JOURNAL OF MODERN OPTICS, 2000, VOL. 47, NO. 2/3, 187–209

Asymmetric quantum cloning in any dimension

NICOLAS J. CERF

[1]Ecole Polytechnique, Université Libre de Bruxelles, 1050 Bruxelles, Belgium, [2]Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, CA 91125, USA and [3]Information and Computing Technologies Research Section, Jet Propulsion Laboratory, Pasadena, CA 91109, USA

(*Received 31 March 1999; revision received 2 August 1999*)

Abstract. A family of asymmetric cloning machines for N-dimensional quantum states is introduced. These machines produce two imperfect copies of a single state that emerge from non-identical Heisenberg channels. The trade-off between the quality of the copies imposed by quantum mechanics is shown to result from a complementarity akin to the Heisenberg uncertainty principle. More specifically, the probability distributions of the error operators affecting the two copies are the square modulus of two functions related by a Fourier transform. A no-cloning inequality is derived for the special case of isotropic cloners, quantifying the impossibility of perfect cloning: if π_a and π_b are the depolarizing fractions associated with the two copies, the domain in $(\pi_a^{1/2}, \pi_b^{1/2})$-space located inside a particular ellipse representing close-to-perfect cloning is forbidden. More generally, an entropic no-cloning uncertainty relation is also discussed. Finally, the class of asymmetric cloning machines for quantum bits is investigated in detail, and a connection with the capacity of the Pauli channel is displayed.

1. Introduction

A fundamental property of quantum information is that it cannot be copied, in contrast with information we are used to in classical physics. This means that there exists no physical process that can produce perfect copies of a system that is initially in an *unknown* quantum state. This so-called *no-cloning* theorem, recognized by Dieks [1] and Wootters and Zurek [2], is an immediate consequence of the linearity of quantum mechanics, and lies at the heart of quantum theory. Remarkably, if cloning *was* permitted, the Heisenberg uncertainty principle could then be violated by measuring conjugate observables on many copies of a single quantum system. Nevertheless, even if *perfect* quantum cloning is precluded by the uncertainty principle, it is possible to devise a cloning machine that yields *imperfect* copies of the original quantum state, that is, the cloning process necessarily introduces errors. Quantum cloning machines have recently attracted a lot of attention because of their use in connection with quantum communication and cryptography (see, e.g. [3, 4]).

To fix the ideas, consider a cloning machine that duplicates a two-state system (a quantum bit or a qubit) that is initially in an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ whose amplitudes α and β are unknown. It is easy to build a cloning machine that

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online
http://www.tandf.co.uk/JNLS/mop.htm
http://www.taylorandfrancis.com/JNLS/mop.htm

perfectly copies the two basis states $|0\rangle$ and $|1\rangle$, but then it badly duplicates the superpositions $2^{-1/2}(|0\rangle \pm |1\rangle)$. A dual cloning machine can be devised that perfectly copies these superpositions, but at the cost of an imperfect copying of the basis states. In other words, a cloning machine cannot produce perfect copies of *all* possible input states simultaneously. This being so, we may ask how well one can *approximately* duplicate the unknown state of a qubit if the quality of the copies is required to be independent of the input state. This question has been answered by Buzek and Hillery [5] who first showed that it is possible to construct a cloning machine that yields two imperfect copies of a single qubit in state $|\psi\rangle$. Specifically, they defined a universal cloning machine (UCM) which creates two identical copies of $|\psi\rangle$ each characterized by the same density operator $\rho = (2/3)|\psi\rangle\langle\psi| + \mathbb{1}/6$. This machine is called *universal* because it produces copies that are *state-independent*: the fidelity of cloning $f \equiv \langle\psi|\rho|\psi\rangle = 5/6$ does not depend on the input state. Equivalently, the two output qubits of the UCM can be viewed as emerging from a depolarizing channel of probability 1/4, that is, a channel whose errors are *isotropic* (the Bloch vector characterizing the state $|\psi\rangle$ is shrunk by a factor 2/3 regardless of its orientation). The UCM was later proved to be optimal by Bruss *et al.* [4] and Gisin and Massar [6], when the quality of a cloner is measured by the fidelity f. The concept of approximate cloning was also extended to optimal m-to-n cloners, which produce m imperfect copies from n identical original qubits [6]. Recently, the optimal cloning of quantum bits was generalized to quantum systems of arbitrary dimensions by Buzek and Hillery [7] (1-to-2 universal cloner), and Werner [8] (m-to-n optimal cloners).

In this paper, we introduce a family of *asymmetric* cloning machines that produce two *non-identical* (approximate) copies of the state of an N-dimensional quantum system. This is in contrast with the cloning machines considered so far, which are symmetric (the copies being identical, or characterized by the same density operator) and isotropic (the copies being state-independent)†. The two copies created by our cloning machines emerge from noisy quantum channels that are defined with a basis of N^2 error operators on N-dimensional inputs that form a Heisenberg group (see [10]). We refer to these channels as *Heisenberg* channels, and the corresponding cloners as *Heisenberg* cloning machines (HCM). A Heisenberg channel is characterized by the N^2-dimensional probability distribution $\mathbf{p}$ of error operators which a quantum state undergoes in the channel. In general, the complementarity between the two copies produced by an asymmetric HCM is shown to result from a genuine *uncertainty principle*, much like that associated with Fourier transforms. Accordingly, the probability distributions $\mathbf{p}$ and $\mathbf{q}$ characterizing the Heisenberg channels leading to the two outputs of the cloner cannot be peaked simultaneously, giving rise to a balance between the quality of the copies. This can in particular be expressed by an entropic no-cloning uncertainty relation, $H(\mathbf{p}) + H(\mathbf{q}) \geq \log_2(N^2)$, where $H(\cdot)$ stands for the Shannon entropy.

In section 2, we discuss the asymmetric cloning of two-dimensional quantum states, in order to prepare the ground for extension to N dimensions. We introduce a *Pauli* cloning machine (PCM) [11], which produces two (generally non-identical)

† A recent study of asymmetric and anisotropic cloning of qubits has been carried out independently by Niu and Griffiths [9].

output qubits, each emerging from a *Pauli* channel. A Pauli channel is a special case ($N = 2$) of a Heisenberg channel which is defined by the four-element group of error operators for qubits, generated by the bit/phase flip errors (see section 2.1). The family of PCMs relies on a parametrization of 4-qubit wave functions for which all qubit pairs are in a mixture of Bell states. In particular, the subclass of *isotropic* asymmetric PCMs is used in order to derive a tight no-cloning inequality for qubits (see equation (1) for $N = 2$). The subclass of *symmetric* (but anisotropic) PCMs is then used to express an upper bound on the quantum capacity of a Pauli channel, generalizing the considerations of Bruss *et al.* [4] for a depolarizing channel.

In section 3, we generalize the Pauli cloning machine to systems of arbitrary dimensions, and define a family of asymmetric Heisenberg cloning machines for N-dimensional states. Our description is based on the N^2 maximally-entangled states of two N-dimensional systems which generalize the Bell states, and the corresponding Heisenberg group of error operators in N dimensions [10]. The family of asymmetric HCMs is used to investigate the complementarity principle governing the trade-off between the quality of the copies of a single N-dimensional state imposed by quantum mechanics. In particular, using a special class of *isotropic* asymmetric HCMs, i.e. cloners whose outputs emerge from (distinct) depolarizing channels, we derive a no-cloning inequality:

$$a^2 + 2ab/N + b^2 \geq 1, \tag{1}$$

where $\pi_a = a^2$ and $\pi_b = b^2$ are the depolarizing fractions of the channels associated with outputs A and B, respectively. It is a tight inequality for all isotropic cloning machines, which is saturated with the HCMs. The corresponding ellipse in (a,b)-space tends to a circle when copying N-dimensional states with $N \to \infty$, which has a simple semi-classical interpretation. The optimal N-dimensional UCM [7, 8] is shown to be a special case (symmetric and isotropic) of these cloners.

2. Pauli cloning machines for quantum bits

2.1. *Characterization of a Pauli channel using the Bell states*

Consider a quantum bit in an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ which is processed by a Pauli channel [11]. A Pauli channel is defined using a group of four error operators (the three Pauli matrices $\sigma_{x,y,z}$ and the identity $\mathbb{1}$), namely it acts on state $|\psi\rangle$ by either rotating it by one of the Pauli matrices or leaving it unchanged. Specifically, the input qubit undergoes a phase-flip (σ_z), a bit-flip (σ_x), or their combination ($\sigma_x\sigma_z = -i\sigma_y$) with respective probabilities p_z, p_x, and p_y, or remains unchanged with probability $p = 1 - p_x - p_y - p_z$. A depolarizing channel corresponds to the special case where $p_x = p_y = p_z$. It is very convenient to describe the operation of a Pauli channel by considering an input qubit X maximally entangled with a reference qubit R (see figure 1). Indeed, a remarkable property of entanglement is that by applying a unitary transformation on just one qubit of a two-qubit system, one can transform any maximally-entangled state into another. Denoting the four maximally-entangled states of two qubits (or Bell states) as

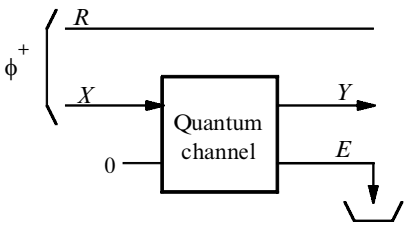

Figure 1. Quantum Pauli channel of input X (initially entangled with a reference R) and output Y. The quantum system E represents an 'environment', initially in a pure state $|0\rangle$, which is traced over so that ρ_{RY} ends up as a Bell mixture.

$$|\Phi^{\pm}\rangle = 2^{-1/2}(|00\rangle \pm |11\rangle),$$
$$|\Psi^{\pm}\rangle = 2^{-1/2}(|01\rangle \pm |10\rangle), \tag{2}$$

it is easy to check that the *local* action of the error operators on one of them, say $|\Phi^+\rangle$, yields the three remaining Bell states, namely†

$$(\mathbb{1} \otimes \sigma_z)|\Phi^+\rangle = |\Phi^-\rangle,$$
$$(\mathbb{1} \otimes \sigma_x)|\Phi^+\rangle = |\Psi^+\rangle, \tag{3}$$
$$(\mathbb{1} \otimes \sigma_x\sigma_z)|\Phi^+\rangle = |\Psi^-\rangle.$$

Therefore, if the input qubit X of the Pauli channel is maximally entangled with a reference qubit R that is unchanged while X is processed by the channel, say if their joint state is

$$|\psi\rangle_{RX} = |\Phi^+\rangle, \tag{4}$$

then the joint state of R and the output Y is a mixture of the four Bell states

$$\rho_{RY} = (1-p)|\Phi^+\rangle\langle\Phi^+| + p_z|\Phi^-\rangle\langle\Phi^-| + p_x|\Psi^+\rangle\langle\Psi^+| + p_y|\Psi^-\rangle\langle\Psi^-|, \tag{5}$$

with $p = p_x + p_y + p_z$. This Bell mixture uniquely characterizes the Pauli channel since the weights of the Bell states are simply the probabilities associated with the four error operators. This alternate description of a Pauli channel based on Bell mixtures happens to be very useful when considering quantum cloning machines.

