PHYSICAL REVIEW A **86**, 022328 (2012)

Hybrid zero-capacity channels

Sergii Strelchuk
Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom

Jonathan Oppenheim
Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom,
University College of London, Department of Physics & Astronomy, London, WC1E 6BT, United Kingdom, and
London Interdisciplinary Network for Quantum Science, London, United Kingdom
(Received 5 July 2012; published 24 August 2012)

There are only two known kinds of zero-capacity channels. The first kind produces entangled states that have positive partial transpose; and the second, states that are cloneable. We consider the family of "hybrid" quantum channels, which lies in the intersection of the above classes of channels and we investigate its properties. This study gives rise to explicit examples of the channels which create bound entangled states that have the property of being cloneable to the arbitrary finite number of parties. Hybrid channels provide an example of highly cloneable binding entanglement channels for which known superactivation protocols must fail; superactivation is the effect where two channels, each with zero quantum capacity, have positive capacity when used together. We give two methods to construct a hybrid channel from any binding entanglement channel. We also find the low-dimensional counterparts of hybrid states: bipartite qubit states which are extendible and possess two-way keys.

DOI: 10.1103/PhysRevA.86.022328 PACS number(s): 03.67.Hk

I. INTRODUCTION

In classical information theory, channels which cannot convey information are boring. The only such channel which has this property is the one where there is no correlation between the input and the output. In contrast, in quantum information theory, such channels (called zero-capacity channels) have a very rich and ill-understood structure. There is a wide and largely unexplored variety of channels which cannot reliably send quantum information. We do not yet know how to characterize such channels, and thus far, there are only two methods known to determine if a channel has zero capacity. One criterion is if the channel produces states that have positive partial transpose (PPT) [1,2], in which case the channel produces states which cannot be distilled into pure state entanglement [3]. A second criterion is if the channel produces states which would lead to cloning [4]; i.e., imagine that the states ψ^{ABE} are produced by the channel, with A being the subsystem held by the sender, B the subsystem by the output of the channel, and E the environment. If the channel has the structure that any state at B could be recreated at E, then we know that the channel must have zero capacity because if arbitrary states could be sent to B, then they would be cloned at E, which we know to be impossible [5].

We believe that there are other kinds of zero-capacity channels, for example, the channels which produce an equal mixture of the Bell states, tensored with separable hiding states as in [6], although there is no proof of this. However, even if we restrict our attention to the two classes of known zero-capacity channels, our current understanding is woefully inadequate. For example, recently it was shown that the lack of capacity of these two classes of channels is only the beginning of the story. Although each class of channel individually has zero capacity, if they are used jointly, they are able to convey quantum information to the receiver. It is as if $0+0=1$. This effect, termed *superactivation*, was discovered by Smith and Yard [7] for two zero-capacity quantum channels: One is the PPT quantum channel which can produce private keys [6]. The second channel is from the class of cloning channels, i.e., symmetric channels which create states ψ^{ABE} which are unchanged after switching B and E. We say that the resulting reduced state ρ^{AB} is 2 extendible, because it has the property of one of the subsystems being cloneable, i.e., we can make a copy of B on a second system E (in this case, just the state ψ^{ABE}). If we can make $k-1$ copies of the state on B, then we say that the state is k-extendible.

The kinds of cloning channels which can be used in superactivation have been extended in [8], but it is still an important open question as to what sorts of channels and what combinations of them can be superactivated. At the moment, however, we do not even know whether all channels that produce PPT bound entangled states can be superactivated. We make progress in showing the opposite, by focusing our attention on the special set of channels that produce states which are both PPT bound entangled and simultaneously cloneable. Since superactivation using these two classes of channels requires one channel from each class, channels which are both PPT and cloneable would only be superactivatable if a third class of zero-capacity channels existed.

The set of states which are both 2-extendible and PPT was shown to be nonempty [9], but the example together with the proof that this state has the above properties was complicated and nonintuitive. In our paper, we construct some simple examples and investigate the overlap between the two classes of channels. Moreover, we investigate the overlap of a much broader set of channels that are not merely 2-extendible but also k-extendible for any $k \geqslant 2$, and we produce an explicit constructive example of the channels from this set for each k. We term them *hybrid* channels. Previously, for $k \geqslant 3$ such channels were only proven to exist [9], but no examples were known. Here, we exhibit a method which can produce an entangling, k-extendible, PPT channel, starting from any entangling PPT channel.

It will be easier to talk about quantum channels in terms of states associated with them by virtue of the Choi-Jamioklowski (CJ) isomorphism, which imparts the properties of the states produced by the channel to those of its CJ state.

The problems of characterization of the set of bound entangled states as well as the set of k-extendible states are currently open. The latter problem is closely related to the problem of separability of quantum states, as the set of bound entangled states with PPT and that of extendible states approach the set of separable states under certain asymptotic conditions. Such lack of structure in describing both sets makes constructing hybrid channels interesting and challenging at the same time.

