Optimal Asymmetric Quantum Cloning

Alastair Kay,[1, 2] Ravishankar Ramanathan,[1] and Dagomir Kaszlikowski[1, 3]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2]*Keble College, Parks Road, University of Oxford, Oxford, OX1 3PG, UK*
[3]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542*
(Dated: August 28, 2012)

While the no-cloning theorem, which forbids the perfect copying of quantum states, is well-known as one of the defining features of quantum mechanics, the question of how well the theory allows a state to be cloned is yet to be completely solved. In this paper, rigorous solutions to the problem of $M \to N$ asymmetric cloning of qudits are obtained in a number of interesting cases. The central result is the solution to the $1 \to N$ universal asymmetric qudit cloning problem for which the exact trade-off in the fidelities of the clones for every N and d is derived. Analogous results are proven for qubits when $M = N - 1$. We also consider state-dependent $1 \to N$ qubit cloning, providing a general parametrization in terms of a Heisenberg star Hamiltonian. In all instances, we determine the feasibility of implementing the cloning economically, i.e., without an ancilla, and determine the dimension of the ancilla when an economic implementation is not possible.

I. INTRODUCTION

Quantum information constitutes a feasibility study of protocols subject to the physical laws of quantum mechanics. When they cannot be realized, it quantifies and determines the best possible result. Often these considerations are made under restrictions such as those of local operations and classical communication. However, even in their absence, there is the fundamental restriction that any protocol must be implemented by a completely positive (CP) map. The quintessential instance of this problem is quantum cloning; it is impossible to take one copy of an unknown quantum state and produce a second identical copy, unless that unknown state is known to be drawn from a set of orthogonal states [1].

The no-cloning theorem, as a cornerstone of quantum theory, is related to many fundamental ideas such as the principle of no-signaling [2], uncertainty relations and state estimation [3]. Apart from the intrinsic theoretical interest, the no-cloning theorem has also found application in quantum cryptography [4] where it enables detection of attempts by an adversary to copy the information on a communication channel. While the no-cloning theorem is now well established, the question of the extent to which an unknown quantum state can be copied has been the subject of intensive research, excellent reviews of which can be found in [5, 6].

The optimal cloning of discrete quantum states began with the idea of the Buzek-Hillery quantum cloning machine which obtains two identical copies of a given unknown qubit state [7]. This has been extended to $M \to N$ cloning [8] where, starting from M copies of the same unknown quantum state, the task is to produce N output copies of as high a quality as possible. While the original cloning machines were symmetric, in the sense that all output copies had the same fidelity, this has also been extended to asymmetric cloning [9]. In this latter task, not all copies need to have the same quality; some output clones can be made to have higher fidelities at the expense of others. This is an important feature since it is

precisely these trade-offs which quantify a potential level of eavesdropping, or the relationship between different correlations in a given quantum state.

The original cloning machines were designed to clone all input pure states of a given dimension d (referred to as "universal cloning"). With prior knowledge of the distribution of the states to be cloned, better strategies can be devised for this, state-dependent, cloning. There are several well-known instances, the most common of which we refer to as "equatorial cloning" [10]: for $d = 2$, the state of the qubit is known to be drawn from the set of states on the equator of the Bloch sphere, $(|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ and any angle $\phi \in (0, 2\pi)$ is equally likely. This generalizes to "phase-covariant" cloning: for $d = 2$, the state of the qubit is drawn from the set $\cos\theta|0\rangle + \sin\theta e^{i\phi}|1\rangle$ with a probability distribution that is independent of the parameter ϕ.

Another important question is the economy of implementation of a cloner; if the optimal cloning machine can be implemented unitarily without any ancillary systems, the cloner is said to be economical, otherwise it is not [11, 12]. The presence or absence of any ancilla systems alters the implementation of the cloner experimentally, the economic cloner being simpler to control and less sensitive to decoherence effects.

In this paper, we apply the powerful formalism of the Choi-Jamiołkowski isomorphism to solve several interesting instances of the cloning problem. The central result constitutes a completion of the study started in [13]; a determination of the optimal cloning fidelities for $1 \to N$ universal asymmetric cloning of qudits (arbitrary N and d). While special case results are known for N up to 4 [9, 14], we proposed in [13] a general solution, but some caveats remained unresolved. We simplify the proof of [13], and extend it to close the potential loopholes in the argument, making use of the Lieb-Mattis theorem [15] to prove that the maximum eigenvalue of the whole system is found in a particular subspace.

The paper is organized as follows. In Section II, we explain the formalism used to obtain bounds on the achiev-

able fidelities in state transformation tasks and state the necessary and sufficient condition for the maximum fidelity to be realized by a completely positive map. We also explain the applicability of the formalism to the problem of cloning quantum states, stating the figure of merit used to define the success of the operation. In section III, we study the $1 \rightarrow N$ qubit cloning problem, providing a parametrization for a class of state-dependent cloners, deriving solutions in the symmetric instance and studying the economy of its implementation. In the asymmetric case, it is proven that if N is odd, the optimal cloner is economical. For even N, no more than one ancilla qubit is required. For equatorial qubit cloning, we solve the asymmetric case for $N = 2$, enabling a simple derivation of the monogamy of the CHSH Bell inequality.

Section IV constitutes the main result of the paper, where the $1 \rightarrow N$ asymmetric universal qudit cloning problem is solved and its economic realization is studied. Many of the technicalities of the proof, which elevate it over the conjectures in [13], are expounded in the Appendix. For $N > 2$, we prove that the optimal machine is economical. For $N = 2$, the optimal machine is not economical, requiring one additional qudit[1]. Subsequently, in Sec. V, the applicability of the formalism to the $M \rightarrow N$ cloning is explained. The penultimate section, Sec. VI, contains the trade-off relations in the optimal fidelities in the two instances where such a relation can be derived, namely $1 \rightarrow N$ qudit cloning and $(N - 1) \rightarrow N$ qubit cloning. The paper concludes with a summary of the work and possible future extensions.

II. THE CHOI-JAMIOŁKOWSKI ISOMORPHISM

We begin with an explanation of the main tool used in the solution of optimal cloning tasks, the well-known Choi-Jamiołkowski isomorphism. This formalism is used in general to find how well a particular state transformation task can be achieved by a quantum process, i.e., a completely positive map [16].

The scenario is that, given one of a set of L states $|\psi_i\rangle$ $(i = 1, \ldots, L)$, we are required to perform a particular state transformation on it, without being told which of the states we have been given. The required transformation may not be achievable exactly within the quantum formalism, but is best approximated within the theory by a completely positive, trace preserving map $\mathcal{E}$ that transforms input state $|\psi_i\rangle$ into $\mathcal{E}(|\psi_i\rangle)$. The success of the state transformation task is then measured by a fidelity given by

$$F = \frac{1}{L} \sum_i \mathrm{Tr}\left(\mathcal{M}_i \mathcal{E}(|\psi_i\rangle)\right).$$

––––––––––

[1] other than extreme cases which reduce to $N = 1$

Here $\mathcal{M}_i$ are positive operators ($\mathcal{M}_i \geq 0$) satisfying $\|\mathcal{M}_i\| \leq 1$ so that F is indeed a fidelity taking values between 0 and 1. If the fidelity takes value 1, we infer that the map has perfectly implemented the required state transformation for all the specified input states. As a simple example, consider being required to transform the states $|\psi_i\rangle$ into states $|\phi_i\rangle$, in which case we simply define $\mathcal{M}_i = |\phi_i\rangle \langle \phi_i|$.

