Entanglement purification via separable superoperators

Eric M. Rains
AT&T Research, Room C290, 180 Park Ave., Florham Park, NJ 07932-0971, USA
(February 16, 1998)

One of the fundamental concepts of quantum information theory is that of entanglement purification; that is, the transformation of a partially entangled state into a smaller-dimensional, more completely entangled state. Of particular interest are protocols for entanglement purification (EPPs) that alternate purely local operations with one- or two-way classical communication. In the present work, we consider a more general, but simpler, class of transformations, called separable superoperators. Since every EPP is a separable superoperator, bounds on separable superoperators apply as well to EPPs; we use this fact to give a new upper bound on the rate of EPPs on Bell-diagonal states, and thus on the capacity of Bell-diagonal channels.

One of the central questions in quantum information theory is that of determining the capacity of quantum channels; that is, the transmission rate below which noiseless transmission of entanglement is possible. In [1], Bennett et al. reduce this problem to that of entanglement purification, the production of maximally entangled states from non-maximally entangled states. In particular, Bennett et al. define two measures of distillable entanglement for a given state $\rho$: $D_1(\rho)$, the rate at which singlet states can be produced from a stream of systems in state $\rho$ using local operations together with one-way classical communication, and $D_2(\rho)$, the rate when two-way classical communication is allowed. While $D_2(\rho)$ is clearly the maximum that can be physically achieved, the set of allowed transformations is extremely complicated. For this reason, we will introduce a third measure $D_4(\rho)$, or separably distillable entanglement, which, while it allows unphysical operations, is more amenable to analysis. In particular, we will derive an upper bound on $D_4(\rho)$, which then immediately gives a bound on $D_2(\rho)$.

Let $\rho$ be a mixed state on a bipartite Hilbert space $V \otimes V$. We define the entanglement fidelity of $\rho$ as

$$F(\rho) = \phi^+(V)\rho\phi^+(V),$$

where $\phi^+(V)$ is the maximally entangled state

$$\frac{1}{\sqrt{\dim(V)}} \sum_{0 \leq i < \dim(V)} |i\rangle \otimes |i\rangle.

(2)

Note that $\phi^+(V)$ does depend on the basis chosen for $V$, but only up to local unitary operations. For any set $S$ of physical transformations, the distillable entanglement $D_S(\rho)$ is defined as the largest number such that there exists a sequence of transformations $P_i \in S$, with $P_i$ mapping states on $V^\otimes n_i$ to states on $W_i$, such that

$$\lim_{i \to \infty} F(P_i(\rho)) = 1$$

and

$$\lim_{i \to \infty} \frac{\log_2 \dim W_i}{n_i} = D_S(\rho).$$

(4)

In other words, $D_S(\rho)$ is the rate at which entanglement can be distilled from a stream of systems in the state $\rho$, using only transformations from $S$. The 1-locally distillable entanglement $D_1(\rho)$ corresponds to the case when $S$ consists of 1-local operations, that is local operations together with one-way classical communication, and analogously for $D_2(\rho)$.

For the new measure $D_4(\rho)$, we take the set $S$ to be the set of separable superoperators. Recall that if $V$ and $W$ are (finite-dimensional) Hilbert spaces, a superoperator (more correctly, a completely positive trace-preserving map) $A$ from $V$ to $W$ is a linear transformation from operators on $V$ to operators on $W$, such that $A \otimes \text{Id}(V')$ maps density operators on $V \otimes V'$ to density operators on $W \otimes V'$, for any $V'$. Clearly, any physical transformation must be a superoperator; moreover, it can be shown [2] that any superoperator is realizable via unitary operations and partial traces. Moreover, a superoperator can always be written in the form

$$\rho \mapsto \sum_i A_i \rho A_i^\dagger,$$

(5)

where the $A_i$ are linear transformations from $V$ to $W$ such that

$$\sum_i A_i^\dagger A_i = \text{Id}(V),$$

(6)

although such representation is by no means unique. If $V = V_1 \otimes V_2$ and $W = W_1 \otimes W_2$, a separable superoperator is one which has a representation of the form (5), in which each $A_i = A_i^{(1)} \otimes A_i^{(2)}$, with $A_i^{(1)}$ a linear transformation from $V_j$ to $W_j$. Clearly, the space of separable superoperators contains that of 1-local superoperators. Since the space of separable superoperators is closed under multiplication, and symmetric under exchanging of $V_1$ and $V_2$, it follows that every 2-local superoperator is separable.

