acta physica slovaca vol. 48 No. 3, 115 – 132 June 1998

ASYMMETRIC QUANTUM CLONING MACHINES[1]

N.J. Cerf[a,b,c]

(a) *W. K. Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, California 91125*

(b) *Information and Computing Technologies Research Section, Jet Propulsion Laboratory, Pasadena, California 91109*

(c) *Center for Nonlinear Phenomena and Complex Systems, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

Received 7 May 1998, accepted 15 May 1998

A family of asymmetric cloning machines for quantum bits and N-dimensional quantum states is introduced. These machines produce two approximate copies of a single quantum state that emerge from two distinct channels. In particular, an asymmetric Pauli cloning machine is defined that makes two imperfect copies of a quantum bit, while the overall input-to-output operation for each copy is a Pauli channel. A no-cloning inequality is derived, characterizing the impossibility of copying imposed by quantum mechanics. If p and p' are the probabilities of the depolarizing channels associated with the two outputs, the domain in $(\sqrt{p}, \sqrt{p'})$-space located inside a particular ellipse representing close-to-perfect cloning is forbidden. This ellipse tends to a circle when copying an N-dimensional state with $N \to \infty$, which has a simple semi-classical interpretation. The symmetric Pauli cloning machines are then used to provide an upper bound on the quantum capacity of the Pauli channel of probabilities p_x, p_y and p_z. The capacity is proven to be vanishing if $(\sqrt{p_x}, \sqrt{p_y}, \sqrt{p_z})$ lies outside an ellipsoid whose pole coincides with the depolarizing channel that underlies the universal cloning machine. Finally, the tradeoff between the quality of the two copies is shown to result from a complementarity akin to Heisenberg uncertainty principle.

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

[1]Special Issue on Quantum Optics and Quantum Information

mechanics, and lies at the heart of quantum theory. Remarkably, if perfect cloning *was* permitted, the Heisenberg uncertainty principle could be violated by measuring conjugate observables on many copies of a single quantum system.

Consider a cloning machine that duplicates a quantum bit (a 2-state system) that is initially in an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ whose amplitudes are unknown. It is easy to build such a machine that perfectly copies the two basis states $|0\rangle$ and $|1\rangle$, but then it badly duplicates the superpositions $2^{-1/2}(|0\rangle+|1\rangle)$ and $2^{-1/2}(|0\rangle-|1\rangle)$. In other words, it cannot produce *perfect* copies of *all* possible input states. This being so, we may ask how well one can *approximately* duplicate the unknown state of a quantum bit (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 [3] 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, a universal cloning machine (UCM) can be defined that creates two copies characterized each by the same density operator ρ, the fidelity of cloning being $f \equiv \langle\psi|\rho|\psi\rangle = 5/6$. This machine is called *universal* because it produces copies that are *state-independent*: both output qubits emerge from a depolarizing channel of probability $1/4$, that is, the Bloch vector characterizing the input qubit is shrunk by a factor $2/3$ regardless its orientation. The UCM was later proved to be optimal by Bruss et al. [4], and Gisin and Massar [5]. The concept of approximate cloning was also generalized to n-plicating machines, that is, cloners that yield n imperfect copies of a single qubit [5, 6]. Quantum cloning machines have attracted a lot of attention because of their use in connection with quantum communication and cryptography (see, e.g., [4, 7]). For example, an interesting application of the UCM is that it can be used to establish an upper bound on the quantum capacity C of a depolarizing channel, namely $C = 0$ at $p = 1/4$ [4].

In this paper, we introduce a family of *asymmetric* cloning machines that produce two distinct (approximate) copies of a single quantum state. This is in contrast with the cloning machines considered before, which were symmetric (both outputs being characterized by the same density operator). We consider the asymmetric cloning of both two-dimensional and N-dimensional quantum states. Using a particular class of asymmetric cloners whose outputs emerge from (distinct) depolarizing channels, we derive a *no-cloning inequality* governing the tradeoff between the quality of the copies of a single state imposed by quantum mechanics: $a^2 + 2ab/N + b^2 \geq 1$, where $s_a = 1 - a^2$ and $s_b = 1 - b^2$ is the scaling factor of the channel associated with output A and B, respectively. It is, by construction, a tight inequality which is saturated using our cloners. More generally, the complementarity between the two copies is shown to result from an *uncertainty principle* that relates the outputs of the cloner, much like that associated with Fourier transforms. Consequently, the probability distributions characterizing the channels underlying the two outputs cannot be peaked simultaneously, giving rise to a balance between the fidelity of the two copies.