The fidelity can now be rewritten in a manner that yields definite upper bounds. This is accomplished by the isomorphism as follows. Since $\mathcal{E}$ is a completely positive map, its operation on a subsystem O of a bipartite entangled state (entangled between input system I and output O) is well defined. Let us denote the maximally entangled state of interest as

$$|B\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |\phi_i\rangle_I |\phi_i\rangle_O \,,$$

where the basis states $|\phi_i\rangle$ ($i = 0, \ldots, d-1$) span the subspace occupied by the set of input states $|\psi_i\rangle$ (which have dimension d). The action of the composite map, composed of the identity on the input space and the desired map $\mathcal{E}$ on the output space of the maximally entangled state gives us the output χ_{IO},

$$\mathbb{1}_I \otimes \mathcal{E}(|B\rangle)_O = \chi_{IO}.$$

The condition that $\mathcal{E}$ be trace preserving then implies that $\mathrm{Tr}(\chi_{IO}) = \langle B|B\rangle = 1$. If the map is not trace preserving, this would instead yield $\mathrm{Tr}(\chi_{IO}) \leq 1$, which will not alter our conclusions since we are interested in finding an upper bound to the fidelity of state transformation. The fidelity can now be evaluated as

$$F = \frac{d}{L} \sum_i \mathrm{Tr}\left(\chi_{IO}(|\psi_i\rangle \langle \psi_i|_I^T \otimes \mathcal{M}_i)\right),$$

where the superscript T denotes transposition. If we define a matrix R as

$$R = \frac{d}{L} \sum_i |\psi_i\rangle \langle \psi_i|_I^T \otimes \mathcal{M}_i, \qquad (1)$$

then we obtain

$$F = \mathrm{Tr}(R\chi_{IO}) \leq \mathrm{Tr}(\chi_{IO})r_{\max} \leq r_{\max} \qquad (2)$$

where $r_{\max}$ is the maximum eigenvalue of matrix R. We thus arrive at the important conclusion that the maximum fidelity achievable within quantum theory for a given state transformation task is bounded by the maximum eigenvalue of a suitable matrix R.

A few points are worthy of emphasis. The dimension d appearing in the equations above is the dimension of the subspace of Hilbert space spanned by the set of states $|\psi_i\rangle$. Even if the states $|\psi_i\rangle$ are defined on M qubits, it is not necessarily the case that $d = 2^M$, since the states might exist on a smaller subspace. Such is indeed the

case when we are performing the $M \to N$ cloning task as we shall see in a section V. For a continuous set of states, the sum appearing in the definition of R (Eq. (1)) transforms to an integral. The factor of $1/L$ appearing in Eq. (1) stems from the assumption that each of the input states $|\psi_i\rangle$ is equally likely. If this is not the case, these parameters can be adjusted based on a given probability distribution of the input states.

The fact that the state transformation problem has been transformed into the problem of finding the maximum eigenvalue of a matrix is interesting and highly useful. Even if the matrix R proves to be difficult to diagonalize exactly, one can use many techniques (borrowed for instance from condensed matter physics) to bound the achievable fidelities. One example of such a technique that has been used in finding bounds on ground state energies of condensed matter systems is to upper bound the norm of the matrix by the sum of the norms of the constituent terms [17].

A. Achieving the Maximum Fidelity

From the equations above, we see that the maximum eigenvector, $|\Psi\rangle$, of the matrix R defines the optimal strategy if it can be realized. If $|\Psi\rangle$ is unique, it can be expressed as a pure bipartite state between the subsystems I and O with a Schmidt decomposition

$$|\Psi\rangle = \sum_{n=0}^{d-1} \beta_n |\phi_n\rangle |\lambda_n\rangle .$$

When the Schmidt coefficients are given by $\beta_n^2 = \frac{1}{d}$, the state is maximally entangled across the input/output partition and can be implemented by a unitary U, defined as

$$U|\phi_n\rangle = |\lambda_n\rangle \qquad \forall n.$$

Here the relevant Hilbert spaces are extended as necessary so that they have the same size. In this instance, the optimal strategy is called economical, meaning that one does not require an ancilla for the operation to be implemented. In fact, even if the maximum eigenvector is not unique, provided there exists a superposition of the maximum eigenvectors that is maximally entangled, the optimal map can be implemented as a unitary and is therefore economical.

More generally, if there exists a mixture of the maximum eigenvectors of R, ρ_R, such that $\mathrm{Tr}_O\rho_R$ is maximally mixed, then this can be implemented as a CP map or, equivalently, a unitary operator over a larger Hilbert space, in which case the operation is no longer economical. The condition for implementation of the state transformation task optimally by a CP map is therefore

$$\mathrm{Tr}_O\rho_R = \frac{1}{d}\mathbb{1}_I.$$

That this condition is sufficient is seen easily by recognizing that one can add an auxiliary Hilbert space to purify ρ_R. The overall pure state then defines a unitary as in the previous case although this operation is not economical. That this condition is also necessary is seen by writing the optimal CP map using the Kraus decomposition as

$$\mathcal{E}(\rho) = \sum_i A_i \rho A_i^\dagger$$

where $\sum_i A_i^\dagger A_i = \mathbb{1}$. We then find that

$$\rho_R = \mathbb{1}_I \otimes \mathcal{E}_O(|B\rangle\langle B|) = \sum_i A_i^O |B\rangle\langle B|_{IO} A_i^{O\dagger}.$$

And upon performing the partial trace over O, we obtain

$$\mathrm{Tr}_O\rho_R = \mathrm{Tr}_O\left(\sum_i A_i^\dagger A_i |B\rangle\langle B|_{IO}\right),$$

which can be reduced using the completeness relation for the Kraus operators $\sum_i A_i^\dagger A_i = \mathbb{1}$ to $\mathrm{Tr}_O\rho_R = \frac{1}{d}\mathbb{1}_I$.

As a final remark we mention that the optimal strategy can also be implemented by teleporting the input state onto spin I of a resource state which could be either $|\Psi\rangle$ or the purification of ρ_R. The different measurement results of teleportation can be corrected for by action on the output space if the state satisfies the required trace condition. In the case of cloning, this gives rise to telecloning protocols.

B. Application to cloning quantum states

The potentially powerful formalism described above is now used in the problem of the optimal cloning of quantum states. In the cloning process, we start with an unknown quantum state $|\psi\rangle$ of Hilbert space dimension d, and aim to produce N copies of the state. It is known that this state is drawn from a possible set of states Σ with distribution $f(\psi)$ that is normalized as

$$\int_\Sigma f(\psi)d\psi = 1.$$

Dividing the output space O into N qudits labeled 1 to N, our aim is to optimize the quality of the N different copies to be produced. There are different figures of merit that can be applied to cloning (i.e. different definitions of the $\mathcal{M}_i$). The simplest figure of merit is the *global fidelity*, for which $\mathcal{M}_i = |\psi_i\rangle\langle\psi_i|^{\otimes N}$. The solution to the cloning problem in terms of the global fidelity is known [18] and will not concern us in the rest of the paper. Instead, we consider the *single copy fidelity*, in which we take the global output state $\rho_{1\dots N}$, and assess the fidelity of a single copy on a given site n, $F_n = \mathrm{Tr}(|\psi_i\rangle\langle\psi_i|_n \rho_{1\dots N})$. To this end, we define

$$\mathcal{M}_i = \sum_{n=1}^{N} \alpha_n |\psi_i\rangle\langle\psi_i|_n$$

where imposing $\alpha_n \geq 0$ and $\sum_{n=1}^{N} \alpha_n = 1$ ensures that the $\mathcal{M}_i$ satisfy the required property $\|\mathcal{M}_i\| \leq 1$ in addition to $\mathcal{M}_i \geq 0$. In particular, $F = 1$ can still only be achieved if the output state is $|\psi_i\rangle^{\otimes N}$ for all inputs i. For generality, we assign different weights α_n to the different copies, emphasizing a possible desire for different qualities of output, although a common desire is equal qualities, $\alpha_n = 1/N$. The latter case is called optimal symmetric cloning while the general scenario is the optimal asymmetric cloning problem from 1 to N copies.

