

Optimal Superdense Coding of Entangled States

Anura Abeyesinghe, Patrick Hayden, Graeme Smith, and Andreas J. Winter

Abstract—In this paper, we present a one-shot method for preparing pure entangled states between a sender and a receiver at a minimal cost of entanglement and quantum communication. In the case of preparing unentangled states, an earlier paper showed that a $2l$ -qubit quantum state could be communicated to a receiver by physically transmitting only $l + o(l)$ qubits in addition to consuming l ebits of entanglement and some shared randomness. When the states to be prepared are entangled, we find that there is a reduction in the number of qubits that need to be transmitted, interpolating between no communication at all for maximally entangled states and the earlier two-for-one result of the unentangled case, all without the use of any shared randomness. We also present two applications of our result: a direct proof of the achievability of the optimal superdense coding protocol for entangled states produced by a memoryless source, and a demonstration that the quantum identification capacity of an ebit is two qubits.

Index Terms—Concentration of measure, entanglement, identification, remote state preparation, superdense coding.

I. INTRODUCTION

A SENDER's power to communicate with a receiver is frequently enhanced if the two parties share entanglement. The best-known example of this phenomenon is perhaps superdense coding [1], the communication of two classical bits of information by the transmission of one quantum bit and consumption of one ebit. If the sender knows the identity of the state to be sent, superdense coding of *quantum states* also becomes possible, with the result that, asymptotically, two qubits can be communicated by physically transmitting one qubit and consuming one bit of entanglement [2], [3]. In [2] it was furthermore shown that a sender (Alice) can asymptotically share a two qubit entangled state with a receiver (Bob) at the same qubit and ebit rate, along with the consumption of some shared randomness. That result, however, failed to exploit one of the most basic observations about superdense coding: highly entangled states are much *easier* to prepare than nonentangled states. Indeed, maximally entangled states can be prepared with no communication from the sender at all.

Manuscript received September 28, 2004; revised April 17, 2006. The work of A. Abeyesinghe, P. Hayden, and G. Smith was supported by the U.S. National Science Foundation under Grant EIA-0086038. P. Hayden was also supported by the Sherman Fairchild Foundation. A. J. Winter was also supported by the EC project RESQ under Contract IST-2001-37559.

A. Abeyesinghe and G. Smith are with the Institute for Quantum Information, California Institute of Technology (Caltech 107-81), Pasadena, CA 91125 USA (e-mail: anura@caltech.edu; graeme@caltech.edu).

P. Hayden is with the School of Computer Science, McGill University, Montreal, QC H2A 3A7, Canada (e-mail: patrick@cs.mcgill.ca).

A. J. Winter is with the Department of Mathematics, University of Bristol, Bristol BS8 1UB, U.K. (e-mail: a.j.winter@bris.ac.uk).

Communicated by E. Knill, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2006.878174

In this paper, we construct a family of protocols that take advantage of this effect, finding that even partial entanglement in the state to be shared translates directly into a reduction in the amount of communication required. Recall that every bipartite pure state can be written in the form $|\varphi_{AB}\rangle = \sum_i \sqrt{\lambda_i} |e_i\rangle |f_i\rangle$, where $\langle e_i | e_j \rangle = \langle f_i | f_j \rangle = \delta_{ij}$ and $\lambda_i \geq 0$ [4]. Since the numbers $\sqrt{\lambda_i}$, known as *Schmidt coefficients*, are the only local invariants of $|\varphi_{AB}\rangle$, they entirely determine the non-local features of the state. In the case of one-shot superdense coding, we find that it is the largest Schmidt coefficient that plays a crucial role. More specifically, we show how Alice can, with fidelity at least $1 - \kappa$, share with Bob any pure state that has reduction on Bob's system of dimension d_S and maximum Schmidt coefficient $\sqrt{\lambda_{\max}}$ by transmitting $\frac{1}{2} \log d_S + \frac{1}{2} \log \lambda_{\max} + O(\log(1/\kappa) \log \log d_S)$ qubits and consuming $\frac{1}{2} \log d_S - \frac{1}{2} \log \lambda_{\max} + O(\log(1/\kappa) \log \log d_S)$ ebits. We also show that these rates are essentially optimal.

In the spirit of [5], this new protocol can be viewed as the “father” of the noiseless, visible state communication protocols. Composing it with teleportation generates an optimal *remote state preparation* [6], [7] protocol. Applying it to the preparation of states drawn from a memoryless source generates all the optimal rate points of the triple cbit-qubit-ebit trade-off studied in [8], when combined with quantum-classical trade-off coding [9], [10]. An inspiration for the present work was Harrow's alternative construction of optimal protocols in this memoryless setting that made use of coherent classical communication [11] and pre-existing remote state preparation protocols [12]. Harrow's techniques provided strong circumstantial evidence that the protocol we present here should exist.

The rest of the paper is structured as follows. We begin in Section II by presenting the universal protocol for superdense coding of entangled states and then prove its optimality, along with that of the associated remote state preparation protocol, in Section III. Section IV contains an easy application of typical subspace techniques to the task of developing an optimal protocol for preparing states generated by a memoryless source. Section V provides another application of the protocol, this time to the theory of identification [13], [37], [14]. Specifically, we show that the quantum identification capacity of an ebit is two qubits.

Notation: We use the following conventions throughout the paper. \log and \exp are always taken base 2. Unless otherwise stated, a “state” can be pure or mixed. The density operator $|\varphi\rangle\langle\varphi|$ of the pure state $|\varphi\rangle$ will frequently be written simply as φ . If φ_{AB} is a state on $A \otimes B$, we refer to the reduced state on A as φ_A . Sometimes we omit subscripts labeling subsystems, in which case the largest subsystem on which the state has been defined should be assumed: $\varphi = \varphi_{AB}$ in the bipartite system $A \otimes B$, for example. A system we call A will have a Hilbert space also called A with a dimension d_A . $\mathcal{U}(d)$ denotes the unitary group on \mathbb{C}^d , and $\mathcal{B}(\mathbb{C}^d)$ the set of linear transforma-

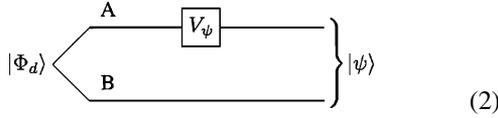
tions from \mathbb{C}^d to itself. We write the fidelity between two states ρ and σ as $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ and the von Neumann entropy of a state ρ as $S(\rho) = -\text{Tr}\rho \log \rho$.

