University of Warsaw
Faculty of Mathematics, Informatics and Mechanics

Łukasz Pankowski

On some communicational properties of quantum states

PhD dissertation

Supervisor
dr hab. Michał Horodecki, prof. UG

Institute od Theorethical Physics and Astrophysics
University of Gdańsk

September 2011

Author's declaration:
aware of legal responsibility I hereby declare that I have written this dissertation myself and all the contents of the dissertation have been obtained by legal means.

September 19, 2011 ....
date *Łukasz Pankowski*

Supervisor's declaration:
the dissertation is ready to be reviewed

September 19, 2011 ....
date *dr hab. Michał Horodecki, prof. UG*

Contents

O pewnych komunikacyjnych własnościach stanów kwantowych

Słowa kluczowe: kwantowe splątanie, destylacja splątania, kwantowa kryptografia, stany bezpieczne, klucz destylowalny, stany o związanym splątaniu

Matematyczna Klasyfikacja Dziedzin AMS 2000:
81P68 Kwantowe obliczenia i kwantowa kryptografia

Matematyczna Klasyfikacja Dziedzin AMS 2010:
81P94 Kwantowa kryptografia
81P45 Kwantowa informacja, komunikacja, sieci

W niniejszej rozprawie rozważamy dwa kwantowe problemy komunikacyjne: problem istnienia stanów NPT[1] o związanym splątaniu i problem destylowalności prywatnego (kryptograficznego) klucza ze splątanych stanów PPT.

Destylowalność klucza ze splątanych stanów PPT 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. A spośród mieszanek dwóch specjalnie dobranych pbitów wskazujemy splątane stany PPT.

- *Mieszanie czterech prywatnych bitów.* W tym przypadku podajemy czy 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). A spośród mieszanek specjalnie dobranych

[1] Stan PPT to stan o dodatniej częściowej transpozycji, a stan NPT to stan o niedodatniej częściowej transpozycji.

czterech pbitów wskazujemy splątane stany PPT o destylowalnym kluczu znajdujące się dowolnie blisko zbioru stanów separowalnych.

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). A także porównujemy maksymalną entropię von Neumanna stanów PPT o destylowalnym kluczu będących mieszankami dwóch i czterech pbitów. Rozważamy również związek naszych wyników z destylowalnością splątania przez kanały typu *erasure*. Na koniec podajemy wystarczający warunek destylowalności klucza dla ogólnych stanów.

Destylacja stanów NPT Wernera za pomocą własności $\frac{1}{2}$ Problem istnienia stanów NPT o związanym splątaniu jest problemem otwartym od czasu publikacji [4]. 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 [5]. 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 [6]. 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 [7, 8], 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*): stan ϱ_W jest n-niedestylowalny wtedy i tylko wtedy gdy własność $\frac{1}{2}$ jest dla n spełniona. Stan ϱ_W spełnia własność $\frac{1}{2}$ dla zadanego n jeśli przekrycie wszystkich stanów ϕ_2 o rzędzie Schmidta dwa z pewnym operatorem Q_n nie przekracza $\frac{1}{2}$, innymi słowy dla wszystkich stanów ϕ_2 o rzędzie Schmidta dwa $\langle\phi_2|Q_n|\phi_2\rangle \leq \frac{1}{2}$. Jeśli dla danego stanu ϕ_2 zachodzi $\langle\phi_2|Q_n|\phi_2\rangle \leq \frac{1}{2}$ 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 i rozwiązujemy go dla macierzy normalnych. Z tego wynika, że wszystkie stany o rzędzie Schmidta dwa izomorficzne z macierzami normalnymi (przez tzw. izomorfizm stanów i operatorów) mają własność $\frac{1}{2}$. 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 $\frac{1}{2}$.

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 [6].

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 $F_1(\varrho_W)$ przy użyciu ortogonalnej bazy liniowej przestrzeni operatorów komutujących z operacjami unitarnymi postaci $U \otimes U \otimes U$ zaprezentowanej w [9]. 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 $F_1(\varrho_W)$.

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 ortogonalnej bazy liniowej przestrzeni operatorów komutujących z unitarnymi operacjami postaci $U \otimes U \otimes U$ zaprezentowanej w [9] co pozwala nam dojść aż do

$n = 8$. Dla $k > 1$ używamy bezpośrednich obliczeń numerycznych, choć wysoce zoptymalizowanych.

On some communicational properties of quantum states

Keywords: quantum entanglement, distillation of entanglement, quantum cryptography, private states, distillable key, bound entangled states

AMS Mathematical Subject Classification 2000:
81P68 Quantum computation and quantum cryptography

AMS Mathematical Subject Classification 2010:
81P94 Quantum cryptography
81P45 Quantum information, communication, networks

In the thesis two quantum communicational problems are investigated: the problem of the existence of NPT[2] bound entangled states and the problem of key-distillability of PPT entangled states.

Key-distillability of PPT entangled states In [1] it was shown that one can obtain private key from bound entangled PPT states. This was quite surprising as in that time security proofs of prepare and measure protocols (a sublass of quantum key distribution protocols) had been based on showing equivalence to the distillation of maximally entangled states which have led to the belief that security of the quantum cryptography is always connected to the distillation of the maximally entangled states. The approach taken in [1] to obtaining the private key from PPT states is to approximate private bit with a PPT state. This resulted in key-distillable PPT states only in large dimensions.

In chapter 3 we present results published in [2, 3] where another approach based on mixing orthogonal private bits is used. This approach allows for key-distillable PPT states even in low dimensions starting from $4 \otimes 4$. Two cases are considered:

- *Mixing of two private bits.* In this case the rate of distillation of the private key from a given state using Devetak-Winter protocol is presented. And among the key-distillable mixtures of two specially chosen private bits we obtain PPT entangled states.

- *Mixing of four private bits.* In this case the key distillability of mixtures of private bits by Devetak-Winter protocol with recurrence preprocessing is considered (we provide a sufficient condition and the condition is extensional: we do not provide key rate). And among the mixtures of four specially chosen private bits we present PPT entangled states arbitrary close to the set of the separable states.

[2] PPT state stands for a state which has positive partial transpose. NPT state is a state with non-positive partial transpose.

Also Devetak-Winter protocol with and without recurrence preprocessing are compared in the context of tolerable white noise in the case of mixing two private bits. Moreover maximal von Neumann entropy is compared between key-distillable PPT states being mixtures of two and four private bits. We also consider links of our research with distillability via erasure channel. Finally, we provide a sufficient condition for key-distillability for general states.

Distillation of NPT Werner state by half-property The problem of existence of bound entangled NPT states is open since the publication of [4]. Since that paper many partial results have been obtained. In particular it was shown that it is enough to concentrate on the class of the Werner states as if there exist NPT bound entangled states then there exist NPT bound entangled Werner states [5]. Formally, a state ϱ is *n-copy distillable* if n copies of ϱ can be locally projected to obtain a two-qubit NPT state.

In chapter 4 we present results published in [6]. We concentrate on a particular $4 \otimes 4$ Werner state which is the most entangled of the so-called *suspicious* Werner states. Let us denote this state with ϱ_W. The state ϱ_W is conjectured to be undistillable [7, 8] so we consider the condition for its n-undistillability (instead of the condition for its n-distillability). We translate n-undistillability of ϱ_W to a condition called the *half-property.* That is ϱ_W is n-undistillable if and only if the *half-property* for n is satisfied. The state ϱ_W satisfies the half-property for a given n if the overlap of all the Schmidt rank two states ϕ_2 with some projector Q_n does not exceed 1/2. If for a given ϕ_2 the overlap $\langle\phi_2|Q_n|\phi_2\rangle \leq \frac{1}{2}$ then ϕ_2 is said to *have* the half-property.

It is known that ϱ_W is 1-undistillable. We first consider the problem of its 2-undistillability. We do not solve the problem of 2-undistillability of ϱ_W but provide wide classes of Schmidt rank two states having the half-property for $n = 2$. In particular, we translate the problem of the half-property for $n = 2$ into a matrix analysis problem which we solve for normal matrices. This implies that all Schmidt rank two states isomorphic to normal matrices (trough so-called state-operator isomorphism) have the half-property. Also using the notion of so-called *common degrees of freedom* we show that any state having on each pair at least one subsystem with one qubit support has the half-property.

For general n, we compute maximal overlap of product states ϕ_1 with the projector Q_n and provide the form of ϕ_1 states attaining the maximum. We also present a bound on the overlap $\langle\phi_2|Q_n|\phi_2\rangle$ in terms of the overlap $\langle\phi_1|Q_n|\phi_1\rangle$. Unfortunately, this bound in the limit of $n \to \infty$ gives the trivial bound that the overlap does not exceed one. For $n = 2$ we provide numerical bounds better than 3/4 (which comes from $\langle\phi_1|Q_2|\phi_1\rangle$) and recall the analytical bound of $0.74971 < 3/4$ proven in [6].

Distillation using extendible maps In chapter 5 we consider another approach to the problem of existence of bound entangled NPT states. Let us recall that a state is distillable if and only if Alice and Bob may from many copies of the state with some probability obtain using local operations and classical

communication (LOCC) a maximally entangled state. To prove that a state is undistillable we can allow Alice and Bob to use a superclass of LOCC which is easier in mathematical consideration. Now, if the state is undistillable using the operations of the superclass then it is also undistillable using LOCC. We use the class of k-extendible maps which in the limit of $k \to \infty$ tend to the set of separable maps. One may hope that using k-extendible maps some *suspicious* Werner states may be proven undistillable.

First, for a given state ϱ we consider the supremum of the fidelity of $\Lambda(\varrho)$ with a maximally entangled state where the supremum is taken over all k-extendible maps Λ. Let us denote this supremum with $F_k(\varrho)$. We connect the value of the supremum $F_k(\varrho)$ to positivity of some matrix. We also introduce a subclass of k-extendible maps called 'measure-and-prepare' maps and connect supremum over this class to positivity of some (lower dimensional) matrix but parametrized with k parameters.

We show that, although k-extendible maps in a sense converge to the class of separable maps for large k, they are surprisingly powerful. First of all, for any fixed k, the class of k-extendible maps can distill any state but maximally mixed one, if large enough number of copies is available. Second, even in single copy, the maps can provide fidelity 1 (with some nonzero probability) for any state which has a $(k-1)$-extendible state in its kernel. In particular, k-extendible maps are not stable under local embedding into a larger Hilbert space.

For the Werner states we obtain the analytical formula for $F_1(\varrho_W)$ using the orthogonal basis in the linear space of operators that commute with unitary operators of the form $U \otimes U \otimes U$ given in [9]. Analogously, we obtain the analytical formula for the subclass of 1-extendible 'measure-and-prepare' maps which happens to be identical to the formula for all 1-extendible maps, i.e., to $F_1(\varrho_W)$.

At the end, we use numerical computations to obtain plots of $F_k(\varrho_W^{\otimes n})$ for some values of the number of extensions k and the number of copies n. In case of $k = 1$ using the above basis from [9] allows us to go with the number of copies up to $n = 8$. For $k > 1$ direct computation (but highly optimized) was used.

Acknowledgments

I want to thank my supervisor Michał Horodecki for his encouragement and support without which this thesis would not be possible.

The biggest thanks are to my parents Elżbieta and Leszek who gave me my life and lots of their love. I want to thank my friends Karol, Sebastian, Darek and my brother Daniel.

I also want to thank all of the people I had a pleasure to work with during my research in quantum information: Michał Horodecki, Paweł Horodecki, Barbara Synak-Radtke, Fernando G.S.L. Brandão, Andrzej Grudka, Karol Horodecki, Ryszard Horodecki, Marco Piani.

The work is supported by Polish Ministry of Science and Higher Education grant no. 3582/B/H03/2009/36 and by the European Commission through the Integrated Project FET/QIPC QESSENCE. This work was done in National Quantum Information Centre of Gdańsk.

Chapter 1

Introduction

Entanglement — the correlations between (possibly distant) subsystems of a quantum system which does not have any analog in our every-day macroscopic world — is a source of many puzzles since its discovery [10, 11] in 1935. Indeed, entanglement seemed so peculiar to Einstein, Podolsky and Rosen that they suggested that one can explain the results of measurements by some hidden variable model. I.e., they suggested that the results of the measurements come from some unknown to us properties (so-called hidden variables) if we knew those hidden variables then we would have known the results of the measurements. In this consideration they used an entangled state.

On the contrary, in 1964 John Bell proposed [12] an inequality that must be satisfied if the hidden variable model is an adequate description of quantum mechanics. He showed that the measurements obtained from entangled states may violate this inequality hence the hidden variable model is not an adequate description of quantum mechanics. This theoretical result has been later confirmed in an experiment [13] to finally eliminate the opposite resolution of the Bell inequality which would state that hidden variable model is correct but quantum mechanical model is wrong.

In 1991 Nicolas Gisin published a short note [14] showing that every entangled pure state violates some Bell inequality. But a harder puzzle have been unsolved: what is the situation for the more general mixed states (represented by density matrices)? In 1989 Reinhard Werner introduced a class of mixed entangled states [15] — now commonly called *Werner states* — which are entangled but results of thier direct measurements can be explained by hidden variable model which he explicitly stated therein (this is never the case for entangled pure states as shown by Gisin). Later, in 1995 Sandu Popescu showed [16] for a subclass of the Werner states that although they are not violating any of the Bell inequalities when subjected to a direct measurement they could be preprocessed to do so. Namely, using a local filter and classical communication one can, with some probability, obtain from them highly entangled states which violate the CHSH [17] Bell inequality to a large degree. This is a simple example of *distillation of entanglement.* In the following year 1996, a protocol for distillation of entanglement from two-qubit states have been proposed [18]. The protocol can distill nearly perfect singlets (maximally entangled states) from many copies of a two-qubit state if its overlap with singlet is greater than $\frac{1}{2}$.

The importance of distillation of entanglement comes from two directions:

1. on one hand from the tasks, such as teleportation of an unknown state [19] which can be performed if two parties share maximally entangled states (a universal and powerful resource); and

2. on the other hand from the uncontrolled interaction with environment which may weaken the entanglement of the states shared by the parties (a destructive power of noise).

So the important question is: whether all entangled mixed states are distillable? For a pure states, a positive answer was obtained in 1996 by Charles Bennett *et al.* [20]. In 1997 Horodeckis [21] obtained a positive answer for the special case of two-qubit states: all entangled two-qubit states are distillable. But, in 1998 they have shown [4] that for the general case the answer is: no. They showed that an entangled state to be distillable must violate *Peres criterion* (a necessary condition for a mixed state to be separable — i.e., not entangled [15] — introduced in 1996 by Asher Peres [22]) and on the other hand they have recalled examples of entangled states satisfying Peres criterion introduced a year before by Paweł Horodecki [23]. This way they showed that there are entangled states which are undistillable and they called them *bound entangled states*, in analogy to the bound energy from thermodynamics.

The states which satisfy the Peres criterion are now called the PPT states (for *Positive Partial Transpose*) and the states which violate the Peres criterion are now called the NPT states (for *Non-positive Partial Transpose*). In [4] examples of PPT bound entangled states are given and the question is stated, which remains still open: are all NPT states distillable (which would give *partial transpose* as the simple mathematical tool to decide if a state is distillable) or is it that there are also NPT bound entangled states?

Quantum teleportation together with distillation of entanglement allow two distant parties to reliably transmit quantum states (unknown to the sender) even if they initially shared noisy entangled states and they are not connected with a quantum channel. But there is another extremely practical communicational task that is allowed and secured by quantum mechanics: *quantum cryptography.*

Quantum cryptography, pioneered by Wiesner [24] (published in 1983), allows distant parties to obtain cryptographic key (we will also call it private key) based on physical impossibility of eavesdropping. Namely, if the transmitted signal is encoded into quantum states, then by reading it, eavesdropper always introduces noise into the signal. Thus Alice and Bob — the parties who want to communicate privately — can measure the level of noise and detect whether their transmission is secure (even if the noise was solely due to eavesdropping). There are two types of quantum key distribution protocols: *prepare and measure* (as the original BB84 protocol [25] published by Bennett and Brassard in 1984) and protocols based on a shared entangled state (originated from the Ekert's protocol [26] introduced in 1991). For quite a time security proofs of prepare and measure protocols had been based on showing equivalence to the distillation (by local operations and classical communication) of maximally entangled states (the first such proof is due to Shor and Preskill [27], published in 2000). It have led to the belief that security of the quantum cryptography is always connected to the distillation of the maximally entangled states (this issue was perhaps first touched by Gisin and Wolf [28] in 2000).

This belief suggested that one could not obtain secure key from bound entangled states [4], i.e., states from which maximally entangled states cannot be distilled. On the contrary, the key-distillable bound entangled states have been found [1] and examples of low dimensional states have been provided [2]. The multipartite case was also considered [29]. There are two approaches to obtaining cryptographic key from bound entangled PPT states: one is based on approximating private bit with a PPT state [1, 30] and the other one — on mixing orthogonal private bits [2, 3].

Distillation of cryptographic key from quantum states may be seen as a generalization of the problem of distillation of entanglement. Indeed, distillation of entanglement is a process in which Alice and Bob obtain singlets which are examples of private bits. While, distillation of cryptographic key is a process in which one obtains private bits (which in particular could be singlets).

This thesis presents some of the results on the way to solve two important puzzles (open problems) of the quantum information theory:

1. are there NPT bound entangled states? — we aproach this problem from two different perspectives. The results presented in chapters 4 and 5 have been published in [6, 31]:

   - 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]

2. deeper understanding of PPT bound entangled states that are key distillable — namely, we provide a broad class of PPT bound entangled states which are key-distillable. The results presented in chapter 3 have been published in [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]

Chapter 2

Definitions and previous results

In this chapter we give definitions of the quantum informational concepts used in the following chapters. First, we explain the difference between a bit (as used in classical computing) and a qubit (used in quantum information). Then, we introduce Dirac notation: the notation of linear algebra used in quantum information. Next, we introduce two notions of the state of a quantum system: the pure state and the density matrix. We then explain partial trace, a mathematical operation which given a state of the total system gives us the state of its subsystem. Next we introduce important classes of quantum states: the separable states, the PPT states, the NPT states, the Bell diagonal states, and the Werner states. Then, we introduce measurement and unitary operations and collect all the physically realizable operations introduced before and give two equivalent formulations of the set of all physically realizable operations (Completely Positive Trace Preserving maps and formulation given with Kraus operators). We also define Quantum channel. Later, we give short introduction to distillation of entanglement and to quantum cryptography.

2.1 Bits and qubits

In *classical* computing information is stored and processed using two state registers called *bits*. The adjective *classical* is widely used in the context of quantum information and quantum computation to describe concepts, methods, and algorithms that refer to physics of the macroscopic world in contrast to concepts, methods, and algorithms of quantum information and quantum computation which take into account the effects postulated (and observed in nature) by quantum mechanics.

A simplest quantum register, in analogy to classical bit, is called a *qubit* (i.e., quantum bit). A qubit can be realized physically as a single particle (e.g., a photon) but here we are interested in the mathematical model of the qubit (and more generally: a quantum register). Mathematically, a qubit may be seen as a generalization of the bit which catches the richer structure of quantum mechanics in contrast to the Boolean logic used in classical computers. Note, that we say a bit (qubit) to denote the single bit (qubit) register and denote its state as the *state* of the bit (qubit).

We now point out some of the properties of qubits which differ them from classical bits:

1. Bits can have only two possible values, i.e., states (0 and 1) while qubits can be in one of two basic states $|0\rangle$ and $|1\rangle$ but also in a so-called *superposition* (i.e., linear combination) of the two basic states.

2. It is always possible to read out the value stored in a bit (we assume perfect registers). In contrast, it is possible to measure (read out) the value stored in a qubit only if it is in one of the basic states $|0\rangle$ or $|1\rangle$. Otherwise, if a qubit is in the superposition of basic states then after the measurement the state of the qubit probabilistically collapses into one of the basic states $|0\rangle$ or $|1\rangle$, so the state of the system is changed by the measurement. In particular, this implies that one cannot copy the state of the qubit, while coping is a natural and obvious operation to perform on the state of a bit.

3. Moreover, knowing the state of the register consisting of more than one qubit gives us, in general, only partial knowledge of the the states of particular qubits. This peculiarity happens if the qubits are *entangled*.

We denoted the basic states of a qubit with $|0\rangle$ and $|1\rangle$. This notation is called the *Dirac notation*.

2.2 Dirac notation

States of qubits and, in general, quantum registers are represented with vectors and matrices of complex numbers. To this end, a little bit strange at first sight but in fact extremely convenient, notation is used: the so-called *Dirac notation*.

Vectors In Dirac notation a column vector from a d dimensional Hilbert space $\mathbb{C}^d$ is denoted by $|x\rangle$ and its Hermitian adjoin $|x\rangle^\dagger$ is denoted by $\langle x|$, so we have

$$|x\rangle = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{d-1} \end{bmatrix} \qquad \langle x| \equiv |x\rangle^\dagger = \begin{bmatrix} x_0^* & x_1^* & \cdots & x_{d-1}^* \end{bmatrix} \tag{2.1}$$

where $x_i \in \mathbb{C}$ and x_i^* denotes complex conjugation of x_i. The Hermitian adjoin $\langle x|$ is sometimes called a *bra* and the column vector $|x\rangle$ is often called a *ket*.

In particular, we will use $|i\rangle$ to denote a vector having only one nonzero element on i-th position, i.e.,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad |d-1\rangle = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix} \qquad |i\rangle = \begin{bmatrix} \delta_{i0} \\ \delta_{i1} \\ \vdots \\ \delta_{i,d-1} \end{bmatrix} \qquad \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases} \tag{2.2}$$

Whenever a digit or an indexing variable i, j and k is used inside a ket it denotes a corresponding vector with a single non-zero element.

Inner product The *inner product* of vectors x and y is given by the matrix multiplication

$$\langle x|y\rangle \equiv \langle x|\,|y\rangle = \begin{bmatrix} x_0^* & x_1^* & \cdots & x_{d-1}^* \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{d-1} \end{bmatrix} = \sum_{i=0}^{d-1} x_i^* y_i. \tag{2.3}$$

Dirac notation is also called bracket notion, which comes from $\langle$ and $\rangle$ brackets used in the inner product $\langle x|y\rangle$ and thus the names *bra* and *ket* used to denote Hermitian adjoint $\langle x|$ and column vector $|y\rangle$ comes from splitting the word bra-ket into syllables.

Vector norm We define the *vector norm* in the Hilbert space $\mathbb{C}^d$ using the inner product of an arbitrary vector $|x\rangle$ as

$$\|x\| = \sqrt{\langle x|x\rangle}. \tag{2.4}$$

Orthonormal basis A set of vectors $\{|e_i\rangle\}_{i=0}^{d-1}$ is called an *orthonormal basis* for $\mathbb{C}^d$ if two conditions are satisfied

1. every vector $|x\rangle \in \mathbb{C}^d$ can be written as a linear combination of vectors from $\{|e_i\rangle\}_{i=0}^{d-1}$

$$|x\rangle = \sum_{i=0}^{d-1} a_i |e_i\rangle \tag{2.5}$$

   where $a_i \in \mathbb{C}$.

2. vectors $|e_i\rangle$ are normalized and mutually orthogonal, i.e., $\langle e_i|e_j\rangle = \delta_{ij}$.

We will denote orthonormal basis with either $\{|e_i\rangle\}_{i=0}^{d-1}$ or $\{|f_i\rangle\}_{i=0}^{d-1}$. When one mentions a basis in the context of quantum information it is assumed that the basis is orthonormal.

There is an orthonormal basis of a particular importance called the *standard basis*. The standard basis is denoted as

$$\{|i\rangle\}_{i=0}^{d-1} = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}. \tag{2.6}$$

Matrices The result of the multiplication $|x\rangle\langle y|$ gives a matrix

$$|x\rangle\langle y| = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{d-1} \end{bmatrix} \begin{bmatrix} y_0^* & y_1^* & \cdots & y_{d-1}^* \end{bmatrix} = \begin{bmatrix} x_0 y_0^* & x_0 y_1^* & \cdots & x_0 y_{d-1}^* \\ x_1 y_0^* & x_1 y_1^* & \cdots & x_1 y_{d-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ x_{d-1} y_0^* & x_{d-1} y_1^* & \cdots & x_{d-1} y_{d-1}^* \end{bmatrix}. \tag{2.7}$$

In particular, the result of a multiplication of vectors from the standard basis $|i\rangle\langle j|$ is a matrix with a single nonzero element in i-th row and j-th column. Thus, every operator A acting on a Hilbert space $\mathbb{C}^d$ (i.e., a $d \times d$ matrix) can be written as

$$A = \sum_{i,j=0}^{d-1} a_{ij} |i\rangle\langle j| = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0,d-1} \\ a_{10} & a_{11} & \cdots & a_{1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{d-1,0} & a_{d-1,1} & \cdots & a_{d-1,d-1} \end{bmatrix} \tag{2.8}$$

where $a_{ij} \in \mathbb{C}$.

Trace norm For matrices we will only use the *trace norm* that is the sum of the singular values of a matrix

$$\|A\| = \sum_i \sigma_i(A) \tag{2.9}$$

where $\sigma_i(A) \geq 0$ denote singular values of matrix A.

Projectors Let us recall that an operator P is called a *projector* if it satisfies $P^2 = P$ and $P^\dagger = P$. We will mostly use letter P and sometimes Q to denote projectors. Every projector onto a k dimensional subspace of $\mathbb{C}^d$ can be written as

$$P = \sum_{i=0}^{k-1} |e_i\rangle\langle e_i| \tag{2.10}$$

where $\{|e_i\rangle\}_{i=0}^{k-1}$ is an orthonormal basis for the subspace and, in particular, if $k = d$ then the projector P is equal to the *identity matrix* I that is a projector onto the total space $\mathbb{C}^d$. We use $\mathcal{H}_P$ to denote the Hilbert space corresponding to projector P.

In particular, if $\|x\| = 1$ then $|x\rangle\langle x|$ is the projector onto a one dimensional space spanned by the vector $|x\rangle$.

We will call expression $\langle x|P|x\rangle$ the *overlap* of x with P.

2.3 Pure state of a quantum system

A quantum system is modeled as d dimensional Hilbert space $\mathbb{C}^d$. If a quantum system is not in an interaction with the environment (is not entangled with the environment) then it is in a so-called *pure state*. We will denote the pure state of a quantum system with Greek letters ψ, ϕ and sometimes χ; putting them in the ket, e.g., $|\phi\rangle$, in formulas but referring to a state ϕ (without the ket) in a text. The pure state of a quantum system is represented by a vector $|\psi\rangle \in \mathbb{C}^d$ satisfying $\|\psi\| = 1$.

Each of the vector of the standard basis $|0\rangle$, $|1\rangle$, ..., $|d-1\rangle$ is a valid state of a d dimensional quantum system. But also any normalized linear combination (called *superposition*) of those vectors is a valid state of the quantum system

$$|\psi\rangle = \sum_{i=0}^{d-1} a_i |i\rangle = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{d-1} \end{bmatrix} \tag{2.11}$$

where the coefficients $a_i \in \mathbb{C}$ must satisfy the normalization condition

$$\|\psi\| = \sqrt{\sum_{i=0}^{d-1} |a_i|^2} = 1. \tag{2.12}$$

In particular, a two dimensional quantum system $\mathbb{C}^2$ is called a *qubit*. The pure state of a qubit has the form

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{2.13}$$

where the complex coefficients a and b must satisfy $|a|^2 + |b|^2 = 1$. In the column vector notation the state of the qubit is simply

$$|\psi\rangle = a|0\rangle + b|1\rangle = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}. \tag{2.14}$$

2.4 Bipartite and multipartite states

Suppose there are two distant parties (or laboratories) traditionally called Alice and Bob, and each of them holds a quantum system. Suppose Alice's system is d_A dimensional ($\mathbb{C}^{d_A}$) and Bob's system is d_B dimensional ($\mathbb{C}^{d_B}$). Now, we can consider Alice's and Bob's systems together as a single larger quantum system. From the perspective of this larger system we call Alice's and Bob's systems the *subsystems* of this *total* system and often abbreviate their names to single letters, i.e., we call them subsystem A and subsystem B. We call the total system a *bipartite* system (and its state a *bipartite* state) as it consists of two subsystems A and B. The name bipartite usually suggests the parties are distant.

The Hilbert space needed to describe the state of the total system is $d_A d_B$ dimensional. In particular, if Alice and Bob each have a single qubit systems ($d_A = d_B = 2$) then the total system is 4 dimensional. More generally, if Alice has n qubits and Bob has m qubits then their subsystems are 2^n and 2^m dimensional and the total system is 2^{n+m} dimensional. Thus the storage required to simulate quantum system on a classical computer grows exponentially with the number of simulated qubits. This is in contrast to classical bits, where if Alice has n bit register and Bob has m bit register the total register has $n+m$ bits (required storage grows linearly).

We denote the $d_A d_B$ dimensional Hilbert space of the total system as $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ which is isomorphic to $\mathbb{C}^{d_A d_B}$. The operator $\otimes$ is called the *tensor product*, it is also known as the Kronecker product in other scientific communities. We will often abbreviate $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ to $d_A \otimes d_B$, for example $2 \otimes 2$ represents a Hilbert space of a two-qubit system.

Now, let $\{|i\rangle\}_{i=0}^{d_A-1}$ be the standard basis for Alice system and $\{|j\rangle\}_{j=0}^{d_B-1}$ be the standard basis for Bob's system then the vectors

$$|i\rangle_A \otimes |j\rangle_B \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \tag{2.15}$$

for $i \in \{0, \dots, d_A - 1\}$ and $j \in \{0, \dots, d_B - 1\}$ form the standard basis for the $d_A d_B$ dimensional system $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$. For clarity, we subscribed kets with the names of the corresponding subsystems.

As already mentioned, the space $\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ is isomorphic to the space $\mathbb{C}^{d_A d_B}$: the vector $|i\rangle_A \otimes |j\rangle_B \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}$ corresponds to the vector $|k\rangle \in \mathbb{C}^{d_A d_B}$ where $k = i d_B + j$. For e.g., a two-qubit state may be in a state

$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}. \tag{2.16}$$

In general, the tensor product of two matrices A and B where A is a $n \times m$ matrix has the following block matrix form

$$A \otimes B \equiv \begin{bmatrix} a_{00}B & a_{01}B & \cdots & a_{0,m-1}B \\ a_{10}B & a_{11}B & \cdots & a_{1,m-1}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0}B & a_{n-1,1}B & \cdots & a_{n-1,m-1}B \end{bmatrix} \tag{2.17}$$

In particular, this formulation also works for $|x\rangle \otimes |y\rangle$ as $|x\rangle$ and $|y\rangle$ are simply column vectors.

We will also use the *tensor power* of a matrix given by

$$A^{\otimes n} = \underbrace{A \otimes A \otimes \cdots \otimes A}_{n}. \tag{2.18}$$

Since $|x\rangle|y\rangle$ is illegal as the matrix multiplication (two column vectors) thus it is widely used as an abbreviation of the tensor product $|x\rangle \otimes |y\rangle$. The vector

$|x\rangle\otimes|y\rangle$ may also be written as a single ket with tensor product inside $|x\otimes y\rangle$, this improves readability of some formulas by avoiding ambiguity. So the following are equivalent

$$|x\rangle \otimes |y\rangle = |x\rangle|y\rangle = |x \otimes y\rangle. \tag{2.19}$$

In the case of the vectors from the standard basis, $|i\otimes j\rangle$ is frequently abbreviated even further to $|ij\rangle$. So we have

$$|i\rangle \otimes |j\rangle = |i\rangle|j\rangle = |i \otimes j\rangle = |ij\rangle \tag{2.20}$$

$$|0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |0 \otimes 1\rangle = |01\rangle. \tag{2.21}$$

For clarity, we sometimes label the vectors with the name of the subsystems, even in the abbreviated form

$$|ij\rangle_{AB} \equiv |i\rangle_A \otimes |j\rangle_B. \tag{2.22}$$

If Alice's system is in a state $|\psi\rangle$ and Bob's system is in a state $|\phi\rangle$ then the total system is in a state

$$|\psi\rangle \otimes |\phi\rangle. \tag{2.23}$$

Such a state is called a *product state* as the state of the total system is a tensor product of the states of its subsystems. The subsystems of a product state are completely independent: Alice can prepare her system in a state $|\psi\rangle$ in her laboratory and Bob can prepare his system in a state $|\phi\rangle$ in his laboratory, and they do not have to communicate to do so.

Entanglement Now suppose that at the beginning Alice has both subsystems A and B in her laboratory and she prepares a state of the total system and then sends subsystem B to Bob keeping subsystem A in her laboratory. Having access to the total system, she can prepare the total system in a superposition which is not a *product state*. A pure state which is not a product state is called an *entangled state*. The best known entangled state is a two-qubit state of the form

$$|\psi_-\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B) \tag{2.24}$$

which is called the *singlet state*.

If the total system AB is in an entangled state ψ_{AB} then we say that Alice and Bob *share* the state ψ_{AB}. If ψ_{AB} is an entangled state then one cannot describe the state of the individual subsystems A and B as pure states. A more general notion of a state is necessary to describe them. This more general notion of the state — called the *density matrix* — will be described in the next section.

The singlet is an example of so-called *maximally entangled states*. It is also a member of a two-qubit orthonormal basis called the *Bell basis* which consists of four maximally entangled states (in contrast to the standard basis which consists only of product states). The four states ψ_i of the Bell basis are called the *Bell states* and are given by

$$\begin{aligned} |\psi_{1,2}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \\ |\psi_{3,4}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned} \tag{2.25}$$

For a general d dimensional Hilbert space $\mathbb{C}^d$ the canonical maximally entangled state is a generalization of the ψ_1 Bell state and has the form

$$|\phi_+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle. \tag{2.26}$$

Multiple subsystems We will also consider bipartite states consisting of more than two subsystems, such as $|00\rangle_{AA'} \otimes |10\rangle_{BB'}$ where subsystems A and A' belong to Alice and subsystems B and B' belong to Bob. Here, only one of the tensor products is written explicitly to visually separate Alice's subsystems from Bob's subsystems. Sometimes small letters a and b will be used instead of A' and B' to emphasize that subsystems a and b are qubits.

Another example of a bipartite state having multiple subsystems is

$$|\psi_-\rangle_{AB} \otimes |\psi_-\rangle_{A'B'} \tag{2.27}$$

which consists of two singlets shared by Alice and Bob. This state could also be written in a shorter form $|\psi_-\rangle^{\otimes 2}$ if we do not have to give the explicit names of the subsystems and it is obvious from the context that we mean (2.27) and not

$$|\psi_-\rangle_{AA'} \otimes |\psi_-\rangle_{BB'} \tag{2.28}$$

which consists of two singlets one in the Alice's laboratory and the second one in the Bob's laboratory. In fact, if we use a tensor power such as $|\psi_-\rangle^{\otimes n}$ we always mean (unless explicitly stated otherwise) that individual $|\psi_-\rangle$ states are shared by Alice and Bob. In this case we call individual states $|\psi_-\rangle$ *copies* as Alice and Bob clearly share n identical copies of the state $|\psi_-\rangle$.

