Optimal cloning of qubits given by an arbitrary axisymmetric distribution on the Bloch sphere

Karol Bartkiewicz and Adam Miranowicz
Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland
(Received 6 July 2010; published 22 October 2010)

We find an optimal quantum cloning machine, which clones qubits of arbitrary symmetrical distribution around the Bloch vector with the highest fidelity. The process is referred to as phase-independent cloning in contrast to the standard phase-covariant cloning for which an input qubit state is *a priori* better known. We assume that the information about the input state is encoded in an arbitrary axisymmetric distribution (phase function) on the Bloch sphere of the cloned qubits. We find analytical expressions describing the optimal cloning transformation and fidelity of the clones. As an illustration, we analyze cloning of qubit state described by the von Mises–Fisher and Brosseau distributions. Moreover, we show that the optimal phase-independent cloning machine can be implemented by modifying the mirror phase-covariant cloning machine for which quantum circuits are known.

DOI: 10.1103/PhysRevA.82.042330 PACS number(s): 03.67.−a, 05.30.−d, 42.50.Dv

I. INTRODUCTION

The no-cloning theorem [1] states that no quantum-mechanical evolution exists which would transform an unknown quantum state $|\psi\rangle$ according to $|\psi\rangle \to |\psi\rangle|\psi\rangle$. This is provided by the linearity of quantum mechanics. The no-cloning theorem guaranties, e.g., the security (privacy) of quantum-communication protocols including quantum key distribution.

Exact cloning is impossible; however, imperfect (optimal) cloning is possible as it was first shown by Bužek and Hillery [2] by designing a $1 \to 2$ cloning machine, referred to as the *universal cloner* (UC). The cloning machine prepares two approximate copies of an unknown pure qubit state. The UC generates two qubit states with the same fidelity $F = 5/6$. Fidelities of the clones to the initial pure state are equal $F_1 = F_2$. Therefore, the UC is a state-independent symmetric cloner.

It was later shown that for the $1 \to M$ UC, a relation between the optimum fidelity F of each copy and the number M of copies is given by $F = (2M + 1)/(3M)$ [3]. Setting $M \to \infty$ corresponds to a classical copying process with $F = 2/3$, which is the best fidelity that one can achieve with only classical operations.

Further works have extended the concept to include cloning of qudits, cloning of continuous-variable systems, or state-dependent cloning (non-universal cloning), which can produce clones of a specific set of qubits with much higher fidelity than the UC [4–16] (see also reviews [17,18] and references therein).

The study of the state-dependent cloning machines is important because it is often the case that we have some *a priori* information on a given quantum state that we want to clone, but we do not know it exactly. Then, by employing the available *a priori* information, we can design a cloning machine which outperforms the UC for some specific set of qubits. For example, if it is known that the qubit is chosen from the equator of the Bloch sphere then the so-called *phase-covariant cloners* (PCCs) have been designed [7,11], and it was shown to be optimal providing a higher fidelity than the UC.

Phase-covariant cloning of qubits has been further explored. For example, Fiurášek [9] studied the PCCs with known expectation value of Pauli's σ_z operator and provided two optimal symmetric cloners: one for the states in the lower and the other for those in the upper hemisphere of the Bloch sphere. Hu *et al.* [13] studied phase-independent cloning of qubits uniformly distributed on a belt of the Bloch sphere. Bartkiewicz *et al.* [12] provided an optimal cloning transformation, referred to as the *mirror phase-covariant cloning* (MPCC), for qubits of known modulus of expectation value of Pauli's σ_z operator.

Optimal cloning plays a crucial role in, e.g., quantum cryptography. Security analyses of the quantum key distribution protocols against coherent and incoherent attacks using quantum cloners can be found in Refs. [19–23]. Optimal phase-independent cloners seem to play a special role there. One example of the optimal phase-independent cloning machines is the PCC, which can be used in an optimal attack on the BB84 quantum key distribution protocol [19–21]. Another example is the UC, which enables an optimal incoherent attack on the six-state protocol [19,22,23].

Our paper is devoted to *phase-independent cloning*, which refers to cloning of qubits assuming that their distribution (symmetrical around the Bloch vector) is *a priori* known. It is related to the optimal state estimation [24] and to phase-independent telecloning and telemapping [16]. Phase-independent cloning includes the majority of all known optimal cloning machines as special cases. One of the exceptions is the phase-dependent cloning machine recently described in Ref. [25].

In this paper, we find that phase-independent cloning can be implemented analogously to the MPCC, e.g., in linear-optical systems [26] or quantum dots [12] (see also Ref. [27]).

Phase-independent cloning is an example of the optimal cloning problem being invariant with respect to the discrete Weyl-Heisenberg group (see, e.g., Ref. [18]).

We also show here that the phase-independent cloning exhibits sudden change in average single-copy fidelity, when the symmetry of the system is reduced from U(2) to U(1).

Optimal cloning also limits the capacity of quantum channels. An example is the Pauli channel and Pauli cloning machines analyzed by Cerf [28]. Our results could be used in a similar analysis for channels that undergo phase-independent damping.

The paper is organized as follows. In Sec. II, we present a general transformation describing an optimal symmetric

$1 \to 2$ cloning of a qubit. In Sec. III, we describe the optimal symmetric $1 \to 2$ cloning of a qubit knowing *a priori* its axisymmetric distribution on the Bloch sphere. This cloning is referred to as the optimal phase-independent cloning. In Sec. IV, we analyze two examples of such cloning of qubits described by the von Mises–Fisher and Brosseau distributions. In Sec. V, we present, probably the most important result of the paper, the optimality proof for the phase-independent cloning transformation. In Sec. VI, we describe a quantum circuit implementing the optimal phase-independent cloning. We conclude in Sec. VII.

