Universal quantum cloning

Master's Thesis
University of Turku
Faculty of Mathematics and
Natural Science
Theoretical Physics
2013
Johannes Nokkala
Referees:
Kalle-Antti Suominen
Tom Kuusela

UNIVERSITY OF TURKU
Faculty of Mathematics and Natural Science

NOKKALA, JOHANNES: Universal Quantum Cloning

Master's Thesis, 91 p.
Theoretical Physics
December 2013

After introducing the no-cloning theorem and the most common forms of approximate quantum cloning, universal quantum cloning is considered in detail. The connections it has with universal NOT-gate, quantum cryptography and state estimation are presented and briefly discussed. The state estimation connection is used to show that the amount of extractable classical information and total Bloch vector length are conserved in universal quantum cloning. The $1 \to 2$ qubit cloner is also shown to obey a complementarity relation between local and nonlocal information. These are interpreted to be a consequence of the conservation of total information in cloning. Finally, the performance of the $1 \to M$ cloning network discovered by Bužek, Hillery and Knight is studied in the presence of decoherence using the Barenco et al. approach where random phase fluctuations are attached to 2-qubit gates. The expression for average fidelity is calculated for three cases and it is found to depend on the optimal fidelity and the average of the phase fluctuations in a specific way. It is conjectured to be the form of the average fidelity in the general case. While the cloning network is found to be rather robust, it is nevertheless argued that the scalability of the quantum network implementation is poor by studying the effect of decoherence during the preparation of the initial state of the cloning machine in the $1 \to 2$ case and observing that the loss in average fidelity can be large. This affirms the result by Maruyama and Knight, who reached the same conclusion in a slightly different manner.

Keywords: Quantum Mechanics, Universal Quantum Cloning, Quantum Information, Decoherence

TURUN YLIOPISTO
Matemaattis-luonnontieteellinen tiedekunta

NOKKALA, JOHANNES: Universaali kvanttikloonaus

Pro gradu -tutkielma, 91 s.
Teoreettinen fysiikka
Joulukuu 2013

Ei-kloonauslauseen ja eräiden tyyppillisten approksimatiivisten kvanttikloonaamisen muotojen esittelyn jälkeen universaalia kvanttikloonaamista tarkastellaan yksityiskohtaisesti. Sen yhteydet universaaliin NOT-porttiin, kvanttikryptografiaan ja tilanarviointiin esitetään, ja näitä yhteyksiä käsitellään lyhyesti. Tilanarviointiyhteyttä käyttäen osoitetaan, että universaalissa kloonauksessa mittaustuloksista saatava klassinen informaatio ja Blochin vektorin kokonaispituus ovat säilyviä suureita. $1 \to 2$ qubittikloonaajan osoitetaan myös noudattavan lokaalin ja epälokaalin informaation välistä komplementaarisuusrelaatiota. Näiden tulkitaan olevan seurausta kokonaisinformaation säilymisestä kloonauksessa. Lopuksi tutkitaan vaihekohinan vaikutusta Bužekin, Hilleryn ja Knightin löytämän $1 \to M$ kloonauspiirin tuottamiin klooneihin käyttäen Barencon ja muiden lähestymistapaa, jossa 2-qubittiportteihin liitetään satunnaisia vaihefluktuaatioita. Kolmelle tapaukselle lasketaan keskimääräisen fideliteetin kaava, jonka havaitaan riippuvan optimaalisesta fideliteetistä ja keskimääräisestä vaihekohinasta tietyllä tavalla. Keskimääräisen fideliteetin kaavan esitetään olevan samaa muotoa myös yleisessä tapauksessa. Vaikka kloonauspiirin todetaan sietävän vaihekohinaa verrattain hyvin, kvanttipiiri-implementaation skaalautuvuuden esitetään olevan heikko tutkimalla tapausta, jossa vaihekohina vaikuttaa myös $1 \to 2$ kvanttikloonaajan alkutilan preparoinnissa ja havaitsemalla, että keskimääräinen fideliteetti voi laskea huomattavasti. Tämä vahvistaa Maruyaman ja Knightin tuloksen, jossa samaan johtopäätökseen päädyttiin hieman eri tavalla.

Asiasanat: Kvanttimekaniikka, universaali kvanttikloonaus, kvantti-informaatio, dekoherenssi

Contents

List of abbreviations

LOCC – Local operations and classical communication

MUBs – Mutually unbiased bases

OSE – Optimal state estimation

POVM – Positive operator valued measure

PPT – Positive partial transpose

QCM – Quantum cloning machine

QIP – Quantum information processing

QKD – Quantum key distribution

TPCP – Trace-preserving completely positive

U-NOT – Universal NOT

UQCM – Universal quantum cloning machine

Introduction

The no-cloning theorem states that an a priori unknown pure state cannot be perfectly copied, that is to say there is no unitary operation U such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ for an arbitrary pure state $|\psi\rangle$. In fact, it can be easily shown by using any two non-orthogonal states that U cannot exist. While simple to prove, this no-go theorem has deep consequences in the field of quantum information processing and is yet another striking difference between classical and quantum information. While perfect copying, or cloning, of states is forbidden by the no-cloning theorem, it is possible to approximately clone an unknown pure state. The subject of this thesis is universal quantum cloning, where all pure states are cloned equally well.

While there are many different forms of universal quantum cloning, the focus will be on universal cloning of pure states lying in a finite-dimensional Hilbert space where the universal quantum cloning machine is a unitary operation and all clones are in the same state after cloning transformation. The purpose of this thesis is to introduce the reader to the field of quantum cloning and in particular to universal quantum cloning, present the connections quantum cloning has with quantum cryptography, spin flips and quantum state estimation, study the information flow and entanglement structure in cloning and analyse how decoherence in the form of random phase fluctuations affects the quantum circuit implementation of a universal quantum cloning machine.

The structure of this thesis is as follows. The first Part has two Sections. First, the no-cloning theorem will be discussed in detail. In the second Section a definition for cloning and a figure of merit to quantify the quality of the clones will be presented. This is followed by a brief review of the most important types of quantum cloning, including state-dependent quantum cloning, where the quality of the clones varies depending on the state that was cloned, as well as some forms of quantum cloning that do not fit the definition given in this thesis but are nevertheless regarded as

cloning. At the end, some forms of experimental quantum cloning will be presented.

In the second Part, a closer look at universal quantum cloning will be taken. A cloning map will be introduced, characterizing the most well-known family of universal quantum cloning machines as a specific kind of symmetric permutation of quantum information among all subsystems during the cloning transformation. The simplest case of producing two approximate clones out of a single input state will be analysed, and a cloning network used to implement it when the input state is a two-level system will be presented. The connections which universal quantum cloning has with quantum cryptography and spin flips will also be presented in this Part.

The third Part is reserved for a short introduction to quantum state estimation, which concerns finding the optimal measurements to determine unknown or partially known quantum states, followed by a presentation of its strong cloning connection: if one could find out an unknown state with a measurement, one could perfectly clone it, and if one could perfectly clone a state, one could determine it with measurements. It will be seen that at the limit of many clones, the fidelities of optimal universal cloning and optimal state estimation coincide when the pure input state is drawn from a uniform distribution of all pure states.

In the fourth Part, after discussing the role of auxiliary systems in cloning, two different conservation laws regarding quantum cloning will be derived and their connection with the principle of conservation of information will be discussed. Also in this Part the entanglement structure of the output of the simplest case of universal quantum cloning machine will be studied and the results are used to show that the clones at the output obey a complementarity relation between local and nonlocal forms of quantum information, which is also related to conservation of information.

In the fifth Part, the effect of decoherence on the state of the clones produced by a specific type of cloning network will be analysed. In this thesis, decoherence is

assumed to cause random phase fluctuations, drawn from a Gaussian distribution, to the complex coefficients of the state of a quantum system as it passes through the quantum gates of the cloning network. While the initial state of the quantum cloning machine itself is required to be prepared in a specific way for the cloning network to work as specified, it is assumed that this can be done without decoherence effects. The effect of the presence of decoherence during the preparation of the quantum cloning machine will however be analysed for the simplest case and the resulting change in the quality of the clones will be compared to other cases.

Finally, the results from all previous Parts will be discussed in the Conclusions.

Part I

Basic concepts

In the first Part of the thesis no-cloning theorem will be introduced, which forbids the perfect cloning of a priori unknown pure states. Next, quantum cloning machines and their classification in different families will be presented and some of the most common classes of them will be reviewed.

1 No-cloning theorem

If information is encoded in a classical carrier, it can be replicated perfectly. This process is called cloning. The ability to freely clone classical information is one of the distinguishing features between classical and quantum information. It has been suggested [1] that the reason why classical information can be cloned is because it can be measured without changing it, and cloning of classical information is actually the act of first measuring the information one would like to clone and then preparing the copy. This cannot be done when information has been encoded in the states of

quantum systems, because of the well-known fact that a single measurement only reveals a tiny amount of information about the state that was measured and causes the quantum state to collapse to one of the eigenstates of the measurement operator. Without some appropriate prior knowledge about the state, a single measurement can never determine it.

It should be pointed out that information may be encoded in a classical way even if its carrier is a quantum system. DNA was presented as a prime example in [2]. The molecules it is made of are certainly quantum systems, but DNA can obviously be perfectly copied because the information is encoded in the nature of the molecules it is made of, namely in their chemical properties as guanine, adenine, thymine, or cytosine, not in their quantum states. It is intuitively expected that determining the type of a molecule can be done without destroying it or changing it into another kind of molecule, and the existence of all known life hinges on this fact.

The process of copying the state of a quantum system on another system while keeping the state of the original system intact, namely, the process $|\psi\rangle\,|0\rangle\,|C\rangle \longrightarrow |\psi\rangle\,|\psi\rangle\,|C_\psi\rangle$, is called (perfect) quantum cloning. Here, $|C\rangle$ and $|C_\psi\rangle$ are the states of an auxiliary system, usually called ancilla, before and after cloning, respectively. The idea of quantum cloning was first introduced in a 1982 publication called "FLASH - A superluminal communicator based upon a new kind of quantum measurement" by Nick Herbert [3]. In his paper, Herbert proposed a clever way to communicate via entanglement and macroscopically distinguishable states of light. He called it FLASH, as an acronym for first light amplification superluminal hookup.

The scheme relied on the ability to clone arbitrary polarization states of single photons, in order to make the states of the incoming photons distinguishable, and this would lead to the possibility of taking advantage of quantum entanglement to send signals. If possible, the speed of communication would depend only on the

speed of the cloner. This is an obvious violation of the no-signalling condition, which states that quantum nonlocality cannot be used to transmit signals carrying information, but the paper was published in spite of this because finding the error was expected to produce interesting responses. That is indeed what happened, and it was shown in various publications [4, 5, 6] that Herbert's idea was flawed because a priori unknown pure states cannot be cloned. This result is now known as the no-cloning theorem, and it can be stated as follows:

There is no unitary quantum operation that can perfectly clone an unknown pure state, or a pure state drawn from a set of two or more nonorthogonal states.

Without no-cloning theorem, superluminal communication would become possible, as shown by Herbert, and this would lead to violation of causality according to special relativity. The impossibility of superluminal communication arises in quantum mechanics as well because of the linearity and trace-preserving properties of physical transformations [7]. The ability to perfectly clone unknown quantum states would also make it possible to completely determine them by making a large ensemble of clones and then performing the necessary measurements on them while keeping the original state intact. On the other hand, no-cloning theorem is the cornerstone of the security of quantum key distribution (QKD) and provides quantum information processing (QIP) with possibilities that its classical counterpart does not have.

The no-cloning theorem can be proven in several ways. In a response to Herbert's 1982 publication, Wootters and Zurek published an article [5] entitled "A single quantum cannot be cloned" later same year, where they showed how the impossibility to perfectly clone arbitrary quantum states follows from the linearity of quantum mechanics.

Consider the horizontal and vertical polarization states $|H\rangle$ and $|V\rangle$ of a photon. Let $|C\rangle$ be the initial state of the cloning machine and $|C_H\rangle$ and $|C_V\rangle$ its final states.

If the cloning transformation is such that

$$\begin{aligned} |H\rangle |C\rangle &\longrightarrow |H\rangle |H\rangle |C_H\rangle \\ |V\rangle |C\rangle &\longrightarrow |V\rangle |V\rangle |C_V\rangle \end{aligned} \tag{I.1}$$

then the cloning of left and right circularly-polarized states, $|L\rangle = (|H\rangle + i |V\rangle)/\sqrt{2}$ and $R = (|H\rangle - i |V\rangle)/\sqrt{2}$ fails, even in the special case $|C_H\rangle = |C_V\rangle$.

$$\begin{aligned} |L\rangle |C\rangle &\longrightarrow (|H\rangle |H\rangle |C_H\rangle + i |V\rangle |V\rangle |C_V\rangle)/\sqrt{2} \neq |L\rangle |L\rangle |C_L\rangle \\ |R\rangle |C\rangle &\longrightarrow (|H\rangle |H\rangle |C_H\rangle - i |V\rangle |V\rangle |C_V\rangle)/\sqrt{2} \neq |R\rangle |R\rangle |C_R\rangle \end{aligned} \tag{I.2}$$

where $|C_L\rangle$ and $|C_R\rangle$ are the final states of the cloning machine. The no-cloning theorem can also be proven by using the unitarity of the cloning transformation. This was done in Sec. 9-4 of Peres's textbook [8]. Let the cloning transformation be a unitary operator U such that for any state $|\phi\rangle$, $U |\phi\rangle = |\phi\rangle |\phi\rangle$. Now, since inner product is preserved under unitary operation, for any two states we should have

$$\langle\psi|\varphi\rangle = \langle\psi|U^\dagger U\varphi\rangle = \langle\psi| \langle\psi|\varphi\rangle |\varphi\rangle = \langle\psi|\varphi\rangle^2 \tag{I.3}$$

but this cannot be true unless $\langle\psi|\varphi\rangle$ is either 0, meaning that the states are orthogonal, or 1, meaning that the states are the same. Thus U cannot exist. Here the state of the cloning machine has been omitted, but including it as an ancilla will not change the result.

Even though no-cloning theorem is usually associated with the linearity of quantum mechanics and no-signalling condition, it can be shown that it and a closely related theorem called no-deletion theorem are both implications of the principle of conservation of quantum information introduced in [9] and further developed in [10]. This principle states that in a closed system, quantum information is conserved. It can also be shown that all theories that do not allow superluminal signalling and predict the violation of at least one Bell inequality have a no-cloning theorem [11].

No-cloning theorem immediately became an important part of physics due to its connection to no-signalling and amplification of light. It was also used to justify the

security of quantum cryptography from its very beginning by Bennett and Brassard in 1984 [12], where it was argued that the nonorthogonality of quantum states used in the encoding of the signal guarantee that any eavesdropping attempts will inevitably cause disturbances in the signal that can be detected, by virtue of the no-cloning theorem. The perfect cloning of noncommuting mixed states where two clones of a single unknown mixed state are created is also impossible. This result was included in [13], where it was shown that noncommuting mixed states cannot be broadcast, which is a process more general than cloning and includes it as a special case.

There is also a closely related theorem called stronger no-cloning theorem [14] that states that if we want to achieve perfect cloning by introducing some supplementary information to the process, then the clone must be created from the supplementary information alone. This means that a cloning machine that both keeps the original state intact and produces clones that contain any information about the original state does not exist - the production of clones that contain information about the original is always accompanied by a distortion of the original state. It was shown in [9] that the violation of this theorem would lead to violation of the no-cloning theorem.

The only set of input states that allows perfect cloning using only unitary operations is a known set of orthogonal states. This condition is very restrictive. Since the perfect cloning of arbitrary pure states is not possible, it is natural to ask how well one can do if one wants to clone approximately. It turns out that one can either create clones with varying but imperfect quality, as is the case with deterministic cloning where the cloning machine consists of a unitary operation only, or one can try to create a perfect clone with some probability that is less than one using probabilistic quantum cloning where a measurement is allowed in addition to a unitary operation. The first approximate quantum cloning machine (QCM) was introduced in 1996 by Bužek and Hillery [15] which could produce two reasonably good copies

out of a single two-state quantum system, or qubit, and after that a great deal of different types of QCMs were proposed, starting a new subfield of QIP. Some of the different forms of approximate quantum cloning will be presented in the next Section.

2 Different forms of approximate quantum cloning

2.1 Definition of quantum cloning

The no-cloning theorem forbids the perfect cloning of an arbitrary pure state via a unitary operation, i.e. perfect deterministic cloning of pure states. What it does allow is the perfect cloning of a state belonging to a known set of orthogonal states, or approximate cloning of other states. If we allow the cloning transformation to include a measurement in addition to a unitary operation, then we may arrive at perfect clones with some probability [16]. This is called probabilistic cloning. It should be mentioned that approximate quantum cloning is often called simply quantum cloning and approximate clones simply clones unless some ambiguity is possible.

There are so many different types of quantum cloning that it would be very difficult to present an exhaustive list of them, but briefly introducing the most common classes of them is what this Section is all about. A common feature to all proposed QCMs is the attempt to distribute the quantum information in the input state(s) to a bigger set of states. Because the information one would like to distribute is encoded in the state of a quantum system, it is subject to the laws of quantum mechanics and this naturally brings about both limitations and advantages foreign to information encoded in a classical way, as will be seen later.

A useful definition for deterministic cloning of pure states as a linear trace-preserving completely positive (TPCP) map was presented in the review by Valerio Scarani, Sofyan Iblisdir and Nicolas Gisin [2]. A linear map $T : \mathcal{H}_{in} \to \mathcal{H}_{out}$ between

two Hilbert spaces is said to be trace-preserving if $Tr(\rho) = Tr(\sigma)$ for all $\sigma = T[\rho]$ where $\rho \in \mathcal{H}_{in}$ and $\sigma \in \mathcal{H}_{out}$. It is said to be positive if it maps positive operators to positive operators, that is to say $T[\rho] \geq 0$ for all $\rho \in \mathcal{H}_{in}$, $\rho \geq 0$. Finally, it is said to be completely positive if the map $T \otimes \mathbb{I}_d$ is positive for all $d \in \mathbf{N}$ where $\mathbb{I}_d$ is the $d \times d$ identity matrix.

Scarani et al. suggested that since any interaction between two or more quantum systems, possibly mediated by an ancilla, has the effect of redistributing the quantum information between all subsystems, then a process would be determined as cloning by the form of the input state as follows:

$$(|\psi\rangle^{\otimes N}) \otimes (|0\rangle^{\otimes M-N}) \otimes |C\rangle \xrightarrow{U} |\Psi\rangle \tag{I.4}$$

where N input states and $M - N$ blank copies in initially arbitrary states together with an ancilla evolve according to a unitary operator U into a final state. Note that N must be smaller than M. This would in turn define the QCM as the linear TPCP map, or equivalently as the pair U, $|C\rangle$. In the final state the quantum information in the input state(s) is distributed in some way among all M subsystems and the ancilla, if one is used. Thus M imperfect clones have been produced from N input states. Note that this is a generalization of the common $1 \rightarrow 2$ cloning scheme to $N \rightarrow M$ case. Since this is a description of deterministic cloning, i.e. the case where a cloning machine is defined by a unitary operation and possibly an ancilla, it does not account for probabilistic cloning and some of the more novel forms of quantum cloning such as telecloning, which combines quantum cloning and quantum teleportation.

In the context of quantum cloning of binary quantum systems, the unknown input state $|\psi\rangle$ in the above definition is usually taken to be a qubit. A qubit is a two-state quantum system that has a fixed orthonormal basis called a computational basis corresponding to classical bit values 0 and 1, usually denoted by states $\{|0\rangle, |1\rangle\}$, and quantum computation is done in this basis. The d-dimensional

generalization of qubit is called qudit.

Even though the definition (I.4) includes trivial cases, such as a simple swap of states between quantum systems, the interesting cases are considered to be those that can produce clones with a good quality, preferably with the best quality allowed by the laws of quantum mechanics. When this is the case, the QCM in question is said to be optimal. But before one can decide whether a particular cloning transformation is optimal or not, one needs some figure of merit that one uses to measure the quality of clones. Fidelity is the most commonly used figure of merit in literature, and can be used to measure either single-copy fidelity, where single clones and input states are compared, or global fidelity, which compares the output state of M clones to the ideal output state that would be produced by a perfect cloner. In quantum cloning, single-copy fidelity is often referred to simply as fidelity. This thesis follows the same convention and thus all fidelities mentioned later are single-copy fidelities unless stated otherwise.

2.2 Fidelity as a figure of merit for cloning

Fidelity $F(\rho, \sigma)$ measures the closeness of different quantum states described by their respective density matrices ρ and σ. In quantum cloning, it is defined as

$$F(\rho, \sigma) = \left(\mathrm{Tr} \sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right)^2 \tag{I.5}$$

This is the expression used by Uhlmann [17] and Jozsa [18] and it is sometimes called Uhlmann fidelity. There is an alternative definition $F'(\rho, \sigma) = \sqrt{F(\rho, \sigma)}$, but it is never used in the context of quantum cloning. Fidelity (I.5) gains its maximum value of 1 when its arguments describe the same state, and minimum value of 0 when the states are orthogonal to each other. It has many properties that make it behave almost like a metric on the space of density matrices: it is non-negative and symmetric in its arguments, for example. Fidelity is not a metric, however, since it does not obey the triangle inequality and has a value of 1 rather than 0 when its

arguments are the same. It can be used to define an angle between pure quantum states which is a metric by letting $\cos(\theta_{\psi,\phi}) = F(\psi,\phi)$.