For the single copy fidelity, on which we henceforth concentrate exclusively, the matrix R is seen to be

$$R = \int_{\Sigma} f(\psi) d\psi \, |\psi\rangle \, \langle\psi|_I^T \otimes \sum_{n=1}^{N} \alpha_n \, |\psi\rangle \, \langle\psi|_n . \qquad (3)$$

We are considering here cloning from a single copy of $|\psi\rangle$ so that the problem is $1 \to N$ cloning. This means that the dimension of the input Hilbert space I is no larger than d, and the basis is simply $|i\rangle$ for $i = 0 \ldots d-1$.

III. STATE DEPENDENT CLONING OF QUBITS

In this section, we illustrate the above formalism by restricting to the common case of qubits ($d = 2$), parameterizing the input state by

$$|\psi\rangle = \cos\frac{\theta}{2} \, |0\rangle + \sin\frac{\theta}{2} e^{i\phi} \, |1\rangle$$

for some distribution function $f(\theta, \phi)$. We impose two restrictions on the input distribution function $f(\theta, \phi)$, namely: (i) $f(\theta, \phi)$ is phase covariant, meaning it is independent of ϕ, i.e., $f(\theta, \phi) = f(\theta)$ and (ii) $f(\theta, \phi)$ is symmetric about the equator of the Bloch sphere, i.e., $f(\theta) = f(\pi - \theta)$.

Using these assumptions[2], the matrix R for the $1 \to N$ cloning of qubits can be written as

$$R = \tfrac{1}{2}\mathbf{1} + \sum_{n=1}^{N} \alpha_n \Gamma \left(XX - YY + \frac{1-4\Gamma}{2\Gamma} ZZ \right)_{0,n} ,$$

where X, Y and Z are the familiar Pauli matrices, and

$$\Gamma = \frac{1}{4} \int f(\theta, \phi) \sin^2 \theta \, d\theta \, d\phi.$$

The parameter, Γ, varying between 0 and $\frac{1}{4}$ provides an intuitive interpretation regarding the distribution of states over the Bloch sphere - the larger the value, the more tightly packed the states are around the equator. We would now like to find the maximum eigenvector and maximum eigenvalue of R. The problem can be recast by applying a rotation Y_0 to R, and instead demanding the minimum eigenvector (ground state) of a new matrix $\tilde{R}$ given as

$$\tilde{R} = -\tfrac{1}{2}\mathbf{1} + \sum_{n=1}^{N} \alpha_n \Gamma \left(XX + YY + \frac{1-4\Gamma}{2\Gamma} ZZ \right)_{0,n} .$$

This matrix $\tilde{R}$ is familiar as the Hamiltonian for an anisotropic Heisenberg model on a star configuration and we can proceed to find its ground state.

Before we do that, let us analyze the possibility of implementing the above optimal qubit cloning transformation economically. To do so, we observe that $\tilde{R}$ commutes with the operator $\sum_{n=0}^{N} Z_n$, so that the system divides into a series of excitation subspaces. We also note that $[\tilde{R}, X^{\otimes(N+1)}] = 0$, which maps the k excitation subspace to the $N+1-k$ excitation subspace. These two observations enable us to make some general statements about the entanglement of the ground state, and hence about the economy of cloning. To do this, consider the minimum eigenvector in an M excitation subspace, which can be split between the input and output systems,

$$|\Psi_M\rangle = \alpha \, |0\rangle \, |\phi_M\rangle + \beta \, |1\rangle \, |\phi_{M-1}\rangle .$$

Since the corresponding state in an $N+1-M$ excitation subspace,

$$|\Psi_{N+1-M}\rangle = \alpha \, |1\rangle \, X^{\otimes N} \, |\phi_M\rangle + \beta \, |0\rangle \, X^{\otimes N} \, |\phi_{M-1}\rangle$$

is also an eigenvector, one can construct the state

$$\frac{1}{\sqrt{2}} (|\Psi_M\rangle + |\Psi_{N+1-M}\rangle)$$

which is also an eigenvector with the same eigenvalue. It is readily verified to be maximally entangled unless $M = \frac{1}{2}N$, $\frac{1}{2}(N+1)$ or $\frac{1}{2}N + 1$. For odd N, consider the subspace with $\frac{1}{2}(N+1)$ excitations. If $|\Psi_{(N+1)/2}\rangle$ is the unique minimum eigenvector in this subspace, then invariance under $X^{\otimes(N+1)}$ proves that it must be maximally entangled. On the other hand, if this state is not the unique minimum eigenvector, there always exists a state in the degenerate space which is maximally entangled. Hence, for odd N, the optimal cloner is always economical, meaning that no ancillary system is required to implement the cloning transformation. For even N, this is not necessarily true, but no more than one additional qubit is required because one can increase N by 1 and then implement the optimal cloner, imposing that one of the fidelities is $\frac{1}{2}$ ($\alpha_{N+1} = 0$).

A. Symmetric Cloning

The most commonly studied instance of cloning is where all the output copies are required to have the same

---

[2] The assumptions specified have a natural interpretation, but in practice one only needs the following four integrals to vanish: $\int f(\theta, \phi) d\theta d\phi \cos\theta$, $\int f(\theta, \phi) d\theta d\phi \, e^{i\phi} \sin\theta$, $\int f(\theta, \phi) d\theta d\phi \, e^{i\phi} \sin(2\theta)$ and $\int f(\theta, \phi) d\theta d\phi \, e^{i2\phi} \sin^2 \theta$.

fidelity, so $\alpha_n = \frac{1}{N}$. Thus, we have

$$\tilde{R} = -\frac{1}{2}\mathbf{1} + \Gamma\left(X_I\left(\frac{1}{N}\sum_{n=1}^N X_n\right) + Y_I\left(\frac{1}{N}\sum_{n=1}^N Y_n\right)\right)$$
$$+ \frac{1-4\Gamma}{2}\left(Z_I\left(\frac{1}{N}\sum_{n=1}^N Z\right)\right),$$

The permutation invariance on qubits $1\ldots N$ means that the operators such as $\left(\frac{1}{N}\sum_{n=1}^N X_n\right)$ reduce into a simple direct sum structure [3]. In the present instance therefore, the eigenvalue that we require will always be taken from the fully symmetric subspace, meaning that the problem reduces to solving for the minimum eigenvalue of

$$R' = -\frac{1}{2}\mathbf{1} + \frac{\Gamma}{N}\left(X_I S^{X,N+1} + Y_I S^{Y,N+1} + \Delta Z_I S^{Z,N+1}\right)$$

where $S^{X,k}$ is the X-rotation matrix for a k dimensional space (see the Appendix for further information) and $\Delta = \frac{1-4\Gamma}{2\Gamma}$. The maximum fidelity that can be realized in the cloning transformation is thus given by

$$F = \frac{1}{2} + \frac{\Gamma\Delta}{N} +$$
$$\frac{\Gamma}{N}\max_{i=0\ldots N-1}\sqrt{4(i+1)(N-i) + \Delta^2(N-2i-1)^2}.$$

The choice of the best i depends on the value of Γ. For $\frac{1}{6} \leq \Gamma \leq \frac{1}{4}$, the i should ideally be $(N-1)/2$. However, since i must be an integer, it takes the value $\lfloor N/2 \rfloor$. Hence, in this regime of Γ, the fidelity is given by

$$F = \begin{cases} \frac{1}{2} + \frac{1}{2N} + \frac{\Gamma}{N}(N-1) & N \text{ odd} \\ \frac{1}{2} + \frac{1-4\Gamma}{2N} + \frac{\Gamma}{N}\sqrt{N(N+2)+\Delta^2} & N \text{ even} \end{cases}$$

For $0 \leq \Gamma \leq \frac{1}{6}$, the term is maximized when i is either 0 or $N-1$. Both give the same fidelity,

$$F = \frac{1}{2} + \frac{1-4\Gamma}{2N} + \frac{\Gamma}{N}\sqrt{4N+(N-1)^2\Delta^2}.$$

For classical inputs, when the subset of possible states is only $|0\rangle$ or $|1\rangle$, then it is clear that one should be able to achieve the maximum cloning fidelity 1. This is indeed the case, because when $\Gamma = 0$, the maximum eigenstates of R are $|0\rangle^{\otimes(N+1)}$ and $|1\rangle^{\otimes(N+1)}$ and one can construct a maximally entangled superposition

$$\frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes(N+1)} + |1\rangle^{\otimes(N+1)}\right),$$

proving that there exists a unitary that achieves the optimal fidelity of cloning.

