Optimal cloning of pure states

R. F. Werner*
Institut für Mathematische Physik, Technische Universität Braunschweig, Mendelssohnstraße 3, 38106 Braunschweig, Germany
(Received 17 April 1998)

We construct a unique optimal quantum device for turning a finite number of d-level quantum systems in the same unknown pure state σ into M systems of the same kind, in an approximation of the M-fold tensor product of the state σ. [S1050-2947(98)10109-9]

PACS number(s): 03.67.−a, 02.20.Hj

I. INTRODUCTION

One of the fundamental features distinguishing quantum theory from classical theories is epitomized by the ''no cloning theorem'' [1]. The ''quantum copiers'' forbidden by this theorem, in much the same way as perpetual motion machines are forbidden by the second law of thermodynamics, are defined as follows: A copier takes one quantum system as input and produces as output two systems of the same kind. If one now runs experiments in which each input is prepared according to the same density matrix, either one of the outputs is discarded, and some measurement is then performed on the remaining output, one should get the same statistical results as measured directly on the inputs, for arbitrary initial preparations and final measurements.

The impossibility of cloning machines is intimately connected to other impossible tasks of quantum theory, notably ''joint measurement'' and ''teleportation.'' It is well known that there are some pairs of quantum observables (such as different spin components) that cannot be measured jointly on the same device. This statement implies the no-cloning theorem, since a quantum copier could be operated as a universal joint measuring device: One simply applies the two measuring devices in question to the two outputs of the copier. Hence a copier is a more powerful machine than a joint measuring device. On the other hand, there is a hypothetical machine even stronger than the copier: the ''teleporter,'' which is hence also forbidden by the no-cloning theorem. By definition, ''teleportation,'' or ''classical teleportation'' to avoid confusion with the fundamental process of entanglement enhanced teleportation [2], is the transmission of quantum states (or ''quantum information'') on classical channels. A teleporting device would consist of a measuring apparatus, which produces some classical output (a measuring result) from a quantum input, and a reconstruction apparatus, which prepares quantum systems, taking the results of the previous measurements into account. The criterion for successful teleportation is again the impossibility of distinguishing the outputs of the overall device from the inputs by statistical experiments. To make a copier from a teleporter would be easy: One simply has to make copies of the intermediate classical measuring results (which is a trivial operation for classical data) and to run the reconstruction apparatus on each of these copies. Hence classical teleportation is also impossible.

However, the impossibility of all these devices cannot be the end of the story. For example, while the no-teleportation theorem declares it impossible to determine a quantum state by the classical data obtained in a single measurement, it is clearly possible to determine quantum states by a run of statistical experiments. In fact, according to the statistical interpretation, a quantum state is nothing but a mathematical encoding of all data that can be collected in this way. Therefore, it must be possible to construct devices that take several identically prepared quantum systems as an input, make a measurement, and thereby determine the density matrix describing the preparation to any desired degree of accuracy. This is the problem of quantum state estimation, which has been studied by many authors [3–6]. Of course, we can use this classical information to prepare many new systems (''clones'') in a state that is a close approximation of the input state. Clearly, the quality of the clones will depend on the number of initially available input systems. On the other hand, there will be no limit to the number of clones obtainable in this way because the classical measuring result can be copied and used arbitrarily often.

More recently, there has been an interesting twist to this problem coming from the observation that if only a given number of clones is needed, the procedure via a classical intermediate stage is too wasteful [7]. Indeed, it has been shown [8] that there is, in general, a trade-off between the number of clones and their quality. Clearly, the optimal cloning machine giving a fixed number of copies from a fixed number of identically prepared systems cannot operate via an intermediate classical stage: It has to stay entirely in the quantum world. This paper is a contribution to the theory of such optimal cloning machines.

