m-2}\binom{2}{2-m}=1\,. \tag{4.181}$$

Znając $\alpha_0^2(2)$, $\alpha_1^2(2)$ i $\alpha_2^2(2)$, możemy wyznaczyć na podstawie wzoru 4.95 wartość własną stanu $\tilde{\rho}_2^4$ dla $j=2$

$$\lambda_2^4(2) \;=\; 1x^0-2x^2+1x^4=1-2x^2+x^4\,. \tag{4.182}$$

Jej krotność obliczona ze wzoru 4.97 wynosi:

$$g_2^4 \;=\; 2\,. \tag{4.183}$$

Wszystkie wyniki dla przypadku czterech kopii stanu ρ zebrano w tabeli 4.1.

Tabela 4.1: Wartości własne i ich krotności dla przypadku pomiaru na czterech kopiach stanu ρ_{AB}.

k	$\lambda_k^4(j)$	g_j^n
0	$\lambda_0^4(0)=1$	$g_0^4=1$
1	$\lambda_1^4(0)=1+3x^2$	$g_0^4=1$
	$\lambda_1^4(1)=1-x^2$	$g_1^4=3$
2	$\lambda_2^4(0)=1+3x^2+x^4$	$g_0^4=1$
	$\lambda_2^4(1)=1-x^4$	$g_1^4=3$
	$\lambda_2^4(2)=1-2x^2+x^4$	$g_2^4=2$
3	$\lambda_3^4(0)=1+3x^2$	$g_0^4=1$
	$\lambda_3^4(1)=1-x^2$	$g_1^4=3$
4	$\lambda_4^4(0)=1$	$g_0^4=1$

4.4 Wydajność protokołu

Znając wyrażenie na wartości własne stanu $\widetilde{\rho}_k^n$ oraz ich krotności, możemy powrócić do naszego pierwotnego zagadnienia, czyli wyznaczenia wzoru na entropię stanu ρ_{kAB}^n, a dalej na koherentną informację tego stanu i ostatecznie na wydajność naszego protokołu. Podstawiając do wzoru 4.96 wyrażenie $x = 2q - 1$ oraz dzieląc wartości własne przez czynnik normalizacyjny, dostajemy

$$\begin{aligned}\lambda_k^n(j) &= \frac{1}{\binom{n}{k}}\frac{1}{2^n}\sum_{l=0}^{k}(2q-1)^{2l}\sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r} \\ &\quad \binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r}.\end{aligned} \tag{4.184}$$

Są to wartości własne stanu ρ_{kAB}^n. Należy jednak zaznaczyć, że w powyższym wyrażeniu waga Hamminga k należy do zbioru $\{0,\dots\frac{n}{2}\}$, a nie – jak w poprzednim przypadku – do zbioru $\{0,\dots n\}$. W celu wyznaczenia wartości własnych w pozostałych przypadkach skorzystamy z faktu, że wartości własne dla wagi Hamminga k są takie same jak dla $n-k$. Podstawiając wyrażenie 4.184 do wzoru na entropię stanu i uwzględniając krotność każdej z wartości własnych danej wyrażeniem 4.97, dostajemy

$$\begin{aligned}S(\rho_{kAB}^n) &= \sum_{j=0}^{k}\binom{n}{j}\frac{n-2j+1}{n-j+1}\sum_{l=0}^{k}\frac{1}{\binom{n}{k}}(2q-1)^{2l}\sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r} \\ &\quad \binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r} \\ &\quad \log_2\left(\sum_{l=0}^{k}\frac{1}{\binom{n}{k}}(2q-1)^{2l}\sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r}\right. \\ &\quad \left.\binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r}\right).\end{aligned} \tag{4.185}$$

Podstawiając z kolei 4.185 do 4.13 dostajemy wzór na koherentną informację

$$\begin{aligned}I_c(\rho_{kAB}^n) &= \log_2\binom{n}{k} - \sum_{j=0}^{k}\binom{n}{j}\frac{n-2j+1}{n-j+1}\sum_{l=0}^{k}\frac{1}{\binom{n}{k}}(2q-1)^{2l} \\ &\quad \sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r}\binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r} \\ &\quad \log_2\left(\sum_{l=0}^{k}\frac{1}{\binom{n}{k}}(2q-1)^{2l}\sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r}\right. \\ &\quad \left.\binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r}\right).\end{aligned} \tag{4.186}$$

Aby otrzymać całkowitą wydajność protokołu, wyrażenie to należy podstawić do wzoru 4.7.

Załóżmy obecnie, ze stan z którego destylujemy splątanie jest stanem mieszanym składającym się z dwóch stanów maksymalnie splątanych różniących się fazą i stanu produktowego ortogonalnego do nich, to znaczy

$$\rho_{AB} = p\rho^{'}_{AB} + (1-p)\left|01\right\rangle\left\langle 01\right|_{AB} , \tag{4.187}$$

gdzie

$$\rho^{'}_{AB} = q|\phi^{+}\rangle\langle\phi^{+}|_{AB} + (1-q)|\phi^{-}\rangle\langle\phi^{-}|_{AB} , \tag{4.188}$$

natomiast

$$|\phi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(\left|00\right\rangle_{AB} + \left|11\right\rangle_{AB}\Big) , \tag{4.189}$$

$$|\phi^{-}\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(\left|00\right\rangle_{AB} - \left|11\right\rangle_{AB}\Big) . \tag{4.190}$$

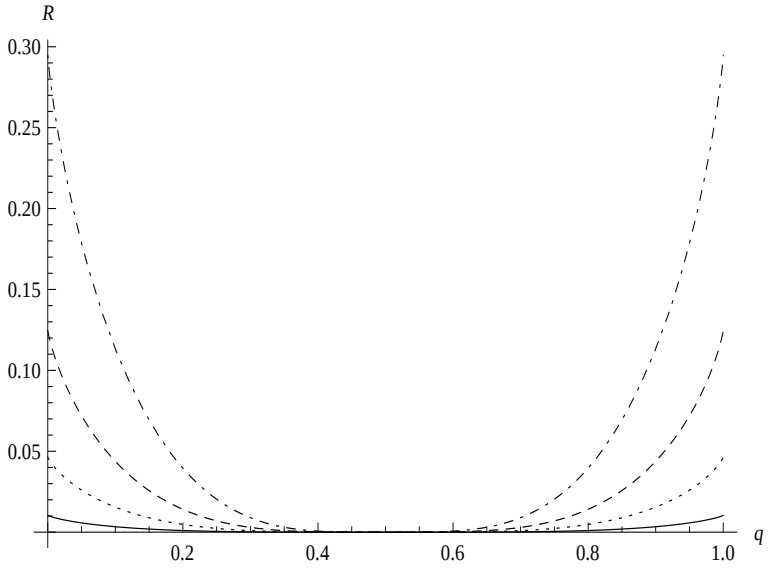
W takim przypadku wydajność naszego protokołu otrzymamy przyjmując we wzorze 4.7 $\alpha = \frac{1}{\sqrt{2}}$. Prowadzi to do następującego wzoru na splątanie wydestylowane z grupy $2^{m-(i-1)}$ par qubitów pod warunkiem, że Alicja i Bob otrzymają te same wyniki pomiarów

$$R_i = \sum_{k=0}^{2^{m-(i-1)}} \Big(\frac{1}{2^{2^{m-(i-1)}}}\binom{2^{m-(i-1)}}{k} I_c(\rho_{kAB}^{2^{m-(i-1)}}) , \tag{4.191}$$

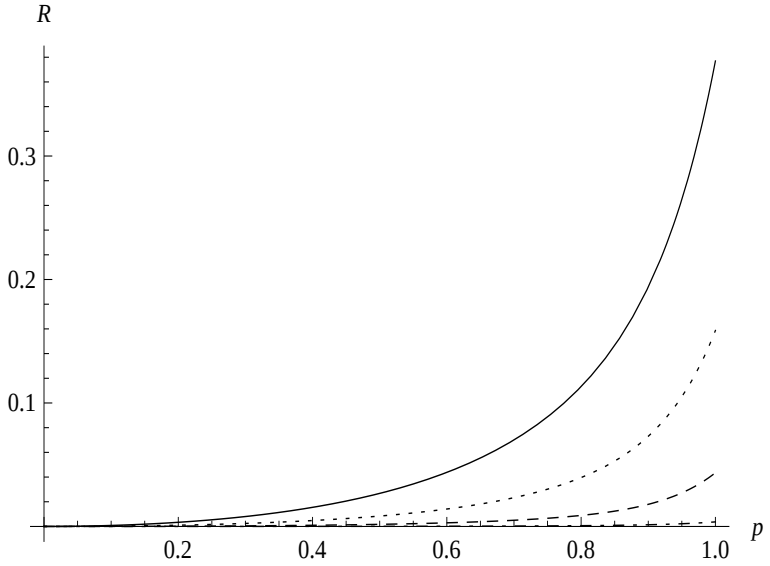
gdzie koherentna informacja jest dana wyrażeniem 4.186.

Na rysunkach 4.1 oraz 4.2 przedstawiono wydajność protokołu bisekcyjno-haszującego w zależności od parametrów q oraz p. Liczba kopii stanu 4.187, na których wykonywany jest pierwszy pomiar, wynosi $n = 16$. Z rysunku 4.1 widzimy, że dla danej wartości p wydajność jest symetryczna względem $q = \frac{1}{2}$. Symetria ta wynika z faktu, że stan 4.187 można przekształcić w stan 4.187 z parametrem q zastąpionym przez $1-q$ za pomocą lokalnej operacji unitarnej Z i ponadto operacja ta komutuje z operatorami rzutowymi 3.3. Wydajność protokołu wraz ze wzrostem q przyjmuje maksymalną wartość dla $q = 0$ i wartość 0 dla $q = \frac{1}{2}$. Zauważmy, że dla $q = \frac{1}{2}$ stan 4.187 jest stanem separowalnym. Z kolei z rysunku 4.2 widzimy, że dla danej wartości q wydajność rośnie od wartości 0 dla $p = 0$ do wartości maksymalnej dla $p = 1$. Pozwala nam to wyciągnąć wniosek, że wydajność protokołu jest niezerowa w całym zakresie parametrów, dla których stan 4.187 jest splątany. Warto również przedstawić, jak wydajność protokołu bisekcyjno-haszującego zależy od liczby kopii stanu 4.187, na których wykonywany jest pierwszy pomiar. Odpowiednie wyniki prezentują rysunki 4.3 i 4.4. Dla porównania przedstawiono również wydajność protokołu haszującego. Widzimy, że dla odpowiednio dużej wartości parametru p i szerokiego zakresu parametru q wydajność rośnie wraz z liczbą kopii stanu 4.187, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym. Ponadto dla szerokiego zakresu parametru p wydajność protokołu bisekcyjno-haszującego

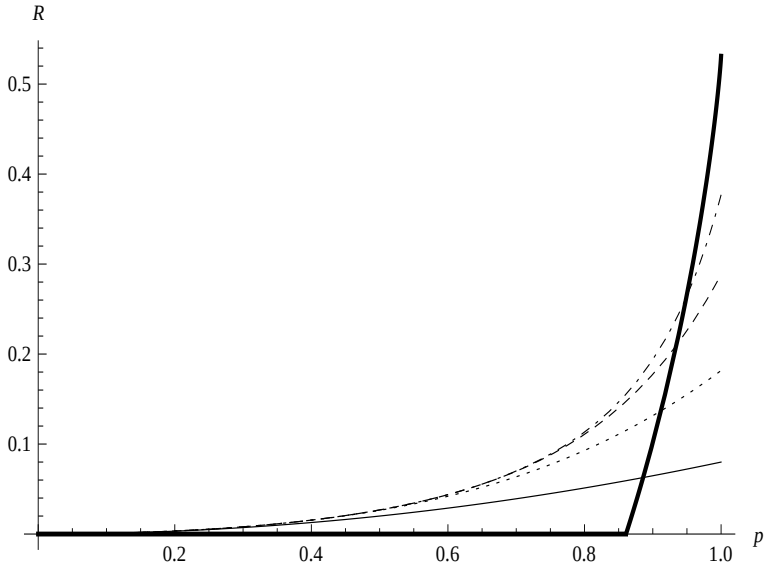
jest większa od wydajności protokołu haszującego. Na zakończenie dodajmy, że wykres dla $n = 2$ odpowiada również protokołowi Bennetta i innych z pracy [7], po którym następuje protokół haszujący.



