Pauli Cloning of a Quantum Bit

Nicolas J. Cerf[1,2,3]
[1]*Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[2]*Information and Computing Technologies Research Section, Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California 91109*
[3]*W. K. Kellogg Radiation Laboratory, California Institute of Technology, Pasadena, California 91125*

(Received 30 March 1998; revised manuscript received 7 January 2000)

A family of asymmetric quantum cloning machines is introduced that produce two approximate copies of a single quantum bit, each copy emerging from a Pauli channel. A no-cloning inequality is derived, describing the balance between the quality of the copies. The Pauli cloning machine is also shown to put a limit on the quantum capacity of Pauli channels.

PACS numbers: 03.67.Hk, 03.65.Bz, 89.70.+c

A remarkable consequence of the linearity of quantum mechanics is that an unknown quantum state *cannot* be duplicated, as recognized after the seminal papers by Dieks [1] and Wootters and Zurek [2]. This so-called *no-cloning* theorem implies that there exists no physical process that produces *perfect* copies of a quantum bit (qubit) that is initially in an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Recently, it has been shown by Buzek and Hillery [3] that it is nevertheless possible to construct a cloning machine that yields two *approximate* copies of a qubit. Specifically, a universal cloning machine (UCM) can be defined that creates two copies each characterized by the same density operator ρ from a single qubit in state $|\psi\rangle$, the fidelity of cloning being $f \equiv \langle\psi|\rho|\psi\rangle = 5/6$. The UCM was later proved to be optimal by Bruss *et al.* [4] and Gisin and Massar [5]. This cloning machine is *universal* in the sense that the copies are state independent [both output qubits emerge from a depolarizing channel of probability $p = (1 - f)3/2 = 1/4$; that is, the Bloch vector characterizing the input $|\psi\rangle$ is shrunk by a factor of $2/3$ regardless its orientation]. A great deal of effort has been devoted recently to quantum cloners because of their use in the context of quantum communication and cryptography (see, e.g., [4,6]). For example, an interesting application of the UCM is that it can be used to establish a limit on the quantum capacity Q of a depolarizing channel, namely, $Q = 0$ at $p = 1/4$ [4].

In this Letter, I introduce a family of *asymmetric* cloning machines that produce two (not necessarily identical) output qubits, each emerging from a Pauli channel (defined below). This family of cloners, which I call *Pauli cloning machines* (PCM), relies on a parametrization of 4-qubit wave functions for which all qubit pairs are in a mixture of Bell states. Using these PCMs, I derive a *no-cloning inequality* governing the tradeoff between the quality of the two copies (this has been later shown to be a *tight* inequality for any cloning machine whose errors are isotropic [7]). I then consider a subclass of *symmetric* PCMs in order to express an upper limit on the quantum capacity Q of a Pauli channel of probabilities p_x, p_y, and p_z: I show that Q vanishes if $(\sqrt{p_x}, \sqrt{p_y}, \sqrt{p_z})$ lies on some ellipsoid whose pole coincides with the depolarizing channel that underlies the UCM.

A Pauli channel acts on a qubit in an arbitrary pure 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 (σ_y) with respective probabilities p_z, p_x, and p_y. A depolarizing channel corresponds to the special case $p_x = p_y = p_z$. An alternate description of the Pauli channel relies on an input qubit X that is initially in a maximally entangled state with a reference qubit R, say, in the Bell state $|\Phi^+\rangle$. Then, the joint state of R and the output Y is a mixture of the four Bell states $|\Phi^\pm\rangle = 2^{-1/2}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = 2^{-1/2}(|01\rangle \pm |10\rangle)$,

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

with $p = p_x + p_y + p_z$. The weights in Eq. (1) uniquely characterize the Pauli channel.

