Prior entanglement, message compression and privacy in quantum communication

Rahul Jain
U.C. Berkeley
Berkeley, USA.
rahulj@eecs.berkeley.edu [*]

Jaikumar Radhakrishnan
Tata Institute of Fundamental
Research, Mumbai, India,
and
Toyota Technological Institute,
Chicago, USA.
jaikumar@tti-c.org

Pranab Sen
University of Waterloo,
Waterloo, Canada.
p2sen@iqc.ca

Abstract

Consider a two-party quantum communication protocol for computing some function $f : \{0,1\}^n \times \{0,1\}^n \to \mathcal{Z}$. We show that the first message of $\mathcal{P}$ can be compressed to $O(k)$ classical bits using prior entanglement if it carries at most k bits of information about the sender's input. This implies a general direct sum result for one-round and simultaneous quantum protocols. It also implies a new round elimination lemma in quantum communication, which allows us to extend recent classical lower bounds on the cell probe complexity of some data structure problems, e.g. approximate nearest neighbor searching on the Hamming cube $\{0,1\}^n$, to the quantum setting. We then show an optimal tradeoff between the privacy losses of Alice and Bob in computing f in terms of the one-round quantum communication complexity of f with prior entanglement. This tradeoff is independent of the number of rounds of communication.

The above message compression and privacy tradeoff results use a lot of qubits of prior entanglement, leading one to wonder how much prior entanglement is really required by a quantum protocol. We show that Newman's [New91] technique of reducing the number of public coins in a classical protocol cannot be lifted to the quantum setting. We do this by defining a general notion of black-box *reduction of prior entanglement that subsumes Newman's technique. Intuitively, a black-box reduction does not change the unitary transforms of Alice and Bob; it only decreases the amount of entanglement of the prior entangled state. We prove that such a black-box reduction is impossible for quantum protocols by exhibiting a particular one-round quantum protocol for the equality function where the black-box technique fails to reduce the amount of prior entanglement by more than a constant factor.*

1 Introduction

Consider a two-party quantum communication protocol $\mathcal{P}$ for computing some function $f : \{0,1\}^n \times \{0,1\}^n \to \mathcal{Z}$. We assume that $\mathcal{P}$ uses only unitary transformations for its internal computation, except at the very end when the final recipient of a message makes a von Neumann measurement of some of her qubits to declare the output. Thus, the joint state of Alice and Bob is always pure during the execution of $\mathcal{P}$. We also assume that the players make *safe* copies of their respective inputs using CNOT gates before commencing the protocol. These safe copies of the inputs are not affected by the subsequent operations of $\mathcal{P}$, and are never sent as messages. In this paper, we consider protocols with and without *prior entanglement*. By prior entanglement, we mean a pure quantum state $|\phi\rangle$ that is shared between Alice and Bob and that is independent of their input (x, y). $|\phi\rangle$ can be supported on an extremely large number of qubits. The unitary transforms of Alice in $\mathcal{P}$ are allowed to address her share of the qubits of $|\phi\rangle$; similarly for Bob. The classical analogue of prior entanglement is shared random bits. Often, the prior entanglement in a quantum protocol is in the form of some number of EPR pairs, one-half of which belongs to Alice and the other half belongs to Bob. We know that for some quantum communication problems, presence of such prior entanglement helps in reducing the communication. For example, the technique of superdense coding [BW92] allows us to often reduce the communication complexity by a multiplicative factor of 2. So a natural question that arises is how much prior entanglement is *really required* by a quantum protocol? For classical communication, Newman [New91] has shown that $O(\log n)$ shared

[*] This work was supported by an Army Research Office (ARO), North California, grant number DAAD 19-03-1-00082.

random bits are sufficient for any protocol. This is tight, as evidenced by the *equality* function on $\{0,1\}^n$ which requires $\theta(\log n)$ bits with private randomness and $O(1)$ bits with shared randomness. We shall return to the question about the power of prior entanglement in quantum communication later. But first, we look at another problem in communication complexity viz. *privacy loss* and *message compression*, and explore the role of prior entanglement with regard to them.

We are interested in the *privacy loss* of Alice and Bob that is inherent in computing f. Privacy in communication complexity was studied in the classical setting by Bar-Yehuda et al. [BCKO93], and in the quantum setting by Klauck [Kla02] and Jain, Radhakrishnan, and Sen [JRS02]. For studying privacy issues in quantum communication, we only consider protocols without prior entanglement. To define the privacy loss of Alice, imagine that Alice follows the protocol $\mathcal{P}$ honestly but Bob is malicious and deviates arbitrarily from $\mathcal{P}$ in order to extract the maximum amount of information about Alice's input. The only constraint on Bob is that Alice should not be able to figure out at any point of time whether he is cheating or not; we call such a cheating strategy of Bob *undetectable*. Suppose $\mu = \mu_{\mathcal{X}} \times \mu_{\mathcal{Y}}$ is a product probability distribution on $\mathcal{X} \times \mathcal{Y}$. Let register X denote the input qubits of Alice, and B denote all the qubits in the possession of Bob at the end of $\mathcal{P}$. We assume the input registers of Alice and Bob are never modified and are never sent as messages in $\mathcal{P}$. Then the privacy loss of Alice under distribution μ at the end of $\mathcal{P}$ is the maximum mutual information $I(X : B)$ over all undetectable cheating strategies of Bob. The privacy loss of Bob can be defined analogously. In the quantum setting Bob has a big bag of undetectable cheating tricks that he can use in order to extract information about X. For instance, he can start the protocol $\mathcal{P}$ by placing a superposition of states $|\mu_{\mathcal{Y}}\rangle$ (for a probability distribution π on $\mathcal{Z}$, $|\pi\rangle \stackrel{\Delta}{=} \sum_z \sqrt{\pi(z)}|z\rangle$) in his input register Y and running the rest of the protocol honestly. This trick works especially well for so-called 'clean' protocols that leave the work qubits of Alice and Bob at the end of the protocol in the state $|0\rangle$. For example, consider the following exact clean protocol $\mathcal{P}$ computing the inner product modulo 2, $x \cdot y$, of two bit strings $x, y \in \{0,1\}^n$: Alice sends her input x to Bob, Bob computes $x \cdot y$ and sends back x to Alice keeping the bit $x \cdot y$ with himself, and finally Alice zeroes out Bob's message by XORing with her input x. If Bob does the above 'superposition cheating' trick for $\mathcal{P}$, his final state at the end of $\mathcal{P}$ becomes $\left(\sum_{y \in \{0,1\}^n} |y, x \cdot y\rangle\right)$. It is easy to see that Bob has n bits of information about x, if x is distributed uniformly in $\{0,1\}^n$. Thus, the privacy loss from Alice to Bob for this protocol is at least $\frac{n}{2}$, under the uniform distribution on $\{0,1\}^n \times \{0,1\}^n$. See [CvDNT98] for more details. Thus, it is conceivable that Alice and Bob use an 'unclean' protocol to compute f in order to minimize their privacy losses. We shall be concerned with proving tradeoffs between the privacy losses of Alice and Bob for any quantum protocol computing f, including 'unclean' ones. Note that defining the privacy loss only for quantum protocols without prior entanglement is without loss of generality, since we can convert a protocol with prior entanglement into one without prior entanglement by sending the entanglement as part of the first message of the protocol; this process does not affect the privacy loss since after the first message is sent, the qubits in the possession of Alice and Bob are exactly the same as before.