Remark. Separable superoperators were implicitly introduced in [3]. There, however, it was implied that the
space of separable superoperators is identical to the space
of 2-local superoperators, which is certainly not obviously
true (and, indeed, can be shown to be false [4]). It is
quite possible, therefore, that $D_i(\rho)$ is strictly greater
than $D_2(\rho)$ for some states $\rho$.

It will be helpful to observe that there is a natural
correspondence between linear transformations from $V$
to $W$ and vectors in $V \otimes W$. If $|i\rangle$ is an orthonormal
basis of $V$, and $A$ is a linear transformation from $V$ to
$W$, then we define a vector

$$|A\rangle = \sum_i |i\rangle \otimes A|i\rangle = \sqrt{\dim(V)} (|i\rangle \otimes A) \phi^+(V). \quad (7)$$

We have the following identities:

$$|A\rangle = \sqrt{\dim(W)} (A^\dagger \otimes \text{Id}(W)) \phi^+(W) \quad (8)$$
$$\langle A|B\rangle = \text{Tr}(A^\dagger B) \quad (9)$$
$$\text{Tr}_V(|B\rangle \langle A|) = BA^\dagger \quad (10)$$
$$\text{Tr}_W(|B\rangle \langle A|) = (A^\dagger B)^t \quad (11)$$

In particular, it follows that for a superoperator $\mathcal{P}$,

$$\text{Tr}_W(\sum_i |P_i\rangle \langle P_i|) = \text{Id}(V). \quad (12)$$

Fix a separable superoperator $\mathcal{P}$ from $V \otimes V$ to $W \otimes W$, where $V$ is an $n$-qubit Hilbert space, and $W$ has
dimension $K$; to be explicit, take

$$\mathcal{P}(\rho) = \sum_i (P_i^{(1)} \otimes P_i^{(2)}) \rho (P_i^{(1)} \otimes P_i^{(2)})^t. \quad (13)$$

To any state $\rho$ on $V \otimes V$, we can associate a fidelity $F_\mathcal{P}(\rho)$
between 0 and 1, namely the fidelity of $\mathcal{P}(\rho)$. Consider,
in particular, the case in which $\rho$ is the pure state

$$\rho(U) = 2^{-n} |U^t\rangle \langle U^t|, \quad (14)$$

where $U$ is an arbitrary unitary operation. Then

$$F_\mathcal{P}(U) \overset{\text{def}}{=} F_\mathcal{P}(\rho(U)) \quad (15)$$
$$= \frac{1}{2^{nK}} \sum_i \left| \text{Tr}(\text{Id}(W)(P_i^{(1)} U \otimes P_i^{(2)}) |P_i^{(1)} \otimes P_i^{(2)})(W) \right|^2$$
$$= \frac{1}{2^{nK}} \sum_i \left| \text{Tr}(P_i^{(1)} (U \otimes \text{Id}(W)) |P_i^{(2)})(W) \right|^2 \quad (16)$$
$$= \frac{1}{2^{nK}} \sum_i \text{Tr}(\rho_i^{(1)} (U \otimes \text{Id}(W)) \rho_i^{(2)} (U^t \otimes \text{Id}(W))), \quad (17)$$

where

$$\rho_i^{(1)} = |P_i^{(1)}\rangle \langle P_i^{(1)}|, \quad (18)$$

and similarly for $\rho_i^{(2)}$. In particular, $\rho_i^{(1)}$ and $\rho_i^{(2)}$ are positive semi-definite Hermitian operators on $V \otimes W$.