Arguably, one of the strongest tests for separability is the one introduced by Doherty *et al.* [9]. There, authors check for the presence of certain necessary conditions held by all separable states—the existence of the k-symmetric extensions with PPT—by solving a semidefinite program. The test itself consists of a sequence of steps performed in succession: at ith step we attempt to construct the ith extension of the quantum state by solving a semidefinite program. If at some step i_0 we fail to construct the i_0th extension for the original state, then we conclude that the state is entangled and provide an entanglement witness for it. This test is known to be complete in the sense that running it for n rounds as $n \to \infty$ we are guaranteed that if the state is entangled we will stop after a finite number of rounds. However, the size of the semidefinite program grows exponentially with the number of extensions we want to construct.

Symmetric extendibility appears in numerous other important applications. It proved to be a useful tool for analysis of the protocols that distill a secure key from quantum correlations [10]. Procedures which increase security in such protocols inherently depend on the ability to break the symmetric extension, because failure to do so could result in an adversary holding one of the extensions thereby compromising the security of the protocol. At the moment, there exist no criterion for the bipartite state to be extendible; however, some partial results that provide sufficient criteria have been discovered [11].

Motivated by the CJ states of different zero-capacity channels used in the original superactivation scenario, in Sec. II we introduce a new one-parameter family of so-called hybrid states, which simultaneously possesses the properties of the two channels in the superactivation example. The CJ state of the first channel has PPT and is bound entangled, and that of the other is 2-extendible, which can be made to be k-extendible by a simple manipulation. Hybrid states and hybrid channels get their name for incorporating those crucial properties of both channels. This family has an entirely different structure compared to the one introduced in [9], where the authors provide the numerical example of a 2-extendible entangled state with PPT and give the proof of existence of the entangled states with PPT which pass the kth test. We provide a simple and explicit scalable construction of k-extendible bound entangled states with PPT, which for any fixed k pass all steps of the separability test up to $(k+1)$st. The proof that our family of states is entangled as well as the distillation protocol is interesting in its own right, since we equip parties with such nonentangling resources as backward unidirectional classical communication together with a backward 50% erasure channel. Following the construction, we investigate the properties of these states, and segregate a family of hybrid states that become more like separable states in the sense that their degree of extendibility increases with the dimension, yet they are far from the set of all separable states. Finally, we show how to make our family of hybrid states, which are extendible with respect to one of the subsystems, into hybrid states that are extendible with respect to both of the subsystems.

In Sec. III we show that hybrid channels constitute examples of channels which produce bound entangled states which cannot be activated by any of the known protocols known to date. Finally, in Sec. IV, we discuss low dimensional hybrid states that are suitable for generating in the laboratory. We explore which of the features of bipartite hybrid states remain when we constrain the dimension of the Hilbert space to be $2 \otimes 2$. It turns out that despite the low dimension, there exist quantum states which are reminiscent of the hybrid states, having two seemly antithetical properties of being 2-extendible and having two-way distillable secret keys. These qubit states present examples of $2 \otimes 2$ systems which are the analogs of the hybrid states in the sense that they demonstrate a relationship between extendibility and the classical key in the absence of PPT, which is similar to that of extendibility and bound entanglement. These states, being low dimensional and therefore more feasible to create in the laboratory, may be of interest to experimenters seeking to incorporate them into a variety of key distribution protocols.

II. BOUND ENTANGLED *K*-EXTENDIBLE STATES

In this section we construct a family of states which have PPT and are k extendible by a particular composition of the states, each with one of the two properties. Depending on which state we take as a starting point for our construction we get two different families with both properties.

In the first case we start with the CJ state of the erasure channel. Then we modify it by replacing the singlet by the CJ state of the binding entanglement channel, which is a bound entangled state with PPT, to obtain the state which retains the property of being k extendible and in addition becomes PPT. In the second case we start with the CJ state of a particular binding entanglement channel and further replace part of the former with the CJ states of the erasure channel. Again, we obtain a bound entangled state with PPT.

We will further consider two quantum channels. The first one, denoted as $\mathcal{N}_\phi$, is a channel which produces bound entangled states ϕ^{AB} with maximally mixed reductions. Its CJ state is PPT. The second channel is the erasure channel $\mathcal{N}_e^p(\rho) = p\rho + (1-p)|e\rangle\langle e|$, which with probability p faithfully transmits the input state to the receiver and with probability $1-p$ outputs a flag signaling that erasure took place.

In the Secs. II A and II B, we show two ways to construct the state with the properties above. Then in Sec. II C, we study the properties of these families, and in Sec. II D, we provide the way for a more flexible construction that admits extensions on both of the parties.

A. Mixing erasure-like states

We turn to constructing the k-extendible states that have the form similar to that of the erasure channel. Consider the CJ state of the $\mathcal{N}_e^{\frac{1}{k}}$:

$$\theta_+^{AB} = \frac{1}{k}\Phi_+^{AB} + \frac{k-1}{k}\mathbb{1}^A \otimes \sigma^B, \tag{1}$$

where $\sigma^B = |e\rangle\langle e|$ is the erasure flag. Now, we construct the higher-dimensional analog of θ_+^{AB}, inserting instead of the maximally entangled state any bipartite bound entangled state with PPT ϕ^{AB} and $\mathrm{Tr}_A\phi^{AB} = \mathbb{1}^B$, $\mathrm{Tr}_B\phi^{AB} = \mathbb{1}^A$, where the subsystems AB are trivially extended to the larger Hilbert space $AA'BB'$:

$$\rho^{ABA'B'} = \frac{1}{k}\phi^{AA'BB'} + \frac{k-1}{k}\mathbb{1}^{AA'} \otimes \sigma^{BB'}. \tag{2}$$