II. OPTIMAL SYMMETRIC CLONING OF QUBITS

Suppose we want to clone a set of qubits, for which some characteristic point is in the following *a priori* known pure state:

$$|\psi\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle, \tag{1}$$

which is parametrized by polar ϑ and azimuthal φ angles on the Bloch sphere. We can express all other qubit states as

$$|\psi(\theta,\phi)\rangle = \cos\frac{\theta}{2}|\psi\rangle + e^{i\phi}\sin\frac{\theta}{2}|\bar{\psi}\rangle, \tag{2}$$

where $|\bar{\psi}\rangle$ is a state orthogonal to $|\psi\rangle$, i.e., $\langle\psi|\bar{\psi}\rangle = 0$. Note that $\cos\theta$ is equal to the scalar product of the Bloch vectors $\vec{r} = [\langle\sigma_x\rangle,\langle\sigma_y\rangle,\langle\sigma_z\rangle]$ and describes an elevation of an arbitrary qubit with respect to the reference qubit $|\psi\rangle$, whereas ϕ angle is an azimuth. Please note, however, that θ is measured from $|\psi\rangle$.

The quality of the cloning can be described by the fidelity of a single clone defined as

$$F_i(\theta,\phi) = \langle\psi(\theta,\phi)|\rho_i|\psi(\theta,\phi)\rangle, \tag{3}$$

where $\rho_i = \mathrm{Tr}_{i\oplus 1}(\rho_{\mathrm{out}})$ is the reduced density matrix of the ith clone ($i = 1,2$) and $\oplus$ denotes summation modulo 2. To obtain an optimal cloner for an arbitrary distribution of qubits, we use average single-copy fidelity F in a way similar to that used for the MPCC [26]. Thus, we express F as

$$F = \frac{1}{2}\int_0^{2\pi}\int_{-1}^{1} g(\theta,\phi)\,[F_1(\theta,\phi) + F_2(\theta,\phi)]\; d\cos\theta\, d\phi, \tag{4}$$

where $g(\theta,\phi)$ is an arbitrary distribution satisfying the normalization condition

$$\int_0^{2\pi}\int_{-1}^{1} g(\theta,\phi)\, d\cos\theta\, d\phi = 1. \tag{5}$$

In the special case of

$$g(\theta,\phi) = \frac{1}{4\pi\sin\vartheta}[\delta(\vartheta-\theta) + \delta(\vartheta+\pi-\theta)], \tag{6}$$

our generalized cloner reduces to the MPCC.

The optimal cloning transformation can be found by maximizing single-copy fidelity F_i, where $i = 1$ or 2, averaged over the distribution $g(\theta,\phi)$ representing the frequency of occurrence of the considered qubits [12].

Note that distributions g describe our classical knowledge about qubits to be cloned. Thus, the distributions g are classical although cloning is quantum. Probably all works on optimal quantum cloning are concerned with cloning of pure quantum states. Indeed, a generic quantum cloning task for pure states can be formulated such that the state to be cloned is drawn from a certain ensemble of pure states with some *a priori* probability and sent to the cloning machine which should produce replicas of the input state. The quality of the cloner is then usually characterized by mean clone fidelity averaged over the whole ensemble. The probability distribution characterizing the ensemble of states which one wants to clone is given by g in our case. So, g is a classical probability distribution on a unit sphere.

An optimal symmetric $1 \to 2$ cloning transformation must be symmetric with respect to the swap operation on clones. So, if we neglect the phase relations, the optimal transformation for an arbitrary distribution of qubits can be expressed as

$$\begin{aligned}
|\psi\rangle_{\mathrm{in}}|00\rangle_{1,2} \to\ & \cos\alpha_+(\cos\beta_+|\psi,\psi\rangle_{1,2} + \sin\beta_+|\bar{\psi},\bar{\psi}\rangle_{1,2}) \\
& \otimes|\bar{\psi}\rangle_3 + \sin\alpha_+|\Psi_+\rangle_{1,2}|\psi\rangle_3, \\
|\bar{\psi}\rangle_{\mathrm{in}}|00\rangle_{1,2} \to\ & \cos\alpha_-(\cos\beta_-|\psi,\psi\rangle_{1,2} + \sin\beta_-|\bar{\psi},\bar{\psi}\rangle_{1,2}) \\
& \otimes|\psi\rangle_3 + \sin\alpha_-|\Psi_+\rangle_{1,2}|\bar{\psi}\rangle_3,
\end{aligned} \tag{7}$$

where $|\Psi_\pm\rangle = (|\psi,\bar{\psi}\rangle \pm |\bar{\psi},\psi\rangle)/\sqrt{2}$, $\langle\bar{\psi}|\psi\rangle = 0$, and subscripts 1 and 2 denote the clones whereas 3 denotes the ancillary qubit. The angles $\alpha_\pm$ and $\beta_\pm$ are found by maximizing the average single-copy fidelity.

It is worth noting that we are *not* analyzing an optimal cloning of mixed qubit states given by

$$\rho = \int_0^{2\pi}\int_{-1}^{1} g(\theta,\phi)|\psi(\theta,\phi)\rangle\langle\psi(\theta,\phi)|\, d\cos\theta\, d\phi. \tag{8}$$

By contrast, we are analyzing cloning of each of the pure qubit states from an ensemble separately. While the distribution $g(\theta,\phi)$ is a weight function for a single-copy fidelity of a qubit state $|\psi(\theta,\phi)\rangle$.

III. OPTIMAL CLONING FOR AXISYMMETRIC DISTRIBUTIONS

In the following, for simplicity, we consider only axisymmetric distributions. The symmetry of the distributions means that the cloning transformation is phase independent (does not depend on azimuthal angle ϕ), i.e., distributions of qubits to be cloned are symmetrical along an arbitrary $|\psi\rangle$ axis. Moreover, we first postulate (as in Ref. [13]) that $\beta_\pm = 0$ and then (in Sec. V) we prove that such transformation is optimal for cloning.

When $\vartheta = \varphi = 0$, see Eq. (1), all the formulas can be rewritten in a computational basis by simply substituting $|\psi\rangle$ and $|\bar{\psi}\rangle$ with $|0\rangle$ and $|1\rangle$, respectively. Please note that one can proceed also in the opposite direction; i.e., one can start assuming that the distributions are centered around poles of the Bloch sphere (a local coordinate system) and later transformed to the basis so that the states match in, e.g., the laboratory frame (a global coordinate system). We choose the first approach, since we believe that it gives better physical intuition of the problem.