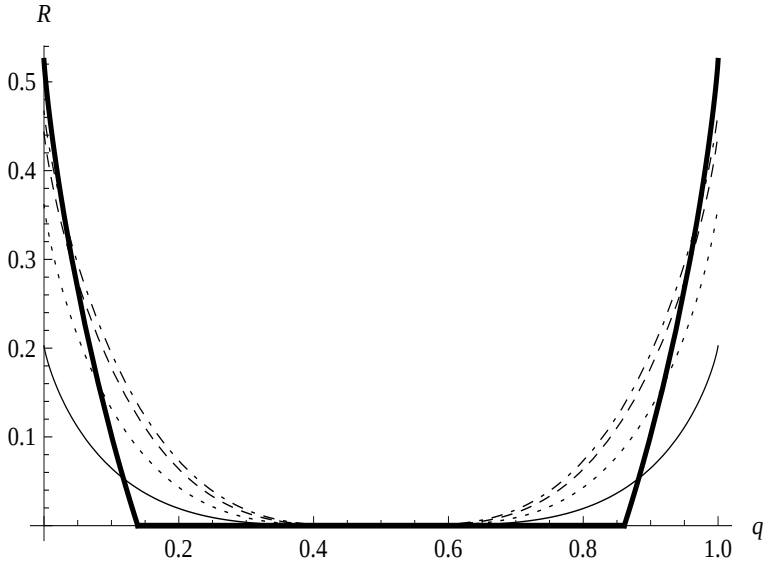
Rysunek 4.1: Zależność wydajności R protokołu bisekcyjno-haszującego dla stanu 4.187 od parametrów q i p: $p = 0,8$ – linia kreskowano-kropkowana, $p = 0,6$ – linia kreskowana, $p = 0,4$ – linia kropkowana, $p = 0,2$ – linia ciągła. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar, wynosi $n = 16$. Źródło: [71].



Rysunek 4.2: Zależność wydajności R protokołu bisekcyjno-haszującego dla stanu 4.187 od parametrów q i p: $q = 0,4$ – linia kreskowano-kropkowana, $q = 0,3$ – linia kreskowana, $q = 0,2$ – linia kropkowana, $q = 0,1$ – linia ciągła. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar, wynosi $n = 16$. Źródło: [71].



Rysunek 4.3: Zależność wydajności R protokołu bisekcyjno-haszującego dla stanu 4.187 od parametru p dla $q = 0,1$ i różnej liczby kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar: $n = 16$ – linia cienka kreskowano-kropkowana, $n = 8$ – linia cienka kreskowana, $n = 4$ – linia cienka kropkowana, $n = 2$ – linia cienka ciągła. Gruba ciągła linia oznacza wydajność protokołu haszującego. Źródło: [71].



Rysunek 4.4: Zależność wydajności R protokołu bisekcyjno-haszującego dla stanu 4.187 od parametru q dla $p = 0,9$ i różnej liczby kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar: $n = 16$ – linia cienka kreskowano-kropkowana, $n = 8$ – linia cienka kreskowana, $n = 4$ – linia cienka kropkowana, $n = 2$ – linia cienka ciągła. Gruba ciągła linia oznacza wydajność protokołu haszującego. Źródło: [71].

ROZDZIAŁ 5

Destylacja splątania ze stanów mieszanych składających się z czystego stanu splątanego i dwóch czystych stanów produktowych

5.1 Opis protokołu

Bisekcyjny protokół destylacji w połączeniu z jednokierunkowym protokołem haszującym może zostać zastosowany również do mieszanych stanów splątanych rzędu 3, składających się z czystego stanu splątanego oraz dwóch czystych stanów produktowych. O wszystkich stanach czystych założymy, że są wzajemnie ortogonalne [78]. Stan ten przedstawimy w następującej postaci

$$\rho_{AB} \;=\; p|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB} + q\,|01\rangle\,\langle 01|_{AB} + r\,|10\rangle\,\langle 10|_{AB}\;, \tag{5.1}$$

gdzie

$$|\phi^+(\alpha)\rangle_{AB} \;=\; \alpha\,|00\rangle_{AB} + \sqrt{1-\alpha^2}\,|11\rangle_{AB}\;. \tag{5.2}$$

Bez straty ogólności przyjmujemy, że parametr α należy do zbioru liczb rzeczywistych.

Załóżmy, że Alicja i Bob posiadają n kopii stanu 5.1. Stan całego układu możemy zapisać następująco

$$\rho_{AB}^{\otimes n} \;=\; \sum_{\substack{k_1,k_2,k_3;\\ k_1+k_2+k_3=n}} \Big(p^{k_1} q^{k_2} r^{k_3} |\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB}^{\otimes k_1} \otimes \tag{5.3}$$

$$|01\rangle\,\langle 01|_{AB}^{\otimes k_2} \otimes |10\rangle\,\langle 10|_{AB}^{\otimes k_3} + \text{permutacje} \Big)\;.$$

Na stanie 5.3 Alicja i Bob stosują protokół bisekcyjny. Stan po pomiarze w przypadku koincydencji wyznaczymy na podstawie wzoru

$$\rho^n_{kAB} = \frac{P_{kA}\otimes P_{kB}\rho^{\otimes n}_{AB}P_{kA}\otimes P_{kB}}{\mathrm{Tr}(P_{kA}\otimes P_{kB}\rho^{\otimes n}_{AB}P_{kA}\otimes P_{kB})}\ , \tag{5.4}$$

gdzie operatory rzutowe P_{kA} i P_{kB} opisane są wzorem 3.3. Zauważmy, że para operatorów rzutowych P_{kA} i P_{kB} anihiluje wszystkie człony we wzorze 5.3, dla których $k_2 \neq k_3$. Stąd liczba stanów $|01\rangle\langle 01|_{AB}$ oraz $|10\rangle\langle 10|_{AB}$ musi być równa. Oznaczymy ją przez j. Wtedy stan po pomiarze możemy zapisać następująco

$$\begin{aligned}\rho^n_{kAB} = {} & \frac{1}{p(n,k,\alpha)}\sum_{j=0}^{k} p^{n-2j}q^j r^j (P_{(k-j)A}|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|^{\otimes n-2j}_{AB}P_{(k-j)A}\otimes \\ & |01\rangle\langle 01|^{\otimes j}_{AB}\otimes|10\rangle\langle 10|^{\otimes j}_{AB} + \text{permutacje})\ ,\end{aligned} \tag{5.5}$$

gdzie przez *permutacje* rozumiemy permutacje par qubitów w stanach $|01\rangle\langle 01|_{AB}$ i $|10\rangle\langle 10|_{AB}$ oraz par qubitów ze stanu $P_{(k-j)A}|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|^{\otimes n-2j}_{AB}P_{(k-j)A}$, przy czym nie uwzględniamy permutacji, które nie zmieniają stanu $P_{(k-j)A}|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|^{\otimes n-2j}_{AB}$ $P_{(k-j)A}\otimes|01\rangle\langle 01|^{\otimes j}_{AB}\otimes|10\rangle\langle 10|^{\otimes j}_{AB}$. Mówiąc ściślej, nie permutujemy między sobą par qubitów na pozycjach $1,...n-2j$, nie permutujemy między sobą par qubitów na pozycjach $n-2j+1,...n-j$ i nie permutujemy między sobą par qubitów na pozycjach $n-j+1,...n$. Natomiast permutujemy na przykład dowolną parę qubitów z pozycji $1,...n-2j$ z dowolną parą qubitów z pozycji $n-2j+1,...n$. Ponieważ wszystkich permutacji mamy $n!$, a permutacji niezmieniających stanu $P_{(k-j)A}|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|^{\otimes n-2j}_{AB}P_{(k-j)A}\otimes|01\rangle\langle 01|^{\otimes j}_{AB}\otimes$ $|10\rangle\langle 10|^{\otimes j}_{AB}$ jest $(n-2j)!j!j!$, więc wyrażenie $(P_{(k-j)A}|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|^{\otimes n-2j}_{AB}P_{(k-j)A}\otimes$ $|01\rangle\langle 01|^{\otimes j}_{AB}\otimes|10\rangle\langle 10|^{\otimes j}_{AB}+\text{permutacje})$ składa się z $\frac{n!}{(n-2j)!j!j!}$ stanów czystych. Co więcej stany te są do siebie wzajemnie ortogonalne. Zauważmy również, że stany $(P_{(k-j)A}|\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|^{\otimes n-2j}_{AB}P_{(k-j)A}\otimes|01\rangle\langle 01|^{\otimes j}_{AB}\otimes|10\rangle\langle 10|^{\otimes j}_{AB}+\text{permutacje})$ z różnymi j mają nośniki na ortogonalnych podprzestrzeniach. Możemy więc od razu wyznaczyć wartości własne stanu 5.5. Wyrażają się one wzorem

$$\lambda(n,k,j,\alpha) = \frac{1}{p(n,k,\alpha)}|\alpha|^{2(n-k-j)}|\sqrt{1-\alpha^2}|^{2(k-j)}\binom{n-2j}{k-j}p^{n-2j}q^j r^j\ . \tag{5.6}$$

Natomiast krotność wartości własnej $\lambda(n,k,j,\alpha)$ wynosi

$$\chi(\lambda(n,k,j,\alpha)) = \frac{n!}{(n-2j)!j!j!}, \tag{5.7}$$

gdzie $j \leqslant \min\{k, n-k\}$. Współczynnik normalizacyjny we wzorach 5.5 i 5.6 musi być wybrany tak, aby suma wszystkich wartości własnych wynosiła 1, a więc przyjmuje on wartość

$$\begin{aligned}p(n,k,\alpha) = {} & \sum_{j=0}^{j\leqslant\min\{k,n-k\}} \frac{n!}{(n-2j)!j!j!}|\alpha|^{2(n-k-j)}|\sqrt{1-\alpha^2}|^{2(k-j)} \\ & \binom{n-2j}{k-j}p^{n-2j}q^j r^j\ .\end{aligned} \tag{5.8}$$

Dodajmy, że współczynnik ten jest jednocześnie prawdopodobieństwem otrzymania zarówno przez Alicję jak i Boba wyniku pomiaru k.