II. THE UNIVERSAL PROTOCOL

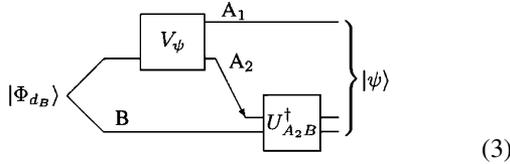
Suppose that Alice would like to share a maximally entangled state with Bob. Clearly, this can be accomplished without any communication—Alice need only perform operations on her half of a fixed maximally entangled state shared between them. In particular, if $|\psi\rangle$ is an arbitrary maximally entangled state and we denote by $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle|i\rangle$ a fixed maximally entangled state, then $|\psi\rangle$ can be expressed as

$$|\psi\rangle = V_\psi \otimes \mathbb{1}_B |\Phi_d\rangle \quad (1)$$

where V_ψ is a unitary transformation of Alice's system which depends on ψ . This identity is equivalent to the following circuit diagram, in which time runs from left to right:



Of course, in general, we would like to prepare an arbitrary state $|\psi_{AB}\rangle$ that may *not* be maximally entangled, and to do so by using as few resources as possible. Our general method is as follows. Alice and Bob initially share a fixed maximally entangled state $|\Phi_{d_B}\rangle$, to which Alice applies an isometry V_ψ . She then sends a subsystem A_2 of dimension d_{A_2} to Bob, who applies a fixed unitary $U_{A_2B}^\dagger$. Alice's goal is to make d_{A_2} as small as possible while still reliably preparing $|\psi_{AB}\rangle$. The procedure can again be summarized with a circuit diagram, although this time it is much less clear whether there exist choices of the operations V_ψ and U_{A_2B} that will do the job:



Circuit (3) does provide a method for preparing the state $|\psi\rangle$ as long as $\mathbb{1} \otimes U_{A_2B} |\psi\rangle$ is maximally entangled across the $A_1 A_2 |B$ cut. (All such states are related by an operation on Alice's system alone.) We will now use this observation, together with the fact that high-dimensional states are generically highly entangled [15]–[20], to construct a protocol that prepares an arbitrary state with high fidelity. The precise statement about the entanglement of generic states that we will need is the following lemma.

Lemma II.1: Let φ be a state on $A \otimes B$ proportional to a projector of rank r and let $U_{AB} \in \mathcal{U}(d_A d_B)$ be chosen according to the Haar measure. Then, if $3 \leq d_B \leq d_A$

$$\begin{aligned} \Pr(S(\text{Tr}_A U_{AB} \varphi U_{AB}^\dagger) < \log d_B - \alpha - \beta) \\ \leq 12r \exp\left(-rd_A d_B \frac{\alpha^2 C}{(\log d_B)^2}\right) \end{aligned} \quad (4)$$

where we may choose $C = (8\pi^2 \ln 2)^{-1}$, and $\beta = \frac{1}{\ln 2} \frac{d_B}{rd_A}$.

It generalizes the following lemma for rank-one φ , which was proved in [3].

Lemma II.2: Let $|\varphi\rangle$ be chosen according to the Haar measure on $A \otimes B$. Then, if $3 \leq d_B \leq d_A$

$$\begin{aligned} \Pr(S(\varphi_B) < \log d_B - \alpha - \beta) \\ \leq \exp\left(-\frac{\alpha^2 C}{(\log d_B)^2} (d_B d_A - 1)\right) \end{aligned} \quad (5)$$

where $C = (8\pi^2 \ln 2)^{-1}$ as before and $\beta = \frac{1}{\ln 2} \frac{d_B}{d_A}$. \square

Proof (of Lemma II.1): If we let R be a space of dimension r and $|\tau_{ABR}\rangle$ be a uniformly distributed state on $A \otimes B \otimes R$, then $\frac{1}{r} \Pi_{\tau_{AB}}$ is equal in distribution to $U_{AB} \varphi U_{AB}^\dagger$, where $\Pi_{\tau_{AB}}$ is the projector onto the support of τ_{AB} . Let σ denote the unitary transformation $\sum_{j=0}^{r-1} |e_{(j+1 \bmod r)}\rangle \langle e_j| + \mathbb{1} - \Pi_{\tau_{AB}}$ that implements a cyclic permutation on the eigenvectors $\{|e_j\rangle\}$ of τ_{AB} corresponding to nonzero eigenvalues. (There are r such eigenvalues except on a set of measure zero, which we will ignore.) We then have

$$\frac{1}{r} \Pi_{\tau_{AB}} = \frac{1}{r} \sum_{k=0}^{r-1} \sigma^k \tau_{AB} \sigma^{-k}. \quad (6)$$

Equation (6), together with the concavity of entropy, implies

$$S\left(\frac{1}{r} \text{Tr}_A \Pi_{\tau_{AB}}\right) \geq \frac{1}{r} \sum_{k=1}^r S(\text{Tr}_A \sigma^k \tau_{AB} \sigma^{-k}) \quad (7)$$

which in turn gives

$$\begin{aligned} \Pr(S(\text{Tr}_A U_{AB} \varphi U_{AB}^\dagger) < \log d_B - \alpha - \beta) \\ \leq \Pr\left(\frac{1}{r} \sum_{k=1}^r S(\text{Tr}_A \sigma^k \tau_{AB} \sigma^{-k}) < \log d_B - \alpha - \beta\right) \\ \leq r \Pr(S(\text{Tr}_A \sigma^k \tau_{AB} \sigma^{-k}) < \log d_B - \alpha - \beta) \\ = r \Pr(S(\tau_B) < \log d_B - \alpha - \beta) \end{aligned} \quad (8)$$

where the final step is a result of the unitary invariance of τ_{ABR} . Applying Lemma II.2 to (8) with $A \rightarrow AR$ and $B \rightarrow B$ reveals that

$$\begin{aligned} \Pr(S(\text{Tr}_A U_{AB} \varphi U_{AB}^\dagger) < \log d_B - \alpha - \beta) \\ \leq 12r \exp\left(-rd_B d_A \frac{\alpha^2 C}{4(\log d_B)^2}\right). \end{aligned} \quad (9)$$

The idea behind the protocol is then simple: we will show that there exists a single unitary U_{A_2B} such that $\mathbb{1}_{A_1} \otimes U_{A_2B} |\psi_{A_1 A_2 B}\rangle$ is almost maximally entangled across the $A_1 A_2 |B$ cut for *all* states $|\psi_{A_1 A_2 B}\rangle$ satisfying a bound on their Schmidt coefficients and whose support on $A_2 \otimes B$ lies in a large subspace $S \subset A_2 \otimes B$. Since any such $\mathbb{1}_{A_1} \otimes U_{A_2B} |\psi_{A_1 A_2 B}\rangle$ is almost maximally entangled, we can then find an *exactly* maximally entangled state which closely approximates it. This state, in turn, can be prepared by the method of Circuit (3). More formally, the following general prescription can be made to succeed:

Protocol: To send an arbitrary pure state with maximal Schmidt coefficient $\leq \sqrt{\lambda_{\max}}$ and reduction of Bob's system to dimension d_S .

