On some communicational properties of quantum states

Autoreferat rozprawy doktorskiej

Łukasz Pankowski

wrzesień 2011

W rozprawie zawarto wyniki badań dotyczących użyteczności stanów dwu układów do następujących zadań komunikacyjnych z zakresu kwantowej informacji:

1. prywatna komunikacja
2. kwantowa komunikacja

Zadanie pierwsze wiąże się z możliwością destylacji klucza kryptograficznego, zadanie drugie z możliwością destylacji maksymalnie splątanych stanów. Jeżeli stan jest splątany, ale nie można z niego wydestylować maksymalnego splątania, mówimy że ma związane splątanie. W rozprawie badano wzajemne związki między powyższymi zadaniami oraz ich powiązanie z następującą matematyczną klasyfikacją stanów dwóch układów. Mianowicie każdy stan dwóch układów należy do jednego z dwóch zbiorów:

- zbioru stanów PPT czyli stanów o dodatniej częściowej transpozycji (ang. *Positive Partial Transpose*), wszystkie stany PPT są niedestylowalne, w szczególności do zbioru PPT należą stany separowalne; albo do
- zbioru stanów NPT czyli stanów o niedodatniej częściowej transpozycji (ang. *Nonpositive Partial Transpose*), jest wciąż otwartym problem czy wszystkie stany NPT są destylowalne czy też istnieją stany NPT niedestylowalne (tzw. stany NPT o związanym splątaniu).

W rozprawie skupiono się na dwóch problemach:

1. problem destylowalności prywatnego klucza ze splątanych stanów PPT (rozdział 3),
2. problem istnienia stanów NPT o związanym splątaniu (dwa podejścia zaprezentowano w rozdziałach 4 i 5).

1 Destylowalność klucza ze splątanych stanów PPT

Kwantowa kryptografia jest jednym z najszerzej rozpoznawanych praktycznych zastosowań kwantowej informacji. Komercyjne rozwiązania są sprzedawane np. przez ID Quantique[1] i MagiQ Technologies[2]. Szeroko w praktyce stosowaną częścią kwantowej kryptografii jest *Kwantowa Dystrybucja Klucza*. Kwantowa dystrybucja klucza nie wprowadza nowych kryptograficznych algorytmów, ale nowe protokoły dystrybucji prywatnego klucza. W praktycznej kryptografii wykorzystuje się algorytm z symetrycznym kluczem (np. 3DES) do szyfrowania przekazywanych danych, lecz ów klucz jest często zmieniany. Do przekazywania nowych kluczy używa się protokołów kryptograficznych z publicznym kluczem (np. RSA). Protokoły kwantowej dystrybucji klucza są w tym kontekście alternatywą dla protokołów z publicznym kluczem. Pierwsze hybrydowe systemy z wykorzystaniem kwantowej dystrybucji klucza zostały utworzone przy współpracy firm Senetas[3] i ID Quantique. Protokoły z publicznym kluczem opierają się na praktycznej niemożliwości rozwiązania trudnego (lub prawdopodobnie trudnego) problemu matematycznego (np. faktoryzacja), podczas gdy protokoły kwantowej dystrybucji klucza są oparte na fizycznej niemożliwości podsłuchiwania: próba podsłuchu prowadzi do wprowadzenia szumu, który może zostać wykryty przez komunikujące się strony (dzisiejsze implementacje kwantowej dystrybucji klucza nie są pozbawione pewnych problemów w tym względzie).

W 2003 roku, w pracy [1] pokazano, że ze stanów PPT o związanym splątaniu można uzyskiwać prywatny klucz. Wynik ten był wówczas dość zaskakujący, gdyż w tamtym czasie dowody bezpieczeństwa protokołów typu *przygotuj i zmierz* (podklasa protokołów kwantowej dystrybucji klucza) polegały na pokazaniu ich równoważności z destylacją stanów maksymalnie splątanych, co doprowadziło do przekonania, że bezpieczeństwo kwantowej kryptografii jest zawsze związane z destylacją stanów maksymalnie splątanych. Podejście do uzyskiwania klucza prywatnego ze stanów PPT przyjęte w [1] polega na przybliżaniu tzw. *prywatnego bitu* (zwanego w skrócie *pbitem*) stanem należącym do zbioru stanów PPT. Podejście to powodowało, że uzyskiwane stany PPT o destylowalnym kluczu były wysokowymiarowe.