Powtarzając rozumowanie z rozdziału 3, dostaniemy następujące wyrażenie na wydajność całego protokołu

$$R = \frac{1}{2^m}\Big(p(S_1)R_1 + p(S_2,F_1)R_2 + \cdots + 2^{i-2}p(S_i,F_{i-1})R_i + \ldots\Big) , \tag{5.9}$$

gdzie $p(S_1)$ jest prawdopodobieństwem tego, że Alicja i Bob otrzymają w pierwszym kroku te same wyniki pomiarów; $p(S_i,F_{i-1})$ jest łącznym prawdopodobieństwem tego, że Alicja i Bob otrzymają w i-tym kroku te same wyniki pomiarów na jednej z dwóch grup $2^{m-(i-1)}$ par qubitów i nie otrzymają tych samych wyników pomiarów w $i-1$-szym kroku dla grupy $2^{m-(i-2)}$ par qubitów składającej się z wymienionych wyżej grup. R_i jest splątaniem wydestylowanym z grupy $2^{m-(i-1)}$ par qubitów pod warunkiem, że Alicja i Bob otrzymali te same wyniki pomiarów. Jeżeli Alicja i Bob dla danej grupy qubitów otrzymali te same wyniki pomiarów, wtedy mogą wydestylować z niej splątanie za pomocą protokołu haszującego (pod warunkiem, że koherentna informacja stanu po pomiarze jest dodatnia). Przypomnijmy, że w takim przypadku Alicja i Bob muszą posiadać wiele grup par qubitów, dla których otrzymali te same wyniki pomiarów i splątanie to należy rozumieć, jako splątanie przypadające na grupę par qubitów. Wymienione wyżej wielkości są dane następującymi wzorami

$$p(S_1) = \sum_{k=0}^{2^m} p(2^m,k,\alpha) , \tag{5.10}$$

$$p(S_i,F_{i-1}) = 2\sum_{k=0}^{2^{m-(i-1)}} p(2^{m-(i-1)},k,\alpha)(1-\sum_{k=0}^{2^{m-(i-1)}} p(2^{m-(i-1)},k,\alpha)) , \tag{5.11}$$

$$R_i = \frac{\sum_{k=0}^{2^{m-(i-1)}} p(2^{m-(i-1)},k,\alpha)\max\{I_c(\rho_{kAB}^{2^{m-(i-1)}}),0\}}{\sum_{k=0}^{2^{m-(i-1)}} p(2^{m-(i-1)},k,\alpha)} , \tag{5.12}$$

gdzie $I_c(\rho_{kAB}^{2^{m-(i-1)}})$ jest koherentną informacją stanu $\rho_{kAB}^{2^{m-(i-1)}}$. Ponadto założyliśmy, że w pierwszym kroku Alicja i Bob dokonują pomiaru na $n=2^m$ parach qubitów. Podstawiając te wzory do wyrażenia 5.9, dostaniemy

$$\begin{aligned} R &= \frac{1}{2^m}\sum_{k=0}^{2^m} p(2^m,k,\alpha)\max\{I_c(\rho_{kAB}^{2^m}),0\} + \\ &+ \frac{1}{2^m}\sum_{i=2}^{m} 2^{i-1}(1-\sum_{k=0}^{2^{m-(i-1)}} p(2^{m-(i-1)},k,\alpha)) \\ &\quad (\sum_{k=0}^{2^{m-(i-1)}} p(2^{m-(i-1)},k,\alpha)\max\{I_c(\rho_{kAB}^{2^{m-(i-1)}}),0\}) . \end{aligned} \tag{5.13}$$

Pozostaje nam do obliczenia koherentna informacja

$$I_c(\rho_{kAB}^n) = S(\rho_{kA(B)}^n) - S(\rho_{kAB}^n) . \tag{5.14}$$

Zarówno entropia podukładu Alicji, jak i entropia podukładu Bob wynosi

$$S(\rho^n_{kA(B)}) \;=\; \log_2 \binom{n}{k}\,, \tag{5.15}$$

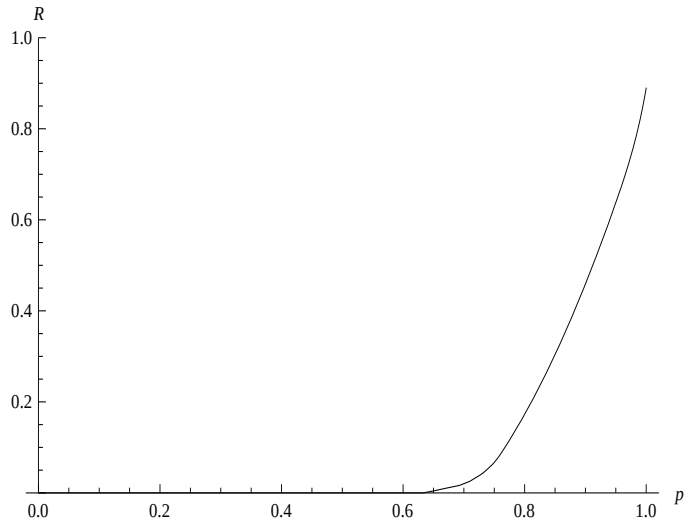
gdzie $\binom{n}{k}$ jest liczbą ciągów n-bitowych zawierających k jedynek. Entropię całego układu możemy obliczyć korzystając z wzorów 5.6, 5.7. Jest ona dana wyrażeniem

$$\begin{aligned} S(\rho^n_{kAB}) \;=\; -\sum_{j=0}^{\min\{k,n-k\}} & \frac{n!}{(n-2j)!j!j!}\frac{|\alpha|^{2(n-k-j)}|\sqrt{1-\alpha^2}|^{2(k-j)}\binom{n-2j}{k-j}p^{n-2j}q^j r^j}{p(n,k,\alpha)} \\ & \log_2\Big(\frac{|\alpha|^{2(n-k-j)}|\sqrt{1-\alpha^2}|^{2(k-j)}\binom{n-2j}{k-j}p^{n-2j}q^j r^j}{p(n,k,\alpha)}\Big). \end{aligned} \tag{5.16}$$

Ostatecznie koherentna informacja wynosi

$$\begin{aligned} I_c(\rho^n_{kAB}) \;=\; & \log_2\binom{n}{k} + \\ & + \sum_{j=0}^{\min\{k,n-k\}} \frac{n!}{(n-2j)!j!j!}\frac{|\alpha|^{2(n-k-j)}|\sqrt{1-\alpha^2}|^{2(k-j)}\binom{n-2j}{k-j}p^{n-2j}q^j r^j}{p(n,k,\alpha)} \\ & \log_2\Big(\frac{|\alpha|^{2(n-k-j)}|\sqrt{1-\alpha^2}|^{2(k-j)}\binom{n-2j}{k-j}p^{n-2j}q^j r^j}{p(n,k,\alpha)}\Big). \end{aligned} \tag{5.17}$$

Na rysunku 5.1 przedstawiono zależność wydajności R protokołu bisekcyjno-haszującego od parametru p dla stanu ρ_{AB}, w którym waga stanu $|01\rangle\langle 01|_{AB}$ jest dwa razy mniejsza od wagi stanu $|10\rangle\langle 10|_{AB}$. Więcej uwagi wydajności protokołu poświęcimy w następnym punkcie.



Rysunek 5.1: Zależność wydajności R protokołu bisekcyjno-haszującego od parametru p dla stanu 5.1 z następującymi parametrami: $q = \frac{1-p}{3}$, $r = \frac{2(1-p)}{3}$ i $\alpha = \frac{1}{\sqrt{2}}$. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 32$.

5.2 Przypadek stanu ρ_{AB} o równych parametrach q i r

Rozważmy przypadek stanu ρ o parametrach $q = r = \frac{1-p}{2}$ oraz $\alpha = \frac{1}{\sqrt{2}}$. Postać tego stanu będzie następująca

$$\rho_{AB} = p|\phi^+\rangle\langle\phi^+|_{AB} + \frac{1-p}{2}(|01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}) , \tag{5.18}$$

gdzie

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) . \tag{5.19}$$

Zauważmy, że stan ten jest szczególnym przypadkiem stanu diagonalnego w bazie Bella, a mianowicie

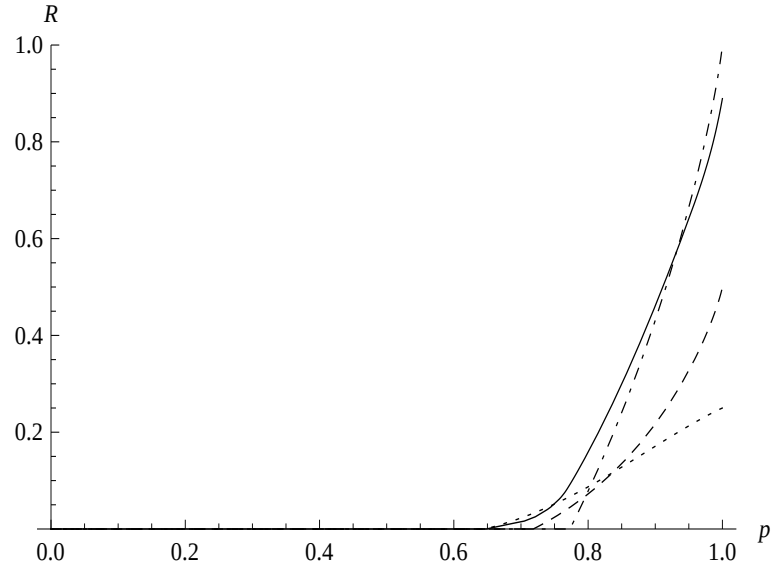
$$\rho_{AB} = p|\phi^+\rangle\langle\phi^+|_{AB} + \frac{1-p}{2}|\psi^+\rangle\langle\psi^+|_{AB} + \frac{1-p}{2}|\psi^-\rangle\langle\psi^-|_{AB} , \tag{5.20}$$

gdzie

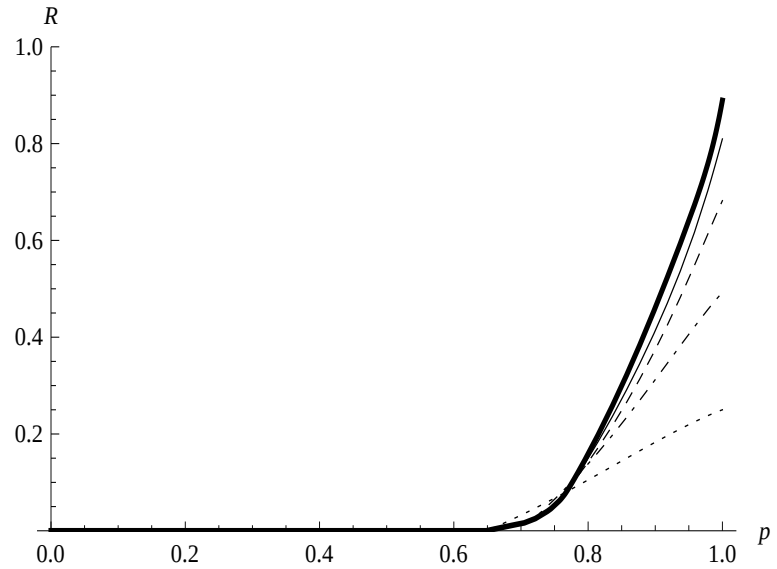
$$|\psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}) . \tag{5.21}$$

Korzystając ze wzorów 5.8, 5.13, 5.17 z $q = r = \frac{1-p}{2}$, otrzymujemy wzór na wydajność protokołu dla stanu 5.18.