A simple correspondence rule can be written relating an arbitrary mixture of Bell states and the associated operation on a qubit $|\psi\rangle$ by a Pauli channel. Start from the Bell mixture

$$\rho_{RY} = (1-p)|\Phi^+\rangle\langle\Phi^+| + \sum_{i=1}^{3} p_i|\Psi_i\rangle\langle\Psi_i|, \tag{6}$$

where $p_1 \le p_2 \le p_3$, $p = p_1 + p_2 + p_3$, and $|\Psi_i\rangle$ stand for the three remaining Bell states ranked by increasing weight. It is straightforward to show that the operation performed by the corresponding channel on an arbitrary state $|\psi\rangle$ is

$$|\psi\rangle \to \rho = (1-p-p_2)|\psi\rangle\langle\psi| + (p_2-p_1)\,\sigma_1|\psi_\perp\rangle\langle\psi_\perp|\sigma_1$$
$$+ (p_3-p_2)\,\sigma_3|\psi\rangle\langle\psi|\sigma_3 + 2(p_1+p_2)\,\mathbb{1}/2, \tag{7}$$

† Note that we use the convention $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$.

where $|\psi_\perp\rangle = -i\sigma_y|\psi^*\rangle = \sigma_x\sigma_z|\psi^*\rangle$ denotes the time-reversed of state $|\psi\rangle$, and σ_i stand for the three Pauli matrices ordered according to p_i (using the correspondence between σ_i and $|\Psi_i\rangle$ given by equation (3)). Thus, the output state ρ is a mixture of four components which correspond respectively to the unchanged, (rotated) time-reversed, rotated, and random fractions.

It is clear from equation (7) that the operation of the channel is *state-independent* only if $p_1 = p_2 = p_3 = p/3$, that is, if the time-reversed and rotated fractions vanish. Then, we have a *depolarizing* channel of probability p, i.e. ρ_{RY} is a Werner state and equation (7) becomes

$$|\psi\rangle \rightarrow \rho = (1 - 4p/3)|\psi\rangle\langle\psi| + (4p/3)\mathbb{1}/2. \tag{8}$$

Thus, the qubit is replaced by a random bit with probability $\pi = 4p/3$ and left unchanged otherwise. (This quantity π is named the *depolarizing fraction*.) Equivalently, the vector characterizing the input qubit in the Bloch sphere is shrunk by a *scaling factor* $s = 1 - 4p/3$ regardless of its orientation, so that the fidelity of the channel, $f = \langle\psi|\rho|\psi\rangle = 1 - 2p/3 = (1 + s)/2$, is independent of the input state. Other channels are necessarily *state dependent*. For example, the '2-Pauli' channel of probability p (i.e. $p_x = p_z = p/2$ and $p_y = 0$) performs the operation

$$\begin{aligned} |\psi\rangle \rightarrow \rho &= (1 - 3p/2)|\psi\rangle\langle\psi| + (p/2)\sigma_y|\psi_\perp\rangle\langle\psi_\perp|\sigma_y + p\,\mathbb{1}/2 \\ &= (1 - 3p/2)|\psi\rangle\langle\psi| + (p/2)|\psi^*\rangle\langle\psi^*| + p\mathbb{1}/2, \end{aligned} \tag{9}$$

while the *dephasing* channel of probability p (i.e. $p_z = p$ and $p_x = p_y = 0$) simply gives

$$|\psi\rangle \rightarrow (1 - p)|\psi\rangle\langle\psi| + p\sigma_z|\psi\rangle\langle\psi|\sigma_z. \tag{10}$$

2.2. *Asymmetric Pauli cloning machines*

We define an *asymmetric* Pauli cloning machine as a machine whose two outputs, A and B, emerge from distinct Pauli channels [11]. Thus, if the input X of the cloner is fully entangled with a reference R, i.e. $|\psi\rangle_{RX} = |\Phi^+\rangle$, the density operators ρ_{RA} and ρ_{RB} must then be mixtures of Bell states. Focusing on the first output A, we see that a 4-dimensional additional Hilbert space is *necessary* in general to 'purify' ρ_{RA} since we need to accommodate its four (generally non-zero) eigenvalues†. The 2-dimensional space of the second output qubit B is thus insufficient for this purpose, so that we must introduce an additional system C of dimension $d_C \geq 2$, which may be viewed as an ancilla or the cloning machine itself.

In the following, we will restrict our attention to Pauli cloning machines constructed with a single additional qubit C, i.e. $d_C = 2$. It happens that a 2-dimensional space for the cloning machine is actually *sufficient* when considering optimal cloners‡. Since we are mainly concerned with optimal PCMs, this

† In other words, if ρ_{RA} results from the partial trace of a pure state in an extended Hilbert space, this space must be at least 16-dimensional as a consequence of the Schmidt decomposition [12].

‡ The fact that optimal cloning can be achieved by a PCM that requires only a one-qubit ancilla was shown by Niu and Griffiths [9] after completion of this work, generalizing what was shown by Bruss *et al.* for the UCM [4].

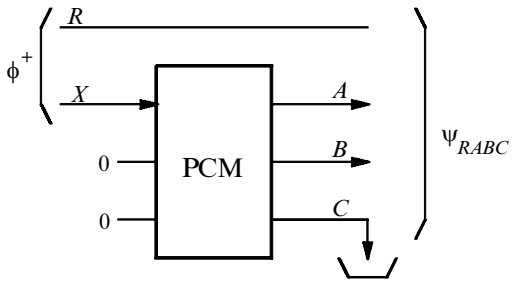

Figure 2. Pauli cloning machine of input X (initially entangled with a reference R) and outputs A and B. The third output C refers to an ancilla or the cloning machine. The three outputs emerge in general from distinct Pauli channels.

restriction is unimportant. Thus, in the following, we will consider PCMs whose operation is fully described by a 4-qubit system ($RABC$), as pictured in figure 2. The qubits R and X are initially in the entangled state $|\Phi^+\rangle$, the two auxiliary qubits being in a prescribed state, e.g. $|0\rangle$. After cloning, the four qubits R, A, B, and C are in a pure state for which ρ_{RA} and ρ_{RB} are mixtures of Bell states (i.e. A and B emerge from a Pauli channel). We will also assume ρ_{RC} to be a Bell mixture, so that C can be viewed as a third output emerging from another Pauli channel.

Instead of specifying a Pauli cloning machine by a particular unitary transformation acting on an arbitrary input state $|\psi\rangle$ (together with the two auxiliary qubits in state $|0\rangle$), here we characterize a PCM by the wave function $|\Psi\rangle_{RABC}$ underlying the entanglement of the three outputs with R. Our problem is thus to find the 4-qubit wave functions that satisfy the requirement that the state of every qubit pair is a mixture of the four Bell states. (It is not necessary that all pairs among $RABC$ are Bell mixtures, but we make this additional requirement here). Making use of the Schmidt decomposition [12] of $|\Psi\rangle_{RABC}$ for the bipartite partition RA versus BC, we see that this state can be written as a superposition of *double Bell* states

$$|\Psi\rangle_{RA;BC} = \{v\,|\Phi^+\rangle|\Phi^+\rangle + z\,|\Phi^-\rangle|\Phi^-\rangle + x\,|\Psi^+\rangle|\Psi^+\rangle + y\,|\Psi^-\rangle|\Psi^-\rangle\}_{RA;BC}, \quad (11)$$

where x, y, z and v are complex amplitudes (with $|x|^2 + |y|^2 + |z|^2 + |v|^2 = 1$). Note that the possible permutations of the Bell states in equation (11) are not considered here for simplicity. The requirement that the qubit pairs RA and BC are Bell mixtures is thus satisfied, that is, $\rho_{RA} = \rho_{BC}$ is of the form of equation (5) with $p_x = |x|^2$, $p_y = |y|^2$, $p_z = |z|^2$, and $1 - p = |v|^2$. A remarkable feature of these double Bell states is that they transform into superpositions of double Bell states for the two remaining partitions of the four qubits $RABC$ into two pairs (RB versus AC, RC versus AB). This implies that $|\Psi\rangle_{RABC}$ is also a superposition of double Bell states (albeit with different amplitudes) for these two partitions, which, therefore, also yield mixtures of Bell states when tracing over half of the system. Specifically, for the partition RB versus AC, we obtain

$$|\Psi\rangle_{RB;AC} = \{v'\,|\Phi^+\rangle|\Phi^+\rangle + z'\,|\Phi^-\rangle|\Phi^-\rangle + x'\,|\Psi^+\rangle|\Psi^+\rangle + y'\,|\Psi^-\rangle|\Psi^-\rangle\}_{RB;AC}, \quad (12)$$

with

$$\begin{aligned} v' &= (v + z + x + y)/2, \\ z' &= (v + z - x - y)/2, \\ x' &= (v - z + x - y)/2, \\ y' &= (v - z - x + y)/2, \end{aligned} \tag{13}$$

implying that the second output B emerges from a Pauli channel with probabilities $q_x = |x'|^2$, $q_y = |y'|^2$ and $q_z = |z'|^2$. Similarly, the third output C is described by considering the partition RC versus AB,

$$|\Psi\rangle_{RC;AB} = \{v''|\Phi^+\rangle|\Phi^+\rangle + z''|\Phi^-\rangle|\Phi^-\rangle + x''|\Psi^+\rangle|\Psi^+\rangle + y''|\Psi^-\rangle|\Psi^-\rangle\}_{RC;AB}, \tag{14}$$

with

$$\begin{aligned} v'' &= (v + z + x - y)/2, \\ z'' &= (v + z - x + y)/2, \\ x'' &= (v - z + x + y)/2, \\ y'' &= (v - z - x - y)/2. \end{aligned} \tag{15}$$

Thus, equations (13) and (15) relate the amplitudes of the double Bell states for the three possible partitions of the four qubits into two pairs, and thereby specify the entire set of asymmetric Pauli cloning machines considered here.