For private coin randomized classical protocols, a related notion called *information cost*, was defined in [BJKS02] to be the mutual information $I(XY : M)$ between the players' inputs and the complete message transcript M of the protocol. For quantum protocols there is no clear notion of a message transcript, hence we use our definition of privacy instead. Also, other than cryptographic reasons there is also another reason why we allow the players to use undetectable cheating strategies. In the above clean protocol $\mathcal{P}$ for the inner product function, if both Alice and Bob were honest the final state of $\mathcal{P}$ would be $|x\rangle \otimes |y, x \cdot y\rangle$, where the first state belongs to Alice and the second to Bob. Under the uniform distribution on x, y the privacy loss from Alice to Bob is 1, whereas the classical information cost is at least n. This shows that in the quantum setting, because of the ability of players to 'forget' information by uncomputing, it is better to allow undetectable cheating strategies for players in the definition of privacy loss in order to bypass examples such as the above.

Jain, Radhakrishnan, and Sen [JRS03] showed that for classical constant round private coin protocols with a product probability distribution on their inputs, one can compress the messages to the information cost of the protocol. Their compression technique does not require any shared randomness. This leads us to wonder whether one can compress the messages of a protocol $\mathcal{P}$ that has low privacy loss for both Alice and Bob. Jain et al.'s [JRS03] compression strategy for classical protocols was 'recipient-non-invasive' in the sense that, for one round protocols, it did not change the computation of the recipient except up to a trivial relabeling of the messages. Unfortunately, they also showed that such a recipient-non-invasive compression result does not hold for quantum protocols; they exhibited a one-round quantum protocol without prior entanglement for the equality function on n-bit strings with constant privacy loss, where any recipient-non-invasive compression strategy cannot compress Alice's message by more than a multiplicative factor of 6! In this paper, we revisit Jain et al.'s [JRS03] 'incompressible' quantum protocol for equality and note that their incompressibility proof breaks down if the new protocol is allowed prior entanglement. Recall that in the classical setting, allowing shared randomness for the new protocol does not affect its communication complexity by much. The question now arises whether one can compress the first message of a quantum protocol without prior entanglement, if the message carries low information about Alice's input and if the new protocol is allowed prior entanglement. We answer this question in the affirmative thus providing a counterpart to the negative result of [JRS03].

Result 1 (Compress first rnd., informal stmt.) *Let μ be a probability distribution on $\mathcal{X} \times \mathcal{Y}$. Let $\mathcal{P}$ be a quantum protocol without prior entanglement for a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ having bounded average error probability under μ. Suppose Alice's first message in $\mathcal{P}$ has mutual information at most k about her input, under distribution μ. Then there is a protocol $\mathcal{P}'$ for f with prior entanglement having similar average error probability under μ, where the first message is classical and $O(k)$ bits long. The communication of $\mathcal{P}'$ for subsequent rounds is the same as in $\mathcal{P}$.*

Remark: Note that in the presence of prior entanglement the communication can be assumed to be classical because of quantum teleportation [BCJ+93].

The proof of the above result uses a technical quantum information-theoretic fact called the *substate theorem* [JRS02]. Essentially, it says that if a quantum encoding of a classical random variable $x \mapsto \sigma_x$ has information at most k about x, then for most x, $\frac{\sigma_x}{2^{O(k)}} \leq \sigma$ (for Hermitian matrices A, B, $A \leq B$ is a shorthand for the statement "$B - A$ is positive semidefinite"), where $\sigma \stackrel{\Delta}{=} \mathsf{E}_x[\sigma_x]$. The classical version of the substate theorem was used by [JRS03] to prove their classical message compression results. Also recently, Chakrabarti and Regev [CR04] used the classical substate theorem to compress the first message of a classical deterministic protocol in their work on cell probe lower bounds for approximate nearest neighbor searching. Our result above can be viewed as the quantum analogue of their result. However, our proof is quite different from the earlier classical compression proofs; in particular, it is not based on a *rejection sampling* [JRS03] argument. Also, it uses prior entanglement in a crucial manner.

Result 1 allows us to prove a general direct sum result for one-round quantum communication protocols with prior entanglement, as well as simultaneous message quantum communication protocol having prior entanglement between Alice and the referee and Bob and the referee only. In the m-fold direct sum problem $f^{\oplus m}$, we are given m independent copies of a function f; we need to communicate and find the function values correctly for each of the m copies. We prove that $Q^{1,\mathrm{pub}}(f^{\oplus m}) \geq m \cdot Q^{1,\mathrm{pub}}(f)$, where $Q^{1,\mathrm{pub}}(f)$ is the bounded error one-round quantum communication complexity of f with prior entanglement. Result 1 also allows us to prove a new *round elimination* result for quantum communication, combined with the 'message switching' technique of [CR04]. To state the round elimination lemma, we first need the following definition.

Definition 1 ($f^{(k),A}$) *Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$. The communication game $f^{(k),A}$ is defined as follows: Alice gets k strings $x_1, \ldots, x_k \in \mathcal{X}$. Bob gets an integer $j \in [k]$, a copy of strings $x_1, \ldots, x_{j-1}$, and a string $y \in \mathcal{Y}$. They are supposed to communicate and determine $f(x_j, y)$. The communication game $f^{(k),B}$ is defined analogously with roles of Alice and Bob reversed.*

Result 2 (Round elim., informal stmt.) *Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a function. Suppose $\mathcal{P}$ is a t-round quantum protocol for $f^{(k),A}$ with prior entanglement having bounded worst case error. Suppose Alice starts the communication and the first and second messages of $\mathcal{P}$ are l_1 and l_2 qubits long respectively. Then there is a $(t-1)$-round protocol for f with prior entanglement having similar worst case error where Bob starts the communication and the first message is $l_2 \cdot 2^{O(l_1/k)}$ qubits long. The subsequent communication in $\mathcal{P}'$ is similar to that in $\mathcal{P}$.*

The above round elimination lemma is useful in situations where Alice's message length l_1 is much smaller than Bob's message length l_2. Such a situation arises in proving cell probe lower bounds for data structure problems like approximate nearest neighbor searching in $\{0,1\}^n$ and set predecessor. Result 2 is the quantum analogue of the classical round reduction technique in [CR04], where it was used crucially in proving optimal randomized cell probe lower bounds for approximate nearest neighbor searching. Recently, Patrascu and Thorup [PT04] used the same classical technique to prove sharper lower bounds for the set predecessor problem. We remark that both these results carry over to the address-only quantum cell probe model (defined in [SV01]) as a consequence of Result 2.

