

# A Semidefinite Program for Distillable Entanglement

Eric M. Rains

**Abstract**—We show that the maximum fidelity obtained by a positive partial transpose (p.p.t.) distillation protocol is given by the solution to a certain semidefinite program. This gives a number of new lower and upper bounds on p.p.t. distillable entanglement (and thus new upper bounds on 2-locally distillable entanglement). In the presence of symmetry, the semidefinite program simplifies considerably, becoming a linear program in the case of isotropic and Werner states. Using these techniques, we determine the p.p.t. distillable entanglement of asymmetric Werner states and “maximally correlated” states. We conclude with a discussion of possible applications of semidefinite programming to quantum codes and 1-local distillation.

**Index Terms**—Entanglement distillation, quantum communication, semidefinite programming.

## I. INTRODUCTION

ONE of the central problems of quantum information theory is entanglement distillation [3], [11]: the production of (approximate) maximally entangled states from a collection of nonmaximally entangled states. Of particular interest are 1-locally distillable entanglement and 2-locally distillable entanglement (the amount of entanglement that can be distilled using local operations and a one-way (two-way) classical channel). Nearly all of the known upper bounds on 1- or 2-locally distillable entanglement actually apply to a larger class of operations, known as positive partial transpose (p.p.t.) operations [11]. This motivates our present study of p.p.t. distillable entanglement.

We study distillable entanglement via a more refined quantity, the “fidelity of distillation,” which measures how close one can come to producing a  $K$ -dimensional maximally entangled state from a given input. In Theorem 3.1 below, we show that the fidelity of p.p.t. distillation can be expressed as the solution to a certain semidefinite program (see [14] for a survey of semidefinite programming). Then any feasible solution to the dual problem (Theorem 3.3) gives us an upper bound on fidelity of distillation.

The rest of the paper is devoted to an exploration of the consequences of this semidefinite program. Section IV gives a number of results that hold in general, including a new bound combining the bounds of [9] and [5], and a theorem (Corollary 4.3) to the effect that maximally entangled states cannot be used to “activate” fidelity of p.p.t. distillation. In Section V, we show that the semidefinite program simplifies in the presence of symmetries; in some cases (e.g., isotropic states, Werner states), this simpli-

fication turns the semidefinite program into a linear program. In the case of asymmetric Werner states, this linear program can be solved exactly, showing that the upper bound of [5] is tight in that case. Section VI sketches a technique for producing asymptotic lower bounds, which we then use to strengthen the hashing lower bound [3] in the p.p.t. case. We also use this technique to partially resolve a conjecture of [9] by determining the p.p.t. distillable entanglement of “maximally correlated” states. Finally, in Section VII, we consider possible applications of semidefinite programming to the problems of quantum codes and 1-local distillation. In particular, using the techniques of Section V, we give a new derivation of the linear programming bound for quantum codes [13], [8], [10].

## II. OPERATORS, SUPEROPERATORS AND OPERATIONS

If  $V$  is a Hilbert space, we denote by  $\mathcal{H}(V)$  the space of Hermitian operators on  $V$ . We also let  $\mathcal{P}(V) \subset \mathcal{H}(V)$  denote the convex cone of positive semidefinite Hermitian operators; we will freely write  $A \geq B$  to mean  $A - B \in \mathcal{P}(V)$ . A state is then an element of  $\mathcal{P}(V)$  of trace 1. Quantum information theory can be thought of as studying the behavior of these concepts under tensor products.

Given an operator  $A \in \mathcal{H}(V \otimes W)$ , we define the “partial trace”  $\text{Tr}_V(A)$  to be the (unique) operator in  $\mathcal{H}(W)$  such that

$$\text{Tr}(\text{Tr}_V(A)B) = \text{Tr}(A(1 \otimes B)) \quad (2.1)$$

for all  $B \in \mathcal{H}(W)$ . Similarly, given a choice of basis for  $W$ , we can define the partial transpose  $A^{\Gamma_W}$  by

$$\text{Tr}(A^{\Gamma_W}(B \otimes C)) = \text{Tr}(A(B \otimes C^t)) \quad (2.2)$$

where  $B \in \mathcal{H}(V)$ ,  $C \in \mathcal{H}(W)$ , and  $C^t$  is the transpose of  $C$  with respect to the chosen basis. Both of these transformations extend by linearity to non-Hermitian operators as well.

A positive operator  $C \in \mathcal{P}(V \otimes W)$  is said to be “separable” if it can be written in the form

$$C = \sum_i A_i \otimes B_i \quad (2.3)$$

with  $A_i \in \mathcal{P}(V)$ ,  $B_i \in \mathcal{P}(W)$ ; in other words

$$C \in \mathcal{P}(V) \otimes \mathcal{P}(W). \quad (2.4)$$

Similarly,  $C$  is said to be p.p.t. if

$$C \in \mathcal{P}(V \otimes W) \cap \mathcal{P}(V \otimes W)^{\Gamma_W}. \quad (2.5)$$

Note that this does not depend on the choice of basis in  $W$ . We also recall that every p.p.t. operator is separable

$$\mathcal{P}(V) \otimes \mathcal{P}(W) \subset \mathcal{P}(V \otimes W) \cap \mathcal{P}(V \otimes W)^{\Gamma_W}. \quad (2.6)$$

A “superoperator” from  $V$  to  $V'$  is a linear transformation from  $\mathcal{H}(V)$  to  $\mathcal{H}(V')$ . The space of superoperators can be nat-

Manuscript received August 23, 2000; revised June 8, 2001.

The author is with AT&T Labs—Research, Florham Park, NJ 07932-0971 USA (e-mail: rains@research.att.com).

Communicated by P. W. Shor, Associate Editor for Quantum Information Theory.

Publisher Item Identifier S 0018-9448(01)08954-4.

urally identified with  $\mathcal{H}(V \otimes V')$ ; to a superoperator  $\Psi$  corresponds the unique operator  $\Omega(\Psi)$  such that

$$\text{Tr}(B\Psi(A)) = \text{Tr}(\Omega(\Psi)(A \otimes B)). \quad (2.7)$$

We also define the adjoint superoperator  $\Psi^*$  by

$$\text{Tr}(A\Psi^*(B)) = \text{Tr}(B\Psi(A)). \quad (2.8)$$

Note that

$$\Psi(A) = \text{Tr}_{V'}(\Omega(\Psi)(A \otimes 1)) \quad (2.9)$$

$$\Psi^*(B) = \text{Tr}_{V'}(\Omega(\Psi)(1 \otimes B)) \quad (2.10)$$

and, if  $\Psi_1: \mathcal{H}(V) \rightarrow \mathcal{H}(V')$  and  $\Psi_2: \mathcal{H}(V') \rightarrow \mathcal{H}(V'')$ , then

$$\begin{aligned} \Omega(\Psi_2 \circ \Psi_1) &= (\Psi_1^* \otimes 1)(\Omega(\Psi_2)) = (1 \otimes \Psi_2)(\Omega(\Psi_1)) \\ &= \text{Tr}_{V''}((\Omega(\Psi_1) \otimes 1_{V''})(1_V \otimes \Omega(\Psi_2))). \end{aligned} \quad (2.11)$$

Of particular interest is the (self-adjoint) superoperator  $A \mapsto A^\dagger$ ; in that case, we find

$$\Omega(t) = \sum_{i,j} (v_i \otimes v_i)(v_j \otimes v_j)^\dagger \geq 0. \quad (2.12)$$

A superoperator is said to be “positive” if  $\Psi(A) \geq 0$  whenever  $A \geq 0$ , and “trace-preserving” if  $\Psi^*(1) = 1$ ; equivalently,  $\text{Tr}_{V'}(\Omega(\Psi)) = 1$ . A superoperator is “completely positive” if it satisfies any of the following equivalent conditions:

- 1)  $1_V \otimes \Psi$  is positive.
- 2) For all Hilbert spaces  $W$ ,  $1_W \otimes \Psi$  is positive.
- 3) There exist operators  $A_i \in \text{Hom}(V, V')$  such that

$$\Psi(A) = \sum_i A_i A A_i^\dagger. \quad (2.13)$$

- 4) For any (some) basis of  $V$ , the partial transpose  $\Omega(\Psi)^{\Gamma_V}$  is positive semidefinite.

Clearly 2)  $\implies$  1), and 3)  $\implies$  2) is straightforward. To see 1)  $\implies$  4), it suffices to observe that

$$\Omega(\Psi)^{\Gamma_V} = (1_V \otimes \Psi)(\Omega(t)) \geq 0. \quad (2.14)$$

Finally, 4)  $\implies$  3) follows by taking an eigenvalue decomposition of  $\Omega(\Psi)^{\Gamma_V}$ . Since the operators we will be dealing with in the sequel are mostly completely positive, we define  $\Omega'(\Psi) = \Omega(\Psi)^{\Gamma_V}$ , and use this to identify the space of superoperators with  $\mathcal{H}(V \otimes V')$ . Thus, the set of completely positive superoperators is identified with  $\mathcal{P}(V \otimes V')$ . An “operation” is defined to be a completely positive, trace-preserving superoperator; we denote the (convex) set of operations from  $V$  to  $V'$  by  $Op(V, V')$ .<sup>1</sup>

On tensor product spaces, there are several classes of operations of interest, which can be defined in terms of the convex sets  $\mathcal{P}$  and  $Op$  as follows:

- $\epsilon$ -local:  $\mathcal{C}_\epsilon = Op(V, V') \otimes Op(W, W')$ .

<sup>1</sup>This differs somewhat from the definition of operation given in [11], in that we are assuming operations to be “nonmeasuring,” but by the main result of that paper, this incurs no loss of generality when studying entanglement distillation.

- 1-local:  $\mathcal{C}_1 = (\mathcal{P}(V \otimes V') \otimes Op(W, W')) \cap Op(V \otimes W, V' \otimes W')$ .
- 1'-local:  $\mathcal{C}_{1'} = (Op(V, V') \otimes \mathcal{P}(W \otimes W')) \cap Op(V \otimes W, V' \otimes W')$ .
- separable:  $\mathcal{C}_\S = (\mathcal{P}(V \otimes V') \otimes \mathcal{P}(W \otimes W')) \cap Op(V \otimes W, V' \otimes W')$ .
- p.p.t.:  $\mathcal{C}_\Gamma = Op(V \otimes W, V' \otimes W') \cap Op(V \otimes W, V' \otimes W')^{\Gamma_{W \otimes W'}}$ .

We also have the class of 2-local operations, defined by allowing arbitrary compositions of 1-local and 1'-local operations. For a different approach to defining these classes, see [11]. We recall

$$\mathcal{C}_\epsilon \subset \mathcal{C}_1, \mathcal{C}_{1'} \subset \mathcal{C}_2 \subset \mathcal{C}_\S \subset \mathcal{C}_\Gamma \quad (2.15)$$

with all inclusions strict in general. (The class  $\mathcal{C}_\epsilon$ , not discussed in [11], is simply the closure of the class of local operations under convex linear combinations (i.e., shared randomness).) Note that each of these classes is closed under tensor products (unlike, say, the class of operations taking p.p.t. operators to p.p.t. operators).