The density matrix of a single clone ρ_i is derived by taking a partial trace (over the ancillary qubit and one of the clones) of the density matrix describing the system after the cloning transformation. As a result we obtain

$$\rho_i = \frac{1}{2}\left[\left((\cos^2\alpha_+ + 1)\cos^2\frac{\theta}{2} + \sin^2\alpha_- \sin^2\frac{\theta}{2}\right)|\psi\rangle\langle\psi| + \left((\cos^2\alpha_- + 1)\sin^2\frac{\theta}{2} + \cos^2\alpha_+\cos^2\frac{\theta}{2}\right)|\bar{\psi}\rangle\langle\bar{\psi}| + \left(\frac{e^{-i\phi}}{\sqrt{2}}\sin\theta\sin\Omega|\psi\rangle\langle\bar{\psi}| + \text{H.c.}\right)\right], \quad (9)$$

where $i = 1,2$ and $\Omega = \alpha_+ + \alpha_-$. Now, we can express the single-copy fidelity, given by Eq. (3), as

$$F_i = \frac{1}{8}\left[2(3+\cos 2\alpha_+)\cos^4\frac{\theta}{2} + 2(3+\cos 2\alpha_-)\sin^4\frac{\theta}{2} + (\sin^2\alpha_+ + \sin^2\alpha_- + 2\sqrt{2}\sin\Omega)\sin^2\theta\right]. \quad (10)$$

We obtain expressions for $\alpha_\pm$ by maximizing, with respect to $g(\theta)$, the average single-copy fidelity F, given by Eq. (4). Any distribution axisymmetric function $g(\theta)$ can be expressed in terms of the Legendre polynomials $P_n(\cos\theta)$ in the following way [29]:

$$g(\theta) = \frac{1}{4\pi}\sum_{n=0}^{\infty}(2n+1)a_n P_n(\cos\theta), \quad (11)$$

$$a_n = \int_0^{2\pi}\int_{-1}^{1} g(\theta)P_n(\cos\theta)\, d\cos\theta\, d\phi. \quad (12)$$

Thus, we present the results in terms of the expansion coefficients a_n.

The form of the expressions for $\alpha_\pm$ depends on a single parameter Γ, which is a generalization of the T parameter in Ref. [13]:

$$\Gamma = \frac{6\sqrt{2}a_1(a_2-1)}{x_+x_-}, \quad (13)$$

where $x_\pm = 1 + 2a_2 \pm 3a_1$. We notice that for a normalized qubit distribution ($a_0 = 1$) one needs to know only a_1 and a_2 in order to fully characterize the corresponding optimal cloning transformation. As long as $|\Gamma| < 1$, we can express the parameters describing the cloning transformation as

$$2\alpha_\pm = \arcsin\Omega \pm \arcsin\Gamma, \quad (14)$$

where

$$\Omega = \frac{2\sqrt{2}(1+2a_2)(1-a_2)}{\sqrt{3x_+x_-\left(3+4a_2^2-3a_1^2-4a_2\right)}}. \quad (15)$$

However, if $|\Gamma| > 1$ then $\alpha_+ = 0$ and $\alpha_- = \frac{\pi}{2}$ or vice versa, and the optimal cloning transformation corresponds to one of the transformations derived by Fiurášek in Ref. [9]. The case of $a_1 = 0$ includes the PCC for $\theta = \pi/2$ and the MPCC [12] ($\alpha_+ = \alpha_-$). Moreover, for $a_1 = a_2 = 0$, we recover the UC transformation [2]. Also the optimal cloning transformation of Hu *et al.* [13] can be derived for an arbitrary belt of the Bloch sphere.

IV. EXAMPLES OF PHASE-INDEPENDENT CLONING

A. Optimal cloning of the von Mises–Fisher distribution

As an example of phase-independent cloning, let us analyze the cloning of qubits described by the von Mises–Fisher distribution (also called the Fisher distribution) [30], which is an analog of the normal distribution but on a two-dimensional sphere in $\mathbf{R}^3$ (see Fig. 1). The distribution describes dispersion on a sphere and has applications not only in physics and mathematical statistics (especially directional statistics) but also in quantitative biology, geology, or text data mining. It is a single-parameter distribution which could be used to describe qubits which undergo a random damping process; for example, weak narrow-band light pulses propagating via real media or spin-1/2 systems in the presence of magnetic field fluctuations. The distribution converges to a two-dimensional Gaussian distribution for large values of κ. For $\kappa = 0$ it becomes a uniform distribution on a sphere.

The von Mises–Fisher distribution is given by

$$g(\theta) = \frac{\kappa\exp(\kappa\cos\theta)}{4\pi\sinh\kappa}, \quad (16)$$

where κ is the concentration parameter (inverted variance), which can also be negative when describing distribution concentrated around $|\bar{\psi}\rangle$. For the von Mises–Fisher distribution,