If the state $|\psi\rangle$ is selected uniformly over the surface of the Bloch sphere ($\Gamma = \frac{1}{6}$), R becomes the Hamiltonian of the isotropic Heisenberg model. The optimal fidelity of symmetric universal cloning, $F = \frac{2N+1}{3N}$, is recovered.

---

[3] When asymmetry is present, but subsets of spins should have the same fidelity, those sets have that direct sum structure, and are replaced by a single spin operator of the correct dimension.

B. Equatorial Cloning

In the case of equatorial cloning, the set of states is restricted to the input distribution function $f(\theta)$ with the specific choice of $\theta = \pi/2$. In this situation, we clone states that are on the equator of the Bloch sphere, $\Gamma = \frac{1}{4}$. While we do not solve this problem for general asymmetry, the fully symmetric case [10] is now easily recovered by our previous considerations.

$$F = \begin{cases} \frac{3N+1}{4} & N \text{ odd} \\ \frac{1}{2} + \frac{\sqrt{N(N+2)}}{4N} & N \text{ even} \end{cases}$$

We can examine the possibility of achieving the optimal cloning fidelity for equatorial qubit cloning in an economical manner even in the general case of arbitrary asymmetries. Even without completely obtaining the solution, we can make the following statement about the entanglement of the telecloning state – any optimal pure state must be maximally entangled. This strong statement, showing that the transformation can be performed economically, follows from the observation that $Z_0(\tilde{R} + \frac{1}{2}\mathbf{1})Z_0 = -(\tilde{R} + \frac{1}{2}\mathbf{1})$. Hence, if $|\Psi_M\rangle$ is a minimum eigenvector in a particular excitation subspace, M, then $Z_0|\Psi_M\rangle$ is a maximum eigenvector in the same excitation subspace. With the exception of eigenvectors of $\tilde{R}$ with eigenvalue $-\frac{1}{2}$ (which give a fidelity smaller than a complete guess), these two states are orthogonal, making the computational basis the Schmidt basis, with equal Schmidt coefficients. Therefore, we can conclude that for arbitrary asymmetries and any N, the optimal equatorial qubit cloner is economical. This generalizes the results in [11] which show explicitly that for the symmetric case and $N = 2$, the equatorial cloner is economical.

Serving as a prelude to the derivation of monogamy relations from solutions to optimal cloning problems in Sec. VI, we make a brief aside to indicate how the monogamy relation of the CHSH Bell inequality [19] arises as a consequence of the consideration of $1 \to 2$ asymmetric equatorial cloning. The CHSH inequality is a two-party two-setting Bell inequality. Up to local unitaries, the operator measured in a CHSH test on a quantum system between parties 0 and n can be expressed as

$$\mathcal{B}_{0n} = \sqrt{2}(XX - YY)_{0n}.$$

This is due to the fact that (up to local unitaries), the individual settings can be chosen to lie in the X-Y plane by both parties. Moreover, for optimal violation for any entangled quantum state, the local settings should be chosen such that they are as far away from being commuting as possible [20]. In this scenario, we would like to derive the optimal trade-off between the CHSH inequality violation between Alice and Bob (each holding a qubit state) and that between Alice and Charlie, i.e., between $\mathcal{B}_{01}$ and $\mathcal{B}_{02}$. Maximizing the cloning fidelity corresponds to finding the maximum eigenvalue, λ, of

$$\frac{1}{2}\mathbf{1} + \frac{1}{4\sqrt{2}}\left(\alpha_1\mathcal{B}_{01} + \alpha_2\mathcal{B}_{02}\right),$$

which implies that the average values of the two CHSH parameters for any state, $\langle \mathcal{B}_{01} \rangle$ and $\langle \mathcal{B}_{02} \rangle$, obey

$$\alpha_1 \langle \mathcal{B}_{01} \rangle + \alpha_2 \langle \mathcal{B}_{02} \rangle \leq 4\sqrt{2}(\lambda - \tfrac{1}{2})$$

where the maximum eigenvalue is given by $\lambda = \frac{1}{2}(\sqrt{\alpha_1^2 + \alpha_2^2} + 1)$. The two asymmetry parameters must satisfy $\alpha_1 + \alpha_2 = 1$, so we can choose them to satisfy

$$\alpha_1 = \langle \mathcal{B}_{01} \rangle \kappa \qquad \alpha_2 = \langle \mathcal{B}_{02} \rangle \kappa,$$

for suitable κ. This choice of the asymmetry parameters implies the well-known monogamy relation for the Bell-CHSH inequality within quantum theory [19]

$$\langle \mathcal{B}_{01} \rangle^2 + \langle \mathcal{B}_{02} \rangle^2 \leq 8.$$

In general, when interpreting the state $|\Psi\rangle$ as a state used in telecloning, its ability to clone well (and hence the general performance of the corresponding unitary cloner) is limited by the monogamy of its correlations. This could be derived for any of the state dependent cloners. Doing so for the universal cloner produced singlet monogamy [13] (see Sec. VI).

IV. $1 \to N$ QUDIT CLONING

We shall now move to the main result of the paper, namely the solution to the general case of $1 \to N$ cloning where the input state lives in an arbitrary Hilbert space dimension d, and the output copies can have differing fidelities. For this qudit cloning problem, we concentrate on the specific case when $f(\psi)$ is uniformly distributed over the set of states according to the Haar measure i.e. we are equally likely to be trying to clone any one qudit pure state. To derive the matrix R for this, the $1 \to N$ universal asymmetric qudit cloning, problem, we write that $|\psi\rangle = U |0\rangle$ and integrate over U to obtain [13]

$$R = d \int dU U^* |0\rangle \langle 0| U^T \otimes \sum_{n=1}^{N} \alpha_n U^\dagger |0\rangle \langle 0|_n U.$$

The integration results in twirling [21] to yield

$$R = \frac{1}{d+1} \mathbf{1} + \frac{d}{d+1} \sum_{n=1}^{N} \alpha_n |B\rangle \langle B|_{0,n}.$$

where $|B\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} |\phi_i\rangle_I |\phi_i\rangle_O$ is the Bell state as defined previously.