The quantum channel, whose CJ state has the form of $\rho^{ABA'B'}$, is an erasure-like channel in the sense that applying it with probability $\frac{1}{k}$ results in Alice and Bob sharing a bound entangled state $\phi^{AA'BB'}$, which has PPT, and the other half of the time Bob receives the erasure flag $\sigma^{BB'}$ (encoded in subspace B'), orthogonal to the support of the $\phi^{AA'BB'}$. The following lemma shows that the state (2) has indeed the desired properties, being a constructive example of a bound entangled state with PPT, which is extendible to arbitrary many parties:

Lemma 1. The state $\rho^{ABA'B'}$ defined in Eq. (2) is k extendible with respect to the subsystem BB', has PPT, and is bound entangled.

Proof. To show that the state is k extendible, we first construct a 2-extension of $\rho^{AA'BB'}$ with respect to the BB' subsystem:

$$\rho^{AA'BB'EE'} = \tfrac{1}{2}\rho^{AA'BB'} \otimes \sigma^{EE'} + \tfrac{1}{2}\rho^{AA'EE'} \otimes \sigma^{BB'}. \tag{3}$$

Noting that $\mathrm{Tr}_{BB'}\rho^{AA'BB'} = \mathbb{1}^{AA'}$, we have $\rho^{AA'BB'} \cong \mathrm{Tr}_{BB'}\rho^{AA'BB'EE'} \cong \mathrm{Tr}_{EE'}\rho^{AA'BB'EE'}$, where the corresponding reductions denote different subsystems isomorphic to each other. Therefore, the state is 2 extendible. In the same way we construct the k extension of Eq. (2):

$$\rho^{AA'\overline{BB'}} = \frac{1}{k}\sum_{i=1}^{k} \rho^{AA'B_iB_i'} \otimes \sigma^{\overline{BB'}\backslash B_iB_i'}, \tag{4}$$

where $\overline{BB'} = B_1B_1' \dots B_kB_k'$, and $\overline{BB'}\backslash B_iB_i'$ denotes the exclusion of B_iB_i' from $\overline{BB'}$.

To show that $\rho^{AA'BB'}$ has PPT it suffices to show that each of the summands has PPT. The state $\phi^{AA'BB'}$ has PPT by definition, and the second summand of $\rho^{AA'BB'}$ represents a separable state, hence it has PPT.

Finally, we need to show that the state $\rho^{ABA'B'}$ is bound entangled. Consider two parties Alice and Bob each holding subsystems AA' and BB' and communicating over a classical channel from Bob to Alice. Bob performs a measurement $M = \{M_0, M_1\}$ with $M_0 = \mathbb{1} - |e\rangle\langle e|$ and $M_1 = |e\rangle\langle e|$ on B', where $|e\rangle$ is the erasure flag, and Bob tells Alice the outcome of the measurement over the classical channel from Bob to Alice. When M_1 is measured, they abort the protocol. Otherwise, they know that they share $\phi^{AA'BB'}$, which is bound entangled. Given that parties cannot create entanglement using a backward classical communication channel alone, this shows that the original state is entangled. ■

For the state (2) to be useful in the protocols requiring entanglement distillation from the shared quantum state, e.g. proving to a third party that they indeed share the state which has some bound entanglement, Alice and Bob need an additional resource, because a classical communication channel from Alice to Bob is insufficient to distill entanglement from the bound entangled state. One might think that equipping the parties with some auxiliary communication resource may be of some help, but clearly this must be a resource with which the parties are incapable of creating entanglement, but only can distill it from their shared state. As we show below, there exists a special class of bound entangled states with PPT and auxiliary communication resource in the form of the 50% erasure channel from Bob to Alice, which enables the parties to distill pure-state entanglement from their shared state.

To overcome the limitation, we consider quantum states which contain d bits of secrecy. They are called private dits (pdits) or twisted ebits and have the generic form [6]

$$\gamma^{(d)} = U P_+^{AB} \otimes \sigma^{A'B'} U^\dagger, \tag{5}$$

where $U = \sum_{i,j=0}^{d-1} |ij\rangle\langle ij|^{AB} \otimes U_{ij}$ is a controlled unitary operation termed *twisting* (with arbitrary unitaries U_{ij}); P_+^{AB} is the projector onto a d-dimensional maximally entangled state $\Phi_+^{AB} = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle^{AB}$; and $\sigma^{A'B'}$ is an arbitrary state called the "shield" subsystem of dimension d', because its presence protects private correlations. In the case when $d = 2$ we will call it a private bit (pbit). Parties that have A and B subsystems of a pdit (known as the "key") can extract $\log_2 d$ ebits by performing $U^\dagger$ if one of them possesses the shield $A'B'$ in its entirety. However, when the shield is split between the two parties, it can be impossible to perform the untwisting using only local operations, and there exist states which are arbitrarily close to pdits, yet no ebits can be produced from them, as they have PPT. For the purposes of our task we construct pbit to be of a particular form [6]:

$$\begin{aligned}\gamma_\pm^{(d)AA'BB'} &= \frac{p}{2}\left(\Phi_\pm^{AB} \otimes \tau_1^{A'B'} + \Phi_\mp^{AB} \otimes \tau_2^{A'B'}\right)\\ &\quad + (1-p)\omega_{\mathrm{sep}}^{AB} \otimes \tau_2^{A'B'}.\end{aligned} \tag{6}$$