W rozdziale 3 prezentujemy rezultaty opublikowane w [2, 3] gdzie użyto innego podejścia opartego o mieszanie ortogonalnych prywatnych bitów. To podejście pozwala na uzyskiwanie stanów PPT o destylowalnym kluczu nawet niskowymiarowych, począwszy od wymiaru $4 \otimes 4$. Rozważamy dwa przypadki

- *Mieszanie dwóch prywatnych bitów.* W tym przypadku podajemy ilość prywatnego klucza, który można wydestylować z mieszanki dwóch pbitów za pomocą protokołu Devetaka-Wintera [4]. Spośród mieszanek dwóch specjalnie dobranych pbitów wskazujemy splątane stany PPT.

- *Mieszanie czterech prywatnych bitów.* W tym przypadku podajemy czy

[1] http://www.idquantique.com/
[2] http://www.magiqtech.com/
[3] http://www.senetas.com/

z danej mieszanki czterech pbitów można uzyskać prywatny klucz za pomocą rekurencji i protokołu Devetaka-Wintera (jest to warunek dostateczny i ma on charakter egzystencjalny — nie podajemy ilości uzyskiwanego prywatnego klucza). Spośród mieszanek specjalnie dobranych czterech pbitów wskazujemy splątane stany PPT o destylowalnym kluczu znajdujące się dowolnie blisko zbioru stanów separowalnych.

Prywatny bit lub *pbit* to stan z którego Alicja i Bob mogą uzyskać bit prywatnego klucza przez bezpośredni pomiar tzw. części klucza: Alicja mierzy swój podukład klucza (oznaczany literą A) a Bob mierzy swój podukład klucza (oznaczany literą B) w wyniku czego uzyskują ten sam wynik, z równym prawdopodobieństwem uzyskiwany przez nich wynik jest zerem lub jedynką i uzyskany wynik pomiaru jest nieznany nikomu innemu poza Alicją i Bobem. Pbit w tak zwanej X-postaci jest dany przez

$$\gamma(X) = \frac{1}{2}\begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix} \tag{1}$$

gdzie X jest dowolnym operatorem spełniającym $\|X\| = 1$. Pbit ma cztery podukłady: $ABA'B'$ gdzie macierz blokowa (1) reprezentuje podukład AB a bloki tej macierzy są operatorami działającym na podukład $A'B'$. Podukłady A i B są podukładami jednokubitowych a wymiary podukładów A' i B' muszą być większe bądź równe 2, zakładamy że wymiary A' i B' są sobie równe i oznaczamy ich wymiar przez d. Podukład AA' należy do Alicji, a podukład BB' należy do Boba. Podukład AB nazywamy częścią klucza a podukład $A'B'$ tarczą (nazewnictwo to dotyczy również mieszanek pbitów rozważanych poniżej) Najniższy wymiar w których istnieje pbit to $4 \otimes 4$, tzn. wszystkie 4 podukłady są jednokubitowe.

W rozdziale 3 prezentujemy klasę $\mathcal{C}$ — zbiór stanów, mieszanek czterech odpowiednio dobranych ortogonalnych pbitów. Następnie dla klasy $\mathcal{C}$ podajemy warunki PPT, warunki destylowalności klucza i warunki separowalności. Posiadanie tych warunków pozwala nam zaprezentować stany PPT należące do klasy $\mathcal{C}$ z których można wydestylowalnym prywatny klucz a znajdujące się dowolnie blisko zbioru stanów separowalnych. Poniżej zamieszczam bardziej szczegółowy opis.

Mieszanie czterech pbitów Definiujemy klasę stanów $\mathcal{C}$ spełniającą trzy warunki:

1. Stan należący do klasy $\mathcal{C}$ jest mieszanką czterech pbitów

$$\varrho = \lambda_1\gamma_1^+ + \lambda_2\gamma_1^- + \lambda_3\gamma_2^+ + \lambda_4\gamma_2^- \tag{2}$$

gdzie prywatne bity są dane przez

$$\gamma_1^\pm = \gamma(\pm X) \qquad \gamma_2^\pm = \sigma_x^A\gamma(\pm Y)\sigma_x^A. \tag{3}$$

2. Między operatorami X i Y zachodzi relacja

$$Y = \frac{X^\Gamma}{\|X^\Gamma\|} \tag{4}$$

i, z definicji pbitu, są one unormowane, czyli $\|X\| = 1$ i $\|Y\| = 1$.

