Information-theoretic limitations on approximate quantum cloning and broadcasting

Marius Lemm
Department of Mathematics, California Institute of Technology, Pasadena, California 91125, USA

Mark M. Wilde
Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

(Received 16 October 2016; published 5 July 2017)

We prove quantitative limitations on any approximate simultaneous cloning or broadcasting of mixed states. The results are based on information-theoretic (entropic) considerations and generalize the well-known no-cloning and no-broadcasting theorems. We also observe and exploit the fact that the universal cloning machine on the symmetric subspace of n qudits and symmetrized partial trace channels are dual to each other. This duality manifests itself both in the algebraic sense of adjointness of quantum channels and in the operational sense that a universal cloning machine can be used as an approximate recovery channel for a symmetrized partial trace channel and vice versa. The duality extends to give control of the performance of generalized universal quantum cloning machines (UQCMs) on subspaces more general than the symmetric subspace. This gives a way to quantify the usefulness of *a priori* information in the context of cloning. For example, we can control the performance of an antisymmetric analog of the UQCM in recovering from the loss of $n-k$ fermionic particles.

DOI: 10.1103/PhysRevA.96.012304

I. INTRODUCTION

A direct consequence of the fundamental principles of quantum theory is that a "machine" (unitary map) that can clone an arbitrary input state [1,2] does not exist. This no-cloning theorem and its generalization to mixed states, the "no-broadcasting theorem" [3], exclude the possibility of making perfect "quantum backups" of a quantum state and are essential for our understanding of quantum information processing. For instance, since decoherence is such a formidable obstacle to building a quantum computer and, at the same time, we cannot use quantum backups to protect quantum information against this decoherence, considerable effort has been devoted to protecting the stored information by way of *quantum error correction* [4–6].

Given these no-go results, it is natural to ask how well one can do when settling for *approximate* cloning or broadcasting. Numerous theoretical and experimental works have investigated such "approximate cloning machines" (see [7–16] and references therein). These cloning machines can be of great help for *state estimation*. They can also be of great help to an adversary who is eavesdropping on an encrypted communication, so knowing the limitations of approximate cloning machines is relevant for *quantum key distribution*.

In this paper, we derive *quantitative limitations* posed on any approximate cloning or broadcast (defined below) by *quantum information theory*. Our results generalize the standard no-cloning and no-broadcasting results for mixed states, which are recalled below (Theorems 1 and 2). We draw on an approach of Kalev and Hen [17], who introduced the idea of studying no broadcasting via the fundamental principle of the monotonicity of the quantum relative entropy [18,19]. When at least one state is approximately cloned while the other is approximately broadcast, we derive an inequality which implies rather strong limitations (Theorem 3). The result can be understood as a quantitative version of the standard no-cloning theorem. The proof uses only fundamental properties of the relative entropy. By invoking recent developments linking the monotonicity of relative entropy to recoverability [20–25], we can derive a stronger inequality (Theorem 4). Under certain circumstances, this stronger inequality provides an *explicit channel* which can be used to *improve the quality* of the original cloning or broadcast (roughly speaking, how close the output is to the input) *a posteriori*. This cloning- or broadcasting-improving channel is nothing but the parallel application of the rotation-averaged Petz recovery map [24], highlighting its naturalness in this context.

Related results proved in the present work (Theorems 6 and 7) compare a given state of n qudits to the maximally mixed state on the (permutation-)symmetric subspace of n qudits. We establish a duality between universal quantum cloning machines (UQCMs) [7–9] and symmetrized partial trace channels in the operational sense that a UQCM can be used as an approximate recovery channel for a symmetrized partial trace channel and vice versa. It is also immediate to observe that these channels are adjoints of each other, up to a constant. A context different from ours in which a duality between partial trace and universal cloning has been observed is in quantum data compression [26].

As a special case of Theorem 6, we recover one of the main results of Werner [9] regarding the optimal fidelity for $k \to n$ cloning of tensor-product pure states $\phi^{\otimes k}$. We also draw an analogy between these results and previous results from [27] regarding photon loss and amplification, the analogy being that cloning is like particle amplification and partial trace is like particle loss.

The methods generalize to subspaces beyond the symmetric subspace: Theorem 8 controls the performance of an analog of the UQCM in recovering from a loss of $n-k$ particles when we are given *a priori information* about the states (in the sense that we know on which subspaces they are supported, e.g., because we are working in an irreducible representation of some symmetry group). As an application of this, we obtain an estimate of the performance of an *antisymmetric* analog of the UQCM for $k \to n$ "cloning" of fermionic particles.

The methods also yield information-theoretic restrictions for general approximate *broadcasts* of two mixed states.

II. BACKGROUND

The well-known no-cloning theorem for pure states establishes that two pure states can be simultaneously cloned iff they are identical or orthogonal. It is generalized by the following two theorems, a no-cloning theorem for mixed states and a no-broadcasting theorem [3,17].

Let σ be a mixed state on a system A. By definition, a (twofold) broadcast of the input state σ is a quantum channel $\Lambda_{A\to AB}$, such that the output state

$$\rho_{AB}^{\text{out}} := \Lambda_{A\to AB}(\sigma_A)$$

has identical marginals $\rho_A^{\text{out}} = \rho_B^{\text{out}} = \sigma$.

A particular broadcast corresponds to the case $\rho_{AB}^{\text{out}} = \sigma_A \otimes \sigma_B$, which is called a *cloning* of the state σ. We call two mixed states σ_1 and σ_2 orthogonal if $\sigma_1\sigma_2 = 0$.

Theorem 1. No cloning for mixed states [3,17]. Two mixed states σ_1,σ_2 can be simultaneously cloned iff they are orthogonal or identical.

Theorem 2. No broadcasting [3]. Two mixed states σ_1,σ_2 can be simultaneously broadcast iff they commute.

By a "simultaneous" cloning or broadcast, we mean that the same choice of $\Lambda_{A\to AB}$ is made for broadcasts of σ_1 and σ_2.

These results were essentially first proved in [3], albeit under an additional minor invertibility assumption. Alternative proofs were given in [17,28–30]. Sometimes Theorem 2 is called the "universal no-broadcasting theorem" to distinguish it from local no-broadcasting results for multipartite systems [31]. Quantitative versions of the local no-broadcasting results for multipartite systems were reviewed very recently by Piani [32] (see also [16]).

No cloning and no broadcasting are also closely related to the monogamy property of entanglement via the Choi-Jamiolkowski isomorphism [29].

In this paper, we study limitations on *approximate* cloning or broadcasting, which we define as follows:

Definition 1. Approximate cloning or broadcast. Let $\sigma,\tilde{\sigma}$ be mixed states. An n-fold *approximate broadcast* of σ is a quantum channel $\Lambda_{A\to A_1\cdots A_n}$ such that the output state has identical marginals $\tilde{\sigma}$. That is, we consider the situation

$$\rho_{A_1}^{\text{out}} = \cdots = \rho_{A_n}^{\text{out}} = \tilde{\sigma}, \tag{1}$$

where $\rho_{A_1\cdots A_n}^{\text{out}} := \Lambda(\sigma_A)$. An *approximate cloning* is an approximate broadcast for which $\rho_{A_1\cdots A_n}^{\text{out}} = \tilde{\sigma}_{A_1} \otimes \cdots \otimes \tilde{\sigma}_{A_n}$. The main case of interest is $n = 2$.

Our main results give bounds on (appropriate notions of) the distance between $\tilde{\sigma}_i$ and σ_i for $i = 1,2$, given any pair of input states σ_1 and σ_2.

Conventions. The notions of approximate cloning and broadcast stated above are direct generalizations of the notions of cloning and broadcasting in the literature related to Theorems 1 and 2. Regarding the input states, these notions are more general than the one used in the cloning-machine literature [13]; we allow for the input states to be arbitrary, whereas they are usually pure tensor-power states $\psi^{\otimes n}$ for cloning machines. Our notion of approximate cloning requires the output states to be tensor-product states. Hence, some quantum cloning machines (in particular the universal cloning machine when acting on general input states) are approximate *broadcasts* by the definition given above.

Let us fix some notation. Given two mixed states ρ and σ, we denote the *relative entropy* of ρ with respect to σ by $D(\rho\|\sigma) := \text{tr}[\rho(\ln\,\rho - \ln\sigma)]$, where ln is the natural logarithm [33]. We define the fidelity by $F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2 \in [0,1]$ [34], where $\|\cdot\|_1$ is the trace norm.

Since all of our bounds involve the relative entropy $D(\sigma_1\|\sigma_2)$ of the input states σ_1 and σ_2, they are informative only when $D(\sigma_1\|\sigma_2) < \infty$. This is equivalent to $\ker\sigma_2 \subseteq \ker\sigma_1$, and we *assume* this in the following for simplicity. We note that if this assumption fails, our results can still be applied by approximating σ_2 (in trace distance) with $\sigma_2^{\varepsilon} := \varepsilon\sigma_1 + (1-\varepsilon)\sigma_2$ for $\varepsilon \in (0,1)$, which satisfies $\ker\sigma_2^{\varepsilon} \subseteq \ker\sigma_1$.