The cloning machines for quantum bits are discussed in the first part of this paper, Sec. 2. We introduce a *Pauli cloning machine* (PCM), which produces two (not necessarily identical) output qubits, each emerging from a Pauli channel [8]. The family of PCMs relies on a parameterization of 4-qubit wave functions for which all qubit pairs are in a mixture of Bell states. The subclass of *symmetric* PCMs is then used in order to express an upper bound on the quantum capacity of a Pauli channel, generalizing the considerations of Ref. [4] for a depolarizing channel. In particular, the capacity of the Pauli channel with probabilities $p_x = x^2$, $p_y = y^2$ and $p_z = z^2$, is shown to be vanishing if (x, y, z) lies outside the ellipsoid $x^2 + y^2 + z^2 + xy + xz + yz = 1/2$, whose pole coincides with the depolarizing channel corresponding to the UCM. In Sec. 3, we generalize the PCM to more than two dimensions, and define a family of asymmetric cloning machines for N-dimensional states. Our description is based on the maximally-entangled states of two N-dimensional systems, which generalize the Bell states. A special case of these cloners is shown to be the symmetric N-dimensional UCM [6]. This family of asymmetric N-dimensional cloners is used to investigate the complementarity principle governing the tradeoff between the quality of the copies.

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 $|\psi\rangle$ which is processed by a Pauli channel. Thus, the qubit is rotated by one of the three Pauli matrices or remains unchanged: it 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. (A depolarizing channel corresponds to the special case where $p_x = p_y = p_z$.) It is convenient to describe the operation of such a channel by considering an input maximally entangled with a reference system. Defining the four maximally-entangled states of two qubits (i.e., the Bell states) as

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \qquad |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{1}$$

we note that the *local* action of the Pauli matrices on one of these states, say $|\Phi^+\rangle$, yields the three remaining Bell states, namely

$$\begin{aligned}(\mathcal{I}\otimes\sigma_z)|\Phi^+\rangle &= |\Phi^-\rangle \\ (\mathcal{I}\otimes\sigma_x)|\Phi^+\rangle &= |\Psi^+\rangle \\ (\mathcal{I}\otimes\sigma_x\sigma_z)|\Phi^+\rangle &= |\Psi^-\rangle\end{aligned} \tag{2}$$

(Note that we use the convention $|0\rangle = |\uparrow\rangle$ and $|1\rangle = |\downarrow\rangle$.) Therefore, if the input qubit I of the Pauli channel is maximally entangled with a reference qubit R, say if their joint state $|\psi\rangle_{RI}$ is the Bell state $|\Phi^+\rangle$, then the joint state of R and the output O is a mixture of the four Bell states

$$\rho_{RO} = (1-p)\,|\Phi^+\rangle\langle\Phi^+| + p_z\,|\Phi^-\rangle\langle\Phi^-| + p_x\,|\Psi^+\rangle\langle\Psi^+| + p_y\,|\Psi^-\rangle\langle\Psi^-|\,, \tag{3}$$

with $p = p_x + p_y + p_z$.

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

$$\rho_{RO} = (1-p)\,|\Phi^+\rangle\langle\Phi^+| + \sum_{i=1}^{3} p_i |\Psi_i\rangle\langle\Psi_i| \tag{4}$$

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

$$\begin{aligned} |\psi\rangle \to \rho &= (1-p-p_2)\,|\psi\rangle\langle\psi| + (p_2-p_1)\,\sigma_1|\psi_\perp\rangle\langle\psi_\perp|\sigma_1 \\ &+ (p_3-p_2)\,\sigma_3|\psi\rangle\langle\psi|\sigma_3 + 2(p_1+p_2)\,\mathcal{I}/2 \end{aligned} \tag{5}$$

where $|\psi_\perp\rangle = -i\sigma_y|\psi^*\rangle = \sigma_x\sigma_z|\psi^*\rangle$ denotes the time-reversed of state $|\psi\rangle$. The four components in the right-hand side of Eq. (5) correspond respectively to the unchanged, (rotated) time-reversed, rotated, and random fraction. It is clear from Eq. (5) 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_{RO} is a Werner state and Eq. (5) becomes

$$|\psi\rangle \to \rho = (1-4p/3)\,|\psi\rangle\langle\psi| + (4p/3)\,\mathcal{I}/2 \tag{6}$$

Thus, the vector characterizing the input qubit in the Bloch sphere is shrunk by a scaling factor $s = 1 - 4p/3$ regardless 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

$$\begin{aligned} |\psi\rangle \to \rho &= (1-3p/2)\,|\psi\rangle\langle\psi| + (p/2)\,\sigma_y|\psi_\perp\rangle\langle\psi_\perp|\sigma_y + p\,\mathcal{I}/2 \\ &= (1-3p/2)\,|\psi\rangle\langle\psi| + (p/2)\,|\psi^*\rangle\langle\psi^*| + p\,\mathcal{I}/2 \end{aligned} \tag{7}$$

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

$$|\psi\rangle \to (1-p)\,|\psi\rangle\langle\psi| + p\,\sigma_z|\psi\rangle\langle\psi|\sigma_z \tag{8}$$

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 [8]. Thus, if the input I of the cloner is fully entangled with a reference R, i.e., $|\psi\rangle_{RI} = |\Phi^+\rangle$, 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 Hilbert space is necessary in general to purify ρ_{RA} since we need to accommodate its four (generally nonzero) eigenvalues. The 2-dimensional space of second output qubit B is thus insufficient for this purpose, so that we must introduce an additional system C, which may be viewed as an ancilla or the cloning machine itself. A 2-dimensional space for C is then sufficient, so that we need to consider a single