3. Operatory X i Y muszą być takie, że $\sqrt{XX^\dagger}$, $\sqrt{X^\dagger X}$, $\sqrt{YY^\dagger}$, $\sqrt{Y^\dagger Y}$ są operatorami PPT-inwariantnymi, tzn. muszą spełniać $A = A^\Gamma$.

Stany klasy $\mathcal{C}$ mają następującą postać blokową

$$\varrho = \frac{1}{2}\begin{bmatrix} (\lambda_1+\lambda_2)\sqrt{XX^\dagger} & \cdot & \cdot & (\lambda_1-\lambda_2)X \\ \cdot & (\lambda_3+\lambda_4)\sqrt{YY^\dagger} & (\lambda_3-\lambda_4)Y & \cdot \\ \cdot & (\lambda_3-\lambda_4)Y^\dagger & (\lambda_3+\lambda_4)\sqrt{Y^\dagger Y} & \cdot \\ (\lambda_1-\lambda_2)X^\dagger & \cdot & \cdot & (\lambda_1+\lambda_2)\sqrt{X^\dagger X} \end{bmatrix}. \tag{5}$$

Operator X W szczególności operator X użyty w definicji klasy $\mathcal{C}$ może mieć postać

$$X = \frac{1}{u}\sum_{i,j=0}^{d-1} u_{ij}|ij\rangle\langle ji| \tag{6}$$

gdzie u_{ij} są elementami jakiejś macierzy unitarnej zadanej na przestrzeni $\mathbb{C}^d$, a

$$u = \sum_{i,j=0}^{d-1} |u_{ij}|. \tag{7}$$

Alternatywna parametryzacja Zamiast parametrów λ_i można parametryzować klasę $\mathcal{C}$ za pomocą trzech parametrów p, α i β zadanych przez

$$p \equiv \lambda_1+\lambda_2 \in [0,1] \qquad \alpha \equiv \frac{\lambda_1-\lambda_2}{\lambda_1+\lambda_2} \in [-1,1] \qquad \beta \equiv \frac{\lambda_3-\lambda_4}{\lambda_3+\lambda_4} \in [-1,1]. \tag{8}$$

Warunki PPT Definicja klasy $\mathcal{C}$ pozwala na uzyskanie prostych warunków PPT. Jeżeli

$$|\lambda_1-\lambda_2| \leqslant (1-\lambda_1-\lambda_2)\|X^\Gamma\|^{-1} \tag{9}$$

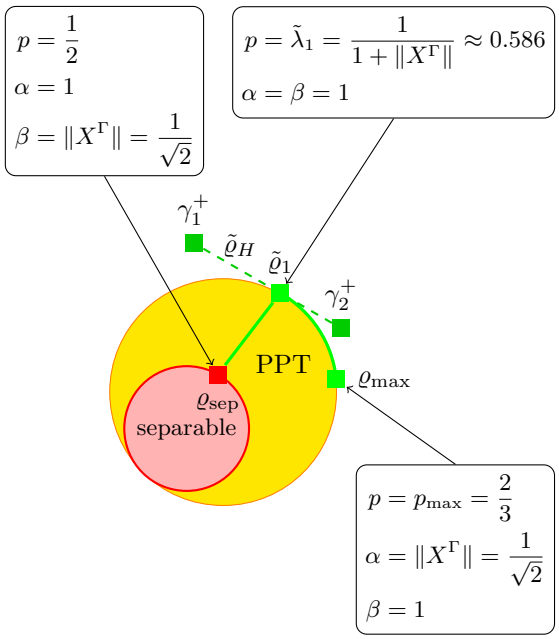
$$|\lambda_3-\lambda_4| \leqslant (\lambda_1+\lambda_2)\|X^\Gamma\| \tag{10}$$

to stan należący do klasy $\mathcal{C}$ jest stanem PPT.

