Quantum communication in noisy environments

Hans Aschauer

SIGILL·UNIVERSI·TAT·LUDOVIC·MAXIM·

München 2004

Quantum communication in noisy environments

Hans Aschauer

Dissertation
an der Sektion Physik
der Ludwig–Maximilians–Universität
München

vorgelegt von
Hans Aschauer
aus Bad Reichenhall

München, den 30. Januar 2004

Erstgutachter: Hans J. Briegel
Zweitgutachter: Ignacio Cirac
Tag der mündlichen Prüfung: 27. April 2005

Contents

Zusammenfassung **xi**

1 Introduction **1**

2 Noisy quantum operations and channels **7**

2.1 Quantum states, operations, and measurements 7
  2.1.1 Quantum states 7
  2.1.2 Quantum operations 8
  2.1.3 Quantum state measurements 9
2.2 Entanglement and quantum channels 10
  2.2.1 Composite quantum systems 10
  2.2.2 Separable and entangled states 12
  2.2.3 Quantum teleportation 13
2.3 Noise in quantum mechanics 14
  2.3.1 Noise channels 14
  2.3.2 Teleportation with imperfect EPR pairs 16
2.4 Entanglement purification 17
  2.4.1 2-Way Entanglement Purification Protocols 18
  2.4.2 Purification with imperfect apparatus 21
  2.4.3 The quantum repeater 24
2.5 Quantum error correcting codes 27
  2.5.1 Classical codes 27
  2.5.2 The Shor code 28
  2.5.3 CSS codes and stabilizer codes 31
  2.5.4 Errors and quantum error correcting codes 33
2.6 Quantum cryptography 33
  2.6.1 The BB84 Protocol 35
  2.6.2 The Ekert protocol 36

2.6.3 Security Proofs 37

3 Factorization of Eve **41**
3.1 The security proof 41
3.1.1 The effect of noise 42
3.1.2 Binary pairs 46
3.1.3 Bell-diagonal initial states 51
3.1.4 Numerical results 55
3.1.5 Non-Bell-diagonal pairs 58
3.2 How to calculate the flag update function 64
3.2.1 Unitary transformations and errors 64
3.2.2 Measurements and measurement errors 66
3.2.3 The reset rule 67
3.3 Discussion 69

4 Cluster state purification **71**
4.1 The cluster purification protocol 72
4.1.1 Cluster states 72
4.1.2 Description and analytical treatment of the protocol . . 73
4.1.3 Numerical analysis of the protocol 75
4.1.4 Results 76
4.2 Noisy operations 77
4.2.1 One-qubit white noise 78
4.2.2 Results 80
4.3 On the security of the protocol 80
4.3.1 The flag update function 82
4.3.2 The conditional fidelity 84
4.4 Generalized cluster states 86

5 Entanglement purification protocols from quantum codes **89**
5.1 Creating purification protocols from coding circuits 90
5.1.1 Encoding and decoding 90
5.1.2 Error detection vs. error correction 93
5.2 The hashing protocol and quantum codes 94
5.3 Numerical results 98
5.3.1 Purification curves 98
5.3.2 Efficiency of the protocols 102

6 The tensorspace software library 109
6.1 Introduction . . . 109
6.2 Basic concepts . . . 110
  6.2.1 Parties . . . 110
  6.2.2 States . . . 111
  6.2.3 Operations . . . 112
6.3 Diagonal density operators . . . 113
6.4 QTENSORSPACE by examples . . . 114
  6.4.1 CNOT operation . . . 114
  6.4.2 Teleportation . . . 115
  6.4.3 Teleportation using noisy EPR pairs . . . 116
  6.4.4 Cluster states . . . 117
6.5 Mathematics of qtensors . . . 119

7 Local invariants for multi-partite quantum states 121
7.1 State tomography . . . 122
7.2 Invariant decomposition of the state space . . . 123
7.3 Other invariants . . . 128

List of Figures

2.1 The entanglement purification protocol and process. 19
2.2 The purification curve for the IBM protocol 22
2.3 The nested entanglement purification protocol 26
2.4 Quantum logic network of the Shor code 30
2.5 The Ekert protocol 37

3.1 The lab demon 44
3.2 Entanglement purification with binary pairs 49
3.3 Fixpoint map for binary entanglement purification 50
3.4 Illustration of the purification curve for variouse noise levels . 52
3.5 The actual purification curve 53
3.6 Evolution of the Bell-diagonal elements in the subensembles . 56
3.7 Evolution of the fidelity and conditional fidelity 57
3.8 Three purification regimes 59
3.9 Fidelity "phase-transition" at the purification threshold 60
3.10 Efficiency of the purification protocol 61

4.1 The cluster purification protocol 73
4.2 Combinations of the sub-protocols 75
4.3 Minimum fidelity in the cluster purification protocol 77
4.4 Fidelities F and F^{cond} in the cluster purification protocol . . . 86
4.5 Graph states 87

5.1 Equivalence between quantum coding/decoding and EPP . . . 91
5.2 An example of an encoding circuit 92
5.3 A map of quantum error correcting codes. 97
5.4 Purification curves for the $[\![5,1,3]\!]$ and the $[\![11,1,5]\!]$ EDM-EPP. 101
5.5 Purification curves of the noisy$[\![5,1,3]\!]$ EDM and ECM EPP . 103

5.6 Purification curves of the noisy $[\![11, 1, 5]\!]$ EDM and ECM EPP 104
5.7 Efficiency of the protocols without errors 106

Abstract

In this thesis, we investigate how protocols in quantum communication theory are influenced by noise. Specifically, we take into account noise during the transmission of quantum information and noise during the processing of quantum information. We describe three novel quantum communication protocols which can be accomplished efficiently in a noisy environment: (1) Factorization of Eve: We show that it is possible to disentangle transmitted qubits *a posteriori* from the quantum channel's degrees of freedom. (2) Cluster state purification: We give multi-partite entanglement purification protocols for a large class of entangled quantum states. (3) Entanglement purification protocols from quantum codes: We describe a constructive method to create bipartite entanglement purification protocols form quantum error correcting codes, and investigate the properties of these protocols, which can be operated in two different modes, which are related to quantum communication and quantum computation protocols, respectively.

In dieser Arbeit wird untersucht, wie Quantenkommunikationsprotokolle durch Rauschen beeinflusst werden. Insbesondere berücksichtigen wir Rauschen während der Übertragung der Quanteninformation *und* Rauschen während ihrer Verarbeitung. Wir beschreiben drei neue Quantenkommunikationsprotokolle, die in einer verrauschten Umgebung effizient umgesetzt werden können: (1) Abfaktorisierung von Eve: Wir zeigen, dass es möglich ist, bereits übertragene Qubits *nachträglich* von Freiheitsgraden des Kommunikationskanals zu entschränken. (2) Cluster-Zustands-Reinigung: Wir geben viel-parteien Verschränkungsreinigungsprotokolle für eine große Klasse von verschränkten Quantenzuständen an. (3) Verschränkungsreinigungsprotokolle von Quantencodes: Wir beschreiben eine konstruktive Methode, um bipartite Verschränkungsreinigungsprotokolle aus Fehler korrigierenden Codes zu erzeugen, und untersuchen die Eigenschaften dieser Protokolle, die in zwei Betriebsarten existieren, die mit Quantenkommunikationsprotokollen bzw. mit Quantenrechenprotokollen in Verbindung stehen.

Chapter 1

Introduction

> *'I can't believe that!' said Alice.*
> *'Can't you?' the Queen said in a pitying tone. 'Try again: draw a long breath, and shut your eyes.' Alice laughed. 'There's no use trying,' she said; 'one cannot believe impossible things.' 'I daresay you haven't had much practice,' said the Queen. 'When I was your age, I always did it for half-an-hour a day. Why, sometimes I've believed as many as six impossible things before breakfast.'*
> LEWIS CARROLL, *Through the Looking Glass*

Quantum mechanics and its interpretation During the last century, quantum theory has proved to be a very successful theory, which accurately describes the physical reality of the microscopic and mesoscopic world. Today, no physical experiment is known which contradicts the predictions made by quantum theory. This is even more remarkable, since measurement accuracy has increased, and the size of the systems under consideration has decreased at a fast pace.

The fact that quantum theory allows for an accurate *description* of reality is obvious from many physical experiments, and has probably never been seriously disputed. On the other hand, for the *interpretation* of quantum mechanics, things could not be more different: ever since the theory of quantum mechanics has been developed, the question *How can the mathematical formulation of quantum mechanics be interpreted?* lead to a discussion, in which people with different philosophical backgrounds gave different and often contradicting answers. The point at issue was that the theory of quantum mechanics does not account for single measurement outcomes in a deterministic way. The most widely accepted interpretation of quantum mechanics was the so-called *Copenhagen interpretation*, which was developed mainly by Bohr and Heisenberg in the 1920's. It is argued that a measurement causes an instantaneous collapse of the wave function which describes the quantum system, the result of this collapse being intrinsically random.

The most prominent opponent to the Copenhagen interpretation was Albert Einstein, who had developed "away from positivistic instrumentalism to a rational realism" [42]. Consequently, Einstein did not like the idea of genuine randomness in nature, which was an important element of the Copenhagen interpretation. Instead, he considered quantum mechanics to be incomplete, and suggests that there had to be "hidden" variables which would account for the random measurement results.

In fact, it was the famous paper "Can quantum mechanical description of physical reality be considered complete?", authored by Einstein, Podolsky and Rosen (EPR) in 1935 [31], which condensed the philosophical discussion into a physical argument. They claim that given a specific experiment, in which the outcome of a measurement could (in principle) be known before the measurement takes place, there must exist something in the real world, an "element of reality", which determines the measurement outcome. In addition, they claim that these elements of reality are local, in the sense that they belong to a certain point in space-time, and may only be influenced by events which are located in the backward light cone of this point in space-time. Even though these claims sound reasonable and convincing, they are assumptions about nature, which are nowaday called the assumption of *local realism*.

EPR continue their argument by giving a thought experiment, which employs pairs of entangled particles. Their analysis of this experiment shows that both position *and* momentum of the particles are elements of reality; however, quantum mechanics does not include states for which position and momentum are well-defined simultaneously. From this, EPR conclude that quantum mechanics is *incomplete*: it lacks a description of variables, which correspond to the elements of reality. For this reason, these variables were later called hidden variables, or, more precisely, local hidden variables.

Bell's theorem For three decades, it remained a matter of "philosophical taste", whether to believe in the existence of local hidden variables or not: no empirical method to prove the existence or non-existence of hidden variables was known, and many physicists believed that no such method would exist.

In 1964, however, J. S. Bell noticed [9] that the existence of local hidden variables implies a certain inequality (the Bell inequality) between measurement outcomes, while quantum mechanics predicts measurement outcomes which violate this inequality. In so-called Bell experiments, it is thus possible to check whether the predictions of quantum mechanics are correct (in which case local hidden variable theories were ruled out), or whether nature obeys the Bell inequality (in which case quantum mechanics would predict wrong measurement results): quantum mechanics would be wrong rather than incomplete.

Bell experiments have been performed many times (see, e. g., [35, 8, 82, 65]), and they were in excellent agreement with the predictions of quantum mechanics. However, the importance of Bell's experiment is not due to the fact that quantum mechanics has one more time shown to give a precise description of nature; it shows that the microscopic world is guided by laws which are inherently non-classical; it is not possible (and, as a consequence, not necessary) to add something to quantum mechanics which would make it a classical theory.

Bell's inequality and its experimental violation destroyed the hope that quantum mechanics can be described by a classical theory. However, the insight that quantum mechanics is a non-classical theory did not only destroy hopes, but also allowed the dawn of a new era in quantum physics: Physicists started to realize that if quantum physics is non-classical, it might also allow us to do things which are not possible or at least not feasible in a classical world.

Quantum information theory The theory of quantum information is being developed as a result of the effort to generalize (classical) information theory to a quantum world. Quantum information theory aims to answer the question: *What happens to the concept of information if information is stored in the state of a quantum system?*

It is a strength of classical information theory that it does not need to ask the questions about the physical representation of information; there is no need for a ink-on-paper information theory, or a floppy disk information theory. This is due to the fact that it is always possible to efficiently transform information from one representation to another representation.

For this reason, one might be tempted to believe that it is not important whether information is stored in classical or in quantum systems. However, this is not the case: it is, e. g., not possible to write down the previously unknown information contained in the polarization of a photon in ink on paper. In general, quantum mechanics does not allow us to read out the state of an quantum system with arbitrary precision. Moreover, the existence of Bell correlations between quantum systems shows that the (quantum) information content of a quantum system cannot be converted into classical information.

However, Schumacher showed in 1995 [70] that it is *in principle* possible to transform quantum information between quantum systems of sufficient quantum information capacity. The quantum information content of a quantum message $\mathcal{M}$ can for this reason be measured in terms of the minimum number n of two-level systems which are needed to store the message: $\mathcal{M}$ consists of n *qubits* [70].

In its original quantum information theoretical sense, the term *qubit* is thus a measure for the amount of quantum information. A two-level quantum system can carry at most one qubit, in the same sense as a classical binary digit $\mu \in \{0, 1\}$ can carry at most one classical bit. However, the term *qubit* is very often used as a synonym for two-level quantum systems.

Noise and quantum information A (pure) one-qubit state is specified by two real parameters. In this sense, quantum information is similar to analog (in contrast to digital) classical information. Analog information processing seems, on the first sight, to be much more efficient than digital information processing, since an analog information carrier could contain an infinite amount of information. However, analog information processing is being (or already has been) replaced by digital information processing. From this one can see that, in practice, analog information processing performs worse than digital information processing.

It is the presence of *noise*, which is responsible for this gap between the theoretical promises and the practical applicability of analog information: First, in the presence of noise, the information content of an analog information carrier is no longer infinite, but finite. This is a consequence of Shannon's noisy coding theorem [72]. Second, it is very difficult to protect the remaining finite information content of analog information carriers against noise.

The example of classical analog information shows that quantum information processing schemes must necessarily be tolerant against noise; otherwise, there would not be a chance for them to ever become useful. It was thus a major break-trough for the theory of quantum information, when quantum error correction codes and fault-tolerant quantum computation schemes were discovered (see Section 2.5 and references therein).

In quantum communication theory, one is interested in scenarios where distant parties exchange quantum messages. Of course, the transmission of quantum messages may be regarded as trivial special cases of quantum computation, and fault tolerant quantum computation would solve the problem of noise in quantum communication. However, it has been shown that there exists a different method to deal with noise in bipartite communication scenarios, the so-called quantum repeater [17, 29, 36]. The advantage of the quantum repeater over fault tolerant quantum computation methods is that the "threshold" noise level, i. e. the noise level up to which quantum communication is possible, is allowed to be two orders of magnitude higher.

Quantum communication in noisy environments is for this reason a promising topic, which is discussed in the present thesis. After introducing basic concepts of quantum information theory and quantum communication (Chapter 2), we present three novel quantum communication protocols or scenarios:

- Factorization of Eve (Chapter 3): We show that it is possible to actively disentangle qubits, which have been sent through a noisy quantum channel, from the channel's degrees of freedom. Entanglement purification and the quantum repeater can thus be used as tools for quantum cryptography (published in [3, 4]).

- Cluster state purification (Chapter 4): A novel class of multi-partite entanglement purification protocols is discussed, which allow n distant parties to purify a large class of n-party entangled states. It is shown that this protocol works in a noisy environment even if the number n of parties is large (published in [28, 7])

- Entanglement purification protocols from quantum codes (Chapter 5): We give a constructive method which is capable of translating quantum error correcting or detecting codes into entanglement purification protocols, and investigate the efficiency and noise tolerance of several such protocols. In addition, we find that it is the availability of two-way communication which is responsible for the high fault-tolerance of the quantum repeater. The results in this chapter are unpublished.

In Chapter 6, we give a short introduction into the QTENSORSPACE software library, which has been used to produce most of the numeric results in this thesis. Chapter 7 supplements the other chapters by introducing a different notation for quantum states.[1] We show that in this notation, the subsystem structure of multi-partite quantum systems is very transparent, and use it to give a novel multi-partite entanglement criterion (published in [6]).

---

[1] In fact, this notation has already been introduced by J. Schwinger in 1960 [71].

Chapter 2

Noisy quantum operations and channels

2.1 Quantum states, operations, and measurements

In quantum mechanics, like in many other theories in physics, the *state* of a system is a mathematical quantity, which summarizes the information about the system accessible to the theory. The dynamics of systems can thus be completely described in terms of state transformations. In this section, we give a brief overview of states and their transformations in quantum mechanics, and conclude with a description of measurements in quantum mechanics.

2.1.1 Quantum states

A state is usually defined as a mathematical object, from which all empirical data can be derived. Associated to this object is a preparation process, i. e. a physical setup which allows an experimentalist to prepare a system such that it is described by the given state. In many classical theories, the empirical data consist of measurement outcomes, i. e. given a state and a measurement, one can calculate the result of the measurement. The result consists then of a single real number. In quantum mechanics (as well as in statistical physics), the situation is different: Given a fixed preparation an measurement setup, one does not necessarily get fixed measurement results for a given state. However, one *does* get measurement results according to a fixed probability distribution. For this reason, empirical data does in general not consist of individual measurement outcomes, but of probability distributions for the results.

In quantum mechanics, a state ρ is given by a so-called *density operator*, i. e. a non-negative hermitian operator acting on a Hilbert space $\mathcal{H}$, which is obeys the normaliziation condition $\operatorname{tr}\rho = 1$. If the density operator ρ is a projector, it is called a *pure state*. In this case, there exists a *state vector* $|\psi\rangle$ such that $\rho = |\psi\rangle\langle\psi|$. When it does not lead to ambiguities, we also call state vectors states.

2.1.2 Quantum operations

The *time evolution* of a physical system is mathematically described by an operation on the state space. These transformations can be either infinitesimal or finite. Infinitesimal transformations usually describe a continuous time evolution, and are then given by a differential equation. Finite transformation, on the other hand, describe a non-continuous shift in the state space, which might be the net effect of a continuous transformation acting for a given time.

The Schrödinger equation

$$i\hbar\frac{\partial}{\partial t}\rho = -[\rho, H] \tag{2.1}$$

describes the continuous time evolution of a closed quantum mechanical system. For finite time intervals $[t_i, t_f]$, one can easily check (by integrating Eq. 2.1) that the time evolution of a state ρ is given by

$$\rho \longrightarrow \rho' = U\rho U^\dagger \tag{2.2}$$

with a unitary operator $U = U(t_1, t_2)$, which does not depend on the state ρ.

Throughout this thesis, we will concentrate on finite transformations. Whenever we use terms like “a unitary operation U is applied to a state ρ”, we bear in mind that this requires a suitable Hamiltonian, which has to govern the evolution of the system for a given time.

Most generally, finite quantum operations are given by so-called completely positive trace conserving maps (CP-map).[1]This means that any CP-map can, in principle, be implemented experimentally, and any operation,

---

[1] *Positivity* means that positive operators are mapped onto positive operators. *Complete* positivity means that an extension of the map to a larger system (which contains the original system as a sub-system) is still positive.

which is given by some experimental setup, can be described by a CP-map. A well-known representation of CP-maps is the *operator-sum representation*, which is given in terms of so-called Kraus operators A_i [50]. Kraus operators are linear operators with the only restriction that they obey the normalization condition $\sum_i A_i A_i^\dagger = \mathbb{I}$. Using these operators, the map is then given by

$$\rho \longrightarrow \rho' = \sum_i A_i^\dagger \rho A_i. \tag{2.3}$$

A different representation of CP-maps is the so-called unitary representation: Consider a quantum system A in the state ρ_A, and a quantum system B in the state ρ_B. Now we assume that there exists an interaction between both subsystems; however, the total system is considered to be closed. If this interaction acts for some finite time, it will result in a unitary transformation of the total state, $\rho = \rho_A \otimes \rho_B \rightarrow \rho' = U(\rho_A \otimes \rho_B)U^\dagger$. If we are only interested in how the interaction affects the subsystem A, we can calculate the state of system A after the interaction by tracing out system B,

$$\rho_A \rightarrow \rho'_A = \mathrm{tr}_B\, U(\rho_A \otimes \rho_B)U^\dagger, \tag{2.4}$$

which is clearly a CP-map. But also the converse is true: One can show that any CP-map which acts on a system A, there exists a system B, a state ρ_B, and a unitary operations U, such that the CP-map is given by Eq. 2.4.

2.1.3 Quantum state measurements

Measurements are operations on quantum systems, in which the experimentalist gains information about the state of the system. Mathematically, the effect of a measurement operation on the state of a quantum system can*not* be described in terms of a CP-map,[2] but, rather, in terms of a positive operator valued measure (POVM) [61]. A POVM is given by a set P_i of projection operators, which act on the Hilbert space of the quantum system, with the property

$$\sum_i P_i = \mathbb{I}. \tag{2.5}$$

---

[2] This implies that a measurement cannot be described by a unitary operation which acts jointly on the measured quantum system and the measurement apparatus. This impossibility is the reason for the so-called measurement problem in the interpretation of quantum mechanics.

Each projection operator P_i corresponds to a measurement result m_i, which occurs in the measurement with probability $p_i = \operatorname{tr} P_i \rho$.

A special case of a POVM is given by a projective measurement, where the projectors P_i are pairwise orthogonal, i. e. $P_i P_j = \delta_{ij} \mathbb{I}$. It is convenient to describe a projective measurement in terms of a hermitian operator O, so that the projectors P_i are the projectors onto the eigenspaces of O. The operator O is then called an *observable*, which is associated with the measured physical quantity. Usually, the eigenvalues of O are chosen such that they represent the measurement results.

In an experiment, operations and measurements are usually combined. Such a combination is called a *selective quantum operation*, and the state transformation is given by the expression

$$\rho \rightarrow \begin{cases} \rho'^{(1)} = & p_1 \sum_i A_i^{(1)^\dagger} \rho A_i^{(1)} \\ \vdots & \\ \rho'^{(n)} = & p_n \sum_i A_i^{(n)^\dagger} \rho A_i^{(n)} \end{cases} , \tag{2.6}$$

where the upper index denotes the measurement result, and the probability p_i is the probability for the result i.

2.2 Entanglement and quantum channels

2.2.1 Composite quantum systems

If a quantum system is completely described by several independent properties (degrees of freedom), the Hilbert space of the total system is given by the tensor product of the Hilbert spaces of the individual degrees of freedom. However, in general, the elementary factors of such a product space are not fixed; in many cases, it is a matter of convenience which degrees of freedom are chosen to be elementary. A well-known example for this freedom in choice is a quantum system which consists of two angular momenta: in some cases it is useful to describe the system in terms of the individual angular momenta, in other cases, when there exists a specific “coupling” between both momenta, it is advantageous to choose the total angular momentum.

A special case of composite quantum systems are systems, which consist of spatially separated subsystems. Spatially separated means in this context, that there are no interactions between the individual subsystems (*parties*).

In this case, there is a *natural* tensor space structure of the Hilbert space. In Chapter 7 we review a formalism which allows us to write the state space of multi-party states as a real vector space. This vector space can be decomposed into orthogonal subspaces, each of which represents knowledge about correlations between a specific subset of parties, or about a single party.

The natural tensor space structure in multi-partite scenarios is also obeyed by operations and measurements: each subsystem evolves individually, and a selective quantum operation (Eq. 2.6) of the total system is always a product of selective quantum operations on the subsystems (local operations).

It is obvious that a scenario where we do not allow for any interaction between distant subsystems is too restricted in order to show many interesting features. We can, however, allow for interaction in a very controlled way, using the concept of a communication channel. A communication channel allows distant parties to coordinate their local operations, if they are allowed to exchange classical information through the channel (local operations and classical communication, LOCC). In this case, the Kraus operators (Eq. 2.3) which describe the coordinated quantum operations, and projectors (Eq. 2.5) are still products of local Kraus operators, while the CP-map is no longer necessarily a product map.

If the distant parties are allowed to exchange *quantum information* (in addition to classical information) through the communication channel, one can easily show that they can implement *any* quantum operation, i. e. any CP-map. However, such *quantum communication* scenarios differ in many aspects from scenarios, where the subsystems are not separated:

- Quantum communication may be considered expensive, so that one is interested in minimizing the amount of quantum information which is required for a given task (*quantum communication complexity* (see, e. g., [2]).

- Quantum information carriers may be intercepted when they are sent from a party A to a party B, while A and B require that the transmitted (quantum) information remains secret (*quantum cryptography*, see Section 2.6 and Chapter 3).

- The quantum channel may not allow for *perfect* transmission of quantum information, i. e. it may introduce noise. Quantum error correcting codes (see Section 2.5), entanglement purification (see Section 2.4), or a combination of both (see Chapter 5) can be used to overcome the detrimental effects of noise.

2.2.2 Separable and entangled states

If n separated parties a, b, $c \ldots$ start with quantum systems which have been prepared locally and independently, it is an interesting question which global quantum states they can generate, if they are only allowed to use local operations and classical communication. States which can be created in this way are called *separable*. One can verify that a n-party quantum state is separable if and only if it can be written in the form

$$\rho = \sum_i p_i \rho_i^{(a)} \otimes \rho_i^{(b)} \otimes \rho_i^{(c)} \cdots , \tag{2.7}$$

where the weights p_i are non-negative and sum up to unity.

States which are *not* separable are called *entangled*. Entangled states are thus quantum states, which cannot be created without interaction between the distant sub-systems, or without quantum communication between the distant parties.

Given a n-party density operator ρ, it is generally a hard problem to decide whether ρ represents a separable or an entangled state.

Bipartite entangled quantum systems are often called *EPR pairs*, due to the famous paper by Einstein, Podolsky and Rosen [31]. In the context of quantum information theory, EPR pairs usually consist of two entangled two-level systems (qubits), one owned by Alice, and the other by Bob. Maximally entangled two-qubit states are called *Bell states*; one can find four orthogonal Bell states, which form a basis of the two-qubit Hilbert space, the *Bell basis*:

$$\begin{aligned}
\left|\Phi^+\right\rangle &\equiv |\mathcal{B}_{00}\rangle = 1/\sqrt{2}\,(|00\rangle + |11\rangle) \\
\left|\Phi^-\right\rangle &\equiv |\mathcal{B}_{10}\rangle = 1/\sqrt{2}\,(|00\rangle - |11\rangle) \\
\left|\Psi^+\right\rangle &\equiv |\mathcal{B}_{01}\rangle = 1/\sqrt{2}\,(|01\rangle + |10\rangle) \\
\left|\Psi^-\right\rangle &\equiv |\mathcal{B}_{11}\rangle = 1/\sqrt{2}\,(|01\rangle - |10\rangle)
\end{aligned} \tag{2.8}$$

2.2.3 Quantum teleportation: entanglement as a resource

In quantum communication, the importance of entanglement lies in the fact that, supplemented by classical communication, it is a resource which is equivalent to a quantum channel: If Alice and Bob are connected with a quantum channel, Alice can create an EPR pair locally and send one half through the quantum channel to Bob. On the other hand, if Alice and Bob own EPR pairs, they can use them to teleport [11] qubits, even when they are not connected via some "real" quantum channel.

Let us briefly review the quantum teleportation protocol. In the beginning, Alice has two qubits in her hands, A_1 and A_2. The former is the qubit which she is going to teleport ($|\psi_{A_1}\rangle$), the latter is one have of an EPR pair ($\left|\Phi^+_{A_2B}\right\rangle = 1/\sqrt{2}\,(|0_{A_2}0_B\rangle + |1_{A_2}1_B\rangle)$). The other half of this EPR pair is in Bob's hands. The protocol consists of two steps:

Step 1: Alice performs a Bell measurement on her two qubits, i. e. she projects them onto one of the four Bell states. Since the qubits were not entangled, the measurement result is completely random.

Step 2: Alice tells Bob her measurement result. Conditioned on the result, Bob performs one of four unitary operations on his remaining qubit.

In order to sketch the analysis of this protocol, we concentrate on the case that Alice measures a Φ^+-state in her Bell-measurement. The state after the Bell-measurement, modulo normalization, is given by

$$\langle\Phi^+_{A_1A_2}|\psi_{A_1}\rangle|\Phi^+_{A_2B}\rangle = \langle\psi_{A_2}|\Phi^+_{A_2B}\rangle = |\psi_B\rangle. \tag{2.9}$$

In this equation, we used the convention that $|\psi_X\rangle$ is the state of the teleported qubit, carried by qubit X.[3]

As we have seen above, in order to teleport one qubit, Alice and Bob need to share one perfect EPR pair, say in the state $|\Phi^+\rangle$. Conceptually, the

---

[3] Note that it actually makes sense to talk about a given state carried by different quantum systems X and Y, since the existence of the Bell state $|\Phi^+_{XY}\rangle$ requires to fix the *computational basis* for both qubits; states on qubit X and Y are called equal, if the have the same expansion coefficients in both computational bases. More generally, given a Hilbert space isomorphism between two quantum systems X and Y, the conjugate of the isomorphism can be interpreted (modulo normalization) as a maximally entangled state $|\Phi^+_{XY}\rangle$, and *vice versa*.

easiest way for them to create this shared pair is the following: Alice creates the EPR pair locally and sends one of its components to Bob, through a perfect, i. e. noiseless, quantum channel. The EPR pairs can then be used as a resource, which allows Alice and Bob to exchange quantum information, even if they are not connected by a physical quantum channel. For this reason, a shared EPR pair is often called a *quantum teleportation channel*.

2.3 Noise in quantum mechanics

2.3.1 Noise channels

In real-world experiments, a quantum system A cannot be completely closed; it interacts inevitably with its surroundings, the *environment*. By definition, this interaction results in a CP-map on system A; indeed, it is a physical realization of the unitary representation of CP-maps (Eq. 2.4). Consequently, given a suitable environment and a suitable interaction, the interaction with the environment can result in *any* CP-map, i. e. in any quantum operation.

If we accept that the interaction with the environment is the source of noise in quantum mechanics, we are left in a dilemma: it is obvious that it does not make sense to identify noise with arbitrary quantum operations. For this reason, we restrict ourselves to a specific class of quantum operations, when we are interested in the effects of noise. The maps in this class are called *noise channels*.[4] Noise channels are often described in terms of an operator sum representation, which contains few parameters in order to accommodate for the "amount" and kind of noise which is to be introduced.

With respect to composite quantum systems, we require noise channels to fulfil the following properties:

- Noise acts locally, i. e. the noise does not introduce correlations between remote quantum systems. Mathematically, this means that the noise channel which describes the total system is a product of local noise channels.

- Noise may introduce correlations between quantum systems, on which

---

[4] Note that a noise channel is quite different from a quantum channel. A noise channel does not connect distant parties, it merely describes the time evolution of a system. If a (physical realization of a) quantum channel is the source of noise, we call it a *noisy* quantum channel

a joint operation is performed; e. g. a unitary operation which acts on two subsystems jointly is in general accompanied by correlated noise on both subsystems.

- Noise channels are memoryless, i. e. if it acts repeatedly on the same or on different quantum systems, these actions are independent. Note that this property is always fulfilled by the definition of noise channels as a CP-map. If we were interested in noise channels with memory, we would need to define a enlarged (memoryless) noise channel which acts on the state space of all quantum systems under consideration simultaneously.

A most important and well-known example of a noise channel is the so-called *depolarizing channel*, which introduces *white noise*. The depolarizing channel is given by the map

$$\rho \rightarrow \rho' = p\rho + \frac{1-p}{d}\mathbb{I}, \tag{2.10}$$

where d is the dimension of the quantum system, and p is called the *reliability* of the channel. If the noise channel acts on one subsystem A of a composite system, we have to take into account the reduced density operator $\mathrm{tr}_A\,\rho$, i. e. the state of the subsystems, which are not affected by the noise channel:

$$\rho \rightarrow \rho' = p\rho + \frac{1-p}{d_A}\mathbb{I}_A \otimes \mathrm{tr}_A\,\rho \tag{2.11}$$

Here, d_A is the dimension of the subsystem A. If A itself is a composite system comprised by n qubits $a_1, \dots a_n$, we call the noise channel an *n-qubit depolarizing channel*. In this case, we can rewrite Eq. 2.11 using Kraus operators which are proportional to products of Pauli matrices $\sigma_0 \equiv \mathbb{I}, \sigma_1 = \sigma_x, \sigma_2 = \sigma_y, \sigma_3 = \sigma_z$, which act on qubits a_i:

$$\rho \rightarrow \rho' = \sum_{i_1,\dots i_n=0}^{3} f_{i_1\dots i_n}\sigma_{i_1}^{(a_1)} \cdots \sigma_{i_n}^{(a_n)}\, \rho\, \sigma_{i_1}^{(a_1)} \cdots \sigma_{i_n}^{(a_n)}, \tag{2.12}$$

where $f_{0\cdots 0} = \frac{(4^n-1)p+1}{4^n}$ and $f_{i_1\cdots i_n} = \frac{1-p}{4^n}$ for $(i_1, \dots, i_n) \neq (0, \dots, 0)$.

If we allow the coefficients $f_{i_1\dots i_n}$ to be arbitrary non-negative numbers which sum up to unity, Eq. 2.12 describes the *n-qubit correlated Pauli channel*, which is the most general noise channel which is studied in this thesis explicitly.

Noisy quantum operations The noise channels, as described above, are constructed so that they describe the effect of noise alone. This is what we observe if quantum states are stored (quantum memory) or sent between parties at distant locations (quantum communication), where the aim is to keep the state as it is.

On the other hand, the detrimental effects of noise are also visible in quantum operations, where quantum information is being processed. In this case, the interaction, which gives rise to the desired quantum operation, is accompanied by the interaction with the environment — they "happen at the same time". Nevertheless, we can formally decompose an imperfect unitary operation into the application of a noise channel and the desired quantum operation: be $\hat{U}$ the superoperator of the desired unitary operation U (i. e. $\hat{U}\rho \equiv U\rho U^\dagger$), and be $\hat{V}$ the superoperator, which describes the imperfect unitary operation. The time evolution is then given by

$$\rho \to \rho' = \hat{V}\rho = \hat{U}\underbrace{\hat{U}^{-1}\hat{V}}_{\equiv\hat{W}}\rho, \tag{2.13}$$

where we interpret $\hat{W}$ as the superoperator of a noise channel, which is applied before the unitary operation $\hat{U}$.

A more general approach to describe noisy quantum operations is given in [36], where noise is discussed in terms of arbitrary quantum operations, with the restriction that they are close (in terms of a suitable measure on the space of all CP-maps) to an ideal quantum operation. Due to its generality, this approach is very appealing. It is, on the other hand, technically involved, and many effects of noise can be studied using noise channels of the form 2.12.

2.3.2 Teleportation with imperfect EPR pairs

In the discussion of the teleportation protocol in Section 2.2.3, we assumed that Alice and Bob share perfect EPR pairs, i. e. pairs of qubits in a maximally entangled state. However, for all practical purposes, Alice and Bob are only able to share *approximately* perfect EPR pairs, and thus the question arises how well quantum teleportation works with *imperfect* EPR pairs.

For the analysis, we assume that Alice and Bob are connected by a noisy quantum channel, which is a one-qubit depolarizing channel with reliability p (see Eq. 2.10). In a first step, Alice creates one Bell pair in the state $\rho =$

$|\Phi^+\rangle\langle\Phi^+|$ locally, and sends one half of the pair through the quantum channel to Bob. Under the action of the noise channel, the state is transformed into the state $\rho' = p\,|\Phi^+\rangle\langle\Phi^+| + (1-p)/4\,\mathbb{I}$. Note that ρ' is of the Werner form [83].

As the second step, they the imperfect EPR pair ρ' in order to teleport a state $|\psi\rangle$ from Alice to Bob. By a calculation similar to Eq. 2.9, one can easily find that the state of the teleported qubit is $\rho_{\text{teleported}} = p\,|\psi\rangle\langle\psi| + (1-p)/2\mathbb{I}$, which is the same state as if Alice had sent the state $|\psi\rangle$ through the physical quantum channel directly.

In other words, the EPR pair stores the properties of the quantum channel through which it had been distributed.[5] In the next Section, however, we will see that it is possible to enhance the entanglement properties of the EPR pairs after they have been distributed, which leads to a teleportation channel of a better quality than the physical channel which connects Alice and Bob.

2.4 Entanglement purification

In this section, we will see that it is possible for two communicating parties, Alice and Bob, to create highly entangled pairs of qubits, even if they are connected by a rather noisy quantum channel. Note that the channel should not be too noisy — it must still be possible to distribute entanglement through the channel.

The method which allows Alice and Bob to create these highly entangled pairs of qubits is called *entanglement purification*. [13, 14, 25]. Simply speaking, entanglement purification protocols create an ensemble of highly entangled pairs out of a larger ensemble of pairs with low fidelity. The fidelity of a quantum state ρ is defined as its overlap with a given Bell state $|\Phi^+\rangle$, say, i. e. $F = \langle\Phi^+|\,\rho\,|\Phi^+\rangle$.

The purified pairs provide Alice and Bob with a purified quantum teleportation channel. If this channel is used for quantum communication, the already transmitted qubits are *a posteriori* protected against an unwanted interaction with the channel. In Chapter 3, we will see that this fact can be exploited for quantum cryptographic protocols.

---

[5] Given an imperfect EPR pair, the action of the corresponding noise channel can, in general, be recovered probabilistically. This result is a special case of the isomorphism between states and quantum operations [22, 30].

In order to perform an entanglement purification protocol, classical communication between Alice and Bob is necessary. This means, that both Alice and Bob perform measurements on their respective qubits, and tell each other the measurement outcomes. For some protocols only *one-way* communication is required, i. e. only Alice will send classical messages to Bob. It has been shown by Bennett *et al.* [14], that these one-way entanglement purification protocols are equivalent to quantum error correcting codes (see Section 2.5).

2.4.1 2-Way Entanglement Purification Protocols

The two-way entanglement purification protocols (2-EPP) which we present here have been developed by Bennett *et al.* [13] and, later, by Deutsch *et al.* [25]. Since these protocols work in recursive way, they are often referred to as *recurrence protocols.* In order to distinguish between both protocols, we will call them *IBM* and *Oxford* protocol, respectively. The IBM protocol introduces a *twirling* operation after each purification step, which transforms the state of the EPR pairs into the Werner form. Since Werner states [83] are described by only one real parameter, all calculations can be done analytically. A disadvantage of the IBM protocol is that it is less efficient in producing pure states from noisy ones than the Oxford protocol. Qualitatively, there is no difference between both protocols.