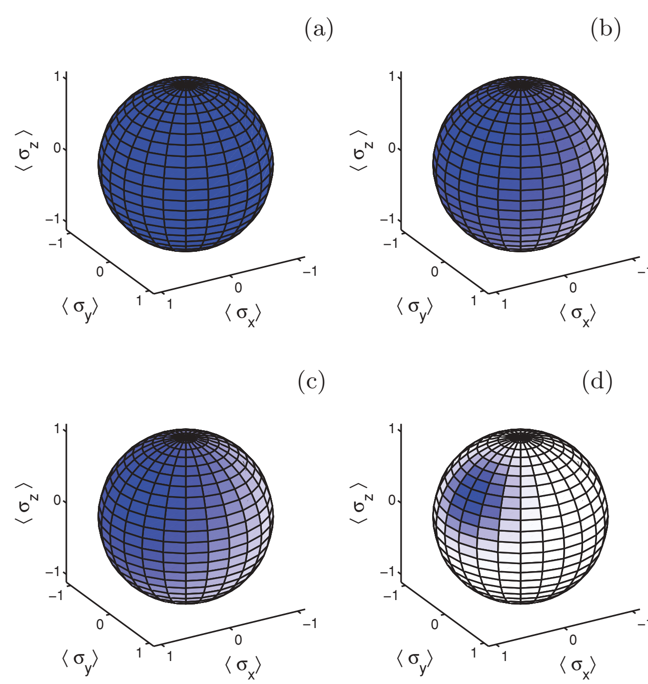

FIG. 1. (Color online) Qubit states described on the Bloch sphere by the von Mises–Fisher distribution (where the symmetry axis is rotated from the north pole by $\vartheta = \pi/3$ and $\varphi = \pi/35$) divided by its largest value for (a) $\kappa = 0$, (b) $\kappa = 0.3305$, (c) $\kappa = 1$, and (d) $\kappa = 10$. The darker the region, the higher the values of the probability distribution function. The mean value $\langle\sigma_z\rangle = 1$. The optimal cloning machines are the UC [2] for case (a) and the PCC [9] for the other cases. Note that the transition area between (a) and (b) corresponds neither to the UC nor the PCC.

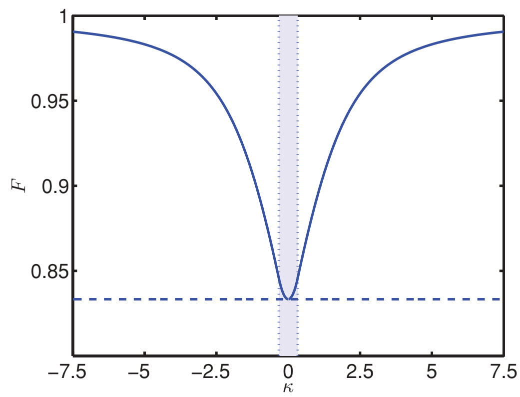

FIG. 2. (Color online) Average single-copy fidelity F vs. concentration κ. The dashed line for $F = 5/6$ corresponds to the UC limit, which is reached for $\kappa = 0$. The shaded area corresponds to the range $-0.3305 < \kappa < 0.3305$, where the PCC is no longer optimal.

we get the expansion coefficients, defined in Eq. (12), as follows:

$$a_1 = -1/\kappa + \coth\kappa, \\ a_2 = 1 - 3\kappa a_1. \tag{17}$$

If $\kappa \geqslant 0.3305$ then the PCC transformation of Fiurášek's [9] is optimal. On the other hand, if $\kappa = 0$ the optimal cloning transformation corresponds to the UC [2]. So, practically, a very small axisymmetric concentration of qubits (small value of κ), as shown in Fig. 1 (Fig. 2), is enough to determine which of the two cloning transformations is optimal.

We can see in Fig. 2 that the optimal cloning is related to the symmetry of the cloned set of qubits (see, e.g., Ref. [31]). As one would expect, there is a sudden change in the average single-copy fidelity when the set of cloned qubits reduces its symmetry from U(2) to U(1).

It is somewhat surprising that the von Mises–Fisher distribution, which is an analog of Gaussian distribution on a sphere, is not widely used in Monte Carlo simulations. This is because of its computational overhead. A more popular one-parameter phase distribution on a sphere is the Henyey-Greenstein function [32], for which $a_n = h^n$ and h is the anisotropy factor equal to the average of $\cos\theta$. The Henyey-Greenstein function is widely used in simulations of, e.g., volume scattering processes. The explicit form of this function is similar to the Brosseau distribution discussed in the following subsection.

B. Optimal cloning of the Brosseau distribution

Another example of phase-independent cloning is cloning of photons of known statistics of a single Stokes parameter, e.g., S_1. Statistics of the Stokes parameters was studied in detail by Barakat [33]; however, for us the statistics of the normalized Stokes parameters is of greater interest since it describes the state of a single photon.

In the quantum regime, the normalized Stokes parameters $s_i = S_i/S_0$ for $i = 1,2,3$ correspond to Pauli's operators in the following way: $s_1 = \sigma_z$, $s_2 = \sigma_x$, and $s_3 = \sigma_y$. Here, the matrices are defined in the basis of $\{|\psi\rangle = |H\rangle, |\bar{\psi}\rangle = |V\rangle\}$, i.e., for the horizontal and vertical polarization states, correspondingly.

For a Gaussian stochastic plane-wave field, the normalized Stokes s_1 parameter has the following probability distribution function derived by Brosseau [34]:

$$g(\theta) = \frac{(1-P^2)(1-\mu\cos\theta)}{2[(1-\mu\cos\theta)^2 - (1-\cos^2\theta)(P^2-\mu^2)]^{\frac{3}{2}}}, \tag{18}$$

where $\cos\theta = s_1$ is the Stokes parameter, P is the degree of polarization, and $\mu = \langle S_1\rangle/\langle S_0\rangle$; moreover, $P^2 - \mu^2 \geqslant 0$. The Brosseau distribution has the same asymptotic behavior as the von Mises–Fisher distribution if analyzed for two limiting values of P. For $P = 0$, we have unpolarized light and the resulting distribution is uniform, which corresponds to the UC. For $P = 1$, the polarization can be described as $\cos\theta|H\rangle + \exp(i\phi)\sin\theta|V\rangle$, where θ is fixed and ϕ is an unknown constant. So, the distribution converges to Dirac's δ function $\delta(\cos\theta - \mu)$, which corresponds to the PCC [9]. Then the distribution is given by two physical parameters P and μ describing our knowledge about the polarization state of the photon. The lowest degree of polarization is given as $P^2 = \mu^2$, this corresponds to a situation in which phase ϕ is random (see Fig. 3). By varying those two parameters, we can construct various qubit distributions, as shown, e.g., in Fig. 4. For the Brosseau [34] distribution, the a_i coefficients are more complicated than those in Eq. (17) as given by

$$a_1 = \frac{1-P^2}{2}(I_1 - \mu I_2), \\ a_2 = \frac{3}{4}(1-P^2)(I_2 - \mu I_3) - \frac{1}{2}, \tag{19}$$

where

$$I_n = \int_{-1}^{1} \frac{x^n}{(1+\mu^2-P^2-2x\mu+x^2P^2)^{3/2}}\, dx. \tag{20}$$