Apart from bipartite states, we will also consider multipartite states, in particular, three-partite states, mainly in the context of quantum cryptography, where apart from the two parties Alice and Bob involved in the private communication we will also consider a third party called Eve (for eavesdropper) who will try to obtain some knowledge of private communication between Alice and Bob.

Schmidt decomposition Every bipartite pure state ψ defined on $d_A \otimes d_B$ can be written in its so-called *Schmidt decomposition*

$$|\psi\rangle = \sum_{i=0}^{k-1} \mu_i \, |e_i\rangle_A \otimes |f_i\rangle_B \tag{2.29}$$

where $k \leq \min\{d_A, d_B\}$ is called the *Schmidt rank* of the state ψ and we will denote it by $\mathrm{Sch}(A:B) \equiv k$ where the relevant state ψ will be evident from the context; the coefficients μ_i are called the *Schmidt coefficients* of the state ψ and are positive numbers and their squares form a probability distribution, i.e.,

$$\sum_{i=0}^{k-1} \mu_i^2 = 1 \tag{2.30}$$

while $\{|e_i\rangle\}_{i=0}^{d_A}$ and $\{|f_i\rangle\}_{i=0}^{d_B}$ are orthonormal basis for subsystems A and B, respectively.

If the state ψ is a state of a quantum system having multiple subsystems, for e.g., $AA'BB'$ then the state ψ has several Schmidt decompositions each corresponding to a partition of its subsystems into two groups, for e.g., $AA' : BB'$ where the first group AA' belongs to Alice and and the second group BB' belongs to Bob. We call such a partition of subsystems a *cut*. In particular, in the text instead of $AA' : BB'$ cut we can also say AA' versus BB' cut or Alice versus Bob cut (if it is obvious from the context which subsystems belong to Alice and which to Bob). But we can also consider other cuts such as $A : A'BB'$ and even $AB : A'B'$. So we have the following Schmidt decompositions of ψ corresponding to the those three cuts

$$|\psi\rangle_{AA'BB'} = \sum_{i=0}^{k-1} \mu_i \, |e_i\rangle_{AA'} \otimes |f_i\rangle_{BB'} \tag{2.31}$$

$$= \sum_{i=0}^{k'-1} \mu_i' \, |e_i'\rangle_{A} \otimes |f_i'\rangle_{A'BB'} \tag{2.32}$$

$$|\psi\rangle_{ABA'B'} = \sum_{i=0}^{k''-1} \mu_i'' \, |e_i''\rangle_{AB} \otimes |f_i''\rangle_{A'B'} \tag{2.33}$$

where $\mathrm{Sch}(AA' : BB') = k$, $\mathrm{Sch}(A : A'BB') = k'$, and $\mathrm{Sch}(AB : A'B') = k''$ are Schmidt ranks of ψ in $AA' : BB'$, $A : A'BB'$, and $AB : A'B'$ cuts, respectively. Here, $|\psi\rangle_{AA'BB'}$ and $|\psi\rangle_{ABA'B'}$ both represent the same state ψ but with different order of subsystems so they are different vectors

$$|\psi\rangle_{AA'BB'} \neq |\psi\rangle_{ABA'B'}. \tag{2.34}$$

In the context where Schmidt rank of the state is important, we will denote a pure state of rank k in a given cut $A : B$ as $\phi_k^{A:B}$ (subscripted with the rank and the cut) and the set of all such states as $\mathrm{SR}_k(A : B)$, so we have $\phi_k^{A:B} \in \mathrm{SR}_k(A : B)$. For e.g., we will use $\phi_1^{A:B}$, $\phi_2^{A:B}$ and $\mathrm{SR}_2(AA' : BB')$. The cut may be omitted if evident from the context.

2.5 Density matrices or mixed states of a quantum system

If a quantum system has been prepared in a pure state and it is kept isolated from other systems, that is it is not interacting with other systems especially with the so-called *environment* (any other quantum system that we do not control) then we can use the notion of pure states to describe the state of the system. But if we want to ask for the state of a subsystem of an entangled system or we want to model the interaction of our state with any other system we have to use the more general notion of *density matrices* to model the state of subsystem or the state of an interacting system.

The state of the d dimensional quantum system $\mathbb{C}^d$ may be modeled by $d \times d$ matrix (i.e., an operator acting on $\mathbb{C}^d$ space) called the *density matrix.* The density matrix ϱ is a matrix satisfying two conditions:

1. it is a positive semidefinite matrix ($\varrho \geq 0$), i.e., has only nonnegative eigenvalues $\lambda_i \geq 0$ and

2. it is normalized

$$\mathrm{Tr}\varrho = \sum_{i=0}^{d-1} \lambda_i = 1 \tag{2.35}$$

Density matrices are usually denoted by Greek letters ϱ, σ, and — to denote the so-called private bits — γ.

We can observe that eigenvalues of a density matrix form a discrete probability distribution so we will often denote them with p_i rather then λ_i. The fact that a density matrix is (by definition) positive semidefinite implies that the density matrix is a *Hermitian* operator that is $\varrho^\dagger = \varrho$.

Whenever we will refer to the *state* of the quantum system we will mean the density matrix representing the state of the quantum system unless we explicitly mention the system is in a *pure* state.

Spectral decomposition As the density matrix ϱ is positive semidefinite matrix ($\varrho \geq 0$) it can be represented by its *spectral decomposition*

$$\varrho = \sum_{i=0}^{d-1} p_i |\psi_i\rangle\langle\psi_i| \tag{2.36}$$

where $p_i \geq 0$ are eigenvalues of ϱ and form a discrete probability distribution, and ψ_i are normalized eigenvectors of ϱ, so ψ_i are mutually orthogonal pure states. If all nonzero p_i are distinct then the spectral decomposition is unique.

The spectral decomposition (2.36) is actually possible for any *normal operator* A (i.e., operator satisfying $A^\dagger A = AA^\dagger$) but for the general normal matrix the eigenvalues are complex numbers. For a subclass of normal matrices called

Hermitian operators (i.e., operators satisfying $A = A^\dagger$) the eigenvalues are real numbers. And the subclass of Hermitian operators called *positive semidefinite operators* (which we denote by $A \geq 0$) is defined by having nonnegative eigenvalues.

Pure states If a quantum system is in a pure state ψ the state of the system can also be represented as a density matrix (let us denote it by ϱ) of the form

$$\varrho = |\psi\rangle\langle\psi|. \tag{2.37}$$

The pure state (2.37) is a special case of the spectral decomposition (2.36) where there is only one eigenvector ψ associated with the only nonzero eigenvalue equal to 1.

By referring to a pure state ψ we may mean the vector $|\psi\rangle$ or the density matrix $|\psi\rangle\langle\psi|$. Which one we actually mean should be evident from the context and on the other hand they are, in a sense, equivalent so this should not lead to any ambiguity. Every pure state written as a density matrix is also a one dimensional projector

$$P_\psi = |\psi\rangle\langle\psi| \tag{2.38}$$

on a subspace spanned by ψ. In particular, we will use the projectors

$$\Phi^+ = |\phi_+\rangle\langle\phi_+| \tag{2.39}$$

$$\Psi^- = |\psi_-\rangle\langle\psi_-| \tag{2.40}$$

where ϕ_+ is a maximally entangled state given by (2.26) and ψ_- is the singlet state given by (2.24).

Examples Now, suppose Alice has a quantum system and she prepares it randomly either in a state ψ with probability p or in a state ϕ with probability $1-p$. Then she sends the state ϱ prepared in this way to Bob telling Bob *how* she prepared the state without telling him *which* of the state was randomly chosen. From Bobs perspective the state ϱ is not pure but nevertheless he has some knowledge about it and this knowledge can be expressed with a density matrix

$$\varrho = p|\psi\rangle\langle\psi| + (1-p)|\phi\rangle\langle\phi|. \tag{2.41}$$

We say that such ϱ is a *mixture* of states ψ and ϕ. We also say that ϱ is a *mixed state* which strictly speaking means the state is represented as a density matrix and is not in a pure state (so a state may be either pure or mixed). But it is also common to use the term *mixed state* to refer to any state represented as a density matrix (which could in particular be a pure state) thus, in this case, the word *mixed* is used to stress that we do not restrict ourselves to the set of pure states.

In general, if Alice wants to send state ϱ to Bob then she can randomly select one of ψ_i with probability p_i where p_i and ψ_i come from the spectral decomposition (2.36) of ϱ.

Now, suppose Alice have sent Bob a state ϱ but have told him nothing about the way she prepared the state. Bob can still represent his complete lack of knowledge as a density matrix called the *maximally mixed state* which has the form

$$\varrho = \frac{\mathrm{I}}{d} \tag{2.42}$$

where I stands for the identity matrix.

But if Alice prepares many copies of ϱ according to the same recipe and sends them to Bob but she does not tell him the recipe she used then Bob does not have to assume he have obtained maximally mixed states (2.42): by the so-called *quantum tomography* he can learn the density matrix of ϱ or, in other words, he learns the spectral decomposition of ϱ (subject to some error, depending on the number of copies of the state used for the tomography). Bob can also use tomography if he does not fully trust Alice is really using the promised recipe.

Noise As maximally mixed state represents no knowledge about the state of the system it is well suited to represent the uncontrolled interaction with the environment, i.e., it can be used to model the effect of noise. This time, suppose Alice is sending a state ϱ to Bob by a noisy quantum channel and the channel between Alice and Bob transmits a given state faithfully with probability $1-\varepsilon$ but with probability ε the state is completely destroyed on a way by the interaction with an environment. Then if Alice sends a state ϱ to Bob then Bob receives the state

$$\varrho' = (1-\varepsilon)\varrho + \varepsilon\frac{\mathrm{I}}{d}. \tag{2.43}$$

Preparation Let us come back to the example of Alice sending a mixture of ψ and ϕ. If ψ and ϕ are orthogonal then (2.41) is a spectral decomposition of ϱ. But if they are not orthogonal then the spectral decomposition is given by (2.36) where only p_0 and p_1 are nonzero and the associated eigenvectors ψ_1 and ψ_2 belong to a subspace spanned by ψ and ϕ. Thus in general, spectral decomposition gives one possible way of preparing a state with a given density matrix ϱ but there are many other recipes of the form

$$\varrho = \sum_{i=0}^{k-1} p_i |\psi_i\rangle\langle\psi_i| \tag{2.44}$$

of preparing a state in the state ϱ. Such a recipe for a preparation of ϱ given as a set of states ψ_i with associated probabilities p_i of the form

$$\{(p_i, \psi_i)\}_{i=0}^{k-1} \tag{2.45}$$

is called an *ensemble*. So spectral decomposition provides one of many possible ensembles that may be used to prepare a state ϱ but this ensemble has a unique feature: all ψ_i are mutually orthogonal.

2.5.1 Partial trace and the state of a subsystem

Suppose Alice and Bob share a quantum system in a state ϱ_{AB} consisting of two subsystems A and B: Alice holds subsystem A and Bob holds subsystem B. We denote the state of subsystem A as ϱ_A and the state of subsystem B as ϱ_B and their dimensions with d_A and d_B, respectively. We can compute the states ϱ_A and ϱ_B of subsystems A and B from the state of the total system ϱ_{AB} using an operation called the *partial trace*.

We first recall that the trace of any $d \times d$ matrix X could be written as

$$\mathrm{Tr} X = \sum_{i=0}^{d-1} \langle i | X | i \rangle \tag{2.46}$$

where instead of the standard basis $\{|i\rangle\}_{i=0}^{d-1}$ any orthonormal basis $\{|e_i\rangle\}_{i=0}^{d-1}$ could be used. Now, the partial trace is a linear operation which applied to a product of two matrices performs a trace only on the subsystem (or subsystems) given in subscript

$$\mathrm{Tr}_A(X_A \otimes X_B) \equiv \mathrm{Tr}(X_A) \otimes X_B = \mathrm{Tr}(X_A) X_B \tag{2.47}$$

$$\mathrm{Tr}_B(X_A \otimes X_B) \equiv X_A \otimes \mathrm{Tr}(X_B) = \mathrm{Tr}(X_B) X_A \tag{2.48}$$

In particular, as density matrices have trace equal to 1, we have

$$\mathrm{Tr}_A(\sigma_A \otimes \sigma_B) = \mathrm{Tr}(\sigma_A) \otimes \sigma_B = \mathrm{Tr}(\sigma_A)\sigma_B = \sigma_B \tag{2.49}$$

$$\mathrm{Tr}_B(\sigma_A \otimes \sigma_B) = \sigma_A \otimes \mathrm{Tr}(\sigma_B) = \mathrm{Tr}(\sigma_B)\sigma_A = \sigma_A \tag{2.50}$$

So we see that if Alice and Bob share a product state $\sigma_A \otimes \sigma_B$ in the effect of *tracing out* one of the subsystems we obtain the state of the second one. But this is, actually, true for an arbitrary state ϱ_{AB} shared by Alice and Bob — by the operation of the partial trace of one of the subsystems (B or A) we obtain the state of the other subsystem (ϱ_A or ϱ_B):

$$\varrho_A \equiv \mathrm{Tr}_B(\varrho_{AB}) \qquad \varrho_B \equiv \mathrm{Tr}_A(\varrho_{AB}). \tag{2.51}$$

The partial trace of a bipartite operator X_{AB} is given by

$$\mathrm{Tr}_A(X_{AB}) \equiv \sum_{i=0}^{d_A-1} \langle i|_A \otimes \mathrm{I}_B \; X_{AB} \; |i\rangle_A \otimes \mathrm{I}_B \tag{2.52}$$

$$\mathrm{Tr}_B(X_{AB}) \equiv \sum_{i=0}^{d_B-1} \mathrm{I}_A \otimes \langle i|_B \; X_{AB} \; \mathrm{I}_A \otimes |i\rangle_B. \tag{2.53}$$

In the above sum, vectors from the standard basis $|i\rangle$ have been used on the subsystem which we traced out (forgotten) and identity operator have been used on a subsystem which have been left in the resulting expression. This generalizes to more subsystems — we use $|i\rangle$ on all traced out subsystems and identity on all subsystems that are left in the resulting expression, for example

$$\mathrm{Tr}_{A'B'}(X_{AA'BB'}) \equiv \sum_{i,j=0}^{\substack{i=d_{A'}-1\\ j=d_{B'}-1}} \mathrm{I}_A \otimes \langle i|_{A'} \otimes \mathrm{I}_B \otimes \langle j|_{B'}\, X_{AA'BB'}\, \mathrm{I}_A \otimes |i\rangle_{A'} \otimes \mathrm{I}_B \otimes |j\rangle_{B'}. \tag{2.54}$$

We will sometimes use the term *reduction* to refer to the state of a subsystem.

2.5.2 Separable states, PPT and NPT states

If Alice and Bob share a pure state then there are only two possibilities, either:

1. each of them holds a pure state — so they share a product state of the form $|\psi\rangle_A \otimes |\phi\rangle_B$ and the states of subsystem A and B are unrelated, or
2. they share an entangled state — i.e., there is some quantum mechanical correlation between subsystems A and B which has no analog in our everyday macroscopic world.

Analogously, each density matrix ϱ shared by Alice and Bob is either a non-entangled one, called a *separable state*, or an *entangled one.* But, the definition of a separable state is slightly more complicated than the definition of a pure product state.

Suppose, Alice and Bob prepare a pure product state $|\psi\rangle_A \otimes |\phi\rangle_B$: Alice prepares her subsystem in a state ψ and Bob prepares his system in a state ϕ. Each of them acts locally in her/his own laboratory and they can do this even if they have never met each other before — the state is obviously not entangled. Analogously, Alice can prepare her subsystem in a state ϱ and Bob can prepare his subsystem in a state σ and the state of the total system $\varrho \otimes \sigma$ is not entangled: it is a product state but not a pure product state (unless both ϱ and σ are pure). Now suppose, Alice selects randomly an integer i (out of some finite set), each with probability p_i, and sends her choice to Bob and then depending on integer i they jointly — each acting in her/his own laboratory — prepare a product state $\varrho_i \otimes \sigma_i$. The density matrix of such a state ϱ has the form

$$\varrho = \sum p_i\, \varrho_i \otimes \sigma_i \tag{2.55}$$

and such a state is not entangled as it can be prepared by randomly selecting one of several (not entangled) product states according to a finite probability distribution. States of the form (2.55) are called *separable states.* Now, every state which is not of this form is called an *entangled state*.

In general, given a density matrix ϱ it is a computationally hard problem to decide if it is a separable state [32]. But there is an important necessary condition for separability of a given state ϱ called the *Peres criterion* [22] which states that for a given state ϱ to be separable its *partial transposition* must be a positive semidefinite operator

$$\varrho^\Gamma \geq 0. \tag{2.56}$$

In the special case of states of $2 \otimes 2$ and $2 \otimes 3$ Hilbert spaces the Peres criterion is the necessary and sufficient condition for separability [33].

Before defining the partial transposition, we first recall that the *transposition* of a matrix can be defined as a linear superoperator that transposes every matrix from the $|i\rangle\langle j|$ basis, i.e.,

$$(aA + bB)^T = aA^T + bB^T \tag{2.57}$$

$$(|i\rangle\langle j|)^T = |j\rangle\langle i|. \tag{2.58}$$

Thus for any matrix

$$X = \sum_{ij} a_{ij} |i\rangle\langle j| \tag{2.59}$$

its transposition is given by

$$X^T \equiv \sum_{ij} a_{ij} |j\rangle\langle i|. \tag{2.60}$$

Now, the *partial transposition* denoted with X^Γ of a bipartite matrix X can be specified as a linear superoperator that transposes a second subsystem of every matrix from the product basis $|i\rangle\langle j| \otimes |k\rangle\langle l|$, i.e.,

$$(aA + bB)^\Gamma = aA^\Gamma + bB^\Gamma \tag{2.61}$$

$$(|i\rangle\langle j| \otimes |k\rangle\langle l|)^\Gamma = |i\rangle\langle j| \otimes |l\rangle\langle k|. \tag{2.62}$$

Thus for any bipartite matrix

$$X = \sum_{ijkl} a_{ijkl} |i\rangle\langle j| \otimes |k\rangle\langle l| \tag{2.63}$$

its partial transposition is given by

$$X^\Gamma \equiv \sum_{ijkl} a_{ijkl} |i\rangle\langle j| \otimes |l\rangle\langle k|. \tag{2.64}$$

If a bipartite density matrix ϱ has a positive semidefinite partial transpose $\varrho^\Gamma \geq 0$ then we call ϱ a *PPT state* (*Positive Partial Transpose*) and if the partial transpose of ϱ is a nonpositive operator $\varrho^\Gamma \ngeq 0$ then we call ϱ an *NPT state* (*Nonpositive Partial Transpose*). Now, the Peres criterion states that every separable state is a PPT state, so PPT is a precondition for separability. And in the special case of $2 \otimes 2$ and $2 \otimes 3$ states a state is separable if and only if it is a PPT state and, on the other hand, it is entangled if and only if it is an NPT state.

2.5.3 Bell diagonal states

There is an important class of two-qubit density matrices called *Bell diagonal states*

$$\varrho = \sum_{i=1}^{4} p_i |\psi_i\rangle\langle\psi_i| \tag{2.65}$$

where ψ_i are Bell states given by (2.25). The name comes from the fact that Bell states ψ_i form an orthonormal basis and so states of the class (2.65) are by definition diagonal if written in this basis. We will use Bell diagonal states in the context of quantum cryptography.

As explained in a previous section, the two-qubit state can either be separable or entangled and positivity of the partial transposition of a density matrix can be used to distinguish between them. Let us consider the density matrix of a Bell diagonal state and its partial transposition

$$\varrho = \begin{bmatrix} p_1+p_2 & 0 & 0 & p_1-p_2 \\ 0 & p_3+p_4 & p_3-p_4 & 0 \\ 0 & p_3-p_4 & p_3+p_4 & 0 \\ p_1-p_2 & 0 & 0 & p_1+p_2 \end{bmatrix} \tag{2.66}$$

$$\varrho^\Gamma = \begin{bmatrix} p_1+p_2 & 0 & 0 & p_3-p_4 \\ 0 & p_3+p_4 & p_1-p_2 & 0 \\ 0 & p_1-p_2 & p_3+p_4 & 0 \\ p_3-p_4 & 0 & 0 & p_1+p_2 \end{bmatrix}. \tag{2.67}$$

For $\varrho^\Gamma \geq 0$ both outer and inner blocks must be positive semidefinite, i.e.,

$$\begin{bmatrix} p_1+p_2 & p_3-p_4 \\ p_3-p_4 & p_1+p_2 \end{bmatrix} \geq 0 \quad \wedge \quad \begin{bmatrix} p_3+p_4 & p_1-p_2 \\ p_1-p_2 & p_3+p_4 \end{bmatrix} \geq 0 \tag{2.68}$$

that is

$$p_1+p_2 \geq |p_3-p_4| \quad \wedge \quad p_3+p_4 \geq |p_1-p_2| \tag{2.69}$$

which is satisfied if all $p_i \leq \frac{1}{2}$. Thus the Bell diagonal state is separable if all $p_i \leq \frac{1}{2}$ and entangled when $p_i > \frac{1}{2}$ for some i.

2.5.4 Werner states

Another important class of states are the so-called *Werner states* [15]. We will use Werner states in the context of distillation of entanglement. Werner states are states defined on $d \otimes d$ Hilbert space as a mixture of two states

$$\varrho_W \equiv p\varrho_s + (1-p)\varrho_a \tag{2.70}$$

and the states ϱ_s and ϱ_a are given by

$$\varrho_s = \frac{P_s}{d_s}, \quad \varrho_a = \frac{P_a}{d_a} \tag{2.71}$$

where P_s and P_a are projectors onto the *symmetric* and *antisymmetric* subspaces and d_s and d_a are their dimensions

$$P_s = \frac{1}{2}(\mathrm{I} + V) \qquad d_s = \frac{d(d+1)}{2} \tag{2.72}$$

$$P_a = \frac{1}{2}(\mathrm{I} - V) \qquad d_a = \frac{d(d-1)}{2}. \tag{2.73}$$

The operator V is the *swap operator* which acting on a bipartite state swaps its subsystems

$$V|\psi \otimes \phi\rangle = |\phi \otimes \psi\rangle \tag{2.74}$$

The swap operator has the following matrix form

$$V \equiv \sum_{i,j=0}^{d-1} |ij\rangle\langle ji|. \tag{2.75}$$

Alternatively, Werner states could be defined directly in terms of operators I and V as

$$\varrho_W \equiv \frac{\mathrm{I} + \alpha V}{d^2 + \alpha d}. \tag{2.76}$$

Werner states are $U \otimes U$ invariant, i.e., applying the same unitary operator U (see section 2.7) to both subsystems does not change a Werner state

$$\varrho_W = U \otimes U \, \varrho_W \, U^\dagger \otimes U^\dagger. \tag{2.77}$$

2.6 Measurement

The *von Neumann measurement* of a quantum system or simply the *measurement* is a process performed on the system in the effect of which we obtain some knowledge about the state of the system before the measurement but we, in general, pay the price of irreversible modification or even destruction of a state of the system. The result of the measurement is an integer number i and the state of the system after the measurement depends on the obtained result i and, if it is not completely destroyed, also depends on an initial state ϱ.

Measurement of a qubit system Let us first consider a measurement of a qubit system. The qubit is a generalization of the classical bit and the classical bit can only have one of two states (0 or 1) and the state can be read out from the bit. We could restrict ourselves to use a qubit as a bit: prepare the state of the qubit only in one of the states $|0\rangle$ and $|1\rangle$ and use only such quantum operations that represent classical gates. In this restricted case, the measurement of the qubit works just like a read out of the bit — it gives the result 0 if the qubit has the state $|0\rangle$ or 1 if the qubit is in the state $|1\rangle$ and the measurement does not change the state of the qubit. But this is not the case in general, if the qubit is prepared in a state ψ which is neither $|0\rangle$ nor $|1\rangle$ and the measurement checks whether ψ is one of $|0\rangle$ or $|1\rangle$ then

1. the result of the measurement will be 0 with probability $p_0 = |\langle\psi|0\rangle|^2$ and the qubit will be in the state $|0\rangle$ after the measurement, or

2. the result of the measurement will be 1 with probability $p_1 = |\langle\psi|1\rangle|^2$ and the qubit will be in the state $|1\rangle$ after the measurement.

So in general measurement of a quantum system is a random process which modifies the state of the system. In fact, the measurement of a qubit destroys the initial state ψ leaving us with one bit of information — the result of the measurement i — and with a system in a state $|0\rangle$ or $|1\rangle$ which is completely determined by the result i and does not contain any further knowledge of ψ. So from a rich structure of a qubit we can read, by measurement, only one bit of information and the rest of the information is lost after the measurement.

The above measurement is called the *measurement in the standard basis* because we asked whether the qubit is in one of the states of the standard basis ($|0\rangle$ or $|1\rangle$) but a measurement may also be done in any other orthonormal basis $\{|e_0\rangle, |e_1\rangle\}$ then vectors $|i\rangle$ must be replace with $|e_i\rangle$ in the above consideration.

Using projectors We can reformulate the effect of a measurement of a qubit in the standard basis (or analogously in any other orthonormal basis) using the projectors onto the states of the standard basis

$$P_0 = |0\rangle\langle 0|, \quad P_1 = |1\rangle\langle 1|. \tag{2.78}$$

In the effect of the measurement of the qubit in a state ψ in the standard basis we obtain the result i (0 or 1) with probability

$$p_i = \langle\psi|P_i|\psi\rangle = \mathrm{Tr} P_i|\psi\rangle\langle\psi|P_i \tag{2.79}$$

and the qubit after the measurement is in the state

$$|\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{p_i}} = |i\rangle. \tag{2.80}$$

If a qubit before the measurement is in a state ϱ then after the measurement in the standard basis we obtain the result i (0 or 1) with probability

$$p_i = \mathrm{Tr} P_i \varrho P_i \tag{2.81}$$

and the qubit after the measurement is in the pure state

$$\varrho_i = \frac{P_i \varrho P_i}{p_i} = |i\rangle\langle i|. \tag{2.82}$$

Direct sum Let us recall that each Hilbert space $\mathcal{H} = \mathbb{C}^d$ can be represented as a direct sum of $k \leq d$ orthogonal subspaces

$$\mathcal{H} = \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_{k-1} \tag{2.83}$$

where each of the subspaces corresponds to a projector P_i projecting onto the subspace $\mathcal{H}_i$. Due to the above equality the projectors P_i must satisfy

$$\sum_{i=0}^{k-1} P_i = \mathrm{I}. \tag{2.84}$$

We will call this representation the *partition* of a Hilbert space $\mathcal{H}$ into subspaces. In particular any orthonormal basis partitions the Hilbert space into d one dimensional subspaces with $P_i = |e_i\rangle\langle e_i|$.

Von Neumann measurement Now, the *von Neumann measurement* of a quantum system represented by a d-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$ corresponds to a particular partition of the Hilbert space into subspaces. In particular if all the subspaces are one dimensional the partition corresponds to some orthonormal basis $\{|e_i\rangle\}_{i=0}^{d-1}$ and we call such a measurement a *measurement in the basis* $\{|e_i\rangle\}_{i=0}^{d-1}$. Let ϱ be the state of the system before the measurement. The measurement is a process which checks to which of the subspaces $\mathcal{H}_i$ the state belongs to. If ϱ belongs to one of the subspaces $\mathcal{H}_i$ that is $\varrho = P_i \varrho P_i$ then the state of the system is not changed by the measurement and the result of the measurement is the index i of the subspace to which ϱ belongs. If ϱ is not contained in one of the subspaces $\mathcal{H}_i$ then it will be projected onto one of the subspaces and the result i of the measurement will return the index of the subspace onto which ϱ have been projected by the measurement. Namely, with probability

$$p_i = \mathrm{Tr} P_i \varrho P_i \tag{2.85}$$

the measurement gives the result i and the state after the measurement has the form

$$\varrho_i = \frac{P_i \varrho P_i}{p_i}. \tag{2.86}$$

In the case where the state before the measurement is a pure state $\varrho = |\psi\rangle\langle\psi|$ we can also use the formulas

$$p_i = \langle\psi|P_i|\psi\rangle, \quad |\psi_i\rangle = \frac{P_i|\psi\rangle}{\sqrt{p_i}}. \tag{2.87}$$

where ψ_i is the pure state of the system if a result i was obtained.

The von Neumann measurement in some basis may be used to discriminate between orthogonal quantum states of that basis as it was for $|0\rangle$ and $|1\rangle$ in the case of a qubit system.

Measurement of a subsystem Having a bipartite state ϱ_{AB} we can do the measurement corresponding to some projectors P_i on a single subsystem, let it be subsystem A. The above measurement scheme applied directly to the state ϱ_A of the measured subsystem will tell us what are the probabilities p_i of obtaining result i and the corresponding output state $\varrho_A^{(i)}$. But this does not tell us what will be the state of the total system after the measurement. To learn this we have to consider the equivalent measurement on the total system using the projectors $P_i \otimes \mathrm{I}_B$ which will give us the same probabilities p_i of obtaining result i but with the corresponding output state $\varrho_{AB}^{(i)}$ of the total system. Analogously, for a measurement of a single subsystem of a multipartite state we use P_i on the measured system and identity operators on all the others. Thus, we see that measurement of a subsystem is a special case of measurement of the total system.

Embedding the result The output of the measurement of a state ϱ is an integer result i and a corresponding state ϱ_i but we can also encode the result i of the measurement into a subsystem of a larger output state, in this form — which we here call an *embedded measurement* — the measurement is simply a linear superoperator M that irreversibly transforms one state into another one ($\tilde{\varrho} \to \tilde{\varrho}' = M(\tilde{\varrho})$). For this we introduce an additional subsystem called R of dimension k to encode the result of the measurement

$$\tilde{\varrho} = \varrho \otimes |0\rangle_R\langle 0| \tag{2.88}$$

and the measurement M has the form

$$M(\tilde{\varrho}) \equiv \sum_{i=0}^{k-1} p_i\, \varrho_i \otimes |i\rangle_R\langle i| = \sum_{i=0}^{k-1} P_i \varrho P_i \otimes |i\rangle_R\langle i| \tag{2.89}$$

where p_i and ϱ_i are given by (2.85) and (2.86), respectively. Having the output state $\tilde{\varrho}'$ we can always read out (with a non-destructive measurement in the standard basis) from subsystem R which ϱ_i we do have at hand.

Generalized measurement — POVM (Positive Operator Valued Measure) is a generalization of the von Neumann measurement. It is physically realizable as a von Neumann measurement on a larger Hilbert space then the Hilbert space of ϱ but mathematically can be written as a measurement on the Hilbert space of the measured state ϱ given as a set of operators satisfying

$$A_i \geq 0 \tag{2.90}$$

$$\sum_i A_i = \mathrm{I} \tag{2.91}$$

where the sum may contain any number of operators (increasing the number of operators increases the larger space used for physical realization). The probability of obtaining outcome i is given by

$$p_i = \mathrm{Tr}(A_i \varrho). \tag{2.92}$$

A longer introduction to the POVM measurements may be found in [34].

2.7 Unitary operators – reversible transformations of quantum systems

Having a quantum system in a state ϱ (or ψ) we can transform it reversibly to the state ϱ' (or ψ') such a physical operation is represented by a *unitary operator*. The reversibility of this transformation means that we can later apply another unitary operator that will bring the state back to ϱ (or ψ).

A *unitary operator* U, or simply *unitary* U, is a matrix satisfying $UU^\dagger = \mathrm{I}$. Columns (and analogously rows) of a unitary operator U form the orthonormal basis $|e_i\rangle_{i=0}^{d-1}$ and so it can be written as

$$U = \sum_{i=0}^{d-1} |e_i\rangle\langle i| \tag{2.93}$$

and the effect of a unitary is clearly a change of basis

$$U|i\rangle = |e_i\rangle. \tag{2.94}$$

A unitary operator represents a reversible transformation of the state of a quantum system. By applying the unitary U to quantum system in a state ψ or ϱ we obtain a quantum system in a state ψ' or ϱ'

$$|\psi'\rangle = U|\psi\rangle \qquad\qquad \varrho' = U\varrho U^\dagger. \tag{2.95}$$

Now, by the very definition of a unitary matrix we have $UU^\dagger = \mathrm{I}$ and thus $U^\dagger$ is another unitary that reverses the effect of the unitary U

$$U^\dagger|\psi'\rangle = U^\dagger U|\psi\rangle = |\psi\rangle \qquad U^\dagger\varrho' U = U^\dagger U\varrho U^\dagger U = \varrho. \tag{2.96}$$

Local and global unitaries Having a bipartite state ϱ_{AB} we can apply a unitary U_A to its subsystem A and unitary U_B to its subsystem B, this is done with a product unitary $U_A \otimes U_B$:

$$U_A \otimes U_B\, \varrho_{AB} U_A^\dagger \otimes U_B^\dagger \tag{2.97}$$

In particular, doing nothing can be represented as a unitary matrix – the identity matrix I. So, $U_A \otimes \mathrm{I}_B$ is a unitary matrix that acts only on subsystem A:

$$U_A \otimes \mathrm{I}_B\, \varrho_{AB} U_A^\dagger \otimes \mathrm{I}_B. \tag{2.98}$$

We say that this is a *local* unitary, i.e., acting on a specific subsystem. If A is Alice's subsystem then Alice can apply unitary U_A on her subsystem and effectively apply unitary $U_A \otimes \mathrm{I}_B$ to the total system. In contrast we call a unitary U_{AB} acting on the total system a *global* unitary. Physical realization of the global unitary requires access to the total system, which is not possible if the subsystems are distant. (Unless some other global resources are available such as classical communication together with entangled state). The swap operator

V defined with (2.75) is a good example of a global unitary that exchanges the states of two subsystems

$$V|\psi \otimes \phi\rangle = |\phi \otimes \psi\rangle. \tag{2.99}$$

We will sometimes use the unitary subscripted with a subsystem, for e.g., U_A, to represent a unitary on the total system that only changes subsystem A and acts as identity on other subsystems, i.e., such U_A is given by $U_A = U'_A \otimes \mathrm{I}_B$ where U'_A is defined on subsystem A.

Examples There are three important single qubit unitaries denoted by σ_x, σ_y and σ_z called the *Pauli matrices*. The Pauli matrices have the following form

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.100}$$

Pauli matrices with identity matrix form a basis for the single qubit unitaries.

Another important single qubit unitary is the *Hadamard gate*

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{2.101}$$

The Hadamard gate is a *unimodular matrix* that is a matrix with all elements a_{ij} having the same modulus, i.e., $|a_{ij}| = a$. Unimodular unitary matrices exist for every dimension d, in particular a tensor power of Hadamard matrix $H^{\otimes k}$ is a unimodular matrix of dimension $d = 2^k$.