From a physical perspective, the only natural classes are those of ( $\epsilon, 1, 1', 2$ )-local operations. The difficulty, however, is that in none of these cases do we have an effective way to decide whether a given operation belongs to the class; this is especially true in the case of 2-local operations. Thus, the class of separable operations is important as a simplification of the class of 2-local operations, while the class of p.p.t. operations is important as the smallest class containing the 2-local class for which we can effectively decide membership. For instance, all of the known upper bounds on 2-locally distillable entanglement are really bounds on p.p.t. distillable entanglement; to a large extent, this even applies to upper bounds on 1-locally distillable entanglement. Similarly, a lower bound on p.p.t. distillable entanglement provides a limit on how far the current methods can take us.

### III. FIDELITY OF DISTILLATION

For any integer  $K > 0$ , we define the “maximally entangled” state  $\Phi(K) \in \mathcal{H}(\mathbb{C}^K \otimes \mathbb{C}^K)$  by

$$\Phi(K) = \frac{1}{K} \Omega'(1_{\mathbb{C}^K}) = \frac{1}{K} \sum_{1 \leq i, j \leq K} (e_i \otimes e_i)(e_j \otimes e_j)^\dagger. \quad (3.1)$$

Given any other state  $\rho$ , the “fidelity” of  $\rho$  is defined by

$$F(\rho) = \text{Tr}(\Phi(K)\rho). \quad (3.2)$$

*Definition 1:* Let  $\rho \in \mathcal{P}(V \otimes W)$  be a state, and let  $K > 0$  be an integer. The “fidelity of  $K$ -state p.p.t. distillation”  $F_\Gamma(\rho; K)$  is defined by

$$F_\Gamma(\rho; K) = \max_{\Psi} F(\Psi(\rho)) \quad (3.3)$$

where  $\Psi$  ranges over all p.p.t. operations from  $\mathcal{H}(V \otimes W)$  to  $\mathcal{H}(\mathbb{C}^K \otimes \mathbb{C}^K)$ .

*Remark:* We can define  $F_\epsilon, F_1, F_2$ , etc., similarly.

This is a refinement of the concept of distillable entanglement; indeed, we can define (see [3], [11]) the following.

*Definition 2:* Let  $\rho$  be as above. The p.p.t. distillable entanglement  $D_\Gamma(\rho)$  of  $\rho$  is defined to be the supremum of all positive numbers  $r$  such that

$$\lim_{n \rightarrow \infty} F_\Gamma(\rho^{\otimes n}; \lfloor 2^{rn} \rfloor) = 1.$$

Thus, a study of  $F_\Gamma$  is likely to provide insights into  $D_\Gamma$ , as we shall indeed find below.

We first observe that the optimization problem defining  $F_\Gamma$  can be rewritten as an optimization over operators.

*Theorem 3.1:* For any state  $\rho$  and any positive integer  $K$

$$F_\Gamma(\rho; K) = \max_F \text{Tr}(F\rho) \quad (3.4)$$

where  $F$  ranges over Hermitian operators such that

$$0 \leq F \leq 1, \quad -1/K \leq F^\Gamma \leq 1/K. \quad (3.5)$$

*Proof:* Let  $\Psi$  be the operation maximizing  $F(\Psi(\rho))$  in the definition of  $F_\Gamma(\rho; K)$ . Clearly, if we compose  $\Psi$  with any operator of the form  $U \otimes \bar{U}$ , this leaves  $F(\Psi(\rho))$  unchanged. The same must then be true after averaging over  $U(K)$  (“twirling” [3]). We may thus assume  $\Psi = \mathbf{T} \circ \Psi$ , where  $\mathbf{T}$  is the twirling superoperator. We find

$$\begin{aligned} \mathbf{T}(A) &= \text{Tr}(A\Phi(K))\Phi(K) \\ &\quad + \frac{1}{K^2 - 1} \text{Tr}(A(1 - \Phi(K)))(1 - \Phi(K)); \end{aligned} \quad (3.6)$$

$\mathbf{T}(A)$  must have the form  $a\Phi(K) + b(1 - \Phi(K))$ , and since

$$\text{Tr}(\mathbf{T}(A)) = \text{Tr}(A) \quad \text{and} \quad \text{Tr}(\mathbf{T}(A)\Phi(K)) = \text{Tr}(A\Phi(K)) \quad (3.7)$$

we can solve for  $a$  and  $b$ . It follows that

$$\begin{aligned} \Omega(\mathbf{T}) &= \Phi(K) \otimes \Phi(K) + \frac{1}{K^2 - 1} (1 - \Phi(K)) \\ &\quad \otimes (1 - \Phi(K)) = \Omega'(\mathbf{T}). \end{aligned} \quad (3.8)$$

But then we compute

$$\Omega'(\Psi) = \Omega'(\mathbf{T} \circ \Psi) = (\Psi^* \otimes 1)(\Omega'(\mathbf{T})) \quad (3.9)$$

$$\begin{aligned} &= \Psi^*(\Phi(K)) \otimes \Phi(K) \\ &\quad + \frac{1}{K^2 - 1} \Psi^*(1 - \Phi(K)) \otimes (1 - \Phi(K)). \end{aligned} \quad (3.10)$$

Setting  $F = \Psi^*(\Phi(K))$ , we obtain

$$\Omega'(\Psi) = F \otimes \Phi(K) + \frac{1}{K^2 - 1} (1 - F) \otimes (1 - \Phi(K)). \quad (3.11)$$

This operator is positive if and only if  $F \geq 0$  and  $(1 - F) \geq 0$ . We also find

$$\begin{aligned} \Omega(\Psi)^\Gamma &= F^\Gamma \otimes \Phi(K)^\Gamma \\ &\quad + \frac{1}{K^2 - 1} (1 - F^\Gamma) \otimes (1 - \Phi(K)^\Gamma) \quad (3.12) \\ &= \frac{1}{K + 1} (1/K + F^\Gamma) \otimes (1 + K\Phi(K)^\Gamma)/2 \\ &\quad + \frac{1}{K - 1} (1/K - F^\Gamma) \otimes (1 - K\Phi(K)^\Gamma)/2. \end{aligned} \quad (3.13)$$

Since  $(1 \pm K\Phi(K)^\Gamma)/2$  are orthogonal projections, we find that  $\Omega(\Psi)^\Gamma$  is positive if and only if

$$-1/K \leq F^\Gamma \leq 1/K. \quad (3.14)$$

The theorem follows by noting

$$F(\Psi(\rho)) = \text{Tr}(F\rho). \quad (3.15)$$

□

*Definition 3:* An operator that satisfies the inequalities (3.5) will be said to be *primal feasible* for  $F_\Gamma(\rho; K)$ ; if it maximizes  $\text{Tr}(F\rho)$ , it will be said to be *primal optimal*.

We will use this result to define  $F_\Gamma(\rho; K)$  for all positive-real values of  $K$ ; for an interpretation, see the remark following Corollary 4.3 below.

*Theorem 3.2:* The function  $F_\Gamma$  is convex in  $\rho$  and concave in  $1/K$ ; that is, for  $0 \leq \pi \leq 1$

$$F_\Gamma(\pi\rho_1 + (1 - \pi)\rho_2; K) \leq \pi F_\Gamma(\rho_1; K) + (1 - \pi)F_\Gamma(\rho_2; K) \quad (3.16)$$

$$\begin{aligned} F_\Gamma(\rho; (K_1 K_2)/(\pi K_2 + (1 - \pi)K_1)) \\ \geq \pi F_\Gamma(\rho; K_1) + (1 - \pi)F_\Gamma(\rho; K_2). \end{aligned} \quad (3.17)$$

In particular,  $F_\Gamma$  is continuous in both variables.

*Proof:* Let  $F$  be primal optimal for

$$F_\Gamma(\pi\rho_1 + (1 - \pi)\rho_2; K).$$

Then

$$\begin{aligned} F_\Gamma(\pi\rho_1 + (1 - \pi)\rho_2; K) \\ = \text{Tr}(F(\pi\rho_1 + (1 - \pi)\rho_2)) \end{aligned} \quad (3.18)$$

$$= \pi \text{Tr}(F\rho_1) + (1 - \pi) \text{Tr}(F\rho_2) \quad (3.19)$$

$$\leq \pi F_\Gamma(\rho_1; K) + (1 - \pi)F_\Gamma(\rho_2; K). \quad (3.20)$$

Similarly, let  $F_1$  and  $F_2$  be primal optimal for  $F_\Gamma(\rho; K_1)$  and  $F_\Gamma(\rho; K_2)$ , respectively. Then  $\pi F_1 + (1 - \pi)F_2$  is primal feasible for  $F_\Gamma(\rho; (K_1 K_2)/(\pi K_2 + (1 - \pi)K_1))$ , thus, giving the second inequality. □

The above optimization problem is an instance of what is known as “semidefinite programming” (SDP) [14]. That is, it involves the optimization of a linear function subject to the constraint that certain operators (depending linearly on the variables) must be positive semidefinite. This has several consequences, including the computational one that semidefinite programs can be solved in polynomial time (typically polynomial in the dimension, although special structure can greatly reduce this). Another consequence is that there is a notion of duality for SDPs.

For a Hermitian operator  $A$ , we define the positive part  $A_+$  and negative part  $A_-$  to be the unique positive operators such that

$$A_+ - A_- = A \quad A_+ A_- = 0. \quad (3.21)$$

We also define  $|A| = A_+ + A_-$ .

*Theorem 3.3:* For any state  $\rho \in \mathcal{H}(V \otimes W)$  and any positive real number  $K$

$$F_{\Gamma}(\rho; K) = \min_{D \in \mathcal{H}(V \otimes W)} \text{Tr}(\rho - D)_+ + \frac{1}{K} \text{Tr}|D^{\Gamma}|. \quad (3.22)$$

*Proof:* Let  $F$  be an operator satisfying the constraints above. Then for any operators  $A, B, C$ , we have

$$\begin{aligned} \text{Tr}(F\rho) &= \text{Tr}(A) + 1/K \text{Tr}(B + C) \\ &\quad - \text{Tr}((-\rho + A + B^{\Gamma} - C^{\Gamma})F) \\ &\quad - \text{Tr}(A(1 - F)) - \text{Tr}(B(1/K - F^{\Gamma})) \\ &\quad - \text{Tr}(C(1/K + F^{\Gamma})). \end{aligned} \quad (3.23)$$

If  $A \geq 0, B \geq 0, C \geq 0$ , and

$$A \geq \rho - (B - C)^{\Gamma} \quad (3.24)$$

then the last four terms are all nonnegative, and we have

$$\text{Tr}(F\rho) \leq \text{Tr}(A) + 1/K \text{Tr}(B + C) \quad (3.25)$$

and, thus,

$$F_{\Gamma}(\rho; K) \leq \text{Tr}(A) + 1/K \text{Tr}(B + C). \quad (3.26)$$

In fact, by the theory of duality for SDPs, this inequality can be made tight, to wit

$$F_{\Gamma}(\rho; K) = \min_{A, B, C} \text{Tr}(A) + 1/K \text{Tr}(B + C) \quad (3.27)$$

minimizing over operators satisfying the constraints. Upon adding a variable  $D$  with  $D = (B - C)^{\Gamma}$ , the constraints become

$$A, B, C \geq 0 \quad A \geq \rho - D \quad B + C = D^{\Gamma}. \quad (3.28)$$

We, thus, find

$$\begin{aligned} F_{\Gamma}(\rho; K) &= \min_D \left( \min_{\substack{A \geq 0 \\ A \geq \rho - D}} \text{Tr}(A) + \frac{1}{K} \min_{\substack{B, C \geq 0 \\ B - C = D^{\Gamma}}} \text{Tr}(B + C) \right). \end{aligned} \quad (3.29)$$

But we readily see that

$$\min_{\substack{A \geq 0 \\ A \geq \rho - D}} \text{Tr}(A) = \text{Tr}(\rho - D)_+ \quad (3.30)$$

$$\min_{\substack{B, C \geq 0 \\ B - C = D^{\Gamma}}} \text{Tr}(B + C) = \text{Tr}|D^{\Gamma}| \quad (3.31)$$

proving the theorem.  $\square$

*Definition 4:* An operator  $D \in \mathcal{H}(V \otimes W)$  such that

$$F_{\Gamma}(\rho; K) = \text{Tr}(\rho - D)_+ + \frac{1}{K} \text{Tr}|D^{\Gamma}| \quad (3.32)$$

will be said to be *dual optimal* for  $F_{\Gamma}(\rho; K)$ .