Zależność wydajności R od parametru p dla liczby kopii stanu ρ_{AB}, na której wykonywany jest pierwszy pomiar $n = 32$, jest przedstawiona na rysunku 5.2. Dodatkowo przedstawiono wydajność protokołu haszującego i protokołu rekurencyjnego połączonego z protokołem haszującym. W pierwszym przypadku wykonano jeden krok rekurencji i na otrzymanym stanie zastosowano protokół haszujący. W drugim przypadku wykonano dwa kroki rekurencji i na otrzymanym stanie zastosowano protokół haszujący. Zauważmy, że protokół rekurencyjny, w przeciwieństwie do protokołu bisekcyjno-haszującego, jest mało wydajny dla dużych wartości parametru p. Dodajmy jednak, że dla $p > 1/2$ protokół rekurencyjny (z odpowiednio dużą liczbą kroków) w połączeniu z protokołem haszującym, pozwala wydestylować splątanie z niezerową wydajnością. Natomiast, jak widać z rysunku 5.2, bisekcyjno-haszujący protokół destylacji splątania dla $n = 32$ pozwala wydestylować splątanie tylko dla $p > 0,6484$. Pojawia się wobec tego pytanie, czy zwiększając liczbę kopii, na których wykonywany jest pierwszy pomiar, można zwiększyć wydajność protokołu bisekcyjno-haszującego. Na rysunku 5.3 przedstawiono, jak wydajność R zależy od tej liczby. Na podstawie tego rysunku można wyciągnąć wniosek, że zwiększając n powyżej 32 raczej nie można zdecydowanie poprawić wydajności protokołu.



Rysunek 5.2: Zależność wydajności R różnych protokołów destylacji splątania od parametru p: protokół biesekcyjno-haszujący – linia ciągła, protokół haszujący – linia kreskowano-kropkowana, protokół rekurencyjny połączony z protokołem haszującym dla jednego kroku rekurencji – linia kreskowana, protokół rekurencyjny połączony z protokołem haszującym dla dwóch kroków rekurencji – linia kropkowana. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 32$.



Rysunek 5.3: Zależność wydajności R protokołu bisekcyjno-haszującego od parametru p dla rożnej liczby kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar: $n = 2$ – linia kropkowana, $n = 4$ – linia kreskowano-kropkowana, $n = 8$ – linia kreskowana, $n = 16$ – linia ciągła cienka, $n = 32$ – linia ciągła gruba.

ROZDZIAŁ 6

Dolne ograniczenia na pojemność Q_2 wybranych kanałów kwantowych

6.1 Wprowadzenie

Wykorzystując bisekcyjny lub bisekcyjno-haszujący protokół destylacji splątania, znajdziemy dolne ograniczenia na pojemność Q_2 dla następujących kanałów kwantowych:

- kanału tłumiącego amplitudę,
- kanału będącego złożeniem kanału tłumiącego amplitudę i kanału zmieniającego fazę,
- uogólnionego kanału tłumiącego amplitudę.

Ograniczenia te we wszystkich przypadkach znajdziemy w następujący sposób. Najpierw Alicja przygotuje u siebie czyste stany splątane, po czym prześle przez kanał kwantowy po jednym qubicie z każdego stanu do Boba. W ten sposób Alicja i Bob otrzymają pewne mieszane stany splątane. Następnie Alicja i Bob wydestylują z tych stanów stany maksymalnie splątane. Wreszcie, wykorzystując wydestylowane stany maksymalnie splątane, Alicja teleportuje qubity niosące informację kwantową do Boba. Dolne ograniczenie na pojemność Q_2 kanału kwantowego będzie wtedy równe wydajności protokołu destylacji splątania dla mieszanych stanów splątanych, otrzymanych z początkowych czystych stanów splątanych. Chcąc otrzymać jak największe dolne ograniczenie na pojemność

Q_2 kanału kwantowego, wydajność tę zoptymalizujemy po początkowych czystych stanach splątanych. Ograniczymy się przy tym tylko do takich stanów, dla których znamy analityczny wzór na wydajność protokołu destylacji splątania.

6.2 Dolne ograniczenie na pojemność Q_2 dla kanału tłumiącego amplitudę

Załóżmy, że Alicja przygotuje wiele par qubitów w stanach splątanych

$$|\phi(\alpha)\rangle_{AB} = \alpha\,|00\rangle_{AB} + \sqrt{1-\alpha^2}\,|11\rangle_{AB} \ . \tag{6.1}$$

Następnie Alicja przesyła po jednym qubicie z każdej pary do Boba za pomocą kanału tłumiącego amplitudę. W ten sposób powstaje wiele mieszanych stanów splątanych postaci

$$\begin{aligned} \rho_{AB} &= I \otimes E_0^{\mathsf{ad}} |\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB} (I \otimes E_0^{\mathsf{ad}})^\dagger + \\ &+ I \otimes E_1^{\mathsf{ad}} |\phi^+(\alpha)\rangle\langle\phi^+(\alpha)|_{AB} (I \otimes E_1^{\mathsf{ad}})^\dagger \ , \end{aligned} \tag{6.2}$$

gdzie

$$E_0^{\mathsf{ad}} = |0\rangle\langle 0|_B + \sqrt{1-\gamma}\,|1\rangle\langle 1|_B \ , \tag{6.3}$$

$$E_1^{\mathsf{ad}} = \sqrt{\gamma}\,|0\rangle\langle 1|_B \ , \tag{6.4}$$

są operatorami Krausa dla tego kanału (porównaj 2.12-2.13). Stan 6.2 w postaci jawnej wygląda następująco

$$\begin{aligned} \rho_{AB} &= \alpha^2\,|00\rangle\langle 00|_{AB} + (1-\alpha^2)(1-\gamma)\,|11\rangle\langle 11|_{AB} + \\ &+ \alpha\sqrt{1-\alpha^2}\sqrt{1-\gamma}(|00\rangle\langle 11| + |11\rangle\langle 00|_{AB}) + \\ &+ (1-\alpha^2)\gamma\,|10\rangle\langle 10|_{AB} \ . \end{aligned} \tag{6.5}$$

Po prostych przekształceniach otrzymujemy

$$\rho'_{AB} = p'\,|\phi^+(\alpha')\rangle\langle\phi^+(\alpha')|_{AB} + (1-p')\,|01\rangle\langle 01|_{AB} \ , \tag{6.6}$$

gdzie

$$|\phi^+(\alpha')\rangle_{AB} = \alpha'\,|00\rangle_{AB} + \sqrt{1-(\alpha')^2}\,|11\rangle_{AB} \ , \tag{6.7}$$

$$\alpha' = \frac{\alpha}{\sqrt{1-(1-\alpha^2)\gamma}} \ , \tag{6.8}$$

$$p' = 1-(1-\alpha^2)\gamma \ . \tag{6.9}$$

Widzimy, że stan 6.6 ma taką samą postać jak stan 3.1. Można więc do wielu kopii tego stanu zastosować protokół destylacji splątania opisany w punkcie 3.1 rozdziału 3.

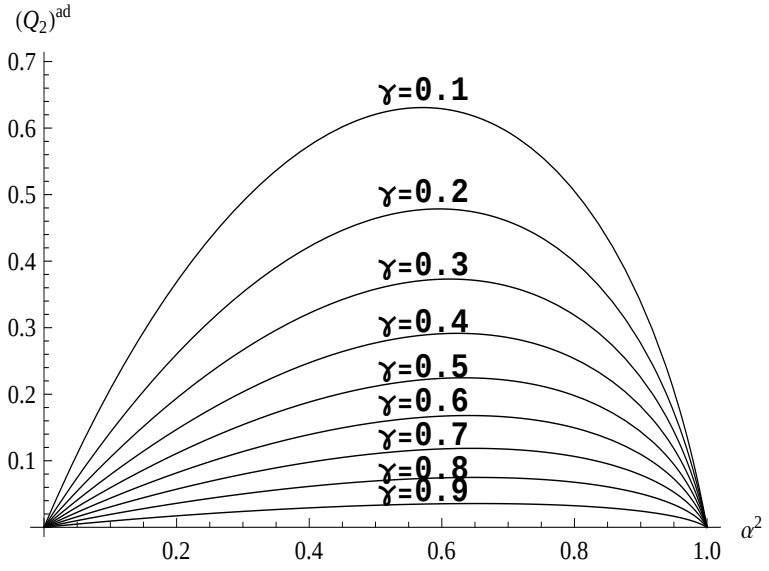
Podstawiając zależności 6.8 i 6.9 do wzorów 3.14 i 3.16, otrzymujemy wzór na dolne ograniczenie na pojemność Q_2 kanału tłumiącego amplitudę

$$Q_2^{\mathsf{ad}} \geqslant \frac{1}{2^m}\sum_{i=1}^{m} p'^{\,2^{m-(i-1)}}(2^{i-1}R_i^{\mathsf{ad}} - 2^i R_{i+1}^{\mathsf{ad}}) \,, \tag{6.10}$$

gdzie

$$R_i^{\mathsf{ad}} = \sum_{k=0}^{2^{m-(i-1)}} \alpha'^{\,2(2^{m-(i-1)}-k)}(\sqrt{1-\alpha'^{\,2}})^{2k}\binom{2^{m-(i-1)}}{k} \times \log_2\binom{2^{m-(i-1)}}{k} \,. \tag{6.11}$$

Zależność dolnego ograniczenia na pojemność Q_2^{ad} od parametru α^2 dla różnych wartości współczynnika tłumienia γ przedstawiono na rysunku 6.2[1]. Jako liczbę kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, przyjęto $n = 64$. Natomiast w tabeli 6.1 podano maksymalne wartości tego ograniczenia i odpowiadające im wartości parametru α^2.



Rysunek 6.1: Zależność dolnego ograniczenia na pojemność Q_2^{ad} kanału tłumiącego amplitudę od parametru α^2 dla różnych wartości współczynnika tłumienia γ. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$.

[1]Użyto parametru α^2 zamiast α, ponieważ lepiej oddaje on symetrię problemu. W takiej parametryzacji wartość $\alpha^2 = \frac{1}{2}$ odpowiada przygotowaniu przez Alicję stanów maksymalnie splątanych.