There are several variations of the optimal cloning problem, which are perhaps best described in the form of a game. Fixed parameters in this game are the Hilbert space $\mathcal{H}$ describing the type of systems making up the inputs as well as the outputs to the cloning device. Its (always finite) dimension will be denoted by $d=\dim \mathcal{H}$. Most work so far has been done on the ''quantum bit (qubit) case'' $d=2$. Also fixed will be the number N of input systems and the number M of output systems. The game is played by two physicists called Alice and Clare. (If the paradigmatic eavesdropper is Eve, why should the paradigmatic cloner not be Clare?). Alice's first step is to choose a preparation for quantum systems with Hilbert space $\mathcal{H}$, as described by a density matrix

*Electronic address: R.Werner@tu-bs.de

σ, say. She then proceeds to run her preparing procedure N times, thus producing a composite system in the Hilbert space $\mathcal{H}\otimes\cdots\otimes\mathcal{H}=\mathcal{H}^{\otimes N}$ (a tensor product of N copies) in the state $\sigma^{\otimes N}$, and sends the prepared particles to Clare. Clare's move is to run a cloning device T of her choice, making $M>N$ systems out of the given N systems. (The mathematical objects qualifying as ''devices'' in this context will be defined in Sec. II.) The next step is to compare Clare's M output systems with the state $\sigma^{\otimes M}$, which Alice supplies by running her original preparation M times. Clare scores in this game whenever her output is sufficiently similar to $\sigma^{\otimes M}$. There are different ''figures of merit'' on which Clare's scores might be based, resulting in different versions of the cloning game and possibly in different ''optimal'' cloning devices T. Some of the simplest are based on a simple extension of the game: We allow Alice a further move, challenging the quality of Clare's clones, by choosing some observable. The two then each measure the expectation value of this observable on their respective M-particle states and the overall score is based on the difference of these expectation values.

Apart from the fine points of the comparison, two basic choices have to be made in the rules of this game, leading to four different versions of the game. The first choice concerns constraints on the initial preparation σ done by Alice. For the discussion of eavesdropping on quantum cryptography channels it is often of interest to allow only a small number of states (e.g., two) [9]. Orthogonal states can obviously be cloned perfectly. However, we are interested in so-called *universal* cloning machines [10], which work on generic (and unknown) inputs. Still there is a choice to be made, namely, whether or not Alice is required to prepare a *pure state* $\sigma=|\varphi\rangle\langle\varphi|$ given by a wave vector φ. Here the present paper follows most of the current literature by imposing purity. The reason is mostly that the full mixed-state problem seems to be a lot more involved, even in the classical case, and it seems wise to gain a full understanding of the simpler case first.

The second choice to be made in the rules is whether Alice really challenges Clare's full M-particle output state or just one clone at a time. That is, we could constrain her to challenge Clare's result by selecting only one of the M clones and demanding a one-particle observable of her choice to be measured on it. This constraint on Alice is in keeping with the definition of the quantum copier, which also imposes only conditions on one output at a time. This ''*one-particle-test*'' version of the cloning problem has been considered in the qubit case in several recent papers [7,6,11]. It turns out, however, that it is the more difficult problem for $d>2$. Therefore, in this paper we will give a full analysis of the ''pure-state–many-particle-test'' cloning problem for arbitrary d.

The pure-state–one-particle-test version is settled in the $d=2$ case [7], where the representation theory of SU_2 makes a full analysis relatively simple. The optimal cloning device found by Gisin and Massar is the same as the one found in the present paper for the many-particle test version. The case of general d is solved in [21]. The optimal cloning devices fit perfectly into the framework for the *classical limit* (in this case, of SU_d-spin systems), set up in [12–14]. In this way, a precise meaning can be given to the intuition that cloning very (infinitely) many copies is equivalent to the cloning procedure via classical measurement and subsequent preparation. This connection, which requires the explanation of more formalism than this paper can take, will be explored in a later paper.