In general, a single qubit unitary can be written using the following parametrization [35]

$$U = e^{i\alpha} \begin{bmatrix} e^{i\left(-\frac{\beta}{2}-\frac{\delta}{2}\right)} \cos\left(\frac{\gamma}{2}\right) & -e^{i\left(-\frac{\beta}{2}+\frac{\delta}{2}\right)} \sin\left(\frac{\gamma}{2}\right) \\ e^{i\left(\frac{\beta}{2}-\frac{\delta}{2}\right)} \sin\left(\frac{\gamma}{2}\right) & e^{i\left(\frac{\beta}{2}+\frac{\delta}{2}\right)} \cos\left(\frac{\gamma}{2}\right) \end{bmatrix}. \tag{2.102}$$

where $\alpha \in [0, 2\pi)$ and $\beta, \gamma, \delta \in [0, \pi)$, i.e., the parametrization needs only four real parameters. An analogous parametrization of a unitary matrix of an arbitrary dimension can be found in appendix B of [36].

2.8 General operations on quantum systems

We discussed how the quantum system is modeled by a Hilbert space and how its state could be described as a vector representing the pure state of the system or as a density matrix. We also introduced the complete set of possible operations on the quantum system but now we collect them together. We present the operations for a bipartite states ϱ_{AB} and ψ_{AB} to avoid excessive notation, but they naturally generalize to a state with many subsystems. Having a quantum system in a possibly unknown state ϱ_{AB} or ψ_{AB} we can:

1. Perform a reversible transformation of the state of the system represented by a unitary operator U
$$\varrho'_{AB} = U\varrho_{AB}U^\dagger \qquad\qquad |\psi'\rangle_{AB} = U|\psi\rangle_{AB}. \tag{2.103}$$
2. Introduce a new subsystem, let us denote it by E, in any state
$$\varrho'_{ABE} = \varrho_{AB}\otimes|0\rangle_E\langle 0| \qquad\qquad |\psi'\rangle_{ABE} = |\psi\rangle_{AB}\otimes|0\rangle_E \tag{2.104}$$
3. Throw away a subsystem (put it in to the trash can, send it to another party or simply put it on a side as we focus on the remaining subsystems), this is done using the partial trace
$$\varrho_A = \mathrm{Tr}_B\varrho_{AB} \qquad\qquad \varrho_A = \mathrm{Tr}_B|\psi\rangle_{AB}\langle\psi| \tag{2.105}$$
4. Measure the state of the system
$$\varrho_{AB} \xrightarrow{M} \{i, p_i, \varrho_{AB}^{(i)}\} \qquad\qquad \psi_{AB} \xrightarrow{M} \{i, p_i, \psi_{AB}^{(i)}\} \tag{2.106}$$
or with the result embedded into additional result subsystem R
$$\tilde{\varrho} = \varrho\otimes|0\rangle_R\langle 0| \tag{2.107}$$
$$M(\tilde{\varrho}) = \sum_{i=0}^{k-1} p_i\,\varrho_i\otimes|i\rangle_R\langle i| = \sum_{i=0}^{k-1} P_i\varrho P_i\otimes|i\rangle_R\langle i|. \tag{2.108}$$

We already introduced all of the above operations before.

Physically realizable quantum operations If a *map* $\Lambda : B(\mathbb{C}^d) \to B(\mathbb{C}^{d'})$ which transforms a $d\times d$ matrix into a $d'\times d'$ matrix (also called a superoperator) is a physically realizable quantum operation then for every density matrix ϱ also $\Lambda(\varrho)$ is a density matrix but that is only a necessary condition but not a sufficient one. The tensor product of the maps Λ_1 and Λ_2 is defined by its action on a tensor product of states $\Lambda_1\otimes\Lambda_2(\varrho_A\otimes\varrho_B) = \Lambda_1(\varrho_A)\otimes\Lambda_2(\varrho_B)$. Each of the above four types of quantum operations are physically realizable quantum operations (where measurement is taken in its embedded version). And every physically realizable quantum operation Λ can be represented as a composition of the above four operations. We now provide two equivalent formulations of a set of all physically realizable quantum operations:

Completely Positive Trace Preserving maps A map Λ is a physically realizable quantum operation iff it is *completely positive* (CP) and *trace preserving* (TP). Where

1. A map Λ is *positive* if it preserves positivity of its argument

$$\varrho \geq 0 \;\Rightarrow\; \Lambda(\varrho) \geq 0 \tag{2.109}$$

   A map Λ is *completely positive* (CP) if the map $\Lambda \otimes I$ is a positive

$$\varrho \geq 0 \;\Rightarrow\; \Lambda \otimes I(\varrho) \geq 0 \tag{2.110}$$

   for any dimension of I where I is the identity map $I(\sigma) = \sigma$ and ϱ has a dimension appropriate to be the input of $\Lambda \otimes I$.

2. A map Λ is *trace preserving* (TP) if it satisfies

$$\mathrm{Tr}\Lambda(\varrho) = \mathrm{Tr}\varrho. \tag{2.111}$$

Transposition, let us denote it with T, is an example of a map that is positive and trace preserving but not completely positive. This feature has been used in the Peres criterion: the criterion says that $I \otimes T(\varrho)$ must be positive if ϱ is separable, and thus the reverse indicates that ϱ is entangled. In general, such maps which are positive but not completely positive are called *entanglement witnesses*. That is because for every witness map W the expression $I \otimes W(\varrho)$ is positive for all separable states and thus $I \otimes W(\varrho) < 0$ gives the evidence that ϱ is an entangled state.

Kraus operators A map Λ is a physically realizable quantum operation iff its action can be given with the so-called Kraus operators V_i

$$\Lambda(\varrho) = \sum_i V_i \varrho V_i^\dagger \tag{2.112}$$

where V_i are arbitrary operators satisfying

$$\sum_i V_i^\dagger V_i = \mathrm{I}. \tag{2.113}$$

Separable operations The particularly important subclass of physically realizable quantum operations is the set of *separable opearations* having the following form in the decomposition to Kraus operators

$$\Lambda(\varrho_{AB}) = \sum_i A_i \otimes B_i \, \varrho_{AB} \, A_i^\dagger \otimes B_i^\dagger \tag{2.114}$$

where A_i and B_i are arbitrary operators acting on subsystems A and B, respectively, and satisfing

$$\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathrm{I}. \tag{2.115}$$

Local operations and classical communication (LOCC) There is an important subclass of quantum operations called *LOCC operations* which we introduce for a bipartite state (Alice and Bob) but it can be naturally generalized for the multipartite case. Let Alice and Bob share a quantum state such that Alice has subsystem A and Bob has subsystem B of the total system AB. Now, Alice can perform every physically realizable quantum operation on her subsystem A and Bob can perform every physically realizable quantum operation on his subsystem B. The operations that Alice and Bob can perform are called *Local Operations* as each of them can perform quantum operations only in her/his own laboratory. As Alice and Bob may perform local measurement it is often desirable to inform the other party what was the result of the measurement, thus we allow Alice and Bob for *Classical Communication*, i.e., they are allowed to send bits in both ways (from Alice to Bob and from Bob to Alice).

In contrast, if Alice and Bob have access to the reliable quantum channel then they can perform any *global operation*, i.e., operation on the total system. As Alice may send her subsystem A to Bob then Bob can perform any physically realizable quantum operation on the total system AB and send subsystem A back to Alice.

It is easy to observe that if the state ϱ shared by Alice and Bob is separable (i.e., not entangled) then the state $\Lambda(\varrho)$ after they apply any LOCC operation Λ remains separable.

2.9 Quantum channel

Suppose, Alice has a quantum system in an unknown to her state ϱ and she wants to send this state to Bob. She can do this if they are connected with a quantum channel that can *reliably* transmit qubits from Alice to Bob. See figure 2.1. The figure illustrates that the the quantum channel is only sending the state and not coping it — the state is no longer on the sender side.

A reliable quantum channel could for example be used to perform a global operation: Alice can send her subsystem to Bob then Bob having both subsystems can perform some quantum operation on the total system and send Alice's subsystem back after the operation. So the quantum channel is a powerful quantum resource.

The quantum channel which reliably transmits a state is an ideal one and, in general, a quantum channel is not perfect. Every quantum channel can be represented as a physically realizable quantum operation Λ which transforms the input state ϱ into the output state ϱ', i.e., Λ is a completely positive trace preserving map and can be represented with the Kraus operators.

But there is another representation which nicely encodes the essence of a quantum channel: the transmitted state ϱ enters into the channel where it is interacting with a environment (a new subsystem E), the interaction can be represented as a unitary operator on a total system of ϱ and the environment. But the environment is out of control of the receiver so to obtain the output

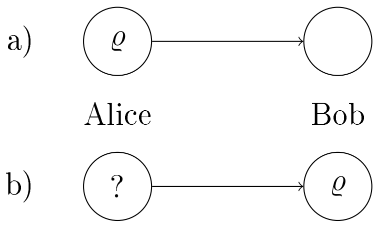

Figure 2.1: Single use of a reliable quantum channel: a) before sending a qubit; b) after sending a qubit (Alice's subsystem is in a state unrelated to ϱ).

state we have to trace out the environment. Thus

$$\Lambda(\varrho) = \mathrm{Tr}_E\, U\, \varrho \otimes |0\rangle_E\langle 0|\, U^\dagger. \tag{2.116}$$

2.10 Entropic functions

We recall that the *binary entropy* is given by

$$h(p) \equiv -p\log_2 p - (1-p)\log_2(1-p) \tag{2.117}$$

The *von Neumann entropy* of a density matrix is given by

$$S(\varrho) \equiv -\mathrm{Tr}(\varrho \log_2 \varrho) \tag{2.118}$$

where expression $\varrho\log_2\varrho$ is applied to eigenvalues, i.e., eigenvalues of $\varrho\log_2\varrho$ are equal to $\lambda_i\log_2\lambda_i$ where λ_i are the eigenvalues of ϱ. So we have

$$S(\varrho) = -\sum \lambda_i \log_2 \lambda_i. \tag{2.119}$$

Now, the *mutual information* of ϱ in A versus B cut is given by

$$I(A:B) \equiv S(\varrho_A) + S(\varrho_B) - S(\varrho_{AB}). \tag{2.120}$$

2.11 Distillation of entanglement

Distillation, in general, is a process in which an imperfect resource is transformed into a perfect resource or a resource that is arbitrary close to the perfect one. *Distillation of entanglement* is a process of obtaining perfect entanglement (maximally entangled states; singlets) from many copies of a given entangled state ϱ, i.e., from $\varrho^{\otimes n}$ for some finite n.

But why maximally entangled states are considered an important resource? The importance of distillation of entanglement follows from the tasks, such as teleportation of an unknown state [19], which are possible for two distant parties if they share maximally entangled states (a universal and powerful resource). On the other hand the uncontrolled interaction with environment may weaken the entanglement of the states shared by the parties (a destructive power of noise) and thus requiring distillation.

Distillation The process of distillation can be illustrated with

$$\varrho^{\otimes k} \xrightarrow{p>0} \psi_+. \tag{2.121}$$

That is: the state ϱ is distillable if for some finite k Alice and Bob can by LOCC operations obtain from k copies of ϱ a maximally entangled state ψ_+ with nonzero probability $p > 0$.

More formally, a state ϱ is *n-copy distillable* iff n copies of ϱ can be locally projected to obtain a two-qubit NPT state, i.e.,

$$\varrho_2 = \frac{1}{N} P_A \otimes P_B \, \varrho^{\otimes n} \, P_A \otimes P_B \tag{2.122}$$

where ϱ_2 is a two-qubit state satisfying $\varrho_2^\Gamma \ngeq 0$, N is a normalization factor, and P_A and P_B are rank two projectors. The obtained two-qubit NPT state is distillable to a maximally entangled state ψ_+ (see below). Or equivalently, a state ϱ is *n-copy distillable* iff

$$\inf_{\phi_2} \langle \phi_2 | \varrho^{\Gamma \otimes n} | \phi_2 \rangle < 0 \tag{2.123}$$

where the infimum is taken over all pure states with Schmidt rank two in Alice versus Bob cut.

Now, we say that a state ϱ is *distillable* if it is n-distillable for some finite n.

History The distillation of entanglement was pioneered in 1995 by Sandu Popescu [16]. Popescu showed that some Werner states which does not violate the CHSH [17] Bell inequality and so are far away from maximally entangled states can be with some non-zero probability transformed into states that are highly entangled, close to maximally entangled state and violating the CHSH inequality in a great degree. In the following year 1996, a protocol for distillation of entanglement from two-qubit states have been proposed by Charles Bennett and coworkers [18]. The protocol can distill nearly perfect singlets from many copies of a two-qubit state if its fidelity with singlet is greater than $\frac{1}{2}$.

If maximally entangled states consist a valuable resource then the important question is whether all entangled states are distillable? The case of pure states have been solved in 1996 by Charles Bennett and coworkers [20]: all entangled pure states can be distilled to maximally entangled states. But is the same true for all entangled density matrices? In 1997 Horodeckis [21] obtained a positive answer for the special case of two-qubit states: all entangled two-qubit states are distillable.

But in 1998 it was shown [4] that for the general case the answer is: no. They showed that an entangled state to be distillable must violate the *Peres criterion* (a necessary condition for a mixed state to be separable – i.e., not entangled [15] – the criterion was introduced in 1996 by Asher Peres [22]) and on the other hand they recalled examples of entangled states satisfying Peres criterion introduced a year before by Paweł Horodecki [23]. In this way they showed that there are entangled states which are undistillable and they called them *bound entangled states*, in analogy to bound energy from thermodynamics. We can restate the result obtained in [4] in other words: PPT entangled states exist and although entangled they are not distillable. (As separable/LOCC operations cannot transform PPT state into an NPT state). This reformulation revels a problem still opened since [4]: whether all NPT states are distillable or whether there also exist NPT bound entangled states?

In [5] it was shown that if there exist NPT bound entangled states then there must exist NPT bound entangled Werner states so it is enough to consider distillability of Werner states. In two chapters concerning distillability of NPT states we will concentrate on the problem of distillability of Werner states. In [7, 8] (David P. DiVincenzo and coworkers; W. Dür and coworkers) subsets of n-copy undistillable Werner states was given for any finite n. Those subsets are decreasing with n and in the limit of $n \to \infty$ one obtains the empty set. One could ask if proving n-copy undistillability for some n can imply $n+1$ undistillability? Unfortunately it is not the case: John Watrous [37] showed that for any n one can construct n-copy undistillable state which is $n+1$ distillable.

One can attack the problem of distillability of NPT states by allowing Alice and Bob to use a superclass of LOCC operations which simplifies mathematical consideration. If some NPT state is undistillable by this superclass it is also undistillable by LOCC operations. Such attempt was made by Tilo Eggeling and coworkers in [38] where PPT preserving class of operations where used: unfortunately all NPT states are distillable by PPT preserving operations so this class of operations is to powerful. In chapter 5 we consider other superclasses of LOCC operations called k-extendible maps. Although the k-extendible maps appear to be surprisingly powerful but the so far obtained results are not conclusive.

Consequences If all NPT states would be distillable we would have a mathematically simple method of deciding if a state is distillable: one would consider positivity of partial transposition: if it is positive (the state is PPT) then the state is undistillable and if it was negative (for NPT states) the state would be distillable.

On the other hand, if there are NPT bound entangled states several consequences have been discovered. Peter W. Shor and coworkers showed [39] a surprising consequence: for some hypothetical bound entangled NPT state ϱ there exists another bound entangled state σ such that the joint state $\varrho \otimes \sigma$ is no longer a bound entangled state. Later, Vollbrecht and Wolf showed [40] that an arbitrary NPT bound entangled state would exhibit such a property (it also follows from [38] via so-called Choi-Jamiołkowski isomorphism). Such a phenomenon of 'superactivation' has been indeed found in a multipartite case [41] and translated into extreme nonadditivity of multipartite quantum channel capacities [42]. (In a multipartite case, though still very strange, it is less surprising than in a bipartite case due to a rich state structure allowed by many possible splits between the parties.) In quantum communication language the phenomenon of 'superactivation' would mean that two channels (supported by

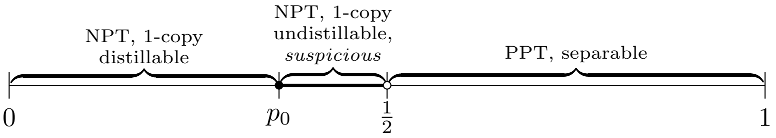

Figure 2.2: Distillability ranges for Werner states

two-way classical communication) none of them separately can convey quantum information if put together, can be used for reliable transmission of qubits. Analogous problem for channels that are not supported by classical communication was solved by Smith and Yard [43] (see also [44] in this context). Another implication of the existence of NPT bound entangled states is that the basic measure of entanglement — the *distillable entanglement* — would be non-convex.

Werner states For a single parameter class of Werner states introduced in section 2.5.4 we have three ranges of the parameter p concerning distillability (see figure 2.2):

1. for $p \in [\frac{1}{2}, 1]$ the Werner states are separable (and thus PPT),
2. for $p \in [0, p_0)$ where $p_0 = \frac{d+1}{4d-2}$ the Werner states are NPT 1-copy distillable,
3. for $p \in [p_0, \frac{1}{2})$ the Werner states are NPT 1-copy undistillable and conjectured to be undistillable [7, 8] (We will call them the *suspicious* Werner states).

2.12 Quantum cryptography

Quantum cryptography is one of the most widely recognized practical application of quantum information. Commercial solutions are sold by for example ID Quantique[1] and MagiQ Technologies[2]. The widely used in practice part of the quantum cryptography is the *Quantum Key Distribution* (QKD). The Quantum Key Distribution does not introduce new cryptographic algorithms but new protocols of distributing private keys. In practical cryptography one usually uses a symmetric-key algorithm such as for example Triple DES (3DES) to encrypt the data but the private key used is changed frequently. For distributing new keys public-key cryptography, such algorithms as RSA (which stands for the authors Rivest, Shamir and Adleman), are frequently used in practice. Now, Quantum Key Distribution gives a new way of distributing those frequently changed keys (first such commercial hybrid systems have been produced in collaboration by Senetas[3] and ID Quantique). Security of classical algorithms such as RSA is

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

based on difficulty of solving computationally hard (or supposedly hard) mathematical problems (such as factorization): that is their security is based on *practical* impossibility of solving those mathematical problems even using a cluster of many today's computers in a reasonable time. In contrast, QKD protocols are based on *physical* impossibility of eavesdropping: due to the impossibility of cloning of quantum states any attempt of reading the states introduces the noise and Alice and Bob — the parties that want to communicate secretly — can measure the level of noise and learn whether the keys generated by the quantum apparatus are secure. One should add that the current implementations are not free from loopholes, see [45].

There are two kinds of QKD protocols:

1. algorithms based on sending non-orthogonal quantum states by Alice and their measurements by Bob, so-called *prepare and measure* protocols, the original BB84 algorithm [25] is of this kind, and

2. algorithms based on measurements of shared orthogonal states, such as Ekert protocol [26].

For quite a time security proofs of prepare and measure protocols had been based on showing the equivalence of the prepare and measure protocol of interest with entanglement distillation, i.e., distillation of maximally entangled states (first such proof is due to Peter Shor and John Preskill [27]). Thus it was quite widely believed that this equivalence is essential to the problem of distillation of private key from quantum states, this was probably first touched by Nicolas Gisin and Stefan Wolf [28]. If this belief was true then one could not obtain secure key from bound entangled states. But the opposite was shown: new class of so-called *private states* [1, 30] have been introduced and it was shown that distillation of private key from quantum states is not equivalent to distillation of entanglement but is a generalization of distillation of entanglement. It was shown that distillation of private key from quantum states is equivalent to distillation of private states. And maximally entangled states belong to the set of private states but there are many other private states and some of them (if a large enough dimension is considered) are close to the set of bound entangled PPT states and thus by introducing some noise to such states one can obtain key-distillable bound entangled states.

The method of obtaining bound entangled states from which one can distill cryptographic key introduced in [1] and widely explained in [30] was only applicable for high dimensional states. Later, a method based on mixing of two specially chosen orthogonal private states was introduced in [2] this construction is possible in low dimensions even for $4 \otimes 4$ states, i.e., Alice has a two-qubit subsystem and Bob has a two-qubit subsystem. The construction gives the states on the boundary of the set of PPT states but by continuity it was argued that there are also key-distillable states inside the set of PPT entangled states.

The method used in [2] have been generalized to mixtures of four specially chosen orthogonal private states [3]. Those generalized states are also laying inside the set of the PPT states even approaching arbitrary close to the set of separable states. But this generalization comes with a price: in [2] the so-called Devetak-Winter protocol [46] (which requires only one-way communication) was enough to obtain private key from the states on the boundary of the PPT states while to enter far into the set of PPT states [3] one has to use the so-called recurrence preprocessing before applying the Devetak-Winter protocol. The use of the recurrence preprocessing causes the decrease of the key rate.

The results obtained in [2] and [3] are introduced in the next chapter but to this end we need to introduce *private bits* an important subclass of the set of private states and the technique called privacy squeezing.

2.13 Private bits and privacy squeezing

First we have to specify what do we understand by the *private key*. A private key is

1. a perfectly random string of bits, i.e., the bits are independent and zeros and ones are equally probable, and such that
2. nobody else knows this random string of bits apart from the securely communicating parties called Alice and Bob, i.e., it is perfectly secure.

Private key from maximally entangled states One can obtain a single bit of private key from a maximally entangled state

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{2.124}$$

Suppose Alice and Bob share the state ϕ_+. They can both measure their subsystems in the standard basis or any other basis (but the same for Alice and Bob) and then they obtain one bit of private key: they both get the same result, zero with probability $\frac{1}{2}$ or one with probability $\frac{1}{2}$. The result is decided when first of them measures her/his subsystem and it is secret, i.e., unknown to anyone other than Alice and Bob. The private key from ϕ_+ is obtained *directly*, i.e., Alice and Bob measure a single copy of ϕ_+ and obtain a bit of private key — no postprocessing is required. Thus if one can show that some QKD protocol is equivalent to distillation of maximally entangled states and measurements on those states, such as the proof by Shor and Preskill [27], then the QKD protocol is secure. Alice and Bob could also share a state

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{2.125}$$

that has anti-correlation or anty-key: for this maximally entangled state they obtain opposite results and one of them have to negate the result.

But in [1] a wider class of states, called *private states*, have been introduced from which one can directly obtain private key. Private states are simply all of the states from which one can by direct measurement obtain private key. This class is a generalization of the class of maximally entangled states. But in this generalized class of private states there is a single basis called the *secure basis* in which Alice and Bob have to measure to obtain the private key while other basis do not guarantee security. In contrast, for the maximally entangled state[4] every local basis (but the same for Alice and Bob) is secure. In this thesis we will always use the standard basis as the secure basis of private states as this simplifies the consideration. And we also consider only a subclass of private states called *private bits*.

Private bit A *private bit* or *pbit* is a state from which one can directly obtain at least one bit of private key. The private bit in its so-called *X-form* is given by

$$\gamma(X) = \frac{1}{2}\begin{bmatrix} \sqrt{XX^\dagger} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \sqrt{X^\dagger X} \end{bmatrix} \tag{2.126}$$

where X is an arbitrary operator satisfying $\|X\| = 1$. The private bit has four subsystems: $ABA'B'$ where block matrix (2.126) represents AB subsystem and the blocks are operators acting on an $A'B'$ subsystem. Subsystems A and B are single qubit subsystems while dimensions of A' and B' must be greater or equal to 2, we assume dimensions A' and B' are equal and denote them by d. Subsystem AA' belongs to Alice while subsystem BB' belongs to Bob. The lowest dimension of the pbit is $4 \otimes 4$, i.e., all four subsystems are qubits. All of the states presented in block matrix form and in the context of quantum cryptography will have this structure. For the private bit given by (2.126) Alice and Bob may obtain single bit of private key when they measure subsystems A and B in the standard basis [5] (i.e., standard basis is the secure basis). Therefore, subsystem AB is called the *key part* of the pbit, while subsystem $A'B'$ is called the *shield* of the pbit, as it protects correlations contained in the key part from an eavesdropper. These names (the key part and the shield) apply not only to pbits but also to mixtures of pbits and general states having $ABA'B'$ subsystems. Note that it may happen that Eve (a canonical name of an eavesdropper) possesses a copy of the shield subsystem (when, e.g., the shield consists of two flag states — states with disjoint support) yet it does not compromise the security of the key because the very presence of the shield subsystem in Alice's and Bob's hands protects the bit of key from an eavesdropper.

Privacy squeezing From private bits one can obtain private key by direct measurement in the secure basis. In contrast, for a general state ϱ with $ABA'B'$

[4] Each maximally entangled state may be transformed by a local unitary on either Alice or Bob site to the maximally entangled state given by (2.26).

[5] One can also consider private bits with different secure basis but in this thesis we only consider the standard basis as secure basis.

subsystems one may obtain imperfect secret correlations which are typically neither perfectly random nor perfectly secure. Such imperfect secret correlations require distillation of the private key — classical postprocessing to improve both randomness and security (so called privacy amplification). This means that one needs many copies of the state ϱ, i.e., $\varrho^{\otimes n}$, and the amount of distillable private key $K_D(\varrho)$ per copy of the state and measured in bits, if nonzero, is often less than one. We use $K^{\mathcal{P}}(\varrho)$ to denote the amount of private key-distillable from ϱ by the protocols consisting of a measurement of the key part in the standard basis followed by classical postprocessing — the recurrence followed by Devetak-Winter protocol (cf. [47] for two-qubit states). In the consideration below in this section one can replace $\mathcal{P}$ with DW to restrict the classical postprocessing to using of sole Devetak-Winter protocol without the recurrence and all of the results will still hold.

Given a general state ϱ with $ABA'B'$ subsystems one can lower bound the amount of the private key $K^{\mathcal{P}}(\varrho)$ distillable from ϱ using the method called the *privacy squeezing* [30] (analogously for $K^{DW}(\varrho)$). The essence of privacy squeezing is that instead of considering the original state ϱ we can consider a much simpler object — a two-qubit state σ — called the *privacy-squeezed state* of the original state ϱ. Where the states ϱ and σ are connected with the following relation [6]

$$K^{\mathcal{P}}(\varrho) \geq K^{\mathcal{P}}(\sigma). \tag{2.127}$$

That is one can use protocols designed for two-qubit states (see e.g., [48, 47, 49]) to compute the amount of key-distillable from the privacy-squeezed state σ and then at least the same amount of private key is distillable from the original state ϱ by the same set of considered protocols ($\mathcal{P}$ or DW).

The privacy squeezing method can be used for any *spider state*, i.e., a state of the form

$$\varrho = \begin{bmatrix} C & \cdot & \cdot & D \\ \cdot & E & F & \cdot \\ \cdot & F^\dagger & E' & \cdot \\ D^\dagger & \cdot & \cdot & C' \end{bmatrix} \tag{2.128}$$

(where zero blocks have been marked with dots). And the two-qubit privacy-squeezed state of the spider state has the form

$$\sigma = \begin{bmatrix} \|C\| & \cdot & \cdot & \|D\| \\ \cdot & \|E\| & \|F\| & \cdot \\ \cdot & \|F\| & \|E'\| & \cdot \\ \|D\| & \cdot & \cdot & \|C'\| \end{bmatrix}. \tag{2.129}$$

If a spider state satisfies $\|C\| = \|C'\|$ and $\|E\| = \|E'\|$ then its privacy-squeezed state is a Bell diagonal state.

[6] Actually, it is true for any protocol based on postprocessing of classical data obtained from measurement in the basis in which the privacy-squeezing is performed.

Before we explain why the privacy squeezing works we have to introduce an important ingredient of the proof: a *twisting* operation, i.e., a unitary transformation of the following form

$$U = \sum_{ij} |ij\rangle_{AB}\langle ij| \otimes U_{ij}^{A'B'} \tag{2.130}$$

Twisting is a global operation and it is never performed by Alice and Bob but it is an important ingredient of the proof. Its usefulness comes from the property that

$$K^{\mathcal{P}}(\varrho) = K^{\mathcal{P}}(U\varrho U^\dagger). \tag{2.131}$$

i.e., twisting does not change the amount of key one can obtain from the state using $\mathcal{P}$ protocols.

Now, given a spider state ϱ defined by (2.128) privacy squeezing consists of the two steps:

1. One selects such a twisting operation U which transforms off diagonal blocks D and F of ϱ into positive operators $U_{00}DU_{11}$ and $U_{01}FU_{10}$. So in $U\varrho U^\dagger$ all blocks are positive operators as diagonal blocks in a density matrix are positive and stay positive after unitary transformation.

2. Now, we trace out $A'B'$ subsystem to obtain the privacy squeezed state

$$\sigma = \mathrm{Tr}_{A'B'} U\varrho U^\dagger \tag{2.132}$$

tracing out $A'B'$ subsystem replaces each of the block A_{ij} of $U\varrho U^\dagger$ with its trace $\mathrm{Tr}A_{ij}$ in (2.132) but as all of the blocks are positive and for a positive operator A we have $\mathrm{Tr}A = \|A\|$ thus finally the privacy squeezed state has the form (2.129).

The twisting does not change $K^{\mathcal{P}}$ and tracing out $A'B'$ which is equivalent to giving it to Eve may only decrease $K^{\mathcal{P}}$ so we have

$$K^{\mathcal{P}}(\varrho) = K^{\mathcal{P}}(U\varrho U^\dagger) \geq K^{\mathcal{P}}(\mathrm{Tr}_{A'B'} U\varrho U^\dagger) = K^{\mathcal{P}}(\sigma) \tag{2.133}$$

and so one can distill from the original state ϱ at least as much key using protocols $\mathcal{P}$ as one can obtain from the privacy-squeezed state σ. Thus one can say that one *squeezes* the private key in some sense spread between the key part and the shield of ϱ into the key part of $U\varrho U^\dagger$ and thus effectively into σ (as σ is just like $U\varrho U^\dagger$ but with the probably useless shield $A'B'$ given to Eve).

Twisting explained But why twisting does not change $K^{\mathcal{P}}$? Having a state ϱ with subsystems $ABA'B'$ we consider its so-called *purification* that is a pure state $\psi_{ABA'B'E}$ such that

$$\mathrm{Tr}_E|\psi_{ABA'B'E}\rangle\langle\psi_{ABA'B'E}| = \varrho. \tag{2.134}$$

The purification is not unique but different purifications differ only by a local unitary on E subsystem which is irrelevant in our consideration. We called the introduced subsystem E: it could simply denote the environment but in the context of quantum cryptography it stands for Eve as we suppose the worst case scenario that whole environment (i.e., what is not controlled by Alice and Bob) is controlled by the eavesdropper Eve. Now in the protocols $\mathcal{P}$ we measure subsystems A and B in the standard basis and disregard the shield (but we do not give it to Eve) and consider a state ϱ'_{ABE} which is called a *ccq* state as after the measurement both A and B are classical registers and only Eve holds a quantum system, one of the states ϱ_{ij} where i and j are the results of the measurements. Now, in protocol of the class $\mathcal{P}$ one extracts private key from the *ccq* state and twisting does not change the *ccq* state so it also does not change $K^{\mathcal{P}}$.

From a *ccq* state ϱ'_{ABE} Alice and Bob can distill using the (one-way) Devetak-Winter protocol the following amount of key

$$K^{DW}(\varrho'_{ABE}) = I(A:B) - I(A:E) \tag{2.135}$$

where $I(X:Y)$ is the mutual entropy in X versus Y cut.

For a deeper discussion of the privacy squeezing see [30], although the name *spider state* is not used there.

Chapter 3

Private key from PPT states

In this chapter by mixing properly chosen private bits we obtain key-distillable states which are bound entangled and may even lay arbitrary close to the set of separable states. We also provide sufficient condition to obtain private key from such mixtures and further generalize the condition for arbitrary states.

The results presented in this chapter have been published in [2][1] and [3].

3.1 Mixing two private bits

Let us consider mixtures of two orthogonal private bits

$$\tilde{\varrho} = \lambda_1 \gamma_1^+ + (1-\lambda_1)\gamma_2^+ \tag{3.1}$$

where

$$\gamma_1^+ = \gamma(X) \qquad \gamma_2^+ = \sigma_x^A \gamma(Y) \sigma_x^A \tag{3.2}$$

i.e., γ_1^+ is a pbit that has a key and γ_2^+ is a pbit having an antikey (as we applied σ_x on subsystem A) and operators X and Y are defined on $d \otimes d$ Hilbert space and has the form

$$X = \frac{1}{u}\sum_{i,j=0}^{d-1} u_{ij}|ij\rangle\langle ji| \qquad Y = \frac{X^\Gamma}{\|X^\Gamma\|} \tag{3.3}$$

where u_{ij} are elements of some unitary matrix on $\mathbb{C}^d$ and

$$u = \sum_{i,j=0}^{d-1} |u_{ij}|. \tag{3.4}$$

The states $\tilde{\varrho}$ have the following block diagonal form

$$\tilde{\varrho} = \frac{1}{2}\begin{bmatrix} \lambda_1\sqrt{XX^\dagger} & \cdot & \cdot & \lambda_1 X \\ \cdot & (1-\lambda_1)\sqrt{YY^\dagger} & (1-\lambda_1)Y & \cdot \\ \cdot & (1-\lambda_1)Y^\dagger & (1-\lambda_1)\sqrt{Y^\dagger Y} & \cdot \\ \lambda_1 X^\dagger & \cdot & \cdot & \lambda_1\sqrt{X^\dagger X} \end{bmatrix}. \tag{3.5}$$

[1] The class obtained in [2] was also presented in [50].

Private key from privacy-squeezed state The privacy-squeezed state of $\tilde{\varrho}$ is a Bell diagonal state of the form

$$\tilde{\sigma} = \lambda_1 |\psi_1\rangle\langle\psi_1| + (1-\lambda_1)|\psi_3\rangle\langle\psi_3| \tag{3.6}$$

where ψ_i are the Bell states given by (2.25) and coefficients λ_1 and $1-\lambda_1$ are the eigenvalues of the privacy-squeezed state. The purification of privacy-squeezed state has the form

$$|\psi'_{ABE}\rangle = \sqrt{\lambda_1}|\psi_1\rangle_{AB}|e_1\rangle_E + \sqrt{1-\lambda_1}|\psi_3\rangle_{AB}|e_3\rangle_E \tag{3.7}$$

Now, suppose Alice, Bob and Eve share the state ψ'_{ABE} (i.e., we assume the worst case scenario — Eve controls the whole environment). And Alice and Bob want to know how much private key K^{DW} they can distill from ψ'_{ABE}. They measure the state ψ'_{ABE} in the standard basis and obtain a *ccq* state of the form

$$\sigma_{ABE}^{(ccq)} = \frac{\lambda_1}{2}[P_{|00\rangle} + P_{|11\rangle}] \otimes P_{e_1} + \frac{1-\lambda_1}{2}[P_{|01\rangle} + P_{|10\rangle}] \otimes P_{e_3} \tag{3.8}$$

where $P_\psi = |\psi\rangle\langle\psi|$.