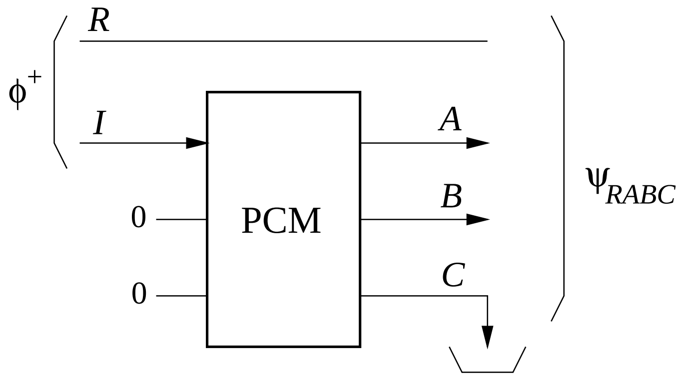

Fig. 1. Pauli cloning machine of input I (initially entangled with a reference R) and outputs A and B. The third output C refers to an ancilla or the cloning machine. The three outputs emerge in general from distinct Pauli channels.

additional qubit C for the cloning machine, as shown in Refs. [3, 4]. As a consequence, we are led to consider a 4-qubit system in order to fully describe the PCM, as pictured in Fig. 1. Before cloning, the qubits R and I are 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 (A and B emerge from a Pauli channel). As we shall see, ρ_{RC} happens to be also a mixture of Bell states, so that C can be viewed as a third output emerging from a Pauli channel.

Instead of specifying a PCM by a particular unitary operation acting on the state $|\psi\rangle$ of the input qubit I (together with the two auxiliary qubits in a fixed state $|0\rangle$), it is more convenient to characterize it by the wave function $|\Psi\rangle_{RABC}$ underlying the entanglement of the three outputs with R. So, our goal is to find in general the 4-qubit wave functions that satisfy the requirement that the state of every pair of two qubits is a mixture of the four Bell states. Making use of the Schmidt decomposition of $|\Psi\rangle_{RABC}$ for the bipartite partition RA vs BC, it is clear that this state can be written as a superposition of *double Bell* states

$$|\Psi\rangle_{RA;BC} = \left\{ v\,|\Phi^+\rangle|\Phi^+\rangle + z\,|\Phi^-\rangle|\Phi^-\rangle + x\,|\Psi^+\rangle|\Psi^+\rangle + y\,|\Psi^-\rangle|\Psi^-\rangle \right\}_{RA;BC}, \quad (9)$$

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 Eq. (9) are not considered here for simplicity. The above requirement is then satisfied for the qubit pairs RA and BC, that is, $\rho_{RA}=\rho_{BC}$ is of the form of Eq. (3) with $p_x=|x|^2$, $p_y=|y|^2$, $p_z=|z|^2$, and $1-p=|v|^2$. It is important to note that these double Bell states for the partition RA vs BC transform into superpositions of double Bell states for the two other possible partitions of the four qubits $RABC$ into two pairs (RB vs AC, RC vs AB). For example, the transformation associated with the partition RB vs AC is

$$|\Phi^+\rangle_{RA}\,|\Phi^+\rangle_{BC} = \frac{1}{2}\left\{ |\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle \right\}_{RB;AC}$$

$$|\Phi^-\rangle_{RA}\,|\Phi^-\rangle_{BC} = \frac{1}{2}\left\{|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle - |\Psi^+\rangle|\Psi^+\rangle - |\Psi^-\rangle|\Psi^-\rangle\right\}_{RB;AC}$$
$$|\Psi^+\rangle_{RA}\,|\Psi^+\rangle_{BC} = \frac{1}{2}\left\{|\Phi^+\rangle|\Phi^+\rangle - |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle - |\Psi^-\rangle|\Psi^-\rangle\right\}_{RB;AC}$$
$$|\Psi^-\rangle_{RA}\,|\Psi^-\rangle_{BC} = \frac{1}{2}\left\{|\Phi^+\rangle|\Phi^+\rangle - |\Phi^-\rangle|\Phi^-\rangle - |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\right\}_{RB;AC} \quad (10)$$

(For the partition RC vs AB, these expressions are similar up to an overall sign in the transformation of the state $|\Psi^-\rangle_{RA}\,|\Psi^-\rangle_{BC}$.) This implies that $|\Psi\rangle_{RABC}$ is also a superposition of double Bell states (albeit with different amplitudes) for these two other partitions, which, therefore, also yield mixtures of Bell states when tracing over half of the system. Specifically, for the partition RB vs AC, we obtain

$$|\Psi\rangle_{RB;AC} = \left\{v'\,|\Phi^+\rangle|\Phi^+\rangle + z'\,|\Phi^-\rangle|\Phi^-\rangle + x'\,|\Psi^+\rangle|\Psi^+\rangle + y'\,|\Psi^-\rangle|\Psi^-\rangle\right\}_{RB;AC}\,, \quad (11)$$