II. STATEMENT OF THE PROBLEM

In order to state the optimal cloning problem precisely we must first state what the admissible ''quantum devices'' are among which we are looking for an optimal one. There are two ways of approaching this problem, which are fortunately equivalent: In either case, each device is characterized by its action on quantum states. Thus if the input systems are described in a Hilbert space $\mathcal{H}$ and consequently the input states are density matrices on $\mathcal{H}$ and the output systems are described in a Hilbert space $\mathcal{K}$, a quantum device is given by a map T taking density matrices over $\mathcal{H}$ into density matrices over $\mathcal{K}$. The first approach to characterizing the admissible maps T is the axiomatic one: A minimal requirement for T to be consistent with the statistical interpretation of quantum theory is that T must respect convex combinations (incoherent mixtures) of states. This allows the extension of T to a *linear* operator from the space of trace class operators over $\mathcal{H}$ into the trace class operators over $\mathcal{K}$. This linear operator has to take positive elements into positive elements, which is usually expressed by calling T a *positive* (super)operator. If this condition remains valid if T is applied only to a part of a larger system, T is called *completely positive*. Since T takes density matrices into density matrices, it also has to respect normalization (i.e., the trace). Therefore, according to the axiomatic definition, an admissible machine must be given by a completely positive trace preserving linear operator T. The second definition of ''admissible devices'' is constructive. It allows only operations that can be done by first coupling the given system to an auxiliary one (often called the ''ancilla''), then making the two interact, as described by a unitary transformation, and finally restricting to a suitable subsystem of the combined system by taking a partial trace over the ancilla and perhaps further subsystems. Each of these steps is a completely positive trace preserving operation, so clearly every quantum device admissible in the constructive approach is also admissible by the axiomatic approach. However, the converse is also true (by virtue of the Stinespring dilation theorem [15]): Every linear completely positive trace preserving map can be constructed in the way described.

Let us now turn to the description of figures of merit for quantum cloning devices, i.e., on quantitative ways of expressing the ''closeness'' between the output $T(\sigma^{\otimes N})$ of Clare's cloning device and the state $\sigma^{\otimes M}$, which the nonexistent ideal cloner would achieve. This question has to be treated rather carefully for the mixed state versions of the cloning game. Possible candidates here are the trace norm difference $\|T(\sigma^{\otimes N})-\sigma^{\otimes M}\|_1$ or perhaps another p norm [16] such as the Hilbert-Schmidt norm or the relative entropy $S(T(\sigma^{\otimes N}),\sigma^{\otimes M})$ [17]. In principle, the optimal cloner might depend on the figure of (de)merit chosen. However, in the pure state case they all lead to the same optimum. In this paper we will use an even simpler figure of merit, which makes sense only in the pure case, namely, the *fidelity*

$\mathrm{tr}[\sigma^{\otimes M}T(\sigma^{\otimes N})]$, which would be 1 for the nonexistent ideal cloner. Good cloning means to bring this quantity as close to 1 as possible for all input states σ. The worst result

$$\mathcal{F}(T)=\inf_{\sigma,\mathrm{pure}}\mathrm{tr}[\sigma^{\otimes M}T(\sigma^{\otimes N})] \tag{1}$$

is taken as the figure of merit. So Clare's and our problem is to maximize $\mathcal{F}(T)$ by a judicious choice of T, given $\mathcal{H}$, N, and M. The optimum will be denoted by $\hat{\mathcal{F}}=\sup_T\mathcal{F}(T)$ and depends on the three integers $d=\dim\mathcal{H}$, N, and M.

We note in passing that so far we have only considered the problem of minimizing the worst case losses for Clare in a game of the type described. It would be interesting to take the game theoretic description more seriously and to ask for the equilibrium points of the variants of this game in the sense of von Neumann's theory of two-person games [18].

III. DESCRIPTION OF THE OPTIMAL CLONING MACHINES

In this section we will define the cloning maps, which will be shown to be the unique optimal ones in Sec. IV. Since we are considering only pure input states $\sigma^{\otimes N}$, it suffices to consider the action of T on such states and their linear combinations. These will be operators on the span of the vectors of the form $\varphi\otimes\cdots\otimes\varphi=\varphi^{\otimes N}\in\mathcal{H}^{\otimes N}$. Our first task is to collect some of the basic properties of this space.