- 1) Alice and Bob share a maximally entangled state of $\log d_B = \frac{1}{2}(\log d_S - \log \lambda_{\max}) + o(\log d_S)$ ebits on their joint system AB .
- 2) Alice applies a local partial isometry V_ψ with output on two subsystems A_1 and A_2 . The size of A_2 is $\log d_{A_2} = \frac{1}{2}(\log d_S + \log \lambda_{\max}) + o(\log d_S)$.
- 3) Alice sends A_2 to Bob.
- 4) Bob applies $U_{A_2B}^\dagger$ followed by a projection onto S , which is embedded as a subspace of A_2B .

Proposition II.3: Let $0 < \kappa \leq 1$. For sufficiently large d_S , and for d_{A_2} and d_B as defined in the Protocol, there exists choices of V_ψ which depends on the input state $|\psi_{A_1S}\rangle$ and U_{A_2B} such that for all input states $|\psi_{A_1S}\rangle$ with largest Schmidt coefficient $\leq \sqrt{\lambda_{\max}}$, the output of the protocol has fidelity at least $1 - \kappa$ with $|\psi_{A_1S}\rangle$.

Proof: Our method will be to show that if U_{A_2B} is chosen according to the Haar measure, then the corresponding protocol has a nonzero probability over choices of U_{A_2B} of achieving high fidelity for all states that satisfy the restriction on their Schmidt coefficients, establishing the existence of a particular U_{A_2B} for which this is true. Now, to ensure that the protocol succeeds on a given $|\psi_{A_1S}\rangle$, we only need to ensure that $\mathbb{1}_{A_1} \otimes U_{A_2B} |\psi_{A_1S}\rangle$ is highly entangled across the $A_1A_2|B$ cut, which amounts to showing that $S(\text{Tr}_{A_2} U_{A_2B} \psi_S U_{A_2B}^\dagger)$ is close to $\log d_B$. This is exactly what Lemma II.1 tells us is overwhelmingly likely for an individual random state $|\varphi_{A_1S}\rangle$ maximally entangled with a subspace A'_1 of A_1 . By standard arguments, this will ensure that there exists a unitary U_{A_2B} such that $S(\text{Tr}_{A_2} U_{A_2B} \varphi_S U_{A_2B}^\dagger)$ is close to $\log d_B$ for all the states on S maximally entangled with A'_1 . Majorization can then be used to extend the argument to general states $|\psi_{A_1S}\rangle$ with bounded largest Schmidt coefficient.

We begin by restricting to the case of states $|\varphi_{A'_1S}\rangle$ maximally entangled between S and a fixed subspace $A'_1 \subseteq A_1$, with $d_{A'_1} = \lfloor 1/\lambda_{\max} \rfloor$. Now, let $\mathcal{N}_{A'_1S}^\gamma$ be a trace norm γ -net for such states. It is possible to choose $|\mathcal{N}_{A'_1S}^\gamma| \leq (5/\gamma)^{2d_{A'_1} d_S}$ (see, for example, [21]). We will fix γ later. By the definition of the net and the contractivity of the trace norm under the partial trace, for every maximally entangled state $|\varphi\rangle$ on $A'_1 \otimes S$ there is a state $|\tilde{\varphi}\rangle \in \mathcal{N}_{A'_1S}^\gamma$ such that

$$\left\| \text{Tr}_{A_2} \left(U_{A_2B} \varphi_S U_{A_2B}^\dagger \right) - \text{Tr}_{A_2} \left(U_{A_2B} \tilde{\varphi}_S U_{A_2B}^\dagger \right) \right\|_1 \leq \|\varphi - \tilde{\varphi}\|_1 \leq \gamma \quad (10)$$

which, by the Fannes inequality [22], implies that

$$\left| S \left(\text{Tr}_{A_2} \left(U_{A_2B} \varphi_S U_{A_2B}^\dagger \right) \right) - S \left(\text{Tr}_{A_2} \left(U_{A_2B} \tilde{\varphi}_S U_{A_2B}^\dagger \right) \right) \right| \leq \delta + \eta(\gamma) \quad (11)$$

where $\delta = \gamma \log d_B$ and $\eta(t) = -t \log t$ for $\gamma \leq 1/4$. Noting that all the states $|\psi_{A_1S}\rangle$ have the same reduction on Bob, we have

$$\begin{aligned} & \Pr \left(\inf_{|\varphi_{A'_1S}\rangle} S \left(\text{Tr}_{A_2} U_{A_2B} \varphi_S U_{A_2B}^\dagger \right) < \log d_B - \alpha - \beta - \delta - \eta(\gamma) \right) \\ & \leq |\mathcal{N}_{A'_1S}^\gamma| \Pr \left(S \left(\text{Tr}_{A_2} U_{A_2B} \varphi_S U_{A_2B}^\dagger \right) < \log d_B - \alpha - \beta \right) \\ & \leq \left(\frac{5}{\gamma} \right)^{2d_{A'_1} d_S} 4d_{A'_1} \exp \left(-d_{A'_1} d_{A_2} d_B \frac{\alpha^2 C}{4(\log d_B)^2} \right) \end{aligned} \quad (12)$$

where $\beta = d_B / (2 \ln 2 d_{A'_1} d_{A_2})$. Choosing $\alpha = \beta =: \epsilon/4 \leq 1/4, \gamma = \alpha^2 / (4 \log d_B)$ and

$$d_S < d_{A_2} d_B \frac{\alpha^2 C}{8(\log d_B)^2 \log(20 \log d_B / \alpha^2)} - 1$$

we find that the probability bound (13) is less than 1. For our choice of parameters, we have furthermore $\alpha + \beta + \delta + \eta(\gamma) \leq 4\alpha = \epsilon$, using $\eta(x) \leq 2\sqrt{x}$ for $x \leq 1/4$. We have chosen parameters such that $d_{A_2} = d_B / (2 \ln 2 \alpha d_{A'_1})$.