We now turn our attention to privacy loss and compressing the many rounds of communication of a quantum protocol, not just the first round. We prove the following result using the substate theorem [JRS02].

Result 3 (Compress many rounds, informal stmt.) *Let μ be a product probability distribution on $X \times Y$. Let $\mathcal{P}$ be a t-round quantum protocol without prior entanglement for a function $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ having bounded average error probability under μ. Let k_a, k_b denote the privacy losses of Alice and Bob respectively under distribution μ after t' rounds of communication in $\mathcal{P}$. Then there is a $t - t' + 2$-round protocol $\mathcal{P}'$ for f with prior entanglement having similar average error probability under μ, and satisfying the following properties:*

1. *The first message of $\mathcal{P}'$ is from Alice to Bob, it is classical and $k_a 2^{O(k_b)}$ bits long;*

2. *The second message of $\mathcal{P}'$ is from Bob to Alice, it is classical and $O(k_b)$ bits long;*

3. *The communication of $\mathcal{P}'$ for subsequent rounds is the same as the communication of $\mathcal{P}$ in rounds $t'+1, \ldots, t$.*

Remark: Result 1 does not follow from Result 3. Result 1 holds for any probability distribution on $\mathcal{X} \times \mathcal{Y}$ whereas our proof of Result 3 requires product distributions. It is open whether a multiround compression result can be proved for non-product distributions, even for classical protocols.

Result 3 allows us to prove a general tradeoff between the privacy loss k_a of Alice and the privacy loss k_b of Bob at the end of a quantum protocol $\mathcal{P}$ computing a function f viz. that $k_a 2^{O(k_b)} \geq Q_{[\,]}^{1,A \rightarrow B,\mathrm{pub}}(f)$, where $Q_{[\,]}^{1,A \rightarrow B,\mathrm{pub}}(f)$ is the one-round quantum communication complexity (with Alice communicating) of f with prior entanglement having bounded average error under maximized over all product distributions. It also shows that the privacy loss for computing f is lower bounded by $\log Q_{[\,]}^{1,\mathrm{pub}}(f)$. This latter result can be viewed as the privacy analogue of Kremer's result [Kre95] that the bounded error quantum communication complexity of f is lower bounded by the logarithm of its deterministic one-round communication complexity. Result 3 also allows us to show a weak general direct sum result for quantum protocols. All these results are optimal in general as evidenced by the index function problem [ANTV02]. Recall that in the index function problem, Alice is given a database $x \in \{0,1\}^n$ and Bob is given an index $i \in [n]$. They have to communicate and determine x_i. The one-round quantum communication complexity from Alice to Bob for this problem is $\Omega(n)$, even for bounded average error under the uniform distribution and in the presence of prior entanglement. Thus, we get the privacy tradeoff $k_a 2^{O(k_b)} \geq n$ for the index function problem. This is optimal; consider a deterministic protocol where Bob sends the first b bits of his index and Alice replies by sending all the $\frac{n}{2^b}$ bits of her database consistent with Bob's message. Earlier, Jain, Radhakrishnan, and Sen [JRS02] had proved the same privacy tradeoff for the index function problem specifically. Our general tradeoff above can be viewed as an extension of their result to all functions.

The above message compression results use a huge amount of prior entanglement. The prior entanglement seems to be crucial in view of the 'recipient-non-invasive incompressibility' result of [JRS03]. This brings us back to our original question: How much prior entanglement is *really required* by a quantum protocol? One might hope to extend Newman's [New91] proof that a classical protocol needs only $O(\log n)$ shared random bits to the quantum setting. Newman's proof uses a Chernoff-based sampling argument on the shared random bit strings to reduce their number to $O(n)$. The reduction is done in a *black-box* fashion i.e. it does not change the computation of Alice and Bob in the protocol. In the quantum setting, one might similarly hope to reduce the amount of entanglement of the prior entangled state $|\phi\rangle$ to $O(n)$ and leave the unitary transforms of Alice and Bob unaffected i.e. the hope is to find a black-box Newman-style prior entanglement reduction technique. We show that such a black-box reduction is impossible. To state our result precisely, we need the following definitions.

Definition 2 (Similar protocols) *Two protocols $\mathcal{P}$ and $\mathcal{P}'$ with prior entanglement and outputting values in $\mathcal{Z}$ are called* similar protocols *if both use the same number of qubits and the same unitary transformations and measurements, have the same amount of communication and for all $(x,y) \in \{0,1\}^n \times \{0,1\}^n$, $\|\mathcal{P}(x,y) - \mathcal{P}'(x,y)\|_1 < 1/20$. Here, $\mathcal{P}(x,y)$, $\mathcal{P}'(x,y)$ are the probability distributions on $\mathcal{Z}$ of the output of protocol $\mathcal{P}$, $\mathcal{P}'$ on input (x,y). $\mathcal{P}$, $\mathcal{P}'$ may use different quantum states as their input independent prior entanglement.*

Definition 3 (Amt. of entanglement) *For a bipartite pure state $|\phi\rangle_{AB}$, consider its* Schmidt decomposition, *$|\phi\rangle = \sum_{i=1}^{k} \sqrt{\lambda_i} |a_i\rangle \otimes |b_i\rangle$, where $\{a_i\}$ is an orthonormal set and so is $\{b_i\}$, $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$. The* amount of entanglement *of $|\phi\rangle_{AB}$ is defined to be $E(|\phi\rangle_{AB}) \stackrel{\Delta}{=} -\sum_i \lambda_i \log \lambda_i$. The* Schmidt rank *of $|\phi\rangle_{AB}$ is defined to be k.*

One might hope that the following conjecture is true.

Conjecture 1 *For any protocol $\mathcal{P}$ for $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \mathcal{Z}$ with prior entanglement, there exists a similar protocol $\mathcal{P}'$ that starts with prior entanglement $|\phi\rangle_{AB}$, $E(|\phi\rangle_{AB}) = O(\log n)$.*

We prove that the above conjecture is *not* correct for quantum communication protocols. The proof follows by sharpening the geometric arguments behind the proof of the 'recipient-non-invasive incompressibility' result of [JRS03].

Result 4 (No black-box red. of prior entang.) *Let us denote the equality function on n-bit strings by EQ_n . There exists a one-round quantum protocol $\mathcal{P}$ for EQ_n with $\frac{2n}{3} + \log n + \theta(1)$ EPR pairs of prior entanglement and communicating 4 bits, such that there is no similar protocol $\mathcal{P}'$ that starts with a prior entangled state $|\phi\rangle_{AB}$, $E(|\phi\rangle_{AB}) \leq n/600$.*

The above result shows that in order to reduce prior entanglement in quantum communication, one has to look beyond black-box arguments and change the unitary transforms of Alice and Bob. This appears to be quite difficult.

Organization of the paper: In the next section, we collect some preliminaries that will be required in the proofs of the message compression results. In Section 3, we prove our results on first round compression and round elimination in quantum protocols. We prove our multi-round compression result in Section 4. In Section 5, we show that black-box reduction of prior entanglement in quantum communication is impossible.