with

$$\begin{aligned} v' &= (v+z+x+y)/2 \\ z' &= (v+z-x-y)/2 \\ x' &= (v-z+x-y)/2 \\ y' &= (v-z-x+y)/2 \end{aligned} \quad (12)$$

implying that the second output B emerges from a Pauli channel with probabilities $p'_x = |x'|^2$, $p'_y = |y'|^2$, and $p'_z = |z'|^2$. Similarly, the third output C is described by considering the partition RC vs AB,

$$|\Psi\rangle_{RC;AB} = \left\{v''\,|\Phi^+\rangle|\Phi^+\rangle + z''\,|\Phi^-\rangle|\Phi^-\rangle + x''\,|\Psi^+\rangle|\Psi^+\rangle + y''\,|\Psi^-\rangle|\Psi^-\rangle\right\}_{RC;AB}\,, \quad (13)$$

with

$$\begin{aligned} v'' &= (v+z+x-y)/2 \\ z'' &= (v+z-x+y)/2 \\ x'' &= (v-z+x+y)/2 \\ y'' &= (v-z-x-y)/2 \end{aligned} \quad (14)$$

Thus, Eqs. (12) and (14) 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.

2.3. No-cloning inequality for quantum bits

Let us consider the class of asymmetric PCMs whose outputs A and B emerge from (distinct) *depolarizing* channels. Assume that the first output A emerges from a depolarizing channel of probability $p = 3|x|^2$, i.e.,

$$\rho_{RA} = |v|^2|\Phi^+\rangle\langle\Phi^+| + |x|^2\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\right)\,, \quad (15)$$

with $|v|^2 + 3|x|^2 = 1$. Then, from Eq. (12), we have $v' = (v+3x)/2$ and $x' = (v-x)/2$, resulting in

$$\rho_{RB} = \frac{|v+3x|^2}{4}|\Phi^+\rangle\langle\Phi^+| + \frac{|v-x|^2}{4}\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\right) . \quad (16)$$

Thus, the second output B also emerges from a depolarizing channel of probability $p' = 3|x'|^2 = \frac{3}{4}|v-x|^2$, implying that both outputs of this asymmetric PCM are state-independent as they simply correspond to a (different) scaling of the vector characterizing the input qubit in the Bloch sphere. (The third output C emerges in general from a different Pauli channel.) The relation between the parameters x and x' characterizing the two outputs can be written as

$$|x|^2 + \mathrm{Re}(x^* x') + |x'|^2 = \frac{1}{4} \quad (17)$$

Clearly, the best cloning (minimum values for $|x|$ and $|x'|$) is achieved when the cross term is the largest in magnitude, that is when x and x' have the same phase. For simplicity, we assume here that x and x' are real and positive. Consequently, the tradeoff between the quality of the two copies can be described by the *no-cloning inequality*

$$x^2 + xx' + x'^2 \geq \frac{1}{4} , \quad (18)$$

where the copying error is measured by the probability of the depolarizing channel underlying each output, i.e., $p = 3x^2$ and $p' = 3x'^2$ (with $x, x' \geq 0$). Equation (18) corresponds to the domain in the (x, x')-space located outside an ellipse whose semiminor axis, oriented in the direction $(1,1)$, is $1/\sqrt{6}$, as shown in Fig. 2. (The semimajor axis is $1/\sqrt{2}$.) The origin in this space corresponds to a (nonexisting) cloner whose two outputs would be perfect $p = p' = 0$, while to distance to origin measures $(p+p')/3$. The ellipse characterizes the ensemble of values for p and p' that can actually be achieved with a PCM. It intercepts its minor axis at $(1/\sqrt{12}, 1/\sqrt{12})$, which corresponds to the universal cloning machine (UCM), i.e., $p = p' = 1/4$, as discussed below. This point is the closest to the origin (i.e., the cloner with minimum $p + p'$), and characterizes in this sense the best possible copying. The UCM is the only symmetric cloner belonging to the class of PCM considered here (i.e., cloners whose outputs are depolarizing channels); other symmetric cloners will be considered in Sec. 2.4. The ellipse 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 ($p' = 0$). Of course, $(0, 1/2)$ corresponds to the symmetric situation. The dimensional argument used in Sec. 2.2. strongly suggests that the imperfect cloning achieved by such an asymmetric PCM is optimal: a single additional qubit C for the cloner is sufficient to perform the best cloning, i.e., to achieve the minimum p and p' for a fixed ratio p/p'. (This is proven rigorously for the special case $p = p'$ in Ref. [4]). Also, introducing a phase difference between x and x' results in a set of PCMs characterized by an ellipse that is less eccentric and tends to a circle of radius $1/2$ for a phase difference of $\pi/2$. Consequently, the no-cloning inequality (18) is saturated when x and x' have the same

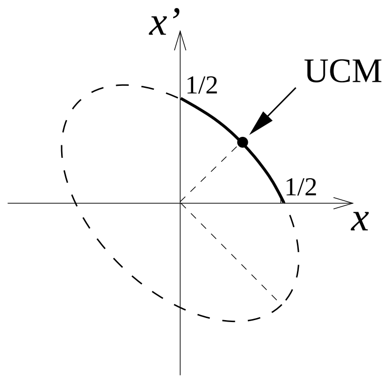

Fig. 2. Ellipse delimiting the best quality of the two outputs of an asymmetric PCM that can be achieved simultaneously (only the quadrant $x, x' \geq 0$ is of interest here). The outputs emerge from depolarizing channels of probability $p = 3x^2$ and $p' = 3x'^2$. Any close-to-perfect cloning characterized by a point inside the ellipse is forbidden.