Moreover, relaxing the restriction on the input states now, suppose that $|\psi\rangle$ is any state on $A_1 \otimes S$ satisfying the condition $\|\psi_S\|_\infty \leq \lambda_{\max}$. Then any such ψ_S is majorized by any φ_S maximally entangled with A'_1 , so that ψ_S can be written as a convex combination $\sum_j p_j W_j \varphi_S W_j^\dagger$, where each W_j is unitary [23]. It then follows from the concavity of the entropy that

$$\begin{aligned} & S \left(\text{Tr}_{A_2} U_{A_2B} \psi_S U_{A_2B}^\dagger \right) \\ & \geq \min_j S \left(\text{Tr}_{A_2} U_{A_2B} W_j \varphi_S W_j^\dagger U_{A_2B}^\dagger \right). \end{aligned} \quad (14)$$

Therefore, the probability of (12) is actually an upper bound for

$$\Pr \left(\inf_{|\psi_{A_1S}\rangle} S \left(\text{Tr}_{A_2} U_{A_2B} \psi_S U_{A_2B}^\dagger \right) < \log d_B - \epsilon \right). \quad (15)$$

Thus, with our choice of parameters, there is a unitary U_{A_2B} such that for all states $|\psi\rangle$ on $A_1 \otimes S$ satisfying the requirement that $\text{Tr}_{A_1} \psi$ have eigenvalues $\leq \lambda_{\max}$, we have

$$S(\psi'_B) \geq \log d_B - \epsilon \quad (16)$$

introducing $|\psi'\rangle = (\mathbb{1} \otimes U_{A_2B}) |\psi\rangle$. Since this can be rewritten as $S(\psi'_B \| \mathbb{1}_B / d_B) = \log d_B - S(\psi'_B) \leq \epsilon$, it in turn implies [24] that, for such states

$$\|\psi'_B - \mathbb{1}_B / d_B\|_1 \leq \sqrt{2 \ln 2 \epsilon} =: \kappa \quad (17)$$

and, therefore, that $F(\psi'_B, \mathbb{1}_B / d_B) \geq 1 - \kappa$. By Uhlmann's theorem [25], [26], there exists a purification Φ_ψ of $\mathbb{1} / d_B$ such that $|\langle \psi' | \Phi_\psi \rangle|^2 \geq 1 - \kappa$. Starting from a fixed maximally entangled state $|\Phi_0\rangle, |\Phi_\psi\rangle$ can be prepared by Alice using a local operation

V_ψ on A_1A_2 alone. Sending the system A_2 to Bob and having him perform $U_{A_2B}^\dagger$ completes the protocol. The final state has fidelity at least $1 - \kappa$ with $|\Psi\rangle$.

We end with the accounting: the foregoing discussion implies that we may choose

$$\begin{aligned}\log d_{A_2} &= \frac{1}{2}(\log d_S + \log \lambda_{\max}) \\ &\quad - O(\log \kappa) + O(\log \log d_S) \\ \log d_B &= \frac{1}{2}(\log d_S - \log \lambda_{\max}) \\ &\quad - O(\log \kappa) + O(\log \log d_S).\end{aligned}\quad \square$$

The main idea behind the proof, combining an exponential concentration bound with discretization, has been used a number of times recently in quantum information theory [21], [12], [2]. (It is, of course, much older; see [27].) If there is a twist in the present application, it is illustrated in (13). Since d_S is comparable in size to $d_{A_2}d_B$, any prefactor significantly larger than $(5/\gamma)^{2d_{A_1}d_S}$ would have caused the probability bound to fail. Therefore, it was crucial to first restrict to states maximally entangled between A'_1 and S , giving the manageable prefactor, and then extend to general states and larger A_1 using majorization.

III. OPTIMALITY OF THE PROTOCOL

The communication and entanglement resources of Proposition II.3 are optimal up to terms of lower order than $\log d_S$ or $\log \lambda_{\max}$: the amount of quantum communication cannot be reduced, neither can the sum of the entanglement and quantum communication. (Entanglement alone can be reduced at the cost of increasing the quantum communication.) We will demonstrate the result in two steps. First, we prove an optimality result for the task of remotely preparing entangled quantum states using entanglement and *classical* communication. We then show that by teleporting the quantum communication of our superdense coding protocol for entangled states, we generate the optimal remote state preparation protocol, meaning the original superdense coding protocol must have been optimal.

Proposition III.1: A remote state preparation protocol of fidelity $F \geq 1/2$ for all d_S -dimensional states with maximum Schmidt coefficient $\leq \sqrt{\lambda_{\max}}$ must make use of at least

$$\log d_S + \log \lambda_{\max} + \log F - 2 \text{ cbits}$$

and

$$\log d_S - 18\sqrt{1-F} \log d_S - 2\eta(2\sqrt{1-F}) \text{ ebits}$$

where $\eta(t) = -t \log t$.

Proof: Consider a remote state preparation protocol involving the transmission of exactly $\log K$ cbits which can, with fidelity F , prepare all d_S -dimensional states having maximum Schmidt coefficient $\sqrt{\lambda_{\max}}$. We will show that causality essentially implies that K must be roughly as large as $d_S \lambda_{\max} F$.

In particular, suppose Alice wants to send Bob a message $i \in \{1, \dots, \lfloor \frac{d_S}{a} \rfloor\}$, with $a = \lceil \frac{1}{\lambda_{\max}} \rceil$. One way she can accomplish this is by preparing (a purification of) the state $\sigma_i = \frac{1}{a} \sum_{k=1+a(i-1)}^{ai} |k\rangle\langle k|$ on Bob's system, with some fixed basis

$\{|k\rangle\}$. The remote state preparation protocol will produce a state ρ_i for Bob which will have a fidelity F with the intended state, σ_i . In order to decode the message, Bob simply measures $\Pi_i = \sum_{k=1+a(i-1)}^{ai} |k\rangle\langle k|$. His probability of decoding the message Alice intended is $\text{Tr}(\rho_i \Pi_i) \geq F$.

Now, imagine that Alice and Bob use the same protocol, with the modification that rather than Alice sending cbits, Bob simply guesses which $j \in \{1, \dots, K\}$ Alice would have sent. The probability of Bob correctly identifying i in this case is thus at least $\frac{F}{K}$ —he has a probability $\frac{1}{K}$ of correctly guessing j and, given a correct guess, a conditional probability F of correctly identifying i . However, since this protocol involves no forward communication from Alice to Bob, it can succeed with probability no greater than $\lfloor \frac{d_S}{a} \rfloor^{-1}$ (by causality), hence $K \geq F \lfloor \frac{d_S}{a} \rfloor$, which implies that $K \geq \log d_S + \log \lambda_{\max} + \log F - 2$.