2 Preliminaries

All our message compression arguments are based on the following common idea: If Alice does not reveal much information about her input, then it must be the case that Bob's state after receiving Alice's messages does not vary much (as Alice's input varies). In this situation, Alice and Bob can start in a suitable input independent state and Alice can account for the variation by applying appropriate local transformations on her registers. We formalize this idea using the notion of a (δ, α)-corrector, and establish the existence of such correctors by appealing to an information-theoretic result called the *substate theorem* due to Jain, Radhakrishnan, and Sen [JRS02].

Fact 1 (Substate theorem, [JRS02]) *Let $\mathcal{H}, \mathcal{K}$ be two finite dimensional Hilbert spaces and $\dim(\mathcal{K}) \geq \dim(\mathcal{H})$. Let $\mathbb{C}^2$ denote the two dimensional complex Hilbert space. Let ρ, σ be density matrices in $\mathcal{H}$ such that $S(\rho \| \sigma) < \infty$. Let $|\overline{\rho}\rangle$ be a purification of ρ in $\mathcal{H} \otimes \mathcal{K}$. Then, for $r > 1$, there exist pure states $|\phi\rangle, |\theta\rangle \in \mathcal{H} \otimes \mathcal{K}$ and $|\overline{\sigma}\rangle \in \mathcal{H} \otimes \mathcal{K} \otimes \mathbb{C}^2$, depending on r, such that $|\overline{\sigma}\rangle$ is a purification of σ and $\| |\overline{\rho}\rangle\langle\overline{\rho}| - |\phi\rangle\langle\phi| \|_{\mathrm{tr}} \leq \frac{2}{\sqrt{r}}$, where*

$$|\overline{\sigma}\rangle \stackrel{\Delta}{=} \sqrt{\frac{r-1}{r2^{rk}}}\, |\phi\rangle|1\rangle + \sqrt{1 - \frac{r-1}{r2^{rk}}}\, |\theta\rangle|0\rangle$$

and $k \stackrel{\Delta}{=} 8S(\rho\|\sigma) + 14$. Note that one can, by means of a local unitary operator on $\mathcal{K} \otimes \mathbb{C}^2$, transform any known purification $|\overline{\sigma'}\rangle$ of σ to $|\overline{\sigma}\rangle$. Also, measuring the last qubit of $|\overline{\sigma}\rangle$ and observing a $|1\rangle$ puts the remaining qubits into the state $|\phi\rangle$. It follows that for every purification $|\overline{\sigma'}\rangle$ of σ, there is an unnormalized superoperator $\mathcal{M}$, depending on $|\overline{\sigma'}\rangle$, acting on the qubits of $|\overline{\sigma'}\rangle$ other than those of σ, such that $\mathcal{M}(|\sigma'\rangle\langle\sigma'|)$ normalized is equal to $|\phi\rangle$. Furthermore, this superoperator succeeds with probability at least $\frac{r-1}{r2^{rk}}$.

Definition 4 ((δ, α)-corrector) *Let Alice and Bob form a bipartite quantum system. Let X denote Alice's input register, whose values range over the set $\mathcal{X}$. For $x \in \mathcal{X}$, let σ_x be a state wherein the state of the register X is $|x\rangle$; that is, σ_x has the form $|x\rangle\langle x| \otimes \rho_x$. Let μ be a probability distribution on $\mathcal{X}$. Let σ be some other joint state of Alice and Bob. A (δ, α)-corrector for the ensemble $\{\{\sigma_x\}_{x \in \mathcal{X}}; \sigma\}$ with respect to the distribution μ is a family of unnormalized superoperators $\{\mathcal{M}_x\}_{x \in \mathcal{X}}$ acting only on Alice's qubits such that:*

1. *$r_x \stackrel{\Delta}{=} \mathsf{Tr}\mathcal{M}_x(\sigma) = \alpha$ for all $x \in \mathcal{X}$, that is, $\mathcal{M}_x$ when applied to σ succeeds with probability exactly α.*
2. *$\mathcal{M}_x(\sigma)$ has the form $|x\rangle\langle x| \otimes \rho'_x$, that is, the state of the register X of Alice is $|x\rangle$ when $\mathcal{M}_x$ succeeds.*
3. *$\mathsf{E}_\mu \left[\left\| \sigma_x - \frac{1}{\alpha}\mathcal{M}_x(\sigma) \right\|_{\mathrm{tr}} \right] \leq \delta$, that is, $\mathcal{M}_x$ on success* corrects *the state σ by bringing it to within trace distance δ from σ_x.*

We shall also need the following observation.

Proposition 1 *Suppose a boolean-valued measurement $\mathcal{M}$ succeeds with probabilities p, q on quantum states ρ, σ respectively. Let ρ', σ' be the respective quantum states if $\mathcal{M}$ succeeds. Then, $\|\rho' - \sigma'\|_{\mathrm{tr}} \leq \frac{1}{\max\{p,q\}} \|\rho - \sigma\|_{\mathrm{tr}}$.*

Proof: We formalize the intuition that if some measurement distinguishes ρ' and σ', then there is a measurement that distinguishes ρ and σ. Assume $p \geq q$ (otherwise interchange the roles of ρ and σ). Now there exists (see e.g. [AKN98]) an orthogonal projection M', such that $\mathsf{Tr}M'(\rho' - \sigma') = \frac{\|\rho' - \sigma'\|_{\mathrm{tr}}}{2}$. Let M'' be the POVM element obtained by first applying POVM $\mathcal{M}$ and on success applying M'. Then the probability of success of M'' on ρ is $p \cdot \mathsf{Tr}M'\rho'$, and the probability of success of M'' on σ is $q \cdot \mathsf{Tr}M'\sigma' \leq p \cdot \mathsf{Tr}M'\sigma'$. Thus,

$$\begin{aligned}
\frac{1}{2}\|\rho - \sigma\|_{\mathrm{tr}} &\geq \mathsf{Tr}M''\rho - \mathsf{Tr}M''\sigma \\
&\geq p(\mathsf{Tr}M'\rho' - \mathsf{Tr}M'\sigma') \\
&= \frac{p}{2} \cdot \|\rho' - \sigma'\|_{\mathrm{tr}},
\end{aligned}$$

implying that $\|\rho' - \sigma'\|_{\mathrm{tr}} \leq \frac{\|\rho - \sigma\|_{\mathrm{tr}}}{p}$. ■

We are now ready to use the substate theorem to show the existence of good correctors when Bob's state does not contain much information about Alice's input. While applying the substate theorem below, it will be helpful to think of Alice's Hilbert space as $\mathcal{K} \otimes \mathbb{C}^2$ and Bob's Hilbert space as $\mathcal{H}$ in Fact 1.