It is worth noting that the field discussed by Brosseau in Ref. [34] was analyzed using the classical description of the polarized light. Namely, he considered a Gaussian stochastic plane-wave field. In his main formula, Brosseau used the

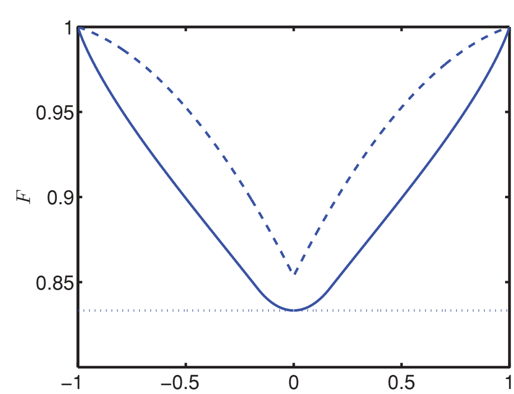

FIG. 3. (Color online) Average single-clone fidelity F vs. parameter μ for $\mu^2 = P^2$ (solid) and $\mu \neq P = 1$ (dashed curve). The dotted line for $F = 5/6$ shows the UC limit, which is reached for $\mu = P = 0$, whereas the dashed curve corresponds to the fidelity of the PCC.

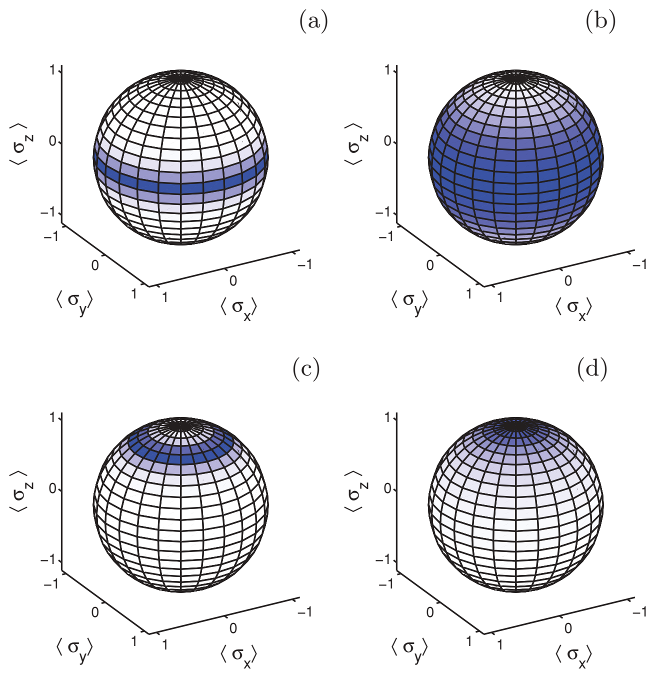

FIG. 4. (Color online) Same as Fig. 1, but for the Brosseau distribution assuming (a) $\mu = 0$, $P = 0.99$, (b) $\mu = 0$, $P = 0.65$, (c) $\mu = 0.8$, $P = 0.99$, and (d) $\mu = 0.8$, $P = 0.8$. The optimal cloning machines are the MPCC [12] with $\Lambda = \cos\alpha_+$ for case (a) and the PCC [9] for the other cases.

following notations: the angular brackets denote the time average, while P is the classical degree of polarization. So, we use Eq. (18), which was obtained using a classical description of light for a quantized field. Thus, one can raise an objection that the use of a final classical distribution $g(\theta)$, obtained using the classical degree of polarization and the time average of the Stokes parameters, in the case of a quantum description of the field is incorrect.

To show that the application of classical distributions $g(\theta)$ for quantum cloning is indeed correct, let us clarify the following point: The optimal quantum phase-cloning described in the present manuscript and in the vast majority of papers on quantum cloning (see reviews [17,18] and references therein) is *not* cloning of mixed qubit states, but it is cloning of a pure qubit state from an ensemble. We know *a priori* that the ensemble is described by some distribution $g(\theta)$ which represents our classical partial knowledge about the qubit to be cloned. Thus, the distribution is classical although cloning transformation is quantum.

Our application of classical distribution $g(\theta)$ is in complete agreement with other works on optimal cloners (see Table I). Our examples include (i) the universal cloners of Bužek and Hillery [2], where the classical distribution $g(\theta)$ is equal to $\frac{1}{4\pi}$, (ii) the optimal phase-covariant cloners of Bruß *et al.* [5,7] (for $\vartheta = \pi/2$) and of Fiurášek [8,9] (for any ϑ), where $g(\theta)$ is given by Dirac's δ function $\delta(\vartheta-\theta)/(2\pi\sin\vartheta)$, (iii) the optimal mirror phase-covariant cloners of Bartkiewicz *et al.* [12], where $g(\theta)$ is given by Eq. (6), and (iv) the optimal quantum cloners of a state in a belt of Bloch sphere as described by Hu *et al.* [13], where $g(\theta)$ is given by a rectangle distribution, i.e., states are assumed to be uniformly distributed in a region forming a belt between two latitudes on the Bloch sphere.

V. OPTIMALITY PROOF FOR THE PHASE-INDEPENDENT CLONING TRANSFORMATION

Cloning transformations can be described by a completely positive trace-preserving map (CPTP) χ, which can be written with the use of the inverse Jamiołkowski isomorphism [35] as follows:

$$\rho_{\rm out} = {\rm Tr}_{\rm in}\left(\chi\rho_{\rm in}^T \otimes \mathbb{1}^{\otimes 2}\right). \tag{21}$$

The average single-copy fidelity (the figure of merit when maximized) can be expressed as

$$F = {\rm Tr}(\chi R), \tag{22}$$

and

$$R = \frac{1}{2}\int_0^{2\pi}\int_{-1}^{1} \rho_{\rm in}^T \otimes (\rho_{\rm in}\otimes\mathbb{1} + \mathbb{1}\otimes\rho_{\rm in})\, g(\theta)\, d\cos\theta\, d\phi. \tag{23}$$

TABLE I. Summary of optimal phase-independent symmetric $1 \to 2$ cloning machines for qubits.