The main route towards solving this is to notice that any symmetric state $|\Phi\rangle$ of $N - 1$ qudits (meaning the same state is returned when any pair of qudits is exchanged) allows one to write down states $\{|\Psi_m\rangle = |B\rangle_{0,m} |\Phi^{N-1}\rangle_{1,2...N \neq m}\}$ that span a subspace of R. The permutation invariance ensures that

$$|B\rangle \langle B|_{0,m} |\Psi_n\rangle = \frac{1 + (d-1)\delta_{n,m}}{d} |\Psi_m\rangle.$$

Within the subspace, the eigenvectors of the matrix R are described by

$$|\Psi\rangle = \sum_{n=1}^{N} \beta_n |\Psi_n\rangle, \tag{4}$$

subject to the normalization condition

$$\left(\sum_{n=1}^{N} \beta_n \right)^2 + (d-1) \sum_{n=1}^{N} \beta_n^2 = d. \tag{5}$$

Here the coefficients $\{\beta_n\}$ are chosen such that they form a vector which is the maximum eigenvector of the matrix

$$\sum_{n,m=1}^{N} \alpha_n |n\rangle \langle m| + (d-1) \sum_{n=1}^{N} \alpha_n |n\rangle \langle n|. \tag{6}$$

By definition, then, this is the maximum eigenvector of the particular subspace, eigenvalue λ. If it were the maximum eigenvector of the entire matrix R, the cloning fidelity would be given by $F \leq \frac{1+\lambda}{d+1}$. To prove that this eigenvector is indeed the maximum eigenvector, we invoke a variant of the Lieb-Mattis Theorem [15]. Indeed, if $d = 2$, no modification is required, and [15] instantly proves that we have the maximum eigenvector because, by the previous results, we are searching for the ground state of a Heisenberg star. The full proof for arbitrary d is deferred to the Appendix.

It should be noted that the matrix in Eq. (6), which is derived from the matrix R and used to choose the particular set of $\{\beta_n\}$, is independent of the choice of $|\Phi\rangle$. Also note that since the matrix in Eq. (6) is real, the coefficients β_n can be taken to be real, justifying the absence of conjugates in the normalisation condition.

A. Possibility of economic universal qudit cloning

Having proved, as in the Appendix, that the state Eq. (4) gives the maximum eigenvector of R and that the optimal fidelity is given by $F \leq \frac{1+\lambda}{d+1}$, we need to check that this bound can be saturated by verifying that the maximum eigenvector corresponds to an implementable CP map. To show this, we need to demonstrate that there exists a superposition or mixture of the set of optimal states such that the partial trace over the outputs returns a maximally mixed state on the input (Sec. II).

Eq. (4) offers plenty of freedom in selecting the symmetric state $|\Phi\rangle$. Hence, we will pick a particular symmetric state

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes(N-1)}.$$

Provided $N > 2$, tracing out qudits 1 to N of the corresponding $|\Psi\rangle$ just leaves

$$\rho_0 = \tfrac{1}{d} \mathbf{1},$$

i.e. $|\Psi\rangle$ is maximally entangled, so the optimal map can be implemented, and that implementation is economical.

On the other hand, for $N = 2$, one can examine an arbitrary $|\Phi\rangle$ and prove that the maximally entangled state only occurs if $\beta_1\beta_2 = 0$ i.e. one of the clones will be perfect, and the other has no information about the input qudit at all; this is the trivial $N = 1$ case. Otherwise, economical optimal cloning if impossible for $N = 2$. Nevertheless, one can readily verify that the mixed state formed by the maximum eigenvectors

$$\rho = \frac{1}{d}\sum_{i=0}^{d-1}|\Psi_i\rangle\langle\Psi_i|$$

has the required partial trace $\rho_0 = \frac{1}{d}\mathbf{1}$, meaning that the optimal fidelity can be realized with only one ancilla of dimension d. The results of [11], where it was proven that universal economical cloning is impossible for the $1 \to 2$ case, are clearly a special case of this result.

V. $M \to N$ QUBIT CLONING

The study of the optimal cloning machines can be extended to the case when, instead of a single input copy of the state to be cloned, multiple copies are provided. The matrix R can be derived for this scenario in a similar manner to the previous sections. The difference here is that the dimension d' of the input space is not simply d^M. Instead, d' is the dimension of the fully symmetric subspace of the M qudits. The matrix R is therefore defined as

$$R = d'\int f(\psi)d\psi \bigotimes_{m=1}^{N}|\psi\rangle\langle\psi|_{I_m}^T \sum_{n=1}^{N}\alpha_n|\psi\rangle\langle\psi|_n.$$

As before, the maximum eigenvalue of R upper bounds the achievable fidelity of the cloning transformation and, if there exists some superposition of the maximum eigenvectors which is maximally bipartite entangled between the input qudits and the output ones, the maximum fidelity can be achieved by a unitary operation.

Here, we concentrate on the special case of universal $M \to N$ qubit cloning. After performing the twirling operation and projecting the input spins onto the symmetric subspace, we obtain

$$R = \sum_n \alpha_n R_n$$

with

$$2R_n = \mathbf{1} + \frac{1}{M+2}(S_I^{X,M+1}X_n - S_I^{Y,M+1}Y_n + S_I^{Z,M+1}Z_n).$$

The fidelities of the output copies are then given by $F_n = \langle\Psi|R_n|\Psi\rangle$ with the final fidelity being $F = \sum_n \alpha_n F_n$.

The proof strategy exactly mirrors that of the $1 \to N$ universal cloning task (see the Appendix). We first observe that the set of states

$$|\psi_{x,i}\rangle = \frac{1}{\sqrt{M+1}}\sum_{n=0}^{M}|n\rangle_I\left|\Phi_n^M\right\rangle_{\{x_k=1\}}\left|\Phi_i^{N-M}\right\rangle_{\{x_k=0\}}$$

forms a closed subspace. Here $|n\rangle_I$ represents the basis elements for the input symmetric subspace and $x \in \{0,1\}^N$ is an N-bit string of weight M. The superposition above therefore denotes that a symmetric state $\left|\Phi_n^M\right\rangle$ is the state of the M output spins for which the bit value in the bit string is 1 (of which n are in the state $|1\rangle$ and $M - n$ are $|0\rangle$). $\left|\Phi_i^{N-M}\right\rangle$ is the symmetric state of the remaining $N - M$ output spins with i qubits in the state $|1\rangle$. To verify that these states form a closed subspace of R, note that

$$R_n|\psi_{x,i}\rangle = \begin{cases} |\psi_{x,i}\rangle & x_n = 1 \\ \frac{1}{M+2}\left(|\psi_{x,i}\rangle + \sum_y |\psi_{y,i}\rangle\right) & x_n = 0 \end{cases}$$

Here the sum over y is over all bit strings $y \in \{0,1\}^N$ of weight M with the condition that $y = x$ in all except two places, one of which is bit n, $y_n = 1$. The relation

$$\langle\psi_{x,i}|\psi_{z,i}\rangle = \frac{1}{M+1-x\cdot z}$$

then implies the normalization condition.

Since the $\{|\psi_{x,i}\rangle\}$ span the space, we can write

$$|\Psi_i\rangle = \sum_x \beta_x |\psi_{x,i}\rangle. \tag{7}$$

The matrix R within this restricted subspace, $\tilde{R}$, is written, for bit strings $x, y \in \{0,1\}^N$ of weight M, as

$$\tilde{R}_{x,y} = \begin{cases} \frac{1}{M+2} + \frac{M+1}{M+2}\sum_{n:x_n=1}\alpha_n & x = y \\ \frac{1}{M+2}\sum_{n:x_n=0}\alpha_n\delta_{y_n=1} & x\cdot y = M-1 \end{cases}$$

So, at least in principle, the maximum eigenvalue of this matrix can be found. The Lieb-Mattis theorem is directly applicable, so we prove that the subspace contains the maximum eigenvector for the entire R, revealing the upper bound on the optimal cloning fidelity. It still remains to be checked that the optimal fidelity can be implemented by a CP map, which is more readily achieved on a case-by-case basis.