III. MAIN RESULTS

We will now present our main results. All proofs are rather short and deferred to the next section.

A. Restrictions on approximate cloning or broadcasting

Our first main result concerns limitations if σ_1 is approximately broadcast n-fold while σ_2 is approximately cloned n-fold.

Theorem 3. Limitations on approximate cloning or broadcasting. Fix two mixed states σ_1 and σ_2. Let $\Lambda_{A\to A_1\cdots A_n}$ be a quantum channel such that $n \geqslant 2$ and the two output states $\rho_{i,A_1\cdots A_n}^{\text{out}} := \Lambda(\sigma_{i,A})$ for $i = 1,2$ satisfy

$$\begin{aligned} \rho_{1,A_1}^{\text{out}} &= \cdots = \rho_{1,A_n}^{\text{out}} = \tilde{\sigma}_1, \\ \rho_{2,A_1\cdots A_n}^{\text{out}} &= \tilde{\sigma}_{2,A_1} \otimes \cdots \otimes \tilde{\sigma}_{2,A_n}. \end{aligned} \tag{2}$$

Thus, $\Lambda_{A\to A_1\cdots A_n}$ approximately broadcasts $\sigma_{1,A}$ and approximately clones $\sigma_{2,A}$. Then

$$\begin{aligned} D(\sigma_1\|\sigma_2) - D(\tilde{\sigma}_1\|\tilde{\sigma}_2) &\geqslant (n-1)D(\tilde{\sigma}_1\|\tilde{\sigma}_2) \\ &\geqslant \frac{n-1}{2}\|\tilde{\sigma}_1 - \tilde{\sigma}_2\|_1^2. \end{aligned} \tag{3}$$

The second inequality in (3) follows from the quantum Pinsker inequality (see [35], Theorem 1.15).

To see that (3) is indeed restrictive for approximate cloning or broadcasting, let $n = 2$ and suppose without loss of generality that $\sigma_1 \neq \sigma_2$, so that $\delta := \frac{1}{6}\|\sigma_1 - \sigma_2\|_1^2 > 0$. We can use the triangle inequality for $\|\cdot\|_1$ and the elementary inequality $2ab \leqslant a^2 + b^2$ on the right-hand side in (3) to get

$$D(\sigma_1\|\sigma_2) - D(\tilde{\sigma}_1\|\tilde{\sigma}_2) + \frac{\|\sigma_1 - \tilde{\sigma}_1\|_1^2}{2} + \frac{\|\sigma_2 - \tilde{\sigma}_2\|_1^2}{2} \geqslant \delta.$$

Since σ_1 and σ_2 are fixed, the same is true for $\delta > 0$. Hence, for any approximate cloning or broadcasting operation (2), at least one of the following three statements must hold: (1) σ_1 is far from $\tilde{\sigma}_1$ (i.e., the channel acts poorly on the first state), (2) σ_2 is far from $\tilde{\sigma}_2$ (i.e., the channel acts poorly on the first state), or (3) there is a large decrease in the distinguishability of the states under the action of the channel in the sense that

$D(\sigma_1\|\sigma_2) - D(\tilde{\sigma}_1\|\tilde{\sigma}_2)$ is bounded from below by a constant. Thus, we have a quantitative version of Theorem 1 [note that for $\sigma_i = \tilde{\sigma}_i$ ($i = 1,2$), Theorem 4 implies $\sigma_1 = \sigma_2$].

As anticipated in the Introduction, we can prove a stronger version of Theorem 3 by invoking recent developments linking monotonicity of the relative entropy to recoverability [20–25]. The stronger version involves an additional non-negative term on the right-hand side in (3), and it contains an additional integer parameter $m \in \{1,\dots,n\}$ (the case $m = n$ corresponds to Theorem 3; the case $m = 1$ is also useful as we explain after the theorem).

Theorem 4. Stronger version of Theorem 3. Under the same assumptions as in Theorem 3, for all $m \in \{1,\dots,n\}$, there exists a recovery channel $\mathcal{R}^{(m)}_{A_1\cdots A_m\to A}$ such that

$$D(\sigma_1\|\sigma_2) - m D(\tilde{\sigma}_1\|\tilde{\sigma}_2) \geqslant -\ln\, F\big(\sigma_1,(\mathcal{R}^{(m)}_{A_1\cdots A_m\to A}\circ \mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_1)\big). \quad (4)$$

The recovery channel $\mathcal{R}^{(m)} \equiv \mathcal{R}^{(m)}_{A_1\cdots A_m\to A}$ satisfies the identity $\sigma_2 = \mathcal{R}^{(m)}(\tilde{\sigma}_2^{\otimes m})$. There exists an explicit choice for such an $\mathcal{R}^{(m)}$ with a formula depending only on σ_2 and Λ, as can be seen from [24] or (20).

One can generalize Theorem 4 to the case of "$k \to n$ cloning" [13] where one starts from k-fold tensor copies $\sigma_1^{\otimes k}$ and $\sigma_2^{\otimes k}$ and broadcasts the former and clones the latter to states on an n-fold tensor product. That is, we have the following theorem:

Theorem 5. Consider the more general situation in which we begin with $k \leqslant n$ tensor-product copies of the state σ_i for $i \in \{1,2\}$, and suppose that the channel $\Lambda_{A_1\cdots A_k\to A_1\cdots A_n}$ approximately broadcasts σ_1, in the sense that

$$\mathrm{tr}_{A_1\cdots A_n\setminus A_j}\left[\Lambda_{A_1\cdots A_k\to A_1\cdots A_n}\left(\sigma_1^{\otimes k}\right)\right] = \tilde{\sigma}_1,$$

and approximately clones σ_2, in the sense that

$$\Lambda_{A_1\cdots A_k\to A_1\cdots A_n}\left(\sigma_2^{\otimes k}\right) = \tilde{\sigma}_2^{\otimes n}.$$

Then, for every $m \in \{1,\dots,n\}$, there exists a recovery channel $\mathcal{R}^{(m,k)}_{A_1\cdots A_m\to A_1\cdots A_k}$ such that

$$k D(\sigma_1\|\sigma_2) - m D(\tilde{\sigma}_1\|\tilde{\sigma}_2) \geqslant -\ln\, F\big(\sigma_1,(\mathcal{R}^{(m,k)}_{A_1\cdots A_m\to A_1\cdots A_k}\circ \mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)\left(\sigma_1^{\otimes k}\right)\big),$$

and the recovery channel $\mathcal{R}^{(m,k)}_{A_1\cdots A_m\to A_1\cdots A_k}$ satisfies

$$\sigma_2^{\otimes k} = \mathcal{R}^{(m,k)}_{A_1\cdots A_m\to A_1\cdots A_k}\left(\tilde{\sigma}_2^{\otimes m}\right).$$

To see how the additional remainder term in (4) can be useful, we apply Theorem 4 with $m = 1$. It implies that there exists a recovery channel $\mathcal{R}^{(1)}$ such that

$$D(\sigma_1\|\sigma_2) - D(\tilde{\sigma}_1\|\tilde{\sigma}_2) \geqslant -\ln F(\sigma_1,\mathcal{R}^{(1)}(\tilde{\sigma}_1)), \qquad \sigma_2 = \mathcal{R}^{(1)}(\tilde{\sigma}_2). \quad (5)$$

Now suppose that we are in a situation where the left-hand side in (5) is less than some $\varepsilon > 0$. Then, (5) implies that $\sigma_1 \approx \mathcal{R}^{(1)}(\tilde{\sigma}_1)$ and $\sigma_2 = \mathcal{R}^{(1)}(\tilde{\sigma}_2)$, where $\approx$ stands for $-\ln F(\sigma_1,\mathcal{R}^{(1)}(\tilde{\sigma}_1)) < \varepsilon$. In other words, we can (approximately) recover the input states σ_i from the output marginals $\tilde{\sigma}_i$. Therefore, in the next step, we can improve the quality of the cloning or broadcasting channel Λ by postcomposing it with n parallel uses of the local recovery channel $\mathcal{R}^{(1)}$. Indeed, the *improved cloning channel* $\Lambda_{\mathrm{impr}} := (\mathcal{R}^{(1)})^{\otimes n}\circ\Lambda$ has the new output states $\rho^{\mathrm{impr}}_{i,A_1\dots A_n} := \Lambda_{\mathrm{impr}}(\sigma_i)$ ($i = 1,2$), which satisfy

$$\rho^{\mathrm{impr}}_{1,A_1} = \cdots = \rho^{\mathrm{impr}}_{1,A_n} = \mathcal{R}^{(1)}(\tilde{\sigma}_1) \approx \sigma_1,$$
$$\rho^{\mathrm{impr}}_{2,A_1\cdots A_n} = \sigma_{2,A_1}\otimes\cdots\otimes\sigma_{2,A_n}.$$

Here, $\approx$ again stands for $-\ln F(\sigma_1,\mathcal{R}^{(1)}(\tilde{\sigma}_1)) < \varepsilon$.

That is, we have found a strategy to improve the output of the cloning channel Λ, namely, to the output of Λ_{impr}.