When used as a figure of merit in quantum cloning of pure states, fidelity becomes

$$F = \langle\psi|\rho|\psi\rangle \tag{I.6}$$

where ρ is the reduced density operator of one of the clones and $|\psi\rangle$ the pure input state. It measures the overlap between the states. It should be pointed out that even though the minimum value of fidelity is 0, the worst possible fidelity for a d-level clone produced by a QCM is $1/d$, corresponding to a maximally mixed state which contains no information about the input state [2]. Fidelity can be used to write the state of the clones in a simple way that describes their quality. For example, the reduced density operators of the clones produced by the first approximate cloning machine by Bužek and Hillery mentioned in the previous Section can be written in terms of the input state $|\psi\rangle$ and fidelity F as

$$\rho = F\,|\psi\rangle\langle\psi| + (1-F)\,|\psi^{\perp}\rangle\langle\psi^{\perp}| \tag{I.7}$$

where $|\psi^{\perp}\rangle$ is the state orthogonal to $|\psi\rangle$ and $F = 5/6$. Fidelity, as a figure of merit, plays an important role in the classification of QCMs. For example, the Bužek-Hillery cloning machine is said to be symmetric, because the fidelity of both clones is equal, and universal, because F is independent of the input state $|\psi\rangle$. The other feature useful in the classification of QCMs defined by I.4 is the "preferred" set of input states the QCM in question can clone well. Of greatest interest are usually optimal cloning machines, i.e. cloning machines that can clone their designated set of input states with the largest possible fidelity. Sub-optimal cloning can be sometimes preferred however, particularly in the case of experimental quantum cloning where the optimal cloning may be more difficult to realize than some sub-optimal scheme with a quality close to optimal: for example, one may use optimal state estimation to implement a measure-and-prepare cloner to approximate an $N \to M$ cloner with large M. This will be discussed more in Part 3.

How does one find bounds on fidelity for different quantum cloning schemes? No-cloning theorem simply states that perfect cloning is impossible. On the other hand, no-signalling condition, one of the reasons no-cloning theorem was first formulated, may be violated even with a non-ideal cloning machine if it is good enough [19], so it is a stronger requirement and it can be expected to provide more accurate bounds on the quality of cloning than no-cloning theorem. It did not take long after Bužek and Hillery presented their QCM in 1996 for Bruß et al. to prove that it was actually the optimal $1 \to 2$ state-independent quantum cloner for qubits two years later [20]. Their proof was not based on the preservation of no-signalling condition, but in [19] it was shown how the upper bound for fidelity in this case can be recovered by demanding that the cloning process has some intrinsic noise which prevents the use of the QCM to achieve signalling and then calculating the minimum amount of noise needed to preserve causality. Even though this simple technique alone may not be sufficient to find the optimal fidelity in other cases, as was argued in [7], it can nevertheless be used to find upper bounds on fidelity that, when saturated, prove the optimality of a cloner. A more technical approach to the problem relies on the isomorphism between completely positive maps and positive semidefinite operators and presenting it is out of the scope of this thesis, but an interested reader can look it up for example in [21].

In the case of pure finite-dimensional input states, it can be shown [22] that the optimal universal cloning transformation can only shrink the (generalized) Bloch vector representing the d-level system, or qudit, without causing any rotations. Because of this, shrinking factor η is also sometimes used as a figure of merit in quantum cloning. When considering pure input states, there exists a simple relation between fidelity and shrinking factor which allows one to recover fidelity when shrinking factor is known. It is

$$F = \frac{1}{d}(1 + (d-1)\eta) \tag{I.8}$$

The relation (I.8) is not valid for mixed input states. Also notice that in general, one cannot reverse the relation because unlike fidelity, shrinking factor is not defined for any two states. It can be shown that if one uses the clones produced by the optimal $N \to K$ UQCM as input for the optimal $K \to M$ UQCM, the overall shrinking factor is recovered by simply multiplying the optimal shrinking factors of the two cloners [20], in other words the shrinking factors of concatenated cloners multiply. When cloning mixed states, shrinking factor is used more often than fidelity because mixed state cloners that are optimal with regards to fidelity are either not known, or in some cases can even be shown to not exist. This will be elaborated on in Section 2.5.3.

2.3 Universal quantum cloning

Cloning transformations where the quality of the cloned states does not depend on the input state are called universal cloning transformations, and they are often called UQCM, short for universal QCM. Another way to define universality is to demand that the cloning machine is covariant with respect to a unitary operation [19]. The first QCM was the optimal $1 \to 2$ UQCM for qubits, producing two clones of equal fidelity from a single input state. A natural extension is the $N \to M$ qubit cloner. One was presented by Gisin and Massar [23], and it was later generalized to arbitrary finite dimension d [22, 24] and the optimal fidelity was found to be

$$F_{N\to M}(d) = \frac{N}{M} + \frac{(M-N)(N+1)}{M(N+d)} \tag{I.9}$$

which recovers the fidelity 5/6 of the optimal qubit duplicator for $d = 2$, $N = 1$ and $M = 2$. Like the Bužek-Hillery cloning machine, both of these UQCM produce clones of equal fidelity.

When the quality of all M clones is the same, the UQCM is said to be symmetric. Otherwise it is asymmetric. In the latter case, the optimality condition of the cloning

transformations can be found by trade-off relations which in the case of fidelity limit the sum of the fidelities of different clones [25].

Asymmetric quantum cloning in general is of interest particularly when analyzing the security of some quantum key distribution protocols, because the optimal eavesdropping strategy, when it is known, often turns out to coincide with optimal asymmetric cloning [26, 27] but this is not always the case [28]. This will be discussed in Part 2.

It should be pointed out that the output of the Bužek-Hillery UQCM is clearly entangled, and it can be shown that the concurrence between clone and ancilla is higher than between clones. This is related to the principle of conservation of quantum information and will be studied in Part 4.

2.4 State-dependent quantum cloning

When the quality of the clones produced by a cloning transformation depends on the input state, the cloning transformation is said to be state-dependent. Generally speaking, state-dependent cloning may produce clones of some specific set of input states with a better quality than universal cloning, but at the expense of cloning poorly other states. For example, a particular optimal state-dependent cloning machine, called phase-covariant cloning machine, can clone qubits located in the equator of the Bloch sphere better than optimal UQCM, but clones poorly qubits located near the poles. This means that if one has some partial information about the input state, one can often improve the quality of the clones by using the appropriate optimal state-dependent cloning machine instead of the optimal UQCM.

It should be pointed out that partial information about the input states does not always lead to the possibility of better cloning. For example, the optimal duplicator of the states used in six-state QKD protocol is the Bužek-Hillery UQCM. In other words, it is not possible to clone these six states better with some state-dependent

cloning machine [20]. The study of minimal input sets defining a UQCM is a closely related problem, and it was shown [29] that in the case of optimal $1 \to 2$ cloning of qubits the minimal set is four states on the vertices of a tetrahedron. On the other hand, if we wish to clone at best two arbitrary pure states of qubits $|\psi\rangle$ and $|\phi\rangle$ related by $\langle\psi|\phi\rangle = s$, then we can achieve perfect cloning for $s = 0$ and $s = 1$, and even the minimum fidelity $F_{min} \approx 0.987$, achieved when $s = 1/2$, is very high [20].

It can be shown that when looking for optimal cloners (in the sense that the worst-case global fidelity is maximized), it is sufficient to consider cloning maps that are covariant with respect to the group under which the set of input states R is invariant. Consequently, a cloning machine that optimally clones all the states $\psi \in R$ is state-independent within R [24].

2.4.1 Phase-covariant cloning

Consider a set of input states of the form

$$|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2} \tag{I.10}$$

or the equatorial qubits of the Bloch sphere. Cloning transformations whose quality does not depend on the phase ϕ are called phase-covariant. They are covariant with respect to a rotation of ϕ. The balanced superpositions of the computational basis states, i.e. states of the form

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\phi_j} |j\rangle \tag{I.11}$$

are a generalization of equatorial qubits to an arbitrary finite dimension d and respective QCM are sometimes said to be multi-phase covariant, and they a covariant with respect to all rotations of ϕ_j. Like UQCM, phase-covariant QCMs can be symmetric or asymmetric. An important difference between these two classes of cloners is that unlike in universal cloning, the optimal phase-covariant cloning transformation can depend on whether single-copy fidelity or global fidelity is considered

[30].

The first phase-covariant cloner studied was the $1 \to 2$ phase-covariant cloner for qubits that was presented in [30] as the optimal individual eavesdropping attack on the BB84 protocol and it was optimal with regards to single-copy fidelity. The optimal $1 \to M$ phase-covariant cloning for qubits was presented in [31] were single-copy fidelity was considered. In the same publication the optimal $N \to M$ phase-covariant qubit cloner was conjectured, and it was shown in [32] that the conjectured cloner was indeed optimal when N and M had the same parity, however the optimal transformation was otherwise different. The optimal $1 \to 2$ phase-covariant cloner for qudits has been investigated by several parties [33, 34, 35] and the optimal transformation has been found. To the author's knowledge, the optimal $N \to M$ phase-covariant qudit cloner has not been presented yet.

Unlike UQCM, these cloning transformations can be made economical, i.e. ancilla-free, meaning that they do not require the use of auxiliary systems. This can be desirable, since the presence of an ancilla may complicate the experimental implementation of a given QCM. Optimal economical cloning machines for equatorial qubits (symmetric and asymmetric case) have been derived and they perform with the same fidelity as their ancilla-assisted counterparts [36].

Economical optimal universal cloning is impossible [37]. Sub-optimal economical universal quantum cloning has not been studied much because the few known examples of this are considered rather uninteresting. For example, the so-called trivial amplification, where the original qubit is left unperturbed and a new qubit is produced in a random state, achieves an average fidelity of $F = 3/4$ and is both economical and universal in the sense of average single-copy fidelity. In [38] it was also argued that optimal economical realization for phase-covariant $1 \to 2$ quantum cloning is only possible for qubits, but a sub-optimal economical cloner for qudits was nevertheless constructed. In the same paper it was pointed out that the $1 \to M$

case is less restrictive and may have optimal economical realizations in dimensions higher than two.

It was pointed out in [39] that even though the optimal economical and normal phase-covariant QCM may have the same fidelity, the output states of economical and normal cloners can still be different. Specifically, the $1 \to 2$ phase-covariant quantum cloning optimal with regards to single-copy fidelity was considered, and it was shown that the clones (eqs. 193 and 194 in the reference) produced by ancilla-assisted and economical cloning transformations were clearly different, albeit having equal fidelities with the input state.

As was stated earlier, optimal state-dependent cloning may perform better than universal cloning. For example the optimal symmetric $1 \to 3$ phase-covariant QCM for qubits achieves a fidelity of $5/6$, same as that of the optimal $1 \to 2$ UQCM so in this case we can get a third clone with the same quality "for free" if we know that the input states are equatorial. As a final note, similarly how UQCM are connected to state estimation, phase-covariant QCM are connected to phase estimation, and the qubit case was studied in [40].

2.4.2 Fourier-covariant cloning

The Fourier-covariant cloner clones equally well two mutually unbiased bases (MUBs) that are discrete Fourier transforms of each other. As the name suggests, Fourier-covariant cloning transformations are covariant with respect to a Fourier-transform. It is the optimal eavesdropping strategy based on individual cloning attacks on d-dimensional generalizations of the BB84 protocol [27].

In the case of qubits, the eigenstates of the three Pauli matrices play the role of three MUBs. Specifically, if the states of two MUBs are cloned equally one gets the phase-covariant cloner for qubits. It was pointed out in [21] that because all pairs of MUBs are unitarily equivalent in a two-dimensional Hilbert space, Fourier-covariant

qubit cloner coincides with the phase-covariant qubit cloner.

The Fourier-covariant asymmetric $1 \to 2$ qutrit (three-level system) cloner was studied in [41] and was found to have a fidelity even higher than that of the optimal phase-covariant qutrit cloner, which is to be expected since the set of input states is smaller for the former cloner. The $1 \to 2$ case was extended to asymmetric cloning in arbitrary finite dimension in [27].

2.4.3 Real cloning machines

Consider the set of real superpositions of the computational basis $|j\rangle$:

$$|\psi\rangle = \sum_{j=0}^{d-1} n_j \, |j\rangle \tag{I.12}$$

where $n_j \in \mathbf{R}$ and $\sum_{j=0}^{d-1} n_j^2 = 1$. A cloning machine that clones all input states of this form equally well is called a real cloning machine. Real cloning machines were presented as a new class of symmetric $1 \to 2$ qudit cloners in [42], and the optimality of the cloning transformations was proven with the use of no-signalling condition in the same publication.

In the case of qubits, the set of real states is $a\,|0\rangle + b\,|1\rangle$ with $a, b \in \mathbf{R}$ and $a^2 + b^2 = 1$. They lie in the x-z equator of the Bloch sphere which is unitarily equivalent to the x-y equator (I.10) and thus the fidelities of the optimal phase-covariant and real cloning machines coincide. Like phase-covariant cloning machines, real cloning machines can be made economical. In fact, the cloning network used to implement the Bužek-Hillery UQCM can be used for economical $1 \to 3$ real qubit cloning with just a minor modification in the preparation of the initial state of the cloning machine [43]. In [21] the following result was presented for $1 \to 2$ cloning in higher dimensions:

$$F_{1\to2}^{Fourier-covariant} > F_{1\to2}^{Real} > F_{1\to2}^{phase-covariant} > F_{1\to2}^{Universal} \tag{I.13}$$

A partial explanation for this result is based on the respective sets of input states for these cloners: in a sense, these sets of input states contain strictly different amounts of information and the optimal cloning fidelities are thus different.

2.5 Others

2.5.1 Probabilistic quantum cloning

All cloning discussed in previous subsections was deterministic cloning of pure states, in other words, cloning defined by (I.4), but there are other forms of quantum cloning. One of them is called probabilistic quantum cloning where the cloning transformation consists of a unitary operation and a measurement, which leads to a < 1 chance to arrive at perfect clones but sometimes it fails to produce any clones.

Measurements are performed on the ancillas, which are chosen in such a way that the measurement result tells us whether the cloning process succeeded or failed. There are also probabilistic cloning schemes that can generate approximate copies that nonetheless have a fidelity larger than that of any deterministic scheme.

Probabilistic cloning was introduced in 1998 by Duan and Guo, and also by Chefles and Barnett, and it was shown that a set of linearly independent states can be perfectly copied with some probability [44, 45]. It was pointed out in [46] that the no-signalling condition restricts the number of clones produced by a probabilistic cloning machine in a given d-dimensional Hilbert space: if the cloning machine succeeds with a non-vanishing probability, then no more than d clones can be created. Probabilistic cloning was later extended to infinite continuous sets of input states in [47], where it was shown that optimal universal cloner cannot be improved by probabilistic cloning, however it can be useful when the set of input states is restricted.

Probabilistic schemes for various other QIP tasks have also been considered. The connection between probabilistic cloning and state discrimination was recognized

already in the article by Duan and Guo, and like other forms of cloning it is related to the security analysis of various QKD protocols.

2.5.2 Continuous-variable quantum cloning

Cloning of qudits, i.e. states of d-level systems where d is arbitrary but finite, is different from the case of cloning continuous-variable states such as coherent states, lying in an infinite-dimensional Hilbert space. Universal cloning of such states is not considered to be very interesting, because it can be easily shown that in the limit of a large Hilbert space dimension, fidelity (I.9) tends to N/M, which can be achieved with rather uninteresting strategies. The most studied case of continuous-variable quantum cloning is the cloning of coherent states, which was presented by Cerf et al. in [48], where a $1 \to 2$ cloning transformation that copies equally well the states of two conjugate variables was presented.

The cloning machine presented by Cerf et al. was a Gaussian cloner. This means that the reduced state of a single clone satisfies the Gaussian condition, e.g. the requirement that it is the bivariate Gaussian mixture. Gaussian continuous-variable quantum cloning has been studied extensively. The optimal fidelity of $N \to M$ Gaussian cloner for coherent states was presented in [49]. It was pointed out that this $N \to M$ Gaussian cloner can be used for optimal cloning of squeezed states as well with minor modifications. An implementation of the cloner with a phase-sensitive linear amplifier and a network of beam splitters was presented in [50].

Like with phase-covariant quantum cloning, the optimal cloning transformation depends on whether single-copy or global fidelity is used. It can be shown that the cloners that are optimal with regards to global fidelity are always Gaussian, but when M is finite, then the cloners optimal with regards to single-copy fidelity are non-Gaussian [51].

2.5.3 Mixed states quantum cloning

When using mixed input states, one is usually interested in broadcasting rather than cloning, which means that the marginal density operators of the separate systems at the output are the same as the input states to be broadcast. This is because it is possible to broadcast a mixed state ρ in such a way that the joint state is not in the product form $\rho \otimes \rho$ but the local one-copy density matrices might still be ρ because of quantum correlations or entanglement.

Even though it was shown as early as 1996 by Barnum et al. [13] that no-cloning theorem for the $1 \rightarrow 2$ case can be extended to mixed states as well, in the sense that non-commuting mixed states cannot be broadcast, the study of quantum cloning is still mostly focused on cloning pure input states. Upper bounds for global fidelity for both universal and state-dependent mixed state cloners were derived in 2003 by Rastegin [52, 53], but cloning transformations saturating these upper bounds could not be found.

Two years later, it was pointed out that the no-broadcasting of non-commuting mixed states cannot be generalized to more than one input case. The first optimal results on mixed-state quantum cloning for qubits were included in the same publication [54]. Fidelity was not used as the figure of merit, however, and the $N \rightarrow M$ UQCM presented was optimal and universal in the sense of the shrinking factor of a single output instead. It was later proved [55] that a $1 \rightarrow M$ mixed-state UQCM that is universal in the sense of fidelity does not exist. Probabilistic broadcasting of mixed input states was studied in [56].

2.5.4 Quantum entanglement cloning

Quantum entanglement is a valuable resource in QIP. It is a fully quantum mechanical phenomenon without a classical counterpart and is used in many well-known schemes such as quantum teleportation. Quantum entanglement is often studied

under local operations and classical communication, or LOCC, condition, because entanglement cannot increase under LOCC [57]. A no-go theorem similar to no-cloning theorem was presented in a publication by Koashi and Imoto [58] where it was stated that quantum entanglement cannot be freely cloned but is limited by the laws of quantum mechanics, much like the cloning of pure states.

Various schemes on cloning of entanglement were studied in [59], where it was shown that in the case of an unknown maximally entangled two-qudit state as the input state entanglement cannot be cloned perfectly. In the same paper the fidelity of an optimal $1 \rightarrow 2$ symmetric entanglement cloner universal over the set of maximally entangled $d \times d$-dimensional states was derived, which in the case of two-qubit states had the fidelity $F \approx 0.717$.

In the case of cloning of quantum states we can achieve faithful copies in the special case that the state to be cloned belongs to a known set of orthogonal states. A similar result for entanglement cloning exists [60] with the difference than LOCC constraint limits the number of orthogonal entangled states for which perfect cloning is possible. In the case of qubits, it can be shown [61] that when the state to be cloned is one of the Bell states, then perfect $1 \rightarrow 2$ cloning by LOCC is possible. Because any two Bell states can be discriminated by LOCC [62] this can be done in many ways, but in the spirit of proper cloning it is indeed possible to perfectly clone an unknown Bell state without using local discrimination. This can be done with the help of a maximally entangled ancilla and C-NOT gates. In the $1 \rightarrow 2$ case only one known state, the ancillary state, is consumed. In the sense of entanglement resource used, this C-NOT scheme is optimal.

2.5.5 Telecloning

Quantum teleportation allows the faithful transmission of an unknown quantum state between two spatially separated parties by using a maximally entangled state

as a resource. Quantum telecloning can be seen as a natural extension of this well-known scheme [63] where there is a single receiver for the unknown state. Because of no-cloning theorem, when one extends the teleportation to the case of multiple receivers, one can no longer have ideal teleported states. Optimal telecloning is of course possible, and it can be done either deterministically or probabilistically. It is possible for the sender to first use QCMs locally and then teleport the cloned states to receivers, but this is different from telecloning.

In a nutshell, the sender Alice holds an unknown one-qubit state $|\psi\rangle$ that she wishes to teleclone to M receivers, who may be assisted by ancillas. They all share a multipartite entangled state $|\Psi\rangle$ as a starting resource, which is such that after Alice performs a local measurement and informs the other parties of its result using classical communication, the receivers can each obtain an optimal copy using local rotations. This kind of optimal $1 \to M$ telecloning of qubits was studied by [64] and more general schemes of $1 \to M$ telecloning of qudits and the $N \to M$ telecloning of qubits have been presented as well [65, 66]. Both symmetric and asymmetric cases have been studied, as well as the telecloning of continuous variables [67]. Phase-covariant telecloning can be made economical [68, 69].

When the entangled state used is maximally entangled, the telecloning process is reversible because there is no loss of quantum information. The reverse process is called remote state concentration [70]. On the other hand, if nonmaximum entanglement is used then the telecloning scheme is irreversible.

2.6 Experimental quantum cloning

Early proposals of how to implement discovered cloning transformations experimentally consisted of several quantum gates, but they were not feasible. The first explicit proposal on how to experimentally realize quantum cloning was presented in 2000 by Simon, Weihs and Zeilinger [71]. It was based on stimulated emission,

and it was shown that optimal cloning could be achieved with it. It was pointed out how unavoidable spontaneous emission prevents perfect cloning. Another scheme based on parametric down-conversion was also presented in the same publication, and it was shown that optimal fidelity could be reached with it as well. In this case, intrinsic noise in the down-conversion process results in approximate clones.

Nuclear magnetic resonance (NMR) was used to implement the Bužek-Hillery UQCM in [72] with the use of a three-qubit NMR device. The probabilistic quantum cloning experimentally realized in a NMR system is reported in [73]. Universal $1 \rightarrow 2$ quantum cloning of qubits via parametric down-conversion of photons was reported in 2002 [74] and a fidelity close to optimal was achieved. In 2004 the use of a beam splitter to achieve universal $1 \rightarrow 2$ quantum cloning and universal NOT gate for polarization states of single photons was reported [75], reaching a near-optimal fidelity. It was stated that although useful in many ways, the scalability of the beam splitter scheme is not very good. Quantum cloning via cavity quantum electrodynamics (QED) using information encoded in atomic states of rubidium atoms was proposed in 2003 [76] and since then, the use of cavity QED to achieve cloning has been proposed with many different carriers of information, such as ion traps and cavity-assisted atomic interactions [77, 78].

The various quantum cloning schemes presented so far can, in principle, be implemented by any d-state quantum systems, but optical quantum cloners, that is to say quantum cloners that use photons as carriers of information, are the most studied case. This is because photons represent the ideal flying qubits: they can be transmitted over long distances, they are resilient against decoherence due to their very weak interaction with environment and qubits can be encoded into single photons in many ways. It is also possible to use the so called time-bin encoding to use photons as carriers of qudits. The bosonic nature of photons may also be useful in the experimental implementation of some cloning schemes. For example, the pro-

jection onto symmetric subspace, which is necessary in optimal universal $N \to M$ cloning, can be easily done with linear optics.