Warunek destylowalności klucza Jeśli stan z klasy $\mathcal{C}$ spełnia warunek

$$(\lambda_1-\lambda_2)^2 > (\lambda_1+\lambda_2)(1-\lambda_1-\lambda_2). \tag{11}$$

to można z niego wydestylować prywatny klucz za pomocą pomiaru części klucza w bazie standardowej oraz zastosowania rekurencji i protokołu Devetaka-Wintera.



Rysunek 1: Klasa stanów PPT o destylowalnym kluczu (linia ciągła), ze stanów tej klasy można uzyskać prywatny klucz dowolnie blisko seporawalnego stanu ϱ_{sep}.

Warunki separowalności Jeśli stan z klasy $\mathcal{C}$ wymiaru $4 \otimes 4$ gdzie operator X zadany jest równaniem (6) spełnia warunki

$$\lambda_1 \leqslant \frac{1}{2} \tag{12}$$

$$\lambda_2 \leqslant \frac{1}{2} \tag{13}$$

$$|\lambda_3 - \lambda_4| \leqslant (\lambda_1 + \lambda_2)\|X^\Gamma\| \tag{14}$$

$$|\lambda_3 - \lambda_4| \leqslant (1 - \lambda_1 - \lambda_2)\|X^\Gamma\| \tag{15}$$

to jest stanem separowalnym.

Klucz ze stanów PPT dowolnie blisko stanów separowalnych Rozważmy podklasę stanów $\mathcal{C}$ wymiaru $4 \otimes 4$ gdzie operator X zadany jest równaniem (6). Jako macierz U w definicji operatora X bierzemy bramkę Hadamard.

Rysunek 1 ilustruje dwie podklasy

1. Klasę $\tilde{\varrho}_H$ reprezentowana przez linię kreskowaną będącą mieszanką dwóch pbitów γ_1^+ and γ_2^+. Większość stanów tej klasy to stany NPT za wyjątkiem jednego stanu $\tilde{\varrho}_1$, który jest stanem PPT.

2. Klasa reprezentowana przez linię ciągłą od ϱ_{sep} przez $\tilde{\varrho}_1$ do $\varrho_{\max}$. Jest to klasa stanów PPT i z każdego stanu tej klasy za wyjątkiem krańcowych ϱ_{sep}

i $\varrho_{\max}$[4] można wydestylować prywatny klucz. W szczególności do tej klasy należą stany PPT o destylowalnym kluczu leżące dowolnie blisko stanu ϱ_{sep}, a w związku z tym dowolnie blisko zbioru stanów separowalnych.

Stany tej klasy otrzymuje się wybierając parametr $p \in [\frac{1}{2}, p_{\max}]$ gdzie $p = \frac{1}{2}$ daje ϱ_{sep}, a $p_{\max} = (1 + \|X^\Gamma\|^2)^{-1} = \frac{2}{3}$ daje $\varrho_{\max}$. Parametry α i β ustalamy według wzorów

$$\alpha = \min(1, \alpha_1) \qquad \beta = \min(1, \alpha_1^{-1}) \tag{16}$$

gdzie

$$\alpha_1 = \frac{1-p}{p}\|X^\Gamma\|^{-1} = \frac{1-p}{p}\sqrt{2}. \tag{17}$$

Przedział $p \in [\frac{1}{2}, \tilde{\lambda}_1]$ gdzie $\tilde{\lambda}_1 = \frac{1}{1+\|X^\Gamma\|}$ jest reprezentowany przez odcinek od ϱ_{sep} do $\tilde{\varrho}_1$, a przedział $p \in [\tilde{\lambda}_1, p_{\max}]$ jest reprezentowany przez łuk od $\tilde{\varrho}_1$ do $\varrho_{\max}$.

Dostateczny warunek destylowalności klucza W rozdziale 3 dowodzimy dostateczny warunek destylowalności klucza z ogólnych stanów:

Proposition 1 *Dla dowolnego stanu*

$$\varrho = \begin{bmatrix} A & B & C & D \\ B^\dagger & E & F & G \\ C^\dagger & F^\dagger & H & I \\ D^\dagger & G^\dagger & I^\dagger & J \end{bmatrix} \tag{18}$$

jeśli

$$\max(\|D\|^2, \|F\|^2) > \frac{1}{4}(\|A\| + \|J\|)(\|E\| + \|H\|) \tag{19}$$

wówczas Alicja i Bob mogą z wielu kopii stanu ϱ wydestylować prywatny klucz stosując najpierw do części klucza stanu ϱ twirling $\Lambda'_{XX} \circ \Lambda_{ZZ}$ a następnie mierząc część klucza wielu kopii stanu ϱ i na koniec stosując do uzyskanych wyników pomiarów rekurencję i protokół Devetaka-Wintera.