We now have the tools to analyse the complementarity between the two copies produced by an asymmetric PCM. Let us rewrite the amplitudes of $|\psi\rangle_{RA;BC}$ as a two-dimensional discrete function $\alpha_{m,n}$ with $m,n = 0,1$:

$$|\Psi\rangle_{RA;BC} = \left\{\alpha_{0,0}|\Phi^+\rangle|\Phi^+\rangle + \alpha_{0,1}|\Phi^-\rangle|\Phi^-\rangle + \alpha_{1,0}|\Psi^+\rangle|\Psi^+\rangle + \alpha_{1,1}|\Psi^-\rangle|\Psi^-\rangle\right\}_{RA;BC}. \tag{16}$$

Thus, output A emerges from a Pauli channel characterized by the probability distribution $p_{m,n} = |\alpha_{m,n}|^2$, where $p_{0,1} = p_z$, $p_{1,0} = p_x$, $p_{1,1} = p_y$, and $p_{0,0}$ is simply the probability that the qubit remains unchanged. Similarly, letting

$$|\Psi\rangle_{RB;AC} = \left\{\beta_{0,0}|\Phi^+\rangle|\Phi^+\rangle + \beta_{0,1}|\Phi^-\rangle|\Phi^-\rangle + \beta_{1,0}|\Psi^+\rangle|\Psi^+\rangle + \beta_{1,1}|\Psi^-\rangle|\Psi^-\rangle\right\}_{RB;AC}, \tag{17}$$

output B can be characterized by the two-dimensional probability distribution $q_{m,n} = |\beta_{m,n}|^2$. Using this notation, it appears that equation (13) is simply a two-dimensional discrete Fourier transform†,

$$\beta_{m,n} = \frac{1}{2}\sum_{x=0}^{1}\sum_{y=0}^{1}(-1)^{nx+my}\alpha_{x,y}. \tag{18}$$

This emphasizes that, if output A is close to perfect ($\alpha_{m,n}$ is a peaked function), then output B is very noisy ($\beta_{m,n}$ is a flat function), and vice versa. Consequently, the probability distributions $p_{m,n} = |\alpha_{m,n}|^2$ and $q_{m,n} = |\beta_{m,n}|^2$ characterizing the channels leading to outputs A and B cannot have a variance simultaneously

† Equation (18) is a 2-dimensional discrete Fourier transform if it is understood that m is dual to y (n is dual to x).

tending to zero, giving rise to an *uncertainty principle* governing the trade-off between the quality of the copies. This will be shown to hold for N-dimensional cloning machines in section 3.2.

2.3. *No-cloning inequality for quantum bits*

To illustrate this complementarity between the two copies, let us consider the class of *isotropic* asymmetric PCMs, i.e. cloners whose outputs A and B emerge from (distinct) *depolarizing* channels. The corresponding set of conditions is

$$\begin{aligned} |\alpha_{0,1}| &= |\alpha_{1,0}| = |\alpha_{1,1}|, \\ |\beta_{0,1}| &= |\beta_{1,0}| = |\beta_{1,1}|. \end{aligned} \tag{19}$$

Note that the transformation defined by equation (18),

$$\begin{pmatrix} \beta_{0,0} \\ \beta_{0,1} \\ \beta_{1,0} \\ \beta_{1,1} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \begin{pmatrix} \alpha_{0,0} \\ \alpha_{0,1} \\ \alpha_{1,0} \\ \alpha_{1,1} \end{pmatrix} \tag{20}$$

admits a 3-fold degenerate eigenvalue $\lambda_1 = 1$ (associated with the eigenspace $\alpha_{0,0} = \alpha_{0,1} + \alpha_{1,0} + \alpha_{1,1}$), and an eigenvalue $\lambda_2 = -1$ (associated with the eigenvector $\alpha_{0,1} = \alpha_{1,0} = \alpha_{1,1} = -\alpha_{0,0}$). Therefore, conditions (19) hold simultaneously, if we have

$$\begin{pmatrix} \alpha_{0,0} \\ \alpha_{0,1} \\ \alpha_{1,0} \\ \alpha_{1,1} \end{pmatrix} = c \begin{pmatrix} 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \tag{21}$$

and

$$\begin{pmatrix} \beta_{0,0} \\ \beta_{0,1} \\ \beta_{1,0} \\ \beta_{1,1} \end{pmatrix} = c \begin{pmatrix} 3 \\ 1 \\ 1 \\ 1 \end{pmatrix} + d \begin{pmatrix} 1 \\ -1 \\ -1 \\ -1 \end{pmatrix}, \tag{22}$$

where c and d are complex numbers with normalization $12|c|^2 + 4|d|^2 = 1$. Note that equations (21) and (22) simply correspond to $\alpha_{0,1} = \alpha_{1,0} = \alpha_{1,1}$ and $\beta_{0,1} = \beta_{1,0} = \beta_{1,1}$, instead of equation (19). Now, equation (21) can be rewritten as

$$\begin{pmatrix} \alpha_{0,0} \\ \alpha_{0,1} \\ \alpha_{1,0} \\ \alpha_{1,1} \end{pmatrix} = \hat{a} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \frac{a}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \tag{23}$$

where $a = 2(c + d)$ and $\hat{a} = 2(c - d)$ correspond to the 'flat' (random) and 'peaked' (perfect) components of the first output, respectively. Similarly, for the second output, we can rewrite equation (22) as

$$\begin{pmatrix} \beta_{0,0} \\ \beta_{0,1} \\ \beta_{1,0} \\ \beta_{1,1} \end{pmatrix} = \hat{b} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \frac{b}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \tag{24}$$

where $b = 2(c - d)$ and $\hat{b} = 2(c + d)$ correspond again to the 'flat' and 'peaked' components. Note that $|a|^2 = \pi_a$ and $|b|^2 = \pi_b$, where π_a (π_b) is the depolarizing fraction of the channel leading to output A (B). Indeed,

$$\begin{aligned} \rho_{RA} &= (1 - |a|^2)|\Phi^+\rangle\langle\Phi^+| + |a|^2 \frac{\mathbb{1} \otimes \mathbb{1}}{4}, \\ \rho_{RB} &= (1 - |b|^2)|\Phi^+\rangle\langle\Phi^+| + |b|^2 \frac{\mathbb{1} \otimes \mathbb{1}}{4}, \end{aligned} \tag{25}$$

so that the input qubit is replaced by a random qubit with probability π_a or left unchanged with probability $1 - \pi_a$ in the channel leading to output A (and similarly for channel B). Now, using $c = (a + b)/4$, $d = (a - b)/4$, and the normalization condition, we obtain

$$|a|^2 + \mathrm{Re}(a^* b) + |b|^2 = 1, \tag{26}$$

that is, an ellipse representing a set of cloners in the (a,b)-space. By varying the relative phase θ between a and b (the global phase is irrelevant), one varies the eccentricity of this ellipse: $|a|^2 + |ab| \cos\theta + |b|^2 = 1$. Clearly, the best cloning (minimum values for the polarizing fractions $|a|^2$ and $|b|^2$) is achieved when the cross-term in equation (26) is the largest in magnitude, that is when a and b have the same (or opposite) phases. It is therefore sufficient to consider a and b real and positive if we are only interested in optimal cloners.

As a consequence, the trade-off between the quality of the copies can be described by the *no-cloning inequality*†

$$a^2 + ab + b^2 \geq 1, \tag{27}$$

where the copying error is measured by $\pi_a = a^2$ and $\pi_b = b^2$ (with $a,b \geq 0$), i.e. the *depolarizing fraction* of the channels leading to outputs A and B, respectively. This no-cloning inequality can also be recast in terms of the depolarizing probabilities. This is done by substituting $a = 2x$ and $b = 2x'$, which yields

$$x^2 + xx' + x'^2 \geq \frac{1}{4}, \tag{28}$$

where the copying error is now measured by the probability of the depolarizing channel underlying each output, i.e. $p = 3x^2 = 3\pi_a/4$ and $q = 3x'^2 = 3\pi_b/4$ (with $x,x' \geq 0$). Given that a single additional qubit C is sufficient for an optimal cloner, the imperfect cloning achieved by such an isotropic PCM is *optimal*: the PCM achieves the minimum p and q for a fixed ratio p/q. Thus, equation (27) or (28) is the tightest no-cloning bound that can be written for a qubit‡.

† The no-cloning inequality associated with N-dimensional quantum states (instead of qubits) will be investigated in section 3.3. There, we will see that the cross-term in equation (27) is simply replaced by $2ab/N$, implying that the ellipse tends to a circle of radius one at the limit of large N.