The span of the tensor powers $\varphi^{\otimes N}$ can be described very easily: It is precisely the space of vectors that are invariant under all permutations, or the ''Bose subspace'' of $\mathcal{H}^{\otimes N}$ in physical terminology. We will denote it by $\mathcal{H}_+^{\otimes N}$. A convenient basis in this space is the ''occupation number basis'' canonically associated with some basis in the one-particle space $\mathcal{H}$. It is labeled by tuples $(n_1,\ldots,n_d)$ with $\Sigma_\kappa n_\kappa=N$. A generating function for this basis is given by the tensor power vectors $\varphi^{\otimes N}$, the variables in the generating function being the components $\varphi_1,\ldots,\varphi_d$ of φ in the given basis of $\mathcal{H}$. Explicitly,

$$\varphi^{\otimes N}=\sqrt{N!}\sum_{n_1,\ldots,n_d}\prod_{\kappa=1}^{d}\frac{\varphi_\kappa^{n_\kappa}}{\sqrt{n_\kappa!}}|n_1,\ldots,n_d\rangle. \tag{2}$$

It is easily checked, using this basis that the dimension of $\mathcal{H}^{\otimes N}$ is

$$d[N]=(-1)^N\binom{-d}{N}=\binom{d+N-1}{N}, \tag{3}$$

where $d=\dim\mathcal{H}$. We will denote by s_N the orthogonal projection of $\mathcal{H}^{\otimes N}$ onto $\mathcal{H}_+^{\otimes N}$. A crucial feature of the symmetric subspace is that the unitary operators $U^{\otimes N}$ leave it invariant and act on it irreducibly. That is to say, any operator A supported by $\mathcal{H}_+^{\otimes N}$ ($A=As_N=s_NA$), which commutes with all $U^{\otimes N}$, must be a multiple of s_N, i.e., of the identity operator on $\mathcal{H}_+^{\otimes N}$.

The optimal cloning map has to take density operators on $\mathcal{H}_+^{\otimes N}$ to operators on $\mathcal{H}^{\otimes M}$. An easy way to achieve such a transformation is to tensor the given operator ρ with the identity operators belonging to tensor factors $N+1$ through M, i.e., to take $\rho\mapsto\rho\otimes\mathbb{1}^{\otimes(M-N)}$. This breaks the symmetry between the clones, making N perfect copies and $N-M$ states, which are the worst possible ''copies.'' Moreover, it does not map to states on the Bose sector $\mathcal{H}_+^{\otimes M}$, which would certainly be desirable, as the target states $\sigma^{\otimes M}$ are supported by that subspace. An easy way to remedy both defects is to compress the operator to the symmetric subspace with the projection s_M. With the appropriate normalization this is our definition of the cloning map, later shown to be optimal:

$$\hat{T}(\rho)=\frac{d[N]}{d[M]}\,s_M(\rho\otimes\mathbb{1}^{\otimes(M-N)})s_M. \tag{4}$$

Complete positivity is obvious from the form of $\hat{T}$. So in order to verify that this is a legitimate cloning map, we only have to check that the normalization factor is chosen correctly to make $\hat{T}$ trace preserving. To begin with, tr $\hat{T}(\rho)$ is a linear functional of ρ and can hence be written as $\mathrm{tr}(\rho X)$ for a suitable positive operator X on $\mathcal{H}_+^{\otimes N}$. From the *covariance* of $\hat{T}$, i.e., the property

$$T(U^{\otimes N}\rho U^{*\otimes N})=U^{\otimes M}T(\rho)U^{*\otimes M}, \tag{5}$$

one concludes that X commutes with $U^{\otimes N}$ and, by irreducibility, X must be a multiple of the identity. It remains to be shown that this multiple is 1 or, equivalently, that the trace of *some* density matrix is preserved by $\hat{T}$. To this end we consider the maximally mixed density matrix $\tau_N=d[N]^{-1}s_N$ on $\mathcal{H}_+^{\otimes N}$, which is also characterized as the unique density matrix on $\mathcal{H}_+^{\otimes N}$ invariant under sitewise rotations $\rho\mapsto U^{\otimes N}\rho U^{*\otimes N}$. Then $\hat{T}(\tau_N)=d[M]^{-1}s_M(s_N\otimes\mathbb{1}^{M-N})s_M=d[M]^{-1}s_M=\tau_M$. Hence $\hat{T}$ as defined in Eq. (4) is trace preserving.