Tabela 6.1: Maksymalne wartości dolnego ograniczenia na pojemność Q_2^{ad} kanału tłumiącego amplitudę dla różnych wartości współczynnika tłumienia γ oraz wartości parametru α^2, które im odpowiadają. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjnym, wynosi $n = 64$.

γ	Q_2^{ad}	α^2
$0,1$	$0,630819$	$0,570914$
$0,2$	$0,478489$	$0,59591$
$0,3$	$0,373067$	$0,611936$
$0,4$	$0,2915$	$0,623666$
$0,5$	$0,224687$	$0,632738$
$0,6$	$0,167981$	$0,639943$
$0,7$	$0,118655$	$0,645728$
$0,8$	$0,0749596$	$0,650363$
$0,9$	$0,0356947$	$0,654009$

6.3 Dolne ograniczenie na pojemność Q_2 dla kanału tłumiącego amplitudę i zmieniającego fazę

Niech Alicja prześle do Boba po jednym qubicie z każdej wielu par qubitów w stanie 6.1 przez kanał tłumiący amplitudę i zmieniający fazę. Operatory Krausa dla takiego kanału są następujące (porównaj 2.31-2.33)

$$E_0^{\mathsf{adpf}} = \sqrt{1-\eta}(|0\rangle\langle 0|_B + \sqrt{1-\gamma}\,|1\rangle\langle 1|_B)\ , \tag{6.12}$$

$$E_1^{\mathsf{adpf}} = \sqrt{\eta}(|0\rangle\langle 0|_B - \sqrt{1-\gamma}\,|1\rangle\langle 1|_B)\ , \tag{6.13}$$

$$E_2^{\mathsf{adpf}} = \sqrt{\gamma}\,|0\rangle\langle 1|_B\ . \tag{6.14}$$

Na wyjściu kanału, pojedynczy stan mieszany będzie miał postać

$$\begin{aligned}\rho_{AB} &= \alpha^2|00\rangle\langle 00|_{AB} + (1-\alpha^2)(1-\gamma)|11\rangle\langle 11|_{AB} + \\ &+ \alpha\sqrt{1-\alpha^2}(2\eta-1)\sqrt{1-\gamma}(|00\rangle\langle 11|_{AB} + |11\rangle\langle 00|_{AB}) + \\ &+ (1-\alpha^2)\gamma|10\rangle\langle 10|_{AB}\ .\end{aligned} \tag{6.15}$$

Stan 6.15 możemy przedstawić w formie

$$\begin{aligned}\rho'_{AB} &= p'((1-\eta)|\phi^+(\alpha')\rangle\langle\phi^+(\alpha')|_{AB} + \eta|\phi^-(\alpha')\rangle\langle\phi^-(\alpha'|_{AB}) + \\ &+ (1-p')|01\rangle\langle 01|_{AB}\ ,\end{aligned} \tag{6.16}$$

gdzie

$$|\phi^+(\alpha')\rangle_{AB} = \alpha' |00\rangle_{AB} + \sqrt{1-(\alpha')^2}\,|11\rangle_{AB} \ , \tag{6.17}$$

$$|\phi^-(\alpha')\rangle_{AB} = \alpha' |00\rangle_{AB} - \sqrt{1-(\alpha')^2}\,|11\rangle_{AB} \ , \tag{6.18}$$

$$\alpha' = \frac{\alpha}{\sqrt{1-(1-\alpha^2)\gamma}} \ , \tag{6.19}$$

$$p' = 1-(1-\alpha^2)\gamma \ . \tag{6.20}$$

Zauważmy, że stan ten ma postać 4.1. Możemy więc do wielu kopii tego stanu zastosować bisekcyjno-haszujący protokół destylacji splątania. Podstawiając odpowiednie wartości do wzorów 4.6, 4.7 i 4.186 dostaniemy następujące wyrażenie na dolne ograniczenie na pojemność Q_2 dla kanału tłumiącego amplitudę i zmieniającego fazę

$$Q_2^{\mathsf{adpf}} \geqslant \frac{1}{2^m}\sum_{i=1}^{m} p'^{\,2^{m-(i-1)}}(2^{i-1}R_i^{\mathsf{adpf}} - 2^i R_{i+1}^{\mathsf{adpf}}) \ , \tag{6.21}$$

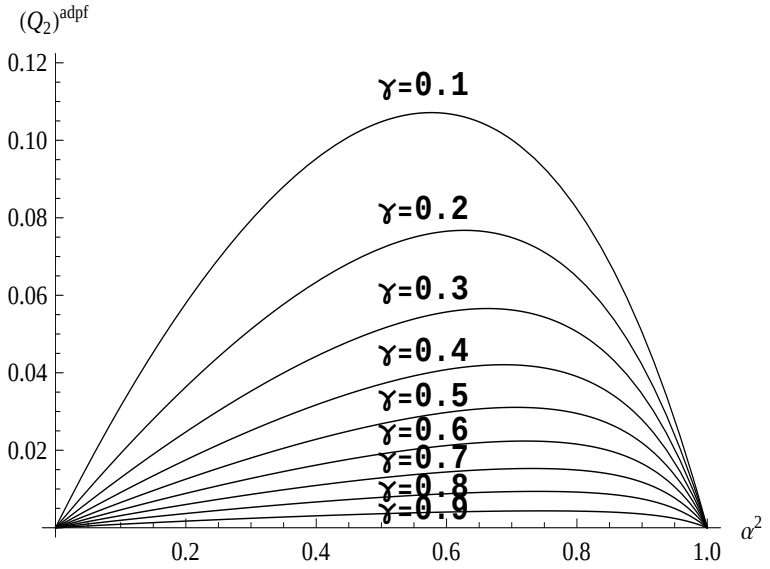
gdzie

$$R_i^{\mathsf{adpf}} = \sum_{k=0}^{2^{m-(i-1)}} \alpha^{2(2^{m-(i-1)}-k)}(\sqrt{1-\alpha^2})^{2k}\binom{2^{m-(i-1)}}{k} I_c(\rho_{kAB}^{2^{m-(i-1)}}) \tag{6.22}$$

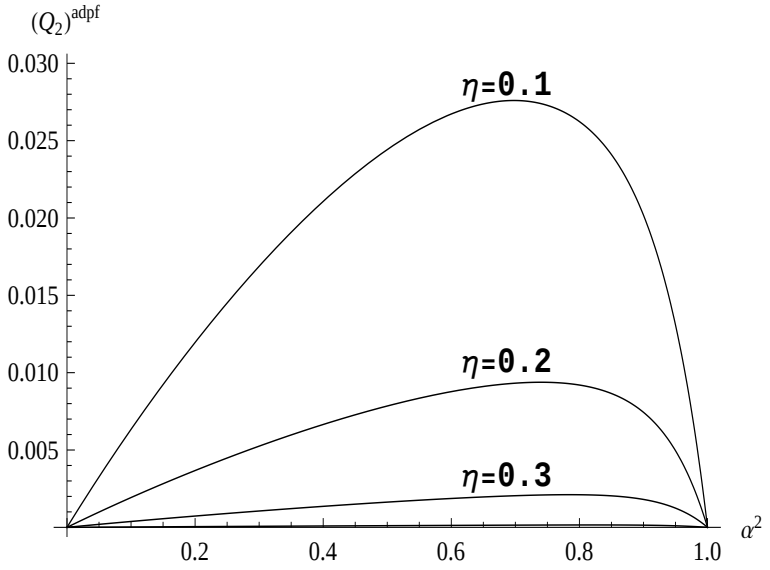
oraz

$$\begin{aligned} I_c(\rho_{kAB}^n) = {} & \log_2\binom{n}{k} - \sum_{j=0}^{k}\binom{n}{j}\frac{n-2j+1}{n-j+1}\sum_{l=0}^{k}\frac{1}{\binom{n}{k}}(1-2\eta)^{2l} \\ & \sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r}\binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r} \\ & \log_2\left(\sum_{l=0}^{k}\frac{1}{\binom{n}{k}}(1-2\eta)^{2l}\sum_{r=\min\{l,k-j\}}^{\max\{0,l-j\}}(-1)^{l-r}\right. \\ & \left.\binom{k-j+l-r}{l}\binom{n-k-l+r}{r}\binom{j}{l-r}\right) . \end{aligned} \tag{6.23}$$

Na rysunkach 6.2 i 6.3 przedstawiono zależność dolnego ograniczenia na pojemność Q_2^{adpf} od parametru α^2 dla różnych wartości współczynników tłumienia γ i współczynników zmiany fazy. Jako liczbę kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, przyjęto $n = 16$. Natomiast w tabelach 6.2 i 6.3 podano maksymalne wartości tego ograniczenia i odpowiadające im wartości parametru α^2.



Rysunek 6.2: Zależność dolnego ograniczenia na pojemność Q_2^{adpf} kanału tłumiącego amplitudę i zmieniającego fazę od parametru α^2 dla różnych współczynników tłumienia γ i współczynnika zmiany fazy $\eta = 0, 2$. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 16$.



Rysunek 6.3: Zależność dolnego ograniczenia na pojemność Q_2^{adpf} kanału tłumiącego amplitudę i zmieniającego fazę od parametru α^2 dla różnych współczynników zmiany fazy η i współczynnika tłumienia $\gamma = 0, 8$. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 16$.

Tabela 6.2: Maksymalne wartości dolnego ograniczenia na pojemność Q_2^{adpf} kanału tłumiącego amplitudę i zmieniającego fazę dla różnych wartości współczynników tłumienia γ i współczynnika zmiany fazy $\eta = 0,2$ oraz wartości parametru α^2, które im odpowiadają. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 16$.

γ	Q_2^{adpf}	α^2
$0,1$	$0,107143$	$0,576548$
$0,2$	$0,0767587$	$0,627465$
$0,3$	$0,0565781$	$0,66257$
$0,4$	$0,0420765$	$0,687778$
$0,5$	$0,0310697$	$0,706445$
$0,6$	$0,0223743$	$0,720576$
$0,7$	$0,0152913$	$0,731438$
$0,8$	$0,00938069$	$0,739883$
$0,9$	$0,00435065$	$0,746509$

Tabela 6.3: Maksymalne wartości dolnego ograniczenia na pojemność Q_2^{adpf} kanału tłumiącego amplitudę i zmieniającego fazę dla różnych wartości współczynników zmiany fazy η i współczynnika tłumienia $\gamma = 0,8$ oraz wartości parametru α^2, które im odpowiadają. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 16$.