(or opposite) phase. The domain inside the ellipse corresponds then to the values for p and p' that cannot be achieved simultaneously, reflecting the impossibility of close-to-perfect cloning, and Eq. (18) is the tightest no-cloning bound that can be written for a qubit.

2.4. Symmetric Pauli cloning machines

Consider now the class of symmetric PCMs that have both outputs emerging from a *same* Pauli channel, i.e., $\rho_{RA} = \rho_{RB}$. Using Eq. (12), we obtain the conditions

$$\begin{aligned}
|v|^2 &= |v+z+x+y|^2/4 \\
|z|^2 &= |v+z-x-y|^2/4 \\
|x|^2 &= |v-z+x-y|^2/4 \\
|y|^2 &= |v-z-x+y|^2/4
\end{aligned} \tag{19}$$

which yields

$$v = x + y + z \ , \tag{20}$$

where x, y, z, and v are assumed to be real. Equation (20), 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,

$$x^2 + y^2 + z^2 + xy + xz + yz = \frac{1}{2} \ , \tag{21}$$

is an oblate ellipsoid E with symmetry axis along the direction $(1, 1, 1)$, as shown in Fig. 3. The semiminor axis (or polar radius) is 1/2 while the semimajor axis (or equatorial radius) is 1. In this representation, the distance to the origin is $p_x + p_y + p_z$, so

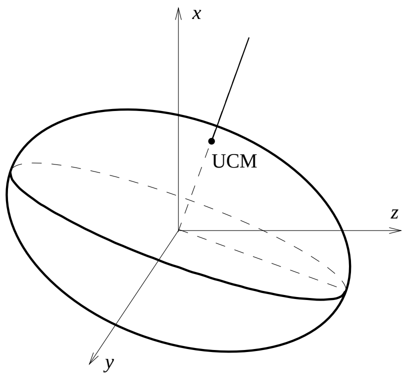

Fig. 3. Oblate ellipsoid representing the class of symmetric PCMs whose two outputs emerge from the same Pauli channel of parameters $p_x = x^2$, $p_y = y^2$, and $p_z = z^2$ (only the octant $x, y, z \geq 0$ is considered here). The pole of this ellipsoid corresponds to the UCM. The capacity of a Pauli channel that lies outside this ellipsoid must be vanishing.

that the pole $(1/\sqrt{12}, 1/\sqrt{12}, 1/\sqrt{12})$ of this ellipsoid—the closest point to the origin—corresponds to the special case of a depolarizing channel of probability $p = 1/4$. Thus, this particular PCM reduces to the UCM. 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 ($p_x = p_y = p_z$).

2.5. 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 independent. Using Eqs. (14) and (20), we obtain $v'' = x + z$, $z'' = y + z$, $x'' = x + y$, and $y'' = 0$. Therefore, we have

$$\rho_{RC} = \rho_{AB} = |x+z|^2 \, |\Phi^+\rangle\langle\Phi^+| + |y+z|^2 \, |\Phi^-\rangle\langle\Phi^-| + |x+y|^2 \, |\Psi^+\rangle\langle\Psi^+| \, . \qquad (22)$$

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

$$S(AB) = -\mathrm{Tr}(\rho_{AB} \log \rho_{AB}) = H\left[|x+z|^2, |y+z|^2, |x+y|^2\right] \qquad (23)$$

with $H[\cdot]$ denoting the Shannon entropy. 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 Eq. (21), we get $x = y = z = 1/\sqrt{12}$, so that the wave function underlying the UCM is

$$|\Psi\rangle_{RA;BC} = \sqrt{\frac{3}{4}} \, |\Phi^+\rangle_{RA} |\Phi^+\rangle_{BC} + \sqrt{\frac{1}{12}} \, \{|\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\}_{RA;BC} \qquad (24)$$

Consequently

$$\rho_{RA} = \rho_{RB} = \frac{3}{4} \, |\Phi^+\rangle\langle\Phi^+| + \frac{1}{12} \left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\right) \qquad (25)$$

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

$$|\psi\rangle \to \frac{2}{3}\,|\psi\rangle\langle\psi| + \frac{1}{3}\,(\mathcal{I}/2) \tag{26}$$

so that the scaling factor is $s = 1 - 4p/3 = 2/3$ while the fidelity of cloning is $f = 1 - 2p/3 = 5/6$ [3]. For the partition RC vs AB, we obtain

$$|\Psi\rangle_{RC;AB} = \sqrt{\frac{1}{3}}\,\{|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle\}_{RC;AB} \tag{27}$$