The value of $\mathcal{F}(\hat{T})$ is determined by observing that, for a pure state σ on $\mathcal{H}$, $\sigma^{\otimes M}$ is a one-dimensional projection, which is smaller than both s_M and $(\sigma^{\otimes N}\otimes\mathbb{1}^{\otimes(M-N)})$. Hence

$$\begin{aligned}\mathcal{F}(\hat{T})&=\frac{d[N]}{d[M]}\,\mathrm{tr}[\sigma^{\otimes M}s_M(\sigma^{\otimes N}\otimes\mathbb{1}^{\otimes(M-N)})s_M]\\&=\frac{d[N]}{d[M]}\,\mathrm{tr}(\sigma^{\otimes M})=\frac{d[N]}{d[M]}.\end{aligned} \tag{6}$$

We conclude this section by computing the performance of $\hat{T}$ with respect to the one-particle test version of the cloning problem. Some of our considerations will be valid for any cloning map T (not necessarily $T=\hat{T}$), which maps density matrices on $\mathcal{H}_+^{\otimes N}$ into density matrices on $\mathcal{H}_+^{\otimes M}$ and satisfies the covariance condition (5). For any density matrix ρ on $\mathcal{H}^{\otimes N}$, we denote by $R(\rho)$ its one-site restriction defined by $\mathrm{tr}[R(\rho)A]=\mathrm{tr}[\rho(A\otimes\mathbb{1}^{\otimes(N-1)})]$. Consider the one-site restriction $R(T(\sigma^{\otimes N}))$. By covariance of T, this must be a density matrix on the one-site Hilbert space $\mathcal{H}$, commuting with all unitaries U, which commute with σ. Hence we can write it as

$$R(T(\sigma^{\otimes N}))=\gamma(T)\sigma+[1-\gamma(T)]\tau_1, \tag{7}$$

where $\tau_1=d^{-1}\mathbb{1}$ is the totally mixed density matrix on $\mathcal{H}$. By covariance of T, the number $\gamma(T)$ does not depend on σ and

is called the *Black Cow factor*[1] of T. Surprisingly, it is useful also for the discussion of ''cloning in stages'' from N to M to R systems, even though in the second stage the cloner from M to R systems no longer finds a product density matrix $\sigma^{\otimes M}$. In fact, on the right-hand side of Eq. (7) we can write $R(\sigma^{\otimes N})$ for σ and it is clear that Eq. (7) becomes

$$R(T(\rho))=\gamma(T)R(\rho)+[1-\gamma(T)]\mathrm{tr}(\rho)\tau_1 \tag{8}$$

for all ρ in the linear span of the operators $\sigma^{\otimes N}$. However, these are *all* density matrices on $\mathcal{H}_+^{\otimes N}$: This can be seen by inserting the expansion (2) into $\sigma^{\otimes N}=|\varphi^{\otimes N}\rangle\langle\varphi^{\otimes N}|$ and observing that from the resulting power series in φ_κ and $\overline{\varphi_\kappa}$ the coefficients $|n\rangle\langle m|$ can be extracted. Hence Eq. (8) holds for all cloning maps T satisfying the assumptions stated at the beginning of this paragraph.

As a corollary we obtain the equation $\gamma(T_{RM}T_{MN})=\gamma(T_{RM})\gamma(T_{MN})$ for cloning in stages. Since the family of optimal cloners defined by Eq. (4) obviously satisfies the concatenation property $\hat{T}_{RM}\hat{T}_{MN}=\hat{T}_{RN}$, we find that the Black Cow factor for these must be of the form $\gamma(\hat{T}_{MN})=\gamma_N/\gamma_M$.

To compute $\gamma(\hat{T}_{MN})$ for Eq. (4), we use the normalization property of $\hat{T}$ in the form $\mathrm{tr}(s_M\sigma^{\otimes N}\otimes\mathbb{1}^{\otimes(M-N)})=d[M]/d[N]$ for any pure σ. Then, on the one hand, we find that

$$\mathrm{tr}[\sigma R\hat{T}(\sigma^{\otimes N})]=\gamma(\hat{T})+[1-\gamma(\hat{T})]/d,$$