Thus, given any operator  $D$ , we obtain bounds on fidelity of distillation, and conversely any such bound can in principle be shown by choosing a suitable operator  $D$ . For instance, Theorem 3.2 could also be proved as follows.

*Proof:* If  $D_1$  and  $D_2$  are dual optimal for  $F_{\Gamma}(\rho_1; K)$  and  $F_{\Gamma}(\rho_2; K)$ , then

$$\begin{aligned} &F_{\Gamma}(\pi\rho_1 + (1 - \pi)\rho_2; K) \\ &\leq \text{Tr}(\pi\rho_1 + (1 - \pi)\rho_2 - \pi D_1 + (1 - \pi)D_2)_+ \\ &\quad + \frac{1}{K} \text{Tr}|\pi D_1^{\Gamma} + (1 - \pi)D_2^{\Gamma}| \end{aligned} \quad (3.33)$$

$$\begin{aligned} &\leq \pi(\text{Tr}(\rho_1 - D_1)_+ + \text{Tr}|D_1^{\Gamma}|) \\ &\quad + (1 - \pi)(\text{Tr}(\rho_2 - D_2)_+ + \text{Tr}|D_2^{\Gamma}|) \end{aligned} \quad (3.34)$$

$$= \pi F_{\Gamma}(\rho_1; K) + (1 - \pi)F_{\Gamma}(\rho_2; K). \quad (3.35)$$

Similarly, if  $D$  is dual optimal for

$$F_{\Gamma}(\rho; (K_1 K_2)/(\pi K_2 + (1 - \pi)K_1))$$

then

$$\begin{aligned} &F_{\Gamma}(\rho; (K_1 K_2)/(\pi K_2 + (1 - \pi)K_1)) \\ &= \text{Tr}(\rho - D)_+ + \left( \pi \frac{1}{K_1} + (1 - \pi) \frac{1}{K_2} \right) \text{Tr}|D^{\Gamma}| \end{aligned} \quad (3.36)$$

$$\begin{aligned} &= \pi \left( \text{Tr}(\rho - D)_+ + \frac{1}{K_1} \text{Tr}|D^{\Gamma}| \right) \\ &\quad + (1 - \pi) \left( \text{Tr}(\rho - D)_+ + \frac{1}{K_2} \text{Tr}|D^{\Gamma}| \right) \end{aligned} \quad (3.37)$$

$$\geq \pi F(\rho; K_1) + (1 - \pi)F(\rho; K_2). \quad (3.38)$$

$\square$

#### IV. GENERAL RESULTS

*Lemma 4.1:* For any integer  $d \geq 1$ , and any  $K > 0$

$$F_{\Gamma}(\Phi(d); K) = \min(1, d/K).$$

*Proof:* For  $K \geq d$ , take  $F = d/K, D = \Phi(d)$ . For  $K \leq d$ , take  $F = \Phi(d), D = 0$ .  $\square$

*Theorem 4.2:* For any states  $\rho_1$  and  $\rho_2$ , and any  $K, K' > 0$

$$\begin{aligned} &F_{\Gamma}(\rho_1; K') F_{\Gamma}(\rho_2; K/K') \\ &\leq F_{\Gamma}(\rho_1 \otimes \rho_2; K) \leq F_{\Gamma}(\rho_1; K/\text{Tr}|\rho_2^{\Gamma}|). \end{aligned} \quad (4.1)$$

*Proof:* For the first inequality, let  $F_1$  and  $F_2$  be primal optimal for  $F_{\Gamma}(\rho_1; K')$ , and  $F_{\Gamma}(\rho_2; K/K')$ ; then  $F_1 \otimes F_2$  is primal feasible for  $F_{\Gamma}(\rho_1 \otimes \rho_2; K)$ , giving the inequality.

For the second inequality, let  $D$  be dual optimal for  $F_{\Gamma}(\rho_1; K/\text{Tr}|\rho_2^{\Gamma}|)$ . Then, taking  $D' = D \otimes \rho_2$ , we have

$$\begin{aligned} &F_{\Gamma}(\rho_1 \otimes \rho_2; K) \\ &\leq \text{Tr}((\rho_1 \otimes \rho_2) - (D \otimes \rho_2))_+ + \frac{1}{K} \text{Tr}|(D \otimes \rho_2)^{\Gamma}| \end{aligned} \quad (4.2)$$

$$= \text{Tr}(\rho_1 - D)_+ + \frac{\text{Tr}|\rho_2^{\Gamma}|}{K} \text{Tr}|D^{\Gamma}| \quad (4.3)$$

$$= F_{\Gamma}(\rho_1; K/\text{Tr}|\rho_2^{\Gamma}|). \quad (4.4)$$

$\square$

In particular, if  $F_{\Gamma}(\rho_2; \text{Tr}|\rho_2^{\Gamma}|) = 1$ , then equality holds in this theorem, taking  $K' = K/\text{Tr}|\rho_2^{\Gamma}|$ . Since this is true for  $\Phi(d)$ , we obtain the following.

*Corollary 4.3:* For all integers  $d$ , all  $K > 0$ , and any state  $\rho$

$$F_{\Gamma}(\rho \otimes \Phi(d); dK) = F_{\Gamma}(\rho; K). \quad (4.5)$$

*Remark:* This gives us another way to define  $F_{\Gamma}(\rho; K)$  for general  $K > 0$ . For rational  $K > 0$ , we can define

$$F_{\Gamma}(\rho; p/q) = F_{\Gamma}(\rho \otimes \Phi(q); p) \quad (4.6)$$

which is well defined by the theorem. Since the resulting function is nonincreasing in  $K$ , there is a unique way to extend it to a left-continuous function of  $K$ , which must then agree with our earlier definition.

Another example is when  $\rho_2$  is p.p.t.; then  $\text{Tr} |\rho_2^{\Gamma}| = 1$ . We have the following.

*Corollary 4.4:* For all  $K > 0$ , any state  $\rho$ , and any p.p.t. state  $\rho'$

$$F_{\Gamma}(\rho \otimes \rho'; K) = F_{\Gamma}(\rho; K). \quad (4.7)$$

*Corollary 4.5:* For any  $K > 0$  and any state  $\rho$

$$\min(1, 1/K) \leq F_{\Gamma}(\rho; K) \leq \min(1, \text{Tr} |\rho^{\Gamma}|/K). \quad (4.8)$$

*Proof:* By the theorem, we have, writing  $\rho = \Phi(1) \otimes \rho'$

$$\begin{aligned} \min(1, 1/K) &= F_{\Gamma}(\Phi(1); K) F_{\Gamma}(\rho'; 1) \\ &\leq F_{\Gamma}(\rho; K) \leq F_{\Gamma}(\Phi(1); K/\text{Tr} |\rho^{\Gamma}|) \\ &= \min(1, \text{Tr} |\rho^{\Gamma}|/K). \end{aligned} \quad (4.9)$$

□

Asymptotically, the theorem becomes the following.

*Corollary 4.6:* For any pair of states  $\rho_1, \rho_2$

$$D_{\Gamma}(\rho_1) + D_{\Gamma}(\rho_2) \leq D_{\Gamma}(\rho_1 \otimes \rho_2) \leq D_{\Gamma}(\rho_1) + \log_2 \text{Tr} |\rho_2^{\Gamma}|. \quad (4.10)$$

In particular

$$D_{\Gamma}(\rho \otimes \Phi(d)) = D_{\Gamma}(\rho) + \log_2(d) \quad (4.11)$$

and for any p.p.t. state  $\rho'$

$$D_{\Gamma}(\rho \otimes \rho') = D_{\Gamma}(\rho). \quad (4.12)$$

*Remark 1:* Subtracting  $D_{\Gamma}(\rho_1)$  from the inequality, we obtain the bound  $D_{\Gamma}(\rho) \leq \log_2 \text{Tr} |\rho^{\Gamma}|$  of [5]. (But see Theorem 4.13 below.) See also [16], for an independent rederivation.

*Remark 2:* For other classes of operations, (4.11) is known only when  $D(\rho) > 0$  [3].

Since Definition 1 maximizes over all p.p.t. operations, we can obtain relations between different values of  $\rho$  and (integral)  $K$  by composing with appropriate p.p.t. operations. The next two results extend this. We recall from [9] that for a superoperator  $\Psi$ ,  $\Psi^{\Gamma}$  is defined by

$$\Psi^{\Gamma}(\rho) = \Psi(\rho^{\Gamma})^{\Gamma}. \quad (4.13)$$

Note that  $\Omega(\Psi^{\Gamma}) = \Omega(\Psi)^{\Gamma_{W \otimes W'}}$ , and thus  $\Psi$  is p.p.t. if and only if  $\Psi$  and  $\Psi^{\Gamma}$  are completely positive.

*Theorem 4.7:* For any state  $\rho$ , any  $K > 0$ , and any trace-preserving superoperator  $\Psi$  such that both  $\Psi$  and  $\Psi^{\Gamma}$  are positive

$$F_{\Gamma}(\Psi(\rho); K) \leq F_{\Gamma}(\rho; K). \quad (4.14)$$

*Proof:*

(First proof) Let  $F$  be primal optimal for  $F(\Psi(\rho); K)$ . Then  $\Psi^*(F)$  is primal feasible for  $F(\rho; K)$ , so

$$F_{\Gamma}(\Psi(\rho); K) = \text{Tr}(F\Psi(\rho)) = \text{Tr}(\Psi^*(F)\rho) \leq F_{\Gamma}(\rho; K). \quad (4.15)$$

(Second proof) Let  $D$  be dual optimal for  $F_{\Gamma}(\rho; K)$ . Then

$$F_{\Gamma}(\Psi(\rho); K) \leq \text{Tr}(\Psi(\rho) - \Psi(D))_+ + 1/K \text{Tr} |\Psi(D)^{\Gamma}| \quad (4.16)$$

$$\leq \text{Tr} \Psi((\rho - D)_+) + 1/K \text{Tr} \Psi^{\Gamma}(|D^{\Gamma}|) \quad (4.17)$$

$$= \text{Tr}(\rho - D)_+ + 1/K \text{Tr} |D^{\Gamma}| \quad (4.18)$$

$$= F_{\Gamma}(\rho; K). \quad (4.19)$$

Here we used the facts that for a positive superoperator  $\Psi$  and an arbitrary operator  $\rho$

$$\text{Tr}(\Psi(\rho)_+) \leq \text{Tr}(\Psi(\rho_+)) \quad \text{and} \quad \text{Tr}(|\Psi(\rho)|) \leq \text{Tr}(\Psi(|\rho|)). \quad (4.20)$$

□

*Remark:* It follows from this that we cannot improve on the p.p.t. fidelity by using trace-preserving superoperators  $\Psi$  such that both  $\Psi$  and  $\Psi^{\Gamma}$  are positive. In fact, one can show using the techniques of Section V that any such operator that produces isotropic output must in fact be p.p.t.