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 the unitary transformation which implements the UCM [3] is

$$\begin{aligned} |0\rangle_I\,|00\rangle &\to \sqrt{\frac{2}{3}}|00\rangle_{AB}\,|0\rangle_C + \sqrt{\frac{1}{3}}|\Psi^+\rangle_{AB}\,|1\rangle_C \\ |1\rangle_I\,|00\rangle &\to \sqrt{\frac{2}{3}}|11\rangle_{AB}\,|1\rangle_C + \sqrt{\frac{1}{3}}|\Psi^+\rangle_{AB}\,|0\rangle_C \end{aligned} \tag{28}$$

Indeed, using Eq. (28), we have

$$|\Phi^+\rangle_{RI}|00\rangle \to \sqrt{\frac{1}{3}}\big(|00\rangle_{AB}\,|00\rangle_{RC} + |11\rangle_{AB}\,|11\rangle_{RC}\big) + \sqrt{\frac{1}{6}}|\Psi^+\rangle_{AB}\big(|01\rangle_{RC} + |10\rangle_{RC}\big) \tag{29}$$

so that the initial state of I (maximally entangled with the reference R) is transformed into the wave function Eq. (27). The latter implies

$$\rho_{RC} = \rho_{AB} = \frac{1}{3}\,\big(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+|\big) \tag{30}$$

showing that the joint entropy of the two outputs is maximum (remember that the singlet $|\Psi^-\rangle$ component must vanish). Thus, the third output of the UCM emerges from a 2-Pauli channel of probability 2/3. Using Eq. (7), we see that the corresponding operation on an arbitrary state $|\psi\rangle$ is

$$|\psi\rangle \to \frac{1}{3}\,|\psi^*\rangle\langle\psi^*| + \frac{2}{3}\,(\mathcal{I}/2) \tag{31}$$

as noted in Ref. [6].

2.6. Related bound on the capacity of the Pauli channel

The class of symmetric PCMs characterized by Eq. (21) can be used in order to put a limit on the quantum capacity of a Pauli channel, thereby extending the result of Bruss et al. [4] for the depolarizing channel. Consider a 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 (obliviously of the other output) would lead to a violation of the no-cloning theorem if the capacity $C(p_x, p_y, p_z)$ was nonzero. Since C is a nonincreasing 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 have

$$C(p_x, p_y, p_z) = 0 \qquad \text{if } (x, y, z) \notin E \tag{32}$$

that is, the quantum capacity is vanishing for any Pauli channel that lies *outside* the ellipsoid E. In particular, Eq. (21) 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 $p = 1/2$ ($p_x = p_y = 0$, $p_z = 1/2$). Furthermore, using the fact that C cannot be superadditive for a convex combination of a perfect and a noisy channel [9], an upper bound on C can be written using a linear interpolation between the perfect channel $(0, 0, 0)$ and any Pauli channel lying on E:

$$C \leq 1 - 2(x^2 + y^2 + z^2 + xy + xz + yz) \ . \tag{33}$$

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 Eq. (20), 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 $x, y, z \geq 0$.

2.7. Quantum triplicators based on the PCM

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 Eq. (20), yields the conditions $(v = x + z) \wedge (y = 0)$. 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 "2-Pauli" channel ($p_y = 0$), so that these triplicators are *state-dependent*, in contrast with the one considered in Ref. [5]. (For describing a *state-independent* triplicator, a 6-qubit wave function should be used, that is, the cloner should consist of 2 qubits.) These triplicators are represented by the intersection of E with the xz-plane, that is, the ellipse

$$x^2 + z^2 + xz = \frac{1}{2} \ , \tag{34}$$

whose semiminor axis is $1/\sqrt{3}$ [oriented along the direction $(1, 1)$] and semimajor axis is 1. The intersection of this ellipse with its semiminor axis ($x = z = 1/\sqrt{6}$) corresponds to the 4-qubit wave function

$$|\Psi\rangle_{abcd} = \frac{2}{\sqrt{6}}|\Phi^+\rangle|\Phi^+\rangle + \frac{1}{\sqrt{6}}|\Phi^-\rangle|\Phi^-\rangle + \frac{1}{\sqrt{6}}|\Psi^+\rangle|\Psi^+\rangle \ , \tag{35}$$

which is symmetric under the interchange of any two qubits and maximizes the 2-bit entropy (or minimizes the mutual entropy between any two outputs of the triplicator, making them maximally independent). Equation (35) 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 Eq. (7), the (state-dependent) operation of this triplicator on an arbitrary qubit can be written as

$$|\psi\rangle \to \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^*\rangle\langle\psi^*| + \frac{1}{3}(\mathcal{I}/2)\,. \tag{36}$$

If $|\psi\rangle$ is real, Eq. (36) reduces to the triplicator that was considered in Ref. [10]. The fidelity of cloning is then the same as for the UCM, i.e., $f = 5/6$, regardless the input state (provided it is real).