and, on the other hand,

$$\begin{aligned}
&\mathrm{tr}[\sigma R\hat{T}(\sigma^{\otimes N})]\\
&\quad=\mathrm{tr}[(\sigma\otimes\mathbb{1}^{\otimes(M-1)})\hat{T}(\sigma^{\otimes N})]=\frac{1}{M}\sum_k\ \mathrm{tr}[\sigma^{(k)}\hat{T}(\sigma^{\otimes N})]\\
&\quad=\frac{d[N]}{Md[M]}\sum_k\ \mathrm{tr}[\sigma^{(k)}s_M(\sigma^{\otimes N}\otimes\mathbb{1}^{\otimes(M-N)})s_M]\\
&\quad=\frac{d[N]}{Md[M]}\sum_k\ \mathrm{tr}[\sigma^{(k)}(\sigma^{\otimes N}\otimes\mathbb{1}^{\otimes(M-N)})s_M]\\
&\quad=\frac{d[N]}{Md[M]}\left\{N\frac{d[M]}{d[N]}+(M-N)\frac{d[M]}{d[N+1]}\right\}\\
&\quad=\frac{N}{M}+\frac{M-N}{M}\frac{N+1}{d+N},
\end{aligned}$$

where in the second line we used the abbreviation $\sigma^{(k)}$ for the tensor product of M operators, all of which are $\mathbb{1}$, except the kth, which is σ. At the fourth equality we used that the sum $\Sigma_k\sigma^{(k)}$ commutes with permutations and hence with s_M. Solving for $\gamma(\hat{T})$, we find the Black Cow factor of Eq. (4) to be

$$\gamma(\hat{T})=\frac{N}{d+N}\frac{d+M}{M}. \tag{9}$$

This is a quotient, as expected. Specializing to $d=2$, we find this result also in agreement with the value found in [19] by combining the Black Cow concatenation argument with the previously determined optimal value for state determinations. Again this is to be expected because the optimal cloner found in the one-particle-test version of the problem (for $d=2$) agrees with Eq. (4). Moreover, this result agrees with the special case $N=1$, $M=2$, with arbitrary d attained by an example in [20], but not proved to be optimal. The optimal solutions to the one-particle-test and many-particle-test versions of the cloning problem coincide also for $d>2$ and general $M>N$ [21].

IV. PROOF OF OPTIMALITY

In this section we will prove the optimality of the cloning map $\hat{T}$, defined in Eq. (4), with respect to the figure of merit $\mathcal{F}$ from Eq. (1). Let

$$\hat{\mathcal{F}}=\sup_T\mathcal{F}(T) \tag{10}$$

be the best bound for $\mathcal{F}(T)$. Since $\mathcal{F}$ is an infimum of continuous functions, it is an upper semicontinuous function, and since the set of admissible T is compact (bounded and closed in a finite dimensional vector space), the supremum (10) is attained, i.e., optimal cloners with $\mathcal{F}(T)=\hat{\mathcal{F}}$ do exist.

For a pure state σ, rotated by unitary U on $\mathcal{H}$, we will write $\sigma_U\equiv U\sigma U^*$. The average of any cloning map with respect to sitewise rotations will be denoted by

$$\overline{T}(\rho)=\int dU\ U^{*\otimes M}T(U^{\otimes N}\rho U^{*\otimes N})U^{\otimes M}, \tag{11}$$

where dU denotes the integration with respect to the normalized Haar measure of the unitary group of $\mathcal{H}$. Then $\overline{T}$ is again an admissible cloning map and $T=\overline{T}$ if and only if T satisfies the covariance condition (5).

Theorem. For any cloning map from N to M systems,

$$\mathcal{F}(T)\leqslant d[N]/d[M],$$

with equality if and only if $T=\hat{T}$.