To be precise, we want to distinguish between the purification *protocol* and the *distillation process* (see Fig. 2.1).

In each step, the purification protocol acts on two pairs of qubits. In order to illustrate the protocol, we shall assume — in this section — that these two pairs are described by the density operator $\rho_{AB} \otimes \rho_{AB}$, which is thus a four-qubit density operator. The Oxford protocol (see Fig. 2.1) consist of the following steps:

1. Alice and Bob perform one-qubit $\pi/4$ rotations about the x-axis on each of their qubits (in opposite directions). If the qubits were stored e. g. in atomic/ionic degrees of freedom inside a trap, this could be implemented by (simple) laser pulses.

2. Both Alice and Bob perform a CNOT-operation (controlled NOT) [15], where they use their respective particle of pair one (two) as the source (target). This is the part of the protocol which is most difficult to perform experimentally.

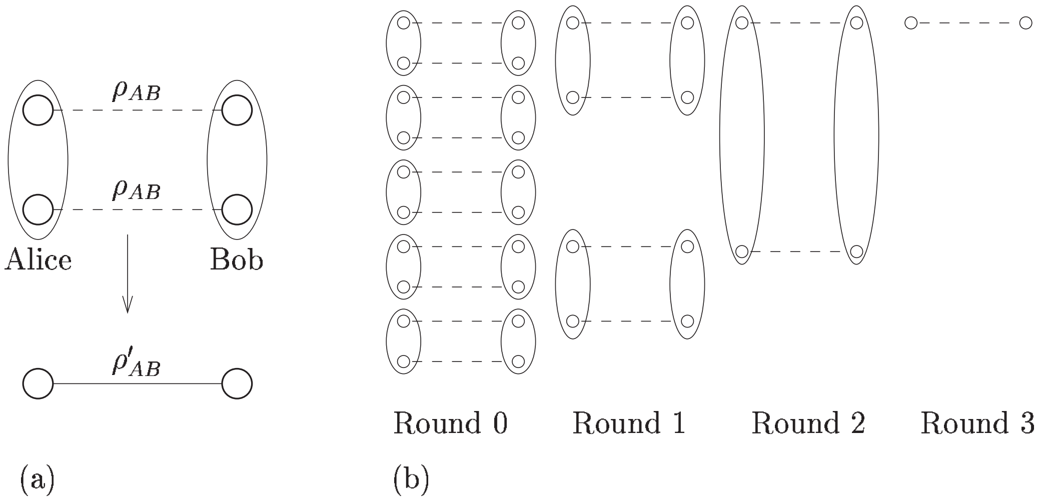


Figure 2.1: (a) The entanglement purification protocol is a (probabilistic) protocol, which creates a stronger entangled pair of qubits out of two pairs with weaker entanglement. Conventionally, these pairs are called source and target pair, respectively. Through an interaction between the qubits of the source and the target pair, realizing a so-called CNOT operation on each side, the states of all four qubits become correlated. By measuring the qubits of the target pair, the source pair is probabilistically projected into a new state ρ'_{AB}, which is more entangled than the original state ρ_{AB}.(b) The distillation process consists of several *rounds*. In each round, the pairs are combined into groups of two at a time, and the purification protocol is applied to them. From round to round, the entanglement of the remaining pairs is increased.

3. Finally, both Alice and Bob measure the qubits which belong to pair two in the σ_z-basis, and tell each other the results (two-way communication). Whenever the results coincide, the keep pair one, otherwise they discard it. In either case, they have to discard the second pair, because it is projected onto a product state by the measurement.

In order to see how this protocol works, it is useful to write the density matrices in the Bell basis, i. e. in the basis of the two-qubit Hilbert space, which consists of the four Bell states $|\Phi^\pm\rangle = 1/\sqrt{2}\,(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = 1/\sqrt{2}\,(|01\rangle \pm |10\rangle)$:

$$\rho_{AB} = A\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + B\left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + C\left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + D\left|\Phi^-\right\rangle\!\left\langle\Phi^-\right| + \begin{array}{c}\text{off-diag.}\\ \text{elements}\end{array} \tag{2.14}$$

The coefficients A, B, C, and D are called the *Bell diagonal elements* of the density matrix ρ_{AB}. For any physical state, these coefficients have to fulfill the normalization condition $\operatorname{tr}\rho_{AB} = A + B + C + D = 1$.

As it turns out, the Bell diagonal elements A', B', C' and D' of the remaining pair do not depend on the off-diagonal elements of ρ_{AB}. For this reason, we can find a recurrence relation for the Bell diagonal elements, which describes their evolution during the distillation process (the index n belongs to the state of the pairs at the beginning of round number n in the distillation process):

$$\begin{aligned} A_{n+1} &= \frac{A_n^2 + B_n^2}{N}, \quad & B_{n+1} &= \frac{2C_nD_n}{N} \\ C_{n+1} &= \frac{C_n^2 + D_n^2}{N}, \quad & D_{n+1} &= \frac{2A_nB_n}{N} \end{aligned} \tag{2.15}$$

The normalization $N_n = (A_n + B_n)^2 + (C_n + D_n)^2$ is equal to the probability, p_{success}, that Alice and Bob obtain the same measurement results in step 3 of the protocol. Even though no analytical solution has been found for this recurrence relation, it has been shown (numerically in [25] and later analytically [53]) that it converges to the fixpoint $A^\infty = 1, B^\infty = C^\infty = D^\infty = 0$, if and only if the initial fidelity is greater than 1/2. In this case, also the off-diagonal elements will vanish, since the density matrix has to remain positive. In other words, whenever Alice and Bob are supplied with EPR pairs with a fidelity of more than 50%, they can distill (asymptotically) perfect EPR pairs.

For the IBM protocol, one only needs one recurrence relation, since (one-parametric) Werner states, described by $A = F, B = C = D = (1 - F)/3$ and vanishing off-diagonal elements in (2.14), are mapped onto Werner states. This map is shown in Fig. (2.2a). The map has tree fixpoints. Two of these fixpoints are attractive (at $F = 1/4$ and $F = 1$), and the remaining one (at $F = 1/2$) is repulsive. Thus, if one starts the distillation process with a fidelity greater than 1/2, one will finally reach EPR pairs in a pure state. If the initial fidelity is smaller than 1/2, one will finally be left with completely depolarized pairs, which correspond to a Werner state with a fidelity of 1/4.

2.4.2 Purification with imperfect apparatus

Up to now, we have assumed that the only source of decoherence is the quantum channel which connects Alice and Bob. For practical implementations, however, this is an over-simplification. Indeed, there are many operations involved in the distillation process: Qubits have to be stored for a certain time, one- and two-qubit unitary operations will act on them, and there are measurements. Each of these operations is a source of noise by itself. It would be inconsistent to ignore this source of noise. So the following question arises: What are the conditions which we have to impose on the apparatus so that entanglement distillation works at all?

As we have mentioned in the context of fault-tolerant quantum computation, there exists a certain noise threshold for the elementary operations, below which fault-tolerant quantum computation is possible. In the case of 2-EPP we will find a threshold which is much more favorable than the threshold for fault-tolerant quantum computation.

In order to get a qualitative understanding of the influence of noisy operation on the entanglement distillation process, we look again at the purification curve (Fig. (2.2)). The curve shows how the fidelity after a purification step depends on the previous fidelity. If noise is introduced in the purification process itself, it is intuitively clear that only a smaller increase in fidelity can be achieved: the purification curve is “pulled down”. In Fig. (2.2b) this is shown schematically. We thus expect that in the case of noisy operations, one has to start with a greater initial fidelity in order to purify at all, and that the maximum fidelity which can be reached will be smaller than unity.

If the noise level is increased, one reaches the situation that two of the fixpoints will merge. At even higher noise levels, the purification curve has

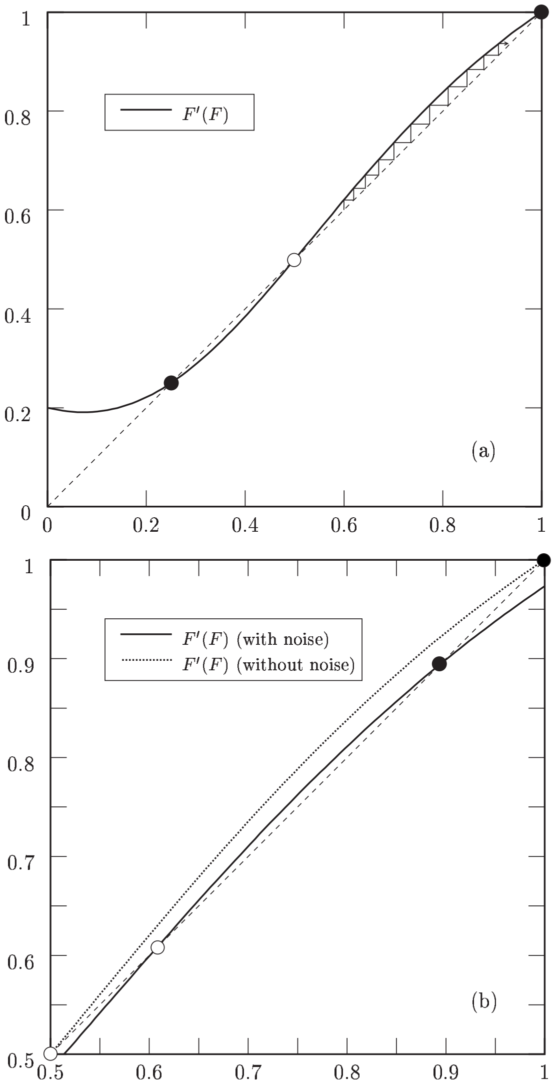


Figure 2.2: The purification curve for the IBM protocol [13, 14] for perfect (i. e. noiseless) apparatus (a). The staircase denotes how the fidelity increases from round to round in the distillation process of Fig. 2.2b). If the apparatus is imperfect, the purification curve is "pulled down" (b) and the fixpoints move towards each other. The upper fixpoint of the curves indicates the maximum achievable fidelity $F_{\max}$, which can be reached asymptotically by the respective purification protocols; $F_{\max}$ decreases with an increasing noise level. Attractive fixpoints are denoted by black circles, repulsive fixpoints by white circles.

only the trivial fixpoint which corresponds to completely depolarized pairs: the distillation process breaks down and does not work any longer.

The quantitative investigation of entanglement purification with noisy apparatus [36, 17] shows that the above considerations are qualitatively correct. For the calculation, the following noise model has been assumed [17]:

- The unitary evolution of the qubits is accompanied by a depolarizing channel. It is well-known that this can be written in a time-integrated form
  $$\rho_{AB} \to p\, U_A \rho_{AB} U_A^{-1} + \frac{1-p}{d} \mathbb{I}_A \otimes \mathrm{tr}_A\, \rho_{AB}. \tag{2.16}$$
  Here, ρ_{AB} is the density operator which describes the state of a bipartite quantum system, U_A is the desired unitary operation (which is assumed to act only on the quantum system at party A), d is the dimension of the Hilbert space of A's system, and p is the *reliability* of the quantum operation. For $p = 1$, there is no noise at all, and for $p = 0$, the quantum system at A becomes completely depolarized.

- Measurements give the correct results only with a certain probability η. This can be conveniently described in terms of a POVM (positive operator valued measure, see Section 2.1.3),
  $$\begin{aligned} M_0 &= \eta\, |0\rangle\langle 0| + (1-\eta)\, |1\rangle\langle 1| \\ M_1 &= \eta\, |1\rangle\langle 1| + (1-\eta)\, |0\rangle\langle 0|\,, \end{aligned} \tag{2.17}$$
  for one-qubit measurements in the σ_z basis. Here, $\mathrm{tr}(M_j \rho)$ describes the probability with which the detector indicates the result "j" for the measured qubit.

As one can see from Eq. (2.16), we have to distinguish between one- and two-qubit operations, if they are accompanied by noise: a two-qubit depolarizing channel is different from two one-qubit depolarizing channels. The first is an example of a *correlated* noise channel, the latter of an *uncorrelated* noise channel. The reliability of one- and two-qubit operations is referred to as p_1 and p_2, respectively. Whether or not entanglement purification is possible with a certain protocol, depends on the three parameters p_1, p_2, and η. For all these parameters, one gets a noise threshold in the percent regime, which is about two orders of magnitude better than the noise threshold for fault-tolerant quantum computation.

2.4.3 The quantum repeater

We have seen in the previous section that for a moderate noise level (of the order of a few percent for the recurrence protocols of Refs. [13, 26]), entanglement purification remains an efficient tool for establishing high-fidelity (although not perfect) EPR pairs. This means that using entanglement purification, quantum communication is possible up to distances of the order of coherence length of a noisy channel. The restriction to the coherence length is due to the fact that the fidelity of the initial ensemble needs to be above the value $F_{\min}(> 1/2)$.

Long-distance quantum communication Long-distance quantum communication describes a situation where the distance between the parties is typically much greater than the coherence- and absorption length of a quantum channel. As the depolarisation errors and the absorption losses scale exponentially with the length of the channel, one cannot send qubits directly through the channel.

To solve this problem, there are two solutions known. The first is to treat quantum communication as a (very simplistic) special case of quantum computation. The methods of fault tolerant quantum computation [63, 48] and quantum error correction (see Section 2.5) could then be used for the communication task. An explicit scheme for data transmission and storage has been discussed by Knill and Laflamme [46], using the method of concatenated quantum coding. While this idea shows that it is *in principle* possible to get polynomial or even polylogarithmic [45, 1, 49] scaling in quantum communication, it has an important drawback: long-distance quantum communication using this idea is as difficult as fault tolerant quantum computation, despite the fact that *short* distance QC is (from a technological point of view) already ready for practical use.

The other solution for the long-distance problem is the entanglement based quantum repeater (QR) [17, 29] with two-way classical communication. It employs both entanglement purification [13, 14, 26] and entanglement swapping [11, 86, 59] in a meta-protocol, the nested two-way entanglement purification protocol (NEPP, see below). The apparatus used for quantum operations in the NEPP tolerates noise on the (sub-) percent level. As this tolerance is two orders of magnitude less restrictive than for fault tolerant quantum computation, it seems to make the quantum repeater a promising concept also for practical realization in the future. It should be noted that the quantum repeater has been designed not only to solve the problem of *decoherence*, but also of *absorption*. For the latter, the possiblity of quantum storage is required at the repeater stations. An explicit implementation that takes into account absorption is given by the photonic channel of Ref. [78, 79] (see also [16]).

The nested entanglement purification protocol In the following description of the nested entanglement purification meta-protocol, we assume that Alice and Bob are seperated by a distance L. Several repeater stations are placed between Alice and Bob, at distances l_0 (see Fig. 2.3). For simplicity we assume that the number of repeater stations, including Bob, is a power of two, i. e. $N \equiv L/l_0 = 2^n$. The distance l_0 is chosen such that it is possible to distribute pairs of entangled qubits with a certain fidelity $F_0 > F_{\min}$ (dashed lines in Fig. 2.3) and with not too high absorption losses between adjacent repeater stations. Using an entanglement purification protocol [13, 26], entangled pairs with a fidelity F_1 (solid lines in Fig. 2.3) are created between the adjacent repeater stations. Entanglement swapping [11, 86, 59] is employed to create pairs of entangled qubits which are seperated by a longer distance of $l_1 = 2l_0$, with a reduced fidelity F. For simplicity, we assume that $F = F_0$.

By iterating this process, one can now create entangled pairs over a distance $l_2 = 4l_0 = 2^2 l_0$. Finally, after n iteration steps, pairs of entangled qubits are created which are seperated by the distance $L = Nl_0 = 2^n l_0$. In other words, Alice and Bob now share entangled EPR pairs.

For an estimation of the resources needed to create one entangled pair of qubits connecting Alice and Bob, we assume that the entanglement purification process consumes k pairs of fidelity F_0 in order to create one pair with fidelity F_1. It is thus easy to see that the number K of entanglement purification steps grows exponentially with the number n of nesting levels. Under the conditions given above, we have $K = k^n$, if we further assume that entanglement purification in different segments is carried out in parallel. On the other hand, also the distance between both parts of the entangled pair grows exponentially in the number of nesting levels, i. e. $d(n) = 2^n l_0$. By eliminating n in both formulas, we get $K(d) = k^{\log_2 d/l_0} = (d/l_0)^{\log_2 k}$, i. e. the number K of purification steps is polynomial in the distance d between Alice and Bob. A similar polynomial relation is obtained if the full analysis (without simplifying assumptions) is performed [17].

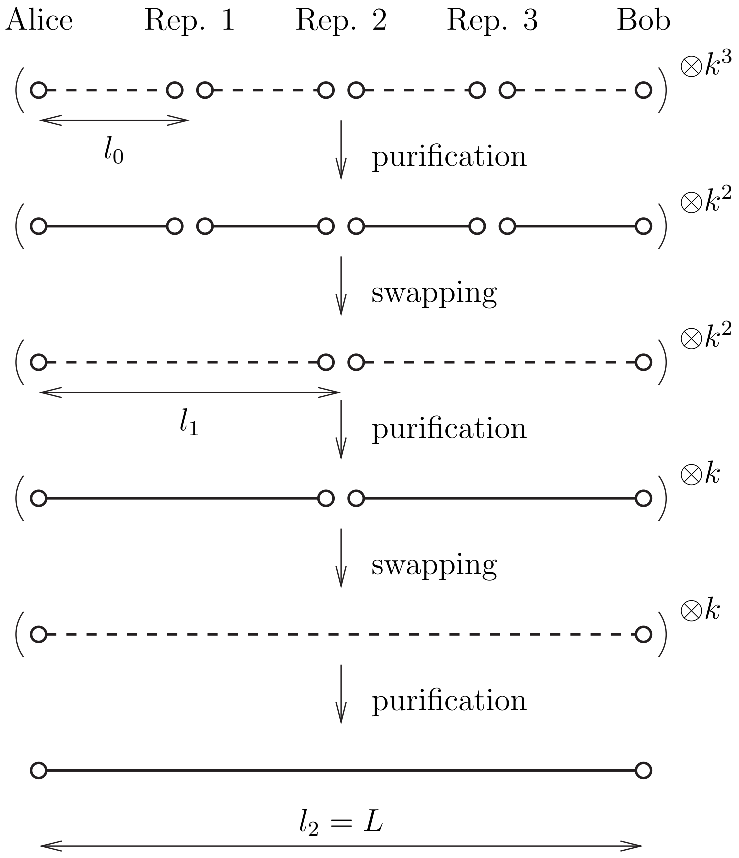


Figure 2.3: The nested entanglement purification protocol of the quantum repeater. Alice and Bob are separated by the distance $L = 4l_0$. Initially, k^3 low-fidelity pairs (dashed lines) are shared between adjacent stations. Using entanglement purification, the fidelity of the pairs is increased (solid lines), and with entanglement swapping, the distance between the end-points of entangled pairs is increased. Entanglement purification and swapping form one nesting step in the NEPP.

2.5 Quantum error correcting codes

In the previous section, we introduced entanglement purification as a tool which can be used to get rid of the detrimental effects of noise in quantum protocols. Even earlier than entanglement purification, in 1995, quantum error correcting codes (QECC) have been invented by Shor [73] in order to solve the same problem. It has been shown by Bennett *et al.* [14], that quantum error correcting codes and entanglement purification protocols which involve only one-way communication are equivalent. In Chapter 5, we analyze this relation in detail.

2.5.1 Classical codes

The idea to protect quantum states against noise with the help of codes has been inspired by classical coding theory. Indeed, in many cases classical error correcting codes can be used to build quantum error correcting codes. In the following, we show how this is accomplished for the Shor code.

Let us start with the definition of classical codes. In mathematical terms, classical error correcting codes are given by a map

$$f_{\mathcal{C}} : \{0,1\}^k \to \{0,1\}^n, \tag{2.18}$$

where k is the number of bits which are encoded, and n is the dimension of the code space, or the number of bits into which the information is encoded. For the special case of *linear* codes, $f_{\mathcal{C}}$ is a linear map.[6] The image $\mathcal{C} = \mathrm{Im}(f_{\mathcal{C}})$ is the set of *codewords*, or the *code*. A linear code is thus a linear subspace of $\{0,1\}^n$ of dimension k.

In order to characterize the error correction properties of a code, the *minimum distance* d of the code is introduced, which is the minimum Hamming distance between any two codewords. The Hamming distance of two codewords is defined as the number of bits which have to be flipped, in order to transform one codeword into the other. A code with minimum distance d can correct at most $\lfloor (n-1)/2 \rfloor$ errors.

The three numbers n, k, and d are important for the characterization of a code (even though there may exist more than one code for given values for n, k, and d); such codes are called $(\!(n,k,d)\!)$ codes.

---

[6] In this case, we interpret the sets $\{0,1\}^k$ and $\{0,1\}^n$ as vector spaces over the field $\mathbb{F}_2$.

The simplest classical error correcting code is probably the repetition code. Assume that a sender (*Alice*) wants to transmit a classical message, which consists of one classical bit i, to the receiver (*Bob*). Since they are connected by a noisy communication channel, sometimes the bit gets flipped (inverted) during the transmission. In order to overcome this problem, Alice sends her bit to Bob n times. After receiving the n bits, Bob performs a "majority vote" in order to restore the original message: if more than half of the bits are in state i', Bob assumes that Alice has sent the message bit i'. Clearly, the minimum distance of this code is n: the n bit repetition code is a $(\!(n, 1, n)\!)$ code.

2.5.2 The Shor code

The no-cloning theorem [84] disallows a straightforward translation of the repetition code into a quantum error correcting code: Already the first step of the encoding operation (copy the qubit n times) would fail. However, quantum mechanics allows us to create *imperfect* copies of a given input state: if the qubit which we want to copy is in a basis state $|i\rangle$ of the computational basis, we can copy it in an ancilla $|0\rangle_A$. The map $|0\rangle_A|i\rangle \rightarrow |i\rangle_A|i\rangle$ can be implemented using a CNOT gate. Note that, for some input states, this cloning quantum network does not produce copies of the input at all: if we consider the input state $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$, we find that the result of the CNOT operation produces a maximally entangled Bell state $|\Phi^{\pm}\rangle$, for which the individual density operators of both qubits are maximally mixed. However, there exist quantum cloning networks which perform better that the CNOT gate; the optimal (but, of corse, not perfect) cloning network has been given in [19, 20].

For $n = 3$, we have depicted the encoding circuit, the quantum channel, and the decoding circuit in Fig. 2.4(a). After the decoding operation has been performed, both ancilla qubits are measured in the computational basis. One can easily see that one spin-flip operation $\sigma_x^{(j)}$, applied to an arbitrary qubit $j = 1, 2, 3$, can be identified: if one of the ancilla qubits yields the measurement result "1", it is clear that this ancilla qubit has been flipped during the transmission, and no action has to be taken. However, if both ancilla qubits yield the measurement result "1", the central qubit must have been flipped; this error can be corrected by applying an additional spin flip operation to the central qubit.

Note that spin flip operations are not the only non-trivial error operations that can be applied to quantum states; in fact, an error operation could be any CP-map (see Section 2.1.2). Nevertheless, for the analysis of noise, it is enough to consider an error model where random Pauli rotations are applied to the individual qubits with a certain "error rate", which is a realization of the one-qubit Pauli channel (see Eq. 2.12). This model is more general than it appears to be at first sight but it needs a justification to which we shall return below.

While this so-called quantum repetition code is able to correct one spin flip error which has been applied to an arbitrary transmitted qubit, it is not able to correct phase flip errors. If the dotted Hadamard transformations are applied to the qubits before and after the transmission, the role of spin flip and phase flip errors is exchanged, so that the code can correct one phase flip error.

If each of the three code qubits of the repetition code (in its phase-flip correcting version) is encoded once more, again using the repetition code, one has created a code which is capable of correcting one arbitrary spin-flip, phase-flip, or combined spin- and phase-flip error (see Fig. 2.4 (b)): the Shor code [73].

After the decoding operation, the eight ancilla qubits $|\epsilon_j\rangle$ (with $j = 1,2,3,4,6,7,8,9$ are measured in the σ_z basis, with measurement results ϵ_j (error syndrome). The central qubit is in state $|\phi'\rangle = U(\epsilon_1 \dots \epsilon_4, \epsilon_6 \dots \epsilon_9)|\phi\rangle$, where the unitary transformation $U(\epsilon_1 \dots \epsilon_4, \epsilon_6 \dots \epsilon_9) \in \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}$, is uniquely determined by the error syndrome: A spin flip error, which has been applied to an arbitrary qubit during the transmission, can be identified by the values $\epsilon_1, \epsilon_3, \epsilon_4, \epsilon_6, \epsilon_7$, and ϵ_9, and a phase flip error can be identified by ϵ_2 and ϵ_8.

For a mathematical description of quantum error correcting codes, we are interested in the (unitary) map realized by the encoding operation,

$$ENC: \; (\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \cdots |0\rangle \longmapsto \alpha|0\rangle_S + \beta|1\rangle_S \tag{2.19}$$

in which the states

$$\begin{aligned} |0\rangle_S &= 2^{-3/2}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \\ |1\rangle_S &= 2^{-3/2}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)\,. \end{aligned} \tag{2.20}$$

denote the so-called *code words* of the (9-bit) Shor code. Unlike classical codes, the *quantum code* is defined as the linear *span* of the codewords,

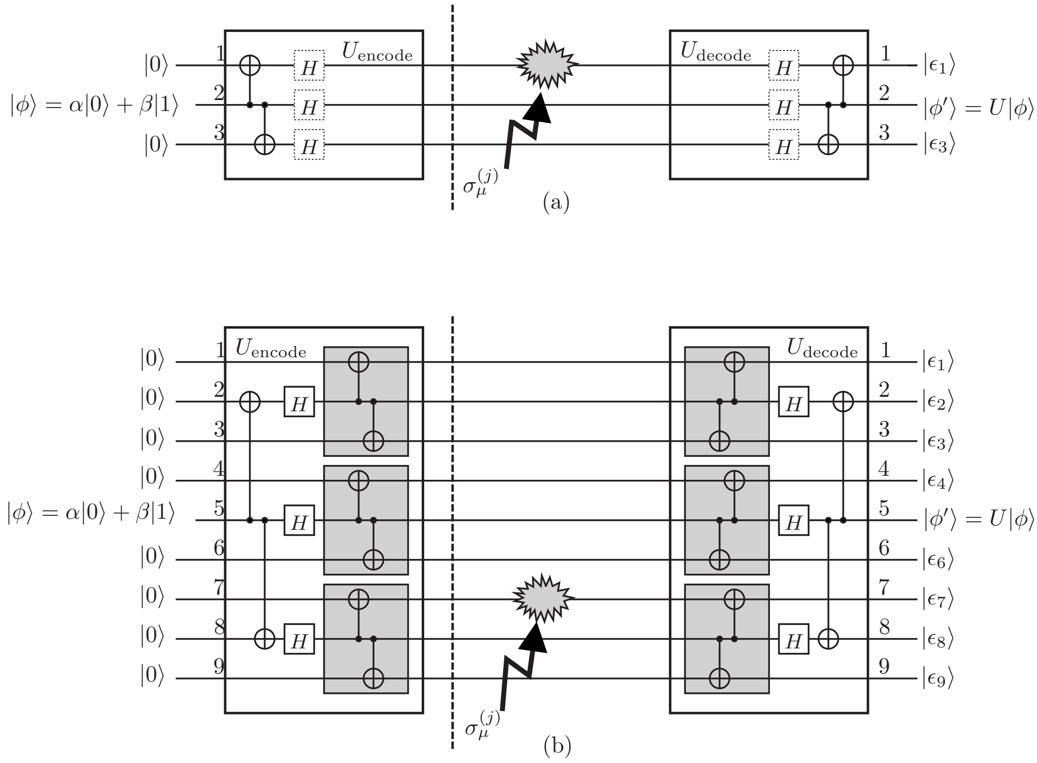


Figure 2.4: Coding circuit, transmission of encoded data through a noisy channel, and decoding circuit for the (a) quantum repetition code and (b) the Shor code. A “random rotation” $\sigma_\mu^{(j)}$ on qubit j in the encoded state translates into a certain “error syndrome” ϵ_1, ϵ_2 (for the repetition code) and $\epsilon_1, \dots, \epsilon_4, \epsilon_6, \dots, \epsilon_9$ (for the Shor code) and a corresponding unitary operation $U = U(\vec{\epsilon})$ on the central qubit (see text). The networks uses the Hadamard-Rotation $H_j = 1/\sqrt{2}(\sigma_x^{(j)} + \sigma_z^{(j)})$ and the CNOT gate ($\overset{\bullet}{\oplus} = \mathrm{CNOT}_{i,j} = \frac{1+\sigma_z^{(i)}}{2} + \frac{1-\sigma_z^{(i)}}{2}\sigma_{x,j}$). If the dotted Hadamard gates are inserted into the coding circuits of the repetition code, it protects against one phase flip operation.

which is a subspace of the nine qubit Hilbert space. This subspace is often also refereed to as the *code space*.

For the Shor code, the code words $|0\rangle_S$ and $|1\rangle_S$ are tensor products of entangled three-qubit states of the form $|000\rangle \pm |111\rangle$, the so-called Greenberger-Horne-Zeilinger (GHZ) states [40], which play a prominent role for the interpretation of quantum mechanics. [40, 57]. One can easily check that after the encoding (see dotted line in Fig. 2.4), the reduced density operator of each of the qubits is totally mixed; that is, the *individual* state of the particles carries no information about $|\phi\rangle$.[7]

By reading off the error syndrome, and subsequently applying the correction operation $U^{-1}(\epsilon_1 \ldots \epsilon_4, \epsilon_6 \ldots \epsilon_9)$, the central qubit is transformed back to its initial state. Please note that the central qubit remains unmeasured, and no information about the state $|\phi\rangle$ is obtained at any step of the protocol. By iteration of the sequence *decoding* → *syndrome measurement* & *correction* → *encoding* [51] an unknown quantum state can thus be protected against decoherence over a time significantly longer than the decoherence time.

The effect of the random rotations $\sigma_\mu^{(j)}$ is to map the code space $\mathcal{H}_S$ to a set of orthogonal error spaces $\sigma_\mu^{(j)}\mathcal{H}_S \perp \mathcal{H}_S$. The images of the code words thereby satisfy the following orthogonality relations ${}_S\langle 0|\sigma_\mu^{(j)}\sigma_\nu^{(k)}|1\rangle_S = 0$ and ${}_S\langle 0|\sigma_\mu^{(j)}\sigma_\nu^{(k)}|0\rangle_S = \langle 1|\sigma_\mu^{(j)}\sigma_\nu^{(j)}|1\rangle_S$ for all j, k, μ, ν. Theses relations ensure [14, 47], that all errors $\sigma_\mu^{(j)}$ can, in fact, be corrected.

2.5.3 CSS codes and stabilizer codes

The Shor code was the first quantum error correcting code found that can correct all of the four errors (spin flip, phase flip, spin&phase flip, identity) on any one of the qubits. As we have seen, the Shor code uses two coding steps. Both steps consist of codes, which are capable of correcting phase flip errors and spin flip errors, respectively. Both codes are in fact classical linear codes; their properties guarantee that both encoding steps do not in-

---

[7] Quantum error correcting codes are indeed constructed in such a way that the state of individual qubits in a codeword becomes completely undetermined. As was shown by DiVincenzo and Peres [27], the codewords satisfy generalized Mermin relations [57] that exclude the possibility of consistently assigning a predetermined value to complementary observables of each qubit. From the measurement of an individual qubit one can thus not gain any information about $|\phi\rangle$. In the positive sense this means that an uncontrolled interaction of the environment with one of the qubits does not (necessarily) lead to an irreversible *loss* of information.

terfere. Calderbank and Shor [21], and, independently, Steane [75] found the conditions which two classical codes have to obey, so that their combination leads to a quantum error correcting code: The orthogonal complement of the second code has to be a subset of the first code. Quantum error correcting codes, which are constructed in this way, are called Calderbank-Shor-Steane (CSS) codes.

Besides the fact that the CSS construction can be used to create quantum error correcting codes, the simple structure of CSS codes makes them suitable for a security proof of quantum cryptography (see Section 2.6) which has been given by Shor and Preskill [74]. This proof employes and requires CSS codes; more general quantum error correcting codes would not work for this proof.

A number of other codes were found, which do not belong to the CSS class, among them a so-called 'perfect' code using a minimum number of only 5 qubits [51, 14]. For general quantum error correcting codes, it is useful to introduce the *stabilizer* of the code, which can be defined using the decoding operation $U_{\text{decode}} = U^{-1}_{\text{encode}}$: Be $\sigma_z^{(j)}$ the z Pauli-Operator of the ancilla qubit j. The stabilizer operator M_j is then given by

$$M_j = U_{\text{decode}} \sigma_z^{(j)} \, . \tag{2.21}$$

In the case of the Shor code, the eight ancilla qubits have the numbers $j = 1, 2, 3, 4, 6, 7, 8, 9$, and one can easily show that the stabilizer operators are given by

$$\begin{aligned}
M_1 &= \sigma_z^{(1)} \sigma_z^{(2)} \, , \\
M_2 &= \sigma_x^{(1)} \sigma_x^{(2)} \sigma_x^{(3)} \sigma_x^{(4)} \sigma_x^{(5)} \sigma_x^{(6)} \, , \\
M_3 &= \sigma_z^{(2)} \sigma_z^{(3)} \, , \\
M_4 &= \sigma_z^{(4)} \sigma_z^{(5)} \, , \\
M_6 &= \sigma_z^{(5)} \sigma_z^{(6)} \, , \\
M_7 &= \sigma_z^{(7)} \sigma_z^{(8)} \, , \\
M_8 &= \sigma_x^{(4)} \sigma_x^{(5)} \sigma_x^{(6)} \sigma_x^{(7)} \sigma_x^{(8)} \sigma_x^{(9)} \, , \\
M_9 &= \sigma_z^{(8)} \sigma_z^{(9)} \, .
\end{aligned} \tag{2.22}$$

As in the case of classical codes, it is possible to construct codes which encode $k > 1$ qubits, and codes which are able to correct more than a single qubit error. The code words are entangled states of an increasing number n of qubits. Analogous to the case of classical codes, the number of single qubit errors that can be corrected is determined by the minimum distance d of the code; in order to correct one error, a minimum distance of $d \leq 3$ is necessary. The distance of a pair of codewords is defined as the number of Pauli operations which are required to transform one codeword into the other codeword. A general quantum code which encodes k qubits into codewords of length n, and which has a minimum distance d, is called a $[\![n, k, d]\!]$ quantum code.

2.5.4 Errors and quantum error correcting codes

Let us return to the question whether the model of an error as a random unitary rotation is reasonable. As we have described in Section 2.3, the interaction of the qubits with the environment can be described as a unitary evolution in the Hilbert space of the total system consisting of both the qubits and the environment. In this sense, *errors do not happen*, noise is a continuous process. The effect of noise is a CP-map, which can be written in a Kraus representation (Eq. 2.3), i. e. as a convex combination of "error"-operations acting on the qubits. In general, the error operations are different from the Pauli rotations. However, one can show that it is possible to find a Kraus representation which is an expansion in the interaction strength. In this expansion, the term of zeroth order is proportional to the identity operator, the terms of first order are proportional to one-qubit Pauli rotations, etc. [76].

The measurement of the ancilla qubits (i. e., the measurement of the stabilizer operators) projects the state of the encoded quantum word into one of the error spaces. It is this measurement which is responsible for the "digitalization of noise" [76], i. e., the stabilizer measurements *make the errors happen.*

2.6 Quantum cryptography

One of the experimentally most advanced fields in quantum communication is quantum cryptography. In this section, we will describe the two basic protocols of quantum cryptography. We show that decoherence in the (untrusted) quantum channel as well as in the (trusted) apparatus plays an important role in the security analysis of quantum cryptography protocols.

The communication scenario in the cryptographic context looks as follows: Alice wants to send a confidential message (*clear-text*) to Bob, while a third communication party, Eve, wants to listen in and learn as much as possible about the message. In order to achieve her goal, Alice encrypts the message using some cryptographic method. The encrypted message is called *ciphertext*. A cryptographic protocol is considered *good*, if it is possible to restrict the information which Eve can obtain to any desired level.

There exist several categories of *classical* cryptographic protocols; these include symmetric key ciphers, asymmetric key ciphers and one-time pads. All these protocols have advantages and disadvantages, but the most eminent advantage of the one-time pad is that it has been proved to be secure in the information theoretical sense: one can show that an eavesdropper can gain no information (zero bits of information) about the message, even if he or she knows every single bit of the encrypted message. To this end, it is however necessary that Alice and Bob share a secret and random key, which must at least be as long as the message which Alice wants to transmit, and that this key will only be used once (thus the name *one-time pad*).

The one-time pad works as follows: As a key, Alice and Bob share a secret string of zeros and ones $s = (s_1, s_2, \dots, s_N)$. Similarly, Alice can write the clear-text (like any piece of information) as a string of zeros and ones, using some encoding which Alice and Bob agree on publicly. The clear-text is thus given in a *binary representation* $t = (t_1, t_2, \dots, t_N)$. For the ciphertext, Alice adds the key and the clear-text bitwise modulo 2: $c = (s_1 \oplus t_1, s_2 \oplus t_2, \dots, s_N \oplus t_N)$. In order to decrypt the message, Bob simply adds the key bitwise (modulo 2) to the ciphertext, and gets back the binary representation of the clear-text.

The key used in the one-time pad protocol is a valuable resource, to both the legitimate communication parties and to an eavesdropper: Alice and Bob use up the key during the communication. In order to supply themselves with a new key, they have to meet each other physically. On the other hand, if Eve knows the key, the communication between Alice and Bob is no longer a secret for her; for this reason, the cryptographic key might be a valuable target for theft or bribery. The aim of quantum cryptography is to solve this shortcoming of classical cryptography. In most quantum cryptography protocols, the quantum part of the protocol is related to the distribution of a key (quantum key distribution, QKD), which can afterwards, as soon as it is established, be used for a classical one-time pad protocol.