*Lemma 4.8:* For any state  $\rho$ , the function  $KF_{\Gamma}(\rho; K)$  is non-decreasing in  $K$ , while the function

$$(KF_{\Gamma}(\rho; K) - 1)/(K - 1) \quad (4.21)$$

is nonincreasing in  $K$ .

*Proof:* We first consider  $KF_{\Gamma}(\rho; K)$ . Writing  $F' = KF$ , we have

$$KF_{\Gamma}(\rho; K) = \max_{F'} \text{Tr}(F'\rho) \quad (4.22)$$

with  $F'$  subject to the constraints

$$0 \leq F' \leq K, \quad -1 \leq F'\Gamma \leq 1. \quad (4.23)$$

Since increasing  $K$  increases the feasible set, the maximum cannot decrease. Dually

$$KF_{\Gamma}(\rho; K) = \min_D K \text{Tr}(\rho - D)_+ + \text{Tr} |D^{\Gamma}| \quad (4.24)$$

which is nondecreasing in  $K$  for any choice of  $D$ .

For  $(KF_{\Gamma}(\rho; K) - 1)/(K - 1)$ , we proceed similarly; taking  $F' = (KF - 1)/(K - 1)$ , we have

$$(KF_{\Gamma}(\rho; K) - 1)/(K - 1) = \max_{F'} \text{Tr}(F'\rho) \quad (4.25)$$

with  $F'$  subject to the constraints

$$-1/(K - 1) \leq F' \leq 1 \quad -2/(K - 1) \leq F'\Gamma \leq 0. \quad (4.26)$$

These constraints become harder to satisfy as  $K$  increases, and thus the maximum cannot increase. Dually

$$(KF_{\Gamma}(\rho; K) - 1)/(K - 1) = \min_D (K \operatorname{Tr}(\rho - D)_+ + \operatorname{Tr}|D^{\Gamma}| - 1)/(K - 1). \quad (4.27)$$

But

$$\begin{aligned} & \frac{1}{K-1} (K \operatorname{Tr}(\rho - D)_+ + \operatorname{Tr}|D^{\Gamma}| - 1) \\ &= \frac{1}{K-1} (K \operatorname{Tr}(\rho - D)_+ + \operatorname{Tr}(D^{\Gamma}) + 2 \operatorname{Tr}(D^{\Gamma})_- - 1) \end{aligned} \quad (4.28)$$

$$= \frac{1}{K-1} (K \operatorname{Tr}(\rho - D)_+ - \operatorname{Tr}(\rho - D) + 2 \operatorname{Tr}(D^{\Gamma})_-) \quad (4.29)$$

$$= \operatorname{Tr}(\rho - D)_+ + \frac{1}{K-1} (\operatorname{Tr}(\rho - D)_- + 2 \operatorname{Tr}(D^{\Gamma})_-). \quad (4.30)$$

This, of course, is nonincreasing in  $K$ , so we are done.  $\square$

For integer  $K$ , this corresponds to composition by the following p.p.t. operations.

*Lemma 4.9:* Let  $I_d(f)$  denote the isotropic state

$$I_d(f) := f\Phi(d) + \frac{1-f}{d^2-1} (1 - \Phi(d)) \quad (4.31)$$

of dimension  $d$  and fidelity  $f$ . If  $f \leq 1/d$ , then for all  $K > 0$

$$F_{\Gamma}(I_d(f); K) = 1/K. \quad (4.32)$$

Otherwise, for  $0 < K \leq d$

$$F_{\Gamma}(I_d(f); K) = 1/K + \frac{fd-1}{d-1} (1 - 1/K) \quad (4.33)$$

and for  $K \geq d$

$$F_{\Gamma}(I_d(f); K) = \frac{fd}{K}. \quad (4.34)$$

*Proof:* For the first claim, take  $F = 1/K$ ,  $D = I_d(f)$ , at which point  $D^{\Gamma} \geq 0$ , so  $\operatorname{Tr}|D^{\Gamma}| = 1$ . For the second claim, take

$$F = 1/K + \frac{d\Phi(d) - 1}{d-1} (1 - 1/K) \quad (4.35)$$

$$D = \frac{1-f}{d^2-1} (1 + d\Phi(d)). \quad (4.36)$$

Finally, for the third claim, take

$$F = \Phi(d) \frac{d}{K} \quad (4.37)$$

$$D = I_d(f). \quad (4.38)$$

In each case, the lower bound coming from  $F$  agrees with the upper bound coming from  $D$ , and thus both  $F$  and  $D$  are optimal.  $\square$

*Remark:* In particular, we have

$$F_{\Gamma}(I_d(f); d) = \max(1/d, f).$$

The fidelity of an entangled isotropic state cannot be increased by p.p.t. operations.

It is instructive to translate the relative entropy bounds of [15], [9] in terms of the dual SDP. We recall the definition

$$S(\rho||\sigma) = -\operatorname{Tr}(\rho(\log_2 \rho - \log_2 \sigma)) \quad (4.39)$$

and the following result.

*Lemma 4.10 [4, Theorem 2.2]:* Let  $\rho, \sigma \in \mathcal{P}(V)$ , with  $\rho$  a state. For  $0 < \epsilon < 1$  and  $n \in \mathbb{Z}^+$ , define

$$\gamma_n(\epsilon) := -\frac{1}{n} \log_2 \min_P \operatorname{Tr}(\sigma^{\otimes n} P) \quad (4.40)$$

where  $P$  ranges over projection operators on  $V^{\otimes n}$  such that  $\operatorname{Tr}(P\rho) \geq 1 - \epsilon$ . Then

$$\liminf_{n \rightarrow \infty} \gamma_n(\epsilon) \geq S(\rho||\sigma) \quad (4.41)$$

$$\limsup_{n \rightarrow \infty} \gamma_n(\epsilon) \leq \frac{1}{1-\epsilon} S(\rho||\sigma). \quad (4.42)$$

*Remark:* In [4], this is stated only when  $\sigma$  is a state; scale invariance gives the result in general. Also, if both  $\rho$  and  $\sigma$  are diagonal, we may restrict  $P$  to be diagonal as well; this is just the analogous result of classical information theory.

We then have the following theorem.

*Theorem 4.11 [9]:* For any state  $\rho$  and any p.p.t. state  $\sigma$

$$D_{\Gamma}(\rho) \leq S(\rho||\sigma). \quad (4.43)$$

*Proof:* We need to show that for any  $x > S(\rho||\sigma)$

$$\limsup_{n \rightarrow \infty} F_{\Gamma}(\rho^{\otimes n}; 2^{xn}) < 1. \quad (4.44)$$

Choose  $y$  between  $x$  and  $S(\rho||\sigma)$ , and consider the dual SDP bound with

$$D = 2^{yn} \sigma^{\otimes n}. \quad (4.45)$$

Then  $D$  is p.p.t., so  $1/K \operatorname{Tr}|D^{\Gamma}| = 2^{(y-x)n} \rightarrow 0$ ; the first term is bounded below 1 by the following lemma.  $\square$

*Lemma 4.12:* Let  $\rho$  and  $\sigma$  be arbitrary states, and let  $y$  be a nonnegative real number. Then

$$\limsup_{n \rightarrow \infty} \operatorname{Tr}(\rho^{\otimes n} - 2^{yn} \sigma^{\otimes n})_+ < 1 \quad (4.46)$$

whenever  $y > S(\rho||\sigma)$ .

*Proof:* Let  $P_n(y)$  be the projection onto the positive part of

$$\rho^{\otimes n} - 2^{yn} \sigma^{\otimes n}. \quad (4.47)$$

Then we need to show that

$$\begin{aligned} F_n(y) &:= \operatorname{Tr}((\rho^{\otimes n} - 2^{yn} \sigma^{\otimes n}) P_n(y)) \\ &= \operatorname{Tr}(\rho^{\otimes n} P_n(y)) - 2^{yn} \operatorname{Tr}(\sigma^{\otimes n} P_n(y)) \end{aligned} \quad (4.48)$$

is bounded below 1. Fix  $\epsilon$  and consider the statement  $F_n(y) \geq 1 - \epsilon$ . For this to be true, we must certainly have

$$\operatorname{Tr}(\rho^{\otimes n} P_n(y)) \geq 1 - \epsilon \quad (4.49)$$

$$\operatorname{Tr}(\sigma^{\otimes n} P_n(y)) \leq 2^{-yn} \epsilon. \quad (4.50)$$

Letting  $y(\epsilon)$  be the largest value of  $y$  such that these inequalities simultaneously hold for infinitely many  $n$ , we conclude by Lemma 4.10 that

$$y(\epsilon) \leq \frac{1}{1-\epsilon} S(\rho||\sigma). \quad (4.51)$$

In particular, if  $y > S(\rho|\sigma)$ , then there exists  $\epsilon$  such that  $y > y(\epsilon)$ , so

$$\limsup_{n \rightarrow \infty} F_n(y) < 1 - \epsilon \quad (4.52)$$

as required.  $\square$

*Remark:* Similarly, using the fact that  $P_n(y)$  is optimal among projections, we can conclude from the other half of Lemma 4.10 that  $\lim_{n \rightarrow \infty} F_n(y) = 1$  when  $y < S(\rho|\sigma)$ . We also have the natural conjecture that the lemma can be strengthened to, say,  $\lim_{n \rightarrow \infty} F_n(y) = 0$  when  $y > S(\rho|\sigma)$ .

This, of course, suggests that we should remove the requirement that  $\sigma$  be p.p.t.; the same proof then gives the following statement.

*Theorem 4.13:* For any states  $\rho$  and  $\sigma$

$$D_\Gamma(\rho) \leq S(\rho|\sigma) + \log_2 \text{Tr} |\sigma^\Gamma|. \quad (4.53)$$

When  $\sigma$  is p.p.t., we recover the previous bound, while when  $\sigma = \rho$ , we obtain the bound of [5] (see the remark following Corollary 4.6 above). Note that we could also have obtained this result using [9, Theorem 1], based on the fidelity bound of Corollary 4.5; this is essentially just the dual of the above proof.<sup>2</sup>

The proof given above was chosen to emphasize the fact that any bound on p.p.t. distillable entanglement can in principle be deduced from the dual SDP bound.

If we define

$$\mathcal{B}(\rho, \sigma) := S(\rho|\sigma) + \log_2 \text{Tr} |\sigma^\Gamma| \quad (4.54)$$

then we have the following.