We apply the formula (2.135) to obtain the amount of private key Alice and Bob can distill using Devetak-Winter protocol

$$K^{DW}(\sigma_{ABE}^{(ccq)}) = I(A:B) - I(A:E) = 1 - h(\lambda_1) \tag{3.9}$$

where $I(X:Y)$ stands for the mutual information in X versus Y cut and h for the binary entropy.

Private key from a bound entangled states Thus by privacy squeezing we obtain that from the original state $\tilde{\varrho}$, using the Devetak-Winter protocol, one can distill

$$K^{DW}(\tilde{\varrho}) = 1 - h(\lambda_1) \tag{3.10}$$

of the private key.

Now, if λ_1 is equal to

$$\lambda_1 = \tilde{\lambda}_1 \equiv \frac{1}{1+\|X^\Gamma\|}. \tag{3.11}$$

then the state $\tilde{\varrho}$ is a PPT-invariant state (laying on the boundary of the set of PPT states) and hence $\tilde{\varrho}$ is bound entangled.

One can argue by continuity of distillable key K_D that if there are key-distillable states on the boundary of the set of PPT states then there also have to be key-distillable states inside the set of PPT states.

To maximize K^{DW} obtained from the PPT-invariant state for a given dimension d of subsystems A' and B' one has to use in (3.3) a unimodular unitary[2],

[2] By use of Lagrange multipliers with slightly more general constraints $\sum_{ij}|u_{ij}|^2 = d$ one gets that optimal U is unimodular.

i.e., a unitary having all of the elements satisfying

$$|u_{ij}| = \frac{1}{\sqrt{d}} \tag{3.12}$$

which gives

$$\|X^\Gamma\| = \frac{1}{\sqrt{d}}. \tag{3.13}$$

In particular, for dimension $d = 2^k$ the unimodular unitary has the form $U = H^{\otimes k}$ (H is the Hadamard gate). And in the case of $d = 2$ we have $U = H$ and denote the PPT-invariant state with $\tilde{\varrho}_H$. From $\tilde{\varrho}_H$ we can distill

$$K^{DW}(\tilde{\varrho}_H) = 0.0213399 \tag{3.14}$$

of the private key and the density matrix $\tilde{\varrho}_H$ has the form

$$\tilde{\varrho}_H = \left[\begin{array}{cccc|cccc|cccc|cccc}
s & \cdot & \cdot & \cdot & & & & & & & & & s & \cdot & \cdot & \cdot \\
\cdot & s & \cdot & \cdot & & & & & & & & & \cdot & \cdot & s & \cdot \\
\cdot & \cdot & s & \cdot & & & & & & & & & \cdot & s & \cdot & \cdot \\
\cdot & \cdot & \cdot & s & & & & & & & & & \cdot & \cdot & \cdot & -s \\
\hline
& & & & t & \cdot & \cdot & \cdot & s & \cdot & \cdot & s & & & & \\
& & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & \\
& & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & \\
& & & & \cdot & \cdot & \cdot & t & s & \cdot & \cdot & -s & & & & \\
\hline
& & & & s & \cdot & \cdot & s & t & \cdot & \cdot & \cdot & & & & \\
& & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & \\
& & & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & & & \\
& & & & s & \cdot & \cdot & -s & \cdot & \cdot & \cdot & t & & & & \\
\hline
s & \cdot & \cdot & \cdot & & & & & & & & & s & \cdot & \cdot & \cdot \\
\cdot & \cdot & s & \cdot & & & & & & & & & \cdot & s & \cdot & \cdot \\
\cdot & s & \cdot & \cdot & & & & & & & & & \cdot & \cdot & s & \cdot \\
\cdot & \cdot & \cdot & -s & & & & & & & & & \cdot & \cdot & \cdot & s
\end{array}\right] \tag{3.15}$$

where

$$s = \frac{\sqrt{2}}{8(1+\sqrt{2})} \approx 0.07 \qquad t = \frac{1}{4(1+\sqrt{2})} \approx 0.10 \tag{3.16}$$

While by the Devetak-Winter protocol we can distill approximately 0.02 bits of private key from $\tilde{\varrho}_H$ the best known upper bound so far is approximately 0.116. This comes from relative entropy of entanglement E_r being the upper bound for distillable key K_D and we can obtain

$$K_D(\tilde{\varrho}_H) \le E_r(\tilde{\varrho}_H) < 0.116. \tag{3.17}$$

This upper bound for E_r can be obtained by considering a separable state of the same form as $\tilde{\varrho}_H$ but having

$$s = \frac{1}{16} \qquad t = \frac{1}{8}. \tag{3.18}$$

Recurrence It has been shown that using the recurrence does not increase the amount of the private key that can be distilled from the PPT-invariant states considered in this section. But it increases the robustness of the state against the noise which we will show further in this chapter.

3.2 Mixing four private bits: class $\mathcal{C}$

Let us define the class $\mathcal{C}$ to denote the class of states satisfying three conditions:

1. A state of the class $\mathcal{C}$ is a mixture of four orthogonal private bits
$$\varrho = \lambda_1\gamma_1^+ + \lambda_2\gamma_1^- + \lambda_3\gamma_2^+ + \lambda_4\gamma_2^- \tag{3.19}$$
where the private bits are given by
$$\gamma_1^\pm = \gamma(\pm X) \qquad \gamma_2^\pm = \sigma_x^A\gamma(\pm Y)\sigma_x^A. \tag{3.20}$$

2. The operators X and Y are related by
$$Y = \frac{X^\Gamma}{\|X^\Gamma\|} \tag{3.21}$$
and, by definition of the pbit, they are normalized, i.e., $\|X\| = 1$ and $\|Y\| = 1$.

3. The operators X and Y must be such that operators $\sqrt{XX^\dagger}$, $\sqrt{X^\dagger X}$, $\sqrt{YY^\dagger}$, $\sqrt{Y^\dagger Y}$ are all PPT-invariant, i.e., must satisfy $A = A^\Gamma$.

States of the class $\mathcal{C}$ have the following block matrix form
$$\varrho = \frac{1}{2}\begin{bmatrix} (\lambda_1+\lambda_2)\sqrt{XX^\dagger} & \cdot & \cdot & (\lambda_1-\lambda_2)X \\ \cdot & (\lambda_3+\lambda_4)\sqrt{YY^\dagger} & (\lambda_3-\lambda_4)Y & \cdot \\ \cdot & (\lambda_3-\lambda_4)Y^\dagger & (\lambda_3+\lambda_4)\sqrt{Y^\dagger Y} & \cdot \\ (\lambda_1-\lambda_2)X^\dagger & \cdot & \cdot & (\lambda_1+\lambda_2)\sqrt{X^\dagger X} \end{bmatrix}. \tag{3.22}$$

Alternative parametrization Instead of parameters λ_i one can also parametrize class $\mathcal{C}$ with three parameters p, α and β defined as follows
$$p \equiv \lambda_1 + \lambda_2 \in [0,1] \tag{3.23}$$
$$\alpha \equiv \frac{\lambda_1-\lambda_2}{\lambda_1+\lambda_2} \in [-1,1] \tag{3.24}$$
$$\beta \equiv \frac{\lambda_3-\lambda_4}{\lambda_3+\lambda_4} \in [-1,1]. \tag{3.25}$$

Parameter p denotes the probability of the correlation (versus anticorrelation) and α and β denote in a sense the degree of dephasing of the correlation and anticorrelation, respectively. (This can be clearly seen when we pass to privacy-squeezed state, see equation (3.32)). I.e., α and β measure security of correlation and anticorrelation (the value 1 stands for perfectly secure).

The mixtures of two private bits $\tilde{\varrho}$ considered in previous section is the subset of the class $\mathcal{C}$ satisfying $\lambda_2 = \lambda_4 = 0$ or alternatively $\alpha = \beta = 1$.

Now, the original parameters λ_i may be expressed in terms of parameters p, α and β as
$$\lambda_{1,2} = \frac{1\pm\alpha}{2}p \qquad \lambda_{3,4} = \frac{1\pm\beta}{2}(1-p). \tag{3.26}$$

PPT conditions The items 2 and 3 of the definition of the class $\mathcal{C}$ allows us to define simple PPT conditions. If a state from the class $\mathcal{C}$ satisfies

$$|\lambda_1 - \lambda_2| \leq (1 - \lambda_1 - \lambda_2) \|X^\Gamma\|^{-1} \tag{3.27}$$

$$|\lambda_3 - \lambda_4| \leq (\lambda_1 + \lambda_2) \|X^\Gamma\| \tag{3.28}$$

or equivalently

$$|\alpha| \leq \min(1, \alpha_1) \tag{3.29}$$

$$|\beta| \leq \min(1, \alpha_1^{-1}) \tag{3.30}$$

where

$$\alpha_1 = \frac{1-p}{p} \|X^\Gamma\|^{-1}. \tag{3.31}$$

then the state is a PPT state.

Privacy squeezing The privacy-squeezed state of a state of the class $\mathcal{C}$ has the form

$$\sigma = \sum_{i=1}^{4} \lambda_i |\psi_i\rangle\langle\psi_i| = \frac{1}{2} \begin{bmatrix} p & \cdot & \cdot & \alpha p \\ \cdot & (1-p) & \beta(1-p) & \cdot \\ \cdot & \beta(1-p) & (1-p) & \cdot \\ \alpha p & \cdot & \cdot & p \end{bmatrix} \tag{3.32}$$

where ψ_i are Bell states given by (2.25). Thus the privacy-squeezed state is a Bell diagonal state and parameters λ_i are simply the eigenvalues of the privacy-squeezed state that is why we have chosen to denote them with the Greek letter λ.

Operators X and Y In particular, the PPT-invariance of the diagonal blocks (item 3 of the definition of the class $\mathcal{C}$) holds for

$$X = \frac{1}{u} \sum_{i,j=0}^{d-1} u_{ij} |ij\rangle\langle ji| \tag{3.33}$$

where u_{ij} are elements of some unitary matrix on $\mathbb{C}^d$ and

$$u = \sum_{i,j=0}^{d-1} |u_{ij}|. \tag{3.34}$$

For the operator X given by (3.33) we have

$$\|X^\Gamma\| = \frac{d}{u}, \qquad \frac{1}{\sqrt{d}} \leq \|X^\Gamma\| \leq 1 \tag{3.35}$$

where the minimum is achieved for the unimodular unitary [2] and maximum for the identity matrix.

In case of $d = 2$ we will also consider the subclass of the class $\mathcal{C}$ with operators X and Y given by

$$Y = q\, Y_{U_1} + (1-q)\, \sigma_x^{A'} Y_{U_2} \sigma_x^{A'}, \quad X = \frac{Y^\Gamma}{\|Y^\Gamma\|} \tag{3.36}$$

where $0 \leq q \leq 1$ and

$$Y_U = \frac{1}{d} \sum_{i,j=0}^{d-1} u_{ij} |ii\rangle\langle jj|. \tag{3.37}$$

Unitaries U_1 and U_2 must have the same global phase, i.e., $\alpha_1 = \alpha_2$ in the parametrization of a single qubit unitary given by (2.102). In particular, one may take $U_1 = U_2$.

Subclass ϱ_U We will sometimes write ϱ_U to denote the subclass of the class $\mathcal{C}$ with operator X given by (3.33) or to stress using a concrete unitary in the definition of X, in particular, we will consider the subclass ϱ_H where u_{ij} are elements of the Hadamard unitary matrix.

3.3 Distillability of private key

We now give a sufficient condition for distillability of private key from states having Bell diagonal privacy-squeezed states which in particular includes the class $\mathcal{C}$.

Lemma 3.1. *A Bell diagonal state*

$$\sigma = \sum_{i=1}^{4} \lambda_i |\psi_i\rangle\langle\psi_i| = \begin{bmatrix} c & \cdot & \cdot & d \\ \cdot & e & f & \cdot \\ \cdot & f & e & \cdot \\ d & \cdot & \cdot & c \end{bmatrix} \tag{3.38}$$

is key-distillable (i.e., one can from σ obtain nonzero amount of private key) by the measurement in the standard basis and processing of the the resulting classical data (actually, by using the recurrence followed by the Devetak-Winter protocol, i.e., $\mathcal{P}$ protocols) if and only if [47]

$$\max\{(\lambda_1 - \lambda_2)^2, (\lambda_3 - \lambda_4)^2\} > (\lambda_1 + \lambda_2)(1 - \lambda_1 - \lambda_2) \tag{3.39}$$

or equivalently if and only if

$$\max\{d^2, e^2\} > ce. \tag{3.40}$$

Let us consider a state ϱ having the Bell diagonal privacy-squeezed state σ that is a state of the form

$$\varrho = \begin{bmatrix} C & \cdot & \cdot & D \\ \cdot & E & F & \cdot \\ \cdot & F^\dagger & E' & \cdot \\ D^\dagger & \cdot & \cdot & C' \end{bmatrix} \tag{3.41}$$

and satisfying $\|C\| = \|C'\|$ and $\|E\| = \|E'\|$. Its privacy-squeezed state has the form

$$\sigma = \begin{bmatrix} \|C\| & \cdot & \cdot & \|D\| \\ \cdot & \|E\| & \|F\| & \cdot \\ \cdot & \|F\| & \|E\| & \cdot \\ \|D\| & \cdot & \cdot & \|C\| \end{bmatrix}. \tag{3.42}$$

And as σ is a Bell diagonal state using lemma 3.1 we obtain that σ is key-distillable if and only if it satisfies

$$\max\{\|D\|^2, \|F\|^2\} > \|C\| \, \|E\|. \tag{3.43}$$

Thus by the method of privacy squeezing one obtains that from the state ϱ having the Bell diagonal privacy-squeezed state σ one can obtain nonzero private key by protocols $\mathcal{P}$ if ϱ satisfies condition (3.43) (it is a sufficient but not a necessary condition).

One can observe that condition (3.43) is equivalent to having one of the following matrices nonpositive

$$\begin{bmatrix} \|C\| & \|D\| \\ \|D\| & \|E\| \end{bmatrix}, \quad \begin{bmatrix} \|C\| & \|F\| \\ \|F\| & \|E\| \end{bmatrix}. \tag{3.44}$$

One can also observe that

$$\|C\| \, \|E\| = \frac{1}{4} p_e (1 - p_e) \tag{3.45}$$

where p_e is the probability of error (i.e. anticorrelation) when the key part is measured in the standard basis.

Private key from the class $\mathcal{C}$ Thus, for a state ϱ of the class $\mathcal{C}$ due to the form (3.32) of the privacy-squeezed state and from above consideration the sufficient condition for obtaining nonzero private key by protocols $\mathcal{P}$ from ϱ has the form

$$(\lambda_1 - \lambda_2)^2 > (\lambda_1 + \lambda_2)(1 - \lambda_1 - \lambda_2) \tag{3.46}$$

or equivalently

$$\alpha^2 > \frac{1-p}{p}. \tag{3.47}$$

Actually, the above key condition holds for a wider class of states than the class $\mathcal{C}$: the class having arbitrary but normalized operators X and Y.

Now, we can observe that for a state of the class $\mathcal{C}$ to be both PPT and key-distillable it must satisfy both (3.29) and (3.47). For a given value of the parameter p there exists α satisfying both conditions iff $p \in (\frac{1}{2}, p_{\max})$ where

$$p_{\max} = \frac{1}{1 + \|X^\Gamma\|^2}. \tag{3.48}$$

Tolerable white noise Given a state ϱ having a Bell diagonal privacy-squeezed state we can ask how much white noise one can admixture to the state for the state to remain key-distillable. Such a fraction of noise, let us denote it with δ, can be seen as a simple measure of robustness of the particular QKD protocol to noise.

Having a state ϱ we define the state with ε of noise admixtured as

$$\varrho_\varepsilon = (1-\varepsilon)\varrho + \varepsilon\frac{\mathrm{I}}{d^2} \tag{3.49}$$

Now, we say that δ is the *tolerable noise* of a key distillation protocol for a state ϱ if for any $\varepsilon < \delta$ the state ϱ_ε with ε of the white noise admixtured remains key-distillable with that protocol.

Having $p > \frac{1}{2}$, the tolerable noise for protocols $\mathcal{P}$ for the class $\mathcal{C}$ is given by

$$\delta = 1 - \frac{1}{\sqrt{8(\lambda_1^2+\lambda_2^2) - 4(\lambda_1+\lambda_2)+1}} \tag{3.50}$$

$$= 1 - \frac{1}{\sqrt{4\,(1+\alpha^2)\;p^2 - 4\,p + 1}}. \tag{3.51}$$

In particular, for a key-distillable PPT state $\tilde{\varrho}_H$ with $\lambda_1 = \tilde{\lambda}_1$ where $\tilde{\lambda}_1$ is given by (3.11) the tolerable noise for the Devetak-Winter protocol with the recurrence preprocessing (3.50) is approximately equal to 0.155 while for the sole Devetak-Winter protocol it is approximately equal to 0.005 (computed numerically), i.e., it is 31 times smaller. (See figure 3.1).

3.4 Separability condition

To obtain private key from bound entangled states arbitrary close to the set of separable states we propose a separability condition for a subclass of the class $\mathcal{C}$. We present a sufficient separability condition for a state ϱ_U with $d = 2$ (i.e., for $4 \otimes 4$ states).

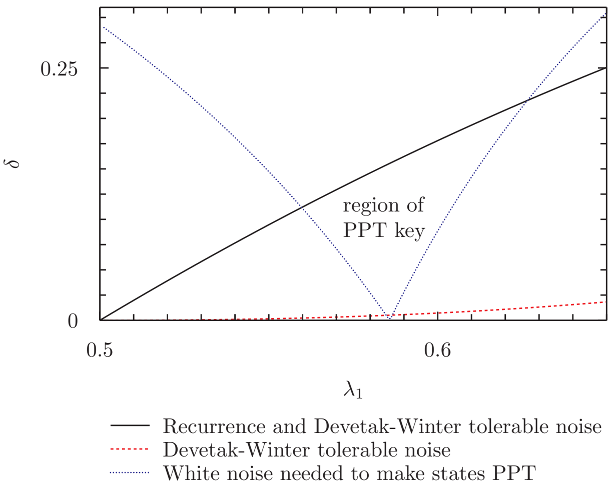

Figure 3.1: Comparison of $\tilde{\varrho}_H$ tolerable noise in case of using the Devetak-Winter protocol with and without the recurrence preprocessing.

A state ϱ_U with $d = 2$ is separable if it satisfies

$$\lambda_1 \leq \frac{1}{2} \tag{3.52}$$

$$\lambda_2 \leq \frac{1}{2} \tag{3.53}$$

$$|\lambda_3 - \lambda_4| \leq (\lambda_1 + \lambda_2)\|X^\Gamma\| \tag{3.54}$$

$$|\lambda_3 - \lambda_4| \leq (1 - \lambda_1 - \lambda_2)\|X^\Gamma\| \tag{3.55}$$

or equivalently if

$$|\alpha| \leq \frac{1-p}{p} \tag{3.56}$$

$$|\beta| \leq \frac{p}{1-p}\|X^\Gamma\| \tag{3.57}$$

$$|\beta| \leq \|X^\Gamma\|. \tag{3.58}$$

Decomposition into two-qubit states The above separability conditions come from the decomposition of ϱ_U into a mixture of four two-qubit operators ϱ_{ij}. We first demand that operators ϱ_{ij} are states (i.e., they must be positive) which is guaranteed by the condition (3.55) or equivalently (3.58). If this condition is satisfied ϱ_U is a mixture of four Bell diagonal states

$$\varrho_U = \sum_{i,j=0}^{1} \frac{|u_{ij}|}{u}\varrho_{ij}. \tag{3.59}$$

where u_{ij} are the elements of the unitary matrix on $\mathbb{C}^2$ used to define operator X in (3.33) and u is given by (3.34). All four Bell diagonal states ϱ_{ij} have the same set of eigenvalues. And a Bell diagonal state is separable if all of its eigenvalues are less or equal $\frac{1}{2}$ (see section 2.5.3): this is guaranteed by the remaining conditions (3.52)-(3.54) or equivalently (3.56) and (3.57). Note that conditions (3.54) and (3.57) are identical to the PPT conditions for the class $\mathcal{C}$ given by (3.28) and (3.30), respectively.

Now we have

$$\varrho_{ij} = V_{AA'}^{(ij)} \otimes V_{BB'}^{(ij)} \, \tilde{\varrho}_{ij} \, V_{AA'}^{(ij)\dagger} \otimes V_{BB'}^{(ij)\dagger} \tag{3.60}$$

where

$$\begin{aligned}
V_{AA'}^{(00)} &= |00\rangle\langle 0| + |10\rangle\langle 1| & V_{BB'}^{(00)} &= |00\rangle\langle 0| + |10\rangle\langle 1| & (3.61)\\
V_{AA'}^{(01)} &= |00\rangle\langle 0| + |11\rangle\langle 1| & V_{BB'}^{(01)} &= |01\rangle\langle 0| + |10\rangle\langle 1| & (3.62)\\
V_{AA'}^{(10)} &= |01\rangle\langle 0| + |10\rangle\langle 1| & V_{BB'}^{(10)} &= |00\rangle\langle 0| + |11\rangle\langle 1| & (3.63)\\
V_{AA'}^{(11)} &= |01\rangle\langle 0| + |11\rangle\langle 1| & V_{BB'}^{(11)} &= |01\rangle\langle 0| + |11\rangle\langle 1| & (3.64)
\end{aligned}$$

and

$$\tilde{\varrho}_{ij} = \frac{1}{2} \begin{bmatrix} \lambda_1 + \lambda_2 & \cdot & \cdot & (\lambda_1 - \lambda_2) e^{i\phi_{ij}} \\ \cdot & \lambda_3 + \lambda_4 & \frac{\lambda_3 - \lambda_4}{\|X^\Gamma\|} e^{i\phi_{ij}} & \cdot \\ \cdot & \frac{\lambda_3 - \lambda_4}{\|X^\Gamma\|} e^{-i\phi_{ij}} & \lambda_3 + \lambda_4 & \cdot \\ (\lambda_1 - \lambda_2) e^{-i\phi_{ij}} & \cdot & \cdot & \lambda_1 + \lambda_2 \end{bmatrix} \tag{3.65}$$

where ϕ_{ij} comes from the polar decomposition of u_{ij}

$$u_{ij} = |u_{ij}| e^{i\phi_{ij}} \tag{3.66}$$

and u_{ij} are elements of the single qubit unitary matrix used to define operator X in (3.33).

Note that we use other then usual order of subsystems: $AA'BB'$.

3.5 PPT key arbitrary close to separability

Having separability conditions, PPT conditions and key distillability conditions for states ϱ_U with $d = 2$ (i.e., $4 \otimes 4$ states) we can present a class of states, subclass of ϱ_H (H stands for the Hadamard unitary), with private key arbitrary close to the separable states. To obtain private key arbitrary close to the set of separable states the chosen separable state to which we approach must have $p = \frac{1}{2}$ otherwise for $p \neq \frac{1}{2}$ we will loose key distillability property before getting arbitrary close to the separable state.

Now, the figure 3.2 illustrate two classes of states:

1. The class $\tilde{\varrho}_H$ — illustrated by the dash line connecting states γ_1^+ and γ_2^+. All states of this class has $\alpha = \beta = 1$ and $p \in [0, 1]$. Most of the states of this class are NPT and there is only single PPT state for p given by (3.11) laying on the boundary of PPT states, we denote this state with $\tilde{\varrho}_1$. The class is described in section 3.1.

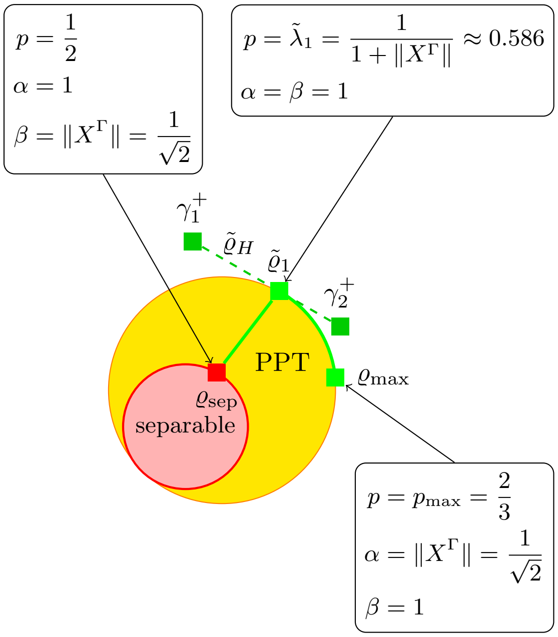
$p = \frac{1}{2}$
$\alpha = 1$
$\beta = \|X^\Gamma\| = \frac{1}{\sqrt{2}}$
$p = \tilde{\lambda}_1 = \frac{1}{1+\|X^\Gamma\|} \approx 0.586$
$\alpha = \beta = 1$
γ_1^+
$\tilde{\varrho}_H$
$\tilde{\varrho}_1$
γ_2^+
PPT
$\varrho_{\max}$
ϱ_{sep}
separable
$p = p_{\max} = \frac{2}{3}$
$\alpha = \|X^\Gamma\| = \frac{1}{\sqrt{2}}$
$\beta = 1$

Figure 3.2: A class of key-distillable PPT entangled states: (a) the solid line from $\tilde{\varrho}$ on the boundary of the PPT entangled states (inclusive) to the boundary of the set of separable states, arbitrary close to ϱ_{sep}; (b) the arc of PPT-invariant states starting in $\tilde{\varrho}$ and approaching arbitrary close to $\tilde{\varrho}_{\max}$.

2. The solid line from ϱ_{sep} through $\tilde{\varrho}_1$ to $\varrho_{\max}$ denotes a class of states which are key-distillable in every point excluding the boundary states ϱ_{sep} and $\varrho_{\max}$.[3] In particular, there are key-distillable states arbitrary close to the separable state ϱ_{sep} and thus to the set of separable states. One obtains states from the class by choosing $p \in [\frac{1}{2}, p_{\max}]$ where $p = \frac{1}{2}$ gives ϱ_{sep} and $p_{\max} = (1 + \|X^\Gamma\|^2)^{-1} = \frac{2}{3}$ gives $\varrho_{\max}$ and

$$\alpha = \min(1, \alpha_1) \qquad \beta = \min(1, \alpha_1^{-1}) \tag{3.67}$$

where α_1 is given by (5.73) and has the value

$$\alpha_1 = \frac{1-p}{p}\sqrt{2}. \tag{3.68}$$

The range $p \in [\frac{1}{2}, \tilde{\lambda}_1]$ where $\tilde{\lambda}_1$ is given by (3.11) is represented by the straight line from ϱ_{sep} to ϱ_1. While the range $p \in [\tilde{\lambda}_1, p_{\max}]$ is represented by the arc from ϱ_1 to $\varrho_{\max}$.

3.6 States ϱ_H as mixtures of Bell states with ‘flags’

States of the class ϱ_H are separable in the $AB : A'B'$ cut, i.e., subsystems AB and $A'B'$ of ϱ_H are only classically correlated. A state from ϱ_H can be decomposed

[3] Actually for $\varrho_{\max}$ we do not know if it is key-distillable we know that one cannot obtain private key from $\varrho_{\max}$ using our approach.

into a mixture of four states. Each of the four states has a Bell state ψ_i on the subsystem AB and some corresponding state on $A'B'$.

One can select parameters $p \in [0,1]$, $\alpha \in [-1,1]$, and $\beta \in [-1,1]$ satisfying both the PPT conditions (3.29) and (3.30) and the key condition (3.47), and prepare a corresponding PPT and thus bound entangled key-distillable state from the class ϱ_H which has the form

$$\varrho_H = \sum_{i=1}^{4} q_i \, |\psi_i\rangle\langle\psi_i|_{AB} \otimes \varrho^{(i)}_{A'B'} \tag{3.69}$$

where the Bell states ψ_i are given by (2.25) and the correlated states are the following:

$$\varrho^{(1)} = \alpha\frac{1}{2}(P_{|00\rangle} + P_{\psi_3}) + (1-\alpha)\frac{\mathrm{I}}{4} \tag{3.70}$$

$$\varrho^{(2)} = \alpha\frac{1}{2}(P_{|11\rangle} + P_{\psi_4}) + (1-\alpha)\frac{\mathrm{I}}{4} \tag{3.71}$$

$$\varrho^{(3,4)} = \beta P_{\chi_\pm} + (1-\beta)\frac{1}{2}(P_{|00\rangle} + P_{|11\rangle}) \tag{3.72}$$

where P_ψ denotes the projector onto a pure state ψ and

$$\chi_\pm = \frac{1}{\sqrt{2 \pm \sqrt{2}}}(|00\rangle \pm |\psi_1\rangle) \tag{3.73}$$

$$q_1 = q_2 = \frac{p}{2} \tag{3.74}$$

$$q_3 = q_4 = \frac{1-p}{2}. \tag{3.75}$$

States that satisfy both PPT and key distillability conditions are bound entangled (i.e., they cannot be separable, as entanglement is a precondition of private key distillability [51]).

3.7 Maximizing von Neumann Entropy

In this section, we find $4 \otimes 4$ key-distillable PPT states with a quite high von Neumann entropy for two subclasses of the class $\mathcal{C}$ and summarize the results in a table.

3.7.1 Entropy for states of the class $\mathcal{PK}_d$

Let $\mathcal{PK}_d$ denote a subclass of the class $\mathcal{C}$ satisfying

1. X is given by (3.33) (the class is subscripted with the dimension of the unitary used to define operator X),
2. the states are PPT,

3. the states are key-distillable by (3.46) (or equivalently by (3.47)).

The name $\mathcal{PK}_d$ comes from as shortcut of PPT and key-distillable. Now, we find the supremum of the von Neumann entropy over states from the class $\mathcal{PK}_d$.

As ϱ_U (and thus a state from $\mathcal{PK}_d$) is a mixture of four orthogonal private bits its von Neumann entropy is given by

$$S(\varrho_U) = h(p) + p\left(H\left(\frac{1-\alpha}{2}\right) + S(\sqrt{X^\dagger X})\right) \\ + (1-p)\left(H\left(\frac{1-\beta}{2}\right) + S(\sqrt{Y^\dagger Y})\right) \quad (3.76)$$

where

$$S(\sqrt{X^\dagger X}) \leq 2\log_2 d \quad (3.77)$$

$$S(\sqrt{Y^\dagger Y}) = \log_2 d \quad (3.78)$$

and the maximal value in (3.77) is achieved if the unitary used to define X in (3.33) is unimodular. A unimodular unitary also maximizes the allowed range of p given by (3.48), as it achieves minimum of $\|X^\Gamma\|$. Hence, to maximize the entropy, it is enough to consider a unimodular unitary. The supremum is achieved for a state with $p = p_{\max}$, $\beta = 0$, and $\alpha = \sqrt{\frac{1-p}{p}}$ (which no longer satisfies our key-distillability condition) thus

$$\sup_{\varrho_U \in \mathcal{PK}_d} S(\varrho_U) = \sup_{p\in(\frac{1}{2},p_{\max})} \left((1+p)\log_2 d + (1-p) + h(p) + pH\left(\frac{1-\sqrt{\frac{1-p}{p}}}{2}\right)\right) \quad (3.79)$$

where $p_{\max} = (1 + \|X^\Gamma\|^2)^{-1}$ comes from (3.48).

In particular, for $d = 2$, i.e., ϱ being $4 \otimes 4$ states, the supremum is achieved for state having $p = p_{\max} = 2/3$ which gives

$$\sup_{\varrho_U \in \mathcal{PK}_2} S(\varrho_U) \approx 3.319. \quad (3.80)$$

The supremum corresponds to a state $\varrho_{\max}$ on figure 3.2 but with $\beta = 0$.

3.7.2 Entropy for states of a class larger than ϱ_U

For the subclass ϱ of the class $\mathcal{C}$ with $d = 2$ and X and Y given by (3.36), we are able to obtain

$$S(\varrho) \approx 3.524 \quad (3.81)$$

for $U_1 = U_2 = H$, $q \approx 0.683$, $\beta = 0$ and α, p taken as in the previous subsection. It seems to be the supremum of the von Neumann entropy for this selection of operators X and Y.

3.7.3 Summary

Here, we summarize the results of maximizing von Neumann entropy of $4 \otimes 4$ key-distillable PPT states in the following table:

$S(\varrho)$	ϱ satisfying PPT and key conditions
2.564	class $\tilde{\varrho}$ from [2] with $p = \tilde{\lambda}_1$, the maximum is achieved for $U = H$
3.319	class ϱ_U, the supremum is described in section 3.7.1
3.524	class $\mathcal{C}$ with X and Y given by (3.36), a supposed supremum is described in section 3.7.2

3.8 Distillability via erasure channel

In [43], it was shown that two zero capacity channels, if combined together, can have nonzero capacity. One of the channels was related (through so called Choi-Jamiołkowski (CJ) isomorphism) to a bound entangled but key-distillable state, while the other was a so called symmetrically extendable channel. In particular, authors considered an example, where the first channel had $4 \otimes 4$ CJ state from the class $\tilde{\varrho}$ described in section 3.1 while the second one was the 50%-erasure channel. In [52] a simpler scheme was proposed, which also allows to observe this curious phenomenon.

The second approach amounts to sending a subsystem A' of a state defined on systems $ABA'B'$ through the 50%-erasure channel and checking the coherent information of the resulting state. If it is positive one concludes that the capacity of combined channel is also positive. Here, we shall use this approach to see how the presence of coherence β influences the phenomenon.

Coherent information after sending the A' subsystem through the 50%-erasure channel is given by

$$I_{\text{coh}} = \frac{1}{2}(S_{A'BB'} - S) + \frac{1}{2}(S_{BB'} - S_{ABB'}) \tag{3.82}$$

where S, $S_{A'BB'}$, and $S_{BB'}$ are given by (3.76), (3.83), and (3.84), respectively, and $S_{ABB'}$ is computed numerically.

For a PPT state $\tilde{\varrho}$ described in section 3.1 with X given by (3.33) and based on unimodular unitary and having $\lambda_1 = \tilde{\lambda}_1$, where $\tilde{\lambda}_1$ is given by (3.11), the coherent information is positive starting from $d = 11$. For a similar state of our class with $p = \tilde{\lambda}_1$, $\alpha = 1$ and $\beta = 0$ the coherent information is positive starting from $d = 22$.