Optimal cloning machine	Distribution $g(\theta)$	Single-copy fidelity F
Universal cloner (UC)	$\frac{1}{4\pi}$	$\frac{5}{6}$
Phase-covariant cloner (PCC)[a]	$\frac{\delta(\vartheta-\theta)}{2\pi\sin\vartheta}$	$\frac{1}{8}[5+\sqrt{2}+2\cos(\theta+\kappa)-(\sqrt{2}-1)\cos(2\theta)]$
Mirror phase-covariant cloner (MPCC)[b]	$\frac{\delta(\vartheta-\theta)+\delta(\vartheta+\pi-\theta)}{4\pi\sin\vartheta}$	$\frac{1+\Lambda^2}{2}-\frac{1}{2}\sin^2\theta(\Lambda^2-\Lambda\bar{\Lambda}\sqrt{2})$
Cloner of Bloch-sphere belt[c,d]	$\frac{u(\theta+\vartheta_1)-u(\theta-\vartheta_2)}{2\pi(\cos\vartheta_1-\cos\vartheta_2)}$	Eq. (10) with Eq. (15)[e] from Ref. [13]
Cloner of von Mises–Fisher distribution[c]	$\frac{\kappa\exp(\kappa\cos\theta)}{4\pi\sinh\kappa}$	Eq. (10) with Eq. (17)
Cloner of Brosseau distribution[c]	$\frac{(1-P^2)(1-\mu\cos\theta)}{2[(1-\mu\cos\theta)^2-(1-\cos^2\theta)(P^2-\mu^2)]^{\frac{3}{2}}}$	Eq. (10) with Eq. (19)

[a] $\kappa = 0$ for $0 \leqslant \vartheta < \frac{\pi}{2}$ and $\kappa = \pi$ for $\frac{\pi}{2} \leqslant \vartheta \leqslant \pi$;
[b] $\Lambda = \sqrt{1-\bar{\Lambda}^2}$, Λ depends on ϑ as given in Ref. [12].
[c] The explicit expression for F is lengthy and therefore is not shown here, but it can be directly derived from the quoted equations.
[d] u is Heviside's step function.
[e] In Ref. [13], $\alpha \equiv \alpha_+$ and $\beta \equiv \alpha_-$.

Since the cloning transformation for the set of cloned qubits needs to be symmetric with respect to an arbitrary rotation U about the state $|\psi\rangle$ and to swapping $U_{\rm swap}$ of the clones, the following commutation relations should hold:

$$\begin{aligned} [\chi, U^* \otimes U^{\otimes 2}] &= 0, \\ [\chi, \mathbb{1} \otimes \mathrm{U_{SWAP}}] &= 0. \end{aligned} \tag{24}$$

The commutation relations and trace-preserving condition restrict the χ matrix to the following form (in $\{|\psi\rangle,|\bar{\psi}\rangle\}^{\otimes 3}$ basis):

$$\chi = \begin{bmatrix} \eta_1 & 0 & 0 & 0 & 0 & \zeta_1 & \zeta_1 & 0 \\ 0 & \eta_2 & \eta_3 & 0 & 0 & 0 & 0 & \zeta_2 \\ 0 & \eta_3 & \eta_2 & 0 & 0 & 0 & 0 & \zeta_2 \\ 0 & 0 & 0 & \eta_4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \xi_4 & 0 & 0 & 0 \\ \zeta_1 & 0 & 0 & 0 & 0 & \xi_2 & \xi_3 & 0 \\ \zeta_1 & 0 & 0 & 0 & 0 & \xi_3 & \xi_2 & 0 \\ 0 & \zeta_2 & \zeta_2 & 0 & 0 & 0 & 0 & \xi_1 \end{bmatrix}, \tag{25}$$

where $\xi_4 = 1 - 2\xi_2 - \xi_1$ and $\eta_4 = 1 - 2\eta_2 - \eta_1$. It is more convenient to use another basis to express χ and R operators, i.e., $\{|\psi,\psi,\psi\rangle, |\bar{\psi}\rangle|\Psi_+\rangle, |\bar{\psi},\bar{\psi},\bar{\psi}\rangle, |\psi\rangle|\Psi_+\rangle, |\bar{\psi}\rangle|\Psi_-\rangle, |\psi\rangle|\Psi_-\rangle, |\psi,\bar{\psi},\bar{\psi}\rangle, |\bar{\psi},\psi,\psi\rangle\}$. In this new basis, the operators have the following block form:

$$\chi = \bigoplus_{i=1}^{6} \chi_i, \quad R = \bigoplus_{i=1}^{6} R_i, \tag{26}$$

where $\chi_{1(2)}$ and $R_{1(2)}$ are 2×2 matrices. The χ_i and R_i elements for $i = 3,\ldots,6$ are not negative numbers limited by trace of χ (Tr $\chi = 2$). The average single-copy fidelity can be expressed using Einstein's summation convention as

$$F = \mathrm{Tr}\,(R_i \chi_i). \tag{27}$$

The fidelity is a convex superposition, and the matrix elements χ_i (for $i = 3,4,5,$ and 6) are numbers $\in [0,2]$. Therefore, it can be proved that for any distribution $g(\theta)$ for $i \in \{5,6\}$ we have $\mathrm{Tr}\,(R_i\chi_i) \leqslant 1/2$. Moreover, for $i \in \{3,4\}$ we have $\mathrm{Tr}\,(R_i\chi_i) \leqslant F_{\rm PCC}$, where $F_{\rm PCC}$ is the single-copy fidelity of the PCC averaged over inputs characterized by $g(\theta)$. The PCC is derived only from χ_1 and χ_2.