*Theorem 4.14:* For any states  $\rho$  and  $\sigma$ , and any trace-preserving superoperator  $\Psi$  with both  $\Psi$  and  $\Psi^\Gamma$  positive

$$\mathcal{B}(\Psi(\rho), \Psi(\sigma)) \leq \mathcal{B}(\rho, \sigma). \quad (4.55)$$

For any other state  $\rho'$  and real number  $0 < p < 1$

$$\mathcal{B}(p\rho + (1-p)\rho', \sigma) \leq p\mathcal{B}(\rho, \sigma) + (1-p)\mathcal{B}(\rho', \sigma). \quad (4.56)$$

Finally, we have in general

$$\mathcal{B}(\rho \otimes \rho', \sigma \otimes \sigma') = \mathcal{B}(\rho, \sigma) + \mathcal{B}(\rho', \sigma'). \quad (4.57)$$

*Proof:* Indeed, this is true for each of the functions  $S(\rho|\sigma)$  and  $\log_2 \text{Tr} |\sigma^\Gamma|$  individually, so must be true for their sum.  $\square$

In general,  $\mathcal{B}$  is *not* convex in  $\sigma$ . In particular, we cannot assume that a local maximum of  $\mathcal{B}$  is necessarily a global maximum. This is likely to make it very difficult to explicitly compute  $\min_\sigma (\mathcal{B}(\rho, \sigma))$ , although one can still, of course, obtain bounds from any given value of  $\sigma$ .

## V. EXPLOITING SYMMETRIES

If the state  $\rho$  has a large group of local symmetries, we can greatly simplify the primal and dual SDPs, in several cases to the point of being *linear* programs. The key observation is that, by the proof of Theorem 4.7, we have the following theorem.

<sup>2</sup>M. Horodecki, P. Horodecki, and R. Horodecki (personal communication) have pointed out a third proof via [6, Theorem 2]; it is reasonably straightforward to show that the new bound satisfies their criteria for an upper bound to distillable entanglement.

*Theorem 5.1:* Let  $\Psi$  be a trace-preserving superoperator with both  $\Psi$  and  $\Psi^\Gamma$  positive. Then, for any state  $\rho = \Psi(\rho)$  and any  $K > 0$ , if  $F$  is primal optimal and  $D$  dual optimal for  $F_\Gamma(\rho; K)$ , so are  $\Psi^*(F)$  and  $\Psi(D)$ . In particular, if  $\Psi^2 = \Psi$ , we may assume that  $F$  is  $\Psi^*$ -invariant and  $D$  is  $\Psi$ -invariant.

*Corollary 5.2:* Let  $G$  be any closed subgroup of  $U(k) \otimes U(l)$ , and let  $\rho$  be a  $G$ -invariant state; that is, a state such that for all  $U \in G$ ,

$$U\rho U^\dagger = \rho. \quad (5.1)$$

Then for any  $K > 0$ , there exists primal optimal  $F$  and dual optimal  $D$  invariant under  $G$ . If we further have

$$U_0 \rho^t U_0^\dagger = \rho \quad (5.2)$$

for some  $U_0 \in U(k) \otimes U(l)$  with  $U_0 \overline{GU_0} = G$ , then we may further take

$$U_0 F^t U_0^\dagger = F \quad (5.3)$$

$$U_0 D^t U_0^\dagger = D. \quad (5.4)$$

*Proof:* Let  $\Psi$  be the superoperator

$$\Psi: \rho \mapsto \int_{U \in G} U \rho U^\dagger \quad (5.5)$$

integrating with respect to the uniform probability measure on  $G$ . This is trace-preserving,  $\epsilon$ -local (thus p.p.t.), and satisfies  $\Psi = \Psi^* = \Psi^2$ . The first claim thus follows from the theorem.

Similarly, if  $\Psi'$  is the superoperator

$$\Psi': \rho \mapsto \frac{1}{2} \left( \Psi(\rho) + U_0 \Psi(\rho)^t U_0^\dagger \right) \quad (5.6)$$

then the theorem applies to  $\Psi'$ .  $\square$

*Remark:* In particular, if  $\rho$  is real, then we can take  $U_0 = 1$ , allowing us to force  $F$  and  $D$  to be real as well. If  $\rho = U_0 \rho^t U_0^\dagger$  for some  $U_0$ , we will say that  $\rho$  is pseudoreal.

To apply this, it will be helpful to work in greater generality initially. Suppose simply that  $\rho$  is a Hermitian operator invariant under a subgroup  $G \subset U(k)$ ; we would like an efficient representation of  $\rho$  in which it is still straightforward to test positivity.

Clearly,  $\rho$  is invariant under  $G$  if and only if  $\rho$  commutes with every element of  $G$ . But then  $\rho$  in fact commutes with the algebra  $\mathbb{C}[G]$  of linear combinations of elements of  $G$ . In other words,  $\rho$  must be an element of the centralizer algebra  $A$  of  $\mathbb{C}[G]$ . From representation theory, we have the following lemma.

*Lemma 5.3:* There exists a unitary change of basis exhibiting an isomorphism

$$\mathbb{C}[G] \cong \oplus_\lambda (\text{Mat}(d_\lambda, \mathbb{C}) \otimes 1_{m_\lambda}) \quad (5.7)$$

for appropriate constants  $d_\lambda$  and  $m_\lambda$  such that

$$\sum_\lambda d_\lambda^2 = \dim(\mathbb{C}[G]) \quad (5.8)$$

$$\sum_\lambda m_\lambda d_\lambda = k. \quad (5.9)$$

In the same basis, the centralizer algebra is given by

$$\oplus_\lambda (1_{d_\lambda} \otimes \text{Mat}(m_\lambda, \mathbb{C})). \quad (5.10)$$

In particular, the state  $\rho$  is determined by a set of Hermitian operators  $\rho_\lambda$ , with dimensions  $m_\lambda$ ; furthermore,  $\rho$  is positive if and only if  $\rho_\lambda$  is positive for each  $\lambda$ . Pseudoreality conditions also carry over readily: in an appropriate basis, they produce conditions of the form a)  $\rho_\lambda$  real, b)  $\rho_\lambda = \overline{\rho_\lambda}$ , or c)  $\rho_\lambda$  quaternionic. Finally, we have the trace identity

$$\text{Tr}(\rho\sigma) = \sum_{\lambda} d_{\lambda} \text{Tr}(\rho_{\lambda}\sigma_{\lambda}). \quad (5.11)$$

In particular, our simplification of  $F_{\Gamma}$  above can be viewed as a special case of this, based on the following two examples.

*Example:* Let  $G_i$  be the subgroup of  $U(d^2)$  consisting of operators  $U \otimes \overline{U}$ . Any  $G_i$ -invariant operator can be written in the form

$$\rho = x\Phi(d) + y(1 - \Phi(d)) \quad (5.12)$$

with  $\rho \geq 0$  iff  $x, y \geq 0$ .

Partial-transposing the above example, we get another example.

*Example:* Let  $G_w$  be the subgroup of  $U(d^2)$  consisting of operators  $U \otimes U$ . Any  $G_w$ -invariant operator can be written in the form

$$\rho = \frac{x}{2}(1 + d\Phi(d)^{\Gamma}) + \frac{y}{2}(1 - d\Phi(d)^{\Gamma}) \quad (5.13)$$

with  $\rho \geq 0$  iff  $x, y \geq 0$ .

The following is another important example.

*Example:* Let  $\rho$  be a state of dimension  $d$ . Then the state  $\rho^{\otimes n}$  is invariant under the symmetric group  $S_n$ , acting by permuting the tensor factors. If  $\rho'$  is a generic  $S_n$ -invariant operator, then the blocks  $\rho'_{\lambda}$  are in one-to-one correspondence with the degree  $n$  representations of  $GL_d(\mathbb{C})$ , in such a way that  $\rho^{\otimes n}$  maps to the image of  $\rho$  in the corresponding representation.

If  $\rho$  itself has symmetries, then we can simplify further. If  $A(x, y)$  is a homogeneous polynomial in two variables, then we write

$$A(x, y) \succeq 0 \quad (5.14)$$

to denote the condition that  $A$  has nonnegative coefficients; similarly

$$A(x, y) \preceq B(x, y) \quad (5.15)$$

means that  $B(x, y) - A(x, y)$  has nonnegative coefficients.

*Theorem 5.4:* For any real numbers  $0 \leq f \leq 1$ ,  $K > 0$ , and any integers  $d > 1$ ,  $n > 0$

$$F_{\Gamma}(Id(f)^{\otimes n}; K) = \max_{B, S} B(f, (1-f)/(d^2-1)) \quad (5.16)$$

where  $B(x, y)$  and  $S(x, y)$  range over homogeneous polynomials of degree  $n$  such that

$$0 \leq B(x, y) \leq (x + (d^2 - 1)y)^n \quad (5.17)$$

$$\begin{aligned} & -\frac{1}{K} \left( \frac{d^2 + d}{2} x + \frac{d^2 - d}{2} y \right)^n \\ & \preceq S(x, y) \preceq \frac{1}{K} \left( \frac{d^2 + d}{2} x + \frac{d^2 - d}{2} y \right)^n \end{aligned} \quad (5.18)$$

$$S(x, y) = B \left( \frac{(d+1)x - (d-1)y}{2}, \frac{x+y}{2} \right). \quad (5.19)$$

*Proof:* Let  $F$  be primal optimal for  $F_{\Gamma}(Id(f)^{\otimes n}; K)$  such that  $F$  is invariant under  $S_n$  and  $G_i^n$ . The representations of this group are in one-to-one correspondence with the integers  $0 \leq \lambda \leq n$ , with  $d_{\lambda} = \binom{n}{\lambda} (d^2 - 1)^{\lambda}$  and  $m_{\lambda} = 1$ . Writing

$$B_{\lambda} = d_{\lambda} F_{\lambda} \quad (5.20)$$

$$B(x, y) = \sum_{\lambda} B_{\lambda} x^{n-\lambda} y^{\lambda} \quad (5.21)$$

we have

$$\text{Tr}(F Id(f)^{\otimes n}) = \sum_{\lambda} d_{\lambda} F_{\lambda} (\rho^{\otimes n})_{\lambda} \quad (5.22)$$

$$= \sum_{\lambda} B_{\lambda} f^{n-\lambda} ((1-f)/(d^2-1))^{\lambda} \quad (5.23)$$

$$= B(f, (1-f)/(d^2-1)). \quad (5.24)$$

We next observe that  $0 \leq F$  iff  $0 \leq B(x, y)$  and  $F \leq 1$  iff

$$B(x, y) \preceq \sum_{\lambda} d_{\lambda} x^{n-\lambda} y^{\lambda} = (x + (d^2 - 1)y)^n. \quad (5.25)$$