Amplification of light has played an important role in quantum cloning ever since its beginning: in the FLASH scheme mentioned earlier, a perfect optical quantum cloner was employed. A natural way to realize optical quantum cloning is indeed via amplification of light. Cloning can be done using stimulated emission where the medium emits photons in the same state as the input photons. Phase-covariant cloning is of great interest here, because it has optimal economical implementations which make the implementation of the cloning transformation simpler by removing the need to have an ancilla, see for example [79] and [80] where optics system and NMR system were used, respectively. Some have even suggested that phase-covariant cloning of photons can lead to compound systems visible to human eye [81] where tens of thousands of photons are produced at the output. Continuous-variable quantum cloning can be realized using linear beam splitters and homodyne detection, as was proposed and demonstrated in [82] where a $1 \to 2$ Gaussian cloner was presented achieving a fidelity very close to optimal.

It should be pointed out that in experimental quantum cloning, the definition of fidelity is different but analogous to the definition (I.6), and is related to the relative frequency of clones and noise [83]. For a good review on optical quantum cloning, an interested reader should see the review by Cerf and Fiurasek [21].

Part II

Universal quantum cloning

In this Part, universal quantum cloning will be discussed. After sketching the basics the simplest case of creating two imperfect clones from a single pure input state will

be analysed using the quantum circuit formalism. In the next Section, the Bloch sphere formalism, spin flipping transformation and its connection to cloning will be presented. The last Section concerns with the connection between cloning and quantum cryptography.

3 Basic idea

When considering the deterministic cloning of pure states and fidelity as the figure of merit, UQCM are those cloning transformations in (I.4), defined by unitary operator U and ancilla $|C\rangle$, where fidelity (I.6) is independent of the input state $|\psi\rangle$. They can be further classified by considering the dimension d of the Hilbert space where state $|\psi\rangle$ lies, the number of input states N and clones M, whether the fidelity of all M clones is the same (symmetric case) or not (asymmetric case) and whether the upper bound for fidelity allowed by quantum mechanics is saturated by the UQCM in question (optimal case) or not. They have been studied extensively and results exist for optimal symmetric $N \to M$ UQCM in arbitrary finite dimension d [22].

Generally speaking, all deterministic $N \to M$ cloning transformations are TPCP linear maps $T : \mathcal{H}^{\otimes N} \longrightarrow \mathcal{H}^{\otimes M}$, and according to a well-known theorem by Kraus [84], any such map can be implemented by appending an ancilla to the system, let the whole undergo a unitary evolution, then trace out the ancilla. This is described in Fig. 1. In the case of optimal $1 \to 2$ universal qudit cloning, it has been rigorously proved that the cloning transformation must always be ancilla-assisted [37, 38] and all known optimal $N \to M$ qudit cloners require $M - N$ ancillary qudits. After the ancilla has been traced out, the information encoded in the input state of N identical qudits can be found in the output state of M clones, distributed evenly if the cloner is symmetric. To be precise, some of the information will also be distributed to the ancillary states in the unitary transformation. This will be discussed in Section 5.

The optimal universal case is special not only because all known cloners are

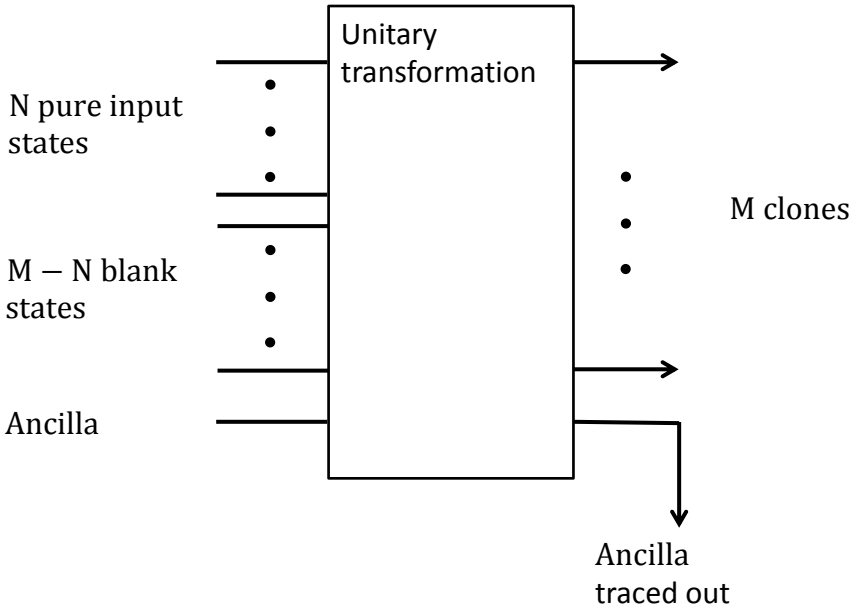

Figure 1. A deterministic $N \to M$ quantum cloning machine. The intial states of the blank copies and ancillae together can be regarded as the initial state of the cloning machine.

ancilla-assisted, but also because the optimality of a universal cloning transformation does not depend on whether single-copy or global fidelity is considered [22]. This becomes important when one takes a look at the optimality proofs of general symmetric UQCM introduced in the previous chapter. The one presented by Gisin and Massar is indeed the optimal symmetric $N \to M$ universal qubit cloner, but in the original publication, only numerical proof for optimality was presented. Because the input state has N qubits in identical states, it is invariant under the permutation of the individual qubits and consequently the input state belongs to the symmetric subspace of N qubits, $\mathcal{H}_+^N$. An analytical proof that relied on the assumption that the output state belongs to the symmetric subspace $\mathcal{H}_+^M$ was presented by Bruß et al. [20] but this assumption, while easily shown to be true when some global figure of merit is considered, is difficult to verify in the case of single-copy fidelity and was only a conjecture at the time.

The optimality proof and an extension of the Gisin-Massar cloner to arbitrary

finite dimension d were presented in the excellent publication by Keyl and Werner [22], where it was shown that the optimal symmetric UQCM for qudits is a TPCP map $T : \mathcal{H}_+^N \longrightarrow \mathcal{H}_+^M$ regardless of the figure of merit considered. The T presented is elegant and also an intuitive one. The output density matrix ρ_M of M clones produced from N d-level systems is of the form

$$\rho_M = T[\rho_N] = \lambda S_M(\rho_N \otimes \mathbb{I}^{\otimes(M-N)})S_M \tag{II.1}$$

where the normalization factor

$$\lambda = \frac{dim(\mathcal{H}_+^N)}{dim(\mathcal{H}_+^M)}; \quad dim(\mathcal{H}_+^N) = \frac{(d+N-1)!}{N!(d-1)!} \tag{II.2}$$

preserves the trace, S_M is the projector from $\mathcal{H}^{\otimes M}$ to $\mathcal{H}_+^M$, $\rho_N = (|\psi\rangle\langle\psi|)^{\otimes N}$ is the input state of N original qudits in pure state ψ and $\mathbb{I}$ is the $d \times d$ identity matrix. It should be pointed out that up to a constant, S_M is just the sum of all possible permutations of M pure states. A natural way to interpret this result is that the unknown information, originally carried in ρ_N, is distributed among $M - N$ blank qudits and N input qudits in a completely symmetric way. It was pointed out in [2] that it is the quantum symmetrization that distinguishes optimal universal cloning from trivial schemes.

Another important property of optimal universal cloning of qudits is that the cloning transformation can only cause shrinking of the vector representing the state in a generalized Bloch vector picture. Thus it can be said that optimal universal cloning transformations are isotropic [85].

An illustrative example of the use of the cloning map (II.1), as well as the $1 \rightarrow 2$ UQCM in quantum circuit formalism, will be presented in Section 4.1. In this simplest case, the optimal universal quantum cloning can be achieved by a combination of the identity transformation and state swap, in other words, it is of the form $|\psi\rangle_1 |0\rangle_2 |C\rangle_C \longrightarrow c_1 |\psi\rangle_1 |\Psi\rangle_{2C} + c_2 |\psi\rangle_2 |\Psi\rangle_{1C}$ where c_1 and c_2 are constants. It is a straightforward exercise to generalize this result to any values of N and M

with the help of cloning map (II.1). This also makes it easy to see how any form of deterministic cloning can be thought of as distribution of quantum information encoded in N pure input states to M states.

The fidelity of clones in the output state of Werner's cloning map, optimal for arbitrary values of d, N and M, is

$$F_{N\to M}(d) = \frac{M(N+1)+N(d-1)}{M(N+d)} \tag{II.3}$$

Another symmetric $N \to M$ UQCM for qudits, also saturating the optimal fidelity bounds, was presented by Fan et al. [86] as a unitary transformation on the orthogonal normalized basis $|\mathbf{n}\rangle$ of $\mathcal{H}_+^N$, and a set of $M-N$ ancillary qudits. The output density matrix ρ_M can be obtained by writing the N identical pure input states in terms of $|\mathbf{n}\rangle$ and then applying the transformation and tracing out the ancillary states as usual. This was shown to be equivalent to Werner's cloning map (II.1) by Wang et al. [87] who also proposed a unified UQCM, constituted by pure input states and the $M-N$ prepared maximally entangled states acting as both blank states and ancillary states. The cloning transformation of this unified UQCM is always realized by symmetric projection. It was shown to be equivalent to (II.1) and it was also suggested that it could be adjusted to different asymmetric UQCM and perhaps even to the presently absent general asymmetric UQCM. There is an interesting connection between symmetric UQCM and state estimation, as well as between asymmetric UQCM and quantum cryptography. The former will be explored in Part III, and the latter in this Part.

4 $1 \to 2$ case, cloning network

4.1 The Bužek-Hillery UQCM

The task of distributing equally the information carried in an arbitrary pure state of a single qubit to states of two qubits as well as possible in such a way that

the process performs equally well for all pure input states can be achieved with the Bužek-Hillery UQCM mentioned in Part I. Consider an orthonormal basis $|0\rangle$ and $|1\rangle$ of the two-dimensional Hilbert space. The explicit form of the cloning transformation is

$$\begin{aligned} U|0\rangle_1|0\rangle_2|0\rangle_C &= \sqrt{\frac{2}{3}}|0\rangle_1|0\rangle_2|0\rangle_C + \sqrt{\frac{1}{6}}(|0\rangle_1|1\rangle_2|1\rangle_C + |1\rangle_1|0\rangle_2|1\rangle_C) \\ U|1\rangle_1|0\rangle_2|0\rangle_C &= \sqrt{\frac{2}{3}}|1\rangle_1|1\rangle_2|1\rangle_C + \sqrt{\frac{1}{6}}(|0\rangle_1|1\rangle_2|0\rangle_C + |1\rangle_1|0\rangle_2|0\rangle_C) \end{aligned} \tag{II.4}$$

where the sub-indexes 1, 2 and C refer to the input state, blank copy and ancilla, respectively. Consider an arbitrary normalized pure input state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and its orthogonal complement $|\psi^\perp\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$. By linearity and using the identity $|1\rangle|0\rangle - |0\rangle|1\rangle = |\psi\rangle|\psi^\perp\rangle - |\psi^\perp\rangle|\psi\rangle$ it can be shown that $|\psi\rangle$ will be transformed as

$$U|\psi\rangle_1|0\rangle_2|0\rangle_C = \sqrt{\frac{2}{3}}|\psi\rangle_1|\psi\rangle_2|\psi^\perp\rangle_C - \sqrt{\frac{1}{6}}(|\psi\rangle_1|\psi^\perp\rangle_2|\psi\rangle_C + |\psi^\perp\rangle_1|\psi\rangle_2|\psi\rangle_C) \tag{II.5}$$

The output state ρ_{out} of the cloning machine, which is the state of the compound system of the two clones, can be obtained by tracing out the ancilla from the r.h.s. of the above transformation. Then one gets

$$\rho_{out} = \frac{2}{3}(|\psi\rangle\langle\psi|)^{\otimes 2} + \frac{1}{6}(|\psi\rangle|\psi^\perp\rangle + |\psi^\perp\rangle|\psi\rangle)(\langle\psi|\langle\psi^\perp| + \langle\psi^\perp|\langle\psi|) \tag{II.6}$$

This output state can be recovered from the map (II.1) by letting $d = 2$, $N = 1$ and $M = 2$. The normalization factor (II.2) is then $\lambda = \frac{2}{3}$, and the projector S_2, that maps states from the Hilbert space of two qubits to its symmetric subspace $\mathcal{H}_+^2$, can be written in terms of the identity operator $\mathbb{I}^{\otimes 2}$ and the permutation operator $\mathcal{P}$ as $S_2 = \frac{1}{2}(\mathbb{I}^{\otimes 2} + \mathcal{P})$, where $\mathcal{P}|ij\rangle = |ji\rangle$. By inserting λ and S_2 into (II.1), one gets $T[\rho_1] = \rho_2 = \rho_{out}$ as expected.

From this output state, we can obtain the global fidelity achieved by the Bužek-Hillery UQCM:

$$F_{global} = {}^{\otimes 2}\langle\psi|\rho_{out}|\psi\rangle^{\otimes 2} = \frac{2}{3} \tag{II.7}$$

To obtain the single-copy fidelity, one needs to trace out one of the two clones from (II.6), getting the single-copy density matrix that can be written in terms of $|\psi\rangle$ and $|\psi^{\perp}\rangle$ or equivalently in terms of $|\psi\rangle$ and the completely mixed density matrix in two dimensions, $\mathbb{I}/2 = \frac{1}{2}\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$:

$$\rho_1 = \rho_2 = \frac{5}{6}\,|\psi\rangle\,\langle\psi| + \frac{1}{6}\,|\psi^{\perp}\rangle\,\langle\psi^{\perp}| = \frac{2}{3}\,|\psi\rangle\,\langle\psi| + \frac{1}{3}\frac{\mathbb{I}}{2} \tag{II.8}$$

Now it is easy to obtain the fidelity

$$F = \langle\psi|\,\rho_1\,|\psi\rangle = \frac{5}{6} \tag{II.9}$$

which is equal for both clones because this UQCM is symmetric. Both fidelities are optimal. While the optimality for the Bužek-Hillery UQCM has been proven by many authors, the optimality also follows from the fact that the output (II.6) can be recovered from the cloning map (II.1), which is optimal for arbitrary finite values of d, N and M. As shown in (II.8), the density matrix of a clone can be written in the form $\eta\,|\psi\rangle\,\langle\psi| + (1-\eta)\frac{\mathbb{I}}{d}$ and the shrinking factor η caused by the Bužek-Hillery UQCM is found to be 2/3. It can also be recovered from relation (I.8).

If one looks at the state of the ancilla after the cloning transformation by tracing out the degrees of freedom of the clones, one gets

$$\rho_C = \frac{1}{3}\,|\psi\rangle\,\langle\psi| + \frac{2}{3}\,|\psi^{\perp}\rangle\,\langle\psi^{\perp}| = -\frac{1}{3}\,|\psi\rangle\,\langle\psi| + \frac{4}{3}\frac{\mathbb{I}}{2} \tag{II.10}$$

Clearly, the ancilla also contains some information about the input state $|\psi\rangle$ and also about $|\psi^{\perp}\rangle$. In the context of quantum cloning, the state $|\psi^{\perp}\rangle$ is called the anticlone, and the anticlone in the output state of the Bužek-Hillery UQCM is actually the optimal anticlone that can be obtained from a single unknown pure state $|\psi\rangle$. Anticloning will be discussed in more detail in Section 5.

4.2 Cloning network

One way to realize the Bužek-Hillery UQCM is to use a suitable quantum circuit that acts as a cloning network. Here the work of Bužek, Hillery and Bednik [95] is

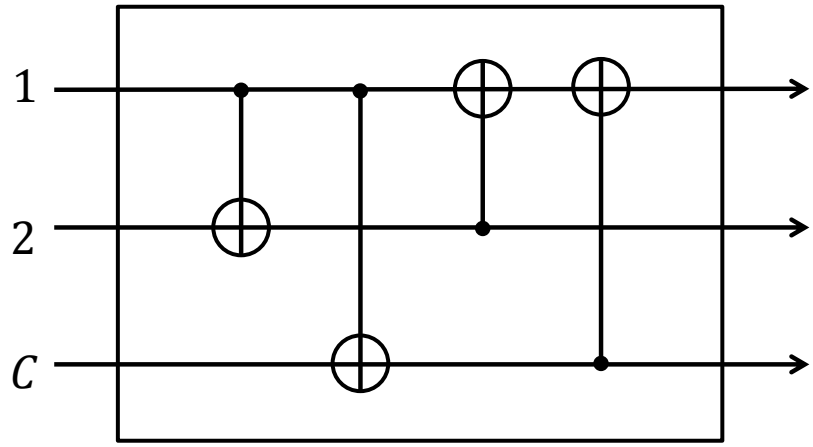

Figure 2. The quantum circuit that can be used as a cloning network by preparing the qubits 2 and C appropriately with qubit 1 being in an unknown pure state. Black dot is the control qubit and $\oplus$ the target qubit.

followed. If the blank state qubit 2 and ancillary qubit C are prepared in a specific way, then this can be done with a sequence of four C-NOT gates. Consider two states $|x\rangle$ and $|y\rangle$ in the computational basis, i.e. $|x\rangle, |y\rangle \in \{|0\rangle, |1\rangle\}$. The action of the C-NOT gate is a two-qubit operator P_{ij}, such that

$$P_{ij} |x\rangle_i |y\rangle_j = |x\rangle_i |x \oplus y\rangle_j \tag{II.11}$$

where $\oplus$ is addition modulo two. Qubit i is said to be the control qubit and qubit j the target qubit. The quantum circuit that can be used for optimal universal $1 \to 2$ quantum cloning is presented in Fig. 2. Its action on states $|x\rangle_1 |y\rangle_2 |z\rangle_C$ in the computational basis is

$$|x\rangle_1 |y\rangle_2 |z\rangle_C \longrightarrow |x \oplus y \oplus z\rangle_1 |x \oplus y\rangle_2 |x \oplus z\rangle_C \tag{II.12}$$

If qubit 1 is our unknown pure state that we would like to clone, then by a clever choice of preparation for qubits 2 and C it is easy to see that the quantum circuit in Fig. 2 becomes a cloning network. It is easy to verify that this quantum circuit can act as both the identity on qubit 1 and swap the state of 1 into qubit 2 with

the following choices for the prepared states of qubits 2 and C:

$$|\psi\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 |0\rangle_C + |1\rangle_2 |1\rangle_C) \longrightarrow |\psi\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 |0\rangle_C + |1\rangle_2 |1\rangle_C) \tag{II.13}$$

$$|\psi\rangle_1 \frac{1}{\sqrt{2}}(|0\rangle_2 |0\rangle_C + |0\rangle_2 |1\rangle_C) \longrightarrow |\psi\rangle_2 \frac{1}{\sqrt{2}}(|0\rangle_1 |0\rangle_C + |1\rangle_1 |1\rangle_C) \tag{II.14}$$

The correct preparation for qubits 2 and C is now obvious: a coherent superposition of the identity (II.13) and state swap (II.14) will result in cloning:

$$\begin{aligned} &|\psi\rangle_1 (\frac{a}{\sqrt{2}}(|0\rangle_2 |0\rangle_C + |1\rangle_2 |1\rangle_C) + \frac{b}{\sqrt{2}}(|0\rangle_2 |0\rangle_C + |0\rangle_2 |1\rangle_C)) \\ \longrightarrow\ &|\psi\rangle_1 \frac{a}{\sqrt{2}}(|0\rangle_2 |0\rangle_C + |1\rangle_2 |1\rangle_C) + |\psi\rangle_2 \frac{b}{\sqrt{2}}(|0\rangle_1 |0\rangle_C + |1\rangle_1 |1\rangle_C) \end{aligned} \tag{II.15}$$

The real parameters a and b control how the information is distributed and must satisfy $a^2 + ab + b^2 = 1$ for the state of the compound system of qubits 2 and C to be normalized. If $b = 1$ all information from qubit 1 is transferred to qubit 2 while if $b = 0$ all information stays in qubit 1. In the general case, the fidelities of the resulting clones are

$$F_1 = 1 - \frac{b^2}{2}; \quad F_2 = 1 - \frac{a^2}{2} \tag{II.16}$$

For the symmetric case one needs to choose $a = b = \frac{1}{\sqrt{3}}$, and then the fidelity of Bužek-Hillery UQCM, or equivalently the fidelity of Werner's cloning map for $N = 1$, $M = 2$, $d = 2$, will be recovered which proves that the cloning network is optimal when $a = b$.

If the three-qubit state is initially $|\psi\rangle_1 |0\rangle_2 |0\rangle_C$ we can use the quantum circuit presented in Fig. 3 consisting of three single-qubit rotations $R_j(\theta)$ and two C-NOT gates, a well-known network for the preparation of an arbitrary two-qubit state, to prepare the qubits 2 and C in the correct entangled state

$$|\Psi\rangle_{2C} = (2|0\rangle_2 |0\rangle_C + |0\rangle_2 |1\rangle_C + |1\rangle_2 |1\rangle_C)/\sqrt{6} \tag{II.17}$$

or the superposition of (II.13) and (II.14) for $a = b = \frac{1}{\sqrt{3}}$. The action of the single-qubit rotation on the computational basis states is

$$R_j(\theta)|0\rangle_j = \cos\theta |0\rangle_j + \sin\theta |1\rangle_j; \quad R_j(\theta)|1\rangle_j = -\sin\theta |0\rangle_j + \cos\theta |1\rangle_j \tag{II.18}$$

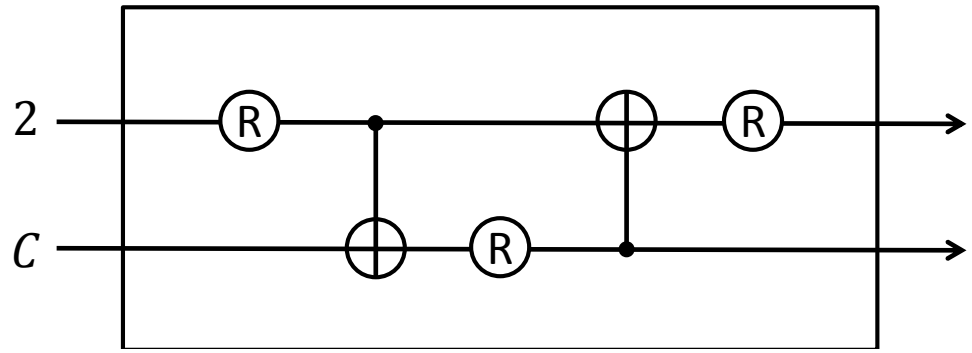

Figure 3. The preparation network that can be used to prepare the qubits 2 and C in any desired two-qubit state by choosing the three single-qubit rotations appropriately.

where $j \in 2, C$. The action of the preparation circuit in Fig. 3 on a two-qubit state $|0\rangle_2 |0\rangle_C$ is

$$|0\rangle_2 |0\rangle_C \longrightarrow R_2(\theta_3) P_{C2} R_C(\theta_2) P_{2C} R_2(\theta_1) |0\rangle_2 |0\rangle_C \tag{II.19}$$

To prepare the state $|\Psi\rangle_{2C}$, we need to solve for the correct values of rotations. One set of such angles (in radians) is

$$\theta_1 = -\cos^{-1}\sqrt{\frac{1}{2} - \frac{1}{2\sqrt{5}}};\ \theta_2 = \cos^{-1}\left(\frac{\sqrt{5}-1}{2\sqrt{3}}\right);\ \theta_3 = -\cos^{-1}\sqrt{\frac{1}{2} - \frac{1}{\sqrt{5}}} \tag{II.20}$$

4.3 Generalizations

If one wishes to keep the amount of input states and clones fixed to 1 and 2, respectively, the Bužek-Hillery UQCM can be generalized in a few ways: by extending to qudits or asymmetric cloning (or both). In the latter case, they are sometimes called quantum information distributors.