VI. FIDELITY TRADE-OFF RELATIONS

The formalism outlined so far reduces the task of finding the optimal universal qubit cloner to that of diagonalizing an $\binom{N}{M} \times \binom{N}{M}$ matrix, although we have not explicitly performed this diagonalization in the asymmetric case. Finding the maximal eigenvalue specifies a trade-off between the parameters $\{\alpha_n\}$ and the qualities of the clones given by $F_n = \langle\Psi|R_n|\Psi\rangle$. Evidently, specifying the solution to the asymmetric cloning problem is best

done in terms of trade-off relations between the various output fidelities. In this section, we derive the fidelity trade-off relations in two cases of interest to us, namely $1 \rightarrow N$ universal qudit cloning and $(N-1) \rightarrow N$ universal qubit cloning.

Whenever the task of finding the maximum eigenvector of R can be reduced to a problem on an N-dimensional space (where N is the number of different fidelities we might have in the asymmetric cloning), we have N parameters β_i in the state

$$|\Psi\rangle = \sum_{n=1}^{N} \beta_i |\psi_i\rangle$$

where $\{|\psi_i\rangle\}$ span the space. The fidelities F_n are simply a quadratic function of the β_i, as is the normalization condition $\langle\Psi|\Psi\rangle = 1$. We can therefore expect to eliminate the β_i in the normalization condition and replace them with the F_n. Intuitively, one can understand that when the dimension of the space is equal to the number of asymmetry parameters α_n, it is possible to explore the entire subspace corresponding to the optimal solution by varying the different parameters α_n. If the dimension of the subspace is greater, this is certainly not possible, and we can only follow a constrained path within the space, as specified by the maximum eigenvector. At that point, extracting the optimal trade-off relation analytically becomes challenging. Fortunately, in the two particular cases specified previously, it is possible to derive these fidelity relationships by the method outlined above. It is important to note that neither case ever actually requires the determination of the maximum eigenvalue of R.

A. Trade-offs for the $1 \rightarrow N$ qudit cloner

For $1 \rightarrow N$ universal qudit cloning, we derived the normalization condition of Eq. (5). This means that a (possibly non-optimal state) must satisfy the inequality

$$\left(\sum_{n=1}^{N} \beta_n\right)^2 + (d-1)\sum_{n=1}^{N} \beta_n^2 \leq d.$$

The cloning fidelities are given by

$$F_n = \frac{1}{d+1} + \frac{1}{d(d+1)}\left((d-1)\beta_n + \sum_{m=1}^{N} \beta_m\right)^2.$$

In order to eliminate the β_n in favor of the cloning fidelities F_n, observe that

$$\sum_{n=1}^{N} \sqrt{d(d+1)F_n - d} = (d-1+N)\sum_{n=1}^{N} \beta_n.$$

For simplicity, the trade-off relations can be expressed in terms of the singlet fraction, $p_{0,n}$. The singlet fraction of a pair of states between 0 and n is defined as

$$p_{0,n} = \max_{U,V} \langle B| U \otimes V \rho_{0,n} U^\dagger \otimes V^\dagger |B\rangle$$

where U and V are arbitrary d-dimensional unitary rotations. It is directly related to the cloning fidelity in $1 \rightarrow N$ universal qudit cloning [22],

$$F_n = \frac{p_{0,n}d + 1}{d+1}.$$

The previous expression can now be rewritten in terms of the singlet fraction as

$$d\sum_{n=1}^{N} \sqrt{p_{0,n}} = (d-1+N)\sum_{n=1}^{N} \beta_n.$$

Eliminating the variables β_n from the normalization condition, the trade-off relation in terms of the singlet fractions for the $1 \rightarrow N$ universal asymmetric qudit cloner is obtained:

$$\sum_{n=1}^{N} p_{0,n} \leq \frac{d-1}{d} + \frac{1}{N+d-1}\left(\sum_{n=1}^{N} \sqrt{p_{0,n}}\right)^2. \quad (8)$$

This relation describes the 'singlet monogamy' [13], in comparison to the tangle monogamy [23] or Bell monogamy [19], as it serves to bound the correlations that are achievable between different sets of spins in any quantum state. It can be seen that this single equation encapsulates the known results on $1 \rightarrow N$ universal asymmetric cloning, subsuming previous results on $1 \rightarrow 4$ cloning [9, 14], and much more besides.

B. Trade-offs for the $(N-1) \rightarrow N$ qubit cloner

Aside from $M = 1$ universal cloning, another instance for which the fidelity trade-off relation can be derived is $(N-1) \rightarrow N$ universal asymmetric qubit cloning. Let us replace the β_x that appear in the solution to this problem in Eq. (7) with γ_n, where, since the bit string x is of length N and weight $N-1$, there is only one zero bit, which we denote as being at position n. For this problem, the normalization condition reads

$$2 \geq \left(\sum_{n=1}^{N} \gamma_n\right)^2 + \sum_{n=1}^{N} \gamma_n^2,$$

while each of the cloning fidelities can be found to be

$$F_n = 1 - \frac{\gamma_n^2}{2}.$$

The elimination of the γ_n therefore leads to the following fidelity trade-off relation for the case of $(N-1) \rightarrow N$ universal asymmetric qubit cloning

$$N - 1 \leq \sum_{n=1}^{N} F_n - \left(\sum_{n=1}^{N} \sqrt{1-F_n}\right)^2, \quad (9)$$

describing the entire set of achievable fidelities.

Finally, to verify that these fidelities can be achieved by a CP map, observe that an equal mixture of the two states $|\Psi_0\rangle$ and $|\Psi_1\rangle$, as in Eq. (7), yields the identity on the $N-1$ input spins when the N output spins are traced out,

$$\tfrac{1}{2}\mathrm{Tr}_{1\ldots N}(|\Psi_0\rangle\langle\Psi_0| + |\Psi_1\rangle\langle\Psi_1|) = \tfrac{1}{N}\mathbf{1}.$$

This implies that this cloning transformation uses one ancilla qubit (i.e. is not economical) but gives the requisite trace satisfying the necessary and sufficient condition for its implementation by a CP map.

VII.   CONCLUSIONS

The efficacy with which a given quantum state can be cloned is an important problem in quantum information, having implications in diverse fields such as quantum cryptography, state estimation, and entanglement monogamy. In this paper, we tackled the problem using the Choi-Jamiołkowski isomorphism, and provided solutions in a number of interesting scenarios. The investigation of $1 \to N$ qubit cloning yielded a parametrization for a large class of state dependent cloners including the equatorial and universal cloners. If N is odd, the optimal cloner is economical and when N is even, no more than one ancilla qubit is required. As an interesting aside, we derived the monogamy relation for the CHSH Bell inequalities in terms of the fidelity trade-offs in the 1 to 2 asymmetric equatorial qubit cloning problem. For the general 1 to N asymmetric equatorial cloning problem, we proved that for any N and any asymmetry, the cloner is economical.

The main result of the paper is the solution to the $1 \to N$ universal asymmetric qudit cloning problem, for which we derived the exact trade-off relations in the fidelities of the output clones, Eq. (8). For $N > 2$, the optimal cloner is economical while for $N = 2$, it is not, requiring one additional ancillary qudit for its implementation. Generalizing to $M \to N$ cloning, we derived the (tight) trade-offs in the fidelities for the special case of $(N-1)$ to N universal cloning of qubits, Eq. (9), and provided some insight into why it is these two cases that yield such a straightforward monogamy relationship.

One aspect that we have not touched upon here is the efficiency of implementation of the optimal cloners. However, states such as those of the $1 \to N$ cloner, Eq. (4), have a concise description in the computational basis, which is sufficient to guarantee that they can be easily prepared, i.e. with circuits that scale as a polynomial in N [24]. While such an argument says nothing about the economy of the implementation, as ancillas may be used in intermediate steps, economy can also be achieved.

The formalism presented here, and, primarily, the techniques for proving optimality, can potentially be applied in many other scenarios. A natural generalization involves the cloning of mixed quantum states, a problem known as broadcasting [25]. There has also been a vast amount of literature on the problem of cloning for continuous variable systems [26] to which the methods may be directly applied. Finally, it is potentially interesting to consider the optimal cloning of quantum observables and entanglement rather than entire quantum states [27].