Similarly, the partial transpose  $F^{\Gamma}$  is invariant under  $S_n$  and  $G_w^n$ . Again the representations are indexed by  $0 \leq \lambda \leq n$ , with

$$d'_{\lambda} = \binom{n}{\lambda} \left( \frac{d^2 + d}{2} \right)^{n-\lambda} \left( \frac{d^2 - d}{2} \right)^{\lambda} \quad (5.26)$$

$$m'_{\lambda} = 1. \quad (5.27)$$

Defining

$$S_{\lambda} = d'_{\lambda} (F^{\Gamma})_{\lambda} \quad (5.28)$$

$$S(x, y) = \sum_{\lambda} S_{\lambda} x^{n-\lambda} y^{\lambda} \quad (5.29)$$

we obtain the condition

$$\begin{aligned} & -\frac{1}{K} \left( \frac{d^2 + d}{2} x + \frac{d^2 - d}{2} y \right)^n \\ & \preceq S(x, y) \preceq \frac{1}{K} \left( \frac{d^2 + d}{2} x + \frac{d^2 - d}{2} y \right)^n. \end{aligned} \quad (5.30)$$

Finally, the relation between  $S(x, y)$  and  $B(x, y)$  obtains by noting that

$$S(x, y) = \text{Tr} \left( F^{\Gamma} \left( \frac{x}{2} (1 + d\Phi(d)^{\Gamma}) + \frac{y}{2} (1 - d\Phi(d)^{\Gamma}) \right)^{\otimes n} \right) \quad (5.31)$$

$$\begin{aligned} & = \text{Tr} \left( F \left( \frac{(d+1)x - (d-1)y}{2} \Phi(d) \right. \right. \\ & \quad \left. \left. + \frac{x+y}{2} (1 - \Phi(d)) \right)^{\otimes n} \right) \end{aligned} \quad (5.32)$$

$$= B \left( \frac{(d+1)x - (d-1)y}{2}, \frac{x+y}{2} \right). \quad (5.33)$$

□

*Remark:* For  $d = 2$ , this linear program appeared in [7] as an upper bound on the fidelity of separable distillation; the observation that it provides a *lower* bound on p.p.t. distillation is new.

Similarly, we get the following.

*Theorem 5.5:* Fix a real number  $0 \leq p \leq 1$  and an integer  $d \geq 2$ , and let  $W_d(p)$  denote the Werner state

$$W_d(p) = \frac{1-p}{d^2+d}(1+T(21)) + \frac{p}{d^2-d}(1-T(21)) \quad (5.34)$$

where  $T(21) = d\Phi(d)^\Gamma$ . Then

$$F_\Gamma(W_d(p)^{\otimes n}; K) = \max_{B,S} B\left(\frac{2(1-p)}{d^2+d}, \frac{2p}{d^2-d}\right) \quad (5.35)$$

where

$$0 \leq B(x, y) \leq \left(\frac{d^2+d}{2}x + \frac{d^2-d}{2}y\right)^n \quad (5.36)$$

$$-\frac{1}{K}(x + (d^2-1)y)^n$$

$$\leq S(x, y) \leq \frac{1}{K}(x + (d^2-1)y)^n \quad (5.37)$$

$$B(x, y) = S\left(\frac{(d+1)x - (d-1)y}{2}, \frac{x+y}{2}\right). \quad (5.38)$$

*Corollary 5.6:* For the antisymmetric Werner state  $W_d(1)$ , we have

$$F_\Gamma(W_d(1); K) = \min\left(1, \frac{d+2}{dK}\right) \quad (5.39)$$

$$D_\Gamma(W_d(1)) = \log_2\left(\frac{d+2}{d}\right). \quad (5.40)$$

For any state  $\rho$

$$F_\Gamma(\rho \otimes W_d(1); K) = F_\Gamma\left(\rho; \frac{dK}{d+2}\right) \quad (5.41)$$

$$D_\Gamma(\rho \otimes W_d(1)) = D_\Gamma(\rho) + D_\Gamma(W_d(1)). \quad (5.42)$$

*Proof:* We observe that

$$\text{Tr}|W_d(1)^\Gamma| = \frac{d+2}{d}.$$

Thus, if we show that  $F_\Gamma(W_d(1); \frac{d+2}{d}) = 1$ , the proof of Corollary 4.3 will apply to give (5.41); taking  $\rho = \Phi(1)$  gives (5.39), and the equations for  $D_\Gamma$  follow immediately. It, thus, remains to show  $F_\Gamma(W_d(1); \frac{d+2}{d}) \geq 1$  (since the other inequality is immediate).

Taking

$$B(x, y) = \left(\frac{d^2+d}{2}\right)\left(\frac{d-2}{d+2}\right)x + \frac{d^2-d}{2}y \quad (5.43)$$

$$S(x, y) = \frac{d}{d+2}(-x + (d^2-1)y) \quad (5.44)$$

we find

$$F_\Gamma\left(W_d(1); \frac{d+2}{d}\right) \geq B\left(0, \frac{2}{d^2-d}\right) = 1. \quad (5.45)$$

□

Similar results apply to “iso-Werner” states—states which are linear combinations of  $1$ ,  $T(21)$ , and  $\Phi(d)$  (invariant under  $O \otimes O$  with  $O \in O(d)$ )—and Bell-diagonal states—states on  $\mathbb{C}^{2 \times 2}$  which are linear combinations of  $\Phi(2)$  and  $\sigma_w \Phi(2) \sigma_w^{-1}$  for  $w \in \{x, y, z\}$ .

Using Theorem 4.14, we can apply the argument of Corollary 5.2 to conclude that when minimizing  $\mathcal{B}(\rho, \sigma)$ , we may insist

that  $\sigma$  possess the symmetries of  $\rho$ . When  $\rho$  is isotropic, we learn nothing new (the earlier bound [7], [15], [9] is unchanged), but when  $\rho$  is Werner, we obtain the following.

*Corollary 5.7:* Fix a real number  $0 \leq p \leq 1$  and an integer  $d > 2$ . Then

$$D_\Gamma(W_d(p)) \leq \min_{\sigma} \mathcal{B}(W_d(p), \sigma)$$

$$= \begin{cases} 0, & 0 \leq p \leq \frac{1}{2} \\ 1+p \log_2(p) \\ \quad + (1-p) \log_2(1-p), & \frac{1}{2} \leq p \leq \frac{1}{2} + \frac{1}{d} \\ \log_2\left(\frac{d-2}{d}\right) + p \log_2\left(\frac{d+2}{d}\right), & \frac{1}{2} + \frac{1}{d} \leq p \leq 1. \end{cases} \quad (5.46)$$

*Proof:* By the above argument, we may assume  $\sigma = W_d(p')$ . Now

$$\begin{aligned} \mathcal{B}(W_d(p), W_d(p')) &= p \log_2\left(\frac{p}{p'}\right) + (1-p) \log_2\left(\frac{1-p}{1-p'}\right) \\ &\quad + \begin{cases} 1, & p' \leq \frac{1}{2} \\ 1 + \frac{2(2p-1)}{d}, & \frac{1}{2} \leq p' \leq 1. \end{cases} \end{aligned} \quad (5.47)$$

We find that the optimal  $p'$  satisfies

$$p' = \begin{cases} p, & 0 \leq p \leq \frac{1}{2} \\ \frac{1}{2}, & \frac{1}{2} \leq p \leq \frac{1}{2} + \frac{1}{d} \\ \frac{p(d-2)}{d+2-4p}, & \frac{1}{2} + \frac{1}{d} \leq p \leq 1. \end{cases} \quad (5.48)$$

Plugging in, we obtain the stated bound. □

*Remark 1:* We observe that this bound is differentiable and convex for  $0 < p < 1$ , and tight for  $p = 1$ .

*Remark 2:* The above bound has recently been independently derived in [1], as the regularized relative entropy of entanglement; that is,

$$\lim_{n \rightarrow \infty} \frac{1}{n} \min_{\sigma \text{ p.p.t.}} S(\rho^{\otimes n} \| \sigma). \quad (5.49)$$

This suggests that the bounds of Theorems 4.11 and 4.13 may regularize to the same bound.

## VI. HASHING ANALOGS

One of the few known lower bounds on distillable entanglement is based on the “hashing” protocol [3]; it will be instructive to consider this bound (for p.p.t. distillation) via the present techniques. The key point of the hashing bound is that on “low-weight” states, it gives fidelity close to 1, while on “high-weight” states, it gives fidelity close to 0. This suggests the reasoning behind the following proof.

*Theorem 6.1:* Fix a fidelity  $\frac{1}{2} \leq f \leq 1$  and an integer  $d > 1$ . Then

$$\begin{aligned} D_\Gamma(I_d(f)) &\geq \max\left(\log_2 d + f \log_2 f + (1-f) \log_2 \frac{1-f}{d+1}, 0\right). \end{aligned} \quad (6.1)$$

*Proof:* Fix an integer  $n > 0$ , and consider the set  $\mathcal{P}_n$  consisting of tensor products

$$P = \otimes_{1 \leq i \leq n} P_i \quad (6.2)$$

with each  $P_i \in \{\Phi(d), 1 - \Phi(d)\}$ ; note, in particular, that  $\mathcal{P}_n$  is a set of mutually orthogonal projections. Since

$$|\Phi(d)^\Gamma| = \frac{1}{d} \quad \text{and} \quad \frac{d-1}{d} \leq |1 - \Phi(d)^\Gamma| \leq \frac{d+1}{d} \quad (6.3)$$

we have

$$|P^\Gamma| \leq d^{-n}(d+1)^{\text{wt}(P)} \quad (6.4)$$

where we define  $\text{wt}(P)$  to be the number of factors equal to  $1 - \Phi(d)$ .

Let us then define an operator

$$F_n(w) = \sum_{\substack{P \in \mathcal{P}_n \\ \text{wt}(P) \leq w}} P. \quad (6.5)$$

We observe that  $F_n(w)$  is a projection, so  $0 \leq F_n(w) \leq 1$ , and that

$$\text{Tr}(F_n(w)(I_d(f)^{\otimes n})) = \sum_{0 \leq i \leq w} \binom{n}{i} f^{n-i}(1-f)^i \quad (6.6)$$

which tends to 1 as  $n \rightarrow \infty$  as long as

$$\omega := \lim_{n \rightarrow \infty} w/n > 1 - f. \quad (6.7)$$

We also compute

$$|F_n(w)^\Gamma| \leq \sum_{\substack{P \in \mathcal{P}_n \\ \text{wt}(P) \leq w}} |P^\Gamma| \leq d^{-n} \sum_{0 \leq i \leq w} \binom{n}{i} (d+1)^i. \quad (6.8)$$

If we take  $\omega < \frac{d+1}{d+2}$ , then we obtain the limit

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{1}{n} \log_2 \left( d^{-n} \sum_{0 \leq i \leq w} \binom{n}{i} (d+1)^i \right) \\ = -\omega \log_2 \omega - (1-\omega) \log_2(1-\omega) \\ + \omega \log_2(d+1) - \log_2(d). \end{aligned} \quad (6.9)$$

But then, by Theorem 3.1, we conclude that

$$D_\Gamma(I_d(f)) \geq \log_2(d) + \omega \log_2 \left( \frac{\omega}{d+1} \right) + (1-\omega) \log_2(1-\omega) \quad (6.10)$$

whenever  $1 - f < \omega < \frac{d+1}{d+2}$ . Since this is decreasing over the range, we obtain the strongest bound by taking the limit as  $\omega \rightarrow 1 - f$ , proving the theorem.  $\square$

*Remark:* When  $d = 2$ , this is precisely the hashing lower bound (albeit weaker, in that it applies only to p.p.t. distillation). However, for  $d > 2$ , the new bound is strictly stronger.