B. Universal cloning machines and symmetrized partial trace channels

In our next results, we consider a particular example of an approximate broadcasting channel well known in quantum information theory [9,11,13], a universal quantum cloning machine. We connect the UQCM to relative entropy and recoverability.

We recall that the UQCM is the optimal cloner for tensor-power pure states in the sense that the marginal states of its output have optimal fidelity with the input state [9,11]. Let k and n be integers such that $1 \leqslant k \leqslant n$. In general, one considers a $k \to n$ UQCM as acting on k copies $\psi^{\otimes k}$ of an input pure state ψ of dimension d (a qudit), which produces an output density operator $\rho^{(n)}$, a state of n qudits. From Werner's work [9], the UQCM is known to be

$$\mathcal{C}_{k\to n}(\omega^{(k)}) \equiv \frac{d[k]}{d[n]}\Pi^{d,n}_{\mathrm{sym}}\big[\Pi^{d,k}_{\mathrm{sym}}\omega^{(k)}\Pi^{d,k}_{\mathrm{sym}}\otimes I^{n-k}\big]\Pi^{d,n}_{\mathrm{sym}}. \quad (6)$$

Here $\Pi^{d,n}_{\mathrm{sym}}$ is the projection onto the (permutation-)symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$, which has dimension $d[n] := \binom{d+n-1}{n}$. We note that $\mathcal{C}_{k\to n}$ is trace preserving when acting on the symmetric subspace.

The main results here are Theorems 6 and 7, which highlight the duality between the UQCM (6) and the following symmetrized partial trace channel:

$$\mathcal{P}_{n\to k}(\cdot) \equiv \Pi^{d,k}_{\mathrm{sym}}\,\mathrm{tr}_{n\to k}\big[\Pi^{d,n}_{\mathrm{sym}}(\cdot)\Pi^{d,n}_{\mathrm{sym}}\big]\Pi^{d,k}_{\mathrm{sym}}. \quad (7)$$

In addition to the operational sense of duality between the partial trace channel $\mathcal{P}_{n\to k}$ and the UQCM $\mathcal{C}_{k\to n}$ which is established by Theorems 6 and 7, the two are dual in the sense of quantum channels (up to a constant). That is, $\mathcal{P}^{\dagger}_{n\to k} = (d[n]/d[k])\mathcal{C}_{k\to n}$.

Our results will quantify the quality of the UQCM for certain tasks in terms of the relative entropy $D(\omega^{(n)}\|\pi^{d,n}_{\mathrm{sym}})$, which is between a general n-qudit state $\omega^{(n)}$ and the maximally mixed state $\pi^{d,n}_{\mathrm{sym}}$ of the symmetric subspace. We consider the maximally mixed state $\pi^{d,n}_{\mathrm{sym}}$ as a natural "origin" from which to measure the "distance" $D(\omega^{(n)}\|\pi^{d,n}_{\mathrm{sym}})$ since it is a (Haar-)random mixture of tensor-power pure states.

We recall what one obtains from the standard monotonicity of the relative entropy, namely,

$$D\big(\omega^{(n)}\big\|\pi^{d,n}_{\mathrm{sym}}\big) \geqslant D\big(\mathcal{P}_{n\to k}(\omega^{(n)})\big\|\mathcal{P}_{n\to k}\big(\pi^{d,n}_{\mathrm{sym}}\big)\big). \quad (8)$$

Our next main result is the following strengthening of the entropy inequality in (8):

Theorem 6. Let $\omega^{(n)}$ be a state with support in the symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$, let $\pi^{d,n}_{\mathrm{sym}}$ denote the maximally mixed state on this symmetric subspace, let $\mathcal{C}_{k\to n}$ denote the UQCM from (6), and let $\mathcal{P}_{n\to k}$ be the symmetrized partial trace channel from (7). Then

$$D\big(\omega^{(n)}\big\|\pi_{\rm sym}^{d,n}\big) \geqslant D\big(\mathcal{P}_{n\to k}(\omega^{(n)})\|\mathcal{P}_{n\to k}\big(\pi_{\rm sym}^{d,n}\big)\big) + D(\omega^{(n)}\|(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\omega^{(n)})). \quad (9)$$

The entropy inequality in (9) can be interpreted as follows: The ability of a $k\to n$ UQCM to recover an n-qubit state $\omega^{(n)}$ from the loss of $n-k$ particles is limited by the decrease of distinguishability between $\omega^{(n)}$ and $\pi_{\rm sym}^{d,n}$ under the action of the partial trace $\mathcal{P}_{n\to k}$. Thus, a small decrease in relative entropy [i.e., $D(\omega^{(n)}\|\pi_{\rm sym}^{d,n}) - D(\mathcal{P}(\omega^{(n)})\|\mathcal{P}(\pi_{\rm sym}^{d,n}))\approx\varepsilon$] implies that a $k\to n$ UQCM $\mathcal{C}_{k\to n}$ will perform well at recovering $\omega^{(n)}$ from $\mathcal{P}_{n\to k}(\omega^{(n)})$. We can also observe that $\mathcal{C}_{k\to n}$ is the Petz recovery map corresponding to the state $\sigma=\pi_{\rm sym}^{d,n}$ and channel $\mathcal{N}=\mathrm{tr}_{n\to k}$, as defined in (20).

As an application of Theorem 6, we consider the special case that is most common in the context of quantum cloning [9,11,13]. We set $\omega^{(n)}=\phi^{\otimes n}$ for a pure state ϕ. In this case,

$$D\big(\phi^{\otimes n}\big\|\pi_{\rm sym}^{d,n}\big) - D\big(\mathcal{P}_{n\to k}(\phi^{\otimes n})\big\|\mathcal{P}_{n\to k}\big(\pi_{\rm sym}^{d,n}\big)\big) = -\ln(d[k]/d[n]) \geqslant D(\phi^{\otimes n}\|\mathcal{C}_{k\to n}(\phi^{\otimes k})). \quad (10)$$

By estimating $D\geqslant -\ln F$, we recover one of the main results of [9], which is that the $k\to n$ UQCM has the following performance when attempting to recover n copies of ϕ from k copies:

$$F(\phi^{\otimes n},\mathcal{C}_{k\to n}(\phi^{\otimes k}))\geqslant d[k]/d[n]. \quad (11)$$

Given the above duality between the symmetrized partial trace channel and the UQCM, we can also consider the reverse scenario.

Theorem 7. With the same notation as in Theorem 6, the following inequality holds:

$$D\big(\omega^{(k)}\big\|\pi_{\rm sym}^{d,k}\big) \geqslant D\big(\mathcal{C}_{k\to n}(\omega^{(k)})\big\|\mathcal{C}_{k\to n}\big(\pi_{\rm sym}^{d,k}\big)\big) + D(\omega^{(k)}\|(\mathcal{P}_{n\to k}\circ\mathcal{C}_{k\to n})(\omega^{(k)})). \quad (12)$$

This entropy inequality can be seen as dual to that in (9), having the following interpretation: if the decrease in distinguishability of $\omega^{(k)}$ and $\pi_{\rm sym}^{d,k}$ is small under the action of a UQCM $\mathcal{C}_{k\to n}$, then the partial trace channel $\mathcal{P}_{n\to k}$ can perform well at recovering the original state $\omega^{(k)}$ back from the cloned version $\mathcal{C}_{k\to n}(\omega^{(k)})$.

C. On photon amplification and loss

There is a striking similarity between the inequalities in (9) and (12) and those from Sec. III A of [27], which apply to photonic channels (cf. [36]). This observation is based on the analogy that cloning is like particle amplification and partial trace is like particle loss.

The partial trace channel is like particle loss, which for photons is represented by a pure-loss channel $\mathcal{L}_\eta$ with transmissivity $\eta\in[0,1]$. Furthermore, a UQCM is like particle amplification, which for bosons is represented by an amplifier channel $\mathcal{A}_G$ of gain $G\geqslant 1$. Let θ_E denote a thermal state of mean photon number $E\geqslant 0$, and let ρ denote a state of the same energy E. A slight rewriting of the inequalities from Sec. III A of [27], given below, results in the following:

$$D(\rho\|\theta_E) \gtrsim D(\mathcal{L}_\eta(\rho)\|\mathcal{L}_\eta(\theta_E)) + D(\rho\|(\mathcal{A}_{1/\eta}\circ\mathcal{L}_\eta)(\rho)), \quad (13)$$

$$D(\rho\|\theta_E) \geqslant D(\mathcal{A}_G(\rho)\|\mathcal{A}_G(\theta_E)) + D(\rho\|(\mathcal{L}_{1/G}\circ\mathcal{A}_G)(\rho)), \quad (14)$$

where the symbol $\gtrsim$ indicates that the entropy inequality holds up to a term with magnitude no larger than $\ln(1/\eta)$ which approaches zero as $E\to\infty$. So we see that (13) is analogous to (9): under a particle loss $\mathcal{L}_\eta$, we can apply a particle amplification procedure $\mathcal{A}_{1/\eta}$ to try and recover the lost particles, with a performance controlled by (13). Similarly, (14) is analogous to (12): under a particle amplification $\mathcal{A}_G$, we can apply a particle loss channel $\mathcal{L}_{1/G}$ to try and recover the original state, with a performance controlled by (14). Observe that the parameters specifying the recovery channels are directly related to the parameters of the original channels, just like the case in (9) and (12). Note that an explicit connection between cloning and amplifier channels was established in [36], and our result serves to complement that connection.