Formulas for $S_{A'BB'}$ and $S_{BB'}$ are as follows:

$$S(\varrho_{A'BB'}) = 1 + \frac{1}{2} S\left(p\sqrt{XX^\dagger} + (1-p)\sqrt{Y^\dagger Y}\right) + \frac{1}{2} S\left(p\sqrt{X^\dagger X} + (1-p)\sqrt{YY^\dagger}\right) \tag{3.83}$$

$$S(\varrho_{BB'}) = 1 + \frac{1}{2} S_B \left(p\sqrt{XX^\dagger} + (1-p)\sqrt{Y^\dagger Y} \right) + \frac{1}{2} S_B \left(p\sqrt{X^\dagger X} + (1-p)\sqrt{YY^\dagger} \right). \quad (3.84)$$

3.9 Condition for obtaining private key from general states

In section 3.3 a sufficient condition for obtaining private key in terms of norms of the nonzero blocks from states having a Bell diagonal privacy-squeezed state was introduced. In this section, we generalize that condition to the case of an arbitrary state.

Let us define two 'twirling' operations (cf. [53])

$$\Lambda_{XX} = \frac{1}{2}(\hat{\mathrm{I}} \otimes \hat{\mathrm{I}} + \hat{\sigma}_x \otimes \hat{\sigma}_x) \quad (3.85)$$

$$\Lambda_{ZZ} = \frac{1}{2}(\hat{\mathrm{I}} \otimes \hat{\mathrm{I}} + \hat{\sigma}_z \otimes \hat{\sigma}_z) \quad (3.86)$$

and one twirling with flags

$$\Lambda'_{XX}(\varrho) = \frac{1}{2}(\varrho \otimes |0\rangle\langle 0| + \hat{\sigma}_x \otimes \hat{\sigma}_x(\varrho) \otimes |1\rangle\langle 1|) \quad (3.87)$$

where $\hat{U}\varrho = U\varrho U^\dagger$, σ_x and σ_z are Pauli matrices given by (2.100).

Private key from a general state We now give a sufficient condition for obtaining private key from a general state.

Proposition 3.1. *For an arbitrary state*

$$\varrho = \begin{bmatrix} A & B & C & D \\ B^\dagger & E & F & G \\ C^\dagger & F^\dagger & H & I \\ D^\dagger & G^\dagger & I^\dagger & J \end{bmatrix} \quad (3.88)$$

if

$$\max(\|D\|^2, \|F\|^2) > \frac{1}{4}(\|A\| + \|J\|)(\|E\| + \|H\|) \quad (3.89)$$

then Alice and Bob can distill private key by first applying twirling $\Lambda'_{XX} \circ \Lambda_{ZZ}$ to the key part and measuring the key part of many copies of the state ϱ and then using the recurrence and the Devetak-Winter protocol.

Remark Note that the right-hand side of equation (3.89) can also be written as $\frac{1}{4}p_e(1-p_e)$ where p_e is the probability of error (i.e. anticorrelation) when key part is measured in the standard basis.

Proof of the proposition 3.1. Alice and Bob first apply twirling $\Lambda'_{XX} \circ \Lambda_{ZZ}$ (an LOCC operation) to the key part and obtain the following state

$$\Lambda'_{XX} \circ \Lambda_{ZZ}(\varrho) = \begin{bmatrix} A \oplus J & \cdot & \cdot & D \oplus D^\dagger \\ \cdot & E \oplus H & F \oplus F^\dagger & \cdot \\ \cdot & F \oplus F^\dagger & E \oplus H & \cdot \\ D \oplus D^\dagger & \cdot & \cdot & A \oplus J \end{bmatrix}. \tag{3.90}$$

This state is now of the spider form and, thanks to flags, we have direct sums within the blocks. Now, the privacy-squeezed state has the following Bell diagonal form

$$\sigma = \begin{bmatrix} \|A\| + \|J\| & \cdot & \cdot & \|D\| + \|D^\dagger\| \\ \cdot & \|E\| + \|H\| & \|F\| + \|F^\dagger\| & \cdot \\ \cdot & \|F\| + \|F^\dagger\| & \|E\| + \|H\| & \cdot \\ \|D\| + \|D^\dagger\| & \cdot & \cdot & \|A\| + \|J\| \end{bmatrix}. \tag{3.91}$$

Then the proof follows from the key condition given in section 3.3. □

Note that in the proof above we use Λ'_{XX}, a twirling with flags. If Λ_{XX}, a twirling without flags, were used instead we would have to replace $\|D\|$ with $\|D + D^\dagger\|$ in (3.89) (analogously for $\|F\|$) which can be much smaller than $\|D\|$, and even equal to zero in the extreme case of antihermitian D, i.e., $D^\dagger = -D$, so in this case no private key can be distilled from $\Lambda_{XX}(\varrho)$ even if ϱ is a private state, i.e., $\varrho = \gamma(D)$.

Note also, that in the proof, we have first applied twirling with flags to the original state, and then the privacy-squeezing operation. Actually, the same state would be obtained if we first apply the privacy squeezing and then apply (standard) twirling. This is illustrated by the following diagram

$$\begin{tikzcd} \varrho \arrow[r, "\Lambda'_{XX}\circ\Lambda_{ZZ}"] \arrow[d, "P_{sq}"'] & \varrho' \arrow[d, "P_{sq}"] \\ \sigma \arrow[r, "\Lambda_{XX}\circ\Lambda_{ZZ}"] & \sigma' \end{tikzcd} \tag{3.92}$$

where P_{sq} stands for the privacy squeezing. As explained above, this diagram would not commute if we used solely twirling without flags. Thus, to seek for key-distillable states, one can go the alternative route, i.e., first compute the privacy-squeezed state, and then, by twirling, obtain a Bell diagonal state. Now, if $\Lambda_{XX} \circ \Lambda_{ZZ}(\sigma)$ satisfies necessary security condition for realistic QKD on a Pauli channel from [47], i.e., its eigenvalues λ_i satisfy (3.46), then ϱ is key-distillable using the sufficient condition introduced in this section.

Chapter 4

Distillation of NPT Werner state by half-property

The problem of existence of NPT bound entangled states is an open question since 1998 [4]. There are many partial results but the problem is still open.

In this chapter we consider distillability of the most entangled of the suspicious Werner states for $d = 4$. (All of the suspicious Werner states are conjectured to be undistillable [7, 8]). We show that the problem of 2-undistillability of the most entangled of the suspicious Werner states for $d = 4$ is equivalent to having the maximum overlap of Schmidt rank to states with some projector Q not exceeding $\frac{1}{2}$. We call this equivalent problem the *half-property*. We show wide ranges of rank two states having the half-property. And we also translate the problem into matrix analysis problem.

The results presented in this chapter have been published in [6].

4.1 Half-property

Let us consider the most entangled of the suspicious Werner states for $d = 4$ and denote it with ϱ_W. Parameter p of ϱ_W in (2.70) is equal to

$$p = p_0 = \frac{d+1}{4d-2} = \frac{5}{14}. \tag{4.1}$$

We recall that the state ϱ_W is n-undistillable iff

$$\inf_{\phi_2 \in \mathrm{SR}_2} \langle \phi_2 | \varrho_W^{\Gamma \otimes n} | \phi_2 \rangle \geq 0 \tag{4.2}$$

where SR_2 is the set of all Schmidt rank two states, cf equation (2.123). (We give the condition for n-undistillability instead of n-distillability because ϱ_W is conjectured to be undistillable). We recall that we use ϕ_1 to denote a product state and ϕ_2 to denote a Schmidt rank two state. Now, as we shall show, n-undistillability of ϱ_W is equivalent to

$$\sup_{\phi_2 \in \mathrm{SR}_2} \langle \phi_2 | Q_n | \phi_2 \rangle \leq \frac{1}{2}. \tag{4.3}$$

where Q_n is a projector. We call (4.3) the *half-property* and say that a given rank two state ϕ_2 *has the half-property* (for given n) if it satisfies the inequality (4.3). The state ϱ_W is n-undistillable if all ϕ_2 states have the half-property (for given n).

We mostly concentrate on the problem of 2-undistillability of ϱ_W and thus will use Q to denote Q_2.

Half-property for $n = 2$ We first prove (4.3) for $Q = Q_2$.

$$\begin{aligned} {\varrho_W^\Gamma}^{\otimes 2} &\sim (\mathrm{I} - \tfrac{1}{2}V)^{\Gamma\otimes 2} = \left(\mathrm{I} - \tfrac{d}{2}\Phi_+\right)^{\otimes 2} \\ &= \underbrace{(\Phi_+^\perp \otimes \Phi_+^\perp + \Phi_+ \otimes \Phi_+)}_{\mathcal{P}_+} - \underbrace{(\Phi_+^\perp \otimes \Phi_+ + \Phi_+ \otimes \Phi_+^\perp)}_{Q=\mathcal{P}_-} \\ &= \mathcal{P}_+ - \mathcal{P}_- \\ &= \mathrm{I}^{\otimes 2} - 2Q \end{aligned} \tag{4.4}$$

where Φ_+ is given by (2.39), $\mathcal{P}_+$ and $Q = \mathcal{P}_-$ are projectors satisfying $\mathcal{P}_+ + \mathcal{P}_- = \mathrm{I}^{\otimes 2}$ which justifies the last equality. Having the last equality we can show the equivalence of the 2-undistillability condition (4.2) to the half-property condition (4.3):

$$\begin{aligned} \inf_{\phi_2} \langle\phi_2|\varrho_W^{\Gamma\otimes n}|\phi_2\rangle \geq 0 &\iff \inf_{\phi_2} \langle\phi_2|(\mathrm{I}^{\otimes 2} - 2Q)|\phi_2\rangle \geq 0 \\ &\iff 1 - 2\sup_{\phi_2} \langle\phi_2|Q|\phi_2\rangle \geq 0 \\ &\iff \sup_{\phi_2} \langle\phi_2|Q|\phi_2\rangle \leq \frac{1}{2} \end{aligned} \tag{4.5}$$

where the projector Q, let us recall, is given by

$$Q = Q_2 = \Phi_+^\perp \otimes \Phi_+ + \Phi_+ \otimes \Phi_+^\perp. \tag{4.6}$$

Half-property for general n For general n we have

$$\varrho_W^{\Gamma\otimes n} \sim (\mathrm{I} - \tfrac{d}{2}\Phi_+)^{\otimes n} = \mathcal{P}_+ - \mathcal{P}_- = \mathrm{I}^{\otimes n} - 2Q_n \tag{4.7}$$

where $\mathcal{P}_+$ and $Q_n = \mathcal{P}_-$ are projectors satisfying $\mathcal{P}_+ + \mathcal{P}_- = \mathrm{I}^{\otimes n}$. Now, from equation

$$(\mathrm{I} - \tfrac{d}{2}\Phi_+)^{\otimes n} = \mathrm{I}^{\otimes n} - 2Q_n \tag{4.8}$$

we obtain

$$Q_n \equiv \mathcal{P}_- = \frac{1}{2}\left(\mathrm{I}^{\otimes n} - \left(\mathrm{I} - \tfrac{d}{2}\Phi_+\right)^{\otimes n}\right) \tag{4.9}$$

and n-undistillability condition (4.2) is equivalent to the half-property condition (4.3) by the reasoning given by equations (4.5) with Q replaced with Q_n.

Recursive formula for $\boldsymbol{Q_n}$ For $d = 4$ operators Q_n satisfy the recursive formula

$$Q_1 = \Phi_+, \tag{4.10}$$
$$Q_{n+1} = Q_n \otimes Q_1^\perp + Q_n^\perp \otimes Q_1. \tag{4.11}$$

The proof is by induction: step $n = 1$ is evident from (4.9); now, for $n + 1$ one can obtain the recursive formula (4.11) by substituting into Q_{n+1} given by (4.9) equation (4.8) once for n and once for 1:

$$\begin{aligned}
Q_{n+1} &= \frac{1}{2}\left(\mathrm{I}^{\otimes n+1} - \left(\mathrm{I} - \tfrac{d}{2}\Phi_+\right)^{\otimes n+1}\right)\\
&= \frac{1}{2}\left(\mathrm{I}^{\otimes n+1} - (\mathrm{I}^{\otimes n} - 2Q_n) \otimes (\mathrm{I} - 2Q_1)\right)\\
&= \mathrm{I}^{\otimes n} \otimes Q_1 + Q_n \otimes (\mathrm{I} - 2Q_1)\\
&= \mathrm{I}^{\otimes n} \otimes Q_1 + Q_n \otimes Q_1^\perp - Q_n \otimes Q_1\\
&= Q_n^\perp \otimes Q_1 + Q_n \otimes Q_1^\perp.
\end{aligned} \tag{4.12}$$

4.2 Existence of nontrivial maxima of $\langle\phi_2|Q|\phi_2\rangle$

State ϱ_W is 1-undistillable

$$\inf_{\phi_2 \in \mathrm{SR}_2} \langle\phi_2|\varrho_W^\Gamma|\phi_2\rangle \geq 0. \tag{4.13}$$

This implies that states of the form $\phi_2 \otimes \phi_1$ which are product between the copies (i.e., in the $AB : A'B'$ cut) must also satisfy

$$\langle\phi_2 \otimes \phi_1|\varrho_W^{\Gamma\otimes 2}|\phi_2 \otimes \phi_1\rangle \geq 0. \tag{4.14}$$

and so we can equivalently say that states of the form $\phi_2 \otimes \phi_1$ have the half-property.

Now, we can ask if states of the form $\phi_2 \otimes \phi_1$ are the only states that attain equality in the half property. If all of the local maxima would be of the $\phi_2 \otimes \phi_1$ form then ϱ_W would be 2-undistillable. But this is not the case: we provide states which are superpositions of $\phi_2 \otimes \phi_1$ and $\phi_1' \otimes \phi_2'$ which also attain equality in the half property and we show that there are rank two states among those superpositions.

We first introduce the following

Fact 4.1. *For any ψ*

$$\sup_{\phi_k \in SR_k} |\langle\phi_k|\psi\rangle|^2 = \sum_{i=1}^{k} \mu_i^2 \tag{4.15}$$

where $\mu_1, \ldots, \mu_k$ are the k largest Schmidt coefficients of ψ in the same cut that ϕ_k has Schmidt rank k, i.e. $AA' : BB'$.

Operator Q may be alternatively written as

$$Q = \mathrm{I} \otimes \Phi_+ + \Phi_+ \otimes \mathrm{I} - 2\Phi_+ \otimes \Phi_+ \tag{4.16}$$

thus

$$\langle \phi_2 \otimes \phi_1 | \, Q \, | \phi_2 \otimes \phi_1 \rangle = p + q - 2pq \leq \frac{1}{2} \tag{4.17}$$

where from fact (4.1) we have the following bounds

$$p = \langle \phi_2 | \Phi_+ | \phi_2 \rangle \leq \frac{2}{d}, \quad q = \langle \phi_1 | \Phi_+ | \phi_1 \rangle \leq \frac{1}{d} \tag{4.18}$$

and the maximal value (for $d = 4$) is obtained by setting $p = \frac{2}{d}$ and any q.

We now consider superposition of $\phi_2 \otimes \phi_1$ and $\phi_1' \otimes \phi_2'$ of the form

$$|\psi\rangle = \sqrt{r} \, |\phi_2\rangle_{AB} \otimes |\phi_1\rangle_{A'B'} + \sqrt{1-r} \, |\phi_1'\rangle_{AB} \otimes |\phi_2'\rangle_{A'B'} \tag{4.19}$$

satisfying

$$\langle \phi_2 | \Phi_+ | \phi_2 \rangle = \langle \phi_2' | \Phi_+ | \phi_2' \rangle = \frac{2}{d} \tag{4.20}$$

$$\langle \phi_1 | \Phi_+ | \phi_1 \rangle = \langle \phi_1' | \Phi_+ | \phi_1' \rangle = 0. \tag{4.21}$$

Such a superposition attains equality in the half property

$$\langle \psi | Q | \psi \rangle = \frac{1}{2}. \tag{4.22}$$

Superpositions (4.19) generally have Schmidt rank higher than two but there are rank two states among them. For example the following class of states

$$|\phi\rangle = \sqrt{r} \, |\phi_+^{(2)}\rangle_{AB} \otimes |01\rangle_{A'B'} + \sqrt{1-r} \, |01\rangle_{AB} \otimes |\phi_+^{(2)}\rangle_{A'B'} \tag{4.23}$$

where

$$|\phi_+^{(2)}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{4.24}$$

This class can be rewritten in Alice versus Bob cut as

$$\begin{aligned} |\phi^{AA':BB'}\rangle = & \frac{1}{\sqrt{2}}|00\rangle_{AA'} \otimes \left(\sqrt{r}|01\rangle + \sqrt{1-r}|10\rangle\right)_{BB'} \\ & + \frac{1}{\sqrt{2}} \left(\sqrt{r}|10\rangle + \sqrt{1-r}|01\rangle\right)_{AA'} \otimes |11\rangle_{BB'} \end{aligned} \tag{4.25}$$

and one can easily see that states of this class are rank two states in Alice versus Bob cut.

4.3 States having ‘normal’ projection on Q

In this section we show that a state ϕ_2 having projection on Q (that is $Q|\phi_2\rangle$) isomorphic via the state–operator isomorphism to a normal operator has the half-property. We first define

State–operator isomorphism By the *state–operator isomorphism* we mean the following one to one correspondence

$$|\psi\rangle = \sum a_{ij}|i\rangle|j\rangle \longleftrightarrow X = \sum a_{ij}|i\rangle\langle j|. \tag{4.26}$$

In this isomorphism $\langle\psi|\psi\rangle = \mathrm{Tr}X^\dagger X$ and the Schmidt coefficients of a state ψ are equal to the singular values of the corresponding operator X. Thus in particular

$$\sup_{\psi\in\mathcal{H}_P} (\mu_1^2+\mu_2^2) = \sup_X(\sigma_1^2+\sigma_2^2) \tag{4.27}$$

where μ_1 and μ_2 are two largest Schmidt coefficients of ψ and σ_1 and σ_2 are two largest singular values of X and the second supremum is taken over all X corresponding via state–operator isomorphism to states from the space $\mathcal{H}_P$.

We have the following lemma, which is a generalization of a similar one for product states [54].

Lemma 4.1. *For any projector P acting on a bipartite system*

$$\sup_{\phi_2\in\mathrm{SR}_2} \langle\phi_2|P|\phi_2\rangle = \sup_{\psi\in\mathcal{H}_P} (\mu_1^2+\mu_2^2) \tag{4.28}$$

where μ_1 and μ_2 are the two largest Schmidt coefficients of ψ and $\mathcal{H}_P$ is the subspace defined by the projector P.

Note that this lemma immediately generalizes to rank k states for arbitrary fixed $k \geq 1$.

Proof. Let us observe that for all $\psi \in \mathcal{H}_P$

$$\langle\phi_2|P|\phi_2\rangle \geq \langle\phi_2|\psi\rangle\langle\psi|\phi_2\rangle. \tag{4.29}$$

Moreover there exists $\psi \in \mathcal{H}_P$ which reaches the equality

$$\langle\phi_2|P|\phi_2\rangle = \langle\phi_2|\psi\rangle\langle\psi|\phi_2\rangle, \tag{4.30}$$

namely $|\psi\rangle = \frac{P|\phi_2\rangle}{\|P|\phi_2\rangle\|}$ if $\|P|\phi_2\rangle\| \neq 0$ or any $\psi \in \mathcal{H}_P$ otherwise. From these two observations we get

$$\langle\phi_2|P|\phi_2\rangle = \sup_{\psi\in\mathcal{H}_P} |\langle\phi_2|\psi\rangle|^2. \tag{4.31}$$

From (4.31) and the fact (4.1) we conclude that

$$\begin{aligned} \sup_{\phi_2\in\mathrm{SR}_2} \langle\phi_2|P|\phi_2\rangle &= \sup_{\psi\in\mathcal{H}_P} \sup_{\phi_2\in\mathrm{SR}_2} |\langle\phi_2|\psi\rangle|^2 \\ &= \sup_{\psi\in\mathcal{H}_P} (\mu_1^2+\mu_2^2) \end{aligned} \tag{4.32}$$

where μ_1 and μ_2 are the two largest Schmidt coefficients of ψ. □

Corollary 4.1. *Now, from lemma 4.1 and equation* (4.27) *we obtain*

$$\sup_{\phi_2}\langle\phi_2|P|\phi_2\rangle = \sup_X(\sigma_1^2+\sigma_2^2) \tag{4.33}$$

where σ_1 and σ_2 are two largest singular values of X and the supremum is taken over all X corresponding via state–operator isomorphism to states from the space $\mathcal{H}_P$.

4.3.1 Half-property in terms of matrices

Every state $\psi_Q \in \mathcal{H}_Q$ where projector Q is given by (4.6) has the form

$$|\psi_Q\rangle = \sqrt{p}\,|\psi_{(1)}\rangle_{AB} \otimes |\phi_+\rangle_{A'B'} + \sqrt{1-p}\,|\phi_+\rangle_{AB} \otimes |\psi_{(2)}\rangle_{A'B'} \tag{4.34}$$

where $p \in [0,1]$ and

$$|\psi_{(1)}\rangle \perp |\phi_+\rangle, \quad |\psi_{(2)}\rangle \perp |\phi_+\rangle. \tag{4.35}$$

Now, the image of a state $\psi_Q \in \mathcal{H}_Q$ in the state–operator isomorphism has the form

$$X = \sqrt{\frac{p}{d}}\,\tilde{A} \otimes \mathrm{I} + \sqrt{\frac{1-p}{d}}\,\mathrm{I} \otimes \tilde{B} \tag{4.36}$$

where

$$\mathrm{Tr}\tilde{A} = \mathrm{Tr}\tilde{B} = 0 \tag{4.37}$$

$$\mathrm{Tr}\tilde{A}^\dagger\tilde{A} = \mathrm{Tr}\tilde{B}^\dagger\tilde{B} = 1. \tag{4.38}$$

The first condition comes from orthogonality of $\psi_{(1)}$ and $\psi_{(2)}$ with ϕ_+ and the second from normalization, i.e., from $\langle\psi_{(i)}|\psi_{(i)}\rangle = 1$.

Simple form Now, we can simplify condition (4.36) by absorbing the coefficients info the operators. This way we obtain that the image of $\psi_Q \in \mathcal{H}_Q$ in the state–operator isomorphism has the form

$$X = A \otimes \mathrm{I} + \mathrm{I} \otimes B \tag{4.39}$$

where

$$\mathrm{Tr}A = \mathrm{Tr}B = 0, \quad \mathrm{Tr}A^\dagger A + \mathrm{Tr}B^\dagger B = \frac{1}{d}. \tag{4.40}$$

Half-property in terms of matrices Thus the half-property is satisfied iff for all operators X of the form (4.39) the sum of squares of the two largest singular values of X does not exceed $\frac{1}{2}$, i.e.,

$$\sigma_1^2 + \sigma_2^2 \leq \frac{1}{2}. \tag{4.41}$$

This follows from the corollary 4.1.

4.3.2 Half-property for states having ‘normal’ projection on Q

In this section we show that a state ϕ_2 having normal projection on Q (i.e., a state for which $Q|\phi_2\rangle$ is isomorphic trough the state–operator isomorphism to a normal operator X) has the half-property.

Let us note that the operator X given in equation (4.39) is normal iff operators A and B are normal. As normal matrices are diagonalizable and their singular values are equal to moduli of eigenvalues we arrive at an optimization problem over numbers rather than matrices which we will now solve. Namely we have

Constraints in terms of eigenvalues The constraints (4.40) can be reformulated as constraints on eigenvalues of A and B denoted by a_i and b_i. The constraints in terms of eigenvalues a_i and b_i are of the form

$$\mathrm{Tr}A = \sum_{i=1}^{d} a_i = 0, \quad \mathrm{Tr}B = \sum_{i=1}^{d} b_i = 0, \tag{4.42}$$

$$\mathrm{Tr}A^\dagger A + \mathrm{Tr}B^\dagger B = \sum_{i=1}^{d} |a_i|^2 + \sum_{i=1}^{d} |b_i|^2 = \frac{1}{d}. \tag{4.43}$$

Theorem 4.1. *Let $\mathcal{X}_d$ be the subset of normal operators X of the form* (4.39) *satisfying constraints* (4.40). *Then for $d = 4$ we have*

$$\sup_{X\in\mathcal{X}_d} (\sigma_1^2 + \sigma_2^2) \leq \frac{1}{2} \tag{4.44}$$

where σ_1 and σ_2 are the two largest singular values of operator X.

Proof. Since X is diagonalizable then we can replace singular values with moduli of eigenvalues. The latter are of the form

$$\lambda_{ij} = a_i + b_j \tag{4.45}$$

where a_i and b_j are eigenvalues of A and B, respectively. We then have

$$\sup_{X\in\mathcal{X}_d} (\sigma_1^2 + \sigma_2^2) = \sup_{X\in\mathcal{X}_d} (|\lambda_1|^2 + |\lambda_2|^2) \tag{4.46}$$

$$= \sup_{X\in\mathcal{X}_d} \max_{\substack{i,j,k,l\in\{1,\ldots,d\},\\ (i,j)\neq(k,l)}} \left(|a_i + b_j|^2 + |a_k + b_l|^2\right) \tag{4.47}$$

$$= \sup_{X\in\mathcal{X}_d} \max \left\{|a_1 + b_1|^2 + |a_2 + b_2|^2, \right.$$

$$\left. |a_1 + b_1|^2 + |a_1 + b_2|^2\right\} \tag{4.48}$$

where λ_1 and λ_2 are two eigenvalues of X with largest moduli. Equality in the last equation (4.48) comes from the fact that there are two unique settings

1. $i \neq k \wedge j \neq l$ and
2. $i = k \wedge j \neq l \vee i \neq k \wedge j = l$.

In the second setting we consider only one term of the alternative as under the constraints (4.42) and (4.43) we can exchange A and B. We also take arbitrary indices as we can freely relabel eigenvalues of A and B.

Thus to prove the theorem we have to show that the following inequalities hold

$$|a_1 + b_1|^2 + |a_2 + b_2|^2 \leq \frac{1}{2} \tag{4.49}$$

$$|a_1 + b_1|^2 + |a_1 + b_2|^2 \leq \frac{1}{2} \tag{4.50}$$

under the constraints (4.42) and (4.43) with $d = 4$. The first inequality comes directly from the parallelogram identity

$$|x+y|^2 = 2(|x|^2 + |y|^2) - |x-y|^2 \leq 2(|x|^2 + |y|^2) \tag{4.51}$$

which implies

$$|a_1 + b_1|^2 + |a_2 + b_2|^2 \leq 2(|a_1|^2 + |b_1|^2 + |a_2|^2 + |b_2|^2) \leq 2\frac{1}{d} = \frac{1}{2}. \tag{4.52}$$

The second inequality is much more involved and we have moved it to the appendix (proposition A.1) where we prove that

$$|a_1 + b_1|^2 + |a_1 + b_2|^2 \leq \frac{3d-4}{d^2} \tag{4.53}$$

which for $d = 4$ gives (4.50). □

We are now prepared to state the main result of this section

Theorem 4.2. *For $d = 4$ any rank two state $\phi_2 \in SR_2(AA' : BB')$ with the projection on Q ($Q|\phi_2\rangle$) isomorphic through the state–operator isomorphism to a normal operator satisfies the half-property.*

Proof. Let us assume $\langle\phi_2|Q|\phi_2\rangle \neq 0$ (otherwise the conclusion is obvious). By hypothesis ϕ_2 reaches its projection on Q on a state $|\psi_Q\rangle = \frac{Q|\phi_2\rangle}{\|Q|\phi_2\rangle\|} \in \mathcal{H}_Q$ and ψ_Q is isomorphic through the state–operator isomorphism given by (4.26) to a normal operator X. Then using the fact (4.1), equality of the Schmidt coefficients of ψ_Q and the singular values of operator X in the state–operator isomorphism, and theorem 4.1 we obtain

$$\begin{aligned}\langle\phi_2|Q|\phi_2\rangle = |\langle\phi_2|\psi_Q\rangle|^2 &\leq \sup_{\phi_2 \in \mathrm{SR}_2(AA':BB')} |\langle\phi_2|\psi_Q\rangle|^2 \\ &= \mu_1^2 + \mu_2^2 = \sigma_1^2 + \sigma_2^2 \leq \sup_{X \in \mathcal{X}_d} (\sigma_1^2 + \sigma_2^2) \leq \frac{1}{2}\end{aligned} \tag{4.54}$$

where μ_1 and μ_2 are the two largest Schmidt coefficients of ψ_Q in the same cut in which ϕ_2 has rank two (i.e., $AA' : BB'$) while σ_1 and σ_2 are the two largest singular values of operator X, and $\mathcal{X}_d$ is the subset of normal operators X of the form (4.39) satisfying constraints (4.40). □

4.4 Half-property for low Schmidt rank states

In this section we show that any state having on each pair at least one subsystem with one-qubit support satisfies the half-property. For this purpose we introduce the notion of the so-called *common degrees of freedom*.

4.4.1 Half-property via 'common degrees of freedom'

Let us start with the definition of common degrees of freedom.

Common degrees of freedom For a given state ϕ and two of its subsystems denoted by A and B we define a set called *common degrees of freedom* of subsystem A *with* B as

$$\mathrm{cdf}(\phi, A, B) \equiv \{i \in \mathcal{I} : \langle\phi|P_i|\phi\rangle \neq 0\} \tag{4.55}$$

where $\mathcal{I} = \{0, \dots, d-1\}$ and

$$P_i = |ii\rangle\langle ii|_{AB} \otimes \mathrm{I}_{A'B'}. \tag{4.56}$$

We say that subsystem A has at most k common degrees of freedom *with* subsystem B if $|\,\mathrm{cdf}(\phi, A, B)| \leq k$.

Proposition 4.1. *If for a given state ϕ subsystems A with B and A' with B' have at most $\frac{d}{2}$ common degrees of freedom then ϕ satisfies the half-property.*

Proof. Let ϕ be a state such that A with B and A' with B' have at most $\frac{d}{2}$ common degrees of freedom, i.e.,

$$|\,\mathrm{cdf}(\phi, A, B)| \leq \frac{d}{2} \qquad |\,\mathrm{cdf}(\phi, A', B')| \leq \frac{d}{2} \tag{4.57}$$

We take $\mathcal{I}_{AB}$ and $\mathcal{I}_{A'B'}$ to be supersets of above sets but with exactly $\frac{d}{2}$ elements

$$\mathrm{cdf}(\phi, A, B) \subset \mathcal{I}_{AB} \qquad\qquad |\mathcal{I}_{AB}| = \frac{d}{2} \tag{4.58}$$

$$\mathrm{cdf}(\phi, A', B') \subset I_{A'B'} \qquad\qquad |\mathcal{I}_{A'B'}| = \frac{d}{2}. \tag{4.59}$$

Let us also define maximally entangled states on subspaces generated by $\mathcal{I}_{AB}$ and $\mathcal{I}_{A'B'}$:

$$\Phi_{AB} = \frac{2}{d} \sum_{i,j \in \mathcal{I}_{AB}} |ii\rangle\langle jj| \qquad \Phi_{A'B'} = \frac{2}{d} \sum_{i,j \in \mathcal{I}_{A'B'}} |ii\rangle\langle jj|. \tag{4.60}$$

Now, by the very definition of common degrees of freedom ϕ projects only on those operators $|ii\rangle\langle jj|$ which are included in Φ_{AB} and $\Phi_{A'B'}$ thus we have

$$\langle\phi|\mathrm{I}_{AB} \otimes \Phi_+|\phi\rangle = \langle\phi|\mathrm{I}_{AB} \otimes \frac{1}{2}\Phi_{A'B'}|\phi\rangle \tag{4.61}$$

$$\langle\phi|\Phi_+ \otimes \mathrm{I}_{A'B'}|\phi\rangle = \langle\phi|\frac{1}{2}\Phi_{AB} \otimes \mathrm{I}_{A'B'}|\phi\rangle \tag{4.62}$$

$$\langle\phi|\Phi_+ \otimes \Phi_+|\phi\rangle = \langle\phi|\frac{1}{2}\Phi_{AB} \otimes \frac{1}{2}\Phi_{A'B'}|\phi\rangle \tag{4.63}$$

and thus using formula for Q given by (4.16) we have

$$\begin{aligned}\langle\phi|Q|\phi\rangle &= \langle\phi|\mathrm{I}_{AB}\otimes\Phi_+ + \Phi_+\otimes\mathrm{I}_{A'B'} - 2\Phi_+\otimes\Phi_+|\phi\rangle \\ &= \langle\phi|\mathrm{I}_{AB}\otimes\frac{1}{2}\Phi_{A'B'} + \frac{1}{2}\Phi_{AB}\otimes\mathrm{I}_{A'B'} - 2\frac{1}{2}\Phi_{AB}\otimes\frac{1}{2}\Phi_{A'B'}|\phi\rangle \\ &= \frac{1}{2}\langle\phi|\underbrace{\mathrm{I}_{AB}\otimes\Phi_{A'B'} + \Phi_{AB}\otimes\mathrm{I}_{A'B'} - \Phi_{AB}\otimes\Phi_{A'B'}}_{\tilde{Q}}|\phi\rangle \\ &= \frac{1}{2}\langle\phi|\tilde{Q}|\phi\rangle \\ &\leq \frac{1}{2}. \end{aligned} \tag{4.64}$$

So we obtain that for ϕ its projection on Q is equal to $\frac{1}{2}$ of its projection on some other projector $\tilde{Q}$ and the projection of any state on any projector may not exceed one thus finally we have that the projection of ϕ on Q is bounded by $\frac{1}{2}$. □

4.4.2 Application of cdf to low Schmidt rank

Here by use of proposition 4.1 we show that any state which on each pair has at least one subsystem with one-qubit support satisfies the half-property.