[1] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[2] N. Gisin, Phys. Lett. A, **242**, 1 (1998).
[3] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997); D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81** 2598 (1998).
[4] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, India, 175 (1984).
[5] V. Scarani, S. Iblisdir, N. Gisin and A. Acin, Rev. Mod. Phys. **77** 1225 (2005).
[6] N. J. Cerf and J. Fiurášek, Progress in Optics **49**, 455 (2006).
[7] V. Buzek and M. Hillery, Phys. Rev. A **54** 1844 (1996).
[8] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998); M. Keyl and R. F. Werner, J. Math. Phys. **40** 3283 (1999).
[9] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000); J. Fiurasek, R. Filip and N. J. Cerf, Quant. Inform. Comp. **5**, 583 (2005); S. Iblisdir, A. Acin, J. Fiurasek, R. Filip and N. J. Cerf, Phys. Rev. A **72** 042328 (2005).
[10] G. M. D'Ariano and C. Macchiavello, Phys. Rev. A **67**, 042306 (2003).
[11] T. Durt, J. Fiurasek, and N. J. Cerf, Phys. Rev. A **72**, 052322 (2005).
[12] F. Buscemi, G. M. D' Ariano, and C. Macchiavello, Phys. Rev. A **71** 042327 (2005); C. S. Niu and R. B. Griffiths, Phys. Rev. A **60**, 2764 (1999).
[13] A. Kay, D. Kaszlikowski, and R. Ramanathan, Phys. Rev. Lett. **103**, 050501 (2009).
[14] X. Ren, Y. Xiang, and H. Fan, Eur. Phys. J. D **65**, 621 (2011); P. Ćwikliński, M. Horodecki, and M. Studziński, Phys. Lett. A **376**, 2178 (2012).
[15] E. Lieb and D. Mattis, J. Math. Phys. **3**, 749 (1962).
[16] A. Jamiołkowski, Rep. Math. Phys. **3**, 275278 (1972).
[17] P. W. Anderson, Phys. Rev. **83**, 1260 (1951).
[18] J. Fiurášek, Phys. Rev. A **64**, 062310 (2001).
[19] B. Toner, Proc. R. Soc. A **465**, 59 (2009); B. Toner and F. Verstraete, quant-ph/0611001 (2006).
[20] B. S. Tsirelson, Lett. Math. Phys. **4**, 93 (1980); R. Horodecki, P. Horodecki, and M. Horodecki, Phys. Lett. A **200**, 5, 340 (1995).
[21] M. Horodecki and P. Horodecki, Phys. Rev. A **60**, 1888

(1999).

[22] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[23] V. Coffman, J. Kundu and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000); T. J. Osborne and F. Verstraete, Phys. Rev. Lett. **96**, 220503 (2006).

[24] P. Kaye and M. Mosca, in proceedings ICQI (Rochester, New York, USA, 2001).

[25] G. M. DAriano, C. Macchiavello, and P. Perinotti, Phys. Rev. Lett. **95**, 060503 (2005).

[26] N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301 (2000); S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. v. Loock, and S. Massar, Phys. Rev. Lett. **86**, 4938 (2001); J. Fiurasek, Phys. Rev. Lett. **86**, 4942 (2001).

[27] L.- P. Lamoureux, P. Navez, J. Fiurasek and N. J. Cerf, Phys. Rev. A **69**, 040301 (2004); E. Karpov, P. Navez and N. J. Cerf, Phys. Rev. A **72**, 042314 (2005).

[28] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Rev. Mod. Phys. **79**, 555 (2007).

APPENDIX A: DERIVATION OF OPTIMAL UNIVERSAL QUDIT CLONING

In this Appendix, we provide the optimal solution to the $1 \to N$ universal qudit cloning problem. In particular, we find the maximum eigenvector of the matrix R which is defined for this problem as

$$R = \frac{1}{d+1}\mathbf{1} + \frac{d}{d+1}\sum_{n=1}^{N}\alpha_n\left|B\right\rangle\left\langle B\right|_{0,n}.$$

A major ingredient in the derivation of our results is the understanding of symmetries in a system, particularly those of rotational and permutation invariance. We will recap the bare minimum here in order to familiarize the reader with our notation, but for further details, the excellent treatment in [28] can be relied upon. We start by defining the spin operators

$$
\begin{aligned}
S^{X,d} &= \sum_{n=0}^{d-2}\sqrt{(n+1)(d-n-1)}(\left|n\right\rangle\left\langle n+1\right| + \left|n+1\right\rangle\left\langle n\right|) \\
S^{Y,d} &= \sum_{n=0}^{d-2}\sqrt{(n+1)(d-n-1)}(-i\left|n\right\rangle\left\langle n+1\right| + i\left|n+1\right\rangle\left\langle n\right|) \\
S^{Z,d} &= \sum_{n=0}^{d-1}(d-1-2n)\left|n\right\rangle\left\langle n\right|,
\end{aligned}
$$

where the as yet unused subscript will be used later to denote which spin the operators act on. If $d = 2$, these operators will be simply written as X, Y and Z respectively, recovering the usual Pauli operators. In the $1 \to N$ cloning problem, we have one input spin (I) of dimension d', and N output spins $(1\ldots N)$ of dimension d. These will require us to specify the total spin operators

$$
\begin{aligned}
J_X^{d',d} &= -S_I^{X,d'} + \sum_{n=1}^{N}S_n^{X,d} \\
J_Y^{d',d} &= S_I^{Y,d'} + \sum_{n=1}^{N}S_n^{Y,d} \\
J_Z^{d',d} &= -S_I^{Z,d'} + \sum_{n=1}^{N}S_n^{Z,d} \\
J^2 &= J_X^2 + J_Y^2 + J_Z^2
\end{aligned}
$$

Note that we have an unusual combination of negative signs in these definitions. This is due to the symmetry structure not being the usual invariance under the unitaries $U^{\otimes N+1}$. However, note that under the action of

$$U_I = \sum_{n=0}^{d-1}(-1)^n\left|n\right\rangle\left\langle d-1-n\right|$$

on the input spin, this is transformed into the usual total spin operators. For this reason, we instantly recover

the commutation relation $[J_Z, J^2] = 0$. Since R simultaneously commutes with both J^2 and J_Z, it has two quantum numbers S (where $4S(S+1)$ is an eigenvalue of J^2) and M_Z (taking values $-S$ to S in integer steps), providing a lot of information about its structure.

We now use the permutation invariant states of M qudits of fixed excitation number $k = 0 \ldots M(d-1)$ which are denoted as $\left|\Phi_k^M\right\rangle$. In the case of $d = 2$, these are the uniform superposition of all states of M qubits containing k excitations. For a set of M d-dimensional spins, we note their relations to the spin operators,

$$\left(\sum_{m=1}^{M} S_m^{Z,d}\right)\left|\Phi_k^M\right\rangle = (M(d-1) - 2k)\left|\Phi_k^M\right\rangle$$

$$\frac{1}{2}\left(\sum_{m=1}^{M} S_m^{X,d} + iS_m^{Y,d}\right)\left|\Phi_k^M\right\rangle = \sqrt{k(M(d-1)+1-k)}\left|\Phi_{k-1}^M\right\rangle$$

$$\frac{1}{2}\left(\sum_{m=1}^{M} S_m^{X,d} - iS_m^{Y,d}\right)\left|\Phi_k^M\right\rangle = \sqrt{(k+1)(M(d-1)-k)}\left|\Phi_{k+1}^M\right\rangle.$$