The optimal symmetric $1 \to 2$ UQCM for qudits can be recovered from Werner's cloning map (II.1) and the corresponding fidelity can be recovered from (II.3):

$$F_{1\to 2}(d) = \frac{d+3}{2(d+1)} \tag{II.21}$$

From this fidelity, it is easy to see that in the limit of a large Hilbert-space dimension, the optimal $1 \to 2$ cloning fidelity approaches $1/2$, which can be achieved by trivial strategies. Consequently, the universal cloning of continuous variables has received very little attention.

The asymmetric $1 \to 2$ qubit cloning has been studied extensively. One way to implement it is the quantum circuit approach by Bužek et al. presented in Section 4.2. The authors showed that the shrinking factors of the two clones produced by the cloning network using arbitrary values of parameters a and b saturated a trade-off relation that can be equivalently given in terms of fidelity and is called the no-cloning inequality:

$$\sqrt{(1-F_1)(1-F_2)} \geq \frac{1}{2} - (1-F_1) - (1-F_2) \tag{II.22}$$

It is a straightforward exercise to verify that the fidelities (II.16) satisfy the no-cloning inequality (II.22) and are therefore optimal. The quantum circuit approach was later extended to asymmetric universal qudit and continuous variable cloning in [96] where the term quantum information distributor was used to describe this family of universal quantum cloners. It was shown that the same quantum circuit with minor modifications can be used to achieve the task in qudit case as well, but optimality was proven only later by different authors in [97]. The optimal fidelities for qudits are

$$F_1 = 1 - \frac{(d-1)b^2}{d}; \quad F_2 = 1 - \frac{(d-1)a^2}{d} \tag{II.23}$$

where a and b must satisfy $a^2 + \frac{2ab}{d} + b^2 = 1$.

5 Spin flips and anticloning

5.1 Difference between parallel and antiparallel two-spin states

Consider the two-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^2$. The pure states in $\mathbb{C}^2$ form a one-dimensional subspace, which can be geometrically represented using the Bloch sphere. It is a unit sphere with each point corresponding to a pure state and each pair of antipodal points corresponding to mutually orthogonal states. The standard basis states $|0\rangle$ and $|1\rangle$ are usually chosen to be the north and the south pole, respectively.

The point in the Bloch sphere corresponding to an arbitrary pure state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is recovered by letting

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle \tag{II.24}$$

where the polar angle $\theta \in [0, \pi]$ and the azimuthal angle $\phi \in [0, 2\pi]$. This is described in Fig. 4. The angles ϕ and θ specify the Bloch vector $\overrightarrow{r} = (x, y, z)$ of the state where $x = \sin\theta\cos\phi$, $y = \sin\theta\sin\phi$ and $z = \cos\theta$. The Bloch vector of a pure state is always a unit vector. The interior of the Bloch sphere corresponds to mixed states, which are expressed using their Bloch vector and the 2×2 identity matrix $\mathbb{I}$ as $\rho = \frac{1}{2}(\mathbb{I} + \overrightarrow{r} \cdot \overrightarrow{\sigma})$ with $\overrightarrow{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, where σ_i are the Pauli spin matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}; \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{II.25}$$

Consider now a spin-$\frac{1}{2}$ particle polarized along $\overrightarrow{n}$. It is described by a pure state $|\overrightarrow{n}\rangle$, corresponding to the projector $|\overrightarrow{n}\rangle\langle\overrightarrow{n}| = \frac{1}{2}(\mathbb{I} + \overrightarrow{n} \cdot \overrightarrow{\sigma})$.

When one wants to estimate the space direction $\overrightarrow{n}$ from a single spin-$\frac{1}{2}$ particle as well as possible, it is clear that states $|\overrightarrow{n}\rangle$ and $|-\overrightarrow{n}\rangle$ are equally good: the same measurements can be performed and the only difference is that in the case of $|-\overrightarrow{n}\rangle$

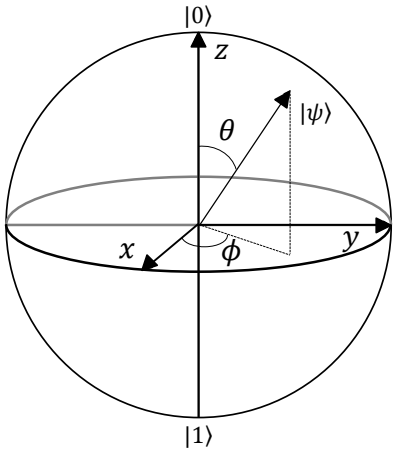

Figure 4. The Bloch vector representation of a pure state $|\psi\rangle$.

the opposite space direction is guessed. An interpretation of this is that the two states contain an equal amount of information about the space direction $\overrightarrow{n}$.

The situation changes if a two-spin state is used. When all different directions are a priori equally likely, then the optimal measurements for the pairs of parallel [98] and antiparallel [99] spins to estimate $\overrightarrow{n}$ have different fidelities: $F_{\parallel} = 3/4$ and $F_{\perp} \approx 0.789$. This is a consequence of the entanglement required by the optimal measurements. A similar result holds for the cloning of antiparallel spins: an optimal $|\overrightarrow{n}, -\overrightarrow{n}\rangle \to |\overrightarrow{n}\rangle^{\otimes M}$ cloning machine achieves higher fidelity than the optimal $2 \to M$ qubit cloner when $M > 6$ [100]. Thus, it would seem that there is more information in $|\overrightarrow{n}, -\overrightarrow{n}\rangle$ about a random space direction $\overrightarrow{n}$ than in $|\overrightarrow{n}, \overrightarrow{n}\rangle$. One explanation of this is that vector $|\overrightarrow{n}, \overrightarrow{n}\rangle$ is invariant under permutations of the measurement sites where the two spin-$\frac{1}{2}$ particles are measured, i.e. it belongs to the 3-dimensional symmetric subspace $\mathcal{H}_{+}^{2}$ while the antiparallel spin states span the whole 4-dimensional Hilbert space $\mathcal{H}^{\otimes 2}$ of two-spin states.

This difference between parallel and antiparallel two-spin states was first reported by Gisin and Popescu in their 1999 publication, where they also showed that flipping a spin of unknown polarization, which would make it possible to measure the parallel and antiparallel states in the same way by simply flipping the second spin first,

cannot be done. Their result, and a publication on universal NOT-gates by Bužek, Hillery and Werner [101], sparked an interest in universal spin-flip and anti-cloning machines which will be discussed next.

5.2 Universal spin-flip and anti-cloning machines

Let $|\overrightarrow{n}\rangle$ be an arbitrary spin-$\frac{1}{2}$ state. Consider maps $|\overrightarrow{n}\rangle \longrightarrow |-\overrightarrow{n}\rangle$ and $|\overrightarrow{n}\rangle \longrightarrow |\overrightarrow{n}, -\overrightarrow{n}\rangle$, which would be the perfect universal spin flip machine and anti-cloning machine, respectively. Both can be done only approximately or probabilistically with a probability that is less than one, because of the no-flipping theorem [102]:

There exists no unitary operation that can flip an arbitrary state or a state drawn from a set of three or more states that do not lie in a great circle of the Bloch sphere.

An intuitive version of the no-flipping theorem is that because unitary operations correspond to proper rotations of the Bloch sphere, the set of qubits lying on any great circle of the Bloch sphere can clearly be complemented by a single rotation of π around a suitable axis. On the other hand, no rotation can implement a point symmetry, which is what a perfect universal spin flip machine would do since the points on the surface of the Bloch sphere corresponding to states $|\overrightarrow{n}\rangle$ and $|-\overrightarrow{n}\rangle$ are antipodes of each other.

Although at first glance similar to no-cloning theorem presented in Part I, there is actually a stark difference between the theorems: two known non-orthogonal states can always be flipped perfectly with a single unitary transformation, and a unitary transformation is guaranteed to exist that can flip any state drawn from a set of states lying on a great circle of the Bloch sphere, such as the equatorial states.

It is easy to see that an operator that would perfectly flip an arbitrary qubit is not unitary but anti-unitary. The rest of the theorem can be proved by using linearity and the requirement of unitarity for flipping transformations. It can also be shown that both no-signalling condition and non-increase of entanglement under

LOCC imply that a unitary operation that could flip three or more qubits not lying on a great circle of the Bloch sphere cannot exist [102].

Following the lesson of no-cloning theorem, approximate spin-flip and anticloning machines have been studied. The optimal universal quantum spin-flip machine was already included in the publication by Gisin and Popescu, and the corresponding fidelity was found to be 2/3, which coincides with the average fidelity of the measurement of spin direction $\overrightarrow{n}$ where one measures the qubit $|\overrightarrow{n}\rangle$ in a randomly chosen basis.

An anti-cloning machine which takes as input an arbitrary qubit $\frac{1}{2}(\mathbb{I} + \overrightarrow{n} \cdot \overrightarrow{\sigma})$ and produces states $\frac{1}{2}(\mathbb{I} + \eta\overrightarrow{n} \cdot \overrightarrow{\sigma})$ and $\frac{1}{2}(\mathbb{I} - \eta\overrightarrow{n} \cdot \overrightarrow{\sigma})$ at the output, where η is the shrinking factor caused by the anti-cloning transformation, was studied and shown to be optimal by Hardy and Song [103], achieving a shrinking factor of 1/3 which corresponds to a fidelity of 2/3, the same as that of the optimal spin-flip machine.

Because the optimal fidelity for both universal spin-flipping and universal anti-cloning can be reached in a measurement-based scheme, where classical information of the qubit is extracted, it is possible for one to prepare as many optimal anticlones as one wants from a single unknown qubit without a decrease in fidelity. This is fundamentally different from optimal quantum cloning, where a fidelity higher than that of measurement is achieved and where additional clones cannot be produced without a decrease in cloning fidelity.

Both spin-flipping and anti-cloning can be done probabilistically, but the probabilistic anticloner is restricted by the no-signalling condition: in a d-dimensional Hilbert space, no more than d clones can be created by the probabilistic anticloner [103]. This can be shown by following the argument in [46] where it was shown how a probabilistic quantum cloner is also restricted by no-signalling.

5.3 Relation to universal NOT-gate

A classical NOT gate complements bits, i.e. it changes 0 to 1 and vice versa. Its quantum mechanical counterpart V would complement qubits: $V|\psi\rangle = |\psi^{\perp}\rangle$. By noticing that the points on the surface of the Bloch sphere corresponding to the orthogonal qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $\psi^{\perp} = \alpha^{*}|1\rangle - \beta^{*}|0\rangle$ are antipodes of each other, it is clear that V is actually the same operation as the spin-flip operation which was already stated to be antiunitary and thus not physical.

An optimal U-NOT gate for qubits that produces an approximation of the output $|\psi^{\perp}\rangle^{\otimes M}$ from an input $|\psi\rangle^{\otimes N}$ was presented by Bužek, Hillery and Werner [101]. Similarly to the optimal spin-flip machine, it was shown that the optimal fidelity can be achieved in a measurement-based scheme. A direct consequence of this is that the optimal fidelity

$$F_{N\to M}^{U-NOT} = \frac{N+1}{N+2} \tag{II.26}$$

of the anticlones depends only on N and coincides with the average fidelity of the optimal state estimation from N copies. In the same publication it was also shown that the gate can be realized as a by-product of a suitable optimal UQCM by tracing out the clones instead of the ancillary states, generalizing the result of the optimal anticlone in the ancilla of the Bužek-Hillery UQCM.

In [47], it was pointed out that since complex conjugation is well defined for any dimension d, the U-NOT gate can be generalized to qudits by noting that the state $|\psi^{\perp}\rangle$ is unitarily equivalent to the state $|\psi^{*}\rangle$ and looking for transformations that approximate the map $\psi^{\otimes N} \longrightarrow \psi^{*} \equiv \psi^{\perp}$. Like before, the optimal fidelity can be achieved in a measurement-based scheme and is thus equal to the average fidelity of the related optimal state estimation. It is

$$F_{N\to M}^{U-NOT}(d) = \frac{N+1}{N+d} \tag{II.27}$$

The experimental implementation of the U-NOT gate achieving fidelities close to optimal have been reported in optics system [104].

6 Cryptography connection

6.1 Quantum key distribution

One particular advantage that quantum information has over classical information is that it can be used to establish secure communication between a sender Alice and a receiver Bob without restricting a possible eavesdropper Eve by anything but the laws of physics, even in the presence of some non-idealities arising from practical implementation[1] [88, 89]. This can be achieved by using a quantum key distribution (QKD) protocol, see Fig. 5, where a random secret key that can be used in cryptographic applications is distilled from quantum mechanically correlated classical information shared by Alice and Bob. Any eavesdropping attempts will in principle be detected because the so-called signal states Alice uses to encode her data are chosen to be non-orthogonal, and consequently cannot be distinguished perfectly. Because of this, eavesdropping inevitably causes perturbations. From the amount of perturbation detected, Alice and Bob can estimate the amount of information leaked to Eve and use classical error correction and privacy amplification protocols to create a secret key that Eve has no information of. The reason why the quantum channel is used to transmit information that will only be used to establish a key is because eavesdropping cannot be detected before the signal has been transmitted to Bob, and consequently privacy can be ensured only afterwards, not in advance. Because of this and the fact that direct communication over a quantum channel, or so called quantum secure direct communication, suffers from a lossy or noisy channel much more than a QKD protocol it has received much less interest than QKD.

The basic idea of a so called "prepare and measure" QKD protocol using qubits in two MUBs goes as follows. First Alice and Bob choose a set of non-orthogonal

[1] Usually the term "unconditional security" is used, but this term can be misleading since most security proofs still limit Eve in some ways, for instance allow Eve to only make some specific kind of attacks, and the somewhat vague use of the term has been criticized.

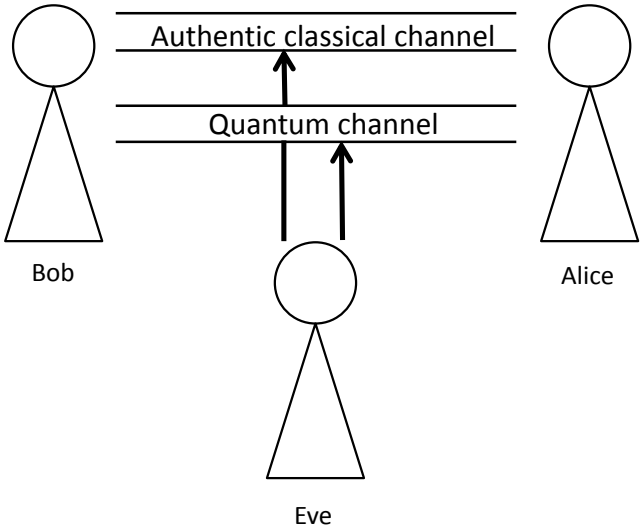

Figure 5. Alice transmits the non-orthogonal signal states to Bob over a quantum channel. Authentic classical channel is used for public communication between Alice and Bob. Eve can freely listen to the classical channel and intercept or send states in the quantum channel.

states (while security can be achieved with just two signal states [90], most QKD protocols use more) that will be used as signal states. Alice sends N qubits, each one in a randomly chosen basis, to Bob through a quantum channel, who measures the incoming qubits also in a randomly chosen basis. Because there are two possible choices for the basis, on average Bob uses the same basis as Alice half the time, measuring the incoming qubit correctly. Next Alice announces the basis used through a classical channel, and Bob discards the bits he measured in incorrect basis. Bob is now left with approximately $N/2$ bits, which constitute the raw key. After estimating the error of the raw key by comparing some random string of bits with Alice over the classical channel, Bob can either use classical error correction and privacy amplification algorithms to create the secret key from the raw key, or discard the raw key and start over if the error is too large.

In order to ensure security, certain conditions must be satisfied. The classical channel must be authentic: Eve can freely listen to it, but if she had complete control over it security would obviously be compromised. Eve must also be isolated from

both Alice and Bob, because even the most sophisticated QKD protocol might fail if Eve is looking over Alice's shoulder. Alice and Bob also need to be able to trust their random number generators and other devices to operate in the way specified by the protocol they are using. They also need to be able to establish an upper bound to the amount of information leaked to Eve, and this is where the study of optimal eavesdropping attacks becomes important.

6.2 Optimal eavesdropping

The goal of optimal eavesdropping is to optimize the trade-off between obtaining most classical information and causing the least disturbance in the original signal state [91]. Knowing the optimal eavesdropping strategy for a given QKD protocol is very important because it is part of its security analysis: it is necessary for Alice and Bob to correctly bound the information Eve has from the amount of perturbation in the quantum channel [92].

The optimal eavesdropping strategy depends on the QKD protocol under study and also on what kind of attacks Eve is allowed to do. The simplest case are the so called incoherent attacks, where Eve attacks each system individually and always uses the same strategy, and has to carry out her measurements before classical post-processing. If Eve can delay all measurements until classical post-processing is over but otherwise attacks as before, her attack is called collective. The most general attack is called a coherent attack.

One possible choice for Eve is to use an asymmetric $1 \to 2$ quantum cloner to clone the intercepted signal state and then keep one clone for herself and send the other clone to Bob. In some cases, the optimal eavesdropping attack turns out to be an optimal cloner. For example, the most dangerous attack against BB84 protocol is the phase-covariant quantum cloner [30] presented in Section 2.4.1, while the optimal eavesdropping strategy against six-state protocol is the optimal UQCM [20],

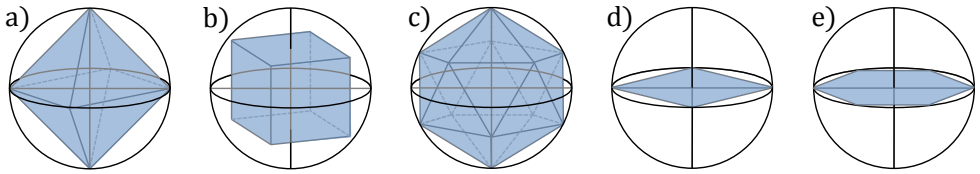

Figure 6. Representation of pure signal states related to UQCM: (a) regular octahedron (b) cube (c) regular icosahedron. Representation of pure signal states related to phase-covariant cloning machine: (d) square (e) regular hexagon. Note that in addition to using these signal states, the QKD protocol and classical post-processing protocols must be equipped with sufficient symmetries for these cloners to be the optimal attacks. See [28] for more information.

presented in Section 2.3. More generally, if Eve is restricted to quantum cloning, then the optimal eavesdropping strategy is the optimal asymmetric cloner and depends on the set of signal states used by Alice and Bob.

The connection of optimal eavesdropping and optimal cloning for protocols using qudits as signal states was studied by Ferenczi and Lütkenhaus [28] and it was found that in general, optimal attack is not optimal cloning. More specifically, protocols using 2, d and $d+1$ MUBs, where d is a prime, were analyzed and it was shown that for protocols with 2 and $d+1$ MUBs the optimal attack is an optimal cloner while the optimal attack for a protocol with d MUBs is not. In the same publication criteria to identify QKD protocols with different signal states but same optimal attack was given and as an example, different QKD protocols with either phase-covariant or universal cloner being the optimal attack were presented. Some examples are illustrated in Fig. 6 as regular shapes inside the Bloch sphere with the pure states located at the vertices.

6.3 Considerations on practical QKD

It is important to understand that the unconditional security proved for various QKD protocols is different from absolute security – the exact conditions specified in

the security proof must be met for the proof to be valid. Taking into account the non-idealities of a physical implementation is necessary in order to prove the security of any realistic QKD scheme. Specifically, many existing security proofs assume that the quantum devices can be trusted to operate as specified; however any deviations from these specifications may introduce loopholes in security. A dramatic example of this is the reported perfect eavesdropping of a running QKD protocol by Gerhardt et al. [93] where the complete key was acquired by Eve without leaving any traces of eavesdropping by taking advantage of a loophole in the photon detectors used by Alice and Bob. Existing QKD protocols may also be vulnerable to so-called Trojan attacks by a malicious manufacturer or a saboteur [94].

Part III

Optimal state estimation

In this Part optimal state estimation (OSE) and its connection to quantum cloning will be discussed. In the first section the basics of OSE will be sketched and in the second the cloning connection will be presented and briefly discussed.

7 Optimal state estimation basics

In quantum state estimation, one tries to estimate an unknown d-level input state ρ_i, drawn from a known continuous set of d-level states, by extracting classical information from ensemble $\rho_i^{\otimes N}$ via measurements. After the measurements have been carried out, a guess state $\rho_i^{\#}$ is prepared according to the measurement results by using a reconstruction rule. This is presented in Fig. 7. A score function $f : \mathbb{C}^d \times \mathbb{C}^d \longrightarrow \mathbb{R}$ is used as a figure of merit to evaluate the quality of the state estimation scheme by comparing the guess state with the original. Usually the score

function is monotonous and assigns a higher score when the guess state is closer to the original state. In the standard setup, we know the dimension d, number of identically prepared states N and the continuous set of input states as well as the prior probability distribution of states in the set, and must find the optimal measurement and reconstruction rule to maximize the average value of the score function.