‡ Equation (28) has been independently derived by Niu and Griffiths in [9], where it was shown that a single qubit is sufficient for C.

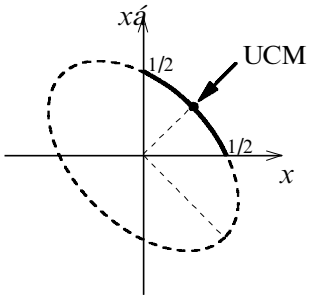

Figure 3. No-cloning inequality for a qubit. The ellipse characterizes the best asymmetric PCMs, whose outputs emerge from depolarizing channels of probability $p = 3x^2$ and $q = 3x'2$ (only the quadrant $x, x' \geq 0$ is of interest here). Any close-to-perfect cloning characterized by a point inside the ellipse is forbidden.

Equation (28) corresponds to the domain in the (x,x')-space located outside an ellipse whose semiminor axis, oriented in the direction $(1,1)$, is $6^{-1/2}$, as shown in figure 3. (The semi-major axis is $2^{-1/2}$.) The origin in this space corresponds to a (non-existent) cloner whose two outputs would be perfect $p = q = 0$, while to distance to origin measures $(p + q)/3$. The ellipse characterizes the ensemble of values for p and q that can be achieved with an optimal PCM. It crosses the x-axis at $(1/2,0)$, which describes the situation where the first output emerges from a 100%-depolarizing channel ($p = 3/4$) while the second emerges from a perfect channel ($q = 0$). Of course, $(0,1/2)$ corresponds to the symmetric situation. This ellipse intercepts its minor axis at $(12^{-1/2},12^{-1/2})$, which corresponds to the universal cloning machine (UCM), i.e. $p = q = 1/4$. This point is the closest to the origin (i.e. the cloner with minimum $p + q$), and characterizes in this sense the best possible cloner. Equivalently, the ellipse corresponding to equation (27) crosses the axes at $(0,1)$ and $(1,0)$, while the closest point to the origin is $(3^{-1/2},3^{-1/2})$ and coincides with the UCM (the outputs of the UCM emerge from two channels whose depolarizing fraction is $\pi_a = \pi_b = 1/3$).

Introducing a phase difference between x and x' results in a set of PCMs characterized by an ellipse which is less eccentric and tends to a circle of radius $1/2$ for a phase difference of $\pi/2$. Consequently, the no-cloning inequality (28) is saturated when x and x' have the same (or opposite) phase. The domain inside the ellipse corresponds therefore to the values for p and q that cannot be achieved simultaneously, reflecting the impossibility of close-to-perfect cloning. Note that the UCM is the only symmetric cloner belonging to the class of isotropic PCMs considered here (i.e. cloners whose outputs are depolarizing channels); other symmetric—but anisotropic—cloners will be considered in section 2.5.

2.4. *No-cloning uncertainty relation*

The complementarity between index m of $\alpha_{m,n}$ and index n of $\beta_{m,n}$ (or conversely) implied by equation (18) can be expressed explicitly by using the Robertson uncertainty relation

$$\langle \Delta O_A^2 \rangle \langle \Delta O_B^2 \rangle \geq \tfrac{1}{4} |\langle [O_A, O_B] \rangle|^2, \tag{29}$$

where O_A and O_B are any two observables, while $\Delta O_A = O_A - \langle O_A \rangle$, and $\Delta O_B = O_B - \langle O_B \rangle$. This relation holds when the quantum expectation values are taken for any quantum state. Consider the 2-qubit state $|\xi\rangle = v|00\rangle + z|01\rangle + x|10\rangle + y|11\rangle$, and choose $O_A = \sigma_z/2 \otimes \mathbb{1}$ and $O_B = \sigma_x/2 \otimes \mathbb{1}$, so that $[O_A, O_B] = i\sigma_y/2 \otimes \mathbb{1}$. Applying equation (29) to $|\xi\rangle$ yields the no-cloning uncertainty relation

$$\underbrace{(|v|^2 + |z|^2)}_{1-p_x-p_y}\underbrace{(|x|^2 + |y|^2)}_{p_x+p_y} \times \underbrace{(|v'|^2 + |x'|^2)}_{1-q_z-q_y}\underbrace{(|z'|^2 + |y'|^2)}_{q_z+q_y} \geq \tfrac{1}{4}|\mathrm{Im}(v^* x + z^* y)|^2. \quad (30)$$

The term $(1 - p_x - p_y)(p_x + p_y)$ is simply the variance of the marginal distribution $p_m = \sum_n p_{m,n}$ associated with the first output, while $(1 - q_z - q_y)(q_z + q_y)$ is the variance of $q_n = \sum_m q_{m,n}$ (associated with the second output). Thus equation (30) gives a lower bound on the product of the variances of p_m and q_n. It is easy to check that when the distribution p_m is peaked ($x = y = 0$ or $v = z = 0$), the lower bound tends to zero, as expected. The bound can also be re-expressed as

$$\tfrac{1}{4}|\mathrm{Im}(v'^* z' + x'^* y')|^2 \quad (31)$$

implying that it also tends to zero when q_n is peaked ($z' = y' = 0$ or $v' = x' = 0$). Unfortunately, the bound depends on the state $|\xi\rangle$, and is not saturated in the case of the UCM. Using equation (29) with $|\xi'\rangle = v'|00\rangle + z'|01\rangle + x'|10\rangle + y'|11\rangle$ one obtains an alternate inequality expressing the duality between $p_n = \sum_m p_{m,n}$ and $q_m = \sum_n q_{m,n}$,

$$\underbrace{(|v|^2 + |x|^2)}_{1-p_z-p_y}\underbrace{(|z|^2 + |y|^2)}_{p_z+p_y} \times \underbrace{(|v'|^2 + |z'|^2)}_{1-q_x-q_y}\underbrace{(|x'|^2 + |y'|^2)}_{q_x+q_y} \geqslant \tfrac{1}{4}|\mathrm{Im}(v^* z + x^* y)|^2. \quad (32)$$

In section 3.4, more general no-cloning uncertainty relations will be derived, based on the *entropic* uncertainty relations for non-commuting observables.

2.5. *Symmetric Pauli cloning machines*

We now consider the class of symmetric PCMs that have two outputs emerging from a *same*—but not necessarily isotropic—Pauli channel, i.e. $\rho_{RA} = \rho_{RB}$. These PCMs must satisfy the conditions $|v'| = |v|$, $|z'| = |z|$, $|x'| = |x|$, and $|y'| = |y|$. The eigenspectrum decomposition of the transformation $(v, z, x, y) \rightarrow (v', z', x', y')$ (cf. equation (20)) implies that these conditions hold for any vector in the eigenspace associated with $\lambda_1 = 1$, or for the eigenvector $x = y = z = -v = 1/2$ associated with $\lambda_2 = -1$. The latter solution corresponds to a trivial PCM whose two outputs are fully depolarizing. The interesting solution is thus

$$v = x + y + z, \quad (33)$$

where x, y, z and v can be assumed to be real. Equation (33), together with the normalization condition, describes a two-dimensional surface in a space where each point (x, y, z) represents a Pauli channel of parameters $p_x = x^2$, $p_y = y^2$ and $p_z = z^2$. (We only consider here the first octant $x, y, z \geq 0$). This surface,

$$x^2 + y^2 + z^2 + xy + xz + yz = \tfrac{1}{2}, \quad (34)$$

is an oblate ellipsoid E with symmetry axis along the direction $(1, 1, 1)$, as shown in figure 4. The semi-minor axis (or polar radius) is $1/2$ while the semi-major axis (or equatorial radius) is 1. In this representation, the distance to the origin is

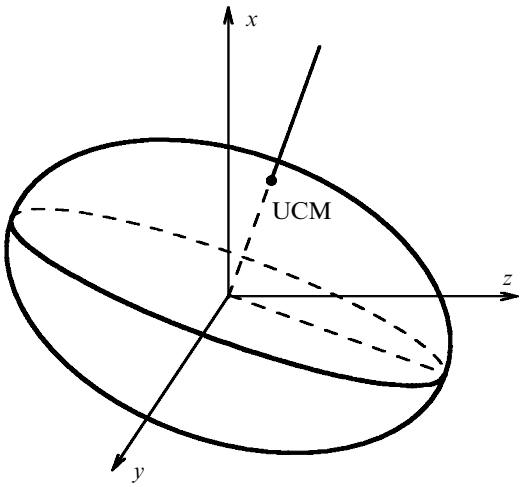

Figure 4. Oblate ellipsoid representing the class of symmetric PCMs whose two outputs emerge from a Pauli channel of parameters $p_x = x^2$, $p_y = y^2$ and $p_z = z^2$ (only the octant $x,y,z \geq 0$ is considered here). The pole of this ellipsoid corresponds to the UCM. (The capacity of a Pauli channel that lies on this ellipsoid must be vanishing, as shown in Appendix A.)

$p_x + p_y + p_z$, so that the pole $(12^{-1/2}, 12^{-1/2}, 12^{-1/2})$ of this ellipsoid—the closest point to the origin—corresponds to a depolarizing channel of probability $p = 1/4$. Thus, this particular symmetric PCM reduces to the UCM and is isotropic. This simply illustrates that the requirement of having an optimal cloning (minimum $p_x + p_y + p_z$) implies that the cloner is state-independent ($p_x = p_y = p_z$). The parametric equations of ellipsoid E are

$$\begin{aligned} x &= \left(\frac{1}{12}\right)^{1/2} \cos(\theta) + \left(\frac{2}{3}\right)^{1/2} \sin(\theta)\, \cos(\phi), \\ y &= \left(\frac{1}{12}\right)^{1/2} \cos(\theta) + \left(\frac{2}{3}\right)^{1/2} \sin(\theta)\, \cos(\phi + 2\pi/3), \\ z &= \left(\frac{1}{12}\right)^{1/2} \cos(\theta) + \left(\frac{2}{3}\right)^{1/2} \sin(\theta)\, \cos(\phi + 4\pi/3), \end{aligned} \tag{35}$$

where the polar angle θ measures the 'distance' from the depolarizing channel underlying the UCM ($\theta = 0$ implies $p_x = p_y = p_z$), while the azimuthal angle ϕ characterizes the distribution among p_x, p_y, and p_z.