D. Restrictions on cloning in general subspaces

We can generalize the discussion in the previous section to arbitrary subspaces. For $1\leqslant k\leqslant n$, let X_n be a d_{X_n}-dimensional subspace of $(\mathbb{C}^d)^{\otimes n}$ and let Y_k be a d_{Y_k}-dimensional subspace of $(\mathbb{C}^d)^{\otimes k}$. We write Π_{X_n} and Π_{Y_k} for the projections onto these subspaces and π_{X_n} and π_{Y_k} for the corresponding maximally mixed states. We generalize the definitions in (6) and (7) to

$$\mathcal{C}_{k\to n}(\cdot)\equiv\frac{d_{Y_k}}{d_{X_n}}\Pi_{X_n}\big[\Pi_{Y_k}(\cdot)\Pi_{Y_k}\otimes I^{n-k}\big]\Pi_{X_n}, \quad (15)$$

$$\mathcal{P}_{n\to k}(\cdot)\equiv\Pi_{Y_k}\,\mathrm{tr}_{n\to k}\big[\Pi_{X_n}(\cdot)\Pi_{X_n}\big]\Pi_{Y_k}. \quad (16)$$

For definiteness, the partial trace $\mathrm{tr}_{n\to k}$ is taken over the last $n-k$ qudits. The cloning map $\mathcal{C}_{k\to n}$ is a direct analog of the UQCM for the specialized task of recovering a state in the subspace X_n from one in the subspace Y_k (previously, X_n and Y_k were both taken to be the symmetric subspace). By inspection, it is completely positive, and if $\mathrm{tr}_{n\to k}[\pi_{X_n}]=\pi_{Y_k}$, then it is trace preserving when acting on any operator with support in X_n.

The same argument that proves Theorem 6 then gives the following:

Theorem 8. Let $\omega^{(n)}$ be a state with support in X_n, and suppose that $\mathrm{tr}_{n\to k}[\omega^{(n)}]$ is supported in Y_k. Then

$$D\big(\omega^{(n)}\big\|\pi_{X_n}\big)\geqslant D\big(\mathcal{P}_{n\to k}(\omega^{(n)})\|\pi_{Y_k}\big) + D(\omega^{(n)}\|(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\omega^{(n)})). \quad (17)$$

The assumption that $\mathrm{tr}_{n\to k}[\omega^{(n)}]$ is supported in Y_k is made for convenience. Without it, the quantity $\mathrm{tr}[\mathcal{P}_{n\to k}(\omega^{(n)})]<1$ would enter in the statement, as can be seen from the proof in the next section. We can obtain a stronger statement under the additional assumption $\mathrm{tr}_{n\to k}[\pi_{X_n}]=\pi_{Y_k}$: it implies $\mathcal{P}_{n\to k}(\pi_{X_n})=\pi_{Y_k}$ and that $(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\omega^{(n)})$ has trace 1.

Theorem 8 controls the performance of the cloning machine $\mathcal{C}_{k\to n}$ (15) in recovering from a loss of $n-k$ particles when *a* *priori* information about the states is given (in the sense that we know on which subspaces they are supported). To see this, consider, e.g., the case of perfect *a priori* information when $\dim X_n = 1$. Then $D(\omega^{(n)}\|\pi_{X_n}) = 0$, so (17) implies that the cloning is perfect, $\omega^{(n)} = (\mathcal{C}_{k\to n} \circ \mathcal{P}_{n\to k})(\omega^{(n)})$.

For nontrivial applications of Theorem 8, a natural class of subspaces to consider is those associated with irreducible group representations, e.g., of the permutation group acting on $(\mathbb{C}^d)^{\otimes n}$. To avoid introducing the representation-theoretic background, we focus here on the case when both X_n and Y_k are taken to be the familiar *antisymmetric* subspace. Physically, the antisymmetric subspace describes fermions, and therefore, our results have bearing on electronic analogs of the photonic scenarios mentioned above.

For this part, we let $d \geqslant n$. An example system for which d can be larger than n is a tight-binding model on d lattice sites, where each site can host a single electron. The antisymmetric subspace X_n has dimension $d_{X_n} = \binom{d}{n}$. The analog of a tensor-power pure state in the antisymmetric subspace is a *Slater determinant* $|\Phi_n\rangle \equiv |\phi_1\rangle \wedge \cdots \wedge |\phi_n\rangle$, where the states $\{|\phi_i\rangle\}_i$ are orthonormal. Appendices A and B review the background and how the marginal $\mathrm{tr}_{n\to k}[\Phi_n]$ is again antisymmetric and has quantum entropy $\ln\binom{n}{k}$. Thus, (17) in Theorem 8 applies to establish the first inequality of the following:

$$\ln\binom{d-k}{d-n} = -\ln\left\{\binom{d}{k}\cdot\left[\binom{n}{k}\binom{d}{n}\right]^{-1}\right\} \geqslant D(\Phi_n\|(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\Phi_n)). \quad (18)$$

Using $D \geqslant -\ln F$ again, we conclude that the performance of the antisymmetric cloning machine $\mathcal{C}_{k\to n}$ in recovering from a loss of $n-k$ fermionic particles is controlled by

$$F(\Phi_n,(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\Phi_n)) \geqslant \left[\binom{d-k}{d-n}\right]^{-1}. \quad (19)$$

We mention that $(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\Phi_n)$ has trace 1; this follows from the identity $\mathrm{tr}_{n\to k}[\pi_{X_n}] = \pi_{Y_k}$ for the antisymmetric subspace (see Lemma 2 in Appendix B). We also mention that the standard symmetric UQCM would produce the zero state in this case and thus yields a (minimal) fidelity of zero.

E. General restrictions on approximate broadcasts

As the Introduction mentioned, our methods imply information-theoretic restrictions on any approximate twofold broadcast. These are relegated to Appendix C.

IV. PROOFS OF THE MAIN RESULTS

An important tool for us will be the lower bound from [24] on the decrease of the relative entropy for a quantum channel $\mathcal{N}$ and states ρ and σ:

Theorem 9 [24]. Let $\beta(t) := \frac{\pi}{2}[1+\cosh(\pi t)]^{-1}$. For any two quantum states ρ,σ and a channel $\mathcal{N}$, the following bound holds:

$$D(\rho\|\sigma) \geqslant D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) - \int_{\mathbb{R}} \ln\, F\big(\rho,\mathcal{R}^t_{\mathcal{N},\sigma}(\mathcal{N}(\rho))\big)\, d\beta(t),$$

where the rotated Petz recovery map $\mathcal{R}^t_{\mathcal{N},\sigma}$ is defined as

$$\mathcal{R}^t_{\mathcal{N},\sigma}(\cdot) := \sigma^{\frac{1+it}{2}}\mathcal{N}^\dagger\big\{[\mathcal{N}(\sigma)]^{-\frac{1+it}{2}}(\cdot)[\mathcal{N}(\sigma)]^{-\frac{1-it}{2}}\big\}\sigma^{\frac{1-it}{2}}, \quad (20)$$

where $\mathcal{N}^\dagger$ is the completely positive, unital adjoint of the channel $\mathcal{N}$. Every rotated Petz recovery map perfectly recovers σ from $\mathcal{N}(\sigma)$:

$$\mathcal{R}^t_{\mathcal{N},\sigma}(\mathcal{N}(\sigma)) = \sigma.$$

In the special case when the applied quantum channel is the partial trace, the inequality becomes the following:

Theorem 10 [24]. Let $\beta(t) := \frac{\pi}{2}[1+\cosh(\pi t)]^{-1}$. For any two quantum states ρ_{AB},σ_{AB}, we have

$$D(\rho_{AB}\|\sigma_{AB}) \geqslant D(\rho_B\|\sigma_B) - \int_{\mathbb{R}} \ln\, F\big(\rho_{AB},\mathcal{R}^t_{A,\sigma}(\rho_B)\big)\, d\beta(t),$$

where the rotated Petz recovery map $\mathcal{R}^t_{A,X}$ is defined in (C4).

We are now ready to give the proof of Theorems 3 and 4.