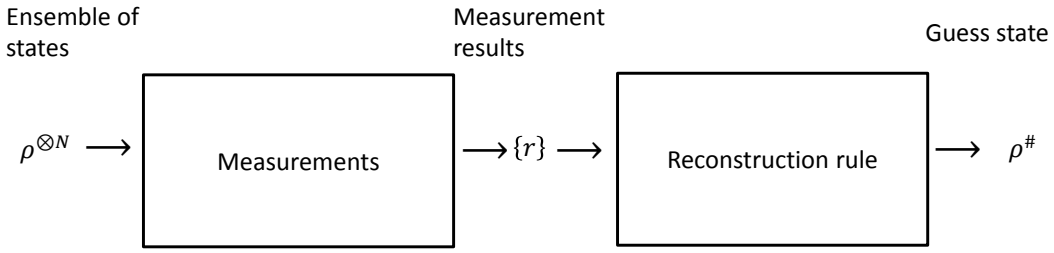

Figure 7. The setup of quantum state estimation. Classical information in the form of measurement results is extracted from the ensemble of states, each identical to the unknown input state, and a guess state is prepared according to these results via a reconstruction rule. The goal is to get a guess state as similar as possible to the original state.

If N is finite, then one cannot learn the state perfectly because of the well-known no-measuring theorem, which states that it is not possible to measure the state of a single quantum system: any single measurement one can carry out will only yield an eigenstate of some observable, which carries very little information about the state in question, namely, that it is not orthogonal to the eigenstate measured. Thus, an unknown state cannot be perfectly estimated simply because states are not observables. It is clear that as N grows larger, one can estimate the state better and at the limit $N \longrightarrow \infty$ one should be able to estimate it perfectly. Thus a natural requirement for any good state estimation scheme is that it achieves perfect estimation at this limit, and in this case the scheme is said to be consistent. In OSE the average score is maximized, and when input states and guess states are both pure, the optimal scheme is the same for all symmetric and monotonous figures of merit,

which can be shown by using the no-signalling condition: if unknown pure states could be discriminated, superluminal communication would become possible [105].

A very closely related but different problem is quantum state discrimination (QSD). The key difference is that in QSD, the set of possible states is finite. A particular strategy in QSD is quantum hypothesis testing, where the number of measurement outcomes is equal to the number of different input states and each outcome corresponds to a guess identical to one of the input states. Then a natural score function with a clear physical interpretation is the probability that the guess is correct. It should be mentioned that similarly to how a state drawn from a known set of orthogonal states can be perfectly cloned, it can also be perfectly discriminated. Otherwise perfect cloning, as well as discrimination, is not possible [106].

The situation is different in OSE. The guess states cannot be the possible states because now the set of possible states is infinite and any realistic scheme should have a finite number of possible measurement outcomes, and thus also of guess states. Also the score function should be different because on average, the guess state is never exactly the same as the original state because in OSE the number of possible input states is infinite.

The most general measurement we are able to carry out on the ensemble $\rho_i^{\otimes N}$ is described by a positive operator valued measure (POVM), which is a set of positive hermitian operators $\{O_r\}$ satisfying $\sum_r O_r = \mathbb{I}$, where $\mathbb{I}$ is the identity operator. Each operator in the set corresponds to a measurement outcome. The probability to get the result r associated with the operator O_r when the input state is ρ_i and we are working with the ensemble $\rho_i^{\otimes N}$ is

$$p_r(\rho_i) = Tr(O_r \rho_i^{\otimes N}) \tag{III.1}$$

Because the operators constituting the POVM are positive and hermitian, the probabilities (III.1) are positive and real, and the completeness condition ensures that they add up to 1, as they should. To make use of these measurement outcomes we

need to establish a reconstruction rule $r \to \rho_r^{\#}$ which tells us which guess state to produce based on the measurement results. Then the average guess state $\bar{\rho}_i^{\#}$ for a given input state ρ_i is just the mixture of possible guess states weighted with their respective probabilities:

$$\bar{\rho}_i^{\#} = \sum_r p_r(\rho_i)\rho_r^{\#} \tag{III.2}$$

Notice that the average guess state (III.2) depends on both the POVM and the reconstruction rule used. To find the optimal POVM and reconstruction rule, which are generally not unique [40], we need to know the prior probability distribution of the possible states as well as the score function. Then we can maximize the average of the score function by varying both $\{O_r\}$ and $\rho_r^{\#}$ over all possible input states ρ_i weighted by their respective probabilities. As a concrete example, we will consider OSE of pure states with average fidelity as the figure of merit.

Suppose that the input state is a qudit $\rho_i = |\psi_i\rangle \langle\psi_i|$, drawn from a continuous set of states and we estimate it by measuring the ensemble $\rho_i^{\otimes N}$. Now the averaged fidelity over the prior probability distribution and all possible outcomes is defined as

$$\bar{F}_N = \sum_i p(\psi_i) \langle\psi_i| \bar{\rho}_i^{\#} |\psi_i\rangle \tag{III.3}$$

where $p(\psi_i)$ is the prior probability distribution of input states and the summation stands symbolically for integration over a suitable measurable set corresponding to the set of input states. The goal of OSE is to maximize average fidelity (III.3) by finding the optimal POVM and the corresponding optimal reconstruction rule.

Most results in OSE have been derived in the case where it is assumed that the states are uniformly and randomly distributed in the set of possible states, making every state equally important. If all states are estimated with the same average fidelity, the OSE scheme is said to be universal (otherwise it is said to be state-dependent). Universality is a reasonable requirement if we suppose that we know nothing else of the original state than its dimension and that it is pure.

A simple case is universal OSE from N qubits, where the possible input qubits are randomly and uniformly distributed in the Bloch sphere. The optimal average fidelity is

$$\bar{F}_N^{Universal}(2) = \frac{N+1}{N+2} \tag{III.4}$$

which tends to 1 when N tends to infinity, as expected. This was shown in [98] by first deriving the optimal fidelity of a reduced version of the problem, which can only be equal or larger than what can be achieved in the general setup, and then showing that it can be achieved by a POVM consisting of an infinite continuous set of operators. In the same paper it was shown that the optimal measurements that achieve this fidelity must be collective: a guess based on any kind of local measurements performed on individual quantum systems will fall short from the optimal one.

A more general case was investigated in [40], and an algorithm which gives the optimal finite POVM with regards to average fidelity was presented. It was shown that a POVM constructed by this algorithm is the optimal one for a general finite-dimensional quantum system. The universal OSE of qubits as well as OSE of equatorial qubits were constructed as examples.

Bruß and Macchiavello [20] derived the optimal average fidelity for qudits by using the connection between cloning and state estimation, and it was found to be

$$\bar{F}_N^{Universal}(d) = \frac{N+1}{N+d} \tag{III.5}$$

and it was also shown that like clones produced in universal cloning, in universal state estimation the average guess state (III.2) can be written in terms of a shrinking factor and the original pure state, meaning that when considering the averaged result from many trials of universal OSE of a fixed unknown input state, the guess state will tend to a shrunk form of the input state vector. As a related result, they showed how the optimal shrinking factor of a more general input state supported in

the symmetric subspace is upper bounded by the optimal shrinking factor of pure states.

OSE from a single coherent state drawn from a set of coherent states $\{|\alpha\rangle\}$ distributed in phase space according to a Gaussian distribution $p(\alpha) = \lambda/\pi exp(-\lambda|\alpha|^2)$ has been investigated [107], and the optimal average fidelity was found to be

$$\bar{F}_1^{Gaussian} = \frac{1+\lambda}{2+\lambda} \tag{III.6}$$

which also tells us that in the case of a flat distribution, or in the limit $\lambda \longrightarrow 0$, the optimal fidelity is 1/2. The optimal phase estimation of squeezed vacuum states and coherent states from an ensemble of such states has also been studied [108] in terms of average Holevo variance.

In a manner similar to cloning, we can call the kind of OSE presented so far deterministic because a guess state can always be prepared. If we allow inconclusive results, it is possible to achieve higher fidelity for the guess states but then the probability of producing a guess state is less than unity – this is called probabilistic OSE. It was stated previously in Part I that the fidelity of universal cloning cannot be improved by any probabilistic scheme. The same holds for probabilistic OSE, which cannot improve the fidelity of universal OSE but may be useful in state-dependent OSE where the set of possible states is restricted. It should be emphasized that the fidelity considered here is a conditional one: it is the average fidelity of the state estimation on the condition that we did not get the inconclusive result. As the conditional average fidelity grows higher, so does the probability of getting an inconclusive result [109].

As was mentioned previously, collective measurements are necessary in OSE. However, they may be difficult to carry out in an experiment. Thus the study of suboptimal schemes which use local measurements is of interest [110]. In particular, it can be shown [111] that local measurements can be asymptotically optimal, in the sense that in the limit of large N their fidelity approaches unity as fast as the

optimal one.

8 Connection to cloning

In the previous section we saw that no-measuring theorem forbids the perfect estimation as well as discrimination of unknown states. This limitation could be easily circumvented with a perfect UQCM: with it, it would be possible to prepare an arbitrary number of perfect clones of the original unknown state and then use any consistent state estimation scheme to acquire full knowledge of the state. Also, if perfect state estimation was possible, we could circumvent the no-cloning theorem by perfectly estimating the unknown state to be cloned and then prepare as many copies as we wanted. Thus, the violation of one of the theorems leads to the violation of the other.

This simple observation shows that there is a connection between OSE and optimal cloning. This connection can be made stronger by considering the optimal fidelities of the two. It can be shown that in the case of pure states and universal fidelity, the following is true:

$$F_{N\to\infty}^{Cloning}(d) = F_N^{OSE}(d) \tag{III.7}$$

In words, the optimal fidelity of the asymptotic UQCM, or $N \to M$ UQCM where $M \longrightarrow \infty$, is equal to OSE from N qudits. The proof presented in [20] was based on concatenating an OSE process with cloning to prove that the fidelity of OSE must be upper bounded by the corresponding optimal cloning fidelity and then concatenating cloning with OSE to show that the optimal cloning fidelity is upper bounded by OSE fidelity, which means that the two optimal fidelities are equal. It should be emphasized that the proof assumes that the prior probability distribution of the input qudits is uniform.

The equality of optimal cloning and OSE fidelities in the case of a uniform prior

probability distribution was also rigorously proven in the case of equatorial qubits [112]. In the case of equatorial qubits, the term phase estimation is often used because by knowing the phase of an equatorial qubit it is determined completely. The proof was based on a similar strategy of concatenating phase estimation with cloning and vice versa.

In the general case, it is easy to prove that for any set of equally likely input states, the OSE fidelity is upper bounded by the optimal cloning fidelity – one way to realize asymptotic cloning from N states is to use state estimation to extract classical information of the input state, enabling us to prepare as many guess states as we desire, but it is clear that the fidelity of these guess states cannot be better than the fidelity of the clones produced by the optimal $N \to \infty$, simply because then the cloner would no longer be optimal.

It might seem plausible that the opposite must be true as well, namely, that asymptotic cloning cannot perform better than OSE, but it was pointed out by Bae and Acin [113] that this assumption is unjustified because of quantum correlations between the clones produced by a cloning machine.

In OSE, one learns classical information about an unknown state one is estimating. This is not the case in quantum cloning, where the state remains unknown even after the cloning process because the information remains in the quantum states at the output. A well-known result is that the output of a QCM is highly entangled. Bae and Acin argued that if the output state was in a product form, we could learn the input state from the output of an asymptotic UQCM because a UQCM can only shrink the Bloch vector, and thus we could learn the direction regardless of what the shrinking factor was. In practice this is not possible because the entanglement of the output state is actually the worst possible for state estimation [114].

The main result of their publication, however, was the rigorous proof that the fidelities of optimal asymptotic cloning and of state estimation are indeed equal

for any (known) initial ensemble of pure states and their proof was based on the monogamy of quantum correlations and the properties of the so-called entanglement breaking channels. In fact, they proved that in the case of pure states, asymptotic optimal cloning is effectively OSE, and the equivalence of the fidelities trivially follows. To the author's knowledge, no results of the equality of asymptotic cloning and OSE in the case of mixed or continuous variable input states exist, but in the former case one should compare shrinking factors instead of fidelities since fidelity is poorly suited for a figure of merit in the cloning of mixed states.

Aside from the cloning connection, there is also a strong connection between OSE and optimal U-NOT gates presented in Section 5: one way to realize an optimal U-NOT gate is to first perform OSE on the input state and then prepare a state orthogonal to the guess state. Consequently, the fidelities of OSE and optimal U-NOT gates coincide.

Part IV

Further aspects of cloning

In this Part, the information dynamics in quantum cloning will be briefly sketched. First the role of ancilla will be discussed. Next, the optimal fidelities of universal cloning and universal OSE will be used to demonstrate conservation of extractable classical information in universal cloning as well as conservation of total Bloch vector length in the qubit case. As a unitary transformation on pure input states, UQCM conserves the total information, but some of it will turn into entanglement in the cloning process. This will be investigated in the third Section, where the entanglement in the output of Bužek-Hillery UQCM will be considered and the results are used to show that it obeys a complementarity relation between local and nonlocal

information.

9 Role of ancilla

Werner's cloning map (II.1) describes deterministic and symmetric optimal UQCM with the tensor product of N identical d-dimensional pure states at the input and $M > N$ optimal d-dimensional clones at the output. It can be thought of as a TPCP linear map $T : \mathcal{H}_+^N \longrightarrow \mathcal{H}_+^M$ between the symmetric subspaces of the input and output.

According to results presented in Part II, any TPCP linear map may be realized as a unitary transformation by tensoring the input with an ancilla in a specified state, applying a unitary transformation on the compound system and then tracing out the ancilla. In particular, Werner's cloning map may be realized as a unitary transformation on the compound system of N copies of the pure input qudit, $M-N$ blank copies and $M-N$ ancillary qudits [86, 87]. The blank copies and the ancillary states each belong to a Hilbert space with the same dimension as that of the input state. While the blank copies are necessary to carry the cloned states after the cloning transformation, the ancillary states are needed to extend the Hilbert space of the input in order to make the transformation unitary and thus physical.

In Part II, the impossibility of economical $1 \to 2$ optimal UQCM for qudits was mentioned. In short, the impossibility of economical $1 \to 2$ UQCM can be shown by considering an isomorphism between the TPCP linear map corresponding to the cloner and a certain positive semidefinite operator S, which can be defined by applying the cloning map to half of a maximally entangled two-qudit state while keeping the other half unchanged. Then S is the resulting mixed quantum state. The cloning map, and thus also the cloning fidelity, can then be expressed as linear functions of S, the input state and clones. This leads to a definition of another positive semidefinite operator R, which is a sum of integrals of input state and

clones over the possible input states. The cloning fidelity can then be expressed as a trace of operator SR, and the maximum achievable cloning fidelity is upper bounded by the maximum eigenvalue r_{max} of operator R. It is then straightforward to show that no unitary transformation on two qudits exists in $d \geq 2$ which leads to optimal eigenvalue r_{max}.

This eigenvalue criterion was first presented in [37] where $1 \rightarrow 2$ cloning of qubits were considered, and later generalized to $1 \rightarrow 2$ cloning of qudits in [38]. Both S and R depend on the cloning map considered and in the case of equatorial qubits, optimal $1 \rightarrow 2$ cloning can be made ancilla-free. In fact, to date it is the only known case of optimal economical $1 \rightarrow 2$ cloning. In the more general $N \rightarrow M$ case economical cloning is known to become possible for some other cloners as well. For example the cloning circuit described in Section 4 can be used to implement economical $1 \rightarrow 3$ cloning of real states with just a minor modification in the preparation stage of the three input qubits [43].

While all known optimal universal $N \rightarrow M$ qudit cloners use $M - N$ ancillary qudits, no rigorous proofs have been published about the impossibility of economical implementations of these cloners. Also, it has not been studied whether $M - N$ is the absolute minimum number of ancillary states. It would seem that this is so.

In cloning, some of the information in the input states will be distributed to the ancillary states. In the qubit case it is known that optimal $N \rightarrow M$ universal cloning may be done in such a way that after the cloning transformation the ancillary qubits are pairwise separable and carry the optimal anticlones of the original pure state with a fidelity given by eq. (II.26) [101]. The deep reason why this is possible seems to be connected to conservation of total information in quantum cloning, as will be argued in the next subsection.

The compound system of $M - N$ blank copies and ancilla can also be regarded as a program for quantum processor U, the unitary operation implementing the

cloning transformation. This is because U can always be done when the compound system of originals, blank copies and ancillary states has the correct dimension but generally the blank copies and ancillary states need to be prepared in a specific state, or correct program for U, in order to implement cloning.

An example of this is the cloning network presented in Section 4, which can act in many ways depending on the preparation of the blank copy and ancilla. It was already mentioned earlier that in addition to universal cloning, it can be used to implement economical $1 \to 3$ cloning of real states. Aside from cloning, it can be used as a swap or identity network.

10 Conservation laws

10.1 Conservation of classical information

Consider a qubit $|\psi\rangle$ randomly drawn from the set consisting of all pure states with a uniform distribution over the Bloch sphere. If one wishes to prepare M approximate clones of the state using ensemble $\rho^{\otimes N}$, where $\rho = |\psi\rangle\langle\psi|$ and $N < M$, one may use either a measure-and-prepare strategy, consisting of first optimally estimating the state and then preparing the M approximate clones according to the estimation result, or quantum cloning. The former can be regarded as a classical scheme to achieve the task, because in measurements, classical information is extracted from the ensemble and thus measure-and-prepare schemes may be considered classical channels. In contrast, no classical information is extracted in quantum cloning.

If no other a priori information about the state is available, then the optimal way to estimate it from ensemble $\rho^{\otimes N}$ is to use universal OSE presented in Part III. Then the average guess state is described by the density operator $\bar{\rho}^{\#}$ which can be written in terms of ρ and the completely mixed state $\mathbb{I}/2$ as

$$\bar{\rho}^{\#} = \bar{\eta}_N^{OSE}\rho + (1 - \bar{\eta}_N^{OSE})\frac{\mathbb{I}}{2} \tag{IV.1}$$

where $\bar{\eta}_N^{OSE}$ is a shrinking factor

$$\bar{\eta}_N^{OSE} = \frac{N}{N+2} \tag{IV.2}$$

describing the average shrinking of the Bloch vector in the state estimation process. This shrinking factor can be interpreted as representing the optimal (average) amount of classical information about the state $|\psi\rangle$ that can be extracted from ensemble $\rho^{\otimes N}$ via measurements, and it is also the optimal shrinking factor that can be achieved by a measure-and-prepare cloner. Its classical nature is reflected on the fact that the shrinking factor (IV.2) is independent of the number of clones M.

The quantum strategy employs the optimal $N \to M$ UQCM for the task. Because universal cloning transformations are isotropic, they can only shrink the Bloch vector representing $|\psi\rangle$. The state of a single clone after the cloning transformation is

$$\rho_{clone} = \eta_{N,M}^{UQCM}\rho + (1 - \eta_{N,M}^{UQCM})\frac{\mathbb{I}}{2} \tag{IV.3}$$

where the shrinking factor $\eta_{N,M}^{UQCM}$ can be written in terms of $\bar{\eta}_N^{OSE}$ as

$$\eta_{N,M}^{UQCM} = \bar{\eta}_N^{OSE} + \frac{2N}{M(N+2)} \tag{IV.4}$$

The additional term is always positive, and can therefore be interpreted as the quantum gain per clone from N input states:

$$\delta_{N,M} \equiv \eta_{N,M}^{UQCM} - \bar{\eta}_N^{OSE} = \frac{2N}{M(N+2)} \tag{IV.5}$$

It tends to zero at the asymptotic limit of large M, reflecting the fact that at the asymptotic limit of many clones, the classical and quantum strategies coincide in the sense that single-copy fidelity of the clones coincides with the average fidelity of OSE. The maximum value of quantum gain (IV.5) is 1/3, and it can be reached with either the Bužek-Hillery UQCM or the optimal symmetric $2 \to 3$ UQCM. The shrinking factors are compared in Fig. 8.

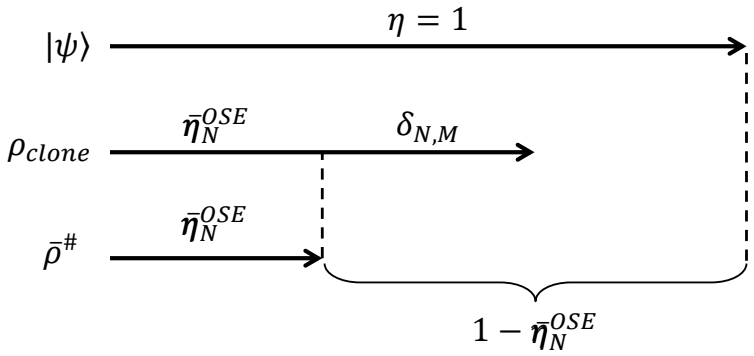

Figure 8. A comparison of shrinking factors in optimal cloning and OSE. The shrinking factor of the pure input state is 1, corresponding to no shrinking. The optimal shrinking factor of a clone is always larger than the average OSE shrinking factor $\bar{\eta}_N^{OSE}$ and can be expressed as the sum of $\bar{\eta}_N^{OSE}$ and a quantum gain $\delta_{N,M}$. At the limit of large M quantum gain vanishes and the shrinking factors coincide, while at the limit of large N both tend to unity. The factor $1 - \bar{\eta}_N^{OSE}$ is related to a loss of information in the estimation process.

One may define the total quantum gain δ_N^{tot} of an $N \to M$ UQCM for qubits as the sum of the quantum gains of all M clones, which is just

$$\delta_N^{tot} \equiv M \times \delta_{N,M} = \frac{2N}{N+2} \tag{IV.6}$$

Because δ_N^{tot} only depends on the number of input states, it can be interpreted as corresponding to the optimal amount of additional information about the state $|\psi\rangle$ in ensemble $\rho^{\otimes N}$ that can be distributed among clones when the quantum strategy is used. Thus a fidelity higher than that of a classical prepare-and-measure scheme can be achieved. In the special case $N = 1$ it is easy to verify that it coincides with the loss of information in estimation, i.e. the following holds for all optimal symmetric 1-to-M UQCM for qubits:

$$\delta_1^{tot} = 1 - \bar{\eta}_1^{OSE} \Leftrightarrow \delta_1^{tot} + \bar{\eta}_1^{OSE} = 1 \tag{IV.7}$$

however δ_N^{tot} is always greater than $1 - \bar{\eta}_1^{OSE}$ when $N > 1$. In fact, the total quantum gain in ensemble $\rho^{\otimes N}$ is exactly N times the average loss of information in OSE. Thus by defining total quantum gain per input qubit δ_N as

$$\delta_N \equiv \frac{\delta_N^{tot}}{N} = \frac{2}{N+2} \tag{IV.8}$$

one arrives at the following conservation law, valid for arbitrary values of N and $M > N$:

$$\delta_N = 1 - \bar{\eta}_N^{OSE} \Leftrightarrow \delta_N + \bar{\eta}_N^{OSE} = 1 \tag{IV.9}$$

While total quantum gain δ_N^{tot} has a clear interpretation as the total gain in fidelity that can be achieved from ensemble $\rho^{\otimes N}$ by keeping information in quantum form throughout the process, the meaning of factor δ_N is at this point still unclear. To clarify this, the qudit case will be investigated next.