If $\rho$ is a mixture of states of the form $\rho(U)$, then $F_\mathcal{P}(\rho)$
can be written as a linear combination of the relevant
$F_\mathcal{P}(\rho(U))$. Of particular interest is the case of the “depo-
larizing” qubit state; that is, the state $\Delta(\epsilon)$ with density matrix

$$\frac{\epsilon}{4} \text{Id} + \frac{1-\epsilon}{2} (|0\rangle \langle 0| + |1\rangle \langle 1|), \quad (19)$$
on a two-state Hilbert space. We can also write

$$\Delta(\epsilon) = f \rho(1) + \frac{1-f}{3} (\rho(\sigma_x) + \rho(\sigma_y) + \rho(\sigma_z)), \quad (20)$$
with $f = 1 - (3/4) \epsilon = F(\Delta(\epsilon))$. We can then write:

$$F_\mathcal{P}(\Delta(\epsilon)^{\otimes n}) = \sum_j f^j \left( \frac{1-f}{3} \right)^{n-j} \sum_{\text{wt}(E)=j} F_\mathcal{P}(E), \quad (21)$$

where $E$ ranges over the set $\mathcal{E}$ of tensor products of matrices
from the set $\{1, \sigma_x, \sigma_y, \sigma_z\}$, and $\text{wt}(E)$ is the number
of components in the tensor product not equal to the identity.
The quantity

$$B_j(\mathcal{P}) = \sum_{\text{wt}(E)=j} F_\mathcal{P}(E) \quad (22)$$
has a form very similar to that of the weight enumerators
studied in [5] and [6]; this suggests that we should consider
the quantity

$$B'_S(\mathcal{P}) = \frac{1}{2^n K} \sum_i \text{Tr}(\text{Tr}_S(\rho_i^{(1)})) \text{Tr}_S(\rho_i^{(2)})), \quad (23)$$
where $\text{Tr}_S(\rho)$ is the partial trace of $\rho$ with respects to the
qubits of $V$ indexed by $S$, as well as $W$ if $0 \in S$. We can
then define a polynomial

$$B'(u, v, x, y) = \sum_{i \neq j} x^i y^{n-i} \sum_{s \subseteq \{i \neq j\}, \text{wt}(s) = n} (u B'_S(\mathcal{P}) + v B'_{\{0\} \cup S}(\mathcal{P})). \quad (24)$$

The arguments in [6] tell us that

$$B'(1, 0, x - y, 2y) = B(x, y) = \sum_i B_i(\mathcal{P}) x^i y^i. \quad (25)$$

On the other hand,

$$B'_{\{0\} \cup S}(\mathcal{P}) = \frac{1}{2^n K} \sum_i \text{Tr} \left( \text{Tr}_S(\text{Tr}_W(\rho_i^{(1)})) \text{Tr}_S(\text{Tr}_W(\rho_i^{(2)})) \right) \quad (26)$$
$$= \frac{1}{2^n K} \sum_i \langle \text{Id} | \text{Tr}_{S \times S} (\text{Tr}_W(\rho_i^{(1)} \otimes S)(\rho_i^{(2)})) | \text{Id} \rangle \quad (27)$$

Since $\mathcal{P}$ is a superoperator, (12) tells us that

$$\sum_i \text{Tr}_W(\rho_i^{(1)} \otimes S)(\rho_i^{(2)})) = \text{Id}(V \otimes V). \quad (28)$$
It follows that

\[ B'_{(0,1,S)}(P) = 2^{|S|}/K, \]  

and thus that

\[ B'(u, v, x, y) = uB(x + y/2, y/2) + v(x + 2y)^n/K. \]  

Since each \( \rho_i^{(1)} \) and \( \rho_i^{(2)} \) is positive semi-definite, the theory of weight enumerators \([6]\) tells us that the polynomials \( B'(u - v, Kv, x - y, 2y) \) and \( B'(v - u, u + v, y - x, x + y) \) have nonnegative coefficients; note that the latter is the analogue of the “shadow” enumerator, which was shown to be nonnegative in \([7]\). These polynomials can be written in terms of \( B(x, y) \), using (30):

\[
\begin{align*}
B'(u - v, Kv, x - y, 2y) &= uB(x, y) + v((x + 3y)^n - B(x, y)), \\
B'(v - u, u + v, y - x, x + y) &= u(1/K)(x + 3y)^n - S(x, y)) \\
&
\end{align*}
\]

where

\[ S(x, y) = B(3x - 3y/2, x + y/2). \]