Operacje twirlingu definiujemy jako

$$\Lambda'_{XX}(\varrho) = \frac{1}{2}(\varrho \otimes |0\rangle\langle 0| + \hat{\sigma}_x \otimes \hat{\sigma}_x(\varrho) \otimes |1\rangle\langle 1|) \tag{20}$$

$$\Lambda_{ZZ} = \frac{1}{2}(\hat{\mathrm{I}} \otimes \hat{\mathrm{I}} + \hat{\sigma}_z \otimes \hat{\sigma}_z) \tag{21}$$

gdzie $\hat{U}\varrho = U\varrho U^\dagger$, a σ_x i σ_z są macierzami Pauliego.

[4] W przypadku $\varrho_{\max}$ nie wiemy czy można z niego uzyskać klucz prywatny, wiemy tylko że nie można z niego uzyskać prywatnego klucza naszą metodą

W rozdziale 3 porównujemy również zastosowanie samego protokołu Devetaka-Wintera i protokołu Devetaka-Wintera z uprzednim zastosowaniem rekurencji w kontekście poziomu tolerowanego białego szumu (w tym porównaniu stosujemy mieszanki dwóch pbitów). Porównujemy również maksymalną entropię von Neumanna stanów PPT o destylowalnym kluczu będących mieszankami dwóch i czterech pbitów. Rozważamy też związek naszych wyników z destylowalnością splątania przez kanały typu *erasure*. Na koniec podajemy wystarczający warunek destylowalności klucza dla ogólnych stanów.

2 Destylacja stanów NPT Wernera za pomocą własności $\frac{1}{2}$

Problem istnienia stanów NPT o związanym splątaniu jest problemem otwartym od czasu publikacji [5]. Od czasu tej publikacji uzyskano wiele częściowych rezultatów. W szczególności pokazano, że wystarczy skupić się na klasie stanów Wernera, gdyż jeśli istnieją stany NPT o związanym splątaniu to istnieją również stany Wernera NPT o związanym splątaniu [6]. Formalnie stan ϱ jest n-destylowalny jeżeli n kopii stanu ϱ można lokalnie sprojektować by uzyskać dwu kubitowy stan NPT.

W rozdziale 4 prezentujemy rezultaty opublikowane w [7]. Koncentrujemy uwagę na stanie Wernera określonym na przestrzeni $4 \otimes 4$ i będącym najbardziej splątanym spośród tzw. *podejrzanych* (ang. *suspicious*) stanów Wernera. Oznaczmy ten stan przez ϱ_W. Przypuszcza się, że stan ϱ_W jest niedestylowalny [8, 9], dlatego rozważamy warunek na jego n-niedestylowalność (zamiast warunku na jego n-destylowalność). Tłumaczymy warunek n-niedestylowalności stanu ϱ_W na warunek nazywany własnością $\frac{1}{2}$ (ang. *half-property*) postaci

$$\sup_{\phi_2 \in \mathrm{SR}_2} \langle \phi_2 | Q_n | \phi_2 \rangle \leqslant \frac{1}{2}. \tag{22}$$

gdzie SR_2 to zbiór stanów o rzędzie Schmidta dwa, a Q_n jest pewnym projektorem którego postać zależy od n, w szczególności Q_2 ma postać

$$Q_2 = \Phi_+^\perp \otimes \Phi_+ + \Phi_+ \otimes \Phi_+^\perp. \tag{23}$$

gdzie

$$\Phi_+ = \sum_{i,j=0}^{d-1} |ii\rangle\langle jj| \qquad \Phi_+^\perp = \mathrm{I} - \Phi_+. \tag{24}$$

Stan ϱ_W jest n-niedestylowalny wtedy i tylko wtedy gdy własność $\frac{1}{2}$ jest dla n spełniona. Jeśli dla danego stanu ϕ_2 zachodzi $\langle \phi_2 | Q_n | \phi_2 \rangle \leqslant \frac{1}{2}$ wówczas mówimy, że stan ϕ_2 *ma* własność $\frac{1}{2}$.