η	Q_2^{adpf}	α^2
$0,1$	$0,0275969$	$0,697841$
$0,2$	$0,00938069$	$0,739883$
$0,3$	$0,002111468$	$0,784226$
$0,4$	$0,0001546$	$0,822914$

6.4 Dolne ograniczenie na pojemność Q_2 dla uogólnionego kanału tłumiącego amplitudę

Dolne ograniczenie na pojemność Q_2 dla uogólnionego kanału tłumiącego amplitudę wyznaczymy analogicznie jak dla kanału tłumiącego amplitudę. Tym razem Alicja przesyła po jednym qubicie z każdej z wielu par qubitów w stanie 6.1 przez uogólniony kanał tłumiący amplitudę, opisany operatorami Krausa postaci (porównaj 2.18-2.20)

$$E_0^{\mathsf{gad}} = \sqrt{1-\xi}\,|0\rangle\langle 0|_B + \sqrt{1-\gamma}\,|1\rangle\langle 1|_B \ , \tag{6.24}$$

$$E_1^{\mathsf{gad}} = \sqrt{\xi}\,|1\rangle\langle 0|_B \ , \tag{6.25}$$

$$E_2^{\mathsf{gad}} = \sqrt{\gamma}\,|0\rangle\langle 1|_B \ . \tag{6.26}$$

Postać pojedynczego stanu mieszanego otrzymamy z następującego wzoru

$$\begin{aligned}\rho_{AB} &= I\otimes E_0^{\mathsf{gad}}|\phi^+(\alpha')\rangle\langle\phi^+(\alpha')|_{AB}(I\otimes E_0^{\mathsf{gad}})^\dagger + \\ &+ I\otimes E_1^{\mathsf{gad}}|\phi^+(\alpha')\rangle\langle\phi^+(\alpha')|_{AB}(I\otimes E_1^{\mathsf{gad}})^\dagger + \\ &+ I\otimes E_2^{\mathsf{gad}}|\phi^+(\alpha')\rangle\langle\phi^+(\alpha')|_{AB}(I\otimes E_2^{\mathsf{gad}})^\dagger \ .\end{aligned} \tag{6.27}$$

Powyższy stan ma jawną postać

$$\begin{aligned}\rho_{AB} &= \alpha^2(1-\xi)\,|00\rangle\langle 00|_{AB} + (1-\alpha^2)(1-\gamma)\,|11\rangle\langle 11|_{AB} + \\ &+ \alpha\sqrt{1-\alpha^2}\sqrt{1-\gamma}\sqrt{1-\xi}(|00\rangle\langle 11|_{AB} + |11\rangle\langle 00|_{AB}) + \\ &+ \alpha^2\xi\,|01\rangle\langle 01|_{AB} + \\ &+ (1-\alpha^2)\gamma\,|10\rangle\langle 10|_{AB} \ .\end{aligned} \tag{6.28}$$

Po prostych przekształceniach otrzymujemy

$$\rho'_{AB} = p'|\phi^+(\alpha')\rangle\langle\phi^+(\alpha')|_{AB} + q'\,|01\rangle\langle 01|_{AB} + r'\,|10\rangle\langle 01|_{AB} \ , \tag{6.29}$$

gdzie

$$|\phi^+(\alpha')\rangle_{AB} = \alpha'\,|00\rangle_{AB} + \sqrt{1-(\alpha')^2}\,|11\rangle_{AB} \ , \tag{6.30}$$

$$\alpha' = \frac{\alpha\sqrt{1-\xi}}{\sqrt{1-(1-\alpha^2)\gamma-\alpha^2\xi}} \ , \tag{6.31}$$

$$p' = 1-(1-\alpha^2)\gamma-\alpha^2\xi \ , \tag{6.32}$$

$$q' = \alpha^2\xi \ , \tag{6.33}$$

$$r' = (1-\alpha^2)\gamma \ . \tag{6.34}$$

Ponieważ stan ten ma taką samą postać jak stan 5.1, wyrażenie na dolne ograniczenie na pojemność Q_2 dla uogólnionego kanału tłumiącego amplitudę otrzymamy ze wzorów

5.8, 5.13 i 5.17 przez podstawienie odpowiednich wartości wyznaczonych we wzorach 6.31 – 6.34. Mamy więc

$$\begin{aligned} Q_2^{\text{gad}} &\geqslant \sum_{k=0}^{2^m} p(2^m,k,\alpha^{'})\max\{I_c(\rho_{kAB}^{2^m}),0\} + \\ &+ \frac{1}{2^m}\sum_{i=2}^{m} 2^{i-1}(1-\sum_{k=0}^{2^{m-i+1}} p(2^{m-i+1},k,\alpha^{'})) \\ &\quad (\sum_{k=0}^{2^{m-i+1}} p(2^{m-i+1},k,\alpha^{'})\max\{I_c(\rho_{kAB}^{2^{m-i+1}}),0\}) \ , \end{aligned} \tag{6.35}$$

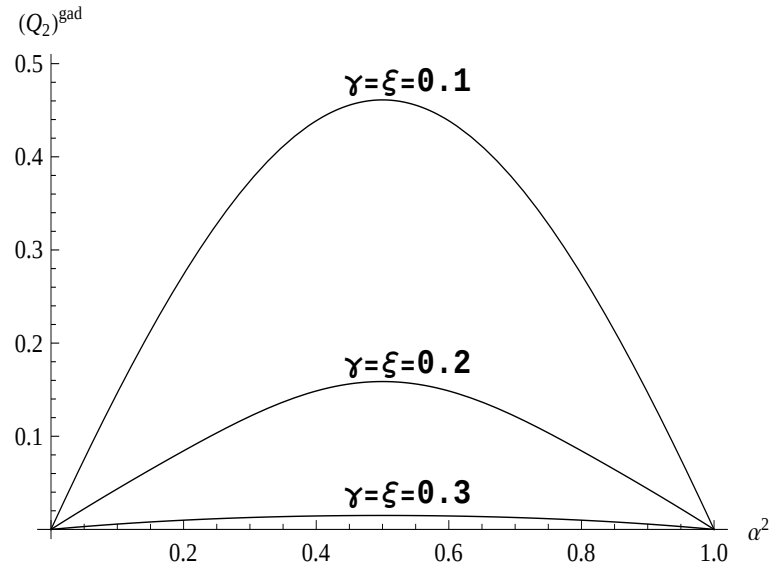
gdzie

$$\begin{aligned} p(n,k,\alpha^{'}) &= \sum_{j=0}^{j\leqslant\min\{k,n-k\}} \frac{n!}{(n-2j)!j!j!}|\alpha^{'}|^{2(n-k-j)}|\sqrt{1-(\alpha^{'})^2}|^{2(k-j)} \\ &\quad \binom{n-2j}{k-j}(p^{'})^{n-2j}(q^{'})^j(r^{'})^j \ , \end{aligned} \tag{6.36}$$

oraz

$$\begin{aligned} I_c(\rho_{kAB}^n) &= \log_2\binom{n}{k} + \\ &+ \sum_{j=0}^{\min\{k,n-k\}} \frac{n!}{(n-2j)!j!j!}\frac{1}{p(n,k,\alpha^{'})} \\ &\quad |\alpha^{'}|^{2(n-k-j)}|\sqrt{1-(\alpha^{'})^2}|^{2(k-j)}\binom{n-2j}{k-j}(p^{'})^{n-2j}(q^{'})^j(r^{'})^j \\ &\quad \log_2\left(\frac{1}{p(n,k,\alpha^{'})}|\alpha^{'}|^{2(n-k-j)}|\sqrt{1-(\alpha^{'})^2}|^{2(k-j)}\binom{n-2j}{k-j}(p^{'})^{n-2j}(q^{'})^j(r^{'})^j\right) . \end{aligned} \tag{6.37}$$

Na rysunku 6.4 przedstawiono zależność dolnego ograniczenia na pojemność Q_2^{gad} uogólnionego kanału tłumiącego amplitudę od parametru α^2 w przypadku, gdy współczynniki tłumienia γ i ξ są równe. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 32$. Z kolei w tabeli 6.4 podano maksymalne wartości tego ograniczenia i odpowiadające im wartości parametru α^2. Zauważmy, że dla wszystkich wartości współczynników tłumienia maksymalna wartość dolnego ograniczenia na pojemność Q_2^{gad} jest osiągana dla $\alpha^2 = \frac{1}{2}$, co odpowiada przygotowaniu przez Alicję stanów maksymalnie splątanych i przesłaniu po jednym qubicie z każdego stanu do Boba. Wynika to z faktu, że współczynniki tłumienia γ i ξ są równe i – co za tym idzie – stan $|0\rangle$ jest tak samo tłumiony jak stan $|1\rangle$. Dodajmy, że dla dużych wartości parametrów tłumienia można otrzymać większą wartość dolnego ograniczenia wykorzystując protokół rekurencyjny w połączeniu z protokołem haszującym.



Rysunek 6.4: Zależność dolnego ograniczenia na pojemność Q_2^{gad} uogólnionego kanału tłumiącego amplitudę od parametru α^2 dla różnych wartości współczynników tłumienia $\gamma = \xi$. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 32$.

Tabela 6.4: Maksymalne wartości dolnego ograniczenia na pojemność Q_2^{gad} uogólnionego kanału tłumiącego amplitudę dla różnych wartości współczynników tłumienia $\gamma = \xi$ oraz wartości parametru α^2, które im odpowiadają. Liczba kopii stanu ρ_{AB}, na których wykonywany jest pierwszy pomiar w protokole bisekcyjno-haszującym, wynosi $n = 32$.

$\gamma = \xi$	Q_2^{gad}	α^2
$0,1$	$0,461087$	$0,5$
$0,2$	$0,158738$	$0,5$
$0,3$	$0,0149814$	$0,5$

ROZDZIAŁ 7

Podsumowanie

W przedstawionej pracy doktorskiej zaprezentowano efektywny protokół destylacji splątania dla stanów mieszanych o niepełnym rzędzie macierzy gęstości. Praca składa się z pięciu głównych rozdziałów. W rozdziale 2 dokonano niezbędnego wprowadzenia do teorii kanałów i pojemności kwantowych, jak również opisano protokoły destylacji splątania, wykorzystywane w dalszych rozdziałach pracy. Zaprezentowano również pojęcia z teorii grup, które zostały zastosowane w rozdziale 4.

Rozdział 3 poświęcony został opisowi bisekcyjnego protokołu destylacji splątania, który zastosowano do stanu mieszanego składającego się ze stanu maksymalnie splątanego i stanu produktowego ortogonalnego do niego. Dodatkowo dla tego stanu rozszerzono zastosowanie protokołu na stany mieszane quditów oraz stany wielqubitowe. Pokazano również, że wydajność protokołu można poprawić poprzez połączenie protokołu bisekcyjnego z protokołem haszującym. W ostatnim podrozdziale tego rozdziału porównano wyniki protokołu bisekcyjno-haszującego z protokołem filtrująco-haszującym.

W rozdziale 4 pokazano, że bisekcyjny protokół destylacji w połączeniu z jednokierunkowym protokołem haszującym można zastosować do destylacji splątania z dwuqubitowego stanu mieszanego składającego się z dwóch stanów splątanych różniących się fazą i stanu produktowego ortogonalnego do nich. Warto nadmienić, że w celu znalezienia wzoru na wydajność protokołu destylacji dla tego stanu, wykorzystano metody teorii grup, a w szczególności metodę symetryzacji Younga i dekompozycji Schura-Weyla.

W rozdziale 5 przedstawiono kolejne zastosowanie bisekcyjno-haszującego protokołu, tym razem do destylacji splątania z dwucząstkowego stanu mieszanego, składającego się z czystego stanu splątanego i dwóch czystych stanów produktowych.