2.6.1 The BB84 Protocol

The first protocol for quantum key distribution was given by Bennett and Brassard in 1984 [10]. This so-called BB84 protocol is widely used in quantum cryptography, since all security considerations are well analyzed, and it is easy to understand.

The protocol works as follows: Alice prepares two random binary strings, the key string $(k_1, k_2, \ldots, k_N)$ and the basis string $(b_1, b_2, \ldots, b_N)$. The randomness of the bits is crucial for the security of the protocol; they must be chosen by a really random process. If a pseudo random number generator was used for this task, the security of the protocol depends on (in most cases unproved) assumptions about the cryptographic qualities of the random number generator.

There are 4 different quantum states which Alice prepares: $|s_0\rangle_0 = |0\rangle$, $|s_1\rangle_0 = |1\rangle$, $|s_0\rangle_1 = |+\rangle \equiv 1/\sqrt{2}(|0\rangle + |1\rangle), |s_1\rangle_1 = |-\rangle \equiv 1/\sqrt{2}(|0\rangle - |1\rangle)$. To give an example, we will now consider the case of qubits which are represented in the polarization degree of freedom of a photon. In this case, the four states which Alice can prepare are horizontally, vertically, or ±45° polarized photons.

Alice sends N photons through the quantum channel to Bob. The state in which the qubits are prepared depends on the key- and and the basis string: the ith qubit is prepared in the state $|s_{k_i}\rangle_{b_i}$.

Bob can measure each photon that arrives in his laboratory either in the $|0\rangle\,/\,|1\rangle$-basis (i. e. in the horizontal/vertical basis), or in the $|+\rangle\,/\,|-\rangle$-basis (i. e. in the ±45° polarized basis). For each individual photon, he selects the measurement basis randomly, and he writes down the chosen basis and the measurement result. When Bob has received and measured the N photons, he is left with two strings of N bits: the basis string and the "result" string.

Alice and Bob exchange their respective basis strings through a classical channel, which may be public; for example, they might announce the basis strings in a newspaper. It is no security breach if Eve knows both basis strings. However, Alice and Bob must make sure that Eve cannot alter these messages. One possibility to achieve this goal is that Alice and Bob posses an initial shared secret, which can be used to check the authenticity and integrity of the basis strings. During the key distribution task, this initial shared secret can be recreated, so that it is not used up; rather, it plays the role of a catalyst. By comparing their basis strings, Alice and Bob can see which photons have been measured in the same basis in which they have been prepared. Whenever the preparation basis and the measurement basis are different, Bob's measurement result is completely random and cannot be used. On the other hand, if the two bases are the same, Bob's measurement result will be strictly correlated with Alice's key bit for the respective photon: Alice's key bits and Bob's measurement results for these photons can be used as a secret key.

Before the key can be used, Alice and Bob have to make sure that the quantum channel has not been eavesdropped. One way to do this is the following: Alice chooses a certain number of the key bits randomly and sends them to Bob through the classical public channel. Bob compares Alice's key bits with his result bits, and if they are equal, they can be sure that there was no eavesdropper who tapped the quantum channel. This is due to the fact that the only quantum operation which does not disturb non-orthogonal quantum states is the identity. In other words: if Eve does not want to disturb the non-orthogonal quantum states which Alice sends, she has to leave them alone.

2.6.2 The Ekert protocol

The main difference between the BB84 protocol and the so-called E91 protocol found by Ekert in 1991 [32] is that it does not use single photons which one communication party sends to the other, but pairs of entangled photons. While its experimental realization is more difficult than the BB84 protocol, it has a theoretical advantage: the security of the E91 protocol is related to the fact that there exists no local realistic theory which explains the outcomes of Bell-type experiments (see Chapter 1). While in the BB84 protocol one has to believe that the quantum mechanical description of photons is complete (i. e. that there exist no (local) variables — "hidden" or not — which could be used to predict Bob's measurement outcomes[8]), the E91 protocol performs a Bell experiment at the same time, which assures that there cannot exist

---

[8] In experiments, classical information about the state which has been prepared might leak out of Alice's laboratory through different degrees of freedom, like the frequency of the photon, or the polarization of a second photon in a multi-photon pulse. This information, which plays the role of hidden variables, could *in principle* be exploited by Eve without introducing noise. For the E91 protocol, this leakage problem does not exist, since there is no information which could leak out of the laboratories until Alice and Bob perform their measurement. In this sense, the BB84 and E91 protocols are *not* equivalent, as stated in [12].

(local) hidden variables.

In the E91 protocol, pairs of entangled photons are prepared, for example in the state $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. It does not matter whether these pairs are produced in Alice's or Bob's laboratory, or by a (potentially untrusted) source in between. One photon of each pair is sent to Alice, the other to Bob. For each photon, Alice and Bob choose one out of a set of three measurement directions at random, and measure the polarization of the photon in this direction (see Fig. 2.5). As in the BB84 protocol, Eve must not be able to predict the choice of the measurement directions. As soon as all pairs are sent to Alice and Bob and they acknowledge that they have performed the measurements, the information about the measurement directions is exchanged (through a public classical channel). Alice and Bob check for which pairs their respective measurement directions were the same; for all pairs where they have chosen different measurement directions, they also exchange the measurement *outcomes* through the public classical channel. With these results, Alice and Bob check that the Bell inequalities [9, 24] are violated. If they are violated, the measurement results for the pairs where they have chosen the same measurement direction must be strictly anti-correlated, and can be used as a key.

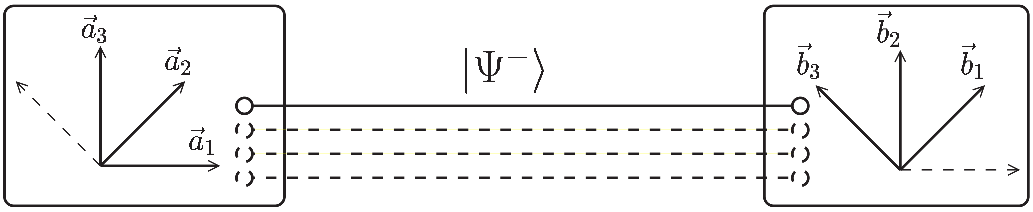


Figure 2.5: The measurement directions in the Ekert protocol. For each EPR pair, Alice and Bob choose independently and randomly one of the three measurement directions $\vec{a}_1, \vec{a}_2, \vec{a}_3$ and $\vec{b}_1, \vec{b}_2, \vec{b}_3$, respectively.

2.6.3 Security Proofs

As we have seen above, the quantum key distribution protocols allow for secure communication, as long as Alice and Bob are connected by a noiseless quantum channel. This is a remarkable result – however, it would be useless for all practical purposes, since all quantum channels are a source of noise. Since Alice and Bob trust only the equipment in their laboratories, they cannot be sure that the noise which they measure can be attributed to the channel. It is *in principle* impossible to distinguish between noise introduced by the quantum channel or by an eavesdropper. For this reason, the communication parties have to deal with the worst case scenario of an eavesdropper, who is present all the time and everywhere, except for the laboratories, which are secure by assumption. The eavesdropper might be hidden behind the noise of the quantum channel, and she might gain partial knowledge of the cryptographic key and, later, of the secret message.

The simplest way to deal with this situation would be to use a better quantum channel. In a practical setting, however, when Alice and Bob are connected by a given quantum channel (e. g. an optical fiber), this possibility is ruled out. In this situation, Alice and Bob can use *privacy amplification* methods, where a shorter and perfectly secure key is distilled out of a longer key, about which Eve might have had considerable knowledge. So-called “ultimate” or “unconditional” security proofs of quantum cryptography show that such protocols do exist.

The first of these proofs has been given by Mayers in 1996 [56] for the BB84 protocol. Shor and Preskill gave a physical interpretation of this proof, as they showed that it could *a posteriori* be understood as a restricted, albeit sufficient, form of quantum error correction and one-way entanglement purification.

A different approach has been taken by Deutsch *et al.* in 1996 [25]. They employ a two-way entanglement purification protocol (2-EPP, see Sec. 2.4) in order to distill almost pure EPR pairs out of many imperfect pairs. If the purified pairs are used for teleportation, the resulting quantum channel is perfectly secure: Since the EPR pairs are in a pure state, they cannot be entangled with any other quantum system. The eavesdropper is thus “factored out” in the total Hilbert space, which we write symbolically as

$$\rho_{\text{Alice,Bob,Eve}} \xrightarrow{\text{2-EPP}} \left|\Psi^+\right\rangle_{AB}\left\langle\Psi^+\right| \otimes \rho_{\text{Eve}}.$$

As we have already seen in Sec. 2.4.2, in a realistic setting the purification protocol does not converge to perfect EPR pairs, but to some more or less mixed state in the Hilbert space of Alice’s and Bob’s qubits. But that means that the argument given above does no longer guarantee that Eve is factored out: *a priori*, there could exist residual entanglement with Eve.

In the next chapter, we show that this is not the case: even in the presence of noise, an eavesdropper is factored out in the course of an (appropriate) entanglement distillation process.

Chapter 3

Factorization of Eve

In this chapter, we show that entanglement distillation using realistic apparatus is sufficient to create *private entanglement*[1] between Alice and Bob, i. e. pairs of entangled qubits of which Eve is guaranteed to be disentangled even though they are not pure EPR pairs. If these pairs are used to teleport quantum information from Alice to Bob, they can be regarded as a *noisy but private quantum channel*.

This will also prove the security of quantum communication using the entanglement-based quantum repeater, since it is only necessary to consider the outermost entanglement purification step in the NEPP, which is performed by Alice and Bob exclusively, i. e. without the support of the parties at the intermediate repeater stations. In particular, it is not necessary to analyze the effect of noisy Bell measurements on the security. In the worst case scenario, Alice and Bob assume that all repeater stations are completely under Eve's control, anyway. For this reason, Alice and Bob are not allowed to make assumptions on the method how the pairs have been distributed.

To summarize, our result implies that long-distance quantum communication, using the quantum repeater, is also secure quantum communication.

3.1 The security proof

In this section we will show that 2–EPP with noisy apparatus is sufficient to factor out Eve in the Hilbertspace of Alice, Bob, their laboratories, and Eve. For the proof, we will first introduce the concept of the *lab demon* as

---

[1] We owe the term *private entanglement* to Charles Bennett.

a simple model of noise. Then we will consider the special case of binary pairs, where we have obtained analytical results. Using the same techniques, we generalize the result to the case of Bell-diagonal ensembles. To conclude the proof, we show how the most general case of ensembles, described by an arbitray entangled state of all the qubits on Alice's and Bob's side, can be reduced to the case of Bell-diagonal ensembles.

3.1.1 The effect of noise

Our security proof takes into account that quantum operations are accompanied by noise. We assume that unitary operations, which act on one qubit (two qubits) are *preceeded* by a one- (two-)qubit correlated Pauli channel (see Section 2.3.1). This restriction is mainly due to technical reasons; however, as we will see below, noise of an arbitrary type can be "regularized" to the Pauli type.

In one entanglement purification step, we concentrate on two EPR pairs. We call the qubits in Alice's hand a_1 and a_2. On the other hand, we can only describe the state of the pairs if we take Bob's degrees of freedom into account. For that reason, we denote these degrees of freedom by an ellipsis $(\ldots)$. Thus, for noise in Alice's apparatus, Eq. (2.12) can then be written as

$$\rho_{a_1 a_2 \ldots} \longrightarrow \sum_{\mu,\nu=0}^{3} f_{\mu\nu} \sigma_\mu^{(a_1)} \sigma_\nu^{(a_2)} \rho_{a_1 a_2 \ldots} \sigma_\mu^{(a_1)} \sigma_\nu^{(a_2)} , \tag{3.1}$$

with the normalization condition $\sum_{\mu,\nu=0}^{3} f_{\mu\nu} = 1$. A similar expresion exist for noise in Bob's laboratory. Note that Eq. (3.1) includes, for an appropriate choice of the coefficients $f_{\mu\nu}$, the one- and two-qubit depolarizing channel and combinations thereof, as studied in [17, 29]; but it is more general. Since the Kraus operators are proportional to (products of) Pauli operators, we call the Pauli operators *error operators*.

Regularization of general types of noise The proof can be extended to more general noise models if a slightly modified protocol is used, where a twirling operation (step 1 of the preprocessing protocol described in Section 3.1.5) is repeated after every distillation round[2]. The concatenated

---

[2] We are grateful to C. H. Bennett for pointing out this possibility.

operation, which consists of a general noisy operation followed by this *regularization* operation, is Bell diagonal i. e. it maps Bell-diagonal states onto Bell-diagonal states, but since it maps *all* states to a Bell-diagonal state, it clearly cannot be written in the form (3.1). However, for the purpose of the proof, it is in fact only necessary that the concatenated map restricted to the space of all Bell-diagonal ensembles can be written in the form (4); we call such a map a *restricted Bell-diagonal map*. Clearly, not all restricted Bell-diagonal maps are of the form (3.1), which can be seen by considering a map which maps any Bell diagonal state to a pure Bell state. Such a map could, however, not be implemented locally. Thus the question remains whether a restricted Bell-diagonal map which can be implemented locally can be written in the form (3.1). Though we are not aware of a formal proof of such a theorem, we conjecture that it holds true: the reduced density operator of each qubit must remain in the maximally mixed state, which is indeed guaranteed by a mixture of unitary rotations. We also have numerical evidence which supports this conjecture. Note that in the case of such an active regularization procedure, it is important that the Pauli rotations which comprise the twirling operation can be performend well enough to keep the evolution Bell diagonal. This is, however, not a problem, since Alice and Bob are able to propagate the Pauli rotations through the unitary operations of the EPP, which allows them to perform the rotations just before a measurement, or, equivalently, to rotate the measurement basis. This is similar to the concept of error correctors (where the error consists in *ommiting* a required Pauli operation), as described in Section 3.2.1, and to the by-product matrix formalism developed in [64].

The lab demon The coefficients $f_{\mu\nu}$ in (3.1) can be interpreted as the joint probability that the Pauli rotations σ_μ and σ_ν occur on qubits a_1 and a_2, respectively. For pedagogic purposes we employ the following interpretation of (3.1): Imagine that there is a (ficticious) little demon in Alice's laboratory — the "lab demon" — which applies in each step of the distillation process randomly, according to the probability distribution $f_{\mu\nu}$, the Pauli rotation σ_μ and σ_ν to the qubits a_1 and a_2, respectively (see Fig. 3.1). The lab demon summarizes all relevant aspects of the lab degrees of freedom involved in the noise process.

Noise in Bob's laboratory, can, as long as we restrict ourselves to Bell diagonal ensembles, be attributed to noise introduced by Alice's lab demon,

Figure 3.1: The lab demon uses a classical random number generator in order to choose which “error operation” he applies to the qubits. Using his pen, he writes down which error operation he had applied to which qubit in which step of the purification process.

without loss of generality; this is, however, not a crucial restriction, as we will show in Section 3.1.5. It is also possible to think of a second lab demon in Bob's lab who acts similarly to Alice's lab demon. This would not affect the arguments employed in this chapter.

The lab demon does not only apply rotations randomly, he also maintains a list in which he keeps track of which rotation he has applied to which qubit pair in which step of the distillation process. What we will show in the following section is that, from the mere content of this list, the lab demon will be able to extract – in the asymptotic limit – full information about the state of each residual pair of the ensemble. This will then imply that, given the lab demons knowledge, the state of the distilled ensemble is a tensor product of pure Bell states. Furthermore, Eve cannot have information on the specific sequence of Bell pairs (beyond their relative frequencies) — otherwise she would also be able to learn, to some extent, at which stage the lab demon has applied which rotation.

From that it follows that Eve is *factored out*, i. e. the overall state of Alice's, Bob's and Eve's particles is described a density operator of the form

$$\rho_{\mathrm{ABE}} = \left(\sum_{i,j=0}^{1} f^{(i,j)} \, |\mathcal{B}_{i,j}\rangle_{\mathrm{AB}} \langle \mathcal{B}_{i,j}| \right) \otimes \rho_{\mathrm{E}} \,, \tag{3.2}$$

where $\sum_{i,j} f^{(i,j)} = 1$, and $\mathcal{B}_{i,j}$ describe the four Bell states as defined in Sec. 3.1.5.

Note that the lab demon was only introduced for pedagogical reasons. In reality, there will be other mechanisms of noise. However, all physical processes that result in the same completely positive map (3.1) are equivalent, i. e. cannot be distinguished from each other if we only know how they map an input state ρ_i onto an output state ρ_f. In particular, the processes must lead to the same level of security (regardless whether or not error flags are measured or calculated by anybody): otherwise they would be distinguishable.

In order to separate conceptual from technical considerations and to obtain analytical results, we will first concentrate on the special case of binary pairs and a simplified error model. After that, we generalize the results to *any* initial state.

3.1.2 Binary pairs

In this section we restrict our attention to pairs in the state

$$\rho_{AB} = A \left|\Phi^+\right\rangle_{AB}\left\langle\Phi^+\right| + B \left|\Psi^+\right\rangle_{AB}\left\langle\Psi^+\right| , \tag{3.3}$$

and to errors of the form

$$\rho_{AB}^{(1)} \otimes \rho_{AB}^{(2)} \to \sum_{\mu,\nu\in\{0,1\}} f_{\mu\nu} U_\mu^{(1)} U_\nu^{(2)} \rho_{AB}^{(1)} \otimes \rho_{AB}^{(2)} U_\mu^{(1)\dagger} U_\nu^{(2)\dagger} \tag{3.4}$$

with $U_0^{(i)} = \mathrm{id}^{(a_i)}$ and $U_1^{(i)} = {\sigma_x}^{(a_i)}$. Eq. (3.4) describes a *two-bit correlated spin-flip channel.* The indices 1 and 2 indicate the source and target bit of the bilateral CNOT (BCNOT) operation, respectively. It is straightforward to show that, using this error model in the 2–EPP, binary pairs will be mapped onto binary pairs.

At the beginning of the distillation process, Alice and Bob share an ensemble of pairs described by (3.3). Let us imagine that the lab demon attaches one classical bit to each pair, which he will use for book-keeping purposes. At this stage, all of these bits, which we call “error flags”, are set to zero. This reflects the fact that the lab demon has the same *a priori* knowledge about the state of the ensemble as Alice and Bob.

In each purification step, two of the pairs are combined. The lab demon first simulates the noise channel (3.4) on each pair of pairs by the process described. Whenever he applies a σ_x operation to a qubit, he inverts the error flag of the corresponding pair. Alice and Bob then apply the 2–EPP to each pair of pairs; if the measurement results in the last step of the protocol coincide, the source pair will be kept. Obviously, the error flag of that remaining pair will also depend on the error flag of the target pair, i. e. the error flag of the remaining pair is a function of the error flags of both “parent” pairs, which we call the *flag update function.* In the case of binary pairs, the flag update function maps two bits (the error flags of *both* parents) onto one bit. In total, there exist 16 different functions $f : \{0,1\}^2 \to \{0,1\}$. From these, the lab demon chooses the logical AND function as the flag update function, i. e. the error flag of the remaining pair is set to “1” if and only if both parent’s error flags had the value “1”.

After each purification step, the lab demon divides all pairs into two subensembles, according to the value of their error flags. By a straightforward calculation, we obtain for the coefficients A_i and B_i, which completely describe the state of the pairs in the subensemble with error flag i, the following recurrence relations:

$$\begin{aligned}
A_0' =& \frac{1}{N}(f_{00}(A_0^2 + 2A_0A_1) + f_{11}(B_1^2 + 2B_0B_1) \\
&+ f_s(A_0B_1 + A_1B_1 + A_0B_0)) \\
A_1' =& \frac{1}{N}\left(f_{00}A_1^2 + f_{11}B_0^2 + f_sA_1B_0\right) \\
B_0' =& \frac{1}{N}(f_{00}(B_0^2 + 2B_0B_1) + f_{11}(A_1^2 + 2A_0A_1) \\
&+ f_s(B_0A_1 + B_1A_1 + B_0A_0)) \\
B_1' =& \frac{1}{N}\left(f_{00}B_1^2 + f_{11}A_0^2 + f_sB_1A_0\right)
\end{aligned} \tag{3.5}$$

with $N = (f_{00} + f_{11})((A_0 + A_1)^2 + (B_0 + B_1)^2) + 2f_s(A_0 + A_1)(B_0 + B_1)$ and $f_s = f_{01} + f_{10}$.

For the case of uncorrelated noise, $f_{\mu\nu} = f_\mu f_\nu$, we obtain the following analytical expression for the fixpoints of the map (3.5):

$$\begin{aligned}
&A_0^\infty = \frac{1}{2} \pm \frac{\sqrt{f_0 - 3/4}}{f_0 - 1} \quad \text{or} \quad A_0^\infty = \frac{1}{2}, \\
&A_1^\infty = 0, \quad B_0^\infty = 0, \quad B_1^\infty = 1 - A_0^\infty.
\end{aligned} \tag{3.6}$$

In the following, we will concentrate on the non-trivial fixpoint defined by the plus sign in the expression for A_0^∞ above, which is the relevant fixpoint for our discussion. Note that, while Eq. (3.6) gives a non-trivial fixpoint of (3.5) for $f_0 \geq 3/4$, this does not imply that this fixpoint is an attractor. In order to investigate the attractor properties, we calculate the eigenvalues of the matrix of first derivatives,

$$M_D = \left.\begin{pmatrix} \frac{\partial A_0'}{\partial A_0} & \cdots & \frac{\partial B_1'}{\partial A_0} \\ \vdots & \ddots & \vdots \\ \frac{\partial A_0'}{\partial B_1} & \cdots & \frac{\partial B_1'}{\partial B_1} \end{pmatrix}\right|_{\text{fixpoint}} . \tag{3.7}$$

We find that the modulus of the eigenvalues of this matrix is smaller than unity for $f_0^{\text{crit}} = 0.77184451 < f_0 \leq 1$, which means that in this interval, the fixpoint (3.6) is also an attractor. This is in excellent agreement with a numerical evaluation of (3.5), where we found that $0.77182 < f_0^{\text{crit}} < 0.77188$.

We have also evaluated (3.5) numerically in order to investigate correlated noise (see Fig. 3.2). Like in the case of uncorrelated noise, we found that the coefficients A_0 and B_1 reach, during the distillation process, some finite value, while the coefficients A_1 and B_0 decrease exponentially fast, whenever the noise level is moderate.

In other words, both subensembles, characterized by the value of the respective error flags, approach a pure state asymptotically: The pairs in the ensemble with error flag "0" are in the state $|\Phi^+\rangle$, while those in the ensemble with error flag "1" are in the state $|\Psi^+\rangle$.

The sum $F^{\mathrm{cond}} = A_0 + B_1$ can be interpreted as the fidelity, which the lab demon would assign to the pairs; we call this sum the *conditional fidelity* of the pairs. Using this definition, the fact that both subensembles approach a pure state translates into the fact that the conditional fidelity approaches unity. Different from the conditional fidelity, the usual fidelity F is given by the sum $F = A_0 + A_1$, i. e. the trace over the error flag.

A map of the fixpoints

In Fig. 3.3, the values of $A_0^\infty, A_1^\infty, B_0^\infty, B_1^\infty, F^\infty$, and $F^{\mathrm{cond},\infty}$ (fixpoint values) have been plotted as a function of the noise parameter f_0. Most interesting in this graph is the shape of the curve representing the conditional fidelity: For all noise parameters $f_0 \leq 0.75$, the conditional fidelity reaches at the fixpoint the value 0.5, while for noise parameters $f_0 \geq 0.77184451$, the conditional fidelity reaches unity. In the intermediate regime $(0.75 < f_0 < 77184451)$, the curve can be fitted by a square root function $F^{\mathrm{cond}}(f_0) = 0.5 + 3.4\sqrt{f_0 - 0.75}$. The inset clearly shows that the values of both A_1 and B_0 vanish at $f_0 = f_0^{\mathrm{crit}}$.

The emergence of the intermediate regime of noise parameters, where the 2–EPP is able to purify and the lab demon does not gain full information on the state of the pairs is somewhat surprising and shows that the factorization of the eavesdropper is by no means a trivial consequence of (noisy) EPP. From a mathematical point of view, it is consistent with the finding after Eq. (3.7).

The purification curve

To understand the emergence of the intermediate regime better, we have plotted the purification curve for binary pairs, i. e. the $F_n^{\mathrm{cond}} - F_{n+1}^{\mathrm{cond}}$-diagram. A problem with this diagram is that the state of the pairs is specified by three independent parameters (A_0, A_1, B_0, B_1 minus normalization), so that

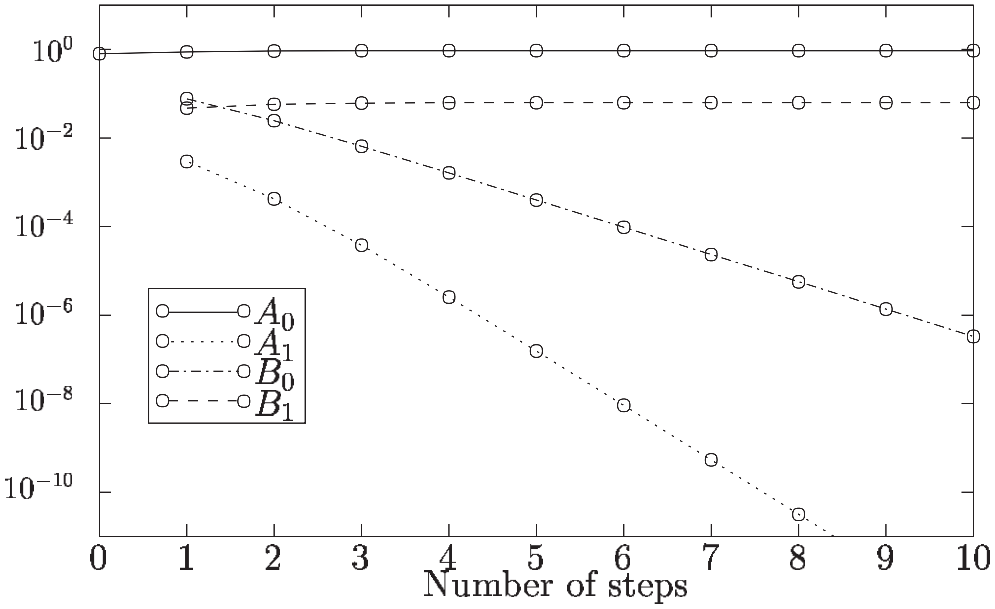


Figure 3.2: The evolution of the four parameters A_0, A_1, B_0, and B_1 in the security regime. Note that both A_1 and B_0 decrease exponentially fast in the number of steps. The initial fidelity was 80%, and the values of the noise parameters were $f_{00} = 0.8575$, $f_{01} = f_{10} = f_{11} = 0.0475$.

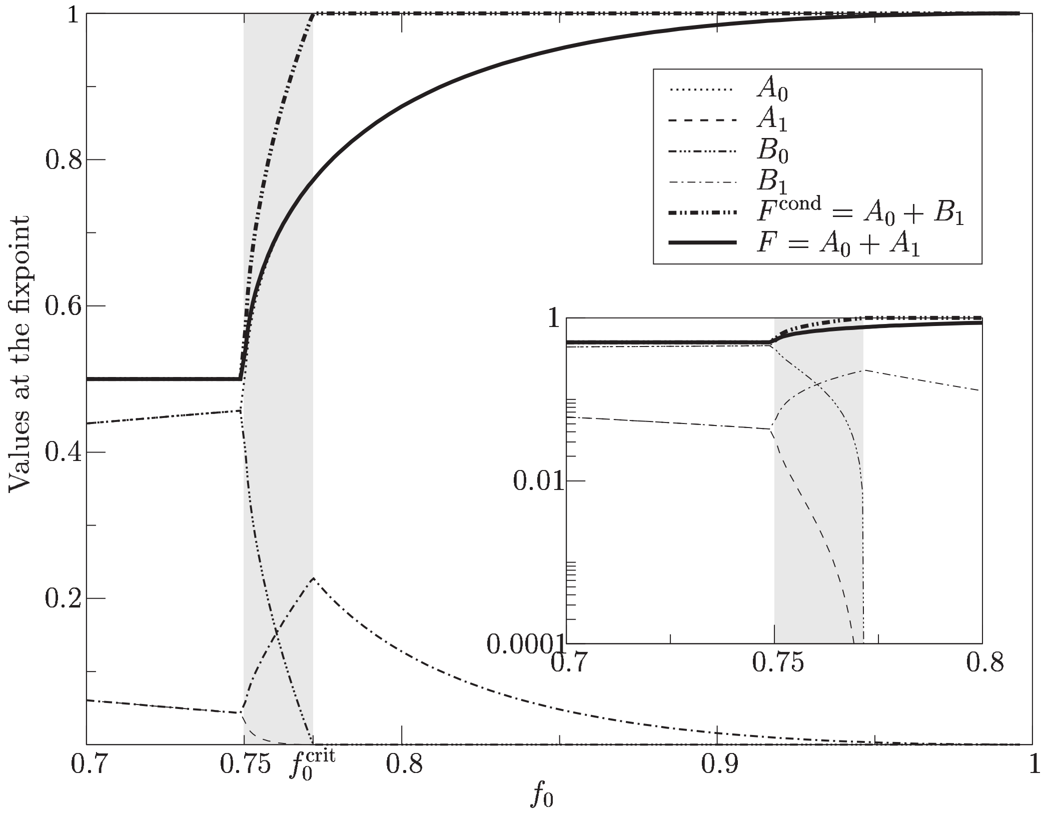


Figure 3.3: The values of $A_0, A_1, B_0, B_1, F, F^{\text{cond}}$ at the fixpoint as a function of the noise parameter f_0. The inset shows the intermediate regime, with a logarithmic scale on the y-axis.

such plots can only show a specific section through the full parameter space. Below we explain in detail how these sections have been constructed. Fig. 3.4 shows an overdrawn illustration of what we found: for noise parameters close to the purification threshold, the purification curves have a point of inflection. If the noise level increases (i. e. f_0 decreases), the curves are quasi "pulled down". For $f_0 = 0.77184451$, the slope of the purification curve at the fixpoint $F^{\text{cond}} = 1$ equals unity. If we further decrease f_0, the fixpoint is no longer an attractor, but due to the existence of the point of inflection, a new attractive fixpoint appeares.

To obtain the one-parametric curves shown in Fig 3.5, we used the following technique: starting with the point $(A_0, A_1, B_0, B_1)^{n=0} = (0.6, 0, 0.4, 0)$, we calculated $(A_0, A_1, B_0, B_1)^{n=1}$ by applying the recursion relations (3.5) once. The points on the straight line in parameter space connecting these two points have then been used as input values for the map given by the nth power of (3.5). For the plot, the resulting curve segments have been concatenated. This procedure has been repeated for all noise parameters f_0 that are specified in Fig. 3.5. Note that at the critical value $f_0^{\text{crit}} = 0.77184451$, the number of iterations required to reach any ϵ-environment of the fixpoint *diverges*. This fact will later be discussed in a more general case, see Fig. 3.9.

To conclude this section, we summarize: For all values of f_0 in the interval $0.77184451 \equiv f_0^{\text{crit}} \leq f_0 \leq 1$, the 2–EPP purifies and at the same time any eavesdropper is factored out. In a small interval, $0.75 < f_0 < f_0^{\text{crit}} \equiv 0.77184451$, just above the threshold of the purification protocol, the conditional fidelity does not reach unity, while the protocol is in the purification regime. Even though this interval is small and of little practical relevance (for these values of f_0 we are already out of the repeater regime [17] and purification is very inefficient), its existence shows that the process of factorization is not trivially connected to the process of purification.

3.1.3 Bell-diagonal initial states

Now we want to show that the same result is true for arbitrary Bell diagonal states (Eq. (2.14)) and for noise of the form (3.1). The procedure is the same as in the case of binary pairs; however, a few modifications are required.

In order to keep track of the four different error operators σ_μ in (3.1), the lab demon has to attach two classical bits to each pair; let us call them the phase error bit and amplitude error bit. Whenever a σ_x (σ_z, σ_y) error occurs, the lab demon inverts the error amplitude bit (error phase bit, both

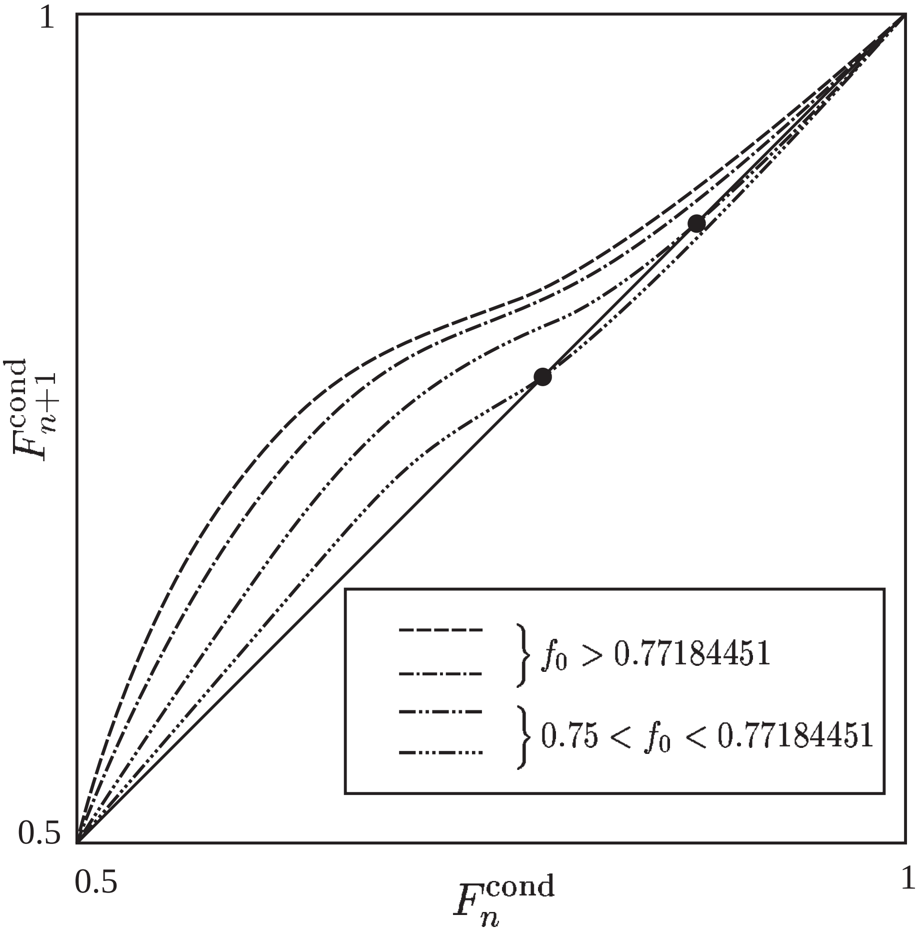


Figure 3.4: Illustration of the purification curve for variouse noise levels f_0. In order to make the point clear, the effect has been strongly overdrawn. See text.

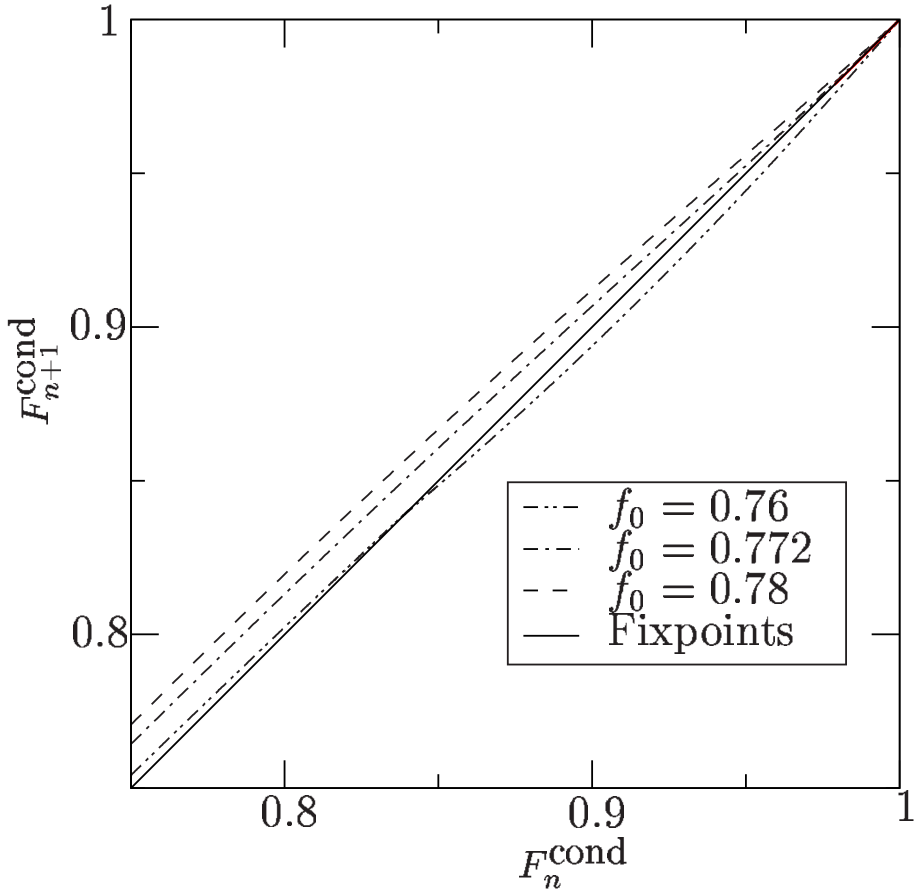


Figure 3.5: Actual data from which Fig. (3.4) has been inferred.

error bits). To update these error flags, he uses the update function given in Tab. 3.1. The physical reason for the choice of this flag update function will be given in the next section.