Theorem 4.3. *Any state ϕ that satisfies*

$$\begin{aligned} &\left(\mathrm{Sch}(A:A'BB') \leq \frac{d}{2} \vee \mathrm{Sch}(B:AA'B') \leq \frac{d}{2}\right) \\ \wedge &\left(\mathrm{Sch}(A':ABB') \leq \frac{d}{2} \vee \mathrm{Sch}(B':AA'B) \leq \frac{d}{2}\right) \end{aligned} \tag{4.65}$$

also satisfies the half-property. Here $\mathrm{Sch}(X:Y)$ *denotes the Schmidt rank of the state ϕ in the X versus Y cut.*

Observation 4.1. *The operator Q is $U_A\otimes V_{A'}\otimes U_B^*\otimes V_{B'}^*$ invariant. (Where U and V are unitaries).*

Proof of theorem 4.3. The hypothesis may be expanded into a four-term alternative. We prove the conclusion for one of the terms (for the others the proof is analogous). Now suppose

$$\mathrm{Sch}(A:A'BB') \leq \frac{d}{2} \ \wedge\ \mathrm{Sch}(A':ABB') \leq \frac{d}{2} \tag{4.66}$$

I.e., ϕ have the Schmidt rank at most $\frac{d}{2}$ in both $A:A'BB'$ and $A':ABB'$ cuts. This implies that ϕ have the following Schmidt decompositions in these cuts:

$$|\phi\rangle = \sum_{i=0}^{d/2-1} a_i|\psi_i^A\rangle|\psi_i^{A'BB'}\rangle = \sum_{i=0}^{d/2-1} a_i'|\psi_i^{A'}\rangle|\psi_i^{ABB'}\rangle \tag{4.67}$$

We can choose unitary matrices U and V which transform ϕ into

$$|\phi'\rangle = U_A \otimes V_{A'} \otimes U_B^* \otimes V_{B'}^* |\phi\rangle \tag{4.68}$$

$$= \sum_{i=0}^{d/2-1} a_i |i^A\rangle |\tilde{\psi}_i^{A'BB'}\rangle = \sum_{i=0}^{d/2-1} a_i' |i^{A'}\rangle |\tilde{\psi}_i^{ABB'}\rangle \tag{4.69}$$

Now, we can observe that for ϕ' A with B and A' with B' have at most $\frac{d}{2}$ degrees of freedom in common (as there are clearly at most $\frac{d}{2}$ degrees of freedom on A and A' subsystems) thus by applying proposition 4.1 we have

$$\langle \phi' | Q | \phi' \rangle \leq \frac{1}{2} \tag{4.70}$$

and by applying observation 4.1 we finally get

$$\langle \phi | Q | \phi \rangle = \langle \phi' | Q | \phi' \rangle \leq \frac{1}{2}. \tag{4.71}$$

□

4.5 Optimizing over product states and implications

In this section we consider a problem simpler than the original one: the optimization of the overlap of the product states with projector Q_n given by (4.9). For product states optimization of the overlap with Q_n is equivalent to the optimization of the overlap with Q_n^Γ. Knowing the maximum over product states, we can bound the maximum over Schmidt rank two states. For $n = 2$ we will obtain in this way

$$\langle \phi_2 | Q | \phi_2 \rangle \leq \frac{3}{4}. \tag{4.72}$$

However the analysis of n copy case shows that in the limit of $n \to \infty$ one obtains a trivial result that the overlap does not exceed one. Nevertheless this approach can be used to go beyond $\frac{3}{4}$.

4.5.1 Maximum overlap of product states with Q_n

We first observe that for product states finding the maximal overlap with Q_n is equivalent to finding the maximal overlap with Q_n^Γ:

$$\sup_{\phi_1} \langle \phi_1 | Q_n | \phi_1 \rangle = \sup_{\phi_1} \mathrm{Tr}\left(Q_n |\phi_1\rangle\langle\phi_1| \right)^\Gamma = \sup_{\phi_1} \langle \phi_1 | Q_n^\Gamma | \phi_1 \rangle \tag{4.73}$$

where supremum is taken over all product states. This equivalence comes from the fact that partial transpose of a product state $|\phi_1\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ is also a product state

$$\begin{aligned}(|\phi_1\rangle\langle\phi_1|)^\Gamma &= (|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B|)^\Gamma \\ &= |\psi_A\rangle\langle\psi_A| \otimes |\psi_B^*\rangle\langle\psi_B^*| \\ &= |\tilde{\phi}_1\rangle\langle\tilde{\phi}_1|. \end{aligned} \tag{4.74}$$

Following the observation we use Q_n^Γ to find the maximum overlap of product states with Q_n. To this end we consider the spectral decomposition of Q_n^Γ. We have

$$\begin{aligned}Q_n^\Gamma &= \frac{1}{2}\left(\mathrm{I}^{\otimes n} - \left(\mathrm{I} - \tfrac{1}{2}V\right)^{\otimes n}\right) \\ &= \frac{1}{2}\left(\mathrm{I}^{\otimes n} - \left(\tfrac{1}{2}P_s + \tfrac{3}{2}P_a\right)^{\otimes n}\right) \\ &= \sum_{i=0}^{n} \lambda_i A_i \end{aligned} \tag{4.75}$$

where P_s and P_a are the projectors onto the symmetric and the antisymmetric subspaces (given by equations (2.72) and (2.73)) and eigenvalues λ_i and the corresponding eigenspaces A_i are of the form

$$\lambda_i = \frac{1}{2}\left(1 - \frac{3^i}{2^n}\right) \tag{4.76}$$

$$A_i = \sum_{l_j \in \{0,1\},\, \sum l_j = i} P_{l_1} \otimes \cdots \otimes P_{l_n} \tag{4.77}$$

where $P_0 = P_s$ and $P_1 = P_a$. (Note that $\sum_{i=0}^n A_i = \mathrm{I}^{\otimes n}$). One can observe that eigenvalues of Q_n^Γ are in decreasing order and the largest eigenvalue λ_0 is associated with the eigenspace $A_0 = P_s^{\otimes n}$. In particular for, $n = 2$ we have

$$\lambda_0 = \frac{3}{8},\ \lambda_1 = \frac{1}{8},\ \lambda_2 = -\frac{5}{8}, \tag{4.78}$$

so that

$$Q_2^\Gamma = \frac{3}{8} P_s \otimes P_s + \frac{1}{8}(P_a \otimes P_s + P_s \otimes P_a) - \frac{5}{8} P_a \otimes P_a. \tag{4.79}$$

The overlap of product states with Q_n^Γ is bounded by its largest eigenvalue λ_0 and this value is attainable as there are product states in the corresponding eigenspace $A_0 = P_s^{\otimes n}$. As already noted it also gives the maximum overlap of product states with Q_n so we finally have

$$\sup_{\phi_1} \langle\phi_1|Q_n|\phi_1\rangle = \sup_{\phi_1} \langle\phi_1|Q_n^\Gamma|\phi_1\rangle = \lambda_0 = \frac{1}{2}\left(1 - \frac{1}{2^n}\right). \tag{4.80}$$

In particular, for two copies this gives $\frac{3}{8}$.

4.5.2 Bound for $\langle\phi_2|Q_n|\phi_2\rangle$ in terms of $\langle\phi_1|Q_n|\phi_1\rangle$

A Schmidt rank two state may be decomposed to

$$|\phi_2\rangle = \sqrt{p}|\phi_1\rangle + \sqrt{1-p}|\phi_1^\perp\rangle, \tag{4.81}$$

where $\langle\phi_1|\phi_1^\perp\rangle = 0$. Now, we observe that

$$\begin{aligned} &\sup_{\phi_2}\langle\phi_2|Q_n|\phi_2\rangle \\ &= \sup_{\phi_1,\phi_1^\perp,p}\left(p\langle\phi_1|Q_n|\phi_1\rangle + (1-p)\langle\phi_1^\perp|Q_n|\phi_1^\perp\rangle + 2\sqrt{p(1-p)}\,\mathrm{Re}\langle\phi_1|Q_n|\phi_1^\perp\rangle\right) \\ &\le \sup_{\phi_1,\phi_1^\perp}\left(\langle\phi_1|Q_n|\phi_1\rangle + |\langle\phi_1|Q_n|\phi_1^\perp\rangle|\right) \end{aligned} \tag{4.82}$$

from Schwarz inequality we have

$$|\langle\phi_1|Q_n|\phi_1^\perp\rangle| \le \sqrt{\langle\phi_1|Q_n|\phi_1\rangle\langle\phi_1^\perp|Q_n|\phi_1^\perp\rangle} \le \lambda_0 = \frac{1}{2}\left(1-\frac{1}{2^n}\right) \tag{4.83}$$

and thus

$$\sup_{\phi_2}\langle\phi_2|Q_n|\phi_2\rangle \le 2\sup_{\phi_1}\langle\phi_1|Q_n|\phi_1\rangle. \tag{4.84}$$

In this way we have obtained the bound for the overlap of the Schmidt rank two states with Q_n in terms of optimal overlap with product states. The same reasoning is also true for any other projector.

Thus, for two copies we obtain the following bound

$$\sup_{\phi_2}\langle\phi_2|Q|\phi_2\rangle \le \frac{3}{4}. \tag{4.85}$$

Unfortunately, this method does not lead to any bound that would hold for all n apart from the trivial bound $\langle\phi_2|Q_n|\phi_2\rangle \le 1$.

4.5.3 The form of the product states attaining maximum on Q_n

In section 4.5.1 we obtained the value of the maximum overlap of product states with Q_n. In this section we find the form of the product states which attain the maximal overlap with Q_n. As in section 4.5.1 we use the equivalent of maximization of the overlap with Q_n and with Q_n^Γ for product states.

For $n = 2$ a state $\tilde{\phi}_1$ attaining maximal overlap with Q^Γ must belong to the subspace $P_s^{AB} \otimes P_s^{A'B'}$ and thus must have the form

$$|\tilde{\phi}_1\rangle = |\psi\psi\rangle_{AB} \otimes |\phi\phi\rangle_{A'B'}. \tag{4.86}$$

Now, a product state ϕ_1 attaining maximal overlap with Q is the partial transpose of $\tilde{\phi}_1$ and thus must have the form

$$|\phi_1\rangle = |\psi\psi^*\rangle_{AB} \otimes |\phi\phi^*\rangle_{A'B'}. \tag{4.87}$$

(See equation (4.74) for the explanation of this partial transposition).

This observation in general case of n copies is contained in the following.

Proposition 4.2. *For any n all rank-one states ϕ_1 attaining maximum on Q_n has the form*

$$|\phi_1\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle_{A_i} |\psi_i^*\rangle_{B_i}. \tag{4.88}$$

Proof. The thesis of the proposition is equivalent to the following statement: for any n all rank-one states $\tilde{\phi}_1$ attaining maximum on Q_n^Γ have the form

$$|\tilde{\phi}_1\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle_{A_i} |\psi_i\rangle_{B_i}. \tag{4.89}$$

We prove it by induction.

1. For $n = 1$ we have $Q_1^\Gamma = \frac{1}{4}V$ and by considering a general product state $|\psi\phi\rangle$ we obtain

$$\langle\psi\phi|V|\psi\phi\rangle = |\langle\psi|\phi\rangle|^2 \tag{4.90}$$

and maximum is attained by product states of the form $|\psi\psi\rangle$ that is of the form (4.89) with $n = 1$.

2. Suppose that for product states maximal overlap with Q_n^Γ is attained only by states of the form (4.89) we show that the same holds for Q_{n+1}^Γ. Let us consider $\tilde{\phi}_1$ for $n+1$. First of all $\tilde{\phi}_1$ is a state of the symmetric subspace in Alice versus Bob cut which (analogously to the reasoning in point 1) implies that it has the form $|\psi\psi\rangle$ in Alice versus Bob cut. Next, we consider Schmidt decomposition of ψ of the form

$$|\psi\rangle = \sum_i a_i |\psi_i\rangle|\phi_i\rangle. \tag{4.91}$$

Now, we can decompose $\tilde{\phi}_1$ as

$$\begin{aligned} |\tilde{\phi}_1\rangle = |\psi\rangle_{Aa}|\psi\rangle_{Bb} &= \left(\sum_i a_i |\psi_i\rangle_A |\phi_i\rangle_a\right)\left(\sum_j a_j |\psi_j\rangle_B |\phi_j\rangle_b\right) \\ &= \sum_{ij} a_i a_j |\psi_i\psi_j\rangle_{AB} |\phi_i\phi_j\rangle_{ab} \end{aligned} \tag{4.92}$$

where AB denotes a subsystem consisting of n pairs and ab denotes a single pair. And we have

$$\begin{aligned}\langle\tilde{\phi}_1|P_s^{\otimes n+1}|\tilde{\phi}_1\rangle &= \sum a_i a_j a_k a_l \langle\psi_i\psi_j|P_s^{\otimes n}|\psi_k\psi_l\rangle\langle\phi_i\phi_j|P_s|\phi_k\phi_l\rangle \\ &= \sum a_i a_j a_k a_l \langle\psi_i\psi_j|P_s^{\otimes n}|\psi_k\psi_l\rangle\frac{1}{2}(\delta_{ik}\delta_{jl}+\delta_{il}\delta_{jk}) \qquad (4.93)\end{aligned}$$

To obtain one in the above expression it is necessary that all the projections are equal to 1. The projection on P_s given in delta-form to be equal to one requires $i = j = k = l$ and it is always one only if $\tilde{\phi}_1$ is product in $AB : ab$ cut. To obtain one on $P_s^{\otimes n}$ the $\psi_i \otimes \psi_i$ state must be of the form (4.89) and thus $\tilde{\phi}_1$ is of the form (4.89).

□

4.5.4 Superpositions of product states with maximum on Q_n

States attaining maximum on Q_n are product between copies thus one can expect that their superpositions have the half property. Indeed it is the case.

Proposition 4.3. *Let $d = 4$ and ϕ_1, $\phi_1^\perp$ be n-copy orthogonal product states with maximum overlap with Q_n, i.e. states of the form*

$$|\phi_1\rangle = \bigotimes_{i=1}^{n} |\psi_i\rangle_{A_i}|\psi_i^*\rangle_{B_i}, \quad |\phi_1^\perp\rangle = \bigotimes_{i=1}^{n} |\tilde{\psi}_i\rangle_{A_i}|\tilde{\psi}_i^*\rangle_{B_i} \qquad (4.94)$$

then their superposition

$$|\phi_2\rangle = \sqrt{p}|\phi_1\rangle + \sqrt{1-p}|\phi_1^\perp\rangle \qquad (4.95)$$

has the following overlap with Q_n

$$\langle\phi_2|Q_n|\phi_2\rangle = \frac{1}{2}\left(1-\frac{1}{2^n}\right) - \sqrt{p(1-p)}\prod_{i=1}^{n}\left(|\langle\psi_i|\tilde{\psi}_i\rangle|^2 - \frac{1}{2}\right). \qquad (4.96)$$

In particular, it is equal to $\frac{1}{2}$ only if $p = \frac{1}{2}$ and ϕ_1, $\phi_1^\perp$ are orthogonal on an odd number of copies and equal on the rest. Otherwise it is less than $\frac{1}{2}$.

Proof. The form of ϕ_1 and $\phi_1^\perp$ comes from proposition 4.2 and their overlap with Q_n from (4.80) thus we have

$$\langle\phi_2|Q_n|\phi_2\rangle = \frac{1}{2}\left(1-\frac{1}{2^n}\right) + 2\sqrt{p(1-p)}\,\mathrm{Re}\langle\phi_1|Q_n|\phi_1^\perp\rangle \qquad (4.97)$$

Thus to finish the proof we will show by induction that

$$\langle\phi_1|Q_n|\phi_1^\perp\rangle = -\frac{1}{2}\prod_{i=1}^{n}\left(|\langle\psi_i|\tilde{\psi}_i\rangle|^2 - \frac{1}{2}\right). \qquad (4.98)$$

1. It is true for $n = 1$

$$\begin{aligned}\langle\phi_1|Q_1|\phi_1^\perp\rangle &= \mathrm{Tr}\left(\Phi_+ \,|\tilde{\psi}_1\rangle\langle\psi_1| \otimes |\tilde{\psi}_1^*\rangle\langle\psi_1^*|\right)^\Gamma \\ &= \frac{1}{d}\mathrm{Tr}\left(V\,|\tilde{\psi}_1\rangle\langle\psi_1| \otimes |\psi_1\rangle\langle\tilde{\psi}_1|\right) \\ &= \frac{1}{d}\langle\psi_1\tilde{\psi}_1|V|\tilde{\psi}_1\psi_1\rangle = \frac{1}{d} = -\frac{1}{2}(0-\frac{1}{2}). \end{aligned} \tag{4.99}$$

where ψ_1 and $\tilde{\psi}_1$ must be orthogonal as ϕ_1 and $\phi_1^\perp$ are orthogonal.

2. Suppose it is true for some n, let us show it also holds for $n+1$. Without loss of generality we can assume ϕ_1 and $\phi_1^\perp$ are orthogonal on one of the first n copies thus we can write

$$|\phi_1\rangle = |\phi\rangle|\psi\psi^*\rangle, \quad |\phi_1^\perp\rangle = |\phi^\perp\rangle|\tilde{\psi}\tilde{\psi}^*\rangle. \tag{4.100}$$

Then by using recursive formula (4.11) and the equality

$$\langle\phi|Q_n^\perp|\phi^\perp\rangle = -\langle\phi|Q_n|\phi^\perp\rangle \tag{4.101}$$

we have

$$\begin{aligned}\langle\phi_1|Q_{n+1}|\phi_1^\perp\rangle &= \langle\phi|Q_n|\phi^\perp\rangle\left(\langle\psi\psi^*|(\mathrm{I}-Q_1)|\tilde{\psi}\tilde{\psi}^*\rangle - \langle\psi\psi^*|Q_1|\tilde{\psi}\tilde{\psi}^*\rangle\right) \\ &= \langle\phi|Q_n|\phi^\perp\rangle\left(\langle\psi\psi^*|\tilde{\psi}\tilde{\psi}^*\rangle - 2\langle\psi\psi^*|Q_1|\tilde{\psi}\tilde{\psi}^*\rangle\right) \\ &= -\frac{1}{2}\prod_{i=1}^{n}\left(|\langle\psi_i|\tilde{\psi}_i\rangle|^2 - \frac{1}{2}\right)\left(|\langle\psi|\tilde{\psi}\rangle|^2 - \frac{2}{d}\langle\psi\tilde{\psi}|V|\tilde{\psi}\psi\rangle\right) \\ &= -\frac{1}{2}\prod_{i=1}^{n+1}\left(|\langle\psi_i|\tilde{\psi}_i\rangle|^2 - \frac{1}{2}\right). \end{aligned} \tag{4.102}$$

It is evident that to maximize (4.96), i.e. obtain $\frac{1}{2}$, one needs $p = \frac{1}{2}$ and (4.98) equal to $2^{-(n+1)}$. This requires $\left||\langle\psi_i|\tilde{\psi}_i\rangle|^2 - \frac{1}{2}\right| = \frac{1}{2}$ for all i, that is ψ_i and $\tilde{\psi}_i$ must be equal or orthogonal and further for (4.98) to be positive ψ_i and $\tilde{\psi}_i$ must be orthogonal on odd number of copies and equal on the rest.

□

4.6 Bounds for maximal overlap with Q for all states ϕ_2.

In this section we show that we can improve the bound obtained by means of product states in the previous section.

4.6.1 Strictly less than 3/4

Let us recall the bound of (4.82) on the overlap of rank two states with Q

$$\sup_{\phi_2}\langle\phi_2|Q_n|\phi_2\rangle \leq \sup_{\phi_1,\phi_1^\perp}\left(\langle\phi_1|Q_n|\phi_1\rangle + \langle\phi_1|Q_n|\phi_1^\perp\rangle\right). \tag{4.103}$$

Let us also recall bounds for two terms of the sum in the above supremum

1. the bound for the first term introduced in (4.80)

$$\sup_{\phi_1}\langle\phi_1|Q_n|\phi_1\rangle = \frac{1}{2}\left(1-\frac{1}{2^n}\right). \tag{4.104}$$

2. the bound for the second term introduced in (4.83)

$$|\langle\phi_1|Q_n|\phi_1^\perp\rangle| \leq \sqrt{\langle\phi_1|Q_n|\phi_1\rangle\langle\phi_1^\perp|Q_n|\phi_1^\perp\rangle} \tag{4.105}$$

From these three bounds we obtain

$$\sup_{\phi_2}\langle\phi_2|Q_n|\phi_2\rangle \leq 1-\frac{1}{2^n}. \tag{4.106}$$

But the equality in the above equation requires both ϕ_1 and $\phi_1^\perp$ to attain maximum overlap on Q_n but then by proposition 4.3 we obtain that superposition of ϕ_1 and $\phi_1^\perp$ has the half property. Thus for any ϕ_2 we have

$$\langle\phi_2|Q_n|\phi_2\rangle < 1-\frac{1}{2^n} \tag{4.107}$$

but from the continuity of (4.104) and (4.105) we also obtain

$$\sup_{\phi_2}\langle\phi_2|Q_n|\phi_2\rangle < 1-\frac{1}{2^n}. \tag{4.108}$$

which in particular for $n=2$ gives

$$\sup_{\phi_2}\langle\phi_2|Q|\phi_2\rangle < \frac{3}{4}. \tag{4.109}$$

Beyond 3/4 The argument of continuity was used in [6] and a slightly better bound was obtained

$$\langle\phi_2|Q|\phi_2\rangle \leq 0.74971 < 3/4. \tag{4.110}$$

Numerical results Numerical optimization suggests that the bound (4.103) is actually equal to $\frac{17}{32}$. If we want to optimize independently both terms of the bound (4.103) we get

$$\sup_{\phi_2}\langle\phi_2|Q|\phi_2\rangle \leq \frac{3}{8} + \sup_{\phi_1,\phi_1^\perp}|\langle\phi_1|Q|\phi_1^\perp\rangle| \tag{4.111}$$

which numerically gives $\frac{5}{8}$. At the moment we do not have analytical proofs of these estimates.

Chapter 5

Distillation using extendible maps

The problem of existence of NPT bound entangled states is an open question since 1998 [4]. There are many partial results but the problem is still open.

One of the possible research directions on a way to find NPT bound entangled states is to allow Alice and Bob to use a broader than LOCC class of operations. In this chapter we will consider the class of *k-extendible operations* which in the limit of $k \to \infty$ tend to separable operations. These are maps, whose corresponding Choi-Jamiołkowski state is k-fold symmetrically extendible.

We shall not require the operations to be trace-preserving. Our main quantity of interest will be fidelity of output with maximally entangled state, that can be obtained with some nonzero probability.

First of all we shall show, that those maps are extremely powerful regarding distillation. Namely, we prove, that for any fixed k, the class of k-extendible maps can distill any state but maximally mixed one, if large enough number of copies is available. Second, even in single copy, the maps can provide fidelity 1 (with some nonzero probability) for any state which has a $(k-1)$-extendible state in its kernel. In particular, they are not stable under local embedding into larger Hilbert space.

We then analyze the case of Werner states. We obtain that curve of attainable fidelity is symmetric with respect to identity, on the interval joining symmetric and antisymmetric state in case of 1- to 4-extendible maps. By use of the orthogonal basis in the linear space of operators that commute with unitary operators of the form $U \otimes U \otimes U$ we obtain analytically the maximal fidelity achievable for single copy of a Werner state and for 1-extendible maps. We consider a subclass of k-extendible maps, which we call '*measure-and-prepare*' maps (they belong to entanglement breaking channels). For single copy of Werner state and $k = 1$ we show that this subclass gives the same fidelity as all 1-extendible maps.

The results presented in this chapter have been published in [31].

5.1 Choi-Jamiołkowski state and k-extendible maps

Let us first define Choi-Jamiołkowski state and then k-extendible maps.

Choi-Jamiołkowski state Let Λ be a Completely Positive map acting on the input system AB with output system ab, i.e.,

$$\Lambda(\varrho_{AB}) = \varrho'_{ab}. \tag{5.1}$$

Now, for a given map Λ we define its *Choi-Jamiołkowski state* (or *CJ state*, for brevity) as

$$\sigma_{A'B'ab} = (\mathrm{id} \otimes \Lambda)\, \Phi^+_{A'A} \otimes \Phi^+_{B'B} \tag{5.2}$$

where A', B' are of the same dimensions as A, B, and Φ^+ is the maximally entangled state; Λ acts on system AB with output system ab and the identity map id acts on subsystem $A'B'$.

If Λ is not trace preserving then the CJ state may be unnormalized.

It turns out that from the CJ state one can reconstruct the map [55]

$$\Lambda(\varrho_{AB}) = d^2 \mathrm{Tr}_{AB}(\sigma_{ABab}\, \varrho^T_{AB} \otimes \mathrm{I}_{ab}). \tag{5.3}$$

For example, Λ is a separable map if and only if its CJ state is separable.

***k*-extendible state and *k*-extendible map** A state ϱ_{AB} is *k-extendible* (on Bob's site) if there exist a state $\varrho_{AB_0 \ldots B_k}$ such that $\varrho_{AB_i} = \varrho_{AB}$ for all i from 0 to k. Analogously, we say that a state ϱ_{AB} is k-extendible on Alice's site if there exist a state $\varrho_{A_0 \ldots A_k B}$ such that $\varrho_{A_i B} = \varrho_{AB}$ for all i from 0 to k.

We call Λ a *k-extendible map* (on Bob's or Alice's site) if its CJ state is a k-extendible state (on Bob's or Alice's site).

We will often consider operators having four subsystems ($ABab$) instead of two (AB) then A, B, A_i, and B_i will be replaced with Aa, Bb, $A_i a_i$, and $B_i b_i$ in the definition of k-extendability. We will use subsystems Bb and $B_0 b_0$ interchangeably and use Ee to denote subsystem $B_1 \ldots B_k, b_1 \ldots b_k$, especially when $k = 1$.

Any separable state is k-extendible for any k. Therefore the set of k-extendible maps includes separable maps. Conversely, if for any k a state is k-extendible then it is separable [56, 56]. Therefore k-extendible maps in a sense tend to separable maps when $k \to \infty$.

5.2 Formula for fidelity with *k*-extendible maps

Let ϱ be a given state and Λ a given completely positive (not necessarily trace-preserving) map acting on the input system AB with the output system ab (we use lowercase letters as we consider two-qubit output system). Now, we apply the map Λ to ϱ and consider the fidelity of the output state $\Lambda(\varrho)$ with the maximally entangled state:

$$F(\varrho, \Lambda) = \begin{cases} \dfrac{\mathrm{Tr}(\Lambda(\varrho)\Phi^+)}{\mathrm{Tr}(\Lambda(\varrho))} & \mathrm{Tr}(\Lambda(\varrho)) > 0 \\ 0 & \mathrm{Tr}(\Lambda(\varrho)) = 0. \end{cases} \tag{5.4}$$

where Φ^+ is the projector onto the maximally entangled stated given by (2.39).

Now we find two conditions equivalent to $F(\varrho, \Lambda) > \alpha$ where $\alpha \geq 0$ (the second of them will be used in the further consideration). Assume first, that $\mathrm{Tr}(\Lambda(\varrho)) > 0$. Then the following inequalities are equivalent

$$F(\varrho, \Lambda) = \frac{\mathrm{Tr}(\Lambda(\varrho)\Phi^+)}{\mathrm{Tr}(\Lambda(\varrho))} > \alpha \tag{5.5}$$

$$\alpha \mathrm{Tr}(\Lambda(\varrho)) - \mathrm{Tr}(\Lambda(\varrho)\Phi^+) < 0 \tag{5.6}$$

$$\mathrm{Tr}(\underbrace{(\alpha \mathrm{I} - \Phi^+)}_{M^\alpha_{ab}}\Lambda(\varrho)) < 0 \tag{5.7}$$

$$\mathrm{Tr}(\Lambda(\varrho)M^\alpha_{ab}) < 0 \tag{5.8}$$

so we obtain an equivalence condition

$$F(\varrho, \Lambda) > \alpha \iff \mathrm{Tr}(\Lambda(\varrho)M^\alpha_{ab}) < 0. \tag{5.9}$$

It is easy to check that this equivalence also holds if $\mathrm{Tr}(\Lambda(\varrho)) = 0$. Now, we use reformulation of $\Lambda(\varrho)$ in terms of the the Choi-Jamiołkowski state of our map Λ given by (5.3). We have

$$\mathrm{Tr}(\Lambda(\varrho)M^\alpha) = d^2 \mathrm{Tr}(\mathrm{Tr}_{AB}(\sigma_{ABab}\varrho^T_{AB} \otimes \mathrm{I}_{ab})M^\alpha_{ab}) \tag{5.10}$$

$$= d^2 \mathrm{Tr}(\mathrm{Tr}_{AB}(\sigma_{ABab}\varrho^T_{AB} \otimes \mathrm{I}_{ab}\mathrm{I}_{AB} \otimes M^\alpha_{ab})) \tag{5.11}$$

$$= d^2 \mathrm{Tr}(\sigma_{ABab}\underbrace{\varrho^T_{AB} \otimes M^\alpha_{ab}}_{X^\alpha_{ABab}}) \tag{5.12}$$

$$= d^2 \mathrm{Tr}(X^\alpha_{ABab}\sigma_{ABab}) \tag{5.13}$$

so we obtain another equivalence condition

$$F(\varrho, \Lambda) > \alpha \iff \mathrm{Tr}(X^\alpha_{ABab}\sigma_{ABab}) < 0 \tag{5.14}$$

where $\alpha \geq 0$.

For states satisfying $\mathrm{Tr}(\Lambda(\varrho)) > 0$ analogous conditions may be obtained for $F(\varrho, \Lambda) < \alpha$ and $F(\varrho, \Lambda) = \alpha$. Thus we obtain the following

Fact 5.1. *For any state ϱ and any completely positive map Λ and $\alpha \geq 0$, the following condition holds*

$$F(\varrho, \Lambda) > \alpha \iff \mathrm{Tr}(\Lambda(\varrho)\, M^\alpha_{ab}) < 0 \iff \mathrm{Tr}(X^\alpha_{ABab}\, \sigma_{ABab}) < 0 \tag{5.15}$$

where $M^\alpha_{ab} = \alpha \mathrm{I} - \Phi^+$ acts on a two-qubit Hilbert space, σ_{ABab} denotes the CJ state of Λ and X^α_{ABab} is given by

$$X^\alpha_{ABab} = \varrho^T_{AB} \otimes M^\alpha_{ab}. \tag{5.16}$$

If additionally $\mathrm{Tr}(\Lambda(\varrho)) > 0$, in particular if ϱ is a full rank state, then we also have

$$F(\varrho, \Lambda) < \alpha \iff \mathrm{Tr}(\Lambda(\varrho)\, M^\alpha_{ab}) > 0 \iff \mathrm{Tr}(X^\alpha_{ABab}\, \sigma_{ABab}) > 0 \tag{5.17}$$

$$F(\varrho, \Lambda) = \alpha \iff \mathrm{Tr}(\Lambda(\varrho)\, M^\alpha_{ab}) = 0 \iff \mathrm{Tr}(X^\alpha_{ABab}\, \sigma_{ABab}) = 0. \tag{5.18}$$

Remark 5.1. *The fidelity is here achievable with some nonzero probability, but the probability can be very small, and may depend on α. E.g., when α tends to 1, the probability may tend to 0.*

We use fact 5.1 to compute the lower and upper bounds for the supremum of $F(\varrho, \Lambda)$ over all k-extendible maps:

Proposition 5.1. *For any state ϱ_{AB} let $F_k(\varrho_{AB})$ denote the supremum of fidelity $F(\varrho_{AB}, \Lambda)$ achievable by k-extendible maps. Now, $F_k(\varrho_{AB})$ is connected to positivity of some operator, namely*

$$F_k(\varrho_{AB}) > \alpha \iff \lambda_{\min}(\hat{S}_k(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee})) < 0 \tag{5.19}$$

and if ϱ is a full rank state then also

$$F_k(\varrho_{AB}) < \alpha \iff \lambda_{\min}(\hat{S}_k(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee})) > 0 \tag{5.20}$$

$$F_k(\varrho_{AB}) = \alpha \iff \lambda_{\min}(\hat{S}_k(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee})) = 0. \tag{5.21}$$

where X^{α}_{ABab} is given by

$$X^{\alpha}_{ABab} = \varrho^{T}_{AB} \otimes M^{\alpha}_{ab} \tag{5.22}$$

subsystem Ee denotes $B_1 \dots B_k, b_1 \dots b_k$ and $\hat{S}_k$ denotes the symmetrization superoperator

$$\hat{S}_k(X) = \frac{1}{k+1} \sum_{i=0}^{k} V_{B_0 b_0 : B_i b_i} X V_{B_0 b_0 : B_i b_i} \tag{5.23}$$

where $V_{Y:Z}$ swaps subsystems Y and Z and, for convenience of labeling, we use B_0 and b_0 to denote B and b, respectively.

Proof. From fact 5.1 we obtain

$$F_k(\varrho_{AB}) = \sup_{\Lambda \in \{\Lambda_k\}} F(\varrho_{AB}, \Lambda) > \alpha \tag{5.24}$$

$$\iff \exists_{\Lambda \in \{\Lambda_k\}} F(\varrho_{AB}, \Lambda) > \alpha \tag{5.25}$$

$$\iff \exists_{\sigma_{ABab} \in \mathrm{EXT}_k} \operatorname{Tr}[X^{\alpha}_{ABab} \sigma_{ABab}] < 0 \tag{5.26}$$

$$\iff \inf_{\sigma_{ABab} \in \mathrm{EXT}_k} \operatorname{Tr}[X^{\alpha}_{ABab} \sigma_{ABab}] < 0. \tag{5.27}$$

where $\{\Lambda_k\}$ denotes the set of all k-extendible maps and EXT_k is the set of all k-extendible states. The right hand side can be transformed as follows

$$\inf_{\sigma_{ABab} \in \mathrm{EXT}_k} \operatorname{Tr}[X^{\alpha}_{ABab}\, \sigma_{ABab}] \tag{5.28}$$

$$= \inf_{\sigma_{ABabEe} \in \mathrm{SYM}_k} \operatorname{Tr}[X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee}\, \sigma_{ABabEe}] \tag{5.29}$$

$$= \inf_{\sigma_{ABabEe}} \operatorname{Tr}\left[X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee}\, \hat{S}_k(\sigma_{ABabEe})\right] \tag{5.30}$$

$$= \inf_{\sigma_{ABabEe}} \operatorname{Tr}\left[\hat{S}_k(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee})\, \sigma_{ABabEe}\right] \tag{5.31}$$

$$= \inf_{\psi_{ABabEe}} \langle \psi_{ABabEe} | \hat{S}_k(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee}) | \psi_{ABabEe} \rangle \tag{5.32}$$

$$= \lambda_{\min}(\hat{S}_k(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee})) \tag{5.33}$$

where SYM_k is the set of all k-symmetric states and $\lambda_{\min}(X)$ denotes the smallest eigenvalue of X. The equality (5.31) comes from $\mathrm{Tr}(\Lambda(A)\,B) = \mathrm{Tr}(A\,\Lambda^\dagger(B))$ for completely positive Λ and from $\hat{S}_k^\dagger = \hat{S}_k$

Thus finally

$$F_k(\varrho_{AB}) > \alpha \iff \lambda_{\min}(\hat{S}_k(X^\alpha_{ABab} \otimes \mathrm{I}_{Ee})) < 0. \tag{5.34}$$

The proof of the additional conditions for full rank ϱ is analogous. Those conditions are given only for full rank states as for full rank states we can use (5.17) and (5.18). □

Corollary 5.1. *For any state ϱ one can achieve any $F(\varrho, \Lambda) \le \alpha$ by some k-extendible map if operator $\hat{S}_k(\varrho^T_{AB} \otimes M^\alpha_{ab} \otimes \mathrm{I}_{Ee})$ is non-positive.*

If additionally ϱ is a full rank state then $F(\varrho, \Lambda) \le \alpha$ is also achievable if the least eigenvalue of $\hat{S}_k(\varrho^T_{AB} \otimes M^\alpha_{ab} \otimes \mathrm{I}_{Ee})$ is equal to 0.