Since both of those polynomials have nonnegative coefficients, we can conclude that the four polynomials

\[ B(x, y), (x + 3y)^n - B(x, y), \]

\[ 1/K(3x + 3y)^n - S(x, y), 1/K(x + 3y)^n + S(x, y), \]

each have nonnegative coefficients. The first two polynomials simply correspond to the fact that

\[ 0 \leq F_p(E) \leq 1 \]

for all \( E \). The second pair of polynomials roughly say that

\[ |S_p(E)| \leq 1/K, \]

for an appropriate definition of \( S_p(E) \); it is not clear what, if anything, this corresponds to physically.

We can now begin to obtain bounds on \( D_s \):

**Theorem 1** Let \( P \) be a separable superoperator from \( V \otimes V \) to \( W \otimes W \), where \( V \) is an \( n \)-qubit Hilbert space, and \( W \) is a \( K \)-dimensional Hilbert space. Then for any \( f \leq 1/2 \),

\[ F_p(f) \overset{\text{def}}{=} F_p(\Delta((4/3)(1-f))) \leq 1/K. \]  

In particular, \( D_s(f) = 0 \).

**Proof.** We have:

\[ F_p(f) = B(f, 1 - f/3) \]

\[ = S(1/2 - f, 1/6 + f/3). \]

Now, the coefficients of \((x + 3y)^n/K - S(x, y)\) are nonnegative, so, for any specific numbers \( x, y \geq 0 \),

\[ (x + 3y)^n/K \geq S(x, y). \]

In particular, this is true for \( x = (1/2) - f \) and \( y = (1/6) + (f/3) \); the result follows immediately. QED

In particular, we obtain the known fact that distillation is impossible for \( f \leq 1/2 \). Moreover, we obtain the following:

**Corollary 1** If \( \rho \) is a separable state on \( W \otimes W \), where \( W \) has dimension \( K \), then \( \rho \) has fidelity at most \( 1/K \). In particular, for any separable state \( \chi \), and any separable superoperator \( P \), \( F_p(\chi) \leq 1/K \).

**Proof.** Suppose, on the other hand, that \( \rho \) had fidelity greater than \( 1/K \). Since \( \rho \) is separable, we could then produce a \( K \times K \)-dimensional bipartite state of fidelity greater than \( 1/K \) from any input state, using only local operations and classical communication. But this contradicts the bound (36). The second statement follows from the fact that the image of a separable state under a separable superoperator is separable. QED

It should also be noted that (36) is tight, since a uniformly distributed ensemble of states \( \psi \otimes \psi \) is certainly separable, and is easily shown to have fidelity \( 1/K \); the argument of the corollary then applies in reverse to construct a separable superoperator of fidelity \( 1/K \).

So far, we have not used the first two constraints. It turns out that these can be used to control how much the output fidelity of a given superoperator can vary as the input fidelity changes. In particular, we will be able to establish, for each rate, a neighborhood of \( f = 1/2 \) for which the output fidelity must still tend to 0.

**Theorem 2** Let \( f \geq 1/2 \). The separably distillable entanglement \( D_s(f) \) of the depolarizing state \( \Delta(\epsilon) \) with fidelity \( f \), satisfies the bound

\[ D_s(f) \leq 1 - H_2(f) \]

\[ = 1 + f \log_2(f) + (1-f) \log_2(1-f). \]

Indeed, any family of separable superoperators of rate greater than \( 1 - H_2(f) \) must have output fidelity tending to 0.

**Proof.** Suppose the theorem were false. Then there would exist a sequence of separable superoperators \( \{P_i\} \), producing a \( K_1 \times K_1 \) bipartite state from \( n_1 + n_2 \) qubits such that \( F_{P_i}(f) \) did not tend to 0, and such that
\( \log_2(K_i)/n_i \) tended to a limit strictly greater than \( 1 - H_2(f) \).