	(00)	(01)	(10)	(11)
(00)	(00)	(00)	(00)	(10)
(01)	(00)	(01)	(11)	(00)
(10)	(00)	(11)	(01)	(00)
(11)	(10)	(00)	(00)	(00)

Table 3.1: The value (phase error, amplitude error) of the updated error flag of a pair that is kept after a 2–EPP step, given as a function of the error flags of P_1 and P_2 (left to right and top to bottom, respectively).

Here, the lab demon divides all pairs into four subensembles, according to the value of their error flag. In each of the subensembles the pairs are described by a Bell diagonal density operator, like in Eq. (2.14), which now depends on the subensemble. That means, in order to completely specify the state of all four subensembles, there are 16 real numbers $A^{ij}, B^{ij}, C^{ij}, D^{ij}$ with $i, j \in \{0, 1\}$ required, for which one obtaines recurrence relations of the form

$$\begin{aligned} A_n^{(00)} &\rightarrow A_{n+1}^{(00)}(A_n^{(00)}, A_n^{(01)}, \ldots, D_n^{(11)}), \\ A_n^{(01)} &\rightarrow A_{n+1}^{(01)}(A_n^{(00)}, A_n^{(01)}, \ldots, D_n^{(11)}), \\ &\vdots \\ D_n^{(11)} &\rightarrow D_{n+1}^{(11)}(A_n^{(00)}, A_n^{(01)}, \ldots, D_n^{(11)}). \end{aligned} \tag{3.8}$$

These generalize the recurrence relations (3.5) for the case of binary pairs, and the relations (2.15) for the case of noiseless apparatus.

Like the recurrence relations (2.15) and (3.5), respectively, these relations are modulo normalization quadratic forms in the 16 state variables $\vec{a} = \left(A^{(00)}, A^{(00)}, \ldots, D^{(11)}\right)^T$, with coefficients that depend on the error parameters $f_{\mu\nu}$ only. In other words, (3.8) can be written in the more compact form (again modulo normalization)

$$\vec{a}'_j = \vec{a} M_j \vec{a}^T, \tag{3.9}$$

where, for each $j \in \{1, \ldots 16\}$, M_j is a real 16×16-matrix whose coefficients are polynomials in the noise parameters $f_{\mu\nu}$.

3.1.4 Numerical results

The 16 recurrence relations (3.8) imply a reduced set of 4 recurrence relations for the quantities $A_n = \sum_{ij} A_n^{(ij)}$, …, $D_n = \sum_{ij} D_n^{(ij)}$ that describe the evolution of the total ensemble (that is, the *blend* [33] of the four subensembles) under the purification protocol. Note that these values are the only ones which are known and accessible to Alice and Bob, as they have no knowledge of the values of the error flags. It has been shown in [17] that under the action of the noisy entanglement distillation process, these quantities converge towards a fixpoint $(A_\infty, B_\infty, C_\infty, D_\infty)$, where $A_\infty = F_{\max}$ is the maximal attainable fidelity [29].

Fig. 3.6 shows for typical initial conditions the evolution of the 16 coefficients $A_n^{(00)} \ldots D_n^{(11)}$. They are organized in a 4×4-matrix, where one direction represents the probability, with which the pair is in a specific Bell state, and the other indicates the value of the error flag. The figure shows the state (a) at the beginning of the entanglement purification procedure, (b) after few purification steps, and (c) at the fixpoint. As one can see, initially all error flags are set to zero and the pairs are in a Werner state with a fidelity of 70%. After a few steps, the population of the diagonal elements starts to grow; however, none of the other elements vanishes. At the fixpoint, all off-diagonal elements vanish, which means that there are *strict correlations* between the states of the pairs and their error flags.

Similar to the case of binary pairs (see Section 3.1.2), we define the fidelity $F_n \equiv A_n$, and the conditional fidelity $F_n^{\text{cond}} \equiv A_n^{(00)} + B_n^{(11)} + C_n^{(01)} + D_n^{(10)}$. Note that the first quantity is the sum over the four $|\Phi^+\rangle$ components in Fig. 3.6, while the latter is the sum over the four diagonal elements. The conditional fidelity is the fidelity which Alice and Bob would assign to the pairs if they knew the values of the error flags, i. e.

$$F_n^{\text{cond}} = \sum_{i,j} \left\langle \Phi^+ \right| \sigma_{i,j} \rho_{i,j} \sigma_{i,j} \left| \Phi^+ \right\rangle , \qquad (3.10)$$

where $\rho_{i,j}$ is the non-normalized state of the subensemble of the pairs with the error flag (i, j). For convenience, we use the phase- and spin-flip bits i and j as indices for the Pauli matrices, i. e. $\sigma_{00} = \mathrm{Id}, \sigma_{01} = \sigma_x, \sigma_{11} = \sigma_y, \sigma_{10} = \sigma_z$. We will utilize the advantages of this notation in Section 3.2.

The results that we obtain are similar to those for the binary pairs. We can again distinguish three regimes of noise parameters $f_{\mu\nu}$. In the high-noise regime (i. e., small values of f_{00}), the noise level is above the threshold

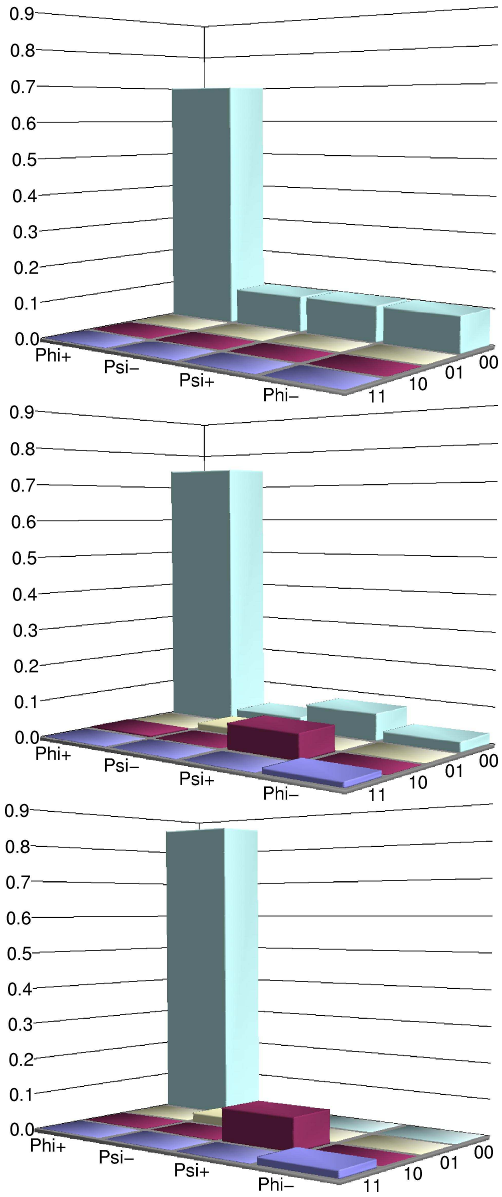


Figure 3.6: Typical evolution of the extended state under the purification protocol for the noise parameters $f_{00} = 0.83981, f_{0j} = f_{i0} = 0.021131$ and $f_{ij} = 0.003712$ for $i, j \in \{1, 2, 3\}$. This corresponds to a combination of one- and two-qubit white noise, as studied in [17, 29], with noise parameters $p_1 = 0.92$ and $p_2 = 0.9466$, considering noise in Alice's lab only, or $p_1 = 0.9592$ and $p_2 = 0.973$, considering noise in Alice's and Bob's laboratory.

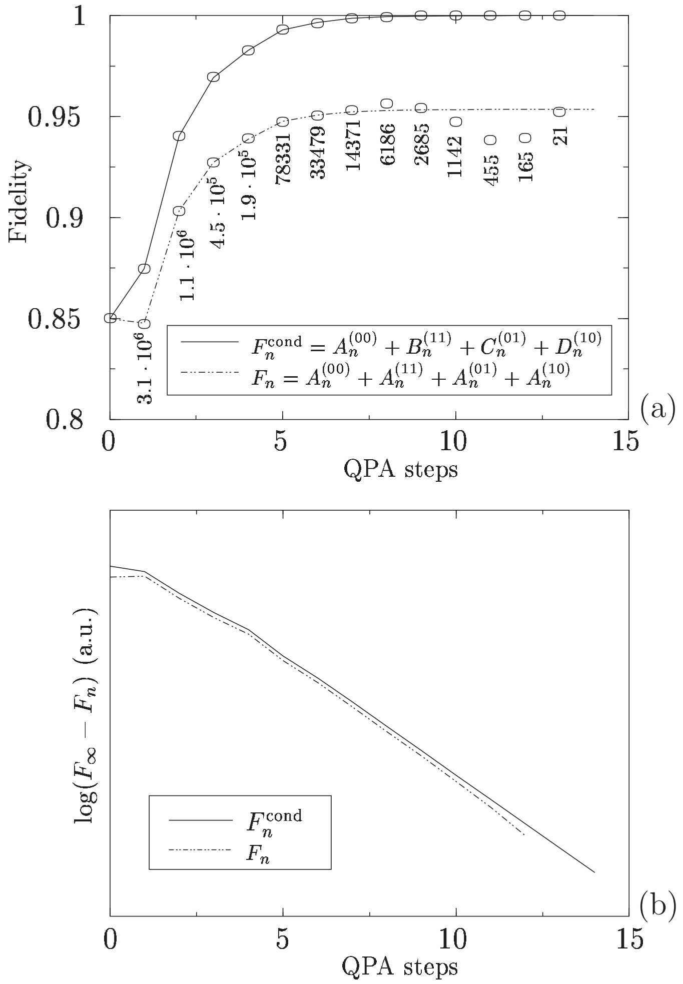


Figure 3.7: (a) The fidelities F and F_{cond} as a function of the number of steps in the security regime of the entanglement distillation process (analytical results (lines) and Monte Carlo simulation (circles)). The noise parameters for this plot were $f_{00} = 0.91279120$, $f_{0j} = f_{i0} = 0.0113896$ and $f_{ij} = 0.0020968$ for $i, j \in \{1, 2, 3\}$, corresponding to white noise with noise parameters $p_1 = 0.96$ and $p_2 = 0.968$ (see Fig. 3.6). The Monte Carlo simulation was started with 10^7 pairs; the numbers indicate how many pairs are left after each step of the distillation process. This decreasing number is the reason for the increasing fluctuations around the analytical curves.(b) The differences of F^{cond} and F and their respective fixpoints, plotted in a logarithmic scale. Both F^{cond} and F reach their fixpoints exponentially with (approximately) the same exponent.

of the 2–EPP and both the fidelity F and the conditional fidelity F^{cond} converge to the value 0.25. In the low-noise regime (i. e., large values of f_{00}), F converges to the maximum fidelity $F_{\max}$ *and* F^{cond} converges to unity (see Fig. 3.7). This regime is the *security regime*, where we know that secure quantum communication is possible. Like for binary pairs, there exists also an intermediate regime, where the 2–EPP purifies but F^{cond} does not converge to unity. For an illustration, see Fig 3.8. Note that the size of the intermediate regime is very small, compared to the security regime. Whether or not secure quantum communication is possible in this regime is unknown. However, the answer to this question is irrelevant for all practical purposes, because in the intermediate regime the distillation process converges very slowly, as shown in Fig. 3.9. In fact, the divergent behaviour of the process near the critical points has features remnant of a phase transition in statistical mechanics.

To estimate the size of the intermediate regime and to compare it to the case of binary pairs (Fig. 3.3), we consider the case of one-qubit white noise, i.e. $f_{\mu\nu} = f_\mu f_\nu$ and $f_1 = f_2 = f_3 = (1 - f_0)/3$. Here, this regime is known to be bounded by

$$0.8983 < f^{\mathrm{crit,lower}} < f_0 < f^{\mathrm{crit,upper}} < 0.8988.$$

Note that the size of the intermediate regime is much smaller than in the case of binary pairs.

Regarding the efficiency of the distillation process, it is an important question how many initial pairs are needed to create one pair with fidelity F^{cond}, corresponding to the *security parameter* $\epsilon \equiv 1 - F^{\mathrm{cond}}$. Both the number of required initial pairs (resources) and the security parameter scale exponentially with the number of distillation steps, so that we expect a polynomial relation between the resources and the security parameter ϵ. Fig. 3.10 confirms this relation in a log-log plot for different noise parameters. The straight lines are fitted polynomial relations; the fit region is indicated by the lines themselves.

3.1.5 Non-Bell-diagonal pairs

In the worst-case scenario, Eve generates an ensemble of N qubit pairs which she distributes to Alice and Bob. For that reason, Alice and Bob are not allowed to make specific assumptions on the state of the pairs. Most generally, the state of the $2N$ qubits, of which Alice and Bob obtain N qubits each,

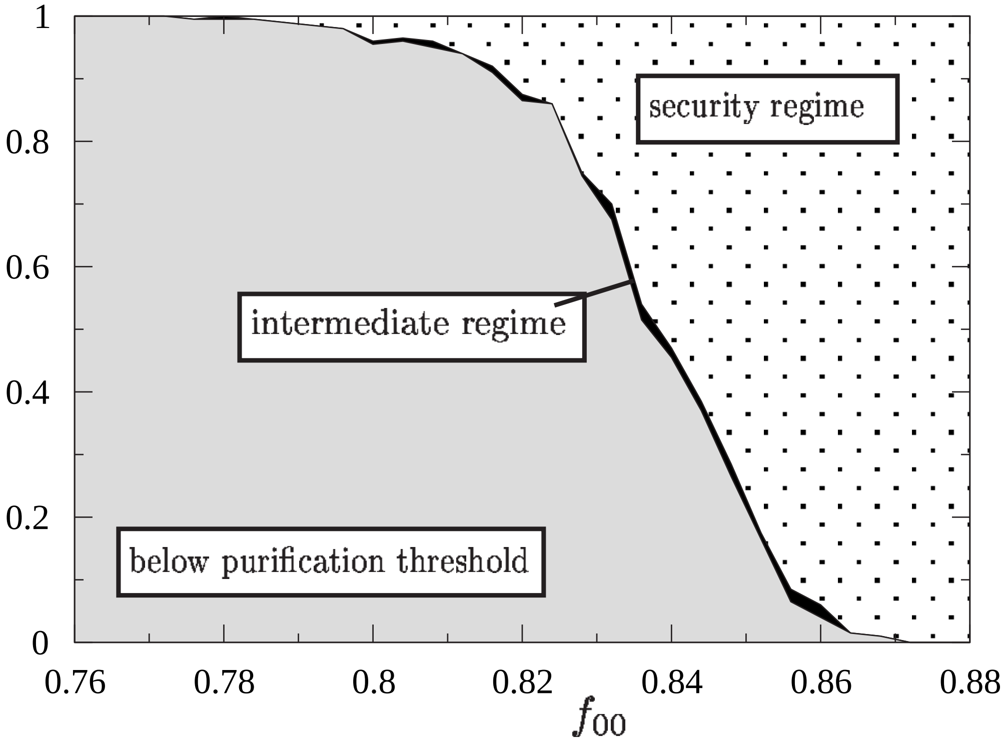


Figure 3.8: The size and the location of the three regimes of the distillation process. For fixed values of f_{00}, the remaining 15 noise parameters $f_{\mu\nu}$ have been choosen at random. Plotted is the relative frequency of finding the noise parameters in any of the three regimes as a function of f_{00}.

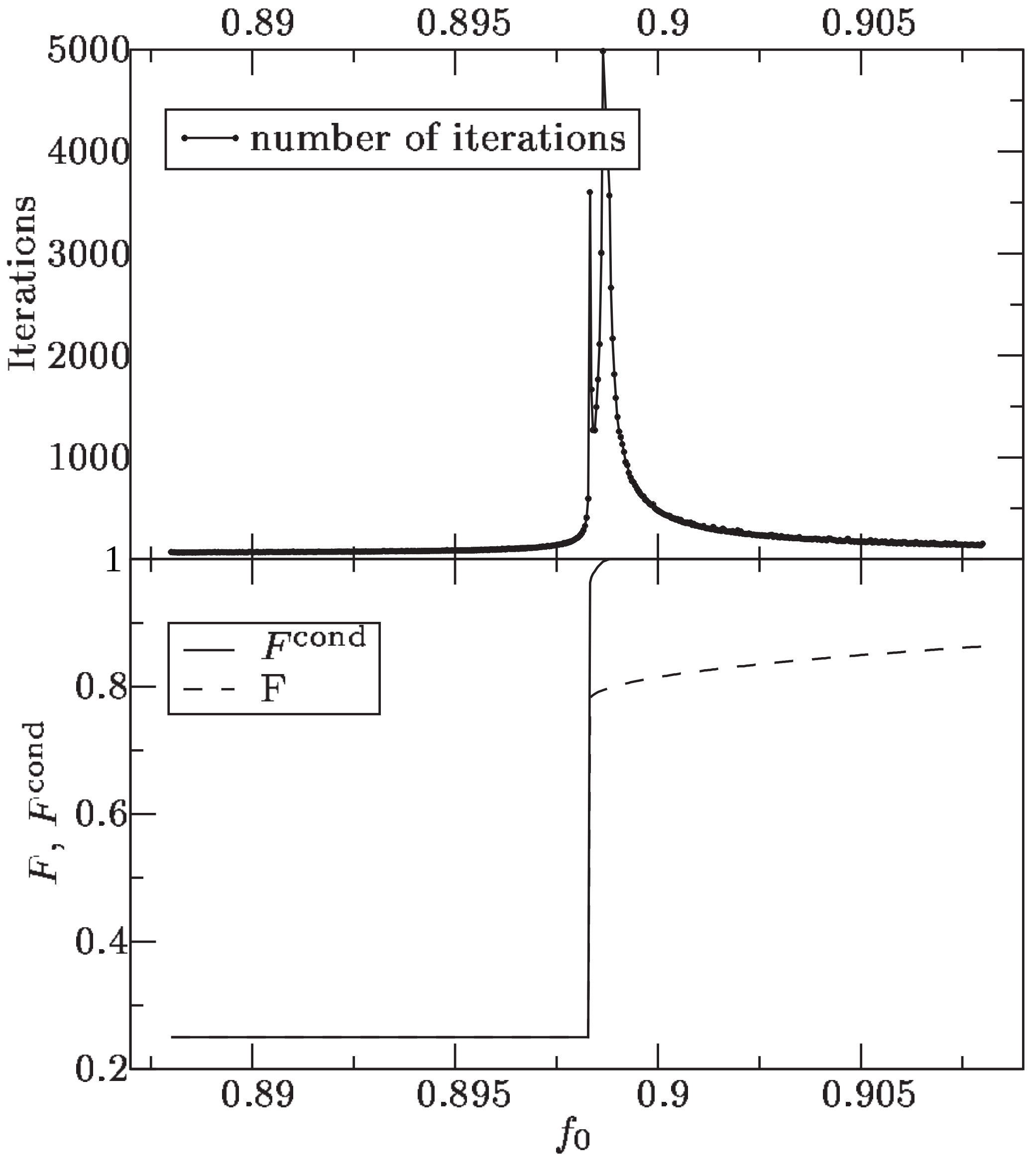


Figure 3.9: The effect of one-qubit white noise on the fidelity F, the conditional fidelity F^{cond} and the number of iterations required for the convergence up to an uncertainty $\epsilon = 10^{-12}$.

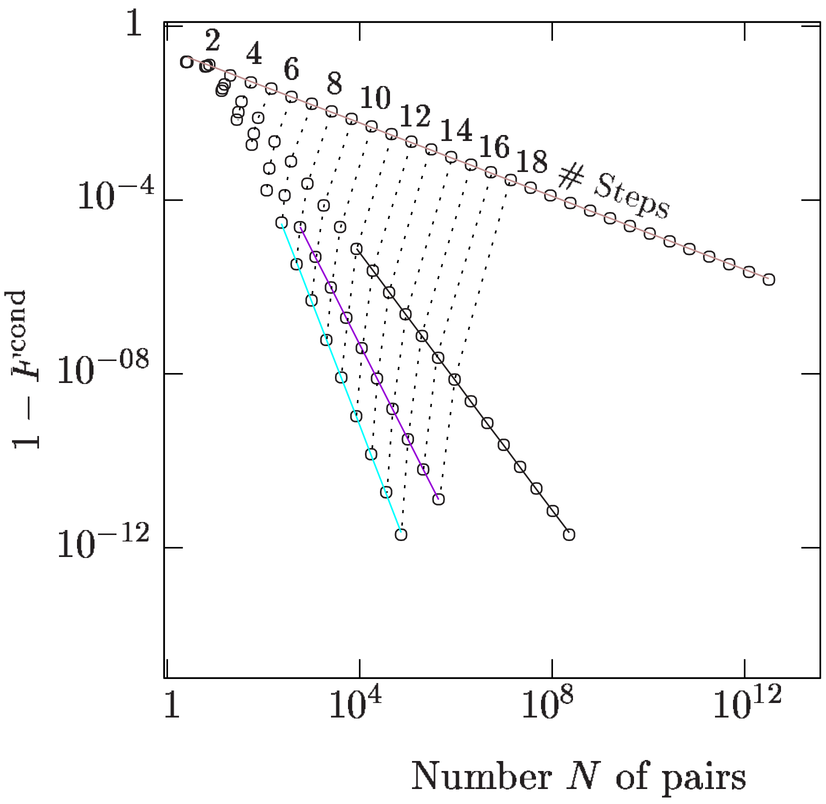


Figure 3.10: Number N of pairs needed to create one pair with conditional fidelity F^{cond}. The initial state of the pairs was of the Werner type with fidelity $F_0 = 85\%$. One- and two-qubit white noise (see Fig. 3.6) has been assumed with the noise parameters $(p_1, p_2) = (0.9333, 0.9466)$, $(0.9733, 0.9786)$, $(0.9866, 0.9833)$, $(0.9933, 0.9946)$ (from top to bottom).

can be written in the form

$$\rho_{AB} = \sum_{\substack{\mu_1\cdots\mu_N \\ \mu'_1\cdots\mu'_N}} \alpha_{\substack{\mu_1\cdots\mu_N \\ \mu'_1\cdots\mu'_N}} |\mathcal{B}^{(a_1b_1)}_{\mu_1}\cdots\mathcal{B}^{(a_Nb_N)}_{\mu_N}\rangle\langle\mathcal{B}^{(a_1b_1)}_{\mu'_1}\cdots\mathcal{B}^{(a_Nb_N)}_{\mu'_N}|. \tag{3.11}$$

Here, $|\mathcal{B}^{(a_jb_j)}_{\mu_j}\rangle$, $\mu_j = 00, 01, 10, 11$ denote the 4 Bell states associated with the two particles a_j and b_j and $j = 1, \ldots, N$, as defined in Eq. 2.8. In general, (3.11) will be an entangled state of $2N$ particles, which might moreover be entangled with additional quantum systems in Eve's hands; this allows for the possibility of so-called coherent attacks [23].

Upon reception of all pairs, Alice and Bob apply a preprocessing protocol to them, which consists of the following steps. Note that the preprocessing protocol is only applied once to the pairs, while the purification protocol (see 2.4.1) is applied in every step of the purification process.

Step 1 On each pair of particles (a_j, b_j), they apply randomly one of the four bi-lateral Pauli rotations $\sigma_k^{(a_j)} \otimes \sigma_k^{(b_j)}$, where k = 0,1,2,3.

Step 2 Alice and Bob randomly renumber the pairs, $(a_j, b_j) \longrightarrow (a_{\pi(j)}, b_{\pi(j)})$ where $\pi(j)$, $j = 1, \ldots, N$ is a random permutation.

These preprocessing steps are required in order to treat correlated pairs correctly. Note that they would also be required for the ideal distillation process [26], if one requires that the process converges for arbitrary states of the form (3.11) to an ensemble of pure EPR states. However, in [26] it is not crucial that the distillation process works for input pairs in the most general state (3.11), since it is possible to check whether the distillation process was successful (by measuring the fidelity of some of the remaining pairs).

In contrast, in the case of imperfect apparatus, we do not know a way to check whether the distillation process was successful. For instance, there is no way to “ask” the lab demon whether the pairs are in a pure state. For this reason, we have to ensure that the distillation process works for all input pairs which passed the initial fidelity check.

In both preprocessing steps, Alice and Bob discard the information which of the rotations and permutations, respectively, were chosen by their random number generator. Thus they deliberately loose some of the information about the ensemble which is still available to Eve (as she can eavesdrop the classical information that Alice and Bob exchange to implement the preprocessing steps). After step 1, their knowledge about the state can be described by the density operator

$$\tilde{\rho}_{AB} = \sum_{\mu_1\dots\mu_N} p_{\mu_1\dots\mu_N} |\mathcal{B}_{\mu_1}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N}^{(a_N b_N)}\rangle\langle\mathcal{B}_{\mu_1}^{(a_1 b_1)} \cdots \mathcal{B}_{\mu_N}^{(a_N b_N)}| \tag{3.12}$$

which corresponds to a *classically correlated ensemble* of pure Bell states. Since the purification protocol that they are applying in the following steps maps Bell states onto Bell states, it is statistically consistent for Alice and Bob to assume after step 1 that they are dealing with a (numbered) ensemble of pure Bell states, where they have only limited knowledge about which Bell state a specific pair is in. The fact that the pairs are correlated means that the order in which they appear in the numbered ensemble may have some pattern, which may have been imposed by Eve or by the channel itself. By applying step 2, Alice and Bob (*i*) deliberately ignore this pattern and (*ii*) randomize the order in which the pairs are used in the subsequent purification steps[3]. For all statistical predictions made by Alice and Bob, they may consistently describe the ensemble by the density operator. [4]

$$\tilde{\tilde{\rho}}_{AB} \;=\; \left(\sum_{\mu} p_\mu |\mathcal{B}_\mu\rangle\langle\mathcal{B}_\mu|\right)^{\otimes N} \equiv (\rho_{ab})^{\otimes N} \tag{3.13}$$

in which the p_μ describe the probability with which each pair is found in the Bell state $|\mathcal{B}_\mu\rangle$. At this point, Alice and Bob have to make sure that $p_{00} \equiv F > F_{\text{min}}$ for some minimum fidelity $F_{\text{min}} > 1/2$, which depends on the noise level introduced by their local apparatus. This test can be performed locally by statistical tests on a certain fraction of the pairs.

As Alice and Bob now own an ensemble of Bell diagonal pairs, they may proceed as described in the previous section. However, it is a reasonable question why Eve cannot take advantage of the additional information which she has about the state of the pairs: as she is allowed to keep the information about the twirl operations in step 1 and 2, from her point of view all the pairs remain in an highly entangled $2N$-qubit state. Nevertheless, all predicions made by Eve must be statistically consistent with the predictions made by

---

[3] This will prevent Eve from making use of any possibly pre-arranged order of the pairs, which Alice and Bob are meant to follow when performing the distillation process.

[4] While, strictly speaking, this equality holds only for $N \to \infty$, the subsequent arguments also hold for the exact but more complicated form of (3.13) for finite N.

Alice and Bob (or, for that matter, their lab demon), which means that the state calculated by Eve must be the same as the state calculated by the lab demon, tracing out Eve's additional information. As the lab demon gets a pure state at the end of the entanglement distillation process, this must also be the result which Eve obtains using her additional information, simply due to the fact that no pure state can be written as a non-trivial convex combination of other states.

3.2 How to calculate the flag update function

In this section, we analyse how errors are propagated in the distillation process. As was mentioned earlier, the state of a given pair that survives a given purification step in the distillation process depends on all errors that occured on pairs in earlier steps, which thus belong to the "family tree" of this pair. We will show that it is possible to summarize the effect of all errors in the family tree of each pair in an error flag, which consists of two classical bits. The values of the error flags can be calculated in a recursive scheme, and we call the recurrence relation the *flag update function.*

Each step of the distillation process consist of a number of unitary operations followed by a measurement, which we treat separately in the following two subsections.

3.2.1 Unitary transformations and errors

Consider an error U_{err} (i.e. a random unitary transformation) that is introduced before a unitary transformation U is performed on a state $|\psi\rangle$. Note that, without loss of generality, it is always possible to split up a noisy quantum operation close to a unitary operation U in two parts: first, a noisy operation close to identity, and afterwards the noiseless unitary operation U. For that reason, it only a matter of interpretation whether we think of a quantum operation which is accompanied by noise, e. g. as described by a master equation of the Lindblad form, or of the combination of some noise channel first and the noiseless quantum operation afterwards.

We call a transformation U_{corr} an *error corrector*, if the equation

$$U\,|\psi\rangle = U_{\mathrm{corr}} U U_{\mathrm{err}}\,|\psi\rangle \tag{3.14}$$

holds for all states $|\psi\rangle$. Equation (3.14) is obviously solved by $U_{\text{corr}} = UU_{\text{err}}^{-1}U^{-1}$.

We want to calculate the error corrector for the Pauli operators and the unitary operation $U_{2-\text{EPP}}$, which consists of the bilateral x-rotations and the BCNOT operation, as described in Section 2.4.1.

In what follows, it is important to note that Pauli rotations and all the unitary operations used in the entanglement purification protocol map Bell states onto Bell states: It is expedient to write the four Bell states as

$$|\mathcal{B}_{ij}\rangle = \frac{1}{\sqrt{2}}\left(|0j\rangle + (-1)^i\,|1\bar{j}\rangle\right), \tag{3.15}$$

using the *phase bit* i and the *amplitude bit* j with $i,j \in \{0,1\}$ [14], which we have implicitly employed in (3.11). In this notation, we get (ignoring global phases): $\sigma_x\,|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i,j\oplus 1}\rangle$, $\sigma_y\,|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i\oplus 1,j\oplus 1}\rangle$, and $\sigma_z\,|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i\oplus 1,j}\rangle$, where σ may act on either side of the pair. The $\oplus$ symbol indicates addition modulo 2. Consistent with this notation, σ_x is referred to as the amplitude flip operator, σ_z as the phase flip operator, and σ_y as the phase and amplitude flip operator.

The effect of the bilateral one-qubit rotation in the 2–EPP can be easily expressed in terms of the phase and amplitude bit,

$$U_x^A \otimes U_x^{B^{-1}}\,|\mathcal{B}_{i,j}\rangle = |\mathcal{B}_{i,j\oplus i}\rangle\,, \tag{3.16}$$

and the same holds for the BCNOT operation:

$$\text{BCNOT}\,|\mathcal{B}_{i,j}\rangle\,|\mathcal{B}_{i',j'}\rangle = |\mathcal{B}_{i\oplus i',j}\rangle\,|\mathcal{B}_{i',j\oplus j'}\rangle\,. \tag{3.17}$$

The effect of the unitary part of the 2–EPP onto two pairs in the states $|\mathcal{B}_{i,j}\rangle$ and $|\mathcal{B}_{i',j'}\rangle$ can be written in the form

$$U_{2-\text{EPP}}\,|\mathcal{B}_{i,j}\rangle\,|\mathcal{B}_{i',j'}\rangle = |\mathcal{B}_{i\oplus i',i\oplus j}\rangle\,|\mathcal{B}_{i',i'\oplus j'\oplus i\oplus j}\rangle\,, \tag{3.18}$$

where the first and second pair plays the role of the "source" and the "target" pair. Instead of (3.18), we will use an even more economic notation of the form $(i,j) \equiv |\mathcal{B}_{i,j}\rangle$. Eq. (3.18) can then be written as

$$(i,j)(i',j') \overset{2-\text{EPP}}{\longrightarrow} (i\oplus i', i\oplus j)(i', i'\oplus j'\oplus i\oplus j). \tag{3.19}$$

It is now straightforward to include the effect of the lab demon, Eq. (3.1). Applying Pauli rotations σ_{pa} and $\sigma_{p'a'}$ to the pairs before the unitary 2–EPP step $(\sigma_{00} = \mathrm{Id}, \sigma_{01} = \sigma_x, \sigma_{11} = \sigma_y, \sigma_{10} = \sigma_z)$, we obtain:

$$\begin{aligned} (i,j)(i',j') &\xrightarrow{\sigma} (i \oplus p, j \oplus a)(i' \oplus p', j' \oplus a') \\ &\xrightarrow{2-EPP} (i \oplus i' \oplus p \oplus p', i \oplus j \oplus p \oplus a) \\ &\qquad (i' \oplus p', i' \oplus j' \oplus i \oplus j \oplus p' \oplus a' \oplus p \oplus a). \end{aligned} \tag{3.20}$$

Comparing Eq. (3.19) and Eq (3.20), we find that the error corrector for the error operation $\sigma_{p,a} \otimes \sigma_{p',a'}$ is given by

$$U_{\text{corr}} = \sigma_{p \oplus p', p \oplus a} \otimes \sigma_{p', p' \oplus a' \oplus p \oplus a}, \tag{3.21}$$

independent of the initial state of the pairs. This is the desired result.

3.2.2 Measurements and measurement errors

As the 2–EPP does not only consist of unitary transformations but also of measurements, it is an important question whether or not errors can be corrected after parts of the system have been measured, and how we can deal with measurement errors. It is important to note that whether or not a pair is kept or discarded in the 2–EPP depends on the measurement outcomes. This means that, depending on the level of noise in the distillation process, different pairs may be distilled, each with a different "family tree" of pairs. This procedure is conceptually different from quantum error correction, in the following sense: In quantum error correction, it is necessary to correct for errors before performing a readout measurement on a logical qubit. In contrast, the lab demon performs all calculations only for bookkeeping purposes. *No* action is taken, and thus *no* error correction is performed, neither by the lab demon, nor by Alice and Bob.

In the analysis of the noisy entanglement distillation process [17, 29], not only noisy unitary operations have been taken into account, but also the effect of noisy measurement apparatus, which is assumed to yield the correct result with the probability η, and the wrong result with the probalility $1 - \eta$. Surprisingly, if only the measurements are noisy (i.e. all unitary operations are perfect), the 2–EPP produces *perfect* EPR pairs, as long as the noise is moderate ($\eta > 63.5\%$). The reason for this property lies in the fact that $F = 1$ is a fixpoint of the 2–EPP even with noisy measurements.

For a physical understanding of this fact, it is useful to note that in the distillation process, while the fidelity of the pairs increases, it becomes more and more unlikely that a pair which should have been discarded is kept due to a measurement error. This means that the increasingly dominant effect of measurement errors is that pairs which should have been kept are discarded. However, this does not decrease the fidelity of remaining pairs, but only the efficiency of the protocols.

This fact is essential for our goal to extend the concept of error correctors to the entire 2–EPP which actually includes measurements: As was shown in 3.2.1, noise in the unitary operations can be accounted for with the help of error correctors, which can be used to keep track of errors through the entire distillation process; on the other hand, the measurement in the 2–EPP may yield wrong results due to noise which occured in an earlier (unitary) operation. This has, however, the same effect as a measurement error, of which we have seen that it does not jeopardize the entanglement distillation process.

3.2.3 The reset rule

From the preceeding two sections, one can identify a first candidate for the flag update function. The idea is the following: The error corrector U_{corr} calculated in 3.2.1 describes how errors on the phase- and amplitude bit are propagated by the 2–EPP. For the lab demon, this means that instead of introducing an error operation $U_{\mathrm{err}} = \sigma_{p,a} \otimes \sigma_{p',a'}$ *before* the unitary part of the 2-EPP, he could, with the same result, introduce the operation $U_{\mathrm{corr}}^{-1} = U_{\mathrm{corr}} = \sigma_{p\oplus p',p\oplus a} \otimes \sigma_{p',p'\oplus a'\oplus p\oplus a}$ as an error operation *afterwards*.

Let us assume, motivated by the preceeding section, that the measurement which follows the unitary operation $U_{2-\mathrm{EPP}}$ does not compromise the concept of error correctors (This assumption will have to be modified later). The lab demon can then consider the error corrector as an recursive update rule for errors on the phase- and amplitude bit, i. e. for the phase- and amplitude error bits which constitute the error flag, in the following way:

At the beginning of the destillation process, the lab demon assigns two classical bits to each of the pairs, both set to the value zero (“0”). Whenever he applies a phase- or amplitude flip to a given pair, he inverts the first or the second bit of its error flag, respectively. For that reason, we call the two bits the *error phase bit* p_e and the *error amplitude bit* a_e.

If, for a given pair of pairs, the purification is successful, the source pair is kept. The error flag of the source pair is now calculated as a function of the previous error flags of both pairs, using the part of the error corrector (Eq. 3.21) which corresponds to the source pair: $(p_e, a_e)(p'_e, a'_e) \rightarrow (p_e \oplus p'_e, p_e \oplus a_e)$.

In any case, the lab demon has to discard the target-pair part of the error corrector, as the target pair is measured and does no longer take part in the distillation process. The knowledge of the error flag of a specific pair implies that the lab demon could undo the effect of all errors introduced in the family tree of this pair. For example, if the error flag has the value (i, j), the lab demon could apply the Pauli operator $\sigma_{i,j}$ in order to undo the effect of all errors he introduced up to that point.

It is well-known that the noiseless protocol asymptotically produces perfect EPR pairs in the state $\mathcal{B}_{0,0}$. It follows that — in the asymptotic limit — a pair with the error flag (i, j) must be in the state $\mathcal{B}_{i,j}$, i. e. the error flags and the states of the pairs are strictly correlated. This means, if the assumption made earlier was true, then the flag update function would be given by $(p_e, a_e)(p'_e, a'_e) \rightarrow (p_e \oplus p'_e, p_e \oplus a_e)$. However, as we will see, the assumption does not hold; for that reason we call this update function a *candidate* for the flag update function.

The candidate has already the important property that states with perfect correlations between the error flags (i. e. only the coefficients A_{00}, B_{11}, C_{01}, and D_{10} are non-vanishing) are mapped onto states with perfect correlations.