Here $p \in (\frac{1}{4},\frac{1}{3})$, and $\tau_1^{A'B'} = \frac{1}{2^k}(\rho_s + \rho_a)^{\otimes k}$ and $\tau_2^{A'B'} = \rho_s^{\otimes k}$ denote Werner hiding states with $\rho_s = \frac{2}{d^2+d}P_s$ and $\rho_a = \frac{2}{d^2-d}P_a$ with $P_\mathrm{s}, P_\mathrm{a}$ denoting projectors on symmetric and asymmetric subspaces, respectively [12], and

$$\omega_{\mathrm{sep}}^{AB} = \tfrac{1}{2}(|01\rangle\langle 01| + |10\rangle\langle 10|)^{AB}. \tag{7}$$

Our construction works equally well with $\gamma_\pm^{(d)}$, and for definiteness, we pick $\gamma_+^{(d)}$. This results in the state

$$\rho_+^{AA'BB'} = \frac{1}{k}\gamma_+^{(d)AA'BB'} + \frac{k-1}{k}\mathbb{1}^{AA'} \otimes \sigma^{BB'}. \tag{8}$$

It is easily seen that $\rho_+^{AAB'B'}$ has all the properties of state (2) according to Lemma 1. Having introduced the state, we also allow backward quantum communication between the parties in the form of the 50% erasure channel *from* Bob to Alice denoted as $\mathcal{N}_{e,B\to A}^{0.5}$. These auxiliary resources alone are not sufficient to distill entanglement, since the quantum and classical capacity of the erasure channel are zero, and one cannot create entanglement using local operations and classical communication. This will not be the case, however, if we allow for the forward classical communication from Alice to Bob. To distill entanglement from the quantum state, Alice and Bob perform the following three-step protocol on the state $\rho_+^{AA'BB'}$:

(1) Bob measures M on the B' subsystem and sends the classical outcome to Alice. If he gets outcome M_1, then they abort the protocol. Otherwise, they proceed to step 2.

(2) Bob uses $\mathcal{N}^{0.5}_{e,B\to A}$ to send the B' subsystem to Alice, with probability $\frac{1}{k}$ he succeeds.

(3) Alice performs the untwisting operation, correctly identifying $\Phi_\pm^{AB}$. She then performs one of the correction operations $\{\sigma_z,\mathbb{1}\}$ to ensure that the final state is Φ_+^{AB}.

At the end of the protocol, with probability $p_s=\frac{1}{8k}$, Alice and Bob share a maximally entangled state Φ_+^{AB}.

B. Mixing pbit-like states

This time we construct the hybrid states by starting from the construction of the PPT pbit (6). Then we substitute the CJ states of the erasure channels $\mathcal{N}_e^{\frac{1}{k}}$, $k\geqslant 2$:

$$e_+^{AB}=\frac{1}{k}\Phi_+^{AB}+\frac{k-1}{k}\mathbb{1}^A\otimes\sigma^B, \tag{9}$$

$$e_-^{AB}=\frac{1}{k}\Phi_-^{AB}+\frac{k-1}{k}\mathbb{1}^A\otimes\sigma^B, \tag{10}$$

instead of the subsystems that contain the singlet to ensure k extendibility. The resulting state has the form

$$\begin{aligned}\eta_\alpha^{AA'BB'}=&\frac{p}{2}\{[\alpha\Phi_+^{AB}+(1-\alpha)\mathbb{1}^A\otimes\sigma^B]\otimes\tau_1^{A'B'}\\&+[\alpha\Phi_-^{AB}+(1-\alpha)\mathbb{1}^A\otimes\sigma^B]\otimes\tau_2^{A'B'}\}\\&+\alpha(1-p)\omega_{\rm sep}^{AB}\otimes\tau_2^{A'B'},\end{aligned} \tag{11}$$

where $\alpha=\frac{1}{k}$, and $\omega_{\rm sep}^{AB}$ is the same as in Eq. (7). State (11) together with (2) represents an explicit example of bound entangled states which pass the hierarchy of the separability criteria introduced by Doherty *et al.* [9] up to any given level. We prove that this state has the same properties as (2) in the following lemma.

Lemma 2. The state $\eta_\alpha^{AA'BB'}$ is k extendible with respect to Bob's subsystem (BB'), has PPT, and is bound entangled.

Proof. The state (11) is k extendible because each $e_\pm^{AB}$ is k extendible by construction and $\omega_{\rm sep}^{AB}$ is separable, hence extendible to an arbitrary number of parties.

To see that the state has PPT we notice that by simple regrouping of the terms we can write it as

$$\eta^{AA'BB'}=\alpha\gamma_+^{AA'BB'}+(1-\alpha)\,\zeta_{\rm sep}, \tag{12}$$

where $\gamma_+^{AA'BB'}$ is the same as in Eq. (6), which has PPT, and the remaining summands are separable, hence arbitrarily extendible.