The entanglement lower bound follows easily from conservation of entanglement under local operations and classical communication (LOCC): let Alice and Bob prepare a maximally entangled state $|\Phi_0\rangle$ of Schmidt rank d_S . If they were able to do this exactly, by the nonincrease of entanglement under LOCC, they would need to start with at least $\log d_S$ ebits. However, the protocol only succeeds in creating a state ρ of fidelity $\geq F$ with $|\Phi_0\rangle$. By a result of Nielsen [28], this implies that for the entanglement of formation

$$E_F(\rho) \geq \log d_S - 18\sqrt{1-F} \log d_S - 2\eta(2\sqrt{1-F}).$$

Since E_F cannot increase under LOCC, the right hand side is also a lower bound on the number of ebits Alice and Bob started with. \square

Corollary III.2: A superdense coding protocol of fidelity $F \geq 1/2$ for all d_S -dimensional states with maximum Schmidt coefficient $\leq \sqrt{\lambda_{\max}}$ must make use of at least $\frac{1}{2} \log d_S + \frac{1}{2} \log \lambda_{\max} + \frac{1}{2} \log F - 1$ qubits of communication. The sum of qubit and ebit resources must be at least $\log d_S - 18\sqrt{1-F} \log d_S - 2\eta(2\sqrt{1-F})$.

Proof: Suppose there exists a superdense coding protocol which can prepare all d_S dimensional states with maximum Schmidt coefficient $\leq \sqrt{\lambda_{\max}}$ and which uses only Q qubits and E ebits. Use teleportation to transmit the qubits, turning it into a remote state preparation protocol.

The qubit cost translates directly to a cbit cost of $2Q$. From Proposition III.1 we infer the lower bound on Q . The protocol including teleportation requires $Q + E$ ebits, thus the lower bound on $Q + E$ follows from Proposition III.1 as well. \square

Thus, when $F \rightarrow 1$ and ignoring terms of order $o(\log d_S)$, the upper resource bounds from our protocol, and the above lower bound coincide.

IV. PROTOCOL FOR A MEMORYLESS SOURCE

The universal protocol of Proposition II.3 is easily adapted to the task of sending states produced by a memoryless source. A standard application of typical subspace techniques gives control of the value of λ_{\max} and the effective size of the states received by Bob, the two parameters determining the resources consumed by the universal protocol. We model the

source $\mathcal{E}_{A_1S} = \{p_i, |\varphi_i^{A_1S}\rangle\}_{i=1}^m$ as a sequence of independent, identically distributed states with

$$|\varphi_{i^n}^{A_1S}\rangle = |\varphi_{i_1}^{A_1S}\rangle \otimes \dots \otimes |\varphi_{i_n}^{A_1S}\rangle \quad (18)$$

occurring with probability $p_{i^n} = p_{i_1}p_{i_2}\dots p_{i_n}$, where $i^n = i_1i_2\dots i_n$. If we define $S(\mathcal{E}_S) = S(\sum_i p_i \text{Tr}_{A_1} |\varphi_i\rangle\langle\varphi_i|)$ and $\bar{S}(\mathcal{E}_S) = \sum_i p_i S(\text{Tr}_{A_1} |\varphi_i\rangle\langle\varphi_i|)$, Harrow combined coherent classical communication and a remote state preparation protocol to demonstrate that a qubit rate of $\frac{1}{2}(S(\mathcal{E}_S) - \bar{S}(\mathcal{E}_S))$ and ebit rate of $\frac{1}{2}(S(\mathcal{E}_S) + \bar{S}(\mathcal{E}_S))$ are simultaneously achievable [11], an optimal result [8] which hinted at the existence of the universal protocol. Here we show how the universal protocol provides an alternate, perhaps more direct, route to Harrow's rate pair.

Proposition IV.1: There exist protocols for superdense coding of entangled states with mean fidelity approaching one and asymptotically achieving the rate pair of $\frac{1}{2}(S(\mathcal{E}_S) - \bar{S}(\mathcal{E}_S))$ qubits and $\frac{1}{2}(S(\mathcal{E}_S) + \bar{S}(\mathcal{E}_S))$ ebits.

Proof: With probability p_{i^n} , Alice needs to prepare the state $|\varphi_{i^n}^{A_1S}\rangle$. Instead, for typical i^n , she prepares a state $|\sigma_{i^n}^{A_1S}\rangle$ obtained by applying a typical projector and a conditional typical projector to $\varphi_{i^n}^S$. When i^n is atypical, the protocol fails.

Given a probability distribution q on a finite set χ , define the set of *typical sequences*, with $\delta > 0$, as

$$\mathcal{T}_{q,\delta}^n = \{x^n : \forall x |N(x|x^n) - nq_x| \leq \delta\sqrt{n}\sqrt{q_x(1-q_x)}\} \quad (19)$$

where $N(x|x^n)$ counts the numbers of occurrences of x in the string $x^n = x_1x_2\dots x_n$. If $\rho = \sum_i p_i \varphi_i^S$ has spectral decomposition $\sum_{j=1}^{d_S} R(j)\Pi_j$, we then define the typical projector to be

$$\Pi_{\rho,\delta}^n = \sum_{j^n \in \mathcal{T}_{R,\delta}^n} \Pi_{j_1} \otimes \dots \otimes \Pi_{j_n} \quad (20)$$

and the conditional typical projector to be

$$\Pi_{\varphi^S,\delta}(i^n) = \bigotimes_{i=1}^m \Pi_{\varphi_i,\delta}^{I_i} \quad (21)$$

where $I_i = \{j \in [n] : i_j = i\}$ and $\Pi_{\varphi_i,\delta}^{I_i}$ refers to the typical projector in the tensor product of the systems $j \in I_i$. In terms of these definitions, $\sigma_{i^n}^{A_1S}$, the state Alice prepares instead of $\varphi_{i^n}^{A_1S}$, is proportional to

$$\left(\mathbb{1}_{A_1} \otimes \Pi_{\rho,\delta}^n \Pi_{\varphi^S,\delta}(i^n)\right) \varphi_{i^n}^{A_1S} \left(\mathbb{1}_{A_1} \otimes \Pi_{\varphi^S,\delta}(i^n) \Pi_{\rho,\delta}^n\right) \quad (22)$$