It has been shown in [4] that an interesting application of the UCM is that it can be used to establish an upper limit on the quantum capacity C of a depolarizing channel, namely $C = 0$ at $p = 1/4$. This result simply relies on the fact that the UCM is symmetric, so that it is natural to extend it to all symmetric PCMs. In Appendix A, we will show that the capacity of the Pauli channel with probabilities $p_x = x^2$, $p_y = y^2$ and $p_z = z^2$, vanishes if (x,y,z) lies on ellipsoid (34), which yields an upper bound on C, namely

$$C \leq 1 - 2(x^2 + y^2 + z^2 + xy + xz + yz). \tag{36}$$

In Appendix B, we show that the UCM can be obtained alternatively by requiring that symmetric PCM is such that the joint state of its two outputs A and B is as close to a product state as possible. The 4-qubit wave function $|\Psi\rangle_{RABC}$ underlying the UCM is analysed in details. Finally, in Appendix C, it is shown that if one requires the PCM to be fully symmetric (i.e. its *three* outputs emerge from the same Pauli channel), one obtains a one-dimensional class of quantum triplicators. We also exhibit the best triplicator within this class, whose three outputs emerge from a '2-Pauli' channel with $p = 1/3$.

3. Heisenberg cloning machines for N-dimensional states

3.1. *Channel characterization using maximally-entangled states*

Consider now the cloning of the state of an N-dimensional system. In order to follow our previous discussion for quantum bits ($N = 2$), we first need to generalize the Bell states and introduce a set of N^2 maximally-entangled (ME) states of two N-dimensional systems, A and B:

$$|\psi_{m,n}\rangle_{AB} = \frac{1}{N^{1/2}} \sum_{j=0}^{N-1} \exp[2\pi i(jn/N)]\,|j\rangle_A |j+m\rangle_B, \tag{37}$$

where the indices m and n ($m,n = 0,\ldots,N-1$) label the N^2 states. Note that, here and below, the ket labels are taken modulo N. Taking the partial trace of any state $|\psi_{m,n}\rangle\langle\psi_{m,n}|$ results in a density operator for A or B given by

$$\rho_A = \rho_B = \frac{1}{N} \sum_{j=0}^{N-1} |j\rangle\langle j| = \mathbb{1}/N \tag{38}$$

implying that A and B are maximally entangled. It is easy to check that the $|\psi_{m,n}\rangle$ are orthonormal and form a complete basis in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. The resolution of identity simply reads

$$\begin{aligned}
\sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle\langle\psi_{m,n}| &= \frac{1}{N} \sum_{m,n} \sum_{j,j'} \exp\{2\pi i[(j-j')n/N]\}\,|j\rangle\langle j'| \otimes |j+m\rangle\langle j'+m| \\
&= \frac{1}{N} \sum_{k,n} \sum_{j,j'} \exp\{2\pi i[(j-j')n/N]\}\,|j\rangle\langle j'| \otimes |k\rangle\langle k+j'-j| \\
&= \sum_{k,j} |j\rangle\langle j| \otimes |k\rangle\langle k| \\
&= \mathbb{1}_A \otimes \mathbb{1}_B,
\end{aligned} \tag{39}$$

where we have made the substitution $j + m = k$ and used the identity

$$\sum_{n=0}^{N-1} \exp\{2\pi i[(j-j')n/N]\} = N\delta_{j,j'}. \tag{40}$$

The maximally-entangled (ME) states $|\psi_{m,n}\rangle$ generalize the Bell states for $N > 2$: in the special case of two maximally-entangled qubits ($N = 2$), we simply have the equivalence $|\psi_{0,0}\rangle = |\Phi^+\rangle$, $|\psi_{0,1}\rangle = |\Phi^-\rangle$, $|\psi_{1,0}\rangle = |\Psi^+\rangle$, and $|\psi_{1,1}\rangle = |\Psi^-\rangle$.

We now describe a quantum Heisenberg channel that processes N-dimensional states by using the correspondence between these ME states and the (Heisenberg)

group of error operators $U_{m,n}$ on an N-dimensional state [10]. In such a channel, an arbitrary state $|\psi\rangle$ undergoes a particular unitary transformation (or error)

$$U_{m,n} = \sum_{k=0}^{N-1} \exp[2\pi i(kn/N)]|k+m\rangle\langle k| \tag{41}$$

with probability $p_{m,n}$ (with $\sum_{m,n} p_{m,n} = 1$). Note that $U_{0,0} = \mathbb{1}$, implying that $|\psi\rangle$ is left unchanged with probability $p_{0,0}$. These error operators generalize the Pauli matrices for qubits: m labels the 'shift' errors (generalizing the bit flip σ_x) while n labels the phase errors (generalizing the sign flip σ_z). If the input of channel X is maximally entangled with a reference R (an N-dimensional system) so that their joint state is $|\psi_{0,0}\rangle = \sum_j |j\rangle|j\rangle/N^{1/2}$, then the joint state of the output Y and R is simply a mixture of the N^2 ME states,

$$\rho_{RY} = \sum_{m,n} p_{m,n}|\psi_{m,n}\rangle\langle\psi_{m,n}| \tag{42}$$

generalizing the mixture of Bell states that we had for qubits in section 2.1. Indeed, applying $U_{m,n}$ *locally* (i.e. to one subsystem, leaving the other unchanged) transforms $|\psi_{0,0}\rangle$ into another ME state,

$$(\mathbb{1} \otimes U_{m,n})|\psi_{0,0}\rangle = |\psi_{m,n}\rangle \tag{43}$$

extending equation (3) to $N > 2$. This allows us to treat the cloning of N-dimensional states following closely section 2.2, that is, by considering a 4-partite pure state, namely the state of a reference system R (initially entangled with the input X), the two outputs A and B, and the cloning machine (or a third output) C. Note that, using the same reasoning as in section 2.2, it appears that the minimum size required for the Hilbert space of the cloning machine is N. In order to purify ρ_{RA}, we need an N^2-dimensional additional space whereas B is only N-dimensional, so that an additional N-dimensional ancilla is *necessary*. We conjecture that it is also sufficient for *optimal* Heisenberg cloning machines, as for Pauli cloning machines†. Consequently, we consider a pure state in an N^4-dimensional Hilbert space in order to characterize the entire set of N-dimensional Heisenberg cloning machines.

3.2. *Asymmetric Heisenberg cloning machines*

We start by expressing the joint state of the four N-dimensional systems R, A, B and C, as a superposition of double-ME states:

$$|\Psi\rangle_{RA;BC} = \sum_{m,n=0}^{N-1} \alpha_{m,n}|\psi_{m,n}\rangle_{RA}|\psi_{m,N-n}\rangle_{BC}, \tag{44}$$

where the $\alpha_{m,n}$ are (arbitrary) complex amplitudes such that $\sum_{m,n}|\alpha_{m,n}|^2 = 1$. This expression reduces to equation (16) for $N = 2$. By tracing the state (44) over B and C, we see that the joint state of R and A is a mixture of the ME states,

$$\rho_{RA} = \sum_{m,n=0}^{N-1} |\alpha_{m,n}|^2|\psi_{m,n}\rangle\langle\psi_{m,n}|, \tag{45}$$

† This conjecture is at least partly confirmed by the proof of optimality of the N-dimensional UCM in [8].

so that A can be viewed as the output of a Heisenberg channel which processes an input maximally entangled with R (the initial joint state being $|\psi_{0,0}\rangle$). Now, we will show that, by interchanging A and B, the joint state of the 4-partite system can be re-expressed as a superposition of double-ME states

$$|\Psi\rangle_{RB;AC} = \sum_{m,n=0}^{N-1} \beta_{m,n} |\psi_{m,n}\rangle_{RB} |\psi_{m,N-n}\rangle_{AC}, \tag{46}$$

where the amplitudes $\beta_{m,n}$ are defined by

$$\beta_{m,n} = \frac{1}{N} \sum_{x,y=0}^{N-1} \exp\{2\pi i[(nx - my)/N]\} \alpha_{x,y}. \tag{47}$$

These amplitudes characterize the quantum channel leading to the second output, B, since the joint state of R and B is again a mixture of ME states,

$$\rho_{RB} = \sum_{m,n=0}^{N-1} |\beta_{m,n}|^2 |\psi_{m,n}\rangle\langle\psi_{m,n}|. \tag{48}$$

Thus, outputs A and B of the Heisenberg cloning machine emerge from channels of respective probabilities $p_{m,n} = |\alpha_{m,n}|^2$ and $q_{m,n} = |\beta_{m,n}|^2$ which are related via equation (47). It is easy to check that equation (47) reduces to equation (18) for qubits ($N = 2$).