I define a Pauli cloning machine as a unitary transformation acting on an input qubit X along with two auxiliary qubits, which may be viewed as the blank copy and an ancilla (or the cloning machine itself). The operation of a PCM is then described by considering a 4-qubit system (see Fig. 1): qubits R and X, which are initially in the entangled state $|\Phi^+\rangle$, and the two auxiliary qubits that are in a prescribed state $|0\rangle$. The PCM admits two outputs, Y_1 and Y_2, which are required to emerge from (distinct) Pauli channels; equivalently, the density operators ρ_{RY_1} and ρ_{RY_2} must be mixtures of Bell states. An additional (or third) output Y_3 must be introduced for the following reason. Assume that the Bell-diagonal state ρ_{RY_1} results from the partial trace of a pure state in an extended Hilbert space. By Schmidt decomposition [8], this implies that a four-dimensional additional space is necessary to accommodate the four eigenvalues of ρ_{RY_1}, so that the two-dimensional space of Y_2 is insufficient for this purpose. In what follows, I restrict myself to the minimal case of a two-dimensional ancilla (the qubit Y_3).

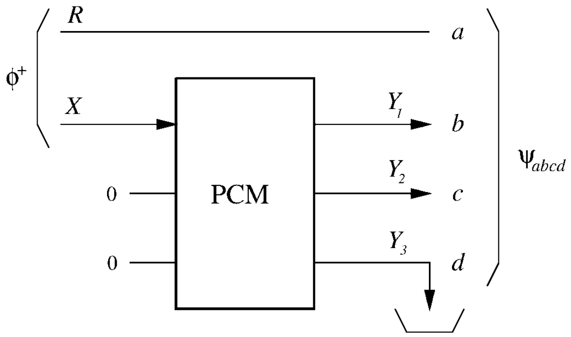

FIG. 1. Pauli cloning machine of input X and outputs Y_1 and Y_2. The additional output Y_3 refers to an ancilla (or the cloning machine). The three outputs emerge from (distinct) Pauli channels.

More specifically, a PCM is specified by the 4-qubit wave function underlying the entanglement of the three outputs with the reference. After cloning, the four qubits are in state $|\Psi\rangle_{RY_1Y_2Y_3}$ for which ρ_{RY_1} and ρ_{RY_2} must be Bell mixtures. I also make the additional requirement that the state of *every* qubit pair is a Bell mixture (in particular, the third output Y_3 also emerges from a Pauli channel). Let us find in general the 4-qubit wave functions $|\Psi\rangle_{abcd}$ that satisfy this requirement. Making use of the Schmidt decomposition for the bipartite partition ab vs cd, $|\Psi\rangle_{abcd}$ can be written as a superposition of *double Bell* states

$$|\Psi\rangle_{abcd} = \{v|\Phi^+\rangle|\Phi^+\rangle + z|\Phi^-\rangle|\Phi^-\rangle + x|\Psi^+\rangle|\Psi^+\rangle + y|\Psi^-\rangle|\Psi^-\rangle\}_{ab;cd}\,, \qquad (2)$$

where x, y, z, and v are complex amplitudes ($|x|^2 + |y|^2 + |z|^2 + |v|^2 = 1$). The qubit pairs ab and cd are then Bell mixtures; that is, $\rho_{ab} = \rho_{cd}$ is of the form of Eq. (1) with $p_x = |x|^2$, $p_y = |y|^2$, $p_z = |z|^2$, and $1 - p = |v|^2$. Remarkably, these double Bell states for the partition ab vs cd transform into superpositions of double Bell states for the two other possible partitions (ac vs bd, ad vs bc), e.g.,

$$|\Phi^+\rangle_{ab}|\Phi^+\rangle_{cd} = \frac{1}{2}\{|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\}_{ac;bd}\,. \qquad (3)$$

This implies that $|\Psi\rangle_{abcd}$ is also a superposition of double Bell states (albeit with different amplitudes) for these two other partitions, which, therefore, also yield Bell mixtures when tracing over half of the system. Table I summarizes the amplitudes of $|\Psi\rangle_{abcd}$ for the three partitions of $abcd$ into two pairs, starting from Eq. (2). Identifying a with the reference qubit (entangled with the input), b and c with the two outputs, and d with the ancilla, Table I characterizes the entire family of PCMs.