To show that the state is bound entangled, it is sufficient to repeat the proof of Lemma 1, with the only difference that Bob performs a measurement $M=\{M_0,M_1\}$ on B. ■

We will henceforth refer to both families of introduced k-extendible states as k-hybrid states.

C. Properties of k-hybrid states

One question of interest is to investigate the bounds on the distance to the set of separable states when the state becomes highly extendible, especially if its extendibility depends on the dimension. In particular, we are interested in how far our family of k-hybrid states can be from the set of all separable states when k is large.

Setting $k=\lfloor f(n)\rfloor$, where $f(n)$ is the function of the sublinear growth, the state (11) provides the the family of states that are $f(n)$-hybrid, with vanishing amount of entanglement on a single-copy level in the limit of large n. The tensor product $(\eta_{\lfloor f(n)\rfloor}^{AA'BB'})^{\otimes n}$ is an $f(n)$-hybrid state, which is very far from the set SEP of separable states.

Lemma 3. Consider the function of sublinear growth $f(n)=o(n)$, and the state $(\eta_{\lfloor f(n)\rfloor}^{AA'BB'})^{\otimes n}$. Then

(a) $$\min_{\sigma\in{\rm SEP}}\left\|\eta_{\lfloor f(n)\rfloor}^{AA'BB'}-\sigma\right\|_1\geqslant\frac{p_s}{\lfloor f(n)\rfloor},\quad p_s\in\left(\frac{1}{32},\frac{1}{28}\right).$$

(b) $$\min_{\sigma^{(n)}\in{\rm SEP}}\left\|\left(\eta_{\lfloor f(n)\rfloor}^{AA'BB'}\right)^{\otimes n}-\sigma^{(n)}\right\|_1\to 1,\quad \text{as}\quad n\to\infty.$$

Proof. The lower bound in (a) follows from the observation that using the protocol described after Lemma 1, Alice and Bob can distill the amount of entanglement which equals the lower bound for all values of p_s in the range. The latter ensures that the state has PPT.

To prove (b) we apply the result from [13], where the authors derived the following lower bound for the trace distance from separable states to states which are bound entangled and have PPT:

$$\min_{\sigma^{(n)}\in{\rm SEP}}\left\|\left(\eta_{\lfloor f(n)\rfloor}^{ABA'B'}\right)^{\otimes n}-\sigma^{(n)}\right\|_1\geqslant 1-r_n, \tag{13}$$

$r_n=(6\epsilon^{-1}+1)(\delta_n+2d\frac{n}{n+n^2})+\epsilon'$, where d is the dimension of the underlying Hilbert space of $\eta_{\lfloor f(n)\rfloor}^{ABA'B'}$, which does not increase with $f(n)$. The terms δ_n,ϵ' indicate the speed of convergence of the values obtained by the process of tomography on $\sigma^{(n)}$ and $(\eta_{\lfloor f(n)\rfloor}^{ABA'B'})^{\otimes n}$ accordingly. They arise as a result of the application the law of large numbers while performing the typical state tomography, and we can assume them to be $\delta_n=\frac{A}{n}$ and $\epsilon'=\frac{B}{n}$ for some constants A,B. Lastly, $\|\eta_{\lfloor f(n)\rfloor}^{AA'BB'}-\sigma\|_1\geqslant\frac{p_s}{\lfloor f(n)\rfloor}=\epsilon$ is taken from the $f(n)$-extendibility condition that is present in the statement of Lemma 3. Putting everything together, we get

$$\lim_{n\to\infty}r_n=\lim_{n\to\infty}\left[[6f(n)+1]\left(\frac{A}{n}+\frac{2dn}{n+n^2}\right)+\frac{B}{n}\right]=0. \tag{14}$$

■

The result of Lemma 3 can be seen from a different perspective: by performing the task of entanglement distillation using an expanded class of operations. If instead of just allowing local operations and classical communication, we allow nonentangling maps, we will be able to distill from $\eta_{\lfloor f(n)\rfloor}^{ABA'B'}$ the amount of entanglement that vanishes as $n\to\infty$. However, the total distillable entanglement of the state $(\eta_{\lfloor f(n)\rfloor}^{ABA'B'})^{\otimes n}$ increases under nonentangling maps as $O(n^\epsilon)$ for some $\epsilon>0$, thereby increasing the distance from the set of all separable states. Each individual state in the tensor product has an ever smaller amount of entanglement which decreases sublinearly as n increases; yet the entanglement of the tensor product increases (also sublinearly). This is not the case if we allow a super linearly vanishing amount of entanglement on the single-copy level as n increases. One may think that by letting the state be $\lfloor f(n) \rfloor$ cloneable, as $f(n)$ increases with n, yet having tensor product far from the set of separable states contradicts the complete hierarchy of separability criteria of [9] in the sense that the constructed state is highly cloneable yet far from the set of separable states. This is not the case, because for every finite n, we simultaneously fix $f(n)$, and for some $t > 0$ we will fail to construct the symmetric extension of the state $\eta^{AA'BB'}_{\lfloor f(n) \rfloor}$ to $f(n) + t$ parties, thereby showing that it is entangled.