Proof. Let T be an optimal cloning device, i.e., $\mathcal{F}(T)=\hat{\mathcal{F}}$. Then, for every pure σ, we have

$$\begin{aligned}
\mathrm{tr}[\sigma^{\otimes M}\overline{T}(\sigma^{\otimes N})]&=\int dU\ \mathrm{tr}[\sigma_U^{\otimes M}T(\sigma_U^{\otimes N})]\\
&\geqslant\int dU\ \mathcal{F}(T)=\hat{\mathcal{F}}.
\end{aligned}$$

Since the left-hand side is independent of σ, it is also equal to $\mathcal{F}(\overline{T})$, hence $\mathcal{F}(\overline{T})\geqslant\hat{\mathcal{F}}$. By definition of $\hat{\mathcal{F}}$ we also have

[1]The reason for this terminology is that this factor plays a central role in discussions of the cloning problem started by Chiara Machiavello and Artur Ekert and further clarified in collaboration with Dagmar Bruß [19]. I learned about this line of argument from an unpublished work by Nicolas Gisin and Sandu Popescu.

$\hat{\mathcal{F}} \geq \mathcal{F}(\overline{T})$, i.e., $\mathcal{F}(\overline{T}) = \hat{\mathcal{F}}$. Hence the integral over the positive quantities $\hat{\mathcal{F}} - \mathrm{tr}[\sigma_U^{\otimes M} T(\sigma_U^{\otimes N})]$ vanishes, which implies that

$$\mathrm{tr}[\sigma^{\otimes M} T(\sigma^{\otimes N})] = \mathcal{F}(T) = \hat{\mathcal{F}}$$

for all σ.

Next consider the rotation invariant density matrix $\tau_N = d[N]^{-1} s_N$ on the symmetric subspace. Since $\overline{T}$ commutes with rotations, τ_N has to be mapped into a likewise rotation invariant density matrix on $\mathcal{H}^{\otimes M}$. In particular, because the representation $U^{\otimes M}$ restricted to the symmetric subspace is irreducible, we must have

$$\overline{T}\left(\frac{s_N}{d[N]}\right) = \lambda \frac{s_M}{d[M]} + (1-\lambda)\mathrm{Rest},$$

where ''Rest'' stands for a density matrix orthogonal to s_M and $0 \leq \lambda \leq 1$. We now use that $\overline{T}(s_N - \sigma^{\otimes N})$ must be a positive operator. Taking its trace with $\sigma^{\otimes M}$ we thus find that

$$0 \leq \mathrm{tr}[\sigma^{\otimes M} \overline{T}(s_N - \sigma^{\otimes N})] = \lambda \frac{d[N]}{d[M]} - \hat{\mathcal{F}}. \qquad (12)$$

Hence $\hat{\mathcal{F}} \leq \lambda d[N]/d[M] \leq d[N]/d[M]$. Since we have already seen in Eq. (6) that $\mathcal{F}(\hat{T}) = d[N]/d[M]$, we have shown that $\hat{\mathcal{F}}$ is equal to this value and $\hat{T}$ is indeed optimal.

It remains to be shown that $\hat{T}$ is the only cloning map achieving this value. From the last string of inequalities e see that for any optimal cloner we must have $\lambda = 1$. This is equivalent to saying that $\overline{T}(\sigma^{\otimes N})$ is supported by the symmetric subspace for all σ and since $\overline{T}$ is an integral over rotated copies of T, the same conclusion also holds for T. Moreover, for an optimal cloner T, the right-hand side of Eq. (12) has to vanish. This is again an integral with respect to dU over a positive function, which hence has to vanish too:

$$\mathrm{tr}[\sigma^{\otimes M} T(s_N - \sigma^{\otimes N})] = 0. \qquad (13)$$

Since the second term in this expression was already shown to be equal to $\hat{\mathcal{F}}$ for all σ, we conclude that $\mathrm{tr}[\sigma^{\otimes M} T(s_N)] = \hat{\mathcal{F}}$ for all σ. The operators $\sigma^{\otimes M}$ span the space of operators on $\mathcal{H}_+^{\otimes M}$. Hence this equation is equivalent to $T(s_N) = \hat{\mathcal{F}} s_M$.