Proof of Theorems 3 and 4. Theorem 3 follows from the $m=n$ case of Theorem 4. Hence, it suffices to prove Theorem 4. We start by noting the following general inequality that holds for states ω and τ, a channel $\mathcal{N}$, and a recovery channel $\mathcal{R}$:

$$D(\omega\|\tau) - D(\mathcal{N}(\omega)\|\mathcal{N}(\tau)) \geqslant -\ln F(\omega,(\mathcal{R}\circ\mathcal{N})(\omega)), \quad (21)$$

$$\tau = (\mathcal{R}\circ\mathcal{N})(\tau), \quad (22)$$

which is a consequence of convexity of $-\ln$ and the fidelity applied to Theorem 9, taking

$$\mathcal{R} := \int_{\mathbb{R}} \mathcal{R}^t_{\mathcal{N},\tau}\, d\beta(t), \quad (23)$$

with $\mathcal{R}^t_{\mathcal{N},\tau}$ as in Theorem 9. To get the inequality, we take $\omega = \sigma_1$, $\tau = \sigma_2$, and $\mathcal{N} = \mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda$. This then gives the inequality

$$D(\sigma_1\|\sigma_2) - D\big((\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_1)\big\|(\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_2)\big) \geqslant -\ln F\big(\sigma_1,(\mathcal{R}^{(m)}_{A_1\cdots A_n\to A}\circ\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_1)\big),$$

where the recovery channel $\mathcal{R}^{(m)}_{A_1\cdots A_n\to A}$ satisfies

$$\sigma_2 = \big(\mathcal{R}^{(m)}_{A_1\cdots A_n\to A}\circ\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda\big)(\sigma_2) = \mathcal{R}^{(m)}_{A_1\cdots A_n\to A}\big(\tilde{\sigma}_2^{\otimes m}\big).$$

Next, we prove that

$$-D\big((\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_1)\big\|(\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_2)\big) \leqslant -mD(\tilde{\sigma}_1\|\tilde{\sigma}_2).$$

We apply $\ln(X\otimes Y) = \ln X\otimes I + I\otimes \ln Y$ and set $H(X) := -\mathrm{tr}[X\ln X]$ to get

$$\begin{aligned}
&-D\big((\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_1)\big\|(\mathrm{tr}_{A_{m+1}\cdots A_n}\circ\Lambda)(\sigma_2)\big)\\
&= -D\big(\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\big\|\tilde{\sigma}_{2,A_1}\otimes\cdots\otimes\tilde{\sigma}_{2,A_m}\big)\\
&= H\big(\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\big) + \mathrm{tr}\big[\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\ln\big(\tilde{\sigma}_{2,A_1}\otimes\cdots\otimes\tilde{\sigma}_{2,A_m}\big)\big]\\
&= H\big(\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\big)\\
&\quad + \sum_{k=1}^m \mathrm{tr}\big\{\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\big[I_{A_1\cdots A_m\setminus A_k}\otimes\ln\big(\tilde{\sigma}_{2,A_k}\big)\big]\big\}.
\end{aligned}$$

Recall our assumption from (2) that the channel broadcasts σ_1 to $\tilde{\sigma}_1$. It gives for every $1 \leqslant k \leqslant m$

$$\mathrm{tr}\left\{\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\left[I_{A_1\cdots A_m\setminus A_k}\otimes \ln\left(\tilde{\sigma}_{2,A_k}\right)\right]\right\} = \mathrm{tr}[\tilde{\sigma}_1 \ln \tilde{\sigma}_2].$$

By the subadditivity of the entropy H and (2), we obtain

$$H\left(\rho^{\mathrm{out}}_{1,A_1\cdots A_m}\right) + m\,\mathrm{tr}[\tilde{\sigma}_1 \ln \tilde{\sigma}_2] \leqslant \sum_{k=1}^{m} H\left(\rho^{\mathrm{out}}_{1,A_k}\right) + m\,\mathrm{tr}[\tilde{\sigma}_1 \ln \tilde{\sigma}_2] = -mD(\tilde{\sigma}_1\|\tilde{\sigma}_2). \quad (24)$$

This proves Theorem 4. ■

The more general version, Theorem 5, can be proved along the same lines. We leave the details to the reader.

Next, we give the proof of Theorem 6.

Proof of Theorem 6. We observe that $\pi^{d,k}_{\mathrm{sym}} = \mathrm{tr}_{n\to k}[\pi^{d,n}_{\mathrm{sym}}]$, which follows easily from the representation $\pi^{d,n}_{\mathrm{sym}} = \int d\psi\ \psi^{\otimes n}$ [37], with the integral being with respect to the Haar probability measure over pure states ψ.

A proof of (9) then follows from a few key steps:

$$\begin{aligned}
&D\big(\omega^{(n)}\big\|\pi^{d,n}_{\mathrm{sym}}\big) - D\big(\mathcal{P}_{n\to k}(\omega^{(n)})\big\|\mathcal{P}_{n\to k}\big(\pi^{d,n}_{\mathrm{sym}}\big)\big)\\
&\quad= -H(\omega^{(n)}) - \mathrm{tr}\left[\omega^{(n)}\ln \pi^{d,n}_{\mathrm{sym}}\right] + H(\mathcal{P}_{n\to k}(\omega^{(n)}))\\
&\qquad+ \mathrm{tr}\left[\mathcal{P}_{n\to k}(\omega^{(n)})\ln \pi^{d,k}_{\mathrm{sym}}\right] \quad (25)\\
&\quad= H(\mathcal{P}_{n\to k}(\omega^{(n)})) - H(\omega^{(n)}) - \ln(d[k]/d[n])\\
&\quad\geqslant D(\omega^{(n)}\|(\mathcal{P}^{\dagger}_{n\to k}\circ\mathcal{P}_{n\to k})(\omega^{(n)})) - \ln(d[k]/d[n])\\
&\quad= D(\omega^{(n)}\|(\mathcal{C}_{k\to n}\circ\mathcal{P}_{n\to k})(\omega^{(n)})). \quad (26)
\end{aligned}$$

The first equality holds by definition of quantum relative entropy, and in the second equality we used the fact that $\mathrm{tr}[\mathcal{P}_{n\to k}(\omega^{(n)})] = \mathrm{tr}[\mathrm{tr}_{n\to k}(\omega^{(n)})] = \mathrm{tr}[\omega^{(n)}] = 1$, wherein the first step holds because $\mathrm{tr}_{n\to k}[\omega^{(n)}]$ is supported in the symmetric subspace. The inequality above is a consequence of Theorem 1 in [27], which states that

$$H(\mathcal{N}(\rho)) - H(\rho) \geqslant D(\rho\|(\mathcal{N}^{\dagger}\circ\mathcal{N})(\rho)) \quad (27)$$

for any state ρ and positive, trace-preserving map $\mathcal{N}$. (We remark that $\mathcal{P}_{n\to k}$ is indeed trace preserving when considered as a map on states supported on the symmetric subspace.) The last equality in (26) follows from the property of relative entropy that $D(\xi\|\tau) - \ln\ c = D(\xi\|c\tau)$ for states ξ,τ and $c > 0$. ■

Essentially the same argument, with minor modifications, also proves Theorems 7 and 8. For the former, we use the facts that $\mathcal{C}_{k\to n}(\pi^{d,k}_{\mathrm{sym}}) = \pi^{d,n}_{\mathrm{sym}}$ and $\mathcal{C}_{k\to n}$ is trace preserving when acting on states supported in the symmetric subspace. For Theorem 8, we use the assumption that $\mathrm{tr}_{n\to k}[\omega^{(n)}]$ is supported in Y_k to get $\mathrm{tr}[\mathcal{P}_{n\to k}(\omega^{(n)})] = 1$. The details are left to the reader.

Finally, we come to the following proof:

Proof of (13) *and* (14). A proof of (13) is as follows. The Hamiltonian here is $a^{\dagger}a$, which is the photon number operator. Let ρ be a state of energy E, and let θ_E be a thermal state of energy E (i.e., $\langle a^{\dagger}a\rangle_{\rho} = \langle a^{\dagger}a\rangle_{\theta_E} = E$). Under the action of a pure-loss channel $\mathcal{L}_{\eta}$, the energies of $\mathcal{L}_{\eta}(\rho)$ and $\mathcal{L}_{\eta}(\theta_E)$ are equal to ηE, and we also find that $\mathcal{L}_{\eta}(\theta_E) = \theta_{\eta E}$. Furthermore, a standard calculation gives $-\mathrm{tr}[\rho\ln\theta_E] = H(\theta_E) = g(E) := (E+1)\ln(E+1) - E\ln E$. Putting this together, we find that

$$\begin{aligned}
&D(\rho\|\theta_E) - D(\mathcal{L}_{\eta}(\rho)\|\mathcal{L}_{\eta}(\theta_E))\\
&\quad= H(\mathcal{L}_{\eta}(\rho)) - H(\rho) + g(E) - g(\eta E)\\
&\quad\geqslant D(\rho\|(\mathcal{A}_{1/\eta}\circ\mathcal{L}_{\eta})(\rho)) - \ln(1/\eta) + g(E) - g(\eta E).
\end{aligned}$$

The first equality is a rewrite using what we mentioned above, and the inequality follows from Sec. III A of [27]. When $E = 0$, $g(E) - g(\eta E) = 0$ also. As E gets larger, $g(E) - g(\eta E)$ monotonically increases and reaches its maximum of $\ln(1/\eta)$ as $E\to\infty$.