Let us prove equations (46) and (47) by considering a single component $|\psi_{\mu,\nu}\rangle_{RA} |\psi_{\mu,N-\nu}\rangle_{BX}$ in equation (44), that is, choosing $\alpha_{m,n} = \delta_{m,\mu}\delta_{n,\nu}$. Then, equation (47) gives $\beta_{m,n} = \exp\{2\pi i[(n\mu - m\nu)/N]\}/N$, so that equation (46) results in

$$\begin{aligned}
|\Psi\rangle_{RB;AC} &= \frac{1}{N} \sum_{m,n} \exp\{2\pi i[(n\mu - m\nu)/N]\} \, |\psi_{m,n}\rangle_{RB} |\psi_{m,N-n}\rangle_{AC} \\
&= \frac{1}{N^2} \sum_{m,n} \sum_{j,j'} \exp\{2\pi i[(n\mu - m\nu)/N]\} \\
&\quad \times \exp\{2\pi i[(j - j')n/N]\} |j\rangle_R |j + m\rangle_B |j'\rangle_A |j' + m\rangle_C \\
&= \frac{1}{N} \sum_{m,j} \exp[-2\pi i(m\nu/N)] |j\rangle_R |j + m\rangle_B |j + \mu\rangle_A |j + \mu + m\rangle_C,
\end{aligned} \tag{49}$$

where we have used $\sum_n \exp\{2\pi i[(\mu + j - j')n/N]\} = N \delta_{j+\mu,j'}$. Making the substitution $k = j + m$, we obtain

$$|\Psi\rangle_{RB;AC} = \frac{1}{N} \sum_{j,k} \exp\{2\pi i[(j - k)\nu/N]\} |j\rangle_R |k\rangle_B |j + \mu\rangle_A |k + \mu\rangle_C, \tag{50}$$

which is indeed equivalent to $|\psi_{\mu,\nu}\rangle_{RA} |\psi_{\mu,N-\nu}\rangle_{BX}$ when interchanging A and B. This proof holds for an arbitrary $\alpha_{m,n}$ as a consequence of the linearity of equation (47).

The latter equation is basically a 2-dimensional discrete Fourier transform, up to an interchange of the indices m and n (n is dual to x, while m is dual to y), and the fact that one has a Fourier transform on index y but an *inverse* Fourier

transform on index x†. The normalization of the $\beta_{m,n}$'s simply results from Parseval's theorem: $\sum_{m,n}|\alpha_{m,n}|^2 = \sum_{m,n}|\beta_{m,n}|^2$. Thus, we have shown that the *complementarity* between the two outputs A and B of an N-dimensional Heisenberg cloning machine is simply governed by the relationship between a function and its Fourier transform. This emphasizes that, if one output is close-to perfect ($\alpha_{m,n}$ is a peaked function), then the second one is very noisy ($\beta_{m,n}$ is a flat function), and vice versa. In other words, the indices of $\alpha_{m,n}$ and $\beta_{m,n}$ act as conjugate variables, so that the probability distributions characterizing the two outputs, $p_{m,n}$ and $q_{m,n}$, cannot have a variance simultaneously tending to zero. (Remember that the index m of $p_{m,n}$ is dual to the index n of $q_{m,n}$, and vice versa.) A symmetric N-dimensional HCM then corresponds simply to a function $\alpha_{m,n}$ whose modulus is equal to the modulus of its Fourier transform, i.e. $|\alpha_{m,n}| = |\beta_{m,n}|$, $\forall m,n$.

3.3. *No-cloning inequality for N-dimensional states*

We now investigate this complementarity principle in the special case of *isotropic* HCMs. Thus, the channel underlying each output is a *depolarizing* channel, that is, all the probabilities $p_{m,n}$ are equal except $p_{0,0}$ (and equivalently for $q_{m,n}$). Assume that $\alpha_{m,n}$ is the superposition of a peaked component $P_{m,n} = \delta_{m,0}\,\delta_{n,0}$ (i.e. a perfect channel) and a flat component $F_{m,n} = 1/N$ (i.e. a fully depolarizing channel), with respective amplitudes $\hat{a}$ and a:

$$\alpha_{m,n} = \hat{a}P_{m,n} + aF_{m,n}. \tag{51}$$

Note that the normalization condition $|\hat{a} + a/N|^2 + (N^2 - 1)|a/N|^2 = 1$ can be written as

$$|\hat{a}|^2 + \frac{2}{N}\,\mathrm{Re}(\hat{a}a^*) + |a|^2 = 1. \tag{52}$$

Tracing over B and C, we see that the first output is characterized by

$$\rho_{RA} = \left[|\hat{a}|^2 + \frac{2}{N}\,\mathrm{Re}(\hat{a}a^*)\right]|\psi_{0,0}\rangle\langle\psi_{0,0}| + |a|^2\,\frac{\mathbb{1}\otimes\mathbb{1}}{N^2}, \tag{53}$$

so that the input state is replaced by a random state with probability $\pi_a = |a|^2$ and left unchanged with probability $1 - \pi_a$. This is the N-dimensional generalization of a depolarizing channel: if $a = 0$, the channel is perfect, while $a = 1$ corresponds to a fully depolarizing channel. Thus, the *depolarization fraction* characterizing output A is π_a, while $s_a = 1 - \pi_a$ is simply the scaling factor for output A. Using equation (47), we see that the second output B is characterized by

$$\beta_{m,n} = \hat{b}P_{m,n} + bF_{m,n}, \tag{54}$$

where $\hat{b} = a$ and $b = \hat{a}$ since $F_{m,n}$ are $P_{m,n}$ are dual under Fourier transform. Here $\pi_b = |b|^2$ is the depolarizing fraction of the channel associated with B. Thus, the complementarity of the two outputs of the class of (asymmetric) isotropic cloners considered here can be simply written as

$$|a|^2 + \frac{2}{N}\,\mathrm{Re}(ab^*) + |b|^2 = 1. \tag{55}$$

† One has $x \xrightarrow{\mathcal{F}^{-1}} n$ and $y \xrightarrow{\mathcal{F}} m$, where $\mathcal{F}$ denotes the discrete Fourier transform.

It is easy to see that the best cloning (the smallest values for $|a|$ and $|b|$) is achieved when the cross-term is the largest in magnitude, that is, when a and b have the same phase. For simplicity, we assume that a and b are real and positive. Therefore, arguing as before, we find a *no-cloning* inequality for an N-dimensional quantum state:

$$a^2 + \frac{2}{N}ab + b^2 \geq 1, \tag{56}$$

where $\pi_a = a^2$ or $\pi_b = b^2$ are the depolarizing fractions underlying outputs A and B, respectively. Equation (56) generalizes the no-cloning inequality for qubits, equation (27). It corresponds to the domain in the (a,b)-space which is outside an ellipse, oriented just as in figure 3, whose semi-minor axis is $[N/(N+1)]^{1/2}$ and semi-major axis is $[N/(N-1)]^{1/2}$. This ellipse intercepts its minor axis at $([N/(2N+2)]^{1/2}, [N/(2N+2)]^{1/2})$, which corresponds to an N-dimensional UCM [7, 8], as discussed in section 3.5.

Note that this ellipse tends to a circle of radius one as N tends to infinity. This means that, at the limit $N \to \infty$, the sum of the depolarizing fractions cannot be lower than one, i.e. $\pi_a + \pi_b \geq 1$. The no-cloning inequality then involves an 'incoherent' sum in this limit (i.e. probabilities are added, while the cross-term disappears), which emphasizes that $N \to \infty$ can be viewed as a semi-classical limit. The optimal cloning machine (with $\pi_a + \pi_b = 1$) can then be understood in classical terms: the input state is sent to output A or B with probability $1 - \pi_a = \pi_b$ or $1 - \pi_b = \pi_a$, respectively, the other output being a random N-dimensional state. Remarkably, there is no such classical interpretation for finite-N cloners, as $(1 - \pi_a) + (1 - \pi_b)$ can then exceed one. For example, for qubits ($N = 2$), we have $\pi_a = \pi_b = 1/3$, so that the input qubit is apparently sent to each output with probability 2/3, which makes a total of 4/3 (!). In some sense, the qubit *can* be cloned with probability 1/3, which is related to the time-reversed fraction 1/3 that is found on the third output of the UCM (see Appendix B). Such a connection between the impossibility of perfect cloning and the impossibility of superluminal signalling has been exploited in [13], where it is used to derive the optimal fidelity of the UCM.

3.4. *Entropic no-cloning uncertainty relation*

As mentioned earlier, the trade-off between the quality of the two copies is the consequence of an 'uncertainty principle' inherent to Fourier transforms. We can express this uncertainty principle in general by making use of the entropic uncertainty relations for non-commuting observables [14–16]. Consider two observables O_A and O_B whose respective set of eigenvectors are $\{|a_j\rangle\}$ and $\{|b_k\rangle\}$. For any quantum state $|\psi\rangle$, the probability distributions

$$\begin{aligned} p_j &= |\langle a_j|\psi\rangle|^2, \\ q_k &= |\langle b_k|\psi\rangle|^2, \end{aligned} \tag{57}$$

associated with the measurement of O_A and O_B cannot be peaked simultaneously if O_A and O_B do not commute. The uncertainty associated with p_j and q_k can be measured by using the Shannon entropies $H[p_j] = -\sum_j p_j \log_2 p_j$ and $H[q_k] = -\sum_k q_k \log_2 q_k$. Then, the entropic inequality

$$H[p_j] + H[q_k] \geq -2\log_2(c), \quad \text{with } c = \max_{j,k} |\langle a_j|b_k\rangle|, \tag{58}$$

can be shown to hold for any state $|\psi\rangle$, thereby expressing the balance between the uncertainty of the measurement of O_A and O_B. Equation (58) can be applied to cloning by considering $|\psi\rangle = \sum_{x,y} \alpha_{x,y}|x,y\rangle$ and observables O_A and O_B with respective eigenvectors $|x,y\rangle$ and $|m,n\rangle = N^{-1}\sum_{x,y} \exp\{2\pi i[(-mx+my)/N]\}|x,y\rangle$ resulting in the entropic no-cloning uncertainty relation

$$H[p_{m,n}] + H[q_{m,n}] \geq \log_2(N^2). \tag{59}$$

Thus, the sum of the entropies of the probability distribution of the N^2 error operators affecting each of the two copies cannot be less than $\log_2(N^2)$. The bound is saturated when one copy is perfect (vanishing entropy) as the other copy corresponds then to a flat distribution (maximum entropy). Note that equation (59) is a special case of the entropic no-cloning inequality derived in [17] which applies to *any* cloning machine: $L_A + L_B \geq 2S$, where L_A and L_B are the *losses* [18] of the channels leading to the two outputs of the cloner while S is the source entropy†. Equation (59) is unfortunately not a tight bound as can be seen for the UCM for qubits ($N = 2$): we have indeed $H[p_{m,n}] = H[q_{m,n}] = 2 - \log_2(3)/2 = 1.21$ bits, so that