This gives us a general technique for proving lower bounds on p.p.t.-distillable entanglement: approximate the given state as a linear combination of projections with well-controlled partial transposes. Our primary application of this will be to “maximally correlated states” [9]. We recall that a maximally correlated operator is one of the form

$$\rho = \rho_\alpha := \sum_{1 \leq i, j \leq k} \alpha_{ij} |ii\rangle\langle jj| \quad (6.11)$$

for some positive Hermitian operator  $\alpha$ , and similarly for a maximally correlated state. In [9], an upper bound was given on the

p.p.t. distillable entanglement, and the conjecture was made that this bound was tight (even for the 1-locally distillable entanglement). We give a partial resolution of this conjecture.

*Theorem 6.2:* For any maximally correlated state

$$\rho_\alpha = \sum_{i,j} \alpha_{ij} |ii\rangle\langle jj| \quad (6.12)$$

the p.p.t. distillable entanglement is given by the formula

$$D_\Gamma(\rho_\alpha) = B(\alpha) := H(\alpha_{11}, \alpha_{22}, \dots) - S(\alpha). \quad (6.13)$$

*Proof:* That this is an upper bound was shown in [9], so it suffices to prove the lower bound. We construct a protocol in two steps.

First, suppose  $\alpha$  possesses a transitive group of symmetries; that is, a transitive group  $G$  of permutations such that

$$\alpha_{\pi(i)\pi(j)} = \alpha_{ij}, \quad \forall \pi \in G, \quad 1 \leq i, j \leq k. \quad (6.14)$$

(For instance, the operator

$$\alpha = \begin{pmatrix} \frac{1}{3} & \frac{i}{6} & \frac{-i}{6} \\ \frac{-i}{6} & \frac{1}{3} & \frac{i}{6} \\ \frac{i}{6} & \frac{-i}{6} & \frac{1}{3} \end{pmatrix} \quad (6.15)$$

is symmetric under the transitive group  $\mathbb{Z}_3$  of cyclic shifts.) We decompose

$$\alpha^{\otimes n} = \sum_{\lambda \in (0,1]} \lambda p_\lambda(n) \quad (6.16)$$

where  $p_\lambda(n)$  is the orthogonal projection onto the  $\lambda$ -eigenspace of  $\alpha^{\otimes n}$ . Then  $p_\lambda(n)$  is symmetric under the transitive group  $G^n$ , and thus has constant diagonal. If we similarly decompose

$$\rho_\alpha^{\otimes n} = \sum_{\lambda \in (0,1]} \lambda P_\lambda(n) \quad (6.17)$$

we find

$$P_\lambda(n) = \rho_{p_\lambda(n)}. \quad (6.18)$$

We can thus apply the following lemma to  $P_\lambda(n)$ .

*Lemma 6.3:* Let  $\rho = \rho_\beta$  be a maximally correlated operator of dimension  $d \times d$  such that  $\beta$  has constant diagonal. Then

$$|\rho^\Gamma| \leq \frac{\text{Tr}(\rho)}{d}. \quad (6.19)$$

*Proof:* We compute

$$\rho^\Gamma = \sum_{i,j} \beta_{ij} |ij\rangle\langle ji|. \quad (6.20)$$

This is a block matrix with one- and two-dimensional blocks; we thus immediately compute that its eigenvalues are  $\beta_{ii}$  for  $1 \leq i \leq d$ , and  $\pm|\beta_{ij}|$  for  $1 \leq i < j \leq d$ . Since  $\beta$  is positive, we have

$$|\beta_{ij}|^2 \leq \beta_{ii}\beta_{jj} \quad (6.21)$$

and, thus, the largest eigenvalue of  $\rho^\Gamma$  in absolute value is  $\max_{1 \leq i \leq d} \beta_{ii}$ . We thus have

$$\max_{1 \leq i \leq d} \beta_{ii} = \frac{1}{d} \sum_{1 \leq i \leq d} \beta_{ii} = \frac{\text{Tr}(\rho)}{d}. \quad (6.22)$$

$\square$

Now, write

$$P(n, x) = \sum_{x \leq \lambda \leq 1} P_\lambda(n) \quad (6.23)$$

$$x_\epsilon = \inf(\{x \in (0, 1]: \text{Tr}(\rho P(n, x)) > 1 - \epsilon\}). \quad (6.24)$$

Then for  $\epsilon > 0$ , we find that since

$$|P(n, x_\epsilon)^\Gamma| \leq \frac{\text{Tr}(P(n, x_\epsilon))}{d^n} \quad (6.25)$$

we have

$$D_\Gamma(\rho) \geq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} -\frac{1}{n} \log_2 \frac{\text{Tr}(P(n, x_\epsilon))}{d^n} \quad (6.26)$$

$$= \log_2 d - S(\alpha). \quad (6.27)$$

Since

$$H(\alpha_{11}, \alpha_{22} \dots) = H(1/d, 1/d, \dots) = \log_2 d$$

we have proved the theorem in the symmetric case.

To reduce the general case to the symmetric case, we adapt the distillation protocol for pure states given in [2]. Given a word  $w$  in the numbers  $1 \dots k$ , we write  $\text{wt}_i(w)$  for the number of times  $i$  appears in  $w$ . Then our first step is, given

$$\rho_\alpha^{\otimes n} = \sum_{w, w'} \left( \prod_{1 \leq m \leq n} \alpha_{w_m, w'_m} \right) |ww\rangle \langle w'w'| \quad (6.28)$$

to measure  $\text{wt}_i$  for  $1 \leq i \leq k$ . Then the resulting (random) state  $\rho_{\alpha'}$  is maximally correlated, and  $\alpha'$  admits a transitive action of  $S_n$ . Now

$$D_\Gamma(\rho_\alpha) = \frac{1}{n} D_\Gamma(\rho_\alpha^{\otimes n}) \geq \frac{1}{n} \mathbf{E}(D(\rho_{\alpha'})) = \frac{1}{n} \mathbf{E}(B(\alpha')), \quad (6.29)$$

where  $\mathbf{E}(\cdot)$  is the expected value, and the inequality follows from the fact that the measurement is local, so cannot increase the expected distillable entanglement. It thus suffices to show that

$$\mathbf{E}(B(\alpha')) = nB(\alpha) + o(n). \quad (6.30)$$

Now, the measurement has at most  $n^k$  different outcomes, so it gives us at most  $k \log_2 n$  bits of information. But then

$$\mathbf{E}(H(\alpha')) \geq nH(\alpha) - k \log_2 n \quad (6.31)$$

$$\mathbf{E}(S(\alpha')) \leq nS(\alpha) \quad (6.32)$$

so we find

$$\mathbf{E}(B(\alpha')) \geq nB(\alpha) - k \log_2 n = nB(\alpha) + o(n), \quad (6.33)$$

as required.  $\square$

We also have the following general result.

*Theorem 6.4:* Fix a finite-dimensional Hilbert space  $V$ , and let

$$1_{V \otimes V} = \sum_{1 \leq i \leq m} P_i \quad (6.34)$$

be a partition of the identity with the  $P_i$  orthogonal projections. For each  $1 \leq i \leq m$ , let  $s_i$  be the largest eigenvalue of  $|P_i^\Gamma|$ . Then for any state  $\rho \in \mathcal{P}(V \otimes V)$ , we have

$$D_\Gamma(\rho) \geq \sum_{1 \leq i \leq m} r_i (\log_2 r_i - \log_2 s_i) \quad (6.35)$$

where

$$r_i := \text{Tr}(P_i \rho). \quad (6.36)$$

*Proof:* To any subset  $S \subset \{1, 2, \dots, m\}^n$ , we associate a projection

$$P_S = \sum_{w \in S} \bigotimes_{1 \leq i \leq n} P_{w_i} \quad (6.37)$$

which satisfies

$$|P_S^\Gamma| \leq \sum_{w \in S} \prod_{1 \leq i \leq n} s_{w_i}. \quad (6.38)$$

For each  $0 < \epsilon < 1$  and each integer  $n \geq 1$ , let  $\beta_n(\epsilon)$  be the minimum over  $S$  of the largest eigenvalue of  $|P_S^\Gamma|$  subject to the constraint  $\text{Tr}(P_S \rho^{\otimes n}) \geq 1 - \epsilon$ . Then

$$D_\Gamma(\rho) \geq \liminf_{\epsilon \rightarrow 0} \liminf_{n \rightarrow \infty} \frac{-\log_2 \beta_n(\epsilon)}{n} \quad (6.39)$$

(take  $F = P_S$ ). Since

$$\text{Tr}(P_S \rho^{\otimes n}) = \sum_{w \in S} \prod_{1 \leq i \leq n} r_{w_i} \quad (6.40)$$

the theorem follows by the classical analog of Lemma 4.10.  $\square$

## VII. CLONES

In this section, we sketch a possible direction to take in applying the above techniques to 1-local questions (quantum codes and distillation protocols).

*Definition 5:* An operator  $A$  on  $(\mathbb{C}^k)^{\otimes n}$  is an “ $n$ -clone” if it can be written in the form

$$A = \sum_i A_i^{\otimes n} \quad (7.1)$$

where each  $A_i$  is a positive operator, or can be written as a limit of such operators.

For a permutation  $\pi \in S_n$ ,  $T(\pi)$  is the operator on  $(\mathbb{C}^k)^{\otimes n}$  that permutes the tensor factors by  $\pi$ ; when  $\pi = 21 \in S_2$ , this agrees with our earlier notation.

*Theorem 7.1:* Let  $A$  be an  $n$ -clone. Then, for all involutions  $\pi \in S_n$ , and all sets  $S \subset \{1, 2, \dots, n\}$  that intersect each 2-cycle of  $\pi$  exactly once, the following operator is positive:

$$(AT(\pi))^{\Gamma_S}. \quad (7.2)$$

*Proof:* Since nonnegative linear combinations and limits of positive operators are positive, it suffices to prove the result for  $A = A_0^{\otimes n}$ . In that case,  $(AT(\pi))^{\Gamma_S}$  factors as a tensor product of the following operators:

$$A, A^\dagger, \text{ and } ((A \otimes A)T(21))^{\Gamma_2}. \quad (7.3)$$

The first two are clearly positive; that the third is positive is a special case of the following lemma.  $\square$

*Lemma 7.2:* For any operator  $A$  (not necessarily Hermitian), the operator

$$((A \otimes A^\dagger)T(21))^{\Gamma_2} \quad (7.4)$$

is positive.