D. Fully extendible states beyond CJ states of the erasure channel

Previously we were working with the states, which were only extendible on one of the parties that possesses the state. Here we look on the bound entangled states with PPT, which are equally extendible on both parties. We will see that they are obtained by a slight modification of the previous constructions, symmetrizing them in a suitable way. To achieve this, we replace the bound entangled state $\phi^{AA'BB'}$ in

$$\rho^{AA'BB'} = \frac{1}{k}\phi^{AA'BB'} + \frac{k-1}{k}\mathbb{1}^{AA'} \otimes \sigma^{BB'} \tag{15}$$

by a state which belongs to the class $\mathcal{I}_{BE}$ of bound entangled states, which are invariant with respect to the exchange of the subsystems.

The following lemma provides a way to take a rather generic bipartite bound entangled state and turn it into a highly extendible state on both parties, which turns out to be K hybrid, where $K = \frac{1}{2}k(k-1)$.

Lemma 4. Let $\rho^{AB} \in \mathcal{I}_{BE}$. Then the state

$$\zeta^{\mathbf{A}} = \frac{1}{K}\sum_{i,j=1,i<j}^{k} \rho^{A_iA_j} \otimes \sigma^{\mathbf{A}\setminus A_iA_j} \tag{16}$$

is K hybrid with the reduced state $\zeta^{A_iA_j} = \mathrm{Tr}_{\mathbf{A}\setminus A_iA_j}(\zeta^{\mathbf{A}})$, where $\mathbf{A} = A_1 \ldots A_k$, and $\sigma^{\mathbf{A}\setminus A_iA_j}$ is the separable state.

Proof. Fix i_0, j_0: $A_{i_0} = A$, $A_{j_0} = B$. From the permutation invariance of ρ^{AB} we have $\mathrm{Tr}_A\rho^{AB} = \mathrm{Tr}_B\rho^{AB}$. This fact and the overall compositional symmetry of Eq. (16) shows that $\forall j : j \neq j_0$: $\zeta^{AB} = \zeta^{A_jB} = \mathrm{Tr}_{\mathbf{A}\setminus\{A_j,B\}}(\zeta^{\mathbf{A}})$. Similarly, $\forall\, i : i \neq i_0$: $\zeta^{AB} = \zeta^{AA_i} = \mathrm{Tr}_{\mathbf{A}\setminus\{A,A_i\}}(\zeta^{\mathbf{A}})$. To show that ζ^{AB} is bound entangled, Bob performs measurement M as in the proof of Lemma 1 on his share of state σ, and communicates the result back to Alice. Now parties share the state ρ^{AB} with probability $\frac{1}{K}$, which is bound entangled. ■

The result of Lemma 4 can be directly generalized to the multipartite case.

One could generate examples of permutationally invariant states from the general bipartite bound entangled states—not necessarily permutationally invariant—symmetrizing them with respect to the additional subsystems, as illustrated in the example below.

Example. Let μ^{AB} be a bipartite bound entangled state. Then the state $\widetilde{\mu}^{AA'BB'} = \frac{1}{2}[|10\rangle\langle 10|^{A'B'} \otimes \mu^{AB} + |01\rangle\langle 01|^{A'B'} \otimes (F\mu^{AB}F)]$, where F is a flip operator, belongs to the set $\mathcal{I}^{AB}$. Take $A_{i_0} = A$, $A_{j_0} = B$, and consider the state

$$\zeta^{AB} = \mathrm{Tr}_{\mathbf{A}\setminus AA'BB'}\left(\frac{1}{K}\sum_{i,j=1,i<j}^{k} \widetilde{\mu}^{A_iA_i'A_jA_j'} \otimes \sigma^{\mathbf{A}\setminus A_iA_j}\right), \tag{17}$$

where $K = \frac{1}{2}k(k-1)$. To see that this is a bound entangled K-hybrid state, Alice and Bob perform the protocol as in the proof of Lemma 4, followed by the projective measurement on a classical register $A'B'$. Depending on the outcome of their measurements, they will share either μ^{AB} or $F\mu^{AB}F$, which is bound entangled.

III. NONTRIVIAL ZERO-CAPACITY CHANNELS WITH NO KNOWN SUPERACTIVATION PROTOCOL

The channels whose CJ states are k hybrid provide an interesting case of zero-capacity channels, whose quantum capacity cannot be superactivated. The latter effect, originally discovered in [7] and later generalized in [8], consists of having two channels $\mathcal{N}_1$ and $\mathcal{N}_2$ which are too noisy to transmit quantum information when used individually but when used together have positive capacity. The first channel in the setup produces bound entangled states with PPT, and another one produces certain 2-extendible states. More formally, superactivation is concisely described by the following relations that must be simultaneously satisfied:

$$\begin{aligned} \mathcal{Q}(\mathcal{N}_1) &= 0,\\ \mathcal{Q}(\mathcal{N}_2) &= 0,\\ \mathcal{Q}(\mathcal{N}_1 \otimes \mathcal{N}_2) &> 0. \end{aligned} \tag{18}$$

Consider a channel $\mathcal{N}_H$ whose CJ state is k hybrid of the form (8). The output of the channel is a PPT bound entangled state which at the same time is k extendible. Such a channel retains the characteristic properties of the pdit channel $\mathcal{N}_{\gamma^{(d)}}$ [8]. Also, this is the first known channel whose CJ state belongs to the set of PPT states, which are simultaneously k-extendible states. One can view this channel as the erasure channel which erases the input state with probability $1 - \frac{1}{k}$. Previously, one could only construct a channel that is binding entangled and whose CJ state belongs to the set of PPT 2-extendible states [9]. It turns out that $\mathcal{N}_H$ cannot be activated using any of the channels that were previously instrumental in all of the protocols for superactivation up to date.