W rozdziale 6 otrzymane w poprzednich rozdziałach wyniki, wykorzystano do obliczenia dolnych ograniczeń na pojemność kwantową Q_2 dla następujących kanałów: kanału tłumiącego amplitudę, uogólnionego kanału tłumiącego amplitudę oraz dla kanału tłumiącego amplitudę i zmieniającego fazę.

Prawie wszystkie wyniki uzyskano w sposób analityczny. Pokazano również, że bisekcyjny lub bisekcyjno-haszujący protokół destylacji zastosowany do wcześniej wymienionych stanów, osiąga w szerokim zakresie parametrów większą wydajność niż ogólnie znane protokoły destylacji.

ROZDZIAŁ 8

Dodatek

8.1 Algebraiczne schematy asocjacji

W pracy [71] przedstawiono dwie alternatywne metody rozwiązania zagadnienia własnego dla stanu ρ_{kAB}^{n}. Pierwszą z nich jest metoda symetryzacji Younga i dekompozycji Schura–Weyla opisana szczegółowo w rozdziale 4, drugą jest metoda algebraicznych schematów asocjacji, której podstawowe zagadnienia zaprezentujemy w tym dodatku. Dowody lematów i twierdzeń można znaleźć w [79, 80].

Definicja 8.1 (Przemienne schematy asocjacji)**.** *Niech X będzie zbiorem mocy n a R_i, gdzie $i \in \{0, 1, \ldots, d\}$, będą podzbiorami $X \times X$ o własnościach:*

1. $R_0 = \{(x, x)\ , x \in X\}$.
2. $X \times X = \bigcup_{i=0}^{d} R_i$, *gdzie* $R_i \cap R_j = \varnothing$ *jeżeli* $i \neq j$.
3. $R_i^t = R_{i'}$ *dla pewnego* $i' \in \{0, 1, \ldots, d\}$, *gdzie* $R_i^t = \{(x, y) | (y, x) \in R_i\}$.
4. *Dla* $i, j, k \in \{0, 1, \ldots, d\}$, *liczba* $z \in X$, *taka że* $(x, z) \in R_i$ *i* $(z, y) \in R_j$ *jest stała jeżeli* $(x, y) \in R_k$. *Stałą tą oznaczymy* p_{ij}^{k}.
5. $p_{ij}^{k} = p_{ji}^{k}\ \forall i, j, k \in \{0, 1, \ldots, d\}$. *Konfigurację* $\Xi = (X, \{R_i\}_{i=0}^{d})$ *nazywamy przemiennymi schematem asocjacji (ang. commutative association scheme) klasy* d. *Nieujemne liczby* p_{ji}^{k} *nazywamy liczbami przecięcia.*

   Dodatkowo przemienne schematy asocjacji o własności

6. $R_i^t = R_i$,

nazywamy symetrycznymi przemiennymi schematami asocjacji.

Dla każdego z przemiennych schematów asocjacji można zdefiniować macierz sąsiedztwa.

Definicja 8.2 (Macierz sąsiedztwa). *k-tą macierzą sąsiedztwa A_k, gdzie $k \in \{0, 1, \ldots, d\}$ dla przemiennego schematu asocjacji $\Xi = (X, \{R_i\}_{i=0}^d)$ nazywamy macierz stopnia $|X| = n$, której wiersze i kolumny są oznaczone przez elementy X, a jej elementy są następujące*

$$(A_k)_{x,y} = \begin{cases} 1 & \text{jeżeli } (x,y) \in R_i \\ 0 & \text{jeżeli } (x,y) \notin R_i \end{cases} \tag{8.1}$$

Macierz sąsiedztwa jest więc macierzą o elementach 0 lub 1. Punkty od 1 do 5 w definicji 8.1 są równoważne następującym własnościom macierzy sąsiedztwa A_i, gdzie $i \in \{0, 1, \ldots, d\}$.

Lemat 8.1. *Niech $\Xi = (X, \{R_i\}_{i=0}^d)$, będzie przemiennym schematem asocjacji. Macierze A_i są dla niego macierzami sąsiedztwa, wtedy i tylko wtedy, gdy*

1. *$A_0 = I$, gdzie I jest macierzą identycznościową.*
2. *$\sum_{k=0}^{d} A_k = J$, gdzie J jest macierzą składającą się z samych jedynek.*
3. *$A_k^t = A_{k'}$ dla pewnego $k' \in \{0, 1, \ldots, d\}$.*
4. *$A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$ dla każdego $i, j, k \in \{0, 1, \ldots d\}$.*
5. *$p_{ij}^k = p_{ji}^k$ dla każdego $i, j, k \in \{0, 1, \ldots d\}$ wtedy i tylko wtedy, gdy $A_i A_j = A_j A_i$ dla każdego $i, j \in \{0, 1, \ldots d\}$.*

   Ponadto dla symetrycznego przemiennego schematu asocjacji mamy

6. *$A_k^t = A_k$ dla każdego $k \in \{0, 1, \ldots d\}$.*

Twierdzenie 8.1. *Niech $(X, \{R_i^X\}_{i=0}^d)$ będzie przemiennym schematem asocjacji. Dalej niech Y będzie zbiorem, na który bijekcja φ odwzorowuje zbiór X, $\varphi : X \to Y$. Wtedy para $(Y, \{R_i^Y\}_{i=0}^d)$, gdzie*

$$R_i^Y \in Y \times Y \ , \tag{8.2}$$

$$R_i^Y = \{(y, y') | (\varphi^{-1}(y), \varphi^{-1}(y')) \in R_i^X \equiv \Phi(R_i^X)\} \tag{8.3}$$

jest przemiennym schematem asocjacji, a jego macierze sąsiedztwa są równe macierzom sąsiedztwa przemiennego schematu asocjacji $(X, \{R_i\}_{i=0}^d)$.

Dowód. Para $(Y, \{R_i^Y\}_{i=0}^d)$ jest przemiennym schematem asocjacji, ponieważ zbiór Y i rodzina zbiorów $\{R_i^Y\}_{i=0}^d$ są odpowiednio bijekcyjnym obrazem X oraz $\{R_i^X\}_{i=0}^d$. Udowodnimy równość ich macierzy sąsiedztwa. Oznaczmy odpowiednio przez $\{A_i^X\}_{i=0}^d$ i $\{A_i^Y\}_{i=0}^d$ macierze sąsiedztwa przemiennych schematów asocjacji $(X, \{R_i^X\}_{i=0}^d)$ oraz $(Y, \{R_i^Y\}_{i=0}^d)$. Możemy napisać

$$\begin{aligned}
(A_i^Y)_{(y,y')} &= \begin{cases} 1 & \text{jeżeli } (y, y') \in R_i^Y \\ 0 & \text{jeżeli } (y, y') \notin R_i^Y \end{cases} \Leftrightarrow \\
&\Leftrightarrow \begin{cases} 1 & \text{jeżeli } (\varphi^{-1}(y), \varphi^{-1}(y')) \in R_i^X \\ 0 & \text{jeżeli } (\varphi^{-1}(y), \varphi^{-1}(y')) \notin R_i^X \end{cases} = \\
&= \begin{cases} 1 & \text{jeżeli } (x, x') \in R_i^X \\ 0 & \text{jeżeli } (x, x') \notin R_i^X \end{cases} = (A_i^X)_{x,x'} \ ,
\end{aligned} \tag{8.4}$$

gdzie $y = \varphi(x)$ i $y' = \varphi(x')$. Stąd otrzymujemy tezę naszego twierdzenia

$$(A_i^X)_{(x,x')} = (A_i^Y)_{(\varphi(x),\varphi(x'))} \ . \tag{8.5}$$

■

Zanim przejdziemy do przedstawienia najważniejszego dla nas przykładu przemiennego schematu asocjacji, musimy wprowadzić definicje symbolu Pochhammera i uogólnionej funkcji hypergeometrycznej.

Definicja 8.3 (Symbol Pochhammera)**.** *Symbol Pochhammera definiujemy następująco*

$$(x)_n = x(x+1)\cdots(x+n-1) \ . \tag{8.6}$$

Jako przykład podamy kilka początkowych wartości symbolu Pochhammera dla nieujemnego n

$$\begin{aligned}
(x)_0 &= 1 \\
(x)_1 &= x \\
(x)_2 &= x^2 + x \\
(x)_3 &= x^3 + 3x^2 + 2x \\
(x)_4 &= x^4 + 6x^3 + 11x^2 + 6x
\end{aligned} \tag{8.7}$$

Definicja 8.4 (Uogólniona funkcja hypergeometryczna)**.** *Uogólniona funkcja hypergeometryczna to nieskończony szereg, który możemy zapisać w następującej postaci*

$$\begin{aligned}
\sum_{k=0}^{\infty} c_k x^k &= {}_pF_q\left(\begin{matrix} a_1, & a_2, & \ldots, & a_p \\ b_1, & b_2, & \ldots, & b_q \end{matrix}; x\right) \\
&= \sum_{k=0}^{\infty} \frac{(a_1)_k, (a_2)_k, \ldots (a_p)_k}{(b_1)_k, (b_2)_k, \ldots (b_q)_k} \frac{x^k}{k!} \ ,
\end{aligned} \tag{8.8}$$

gdzie $(a)_k$ i $(b)_k$ są symbolami Pochhammera.

Lemat 8.2 (Schemat Johnsona)**.** *Niech V będzie zbiorem o mocy n i niech k będzie nieujemną liczbą całkowitą, taką, że $k \leqslant \frac{n}{2}$. Niech X^J będzie zbiorem k-elementowych podzbiorów zbioru V, takim, że $|X^J| = \binom{n}{k}$. Dalej zdefiniujmy*

$$R_l^J \;=\; \{(x,y)|x,y \in X^J, |x \cap y| = k-l\} \;, \tag{8.9}$$

gdzie $l = 0,1,2,\ldots k$. Wtedy para $\Xi^J = (X^J, \{R_i^J\}_{i=0}^k)$ jest przemiennym schematem asocjacji klasy k nazywanym schematem Johnsona.

Macierz sąsiedztwa dla schematu Johnsona A_l^J dla każdego $l \in \{0,1,\ldots,k\}$ ma następujące wartości własne

$$\alpha_l(j) \;=\; \sum_{r=0}^{l}(-1)^{l-r}\binom{k-r}{l-r}\binom{k-j}{l-r}\binom{n-k-j+r}{r} \equiv h_l(j) \;, \tag{8.10}$$

gdzie $j = 0,1,\ldots k$ identyfikuje odpowiednie przestrzenie własne A_l^J, natomiast $h_l(j)$ jest dualnym wielomianem Hahna, to znaczy

$$h_l(j) \;=\; (-1)^l\binom{k}{l}{}_3F_2\left(\begin{matrix} -l, & -k+j, & n-k-j+1 \\ -k, & 1, & \end{matrix}; 1\right) \;, \tag{8.11}$$

gdzie ${}_3F_2$ jest funkcją hypergeometryczną (porównaj definicja 8.4).