Consider \( B(f, \frac{1-f}{3}) \). For a fixed value of \( B(f, \frac{1-f}{3}) \), the lowest possible value of \( B(1/2, 1/6) \) (ignoring all other constraints) is attained when the weight of the \( B \), is concentrated at low \( i \); these are the coefficients for which \( f'((1-f)/3)^{n-i} \) is decreased the most when \( f \) is replaced by \( 1/2 \). In that case, we have:

\[
B(f, \frac{1-f}{3}) \simeq \sum_{0 \leq i < j} \binom{n}{i} f^i (1-f)^{n-i} \tag{42}
\]

for some \( j \). In order for this not to tend to 0 as \( n \) increases, we must have \( j \geq n(1-f) \). But then

\[
B(\frac{1}{2}, \frac{1}{6}) \simeq 2^{-n} \sum_{0 \leq i < j} \binom{n}{i}, \tag{43}
\]

so

\[
B(\frac{1}{2}, \frac{1}{6}) \simeq 2^n \left( H_2(j/n) - 1 \right) \simeq 2^n \left( H_2(f) - 1 \right). \tag{44}
\]

On the other hand, by (36), we know \( B(1/2, 1/6) \leq 1/K \). But then

\[
\log_2(K)/n \lesssim 1 - H_2(f). \tag{45}
\]

QED

This bound is plotted in Figure 1, as well as the weaker bound

\[
D_2(f) \leq E(f) = H_2(\frac{1}{2} + \sqrt{f(1-f)}) \tag{46}
\]

from [1]. In particular, note that the new bound is strictly stronger than the old bound ("entanglement of formation") for \( 1/2 < f < 1 \). Since every 1-local operator is separable, we also get the bound \( D_2(f) \leq 1 - H_2(f) \), which actually improves on the best known upper bounds, for some range of \( f \). For \( 1/2 \leq f \leq 3/4 \), it is known that 1-local operators cannot achieve fidelity close to 1 at any positive rate; if this could be strengthened to more precise bounds on fidelity, the above technique would then provide bounds on \( D_2(f) \) for \( f \geq 3/4 \).

The above argument can be extended to arbitrary Bell-diagonals states; to bound \( D_4(\chi) \) where \( \chi \) is Bell-diagonal with eigenvalues \( \beta_0 \geq \beta_1 \geq \beta_2 \geq \beta_3 \), with \( \beta_0 \geq 1/2 \), simply compare \( \chi \) to the separable Bell-diagonal state \( \chi_0 \) with eigenvalues \( 1/2, \beta_1/(2-2\beta_0), \beta_2/(2-2\beta_0), \) and \( \beta_3/(2-2\beta_0) \). The separability of \( \chi_0 \) implies, by corollary 1, that \( F_\pi(\chi_0) \leq 1/K \); but then (34) allows us to deduce that \( F_\pi(\chi) \) tends to 0 unless

\[
\frac{\log_2(K)}{n} \lesssim 1 - H_2(\beta_0). \tag{47}
\]

In other words, \( D_4(\chi) \leq 1 - H_2(\beta_0) \). Note that this bound is tight in the case \( \beta_2 = \beta_3 = 0 \); in this case, the noise is purely classical in nature, and can be corrected using classical codes.

Vedral and Plenio [8] have independently proved (assuming a certain additivity conjecture) a more general bound on \( D_4 \), which apparently agrees with (47) on Bell-diagonal states.

The author would like to thank André Berthiaume for helpful comments, as well as David DiVincenzo, Peter Shor, and John Smolin for helpful conversations about separable superoperators.

\[ \begin{array}{c|c|c}
\hline
f & 1 - H_2(f) & E(f) \\
\hline
0.1 & 0.4 & 0.4 \\
0.2 & 0.6 & 0.6 \\
0.3 & 0.8 & 0.8 \\
0.4 & 1.0 & 1.0 \\
\hline
\end{array} \]

FIG. 1. Bounds on \( D_2(f) \)