The average shrinking factors of universal OSE from N qudits and the corresponding optimal $N \to M$ UQCM can be recovered from optimal fidelities (III.5) and (II.3) using the relation (I.8). The former is found to be

$$\bar{\eta}_N^{OSE}(d) = \frac{N}{N+d} \tag{IV.10}$$

and the shrinking factor of the corresponding optimal $N \to M$ UQCM can again be expressed in terms of $\bar{\eta}_N^{OSE}(d)$ as

$$\eta_{N,M}^{UQCM}(d) = \bar{\eta}_N^{OSE}(d) + \frac{dN}{M(N+d)} \tag{IV.11}$$

and now one may again define a quantum gain per clone from the ensemble of N qudits as

$$\delta_{N,M}(d) = \frac{dN}{M(N+d)} \tag{IV.12}$$

and from it, total quantum gain $\delta_N^{tot}(d) \equiv M \times \delta_{N,M}(d)$ as well as total quantum gain per input qudit $\delta_N(d) \equiv \frac{\delta_N^{tot}(d)}{N}$. Like before, it is easy to verify that the following is true for arbitrary values of d, N and $M > N$:

$$\delta_N(d) + \bar{\eta}_N^{OSE}(d) = 1 \tag{IV.13}$$

In other words, in optimal cloning the total quantum gain per input qudit is always equal to the average loss of information in OSE regardless of dimension d and the number of input and output states. Thus this conservation law implies that

in optimal universal quantum cloning, the amount of extractable classical information is conserved. This of course means that *the information contents in the input and output of Werner's cloning map are equal*: one may never gain any additional knowledge about an a priori unknown pure state by cloning it, because all of the information in the optimal clones was already in the input state.

This statement was implicit in the observation of Bruß et al. [115] that optimal $N \to M$ cloning can be achieved by either using the optimal $N \to M$ UQCM, or any number of intermediate steps where at each step an optimal cloner is used. This follows from their result stating that the shrinking factors of concatenated cloners multiply and means that the information contents in the input of N pure states and output of $M > N$ optimal clones are always equal in the sense that we may produce $K > M$ clones from either the input or the output with same optimal fidelity.

This equality in information contents can be extended to OSE. From the result of Bruß et al. it follows that the shrinking factors of an optimal $N \to \infty$ UQCM and a cloning transformation consisting of an optimal $N \to M$ UQCM followed by optimal $M \to \infty$ UQCM coincide. The latter can also be thought of as an optimal UQCM that takes as input the compound system of M optimal clones created from the ensemble of N pure input states:

$$\eta_{N,\infty}^{UQCM}(d) = \eta_{N,M}^{UQCM}(d) \times \eta_{M,\infty}^{UQCM}(d) = \eta_{Mclones,\infty}^{UQCM}(d, N) \tag{IV.14}$$

Notice that the last shrinking factor depends also on N because this affects the quality of the M clones. Because of eq. (III.7), the above equation also means that

$$\bar{\eta}_N^{OSE}(d) = \eta_{Mclones,\infty}^{UQCM}(d, N) \tag{IV.15}$$

It is clear that OSE from the compound system of M optimal clones must achieve a shrinking factor at least as good as the optimal $M \to \infty$ cloner with the same input, because otherwise the state estimation scheme would not be optimal. Thus one has

$$\bar{\eta}_{Mclones}^{OSE}(d, N) \geq \eta_{Mclones,\infty}^{UQCM}(d, N) \tag{IV.16}$$

On the other hand, the shrinking factor of OSE cannot be greater than that of cloning because otherwise the cloner would not be optimal. This means that

$$\bar{\eta}^{OSE}_{Mclones}(d,N) \leq \eta^{UQCM}_{Mclones,\infty}(d,N) \tag{IV.17}$$

and thus by combining eqs. (IV.15), (IV.16) and (IV.17), one sees that the following is valid for arbitrary values of N, M and d:

$$\bar{\eta}^{OSE}_{N}(d) = \bar{\eta}^{OSE}_{Mclones}(d,N) \tag{IV.18}$$

In words, the same average shrinking factor is achieved in OSE from either the input or the output of an optimal $N \to M$ UQCM, and this can be interpreted as meaning that the amount of extractable classical information does not change in optimal deterministic universal cloning.

It is also possible to show by using conservation law (IV.13) that when taking into account the ancillary states at the output the total Bloch vector length is conserved in optimal universal cloning and this will be done next.

10.2 Conservation of total Bloch vector length

Consider the Bužek-Hillery UQCM discussed in Section 4. It takes as input a qubit in an arbitrary pure state. The Bloch vector representing this pure input state has a length of 1, corresponding to a shrinking factor $\eta_{in} = 1$. At the output, there are two clones, given by eq. (II.8), and the ancilla, given by eq. (II.10). The states of all three subsystems at the output can be expressed in the form $\eta \left|\psi\right\rangle \left\langle\psi\right| + (1-\eta)\frac{\mathbb{I}}{2}$, and thus from these equations we may recover the shrinking factors of the clones and the ancilla, which are $\eta_1 = \eta_2 = \frac{2}{3}$ and $\eta_C = -\frac{1}{3}$, where subindices 1 and 2 refer to clones and subindex C refers to the ancilla. Now one has

$$\eta_1 + \eta_2 + \eta_C = 1 \tag{IV.19}$$

which is valid for all pure input qubits, because the cloning machine is universal.

Consider now the generalization of the Bužek-Hillery UQCM to optimal $N \to M$ cloning, described in [101]. It has N pure input states and at the output, M clones and $N-M$ ancillary qubits. According to the results presented in Section 5.3, each of the $N-M$ ancillary qubits is an optimal anticlone of the input state after the cloning transformation. Thus one has

$$\eta_N^{anc} = -\eta_N^{U-NOT} \tag{IV.20}$$

Since the optimal shrinking factor of U-NOT may be achieved in a measurement-based scheme, it coincides with $\bar{\eta}_N^{OSE}$. The shrinking factor of the clones is given by eq. (IV.4). Now it is easy to see that the total length of the Bloch vector is conserved:

$$\begin{aligned}\sum \eta_{in} &= N = N(\delta_N + \bar{\eta}_N^{OSE}) = N\bar{\eta}_N^{OSE} + \delta_N^{tot} = (N+M-M)\bar{\eta}_N^{OSE} + M\delta_{N,M} \\ &= M(\bar{\eta}_N^{OSE} + \delta_{N,M}) + (N-M)\bar{\eta}_N^{OSE} = M\eta_{N,M}^{UQCM} + (M-N)\eta_N^{anc} = \sum \eta_{out}\end{aligned} \tag{IV.21}$$

The above equation also offers a partial explanation as to why optimal anticlones may be created in universal cloning in the first place: the total information in the anticlones is exactly the amount of information in $\rho^{\otimes N}$ that will not be distributed among clones in optimal cloning. This would also suggest that $M-N$ is the maximum number of optimal anticlones that can be created in optimal $N \to M$ cloning.

One may try to extend the result (IV.21) to arbitrary finite dimension d. By noticing that the optimal fidelity (III.5) for the anticlone in the qudit case may be achieved in a measurement-based scheme one may conclude that

$$\eta_N^{U-NOT}(d) = \bar{\eta}_N^{OSE}(d) \tag{IV.22}$$

Then by using the conservation law (IV.13) one has

$$\sum \eta_{in} = M\eta_{N,M}^{UQCM}(d) - (M-N)\eta_N^{U-NOT}(d) \tag{IV.23}$$

In fact, since Werner's cloning map (II.1) can be realized as a unitary transformation on N input qudits, $M-N$ blank qudits and $M-N$ ancillary qudits, it seems

plausible that for arbitrary values of N, M and d, there exists an optimal UQCM that preserves the total Bloch vector length.

10.3 Discussion

While the results presented in this Section are interesting, the conservation of total Bloch vector length was derived under the assumption that ancillary states become optimal anticlones in the cloning transformation and may not hold if this assumption is lifted. They can serve as illustrating examples of the conservation of information in optimal quantum cloning, which is a known result that has received attention particularly from the Horodecki family [10, 116].

The idea of quantifying the information content of the output of a cloning machine by considering on one hand how much classical information can be extracted from it with OSE and on the other hand how well it can be cloned is, to the author's knowledge, a new one. It turned out that in optimal universal cloning, both quantities are conserved, as expected.

When the above strategy was used to show the conservation of information in optimal universal cloning, the results published by Bruß et al. in [85, 115] concerning the concatenation of two or more cloning transformations and the concatenation of cloning and state estimation were used. What makes this concatenation possible is that the output of Werner's cloning map is supported on the symmetric subspace, which leads to simple results in spite of the fact that the compound system of the clones is entangled. An interested reader should to see the original publications for more information.

While only those UQCM that may be recovered from Werner's cloning map where considered in this Section, it would be interesting to study more general cases. Similar results could be perhaps derived also in the cases of asymmetric universal cloning, state-dependent cloning and probabilistic cloning. In the cloning

of mixed states the input states have a shrinking factor less than unity and this would also affect the possible conservation law concerning quantum gain in mixed state cloning, if it exists.

11 Entanglement measures

11.1 Basic concepts

Consider two quantum systems A and B, with respective Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The Hilbert space of the composite system ρ_{AB} is the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$. If the state ρ_{AB} can be written as

$$\rho_{AB} = \rho_A \otimes \rho_B \tag{IV.24}$$

for two density matrices $\rho_A \in \mathcal{H}_A$ and $\rho_B \in \mathcal{H}_B$, it is said to be a product state. Product states may be prepared by local operations (LO) and results of measurements performed on the two subsystems are not correlated, i.e. if the measurement devices operate independently then the measurement results are also independent.

If ρ_{AB} can be written as a probability distribution over product states in $\mathcal{H}_A \otimes \mathcal{H}_B$ as

$$\rho_{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B \tag{IV.25}$$

the state is said to be separable. Separable states may be prepared by LOCC and may exhibit classical correlations, i.e. correlations between measurement results that satisfy Bell inequalities and may therefore be reproduced by a classical mechanism. Notice that a product state is a special case of a separable state.

If a state is not separable, it is entangled. The preparation of an entangled state requires global operations, such as C-NOT, and consequently they cannot be prepared by LOCC. Unlike separable states, entangled states may exhibit quantum correlations, i.e. correlations that are stronger than any classical correlations, and

these quantum correlations may lead to a violation of Bell inequalities. A well-known set of maximally entangled two-qubit states are the four Bell states, which exhibit strongest correlations allowed by quantum mechanics. While all states exhibiting quantum correlations are entangled, the reverse is not true: for example some entangled Werner states do not exhibit quantum correlations [117]. States with quantum correlations are used as a necessary resource in some QIP protocols such as teleportation [63] and superdense coding [118], as well as in some QKD protocols [119].

While quantum correlations between two distant subsystems may be used to demonstrate quantum nonlocality, in the sense that a Bell inequality is violated, no-signaling condition states that quantum nonlocality cannot be used to transmit meaningful signals. Another important principle in entanglement theory is that entanglement cannot increase under LOCC [57], that is to say if state ρ is entangled, then by applying any arbitrary LOCC operation Λ_{LOCC} over it, entanglement can only decrease. It can be shown that if one is restricted to LO only, then entanglement is conserved [120].

Given some bipartite state ρ_{AB}, one may ask whether it is separable or entangled. It is known that if the state is pure, it is separable iff it has a Schmidt decomposition of the form $|\psi\rangle = |e\rangle_A \otimes |f\rangle_B$, i.e. it has a Schmidt rank $r = 1$. If the state is mixed, the Schmidt decomposition does not apply. One may use the Peres-Horodecki criterion, or the positive partial transpose (PPT) criterion instead. The partial transposition ρ^{T_A} of ρ is given by transposing only subsystem A. If ρ is separable, the partially transposed density matrix has positive or vanishing eigenvalues. In the simple case of either two-qubit states or qubit-qutrit states, PPT is a necessary and sufficient condition for separability, but in higher dimensions it is only a necessary condition [121].

Entanglement in a pure bipartite state can be measured with the von Neumann

entropy $S(\rho_i) = -\mathrm{Tr}(\rho_i \log \rho_i)$, where ρ_i is the reduced density matrix of one of the subsystems [57]. In the case of mixed states there is no unique entanglement measure; however a good entanglement measure E should fulfill several conditions. For example, on pure bipartite systems it should coincide with the von Neumann entropy of the reduced density matrix, on separable states vanish, and it should obey no-increase of entanglement under LOCC. Other common postulates are additivity and convexity.

Two important entanglement measures for bipartite states are entanglement of formation E_F and entanglement of distillation E_D. The former can be thought of as the smallest amount of maximally entangled states needed to produce the state in question by LOCC and the latter as the largest amount of maximally entangled states that can be produced from the state in question by LOCC. It can be shown that any entanglement measure E appropriate for asymptotic regime of identically prepared entangled pairs satisfies $E_D \leq E \leq E_F$ [122]. While E_D and E_F are difficult to calculate for a general bipartite state, in the special case of an entangled pair of qubits E_F can be calculated from concurrence [123] and E_D can be upper bounded using negativity [124].

Consider a mixed entangled state of two qubits ρ. Let $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$, where ρ^* is the complex conjugate of ρ and $\sigma_y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right)$ is the Pauli spin matrix. Now concurrence is defined as

$$C(\rho) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4) \tag{IV.26}$$

where λ_i are in decreasing order the square roots of the four eigenvalues η_i of the matrix $\rho\tilde{\rho}$. Negativity is another computable measure of entanglement, defined as

$$\mathcal{N}(\rho) = \sum_i \frac{|\lambda_i| - \lambda_i}{2} \tag{IV.27}$$

where λ_i are the eigenvalues of the partially transposed matrix ρ^{T_A}. It is known that for a mixed entangled state of two qubits, negativity is upper bounded by

concurrence and a lower bound for it in terms of concurrence can also be derived while in the special case of pure states the two coincide [125].

While some of the concepts presented above are straightforward to generalize to multipartite states, entanglement is best understood in the case of bipartite compound systems. For instance, the quantification of entanglement in a tripartite system is already much more involved, since a tripartite entangled system may have entanglement only between two subsystems, in which case it is said to be biseparable, or belong to one of the two inequivalent classes of tripartite states with genuine entanglement of all three subsystems [126].

11.2 Entanglement in quantum cloning

The output (II.6) of the Bužek-Hillery UQCM is known to be entangled. Because it is a compound system of two qubits, the PPT condition is both necessary and sufficient to determine this. If the input qubit is in an arbitrary normalized superposition state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the density matrix of the entangled compound system of the clones in the standard basis $\{|11\rangle, |10\rangle, |01\rangle, |00\rangle\}$ is

$$\rho_{12} = \frac{1}{6}\begin{pmatrix} 4|\beta|^2 & 2\alpha^*\beta & 2\alpha^*\beta & 0 \\ 2\alpha\beta^* & 1 & 1 & 2\alpha^*\beta \\ 2\alpha\beta^* & 1 & 1 & 2\alpha^*\beta \\ 0 & 2\alpha\beta^* & 2\alpha\beta^* & 4|\alpha|^2 \end{pmatrix} \tag{IV.28}$$

where the subindex refers to clones 1 and 2 and each component of the matrix is calculated as $\rho_{m\mu,n\nu} = \langle e_m f_\mu| \rho_{out} |e_n f_\nu\rangle$ where $\{|e_m\rangle\}$ and $\{|f_\mu\rangle\}$ are the computational bases of the first and second subsystems, respectively. The components of

partially transposed matrix are given by $\rho^{T_1}_{m\mu,n\nu} = \rho_{n\mu,m\nu}$ and it is found to be

$$\rho_{12}^{T_1} = \frac{1}{6}\begin{pmatrix} 4|\beta|^2 & 2\alpha^*\beta & 2\alpha\beta^* & 1 \\ 2\alpha\beta^* & 1 & 0 & 2\alpha\beta^* \\ 2\alpha^*\beta & 0 & 1 & 2\alpha^*\beta \\ 1 & 2\alpha^*\beta & 2\alpha\beta^* & 4|\alpha|^2 \end{pmatrix} \tag{IV.29}$$

and the corresponding eigenvalues are

$$\left\{\frac{1}{6}, \frac{1}{6}, \frac{2+\sqrt{5}}{6}, \frac{2-\sqrt{5}}{6}\right\} \tag{IV.30}$$

Since one of the eigenvalues is negative, it can be concluded that the clones of Bužek-Hillery UQCM are indeed entangled. In order to calculate concurrence, one needs to first calculate the matrix $\tilde{\rho_{12}} = (\sigma_y \otimes \sigma_y)\rho_{12}^*(\sigma_y \otimes \sigma_y)$. It is found to be

$$\tilde{\rho_{12}} = \frac{1}{6}\begin{pmatrix} 4|\alpha|^2 & -2\alpha^*\beta & -2\alpha\beta^* & 0 \\ -2\alpha\beta^* & 1 & 1 & -2\alpha^*\beta \\ -2\alpha\beta^* & 1 & 1 & -2\alpha^*\beta \\ 0 & -2\alpha\beta^* & -2\alpha\beta^* & 4|\beta|^2 \end{pmatrix} \tag{IV.31}$$

The matrix $\rho_{12}\tilde{\rho_{12}}$ has only one nonzero eigenvalue $\eta = \frac{1}{9}$ and the concurrence between the two clones is found to be

$$C(\rho_{12}) = \frac{1}{3} \tag{IV.32}$$

The negativity can be calculated from the eigenvalues of the partially transposed matrix $\rho_{12}^{T_1}$. It is

$$\mathcal{N}(\rho_{12}) = \frac{\sqrt{5}-2}{6} \tag{IV.33}$$

By tracing out one of the clones, say clone 1, from eq. (II.5), one may recover the state ρ_{2C} of the compound system of one clone and the ancillary qubit C. It is found to be

$$\begin{aligned}\rho_{2C} = \frac{2}{3}|\psi_2\rangle\langle\psi_2| \otimes |\psi_C^\perp\rangle\langle\psi_C^\perp| - \frac{1}{3}(|\psi_2\rangle\langle\psi_2^\perp| \otimes |\psi_C^\perp\rangle\langle\psi_C| + |\psi_2^\perp\rangle\langle\psi_2| \otimes |\psi_C\rangle\langle\psi_C^\perp|) \\ + \frac{1}{6}(|\psi_2^\perp\rangle\langle\psi_2^\perp| \otimes |\psi_C\rangle\langle\psi_C| + |\psi_2\rangle\langle\psi_2| \otimes |\psi_C\rangle\langle\psi_C|)\end{aligned} \tag{IV.34}$$

and the corresponding density matrix in the standard basis is

$$\rho_{2C} = \frac{1}{6}\begin{pmatrix} |\alpha|^2+4|\beta|^2 & \alpha\beta^* & 2\alpha^*\beta & 2 \\ \alpha^*\beta & |\beta|^2 & 0 & 2\alpha^*\beta \\ 2\alpha\beta^* & 0 & |\alpha|^2 & \alpha\beta^* \\ 2 & 2\alpha\beta^* & \alpha^*\beta & |\beta|^2+4|\alpha|^2 \end{pmatrix} \tag{IV.35}$$

The partially transposed matrix is

$$\rho_{2C} = \frac{1}{6}\begin{pmatrix} |\alpha|^2+4|\beta|^2 & \alpha\beta^* & 2\alpha\beta^* & 0 \\ \alpha^*\beta & |\beta|^2 & 2 & 2\alpha\beta^* \\ 2\alpha^*\beta & 2 & |\alpha|^2 & \alpha\beta^* \\ 0 & 2\alpha^*\beta & \alpha^*\beta & |\beta|^2+4|\alpha|^2 \end{pmatrix} \tag{IV.36}$$

and the eigenvalues are

$$\left\{\frac{2}{3}, \frac{1}{6}, \frac{1+\sqrt{17}}{12}, \frac{1-\sqrt{17}}{12}\right\} \tag{IV.37}$$

As before, one of the eigenvalues is negative and thus the compound system of one clone and ancilla is entangled. Matrix $\rho_{2C}^{\tilde{}}$ is

$$\rho_{2C} = \frac{1}{6}\begin{pmatrix} |\beta|^2+4|\alpha|^2 & -\alpha\beta^* & -2\alpha^*\beta & 2 \\ -\alpha^*\beta & |\alpha|^2 & 0 & -2\alpha^*\beta \\ -2\alpha\beta^* & 0 & |\beta|^2 & -\alpha\beta^* \\ 2 & -2\alpha\beta^* & -\alpha^*\beta & |\alpha|^2+4|\beta|^2 \end{pmatrix} \tag{IV.38}$$

and the matrix $\rho_{2C}\rho_{2C}^{\tilde{}}$ has one nonzero eigenvalue $\eta = \frac{4}{9}$. The concurrence between a clone and ancilla is then

$$C(\rho_{2C}) = \frac{2}{3} \tag{IV.39}$$

The negativity is

$$\mathcal{N}(\rho_{2C}) = \frac{\sqrt{17}-1}{12} \tag{IV.40}$$

Thus one sees that the entanglement between a clone and the ancilla is higher than entanglement between two clones. This result can be interpreted using measures of local and nonlocal information introduced in [127] by Cai, Zhou and Guo. In the

publication, a complementarity relation between the two measures of information was derived as a consequence of conservation of information in unitary transformations. This complementarity relation is valid for all quantum channels taking as input a pure state and constituted of unitary operations only, and states that the sum of local and nonlocal information is a conserved quantity. The measure of local information I_F is based on optimal fidelity F between the input and the output, and is defined as

$$I_F \equiv (2F-1)^2 \tag{IV.41}$$

In the case of a mixed two-qubit state, nonlocal information is measured using the square of concurrence C^2, which is just

$$C^2(\rho) \equiv (C(\rho))^2 \tag{IV.42}$$

These information measures can be used to study how information in the unknown input state $|\psi\rangle_{in}$ is distributed in the Bužek-Hillery UQCM. Before the cloning transformation, local information should be 1 and nonlocal information zero, since all information is in the input qubit, initially in a product state with the blank copy and the ancilla. Now, by using the optimal fidelity (II.9) and concurrence (IV.32) it is easy to see that

$$I_F(\rho_1) + I_F(\rho_2) + C^2(\rho_{12}) = 1 \tag{IV.43}$$

This complementarity relation also holds for a clone and the ancilla. The fidelity of the ancilla can be calculated from (II.10) and is found to be $\frac{1}{3}$. Using concurrence (IV.39), one has

$$I_F(\rho_2) + I_F(\rho_C) + C^2(\rho_{2C}) = 1 \tag{IV.44}$$

Because the fidelity of a clone is higher than that of the ancilla, the concurrence between a clone and the ancilla is necessarily higher than that between two clones because the complementarity relation between local and nonlocal information must be satisfied. It should be mentioned that since the Bužek-Hillery UQCM must

satisfy the complementarity relation, concurrences (IV.32) and (IV.39) could have also been calculated from the fidelities of clones and ancilla using relations (IV.43) and (IV.44).