Lemma 1 *For $x \in \mathcal{X}$, let $|\phi_x\rangle \stackrel{\Delta}{=} |x\rangle|\psi_x\rangle$ be a joint pure state of Alice and Bob, where $|x\rangle$ and possibly some other qubits of $|\psi_x\rangle$ belong to Alice's subsystem A, and the remaining qubits of $|\psi_x\rangle$ belong to Bob's subsystem B. Let μ be a probability distribution on $\mathcal{X}$; let $\sigma \stackrel{\Delta}{=} \mathsf{E}_\mu |\phi_x\rangle\langle\phi_x|$ and $|\phi\rangle \stackrel{\Delta}{=} \sum_x \sqrt{\mu(x)}|\phi_x\rangle$. Let X denote the register of Alice containing $|x\rangle$. Suppose $I(X : B) = k$, when the joint state of AB is σ. Then for $\delta > 0$, there is a (δ, α)-corrector $\{\mathcal{M}_x\}_{x \in \mathcal{X}}$ for the ensemble $\{\{|\phi_x\rangle\}; |\phi\rangle\}$ where $\alpha = 2^{-O(k/\delta^3)}$.*

Proof: Let $\rho_x \stackrel{\Delta}{=} \mathsf{Tr}_A|\phi_x\rangle\langle\phi_x|$ and $\rho \stackrel{\Delta}{=} \mathsf{Tr}_A|\phi\rangle\langle\phi|$. Note that $\rho = \mathsf{E}_\mu \rho_x$. Now, $k = I(X : B) = \mathsf{E}_\mu S(\rho_x\|\rho)$. By Markov's inequality, there is a subset $\mathsf{Good} \subseteq \mathcal{X}$, $\Pr_\mu[\mathsf{Good}] \geq 1 - \delta/4$, such that for all $x \in \mathsf{Good}$, $S(\rho_x\|\rho) \leq 4k/\delta$. We will define superoperators $\mathcal{M}_x$ for $x \in \mathsf{Good}$ and $x \notin \mathsf{Good}$ separately, and then show that they form a (δ, α)-corrector.

Fix $x \in \mathsf{Good}$. Using Fact 1 with r to be chosen later, we conclude that for all $x \in \mathsf{Good}$, there is an unnormalized superoperator $\tilde{\mathcal{M}}_x$ acting on A only such that if $q_x \stackrel{\Delta}{=} \mathsf{Tr}\tilde{\mathcal{M}}_x(|\phi\rangle\langle\phi|)$, $\tilde{\sigma}_x \stackrel{\Delta}{=} \frac{\tilde{\mathcal{M}}_x(|\phi\rangle\langle\phi|)}{q_x}$ then, $q_x \geq \frac{r-1}{r2^{4rk/\delta}}$ and $\|\tilde{\sigma}_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}} \leq \frac{2}{\sqrt{r}}$. Now, measure register X in $\tilde{\sigma}_x$ and declare success if the result is x. Let σ'_x be the resulting normalized state when x is observed. Measuring X in $|\phi_x\rangle$ results gives the value x with probability 1. Hence, by Proposition 1,

$$\|\sigma'_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}} \leq \frac{2}{\sqrt{r}}.$$

Furthermore, since $\|\tilde{\sigma}_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}} \leq \frac{2}{\sqrt{r}}$, the probability q'_x of observing x when X is measured in the state $\tilde{\sigma}_x$ is at least $1 - \frac{1}{\sqrt{r}}$, and the overall probability of success is at least $q_x q'_x \geq (1 - \frac{1}{\sqrt{r}})(\frac{r-1}{r2^{4rk/\delta}}) \stackrel{\Delta}{=} \alpha$. In order to ensure that the overall probability of success is exactly α, we do a further *rejection* step: Even on success we artificially declare failure with probability $1 - \frac{\alpha}{q_x q'_x}$. Let $\mathcal{M}_x$ be the unnormalized superoperator which first applies $\tilde{\mathcal{M}}_x$, then measures the register X, and on finding x accepts with probability $\frac{\alpha}{q_x q'_x}$. Thus, for all $x \in \mathsf{Good}$, the probability of success $r_x \stackrel{\Delta}{=} \mathsf{Tr}\mathcal{M}_x(|\phi\rangle\langle\phi|)$ is exactly equal to α. This completes the definition of $\mathcal{M}_x$ for $x \in \mathsf{Good}$.

For $x \notin \mathsf{Good}$, $\mathcal{M}_x$ swaps $|x\rangle$ into register X from some outside ancilla initialized to $|0\rangle$ and declares success artificially with probability $r_x = \alpha$. For all $x \in \mathcal{X}$, let $\sigma'_x \stackrel{\Delta}{=} \frac{\mathcal{M}_x(|\phi\rangle\langle\phi|)}{r_x}$.

Thus for all $x \in \mathcal{X}$, σ'_x contains $|x\rangle$ in register X and $r_x = \alpha$. Finally, we have

$$\begin{aligned}
&\mathsf{E}_\mu \|\sigma'_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}} \\
&\quad\leq \sum_{x \in \mathsf{Good}} \mu(x)\, \|\sigma'_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}} + \sum_{x \notin \mathsf{Good}} \mu(x) \cdot 2 \\
&\quad\leq \frac{2}{\sqrt{r}} + \frac{\delta}{4} \cdot 2.
\end{aligned}$$

For $r = \frac{16}{\delta^2}$, this quantity is at most δ, and we conclude that the family $\{\mathcal{M}_x\}_{x \in \mathcal{X}}$ forms the required (δ, α)-corrector for the ensemble $\{\{|\phi_x\rangle\}_{x \in \mathcal{X}}; |\phi\rangle\}$ with $\alpha = 2^{-O(k/\delta^3)}$. ■

3 Compressing the first message

To state our message compression and round elimination results, we need the following definitions.

Definition 5 ($[t; l_1, \ldots, l_t]^A$ protocol) *In a $[t; l_1, \ldots, l_t]^A$ protocol, there are t rounds of communication with Alice starting, the ith message being l_i qubits long. A $[t; l_1, \ldots, l_t]^B$ protocol is the same but Bob starts the communication.*

Theorem 1 (Compressing the first message) *Let $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ be a function and μ be a probability distribution on $\mathcal{X} \times \mathcal{Y}$. Suppose $\mathcal{P}$ is a $[t; l_1, l_2, \ldots, l_t]^A$ quantum protocol without prior entanglement for f having average error less than ϵ under μ. Let X denote the random variable corresponding to Alice's input and N_1 denote the qubits of Alice's first message in $\mathcal{P}$. Suppose $I(X : N_1) \leq k$. Let $\delta > 0$ be a sufficiently small constant. Then, there is a $[t; \beta, l_2 \ldots, l_t]^A$ quantum protocol $\mathcal{P}'$ with prior entanglement for f with average error less than $\epsilon + \delta$ under μ, where $\beta = O\left(\frac{k}{\delta^3}\right)$. Also, the first message of Alice in $\mathcal{P}'$ is classical.*