$$H[p_{m,n}] + H[q_{m,n}] = 2.42 > 2. \tag{60}$$

Alternate entropic no-cloning uncertainty relations can also be obtained by exploiting the fact that $p_{m,n}$ and $q_{m,n}$ are related by a 2-dimensional Fourier transform. Since the index m of $p_{m,n}$ is dual to the index n of $q_{m,n}$, we can use equation (58) with eigenvectors $|x,y\rangle$ degenerate in y and $|m,n\rangle$ degenerate in m, and consider the overlap between $|x,o\rangle$ and $N^{1/2}\sum_m |m,n\rangle$, which results in

$$H[p_m] + H[q_n] \geq \log_2(N), \tag{61}$$

with $p_m = \sum_n p_{m,n}$ and $q_n = \sum_m q_{m,n}$. Conversely, we have

$$H[p_n] + H[q_m] \geq \log_2(N), \tag{62}$$

with $p_n = \sum_m p_{m,n}$ and $q_m = \sum_n q_{m,n}$. For the UCM for qubits, p_m, p_n, q_m and q_n are all equal to $\{5/6, 1/6\}$, so that $H[p_n] = H[p_m] = H[q_n] = H[q_m] = 0.65$ bits, implying that equations (61) and (62) are not saturated.

3.5. *Symmetric cloning machine or the N-dimensional UCM*

It is easy to find the *symmetric* N-dimensional cloner of the class of isotropic HCMs (i.e. cloners whose outputs emerge from an N-dimensional depolarizing channel) by requiring that $a = b$ in equation (55), which simply results in a depolarizing fraction

$$\pi = |a|^2 = \frac{N}{2(N+1)}. \tag{63}$$

The underlying 4-partite wave function of the reference, the two outputs, and the cloner is

$$|\Psi\rangle_{RA;BC} = \hat{a}\,|\psi_{0,0}\rangle_{RA}|\psi_{0,0}\rangle_{BC} + \frac{a}{N}\sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle_{RA}|\psi_{m,N-n}\rangle_{BC}, \tag{64}$$

† In this paper, we restrict ourselves to cloners whose outputs emerge from Heisenberg channels. In that case, it is easy to show that $H[p_{m,n}]$ and $H[q_{m,n}]$ are simply the losses L_A and L_B of the channels leading to the outputs A and B of the HCM.

with $a = \hat{a} = [N/(2N+2)]^{1/2}$. Using $\sum_{m,n}|\psi_{m,n}\rangle|\psi_{m,N-n}\rangle = \sum_{j,k}|j\rangle|k\rangle|j\rangle|k\rangle$, we find that equation (64) can be rewritten as

$$|\Psi\rangle_{RA;BC} = \left(\frac{1}{2N(N+1)}\right)^{1/2}\sum_{j,k=0}^{N-1}(|j\rangle_R|j\rangle_A|k\rangle_B|k\rangle_C + |j\rangle_R|k\rangle_A|j\rangle_B|k\rangle_C), \tag{65}$$

which immediately implies that it is symmetric under the interchange of A and B, as expected. By tracing over B and C, equation (64) yields

$$\rho_{RA} = \rho_{RB} = \frac{N+2}{2(N+1)}|\psi_{0,0}\rangle\langle\psi_{0,0}| + \frac{1}{2N(N+1)}\sum_{m,n=0}^{N-1}|\psi_{m,n}\rangle\langle\psi_{m,n}|, \tag{66}$$

which shows that this cloner is state independent since it acts on an arbitrary state as

$$|\psi\rangle \to \rho = \frac{N+2}{2(N+1)}|\psi\rangle\langle\psi| + \frac{N}{2(N+1)}(\mathbb{1}/N). \tag{67}$$

Thus, the depolarizing fraction corresponding to both outputs is

$$\pi = |a|^2 = \frac{N}{2(N+1)}, \tag{68}$$

while the scaling factor is is given by

$$s = 1 - |a|^2 = \frac{N+2}{2(N+1)}, \tag{69}$$

in agreement with the expression derived in [7, 8] for the N-dimensional UCM. When $N \to \infty$, the UCM can be viewed as a classical machine that is transmitting the input state to one of the two outputs with probability 1/2, a random state being sent on the other output.

In analogy with what we have done for quantum bits ($N = 2$) in section 2.5, it should be possible to find an entire class of symmetric cloners with $N > 2$, thereby generalizing equation (34). Such a class should be based on functions that are equal (in magnitude) to their Fourier transform. For example, we have the solution $\alpha_{m,n} = g_m G_n$, where g_m is an arbitrary (normalized) N-point function, and $G_n = \sum_{m=0}^{N-1} g_m \exp(2\pi imn/N)/N^{1/2}$ is its discrete (inverse) Fourier transform. Using equation (47), it is straightforward to check that $\beta_{m,n} = \alpha_{m,n}$. This construction should give rise to an upper bound on the quantum capacity of a Heisenberg channel processing N-dimensional states, extending the bound (36) for Pauli channels. This will be investigated elsewhere.

4. Conclusion

We have defined a class of *asymmetric* cloners for quantum bits (Pauli cloning machines) and N-dimensional quantum states (Heisenberg cloning machines). For quantum bits, we have shown that the PCM, whose outputs emerge from two non-identical Pauli channels, generalizes the universal cloning machine of Buzek and Hillery [5]. The class of isotropic (but asymmetric) PCMs allowed us to derive a tight no-cloning inequality for quantum bits, quantifying the impossibility of copying due to quantum mechanics. Using a class of symmetric (but anisotropic) PCMs, we also established an upper bound on the quantum capacity of the Pauli

channel. These considerations have been extended to N dimensions, showing that the notion of asymmetric cloners is quite general. We have defined the N-dimensional HCM, whose outputs emerge from two distinct Heisenberg channels. The N-dimensional universal cloning machine [7, 8] appears as a special case—symmetric and isotropic—of these cloners. Using isotropic (asymmetric) HCMs, we have generalized the no-cloning inequality in order to characterize the impossibility of perfectly copying N-dimensional states. Furthermore, we have shown that the trade-off between the quality of the two copies of an N-dimensional state results from an *uncertainty principle* akin to the complementarity between position and momentum, implying that the probability distributions of the error operators affecting each copy are just the square of two dual functions under a Fourier transform.

Acknowledgments

I am grateful to V. Buzek and A. Peres for very helpful discussions, and to C. Adami for useful comments on the manuscript. This work was supported in part by the NSF under Grant Nos PHY 94-12818 and PHY 94-20470, and by a grant from DARPA/ARO through the QUIC Program DAAH04-96-1-3086.

Appendix A: Bound on the capacity of the Pauli channel

The class of symmetric PCMs characterized by equation (34) can be used in order to put a limit on the quantum capacity of a Pauli channel by extending the result of Bruss *et al.* [4] for the depolarizing channel. Consider a symmetric PCM whose outputs emerge from a Pauli channel of probabilities p_x, p_y and p_z. Applying an error-correcting scheme separately on each output of the cloning machine (ignoring the other output) would lead to a violation of the no-cloning theorem if the capacity $C(p_x,p_y,p_z)$ was non-zero. Thus, the capacity is vanishing on the ellipsoid E:

$$C(x^2,y^2,z^2) = 0 \quad \text{if } x^2 + y^2 + z^2 + xy + xz + yz = \tfrac{1}{2}. \tag{A 1}$$

In particular, equation (A 1) implies that the quantum capacity vanishes for (i) a depolarizing channel with $p = 1/4$ ($p_x = p_y = p_z = 1/12$) [4]; (ii) a '2-Pauli' channel with $p = 1/3$ ($p_x = p_z = 1/6$, $p_y = 0$); and (iii) a dephasing channel with $p = 1/2$ ($p_x = p_y = 0$, $p_z = 1/2$). Since C is a non-increasing function of p_x, p_y and p_z, for $p_x,p_y,p_z \leq 1/2$ (i.e. adding noise to a channel cannot increase its capacity), we also conclude that the quantum capacity is vanishing for any Pauli channel that lies *outside* the ellipsoid E. Furthermore, using the fact that C cannot be super-additive for a convex combination of a perfect and a noisy channel [19], an upper bound on C can be written using a linear interpolation between the perfect channel $(0,0,0)$ and any (zero-capacity) Pauli channel lying on E†:

$$C \leq 1 - 2(x^2 + y^2 + z^2 + xy + xz + yz). \tag{A 2}$$

† The proof in [19] assumes that the noisy channel does not have a vanishing capacity, which happens to be the case on E. However, with the assumption that C is a continuous function of p_x,p_y, and p_z, it extends to the case of interest here. Thus, equation (A 2) is rigorously proven only if such a continuity assumption is made. Some evidence that the proof holds for a zero-capacity channel can be found in [20].

Note that another class of symmetric PCMs can be found by requiring $\rho_{RA} = \rho_{RC}$, i.e. considering C as the second output and B as the cloning machine. This requirement implies $v = x - y + z$ rather than equation (33), which gives rise to the reflection of E with respect to the xz-plane, i.e. $y \to -y$. It does not change the above bound on C because this class of PCMs has noisier outputs in the first octant $x, y, z \geq 0$.