One can also study the entanglement of the tripartite system $|\Psi\rangle_{12C}$ of both clones and the ancilla. This was done by Bruß and Macchiavello [128], who concluded that the tripartite system has genuine entanglement of all three subsystems and is in the W-class. This means that it may be transformed into

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle) \tag{IV.45}$$

by local reversible operations $\mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C}$. State (IV.45) is one of the Werner states, which were originally introduced in [117] and have the property that tracing out one system will leave the remaining systems entangled.

More generally, the correlations in the output of any UQCM make it more difficult to estimate the input state from the clones. It was pointed out in [113] that if the clones were in product state, then by making a large number of clones the input state could be determined since then one could determine the direction of the Bloch vector representing the input state from the clones which are known to be shrunk versions of the input state. This however is not the case and it was shown in [114] that the correlations between clones are the worst possible for estimation of the input state.

Part V

Effect of decoherence on cloning

In this Part, the effect of decoherence on the average fidelity of the clones is analysed. In the first Section, the basic concepts will be briefly explained and the decoherence model used will be presented. Next, the simplest case of $1 \to 2$ cloning will

be considered. In the third Section two other cases are studied and the form of the expression for average fidelity in the case of general $1 \to M$ cloning will be conjectured. In the last Section the results will be discussed.

12 Decoherence

So far when discussing various different UQCM in this thesis, the assumption has been made that the evolution of the compound system of the input state, blank states and ancillary states during the cloning transformation is unitary. This is an idealization because generally only isolated systems evolve unitarily and in a real experiment conducted in a laboratory the quantum system under study can never be truly isolated from the environment.

In short, the environment can be thought of as a quantum system with a very large number of degrees of freedom. Initially, the quantum system of interest is prepared in some specific state and it is in a product state with the environment. During the unitary evolution of the compound system, interactions between the system of interest and the environment will cause them to become entangled. This terminates the unitary evolution of the system of interest. Its state can be obtained by tracing out the degrees of freedom of the environment, and in the presence of system-environment interactions it is generally found to be in a mixed state. This naturally causes errors in any protocol assuming unitary evolution, and specifically it will affect the fidelity of the clones at the output of a UQCM as will be seen in this Part.

While non-unitary evolution of the system caused by interactions with the environment may affect both populations (diagonal elements) and coherences (off-diagonal elements) of its reduced density matrix, the disappearance of coherences, i.e. decoherence, will be analysed in this Part while leaving populations unperturbed. In other words, it has been assumed that decoherence takes place at a

much faster time scale than the changes in populations. This is the case when the environment is in a thermal state.

The decoherence model used is the one by Barenco et al. [129] where it is assumed that the environment introduces random phase fluctuations to the qubit each time it is affected by a two-qubit quantum gate such that

$$\alpha\,|0\rangle + \beta\,|1\rangle \longrightarrow \alpha e^{-i\phi}\,|0\rangle + \beta e^{i\phi}\,|1\rangle \tag{V.1}$$

Here, the cloning network discovered by Bužek, Hillery and Knight [130] is considered. Since the cloning stage of the quantum network implementation of a $1 \to M$ UQCM consists of only C-NOT gates, this can be thought of as a modification of the isolated cloning circuit where each C-NOT gate is replaced by a C-NOT gate followed by a rotation

$$R_z(2\phi) = \begin{pmatrix} e^{-i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix} \tag{V.2}$$

of both the control and the target qubit as in Fig. 9. Each phase fluctuation ϕ is drawn from a Gaussian distribution

$$P(\phi)\mathrm{d}\phi = \frac{1}{\sqrt{2\pi}\delta} \exp\left[-\frac{1}{2}\left(\frac{\phi}{\delta}\right)^2\right] \tag{V.3}$$

where the distribution width δ describes the strength of the system-environment coupling. After the cloning transformation the average fidelity of a clone will be calculated by taking the average over different realisations of the phase fluctuations.

In the next Section, the Bužek-Hillery UQCM will be considered. The average fidelity of the cloning transformation will be calculated in two ways. First by assuming that the preparation stage of the transformation is free of decoherence effects, and next by extending the decoherence effects to the preparation network as well. In the latter case, no phase fluctuations have been attached to the three single-qubit rotations of the preparation network because it was assumed that the rotations are much faster to carry out than the C-NOT gates.

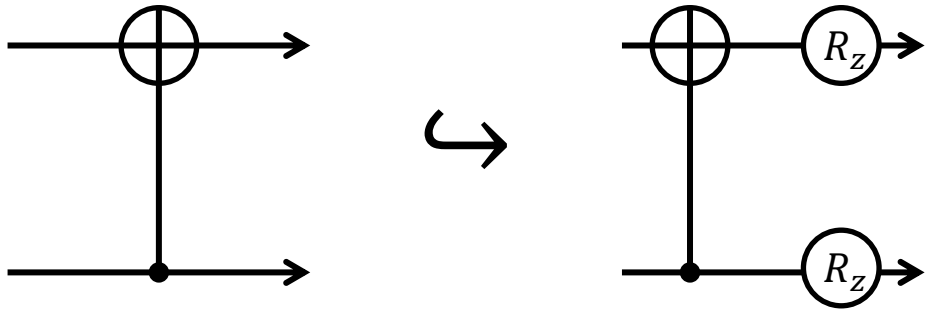

Figure 9. To model the effects of decoherence, each C-NOT gate in the cloning network is replaced by a C-NOT gate followed by a rotation of both the control and the target qubit. The direction and the magnitude of the rotation is the same for both qubits and is drawn from a Gaussian distribution. In the picture, the case where target qubit is above the control qubit is presented.

In the third Section, the $1 \to 3$ and $1 \to 4$ cloners using the cloning network described in Fig. 10 will be analysed under the assumption that the preparation stage of the network is free from decoherence effects. In the last Section, the results and the scalability of the preparation network will be discussed. The number of input states will be 1 throughout this Part because the efficient quantum network to implement $N \to M$ cloning is unknown for any $N > 1$.

13 $1 \to 2$ case

By making the replacement presented in Fig. 9, the action of the cloning network used to realize the Bužek-Hillery UQCM on states $|x\rangle_1 |y\rangle_2 |z\rangle_C$ in the computational basis may be calculated. It is

$$|x\rangle_1 |y\rangle_2 |z\rangle_C \longrightarrow E(x,y,z) |x \oplus y \oplus z\rangle_1 |x \oplus y\rangle_2 |x \oplus z\rangle_C \tag{V.4}$$

where

$$E(x,y,z) = e^{i\phi_1(h(x)+h(x\oplus y))} e^{i\phi_2(h(x)+h(x\oplus z))} e^{i\phi_3(h(y)+h(x\oplus y))} e^{i\phi_4(h(x\oplus z)+h(x\oplus y\oplus z))} \tag{V.5}$$

and

$$h(0) = -1; \quad h(1) = 1 \tag{V.6}$$

The four phase fluctuations are caused by the four C-NOT gates in the cloning network. When the input state is $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and the blank copy and ancilla are prepared in the state (II.17), the reduced density matrix of a clone becomes

$$\rho_1 = \frac{1}{6}\begin{pmatrix} 4|\alpha|^2+1 & 4\alpha\beta^*\mathcal{N}_{1\to2} \\ 4\alpha^*\beta\mathcal{N}^*_{1\to2} & 4|\beta|^2+1 \end{pmatrix} \tag{V.7}$$

where

$$\mathcal{N}_{1\to2} = e^{-2i(\phi_1+\phi_2+\phi_4)}\cos 2\phi_3 \tag{V.8}$$

The corresponding fidelity is

$$\langle\psi|\,\rho_1\,|\psi\rangle = \frac{1}{6}\left[4\left(|\alpha|^4 + (\mathcal{N}_{1\to2}+\mathcal{N}^*_{1\to2})|\alpha|^2|\beta|^2 + |\beta|^4\right)+1\right] \tag{V.9}$$

which reduces to the usual value 5/6 in the ideal case of zero phase fluctuations where $\mathcal{N}_{1\to2} = \mathcal{N}^*_{1\to2} = 1$. The fidelity of the clones is no longer state-independent; however by using average fidelity as a figure of merit their quality can be quantified. Average fidelity can be calculated via parameterization of the complex coefficients as in eq. (II.24):

$$\alpha = \cos\frac{\theta}{2}; \quad \beta = e^{i\phi}\sin\frac{\theta}{2} \tag{V.10}$$

Now average fidelity between input state and clone affected by phase fluctuations during cloning stage, assuming the distribution of pure input states in the Bloch sphere is uniform, is

$$\bar{F} = \frac{1}{4\pi}\int_{\theta=0}^{\pi}\int_{\phi=0}^{2\pi}\langle\psi|\,\rho_1\,|\psi\rangle\sin\theta\,\mathrm{d}\theta\mathrm{d}\phi = \frac{2\,(\mathcal{N}_{1\to2}+\mathcal{N}^*_{1\to2})+11}{18} \tag{V.11}$$

The average value of factor (V.8) can be calculated as an integral over appropriate limits:

$$\langle\mathcal{N}_{1\to2}\rangle = \int \mathcal{N}_{1\to2}P(\phi_1)P(\phi_2)P(\phi_3)P(\phi_4)\,\mathrm{d}\phi_1\mathrm{d}\phi_2\mathrm{d}\phi_3\mathrm{d}\phi_4 \tag{V.12}$$

In this case Gaussian distribution (V.3) has been used and the integral has been evaluated from $-\pi/2$ to $\pi/2$. When calculating the average, one may make use of

the fact that odd functions vanish in the averaging to derive the following relation valid for $i \neq j$:

$$\begin{aligned} \langle \cos 2(\phi_i + \phi_j) \rangle &= \langle \cos 2\phi_i \cos 2\phi_j - \sin 2\phi_i \sin 2\phi_j \rangle \\ = \langle \cos 2\phi_i \rangle \langle \cos 2\phi_j \rangle - \langle \sin 2\phi_i \rangle \langle \sin 2\phi_j \rangle &= \langle \cos 2\phi_i \rangle \langle \cos 2\phi_j \rangle \end{aligned} \tag{V.13}$$

Using it, one recovers the simple expression (assuming that the distribution width, i.e. the strength of system-environment coupling, remains constant during cloning) for the average value

$$\langle \mathcal{N}_{1\to 2} + \mathcal{N}^*_{1\to 2} \rangle = 2 \langle \cos 2\phi \rangle^4 \tag{V.14}$$

The resulting average fidelity is presented for various different distribution widths in Fig. 11. Decoherence-free fidelity is 5/6. Classical cloning limit, i.e the fidelity of the optimal measure-and-prepare cloner, is given by eq. (III.4) and it is 2/3, which is reached when $\langle \mathcal{N}_{1\to 2} + \mathcal{N}^*_{1\to 2} \rangle = 1/2$, or when $\delta \approx 52/125$. When the initial state of the cloning machine is ideal, it turns out that the Bužek-Hillery UQCM is quite robust in the presence of random phase fluctuations. This is a consequence of the low number of gates in the cloning network.

When decoherence is taken into account not only during the cloning stage, but also during the preparation of the initial state (II.17), necessary for cloning network presented in Fig. 2 to perform universal cloning, the situation becomes much more complicated. It is worth pointing out that due to phase fluctuations, the coefficient of $|10\rangle_{2C}$ does not vanish like it should and this introduces more errors in the quantum computation.

By leaving all averaging to the end of the computation, the elements of the density matrix of a clone become very complicated; however the formula for average fidelity can still be expressed in a simple way. After the preparation stage, the coefficients of the states $\{|00\rangle_{2C}, |01\rangle_{2C}, |10\rangle_{2C}, |11\rangle_{2C}\}$ become, respectively,

$$C_{00} = e^{-2i\phi_{\rm I}}\left[\frac{2}{\sqrt{6}} + \left(e^{-2i\phi_{\rm II}} - 1\right)\cos\theta_1\cos\theta_2\cos\theta_3\right] \tag{V.15}$$

$$C_{01} = e^{2i\phi_{\rm I}}\left[\frac{1}{\sqrt{6}} + \left(1 - e^{-2i(2\phi_{\rm I}-\phi_{\rm II})}\right)\cos\theta_1\sin\theta_2\sin\theta_3\right] \tag{V.16}$$

$$C_{10} = e^{-2i\phi_{\rm I}}\left(e^{-2i\phi_{\rm II}} - 1\right)\cos\theta_1\cos\theta_2\sin\theta_3 \tag{V.17}$$

$$C_{11} = e^{2i\phi_{\rm I}}\left[\frac{1}{\sqrt{6}} + \left(e^{-2i\phi_{\rm II}} - 1\right)\cos\theta_1\sin\theta_2\cos\theta_3\right] \tag{V.18}$$

where the angles are given by eq. (II.21) and phase fluctuations $\phi_{\rm I}$ and $\phi_{\rm II}$ are caused by the two C-NOT gates in preparation network presented in Fig. 3. After the cloning stage, also affected by decoherence, the average fidelity becomes

$$\bar{F} = \frac{2A + B + C}{3} \tag{V.19}$$

where

$$A = \frac{5}{6} + \frac{1}{15}\left[\cos\left(4\phi_{\rm I} - 2\phi_{\rm II}\right) + \cos 2\phi_{\rm II}\right] \tag{V.20}$$

$$B = \frac{1}{6} - \frac{1}{15}\left[\cos\left(4\phi_{\rm I} - 2\phi_{\rm II}\right) + \cos 2\phi_{\rm II}\right] \tag{V.21}$$

$$C = 2\cos 2\left(\phi_1 + \phi_2 + \phi_4\right)\left[\mathrm{Re}\left[C_{00}C_{11}^*\right]\cos 2\phi_3 + \mathrm{Im}\left[C_{00}C_{11}^*\right]\sin 2\phi_3\right] \tag{V.22}$$

Note that in the averaging of phase fluctuations, the term in C containing $\sin 2\phi_3$ vanishes because it is an odd function. The real part of the product $C_{00}C_{11}^*$ is

$$\begin{aligned}\mathrm{Re}\left[C_{00}C_{11}^*\right] = \frac{1}{60}\Big[&(3-\sqrt{5})\cos(4\phi_{\rm I} + 2\phi_{\rm II}) \\ &+(7+3\sqrt{5})\cos 4\phi_{\rm I} + (7-3\sqrt{5})\cos 4\phi_{\rm II} + (3+\sqrt{5})\cos 2\phi_{\rm II}\Big]\end{aligned} \tag{V.23}$$

Now there are six phase fluctuations, caused by the C-NOT gates in the preparation and cloning networks. In the decoherence-free case, A reduces to 5/6, B to 1/6 and C to 2/3 and eq. (V.19) returns the ideal fidelity 5/6, as it should. As expected, the decoherence in the preparation network and cloning network will cause a larger drop in average fidelity than cloning under decoherence with ideal preparation. However, for large distribution widths the average fidelity is much closer to those of the $1 \to 3$

and $1 \to 4$ cloners with ideal preparation than the $1 \to 2$ case with ideal preparation, as can be seen from Fig. 11. Classical limit is met earlier than before, when $\delta \approx 29/100$.

14 $1 \to M$ case

Throughout this Section, it is assumed that the initial state of the cloning machine, in other words the initial state of the compound system of the blank copies and ancillary qubits, is ideal. The effect of lifting this assumption will be discussed in the last Section.

The cloning circuit and the corresponding preparation of the initial state of the cloning machine that can be used to realize the optimal $1 \to M$ UQCM was presented by Bužek et al. [130]. It consists of a sequence of $4(M-1)$ C-NOT gates where first the input qubit acts as the control qubit and target qubits are all the other qubits one by one, and then the roles are reversed in a way similar to $1 \to 2$ cloning network. Each clone requires one blank copy and one ancillary qubit. This cloning circuit is presented in Fig. 10.

The reduced density matrix of a clone at the output of the optimal $1 \to 3$ UQCM can be found in a manner similar to what was used in the previous Section. It is

$$\rho_1 = \frac{1}{9} \begin{pmatrix} 5|\alpha|^2 + 2 & \alpha\beta^* \mathcal{N}_{1\to 3} \\ \alpha^* \beta \mathcal{N}^*_{1\to 3} & 5|\beta|^2 + 2 \end{pmatrix} \tag{V.24}$$

where

$$\mathcal{N}_{1\to 3} = \left(3 + e^{-4i\phi_6} + e^{-4i(\phi_6+\phi_7)}\right) e^{2i(\phi_1+\phi_2+\phi_3+\phi_4+\phi_6+\phi_7+\phi_8)} \cos 2\phi_5 \tag{V.25}$$

The phase fluctuations ϕ_i are caused by the eight C-NOT gates in the cloning network. The corresponding fidelity is

$$\langle\psi|\,\rho_1\,|\psi\rangle = \frac{1}{9}\left[5|\alpha|^4 + (\mathcal{N}_{1\to 3} + \mathcal{N}^*_{1\to 3})|\alpha|^2|\beta|^2 + 5|\beta|^4 + 2\right] \tag{V.26}$$

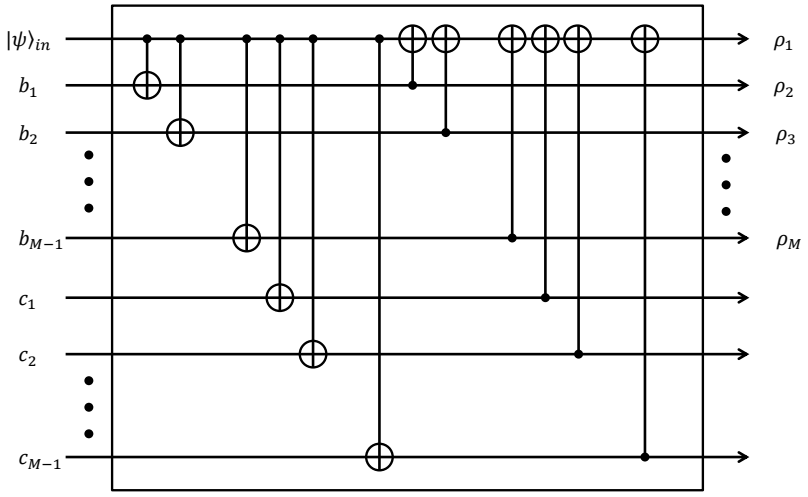

Figure 10. The cloning network for $1 \to M$ UQCM presented by Bužek, Hillery and Knight. The pure input state $|\psi\rangle_{in}$ acts first as the control qubit for a sequence of C-NOT gates affecting all $M-1$ blank copies b_i and $M-1$ ancillary qubits c_i. Then the roles are reversed. When the compound system of blank copies and ancillary qubits is prepared correctly this network performs optimal $1 \to M$ universal cloning. The M clones ρ_i appear at the output.

which reduces to the optimal value $7/9$ when $\phi_i = 0$, as it should. The average value of fidelity (V.26) is

$$\bar{F} = \frac{(\mathcal{N}_{1\to 3} + \mathcal{N}^*_{1\to 3}) + 32}{54} \tag{V.27}$$

The average value of factor (V.25) can be calculated like before. By using the property (V.13) one recovers

$$\langle \mathcal{N}_{1\to 3} + \mathcal{N}^*_{1\to 3} \rangle = 10 \langle \cos 2\phi \rangle^8 \tag{V.28}$$

This time the classical cloning limit is met when $\delta \approx 25/100$.

The $1 \to 4$ case can be treated in exactly the same way. The reduced density matrix of a clone becomes

$$\rho_1 = \frac{2}{5} \begin{pmatrix} \frac{5}{4}|\alpha|^2 + \frac{5}{8} & \alpha\beta^* \mathcal{N}_{1\to 4} \\ \alpha^*\beta \mathcal{N}^*_{1\to 4} & \frac{5}{4}|\beta|^2 + \frac{5}{8} \end{pmatrix} \tag{V.29}$$

Fidelity is

$$\langle\psi|\,\rho_1\,|\psi\rangle = \frac{2}{5}\left[\frac{5}{4}|\alpha|^4 + (\mathcal{N}_{1\to4} + \mathcal{N}^*_{1\to4})|\alpha|^2|\beta|^2 + \frac{5}{4}|\beta|^4 + \frac{5}{8}\right] \tag{V.30}$$

and the average value of fidelity (V.30) is

$$\bar{F} = \frac{4(\mathcal{N}_{1\to4} + \mathcal{N}^*_{1\to4}) + 35}{60} \tag{V.31}$$

In the decoherence-free case the term $\mathcal{N}_{1\to4} + \mathcal{N}^*_{1\to4}$ reduces to $5/2$ and the optimal fidelity $3/4$ of $1 \to 4$ UQCM is recovered. Otherwise it is

$$\begin{aligned}\mathcal{N}_{1\to4} + \mathcal{N}^*_{1\to4} = \cos 2\left(\sum_{i=1}^{6}\phi_i + \phi_8 + \phi_{10} + \phi_{12}\right)\cos 2(\phi_7 + \phi_9 + \phi_{11}) \\ + \cos 2\left(\sum_{i=1}^{6}\phi_i + \phi_{12}\right)\frac{1}{6}(D_1 + D_2)\end{aligned} \tag{V.32}$$

where D_2 is an odd function and will vanish in the averaging process. D_1 has 9 even terms and 1 odd term, and they are functions of phase fluctuations ϕ_7 through ϕ_{11}:

$$\begin{aligned}D_1 = \cos 2\phi_9\left(\cos 2(\phi_7 + \phi_{11})\cos 2(\phi_8 - \phi_{10}) + \cos 2(\phi_7 - \phi_8)\cos 2(\phi_{10} - \phi_{11})\right) \\ + \cos 2\phi_{11}\left(\cos 2(\phi_7 + \phi_8 + \phi_9 + \phi_{10}) + 2\cos 2(\phi_7 + \phi_8 - \phi_9 - \phi_{10})\right) \\ +2\cos 2\phi_8\cos 2(\phi_7 - \phi_9 + \phi_{10} + \phi_{11}) + \cos 2(\phi_7 + \phi_8 - \phi_9 - \phi_{10} - \phi_{11}) \\ - \sin 2\phi_9\cos 2(\phi_7 + \phi_{11})\cos 2(\phi_8 - \phi_{10})\end{aligned} \tag{V.33}$$

By using the property (V.13), one recovers

$$\langle\mathcal{N}_{1\to4} + \mathcal{N}^*_{1\to4}\rangle = \frac{5}{2}\langle\cos 2\phi\rangle^{12} \tag{V.34}$$

As expected, the classical cloning limit is met even earlier, namely when $\delta \approx 18/100$. The average fidelities for various distribution widths are presented in Fig. 11.