Wiadomo, że ϱ_W jest 1-niedestylowalny. W pierwszej kolejności rozważamy problem jego 2-niedestylowalności. Nie rozwiązujemy problemu 2-niedestylowalności

ϱ_W, ale podajemy szerokie klasy stanów o rzędzie Schmidta dwa które mają własność $\frac{1}{2}$ dla $n = 2$. W szczególności tłumaczymy problem własności $\frac{1}{2}$ dla $n = 2$ na problem z zakresu analizy macierzowej:

Równoważny problem macierzowy Własność $\frac{1}{2}$ postaci (22) jest spełniona dla $n = 2$ jeśli dla każdego operatora X postaci

$$X = A \otimes \mathrm{I} + \mathrm{I} \otimes B \tag{25}$$

gdzie A i B są operatorami działającymi na przestrzeni $\mathbb{C}^4$ i spełniającymi

$$\mathrm{Tr}A = \mathrm{Tr}B = 0, \quad \mathrm{Tr}A^\dagger A + \mathrm{Tr}B^\dagger B = \frac{1}{d}. \tag{26}$$

suma dwóch największych wartości singularnych nie prakracza $1/2$

$$\sigma_1^2 + \sigma_2^2 \leqslant \frac{1}{2}. \tag{27}$$

W rozprawie rozwiązujemy ten problem dla macierzy normalnych, z czego wynika, że wszystkie stany o rzędzie Schmidta dwa izomorficzne z macierzami normalnymi (przez tzw. izomorfizm stanów i operatorów) mają własność $\frac{1}{2}$.

Warunek oparty o rzędy Schmidta Wykorzystujemy również tzw. *wspólne stopnie swobody* (ang. *common degrees of freedom*) by pokazać, że stan mający na każdej parze przynajmniej jeden podukład o jednokubitowym nośniku ma własność $\frac{1}{2}$:

Theorem 1 *Dowolny stan ϕ spełniający*

$$\begin{aligned} &\left(\mathrm{Sch}(A : A'BB') \leqslant \frac{d}{2} \vee \mathrm{Sch}(B : AA'B') \leqslant \frac{d}{2}\right) \\ \wedge\ &\left(\mathrm{Sch}(A' : ABB') \leqslant \frac{d}{2} \vee \mathrm{Sch}(B' : AA'B) \leqslant \frac{d}{2}\right) \end{aligned} \tag{28}$$

ma własność $\frac{1}{2}$. Wyrażenie $\mathrm{Sch}(X : Y)$ oznacza rząd Schmidta stanu ϕ w cięciu X versus Y.

Ogólne n Dla ogólnego n obliczamy maksymalne przekrycie stanów produktowych ϕ_1 z projektorem Q_n i podajemy postać stanów osiągających maksimum. Podajemy również ograniczenie na przekrycie $\langle\phi_2|Q_n|\phi_2\rangle$ w terminach przekrycia $\langle\phi_1|Q_n|\phi_1\rangle$. Niestety to ograniczenie w granicy $n \to \infty$ daje tylko trywialne ograniczenie, że przekrycie nie przekracza jedynki. Dla $n = 2$ podajemy również numeryczne ograniczenia lepsze niż $3/4$ (wynikające z $\langle\phi_1|Q_n|\phi_1\rangle$) i przypominamy analityczne ograniczenie $0.74971 < 3/4$ udowodnione w [7].

3 Destylacja za pomocą operacji rozszerzalnych

W rozdziale 5 rozważamy inne podejście do problemu istnienia stanów NPT o związanym splątaniu. Przypomnijmy, że stan jest destylowalny wtedy i tylko wtedy gdy Alicja i Bob mogą z wielu kopii tego stanu z pewnym prawdopodobieństwem uzyskać za pomocą lokalnych operacji i klasycznej komunikacji (LOKK) stan maksymalnie splątany. Aby udowodnić że stan jest niedestylowalny możemy pozwolić Alicji i Bobowi na użycie nadklasy operacji LOKK ułatwiającej rozważania matematyczne. Wówczas, jeśli dany stan jest niedestylowalny przy użyciu rozważanej nadklasy operacji LOKK to jest on również niedestylowalny przy użyciu operacji LOKK. W rozdziale 5 wykorzystujemy klasę operacji k-rozszerzalnych, które w granicy $k \to \infty$ dążą do operacji separowalnych. Można mieć nadzieję, że korzystając z operacji k-rozszerzalnych uda się udowodnić niedestylowalność niektórych z pośród *podejrzanych* stanów Wernera.