A serious deficiency of the candidate function as specified above is that perfect correlations between flags and pairs are not built up (unless they exist from the beginning). By following the distillation process in a Monte Carlo simulation that takes the error flags into account, the reason for this is easy to identify: The population of pairs which carry an amplitude error becomes too large. Now, the amplitude bit (not the amplitude *error* bit!) of a target pair is responsible for the coincidence of Alices and Bobs measurement results; if the amplitude bit has the value zero, the measurement results coincide and the source pair will be kept, otherwise it will be discarded. If the target pair carries an amplitude error, a measurement error will occur, and there are two possibilities: either the source pair will be kept even though it should have been discarded, or *vice versa*, then the source pair will be discarded although it should have been kept. Obviously, the latter case does not destroy the convergence of the entanglement distillation process (but it does have an impact on its efficiency); as Alice and Bob do not have any knowledge of the error flags, there is nothing that can be done in this case, and both pairs are discarded. The first case is more interesting. It is clear that for pairs with perfectly correlated error flags this case will not occur (due to the perfect correlations the amplitude error bit can only have the value one if the amplitude bit has the value one, which is just the second case). This means that we have the freedom to modify the error flags of the remaining pair *without* loosing the property that perfectly correlated states get mapped onto perfectly correlated states. It turns out that *setting both the error amplitude bit and the error phase bit of the remaining pair* to zero (*reset rule*) yields the desired behaviour of the flag update function, so that perfect correlations are being built up.

The amplitude error bit of the target pair is given by $p' \oplus a' \oplus p \oplus a$. The flag update function can thus be written as

$$(p,a)(p',a') \to \begin{cases} (p \oplus p', p \oplus a) & \text{if } p' \oplus a' \oplus p \oplus a = 0 \\ (0,0) & \text{otherwise.} \end{cases} \tag{3.22}$$

For convenience, the values of the flag update function are given in Tab. 3.1.

Note that the reset rule is an *ad hoc* solution: even though the above arguments do not prove that the desired correlations are built up, we can calculate the recurrence relations (3.8) using the flag update function (3.22). Analytical considerations in the case of binary pairs with one-qubit noise (see Sec. 3.1.2) and numerical iterations of Eq. (3.8) for all other cases show the desired result, i. e. that strict correlations are in fact built up.

3.3 Discussion

We have shown in Section 3.1, that the two-way entanglement distillation process is able to disentangle any eavesdropper from an ensemble of imperfect EPR pairs distributed between Alice and Bob, even in the presence of noise, i. e. when the pairs can only be purified up to a specific maximum fidelity $F_{\text{max}} < 1$. Alice and Bob may use these imperfectly purified pairs as a *secure* quantum communication channel. They are thus able to perform secure quantum communication, and, as a special case, secure classical communication (which is in this case equivalent to a key distribution scheme).

In order to keep the argument transparent, we have considered the case where noise of the form (3.1) is explicitly introduced by a fictious lab-demon, who keeps track of all error operations and performs calculations. However, using a simple indistinguishability argument (see Section 3.1.1), we could show that any apparatus with the noise characteristics (3.1) is equivalent to a situation where noise is introduced by the lab demon. This means that the security of the protocol does not depend on the fact whether or not anybody actually calculates the flag update function. It is sufficient to just use a noisy 2–EPP, in order to get a secure quantum channel.

For the proof, we had to make several assumptions on the noise that acts in Alices and Bobs entanglement purification device. One restriction is that we only considered noise which is of the form (3.1). However, this restriction is only due to technical reasons; we conjecture that our results are also true for most general noise models of the form (2.3). More generally, a regularization procedure (c.f. Section 3.1.1) can be used to *actively* make any noise Bell-diagonal. We have also implicitly introduced the assumption that the eavesdropper has no additional knowledge about the noise process, i. e. Eve only knows the publicly known noise characteristics (3.1) of the apparatus. This assumption would not be justified, for example, if the lab demon was bribed by Eve, or if Eve was able to manipulate the apparatus in Alice's and Bob's laboratories, for example by shining in light from an optical fiber. This concern is not important from a principial point of view, as the laboratories of Alice and Bob are considered secure by assumption. On the other hand, this concern has to be taken into account in a practical implementation.

Chapter 4

Cluster state purification

As we have seen in the previous chapters, entanglement and entanglement purification are fascinating and useful concepts in bipartite scenarios, and their theories are well established. In contrast, multi-party entanglement is still not well understood. Not surprisingly, this is reflected in the fact that there are only a few protocols known which are capable of distilling multi-party entangled states.

One well-known multi-party entanglement purification protocol has been described by Murao *et al.* [58], which is able to purify n-qubit GHZ states [40]. Later, Maneva and Smolin [55] gave a description of this protocol in terms of the stabilizer of GHZ states, which is useful in order to understand *why* this protocol works.

Recently, attention has been directed to a class of highly entangled multi-party states, which contains the class of GHZ states. However, there are many states in this class which are different from GHZ states, e. g., with respect to their entanglement properties. The preparation processes (and thus the states themselves) are completely described by undirected graphs. For this reason, these states are called *graph states* [37, 68]. In this chapter, we will show how one can construct an entanglement purification protocol for all graph states, which correspond to a bi-colorable graph. Note that the protocol is similar[1] to the purification protocol of n party GHZ states.

Linear cluster states [18] are special graph states. In the following section, we describe the purification protocol for linear cluster states. As a non-ideal case, we also take into account the noise which is introduced by the purifi-

---

[1] In fact, it is a generalization of the GHZ purification protocol, as we will see in Sec. 4.4

cation apparatus itself (Sec. 4.2). We find that in this case, it is impossible to distill perfect cluster states; however, we can show that the entanglement of the purified cluster states is completely private (Sec. 4.3). In Section 4.4, we generalize the results to the class of bi-colorable graph states.

A more detailed description of the purification of graph states can be found in [28].

4.1 The cluster purification protocol

4.1.1 Cluster states

Cluster states are defined in terms of eigenvalue equations of correlation operators; the specific form of these equations is given by a cluster — or, more generally, a graph — which indicates which qubits have interacted during the creation of this state. Note that there exist in general many graphs which generate a given cluster or graph state (up to local unitary operations). In the special case of n-qubit linear cluster states, which we will consider in the following section, they are given by

$$K_a = \sigma_z^{a-1} \sigma_x^a \sigma_z^{a+1} \tag{4.1}$$

for $a \in \{1 \dots n\}$, where σ_x^μ and σ_z^μ are the Pauli operators acting on qubit μ ($\mu \in \{1, \dots n\}$). Note that we use as a shorthand notation $\sigma_z^0 = \sigma_z^{n+1} = \mathbb{I}$. We call the correlation operator K_a *centered* at qubit a, i. e. at the qubit, where K_a has the σ_x operator. As one can easily see, these n operators commute, and none of them can be written as a product of the others. In fact, they constitute a complete set of commuting observables of the n-qubit system. Thus, there exists a basis of the n-qubit Hilbert space of simultaneous eigenstates of the correlation operators K_a, which we call the *cluster basis*; each element of the cluster basis is called a cluster state $|(k_1, k_2, \dots, k_n)\rangle$, which is uniquely identified by the eigenvalues $k_1, k_2, \dots, k_n$ of the correlation operators ($k_i \in \{-1, 1\}$). We call the cluster state $|\mathcal{C}_0\rangle = |(1, 1, \dots, 1)\rangle$ the *standard* cluster state, and the eigenvalue k_i of a given cluster state its i-th cluster bit.

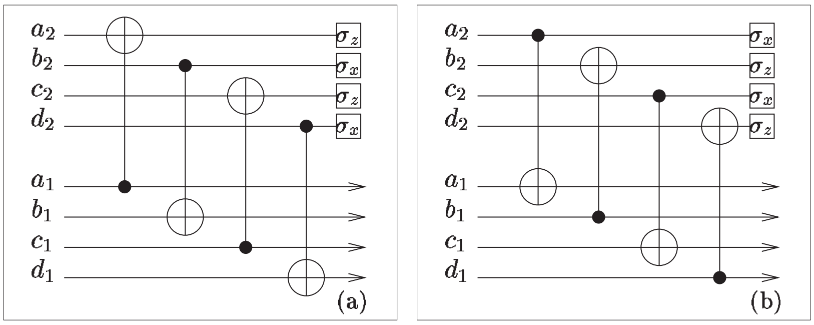


Figure 4.1: Alice, Bob, Charlie and Dora perform an alternating n-party CNOT operation (CNOTs) operation on two cluster states. Afterwards, the qubits of the second cluster state are measured in the σ_z and σ_x-basis, respectively (boxes). In protocol (a), they measure the products of the correlation operators with even numbers, in (b) with odd numbers.

4.1.2 Description and analytical treatment of the protocol

Let us now consider the following n-party protocol **P1**: Two n-party cluster states $\left|\Psi^{(1)}\right\rangle = |(k_1, k_2, \ldots, k_n)\rangle$ and $\left|\Psi^{(2)}\right\rangle = |(l_1, l_2, \ldots, l_n)\rangle$ are distributed to the n parties Alice, Bob, …, Norbert, in such a way that Alice gets the first qubits of both cluster states (a_1 and a_2), Bob gets the second qubits (b_1 and b_2), and so on.

Step 1: Each of the parties performs a controlled NOT (CNOT) operation on his or her pair of qubits, with alternating roles of source and target bit (see Fig. 4.1). In total, they perform the unitary operation

$$\mathrm{CNOTs} = \mathrm{CNOT}^{a_2}_{a_1} \otimes \mathrm{CNOT}^{b_1}_{b_2} \otimes \mathrm{CNOT}^{c_2}_{c_1} \otimes \mathrm{CNOT}^{d_1}_{d_2} \otimes \cdots . \tag{4.2}$$

The resulting state is again a product of cluster states; to be specific,

$$\begin{aligned} |\Psi\rangle_{\mathrm{CNOTs}} \equiv{} & \mathrm{CNOTs}\left|\Psi^{(1)}\right\rangle \left|\Psi^{(2)}\right\rangle = \\ & = |(k_1 l_1, k_2, k_3 l_3, k_4, \ldots)\rangle \, |(l_1, k_2 l_2, l_3, k_4 l_4, \ldots)\rangle . \end{aligned} \tag{4.3}$$

For the proof, we use the following well-known identities, where i_1 and i_2 denote the source and target qubits of a CNOT operation:

$$\begin{aligned} \sigma_z^{i_1}\mathrm{CNOT}^{i_2}_{i_1} &= \mathrm{CNOT}^{i_2}_{i_1}\sigma_z^{i_1}, & \sigma_z^{i_2}\mathrm{CNOT}^{i_2}_{i_1} &= \mathrm{CNOT}^{i_2}_{i_1}\sigma_z^{i_1}\sigma_z^{i_2}, \\ \sigma_x^{i_2}\mathrm{CNOT}^{i_2}_{i_1} &= \mathrm{CNOT}^{i_2}_{i_1}\sigma_x^{i_2}, & \sigma_x^{i_1}\mathrm{CNOT}^{i_2}_{i_1} &= \mathrm{CNOT}^{i_2}_{i_1}\sigma_x^{i_1}\sigma_x^{i_2}. \end{aligned} \tag{4.4}$$

We have to show that $|\Psi\rangle_{\text{CNOTs}}$ is an eigenstate of the correlation operators $K_i^{(\mu)}$ $(i \in \{a, \dots n\})$ of both cluster states $(\mu = 1, 2)$. We have to distinguish four cases:

1. $\mu = 1$ and $i = a, c, \dots$: $K_i^{(1)} |\Psi\rangle_{\text{CNOTs}} = \text{CNOTs}\ K_i^{(1)} K_i^{(2)} \left|\Psi^{(1)}\right\rangle \left|\Psi^{(2)}\right\rangle = k_i l_i |\Psi\rangle_{\text{CNOTs}}$
2. $\mu = 1$ and $i = a, c, \dots$: $K_i^{(1)} |\Psi\rangle_{\text{CNOTs}} = \text{CNOTs}\ K_i^{(1)} \left|\Psi^{(1)}\right\rangle \left|\Psi^{(2)}\right\rangle = k_i |\Psi\rangle_{\text{CNOTs}}$
3. $\mu = 2$ and $i = b, d, \dots$: $K_i^{(2)} |\Psi\rangle_{\text{CNOTs}} = \text{CNOTs}\ K_i^{(2)} \left|\Psi^{(1)}\right\rangle \left|\Psi^{(2)}\right\rangle = l_i |\Psi\rangle_{\text{CNOTs}}$
4. $\mu = 2$ and $i = b, d, \dots$: $K_i^{(2)} |\Psi\rangle_{\text{CNOTs}} = \text{CNOTs}\ K_i^{(1)} K_i^{(2)} \left|\Psi^{(1)}\right\rangle \left|\Psi^{(2)}\right\rangle = k_i l_i |\Psi\rangle_{\text{CNOTs}}$

In all cases, the formulae can be easily checked by using the definitions (4.2) and (4.1) of the CNOTs operation and the correlation operators and applying Eq. (4.4). □

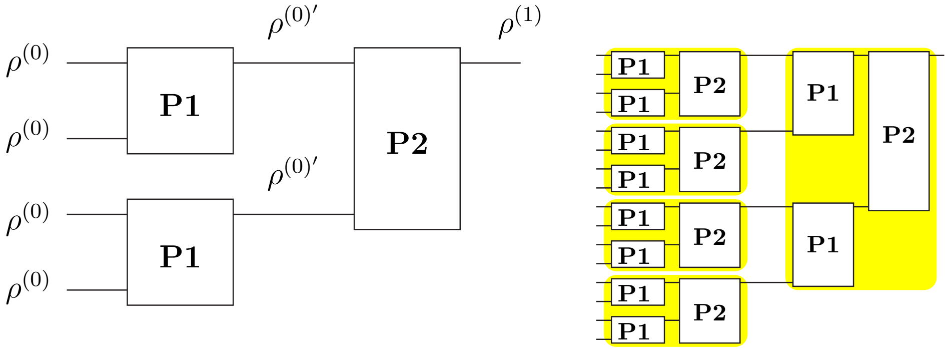
Step 2: All parties measure the qubit which belongs to the second cluster state, again in alternating directions. Alice, Charlie, …measure σ_z, and Bob, Dora,…measure σ_x. Since $K_2 = \sigma_z^a \sigma_x^b \sigma_z^c$, $K_4 = \sigma_z^c \sigma_x^d \sigma_z^e$, and so on, all parties can now cooperatively (using classical communication) calculate the (eigen)values of all even correlation operators, i. e. $k_2 l_2$, $k_4 l_4$ and so on. They keep the cluster state 1 if $k_2 l_2 = k_4 l_4 = \dots = 1$, otherwise it is discarded.

There exists a similar protocol **P2** which allows one to measure the products of the odd values of the correlation operators, i. e. $k_1 l_1$, $k_3 l_3$ and so on (see Fig. 4.1b). Similar to the purification protocol for GHZ states[58], we will use a combination of both protocols in an recursive process in order to distill asymptotically perfect cluster states $|\mathcal{C}_0\rangle$ from an ensemble of imperfect cluster states. We assume that all of these imperfect cluster states are described by the density operator $\rho^{(0)}$, with an initial fidelity $F^{(0)} = \langle \mathcal{C}_0 | \rho^{(0)} | \mathcal{C}_0 \rangle$ greater than some minimum initial fidelity F_{min}.[2]

The combined protocol **P1+P2** works as follows (see Fig. 4.2(a)): the n parties start with four (imperfect) cluster states, which are described by the density operator $\rho^{(0)}$. First, they apply protocol **P1** to two pairs of these cluster states, which (probabilistically) yield two cluster states $\rho^{(0)\prime}$. The

---

[2] As we will see below, the minimum fidelity F_{min} depends on the number n of parties.



(a) (b)

Figure 4.2: (a) The combination of the protocols **P1** and **P2**. Each line represents n qubits, which form a cluster state, while the blocks **P1** and **P2** symbolize the protocols shown in Fig. 4.1(a) and Fig. 4.1(b), respectively. (b) The entanglement purification process is a recursive scheme, where the protocol **P1+P2** is applied repeatedly. In the figure, two recursion steps are shown, which map 16 input states onto one output state.

two output states are then used as input states for the protocol **P2**, which yields $\rho^{(1)}$. The combined protocol can then be used in an recursive process (Fig. 4.2(b)).

4.1.3 Numerical analysis of the protocol

For the analysis of the protocol, it is sufficient to concentrate on density matrices which are diagonal in the cluster basis, because in all operations, the cluster diagonal elements of the density operators do not mix with non-diagonal elements. As we will see, the protocol converges to a state with one diagonal element equal to unity, and all other diagonal elements vanishing. From that it follows that in the final state, all off-diagonal elements also vanish.

In the case of cluster diagonal initial states

$$\rho^{(\mu)} = \sum_{k_1 \ldots k_n} b^{(\mu)}_{k_1 \ldots k_n} |k_1 \ldots k_n\rangle\langle k_1 \ldots k_n| \tag{4.5}$$

(with $\mu = 1, 2$), the states 1 and 2 are completely described by the vectors

$\vec{b}^{(1)} = \left(b^{(1)}_{k_1\cdots k_n}\right)$ and $\vec{b}^{(2)} = \left(b^{(2)}_{l_1\cdots l_n}\right)$ of the diagonal elements of the density operators $\rho^{(1)}$ and $\rho^{(2)}$. Using these vectors, we are able to calculate the outcome $\vec{b}'$ of the protocol **P1** or **P2** with the following algorithm:

```
$\vec{b}' := 0$
for all indices $(k_1, \ldots k_n)$ do
    for all indices $(l_1, \ldots l_n)$ do
        $(k'_1, \ldots, k'_n) := (k_1 l_1, k_2, k_3 l_3 \ldots)$
        if $k_2 l_2 = 1$ and $k_4 l_4 = 1$ and $k_6 l_6 = 1$ and $\ldots$ then
            $b'_{k'_1,\ldots,k'_n} = b'_{k'_1,\ldots,k'_n} + b^{(1)}_{k_1\ldots k_n} b^{(2)}_{l_1\ldots l_n}$
        end if
    end for
end for
```

Algorithm 1: The algorithm with which the result of the protocol **P1** is calculated.

The non-normalized result vector $\vec{b}'$ defines the state of the resulting cluster state. The algorithm for the protocol **P2** is analogous, mainly exchanging the role of even and odd numbers. Note that in these algorithms, it is not necessary to store the tensor product of the two cluster states, rather the tensor product and the projection are calculated “on the fly”. For n-qubit cluster states, the required memory scales like 2^n (only the vector of diagonal elements needs to be stored), and the run-time scales like 2^{2n}.

4.1.4 Results

In order to test the purification protocol, we start with noisy n-party linear cluster states of the form

$$\rho_{\text{initial}} = p\,|(1,\ldots,1)\rangle\langle(1,\ldots,1)| + \frac{1-p}{2^n}\mathbb{I},$$

i. e. with cluster states of fidelity $F = p + (1-p)/2^n$.

If the fidelity F is not too small, the entanglement purification process is in the purification regime, and yields (in the asymptotic limit) perfect cluster states. We find that the minimum fidelity for which the cluster states can still be purified, decays exponentially with the number n of parties (see Fig. 4.3).

For $n = 2$ and $n = 3$, the minimum required fidelity coincides with the values found for the purification of GHZ-states [58]. The reason for this coincidence is that the two- and tree-party linear cluster states are (up to local unitary operations) equal to two- and tree-qubit GHZ states, and that the cluster purification protocol is (in these two cases) equivalent to the GHZ purification protocol.

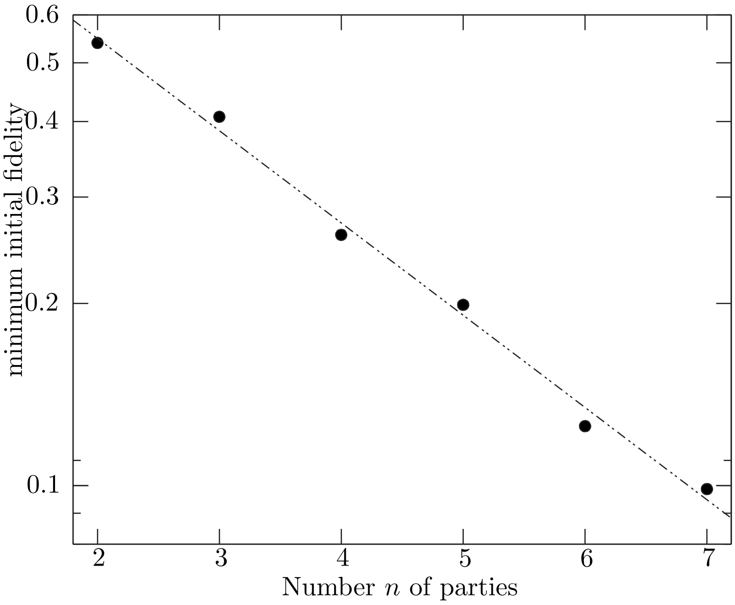


Figure 4.3: The required initial fidelity as a function of the number n of parties. The dotted curve is an exponential fit to the exact values (circles).

4.2 Noisy operations

In a realistic scenario, the n parties have to use some physical apparatus in order to perform the purification protocol. However, no physical apparatus can ever work perfectly, i. e. it will introduce noise by itself. In the case of bipartite entanglement purification, the influence of noisy operations is well-understood (see Section 2.4.2, Chapter 3, and Refs. [17, 36]). The main result is that bipartite entanglement purification still works with noisy apparatus, as long as its reliability is above a certain threshold value. However, there is a price which one has to pay: it is not possible to get perfectly entangled pairs using noisy apparatus; the fidelity will converge to a maximum fidelity $F_{\max} < 1$, which depends on the reliability of the quantum operations.

For the cluster purification protocol, one expects that the situation is quite similar. However, it is not *a priori* clear how the required reliability scales with the number n of parties. In particular, if the required reliability would approach unity (i. e., perfect operations) exponentially with growing n, the cluster purification protocol would not be of any practical use for large n. However, as we will see, the reliability threshold seems to be independent of n.

For the analysis of the purification process using noisy apparatus, we again concentrate on density operators which are diagonal in the cluster basis. On the one hand, this is not really a restriction since it is always possible to get rid of the off-diagonal elements using a twirling operation. On the other hand, it greatly simplifies the calculation; without this simplification, the number n of parties for which it is possible to perform the calculations in a given amount of time and memory would be smaller by a factor of two.

4.2.1 One-qubit white noise

In order to keep the influence of noise computable, we restricted our attention to one-qubit white noise (uncorrelated one-qubit depolarizing channel, see also Eq. 2.10). If we start with a n-qubit state $\rho_{a\cdots n}$ (which later on will be "close" to a pure cluster state), the depolarization of qubit i with reliability p can be written in the form

$$\begin{aligned}\rho_{a\cdots n} \longrightarrow \rho'_{a\cdots n} &= p\rho_{a\cdots n} + \frac{1-p}{2}\mathbb{I}_i \otimes \operatorname{tr}_i \rho_{a\cdots n} \\ &= p\rho_{a\cdots n} + \frac{1-p}{4}\sum_{l=0}^{3} \sigma_l^{(i)}\rho_{a\cdots n}\sigma_l^{(i)} \\ &\equiv \mathcal{D}_p^{(i)}\rho_{a\cdots n},\end{aligned} \tag{4.6}$$

where we defined the (linear) partial depolarization super-operator $\mathcal{D}_p^{(i)}$ of qubit i. The application of noise to all qubits of a cluster state is then given by

$$\rho_{a\cdots n} \to \prod_{i=1}^{n} \mathcal{D}_p^{(i)} \rho_{a\cdots n}. \tag{4.7}$$

The partial depolarization super-operators are convex combinations of the actions of the Pauli operators. One can easily check that for a cluster state $|(k_1, \ldots, k_{i-1}, k_i, k_{i+1}, \ldots k_n)\rangle$, a phase flip on qubit i ($\sigma_x^{(i)}$) inverts the eigenvalue k_i of the correlation operator K_i, and a spin flip on qubit i ($\sigma_x^{(i)}$) inverts the eigenvalues k_{i-1} and k_{i+1} of the adjacent correlation operators. The Pauli operator σ_y inverts thus (up to an irrelevant phase) the eigenvalues k_{i-1}, k_i, and k_{i+1}.

If the density operator $\rho_{a\cdots n}$ is diagonal in the cluster basis (which we conveniently write as $\rho_{a\cdots n} =_{\mathrm{c}} \mathrm{diag}(\vec{d})$), a flip of the i-th cluster bit ($k_i \to -k_i$) changes the diagonal vector in the following way:

$$\vec{d} \longrightarrow \tilde{\sigma}_x^{(i)} \vec{d} \tag{4.8}$$

Here, $\tilde{\sigma}_x^{(i)}$ is the i-th cluster bit flip operator, which looks in the cluster basis like the Pauli operator σ_x in the computational basis. Note that, in general, it is necessary to apply the squared modulus of a unitary operation to the diagonal vector (see Section 6.3). However, the σ_x spin flip operation coincides with its squared modulus.

Since each of the Pauli operators flips zero, one, two or three cluster bits, we get (in the cluster basis)

$$\begin{aligned} \mathcal{D}_p^{(i)}\,\mathrm{diag}\,(\vec{d}) &= \mathrm{diag}\left(\left(\frac{3p+1}{4}\mathbb{I} + \frac{1-p}{4}\left(\tilde{\sigma}_x^{(i)} + \tilde{\sigma}_x^{(i-1)}\tilde{\sigma}_x^{(i+1)} + \tilde{\sigma}_x^{(i-1)}\tilde{\sigma}_x^{(i)}\tilde{\sigma}_x^{(i+1)}\right)\right)\vec{d}\right) \\ &\equiv \mathrm{diag}\left(D_p^{(i)}\vec{d}\right). \end{aligned} \tag{4.9}$$

The effect of a partial depolarization, applied to all n qubits, on the diagonal vector is now given by the product $D_p = \prod_{i=1}^{n} D_p^{(i)}$. For a n-qubit cluster state, D_p is a real $2^n \times 2^n$-matrix, while a general super-operator would be described by a $2^{2n} \times 2^{2n}$-matrix. While this is already a simplification, we can still do better, as we will see in the next paragraphs.

For a given number of qubits n and a reliability parameter p, it is now possible to calculate D_p once and re-use it for each application of the depolarizing channel. However, for large n, it is numerically advantageous to store the one-qubit depolarizing matrices $D_p^{(i)}$ separately, which can be effectively be described by 8×8-matrices (for $1 < i < n$) or 4×4-matrices for $i = 1$ or $i = n$. We define the components of vector $\vec{d} = (d_{k_1k_2\cdots k_n})$ and the matrix $D_p^{(i)} = \left(\delta^{k'_{i-1}k'_ik'_{i+1}}_{k_{i-1}k_ik_{i+1}}\right)$. All indices take the values -1 or 1, so $D_p^{(i)}$ is really a 8×8-matrix. The components of the vector $\vec{d'} = D_p^{(i)}\vec{d}$ are then given by

$$d'_{k_1k_2\cdots k_n} = \sum_{k'_{i-1}k'_ik'_{i+1}} \delta^{k'_{i-1}k'_ik'_{i+1}}_{k_{i-1}k_ik_{i+1}} d_{k_1\cdots k_{i-2}k'_{i-1}k'_ik'_{i+1}k_{i+2}k_n}. \tag{4.10}$$

This method reduces the $n(2^n)^3$-overhead for the calculation of the matrix D_p, which has to be done once, and the 2^{2n}-overhead for the calculation of the product $D_p\vec{d}$, which has to be calculated for each application of the depolarizing channel, to a $n2^n$-overhead for each application of the depolarization.

4.2.2 Results

For bipartite entanglement purification protocols, it is well-known that there exists a threshold value for the reliability of the operations used in the purification process. If the apparatus is worse than this reliability value, then the purification process does not produce any entanglement. If the apparatus is above the threshold, the purification process works, and one can reach entangled quantum states up to some maximum fidelity (which depends on the reliability of the apparatus). Of course, one expects that the situation is quite similar in the case of multi-partite purification protocols. However, it is crucial how the threshold reliability $p_{\text{threshold}}$ of the noisy apparatus depends on the number n of the parties. If the required reliability approached unity for increasing n (maybe even exponentially), the protocol would be practically useless for a large number of parties. However, as it turns out, this is not the case, and the threshold reliability seems to approach a value of about 0.933 for increasing n (see Table 4.1).

4.3 On the security of the protocol

As we have seen in the previous section, it is not possible to distill perfect cluster states using noisy apparatus. For bipartite protocols, however, we have shown in Chapter 3 that even using noisy apparatus it is possible to

$n = 3$	$p_{\text{threshold}} = 0.938$
$n = 4$	$p_{\text{threshold}} = 0.933$
$n = 5$	$p_{\text{threshold}} = 0.934$
$n = 6$	$p_{\text{threshold}} = 0.933$
$n = 7$	$p_{\text{threshold}} = 0.933$

Table 4.1: Threshold values $p_{\text{threshold}}$ for the reliability of one-qubit depolarizing channel. For values greater than the threshold values, the n-party cluster purification protocols are in the purification regime.

distill (asymptotically) *private* Bell pairs, i. e. Bell pairs which are only entangled with the laboratories of the communication parties, but not with any other degree of freedom. In a cryptographic scenario, this means that the Bell pairs are actively disentangled from any eavesdropper who may have, in the worst case, created the Bell pairs. This would allow him or her to intentionally entangle them with additional degrees of freedom which he or she controls.

In this section, we show that this is also possible with the cluster purification protocol: if the parties only have imperfect apparatus which they use to purify cluster states, they will not be able to create perfect cluster states; however, the final state will be disentangled from all channel degrees of freedom.

The proof is analogous to the proof of Chapter 3. In a first step, the noise which the apparatus introduces during the purification process is replaced by a simple toy-model, the *lab demon*. The lab demon is an intelligent source of noise, which uses a classical random number generator in order to apply spin- and phase-flip operations on qubits, according to a given probability distribution $f_{\mu\nu}$. The result of the action of the lab demon is thus the average of the “flipped” quantum states:

$$\rho_{ab\ldots} \to \rho'_{ab} = \sum_{\mu\nu} \sigma_{\mu}^{(a)} \sigma_{\nu}^{(b)} \rho_{ab\ldots} \sigma_{\mu}^{(a)} \sigma_{\nu}^{(b)} \tag{4.11}$$

Here, $\rho_{ab\ldots}$ is a density operator of a quantum system, which includes two qubits a and b that are located at one specific party; however, it will include other qubits, which is indicated by the ellipsis $(\ldots)$. The lab demon acts on the two qubits at the same time, since the quantum operations in the purification protocols are two-qubit operations; for that reason it would be an over-simplification if we assumed that the noise acting on two qubits is uncorrelated.

The lab demons keep notes on which Pauli operators they applied to which qubits in which step of the purification process. As we will show, the mere knowledge of this list will, in the asymptotic limit, suffice to perfectly predict the state of the purified quantum systems. In other words, from the lab demons' point of view, all purified quantum systems end in a pure state. Note that it is not *a priori* clear that the lab demon's knowledge would suffice for the prediction, since the protocol includes measurements, and by introducing errors, the measurement outcomes will be changed, possibly leading to different choices by communicating parties, who might throw away qubits which they should have kept and *vice versa*.

From the list of errors, the lab demons calculate the so-called *error flags*. An error flag as a piece of classical information, which is "attached" to each cluster state. In case of a n qubit cluster state, we need n classical bits $\vec{\lambda}^{(j)} = (\lambda_1^{(j)}, \dots \lambda_n^{(j)}) \in \{-1, 1\}^n$ for the error flag. Here, the index j denotes the number of the cluster state in the ensemble of all cluster states. Initially, before the first step of the purification process, all error flags are set to unity, i. e. $\vec{\lambda}^{(j)} = (1, \dots, 1)$ for all j. Whenever the ith lab demon applies a phase flip operation (σ_z) to the ith qubit of cluster state j, in the error flag j the ith bit is flipped, i. e.

$$\vec{\lambda}^{(j)} = (\lambda_1^{(j)}, \dots \lambda_i^{(j)}, \dots, \lambda_n^{(j)}) \to \vec{\lambda}'^{(j)} = (\lambda_1^{(j)}, \dots - \lambda_i^{(j)}, \dots \lambda_n^{(j)}). \qquad (4.12)$$

If he applied an amplitude flip operation (σ_x), the *adjacent* bits of the error flag are flipped, i. e.

$$\begin{aligned} \vec{\lambda}^{(j)} &= (\lambda_1^{(j)}, \dots \lambda_{i-1}^{(j)}, \lambda_i^{(j)}, \lambda_{i+1}^{(j)}, \dots, \lambda_n^{(j)}) \\ &\to \vec{\lambda}'^{(j)} = (\lambda_1^{(j)}, \dots, -\lambda_{i-1}^{(j)}, \lambda_i^{(j)}, -\lambda_{i+1}^{(j)}, \dots, \lambda_n^{(j)}). \end{aligned} \qquad (4.13)$$

In both purification sub-protocols **P1** and **P2**, two cluster states are combined, one of which (probabilistically) survives. The error flag of the remaining (output) pair is then given by a function of both error flags of the input cluster states. This function is called the *flag update function* for protocol **P1** and **P2**, respectively.

4.3.1 The flag update function

The error flags of the first and second cluster state are given by the vectors $(\kappa_1, \kappa_2, \dots \kappa_n)$ and $(\lambda_1, \lambda_2, \dots \lambda_n)$, respectively. For the sub-protocol **P1**, the flag update function maps these $2n$ classical bits onto n classical bits, i. e.

$$f_{\text{flup}} : \{-1, 1\}^{2n} \to \{-1, 1\}^{n},$$

with

$$\begin{aligned} &(\kappa_1, \dots \kappa_n, \lambda_1, \dots \lambda_n) \\ &\quad \mapsto \begin{cases} (\kappa_1\lambda_1, \kappa_2, \kappa_3\lambda_3, \kappa_4, \dots) & \text{if } \kappa_2\lambda_2 = 1 \text{ and } \kappa_4\lambda_4 = 1 \text{ and } \dots \\ (1, 1, \dots, 1) & \text{otherwise} \end{cases} \end{aligned} \tag{4.14}$$

The first line of the definition takes into account how errors are propagated through the CNOTs operation. This means, that having applied a certain pattern of error operations (given by the error flag vectors) *before* the CNOTs operation is equivalent to applying a different pattern of error operations (given by the new error flag vector, $\vec{\kappa}' = f_{\text{flup}}(\vec{\kappa}, \vec{\lambda})$) *after* the CNOTs operation. The second line in the definition is the so-called *reset rule* (see Section 3.2.3).

It is necessary to introduce the reset rule, otherwise the security proof does not work. The reset rule is found by the following heuristics, which is equivalent to the heuristics used for the bipartite protocol:

The flag update function is only used if in the protocol the first cluster state is kept. This is the case if the values of all even eigenvalues of the second cluster state are equal to unity, i. e. $k_2 l_2 = k_4 l_4 = \dots = 1$ (see description of the protocol, step 2). If this is the case, and, at the same time, at least one of the “new” error flags associated with the even qubits of the second cluster state, has the value “-1”, then the errors in the history of the protocol have summed up in such a way that the first cluster state is kept, even though it would have been discarded, if there had not been introduced any errors. In that case, the error flag of the remaining cluster state is set (re-set) to $(1, 1, \dots 1)$. Note that this coincidence of the two before-mentioned conditions happens infrequently; in fact, in the course of the purification process, the probability for this coincidence converges to zero.

For the sub-protocol **P2**, the flag update function can be constructed by exchanging even and odd numbers. Using this method, an error flag can be calculated for each cluster state in each step of the purification process. By construction, the error flags only depend on the errors introduced by the lab demons.

4.3.2 The conditional fidelity

Using the error flag of each cluster state, it is now possible to divide the ensemble of all cluster states into 2^n sub-ensembles. The state of the sub-ensemble, which belongs to the error flag $\vec{\lambda}$, is labeled $\rho^{(\vec{\lambda})}$. It is convenient to normalize the density operators of the sub-ensembles to the relative frequency of the respective error flags, so that the (normalized) total density operator is just the sum of the density operators of the sub-ensembles. Using this convention, we define the *conditional fidelity*

$$F^{\text{cond}} = \sum_{\vec{\lambda}} \langle(\vec{\lambda})|\rho^{(\vec{\lambda})}|(\vec{\lambda})\rangle; \tag{4.15}$$

here, the state $|(\vec{\lambda})\rangle = |(\lambda_1, \dots, \lambda_n)\rangle$ denotes the cluster state as defined in Sec. 4.1.1. The conditional fidelity is a measure for the *purity* of the cluster states from the lab demons point of view: since the lab demons know the error flags of all cluster states, they can use this information to transform the ensemble of all cluster states into an ensemble with fidelity F^{cond}. In contrast, the usual fidelity, which is just the overlap of the total density operator with the cluster state $|(1, \dots, 1)\rangle$, is given by $F = \langle(1, \dots, 1)|\, \rho_{\text{total}}\, |(1, \dots, 1)\rangle$.

In order to investigate the behavior of the conditional fidelity in the course of the purification process, it is necessary to calculate the states of all 2^n sub-ensembles in each step of the purification process. Again, it is useful to note that all sub-ensembles are diagonal in the cluster basis; the states of all sub-ensembles is thus given by a real $2^n \times 2^n$-matrix M. The columns of this matrix are the vectors of the diagonal elements of the density matrices describing the sub-ensembles. Using this convention, physical action on the qubits is described by a matrix multiplication from the left, and a modification of the error flags is described by a matrix multiplication from the right.