Proof: Let $|\phi_x\rangle$ denote the state vector in $\mathcal{P}$ of Alice's qubits (including her input register) and her first message N_1 just after she sends N_1 to Bob, when she is given input $x \in \mathcal{X}$. Let $|\phi\rangle$ denote the corresponding state vector in $\mathcal{P}$ when the protocol starts with Alice's input registers in the state $\sum_x \sqrt{p_x}|\phi_x\rangle$, where $p_x \stackrel{\Delta}{=} \Pr_\mu[X = x]$. Since $I(X : N_1) \leq k$, Lemma 1 implies that there is a $(\delta/2, \alpha)$-corrector $\{\mathcal{M}_x\}_{x \in \mathcal{X}}$ for the ensemble $\{\{|\phi_x\rangle\}_{x \in \mathcal{X}}; |\phi\rangle\}$ where $\alpha = 2^{-O(k/\delta^3)}$. That is, with $r_x \stackrel{\Delta}{=} \mathsf{Tr}(\mathcal{M}_x|\phi\rangle\langle\phi|)$ and $\sigma'_x \stackrel{\Delta}{=} \frac{\mathcal{M}_x(|\phi\rangle\langle\phi|)}{r_x}$, we have $\mathsf{E}_\mu\left[\|\sigma'_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}}\right] \leq \frac{\delta}{2}$.

We now describe the protocol $\mathcal{P}'$. The protocol $\mathcal{P}'$ starts with $2^\beta \stackrel{\Delta}{=} \alpha^{-1}\log(2/\delta)$ copies of $|\phi\rangle$ as prior entanglement. Alice applies $\mathcal{M}_x$ to each copy of $|\phi\rangle$ and sends the index of the first copy on which she achieves success. Thus, her first message in $\mathcal{P}'$ is classical and $\beta = \log(1/\alpha) + \log\log(2/\delta) = O(k/\delta^3)$ bits long. Alice and Bob use that copy henceforth; the rest of $\mathcal{P}'$ is exactly as in $\mathcal{P}$. The probability that Alice achieves success with $\mathcal{M}_x$ on at least one copy of $|\phi\rangle$ is more than $1 - \frac{\delta}{2}$. Furthermore, the state of Alice's registers and the first message N_1 on this copy is exactly σ'_x. Thus, the probability of error for the protocol $\mathcal{P}'$ is at most

$$\epsilon + \frac{\delta}{2} + \mathsf{E}_\mu\left[\|\sigma'_x - |\phi_x\rangle\langle\phi_x|\|_{\mathrm{tr}}\right] \leq \epsilon + \frac{\delta}{2} + \frac{\delta}{2} \leq \epsilon + \delta.$$

This completes the proof of the theorem. ■

Remark: We can eliminate prior entanglement in quantum protocols by assuming that Alice generates the prior entangled state herself, and then sends Bob's share of the state along with her first message. This can make Alice's first message long, but if the information about X in Alice's first message together with Bob's share of prior entanglement qubits in the original protocol is small, then the conclusions of the theorem still hold.

Corollary 1 (Eliminating the first round) *Under the conditions of Theorem 1, if $t \geq 3$ there is a $[t-1; 2^{\beta} l_2, l_3 + \beta, l_4, \ldots, l_t]^B$ quantum protocol $\tilde{\mathcal{P}}$ with prior entanglement for f with average error at most $\epsilon + \delta$ under μ. If $t = 2$, we get a $[1; 2^{\beta} l_2]^B$ quantum protocol $\tilde{\mathcal{P}}$ with prior entanglement for f with average error at most $\epsilon + \delta$ under μ.*

Proof: Suppose $t \geq 3$. Let N_2, N_3 denote the second and third messages of $\mathcal{P}'$. Consider a $(t-1)$-round protocol $\tilde{\mathcal{P}}$ where Bob begins the communication by sending his messages N_2 for all the 2^{β} copies of $|\phi\rangle$. This makes Bob's first message in $\tilde{\mathcal{P}}$ to be $2^{\beta} l_2$ qubits long. Alice replies by applying $\mathcal{M}_x$ to each copy of $|\phi\rangle$ and sending the index of the first copy on which she achieves success. She also sends her response N_3 corresponding to that copy of $|\phi\rangle$. Thus, her first message in $\tilde{\mathcal{P}}$ is $l_3 + \beta$ qubits long. Note that the operations of Bob and the applications of $\mathcal{M}_x$ by Alice during the first two messages of $\tilde{\mathcal{P}}$ are on disjoint sets of qubits, hence they commute. Thus, the global state vector of $\tilde{\mathcal{P}}$ after the second message is exactly the same as the global state vector of $\mathcal{P}'$ after the third message. Hence the error probability remains the same. This proves the first statement of the corollary. The second statement of the corollary (case $t = 2$) can be proved similarly. ■

Remark: The above corollary can be thought of as the quantum analogue of the 'message switching' lemma of [CR04].

We get the following implication of Theorem 1 to the direct sum problem for one-round quantum communication protocols. Below, $Q^{1,A \to B,\mathrm{pub}}(f)$ denotes the communication complexity of a one-round quantum protocol (with A communicating) with prior entanglement computing f with error at most $1/4$ for any input, and $Q^{\|,\mathrm{pub}}(f)$ denotes the communication complexity of a simultaneous message quantum protocol with prior entanglement between Alice and the referee and Bob and the referee only, computing f with error at most $1/4$ for any input. Recall (see the introduction) that $f^{\oplus m}$ is the m-fold direct sum problem corresponding to the function f.

Corollary 2 *For one-round quantum protocols with prior entanglement, we get $Q^{1,A \to B,\mathrm{pub}}(f^{\oplus m}) \geq m \cdot \Omega(Q^{1,A \to B,\mathrm{pub}}(f))$. For simultaneous protocols with prior entanglement between Alice and the referee, and Bob and the referee only, we get $Q^{\|,\mathrm{pub}}(f^{\oplus m}) \geq m \cdot \Omega(Q^{\|,\mathrm{pub}}(f))$.*

Proof:**(Sketch)** The proof follows by adapting standard mutual information-based direct sum arguments (see e.g. [CSWY01, JRS03]) to the quantum setting and combining them with Theorem 1 and Yao's minimax lemma. We first remove prior entanglement from the one-round protocol for $f^{\oplus m}$ as in the remark following the proof of Theorem 1. After this, we note that the mutual information between Alice's input and her message is at most $2 \cdot Q^{1,A \to B,\mathrm{pub}}(f^{\oplus m})$, irrespective of the number of qubits of prior entanglement in the original protocol [CvDNT98]. ■

Using Corollary 1, we can now prove our new round elimination result for quantum protocols.