Najpierw dla zadanego stanu ϱ rozważamy supremum wierności $\Lambda(\varrho)$ ze stanem maksymalnie splątanym, gdzie supremum jest po wszystkich k-rozszerzalnych operacjach Λ. Oznaczmy to supremum przez $F_k(\varrho)$. Następnie pokazujemy związek wartości supremum $F_k(\varrho)$ z dodatniością pewnej macierzy. Wprowadzamy również podklasę operacji k-rozszerzalnych zwaną operacjami „zmierz-i-przygotuj" (ang. *measure-and-prepare*) i pokazujemy związek supremum po tej klasie z dodatniością pewnej macierzy o mniejszym wymiarze, ale parametryzowanej k parametrami.

Pokazujemy, że — chociaż operacje k-rozszerzalne w pewnym sensie zmierzają do operacji separowalnych dla dużych wartości k — to mają one nadspodziewaną siłę. Przede wszystkim dla dowolnego ustalonego k za pomocą klasy operacji k-rozszerzalnych każdy stan, za wyjątkiem maksymalnie zmieszanego, może zostać wydestylowany jeśli dana jest odpowiednio duża liczba kopii. Po drugie nawet jeśli dysponujemy pojedynczą kopią stanu operacje k-rozszerzalne mogą wydestylować z wiernością 1 każdy stan, który ma $(k-1)$-rozszerzalny stan w jądrze. W szczególności k-rozszerzalne operacje nie są stabilne ze względu na zanurzenie w większej przestrzeni Hilberta.

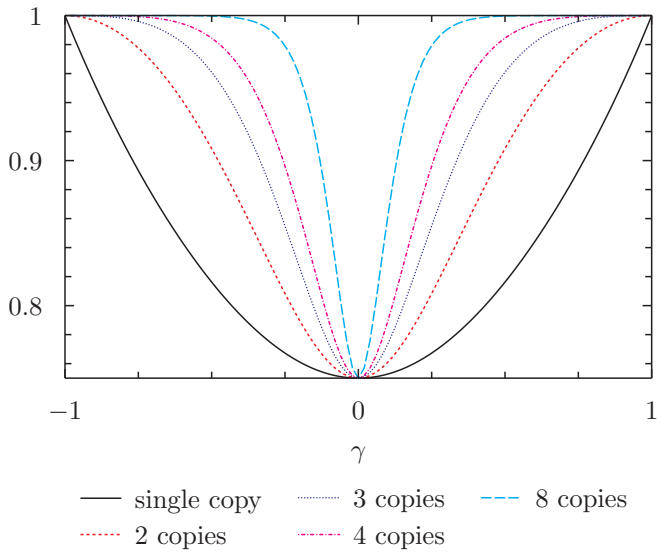
Dla stanów Wernera uzyskujemy analityczny wzór na $F_1(\varrho_W)$ postaci

$$F_1(\varrho_W(\gamma)) = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+2\gamma^2}{4-\gamma^2}} \tag{29}$$

gdzie wykorzystujemy parametryzacje stanów Wernera postaci (pomijamy nieistotną w naszym kontekście normalizację)

$$\varrho_W(\gamma) \sim \mathrm{I} - \gamma V. \tag{30}$$

Wzór (29) uzyskujemy przy użyciu ortogonalnej bazy liniowej przestrzeni operatorów komutujących z operacjami unitarnymi postaci $U \otimes U \otimes U$ zaprezentowanej w [10]. Analogicznie uzyskujemy analityczny wzór dla podklasy zmierz-i-przygotuj klasy operacji 1-rozszerzalnych, który w tym przypadku jest identyczny ze wzorem dla wszystkich operacji 1-rozszerzalnych, czyli jest równy $F_1(\varrho_W)$.