Appendix B: Universal cloning machine

The optimal symmetric PCM (i.e. the UCM) can be obtained alternatively by requiring that the two outputs A and B of a *symmetric* cloner are maximally uncorrelated. Using equations (15) and (33), we obtain $v'' = x + z$, $z'' = y + z$, $x'' = x + y$, and $y'' = 0$. Therefore, we have

$$\rho_{RC} = \rho_{AB} = |x+z|^2 |\Phi^+\rangle\langle\Phi^+| + |y+z|^2 |\Phi^-\rangle\langle\Phi^-| + |x+y|^2 |\Psi^+\rangle\langle\Psi^+|. \quad \text{(B 1)}$$

(This means that the third output C emerges from a Pauli channel with vanishing p_y.) To minimize the correlation between the two copies of the symmetric cloner, we need to maximize the joint von Neumann entropy of the two outputs A and B,

$$S(AB) = -\mathrm{Tr}(\rho_{AB} \log \rho_{AB}) = H[|x+z|^2, |y+z|^2, |x+y|^2], \quad \text{(B 2)}$$

with $H[\cdot]$ denoting the Shannon entropy of the 3-point probability distribution. It is easy to see that the solution with $x, y, z \geq 0$ that maximizes $S(AB)$ is $x = y = z$, that is, the Pauli channel underlying outputs A and B reduces to a depolarizing channel. Using equation (34), we get $x = y = z = 12^{-1/2}$, so that the wave function underlying the UCM is

$$|\Psi\rangle_{RA;BC} = \left(\frac{3}{4}\right)^{1/2} |\Phi^+\rangle_{RA} |\Phi^+\rangle_{BC} + \left(\frac{1}{12}\right)^{1/2} \{|\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\}_{RA;BC}. \quad \text{(B 3)}$$

Consequently

$$\rho_{RA} = \rho_{RB} = \tfrac{3}{4}|\Phi^+\rangle\langle\Phi^+| + \tfrac{1}{12}(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|) \quad \text{(B 4)}$$

reflecting that A and B emerge both from a depolarizing channel with $p = 1/4$,

$$|\psi\rangle \to \tfrac{2}{3}|\psi\rangle\langle\psi| + \tfrac{1}{3}(\mathbb{1}/2). \quad \text{(B 5)}$$

As mentioned above, the corresponding scaling factor is $s = 1 - 4p/3 = 2/3$ while depolarizing fraction is $\pi = 4f/3 = 1/3$. Thus, in some sense, the qubit *can* be perfectly cloned but only with probability $p_{\mathrm{cl}} = 2/3 + 2/3 - 1 = 1/3$. The fidelity of cloning is $f = 1 - 2p/3 = 5/6$ [5].

For the partition RC versus AB, we obtain

$$|\Psi\rangle_{RC;AB} = \left(\frac{1}{3}\right)^{1/2} \{|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle\}_{RC;AB}, \quad \text{(B 6)}$$

implying that the 4-qubit wave function is symmetric under the interchange of A and B (or R and C). It is easy to check that equation (B 6) corresponds to the unitary transformation that implements the UCM as defined in [5]:

$$|0\rangle_X|00\rangle \to \left(\frac{2}{3}\right)^{1/2}|00\rangle_{AB}|0\rangle_C + \left(\frac{1}{3}\right)^{1/2}|\Psi^+\rangle_{AB}|1\rangle_C,$$
$$|1\rangle_X|00\rangle \to \left(\frac{2}{3}\right)^{1/2}|11\rangle_{AB}|1\rangle_C + \left(\frac{1}{3}\right)^{1/2}|\Psi^+\rangle_{AB}|0\rangle_C. \quad \text{(B 7)}$$

Indeed, using equation (B 7), we have

$$|\Phi^+\rangle_{RX}|00\rangle \to \left(\frac{1}{3}\right)^{1/2}(|00\rangle_{AB}|00\rangle_{RC} + |11\rangle_{AB}|11\rangle_{RC}) + \left(\frac{1}{6}\right)^{1/2}|\Psi^+\rangle_{AB}(|01\rangle_{RC} + |10\rangle_{RC}), \quad \text{(B 8)}$$

if the initial state of X is maximally entangled with the reference R. Thus, the 4-qubit wave function is transformed into equation (B 6), as expected. The latter implies

$$\rho_{RC} = \rho_{AB} = \tfrac{1}{3}(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+|), \quad \text{(B 9)}$$

showing that the joint entropy of the two outputs is maximum (remember that the singlet $|\Psi^-\rangle$ component must vanish), or their mutual entropy is minimum. Finally, we see also that the third output of the UCM emerges from a 2-Pauli channel of probability 2/3. Using equation (9), it appears that the corresponding operation on an arbitrary state $|\psi\rangle$ is

$$|\psi\rangle \to \tfrac{1}{3}|\psi^*\rangle\langle\psi^*| + \tfrac{2}{3}(\mathbb{1}/2) \quad \text{(B 10)}$$

as noted in [7]. It should be noted that this time-reversed fraction 1/3 coincides with the probability p_{cl} of violating the no-cloning theorem mentioned above.

Appendix C: Quantum Pauli triplicators

Let us turn to the fully symmetric PCMs that have *three* outputs emerging from the *same* Pauli channel, i.e. $\rho_{RA} = \rho_{RB} = \rho_{RC}$, which corresponds to a family of (non-optimal) quantum *triplicating* machines. The requirement $\rho_{RA} = \rho_{RC}$ implies $v = x - y + z$, which, together with equation (33), yields the conditions

$$(v = x + z) \wedge (y = 0). \quad \text{(C 1)}$$

Incidentally, we notice that if *all* pairs are required to be in the *same* mixture of Bell states, this mixture cannot have a singlet $|\Psi^-\rangle$ component. The outputs of the corresponding triplicators emerge therefore from a Pauli channel with $p_y = 0$, so that these triplicators are *state-dependent*, in contrast with the one considered in [6]†. These triplicators are represented by the intersection of E with the xz-plane, that is, the ellipse

$$x^2 + z^2 + xz = \tfrac{1}{2}, \quad \text{(C 2)}$$

whose semi-minor axis is $3^{-1/2}$ (oriented along the direction $(1,1)$) and semi-major axis is 1. The intersection of this ellipse with its semi-minor axis ($x = z = 6^{-1/2}$) corresponds to the 4-qubit wave function

† For describing a *state-independent* triplicator, a 6-qubit wave function should be used, that is, the cloner should consist of 2 qubits.

$$|\Psi\rangle_{RA;BC} = \frac{2}{6^{1/2}}|\Phi^+\rangle|\Phi^+\rangle + \frac{1}{6^{1/2}}|\Phi^-\rangle|\Phi^-\rangle + \frac{1}{6^{1/2}}|\Psi^+\rangle|\Psi^+\rangle, \qquad (C\,3)$$

which is symmetric under the interchange of any two qubits and maximizes the 2-bit entropy Equation (C 3) thus characterizes the best triplicator of this ensemble, whose three outputs emerge from a '2-Pauli' channel with $p = 1/3$ ($p_x = p_z = 1/6$). According to equation (9), the (state-dependent) operation of this triplicator on an arbitrary qubit can be written as

$$|\psi\rangle \rightarrow \tfrac{1}{2}|\psi\rangle\langle\psi| + \tfrac{1}{6}|\psi^*\rangle\langle\psi^*| + \tfrac{1}{3}(\mathbb{1}/2), \qquad (C\,4)$$

which reduces to the triplicator that was considered in [21]. Note that if $|\psi\rangle$ is real, equation (C 4) reduces to equation (B 5), so that the three outputs are the same as those of the UCM. The fidelity of cloning is then the same as for the UCM ($f = 5/6$) regardless of the input state (provided it is real).

References

[1] Dieks, D., 1982, *Phys. Lett.* **92A,** 271.
[2] Wootters, W. K., and Zurek, W. H., 1982, *Nature*, **299,** 802.
[3] Gisin, N., and Huttner, B., 1997, *Phys. Lett.* A, **228,** 13.
[4] Bruss, D., DiVincenzo, D. P., Ekert, A., Fuchs, C. A., Macchiavello, C., and Smolin, J. A., 1998, *Phys. Rev.* A, **57,** 2368.
[5] Buzek, V., and Hillery, M., 1996, *Phys. Rev.* A, **54,** 1844.
[6] Gisin, N., and Massar, S., 1997, *Phys. Rev. Lett.*, **79,** 2153.
[7] Buzek, V., and Hillery, M., 1999, *Quantum Computing and Quantum Communications, Lecture Notes in Computer Science*, Vol. 1509, edited by C. P. Williams (Berlin: Springer-Verlag) pp. 235–246.
[8] Werner, R. F., 1998, *Phys. Rev.* A, **58,** 1827.
[9] Niu, C.-S., and Griffiths, R. B., 1998, *Phys. Rev.* A, **58,** 4377.
[10] Fivel, D. I., 1995, *Phys. Rev. Lett.*, **74,** 835.
[11] Cerf, N. J., 1998, LANL e-print quant-ph/9803058; to appear in Phys. Rev. Lett.
[12] Ekert, A., and Knight, P. L., 1995, *Am. J. Phys.* **63,** 415.
[13] Gisin, N., 1998, *Phys. Lett.* A, **242,** 1.
[14] Deutsch, D., 1983, *Phys. Rev. Lett.*, **50,** 631.
[15] Kraus, K., 1987, *Phys. Rev.* D, **35,** 3070.
[16] Maassen, H., and Uffink, J. B. M., 1988, *Phys. Rev. Lett.*, **60,** 1103.
[17] Cerf, N. J., 1999, *Quantum Computing and Quantum Communications, Lecture Notes in Computer Science*, Vol. 1509, edited by C. P. Williams (Berlin: Springer-Verlag) pp. 218–234.
[18] Adami, C., and Cerf, N. J., 1997, *Phys. Rev.* A, **56,** 3470.
[19] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., and Wootters, W. K., 1996, *Phys. Rev.* A, **54,** 3824.
[20] Cerf, N. J., 1998, *Phys. Rev.* A, **57,** 3330.
[21] Buzek, V., Braunstein, S. L., Hillery, M., and Bruss, D., 1997, *Phys. Rev.* A, **56,** 3446.