Theorem 2 (Round elimination lemma) *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function and k, t be positive integers. Suppose $t \geq 3$. Suppose $\mathcal{P}$ is a $[t; l_1, l_2, l_3, \ldots, l_t]^A$ quantum protocol with prior entanglement for $f^{(k),A}$ with worst case error less than ϵ. Let $\delta > 0$ be a sufficiently small constant. Let $\beta \triangleq O(\frac{l_1}{\delta^3 k})$. Then there is a $[t-1; 2^{\beta} l_2, l_3 + \beta, \ldots, l_t]^B$ quantum protocol with prior entanglement for f with worst case error at most $\epsilon + \delta$.*

Proof:(**Sketch**) The proof follows by combining the proof technique of Lemma 4 of [Sen03] with Corollary 1. ■

Remark: The above round elimination lemma is in fact the quantum analogue of a recent classical round elimination technique of Chakrabarti and Regev [CR04]. It allows us to extend their optimal randomized cell probe lower bound for approximate nearest neighbor searching in the Hamming cube $\{0,1\}^n$ to the quantum address-only cell probe model defined by Sen and Venkatesh [SV01]. It also allows us to extend the sharper lower bounds for predecessor searching of Patrascu and Thorup [PT04] to the quantum case.

4 Message compression for multi-round protocols

In this section, we state and formally prove our results for compressing messages in multi-round quantum communication protocols for computing a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. In our discussion below, A, X, B, Y denote Alice's work qubits, Alice's input qubits, Bob's work qubits and Bob's input qubits respectively, at a particular point in time.

Definition 6 (Privacy loss) *Let $\mu \triangleq \mu_{\mathcal{X}} \times \mu_{\mathcal{Y}}$ be a product probability distribution on $\mathcal{X} \times \mathcal{Y}$. Suppose $\mathcal{P}$ is a quantum protocol for a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. Consider runs of $\mathcal{P}$ when Alice's input register X starts in the mixed state $\sum_{x \in \mathcal{X}} \mu_{\mathcal{X}}(x) |x\rangle\langle x|$ and Bob's input register Y starts in the pure state $\sum_{y \in \mathcal{Y}} \sqrt{\mu_{\mathcal{Y}}(y)} |y\rangle$. Let B denote the qubits in the possession of Bob including Y, at* *some point during the execution of $\mathcal{P}$. Let $I(X : B)$ denote the mutual information of Alice's input register X with Bob's qubits B. The* privacy loss *of $\mathcal{P}$ for function f on the distribution μ from Alice to Bob at that point in time is $L^{\mathcal{P}}(f, \mu, A, B) \stackrel{\Delta}{=} I(X : B)$. The privacy loss from Bob to Alice, $L^{\mathcal{P}}(f, \mu, B, A)$, is defined similarly. The privacy loss of $\mathcal{P}$ from Alice to Bob for f, $L^{\mathcal{P}}(f, A, B)$, is the maximum over all product distributions μ of $L^{\mathcal{P}}(f, \mu, A, B)$. The privacy loss of $\mathcal{P}$ from Bob to Alice for f, $L^{\mathcal{P}}(f, B, A)$, is defined similarly. The privacy loss from Alice to Bob for f, $L(f, A, B)$, is the infimum over all protocols $\mathcal{P}$ of $L^{\mathcal{P}}(f, A, B)$ at the end of $\mathcal{P}$. The quantity $L(f, B, A)$ is defined similarly.*

Theorem 3 (Compressing many rounds) *Suppose $\mathcal{P}$ is a $[t; l_1, l_2, \ldots, l_t]^A$ quantum protocol without prior entanglement for a function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. Let $\mu \stackrel{\Delta}{=} \mu_{\mathcal{X}} \times \mu_{\mathcal{Y}}$ be a product probability distribution on $\mathcal{X} \times \mathcal{Y}$. Suppose the average error of $\mathcal{P}$ when the inputs are chosen according to μ is at most ϵ. Let k_a, k_b denote the privacy losses of Alice and Bob respectively after t' rounds of communication. Suppose t' is odd (similar statements hold for even t, as well as for interchanging the roles of Alice and Bob). Then, for all sufficiently small constants $\delta > 0$, there exists a $[t - t' + 1; \lambda_1, \lambda_2, l_{t'+2}, \ldots, l_t]^A$ protocol $\mathcal{P}'$ in the presence of prior entanglement such that:*

1. *the average error of $\mathcal{P}'$ with respect to μ is at most $\epsilon + \delta$;*
2. *$\lambda_1 \leq k_a \cdot 2^{O(k_b/\delta^6)}$ and $\lambda_2 \leq l_{t'+1} + O(k_b/\delta^6)$.*

Proof: Consider the situation after t' rounds of $\mathcal{P}$. Let the joint state of Alice and Bob be denoted by

σ_{xy}: when Alice starts $\mathcal{P}$ with x in her input register and Bob starts with y in his input register;

σ_x: when Alice starts with x in her input register and Bob starts with the superposition $\sum_{y \in \mathcal{Y}} \sqrt{\mu_{\mathcal{Y}}(y)} |y\rangle$ in his input register;

σ_y: when Bob starts with y in his input register and Alice starts with the superposition $\sum_{x \in \mathcal{X}} \sqrt{\mu_{\mathcal{X}}(x)} |x\rangle$ in her input register;

σ: when Alice and Bob start with the superposition $\sum_{(x,y) \in \mathcal{X} \times \mathcal{Y}} \sqrt{\mu(xy)} |x\rangle |y\rangle$ in their input registers.

Note that σ_{xy}, σ_x, σ_y and σ are pure states.

We overload the symbols $\mathcal{X}, \mathcal{Y}$ to also denote the superoperators corresponding to measuring in the computational basis the input registers X, Y of Alice and Bob respectively. Whether $\mathcal{X}, \mathcal{Y}$ denote sets or superoperators will be clear from the context. When several superoperators are applied to a state in succession we omit the parenthesis; for example, we write $\mathcal{X}\mathcal{Y}(\rho)$ instead of $\mathcal{X}(\mathcal{Y}(\rho))$ which corresponds to measuring the input registers of Alice and Bob (in this case, their order does not matter).

We will choose $\delta_a, \delta_b > 0$ later. Since the privacy loss of Alice is at most k_a, Lemma 1 implies that there is a (δ_a, α)-corrector $\{\mathcal{M}_x\}_{x \in \mathcal{X}}$ for $\{\{\sigma_x\}_{x \in \mathcal{X}}; \sigma\}$ with $\alpha = 2^{-O(k_a/\delta_a^3)}$. Similarly, since the privacy loss of Bob is at most k_b, there is a (δ_b, β)-corrector $\{\mathcal{M}_y\}_{y \in \mathcal{Y}}$ for $\{\{\sigma_y\}_{y \in \mathcal{Y}}; \sigma\}$ with $\beta = 2^{-O(k_b/\delta_b^3)}$. In particular, with $\mathcal{M}_X \stackrel{\Delta}{=} \mathsf{E}_{\mu_{\mathcal{X}}}[\mathcal{M}_x]$ and $\mathcal{M}_Y \stackrel{\Delta}{=} \mathsf{E}_{\mu_{\mathcal{Y}}}[\mathcal{M}_y]$, we have

$$\left\| \frac{\mathcal{M}_X(\sigma)}{\alpha} - \mathcal{X}(\sigma) \right\|_{\mathrm{tr}} \leq \delta_a, \qquad\qquad (1)$$

$$\left\| \frac{\mathcal{M}_Y(\sigma)}{\beta} - \mathcal{Y}(\sigma) \right\|_{\mathrm{tr}} \leq \delta_b.$$

In our proof, we will take

$$\delta_b \stackrel{\Delta}{=} \left(\frac{\delta}{10} \right)^2, \quad \delta_a \stackrel{\Delta}{=} \frac{\delta_b \beta}{2}. \qquad\qquad (2)$$

The proof has two steps. In the first step, we analyze the protocol $\mathcal{P}'$ given in Figure 1. In $\mathcal{P}'$, Alice and Bob try to recreate the effect of the first t' rounds of the original protocol, but without sending any messages. For this, they start from the state σ (their prior entanglement) and on receiving x and y, apply suitable correcting transformations. In the second step, we shall consider a protocol $\mathcal{P}''$ that starts with several parallel executions of $\mathcal{P}'$.