Rysunek 2: Wierność uzyskiwana przy pomocy operacji 1-rozszerzalnych ze stanów Wernera. Rysunek dobrze ilustruje, że przy dostatecznie dużej ilości kopii każdy stan za wyjątkiem maksymalnie zmieszanego można wydestylować z wiernością dowolnie bliską jedności.

W końcu, korzystając z obliczeń numerycznych, uzyskujemy wykresy $F_1(\varrho_W^{\otimes n})$ dla pewnych ilości rozszerzeń k i ilości kopii n. W przypadku $k = 1$ używamy nadmienionej bazy z [10] co pozwala nam dojść aż do $n = 8$ (rysunek 2). Dla $k > 1$ używamy bezpośrednich obliczeń numerycznych, choć wysoce zoptymalizowanych.

4 Publikacje i współpraca

Rozprawa doktorska bazuje na przytoczonych poniżej publikacjach przygotowanych we współpracy z Michałem Horodeckim, Pawłem Horodeckim oraz z Karolem Horodeckim, Marco Piani, Fernando G.S.L. Brandão i Graeme Smith.

Prace dotyczące problemu destylowalności prywatnego klucza ze splątanych stanów PPT [2, 3]:

- Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki, "Low-dimensional bound entanglement with one-way distillable cryptographic key", IEEE Trans. Inf. Theory **54**, 2621–2625 (2008), arXiv:quant-ph/0506203

- Łukasz Pankowski and Michał Horodecki, "Low-dimensional quite noisy bound entanglement with cryptographic key", J. Phys. A: Math. Theor. **44**, 035301 (2011), arXiv:1008.1226 [quant-ph]

Prace dotyczące problemu istnienia stanów NPT o związanym splątaniu [7, 11]:

- Łukasz Pankowski, Marco Piani, Michał Horodecki, and Paweł Horodecki, "A few steps more towards NPT bound entanglement", IEEE Trans. Inf. Theory **56**, 4085–4100 (2010), arXiv:0711.2613 [quant-ph]

- Łukasz Pankowski, Fernando Guadalupe Santos Lins Brandão, Michał Horodecki, and Graeme Smith, "Entanglement distillation by means of k-extendible maps", arXiv:1109.1779 [quant-ph]

Literatura

[1] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim, "Secure key from bound entanglement," Phys. Rev. Lett. **94**, 160502 (2005), arXiv:quant-ph/0309110

[2] Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki, "Low dimensional bound entanglement with one-way distillable cryptographic key," IEEE Trans. Inf. Theory **54**, 2621–2625 (2008), arXiv:quant-ph/0506203

[3] Łukasz Pankowski and Michał Horodecki, "Low-dimensional quite noisy bound entanglement with cryptographic key," J. Phys. A: Math. Theor. **44**, 035301 (2011), arXiv:1008.1226 [quant-ph]

[4] Igor Devetak and Andreas Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. Lond. A **461**, 207–235 (2005), arXiv:quant-ph/0306078

[5] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, "Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?." Phys. Rev. Lett. **80**, 5239–5242 (1998), arXiv:quant-ph/9801069

[6] M. Horodecki and P. Horodecki, "Reduction criterion of separability and limits for a class of distillation protocols," Phys. Rev. A **59**, 4206–4216 (1999), arXiv:quant-ph/9708015

[7] Łukasz Pankowski, Marco Piani, Michał Horodecki, and Paweł Horodecki, "A few steps more towards NPT bound entanglement," IEEE Trans. Inf. Theory **56**, 4085–4100 (2010), arXiv:0711.2613 [quant-ph]

[8] David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and Ashish V. Thapliyal, "Evidence for bound entangled states with negative partial transpose," Phys. Rev. A **61**, 062312 (2000), arXiv:quant-ph/9910026

[9] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß, "Distillability and partial transposition in bipartite systems," Phys. Rev. A **61**, 062313 (2000), arXiv:quant-ph/9910022

[10] T. Eggeling and R. F. Werner, "Separability properties of tripartite states with $U \otimes U \otimes U$ symmetry," Phys. Rev. A **63**, 042111 (2001)

[11] Łukasz Pankowski, Fernando Guadalupe Santos Lins Brandão, Michał Horodecki, and Graeme Smith, "Entanglement distillation by means of k-extendible maps," arXiv:1109.1779 [quant-ph]