Let us first investigate the complementarity between the two copies produced by a PCM. If output b is characterized by the parameters v, z, x, and y, then output c has $v' = (v + z + x + y)/2$, $z' = (v + z - x - y)/2$, $x' = (v - z + x - y)/2$, and $y' = (v - z - x + y)/2$ [9]. Consider an asymmetric PCM whose two outputs b and c emerge from *depolarizing* channels. In other words, the PCM is required to yield two copies of a qubit that suffer isotropic (but different) errors, $|x| = |y| = |z|$ and $|x'| = |y'| = |z'|$; that is, the vector characterizing the input state $|\psi\rangle$ in the Bloch sphere undergoes a (different) shrinking at each output regardless of its orientation. A simple analysis shows that this implies $x = y = z$, and therefore

$$x' = y' = z' = (v - x)/2\,. \qquad (4)$$

Thus, if output b emerges from a depolarizing channel of probability $p = 3|x|^2$, then output c necessarily emerges from a depolarizing channel of probability $p' = 3|x'|^2 = \frac{3}{4}|v - x|^2$. Using Eq. (4) and the normalization condition $|v|^2 + 3|x|^2 = 1$, the relation between x and x' can be written as

$$|x|^2 + \mathrm{Re}(x^* x') + |x'|^2 = 1/4\,. \qquad (5)$$

The best cloning (minimum $|x|$ and $|x'|$) is achieved when the cross term is largest in magnitude, that is, when x and x' have the same (or opposite) phases. We may thus take x and x' real and positive without loss of generality. As a consequence, the tradeoff between the quality of the two copies of an isotropic PCM can be characterized by the *no-cloning* inequality

$$x^2 + xx' + x'^2 \geq 1/4\,, \qquad (6)$$

where the copying error is measured by the depolarizing probability of the channel underlying each output, i.e., $p = 3x^2$ and $p' = 3x'^2$. In view of the restrictions imposed on the PCM (two-dimensional ancilla, and the requirement that all qubit pairs are Bell diagonal), this

TABLE I. Amplitudes of $|\Psi\rangle_{abcd}$ in terms of the double Bell states for the three possible partitions of the four qubits *abcd* into two pairs.

$\lvert\Psi\rangle_{abcd}$	$\lvert\Phi^+\rangle\lvert\Phi^+\rangle$	$\lvert\Phi^-\rangle\lvert\Phi^-\rangle$	$\lvert\Psi^+\rangle\lvert\Psi^+\rangle$	$\lvert\Psi^-\rangle\lvert\Psi^-\rangle$
ab vs *cd*	v	z	x	y
ac vs *bd*	$\frac{1}{2}(v + z + x + y)$	$\frac{1}{2}(v + z - x - y)$	$\frac{1}{2}(v - z + x - y)$	$\frac{1}{2}(v - z - x + y)$
ad vs *bc*	$\frac{1}{2}(v + z + x - y)$	$\frac{1}{2}(v + z - x + y)$	$\frac{1}{2}(v - z + x + y)$	$\frac{1}{2}(v - z - x - y)$

no-cloning inequality applies only to a restricted set of all the cloners that produce two copies with isotropic errors. Nevertheless, since it is known that a single ancillary qubit is sufficient for the optimal UCM [3,4], I conjectured in a previous version of this paper that Eq. (6) is the tightest no-cloning bound that can be written for the asymmetric cloning of a qubit, and that it is saturated for those PCMs having a phase difference of 0 (or π) between x and x'. After completion of this paper, independent work by Niu and Griffiths [7] was pointed out to me, where this optimality of the PCM is rigorously proven.