Hence, to maximize the fidelity, we have to put $\chi_3 = \chi_4 = \chi_5 = \chi_6 = 0$. This implies that $\eta_2 = \eta_3$, $\xi_2 = \xi_3$ and $1 - \eta_1 = 2\eta_2$, $1 - \xi_1 = 2\xi_2$. Now, the CPTP map depends only on four parameters and can be described as a direct sum (denoted by $\oplus$) of two matrices:

$$\chi = \begin{bmatrix} \eta_1 & \sqrt{2}\zeta_1 \\ \sqrt{2}\zeta_1 & 1-\xi_1 \end{bmatrix} \oplus \begin{bmatrix} \xi_1 & \sqrt{2}\zeta_2 \\ \sqrt{2}\zeta_2 & 1-\eta_1 \end{bmatrix}, \tag{28}$$

where the first matrix acts in a subspace spanned by $\{|\psi,\psi,\psi\rangle, |\bar{\psi},\Psi_+\rangle\}$ and the second by $\{|\bar{\psi},\bar{\psi},\bar{\psi}\rangle, |\psi,\Psi_+\rangle\}$. The map can be parametrized without the loss of generality in the following way:

$$\chi = \begin{bmatrix} \cos^2\alpha_+ & \sqrt{2}\zeta_1 \\ \sqrt{2}\zeta_1 & \sin^2\alpha_- \end{bmatrix} \oplus \begin{bmatrix} \cos^2\alpha_- & \sqrt{2}\zeta_2 \\ \sqrt{2}\zeta_2 & \sin^2\alpha_+ \end{bmatrix}, \tag{29}$$

However, for the extremal CPTP maps [31], we have that $\chi^2_{1(2)} \propto \chi_{1(2)}$. From this condition, we find that $\sqrt{2}\zeta_1 = \cos\alpha_+ \sin\alpha_-$ and $\sqrt{2}\zeta_2 = \cos\alpha_- \sin\alpha_+$. Finally, any CPTP map that maximizes the average single-copy fidelity for an arbitrary axisymmetric distribution $g(\theta)$ can be written in the basis $\{|\psi\rangle,|\bar{\psi}\rangle\}^{\otimes 3}$ as

$$\chi = \begin{bmatrix} c_+^2 & 0 & 0 & 0 & 0 & \frac{s_-c_+}{\sqrt{2}} & \frac{s_-c_+}{\sqrt{2}} & 0 \\ 0 & \frac{s_+^2}{2} & \frac{s_+^2}{2} & 0 & 0 & 0 & 0 & \frac{c_-s_+}{\sqrt{2}} \\ 0 & \frac{s_+^2}{2} & \frac{s_+^2}{2} & 0 & 0 & 0 & 0 & \frac{c_-s_+}{\sqrt{2}} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{s_-c_+}{\sqrt{2}} & 0 & 0 & 0 & 0 & \frac{s_-^2}{2} & \frac{s_-^2}{2} & 0 \\ \frac{s_-c_+}{\sqrt{2}} & 0 & 0 & 0 & 0 & \frac{s_+^2}{2} & \frac{s_-^2}{2} & 0 \\ 0 & \frac{c_-s_+}{\sqrt{2}} & \frac{c_-s_+}{\sqrt{2}} & 0 & 0 & 0 & 0 & c_-^2 \end{bmatrix}, \tag{30}$$

where $c_\pm = \cos\alpha_\pm$ and $s_\pm = \sin\alpha_\pm$. The above map can be decomposed into unitary transformations, given by Eq. (7) (for $\beta_\pm = 0$), by means of the Kraus decomposition [36]. This completes the proof.

VI. QUANTUM CIRCUIT FOR OPTIMAL PHASE-INDEPENDENT CLONING

The analyzed cloning problem can be also expressed in the logical basis. The optimal cloning transformation can be now written as

$$\begin{aligned} |000\rangle &\to \cos\alpha_+|001\rangle + \sin\alpha_+|\psi_+\rangle|0\rangle, \\ |100\rangle &\to \cos\alpha_-|110\rangle + \sin\alpha_-|\psi_+\rangle|1\rangle, \end{aligned} \tag{31}$$

where $|\psi_+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$. The quantum circuit, shown in Fig. 5, performs the following transformation:

$$|\psi_{\rm out}\rangle = U^{(32)}_{\rm CNOT} U^{(21)}_{\rm CNOT} U^{(13)}_{\rm CNOT} U^{(32)}_{\rm CH} U^{(3)}_{R_y} U^{(13)}_{CR_y} |\psi_{\rm in}\rangle, \tag{32}$$

where the superscripts indicate qubits for which the corresponding gate is applied. The basic elements of the circuit are the rotations

$$U_{R_y}(\omega) = \begin{bmatrix} \cos(\omega/2) & -\sin(\omega/2) \\ \sin(\omega/2) & \cos(\omega/2) \end{bmatrix} \tag{33}$$

about the y axis by angle $\omega = 2\alpha_+$ and the controlled rotation $U_{CR_y}(\Phi)$ by angle $\Phi = 2(\alpha_- - \alpha_+)$. In addition, this circuit

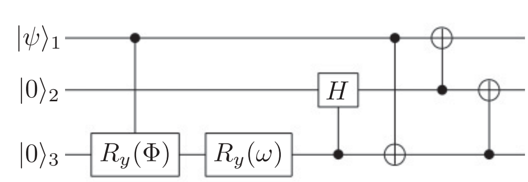

FIG. 5. A quantum circuit which implements the optimal phase-independent cloning transformation of $|\psi(\theta,\phi)\rangle = \cos(\theta/2)|0\rangle + \exp(i\phi)\sin(\theta/2)|1\rangle$ described on the Bloch sphere by arbitrary axisymmetric distribution function $g(\theta)$. From left to right: controlled rotation R_y about the y axis by angle $\Phi = 2(\alpha_- - \alpha_+)$, rotation R_y by angle $\omega = 2\alpha_+$, controlled Hadamard gate, and three CNOT gates.