8.2 Wartości własne macierzy D_l^k z rozdziału 4

Twierdzenie 8.2 (Wartości własne macierzy D_l^k)**.** *Macierze D_l^k, są macierzami sąsiedztwa dla schematu Johnsona. Ich wartości własne wyrażają się wzorem 8.10*

Dowód. Oznaczmy zbiór wektorów ze standardowej bazy podprzestrzeni $\mathcal{H}_k^n$ przez $B(\mathcal{H}_k^n)$. Moc tego zbioru wynosi $|B(\mathcal{H}_k^n)| = \binom{n}{k}$. Wektory te oznaczymy przez $e_i \equiv e(i_1, i_2, \ldots, i_k)$, gdzie $i_1, i_2, \ldots, i_k \in \{1,2,\ldots n\}$ są indeksami jedynek w wektorze bazowym e_i. Stąd zbiór $\{1,2,\ldots,n\} - \{i_1, i_2, \ldots, i_k\}$ składa się z indeksów zer w tym wektorze.

Zauważmy z lematu 8.2, że elementy zbioru X^J, mogą być w naturalny sposób przedstawione w postaci $x\{i_1, i_2, \ldots, i_k\} \equiv x\{i\} \in X^J$, gdzie $i_1, i_2, \ldots, i_k$ oznaczają elementy ze zbioru $V = \{1,2,\ldots,n\}$, które zawierają się w podzbiorze $x\{i_1, i_2, \ldots, i_k\} \in X^J$ o mocy $|X^J| = \binom{n}{k}$. Wobec tego istnieje naturalna bijekcja $\varphi : X^J \to B(\mathcal{H}_k^n)$

$$\varphi(x\{i_1, i_2, \ldots, i_k\}) \;=\; e(i_1, i_2, \ldots, i_k) \;. \tag{8.12}$$

Z twierdzenia 8.1 otrzymujemy, że para $(B(\mathcal{H}_k^n), \{R_i^H\}_{i=0}^k)$, gdzie

$$R_i^H \;=\; \phi(R_i^J) \;, \tag{8.13}$$

jest przemiennym schematem asocjacji o tej samej macierzy sąsiedztwa jak schemat Johnsona. Podzbiory R_i^H zbioru $B(\mathcal{H}_k^n) \times B(\mathcal{H}_k^n)$ opiszemy poniższym lematem

Lemat 8.3.

$$R_l^H \;=\; \phi(R_l^J) = \{(e_i, e_j) \in B(\mathcal{H}_k^n) \times B(\mathcal{H}_k^n) | d(e_i, e_j) = 2l\} \;, \tag{8.14}$$

gdzie $l \in \{0, 1, \ldots k\}$.

Dowód. Jeżeli $(e_i, e_j) \in R_l^H$ wtedy dla

$$\begin{aligned} x &= \varphi^{-1}(e_i) \;, \\ y &= \varphi^{-1}(e_j) \;, \end{aligned} \tag{8.15}$$

gdzie $x, y \in X^J$ mamy, że $(x, y) \in R_l^J$ wtedy i tylko wtedy gdy $|x \cap y| = k - l$. Stąd k-elementowe zbiory x,y mają $k - l$ elementów wspólnych, to znaczy

$$x \;=\; \{i_1, i_2, \ldots i_k, z_1, z_2, \ldots z_{k-l}\} \;, \tag{8.16}$$

$$y \;=\; \{j_1, j_2, \ldots j_k, z_1, z_2, \ldots z_{k-l}\} \;, \tag{8.17}$$

gdzie

$$\{i_1, i_2, \ldots i_k\} \cap \{j_1, j_2, \ldots j_k\} \;=\; \varnothing \tag{8.18}$$

i

$$\begin{aligned} \varphi(x) &= e(i_1, i_2, \ldots i_k, z_1, z_2, \ldots z_{k-l}) \\ \varphi(y) &= e(j_1, j_2, \ldots j_k, z_1, z_2, \ldots z_{k-l}) \;. \end{aligned} \tag{8.19}$$

Z powyższego wnioskujemy, że dystans Hamminga pomiędzy wektorami $\varphi(x) = e_i$ oraz $\varphi(y) = e_j$ jest równy $2l$. ■

Z definicji 8.2 możemy wyciągnąć następujący wniosek.

Wniosek 8.1. *Dla każdego* $l = \{0, 1, \ldots, k\}$

$$(D_l^H)_{e_1, e_2} \;=\; \begin{cases} 1 & \textit{jeżeli } d(e_i, e_j) = 2l \\ 0 & \textit{jeżeli } d(e_i, e_j) \neq 2l \;. \end{cases} \tag{8.20}$$

Teraz dowód twierdzenia 8.2 wynika bezpośrednio z faktu, że

$$\rho_k^n \;=\; \frac{1}{2^n} \sum_{l=0}^{k} p^{2l} D_k^H = \frac{1}{2^n} \sum_{l=0}^{k} p^{2l} D_k^J \;, \tag{8.21}$$

oraz z wzorów 8.10 i 8.11. ■

Bibliografia

[1] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[5] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).

[6] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).

[7] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).

[8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[9] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[11] M. Horodecki, P. W. Shor, and M. B. Ruskai, Rev. Math. Phys. **15**, 629 (2003).

[12] M. Horodecki, P. Horodecki, and R. Horodecki, J. Mod. Opt. **47**, 347 (2000).

[13] I. Devetak and P. W. Shor, Comm. Math. Phys. **256**, 287 (2005).

[14] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).

[15] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).

[16] M. B. Hastings, Nature Physics **5**, 255 (2009).

[17] P. W. Shor, J. Math. Phys. **43**, 4334 (2002).

[18] C. King, IEEE Trans. Info. Theory **49**, 221 (2003).

[19] S. Lloyd, Phys. Rev. A, **55**, 1613 (1997).

[20] P. W. Shor, lecture notes, MSRI Workshop on Quantum Computation (2002), URL `http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/`.

[21] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).

[22] P. W. Shor and J. A. Smolin, arXiv:quant-ph/9604006 (1996).

[23] D. DiVincenzo, P. W. Shor, and J. A. Smolin, Phys. Rev. A **57**, 830 (1998).

[24] G. Smith and J. Yard, Science **321**, 1812 (2008).

[25] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[26] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A, **223**, 1 (1996).

[27] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).

[28] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inf. Theory **48**, 2637 (2002).

[29] C. H. Bennett, I. Devetak, P. Shor, and J. Smolin, Phys. Rev. Lett. **96**, 150502 (2006).

[30] C. H. Bennett, D. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett **78**, 3217 (1997).

[31] D. Leung, J. Lim, and P. Shor, Phys. Rev. Lett. **103**, 240505 (2009).

[32] N. Cai, A. Winter, and R. Yeung, Prob. Inf. Trans. **40**, 318 (2004).

[33] G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).

[34] G. Smith and J. A. Smolin, Phys. Rev. Lett. **102**, 010501 (2009).

[35] K. Li, A. Winter, X. Zou, and G. Guo, Phys. Rev. Lett. **103**, 120501 (2009).

[36] G. Smith and J. A. Smolin, Phys. Rev. Lett. **103**, 120503 (2009).

[37] M. B. Plenio and S. Virmani, Quantum Inf. Comp. **7**, 1 (2007).

[38] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[39] P. W. Shor, Comm. Math. Phys. **246**, 473 (2004).

[40] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[41] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[42] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[43] E. M. Rains, arXiv:quant-ph/9707002 (1997).

[44] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio, and M. Wilkens, Phys. Rev. Lett. **84**, 1611 (2000).

[45] Y.-X. Chen and D. Yang, arXiv:quant-ph/0204004v3 (2002).

[46] S. Hamieh and H. Zaraket, J. Phys. A: Math. Gen. **36**, L387 (2003).

[47] T. Hiroshima and M. Hayashi, Phys. Rev. A **70**, 030302 (2004).

[48] M. F. Cornelio, M. C. de Oliveira, and F. F. Fanchini, Phys. Rev. Lett. **107**, 020502 (2011).

[49] H. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).

[50] W. Dür, H. Briegel, J. I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999).

[51] W. Dür and H. Briegel, Phys. Rev. Lett. **90**, 067901 (2003).

[52] J. Dehaene, M. V. den Nest, B. D. Moor, and F. Verstraete, Phys. Rev. A **67**, 022310 (2003).

[53] E. N. Maneva and J. A. Smolin, Contemp. Math. Series **305**, 203 (2002).

[54] H. Bombin and M. A. Martin-Delgado, Phys. Rev. A **72**, 032313 (2005).

[55] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004).

[56] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).

[57] K. G. H. Vollbrecht and F. Verstraete, Phys. Rev. A **71**, 062325 (2005).

[58] E. Hostens, J. Dehaene, and B. D. Moor, Phys. Rev. A **73**, 062337 (2006).

[59] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[60] G. Alber, A. Delgado, N. Gisin, and I. Jex, quant-ph/0102035 (2001).

[61] Y. W. Cheong, S.-W. Lee, J. Lee, and H.-W. Lee, quant-ph/0512173 (2005).

[62] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, Phys. Rev. A **57**, 4075 (1998).

[63] W. Dür, H. Aschauer, and H.-J. Briegel, Phys. Rev. Lett. **91**, 107903 (2003).

[64] H. Aschauer, W. Dür, and H.-J. Briegel, Phys. Rev. A **71**, 012319 (2005).

[65] C. Kruszynska, A. Miyake, H.-J. Briegel, and W. Dür, Phys. Rev. A **74**, 052316 (2006).

[66] J. M. Renes, F. Dupuis, and R. Renner, arXiv:1109.3195v1 (2011).

[67] A. I. Kostrykin, *Wstęp do algebry* (Wydawnictwo Naukowe PWN, Warszawa, 2008).

[68] G. Banaszak and W. Gajda, *Elementy algebry liniowej cz.I* (Wydawnictwo Naukowo Techniczne, 2002).

[69] K. M. R. Audenaert, *A digest on representation theory of the symmetric group*, URL `http://www.personal.rhul.ac.uk/usah/080/QITNotes_files/Irreps_v06.pdf`.

[70] M. Czechlewski, A. Grudka, S. Ishizaka, and A. Wójcik, Phys. Rev. A **80**, 014303 (2009).

[71] M. Czechlewski, A. Grudka, M. Horodecki, M. Mozrzymas, and M. Studziński, J. Phys. A: Math. Theor. **45**, 125303 (2012).

[72] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[73] N. Gisin, Phys. Lett. A **210**, 151 (1996).

[74] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **78**, 574 (1997).

[75] F. Verstraete, J. Dehaene, and B. DeMoor, Phys. Rev. A **64**, 010101 (2001).

[76] N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **81**, 3279 (1998).

[77] A. Kent, Phys. Rev. Lett. **81**, 2839 (1998).

[78] M. Czechlewski, A. Grudka, and W. Kłobus (2011), wyniki nieopublikowane.

[79] E. Bannai and T. Ito, *Algebraic combinatorics I* (Benjamin/Cummings Publishing Company, 1984).

[80] Wolfram Math World, URL `http://mathworld.wolfram.com`.