Equation (6) corresponds to the domain in the (x, x') space located outside an ellipse whose semiminor axis $b = 1/\sqrt{6}$ is oriented in the direction $(1, 1)$, as shown in Fig. 2. The semimajor axis is $a = 1/\sqrt{2}$. The origin in this space corresponds to a (nonexisting) cloner whose two outputs would be perfect $p = p' = 0$. The ellipse characterizes the ensemble of values for p and p' that can be achieved with a PCM. It intercepts its minor axis at $(1/\sqrt{12}, 1/\sqrt{12})$, which corresponds to the UCM, i.e., $p = p' = 1/4$. This point is the closest to the origin and characterizes in this sense the best possible cloner (i.e., with minimum $p + p'$). Note that the underlying 4-qubit wave function

$$|\Psi\rangle_{abcd} = \sqrt{\frac{3}{4}}\,|\Phi^+\rangle_{ab}|\Phi^+\rangle_{cd} + \sqrt{\frac{1}{12}}\,\{|\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\}_{ab;cd} \tag{7}$$

$$= \sqrt{\frac{1}{3}}\,\{|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle\}_{ad;bc} \tag{8}$$

is symmetric under the interchange of a and d (or b and c), and maximizes the entropy of ad or bc (or minimizes the mutual entropy between the two outputs). 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 domain inside the ellipse corresponds to the values for p and p' that cannot be achieved simultaneously, reflecting the impossibility of close-to-perfect cloning imposed by quantum mechanics.

Consider now a class of *symmetric* PCMs that have both outputs emerging from the *same* Pauli channel, i.e., $\rho_{ab} = \rho_{ac}$. The corresponding set of conditions $|x| = |x'|$, $|y| = |y'|$, and $|z| = |z'|$ admits the solution

$$v = x + y + z\,. \tag{9}$$

(It also has an uninteresting solution $x = y = z = -v = 1/2$ that characterizes a PCM whose two outputs are fully depolarizing.) Equation (9), together with the normalization condition, describes a 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 $p_z = z^2$ (x, y, and z are assumed to be real). This surface,

$$x^2 + y^2 + z^2 + xy + xz + yz = \frac{1}{2}\,, \tag{10}$$

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 $a = 1/2$, while the semimajor axis (or equatorial radius) is $b = 1$. In this representation, the distance to the origin is $p_x + p_y + p_z$, so 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 coincides with the UCM. This simply illustrates that the requirement of having an optimal cloning

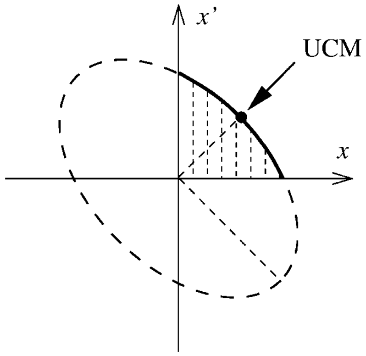

FIG. 2. Ellipse relating the two outputs of an (optimal) isotropic PCM that emerge from depolarizing channels of probability $p = 3x^2$ and $p' = 3x'^2$ (only the quadrant $x, x' \geq 0$ is of interest here). Any close-to-perfect cloning characterized by a point inside the ellipse is forbidden.

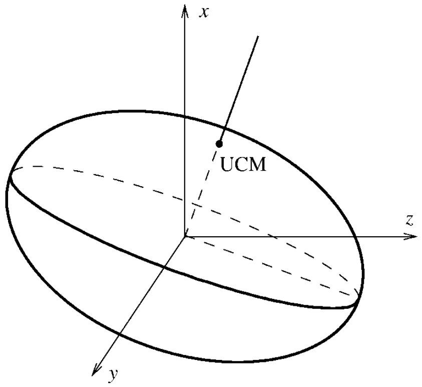

FIG. 3. Ellipsoid representing the class of symmetric PCMs whose two outputs emerge from the same Pauli channel of parameters $p_x = x^2$, $p_y = y^2$, and $p_z = z^2$ (only the octant $x, y, z \geq 0$ is considered here). The capacity of a Pauli channel that lies on this ellipsoid must be vanishing.

(minimum $p_x + p_y + p_z$) implies that the cloner is state independent ($p_x = p_y = p_z$).