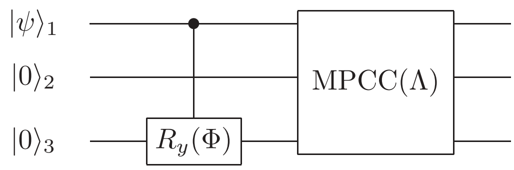

FIG. 6. A quantum circuit, shown in Fig. 5, implementing the optimal phase-independent cloning transformation, is equivalent to the MPCC [12] with $\Lambda = \cos\alpha_+$ together with the controlled rotation R_y by angle $\Phi = 2(\alpha_- - \alpha_+)$.

is composed of the controlled NOT (CNOT) gates, $U_{\rm CNOT}$, and the controlled Hadamard gate, $U_{\rm CH}$, which can be decomposed [12] as $U_{\rm CH}^{(32)} = A^{(2)} U_{\rm CNOT}^{(32)} A^{(2)}$, where

$$A = \frac{1}{\sqrt{4+2\sqrt{2}}} \begin{bmatrix} 1 & 1+\sqrt{2} \\ 1+\sqrt{2} & -1 \end{bmatrix}. \tag{34}$$

The optimal phase-independent cloning can be implemented with the use of a quantum circuit, the MPCC [12] setting for $\Lambda = \cos\alpha_+$ (see Fig. 6). Therefore, with minor modifications (concerning the state preparation of the third qubit), the optimal phase-independent cloning machine can be realized with, e.g., linear optics or quantum dots as described for the MPCC in Refs. [12,26,37].

VII. CONCLUSIONS

We analyzed optimal state-dependent cloning of qubit states, which are described by *a priori* known arbitrary phase-independent (axisymmetric) distribution g on the Bloch sphere. This optimal cloning reduces in special cases to the universal cloning of Bužek and Hillery [2], the phase-covariant cloning of Bruß *et al.* [5] and its generalization by Fiurášek [8,9], the mirror phase covariant cloning (MPCC) of Bartkiewicz *et al.* [12], or cloning of an uniform belt of the Bloch sphere of Hu *et al.* [13].

As an example of the state-dependent cloning, we studied the cloning transformations of qubits described on the Bloch sphere by the von Mises–Fisher and Brosseau distributions, where the first is an analog of normal distribution on a sphere [30] and the latter describes statistics of the Stokes parameters [33,34]. Whereas the first example is more abstract and describes Gaussian-like dispersion, the second example can be used directly to estimate the upper bound for the capacity of a depolarizing channel [28] for photons. Our results can be also applied in security analysis of various quantum-communication protocols, including quantum teleportation [38] and quantum key distribution [19].

Recently, it was shown that phase-independent cloning can be parametrized by four parameters [25]. Here, we proved that only two parameters are sufficient to describe the optimal phase-independent cloning.

Moreover, we showed that the phase-independent cloning is a simple generalization of the MPCC and, thus, can be implemented analogously to the MPCC using photon-polarization qubits [26] and quantum-dot spins [12].

ACKNOWLEDGMENTS

We thank Jaromir Fiurášek and Xiaoguang Wang for discussions. A.M. acknowledges support from the Polish Ministry of Science and Higher Education under Grant No. 2619/B/H03/2010/38.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982); D. Dieks, Phys. Lett. A **92**, 271 (1982).
[2] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[3] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[4] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[5] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[6] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[7] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
[8] J. Fiurášek, Phys. Rev. A **64**, 062310 (2001).
[9] J. Fiurášek, Phys. Rev. A **67**, 052314 (2003).
[10] R. Demkowicz-Dobrzański, M. Kuś, and K. Wódkiewicz, Phys. Rev. A **69**, 012301 (2004).
[11] H. Fan, H. Imai, K. Matsumoto, and X.-B. Wang, Phys. Rev. A **67**, 022317 (2003).
[12] K. Bartkiewicz, A. Miranowicz, and Ş. K. Özdemir, Phys. Rev. A **80**, 032306 (2009).
[13] J. Z. Hu, Z. W. Yu, and X. B. Wang, Eur. Phys. J. D **51**, 381 (2009).
[14] F. Buscemi, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **71**, 042327 (2005).
[15] M. F. Sacchi, Phys. Rev. A **75**, 042328 (2007).
[16] A. Kay, D. Kaszlikowski, and R. Ramanathan, Phys. Rev. Lett. **103**, 050501 (2009).
[17] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, Rev. Mod. Phys. **77**, 1225 (2005).
[18] N. J. Cerf and J. Fiurášek, in *Progress in Optics*, edited by E. Wolf (Elsevier, Amsterdam, 2006), Vol. 49, p. 455.
[19] L. Gyongyosi and S. Imre, WSEAS Trans. Commun. **9**, 165 (2010).
[20] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.
[21] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[22] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[23] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[24] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[25] X. Wu and F. Wu, e-print arXiv:1004.5210v1.
[26] K. Bartkiewicz *et al.* (unpublished).
[27] A. Zhu, K. H. Yeon, and S. C. Yu, J. Phys. B **42**, 235501 (2009).
[28] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[29] W. Kaplan, *Advanced Calculus* (Addison-Wesley, Reading, MA, 1992).
[30] R. A. Fisher, Proc. R. Soc. A **217**, 295 (1953).

[31] G. Chiribella, G. M. D'Ariano, P. Perinotti, and N. J. Cerf, Phys. Rev. A **72**, 042336 (2005).
[32] L. Henyey and J. Greenstein, Astrophys. J. **93**, 70 (1941).
[33] R. Barakat, J. Opt. Soc. Am. A **4**, 1256 (1987).
[34] C. Brosseau, Appl. Opt. **34**, 4788 (1995).
[35] A. Jamiołkowski, Rep. Math. Phys. **3**, 275 (1972).
[36] K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin 1983).
[37] A. Miranowicz, Ş. K. Özdemir, Yu-xi Liu, M. Koashi, N. Imoto, and Y. Hirayama, Phys. Rev. A **65**, 062321 (2002).
[38] Ş. K. Özdemir, K. Bartkiewicz, Y. X. Liu, and A. Miranowicz, Phys. Rev. A **76**, 042325 (2007).