3. Cloning machines for N-dimensional states

3.1. Channel characterization using the 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 need first to introduce the set of maximally-entangled (ME) states of two N-dimensional systems, A and B:

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

where the indices m and n ($m, n = 0, \cdots, N-1$) label the N^2 states. Note that, here and below, the label in the kets 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

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

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 spaces $\mathcal{H}_A \otimes \mathcal{H}_B$. The resolution of identity simply reads

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

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

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

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 use these ME-states in order to describe a quantum channel that processes N-dimensional states. In such a channel, an arbitrary state $|\psi\rangle$ undergoes a particular unitary transformation

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

with probability $p_{m,n}$ (with $\sum_{m,n} p_{m,n} = 1$). Note that $U_{0,0} = \mathcal{I}$, implying that $|\psi\rangle$ is left unchanged with probability $p_{0,0}$. If the input of the channel I is maximally entangled with a reference R (an N-dimensional system) so that their joint state is $|\psi_{0,0}\rangle = \sum_j |j\rangle/\sqrt{N}$, then the joint state of the output O and the reference R is simply a mixture of the N^2 ME-states,

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

generalizing the mixture of Bell states that we discussed in Sec. 2. Indeed, applying $U_{m,n}$ locally to one subsystem, leaving the other unchanged, transforms $|\psi_{0,0}\rangle$ into a ME-state,

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

extending Eq. (2) to $N > 2$. This allows us to treat the cloning of N-dimensional states following closely Sec. 2.2, that is, by considering a 4-partite pure state, namely the state of a reference system R (initially entangled with the input I), the two outputs A and B, and the cloning machine (or a third output) C. Note that, using the same reasoning as in Sec. 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 a N^2-dimensional additional space whereas B is only N-dimensional.) Consequently, we need to consider a pure state in a N^4-dimensional Hilbert space.

3.2. Asymmetric 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 Eq. (9) for $N = 2$. By tracing over B and C the state Eq. (44), we see that the joint state of R and A is a mixture of the ME-states,

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

so that A can be viewed as the output of a channel that 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 reexpressed 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

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

These amplitudes characterize the quantum channel underlying 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, the outputs A and B of the N-dimensional 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 Eq. (47). It is easy to check that Eq. (47) reduces to Eq. (12) for qubits ($N = 2$). Let us prove Eqs. (46) and (47) by considering a single component $|\psi_{\mu,\nu}\rangle_{RA}|\psi_{\mu,N-\nu}\rangle_{BX}$ in Eq. (44), that is, choosing $\alpha_{m,n} = \delta_{m,\mu}\delta_{n,\nu}$. Eq. (47) gives $\beta_{m,n} = \mathrm{e}^{2\pi i[(n\mu-m\nu)/N]}/N$, so that Eq. (46) results in

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

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

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

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 Eq. (47).

Therefore, we have shown that the *complementarity* between the two outputs A and B of an N-dimensional cloning machine is governed by the relationship between a function and its Fourier transform. The tradeoff between the quality of the two copies is simply due to an "uncertainty principle" inherent to Fourier transforms. Indeed, Eq. (47) is basically a 2-dimensional discrete Fourier transform (up to an interchange of the indices m and n, and a minus sign):

$$\beta_{m,n} = F[n,m] \qquad \text{with } F[\tilde{x},\tilde{y}] = \mathcal{F}_2\{\alpha_{N-x,y}\} \tag{51}$$

where $\mathcal{F}_2$ is a 2-dimensional discrete 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 conversely. 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 as a consequence of an uncertainty principle. (Note that the index m of $p_{m,n}$ is dual to the index n of $q_{m,n}$, and conversely.) The normalization of the $\beta_{m,n}$'s simply results from Parseval's theorem: $\sum_{m,n}|\alpha_{m,n}|^2 = \sum_{m,n}|\beta_{m,n}|^2$. A symmetric N-dimensional cloning machine then corresponds essentially to a function $\alpha_{m,n}$ whose square is equal to its squared Fourier transform, i. e., $|\alpha_{m,n}|^2 = |\beta_{m,n}|^2$.

3.3. No-cloning inequality for N-dimensional states

We now investigate this complementarity principle in the special case where 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 function $P_{m,n} = \delta_{m,0}\,\delta_{n,0}$ (i. e., a perfect channel) and a flat function $F_{m,n} = 1/N$ (i. e., a fully depolarizing channel), with respective amplitudes $\overline{a}$ and a:

$$\alpha_{m,n} = \overline{a}\,P_{m,n} + a\,F_{m,n} \tag{52}$$

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

$$|\overline{a}|^2 + \frac{2}{N}\,\mathrm{Re}(\overline{a}a^*) + |a|^2 = 1 \tag{53}$$