The other inequality in (14) for an amplifier channel follows similarly. Under the action of an amplifier channel $\mathcal{A}_G$, the energies of $\mathcal{A}_G(\rho)$ and $\mathcal{A}_G(\theta_E)$ are GE. We also find that $\mathcal{A}_G(\theta_E) = \theta_{GE}$. Proceeding as above, we find that

$$\begin{aligned}
&D(\rho\|\theta_E) - D(\mathcal{A}_G(\rho)\|\mathcal{A}_G(\theta_E))\\
&\quad= H(\mathcal{A}_G(\rho)) - H(\rho) + g(E) - g(GE)\\
&\quad\geqslant D(\rho\|(\mathcal{L}_{1/G}\circ\mathcal{A}_G)(\rho)) + \ln G - [g(GE) - g(E)]\\
&\quad\geqslant D(\rho\|(\mathcal{L}_{1/G}\circ\mathcal{A}_G)(\rho)).
\end{aligned}$$

The first equality is a rewrite, and the inequality follows from Sec. III A of [27]. The last inequality follows because $g(GE) - g(E) = 0$ at $E = 0$, and it monotonically increases as a function of E, reaching its maximum value of $\ln G$ as $E\to\infty$. ■

We close this proof section with a remark on a so far implicit assumption.

Remark 1. Nonidentical marginals case. Some of our results, Theorems 3, 4, and 11 (see below), apply to approximate clonings and broadcasts in the sense of Definition 1. That is, we always assume that the marginals of the output state are identical, i.e.,

$$\rho^{\mathrm{out}}_{i,A_1} = \cdots = \rho^{\mathrm{out}}_{i,A_n} = \tilde{\sigma}_i \quad (i = 1,2). \quad (28)$$

We make this assumption for two reasons: (1) It simplifies the bounds in our main results, and (2) we believe that it is a natural assumption for approximate cloning and broadcasting. However, the methods apply more generally, and they also yield limitations on approximate clonings and broadcasts when (28) is not satisfied.

V. CONCLUSION

In this paper, we have proven several entropic inequalities that pose limitations on the kinds of approximate clonings and broadcasts that are allowed in quantum information processing. Some of the results generalize the well-known no-cloning and no-broadcasting results, restated in Theorems 1 and 2. Other results demonstrate how universal cloning machines and partial trace channels are dual to each other in the sense that one can be used as an approximate recovery channel for the other, with a performance controlled by entropy inequalities. We can also control the performance of an analog of the UQCM for cloning between any two subspaces. In particular, we obtain bounds on its performance in recovering from a loss of $n-k$ fermionic particles.

Note added. Recently, we learned of the related and concurrent work of Marvian and Lloyd [38]. We are grateful to them for passing their manuscript along to us.

ACKNOWLEDGMENTS

We acknowledge discussions with S. Chatterjee and K. Seshadreesan. M.M.W. acknowledges support from the NSF under Award No. 1350397.

APPENDIX A: REDUCTIONS OF SLATER DETERMINANTS AND THEIR QUANTUM ENTROPY

Here we prove the fact that the quantum entropy of the marginal $\mathrm{tr}_{n\to k}[\Phi_n]$ is $\ln\binom{n}{k}$ when Φ_n is a Slater determinant. We can conclude this directly from expression (A4) for the marginal derived below.

Before beginning, let us suppose that $\{|\phi_j\rangle\}_{j=1}^d$ is an orthonormal basis for a d-dimensional Hilbert space $\mathcal{H}$. Letting $d \geqslant n$, a Slater determinant state Φ_n corresponding to this basis and a subset $\{1,\dots,n\}$ is as follows:

$$|\Phi_n\rangle := |\phi_1\rangle \wedge \cdots \wedge |\phi_n\rangle \tag{A1}$$

$$:= \frac{1}{\sqrt{n!}} \sum_{\pi\in S_n} \mathrm{sgn}(\pi)|\phi_{\pi(1)}\rangle \otimes \cdots \otimes |\phi_{\pi(n)}\rangle, \tag{A2}$$

where S_n is the set of all permutations of $\{1,\dots,n\}$ and $\mathrm{sgn}(\pi)$ denotes its signum. Note that we chose the subset $\{1,\dots,n\}$ of $\{1,\dots,d\}$, but without loss of generality we could have chosen an arbitrary one.

Formula (A4) below is surely well known. We include an elementary, but slightly tedious, proof for completeness.

Lemma 1. Marginal of a Slater determinant. Let $d \geqslant n$ and $|\Phi_n\rangle = |\phi_1\rangle \wedge \cdots \wedge |\phi_n\rangle$, with $\{|\phi_j\rangle\}_{j=1}^d$ being an orthonormal basis. A k set A_k is a subset of $\{1,\dots,n\}$ consisting of exactly k elements. For any k set $A_k = \{i_1,\dots,i_k\}$, we define

$$\big|\Phi_{A_k}\big\rangle\big\langle\Phi_{A_k}\big| := \big(\big|\phi_{i_1}\big\rangle \wedge \cdots \wedge \big|\phi_{i_k}\big\rangle\big)\big(\big\langle\phi_{i_1}\big| \wedge \cdots \wedge \big\langle\phi_{i_k}\big|\big). \tag{A3}$$

Then

$$\mathrm{tr}_{n\to k}[|\Phi_n\rangle\langle\Phi_n|] = \frac{1}{\binom{n}{k}} \sum_{A_k\ k-\mathrm{set}} \big|\Phi_{A_k}\big\rangle\big\langle\Phi_{A_k}\big|. \tag{A4}$$

The orthonormality of the states $\{|\Phi_{A_k}\rangle\}$ for fixed k then implies that $H(\mathrm{tr}_{n\to k}|\Phi_n\rangle\langle\Phi_n|) = \ln\binom{n}{k}$, where $H(\rho) = -\mathrm{tr}[\rho\ln\rho]$ is the quantum entropy.

Proof. By definition of the wedge product, we can write $|\Phi_n\rangle\langle\Phi_n|$ as

$$|\Phi_n\rangle\langle\Phi_n| = \frac{1}{n!}\sum_{\pi,\sigma\in S_n} \mathrm{sgn}(\pi\circ\sigma)|\phi_{\pi(1)}\rangle\langle\phi_{\sigma(1)}| \otimes \cdots \otimes |\phi_{\pi(n)}\rangle\langle\phi_{\sigma(n)}|.$$

Here we used the fact that sgn is a group homomorphism, i.e., that $\mathrm{sgn}(\pi\circ\sigma) = \mathrm{sgn}(\pi)\mathrm{sgn}(\sigma)$ for any two permutations π and σ. Taking the partial trace over the last $n-k$ systems yields the following:

$$\begin{aligned}\mathrm{tr}_{n\to k}&[|\Phi_n\rangle\langle\Phi_n|]\\ &= \frac{1}{n!}\sum_{\pi,\sigma\in S_n} \mathrm{sgn}(\pi\circ\sigma)|\phi_{\pi(1)}\rangle\langle\phi_{\sigma(1)}| \otimes \cdots \otimes |\phi_{\pi(k)}\rangle\langle\phi_{\sigma(k)}|\\ &\quad\times \delta_{\pi(k+1),\sigma(k+1)}\cdots\delta_{\pi(n),\sigma(n)}.\end{aligned}$$

In the second equality, we used orthonormality. The product of δ functions implies that we need to consider only permutations π and σ which agree on $\{k+1,\dots,n\}$.

To exploit this, we partition the permutations according to which k set A_k features as the image of $\{1,\dots,k\}$. More precisely, given a k set A_k, we define

$$S_n(A_k) := \{\pi \in S_n \ :\ \pi(\{1,\dots,k\}) = A_k\}.$$

There is a more useful kind of affine representation of the elements of $S_n(A_k)$ as tuples in $S_k \times S_{n-k}$ composed of a fixed bijection $f_{A_k} \in S_n(A_k)$. For definiteness, we define f_{A_k} to be the unique bijection in $S_n(A_k)$, which preserves ordering. Then

$$\pi \in S_n(A_k) \Longleftrightarrow \pi = f_{A_k}\circ(\pi^k,\pi^{n-k}) \tag{A5}$$

for some $\pi^k \in S_k$, $\pi^{n-k} \in S_{n-k}$. Here we wrote (π^k,π^{n-k}) for the permutation that is obtained by applying π^k to the first k variables and π^{n-k} to the last $n-k$ variables.