With respect to approximation, the relevant property of these operators is that, defining

$$\xi_{i^n} = \Pi_{\varphi^S,\delta}(i^n) \varphi_{i^n}^S \Pi_{\varphi^S,\delta}(i^n) \quad (23)$$

we have

$$\begin{aligned} & \text{Tr} \left[\Pi_{\rho,\delta}^n \Pi_{\varphi^S,\delta}(i^n) \varphi_{i^n}^S \Pi_{\varphi^S,\delta}(i^n) \Pi_{\rho,\delta}^n \right] \\ &= \text{Tr}[\xi_{i^n}] - \text{Tr}[(\mathbb{1} - \Pi_{\rho,\delta}^n) \xi_{i^n}] \\ &\geq \text{Tr}[\xi_{i^n}] - \text{Tr}[(\mathbb{1} - \Pi_{\rho,\delta}^n) \varphi_{i^n}^S] \geq 1 - \epsilon \end{aligned} \quad (24)$$

if $\delta = m\sqrt{2d_S}/\epsilon$ (by Lemmas 3 and 6 in [29]). The Gentle Measurement Lemma, referred to as the tender operator inequality in [29], together with a simple application of the triangle inequality implies that $\|\varphi_{i^n}^{A_1S} - \sigma_{i^n}^{A_1S}\|_1 \leq \sqrt{8\epsilon} + 2\epsilon$. For a more detailed proof of these facts and further information about typical projectors, see [29]. If i^n is typical, meaning it is in the set $\mathcal{T}_{p,\delta}^n$ (which occurs with probability at least $1 - m/\delta^2$), then it is also true that

$$\Pi_{\varphi^S,\delta}(i^n) \varphi_{i^n}^S \Pi_{\varphi^S,\delta}(i^n) \leq \Pi_{\varphi^S,\delta}(i^n) 2^{-n\bar{S}(\mathcal{E}_S) + c\delta\sqrt{n}} \quad (25)$$

$$\text{Rank} \Pi_{\rho,\delta}^n \leq 2^{nS(\mathcal{E}_S) + c\delta\sqrt{n}} \quad (26)$$

where $c > 0$ is independent of n and δ . Equation (25) implies that $(1 - \epsilon)\sigma_{i^n}^S \leq 2^{-n\bar{S}(\mathcal{E}_S) + c\delta\sqrt{n}} \Pi_{\rho,\delta}^n$, which in turn leads to the conclusion that $\lambda_{\max}(\sigma_{i^n}^S) \leq \frac{1}{1-\epsilon} 2^{-n\bar{S}(\mathcal{E}_S) + c\delta\sqrt{n}} =: \lambda_{\max}$; (26) provides a bound on the effective dimension of the system S since $\sigma_{i^n}^S \leq \Pi_{\rho,\delta}^n$ for all i^n .

Applying the universal superdense coding protocol to $\sigma_{i^n}^{A_1S}$, we find that the number of qubits that must be sent is

$$\begin{aligned} & \frac{1}{2} [\log \text{Rank} \Pi_{\rho,\delta}^n + \log \lambda_{\max}] + o(n) \\ & \leq \frac{n}{2} [S(\mathcal{E}_S) - \bar{S}(\mathcal{E}_S)] + c\delta\sqrt{n} - \log(1 - \epsilon) + o(n) \end{aligned} \quad (27)$$

while the number of ebits used is

$$\begin{aligned} & \frac{1}{2} [\log \text{Rank} \Pi_{\rho,\delta}^n - \log \lambda_{\max}] + o(n) \\ & \leq \frac{n}{2} [S(\mathcal{E}_S) + \bar{S}(\mathcal{E}_S)] + \log(1 - \epsilon) + o(n) \end{aligned} \quad (28)$$

matching the rates of the proposition. \square

In Section III we used the fact that teleporting the qubits of a superdense coding protocol leads to a remote state preparation protocol. When applied to Proposition IV.1, we get an alternative proof of Proposition 15 of [12]:

Corollary IV.2: There exist protocols for remote state preparation of entangled states with mean fidelity approaching one and asymptotically achieving the rate pair of $S(\mathcal{E}_S) - \bar{S}(\mathcal{E}_S)$ cbits and $S(\mathcal{E}_S)$ ebits.

V. IDENTIFICATION

Quantum message identification, a generalization of hypothesis testing to the quantum setting, has been explored recently in a series of papers [30]–[32]. As opposed to transmission, where the goal is to reliably communicate a message over a channel, identification only allows the receiver to answer a single binary question: is the message x or is it not? A surprising aspect of the theory of identification is that the number of questions that can be answered grows as a doubly exponential function of the number of uses of the channel, as opposed to the well-known singly exponential behavior for transmission [13], [37], [14]. In the quantum setting, a number of versions of the identification (ID) capacity have been defined; these divide broadly into the capacities for quantum resources to identify classical messages and the capacities for those quantum resources to identify quantum messages. In the former case, doubly exponential growth of the number of messages was found, with the most

important result to date that the ID capacity of an ebit, supplemented with negligible rate of forward classical communication, is two [32]. It follows, of course, that the ID capacity of a qubit is also two [31].

In this section, we will instead be focusing on the capacity of an ebit to identify quantum messages, that is, quantum states. We will consider the model with a visible encoder and ID-visible decoder, according to the terminology introduced in [31].

Specifically, we say that we have a quantum-ID code on $\mathcal{B}(\mathbb{C}^d)$ of error $0 < \lambda < 1$ and dimension d_C if there exists an encoding map $\varepsilon : \mathcal{B}(\mathbb{C}^{d_C}) \rightarrow \mathcal{B}(\mathbb{C}^d)$ and a decoding map $D : \mathbb{C}^{d_C} \rightarrow \mathcal{B}(\mathbb{C}^d)$ such that for all pure states $|\varphi\rangle$ and $|\psi\rangle$ on \mathbb{C}^{d_C}

$$|\mathrm{Tr}(\varphi\psi) - \mathrm{Tr}(\varepsilon(\varphi)D\psi)| \leq \frac{\lambda}{2}. \quad (29)$$

This condition ensures that the measurement $(D_\psi, \mathbb{1} - D_\psi)$ can be used on the states $\varepsilon(\varphi)$ to simulate the test $(\psi, \mathbb{1} - \psi)$ applied to the states φ . In the blind encoder, ID-visible decoder case, ε must be quantum channel and D can be an arbitrary assignment to operators $0 \leq D_\psi \leq \mathbb{1}$. It was shown in [31] that for all $0 < \lambda < 1$ there exists a constant $c(\lambda) > 0$ such that on \mathbb{C}^d a quantum-ID code of error λ and $d_C = \lfloor c(\lambda)d^2 \rfloor$ exists. Since, for fixed λ , $\log d_C = 2\log d - \text{const}$, this shows that, asymptotically, one qubit of communication can identify two qubits. We claim that, again asymptotically, but now using a visible encoding map, one ebit plus a negligible (rate of) quantum communication can be used to identify two qubits. Rather than providing a detailed argument, we simply state the method: the states $\varepsilon(\varphi)$ that are output by the blind encoding can be prepared visibly using superdense coding. Because they are extremely mixed, their purifications are highly entangled and Proposition II.3 demonstrates that negligible communication is sufficient.