Proof. From proposition 5.1 some $F > \alpha$ is achievable by some k-extendible map Λ_k, but then one can use a class of k-extendible maps $\Lambda_k^{(p)}$ which with probability p works as Λ_k and with probability $1-p$ return a state orthogonal to Φ^+ to obtain any fidelity $F \le \alpha$. □

Finally, there is the following general question: Can it be, that probabilistically one can get F arbitrary close to one, but with probability one, it is not possible? For LOCC, achieving high F probabilistically, means the same deterministically, by law of large numbers, and postselection. However we do not know whether k-extendible maps can be postselected. Or rather, whether a complement to k-extendible map can be k-extendible.

More precisely: In LOCC case the distillability by means of trace-preserving maps is equivalent to distillability by a non-trace preserving ones. Concerning k-extendible maps, we do not know if it is the case. In this thesis we do not require preserving of trace, and we get that the maps are very powerful. There is a possibility, that trace-preserving maps are not that powerful (hence more useful for the problem of distillability). However they are much harder to deal with.

5.2.1 'Measure-and-prepare' k-extendible maps

Here we consider a subclass of k-extendible maps, which will in a sense decouple the state ϱ from the operator M^α.

Proposition 5.2 (Measure-and-prepare maps are k-extendible)**.** *Consider any two states $\sigma_{AB_0\ldots B_k}$ and $\sigma_{ab_0\ldots b_k}$. We shall denote the reductions σ_{AB_i} by σ_i^{in} and the reductions σ_{ab_i} by σ_i^{out}. Then the following map is k-extendible: Alice and Bob apply to the given state ϱ_{AB} a global probabilistic POVM whose elements are the states $\sigma_0^{in}, \ldots, \sigma_k^{in}$. Then given the outcome i they prepare (globally) the state σ_i^{out} from the set of states $\sigma_0^{out}, \ldots, \sigma_k^{out}$. The CJ state of such a map has the form $\frac{1}{d^2}\mathrm{Tr}_{B_1\ldots B_k\, b_1\ldots b_k}\hat{S}_k(\sigma^T_{AB_0\ldots B_k} \otimes \sigma_{ab_0\ldots b_k})$.*

Remark 5.2. *Since our maps are not necessarily trace-preserving, the POVM elements need not sum to identity.*

Proof of proposition 5.2. We shall prove the case with $k = 1$ for clarity (for higher k the proof is identical). Let us consider postulated CJ state having the following form

$$\sigma_{ABab} = \frac{1}{d^2}\mathrm{Tr}_{Ee}\hat{S}_1(\sigma_{ABE}^T \otimes \sigma_{abe}) = \frac{1}{2d^2}(\sigma_{AB}^T \otimes \sigma_{ab} + \sigma_{AE}^T \otimes \sigma_{ae}) \tag{5.35}$$

Now using (5.3) we obtain

$$\Lambda(\varrho_{AB}) = d^2\mathrm{Tr}_{AB}(\sigma_{ABab}\, \varrho_{AB}^T \otimes \mathrm{I}_{ab}) \tag{5.36}$$

$$= \frac{1}{2}\mathrm{Tr}_{AB}\left(\left(\sigma_{AB}^T \otimes \sigma_{ab} + \sigma_{AE}^T \otimes \sigma_{ae}\right)\, \varrho_{AB}^T \otimes \mathrm{I}_{ab}\right) \tag{5.37}$$

$$= \frac{1}{2}\left(\mathrm{Tr}(\sigma_{AB}^T\varrho_{AB}^T)\sigma_{ab} + \mathrm{Tr}(\sigma_{AE}^T\varrho_{AB}^T)\sigma_{ae}\right) \tag{5.38}$$

$$= \frac{1}{2}\left(\mathrm{Tr}(\varrho_{AB}\sigma_{AB})\sigma_{ab} + \mathrm{Tr}(\varrho_{AB}\sigma_{AE})\sigma_{ae}\right) \tag{5.39}$$

where σ_{AE} and σ_{ae} act on AB and ab subsystems, respectively. Starting from the postulated CJ state of the map (POVM measurement with a numeric output i followed by outputing the state σ_i^{out}) we arrived at the map. Thus the postulated CJ state is the CJ state of the map. The CJ state is a 1-extendible state so the map is a 1-extendible map. □

Examples. The simplest possible map of this form is when Alice and Bob take the state $\sigma_{ab_0\ldots b_k}$ which is symmetric. Then each σ_i^{out} is the same k extendible state, i.e., $\sigma_i^{out} = \sigma^{out}$. And effectively such a map is equivalent to Alice and Bob removing the initial state, and in its place preparing some k-extendible state. Other example is when the output states are $\sigma_0^{out} = \Phi_{ab}^+$ and $\sigma_i^{out} = \frac{1}{4}\mathrm{I}_{ab_i}$ for $i > 0$.

Using fact 5.1 and the form the CJ state of measure-and-prepare map we obtain that fidelity α is achievable by measure-and-prepare maps if and only if the following operator is nonpositive:

$$Z = \sum_{i=0}^{k}(\alpha - F_i)\mathrm{Tr}(\varrho_{AB}\sigma_{AB_i}) \tag{5.40}$$

where F_i are overlaps of σ_{ab_i} with Φ^+, i.e., $F_i = \mathrm{Tr}(\sigma_{ab_i}\Phi^+)$.

Indeed, following the proof of preposition 5.1 we obtain the following criterion:

Proposition 5.3. *Fidelity $F = \alpha$ is achievable if*

$$\inf_{F_1,\ldots,F_k} \lambda_{\min}(Z) < 0 \tag{5.41}$$

where Z is given by (5.40) *and infimum runs over all k-tuples $(F_1, \ldots, F_k)$ allowed by a joint state $\sigma_{ab_0\ldots b_k}$.*

Remark 5.3. *It is enough to consider $F_0, \ldots, F_k$ from the boundary of the region allowed by a considered state $\sigma_{ab_0\ldots b_k}$.*

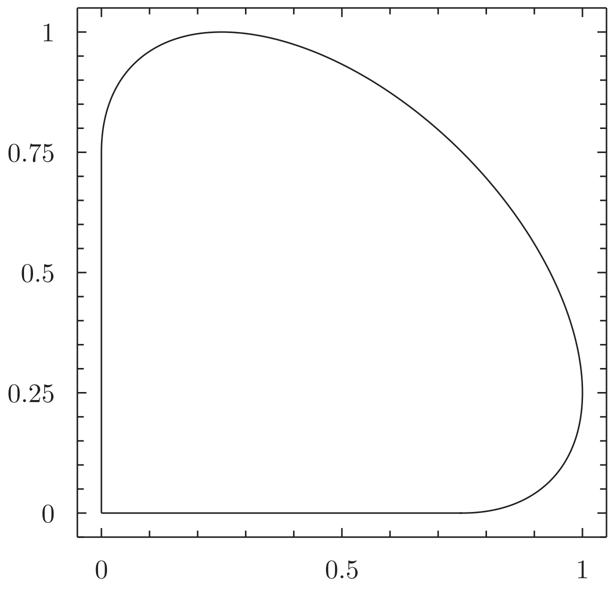

Figure 5.1: Trade-off between fidelities of reductions of a tri-qubit state

Boundary for 1-extendible maps For just one extension, the region of fidelities F_0, F_1 is given by the convex hull of the ellipse [57]:

$$y_+^2 + \frac{1}{3}y_-^2 \leq \frac{1}{16} \tag{5.42}$$

where

$$y_+ = (1 - F_0 - F_1)/2, \quad y_- = (F_0 - F_1)/2. \tag{5.43}$$

and the point $(0, 0)$. This result can also be easily obtained by the use of the orthogonal basis in the linear space of operators that commute with unitary operators of the form $U \otimes U \otimes U$ given in [9]. To this end it is more convenient to consider singlet instead of Φ^+ and then it is enough to restrict to the states that are $U \otimes U \otimes U$ invariant. The allowable region is depicted on figure 5.1.

5.3 The power of k-extendible maps

We first show that k-extendible maps are in general surprisingly powerful:

1. the k-extendible map (for any k) can distill with fidelity $F = 1$ from a single copy of a pure product state,

2. for any k and any state ϱ different from maximally mixed state k-extendible map may distill n copies of ϱ with fidelity arbitrary close to one: for large enough n there exist a k-extendible map that achives the given fidelity.

This unexpected power of k-extendible maps seem to contrast with the fact that in the limit of $k \to \infty$ the k-extendible maps tend to separable maps.

5.3.1 Single copy: Distillation from product states and from identity

Distillation from pure product state Let $\varrho^{AB} = \varrho_A \otimes \varrho_B$ be a product state where ϱ^A is an arbitrary state and $\varrho_B = |0\rangle\langle 0|$ and $|0\rangle$ is an arbitrary fixed vector in subsystem B (for convenience we assume that it belongs to the basis in which transpose is taken in formula (5.22)). Then, it is enough to consider positivity of the operator X'

$$X' = \hat{S}_k \left(|0\rangle\langle 0|_B \otimes M^\alpha_{ab} \otimes \mathrm{I}_{B_1 \ldots B_k, b_1 \ldots b_k} \right) \tag{5.44}$$

where $M^\alpha = \alpha \mathrm{I} - \Phi^+$.

We shall prove the result for $k = 1$. The proof for larger k is analogous. One finds that

$$X' = \frac{1}{2}(P_B \otimes \mathrm{I}_E \otimes M^\alpha_{ab} \otimes \mathrm{I}_e + \mathrm{I}_B \otimes P_E \otimes M^\alpha_{ae} \otimes \mathrm{I}_b) \tag{5.45}$$

$$= \frac{1}{2}(P_B \otimes (P_E + P_E^\perp) \otimes M^\alpha_{ab} \otimes \mathrm{I}_e + (P_B + P_B^\perp) \otimes P_E \otimes M^\alpha_{ae} \otimes \mathrm{I}_b) \tag{5.46}$$

$$= \frac{1}{2}(P_B \otimes P_E \otimes (M^\alpha_{ab} \otimes \mathrm{I}_e + M^\alpha_{ae} \otimes \mathrm{I}_b) \tag{5.47}$$

$$+ P_B \otimes P_E^\perp \otimes M^\alpha_{ab} \otimes \mathrm{I}_e + P_B^\perp \otimes P_E \otimes M^\alpha_{ae} \otimes \mathrm{I}_b) \tag{5.48}$$

where $P = |0\rangle\langle 0|, P^\perp = \mathrm{I} - P$. We see that this operator has a block diagonal form, and e.g., the last block $(P_B^\perp \otimes P_E \otimes M^\alpha_{ae} \otimes \mathrm{I}_b)$ has negative eigenvalue when M^α_{ae} has negative eigenvalue that is for any $\alpha < 1$. Thus fidelity arbitrary close to 1 can be achieved for state ϱ^{AB} by one-extendible maps.

The presented argument also holds, if ϱ_B is proportional to any projector different than identity.

Distillation from maximally mixed state. From the above consideration, it follows that if $\varrho_{AB} = \frac{1}{d_A}\mathrm{I}_A \otimes \frac{1}{d_B}\mathrm{I}_B$, then a 1-extendible map can distill it up to fidelity $F = \alpha$ provided $M_{ab} \otimes \mathrm{I}_e + M_{ae} \otimes \mathrm{I}_b$ is non-positive. One finds that eigenvalues of this operator are equal to $\{2\alpha, (4\alpha - 3)/2, (4\alpha - 1)/2\}$. Thus the operator is non-positive, for $\alpha < 3/4$. Since the state is of a full rank, then not only $F < 3/4$ but also $F = 3/4$ can be obtained.

For k-extendible maps, we need non-positivity of the following operator $\hat{S}_k(M_{ab_0} \otimes \mathrm{I}_{b_1} \otimes \ldots \otimes \mathrm{I}_{b_k})$, where $\hat{S}_k$ symmetrizes over b_i's. Before we discuss the case of k-extendible maps for k larger than 1, let us describe what happened here from another perspective. Namely, the following is a legitimate k-extendible map: to remove the original state, and bring in a k-extendible state σ_{ab}. Indeed, the CJ state of such an operation is given by $\sigma_{ABab} = \frac{1}{d_A}\mathrm{I}_A \otimes \frac{1}{d_B}\mathrm{I}_B \otimes \sigma_{ab}$. (This is clearly a special case of the 'measure-and-prepare' maps.) Thus the fidelity that obviously can be achieved by k-extendible maps is the maximal overlap with Φ^+ possible for a k-extendible bipartite state σ_{ab}. However this is related to universal cloning: such a state would allow to clone with average fidelity (just by teleporting the state through k-extensions of σ_{ab}). The problem of optimal fidelity of universal cloning has been solved e.g., in [58]. Exploiting the formula for 'black cow factor' from this paper, we obtain that the maximal fidelity of k-extendible state on two-qubit system amounts to

$$F_{max}(k) = \frac{1}{2}\frac{k+2}{k+1} \tag{5.49}$$

for $k = 1$ we obtain $F = 3/4$ which is compatible with the above. Thus the maximal fidelity which can be obtained from maximally mixed state by k-extendible operations is given by the formula (5.49).

k-extendible maps are not closed under composition When distilling entanglement with separable and LOCC maps it is enough to obtain $F > 1/2$ and then fidelity arbitrary close to one can also be achieved (see e.g., [18]). As there exists a distillation protocol which achieves fidelity arbitrary close to one for many copies of input state satisfying $F > 1/2$. Such distillation is a concatenation of two protocols: one that achieves $F > 1/2$ and second one which achieves fidelity arbitrary close to one. One can do this because separable and LOCC maps are closed under composition which is not the case for k-extendible maps. This explains why it is possible to obtain fidelity larger than half from a maximally mixed state with a k-extendible map.

k-extendible maps are not stable WRT local embedding The examples of product state and maximally mixed state show that the k-extendible maps are not stable with respect to local embedding into larger Hilbert space. Indeed, the first example goes through, if we replace $|0\rangle\langle 0|$ with whatever projector which does not have full rank. Thus a state $\frac{1}{d}\mathrm{I} \otimes \frac{1}{d}\mathrm{I}$, through the second example is not distillable to maximally entangled state, if it acts on $C^d \otimes C^d$. However, if we consider the same state on $C^d \otimes C^{d'}$ where $d' > d$, fidelity $F = 1$ is possible.

5.3.2 Single copy: A wide class of states which offer $F = 1$

Let us start with a simple condition which, if satisfied, implies that fidelity $F = 1$ can be obtained (with some probability).

Lemma 5.1. *Let ϱ_{AB} be a given state. Suppose, that there exists a state $\sigma_{ABB_1\ldots B_k}$ such that $\mathrm{Tr}(\varrho_{AB}\sigma_{AB_i}) = 0$ and $\mathrm{Tr}(\varrho_{AB}\sigma_{AB}) > 0$, then one can obtain fidelity $F = 1$ from ϱ_{AB} by k-extendible maps.*

Proof. We shall prove for $k = 1$, for larger k proof is similar. We use 'measure-and-prepare' strategy introduced in proposition 5.2. Namely, we take $\sigma_0^{in} = \sigma_{AB}$, $\sigma_1^{in} = \sigma_{AE}$ and $\sigma_0^{out} = \Phi^+_{ab}$, $\sigma_1^{out} = \mathrm{I}_{ab}/4$. Then clearly only outcome $i = 0$ will be observed, and the output state will be Φ^+. □

Proposition 5.4. *If a given state ϱ_{AB} is not a full rank state then one can obtain from a single copy of ϱ_{AB} fidelity $F = 1$ by means of 1-extendible maps (either extendible on Bob's or on Alice's site). The $F = 1$ is achievable by 'measure-and-prepare' maps.*

Proof. We use lemma 5.1. We need to find two bipartite states σ^0_{AB} and σ^1_{AE}, such that they come from some joint tripartite state σ_{ABE} and the first of them has nonzero overlap with ϱ_{AB} and the other one is orthogonal to ϱ_{AB}.

We consider two cases:

1. If there exists a product state $\sigma_A \otimes \sigma_B$ in the kernel of ϱ_{AB} then either

   (a) $\sigma_A \otimes \mathrm{I}_B$ is not in the kernel then we take $\sigma^0_{AB} = \sigma_A \otimes \frac{1}{d_B}\mathrm{I}_B$ and $\sigma^1_{AE} = \sigma_A \otimes \sigma_B$ and by lemma 5.1 we can achieve fidelity $F = 1$ by a 1-extendible map extendible on Bob's site; or

   (b) $\sigma_A \otimes \mathrm{I}_B$ is also in the kernel then there must exist σ'_A such that $\sigma'_A \otimes \mathrm{I}_B$ is not in the kernel (as $\varrho_{AB} \neq 0$) and we take $\sigma^0_{AB} = \sigma'_A \otimes \frac{1}{d_B}\mathrm{I}_B$ and $\sigma^1_{EB} = \sigma_A \otimes \frac{1}{d_B}\mathrm{I}_B$ and by lemma 5.1 we can achieve fidelity $F = 1$ by a 1-extendible map extendible on Alice's site.

2. If there is no product state in the kernel then we take any state from the kernel as σ^1_{AE} and $\sigma^0_{AB} = \sigma^1_A \otimes \frac{1}{d_B}\mathrm{I}_B$ and by lemma 5.1 we can achieve fidelity $F = 1$ by a 1-extendible map extendible on Bobs's site (and also, analogously, on Alice's site).

□

Proposition 5.5. *If a given state ϱ_{AB} has a k-extendible state in the kernel then one can obtain from a single copy of ϱ_{AB} fidelity $F = 1$ by means of $(k+1)$-extendible maps (either extendible on Bob's or on Alice's site).*

Proof. We extend on the proof of proposition 5.4. We consider two cases:

1. If there is a product state in the kernel of ϱ_{AB} then proposition 5.4 gives $\sigma_{ABE} = \sigma_A \otimes \sigma_B \otimes \sigma_E$ which by lemma 5.1 gives fidelity $F = 1$ from a single copy of ϱ_{AB} by means of 1-extendible maps, either extendible on Bob's or on Alice's site. As σ_{ABE} is a product state one can extend it to $\sigma_A \otimes \sigma_B \otimes \sigma_E^{\otimes k}$ for any k to obtain by lemma 5.1 fidelity $F = 1$ from a single copy of ϱ_{AB} by means of $(k+1)$-extendible maps extendible on the same site.

2. If there is no product state in the kernel any state from the kernel can be used as σ_{AE} in the proof of proposition 5.4 so we take the k-extendible one which exists by assumption (we assume it is extendible on Bob's site for states extendible on Alice's site the proof is analogous). Now, since σ_{AE} is k-extendible on Bob's site there exists a state $\sigma_{AB_1\ldots B_{k+1}} \otimes \sigma_B$ such that $\sigma_{AB_i} = \sigma_{AE}$ for i from 1 to $k+1$ and $\sigma_{AB} = \sigma_A \otimes \sigma_B$ by assumption is not in the kernel (as there is no product state in the kernel) and thus, (analogously to the proof of proposition 5.4) by lemma 5.1 we can obtain fidelity $F = 1$ from a single copy of ϱ_{AB} by means of $(k+1)$-extendible maps extendible on Bob's site.

□

The above proposition implies, that any state which has a product state in the kernel can obtain fidelity $F = 1$ from a single copy of the state by k-extendible maps (either extendible on Alice's site or on Bob's site) for all k.

Examples. Consider states ϱ_a and ϱ_s given by (2.71) and proportional to P_a and P_s the projectors onto antisymmetric and symmetric subspaces of $C^d \otimes C^d$, respectively.

The state ϱ_a can obtain fidelity $F = 1$ from a single copy of the state by k-extendible (on both sides) maps for all dimensions for all k. The fidelity $F = 1$ is obtained for all k since the kernel of ϱ_a which is P_s contains a product state. The fidelity $F = 1$ is obtained by maps extendible on both Alice's and Bob's sites since P_a is symmetric with respect to $A \leftrightarrow B$ exchange.

In turn, the state ϱ_s can give $F = 1$ for $k \leq d - 1$. This is because, its complement, the antisymmetric projector is $d - 2$ symmetrically extendible for $d \geq 2$. But by using proposition 5.1 for $d = 3$ we obtain numerically $F = 1$ for each $k \leq 4$ and only for $k \geq 5$ fidelity is decreasing with k (figure 5.3). Which means that for $k = 3$ and $k = 4$ measure-and-prepare maps are to weak to obtain $F = 1$ but general k-extendible maps still can do this.

5.3.3 Many copies: k-extendible maps can distill arbitrary state apart from maximally mixed one

Here we show, that the class of k-extendible maps can distill any state apart from maximally mixed one. We explain this in the case of $k = 1$. The argument for larger k is analogous.

To this end, we consider

$$X = \varrho_{AB}^{\otimes n} \otimes \mathrm{I}_E^{\otimes n} \otimes M_{ab}^{\alpha} \otimes \mathrm{I}_e + \varrho_{AE}^{\otimes n} \otimes \mathrm{I}_B^{\otimes n} \otimes M_{ae}^{\alpha} \otimes \mathrm{I}_b \tag{5.50}$$

By Prop. 5.1 arbitrary fidelity $F < \alpha$ can be obtained if this operator is non-positive for this α. We now argue, that for any $\alpha < 1$, there exists n such that this operator is indeed non-positive. Namely, note that the operator M is non-positive for such α, hence both $M_{ab} \otimes \mathrm{I}_e$ and $M_{ae} \otimes \mathrm{I}_b$ are non-positive. Furthermore, after normalization, the operators $\varrho_{AB}^{\otimes n} \otimes \mathrm{I}_E^{\otimes n}$ and $\varrho_{AE}^{\otimes n} \otimes \mathrm{I}_B^{\otimes n}$ are tensor powers of two distinct states. Therefore they become more and more orthogonal for growing n. In other words, for n large enough, there exist orthogonal projectors P and Q which distinguish the two states with arbitrarily large probability of success. Thus the value $\mathrm{Tr}(XP_{ABE} \otimes \Phi_{ab}^{+} \otimes \mathrm{I}_e)$ will be negative. The exact estimates for the number n of copies needed to obtain negativity for a fixed α can be obtained from Helstrom condition for distinguishing two states (i.e., by estimating trace norm distance between the considered states). For $k > 1$, the same argument applies: we have $k + 1$ different states which are for large n distinguishable by tomography.

5.4 Analytical solution for distillation of Werner states with 1-extendible maps

Let us consider a $d \otimes d$ Werner state in the following parametrization

$$\varrho_W(\gamma) \sim \mathrm{I} - \gamma V \tag{5.51}$$

In this parametrization normalization is not important for our task.

Now, given a Werner state of this form we will compute the analytical formula for the maximum fidelity achievable by applying a 1-extendible map, i.e., $F_1(\varrho_W(\gamma))$. For this task we will use the orthogonal basis in the linear space of operators that commute with unitary operators of the form $U \otimes U \otimes U$ given in [9]. To be able to use this tool, instead of operator $X(\alpha) = \hat{S}_1(X^{\alpha}_{ABab} \otimes \mathrm{I}_{Ee})$ considered in proposition 5.1 we will use similar operator $X'(\alpha)$ where Ψ^- is used instead of Φ^+.

Namely, the operator $X'(\alpha)$ is given by

$$X'(\alpha) = X_1 \otimes Y_1 + X_2 \otimes Y_2 \tag{5.52}$$

where

$$\begin{aligned} X_1 &= \varrho_{AB} \otimes \mathrm{I}_E, & X_2 &= \varrho_{AE} \otimes \mathrm{I}_B \\ Y_1 &= \tilde{M}^{\alpha}_{ab} \otimes \mathrm{I}_e, & Y_2 &= \tilde{M}^{\alpha}_{ae} \otimes \mathrm{I}_b \end{aligned} \tag{5.53}$$

The states ϱ_{AB} and ϱ_{AE} denote the same Werner state given by (5.51) on subsystems AB and AE, as given in respective subscript. Instead of M^{α} we use $\tilde{M}^{\alpha} = \alpha\mathrm{I} - \Psi^-$ thus all operators given by (5.53) are invariant with respect to unitary operations of the form $U \otimes U \otimes U$ which allows us orthogonal basis of such a linear space given in [9].

Now, analogously to the proposition 5.1 we have

$$F_1(\varrho_W(\gamma)) > \alpha \iff \lambda_{\min}(X'(\alpha)) < 0 \tag{5.54}$$

and as Werner states (apart from the boundary ones $\gamma = -1$ and $\gamma = 1$) are full rank states we also have

$$F_1(\varrho_W(\gamma)) < \alpha \iff \lambda_{\min}(X'(\alpha)) > 0 \tag{5.55}$$

$$F_1(\varrho_W(\gamma)) = \alpha \iff \lambda_{\min}(X'(\alpha)) = 0. \tag{5.56}$$

Clearly, X_i are positive. From section 5.3.1, we also know that for $\alpha \geq 3/4$, $Y_1 + Y_2$ is positive too. But $\alpha = 3/4$ can be obtained from any state by 1-extendible maps (by replacing it with a suitable symmetrically extendible state, as discussed in sec. 5.3.1), so it is enough to work with $Y_1 + Y_2$ positive. Let us remind that all the four operators are invariant with respect to unitary operations of the form $U \otimes U \otimes U$. Thus, according to [9], each of them is a linear combination of the following operators

$$\begin{aligned}
R_+ &= \frac{1}{6}(\mathrm{I} + V_{(12)} + V_{(13)} + V_{(23)} + V_{(123)} + V_{(321)}),\\
R_- &= \frac{1}{6}(\mathrm{I} - V_{(12)} - V_{(13)} - V_{(23)} + V_{(123)} + V_{(321)}),\\
R_0 &= \mathrm{I} - R_+ - R_-,\\
R_1 &= \frac{1}{3}(2V_{(23)} - V_{(13)} - V_{(12)}),\\
R_2 &= \frac{1}{\sqrt{3}}(V_{(12)} - V_{(13)}),\\
R_3 &= \frac{i}{\sqrt{3}}(V_{(123)} - V_{(321)}).
\end{aligned} \tag{5.57}$$

Here, V_σ are swaps, permuting systems according to permutation σ (written down in terms of cycles), for e.g.,

$$V_{(12)}|\psi_1 \otimes \psi_2 \otimes \psi_3\rangle = |\psi_2 \otimes \psi_1 \otimes \psi_3\rangle \tag{5.58}$$

$$V_{(123)}|\psi_1 \otimes \psi_2 \otimes \psi_3\rangle = |\psi_3 \otimes \psi_1 \otimes \psi_2\rangle. \tag{5.59}$$

The operator $R_\pm, R_0$ are orthogonal projectors, R_+, R_- being totally symmetric and antisymmetric ones, respectively. The operators R_i, $i = 1, 2, 3$ have support on R_0. This subspace can be decomposed into tensor product of two Hilbert spaces, one of them being a qubit. There is a decomposition such that we have $R_i = \mathrm{I} \otimes \sigma_i$, where σ_i are Pauli matrices, $R_0 = \mathrm{I} \otimes \mathrm{I}_2$.

So we can write

$$\begin{aligned}
X_1 &= \sum_{i\in\mathcal{I}} s_i R_i, & X_2 &= \sum_{i\in\mathcal{I}} \tilde{s}_i R_i\\
Y_1 &= \sum_{i\in\mathcal{I}} t_i R_i, & Y_2 &= \sum_{i\in\mathcal{I}} \tilde{t}_i R_i
\end{aligned} \tag{5.60}$$

where $\mathcal{I} = \{0, 1, 2, 3, +, -\}$. Now, since X_1 and X_2 differ only by a permutations of subsystems, then $s_\pm = \tilde{s}_\pm$ and similarly $t_\pm = \tilde{t}_\pm$. Therefore, due to positivity of X_i and Y_1+Y_2 we obtain that $s_\pm, \tilde{s}_\pm \geq 0$ and $t_+, \tilde{t}_+ \geq 0$. Moreover $t_- = \tilde{t}_- = 0$, as Y_i act on three qubits, where the antisymmetric projector is missing.

This implies that the operator $X_1 \otimes Y_1 + X_2 \otimes Y_2$ is positive if and only if the following two qubit operator is positive

$$X'_{2q}(\alpha) = \frac{1}{2}(X_1^q \otimes Y_1^q + X_2^q \otimes Y_2^q) \tag{5.61}$$

where

$$\begin{aligned}
X_1^q &= \sum_{i=0}^{3} s_i \sigma_i, & X_2^q &= \sum_{i=0}^{3} \tilde{s}_i \sigma_i\\
Y_1^q &= \sum_{i=0}^{3} t_i \sigma_i, & Y_2^q &= \sum_{i=0}^{3} \tilde{t}_i \sigma_i
\end{aligned} \tag{5.62}$$

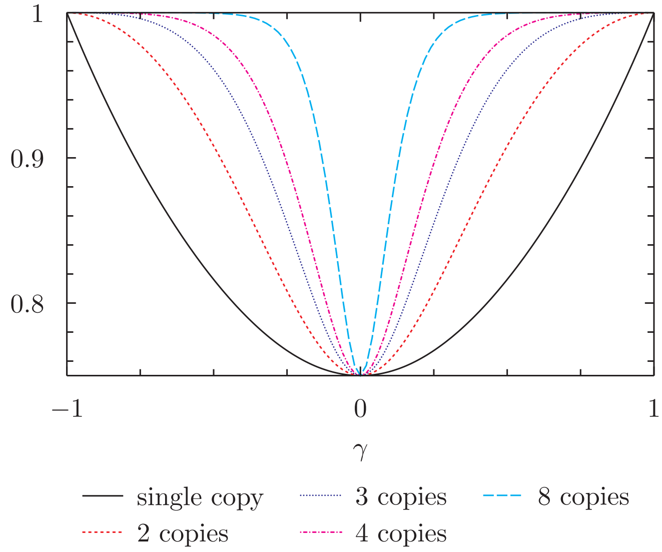

Figure 5.2: Fidelity achievable by 1-extendible maps on n copies of Werner state. $\mathrm{I} - \gamma V$ parametrization is used. One can observe that given sufficiently many copies all states except maximally mixed one are distillable with 1-extendible map with arbitrary fidelity. For $n = 1$ we use the analytical solution (5.76) for more copies we do numerical computations using the method described in section 5.4.

Here σ_0 is the identity on the qubit space and other σ_i are Pauli matrices.

Now, in (5.54)–(5.56) we can use simpler operator $X'_{2q}(\alpha)$ instead of $X'(\alpha)$ as one of them is positive if and only if the other one is positive.

The coefficients s_i etc. can be easily computed, e.g., $s_i = \mathrm{Tr}(X_1 R_i)/\mathrm{Tr}(R_i^\dagger R_i)$: as each of X_i and Y_i is a linear combination of the identity and one of $V_{(12)}$ or $V_{(13)}$ so one can first compute $\mathrm{Tr}(V_{(12)} R_i)/\mathrm{Tr}(R_i^\dagger R_i)$, $\mathrm{Tr}(V_{(13)} R_i)/\mathrm{Tr}(R_i^\dagger R_i)$ and $\mathrm{Tr}(R_i)/\mathrm{Tr}(R_i^\dagger R_i)$, and compute s_i etc. as the proper combination of those.

We obtain

$$s_0 = 1 \qquad t_0 = -\frac{1}{2} + \alpha \tag{5.63}$$

$$s_1 = -\frac{1}{2}\gamma \qquad t_1 = -\frac{1}{4} \tag{5.64}$$

$$s_2 = \frac{\sqrt{3}}{2}\gamma \qquad t_2 = \frac{\sqrt{3}}{4} \tag{5.65}$$

$$s_3 = 0 \qquad t_3 = 0 \tag{5.66}$$

$$\tilde{s}_i = \begin{cases} s_i & i \in \{0,1,3\} \\ -s_i & i = 2 \end{cases} \qquad \tilde{t}_i = \begin{cases} t_i & i \in \{0,1,3\} \\ -t_i & i = 2 \end{cases} \tag{5.67}$$

The two qubit operator $X'_{2q}(\alpha)$ given by (5.61) has the following form in terms of the coefficients s_i and t_i

$$X'_{2q}(\alpha) = \begin{bmatrix} s_0t_0 & s_0t_1 & s_1t_0 & s_1t_1 - s_2t_2 \\ s_0t_1 & s_0t_0 & s_2t_2 + s_1t_1 & s_1t_0 \\ s_1t_0 & s_2t_2 + s_1t_1 & s_0t_0 & s_0t_1 \\ s_1t_1 - s_2t_2 & s_1t_0 & s_0t_1 & s_0t_0 \end{bmatrix} \tag{5.68}$$

and its eigenvalues are given by

$$\lambda_{1,2} = \pm\sqrt{s_2^2t_2^2 + (s_0t_1 - s_1t_0)^2} - s_1t_1 + s_0t_0 \tag{5.69}$$

$$\lambda_{3,4} = \pm\sqrt{s_2^2t_2^2 + (s_0t_1 + s_1t_0)^2} + s_1t_1 + s_0t_0. \tag{5.70}$$

We have to find α_1 such that for any α less then α_1 at least one of eigenvalues $\lambda_2 \leq \lambda_1$ and $\lambda_4 \leq \lambda_3$ is negative. It turns out that both λ_2 and λ_4 are zeroed for the same $\alpha = \alpha_1$ which is the greater of the roots of the equation

$$s_2^2t_2^2 + (s_0t_1 \mp s_1t_0)^2 = (s_1t_1 \mp s_0t_0)^2 \tag{5.71}$$

which is (up to the normalization) equivalent to a quadratic equation

$$(16 - 4\gamma^2)\alpha^2 - (16 - 4\gamma^2)\alpha + (3 - 3\gamma^2) = 0. \tag{5.72}$$

The greater of the solutions of (5.72) has the form

$$\alpha_{\max} = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+2\gamma^2}{4-\gamma^2}}. \tag{5.73}$$

Due to using of the $\mathrm{I} - \gamma V$ parametrization of the Werner state the solution (5.73) has a simple dimension independent form and is a symmetric function.

For all $\alpha < \alpha_{\max}$ operator $X'_{2q}(\alpha)$ and for $\alpha_{\max}$ it is positive with two zero eigenvalues thus by considering (5.54)–(5.56) we finally obtain

$$F_1(\varrho_W(\gamma)) = \frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+2\gamma^2}{4-\gamma^2}}. \tag{5.74}$$

One can transform (5.74) to a $d \otimes d$ parametrization of the Werner state $\varrho_W(p)$ given by (2.70). The transformation can be done using the substitution

$$\gamma = -\frac{2dp - d - 1}{2p - d - 1}. \tag{5.75}$$

In particular for $d = 4$ we obtain

$$F_1(\varrho_W(p)) = \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{15p(1-p)}{25 - 16p^2}}. \tag{5.76}$$

We see that any Werner state apart from maximally mixed one has fidelity larger than 3/4.