By looking at the expressions for average fidelity in the presence of Gaussian phase fluctuations calculated so far, one may try to estimate the form of this expression in the general case of $1 \to M$ cloning realized by this kind of quantum circuit when the phase fluctuations have been averaged. In fact, when averaging the phase fluctuations, all three average fidelities (V.11), (V.27) and (V.31) are found to be of the form

$$\bar{F}_{1\to M} = F_{1\to M} + \zeta\left(\langle\cos 2\phi\rangle^{4(M-1)} - 1\right) \tag{V.35}$$

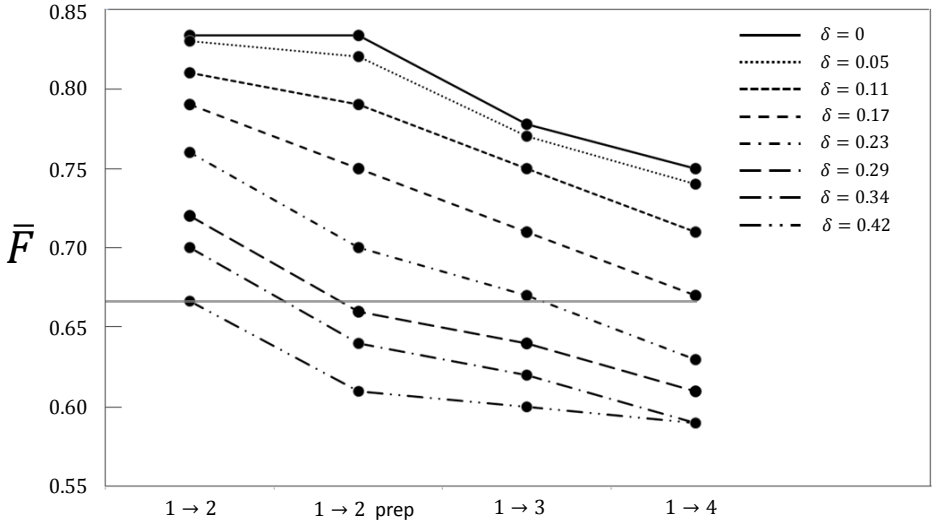

Figure 11. The average fidelities of the four cases of UQCM under consideration in the presence of Gaussian phase fluctuations for eight different distribution widths δ. While it was assumed that the preparation of the initial state of the UQCM was unaffected by phase fluctuations, the case where this assumption is lifted was studied for $1 \to 2$ cloning. The gray line is at average fidelity of $2/3$, or the fidelity of a classical measure-and-prepare cloner.

for some constant ζ where $F_{1\to M}$ is the corresponding optimal fidelity and $4(M-1)$ is the number of gates in the cloning network. These values are $\zeta = 2/9$, $\zeta = 5/27$ and $\zeta = 1/6$ for $1 \to 2$, $1 \to 3$ and $1 \to 4$ UQCM, respectively. If this is indeed the form of the expression for average fidelity in the general case, then the constant ζ should depend on M in some way.

15 Discussion

In this Part, the effect of decoherence on the average fidelity of clones was studied by attaching Gaussian phase fluctuations ϕ_i to each C-NOT gate in the cloning network. By analyzing them, it was shown that in the $1 \to 2$, $1 \to 3$ and $1 \to 4$ cases average fidelity depends linearly on $\langle \cos 2\phi \rangle^{4(M-1)}$, where $4(M-1)$ is the number of C-NOT gates in the cloning network, as in eq. (V.35). The equation is valid for all finite distribution widths δ but requires that the integral (V.12) is from

$-x$ to x where $x \in \mathbf{R}$. Whether this result applies to the general case of $1 \rightarrow M$ universal cloning will be left as a challenge for the interested reader.

In addition, the case where decoherence effects were extended to the preparation of the initial state of the UQCM was studied in the simplest case of $1 \rightarrow 2$ cloning. It turned out that this made the calculation of average fidelity much more complicated, mostly due to the three rotations in the preparation network. It should be pointed out that the last rotation resulted in fluctuations in populations as well. Even though the amount of C-NOT gates increases only by two the difference between average fidelities of the two different $1 \rightarrow 2$ cases becomes significant for large values of δ, suggesting that the preparation network is less robust to phase fluctuations than the cloning network. An intuitive explanation for this is that the cloning network, consisting of only C-NOT gates, is more simple.

The effect of decoherence during the preparation of the initial state of the UQCM in more general cases is bound to be even larger, since while the number of gates in the cloning network is a linear function of M, this is not the case with the preparation network. In fact, the number of gates needed for the preparation of the initial state of the UQCM was analysed by Maruyama and Knight [131] and it was found to grow exponentially with M. In the publication the time needed to perform cloning with a quantum network was estimated and compared to the decoherence time of an ion trap system and it was concluded that due to the large number of gates in the preparation stage, the quantum network implementation of universal cloning can only be done when M is very small. Thus the preparation stage is a major challenge in the experimental realization of a cloning network.

Both in this analysis and in the one by Maruyama and Knight it was assumed that quantum error correction codes are not used. How they could be used here and how their use would affect the quality of clones in universal quantum cloning still remains an untouched topic.

Conclusions

In this thesis, after a review of the key properties of universal quantum cloning and its connection to QKD protocols, U-NOT gate and OSE, the redistribution of information in the input states that are cloned and its conversion to entanglement as well as the effect of Gaussian phase fluctuations to the quality of clones in terms of average fidelity were analysed. The focus was on deterministic symmetric cloning of pure states lying in a finite-dimensional Hilbert space, or cloning transformations described by Werner's cloning map (II.1).

Optimal universal quantum cloning transformations are isotropic unitary transformations which must be ancilla-assisted and as can be seen from the cloning map mentioned above, can be regarded as a kind of permutation of the input state(s) with the blank copies in such a way that i) the output is normalized and supported in the symmetric subspace of M quantum systems and ii) the N input states are permuted with maximally mixed states to ensure universality. From condition i) it follows that after the cloning, the state of all clones is identical and also that optimal UQCM in terms of single-copy fidelity and global fidelity coincide. A good example of how universal cloning works is the cloning network used to implement the well-known Bužek-Hillery UQCM, which can act as both an identity and a swap network depending on the preparation of the blank copy and the ancillary qubit in such a way that at the output, the unknown input state is in a product state with the maximally entangled two-qubit state, whose marginal density operators describe the maximally mixed state. It is noteworthy that the optimal U-NOT gate can be realized as a by-product of a suitable optimal UQCM by tracing out the clones instead of the ancillary states.

Asymmetric cloning in general has a connection with QKD because an eavesdropper may employ an asymmetric QCM to clone an intercepted signal state and send one clone forward while keeping the other clone. While it is not the case in gen-

eral, often the most dangerous attack on a QKD protocol is an asymmetric cloning machine: for example, the asymmetric optimal UQCM is used in the optimal eavesdropping strategy of the six-states protocol. On the other hand, symmetric cloning is related to OSE. When all input states are pure and equally likely, then at the limit of many clones the fidelities of the two coincide. The results of Bae and Acin mentioned in Part III suggest that this equality in fidelities holds in general, i.e. for arbitrary sets of pure input states with unequal a priori probabilities.

In Part IV, by using the OSE connection and shrinking factor as a figure of merit, it was shown that the total quantum gain per input qudit in optimal universal cloning is always equal to the loss of information in OSE and that the shrinking factors of OSE from either the input or the output of an optimal UQCM coincide. This was interpreted as meaning that the amount of extractable classical information is conserved in cloning. Using the conservation law (IV.13) concerning the sum of quantum gain and OSE shrinking factor, it was shown that in the qubit case, the total Bloch vector length is also a conserved quantity. In the case of the Bužek-Hillery UQCM, concurrence and negativity were calculated between two clones and between a clone and the ancilla to show that two clones or a clone and the ancilla obey a complementarity relation between local and nonlocal information.

In the final Part, decoherence effects on $1 \to M$ UQCMs were studied using the quantum circuit formalism. It was assumed that environment causes random phase fluctuations, drawn from a Gaussian distribution, to the complex coefficients of a qubit each time it is affected by a C-NOT gate. The four different cases under study were $1 \to 2$, $1 \to 3$ and $1 \to 4$ cloners with ideal preparation of the initial state of the cloning machine, and $1 \to 2$ UQCM where decoherence effects were extended to the preparation network as well.

In all four cases it was easy to see that decoherence destroys the universality of the cloner. In the former three cases it was seen that when both phase fluctuations

and fidelity are averaged, the resulting expression (V.35) for average fidelity has a simple form and may perhaps apply to cases of higher number of clones. The comparison of average fidelities of all four cases for many different distribution widths suggests that the cloning network described in Fig. 10 is rather robust in the presence of phase fluctuations, and specifically it is more robust than the preparation network presented in Fig. 3. When keeping in mind that the number of gates in the preparation network increases exponentially with the number of clones, it is clear that on the whole, the scalability of this type of UQCM is poor.

It would be interesting to study the information flow during the intermediate steps of the cloning network using the measures of local and nonlocal information presented at the end of Part IV. The complementarity relation should be satisfied at all times, however it might enable a better understanding of the information dynamics in cloning. Also at the moment of this writing, it has not been studied by anyone how the use of quantum error-correction codes would affect cloning in the presence of decoherence.

References

[1] S. Yao, H. Liang and L. Gui-Lu, Chin. Phys. Lett. **28**, 010306 (2011).

[2] V. Scarani, S. Iblisdir, N. Gisin and A. Acin, Rev. Mod. Phys. **77**, 1225 (2005).

[3] N. Herbert, Found. Phys. **12**, 1171 (1982).

[4] G. Ghirardi and T. Weber, Nuovo Cimento Soc. Ital. Fis. **78**, 9 (1983).

[5] W. Wootters and W. Zurek, Nature **299**, 802 (1982).

[6] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[7] D. Bruss, G. D'Ariano, C. Macchiavello and M. Sacchi, Phys. Rev. A **62**, 062302 (2000).

[8] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic PublishersDordrecht, The Netherlands, 1995).

[9] I. Chakrabarty, A. Pati and A. Satyabrata, Stronger no-cloning, no-signalling and conservation of quantum information, arXiv:quant-ph/0605173, 2002.

[10] M. Horodecki, R. Horodecki, A. Sen and U. Sen, Found. Phys. **35**, 2041 (2005).

[11] L. Masanes, A. Acin and N. Gisin, Phys. Rev. A **73**, 012112 (2006).

[12] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, 2006), p. 175.

[13] H. Barnum *et al.*, Phys. Rev. Lett. **76**, 2818 (1996).

[14] R. Jozsa, A stronger no-cloning theorem, arXiv:quant-ph/0204153, 2002.

[15] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[16] L. Duan and G. Guo, Phys. Lett. A **243**, 261 (1998).

[17] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[18] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).

[19] N. Gisin, Phys. Lett. A **242**, 1 (1998).

[20] D. Bruss *et al.*, Phys. Rev. A **57**, 2368 (1998).

[21] N. J. Cerf and J. Fiurasek, in *Optical quantum cloning*, Vol. 49 of *Progress in Optics*, edited by Wolf, E (Elsevier, 2006), pp. 455–545.

[22] M. Keyl and R. Werner, J. Math. Phys. **40**, 3283 (1999).

[23] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[24] R. Werner, Phys. Rev. A **58**, 1827 (1998).

[25] N. Cerf, Acta Phys. Slovaca **48**, 115 (1998).

[26] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).

[27] N. Cerf, M. Bourennane, A. Karlsson and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[28] A. Ferenczi and N. Luetkenhaus, Phys. Rev. A **85**, 052310 (2012).

[29] L. Jing *et al.*, Phys. Rev. A **86**, 062315 (2012).

[30] C. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997).

[31] H. Fan, K. Matsumoto, X. Wang and M. Wadati, Phys. Rev. A **65**, 012304 (2002).

[32] G. D'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).

[33] F. Buscemi, G. D'Ariano and C. Macchiavello, Phys. Rev. A **71**, 042327 (2005).

[34] H. Fan, H. Imai, K. Matsumoto and X. Wang, Phys. Rev. A **67**, 022317 (2003).

[35] L. Lamoureux and N. Cerf, Quantum Information & Computation **5**, 32 (2005).

[36] C. Niu and R. Griffiths, Phys. Rev. A **60**, 2764 (1999).

[37] T. Durt and J. Du, Phys. Rev. A **69**, 062316 (2004).

[38] T. Durt, J. Fiurasek and N. Cerf, Phys. Rev. A **72**, 052322 (2005).

[39] H. Fan *et al.*, Quantum Cloning Machines and the Applications, arXiv:1301.2956, 2002.

[40] R. Derka, V. Buzek and A. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).

[41] N. Cerf, T. Durt and N. Gisin, J. Mod. Opt. **49**, 1355 (2002).

[42] P. Navez and N. Cerf, Phys. Rev. A **68**, 032313 (2003).

[43] V. Buzek, S. Braunstein, M. Hillery and D. Bruss, Phys. Rev. A **56**, 3446 (1997).

[44] L. Duan and G. Guo, Phys. Rev. Lett. **80**, 4999 (1998).

[45] A. Chefles and S. Barnett, J. Phys. A **31**, 10097 (1998).

[46] L. Hardy and D. Song, Phys. Lett. A **259**, 331 (1999).

[47] J. Fiurasek, Phys. Rev. A **70**, 032308 (2004).

[48] N. Cerf, A. Ipe and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).

[49] N. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301 (2000).

[50] S. Braunstein *et al.*, Phys. Rev. Lett. **86**, 4938 (2001).

[51] N. Cerf *et al.*, Phys. Rev. Lett. **95**, 070501 (2005).

[52] A. Rastegin, Phys. Rev. A **67**, 012305 (2003).

[53] A. Rastegin, Phys. Rev. A **68**, 032303 (2003).

[54] G. D'Ariano, C. Macchiavello and P. Perinotti, Phys. Rev. Lett. **95**, 060503 (2005).

[55] L. Chen and Y.-X. Chen, Phys. Rev. A **75**, 062322 (2007).

[56] L. Li *et al.*, J. Phys. A **42**, 175302 (2009).

[57] C. Bennett, H. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[58] M. Koashi and N. Imoto, Phys. Rev. Lett. **81**, 4264 (1998).

[59] E. Karpov, P. Navez and N. Cerf, Phys. Rev. A **72**, 042314 (2005).

[60] F. Anselmi, A. Chefles and M. Plenio, New J. Phys. **6**, 164 (2004).

[61] S. Ghosh, G. Kar and A. Roy, Phys. Rev. A **69**, 052312 (2004).

[62] S. Ghosh *et al.*, Phys. Rev. Lett. **87**, 277902 (2001).

[63] C. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[64] M. Murao, D. Jonathan, M. Plenio and V. Vedral, Phys. Rev. A **59**, 156 (1999).

[65] M. Murao, M. Plenio and V. Vedral, Phys. Rev. A **61**, 032311 (2000).

[66] W. Dur and J. Cirac, J. Mod. Opt. **47**, 247 (2000).

[67] P. van Loock and S. Braunstein, Phys. Rev. Lett. **87**, 247901 (2001).

[68] X.-W. Wang and G.-J. Yang, Phys. Rev. A **79**, 062315 (2009).

[69] X.-W. Wang and G.-J. Yang, Phys. Rev. A **79**, 064306 (2009).

[70] M. Murao and V. Vedral, Phys. Rev. Lett. **86**, 352 (2001).

[71] C. Simon, G. Weihs and A. Zeilinger, Phys. Rev. Lett. **84**, 2993 (2000).

[72] H. Cummins *et al.*, Phys. Rev. Lett. **88**, 187901 (2002).

[73] H. Chen *et al.*, Phys. Rev. Lett. **106**, 180404 (2011).

[74] A. Lamas-Linares, C. Simon, J. Howell and D. Bouwmeester, Science **296**, 712 (2002).

[75] W. Irvine, A. Linares, M. de Dood and D. Bouwmeester, Phys. Rev. Lett. **92**, 047902 (2004).

[76] P. Milman *et al.*, J. Mod. Opt. **50**, 901 (2003).

[77] T. Wu, B.-L. Fang and L. Ye, J. Opt. Soc. Am. B **29**, 2749 (2012).

[78] B. L. Fang, T. Wu and L. Ye, EPL **97**, 60002 (2012).

[79] A. Cernoch *et al.*, Phys. Rev. A **74**, 042327 (2006).

[80] J. Du *et al.*, Phys. Rev. Lett. **94**, 040505 (2005).

[81] E. Nagali, T. De Angelis, F. Sciarrino and F. De Martini, Phys. Rev. A **76**, 042126 (2007).

[82] U. Andersen, V. Josse and G. Leuchs, Phys. Rev. Lett. **94**, 240503 (2005).

[83] I. Khan and J. Howell, Quantum Information & Computation **4**, 114 (2004).

[84] K. Kraus, Lecture Notes in Physics **190**, 1 (1983).

[85] D. Bruss and C. Macchiavello, Phys. Lett. A **253**, 249 (1999).

[86] H. Fan, K. Matsumoto and M. Wadati, Phys. Rev. A **64**, 064301 (2001).

[87] Y.-N. Wang *et al.*, Phys. Rev. A **84**, 034302 (2011).

[88] D. Gottesman, H. Lo, N. Luetkenhaus and J. Preskill, Quantum Information & Computation **4**, 325 (2004).

[89] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).

[90] K. Tamaki, M. Koashi and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[91] C. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).

[92] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[93] I. Gerhardt *et al.*, Nature Communications **2**, 349 (2011).

[94] N. Gisin *et al.*, Phys. Rev. A **73**, 022320 (2006).

[95] V. Buzek, M. Hillery and R. Bednik, Acta Phys. Slovaca **48**, 177 (1998).

[96] S. Braunstein, V. Buzek and M. Hillery, Phys. Rev. A **63**, 052313 (2001).

[97] J. Fiurasek, R. Filip and N. Cerf, Quantum Information & Computation **5**, 583 (2005).

[98] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[99] N. Gisin and S. Popescu, Phys. Rev. Lett. **83**, 432 (1999).

[100] J. Fiurasek, Phys. Rev. A **64**, 062310 (2001).

[101] V. Buzek, M. Hillery and R. Werner, Phys. Rev. A **60**, R2626 (1999).

[102] I. Chattopadhyay *et al.*, Phys. Lett. A **351**, 384 (2006).

[103] D. Song and L. Hardy, Phys. Lett. A **341**, 60 (2005).

[104] F. De Martini, V. Buzek, F. Sciarrino and C. Sias, Nature **419**, 815 (2002).

[105] W.-Y. Hwang and Y.-D. Han, Phys. Rev. A **86**, 032339 (2012).

[106] A. Chefles, Contemporary Physics **41**, 401 (2000).

[107] K. Hammerer, M. Wolf, E. Polzik and J. Cirac, Phys. Rev. Lett. **94**, 150503 (2005).

[108] E. Bagan, A. Monras and R. Munoz-Tapia, Phys. Rev. A **78**, 043829 (2008).

[109] J. Fiurasek, New J. Phys. **8**, 192 (2006).

[110] M. D. de Burgh, N. K. Langford, A. C. Doherty and A. Gilchrist, Phys. Rev. A **78**, 052122 (2008).

[111] E. Bagan, A. Monras and R. Munoz-Tapia, Phys. Rev. A **71**, 062318 (2005).

[112] D. Bruss, M. Cinchetti, G. D'Ariano and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).

[113] J. Bae and A. Acin, Phys. Rev. Lett. **97**, 030402 (2006).

[114] R. Demkowicz-Dobrzanski, Phys. Rev. A **71**, 062321 (2005).

[115] D. Bruss, A. Ekert and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

[116] M. Horodecki and R. Horodecki, Phys. Lett. A **244**, 473 (1998).

[117] R. Werner, Phys. Rev. A **40**, 4277 (1989).

[118] C. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[119] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[120] M. B. Plenio and S. Virmani, Quantum Information & Computation **7**, 1 (2007).

[121] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[122] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).

[123] W. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[124] G. Vidal and R. Werner, Phys. Rev. A **65**, 032314 (2002).

[125] F. Verstraete, K. Audenaert, J. Dehaene and B. De Moor, J. Phys. A **34**, 10327 (2001).

[126] W. Dur, G. Vidal and J. Cirac, Phys. Rev. A **62**, 062314 (2000).

[127] J.-M. Cai, Z.-W. Zhou and G.-C. Guo, Phys. Lett. A **363**, 392 (2007).

[128] D. Bruss and C. Macchiavello, Found. Phys. **33**, 1617 (2003).

[129] A. Barenco, A. Ekert, K.-A. Suominen and P. Torma, Phys. Rev. A **54**, 139 (1996).

[130] V. Buzek, M. Hillery and P. Knight, Fortschr. Phys. **46**, 521 (1998).

[131] K. Maruyama and P. Knight, Phys. Rev. A **67**, 032303 (2003).