The negligible communication cost is encountered frequently in the theory of identification: the classical identification capacity of a bit of shared randomness supplemented by negligible communication is a bit. In [32], it was found that the classical identification capacity of an ebit supplemented by negligible communication is two bits. Our finding here that the quantum identification capacity of an ebit and negligible communication is two qubits provides an alternative proof of this result.

Proposition V.1: If $d_C = \lfloor c(\lambda)d^2/(\log d)^4 \rfloor$, then for all states $|\varphi\rangle \in \mathbb{C}^{d_C}$, approximations $|\Phi'_\varphi\rangle$ of the purifications of the states $\varepsilon(\varphi)$ can be prepared on $\mathbb{C}^a \otimes \mathbb{C}^d$ using $\log d + o(\log d)$ ebits and $o(\log d)$ qubits of communication, in such a way that

$$|\mathrm{Tr}[\varphi\psi] - \mathrm{Tr}[(\mathrm{Tr}_{\mathbb{C}^a} \Phi'_\varphi) D_\psi]| \leq \frac{\lambda}{2}. \quad (30)$$

Proof: From the proof of Proposition 17 in [31], if we choose $a = \lfloor \varepsilon d/2 \rfloor$, $\varepsilon = (\lambda/48)^2$, and a $\lambda/16$ -net in \mathbb{C}^{d_C} , we may let $\varepsilon(\varphi) = \mathrm{Tr}_{\mathbb{C}^a}(V\varphi V^\dagger)$ with $V : \mathbb{C}^{d_C} \rightarrow \mathbb{C}^a \otimes \mathbb{C}^d$ a Haar distributed isometry, and $D_\psi = \text{supp } \varepsilon(\tilde{\psi})$ for the state $\tilde{\psi}$ closest to ψ in the net. Then

$$\begin{aligned} \Pr \left(\exists \psi, \varphi \text{ such that } |\mathrm{Tr}(\varphi\psi) - \mathrm{Tr}(\varepsilon(\varphi)D_\psi)| > \frac{\lambda}{4} \right) \\ \leq \left(\frac{c_0}{\lambda} \right)^{4d_C} \exp(-c_1 d^2 \varepsilon^2) \quad (31) \end{aligned}$$

with absolute constants c_0 and c_1 . (Note that this statement is trivial for $a = 0$ or $a = 1$.) To be precise, in [31] the above probability bound is derived for states in the net, but it is also explained how to use triangle inequality to lift this to all states.

Therefore, the states $\varepsilon(\varphi)$ form a good quantum-ID code. We will demonstrate how to make them using superdense coding. Arguing along the lines of (13), we find that for all $\alpha > 0$, $d_C = \lfloor ad/(\log a)^4 \rfloor$ and sufficiently large d

$$\Pr(\varphi \text{ inf } S(\varepsilon(\varphi)) < \log a - \alpha) < \frac{1}{2}. \quad (32)$$

(This is also a special case of Theorem IV.1 from [3].) By the same reasoning given after (17), there exists a maximally entangled state $|\Phi_\varphi\rangle$ such that $|\langle \Phi_\varphi | V |\varphi\rangle|^2 \geq 1 - \sqrt{2\alpha \ln 2}$. We can, therefore, invoke Proposition II.3 with $d_S = d$ and $\lambda_{\max} = 1/a$ to conclude that for sufficiently large d , states $|\Phi'_\varphi\rangle$ approximating $|\Phi_\varphi\rangle$ to within fidelity $\sqrt{2\alpha \ln 2}$ can be prepared using $\log d + o(\log d)$ ebits and $o(\log d)$ qubits of communication. By an appropriate choice of α , we can therefore ensure that $|\langle \Phi'_\varphi | V |\varphi\rangle|^2 \geq \lambda/4$. Using the triangle inequality, we then find that

$$|\mathrm{Tr}(\varphi\psi) - \mathrm{Tr}(\Phi'_\varphi D_\psi)| \leq \lambda/2 \quad (33)$$

for all pure states $|\varphi\rangle \in \mathbb{C}^{d_C}$.

There is a little subtlety in the proof that is worth considering briefly. The states to be prepared, $|\Phi_\varphi\rangle$, are maximally entangled, so one might think that they can be prepared without any communication at all. The party holding \mathbb{C}^d can, indeed, create them without communication. The party holding the smaller \mathbb{C}^a , however, cannot; local unitary transformations on \mathbb{C}^a will not change the support of the reduction to \mathbb{C}^d , for example. Nonetheless, by appealing to Proposition II.3, we see that the asymmetry disappears in the asymptotic limit if negligible communication is allowed.

VI. DISCUSSION

We have proved the existence of protocols which allow a sender to share entangled states with a receiver while using as little quantum communication as is possible. These protocols interpolate between requiring no communication at all for maximally entangled states and a rate of two remote qubits per sent qubit for product states. An immediate application of the result was a proof that the identification capacity of an ebit is two qubits when visible encoding is permitted.

The question of efficient constructions remains—we would like to have protocols with the same ebit and qubit rates which are implementable in polynomial time (as has been demonstrated for state randomization [21] by Ambainis and Smith [33]). It would also be interesting to know whether stronger success criteria can be satisfied while still achieving the same rates. Specifically, the universal remote state preparation protocol of [12] produces an *exact copy* of the desired state when the protocol succeeds, not just a high fidelity copy. Is such a probabilistic-exact protocol possible in the superdense coding setting? (One could even ask questions about perfectly faithful superdense coding, in analogy to what has been done for remote state preparation

in [34]–[36].) Another natural question is the quantum identification capacity of an ebit in the *blind* scenario. We have shown that it is possible to achieve the identification rate of two qubits per ebit in the case when the identity of the encoded qubits is known, but it is not at all clear whether this rate is achievable when the identity of the qubits is unknown.

ACKNOWLEDGMENT

It is a pleasure to thank Dave Bacon and Debbie Leung for many enjoyable discussions on subjects directly and peripherally related to the contents of this paper. A. J. Winter is grateful for the hospitality of the Caltech’s Institute for Quantum Information.

REFERENCES

[1] C. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on einstein-podolsky-rosen states,” *Phys. Rev. Lett.*, vol. 69, p. 2881, 1992.