To further exploit the optimality condition, we introduce the Stinespring dilation [15] of T in the form

$$T(\rho) = \hat{\mathcal{F}} V^* (\rho \otimes \mathbb{1}_{\mathcal{K}}) V,$$

where $V: \mathcal{H}_+^{\otimes M} \to \mathcal{H}_+^{\otimes N} \otimes \mathcal{K}$ for some auxiliary Hilbert space $\mathcal{K}$ and ρ is an arbitrary density matrix on $\mathcal{H}_+^{\otimes N}$. We have included the factor $\hat{\mathcal{F}}$ in this definition, so that for an optimal cloner $V^*V = \mathbb{1}$. The optimality condition (13) written in terms of V becomes

$$\langle \varphi^{\otimes M}, V^*[(s_N - \sigma^{\otimes N}) \otimes \mathbb{1}_{\mathcal{K}}] V \varphi^{\otimes M} \rangle = \| [(s_N - \sigma^{\otimes N}) \otimes \mathbb{1}_{\mathcal{K}}] V \varphi^{\otimes M} \|^2 = 0,$$

where σ is the one-dimensional projection to $\varphi \in \mathcal{H}$. Equivalently, $[(s_N - \sigma^{\otimes N}) \otimes \mathbb{1}_{\mathcal{K}}] V \varphi^{\otimes M} = 0$, which is to say that $V\varphi^{\otimes M}$ must be in the subspace $\varphi^{\otimes N} \otimes \mathcal{K}$ for every φ.

So we can write $V\varphi^{\otimes M} = \varphi^{\otimes N} \otimes \xi(\varphi)$, with $\xi(\varphi) \in \mathcal{K}$ some vector depending in a generally nonlinear way on the unit vector $\varphi \in \mathcal{H}$. From the above observation that V must be an isometry we can calculate the scalar products of all the vectors $\xi(\varphi)$:

$$\begin{aligned} \langle \varphi, \psi \rangle^M &= \langle \varphi^{\otimes M}, \psi^{\otimes M} \rangle = \langle V\varphi^{\otimes M}, V\psi^{\otimes M} \rangle \\ &= \langle \varphi^{\otimes N} \otimes \xi(\varphi), \psi^{\otimes N} \otimes \xi(\psi) \rangle \\ &= \langle \varphi, \psi \rangle^N \langle \xi(\varphi), \xi(\psi) \rangle_{\mathcal{K}}, \end{aligned}$$

i.e.,

$$\langle \xi(\varphi), \xi(\psi) \rangle_{\mathcal{K}} = \langle \varphi, \psi \rangle^{M-N} = \langle \varphi^{\otimes M-N}, \psi^{\otimes M-N} \rangle.$$

This information is sufficient to compute all matrix elements $\langle \psi_1^{\otimes M}, T(|\varphi_1^{\otimes N}\rangle\langle\varphi_1^{\otimes N}|)\psi_2^{\otimes M} \rangle$, i.e., T is uniquely determined and equal to $\hat{T}$. Q.E.D.

ACKNOWLEDGMENTS

This paper is a response to the many discussions about the cloning problem I had with participants of the ISI Workshop on Quantum Computing, Torino, notably N. Gisin, C. Machiavello, S. Massar, A. Ekert, D. Bruß, S. Popescu, and W. van Dam. I would like to thank several of these participants and also P. Zanardi for comments on an earlier version and M. Keyl for a critical reading of the manuscript.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[3] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[4] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[5] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[6] R. Derka, V. Bužek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).
[7] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[8] M. Hillery and V. Bužek, Phys. Rev. A **56**, 1212 (1997).
[9] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997).
[10] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Machiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[11] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[13] R. F. Werner, e-print quant-ph/9504016.
[14] R. F. Werner and M. P. H. Wolff, Phys. Lett. A **202**, 155 (1995).
[15] A. Menkhaus, thesis for the degree of ''Diplom,'' Universität Osnabrück, 1996 (unpublished).
[16] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
[17] M. Reed and B. Simon, *Methods of Modern Mathematical Physics, Vol. II* (Academic, New York, 1975), Appendix on abstract interpolation.
[18] M. Ohya and D. Petz, *Quantum Entropy and its Use* (Springer-Verlag, Heidelberg, 1993).
[19] J. von Neumann, Math. Ann. **100**, 295 (1928).
[20] D. Bruß, A. Ekert, and C. Machiavello, e-print quant-ph/9712019.
[21] V. Bužek and M. Hillery, e-print quant-ph/9801009.
[22] M. Keyl and R. F. Werner, e-print quant-ph/9807010.