5.4.1 Distillation of Werner states by 1-extendible measure-and-prepare maps

We now consider a single copy of a Werner state and the 'measure-and-prepare' 1-extendible maps. We shall show that the fidelity is the same as in the case of all 1-extendible maps. To this end, we need to find minimum eigenvalue of the operator Z given by (5.41). Using the method from the previous section, we can write Z as

$$Z = (\alpha - F_1)X_1 + (\alpha - F_2)X_2 \tag{5.77}$$

where X_i are given by (5.60). We obtain that

$$Z_q = \sum_{i=0}^{3} \beta_i \sigma_i \tag{5.78}$$

where β_i are given by

$$\beta_i = (\alpha - F_1)s_i + (\alpha - F_2)\tilde{s}_i \tag{5.79}$$

Recall, that $s_3 = \tilde{s}_3 = 0$. Here Z_q denotes the restriction of Z to the qubit, similarly as it was for for X_i^q and Y_i^q.

The operator is positive if and only if

$$\sum_{i=1}^{3} \beta_i^2 \leq \beta_0^2 \tag{5.80}$$

If we put equality there are the following two solutions:

$$\alpha_{1,2} = \frac{1}{2} - y_+ \pm |y_-| f(p,d) \tag{5.81}$$

where

$$f(p,d) = \frac{\sqrt{3}|-2dp + d + 1|}{\sqrt{((2(d-2)p + d + 1))(3(d+1) - 2(d+2)p)}} \tag{5.82}$$

and

$$y_+^2 + \frac{1}{3} y_-^2 = \frac{1}{16} \tag{5.83}$$

with $y_\pm$ given by (5.43). (Note, that the pair of fidelities (0, 0) is not relevant here, and moreover it is enough to consider extremal points of the region of pairs of fidelities, hence we can confine ourselves to (5.83)). We have now to maximize the α's over y_+, y_- satisfying the above constraints. This gives

$$\alpha_{max} = \frac{1}{4}\left(\sqrt{3f(p,d)^2 + 1} + 2\right) \tag{5.84}$$

which, once applied (2.70), is exactly the same as the fidelity achievable with the general 1-extendible map given in equation (5.74).

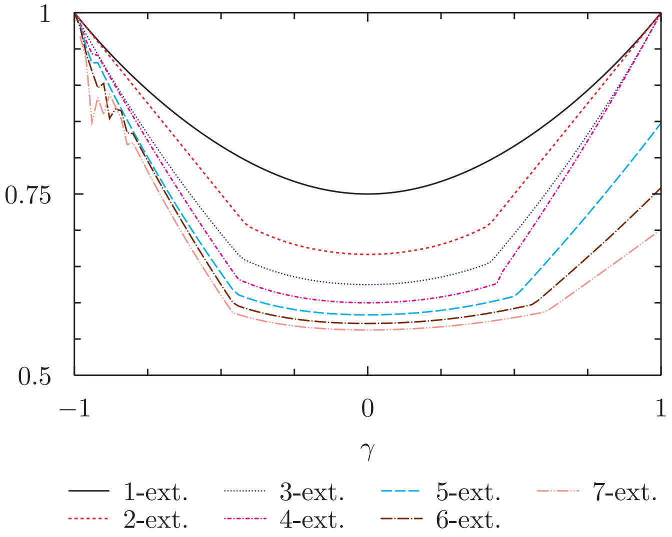

Figure 5.3: Fidelity achievable by means of k-extendible maps for a single copy of Werner state with $d = 3$.

Two copies Note, that in $I + \gamma V$ parametrization, α_{max} does not depend on dimension, which is partially responsible for its very simple form. However the parametrization does not help much for two copies – we are able to obtain the expression for eigenvalues of the expression for two copies

$$X_1^q \otimes X_1^q \otimes Y_1^q + X_2^q \otimes X_2^q \otimes Y_2^q \tag{5.85}$$

in terms of s_i and t_i but these are huge expressions and even after substituting s_i and t_i, i.e., in terms of α and γ they stay huge.

5.4.2 More copies and more extensions

We have obtained numerical results for larger number of copies and k-extendible maps with larger k. We present the results on subsequent figures. On figure 5.2 we present the plot for exemplary numbers of copies up to $n = 8$, and for 1-extendible maps. For $n = 1$ we use the analytical solution (5.76) while for more copies we do numerical computations i.e. we are diagonalizing the operators of the sort of (5.85) with number of X's equal to number of copies. The plot confirms the result of section 5.3.3: for larger and larger number of copies, the fidelity of any state but the maximally mixed one tend to 1.

We have also done exemplary numerical calculations for more extensions and more copies. On figure 5.3 we consider single copy, and k-extendible maps up to $k = 7$. We see that up to $k = 4$ the fidelity for symmetric state (one with $\gamma = 1$) has fidelity equal to 1, and only for $k \geq 5$ the fidelity drops down. As discussed in section 5.3.2, we have analytical proof that $F = 1$ for $k \leq 2$, while the cases of $k = 3, 4$ are still not fully understood. We also can see, that up to $k = 4$ the plots are symmetric with respect to maximally mixed state ($\gamma = 0$). This means

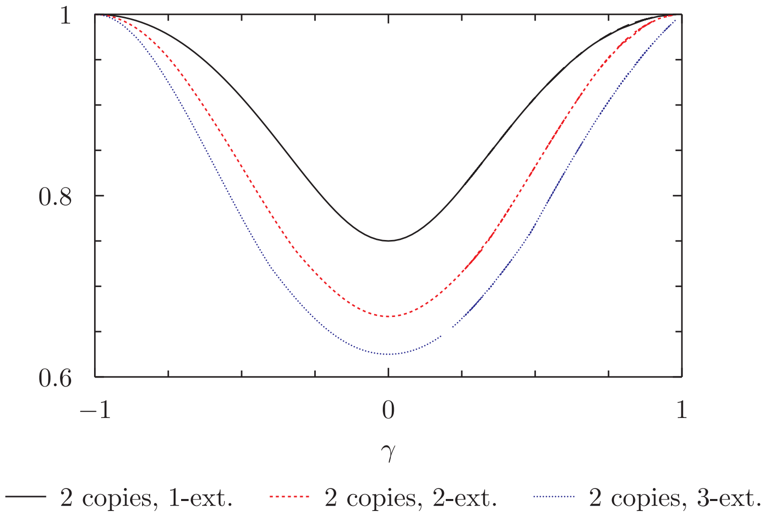

Figure 5.4: Fidelity for two copies, and $k = 1$, 2 and 3 extendible maps. The larger the number k, the lower the curve.

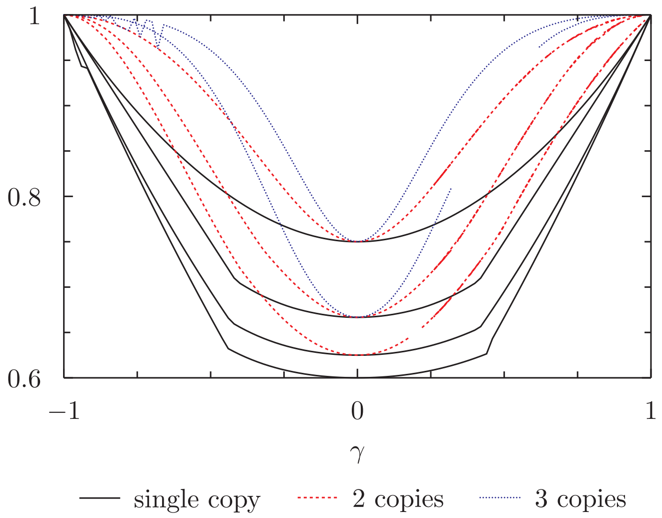

Figure 5.5: Fidelity achievable by means of k-extendible maps for single, two and three copies

that for the classes of k-extendible maps up to $k = 4$, entanglement/separability property of Werner states is completely irrelevant.

Note also, that once k is growing two cusps are forming: the right one will materialize in the coordinates $(\alpha = \frac{1}{2}, \gamma = 1)$ and will mean, that all state with $\gamma > 0$ are not distillable. The left one tends to $(\alpha = \frac{1}{2}, \gamma = -\frac{1}{2}$, where it will constitute the boundary of distillable region according to [8]. Finally, on figure 5.4 we consider two copies and k-extendible maps with $k = 1, 2, 3$ for $d = 3$. and on figure 5.5 we put all the plots together, to visualize, what happens if we change both the number of copies of the state and the number of extensions for the maps.

Chapter 6

Computer tools used during the research

During the research presented in this thesis computer aided computations where used. Both analytical and numerical computations where performed. All presented tools are free software and open source.

Numerical computation For numerical computation a programing language Python[1] was used. Python is an interpreted programming language which allows for quick writing of code and easy debugging. Python together with a Python library NumPy[2] (which adds multidimensional arrays to the Python language) makes an excellent environment for linear algebraic numerical computations. The author of the thesis during his research in quantum information has developed a Python library called *lpqph*[3] (not published) based on NumPy arrays and implementing many functions useful in the context of quantum information. Including an implementation of the Genetic Algorithm and a function which returns a unitary matrix given a vector of random numbers (implementation of an algorithm proposed in [36]) suitable in optimizations with Genetic Algorithm. The Genetic Algorithm was used to obtain first forms of operator X for mixing two private bits (section 3.1) then analytical form was obtained from numerical results and the obtained analytical form was improved and generalized to the form given by (3.3). Genetic Algorithm was also used in the research presented in chapter 4 to confirm numerically the half-property and to obtain numerical upper bounds for the half-property.

To obtain data for most of the plots[4] presented in chapter 5 a Python library called Pysparse[5] was used which includes fast sparse matrix implementation and

[1] http://python.org/

[2] http://numpy.scipy.org/

[3] Partially written in the language C to improve performance and using the tool called Pyrex (http://www.cosc.canterbury.ac.nz/greg.ewing/python/Pyrex/) which greatly simplifies writing Python extensions.

[4] All plots except figure 5.2 which was obtained using the method presented in section 5.4

[5] http://pysparse.sourceforge.net/

the JDSYM algorithm for finding eigenvalues and eigenvectors. The implementation of the JDSYM algorithm apart from sparse matrix implementation provided by Pysparse may use any other matrix implementation which supports matrix-vector multiplication. Such memory-optimized matrix implementation was developed during the research presented in chapter 5. This research works on huge matrices (even $2 \cdot 10^6 \times 2 \cdot 10^6$) for which we had to compute the eigenvalues. Fortunately those matrices are direct sums of smaller blocks so to compute eigenvalues of the whole matrix one can compute eigenvalues of the individual blocks. Matrices of this size does not fit at once in computers memory so we had to split the matrix into blocks (without building the whole matrix) and then prepare blocks in multiple runs in each run preparing such number of blocks which will fit into memory and then compute their eigenvalues.

Analytical computation For analytical computations we used a Computer Algebra System called Maxima[6] and the Python library for symbolic computations called SymPy[7].

Figures Plots were prepared using graph plotting program PyXPlot[8] and other figures were prepared using PGF[9] (Portable Graphics Format) which is a TeX macro allowing for preparation of high-quality graphics.

[6] http://maxima.sourceforge.net/

[7] http://code.google.com/p/sympy/

[8] http://www.pyxplot.org.uk/

[9] http://sourceforge.net/projects/pgf/

Chapter 7

Conclusion

In the thesis two quantum communicational problems where investigated: the problem of the existence of NPT bound entangled states and the problem of key-distillability of PPT entangled states.

Key-distillability of PPT entangled states In chapter 3, in the area of key-distillability of PPT states mixtures of two and four specially chosen private bits (also called pbits) were introduced. The construction is possible in low dimensions starting from $4 \otimes 4$.

For the mixtures of two private bits their key-distillability using Devetak-Winter protocol was considered and the rate of distillation of the private key (efficiency of key distillation in bits of private key per copy of the state) was computed. Mixtures of two pbits laying on the boundary of PPT states was presented which are key-distillable PPT states possible even in low dimension $(4 \otimes 4)$.

For mixtures of four private bits Devetak-Winter protocol was used with recurrence preprocessing. In contrast to mixing two private bits the rate of key distillation was not considered: the key distillation was only considered existentially not quantitatively. For the four pbits case separability conditions were introduced and the key-distillable class of PPT states approaching arbitrary close to the set of separable states was presented. The decomposition of $4 \otimes 4$ class ϱ_H was provided which allows for experimental realization of the states of the class in the lab.

Also Devetak-Winter protocol with recurrence and sole Devetak-Winter protocol where compared in the context of tolerable white noise in the case of mixing two pbits. Moreover maximal von Neumann entropy was compared between the PPT key-distillable mixtures of two pbits and four pbits. Links of our research with distillability via erasure channel were considered. Finally, a sufficient condition for key-distillability for general states was provided.

One could extend on our research and compute the rate of distillation of private key in the case of mixing four private bits using Devetak-Winter protocol with recurrence preprocessing. An interesting open question is whether all PPT entangled states are key-distillable? Or whether PPT key-distillable states are only in close neighborhoods of mixtures of private bits?

Distillation of NPT Werner state by half-property In chapter 4 the problem of n-undistillability of the most entangled of the NPT *suspicious* Werner states for $d = 4$ was considered. Let us denote this state with ϱ_W. The n-undistillability of ϱ_W was translated to the equivalent problem of the so-called *half-property.* The state ϱ_W is n-undistillable if the overlap of the Schmidt rank two states ϕ_2 with projector Q_n does not exceed $1/2$. A particular Schmidt rank two state ϕ_2 which satisfies $\langle\phi_2|Q_n|\phi_2\rangle \leq \frac{1}{2}$ is said to have the half-property.

It is known that ϱ_W is 1-undistillable. So first, the problem of 2-undistillability of ϱ_W was considered: the problem was not solved but wide range of the Schmidt rank two states was shown to have the half-property for $n = 2$. It was shown that there are nontrivial maxima of the overlap of Q_2 with Schmidt rank two states which shows that one could not consider only Schmidt rank two states product in the cut between the copies. Then the half-property problem for $n = 2$ was translated into a matrix analysis problem. The matrix analysis problem was solved for normal matrices which translates back to the half-property as follows: all Schmidt rank two states ϕ_2 which has the 'normal' projection on Q_2 (i.e., $Q_2|\phi_2\rangle$ is isomorphic through the so-called state-operator isomorphism to a normal matrix) satisfy the half-property. Also using the notion of so-called *common degrees of freedom* it was shown that any state having on each pair at least one subsystem with one qubit support satisfies the half-property.

For general n, maximal overlap of product states ϕ_1 with the projector Q_n was computed and also the form of ϕ_1 states attaining the maximum was provided. Also bounds on the overlap $\langle\phi_2|Q_n|\phi_2\rangle$ in terms of the overlap $\langle\phi_1|Q_n|\phi_1\rangle$ was given but in the limit of $n \to \infty$ it, unfortunately, gives the trivial bound that the overlap does not exceed one. For $n = 2$ numerical bounds better than $3/4$ (which comes from $\langle\phi_1|Q_2|\phi_1\rangle$) was provided and the analytical bound of $0.74971 < 3/4$ given in [6] was recalled.

One could extend on our research by analytically proving one of the numerical bounds or even better by solving the matrix analysis problem for general matrices to prove 2-undistillability of ϱ_W. There is still the open and hard problem of whether there are NPT bound entangled states.

Distillation using extendible maps In chapter 5 distillation of entanglement using so called k-extendible maps was considered. The k-extendible maps for large k in a sense converge to separable maps and are shrinking supersets of the separable maps (so in a limit of $k \to \infty$ one obtains standard distillation of entanglement). Those wider than LOCC classes of operations are used because they are easier in mathematical consideration than LOCC maps. One may hope that using k-extendible maps some *suspicious* Werner states may be proven undistillable.

First, for a given state ϱ the supremum of the fidelity of $\Lambda(\varrho)$ with singlet where the supremum is taken over all k-extendible maps was considered. Let us denote this supremum with $F_k(\varrho)$. The value of the supremum $F_k(\varrho)$ was then connected to positivity of some matrix. Then a subclass of k-extendible maps called 'measure-and-prepare' maps was introduced and supremum over this class was also connected to positivity of some (lower dimensional) matrix but parametrized with k parameters.

Later it was shown that, although k-extendible maps in a sense converge to the class of separable maps for large k, they are surprisingly powerful. First of all, for any fixed k, the class of k-extendible maps can distill any state but maximally mixed one, if large enough number of copies is available. Second, even in single copy case, the maps can provide fidelity 1 (with some nonzero probability) for any state which has a $(k-1)$-extendible state in its kernel. In particular, k-extendible maps are not stable under local embedding into a larger Hilbert space.

Then, for the Werner states, the analytical formula for $F_1(\varrho_W)$ was obtained using the orthogonal basis in the linear space of operators that commute with unitary operators of the form $U \otimes U \otimes U$ given in [9]. Analogously, the analytical formula was obtained for the subclass of 1-extendible 'measure-and-prepare' maps which happens to be identical to the formula for all 1-extendible maps, i.e., to $F_1(\varrho_W)$.

Finally, numerical computations were used to obtain plots of $F_k(\varrho_W^{\otimes n})$ for some values of the number of extensions k and the number of copies n. In case of $k=1$ the above basis from [9] was used allowing us to go with the number of copies up to $n=8$. For $k>1$ direct computation (but highly optimized) was used.

To extend on our research, one can use the irreducible representation of symmetric group for $k>1$ which would allow to obtain plots with higher number of copies for $k>1$ and may be one could perhaps also obtain an analytical formula for $F_2(\varrho_W)$.

Appendix A

Proof of a proposition A.1

Lemma A.1. *The minimum value of* $\sum_{i=1}^{d}|\tilde{a}_i|^2$ *subject to* $\sum_{i=1}^{d}\tilde{a}_i = z$ *where* $\tilde{a}_i, z \in \mathbb{C}$ *is obtained by settings* $\tilde{a}_i = \frac{z}{d}$.

Proof. From the parallelogram identity we have

$$\frac{1}{2}|\tilde{a}_i+\tilde{a}_j|^2 = |\tilde{a}_i|^2+|\tilde{a}_j|^2-\frac{1}{2}|\tilde{a}_i-\tilde{a}_j| \leq |\tilde{a}_i|^2+|\tilde{a}_j|^2 \tag{A.1}$$

with equality iff $\tilde{a}_i = \tilde{a}_j$. Thus whenever for some $\tilde{a}_i$, $\tilde{a}_j$ we have $\tilde{a}_i \neq \tilde{a}_j$ we can replace them with two instances of $\frac{\tilde{a}_i+\tilde{a}_j}{2}$ decreasing the value of $\sum_{i=1}^{d}|\tilde{a}_i|^2$ and leaving the constrain satisfied. This implies that the optimal solution is to take all $\tilde{a}_i$ equal, i.e., $\tilde{a}_i = \frac{z}{d}$. □

Proposition A.1. *For all* $d \geq 3$ *dimensional vectors* $\vec{a}$ *and* $\vec{b}$ *with complex elements* $\tilde{a}_i$ *and* $\tilde{b}_i$ *and satisfying the constraints*

$$\sum_{i=1}^{d}\tilde{a}_i = \sum_{i=1}^{d}\tilde{b}_i = 0, \qquad \sum_{i=1}^{d}|\tilde{a}_i|^2+\sum_{i=1}^{d}|\tilde{b}_i|^2 = \frac{1}{d} \tag{A.2}$$

the following equality holds

$$\max_{\vec{a},\vec{b}}\left(|\tilde{a}_1+\tilde{b}_1|^2+|\tilde{a}_1+\tilde{b}_2|^2\right) = \frac{3d-4}{d^2}. \tag{A.3}$$

Corollary A.1. *For* $d=4$ *under this constraints we have*

$$\max_{\vec{a},\vec{b}}\left(|\tilde{a}_1+\tilde{b}_1|^2+|\tilde{a}_1+\tilde{b}_2|^2\right) = \frac{1}{2}. \tag{A.4}$$

Proof of proposition A.1. We denote function (A.3) as f, the vector of all $\tilde{a}_i$ as $\vec{a}$, the vector of all $\tilde{b}_i$ as $\vec{b}$, and we use their polar decompositions

$$\tilde{a}_i = a_i e^{i\alpha_i}, \quad \tilde{b}_i = b_i e^{i\beta_i}, \quad a_i, b_i \in \mathbb{R}. \tag{A.5}$$

In optimizing function f under the constraints (A.2) we shrink the set of possible $\vec{a}$ and $\vec{b}$ in such a way to simplify the form of f and the constraints but keeping at least one of the global maxima within the shrinking set.

1. Without loss of generality we can take $\tilde{a}_1 = a_1 \geq 0$. Thus we optimize

$$f(\vec{a},\vec{b}) = |a_1 + \tilde{b}_1|^2 + |a_1 + \tilde{b}_2|^2 \tag{A.6}$$
$$= 2a_1^2 + b_1^2 + b_2^2 + 2a_1(b_1 \cos\beta_1 + b_2 \cos\beta_2). \tag{A.7}$$

2. We can consider only $\vec{b}$ for which

$$b_1 \cos\beta_1 + b_2 \cos\beta_2 \geq 0. \tag{A.8}$$

(If it is negative we can change its sign by multiplying $\vec{b}$ by $e^{i\pi}$ and thus increase f).

3. In maximizing f under the constraints it is always best to set

$$\tilde{a}_i = -\frac{a_1}{d-1} \qquad (i > 1) \tag{A.9}$$
$$\tilde{b}_i = -\frac{1}{d-2}(\tilde{b}_1 + \tilde{b}_2) \qquad (i > 2) \tag{A.10}$$

Indeed, whenever this setting is not used we can by lemma A.1 obtain some freedom in the second constraint which we can use to increase a_1 and one of b_1 or b_2 without decreasing f. Thus it is enough to consider $\vec{a}$ and $\vec{b}$ satisfying this setting, i.e., we optimize function $f(a_1, \tilde{b}_1, \tilde{b}_2)$ subject to the following constraints

$$\frac{d}{d-1}a_1^2 + b_1^2 + b_2^2 + \frac{1}{d-2}\left|\tilde{b}_1 + \tilde{b}_2\right|^2 = \frac{1}{d},$$
$$a_1 \geq 0, \quad b_1 \cos\beta_1 + b_2 \cos\beta_2 \geq 0. \tag{A.11}$$

4. Further we show that it is enough to consider $\tilde{b}_1, \tilde{b}_2 \in \mathbb{R}$ as replacing $\tilde{b}_1$ with $\tilde{b}_1' = b_1 \cos\beta_1$ and $\tilde{b}_2$ with $\tilde{b}_2' = b_2 \cos\beta_2$ and changing a_1 to a_1' to fit the constraint does not decrease f, i.e., $f(a_1', \tilde{b}_1', \tilde{b}_2') \geq f(a_1, \tilde{b}_1, \tilde{b}_2)$. Namely we have

$$f(a_1', \tilde{b}_1', \tilde{b}_2') = 2a_1'^2 + b_1^2\cos^2\beta_1 + b_2^2\cos^2\beta_2 + 2a_1'(b_1\cos\beta_1 + b_2\cos\beta_2) \tag{A.12}$$

and the main constraint is

$$\frac{d}{d-1}a_1'^2 + b_1^2\cos^2\beta_1 + b_2^2\cos^2\beta_2 + \frac{1}{d-2}\left|b_1\cos\beta_1 + b_2\cos\beta_2\right|^2 = \frac{1}{d}. \tag{A.13}$$

First we show that $a_1' \geq a_1$ which is evident from the difference of main constraints

$$\frac{d}{d-1}(a_1'^2 - a_1^2) = b_1^2\sin^2\beta_1 + b_2^2\sin^2\beta_2 + \frac{1}{d-2}\left(\left|b_1e^{i\beta_1} + b_2e^{i\beta_2}\right|^2 - \left|b_1\cos\beta_1 + b_2\cos\beta_2\right|^2\right) \geq 0. \tag{A.14}$$

Next we use this difference to show that f does not decrease after the replacement

$$
\begin{aligned}
f(a_1', \tilde{b}_1', \tilde{b}_2') - f(a_1, \tilde{b}_1, \tilde{b}_2)& \\
&= 2(a_1'^2 - a_1^2) - b_1^2 \sin^2 \beta_1 - b_2^2 \sin^2 \beta_2 \\
&\quad + 2(a_1' - a_1)(b_1 \cos \beta_1 + b_2 \cos \beta_2) \\
&\qquad \geq \frac{d-2}{d}(b_1^2 \sin^2 \beta_1 + b_2^2 \sin^2 \beta_2) \geq 0. \qquad (A.15)
\end{aligned}
$$

So we can focus on a problem with $\tilde{b}_1, \tilde{b}_2 \in \mathbb{R}$

$$
\begin{aligned}
f(a_1, b_1, b_2) &= 2a_1^2 + b_1^2 + b_2^2 + 2a_1(b_1 + b_2) \qquad (A.16) \\
\frac{d}{d-1} a_1^2 + b_1^2 + b_2^2 &+ \frac{1}{d-2}(b_1 + b_2)^2 = \frac{1}{d}, \\
a_1 \geq 0, &\quad b_1 + b_2 \geq 0. \qquad (A.17)
\end{aligned}
$$

5. In analogous way we show that it is enough to consider $b_1 = b_2 \geq 0$ as taking $b_1' = b_2' = \frac{|b_1+b_2|}{2}$ and changing a_1 to a_1' to fit the constraint does not decrease f. Then the optimization simplifies to

$$
\begin{aligned}
f(a_1, b_1) &= 2(a_1 + b_1)^2 \qquad (A.18) \\
\frac{d}{d-1} a_1^2 + \frac{2d}{d-2} b_1^2 &= \frac{1}{d}, \quad a_1, b_1 \geq 0. \qquad (A.19)
\end{aligned}
$$

6. We compute b_1 from the constraint and substitute to f which gives

$$
f(a_1) = 2\left(a_1 + \sqrt{x - y a_1^2}\right)^2 \qquad (A.20)
$$

$$
a_1 \in \left[0, \sqrt{x/y}\right] \qquad (A.21)
$$

where

$$
x = \frac{d-2}{2d^2}, \qquad y = \frac{d-2}{2(d-1)}. \qquad (A.22)
$$

Function f has its maximum when the expression in the parenthesis has the maximum (as it is nonnegative). We consider its derivative

$$
\frac{\partial}{\partial a_1}\left(a_1 + \sqrt{x - y a_1^2}\right) = 1 - \frac{y a_1}{\sqrt{x - y a_1^2}} \qquad (A.23)
$$

which is zero for

$$
a_1^\star = \sqrt{\frac{x}{y^2 + y}} \qquad (A.24)
$$

and the second derivative is negative in $a_1^\star$ so the maximum is equal to

$$f(a_1^\star) = 2\left(\sqrt{\frac{x}{y^2+y}} + \sqrt{\frac{xy}{y+1}}\right)^2 = 2x(y^{-1}+1) = \frac{3d-4}{d^2} \qquad \text{(A.25)}$$

The global maximum could also be on one of the boundaries but for $d \geq 3$ $f(a_1^\star)$ is always greater than the values on the boundaries.

□

Bibliography

[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] 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

[5] 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

[6] 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]

[7] 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

[8] 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

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

[10] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?.” Phys. Rev. **47**, 777–780 (1935)

[11] E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," Naturwissenschaften **23**, 807–812 (1935)

[12] John S. Bell, "On the Einstein Podolsky Rosen paradox," Physics (Long Island City, N.Y.) **1**, 195 (1964)

[13] A. Aspect, J. Dalibard, and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers," Phys. Rev. Lett. **49**, 1804–1807 (1982)

[14] Nicolas Gisin, "Bell's inequality holds for all non-product states," Phys. Lett. A **154** (1991), note: the title should say *is violated* instead of *holds*

[15] Reinhard F. Werner, "Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model," Phys. Rev. A **40**, 4277–4281 (1989)

[16] Sandu Popescu, "Bell's inequalities and density matrices: Revealing "Hidden" nonlocality," Phys. Rev. Lett. **74**, 2619–2622 (1995), arXiv:quant-ph/9502005

[17] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," Phys. Rev. Lett. **23**, 880–884 (1969)

[18] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," Phys. Rev. Lett. **76**, 722–725 (1996), arXiv:quant-ph/9511027

[19] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895–1899 (1993)

[20] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, "Concentrating partial entanglement by local operations," Phys. Rev. A **53**, 2046–2052 (1996), arXiv:quant-ph/9511030

[21] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, "Inseparable two spin- $\frac{1}{2}$ density matrices can be distilled to a singlet form," Phys. Rev. Lett. **78**, 574–577 (1997)

[22] Asher Peres, "Separability criterion for density matrices," Phys. Rev. Lett. **77**, 1413–1415 (1996)

[23] Paweł Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," Phys. Lett. A **232**, 333 (1997), arXiv:quant-ph/9703004

[24] Stephen Wiesner, "Conjugate coding," Sigact news **15**, 78–88 (1983)

[25] Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Computer Society Press, New York, Bangalore, India, December 1984, 1984) pp. 175–179

[26] Artur K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991)

[27] Peter W. Shor and John Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000), arXiv:quant-ph/0003004

[28] Nicolas Gisin and Stefan Wolf, "Linking classical and quantum key agreement: Is there "bound information"?." in *Advances in Cryptology – CRYPTO 2000* (Springer, 2000) pp. 482–500, arXiv:quant-ph/0005042

[29] Remigiusz Augusiak and Paweł Horodecki, "Multipartite secret key distillation and bound entanglement," Phys. Rev. A **80**, 042307 (Oct. 2009), arXiv:0811.3603 [quant-ph]

[30] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim, "General paradigm for distilling classical key from quantum states," IEEE Trans. Inf. Theory **55**, 1898 (2009), arXiv:quant-ph/0506189

[31] 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]

[32] L. M. Ioannou, "Computational complexity of the quantum separability problem," Quantum Inf. Comp. **7**, 335–370 (2007), arXiv:quant-ph/0603199

[33] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, "Separability of mixed states: Necessary and sufficient conditions," Phys. Lett. A **223**, 1 (1996), arXiv:quant-ph/9605038

[34] Paweł Kurzyński and Andrzej Grudka, "Graphical representation of generalized quantum measurements," arXiv:quant-ph/0604189

[35] Michael A. Nielsen and Isaac L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)

[36] Marcin Poźniak, Karol Życzkowski, and Marek Kuś, "Composed ensembles of random unitary matrices," J. Phys. A: Math. Theor. **31**, 1059 (1998), arXiv:chao-dyn/9707006

[37] John Watrous, "Many copies may be required for entanglement distillation," Phys. Rev. Lett. **93**, 010502 (2004)

[38] Tilo Eggeling, Karl G. H. Vollbrecht, Reinhard F. Werner, and Michael M. Wolf, “Distillability via protocols respecting the positivity of partial transpose,” Phys. Rev. Lett. **87**, 257902 (2001), arXiv:quant-ph/0104095

[39] Peter W. Shor, John A. Smolin, and B. M. Terhal, “Nonadditivity of bipartite distillable entanglement follows from a conjecture on bound entangled Werner states,” Phys. Rev. Lett. **86**, 2681–2684 (2001), arXiv:quant-ph/0010054

[40] Karl Gerd H. Vollbrecht and Michael M. Wolf, “Activating distillation with an infinitesimal amount of bound entanglement,” Phys. Rev. Lett. **88**, 247901 (2002), arXiv:quant-ph/0201103

[41] Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal, “Superactivation of bound entanglement,” Phys. Rev. Lett. **90**, 107901 (2003), arXiv:quant-ph/0005117

[42] W. Dür, J. I. Cirac, and P. Horodecki, “Nonadditivity of quantum capacity for multiparty communication channels,” Phys. Rev. Lett. **93**, 020503 (2004), arXiv:quant-ph/0403068

[43] Graeme Smith and Jon Yard, “Quantum communication with zero-capacity channels,” Science **321**, 1812–1815 (2008), arXiv:0807.4935 [quant-ph]

[44] Łukasz Czekaj and Paweł Horodecki, “Nonadditivity effects in classical capacities of quantum multiple-access channels,” (2008), arXiv:0807.3977

[45] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov, “Perfect eavesdropping on a quantum cryptography system,” Nat. Comm. **2**, 349 (2011), arXiv:1011.0105

[46] 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

[47] A. Acín, J. Bae, E. Bagan, M. Baig, Ll Masanes, and R. Muñoz-Tapia, “Secrecy content of two-qubit states,” Physical Review A **73**, 012327 (2006), arXiv:quant-ph/0411092

[48] Daniel Gottesman and Hoi-Kwong Lo, “Proof of security of quantum key distribution with two-way classical communications,” IEEE Trans. Inf. Theory **49**, 457–475 (2003), arXiv:quant-ph/0105121

[49] Renato Renner, “Security of Quantum Key Distribution,” (Dec. 2005), arXiv:quant-ph/0512258

[50] Karol Horodecki, *General paradigm for distilling classical key from quantum states — on quantum entanglement and security*, Ph.D. thesis, University of Warsaw (2008)

[51] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus, "Entanglement as a precondition for secure quantum key distribution," Phys. Rev. Lett. **92**, 217903 (2004), arXiv:quant-ph/0307151

[52] Jonathan Oppenheim, "For quantum information, two wrongs can make a right," Science **321**, 1783–1784 (2008)

[53] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A **54**, 3824–3851 (1996), arXiv:quant-ph/9604024

[54] A. Acin, G. Vidal, and J. I. Cirac, "On the structure of a reversible entanglement generating set for three–partite states," Quantum Inf. Comp. **3**, 55 (2003), arXiv:quant-ph/0202056

[55] J. I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, "Entangling operations and their implementation using a small amount of entanglement," Phys. Rev. Lett. **86**, 544–547 (2001), arXiv:quant-ph/0007057

[56] R. F. Werner, "An application of Bell's inequalities to a quantum state extension problem," Lett. Math. Phys. **17**, 359–363 (1989)

[57] Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Acín, "Quantum cloning," Rep. Math. Phys. **77**, 1225–1256 (2005), arXiv:quant-ph/0511088

[58] Reinhard F. Werner, "Optimal cloning of pure states," Phys. Rev. A **58**, 1827 (1998), arXiv:quant-ph/9804001

Author's publications not included into the thesis

1. Barbara Synak-Radtke, Łukasz Pankowski, Michal Horodecki, and Ryszard Horodecki, "On some entropic entanglement parameter", arXiv:quant-ph/0608201

2. Łukasz Pankowski and Barbara Synak-Radtke, "Can quantum correlations be completely quantum?", J. Phys. A: Math. Theor. 41 (2008) 075308 arXiv:0705.1370

3. Andrzej Grudka, Michał Horodecki, and Łukasz Pankowski, "Constructive counterexamples to additivity of minimum output Rényi entropy of quantum channels for all p>2", J. Phys. A: Math. Theor. **43**, 425304 (2010), arXiv:0911.2515 [quant-ph]

Index

Nomenclature

$\vert x\rangle$	ket, page 22
$\Vert X\Vert$	trace norm of a matrix X, page 24
$\Vert x\Vert$	vector norm, page 23
$\mathrm{Tr}_A X$	partial trace, page 33
X^Γ	partial transposition, page 35
$\mathcal{H}_P$	Hilbert space corresponding to projector P, page 24
ϕ_k	Schmidt rank k state, e.g., ϕ_1 and ϕ_2, page 29
$\langle x\vert$	bra, page 22
$\otimes$	tensor product, page 26