Lemma 5. Consider $\mathcal{N}_H$ which produces states of the form (8). Then the following conditions must be simultaneously satisfied

$$\begin{aligned} \mathcal{Q}(\mathcal{N}_H) &= 0,\\ \mathcal{Q}(\mathcal{N}_H \otimes \mathcal{N}_{\gamma^{(d)}}) &= 0,\\ \mathcal{Q}(\mathcal{N}_H \otimes \mathcal{N}_e^p) &= 0, \quad p \in \left[\tfrac{1}{2},1\right). \end{aligned} \tag{19}$$

Proof. The first equality follows directly from its membership in the intersection of the set of two zero-capacity channels. Taking $\mathcal{N}_1 = \mathcal{N}_H \otimes \mathcal{N}_{\gamma^{(d)}}$ results in a channel that produces PPT states, hence, $\mathcal{Q}(\mathcal{N}_1) = 0$. Similarly, $\mathcal{N}_2 = \mathcal{N}_H \otimes \mathcal{N}_e^p$ could be represented as another erasure channel with probability of erasure larger than p. Therefore, $\mathcal{Q}(\mathcal{N}_2) = 0$. ■

This curious case of hybrid channels leaves the question of superactivation of such class of channels open. This means that if they can be activated in principle, the activating channel will belong to a completely new class of zero-capacity channels, dissimilar to all zero-capacity channels we know now.

IV. LOW-DIMENSIONAL ANALOG OF HYBRID STATES

All the constructions of the hybrid states pose a challenge to implement in the laboratory, because they require a high-dimensional Hilbert space to exist. It is also known that in $2 \otimes 2$ dimensions hybrid states as we know them cannot exist [2]. We find a low-dimensional analog to the hybrid states, which turns out to be 2 extendible and key distillable with the two-way communication. The existence of such an analog can be easily seen in the dimensions where there exist hybrid states, as each 2-hybrid state gives rise to extendible state with classical key. It is easy to see that such states exist in higher dimensions, as follows from the constructions of the k-hybrid states. Using the state (2), one can construct the $4 \otimes 5$ state which contains a key and is k extendible:

$$\rho_{\min}^{AA'BB'} = \frac{1}{k}\gamma_{\min}^{AA'BB'} + \frac{k-1}{k}\mathbb{1}^{AA'} \otimes \sigma^{BB'}, \tag{20}$$

where $\gamma_{\min}^{AA'BB'}$ is the $4 \otimes 4$ pbit with the smallest possible dimensions of the shield recently introduced in [14], and $\sigma^{BB'}$ is the erasure flag. The authors in [9] exhibit a $3 \otimes 3$ state which achieves the same goal, although there is no known distillation protocol to obtain a key.

From the above considerations it is not possible to construct $2 \otimes 2$ states which achieve the goal, because for the systems on $\mathcal{H}_m \otimes \mathcal{H}_n$, where $mn \leqslant 6$, having PPT implies separability of the state [2]. Therefore, if we lift the requirement for the bipartite state to have PPT, it turns out that it is possible to have a bipartite $2 \otimes 2$ state that is 2-extendible and has a two-way key (denoted as $K_{\leftrightarrow}$). The latter means that if parties possess many copies of the state, they are able to distill the key using a bidirectional classical communication channel. The existence of such states is not at all obvious and even to a certain extent paradoxical, since it passes the second test from the separability hierarchy and yet contains a two-way key.

Here we show the existence of states $\rho^{AB} \in \mathcal{B}(\mathcal{H}_2 \otimes \mathcal{H}_2)$ that are extendible and for which $K_{\leftrightarrow}(\rho^{AB}) > 0$. We turn to the class of Bell-diagonal states for which necessary and sufficient conditions for extendibility have recently been discovered [10]. More formally, let

$$\rho^{AB} = \lambda_1\Phi^+ + \lambda_2\Phi^- + \lambda_3\Psi^+ + \lambda_4\Psi^-, \tag{21}$$

where $\sum_{i=1}^4 \lambda_i = 1$, and $\Phi^\pm,\Psi^\pm$ are Bell states. Put $\alpha_1 = \lambda_1 - \lambda_2 - \lambda_3 + \lambda_4$, $\alpha_2 = \sqrt{2}(\lambda_1 - \lambda_4)$, and $\alpha_3 = \sqrt{2}(\lambda_2 - \lambda_3)$. Then, ρ^{AB} is extendible if and only if any of the following inequalities are satisfied [10]:

$$4\alpha_1(\alpha_2^2 - \alpha_3^2) - (\alpha_2^2 - \alpha_3^2)^2 - 4\alpha_1^2(\alpha_2^2 + \alpha_3^2) \geqslant 0, \tag{22}$$