[2] A. Harrow, P. Hayden, and D. Leung, “Superdense coding of quantum states,” *Phys. Rev. Lett.*, vol. 92, p. 187901, 2004, arXiv:quant-ph/0307221.

[3] P. Hayden, D. Leung, and A. Winter, “Aspects of generic quantum entanglement,” *Comm. Math. Phys.*, 2006, arXiv quant-ph/0407049.

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge University Press, 2000.

[5] I. Devetak, A. W. Harrow, and A. Winter, “A family of quantum protocols,” *Phys. Rev. Lett.*, vol. 93, p. 230504, 2004, arXiv quant-ph/0308044.

[6] H.-K. Lo, “Classical communication cost in distributed quantum information processing—A generalization of quantum communication complexity,” *Phys. Rev. A*, vol. 62, p. 012313, 2000, arXiv:quant-ph/9912009.

[7] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, “Remote state preparation,” *Phys. Rev. Lett.*, vol. 87, p. 077902, 2001, arXiv:quant-ph/0006044.

[8] A. Abeyesinghe and P. Hayden, “Generalized remote state preparation: Trading cbits, qubits, and ebits in quantum communication,” *Phys. Rev. A*, vol. 68, no. 6, p. 062319, 2003, arXiv quant-ph/0308143.

[9] I. Devetak and T. Berger, “Low-entanglement remote state preparation,” *Phys. Rev. Lett.*, vol. 87, no. 9, p. 197901, 2001, arXiv quant-ph/0102123.

[10] P. Hayden, R. Jozsa, and A. Winter, “Trading quantum for classical resources in quantum data compression,” *J. Math. Phys.*, vol. 43, no. 9, pp. 4404–4444, 2002, arXiv:quant-ph/0204038.

[11] A. Harrow, “Coherent communication of classical messages,” *Phys. Rev. Lett.*, vol. 92, no. 9, p. 097902, 2004, arXiv quant-ph/0307091.

[12] C. H. Bennett, P. Hayden, D. Leung, P. W. Shor, and A. Winter, “Remote preparation of quantum states,” *IEEE Trans. Inf. Theory*, vol. 51, pp. 56–74, Jan. 2005, arXiv quant-ph/0307100.

[13] M. O. Rabin and A. C.-C. Yao, unpublished manuscript, 1979, cited in A. C.-C. Yao, “Some questions on the complexity of distributive computing,” *Proc. 11th ACM Symp. Theory of Computing*, pp. 209–213.

[14] R. Ahlswede and G. Dueck, “Identification via channels,” *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 15–29, 1989.

[15] E. Lubkin, “Entropy of an n -system from its correlation with a k -reservoir,” *J. Math. Phys.*, vol. 19, pp. 1028–1031, 1978.

[16] S. Lloyd and H. Pagels, “Complexity as thermodynamic depth,” *Ann. Phys.*, vol. 188, no. 1, pp. 186–213, 1988.

[17] D. Page, “Average entropy of a subsystem,” *Phys. Rev. Lett.*, vol. 71, pp. 1291–1294, 1993.

[18] S. K. Foong and S. Kanno, “Proof of page’s conjecture on the average entropy of a subsystem,” *Phys. Rev. Lett.*, vol. 72, pp. 1148–1151, 1994.

[19] J. Sanchez-Ruiz, “Simple proof of page’s conjecture on the average entropy of a subsystem,” *Phys. Rev. E*, vol. 52, pp. 5653–5655, 1995.

[20] S. Sen, “Average entropy of a quantum subsystem,” *Phys. Rev. Lett.*, vol. 77, no. 1, pp. 1–3, 1996.

[21] P. Hayden, D. Leung, P. Shor, and A. Winter, “Randomizing quantum states: Constructions and applications,” *Commun. Math. Phys.*, vol. 250, no. 2, pp. 371–391, 2004, arXiv:quant-ph/0307104.

[22] M. Fannes, “A continuity property of the entropy density for spin lattice systems,” *Commun. Math. Phys.*, vol. 31, pp. 291–294, 1973.

[23] P. M. Alberti and A. Uhlmann, *Stochasticity and Partial Order*. Dordrecht, The Netherlands: Reidel, 1982.

[24] M. Ohya and D. Petz, *Quantum Entropy and Its Use*, ser. Texts and monographs in physics. Berlin, Germany: Springer-Verlag, 1993.

[25] A. Uhlmann, “The ‘transition probability’ in the state space of a *-algebra,” *Rep. Math. Phys.*, vol. 9, p. 273, 1976.

[26] R. Jozsa, “Fidelity for mixed quantum states,” *J. Mod. Opt.*, vol. 41, pp. 2315–2323, 1994.

[27] V. D. Milman and G. Schechtman, *Asymptotic Theory of Finite Dimensional Normed Spaces*, ser. Lecture Notes in Mathematics. Berlin, Germany: Springer-Verlag, 1986.

[28] M. Nielsen, “Continuity bounds for entanglement,” *Phys. Rev. A*, vol. 61, p. 064301, 2000.

[29] A. Winter, “Coding theorem and strong converse for quantum channels,” *IEEE Trans. Inf. Theory*, vol. 45, pp. 2481–2485, 1999.

[30] R. Ahlswede and A. Winter, “Strong converse for identification via quantum channels,” *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 569–579, Mar. 2002, arXiv quant-ph/0012127.

[31] A. Winter, “Quantum and classical message identification via quantum channels,” *Quantum Inf. Comput.*, vol. 4, pp. 563–578, 2004, arXiv quant-ph/0401060.

[32] ———, Identification Via Quantum Channels in the Presence of Prior Correlation and Feedback arXiv quant-ph/0403203.

[33] A. Ambainis and A. Smith, “Small pseudo-random families of matrices: Derandomizing approximate quantum encryption,” in *Proc. RANDOM 2004*, 2004, arXiv quant-ph/0404075.

[34] A. K. Pati, “Minimum classical bit for remote preparation and measurement of a qubit,” *Phys. Rev. A*, vol. 63, p. 14302, 2001, arXiv:quant-ph/9907022.

[35] M.-Y. Ye, Y.-S. Zhang, and G.-C. Guo, “Faithful remote state preparation using finite classical bits and a nonmaximally entangled state,” *Phys. Rev. A*, vol. 69, p. 022310, 2004, quant-ph/0307027.

[36] D. W. Berry, “Resources required for exact remote state preparation,” *Phys. Rev. A*, vol. 70, p. 062306, 2004, arXiv:quant-ph/0404004.

[37] A. C.-C. Yao, “Some questions on the complexity of distributive computing,” in *Proc. 11th ACM Symp. Theory of Computing*, pp. 209–213.