Applying a one-qubit depolarizing channel is thus formally equivalent to a super-operator acting on the matrix of the diagonal vectors. To be specific, an error operation on qubit i results in flips of the cluster bit $i-1$, i, or $i+1$, respectively (see Eq. 4.8). Simultaneously, bit $i-1$, i, or $i+1$, of the error flag is flipped (Eq. 4.12 and 4.13). The result of applying the error operator

$\sigma_\nu^{(i)}$) is thus (for $\nu = x, y, z$)

$$\begin{aligned} M_z^{(i)} &= \tilde{\sigma}_x^{(i)} M \tilde{\sigma}_x^{(i)} \\ M_x^{(i)} &= \tilde{\sigma}_x^{(i-1)} \tilde{\sigma}_x^{(i+1)} M \tilde{\sigma}_x^{(i-1)} \tilde{\sigma}_x^{(i+1)} \\ M_y^{(i)} &= \tilde{\sigma}_x^{(i-1)} \tilde{\sigma}_x^{(i)} \tilde{\sigma}_x^{(i+1)} M \tilde{\sigma}_x^{(i-1)} \tilde{\sigma}_x^{(i)} \tilde{\sigma}_x^{(i+1)}. \end{aligned} \tag{4.16}$$

Under the action of the depolarizing channel on qubit i, the matrix M is thus transformed into a convex combination of matrices $M_z^{(i)}$,

$$M \to f_0 M + \sum_{\nu=1,2,3} f_\nu M_\nu^{(i)}. \tag{4.17}$$

```
$M' := 0$
for all indices $\vec{k} = (k_1, \dots k_n)$ do
    for all indices $\vec{l} = (l_1, \dots l_n)$ do
        if $k_2 l_2 = 1$ and $k_4 l_4 = 1$ and $k_6 l_6 = 1$ and $\dots$ then
            $\vec{k}' := (k_1 l_1, k_2, k_3 l_3 \dots)$
            for all flags $\vec{\kappa} = (\kappa_1, \dots \kappa_n)$ do
                for all flags $\vec{\lambda} = (\lambda_1, \dots \lambda_n)$ do
                    $\vec{\lambda}' = f_{\mathrm{flup}}(\vec{\kappa}, \vec{\lambda})$
                    $M_{\vec{k}'}^{\vec{\lambda}'} = M_{\vec{k}'}^{\vec{\lambda}'} + M_{\vec{k}}^{\vec{\kappa}} M_{\vec{l}}^{\vec{\lambda}}$
                end for
            end for
        end if
    end for
end for
```

Algorithm 2: The algorithm with which the (non-normalized) result of the application of sub-protocol **P1** can be calculated, taking the error flags into account.

The application of the CNOTs operation and the following measurement can be implemented by the following algorithm. M is the matrix of the diagonal elements of the sub-density-matrices before the sub-protocol **P1** is applied (see Algorith 4.3.2), and M' is the result matrix. Lower indices indicate the physical degrees of freedom, and upper indices indicate the error flags, i. e. the number of the sub-ensemble.

The algorithm calculates for all combinations of cluster states the results of the CNOTs operation (Eq. 4.3). In line 4, we check the result of the measurement of cluster state 2; if the results are such that the first cluster state is kept, it calculates its state $|\vec{k}'\rangle$, and performs for all combinations of error flags the following steps: (i) calculate the value of the new error flag $\vec{\lambda}'$, using the flag update function (line 8), (ii) add to the matrix element $M_{\vec{k}'}^{\vec{\lambda}'}$ the joint probability that cluster state one was in the state $|(\vec{k})\rangle$ with error flag $\vec{\kappa}$ *and* that the cluster state two was in the state $|(\vec{l})\rangle$ with error flag $\vec{\lambda}$ (line 9).

The result of this algorithm is the new matrix M', which containes the (non-normalized) states of all sub-ensembles after one step in the purification process.

For the sub-protocol **P2**, a similar algorithm can be given. As a result, we find that the conditional fidelity converges to unity in the course of the protocol, while the usual fidelity converges to some value $F^{\max}$ (see Fig. 4.4).

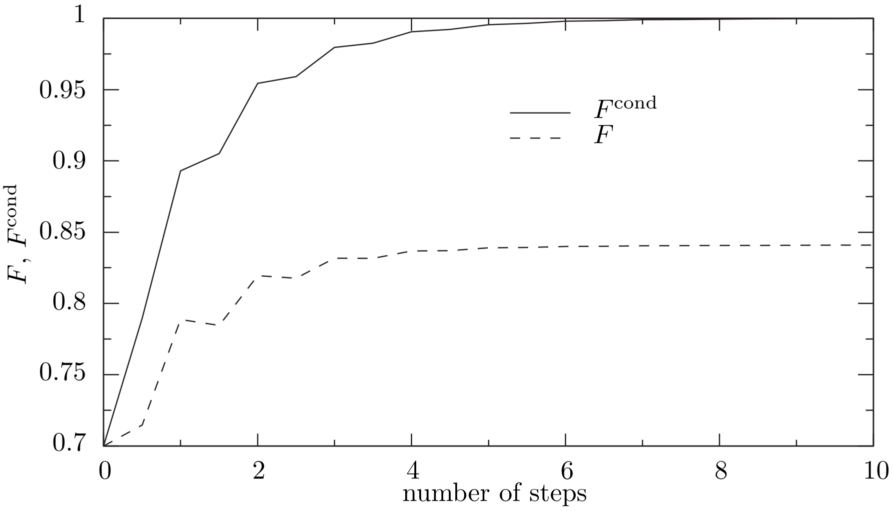
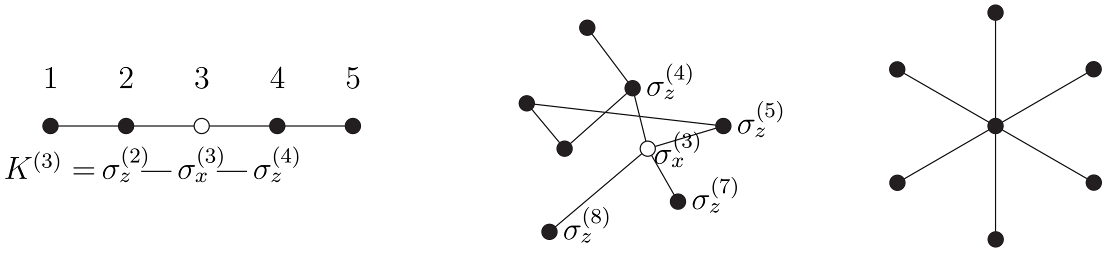


Figure 4.4: The fidelity and the conditional fidelity

4.4 Generalized cluster states

In the previous definition of the correlation operators of cluster states, it was necessary to know which qubits are adjacent to each other. For a linear chain



(a) (b) (c)

Figure 4.5: (a) Linear cluster states. As an example, the correlation operator K^3, which is centered on qubit 3, is shown. (b) Generalized cluster state. Two qubits are neighbors, if they are connected by a line (*edge*) The correlation operator which is centered at qubit 3 (white circle) is given by $K^3 = \sigma_x^{(3)}\sigma_z^{(4)}\sigma_z^{(5)}\sigma_z^{(7)}\sigma_z^{(8)}$. (c) GHZ-states are special kinds of cluster states, where one central qubit is connected to all other qubits.

of qubits, this is obvious: in Fig. 4.5 (a), adjacent qubits are connected by a line. However, we may also think of sets of qubits which are not arranged in a linear chain, or of qubits which are not arranged at all (Fig. 4.5 (b)). In this case, we have to explictly define which qubits are neighbors. In the figure, adjacent qubits are connected by a line, like in the case of a linear chain. Most generally, a neighborship relation is given by an (undirected) graph $G = (N, E)$, where the set N of qubits are the *nodes* of the graph, and the lines which connect the qubits are given by the set E of *edges* of the graph. In mathematical terms, $E \subset \{\{n_1, n_2\} | n_1, n_2 \in N \,\text{and}\, n_1 \neq n_2\}$. For each $i \in N$, we define the set of neighbors $\mathcal{N}(i) = \{j \in N | \{i, j\} \in E\}$.

For a graph $G = (N, E)$ and a qubit $i \in N$, we define a correlation operator $K^{(i)} = \sigma_x^{(i)} \prod_{j \in \mathcal{N}(i)} \sigma_z^{(j)}$. As in the case of linear cluster states, the correlation operators form a complete set of commuting operators, which define a basis of cluster states associated with the graph G.

A special graph is shown in Fig. 4.5 (c). The associated cluster states is – up to local unitaries – a GHZ state. This can be easily seen by looking at the correlation operators, after applying a Hadamard transformation to all but the central qubits. The correlation operators take then the form $K^{(1)} = \sigma_x^{(1)}\sigma_x^{(2)} \ldots \sigma_x^{(n)}$ and $K^{(i)} = \sigma_z^{(1)}\sigma_z^{(i)}$ for $i \in \{2, 3, \ldots n\}$, which are the correlation operators of GHZ states in the canonical form.

A subclass of all (generalized) cluster states are the so-called *bi-colorable graph* states. A graph is called bi-colorable, if there exist two subsets of nodes $N_1, N_2 \subset N$ with $N_1 \cap N_2 = \{\}$, $N_1 \cup N_2 = N$ and $E \subset \{\{n_1, n_2\} | n_1 \in N_1 \text{ and } n_2 \in N_2\}$. This subclass of cluster states is interesting, since it is possible to generalize the cluster purification protocol to bipartite graph states.

As in the case of linear cluster states, the protocol consists of two sub-protocols. We only describe one of the sub-protocols, say **P1**; the other sub-protocol can be easily obtained by exchanging the indices 1 and 2. Two bipartite graph states are distributed to n parties, each of which corresponds to a node of the graph. We call the qubits which belong to the first and the second state $a_1, b_1, \ldots n_1$ and $a_2, b_2, \ldots n_2$, respectively. In a first step, all parties apply a CNOT operation to their pair of qubits, in alternating directions; in total, they apply the operation

$$\mathrm{CNOTs} = \bigotimes_{k \in N_1} \mathrm{CNOT}_{k_1}^{k_2} \otimes \bigotimes_{k \in N_2} \mathrm{CNOT}_{k_2}^{k_1} \tag{4.18}$$

to all qubits. After this operation, all qubits of the second cluster state are measured: the qubits which belong to the subset N_1 are measured in the z-direction, and the remaining qubits are measured in the x-direction; the measurement results are $m_z^{(i)}$ for $i \in N_1$ and $m_x^{(i)}$ for $i \in N_2$, respectively. From these results, the n parties may now calculate the quantities $l_i = m_x^{(i)} \prod_{j \in \mathcal{N}(i)} m_z^{(j)}$ for all i in N_2. If all these quantities are equal to unity, the first cluster state is kept, otherwise it is discarded.

As we have shown [28], using this protocol it is possible to purify all bi-colorable graph states. It is a very interesting open question how the noise threshold depends on the structure of the graph; as we have seen in Section 4.2.2, the noise threshold does not depend on the mere *size*, i. e. the number of qubits of the graph state. However, for n-qubit GHZ states (see Figure 4.5 (c)) the threshold for allowed noise approaches unity exponentially with increasing number n of parties [28].

Chapter 5

Entanglement purification protocols from quantum codes

It has been shown by Bennett *et al.* [14], that quantum error correcting codes (see Section 2.5) are equivalent to one-way entanglement purification protocols, i. e. that it is possible to convert a one-way entanglement purification protocols into a quantum code and *vice versa*. However, the purification protocol which one gets as a result of this procedure does not fit into the "standard scheme" of entanglement purification protocols, which involves (a) distribution of EPR pairs through a noisy channel, (b) local unitary operations on the pairs, (c) measurements, and (d) operations which are conditioned on the measurement results (see Fig. 5.1 (b)). Note that the conditional action in step (d) is not necessarily trace conserving — it often consists of a "keep or throw away" decision. In contrast, the more elaborate protocols which we introduce in this chapter are derived from quantum codes which allow for error *correction* (in contrast to error *detection*); in this case it is possible to perform a conditional error correction operation

In this chapter, we show that a standard encoding/decoding procedure using quantum error correcting codes is *equivalent* to the standard scheme of entanglement purification. Here, we take advantage of the fact that for many quantum codes, encoding and decoding circuits are known explicitly [38]. This allows us to analyze how well the resulting protocols work if the unitary operations cannot be performed perfectly, but are subject to noise.

5.1 Creating purification protocols from coding circuits

5.1.1 Encoding and decoding

Fig. 5.1(a) shows an example of a standard encoding/decoding scheme, where the sender (Alice) wants to transmit the quantum state $|\psi\rangle$ of a qubit to the receiver, Bob. In order to protect the quantum information against errors in the transmission, Alice encodes it in a quantum code using a $[\![5,1,3]\!]$ quantum error correcting code. This is done by an encoding circuit (see Fig. 5.2) which performs the unitary operation U_{enc} on the transmitted qubit and some ancilla qubits. The ancilla qubits are initially in the states $|a_i\rangle$, with $a_i \in \{0,1\}$ (in the computational basis). It is possible for Alice and Bob to agree on the values a_i beforehand, e, g. $a_i = 0$ for all i; in this case, no classical communication is required at all. However, if for some reason Alice and Bob did not agree on these values, Alice has to tell Bob which values she chooses. In the figure, this classical one-way communication channel is indicated by the thick line.

Upon receiving all qubits, Bob performs the decoding operation $U_{\text{dec}} = U_{\text{enc}}^{-1}$ on the qubits and measures the ancilla qubits in the computational basis. The measurement results, together with the initial values a_i of the ancilla qubits, allow Bob to infer a *correction operation* $\mathcal{O}_{\text{corr}}$. If there have not been too many errors in the transmission of the qubits (the numbers depend on the quantum code used), the correction operation will restore the initial state $|\psi\rangle$ of the transmitted qubit.

$[\![n,k,d]\!]$-purification protocols

In Fig. 5.1(b), the setting is different: maximally entangled pairs of qubits in the state $|\Phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ are created somewhere between Alice and Bob; one qubit of each pair is sent to Alice, the other to Bob. Note that the in this figure, there are two time axes: On Bob's side, time increases from left to right, while on Alice's side, time increases from right to left.

Alice performs the transpose of the encoding operation of (a), and measures the "ancilla"-qubits in the computational basis (measurement results a_i). The remaining qubit could be measured in an arbitrary basis (e. g., the σ_z- or the σ_x-basis), thereby projecting it and its partner onto some state $|\psi\rangle$. However, as we will see below, it will be useful to leave this qubit

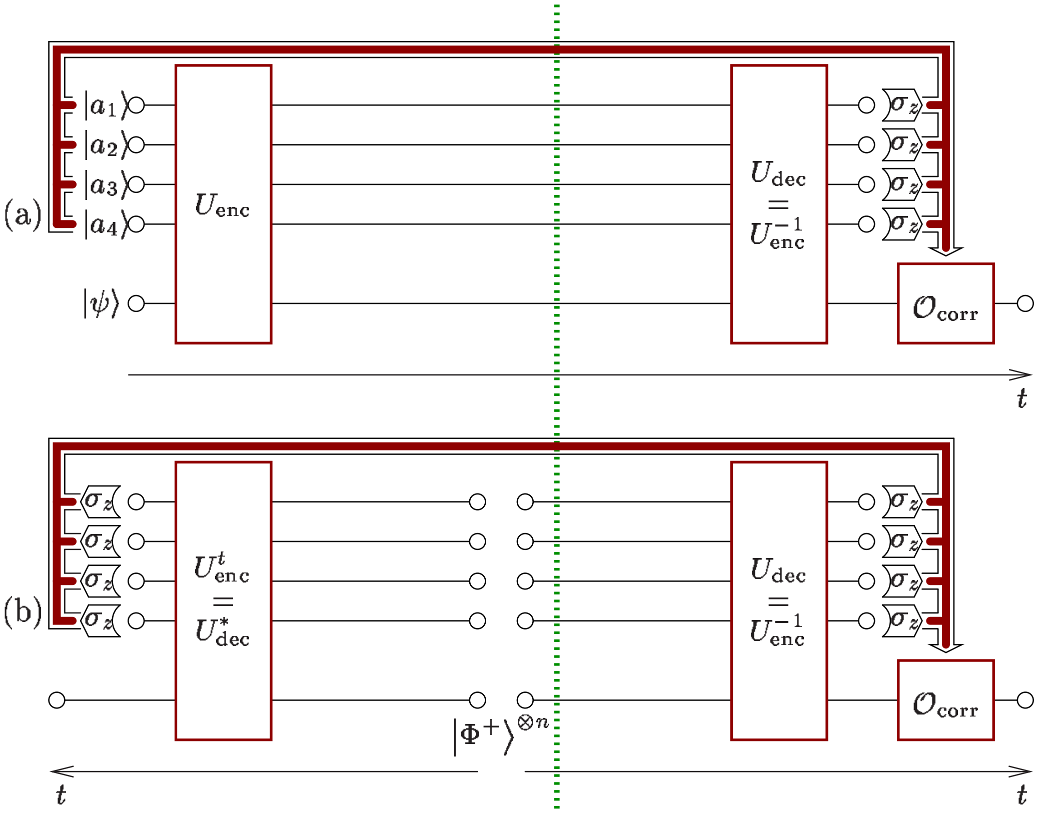

(a)
$|a_1\rangle$
$|a_2\rangle$
$|a_3\rangle$
$|a_4\rangle$
$|\psi\rangle$
U_{enc}
$U_{\mathrm{dec}} = U_{\mathrm{enc}}^{-1}$
σ_z
$\mathcal{O}_{\mathrm{corr}}$
t
(b)
σ_z
$U_{\mathrm{enc}}^t = U_{\mathrm{dec}}^*$
$|\Phi^+\rangle^{\otimes n}$
$U_{\mathrm{dec}} = U_{\mathrm{enc}}^{-1}$
σ_z
$\mathcal{O}_{\mathrm{corr}}$
t
t

Figure 5.1: The equivalence between a quantum coding/decoding scheme (a) and an entanglement purification protocol (b). Note that on the right-hand side of the dotted line, both figures are identical.

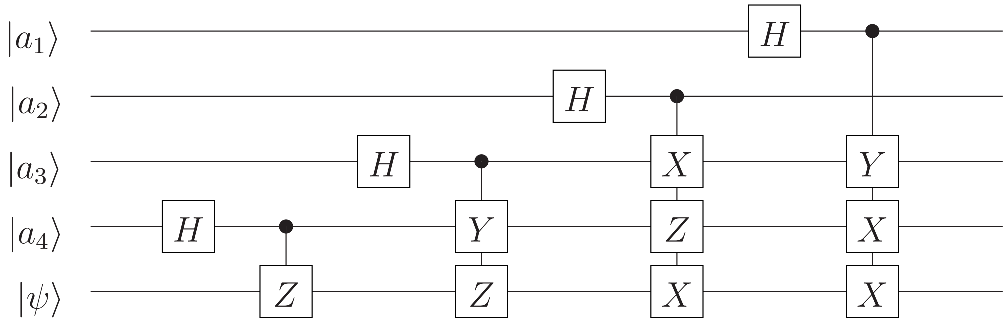


Figure 5.2: An example of an encoding circuit U_{enc} for the code $[\![5,1,3]\!]$ (from [38]).

unmeasured.

Since Alice's qubits were initially entangled with Bob's, the unitary operations and measurements on Alice's side project Bob's qubits into some state. In order to calculate this state, we use the UU^*-invariance of the state $|\Phi^+\rangle_{AB}^{\otimes n}$, i. e. $U_A \otimes U_B^* \, |\Phi^+\rangle_{AB}^{\otimes n} = |\Phi^+\rangle_{AB}^{\otimes n}$, where U_A and U_B is the same unitary operation, performed on Alice's and Bob's qubits, respectively. Note that this invariance implies $U_A \, |\Phi^+\rangle_{AB}^{\otimes n} = U_A U_A^{-1} U_B^t \, |\Phi^+\rangle_{AB}^{\otimes n} = U_B^t \, |\Phi^+\rangle_{AB}^{\otimes n}$. For Bob's state, we thus get

$$|\psi\rangle_B = {}_A\langle a|U^*_{\mathrm{dec,A}}|\Phi^+\rangle_{AB}^{\otimes n} = {}_A\langle a|U^t_{\mathrm{enc,A}}|\Phi^+\rangle_{AB}^{\otimes n} = U_{\mathrm{enc,B}}|a\rangle_B, \tag{5.1}$$

where $|a\rangle_B = |a_1, \ldots\rangle \otimes |\psi\rangle$.

In other words, in Fig. 5.1(b), Alice can prepare *a posteriori* the same type of state which she had prepared in Fig. 5.1(a), so that on the right-hand side of the dotted line, both parts of the figure show the very same situation; after applying the correction operation, Bob's qubit would be in the state $|\psi\rangle$, if Alice had measured her remaining qubit earlier. However, if Alice and Bob do not measure their qubits of the last pair, they are left with a pair which shows perfect σ_x- and σ_z-correlations, if there were not too many errors in the transmission of all qubits: Alice and Bob have created one perfect EPR-pair in the state $|\Phi^+\rangle$ from several "noisy" pairs. Fig. 5.1(b) is thus an entanglement purification protocol, which has been derived from a quantum code.

It should be noted that Bob may choose to discard his qubit (as a special case of a correction operation). In this case, he has to tell Alice to also discard her remaining qubit, and the protocol becomes a two-way entanglement purification protocol.

In general, quantum codes do not only protect one qubit, as in the example of Fig. 5.1; rather, a quantum error correcting code $[\![n,k,d]\!]$ encodes the state of $k \geq 1$ logical qubits into $n > k$ physical qubits. Such quantum codes will be converted into entanglement purification protocols, which create k more entangled pairs from n less entangled pairs. We call such protocols $[\![n,k,d]\!]$ entanglement purification protocols.

5.1.2 Error detection vs. error correction

Like classical codes, quantum codes can be used for error *detection* and for error *correction*. As a general rule, a quantum code $[\![n,k,d]\!]$ (minimum distance d) can detect d errors, and correct $\lfloor (d-1)/2 \rfloor$ errors. For this reason, using the same code, error detection is possible at higher error rates than error correction. On the other hand, error detection without correction requires two-way classical communication between sender (encoder) and receiver (decoder) of the quantum message, in order to guarantee a reliable transmission of the quantum information: whenever the receiver detects an error, he or she needs to send a "please discard and send again"-message to the sender.

In many settings of quantum communication, two-way classical communication is a cheap resource, and a restriction to one-way protocols seems to be artificial. In quantum computation, however, the situation is different, since the encoding takes place *before* the decoding, and the one-way communication is imposed by the temporal order of the encoding/decoding process. For this reason, it is necessary that errors can not only be detected, but also corrected. The error correction has to be performed in a *fault tolerant* way, and the theory of fault tolerant quantum computation shows that this goal can be achieved efficiently, using concatenated quantum codes and quantum gates, which act on encoded ("logical") qubits.

Clearly, quantum communication is a (trivial) quantum computation. However, the fact that in quantum communication two-way classical communication is available might be of advantage. In fact, it has been shown by Bennett *et al.* [14] that there exist quantum states which can be purified by quantum protocols with two-way classical communication, but by no one-way purification protocol.

To summarize, entanglement purification protocols, which are run in error detecting mode (EDM), are 2-EPP, and protocols which are run in error correcting mode (ECM), are 1-EPP.

The equivalence between quantum codes and purification protocols allows us to examine more closely the relation between 1-EPP and 2-EPP, and by comparing $[\![n,k,d]\!]$ EDM and ECM protocols, we will answer the questions: Which of the protocols are more efficient? Which of the protocols are more robust in a noisy environment?

5.2 The hashing protocol and quantum codes

The hashing protocol [14] is – in the asymptotic limit of large numbers N of pairs – a very efficient one-way entanglement purification protocol (1-EPP). However, it is not *a priori* clear how large N has to be in order to get close to the asymptotic limit. Further, the gate complexity of a circuit which implements the hashing protocol increases with increasing N. It is then not clear how the hashing protocol performs if the quantum gates are subject to noise themselves.

Recurrence protocols [13, 25], on the other hand, are two-way entanglement purification protocols (2-EPP). They are less efficient than the hashing protocol, but very tolerant regarding noisy apparatus. Quantum circuits which implement recurrence protocols involve, in general, only few qubits and are thus easy to analyze. Recently, a first experimental realization has been reported [60, 5].

The $[\![n,k,d]\!]$ EPP are a class of entanglement purification protocols, which interpolate between the hashing protocol and the recurrence protocols: On the one hand, one can choose whether to run them as 1-EPP (ECM) or 2-EPP (EDM). On the other hand, both the IBM recurrence protocol and the hashing protocol belong to the class of $[\![n,k,d]\!]$-EPP.

The quantum error correcting codes which belong to the hashing protocol are very interesting: the fact that the hashing protocol exists implies that there exist, in the asymptotic limit $n \to \infty$, quantum error correcting codes $[\![n,k,d]\!]'$ with a relation between the parameters n, k, and d which we derive below. Note that in this case, d is not the minimum distance of the code, but the minimum *likely* distance, which we denote by the prime in the notation of the code parameters. By definition, in such codes there may exist pairs of codewords with a distance of less then d. However, with increasing n, the number of such pairs of codewords has to grow slower than n, so that in the asymptotic limit, it is unlikely to meet such a pair. Note that the minimum likely distance is *not* defined for a given code with a finite n, but in the asymptotic limit $n \to \infty$.

Assume that the hashing protocol is applied to n EPR pairs, which are in a Werner state with fidelity F,

$$\rho = F \left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + (1-F)/3 \left(\left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + \left|\Phi^-\right\rangle\!\left\langle\Phi^-\right|\right).$$

For large n, the properties of this initial ensemble can be translated into the fact that, during the distribution of the pairs, on average $n_{\text{error}} = n(1-F)$ errors have been introduced. The hashing protocols allows us to obtain

$$k = n\left(F\log_2 F + (1-F)\log_2 \frac{1-F}{3}\right) \tag{5.2}$$

perfect EPR pairs from the initial ensemble. The error correcting code related to the hashing protocol is capable of correcting n_{error} errors, i. e. the minimum likely distance of this code is at least $d = 2n_{\text{error}} + 1 = 2n(1-F) + 1$. This allows us to express the initial fidelity in terms of the code parameters,

$$F = 1 - (d-1)/2n. \tag{5.3}$$

By inserting this expression into Eq. 5.2, we obtain the desired relation between the code parameters.

In the discussion above, we assumed that n is very large. For finite n, we have to take into account the fact that the parameters k and d are integer numbers, while the expressions for k and d which one obtains from Eq. 5.2 and Eq. 5.3 do not, in general, yield integer numbers.

Theorem 1 *Be ϵ_1, ϵ_2 (arbitrarily small) real numbers. Then there exists a lower bound $N \in \mathbb{N}$ such that the following statement holds:*

For all $n > N$ and $\tilde{k} < n$ there exists a quantum error correcting code $[\![n, \tilde{k}, \tilde{d}]\!]'$ with $(k - \tilde{k})/n < \epsilon_1$ and $(d - \tilde{d})/n < \epsilon_2$. k and d are such that Eq. 5.2 and Eq. 5.3 hold.

Proof: We consider an ensemble of n EPR pairs which consists of close to, but not less than, $1 - n_{\text{error}}$ Bell pairs in the Φ^+-state, while the other pairs are in one of the other three Bell states so that this ensemble belongs to the set of *typical* ensembles.

Asymptotic behavior of d: The fact that the hashing protocol in the case of *finite* n does not produce perfect EPR pairs has two possible reasons: (1) For finite n, there is a non-vanishing probability that the error rate n_{error}/n exceeds the expected error rate $(1-F)$ by an amount which the protocol cannot account for. For the proof, this possibility is excluded by assumption. (2) There may exist pairs of ensembles of EPR pairs, which cannot be distinguished from each other, even though they belong to the typical set of ensembles. For increasing n, however, the number of such pairs is bound to grow slower than n. If this was not the case, the hashing protocol would not produce perfect EPR pairs in the asymptotic limit. This means that the minimum likely distance of the corresponding quantum code asymptotically obeys Eq. 5.3.

Asymptotic behavior of k: This is exactly the asymptotic number of perfect EPR pairs which can be produced by the hashing protocol. Note that, for a given fidelity F, the Werner state has the maximum entropy, so that Eq. 5.2 is indeed a lower bound for k. □

In order to check how existing quantum error correcting codes compare to codes which are derived from the hashing protocol, we draw many known QECC $[\![n,k,d]\!]$ [38] into a fidelity/yield diagram for the hashing protocol [14]. In this plot, the "fidelity" of a $[\![n,k,d]\!]$ quantum code is given by Eq. 5.3, and the "yield" is defined as k/n. As we have seen above, these quantities represent the actual fidelity and yield only in the asymptotic limit $n \to \infty$, which explains why some of the QECC are located on the left-hand side of the hashing curve:

These quantum codes seem to lead to purification protocols which perform better than the hashing protocol, since they have a greater yield for a given initial fidelity F. However, it should be noted that this comparison is not fair: for a $[\![n,k,d]\!]$-EPP to yield k pairs, it must be guaranteed that not more than $(d-1)/2$ errors are introduced during the distribution of the n EPR pairs, while a noisy quantum channel which is capable of distributing pairs with fidelity F will introduce this amount of errors *on average*.

Nevertheless, it is interesting to see that quantum error correcting codes seem not to exceed the hashing border significantly.

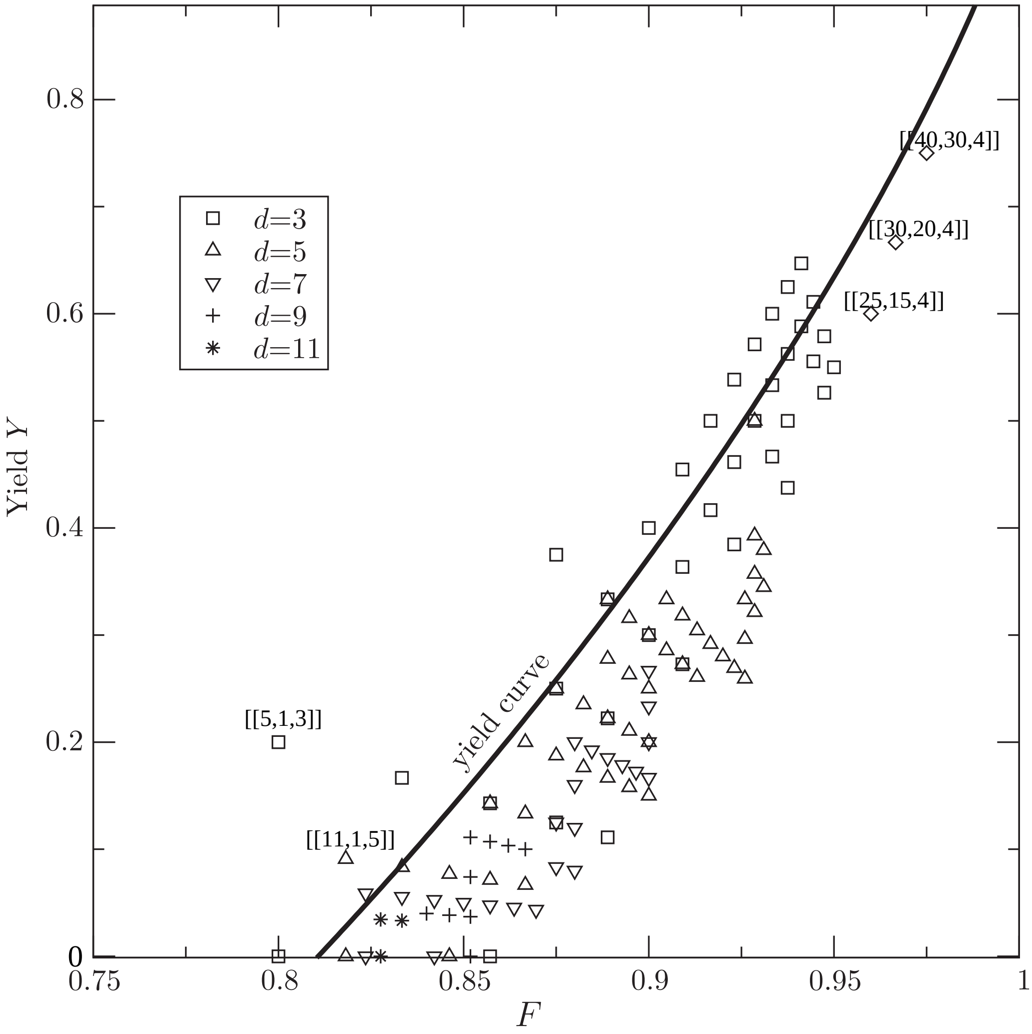


Figure 5.3: A “map” of quantum error correcting codes, drawn into the standard fidelity/yield diagram from [14]. For a code with parameters $[\![n,k,d]\!]$, the fidelity is defined by Eq. 5.3, and the yield is defined as k/n. For some selected codes, the parameters n, k, and d are depicted in the figure.

5.3 Numerical results

In this section, we will show the results of our numerical analysis of $[\![n,k,d]\!]$-entanglement purification protocols, which have been constructed as explained in Section 5.1.

We restricted our attention to codes with $k = 1$, i. e. codes which encode only one qubit. Such codes translate into n-to-1 purification protocols. The reason for this restriction is that we apply the purification protocol iteratively. However, the output states of one purification step are generally correlated, which makes the analysis of the purification process very difficult.

All numerical calculations have been performed using the QTENSORSPACE software library (see Chapter 6). The elementary unitary operations of the protocol map Bell diagonal states onto Bell diagonal states, and the measurements projectors ($|00\rangle\langle 00|+|11\rangle\langle 11| = |\Phi^+\rangle\langle\Phi^+|+|\Phi^-\rangle\langle\Phi^-|$ for measurement results which coincide, and $|01\rangle\langle 01| + |10\rangle\langle 10| = |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|$ for results which do not coincide) are diagonal in the Bell basis. Similar to the approach taken in the analysis of the cluster state purification protocol (Sec. 4.1.3), it is thus sufficient to perform all calculations on the vector of the diagonal elements of the density matrix. For a more detailed discussion of these techniques, see Section 6.3.

The calculation is further simplified by the fact that the elementary unitary operations involve only four qubits at a time, so that they can be expressed as 16×16-matrices. The TENSORSPACE software library has been written in order to handle such mathematical operations efficiently, where operations are performed only on a subsystem of a (large) composite system.

5.3.1 Purification curves

If an entanglement purification protocol is applied to an ensemble of EPR pairs with an initial fidelity F, we are left with a smaller ensemble with a different fidelity F'. Clearly, a single parameter, the fidelity, is not enough to describe the state of EPR pairs. For that reason, we use the convention that if we only write down the fidelity F of an EPR pair, we assume that this pair is in a Werner state with fidelity F. However, this rule can be broken by the entanglement purification protocol itself: if we start with pairs in a Werner state, it is not necessarily the case that the resulting pairs are again in a Werner state.

One way around this difficulty is to use a *twirling operation*, i. e. coordinated, but randomly chosen bilateral rotations, on the resulting EPR pairs, which converts them into EPR pairs in the Werner state, without changing the fidelity. This approach has been taken by Bennett *et al.* [14] ("IBM protocol"). The great advantage of this method is, that the entire purification process is described in terms of one parameter, which simplifies its analytical treatment. One great disadvantage is, however, that the twirling operation decreases the amount of entanglement. For this reason, the IBM protocol is not very efficient.

A different approach has been taken by the Deutsch *et al.* [25] ("Oxford protocol"), which allows the ensemble to leave the space of Werner states. Using this method, the protocol is highly efficient. However, the analytical treatment is quite difficult.

The $[\![5,1,3]\!]$ and $[\![11,1,5]\!]$ protocols in error detection mode In this paragraph, we examine two protocols, which do not require such techniques, since they map Werner states onto Werner states by themselves. The two protocols are the $[\![5,1,3]\!]$-EPP and the $[\![11,1,5]\!]$-EPP in error detecting mode. The fact that they map Werner states onto Werner states is a very surprising result, and we do not know *why* this is the case. In any case, this property is not generic for $[\![n,k,d]\!]$-EPP; there are $[\![n,k,d]\!]$-EPP which do *not* map Werner states onto Werner states.

Since for these protocols the entire purification process is described in terms of one parameter, the *purification curve*, which maps F to F', contains all information needed to analyze the purification process.[1] In Fig. 5.4, we have drawn the purification curves or the $[\![5,1,3]\!]$-EPP and the $[\![11,1,5]\!]$-EPP.

The purification regime for both protocols is $1/2 < F \leq 1$, since in this regime the purification curve lies above the line of fixpoints. It is interesting that, for $F \to 1$, both purification curves become very flat. This implies that one needs only few steps in the purification process in order to get almost perfect EPR pairs. In order to examine the high-fidelity regime of the protocols in more detail, the inset shows a log-log plot of $1-F'$ against $1-F$, which shows that $1-F' \propto (1-F)^d$ (for $F \to 1$), with $d=3$ and $d=5$ for the $[\![5,1,3]\!]$ and the $[\![11,1,5]\!]$ purification protocol, respectively.

It is no coincidence that the exponent d is equal to the minimum distance of the respective code: Assume that n EPR pairs with fidelity $F = 1-\epsilon$ have

---

[1] For comparison with the purification curve of the IBM protocol and for a discussion of the fixpoints and their relation to the purification regime, see Fig. 2.2 on page 22.

been distributed. The probability that they do not contain any error at all is given by $p_0 = F^n \sim 1 - n\epsilon$. If they contain $1, \ldots, d-1$ errors, this is guaranteed to be found by the error detection process. The probability to keep an EPR pair which ideally should have been discarded, is, to the leading order, given by the probability p_d that the ensemble contains d errors, which is proportional to $F^{n-d}(1-F)^d \sim (1-(n-d)\epsilon)\epsilon^d$. The new fidelity $F' = 1-\epsilon'$ is thus, in leading order, given by $\epsilon' = p_d/p_0$, which is (again in leading order) proportional to ϵ^d.

Note that the calculation above gives only a lower bound for the fidelity F', since we have assumed that all non-detectable error situations lead to EPR pairs which are not in the Φ^+-state, which is not necessarily the case.

The fact that there are only few purification steps required in order to reach almost perfect EPR pairs does not necessarily imply that these protocols are very efficient. On the one hand, the protocols are intrinsically wasteful, since in each purification step only one out of n pairs is kept. On the other hand, we have to keep in mind that the purification protocols are probabilistic protocols, in which the remaining pair is kept only with a certain probability p_{succ}, which is indicated by the dashed lines in Fig. 5.4. For a detailed discussion of the efficiency of these protocols, see Section 5.3.2.

The $[\![n,k,d]\!]$ protocols in error detection and correction mode In Fig. 5.5 and Fig. 5.6, we concentrate on the $[\![5,1,3]\!]$ and $[\![11,1,5]\!]$ purification protocol, respectively. We compare the error detection mode (EDM) and the error correction mode (ECM), both with perfect and with noisy local unitary operations.

By comparing both modes of operation of this protocol, we will find out whether the availability of two-way classical communication is advantageous for entanglement purification. Moreover, if the ECM protocol is used in a recursive purification process, this is closely related to concatenated coding, which is an essential ingredient to fault tolerant quantum computation [63, 48].