Under the action of the individual terms in the matrix R, these states transform as

$$|B\rangle\langle B|_{0,n}|B\rangle_{0,m}\left|\Phi_i^{N-1}\right\rangle_{1,2\ldots N\neq m} = \begin{cases} |B\rangle_{0,n}\left|\Phi_i^{N-1}\right\rangle_{1,2\ldots N\neq n} & n = m \\ \frac{1}{d}|B\rangle_{0,n}\left|\Phi_i^{N-1}\right\rangle_{1,2\ldots N\neq n} & n \neq m \end{cases}$$

This therefore implies that the set of states $\{|B\rangle_{0,m}\left|\Phi_i^{N-1}\right\rangle_{1,2\ldots N\neq m}\}$ spans a subspace of R for each i, corresponding to a value of $M_Z = \frac{1}{2}(d-1)(N-1) - i$. Within this subspace, the eigenvectors are given by a superposition

$$|\Psi_i\rangle = \sum_{n=1}^{N} \beta_n |B\rangle_{0,n}\left|\Phi_i^{N-1}\right\rangle_{1,2\ldots N\neq n}, \qquad \text{(A1)}$$

and the coefficients must satisfy the normalization condition

$$\left(\sum_{n=1}^{N} \beta_n\right)^2 + (d-1)\sum_{n=1}^{N} \beta_n^2 = d.$$

Moreover, the coefficients $\{\beta_n\}$ are chosen to be the maximum eigenvector of the matrix

$$\sum_{n,m=1}^{N} \alpha_n |n\rangle\langle m| + (d-1)\sum_{n=1}^{N} \alpha_n |n\rangle\langle n|, \qquad \text{(A2)}$$

this being independent of i. The state Eq. (A1) formed using the coefficients β_n from the maximum eigenvector of the above matrix, is the maximum eigenvector of R within a given subspace i. The cloning fidelity using the maximum eigenvector is then given in terms of the maximum eigenvalue λ as $F = \frac{1+\lambda}{d+1}$. Before we proceed to find the absolute maximum eigenvector of R over all subspaces we examine the known case of symmetric cloning.

1. Symmetric Cloning

For the symmetric cloner where each of the output clones in the $1 \rightarrow N$ universal qudit cloner have the same quality so that $\alpha_n = \frac{1}{N}$, we can readily proceed to calculate the β_n and F. All the β_n are equal, and hence, by the normalization condition, we have

$$\beta_n = \sqrt{\frac{d}{N^2 + N(d-1)}}$$

and the final fidelity is

$$F = \frac{1}{N} + \frac{2(N-1)}{N(d+1)}.$$

This is known to be the optimal fidelity of the symmetric universal qudit cloner [5], so even without finding any other eigenvalues, we infer that these eigenvectors (given by Eq. (A1) with equal β_n) must be the maximal ones. These states, which we denote by $|\Psi_i^{\mathrm{sym}}\rangle$, will be used later in the proof.

Let us make an important observation about these states. The eigenvectors $|\Psi_i^{\mathrm{sym}}\rangle$ within a particular M_Z subspace can be chosen to have a positive amplitude on every basis state except for those special cases in which the qudit state on the input spin 0 does not appear in the rest of the string. For these special cases, such as the state $|31210\rangle$, which does not have a $|3\rangle$ on the any of the sites except spin 0, the amplitude of the eigenvector $|\Psi_i^{\mathrm{sym}}\rangle$ is 0. These special cases can be ignored because they are eigenvectors of R with eigenvalue $1/(d+1)$ (for

any arbitrary set of $\{\alpha_n\}$), and are hence never optimal. It is important to note that not every choice of $\left|\Phi_i^{N-1}\right\rangle$ has this property of having a positive amplitude on every basis state within the particular subspace but one can always choose the eigenvectors $\left|\Psi_i^{\mathrm{sym}}\right\rangle$ to have this property. For example, choices of $\left|\Phi_2^2\right\rangle$ could be $|11\rangle$ or $(|02\rangle+|20\rangle)/\sqrt{2}$ for $d \geq 3$, and these do not have positive amplitude on every basis state of the relevant M_Z, but there are superpositions which do.

2. Asymmetric Cloning

It is now our task to prove that the maximum eigenvector $|\Psi_i\rangle$ given in Eq. (A1) within this subspace of given i is always the maximum eigenvector of R, for arbitrary asymmetries. To do so, we are going to make use of a modified Lieb-Mattis theorem [15]. The idea behind the proof is the following: we will prove that the maximum eigenvector within a given M_Z subspace (making no restriction on S) has non-negative coefficients on all the basis states. Since (apart from the discounted special cases) $\left|\Psi_i^{\mathrm{sym}}\right\rangle$ has positive amplitudes on all these basis states, this implies that

$$\langle\Psi_i|\Psi_i^{\mathrm{sym}}\rangle > 0.$$

Therefore, the $|\Psi_i\rangle$ must be drawn from the subspace $\{|B\rangle_{0,m}\left|\Phi_i^{N-1}\right\rangle_{1,2...N\neq m}\}$, and hence must be the maximum eigenvector that we solve for in Eq. (A2).

This would successfully establish that for the subspaces $M_Z = -\frac{1}{2}(d-1)(N-1), \ldots, \frac{1}{2}(d-1)(N-1)$, we know the maximum eigenvector. The maximum eigenvector in the other subspaces cannot have a larger eigenvalue due to the following argument. If it were true that these other subspaces had an eigenvector with a larger eigenvalue, then this eigenvector must be drawn from a subspace of $S > \frac{1}{2}(d-1)(N-1)$. However, any such eigenvalue is degenerate in M_Z so it would also be present in all other M_Z subspaces from $-S$ to S, in particular in the ones in which we have already found a different maximum eigenvector. So, by contradiction, this establishes that we have the maximum eigenvalue, $F = (1+\lambda)/(d+1)$, and that it is (at least) $(d-1)(N-1)+1$ fold degenerate.

This leaves us with the task of proving that, within a given M_Z subspace, the coefficients of the maximum eigenvector are non-negative. To do so, divide R into two components, R_0 and R_1, where R_0 contains all the diagonal elements, and R_1 is the remainder. In the computational basis, $|a\rangle$, we have $\langle a| R_0 |a\rangle = e_a$ and $\langle a| R_1 |b\rangle = K_{ab}$. Note that $K_{ab} \geq 0$. Assume that in a particular excitation subspace, M_Z, we know the maximum eigenvector,

$$|\psi\rangle = \sum_a f_a |a\rangle,$$

with eigenvalue E_{M_Z}. Hence,

$$\sum_b K_{ba} f_b = (E_{M_Z} - e_a) f_a.$$

Any other state must have a smaller expectation value of R, unless it is also a maximum eigenvector. Let us first try a state $|a\rangle$ as the ansatz. This reveals $e_a \leq E_{M_Z}$. Hence, we can take the modulus of the above equation,

$$\left|\sum_b K_{ba} f_b\right| = (E_{M_Z} - e_a)|f_a|.$$

Next, we try the ansatz state

$$\left|\tilde{\psi}\right\rangle = \sum_a |f_a| |a\rangle.$$

This requires that there is at least one non-zero f_a such that

$$\sum_b K_{ba}|f_b| \leq (E_{M_Z} - e_a)|f_a|$$

but since $\sum_b K_{ba}|f_b| \geq |\sum_b K_{ba} f_b|$, this can only be satisfied with equality for every a, meaning that the coefficients of the maximum eigenvector in each M_Z subspace satisfy

$$f_a \geq 0,$$

up to a global phase factor. This completes the proof that the maximum eigenvector within a given M_Z subspace has non-negative coefficients on all the basis states. By the arguments outlined previously, this establishes that the state Eq. (A1) is the maximum eigenvector of R, the cloning fidelity being given in terms of the maximum eigenvalue λ by $F = \frac{1+\lambda}{d+1}$.