This way of bookkeeping permutations is convenient in (A5) above. Using this representation and the identity (A6) below, we find that

$$\begin{aligned}\mathrm{tr}_{n\to k}&[|\Phi_n\rangle\langle\Phi_n|]\\ &= \frac{1}{n!}\sum_{A_k\ k-\mathrm{set}}\ \sum_{\substack{\pi,\sigma\in S_n(A_k);\\ \pi^{n-k}=\sigma^{n-k}}} \mathrm{sgn}(\pi\circ\sigma)\\ &\quad\times |\phi_{\pi(1)}\rangle\langle\phi_{\sigma(1)}| \otimes \cdots \otimes |\phi_{\pi(k)}\rangle\langle\phi_{\sigma(k)}|\\ &= \frac{1}{n!}\sum_{A_k\ k-\mathrm{set}}\ \sum_{\substack{\pi,\sigma\in S_n(A_k);\\ \pi^{n-k}=\sigma^{n-k}}} \mathrm{sgn}(\pi^k\circ\sigma^k)\\ &\quad\times |\phi_{\pi(1)}\rangle\langle\phi_{\sigma(1)}| \otimes \cdots \otimes |\phi_{\pi(k)}\rangle\langle\phi_{\sigma(k)}|\\ &= \frac{(n-k)!}{n!}\sum_{A_k\ k-\mathrm{set}}\ \sum_{\pi^k,\sigma^k\in S_k} \mathrm{sgn}(\pi^k\circ\sigma^k)\\ &\quad\times \big|\phi_{(f_{A_k}\circ\pi^k)(1)}\big\rangle\big\langle\phi_{(f_{A_k}\circ\sigma^k)(1)}\big|\\ &\quad\otimes\cdots\otimes \big|\phi_{(f_{A_k}\circ\pi^k)(k)}\big\rangle\big\langle\phi_{(f_{A_k}\circ\sigma^k)(k)}\big|.\end{aligned}$$

We used the following identity:

$$\mathrm{sgn}(\pi\circ\sigma) = \mathrm{sgn}(\pi^k\circ\sigma^k). \tag{A6}$$

This is a consequence of the fact that sgn is a group homomorphism. Indeed, we have

$$\begin{aligned}\mathrm{sgn}&(\pi\circ\sigma)\\ &= \big(\mathrm{sgn}\big(f_{A_k}\big)\big)^2\mathrm{sgn}((\pi^k,\pi^{n-k}))\mathrm{sgn}((\sigma^k,\sigma^{n-k}))\\ &= \mathrm{sgn}((\pi^k,\pi^{n-k}))\mathrm{sgn}((\sigma^k,\pi^{n-k}))\\ &= \mathrm{sgn}(\pi^k\circ\sigma^k).\end{aligned}$$

This proves (A6). We now return to (A6) to conclude the proof of (A4). We observe that

$$\mathrm{Perm}(A_k) = \{ f_{A_k} \circ \pi^k \circ f_{A_k}^{-1} \ : \ \pi^k \in S_k \}.$$

To exploit this, we order each k set $A_k = \{i_1,\dots,i_k\}$, with $i_1 < \cdots < i_k$. Then, by definition, $f_{A_k}(j) = i_j$ for all $1 \leqslant j \leqslant k$. From this, we find that

$$f_{A_k} \circ \pi^k(j) = f_{A_k} \circ \pi^k \circ f_{A_k}^{-1}(i_j) =: \tilde{\pi}^k(i_j)$$

produces a permutation $\tilde{\pi}^k \in \mathrm{Perm}(A_k)$. We use this observation to relabel the sum in (A6), and we also use the identity $\mathrm{sgn}(\pi^k\tilde{\sigma}^k) = \mathrm{sgn}(\tilde{\pi}^k \circ \tilde{\sigma}^k)$, which follows from an argument similar to (A6) above. We get

$$\begin{aligned}
&\frac{(n-k)!}{n!} \sum_{A_k\ k-\mathrm{set}} \sum_{\pi^k,\sigma^k \in S_k} \mathrm{sgn}(\pi^k \circ \sigma^k) \\
&\quad \times |\phi_{(f_{A_k}\circ\pi^k)(1)}\rangle\langle\phi_{(f_{A_k}\circ\sigma^k)(1)}| \\
&\quad \otimes \cdots \otimes |\phi_{(f_{A_k}\circ\pi^k)(k)}\rangle\langle\phi_{(f_{A_k}\circ\sigma^k)(k)}| \\
&= \frac{1}{\binom{n}{k}} \sum_{A_k\ k-\mathrm{set}} \frac{1}{k!} \sum_{\tilde{\pi}^k,\tilde{\sigma}^k \in \mathrm{Perm}(A_k)} \mathrm{sgn}(\tilde{\pi}^k \circ \tilde{\sigma}^k) \\
&\quad \times |\phi_{\tilde{\pi}^k(i_1)}\rangle\langle\phi_{\tilde{\sigma}^k(i_1)}| \otimes \cdots \otimes |\phi_{\tilde{\pi}^k(i_k)}\rangle\langle\phi_{\tilde{\sigma}^k(i_k)}| \\
&= \frac{1}{\binom{n}{k}} \sum_{A_k\ k-\mathrm{set}} |\Phi_{A_k}\rangle\langle\Phi_{A_k}|. \qquad \text{(A7)}
\end{aligned}$$

This concludes the proof of Lemma 1. ■

APPENDIX B: THE MAXIMALLY MIXED STATE ON THE ANTISYMMETRIC SUBSPACE

The following lemma allows us to conclude that the stronger form of Theorem 8 applies when considering cloning maps for the antisymmetric subspace.

Lemma 2. Let $\mathcal{H}_n$ denote the antisymmetric subspace of n qudits and let π_n denote the maximally mixed state on $\mathcal{H}_n$. Then

$$\pi_k = \mathrm{tr}_{n\to k}[\pi_n].$$

Proof of Lemma 2. The operator $\mathrm{tr}_{n\to k}[\pi_n]$ is supported on $\mathcal{H}_k$. It also commutes with all unitaries U_k on $\mathcal{H}_k$. Indeed, by properties of the partial trace and the fact that π_n commutes with all unitaries on $\mathcal{H}_n$,

$$\begin{aligned}
U_k \mathrm{tr}_{n\to k}[\pi_n] &= \mathrm{tr}_{n\to k}\big[\big(U_k \otimes I_{\mathcal{H}_{n-k}}\big)\pi_n\big] \\
&= \mathrm{tr}_{n\to k}\big[\pi_n\big(U_k \otimes I_{\mathcal{H}_{n-k}}\big)\big] = \mathrm{tr}_{n\to k}[\pi_n]U_k.
\end{aligned}$$

Since it commutes with all unitaries, $\mathrm{tr}_{n\to k}[\pi_n]$ is proportional to $I_{\mathcal{H}_k}$. Since

$$\mathrm{tr}_{\mathcal{H}_k}[\mathrm{tr}_{n\to k}[\pi_n]] = \mathrm{tr}_{\mathcal{H}_n}[\pi_n] = 1,$$

the proportionality constant must be $1/\dim\mathcal{H}_k = 1/\binom{d}{k}$. This proves the lemma. ■

APPENDIX C: LIMITATIONS ON APPROXIMATE TWOFOLD BROADCASTS

As mentioned in the main text, our method also gives limitations on approximate twofold broadcasting.

Throughout, we restrict our discussion to broadcasts which receive as their input state only a single copy of σ. In particular, we are not in a situation where "superbroadcasting" [39,40] is possible.

Theorem 11. Fix two mixed states σ_1 and σ_2. Suppose that the quantum channel $\Lambda_{A\to AB}$ is a simultaneous approximate broadcast of σ_1 and σ_2, i.e., that

$$\rho_{i,A}^{\mathrm{out}} = \rho_{i,B}^{\mathrm{out}} = \tilde{\sigma}_i, \quad \rho_{i,AB}^{\mathrm{out}} := \Lambda(\sigma_{i,A}) \qquad \text{(C1)}$$

for $i = 1,2$. Then

$$D(\sigma_1\|\sigma_2) - D(\tilde{\sigma}_1\|\tilde{\sigma}_2) \geqslant \Delta_{\mathcal{R}}(\tilde{\sigma}_1,\tilde{\sigma}_2), \qquad \text{(C2)}$$

where we have introduced the (channel-dependent) "recovery difference"

$$\Delta_{\mathcal{R}}(\tilde{\sigma}_1,\tilde{\sigma}_2) := \frac{1}{8}\int_{\mathbb{R}} \big\|\mathcal{R}^t_{B,\rho^{\mathrm{out}}_{2,AB}}(\tilde{\sigma}_{1,A}) - \mathcal{R}^t_{A,\rho^{\mathrm{out}}_{2,AB}}(\tilde{\sigma}_{1,B})\big\|_1^2 \, d\beta(t), \qquad \text{(C3)}$$

which features the probability distribution $\beta(t) := \frac{\pi}{2}[1+\cosh(\pi t)]^{-1}$ and the rotated Petz recovery map defined by

$$\mathcal{R}^t_{A,X}(\cdot) := X_{AB}^{(1+it)/2}\big[I_A \otimes X_B^{-(1+it)/2}(\cdot)X_B^{-(1-it)/2}\big]X_{AB}^{(1-it)/2}. \qquad \text{(C4)}$$

The proof is given at the end of this Appendix. We emphasize that the definition (C3) of the recovery difference $\Delta_{\mathcal{R}}(\tilde{\sigma}_1,\tilde{\sigma}_2)$ is independent of $\rho^{\mathrm{out}}_{1,AB}$. The rotated Petz recovery map (C4) appears in the strengthening of the monotonicity of relative entropy [24], recalled here as Theorem 10. The rotated Petz recovery map is chosen such that the second state is perfectly recovered, i.e.,

$$\mathcal{R}^t_{B,\rho^{\mathrm{out}}_{2,AB}}(\tilde{\sigma}_{2,A}) = \mathcal{R}^t_{A,\rho^{\mathrm{out}}_{2,AB}}(\tilde{\sigma}_{2,B}) = \rho^{\mathrm{out}}_{2,AB}.$$

Proof of Theorem 11. The proof is based on the following key estimate. It is a variant of Theorem 10, which was proved in [24].