*Proof:* We have

$$\begin{aligned} ((A \otimes A^\dagger)T(21))^{\Gamma_2} &= ((A \otimes 1)T(21)(A^\dagger \otimes 1))^{\Gamma_2} \\ &= (A \otimes 1)(T(21))^{\Gamma_2}(A^\dagger \otimes 1). \end{aligned} \quad (7.5)$$

Since

$$T(21)^{\Gamma_2} = \dim(A)\Phi(\dim(A)) \geq 0$$

the result follows.  $\square$

For instance, let  $C$  be a quantum code of length  $n$  over an alphabet of size  $k$ , and consider the following average over codes equivalent to  $C$ :

$$W(C) = \mathbf{E}_{C' \sim C}(P_{C'} \otimes P_{C'}). \quad (7.6)$$

This is clearly a 2-clone, so we conclude that the following operators are positive:

$$W(C) \quad W(C)^\Gamma \quad (W(C)T(21))^\Gamma. \quad (7.7)$$

We also find that  $W(C)$  is invariant under operators of the form  $U \otimes U$ , with  $U$  in the semidirect product of  $S_n$  acting on  $U(k)^{\otimes n}$ . Thus, using the techniques of Section V, we conclude that the three given operators are positive if and only if the following three polynomials have nonnegative coefficients:

$$S_C(x, y) := \text{Tr} \left( W(C) \left( x \frac{1-T(21)}{2} + y \frac{1+T(21)}{2} \right)^{\otimes n} \right) \quad (7.8)$$

$$B_C(x, y) := \text{Tr} \left( W(C)^\Gamma \left( \left( x \frac{1}{d} T(21) + y \left( 1 - \frac{1}{d} T(21) \right) \right)^{\otimes n} \right)^\Gamma \right) \quad (7.9)$$

$$A_C(x, y) := \text{Tr} \left( (W(C)T(21))^\Gamma \left( \left( x \frac{1}{d} T(21) + y \left( 1 - \frac{1}{d} T(21) \right) \right)^{\otimes n} \right)^\Gamma \right). \quad (7.10)$$

Using the fact that  $\text{Tr}(M^\Gamma N^\Gamma) = \text{Tr}(MN)$ , we find

$$S_C(x, y) = A'_C \left( \frac{x+y}{2}, \frac{y-x}{2} \right) \quad (7.11)$$

$$B_C(x, y) = A'_C \left( y, \frac{x-y}{d} \right) \quad (7.12)$$

$$A_C(x, y) = A'_C \left( \frac{x-y}{d}, y \right) \quad (7.13)$$

where

$$A'_C(x, y) := \text{Tr}(W(C)(x + yT(21))^{\otimes n}). \quad (7.14)$$

In other words, these are precisely the weight enumerators of  $C$  [13], [8], [10]. In the full linear programming bound for quantum codes, there is an additional inequality

$$B_C(x, y) - \frac{1}{\dim(C)} A_C(x, y) \geq 0. \quad (7.15)$$

To prove this, we simply extend  $C$  to a self-dual code  $C^+$  by encoding half of  $\Phi(\dim(C))$  into  $C$ . We then have

$$A'_{C^+}(x, y, u, v) = A'_C(x, y)u + A'_C(y, x)v \quad (7.16)$$

so

$$\begin{aligned} S_{C^+}(x, y, u, v) &= \frac{S_C(x, y) - S_C(-x, y)}{2} u + \frac{S_C(x, y) + S_C(-x, y)}{2} v \\ & \quad (7.17) \end{aligned}$$

$$\begin{aligned} B_{C^+}(x, y, u, v) &= \frac{1}{\dim(C)} A_C(x, y)u \\ & \quad + \left( B_C(x, y) - \frac{1}{\dim(C)} A_C(x, y) \right) v \\ & \quad (7.18) \end{aligned}$$

$$\begin{aligned} A_{C^+}(x, y, u, v) &= \frac{1}{\dim(C)} A_C(x, y)u \\ & \quad + \left( B_C(x, y) - \frac{1}{\dim(C)} A_C(x, y) \right) v. \\ & \quad (7.19) \end{aligned}$$

In particular, the polynomial  $B_C(x, y) - \frac{1}{\dim(C)} A_C(x, y)$  must have nonnegative coefficients.

We can thus extend the linear programming bound to higher order invariants [12] by using the relevant symmetry group to decompose the operators attached to

$$W_l(C^+) = \mathbf{E}_{C' \sim C^+} P_{C'}^{\otimes l} \quad (7.20)$$

by Theorem 7.1. Note that since  $W_l(C^+)T(\pi) = W_l(C^+)$  for  $\pi \in S_n$ , we have only  $\lfloor \frac{l}{2} \rfloor + 1$  operators to consider.

Another application of the clone concept is to 1-local operations. Fix a Hilbert space  $V_A \otimes V_B$ , and consider the 1-local operation

$$\Psi = \sum_i \mathcal{A}_i \otimes \mathcal{B}_i \quad (7.21)$$

where  $\mathcal{B}_i$  are operations, and  $\mathcal{A}_i$  are completely positive super-operators such that  $\sum_i \mathcal{A}_i$  is an operation. Then, as remarked in [3], we can extend  $\Psi$  to an operation on the larger Hilbert space  $V_A \otimes V_B^{\otimes n}$  by simply taking

$$\Psi^{(n)} = \sum_i \mathcal{A}_i \otimes \mathcal{B}_i^{\otimes n}. \quad (7.22)$$

Note that this depends not just on  $\Psi$  but also on the specific decomposition (7.21). The following is straightforward.

**Lemma 7.3:** For any 1-local operation  $\Psi$ , any integer  $n > 1$ , and any vector  $v \in V_A \otimes V_A$ , the operator

$$\text{Tr}_A \left( (|v\rangle\langle v| \otimes 1) \left( \Psi^{(n)} \left( \Phi(V_A \otimes V_B^{\otimes n}) \right) \right) \right) \quad (7.23)$$

is an  $n$ -clone.

Using Theorem 7.1, we obtain a number of semidefiniteness constraints that  $\Psi^{(2)}$  must satisfy; these constraints can, in principle, be used to obtain bounds on 1-local distillation. (For instance, the argument of [3] can be restated in these terms, although we have not done so.) Unfortunately, the resulting semidefinite programs tend to be fairly complicated, and thus further ideas would seem to be needed. We also note that the cloning argument is quite fragile; if we define an “activated” fidelity

$$\tilde{F}_1(\rho; K) = \limsup_{d \rightarrow \infty} F_1(\rho \otimes \Phi(d); dK) \quad (7.24)$$

after Corollary 4.3, then we can no longer directly use cloning to bound the corresponding distillable entanglement.

We close with the following new application of the cloning argument.

*Theorem 7.4:* Fix a pair of integers  $1 < K < d$ . Then for all fidelities  $1/d < f < 1$ , we have the strict inequality

$$F_1(I_d(f); K) < 1/K + \frac{fd-1}{d-1} (1-1/K). \quad (7.25)$$

*Proof:* Suppose we had equality. A protocol  $\Psi$  attaining this bound would certainly have to be p.p.t.; thus, if we apply this protocol to  $I_d(f')$ , the output fidelity will take the form  $F(f') = af' + b$  for some constants  $a$  and  $b$ , or equivalently

$$F(f') = \frac{d-f'd}{d-1}a' + \frac{f'd-1}{d-1}b' \quad (7.26)$$

for constants  $a', b'$ . Evaluating this at  $f' = 1/d, f' = 1$ , we find

$$a' \leq 1/K \quad b' \leq 1. \quad (7.27)$$

On the other hand, at  $f' = f$ , we have

$$F(f) = (1/K) \frac{d-f'd}{d-1} + \frac{f'd-1}{d-1}. \quad (7.28)$$

Since the coefficients are both positive, we conclude that  $a' = 1/K, b' = 1$ . In particular,  $\Psi$  must take  $I_d(1) = \Phi(d)$  to  $I_K(1) = \Phi(K)$ .

Now, consider the action of  $\Psi^{(2)}$  on the state  $\Phi(d) \otimes \frac{1}{d} 1_d$ . Since  $\Psi$  takes the pure state  $\Phi(d)$  to the pure state  $\Phi(K)$ , we conclude that  $\Psi^{(2)}$  must take  $\Phi(d) \otimes \frac{1}{d} 1_d$  to a state of the form  $\Phi(K) \otimes X$ ; by symmetry, we conclude that  $X = \frac{1}{K} 1_K$ . But

then tracing away the other copy of  $V_B$ , we find that  $\Psi$  takes  $I_d(1/d^2)$  to  $I_K(1/K^2)$ . On the other hand, we have

$$F(1/d^2) = \frac{d+1-K}{dK} > \frac{1}{K^2}. \quad (7.29)$$

We thus obtain a contradiction, and the theorem follows.  $\square$

*Remark:* From [11], it follows that

$$F_1(I_d(f); K) \geq 1/K^2 + \frac{fd^2-1}{d^2-1} (1-1/K^2) \quad (7.30)$$

whenever  $0 < K \leq d$ . Is this lower bound tight?

## REFERENCES

- [1] K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor, “The asymptotic relative entropy of entanglement,” LANL e-print quant-ph/0103096, Mar. 2001.
- [2] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, “Concentrating partial entanglement by local operations,” *Phys. Rev. A*, vol. 53, no. 4, pp. 2046–2052, 1996. LANL e-print quant-ph/9511030.
- [3] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed state entanglement and quantum error correction,” *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996. LANL e-print quant-ph/9604024.
- [4] F. Hiai and D. Petz, “The proper formula for relative entropy and its asymptotics in quantum probability,” *Commun. Math. Phys.*, vol. 143, no. 1, pp. 99–114, 1991.
- [5] M. Horodecki, P. Horodecki, and R. Horodecki, “Asymptotic entanglement manipulations can be genuinely irreversible,” *Phys. Rev. Lett.*, vol. 84, pp. 4260–4263, 2000. See errata at LANL e-print quant-ph/9912076.
- [6] —, “Limits for entanglement measures,” *Phys. Rev. Lett.*, vol. 84, pp. 2014–2017, 2000. LANL e-print quant-ph/9908065.
- [7] E. M. Rains, “Entanglement purification via separable superoperators,” LANL e-print quant-ph/9707002.
- [8] —, “Quantum weight enumerators,” *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1388–1394, 1998. LANL e-print quant-ph/9612015.
- [9] —, “Bound on distillable entanglement,” *Phys. Rev. A*, vol. 60, no. 1, pp. 179–184, 1999. Errata 63(1), 2001; see also LANL e-print quant-ph/9809082.
- [10] —, “Quantum shadow enumerators,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 2361–2366, Nov. 1999. LANL e-print quant-ph/9611001.
- [11] —, “Rigorous treatment of distillable entanglement,” *Phys. Rev. A*, vol. 60, no. 1, pp. 173–178, 1999. LANL e-print quant-ph/9809078.
- [12] —, “Polynomial invariants of quantum codes,” *IEEE Trans. Inform. Theory*, vol. 46, pp. 54–59, Jan. 2000. LANL e-print quant-ph/9704042.
- [13] P. Shor and R. Laflamme, “Quantum analog of the MacWilliams identities for classical coding theory,” *Phys. Rev. Lett.*, vol. 78, no. 8, pp. 1600–1602, 1997. LANL e-print quant-ph/9610040.
- [14] L. Vandenberghe and S. Boyd, “Semidefinite programming,” *SIAM Rev.*, vol. 38, no. 1, pp. 49–95, 1996.
- [15] V. Vedral and M. B. Plenio, “Entanglement measures and purification procedures,” *Phys. Rev. A*, vol. 57, no. 3, pp. 1619–1633, 1998. LANL e-print quant-ph/9707035.
- [16] G. Vidal and R. F. Werner, “A computable measure of entanglement,” LANL e-print quant-ph/0102117.