$$\alpha_2^2 - \alpha_3^2 - 2\sqrt{2}\alpha_1|\alpha_2| \geqslant 0, \tag{23}$$

$$\alpha_3^2 - \alpha_2^2 + 2\sqrt{2}\alpha_1|\alpha_3| \geqslant 0. \tag{24}$$

For the states expressed in the Bell basis there also exists a sufficient condition for the distillation of key using single-copy measurements plus classical two-way processing protocols, expressed in terms of $\{\lambda_i\}_{i=1}^4$ [15]. It states that by sharing many copies of the state ρ^{AB}, one can distill a secret key if and only if

$$(\lambda_{\max} - \lambda_{\min})^2 > (1 - \lambda_{\max} - \lambda_{\min})(\lambda_{\max} + \lambda_{\min}), \tag{25}$$

where $\lambda_{\max} = \max_i \lambda_i$, and $\lambda_{\min} = \min_i \lambda_i$.

Observation. Systems of inequalities (22)–(24) and (25) are simultaneously satisfiable. The state (21) with eigenvalues satisfying these systems of inequalities are 2-extendible with $K_{\leftrightarrow}(\rho^{AB}) > 0$.

The plot in Fig. 1 describes the triples of eigenvalues $(\lambda_1,\lambda_2,\lambda_3)$ which are compatible with both systems of inequalities.

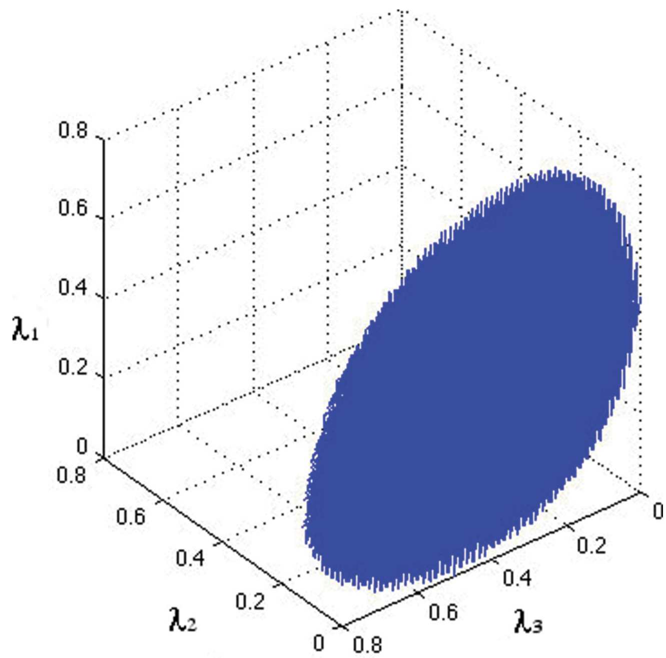

FIG. 1. (Color online) Extendible bipartite qubits with two-way key.

V. CONCLUSIONS

We show an explicit construction of the entangled states with PPT which are k extendible for any fixed k, and explored their properties. In particular, we showed the existence of highly extendible states which are far from the set of separable states. We provided a simple way to distill entanglement when the parties share a hybrid state, which is based on pbits, by giving them a set of nonentangling resources in the form of backward classical channels and backward erasure channels, which has zero capacity.

The method used to construct hybrid states was inspired by the superactivation phenomenon. The corresponding hybrid channel has zero quantum capacity, and it enables the parties to share a hybrid state extendible to any parties. An important open problem is to find another zero-capacity channel which when used jointly with the hybrid channel will superactivate its capacity. It is evident that if such a channel exists, it must neither come from the set of channels which produce bound entangled states with PPT, nor the set of channels whose CJ states are symmetrically extendible. Any such channel must be qualitatively different from all of the zero-capacity channels known to date, and thus help us to better understand the phenomenon of superactivation. Moreover, this problem is intimately related to the hard long-standing open question of the existence of the bound entanglement with negative partial transpose (NPT), which resists the numerous attempts to solve it. Can it be that the CJ states of the new class of zero-capacity channels which are potent to superactivating the capacity of the hybrid channel are examples of the elusive bound entangled states with NPT?

ACKNOWLEDGMENTS

S.S. thanks Trinity College, Cambridge, for its support throughout his Ph.D. studies. J.O. acknowledges the support of the Royal Society.

[1] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[2] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[3] P. Horodecki, M. Horodecki, and R. Horodecki, J. Mod. Opt. **47**, 347 (2000).
[4] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[5] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[6] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Trans. Inf. Theory **55**, 1898 (2009).
[7] G. Smith and J. Yard, Science **321**, 1812 (2008).
[8] F. G. S. L. Brandão, J. Oppenheim, and S. Strelchuk, Phys. Rev. Lett. **108**, 040501 (2012).
[9] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004).
[10] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, Phys. Rev. A **79**, 042329 (2009).
[11] G. O. Myhr and N. Lütkenhaus, Phys. Rev. A **79**, 062307 (2009).
[12] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[13] S. Beigi and P. W. Shor, J. Math. Phys. **51**, 042202 (2010).
[14] Ł. Pankowski and M. Horodecki, J. Phys. A **44**, 035301 (2011).
[15] A. Acín, J. Bae, E. Bagan, M. Baig, L. Masanes, and R. Muñoz-Tapia, Phys. Rev. A **73**, 012327 (2006).