For the case of noisy operations, we consider two-qubit white noise channels with reliabilities $p_2 = 0.95, 0.99, 0.995$ (for the $[\![5,1,3]\!]$ EPP) and $p_2 = 0.9185, 0.9975, 0.998$ (for the $[\![11,1,5]\!]$ EPP), which accompanies each two-qubit operation (see Eq. 2.11 in Section 2.3.1). In order to simplify the calculations, we applied the noise channel only on Alice's side. For Bell diagonal states, however, applying a depolarizing channel with reliability p_2

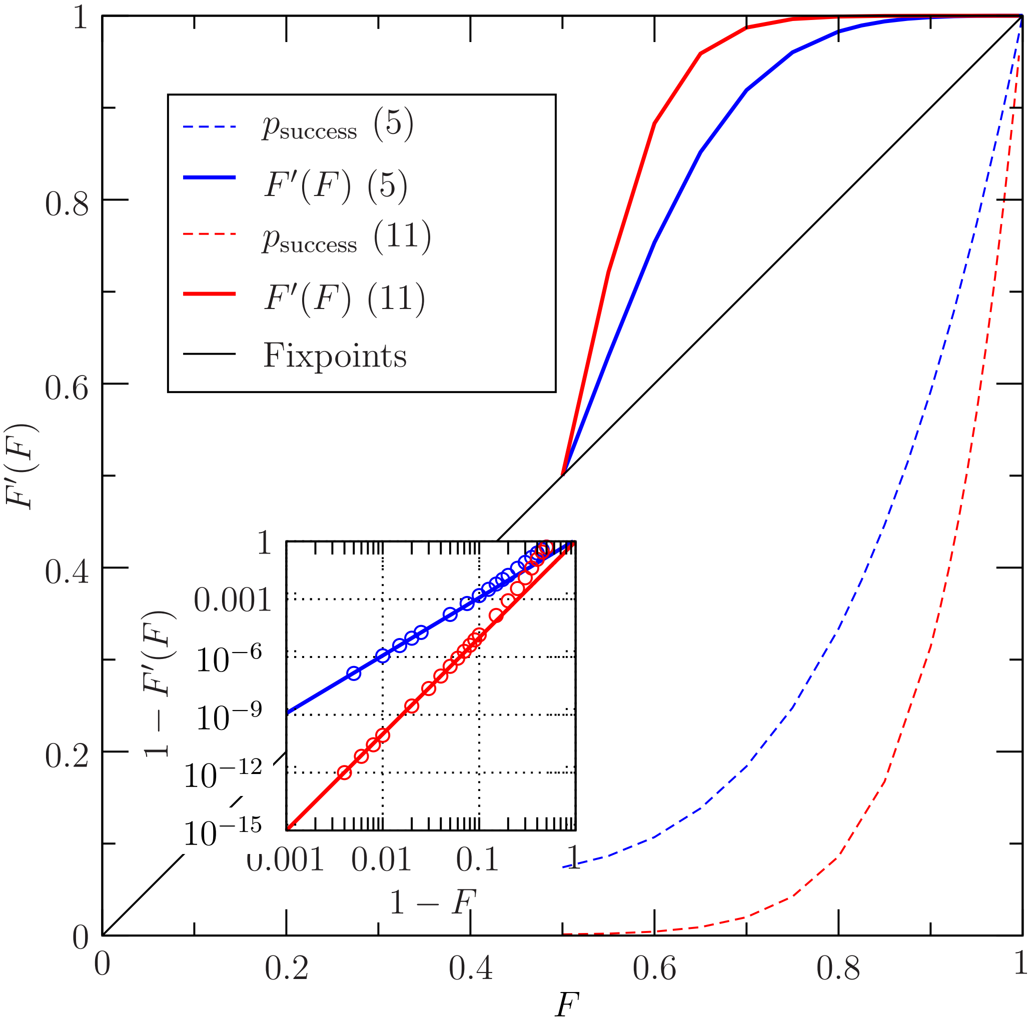


Figure 5.4: Purification curves of protocols derived from a $[\![5, 1, 3]\!]$ code (blue curve) and a $[\![11, 1, 5]\!]$ code (red curve), in error detecting mode (without error correction). These two protocols have the non-trivial property that they map Werner states onto Werner states, so that the purification process is completely described by only one parameter F. The dashed lines show the probability of success p_{succ}, i. e. the probability that the remaining pair is kept. The inset shows a log-log plot of $1 - F'$ against $1 - F$. The circles are the calculated data points, and the straight lines are polynomial fits to this data.

on Alice's side has the same effect as applying a depolarizing channel with reliability $\sqrt{p_2}$ on both sides.

The first thing to note is that the purification regime, i. e. the values of F where the purification curve lies above the $F = F'$ line, is much smaller for protocols in ECM than in EDM, even if no noise is present; in this case, the purification regime is $0.86245 < F \leq 1$ and $0.8635 < F \leq 1$, for the $[\![5,1,3]\!]$ and $[\![11,1,5]\!]$ protocols, respectively. Note that for these protocols, the purification is thus smaller than it is for the hashing protocol $(0.8107103751 < F \leq 1)$.

Second, we see that the ECM-protocols are far less tolerant against noise than the EDM-protocols: The two-qubit reliability threshold values $p_{2,\text{threshold}}$ for the former are 0.995 ($[\![5,1,3]\!]$) and 0.9975, ($[\![11,1,5]\!]$), while for the latter they are 0.89806 and 0.9185, respectively. As it seems, the tolerable noise value $1 - p_{2,\text{threshold}}$ for two-way entanglement purification protocols is almost independent of n (and thus the gate complexity), while one-way entanglement purification protocols tolerate less noise for larger n.

Since for a given quantum error correcting code $[\![n,k,d]\!]$, the corresponding $[\![n,k,d]\!]$ entanglement purification protocols in EDM and ECM use the same quantum gates, and differ only in whether they use two-way classical communication or not, we get the following result:

The high level of fault tolerance of protocols in quantum communication, compared to fault tolerant quantum computation, is *only* due to the availability of two-way classical communication.

5.3.2 Efficiency of the protocols

The efficiency of entanglement purification protocols is usually defined in terms of the *yield* Y of the protocol [14]. The yield is given by the fraction $Y = k/n$, where k is the number of *perfect* EPR pairs which an purification protocol creates out of n imperfect initial EPR pairs. In general, for a given purification protocol, the yield is a function of the input state, or — if we restrict our attention to Werner states — of the input fidelity.

While the yield of purification protocols is an interesting concept for many applications, it has an important drawback: all purification protocols which work on a finite ensemble of EPR pairs have a vanishing yield. In other words, the definition of the yield is only applicable in the asymptotic limit.

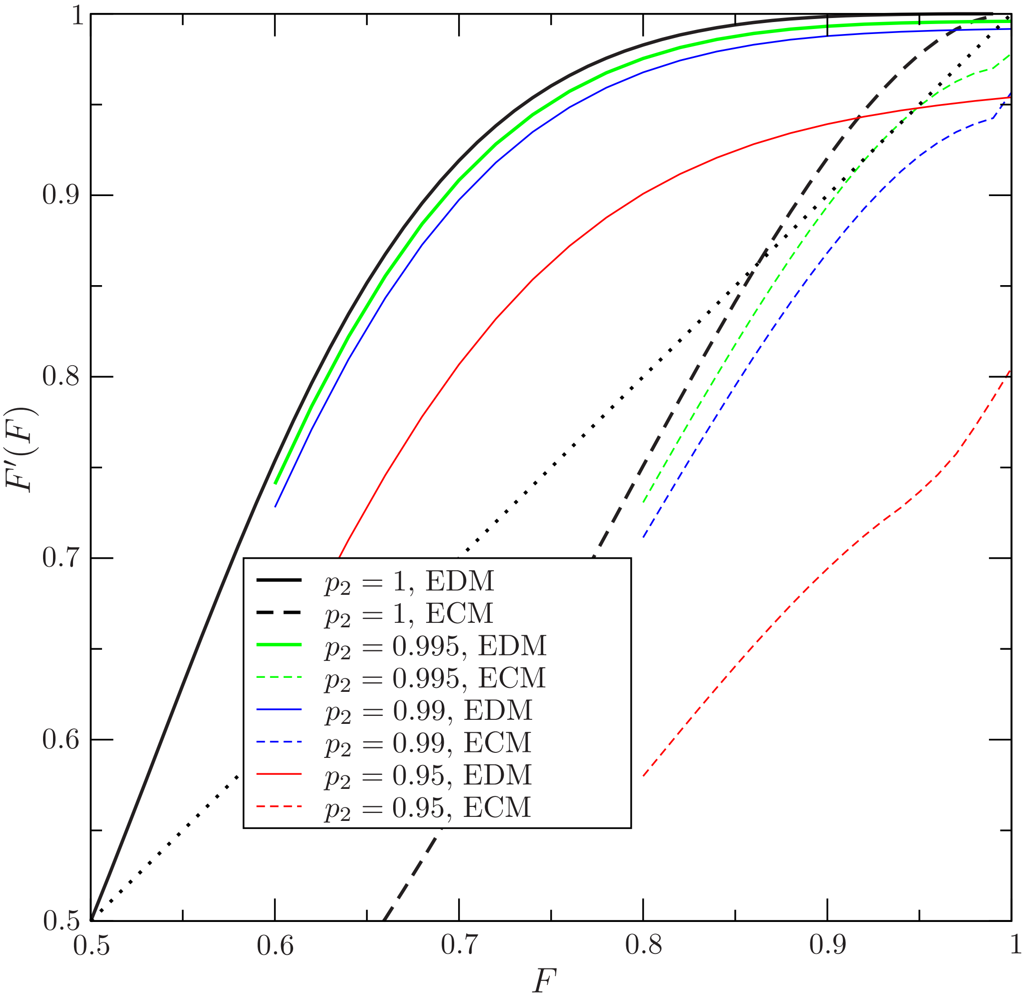


Figure 5.5: Purification curves for protocols derived from a $[\![5, 1, 3]\!]$ code. The protocols are run on noiseless apparatus (black curves) and on noisy apparatus with a two-qubit reliability of p_2 per two-qubit quantum operation. The solid lines show the purification curves for the protocols in error detecting mode, and the dashed lines show the purification curves for protocols in error correction mode. The dotted line is the line of fixpoints.

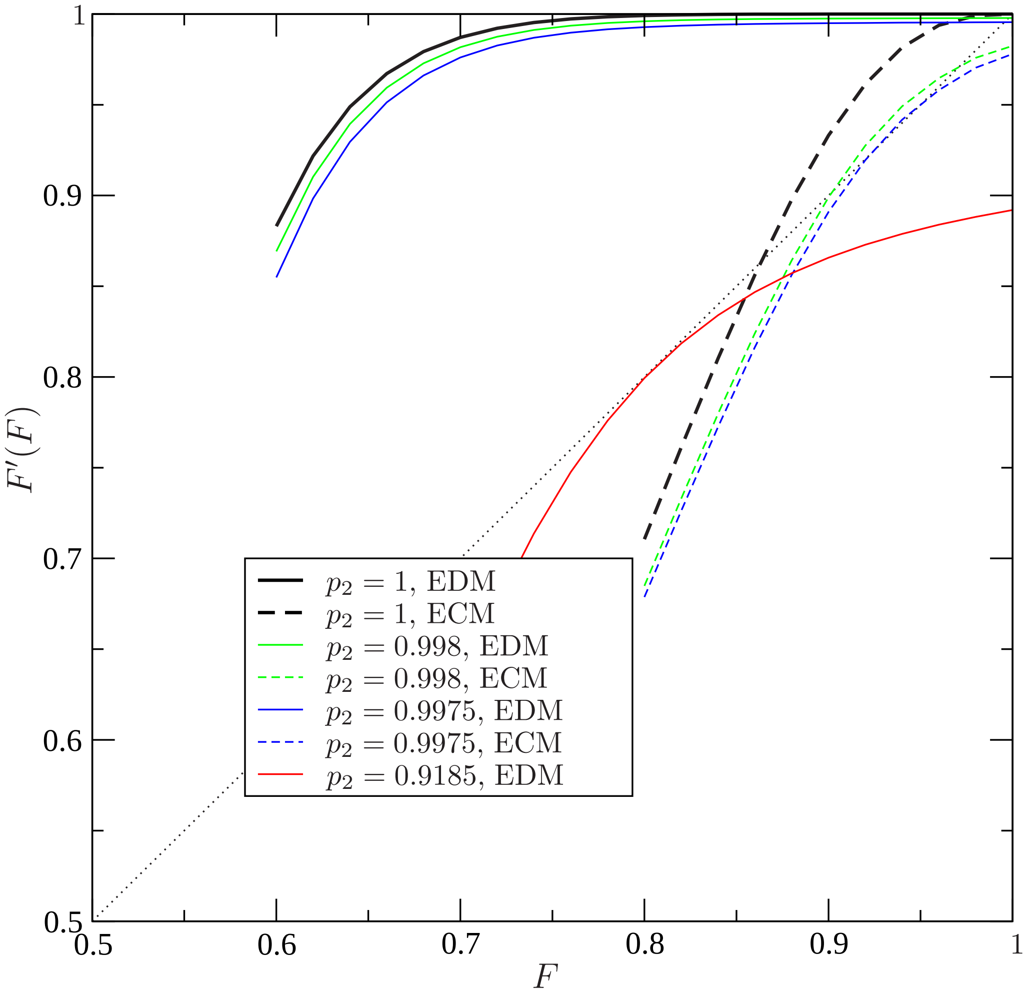


Figure 5.6: Purification curves for protocols derived from a $[\![11, 1, 5]\!]$ code. See Fig. 5.5 for details.

However, even in the asymptotic limit, the yield for recurrence protocols vanishes.

If we consider a "realistic" situation, where the apparatus which performs the purification protocol is a source of noise itself, the definition of the yield has to be modified: there is no EPP known which has a finite yield if it is run on noisy apparatus.

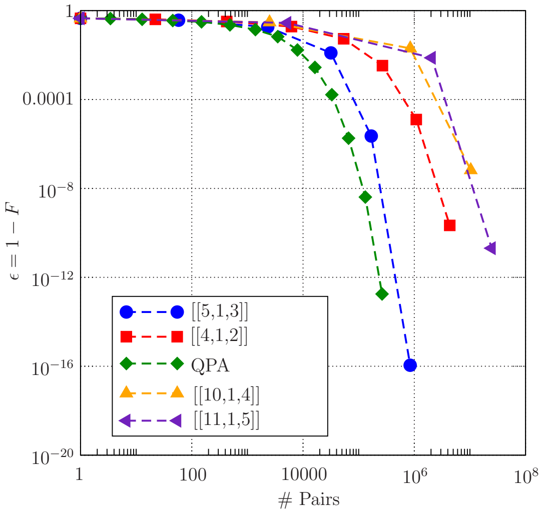
In order to overcome these problems, it is possible to define an "epsilon-Yield" $Y_\epsilon = k'/n$, where k' is the number of EPR pairs of fidelity $F_{\text{final}} = 1-\epsilon$, which a given purification protocol creates out of n imperfect initial EPR pairs. However, one can easily see that this definition has its limitations: since the resulting EPR pairs are still imperfect, one cannot *a priori* exclude the possibility that there exist correlations between the remaining pairs. As it turns out, for all n-to-k purification protocols with $k > 1$ which we have checked, the final states are correlated. In this case, the individual fidelities of the remaining pairs does not suffice for an accurate description of the total quantum states. Whether or not the remaining correlations are a problem for a given quantum communication protocol is not *a priori* clear.

In order to avoid such difficulties, we choose a different figure of merit for the definition of the efficiency of entanglement purification protocols: In Fig. 5.7 we plot the number N of initial pairs which are required to create one pair of fidelity F against $\epsilon = 1 - F$.

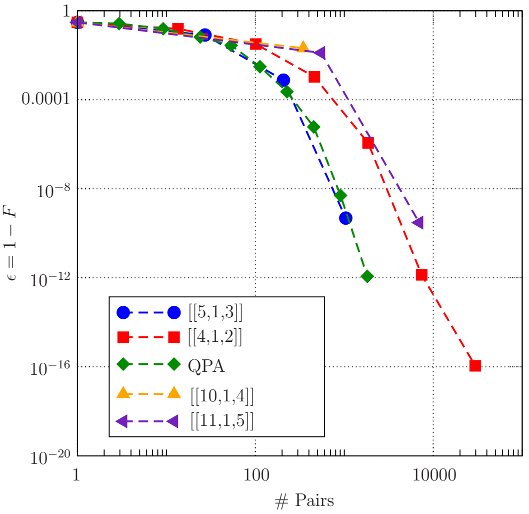
The points in the plots have been calculated as follows: for each $[\![n, 1, d]\!]$ protocol under consideration, we start with an ensemble of N pairs with the initial fidelity $F_{\text{init}} = F^{(0)}$. The number of pairs required to produce one pair after the first purification step is given by $n/p_{\text{succ}}(F^{(0)})$, where $p_{\text{succ}}(F^{(0)})$ is the probability of success of the purification protocol. For the next purification step, n pairs in the state of the remaining pair are required as input pairs, and so on. The total number of input pairs which is required *on average* to create one output pair after step i is the product of the numbers of pairs required to produce one output pair in each individual step in the purification process, i. e.

$$\#\text{pairs} = \frac{n^i}{\prod_{\nu=0}^{i} p_{\text{succ}}(F^{(i)})} \tag{5.4}$$

In the plots, efficient protocols are close to the lower left corner, since for these protocols, fewer pairs are needed to create one final pair with a given fidelity.

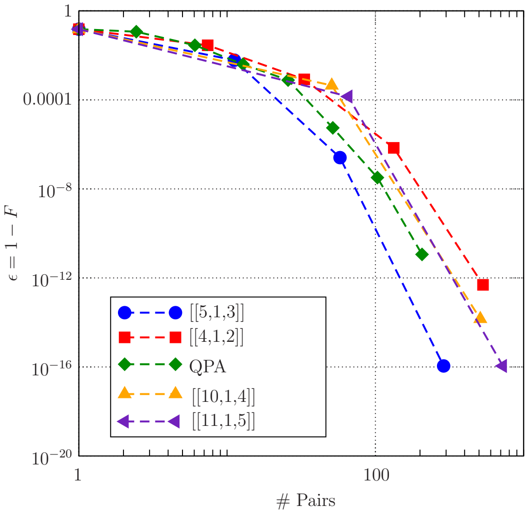


(a) $F_{\text{init}} = 0.55$

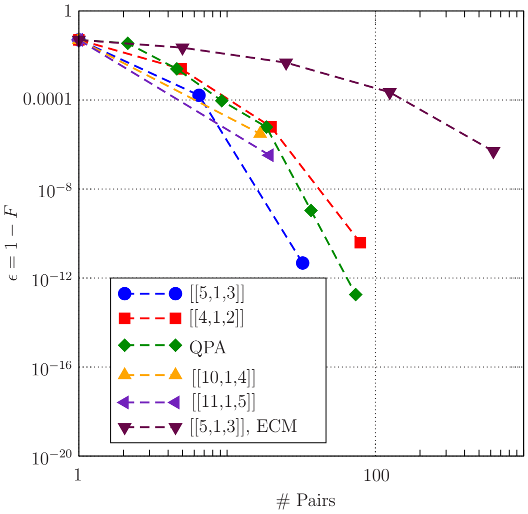


(b) $F_{\text{init}} = 0.70$

Figure 5.7: The number of pairs, with initial fidelity F_{init}, needed to create one pair with fidelity F. In each figure, the different lines correspond to different purification protocols. ⟶



(c) $F_{\text{init}} = 0.85$



(d) $F_{\text{init}} = 0.95$

Figure 5.7 (continued): Protocols labeled with code label $[\![n, m, d]\!]$ are related to a protocol, created from the corresponding code. For reference, we have included the quantum privacy amplification (QPA) protocol [25].

As a surprising result, we find that the simple quantum privacy amplification protocol (QPA) [25] performs very well; at least, for low fidelity initial pairs, this protocol performs better than any of the other protocols. For high fidelity initial states, however, at least the $[\![5,1,3]\!]$ EDM protocol performs better than QPA. In Fig. 5.7(d), we also plot the figure of merit for the $[\![5,1,3]\!]$ ECM protocol. As one can see, this 1-EPP performs much worse than the 2-EPP. Note that in Fig. 5.7(a-c), the initial fidelity is below the purification threshold of the $[\![5,1,3]\!]$ ECM protocol.

Please note that data points with a value of $\epsilon < 10^{-15}$ may be inaccurate, due to numerical cutoff errors.

Chapter 6

The tensorspace software library

6.1 Introduction

In quantum information theory, we often think of quantum systems which consist of several subsystems. These subsystems may be spacially seperated, and for that reason it is quite natural to consider operations which act on these quantum systems seperately (local operations). In mathematical terms, the state $|\psi\rangle_{p_1 p_2 \ldots p_n}$ of the total system is an element of the tensor product of the Hilbert spaces of the subsystems, $\mathcal{H}_{\text{total}} = \mathcal{H}_{p_1} \otimes \mathcal{H}_{p_2} \otimes \cdots \otimes \mathcal{H}_{p_n}$, and a local operation $\mathcal{O}_{\text{local}} = \mathcal{O}_{p_1} \otimes \mathcal{O}_{p_2} \otimes \cdots \otimes \mathcal{O}_{p_n}$ is a tensor product of operations which act on only one of the subsystems.[1]

If a local operation acts on only one subsystem, say p_1, the resulting state is given by

$$
\begin{aligned}
|\psi'\rangle_{p_1 p_2 \ldots p_n} &= \mathcal{O}_{p_1} \otimes \mathbb{I}_{p_2} \otimes \cdots \otimes \mathbb{I}_{p_n} |\psi\rangle_{p_1 p_2 \ldots p_n} && (6.1)\\
&\equiv \mathcal{O}_{p_1} |\psi\rangle_{p_1 p_2 \ldots p_n} . && (6.2)
\end{aligned}
$$

In the latter expression (6.2), the identity operators where left out. Since we know on which subsystem the operation $\mathcal{O}_{p_1}$ acts, this notation is not ambiguous and very easy to read.

On the other hand, if one does numerical calculations in quantum information theory, it is necessary to keep track of all the subsystems, which

---

[1] Local *super*operators, which act on density operators, are in general convex combinations of tensor products.

is usually tedious and error-prone. For example, it is usually necessary to explicitly write down all the identity matrices, as in Eq. (6.1); another complication is that the parties have an implicit order, which has to be the same for all object in a calculation. If the order is not the same, parties have to be exchanged, which may become a non-trivial task if the number of parties is not small.

QTENSORSPACE is a software library which has been written to facilitate these book-keeping tasks in numerical calculations. The design goals were:

- Ease of use. It should be possible to do simple numerical experiments without writing full-blown programs.
- Efficiency with respect to speed and memory usage. Since the complexity of the problems grows exponentially with the number of parties, this is an obvious requirement.
- Readability of code. The code which is needed for a calculation should resemble the mathemtical notation as far as possible.

All objects which live in or act on Hilbert spaces are internally represented by the same type of object (*"qtensors"*). Qtensors are similar to complex matrices in that they have rows and colums. Different from matrices, rows and columns are made up by several indices. In order to use QTENSORSPACE, it is not necessary to know the mathematical details of the implementation. However, for the sake of completenes, we describe the mathemtics of qtensors in Section 6.5.

6.2 Basic concepts

The QTENSORSPACE software library allows the programmer to define states (bras, kets, density operators) and operations, which act on these states (e. g., unitary operations, projections), as well as Hilbert spaces, in which these objects live.

6.2.1 Parties

Hilbert spaces may be product spaces, which consist of several subsystems. In QTENSORSPACE, the "atomic" subsystems are called *parties*. A party is defined, e. g., using the command

```
a = Party("Alice", 3)
```

In this example, *a* is the name under which the newly defined party will be known in the program. `Alice` is an identifier, which can be any string the programmer likes. Finally, 3 is the dimension of the Alice-Hilbert space.

Please note that the software library ignores the identifier completely, so that the command `a1 = Party("Alice", 3)` will define a different party.

In many cases, we are interested in qubits. For this reason, there exists a shortcut for creating two-dimensional parties:

```
b = Qubit("Bob")
```

which is equivalent to `b = Party("Bob",2)`, with the exception that in the *Qubit()*-command, the identifier is optional, and defaults to an empty string.

6.2.2 States

In the QTENSORSPACE library, there exist four commands in order to create states: *Ket()*, *Bra()*, *density_operator*, and *diagonal_vector*. The first three create kets, bras, and density operators, respectively, while the fourth creates a diagonal density operator (see Section 6.3).

A ket $|\psi\rangle$ is most easily defined in its representation in the computational basis, e. g. $|\psi\rangle = |001\rangle_{abc} = |0_a 0_b 1_c\rangle$. In the QTENSORSPACE library, the same state would be defined using the command

```
psi = Ket([a,b,c ],[0,0,1])
```

The *Ket()* command expects, as it first parameter, a comma-separated list of parties, which is enclosed in square brackets. The second argument is a list of numbers, which indicates in which basis states the parties are. If this argument is left out, it is assumed to be the list [0,. . . ,0].

Kets may be added, multiplied with (complex) scalars or multiplied with other kets, if their sets of parties are disjoint. For example, the following statements are perfectly legal:

```
phi_plus = Ket([a,b ],[0,0]) +  Ket([b,a ],[1,1])
psi= phi_plus * Ket([c],[1]) + (1−1j) * Ket([a,b,c ],[0,0,0])
```

In order to normalize this state, the commands `normalize(psi)` can be used. Note that there exists the equivalent command `psi.normalize()`.

The commands *Bra()* and *diagonal_vector()* have the same syntax as the *Ket()* command; the only difference is that they create bras and diagonal density operators, respectively. All operations, which are possible with kets, are also possible with bras and diagonal vectors.

Density operators may be created with the *density_operator()* command, which takes a list of parties as its only required argument. The result of this command is a density operator, which corresponds to a completely depolarized state. To create density operators which describe different states, it is possible to use the *P()* command, which takes a ket as its only argument, and creates a projector onto this state. Like other states, density operators can be added, multiplied (with scalars and with other density operators), and normalized (using the *normalize()* command).

6.2.3 Operations

In QTENSORSPACE general operators are linear maps which map a "source" Hilbert $\mathcal{H}_s$ space onto a "destination" Hilbert space $\mathcal{H}_d$. There exist no restrictions on the sets of parties, which make up both Hilbert spaces; we call the source parties *row parties*, and the destination parties *column parties*, since they correspond to row- and column-indices in the matrix representation of the operator.

General operators may be created using the *operator()* command. It takes two arguments, a list of row parties and a list of column parties. The entries of the corresponding matrix may be set using the *values=* keyword argument (see below). However, this is not the recommended way of creating operators, since it requires a detailed knowledge of the internals of the QTENSORSPACE library.

Alternative methods to create operators are (a) to use predefined operations, like the CNOT operation or Pauli spin operators, as building blocks for bigger operators, or (b) to create them as sums of products of kets and bras.

Rank-1 Projectors are easily defined using the *P()* command, which yields a projector onto the ket which is passed as an argument. Higher-rank projectors can be defined as sums of rank-1 projectors onto mutually orthogonal states.

6.3 Diagonal density operators

In many cases, quantum systems which one wants to examine numerically are not in a pure state, which is described by a state vector $|\psi\rangle$, but in a mixed state, which is given in terms of a density operator ρ. If the Hilbert space of the quantum system has d dimensions, one needs to remember d complex numbers for the state vector, but d^2 complex numbers for the density operator.[2]

Since a density operator is hermitean, there always exists a basis in which it is diagonal. However, many quantum protocols have the additional property that they map density operators which are diagonal in a given basis onto density operators which are diagonal in the same basis. If this is true for each single step of the protocol, we are in the lucky situation that the quantum state can be completely described in terms of the vector $\vec{d}$ of diagonal elements of the density operator.

As a consequence of this simplification, it is possible to *double* the number of quantum systems which we can treat numerically; indeed, in this case, calculations with density operators are no more expansive than calculations with state vectors.

In the QTENSORSPACE software library, vectors of diagonal elements of density operators are created using the *diagonal_vector()* function, which has the same syntax as the *Ket()* and the *Bra()* function.

Unitary operations Unitary operations act on density operators as superoperators. In other words, they are linear maps on the state space. A a unitary operator U, which maps diagonal density operators onto diagonal density operators, maps thus the vector of diagonal elements $\vec{d}$ linearly onto a vector $\vec{d'}$ of diagonal elements, i. e. $\vec{d'} = \tilde{U}\vec{d}$, for a (real) matrix $\tilde{U}$. A trivial calculation yields that $\tilde{U}$ is a matrix which contains element-wise the squared modulus of the entries of the unitary matrix U, i. e.

$$(\tilde{U})_{ij} = (U)_{ij}(U)^*_{ij} \tag{6.3}$$

```
from tensorspace import *
a = Qubit('a')
b = Qubit('b')
```

---

[2] Since the density operator is hermitean, d^2 *real* numbers suffice.

```
rho = diagonal_vector([a,b ],[0,0]) +  diagonal_vector([a,b ],[1,1])
rho.normalize()
print "state␣before␣CNOT", basis_repr(rho)
U_tilde = abs_squared (CNOT(a,b))
rho_1 = U_tilde*rho
print "state␣after␣CNOT", basis_repr(rho_1)
print "tr_b(rho_1)␣=", basis_repr(trace(rho_1,[b]))
```

Program output:

```
state before CNOT 0.500 |0,0><0,0|  +0.500 |1,1><1,1|
state after CNOT 0.500 |0,0><0,0|  +0.500 |1,0><1,0|
tr_b(rho_1) = 0.500 |0><0|  +0.500 |1><1|
```

6.4 qtensorspace by examples

In this section, we give a short introduction to the software library by examples. These examples should whet the reader's appetite, but are not considered a full reference manual to the software library. It should be noted that these examples are written in the *Python* [80] programming language; we do not give a detailed intorduction into this language; however, we think that the examples are self-explanatory and should be readable even without any knowledge of Python (with the exception of example 4, which uses some more sophisticated programming structures, like function definitions and loops).

6.4.1 CNOT operation

In the first example, we define a two-party state, apply unitary operations to it and print it in the computational basis:

```
from tensorspace import *
a = Party("Alice", 2)
b = Party("Bob", 2)
psi = Ket([a,b ],[1,0])
print basis_repr (psi)
print basis_repr ( CNOT(a,b) * psi )
print basis_repr ( CNOT(a,b) * H(a) * psi )
```

Program output:

```
1.000 |1,0>
1.000 |1,1>
0.707 |0,0>  -0.707 |1,1>
```

In line 1, the tensorspace package is loaded. Lines 2 and 3 define two parties, *Alice* and *Bob*, each of which is a two dimensional quantum system (i. e. a qubit).[3] line 4, a quantum state (ket) is defined ($|\psi\rangle = |1_{\text{Alice}}0_{\text{Bob}}\rangle$), which is printed in the computational basis (line 5). Line 6 shows how the controlled-NOT (CNOT) operation with the source bit a and the target bit b acts on $|\psi\rangle$, and line 7 shows that the CNOT operation creates a Bell state $|\Phi^-\rangle = 1/\sqrt{2}(|0,0\rangle - |1,1\rangle)$, if a Hadamard operation is applied to the qubit a first.

6.4.2 Teleportation

In the second example, we show some basic operations which can be applied to states and operators.

```
from tensorspace import *
a1 = Qubit("Alice␣1")
b =  Qubit("Bob")
a2 = Qubit("Alice␣2")
phi_plus_A1B = Ket([a1,b],[0,0]) + Ket([a1,b ],[1,1])
phi_plus_A1B.normalize()
phi_plus_A1A2 = normalize(Bra([a1,a2],[0,0]) + Bra([a1,a2 ],[1,1]))
alpha = 1.2+2j; beta = -2j
psi = normalize(alpha * Ket([a2],[0]) +  beta * Ket([a2 ],[1]))
psi_B = phi_plus_A1A2 * psi * phi_plus_A1B
p = psi_B.dagger() * psi_B
print basis_repr( psi  ), psi . get_parties ()
print basis_repr(normalize(psi_B)), psi_B. get_parties ()
print "Probability␣of␣successful␣teleportation:␣p␣=␣",p
```

Program output:

---

[3] a and b are the *names* of the parties which are known to the program. While parties (like all python objects) may have several names, the description string `"Alice"` or `"Bob"` is always the same for a given party object.

```
(0.391+0.651j) |0>  -0.651j |1> ([], [Party ('Alice 2', 2)])
(0.391+0.651j) |0>  -0.651j |1> ([], [Party ('Bob', 2)])
Probability of successful teleportation: p =  (0.25+0j)
```

Let us again walk through the program line by line. In line 2-4, the quantum systems are defined. Note the shorthand notation `Qubit("xyz")` instead of `Party("xyz", 2)`. Line 5 defines the non-normalized Bell state $|\Phi^+\rangle_{A_1B} = |0,0\rangle + |1,1\rangle$, which is normalized in line 6, by invoking the `normalize()`-method of the ket. In line 7, we define the Bell-state ${}_{A_1A_2}\langle\Phi^+|$, as a bra, since we want to project onto this state. Here, we used a different (but equivalent) method to normalize the state. Line 8 defines two arbitrary (complex) numbers α and β (`j` is the imaginary unit), which define the state $|\psi\rangle_{A_2} = 1/\text{norm}(\alpha\,|0\rangle_{A_2} + \beta\,|1\rangle_{A_2})$ (line 9). Line 10 is the teleportation: we calculate the state

$$|\psi\rangle_B = {}_{A_1A_2}\langle\Phi^+|\psi\rangle_{A_2}\,\left|\Phi^+\right\rangle_{A_1B}.$$

The norm $p = {}_B\langle\psi|\,\psi\rangle_B$ of this state is the probability of successful teleportation (line 11 and 14). In line 12 and 13 we print the states $|\psi\rangle_{A_2}$ and $|\psi\rangle_B$, and we find that the teleportation was successful. By using the `get_parties()`-method, we convince ourselves that the two states live on different quantum systems.

6.4.3 Teleportation using noisy EPR pairs

Up to now, all calculations were done using pure states. In the next example, we calculate the fidelity of the teleported state if the teleportation was done using a noisy EPR pair. Since in this case the EPR pair is in a mixed state, which is described by a density operator, we have to do the calculatios in the density operator language.

```
from tensorspace import *
a1 = Qubit("Alice␣1")
b =  Qubit("Bob")
a2 = Qubit("Alice␣2")
phi_plus_A1B = Ket([a1,b],[0,0]) + Ket([a1,b ],[1,1])
phi_plus_A1B.normalize()
phi_minus_A1B = sigma_z(a1) * phi_plus_A1B
```

```
 8 psi_plus_A1B  = sigma_x(a1) * phi_plus_A1B
 9 psi_minus_A1B = sigma_z(a1) * psi_plus_A1B
10 f = 0.85
11 rho_A1B = f * P(phi_plus_A1B) + (1-f)/3*(P(phi_minus_A1B) +
12                                          P(psi_plus_A1B) +
13                                          P(psi_minus_A1B) )
14 phi_plus_A1A2 = normalize(Bra([a1,a2],[0,0]) + Bra([a1,a2 ],[1,1]))
15 alpha = 1.2+2j; beta = -2j
16 psi_A2 = normalize(alpha * Ket([a2],[0]) + beta * Ket([a2 ],[1]))
17 psi_B  = normalize(alpha * Ket([b],[0]) + beta * Ket([b ],[1]))
18 rho_B = phi_plus_A1A2 * P(psi_A2) * rho_A1B * phi_plus_A1A2.dagger()
19 p = trace(rho_B)
20 rho_B.normalize()
21 fid = format_complex(psi_B.dagger() * rho_B * psi_B)
22 print "Teleportation␣fidelity␣fid␣=␣", fid
23 print "Probability␣of␣successful␣teleportation:␣p␣=␣",p
```

Program output:

```
Teleportation fidelity fid =  0.900
Probability of successful teleportation: p =  (0.25+0j)
```

In lines 5-8, we define the four Bell states, using the Pauli-matrices. The state of the noisy EPR pair is defined in lines 11-13. Here, the function `P(psi)` returns a projector onto the state `psi` (it is just a shorthand notation for `psi*psi.dagger()`, where the method `dagger()` returns, of course, the hermitian transpose). In line 17, we define the reference state of the teleported qubit, which we need to calculate the teleportation fidelity. The result of the teleportation is calculated in line 18,

$$\rho_B = {}_{A_1A_2}\left\langle\Phi^+\right|\rho_{A_2}\otimes\rho_{A_1B}\left|\Phi^+\right\rangle_{A_1A_2}.$$

The trace of ρ_B is the probability of success (line 19), and the teleportation fidelity is calculated in ine 21. Here, we use the `format_complex()` function, in order to get rid of some numerical noise.