The class of symmetric PCMs characterized by Eq. (10) can be used in order to put a limit on the quantum capacity Q [10] of a Pauli channel, thereby extending the result of Bruss *et al.* [4]. Indeed, applying an error-correcting scheme separately on outputs b and c of the PCM (obliviously of the other output) would lead to a violation of the no-cloning theorem if the capacity Q of the channel $X \to Y_1$ (or $X \to Y_2$) was nonzero. Since Q is a nonincreasing function of p_x, p_y, and p_z for $p_{x,y,z} \leq 1/2$ (adding noise to a channel cannot increase its capacity), I conclude that $Q(p_x, p_y, p_z) = 0$ for any Pauli channel (x, y, z) that lies on (or outside) the ellipsoid E. In particular, Eq. (10) 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 Q cannot be superadditive for a convex combination of a perfect and a noisy channel [10], an upper bound on Q can be written using a linear interpolation between the perfect channel $(0, 0, 0)$ and any Pauli channel lying on E:

$$Q \leq 1 - 2(x^2 + y^2 + z^2 + xy + xz + yz). \qquad (11)$$

It must be emphasized that the validity of this bound actually depends on the reasonable—but unproven—conjecture that Q is a continuous function of $p_{x,y,z}$, for the proof in Ref. [10] is not valid at the limit of a noisy channel of vanishing capacity, which happens to be the case on E. Note that another class of symmetric PCMs can be found by requiring $\rho_{ab} = \rho_{ad}$, which implies $v = x - y + z$ rather than Eq. (9). This requirement 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 Q because this class of PCMs has noisier outputs in the octant $x, y, z \geq 0$.

Let us now turn to the fully symmetric PCMs that have *three* outputs emerging from the *same* Pauli channel, which corresponds to a family of (nonoptimal) quantum *triplicating* machines. The requirement $\rho_{ab} = \rho_{ac} = \rho_{ad}$ implies $(v = x + z) \wedge (y = 0)$. 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.) These triplicators are represented by the intersection of E with the xz plane, that is, the ellipse

$$x^2 + z^2 + xz = \frac{1}{2}, \qquad (12)$$

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

$$|\Psi\rangle_{abcd} = \frac{2}{\sqrt{6}}|\Phi^+\rangle|\Phi^+\rangle + \frac{1}{\sqrt{6}}|\Phi^-\rangle|\Phi^-\rangle + \frac{1}{\sqrt{6}}|\Psi^+\rangle|\Psi^+\rangle, \qquad (13)$$

which is symmetric under the interchange of any two qubits and maximizes the 2-bit entropy. Equation (13) thus characterizes the best triplicator of this ensemble, whose three outputs emerge from a "2-Pauli" channel with $p = 1/3$ ($p_x = p_z = 1/6$). Equivalently, the operation of this triplicator on an arbitrary pure state $|\psi\rangle$ can be written as

$$|\psi\rangle \to \frac{1}{2}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^*\rangle\langle\psi^*| + \frac{1}{3}(\mathbb{1}/2), \qquad (14)$$

which coincides with the triplicator that is considered in Ref. [11]. If $|\psi\rangle$ is real, the copies are the same as those yielded by the UCM.

I have introduced an asymmetric Pauli cloning machine which allowed me to derive a no-cloning inequality for quantum bits, quantifying the impossibility of copying due to quantum mechanics. Furthermore, I have established a limit on the quantum capacity of the Pauli channel, relying on a class of symmetric PCMs.

This work was supported in part by the NSF under Grants No. PHY 94-12818 and No. PHY 94-20470, and by a grant from DARPA/ARO through the QUIC Program (No. DAAH04-96-1-3086).

[1] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[2] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[3] V. Buzek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[4] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[5] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[6] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).
[7] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[8] A. Ekert and P. L. Knight, Am. J. Phys. **63**, 415 (1995).
[9] This transformation is simply a two-dimensional discrete Fourier transform, which accounts for the tradeoff between the quality of the copies.
[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[11] V. Buzek, S. L. Braunstein, M. Hillery, and D. Bruss, Phys. Rev. A **56**, 3446 (1997).