Lemma 4. Key estimate. Fix two quantum states σ_1 and σ_2. For any choice of quantum channel $\Lambda_{A\to AB}$, we define

$$\rho_i^{\mathrm{out}} := \Lambda(\sigma_{i,A}) \quad (i = 1,2). \qquad \text{(C5)}$$

Let $\beta(t) = \frac{\pi}{2}[1+\cosh(\pi t)]^{-1}$.

(i) We have

$$\begin{aligned}
&D(\sigma_1\|\sigma_2) - D\big(\rho^{\mathrm{out}}_{1,B}\big\|\rho^{\mathrm{out}}_{2,B}\big) \\
&\quad \geqslant -\int_{\mathbb{R}} \ln F\big(\rho^{\mathrm{out}}_{1,AB},\mathcal{R}^t_{A,\rho^{\mathrm{out}}_{2,AB}}\big(\rho^{\mathrm{out}}_{1,B}\big)\big)\, d\beta(t), \qquad \text{(C6)} \\
&D(\sigma_1\|\sigma_2) - D\big(\rho^{\mathrm{out}}_{1,A}\big\|\rho^{\mathrm{out}}_{2,A}\big) \\
&\quad \geqslant -\int_{\mathbb{R}} \ln F\big(\rho^{\mathrm{out}}_{1,AB},\mathcal{R}^t_{B,\rho^{\mathrm{out}}_{2,AB}}\big(\rho^{\mathrm{out}}_{1,A}\big)\big)\, d\beta(t), \qquad \text{(C7)}
\end{aligned}$$

where the rotated Petz recovery map $\mathcal{R}^t_{A,X}$ was defined in (C4).

(ii) Suppose that the output state $\rho^{\mathrm{out}}_{i,AB}$ has identical marginals, i.e.,

$$\rho^{\mathrm{out}}_{i,A} = \rho^{\mathrm{out}}_{i,B} =: \tilde{\sigma}_i \quad (i = 1,2).$$

Then we have

$$D(\sigma_1\|\sigma_2) - D(\tilde\sigma_1\|\tilde\sigma_2) \geqslant \begin{cases} -\int_{\mathbb{R}} \ln F\big(\rho^{\text{out}}_{1,AB},\mathcal{R}^t_{A,\rho^{\text{out}}_{2,AB}}(\tilde\sigma_{1,B})\big)\, d\beta(t), \\ -\int_{\mathbb{R}} \ln F\big(\rho^{\text{out}}_{1,AB},\mathcal{R}^t_{B,\rho^{\text{out}}_{2,AB}}(\tilde\sigma_{1,A})\big)\, d\beta(t). \end{cases} \tag{C8}$$

Proof of Lemma 4. The standard monotonicity of quantum relative entropy under quantum channels (without a remainder term) gives

$$D(\sigma_1\|\sigma_2) \geqslant D(\Lambda(\sigma_1)\|\Lambda(\sigma_2)) = D\big(\rho^{\text{out}}_1\big\|\rho^{\text{out}}_2\big).$$

Consider the last expression. When we apply the partial trace over the A subsystem to both states and use Theorem 10, we obtain

$$D\big(\rho^{\text{out}}_1\big\|\rho^{\text{out}}_2\big) \geqslant D\big(\rho^{\text{out}}_{1,B}\big\|\rho^{\text{out}}_{2,B}\big) - \int_{\mathbb{R}} \ln F\big(\rho^{\text{out}}_{1,AB},\mathcal{R}^t_{\rho^{\text{out}}_{2,AB}}\big(\rho^{\text{out}}_{1,B}\big)\big)\, d\beta(t).$$

This proves (C6), and (C7) follows from the same argument, except the B subsystem is traced out now. Statement (ii) is immediate. ■

With Lemma 4 at our disposal, we can now prove Theorem 11. We begin by applying Lemma 4, statement (ii), averaging the two lines in (C8). We get

$$D(\sigma_1\|\sigma_2) - D(\tilde\sigma_1\|\tilde\sigma_2) \geqslant -\frac{1}{2}\int_{\mathbb{R}} \ln F\big(\rho^{\text{out}}_{1,AB},\mathcal{R}^t_{B,\rho^{\text{out}}_{2,AB}}(\tilde\sigma_{1,A})\big) d\beta(t) - \frac{1}{2}\int_{\mathbb{R}} \ln F\big(\rho^{\text{out}}_{1,AB},\mathcal{R}^t_{A,\rho^{\text{out}}_{2,AB}}(\tilde\sigma_{1,B})\big) d\beta(t).$$

By an elementary estimate and the Fuchs–van de Graaf inequality [41], we have for density operators ω and τ that

$$-\ln F(\omega,\tau) \geqslant 1 - F(\omega,\tau) \geqslant \tfrac{1}{4}\|\omega-\tau\|_1^2.$$

We apply this to the integrand above, followed by the estimate

$$\|X-Y\|_1^2 + \|X-Z\|_1^2 \geqslant \tfrac{1}{2}\|Y-Z\|_1^2,$$

which is a consequence of the triangle inequality and the elementary bound $2ab \leqslant a^2+b^2$. We conclude

$$D(\sigma_1\|\sigma_2) - D(\tilde\sigma_1\|\tilde\sigma_2) \geqslant \frac{1}{8}\int_{\mathbb{R}} \big\|\mathcal{R}^t_{B,\rho^{\text{out}}_{2,AB}}(\tilde\sigma_{1,A}) - \mathcal{R}^t_{A,\rho^{\text{out}}_{2,AB}}(\tilde\sigma_{1,B})\big\|_1^2\, \mathrm{d}\beta(t).$$

This proves Theorem 11. ■

[1] D. Dieks, Phys. Lett. A **92**, 271 (1982).
[2] W. Wootters and W. Zurek, Nature (London) **299**, 802 (1982).
[3] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[4] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).
[5] P. Mandayam and H. K. Ng, Phys. Rev. A **86**, 012335 (2012).
[6] P. W. Shor, in *Proceedings of the 37th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, D.C., 1996), p. 56.
[7] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[8] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[9] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[10] A. E. Allahverdyan and K. V. Hovhannisyan, Phys. Rev. A **81**, 012312 (2010).
[11] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1999).
[12] A. Lamas-Linares, C. Simon, J. C. Howell, and D. Bouwmeester, Science **296**, 712 (2002).
[13] V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005).
[14] H. Fan, Y.-N. Wang, L. Jing, J.-D. Yue, H.-D. Shi, Y.-L. Zhang, and L.-Z. Mu, Phys. Rep. **544**, 241 (2014).
[15] M.-Z. Zhu and L. Ye, Phys. Rev. A **91**, 042319 (2015).
[16] S. Chatterjee, S. Sazim, and I. Chakrabarty, Phys. Rev. A **93**, 042309 (2016).
[17] A. Kalev and I. Hen, Phys. Rev. Lett. **100**, 210502 (2008).
[18] G. Lindblad, Commun. Math. Phys. **40**, 147 (1975).
[19] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).
[20] O. Fawzi and R. Renner, Commun. Math. Phys. **340**, 575 (2015).
[21] M. Berta, M. Lemm, and M. M. Wilde, Quantum Inf. Comput. **15**, 1333 (2015).
[22] D. Sutter, O. Fawzi, and R. Renner, Proc. R. Soc. A. **472**, 20150623 (2016).
[23] M. M. Wilde, Proc. R. Soc. A **471**, 20150338 (2015).
[24] M. Junge, R. Renner, D. Sutter, M. M. Wilde, and A. Winter, arXiv:1509.07127.
[25] D. Sutter, M. Berta, and M. Tomamichel, Commun. Math. Phys. **352**, 37 (2017).
[26] Y. Yang, G. Chiribella, and M. Hayashi, Phys. Rev. Lett. **117**, 090502 (2016).
[27] F. Buscemi, S. Das, and M. M. Wilde, Phys. Rev. A **93**, 062314 (2016).
[28] G. Lindblad, Lett. Math. Phys. **47**, 189 (1999).
[29] M. S. Leifer, Phys. Rev. A **74**, 042310 (2006).
[30] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, Phys. Rev. Lett. **99**, 240501 (2007).
[31] M. Piani, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **100**, 090502 (2008).
[32] M. Piani, arXiv:1608.02650.
[33] H. Umegaki, Kodai Math. Semin. Rep. **14**, 59 (1962).
[34] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[35] M. Ohya and D. Petz, *Quantum Entropy and Its Use* (Springer, Berlin, 1993).
[36] K. Bradler, IEEE Trans. Inf. Theory **57**, 5497 (2011).
[37] A. W. Harrow, arXiv:1308.6595.
[38] I. Marvian and S. Lloyd, arXiv:1608.07325.
[39] G. M. D'Ariano, C. Macchiavello, and P. Perinotti, Phys. Rev. Lett. **95**, 060503 (2005).
[40] F. Buscemi, G. M. D'Ariano, C. Macchiavello, and P. Perinotti, Phys. Rev. A **74**, 042309 (2006).
[41] C. A. Fuchs and J. van de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1998).