6.4.4 Cluster states

In the next example, we will see how we can check for eigenvector properties of states. As an non-trivial example, we choose four qubit cluster states and their correlation operators, and we show that two such cluster states are mapped onto a product of cluster states by a certain pattern of CNOT operations.

```
from tensorspace import *
def cluster_4(a,b,c,d):
    psi_4 = (Ket([a ],[0]) *  sigma_z(b) + Ket([a ],[1]) *  sigma_0(b)) * \
            (Ket([b ],[0]) *  sigma_z(c) + Ket([b ],[1]) *  sigma_0(c)) * \
            (Ket([c ],[0]) *  sigma_z(d) + Ket([c ],[1]) *  sigma_0(d)) * \
            (Ket([d ],[0])               + Ket([d ],[1]))
    return normalize(psi_4)
def correlations(psi, a,b,c,d):
    print "Eigenvalues␣of␣the␣correlation␣operators:"
    print psi.is_eigenvector(           sigma_x(a)*sigma_z(b)),
    print psi.is_eigenvector(sigma_z(a)*sigma_x(b)*sigma_z(c)),
    print psi.is_eigenvector(sigma_z(b)*sigma_x(c)*sigma_z(d)),
    print psi.is_eigenvector(sigma_z(c)*sigma_x(d))
a1 = Qubit("a1");b1 = Qubit("b1");c1 = Qubit("c1");d1 = Qubit("d1")
a2 = Qubit("a2");b2 = Qubit("b2");c2 = Qubit("c2");d2 = Qubit("d2")
psi_1 = cluster_4(a1,b1,c1,d1)
psi_2 = cluster_4(a2,b2,c2,d2)
correlations(psi_1, a1,b1,c1,d1)
CNOTs = CNOT(a1,a2)*CNOT(b2,b1)*CNOT(c1,c2)*CNOT(d2,d1)
psi_12 = CNOTs * psi_1 * psi_2
correlations(psi_12, a1,b1,c1,d1)
correlations(psi_12, a2,b2,c2,d2)
rho_1 = trace( P(psi_12), [ a2,b2,c2,d2] )  #ρ_1 = tr_{a_2b_2c_2d_2} {|ψ⟩_12⟨ψ|}
for evalue, evector in rho_1.eigenvectors():
    if abs(evalue − 1) < 1e−15:
        correlations(evector, a1,b1,c1,d1)
```

Program output:

```
Eigenvalues of the correlation operators:
(1+0j) (-1+0j) (-1+0j) (-1+0j)
Eigenvalues of the correlation operators:
(1+0j) (-1+0j) (1+0j) (-1+0j)
Eigenvalues of the correlation operators:
(1+0j) (1+0j) (-1+0j) (1+0j)
```

```
Eigenvalues of the correlation operators:
(1-0j) (-1-0j) (1-0j) (-1-0j)
```

Beginning in line 2, we define a function *cluster_4*, which returns a cluster state $|\psi\rangle_{abcd} = (|0\rangle_a \sigma_z^b + |1\rangle_a \sigma_0^b)(|0\rangle_b \sigma_z^c + |1\rangle_b \sigma_0^c)(|0\rangle_c \sigma_z^d + |1\rangle_c \sigma_0^d)(|0\rangle_d + |1\rangle_d$ on four given qubits a, b, c, and d. Note thate while an expression like $|0\rangle_a \sigma_z^b$ only has a physical meaning if we multiply out the whole expression, we are nevertheless able to write it in exactly the same way in the program.

The function *correlations*, defined in lines 8 - 13, prints out the eigenvalues of the four correlations operators for a given cluster state. To do this, we use the *is_eigenvector()* method, which returns the eigenvalue if *psi* is a eigenvector of the operator which is passed a an argument of this method. If it was not an eigenvector, the method would return *None*.

In lines 16 - 18, we create two cluster states on the qubits a_1, b_1, c_1, d_1 and a_2, b_2, c_2, d_2, respectively, and calculate the eigenvalues of the correlation operators for one of them. The *CNOTS* operation, a product of *CNOT* operations in alternating directions (see Fig. 4.1 in Section 4.1.2), is defined in line 19 and applied to the 8 qubit state $|\psi_{12}\rangle$ in line 20. As we see in lines 21 and 22, the resulting state is still an eigenstate of the eight correlation operators, but with different eigenvalues. In other words, it is still a product of cluster states. To check this independently, we trace out the four qubits of the second cluster state (line 23) and look at the eigenvalues of the resulting denisty operator, using the *eigenvectors()*-method. This method returns a list of (eigenvalue,eigenvector)-pairs. Since we are only intersted in eigenvectors which belong to the eigenvalue 1, we use a **for**-loop in order to check all eigenvalues if they are equal to 1 (up to numerical noise). If this is the case, we again print the values of the correlation operators for this state (line 24-25).

6.5 Mathematics of qtensors

A qtensor is an object similar to a complex matrix; one can think of it as a rectangular scheme of complex numbers. Different from a matrix, individual rows and colmuns are not addressed by single indices, but by several indices, each of which belongs to a given quantum-subsystem or party of dimension d_i, and takes values from 0 to $d_i - 1$.

We denote row indices by lower indices, and column indices by upper indices,

$$\mathcal{T} = \left(c^{\{i_1,\dots,i_n\}}_{\{j_1,\dots,j_m\}}\right) = \left(c^I_J\right) . \tag{6.4}$$

As symbolized by the notation in (6.4), we think of row indices and column indices in terms of *sets* J and I, respectively. Consequently, each index may appear only once as a row index or a column index, and the order of indices does not matter. For that reason, we call the indices *named indices*, rather than *positional indices*.

We call a qtensor

- *quadratic*, if the set of row indices is equal to the set of column indices,
- *ket* $|\psi\rangle$, if the set of column indices is empty, and
- *bra* $\langle\psi|$, if the set of row indies is empty.

Two qtensors $\mathcal{T} = \left(c^I_J\right)$ and $\mathcal{T}' = \left(c'^{I'}_{J'}\right)$ are of the *same type*, if $I = I'$ and $J = J'$. For qtensors of the same type we define the sum "+" by element-wise summation.

There is also a product "$*$" for qtensors. Using the index sets $S = I \cap J'$, $\tilde{I} = I \backslash S$, and $\tilde{J} = J' \backslash S$, the multiplication is defined if $\tilde{I}$ and I', as well as J and $\tilde{J}'$ are disjoint. We further use the notation $I'' = \tilde{I} \dot{\cup} I'$, and $J'' = J \dot{\cup} \tilde{J}'$, and finally define

$$\mathcal{T}_1 * \mathcal{T}_2 = \left(c''^{I''}_{J''}\right) = \left(\sum_S c^{\tilde{I}\cup S}_J c'^{I'}_{\tilde{J}'\cup S}\right) . \tag{6.5}$$

The summation over the index set S means the summation over all indices $s \in S$.

Let us discuss three important special cases for the "$*$" product. If $S = I = J'$, the product reduces to the ordinary non-abelian matrix multiplication; if $S = \{\}$, the product is the usual tensor product $\mathcal{T}_1 \otimes \mathcal{T}_2$. Third, if $\mathcal{T}_1$ is quadratic (i. e. $I = J$) and if $I \subset J'$, the product $\mathcal{T}_1 * \mathcal{T}_2$ is of the same type as $\mathcal{T}_2$, i. e. $\mathcal{T}_1$ operates on $\mathcal{T}_2$. In the latter case, one could think of this product as a "smart" sparse matrix version of the product in Eq. (6.1).

Chapter 7

Local invariants for multi-partite quantum states

Quantum mechanical states have a complex description in terms of their density matrix, which comprises all information available about a system under a given experimental situation. Different density matrices correspond to different states of a system, and allow for different predictions on its future behaviour. For many purposes, however, we are only interested in properties of the state (such as its entropy or purity) which are invariant under unitary transformations that correspond to a change of basis in the Hilbert space associated with the system.

For systems composed of several parts, or subsystems, there exists a natural tensor product structur underlying the state space. For such composite systems, the superposition principle gives rise to the phenomenon of entanglement which manifests itself in peculiar “quantum” correlations between results of measurements on its different parts [31, 69, 9]. To capture the essential features of this entanglement, we look for properties of the density matrix that are invariant under *local unitary transformations*, corresponding to a local change of basis in the Hilbert spaces of the individual subystems. Such local invariants have attracted the attention of people working on the foundation of quantum mechanics and, more recently, in quantum information theory [66, 67, 52, 39, 81, 43], where entanglement is perceived as a resource for tasks in quantum communication and computation.

In this paper, we present a family of local invariants of a multi-partite quantum system. These invariants are derived from an invariant decomposition of the state space of the system, regarded as a real vector space of hermitean operators with a scalar product. They have a natural geometric interpretion in terms of the length of projections of vectors onto invariant subspaces, which contain information either about one local subsystem *or* about correlations between a given set of subsystems. Beyond their geometric interpretation, these invariants have a number of merits. They can easily be calculated – even analytically – for many states, and they are directly connected to measurement data [44, 77], i.e. they can be measured straightforwardly in an experiment.

The representation of the density matrix as an element in the real (metric) vector space of hermitean matrices is well known, and a number of researchers have used a similar approach before [71, 41, 66, 67, 34, 85]. Nevertheless, our results add to existing work in at least two respects. First, the explicit decomposition of the state space into a direct sum of invariant sub-spaces makes the identification of invariants quite transparent; it allowed us in fact to find a family of new invariants. Second, from the *convexity* of set of separable states, we are able to derive constraints on the invariants of separable states. This way we can give a new entanglement criterion, which is a true multi-partite criterion i.e. not based on bi-partite splittings.

7.1 State tomography

It is a well known fact that the four Pauli spin matrices $\sigma_0 = \mathbb{I}, \sigma_1 = \sigma_x, \sigma_2 = \sigma_y, \sigma_3 = \sigma_z$ form a real basis of the vector space of the hermitean operators which act on one qubit. With respect to the scalar product $\langle A, B\rangle = \mathrm{tr}(AB)$, the basis vectors are orthogonal. More generally, for a d-dimensional quantum system, there exists a set of $2^d - 1$ traceless hermitean generators of the $SU(d)$, which we call $\sigma_1, \ldots \sigma_{2^d-1}$. One specific choice of these generators is the so-called Cartan-Weyl-construction (see, e. g. [66]). Combined with the unit operator $\mathbb{I} \equiv \sigma_0$, they form a real non-normalized orthogonal basis of the vector space of hermitean operators in d dimensions,

$$\langle \sigma_i, \sigma_j \rangle = \mathrm{tr}(\sigma_i \sigma_j) = \delta_{i,j} d \tag{7.1}$$

Be $P = \{1, 2, \ldots, n\}$ a set of parties and $\mathcal{V}$ the vector space of hermitean operators acting on the n-partite Hilbert space $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \otimes \cdots \otimes \mathcal{H}^{(n)}$, where $\mathcal{H}^{(a)}$ is a Hilbert space of the (finite) dimension d_a. Clearly, the tensor products of the basis operators form a basis

$$\mathcal{B} = \{\sigma^{(1)}_{i_1} \sigma^{(2)}_{i_2} \cdots \sigma^{(n)}_{i_n} | 0 \le i_a \le d_a^2 - 1 \text{ for all } a \in P\} \tag{7.2}$$

of $\mathcal{V}$.

Any n-partite density operator $\rho \in \mathcal{V}$ can thus be expanded in the product basis

$$\rho = \frac{1}{d} \sum_{i_1,i_2,\dots i_n} \left(c_{i_1 i_2 \dots i_n} \sigma^{(1)}_{i_1} \sigma^{(2)}_{i_2} \cdots \sigma^{(n)}_{i_n} \right), \tag{7.3}$$

where $d = \prod_{a=1}^{n} d_a$, and

$$c_{i_1 i_2 \dots i_n} = \operatorname{tr} \left(\rho\, \sigma^{(1)}_{i_1} \sigma^{(2)}_{i_2} \cdots \sigma^{(n)}_{i_n} \right) = \left\langle \sigma^{(1)}_{i_1} \sigma^{(2)}_{i_2} \cdots \sigma^{(n)}_{i_n} \right\rangle_{\rho}. \tag{7.4}$$

In other words, the expansion coefficients $c_{i_1 i_2 \dots i_n}$ are expectation values of products of hermitean operators. Since these expectation values can, in principle, be measured by local measurements (given a sufficiently large ensemble of copies of ρ), one can use this method in order to determine an unknown n-partite quantum state with the help of local measurements and classical communication (quantum state tomography).

7.2 Invariant decomposition of the state space

Be $\sigma = \sigma^{(1)}_{i_1} \sigma^{(2)}_{i_2} \cdots \sigma^{(n)}_{i_n}$ an arbitrary element of the product basis $\mathcal{B}$, and $S = \{a | i_a \neq 0\}$ the set of parties, where σ acts non-trivially. Using this definition, we call σ a S-correlation operator, and the set of all S-correlation operators $\mathcal{B}_S$. It is clear that $\mathcal{B}$ can be written as the union of the (disjoint) sets of S-correlation operators, i. e.

$$\mathcal{B} = \dot{\bigcup}_{S \subset P} \mathcal{B}_S. \tag{7.5}$$

Example: In the case of three qubits, we have eight such sets (with $a, b \in \{1, 2, 3\}$): $\mathcal{B}_{\{\}} = \{\mathbb{I}\}$, $\mathcal{B}_{\{a\}} = \{\sigma^{(a)}_i | i = 1, 2, 3\}$, $\mathcal{B}_{\{a,b\}} = \{\sigma^{(b)}_i \sigma^{(a)}_j | i, j = 1, 2, 3\}$, and $\mathcal{B}_{\{1,2,3\}} = \{\sigma^{(1)}_i \sigma^{(2)}_j \sigma^{(3)}_k | i, j, k = 1, 2, 3\}$.

Theorem 2 *For each set S of parties, the vector space $\mathcal{V}_S = \operatorname{span}(\mathcal{B}_S)$ is invariant under local unitary transformations, which act as isometries on $\mathcal{V}_S$.*

Proof: Be $U^{(a)}$ a unitary operation which acts on party a. If $a \notin S$, all elements of $\mathcal{B}_S$ remain unchanged under the action of $U^{(a)}$. If, on the other hand, $a \in S$, then the orthogonal set of traceless generators $\sigma^{(a)}_i$ ($i > 0$) is transformed into a different set of orthogonal traceless generators, i. e. for $1 \leq i \leq d_a^2 - 1$,

$$\sigma_i^{(a)} \to \tilde{\sigma}_i^{(a)} = \sum_k \left(O(U^{(a)})\right)_{ik} \sigma_k^{(a)}$$

with an orthogonal matrix $O(U^{(a)}) \in SO(d_a^2 - 1)$ [11, 4]. Obviously, both sets of generators span the same set of *all* traceless operators. □

Given a density operator ρ and a set S of parties, the projection of ρ onto the subspaces $\mathcal{V}_S$ is given by

$$\rho_S = \frac{1}{d} \sum_{\sigma \in \mathcal{B}_S} \langle \rho, \sigma \rangle \, \sigma = \frac{1}{d} \sum_{\sigma \in \mathcal{B}_S} \langle \sigma \rangle_\rho \, \sigma. \tag{7.6}$$

Note that ρ_S is *not* the partial trace of ρ over all parties $a \in P \backslash S$, but we have

$$\mathrm{tr}_{P \backslash S} \, \rho = \sum_{S' \subset S} \rho_{S'}. \tag{7.7}$$

Due to Theorem 1, local unitary operations rotate a projection ρ_S only within the subspace $\mathcal{V}_S$. Ignoring the normalization constant $1/d$ leads us to

Corollary 2.1 *For each set S of parties, the squared length of the projection of a state ρ onto the span $\mathcal{V}_S$ of $\mathcal{B}_S$,*

$$L_S(\rho) = \sum_{\sigma \in \mathcal{B}_S} \langle \sigma \rangle_\rho^2 \tag{7.8}$$

is invariant under local unitary transformations. We call $L_S(\rho)$ the S-correlation strength of ρ.

For pure product states, the S-correlation strength is given by

$$L_S^{\text{pure}} = \sum_{S' \subset S} (-1)^{|S| - |S'|} \prod_{a \in S'} d_a, \tag{7.9}$$

where we set $\prod_{a \in \{\}} d_a = 1$. In the special case when ρ is a pure multi-qubit product state, all S-correlation strengths are equal to unity.

Proof: It is enough to show Eq. 7.9 for the case $S = P$, since for all subsets of P, the respective reduced density operators are also pure states.

First we note that, according to (7.5) and (7.8), we have $L_P^{\text{pure}}+\sum_{S\subsetneq P} L_S^{\text{pure}} = \prod_{a\in P} d_a = d$, i. e. we can calculate L_P^{pure} for a n-partite quantum system, if we know L_S^{pure} for all $S \subsetneq P$. For $S = \{\}$, (7.9) holds trivially. Now we assume that (7.9) holds for all $S \subsetneq P$. Using the shorthand notation $m = |P| - |S'|$, we get

$$\begin{aligned} L_P^{\text{pure}} &= \prod_{a\in P} d_a - \sum_{S\subsetneq P}\sum_{S'\subset S}(-1)^{|S|-|S'|}\prod_{a\in S'} d_a \\ &\overset{(*)}{=} \prod_{a\in P} d_a - \sum_{S'\subsetneq P} \underbrace{\sum_{k=0}^{m-1}(-1)^k\binom{m}{k}}_{(-1)^m}\prod_{a\in S'} d_a \\ &= \sum_{S'\subset P}(-1)^{|P|-|S'|}\prod_{a\in S'} d_a \quad . \end{aligned} \tag{7.10}$$

For $(*)$, we counted all sets S with $S' \subset S \subsetneq P$ and with a total of $|S'| + k$ elements, and used $0 = (-1+1)^m = \sum_{k=0}^{m}\binom{m}{k}(-1)^k$. ☐

If S does not contain party a, we note that $L_S(\rho)$ is only a function of the reduced density operator $\operatorname{tr}_a \rho$. Thus, the only invariant which contains information about the total state is $L_P(\rho)$.

A strategy to gain further information about the entanglement properties of a given state ρ uses the concept of *partitions* of the set of parties. To do this, we allow several parties $b_1 \dots b_k$ to apply joint operations. Technically, this is equivalent to a situation where these parties are replaced by a single higher-dimensional quantum system a. In this case, one can calculate the required traceless generators for the new party a as products of the generators of the old parties $b_1 \dots b_k$,

$$\tilde{\sigma}^{(a)}_{i_1\dots i_k} = \sigma^{(b_1)}_{i_1}\sigma^{(b_2)}_{i_2}\cdots\sigma^{(b_k)}_{i_k}, \tag{7.11}$$

with $(i_1,\dots,i_k) \neq (0,\dots,0)$.

Any partitioning can be realized by iteratively joining parties pairwise, say $b_1, b_2 \longrightarrow a$. Using Eq. (7.11), one can easily verify that the correlation strength for a set $S = \{a\} \cup S' = \{a\} \cup \{b_\mu, b_\nu, \dots\}$ of parties, is given by

$$L_{\{a\}\cup S'} = L_{\{b_1\}\cup S'} + L_{\{b_2\}\cup S'} + L_{\{b_1,b_2\}\cup S'}, \tag{7.12}$$

which means that the correlation strengths for coarse partitions are functions of the correlations strengths of the finest partition.

A special partition is obtained if we allow *all* parties to operate jointly, i. e. if the set of parties $\tilde{S}$ consists of a *single* super-party. $L_{\tilde{S}}$ is then invariant under *all* unitary operations, and thus describes a global property of the state. Indeed, we have

$$L_{\tilde{S}}(\rho) = \sum_{\sigma \in \mathcal{B}} \langle \sigma \rangle_\rho^2 - \langle \mathbb{I} \rangle_\rho = d \operatorname{tr}\left(\rho^2\right) - 1, \tag{7.13}$$

so that $L_{\tilde{S}}$ is a measure for the purity of the state ρ.

Using Eq. 7.5 and 7.8, we can re-write the left-hand side of Eq. 7.13 as the sum of all S-correlation strengths,

$$\sum_{\{\} \neq S \subset P} L_S = d \operatorname{tr}\left(\rho^2\right) - 1, \tag{7.14}$$

which allows us to state

Corollary 2.2 *For any state ρ, the sum of all correlation strengths is given by the purity of the state. This implies, in particular, that for states with the same purity, there is a trade-off between local and the different non-local correlations.*

For a pure state $\rho = |\psi\rangle\langle\psi|$, we have $\operatorname{tr}(\rho^2) = \operatorname{tr}(\rho) = 1$, so that Corollary 2.2 can be regarded as a quantitative expression of the folklore saying that in entangled states, the information about the state is contained in its correlations rather than its local properties.

It is a useful fact that the convex structure of the space $\mathcal{V}$ of states is obeyed by the subspaces $\mathcal{V}_S$ separately, in the following sense: If a state is given by a convex sum of states ρ_l, i. e. $\rho = \sum_l p_l \rho_l$ with $p_l > 0$ for all l and $\sum_l p_l = 1$, then the projection of ρ onto each of the subspaces $\mathcal{V}_S$ is the convex sum of the projections of the states ρ_l onto $\mathcal{V}_S$. If ρ is a separable state, it can be written as a convex sum of pure product states. In this case, the projection of ρ onto each of the subspaces $\mathcal{V}_S$ is a convex sum of vectors with the squared length L_S^{pure}, so that the squared length $L_S(\rho)$ cannot exceed L_S^{pure}. This allows us to formulate the entanglement criterion:

Corollary 2.3 *If, for a state ρ there exists a subset S of parties, so that the S-correlation strength is greater than L_S^{pure}, then ρ is entangled.*

It is interesting to note that the entanglement criterion is strongest for the finest partition, in the following sense: Be $b_1, b_2 \to a$ a coarsening as in Eq. (7.12), and be $L_S(\rho) < L_S^{\mathrm{pure}}$ for all $S \subset \{b_1, b_2\} \cup S' \subset P$. Using (7.12) for the state ρ and for product states, we find

$$\begin{aligned} L_{\{a\}\cup S'} &= L_{\{b_1\}\cup S'} + L_{\{b_2\}\cup S'} + L_{\{b_1,b_2\}\cup S'} \\ &\leq L^{\mathrm{pure}}_{\{b_1\}\cup S'} + L^{\mathrm{pure}}_{\{b_2\}\cup S'} + L^{\mathrm{pure}}_{\{b_1,b_2\}\cup S'} \\ &= L^{\mathrm{pure}}_{\{a\}\cup S'}. \end{aligned} \tag{7.15}$$

This means that we do not detect entanglement in any coarse partition, if we do not detect it in the finest partition.

For all states of n qubits, which are diagonal in the basis of so-called graph states [28], the correlation strengths can easily be calculated analytically. This is useful since *any* n-qubit state can be depolarized to this form by local operations and classical communication [28]. Moreover, many entangled multi-partite states which are useful for practical applications, such as generalized GHZ-states [40], quantum error correcting codes [68, 37] or cluster states [18], belong to the class of graph states.

As an illustration, consider the particular case of the state

$$\rho = p\,|GHZ_n\rangle\langle GHZ_n| + \frac{1-p}{2^n}\mathbb{I}$$

, where $|GHZ_n\rangle\langle GHZ_n|$ is the n-qubit GHZ state. Corollary 2.3 yields $L_{\{a_1,\ldots,a_n\}}(\rho) = p^2(2^{n-1} + \delta)$, where $\delta = 0, 1$ for odd or even n, respectively. That is, ρ is definitely entangled, if $p > 1/\sqrt{2^{n-1} + \delta}$.

For multi-qubit states, the entanglement criterion of Corollary 2.3 looks very similar to a criterion for local-realistic descriptions of these states which has been found recently [85]. Despite their similarity, however, the two criteria state different things. While the first is a sufficient criterion for non-separability, the latter is a sufficient criterion for the existence of a local-realistic description of a given state.

Presently, we cannot report an example where the entanglement criterion of Corollary 2.3 is stronger than the criterion found by Peres [62]. Nevertheless, we think that our criterion is of interest. First, our criterion is a real multi-partite entanglement criterion, and as such it is stronger than when it is applied to bipartite splittings (see Eq. 7.15). Second, it can easily be checked experimentally, since the correlation strengths are directly connected to measurement data. This is especially useful for almost-pure states, where

Corollary 2.3 becomes tight; on the other hand, their density matrices (and their partial transposes) have, by definition, small eigenvalues so that for checking the Peres criterion those states have to be measured very precisely.

7.3 Other invariants

The local invariants L_S do not form a complete set of invariants, i. e. they do not contain *all* information about the entanglement properties of a given state. However, the formalism used in this paper allows us identify a larger class of invariants, many of which also have a straight-forward geometrical interpretation.

From the proof of Theorem 2, it follows that the transformation properties of the subspaces $\mathcal{V}_S$ are closely related. In order to show how this can be used for the construction of invariants, we first define the S-correlation tensor C_S, which is composed of the components of the projection ρ_S in (7.6),

$$C_S = \left(\left\langle \prod_{a \in S} \sigma_{i_a}^{(a)} \right\rangle_\rho \right)_{i_a > 0} . \tag{7.16}$$

One can easily see that a contraction of two such tensors with respect to a index i_ν at the same position is invariant under local unitary operations, i. e. under orthogonal transformation $\mathcal{O}$ which affect this index:

$$\begin{aligned} \sum_{i_\nu} c_{\dots i_\nu \dots} c_{\dots i_\nu \dots} &= \sum_{i_\nu, i''_\nu} \delta_{i_\nu, i''_\nu} c_{\dots i_\nu \dots} c_{\dots i''_\nu \dots} \\ &= \sum_{i'_\nu, i_\nu, i''_\nu} \mathcal{O}_{i'_\nu i_\nu} c_{\dots i_\nu \dots} \mathcal{O}_{i'_\nu i''_\nu} c_{\dots i''_\nu \dots} \\ &= \sum_{i'_\nu} \tilde{c}_{\dots i'_\nu \dots} \tilde{c}_{\dots i'_\nu \dots} \end{aligned} \tag{7.17}$$

Any complete contraction of correlation tensors, i. e. a polynomial in the expansion coefficients, in which indices are either zero or summed up pairwise, is thus a local invariant. Examples for such polynomials are $c_{0jk} c_{ij0} c_{i0k}$, $c_{0j00} c_{ij0l} c_{ij'k0} c_{cj'kl}$ (where, as usual, the sum is taken over all indices which occur twice), the correlation strengths L_S, and other objects which can be interpreted as scalar products, such as the scalar product of $\rho_{a_1 a_2 a_3}$ with the tensor product of $\rho_{\{a_1\}}, \rho_{\{a_2\}}$ and $\rho_{\{a_3\}}$,

$$\langle \rho_{\{a_1\}} \otimes \rho_{\{a_2\}} \otimes \rho_{\{a_3\}}, \rho_{\{a_1 a_2 a_3\}} \rangle = \sum_{i,j,k>0} c_{i00} c_{0j0} c_{00k} c_{ijk}. \tag{7.18}$$

Unfortunately, it seems to be not possible to construct a complete set of local invariants using the construction above; for the case of two qubits, there are seven independent invariants which can be written as contraction of correlation tensors; the two remaining invariants are functions of the determinant and sub-determinants of the correlation tensor [34]. A different approach to finding local invariants is to expand the d independent global invariants $\operatorname{tr}(\rho^k)$ $(0 \leq k < d)$ [54] into the operator basis (7.2). For $k = 0$, this yields the (trivial) invariant $\operatorname{tr}\rho$, and for $k = 2$ one finds all $L_S (S \subset P)$ (see Eq. 7.14). For the case of two qubits, it is thus possible to identify all nine independent local invariants in those expansions.

Bibliography

[1] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. 1996. Eprint quant-ph/9611025.

[2] H. Aschauer and H.-J. Briegel. Der Quantenfingerabdruck. *Physik Journal*, 1(1), 2002.

[3] H. Aschauer and H.-J. Briegel. Private entanglement over arbitrary distances, even using noisy apparatus. *Phys. Rev. Lett.*, 88:047902, 2002.

[4] H. Aschauer and H.-J. Briegel. Security proof of quantum cryptography based entirely on entanglement purification. *Phys. Rev. A*, 66:032302, 2002.

[5] H. Aschauer and H.-J. Briegel. Sauber verschränkt. *Physik Journal*, 2(7/8), 2003.

[6] H. Aschauer, J. Calsamiglia, M. Hein, and H.-J. Briegel. Local invariants for multi-partite entangled states, allowing for a simple entanglement criterion. *Quant. Inf. Comp.*, 4:383–395, 2004.

[7] H. Aschauer, W. Dür, and H.-J. Briegel. Multiparticle entanglement purification for two-colorable graph states. *Phys. Rev. A*, 71:012319, 2005.

[8] A. Aspect, P. Grangier, and G. Roger. Experimental test of realistic local theories via Bell's theorem. *Phys. Rev. Lett.*, 47, 1981.

[9] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195, 1964. Reprinted in J. S. Bell, *Speakable and unspeakable in quantum mechanics*, Cambidge University Press, 1987.

[10] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, New York, 1985. IEEE.

[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[12] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557, 1992.

[13] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722, 1996.

[14] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54(5):3824–3851, November 1996.

[15] D. Bouwmeester, A. Ekert, and A. Zeilinger, editors. *The Physics of Quantum Information.* Springer, Berlin, 2000.

[16] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller. The physics of quantum information. chapter Quantum networks II: Communication over noisy channels. Springer, 2000.

[17] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932, 1998.

[18] H. J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.*, 86:910–913, 2000.

[19] V. Buzek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844–1852, 1996.

[20] V. Buzek and M. Hillery. Universal optimal cloning of arbitrary quantum states: From qubits to quantum registers. *Phys. Rev. Lett.*, 81:5003–5006, 1998.

[21] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098, 1996.

[22] 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.

[23] J. I. Cirac and N. Gisin. Coherent eavesdropping strategies for the 4-state quantum cryptography protocol. *Phys. Lett. A*, 229:1, 1997.

[24] 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, 1969.

[25] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818, 1996.

[26] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys. Rev. Lett.*, 77:2818, 1996.

[27] D. P. DiVincenzo and A. Peres. Quantum codewords contradict local realism. *Phys. Rev. A*, 55:4089, 1997.

[28] W. Dür, H. Aschauer, and H.-J. Briegel. Multiparticle entanglement purification for graph states. *Phys. Rev. Lett.*, 91:107903, 2003. eprint quant-ph/0303087.

[29] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller. Quantum repeaters based on entanglement purification. *Phys. Rev. A*, 59:169, 1999.

[30] W. Dür and J. I. Cirac. Nonlocal operations: Purification, storage, compression, tomography, and probabilistic implementation. *Phys. Rev. A*, 64:012317, 2001.

[31] A. Einstein, B. Podolsky, and N. Rosen. Can quantum mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777, 1935.

[32] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[33] B.-G. Englert. Remarks on some basic issues in quantum mechanics. *Z. Naturforsch.*, 54a:11–32, 1999.

[34] B.-G. Englert and N. Metwally. Separability of entangled q-bit pairs. *J. Mod. Opt.*, 47:2221–2231, 2000.

[35] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, 1972.

[36] G. Giedke, H.-J. Briegel, J. I. Cirac, and P. Zoller. Lower bounds for attainable fidelities in entanglement purification. *Phys. Rev. A*, 59:2641, 1999.

[37] M. Grassl. ISIT 2002, Lausanne.

[38] M. Grassl. `http://iaks-www.ira.uka.de/home/grassl/QECC/circuits.html`.

[39] M. Grassl, M. Rötteler, and T. Beth. Computing local invariants of quantum-bit systems. *Phys. Rev. A*, 58:1833, 1998.

[40] D. M. Greenberger, M. Horne, and A. Zeilinger. Going beyond Bell's theorem. In M. Kafatos, editor, *Bell's theorem, quantum theory, and conceptions of the universe*, page 69, Dortrecht, 1989. Kluwer.

[41] F. T. Hioe and J. H. Eberly. n-level coherence vector and higher conservation laws in quantum optics and quantum mechanics. *Phys. Rev. Lett.*, 47:838–841, 1981.

[42] G. Holton. Werner Heisenberg and Albert Einstein. *Physics Today*, 53(7):38, 2000.

[43] G. Jaeger, M. Teodorescu-Frumosu, A. Sergienko, B. E. A. Saleh, and M. C. Teich. Multiphoton Stokes-parameter invariant for entangled states. *Phys. Rev. A*, 67:032307, 2003.

[44] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White. Measurement of qubits. *Phys. Rev. A*, 64:052312, 2001.

[45] A. Y. Kitaev. *Russ. Math. Surv.*, 52:1191, 1997.

[46] E. Knill and R. Laflamme. Eprint quant-ph/9608012, 1996.

[47] E. Knill and R. Laflamme. Theory of quantum error-correcting code. *Phys. Rev. A*, 55:900, 1997.

[48] E. Knill, R. Laflamme, and W. Zurek. Accuracy threshold for quantum computation. 1996.

[49] E. Knill, R. Laflamme, and W. Zurek. *Science*, 279:342, 1998.

[50] K. Kraus. *States, Effects, and Operations*, volume 190 of *Lecture Notes in Physics*. Springer Verlag, Berlin Heidelberg New York Tokyo, 1983.

[51] R. Laflamme, C. Miquel, J. P. Paz, and W. H. Zurek. Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77:198, 1996.

[52] N. Linden and S. Popescu. On multi-particle entanglement. *Fortschr. Physik*, 46:567, 1998.

[53] C. Macchiavello. On the analytical convergence of the QPA procedure. *Phys. Lett. A*, 246:385–388, 1998.

[54] G. Mahler and V. A. Weberruß. *Quantum Networks: Dynamics of Open Nanostructures*. Springer, Berlin, 1995.

[55] E. N. Maneva and J. A. Smolin. Improved two party and multi-party purification protocols. In J. Samuel J. Lomonaco, editor, *Quantum Computation and Quantum Information*, volume 305 of *AMS Contemporary Mathematics*. American Mathematical Society, Providence, RI, 2002.

[56] D. Mayers. In *Advances in Cryptology – Proceedings of Crypto '96*, pages 343–357, New York, 1996. Springer-Verlag. see also quant-ph/9802025.

[57] N. D. Mermin. Quantum mysteries revisited. *Am. J. Phys.*, 58:731, 1990.

[58] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight. Multiparticle entanglement purification protocols. *Phys. Rev. A*, 57:R4075–R4078, 1998.

[59] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. Experimental entanglement swapping: Entangling photons that never interacted. *Phys. Rev. Lett.*, 80:3891–3894, 1998.

[60] J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger. Experimental entanglement purification of arbitrary unknown states. *Nature*, 423:417–422, 2003.

[61] A. Peres. *Quantum Theory: Concepts and Methods.* Kluwer, New York, 1993.

[62] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77:1413, 1996.

[63] J. Preskill. *Proc. Roy. Soc. Lond. A*, 454, 1998.

[64] R. Raussendorf and H.-J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[65] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409:791–794, 2001.

[66] J. Schlienz and G. Mahler. Description of entanglement. *Phys. Rev. A*, 52:4396, 1995.

[67] J. Schlienz and G. Mahler. The maximal entangled three-particle state is unique. *Phys. Lett. A*, 224:39–44, 1996.

[68] D. Schlingemann and R. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 65:012302, 2002.

[69] E. Schrödinger. The quantum postulate and the recent development of atomic theory. *Naturwissenschaften*, 23:807–812,823–828,844–849, 1935.

[70] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51:2738, 1995.

[71] J. Schwinger. Unitary operator bases. *Proc. NAS*, 46(4):570–579, 1960.

[72] C. E. Shannon and W. Weaver. *The mathematical theory of communication.* University of Illinois Press, 1949.

[73] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493, 1995.

[74] P. W. Shor and J. Preskill. Simple proof of the security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441, 2000.

[75] A. Steane. Multi-particle interference and quantum error correction. *Proc. R. Soc. Lond. A*, 452:2551, 1996.

[76] A. Steane. General theory of quantum error correction and fault tolerance. In D. Bouwmeester, A. Ekert, and A. Zeilinger, editors, *The Physics of Quantum Information*, pages 242–252. Springer, Berlin, 2000.

[77] R. T. Thew, K. Nemoto, A. G. White, and W. J. Munro. Qudit quantum-state tomography. *Phys. Rev. A*, 66:012303, 2002.

[78] S. J. van Enk, J. I. Cirac, and P. Zoller. Ideal quantum communication over noisy channels: A quantum optical implementation. *Phys. Rev. Lett.*, 78:4293–4296, 1997.

[79] S. J. van Enk, J. I. Cirac, and P. Zoller. Photonic channels for quantum communication. *Science*, 279:205–208, 1998.

[80] G. van Rossum and the Python Software Foundation. `http://www.python.org`.

[81] F. Verstraete, J. Dehaene, and B. D. Moor. Lorentz singular-value decomposition and its applications to pure states of three qubits. *Phys. Rev. A*, 65:032308, 2002.

[82] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, 1998.

[83] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277, 1989.

[84] W. K. Wootters and W. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[85] M. Zukowski and Č. Brukner. Bell's theorem for general n-qubit states. *Phys. Rev. Lett.*, 88:210401, 2002.

[86] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "event-ready-detectors" Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, 71:4287–4290, 1993.

Lebenslauf

Persönliche Daten

Hans Aschauer

Geb. am 15. 11. 1972 in Bad Reichenhall
Verheiratet, zwei Kinder

Schulbildung

1979–1983	Grundschule Saaldorf
1983–1992	Gymnasium in Laufen/Salzach (Leistungskurse Mathematik und Physik) Abschluss: allgemeine Hochschulreife

Zivildienst

1992–1993	Rettungsdienst (Bayerisches Rotes Kreuz Bad Reichenhall/Freilassing)

Studium

11/1993–03/1999	Studiengang Physik Diplom (Universität München) Diplomarbeit: “Scanrichtungsabhängigkeit bei STM-Aufnahmen von Adsorbaten”. Abschluss: Diplom (Note: sehr gut)
06/1999–01/2004	Promotion in theoretischer Physik, “Quantum communication in noisy environments”.

Beruflicher Werdegang

06/1999–09/2003	Wissenschaftlicher Mitarbeiter an der LMU München
seit 10/2003	Wissenschaftlicher Mitarbeiter, nabios GmbH

München, 17. Mai 2005

Danksagung

Es wäre nicht möglich gewesen, diese Dissertation ohne die Hilfe von vielen Menschen zu verfassen. Hans Briegel war ein Betreuer, der mein Interesse an der Quanteninformatik geweckt hat, mich mit diesem Fachgebiet und der wissenschaftlichen Arbeitsweise vertraut gemacht hat und mir in zahllosen Diskussionen wertvolle Tipps und Denkanstöße gab. Er war aber auch stets offen für interessante Diskussionen und hilfreiche Gespräche zu Themen außerhalb des Fachgebietes oder außerhalb der Physik. Prof. Schenzle nahm mich freundlich in seine Arbeitsgruppe auf und bereicherte außerdem den Forschungsalltag um Episoden aus Wissenschaft und Hochschulpolitik. Robert Raußendorf als meinem Büro- und Leidensgenosse, und alle anderen Kollegen verdanke ich es, dass ich die vergangenen Uni-Jahre in sehr guter Erinnerung behalten werde. Vor allem aber war es meine Frau Susanne, die mir in Durststrecken Kraft und Motivation gab, und die mir in arbeitsreichen Zeiten den Rücken frei hielt.