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

$$\rho_{RA} = \left[|\overline{a}|^2 + \frac{2}{N}\,\mathrm{Re}(\overline{a}a^*)\right]\,|\psi_{0,0}\rangle\langle\psi_{0,0}| + |a|^2\,\frac{\mathcal{I}\otimes\mathcal{I}}{N^2} \tag{54}$$

so that the input state is replaced by a random state with probability $p = |a|^2$ and left unchanged with probability $1-p$. 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. Note that p denotes here the *randomization* probability of the depolarizing channel, that is $p = 1 - s$ where s is the scaling factor (this differs from our notation in Sec. 2). Using Eq. (47), we see that the second output is characterized by

$$\beta_{m,n} = \bar{b}\, P_{m,n} + b\, F_{m,n} \tag{55}$$

where $\bar{b} = a$ and $b = \bar{a}$, since $F_{m,n}$ are $P_{m,n}$ are dual under Fourier transform. Here $q = |b|^2$ is the randomization probability of the depolarizing channel associated with B. Thus, the complementarity of the two outputs of the class of asymmetric cloners considered here (i.e., cloners whose outputs emerge from depolarizing channels) can be simply written as

$$|a|^2 + \frac{2}{N}\mathrm{Re}(ab^*) + |b|^2 = 1 \tag{56}$$

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. Arguing like before, we write a *no-cloning* inequality for an N-dimensional quantum state:

$$a^2 + \frac{2}{N}\, ab + b^2 \geq 1 \tag{57}$$

where $p = a^2$ or $q = b^2$ is the randomization probability underlying output A or B, respectively. This corresponds to the domain in the (a,b)-space which is outside an ellipse, oriented just as in Fig. 2, whose semiminor axis is $\sqrt{N/(N+1)}$ and semimajor axis is $\sqrt{N/(N-1)}$. Equation (57) generalizes the no-cloning inequality for qubits, Eq. (18), which is simply equivalent to Eq. (57) for $N = 2$, substituting $x = a/2$ and $x' = b/2$. This ellipse intercepts its minor axis at $(\sqrt{N/2(N+1)}, \sqrt{N/2(N+1)})$, which corresponds to an N-dimensional UCM [6], as discussed below. 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 randomization probabilities cannot be lower than one, i.e., $p + q \geq 1$. The no-cloning inequality involves an "incoherent" sum in this limit (i.e., probabilities—not amplitudes—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 $p + q = 1$) can then be understood in classical terms: the input state is sent to output A or B with probability $1 - p = q$ or $1 - q = p$, respectively, the other output being a random N-dimensional state. There is no such classical interpretation for finite-N cloners, as $(1-p) + (1-q)$ can then exceed one.

3.4. Symmetric cloning machine or the N-dimensional UCM

It is easy to find the *symmetric* N-dimensional cloner of the class considered above (i.e., cloners whose outputs emerge from an N-dimensional depolarizing channel) by requiring that $a = b$ in Eq. (56), which simply results in

$$p = |a|^2 = \frac{N}{2(N+1)} \tag{58}$$

Thus, the scaling factor corresponding to both outputs is given by

$$s = 1 - |a|^2 = \frac{N+2}{2(N+1)} \tag{59}$$

in agreement with the expression derived in Ref. [6] for an N-dimensional UCM. Note that this cloner is also state-independent and acts on an arbitrary state as

$$|\psi\rangle \to \rho = \frac{N+2}{2(N+1)}\,|\psi\rangle\langle\psi| + \frac{N}{2(N+1)}\,(\mathcal{I}/N) \tag{60}$$

When $N \to \infty$, this 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 Sect. 2.4, it should be possible to find an entire class of symmetric cloners with $N > 2$, thereby generalizing Eq. (21). This would give rise to an upper bound on the quantum capacity of a general channel processing N-dimensional states, extending the bound Eq. (33) for Pauli channels. This will be reported elsewhere.

4. Conclusion

We have defined a class of asymmetric cloning machines for quantum bits and N-dimensional quantum states. For quantum bits, we have shown that the asymmetric Pauli cloning machine, whose outputs emerge from two distinct Pauli channels, generalizes the universal cloning machine of Buzek and Hillery. The 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 PCMs, we have also established an upper bound on the quantum capacity of the Pauli channel of probabilities $p_x = x^2$, $p_y = y^2$, and $p_z = z^2$, namely $C \leq 1 - 2(x^2 + y^2 + z^2 + xy + xz + yz)$. These considerations have been extended to N dimensions, showing that the notion of asymmetric cloners is quite general. The N-dimensional UCM appears as a special case of these cloners (symmetric and state-independent). 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 tradeoff governing the quality of the two outputs results from an uncertainty principle akin to the complementarity between position and momentum.

Acknowledgements I am grateful to V. Buzek for suggesting the extension of the Pauli cloning machine to N-dimensional quantum states. This work was supported in part by the National Science Foundation 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). NJC is Collaborateur scientifique of the Belgian National Fund for Scientific Research.

References

[1] D. Dieks: *Phys. Lett.* **92A** (1982) 271

[2] W.K. Wootters, W.H. Zurek: *Nature* **299** (1982) 802

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

[4] D. Bruss, D.P. DiVincenzo, A.K. Ekert, C.A. Fuchs, C. Macchiavello, J.A. Smolin: *Phys. Rev. A* **57** (1998) 2386

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

[6] V. Buzek, M. Hillery: *Los Alamos e-print quant-ph/9801009*

[7] N. Gisin, B. Huttner: *Phys. Lett. A* **228** (1997) 13

[8] N.J. Cerf: *Los Alamos e-print quant-ph/9803058*

[9] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, W. K. Wootters: *Phys. Rev. A* **54** (1996) 3824

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