Alice and Bob start with the joint state σ as prior entanglement.

Input: Alice is given $x \in X$; Bob is given $y \in Y$.

Alice: Applies superoperator $\mathcal{M}_x$ to her registers.

Bob: Applies superoperator $\mathcal{M}_y$ to his registers.

Figure 1. The intermediate protocol $\mathcal{P}'$

Let $r_{xy} \stackrel{\Delta}{=} \mathsf{Tr}\mathcal{M}_y\mathcal{M}_x(\sigma)$ and let $r \stackrel{\Delta}{=} \mathsf{E}_\mu[r_{xy}]$. Then, r_{xy} is the probability that both Alice and Bob succeed on input (x, y), and r is the probability that they succeed when their input is chosen according to the distribution μ. Let ρ denote the state after t' rounds of $\mathcal{P}$ when the inputs are chosen according to μ i.e. $\rho \stackrel{\Delta}{=} \mathsf{E}_\mu[\sigma_{xy}]$. Observe that $\rho = \mathcal{Y}\mathcal{X}(\sigma)$. Let ρ' be the state at the end of $\mathcal{P}'$, when the inputs are chosen according to μ and we condition on both parties succeeding i.e. $\rho' = \frac{\mathcal{M}_Y \mathcal{M}_X(\sigma)}{r}$.

Claim 1 *(a)* $1 - \frac{\delta_b}{2} \leq \frac{r}{\alpha\beta} \leq 1 + \frac{\delta_b}{2}$.

(b) $\|\rho - \rho'\|_{\mathrm{tr}} \le 2\delta_b$.

(c) $\Pr_\mu\left[\left|\frac{r_{xy}}{r} - 1\right| \ge 2\delta_b^{1/2}\right] \le \delta_b^{1/2}$.

Proof:

(a)

$$\begin{aligned}
\frac{r}{\alpha\beta} &= \frac{\mathsf{Tr}\mathcal{M}_Y\mathcal{M}_X(\sigma)}{\alpha\beta} \\
&= \frac{1}{\beta}\mathsf{Tr}\left(\mathcal{M}_Y\left(\frac{\mathcal{M}_X(\sigma)}{\alpha}\right)\right) \\
&= \frac{1}{\beta}\mathsf{Tr}\mathcal{M}_Y\mathcal{X}(\sigma) + \\
&\quad \frac{1}{\beta}\mathsf{Tr}\mathcal{M}_Y\left(\frac{\mathcal{M}_x(\sigma)}{\alpha} - \mathcal{X}(\sigma)\right).
\end{aligned}$$

The first term on the right is 1 since $\mathcal{M}_{\mathcal{Y}}$ and $\mathcal{X}$ commute as they act on disjoint sets of qubits. For the second term, we have using (1), (2) and the fact that an unnormalized superoperator cannot increase the trace norm, that

$$\left|\frac{1}{\beta}\mathsf{Tr}\mathcal{M}_Y\left(\frac{\mathcal{M}_X(\sigma)}{\alpha} - \mathcal{X}(\sigma)\right)\right| \le \frac{\delta_a}{\beta} = \frac{\delta_b}{2}.$$

(b) Using (1), (2), the fact that a measurement or an unnormalized superoperator cannot increase the trace norm, and that $\mathcal{M}_{\mathcal{Y}}$ and $\mathcal{X}$ commute as they act on disjoint sets of qubits, we get

$$\begin{aligned}
\|\rho - \rho'\|_{\mathrm{tr}} &= \|\mathcal{X}\mathcal{Y}(\sigma) - \rho'\|_{\mathrm{tr}} \\
&\le \left\|\mathcal{X}\frac{\mathcal{M}_{\mathcal{Y}}(\sigma)}{\beta} - \rho'\right\|_{\mathrm{tr}} + \\
&\quad \left\|\mathcal{X}\left(\mathcal{Y}(\sigma) - \frac{\mathcal{M}_{\mathcal{Y}}(\sigma)}{\beta}\right)\right\|_{\mathrm{tr}} \\
&\le \left\|\mathcal{M}_{\mathcal{Y}}\frac{\mathcal{X}(\sigma)}{\beta} - \rho'\right\|_{\mathrm{tr}} + \delta_b \\
&\le \left\|\frac{1}{\beta}\mathcal{M}_Y\frac{\mathcal{M}_X(\sigma)}{\alpha} - \rho'\right\|_{\mathrm{tr}} + \delta_b + \\
&\quad \frac{1}{\beta}\left\|\mathcal{M}_Y\left(\mathcal{X}(\sigma) - \frac{\mathcal{M}_X(\sigma)}{\alpha}\right)\right\|_{\mathrm{tr}} \\
&\le \left\|\frac{1}{\beta}\mathcal{M}_Y\frac{\mathcal{M}_X(\sigma)}{\alpha} - \rho'\right\|_{\mathrm{tr}} + \delta_b + \frac{\delta_a}{\beta} \\
&\le \left\|\frac{r}{\alpha\beta}\frac{\mathcal{M}_Y\mathcal{M}_X(\sigma)}{r} - \rho'\right\|_{\mathrm{tr}} + \frac{3\delta_b}{2} \\
&= \left\|\left(\frac{r}{\alpha\beta} - 1\right)\rho'\right\|_{\mathrm{tr}} + \frac{3\delta_b}{2} \\
&\le 2\delta_b.
\end{aligned}$$

(c) Let τ describe the joint state of the input registers when the combined state of Alice and Bob is ρ; similarly, let τ' be the state of their input registers when the combined state is ρ'; thus,

$$\tau = \sum_{xy} p_{xy}|x\rangle\langle x| \otimes |y\rangle\langle y|$$

and

$$\tau' = \sum_{xy} p_{xy}\frac{r_{xy}}{r}|x\rangle\langle x| \otimes |y\rangle\langle y|.$$

Using part (b), we have

$$\sum_{xy} p_{xy}\left|1 - \frac{r_{xy}}{r}\right| = \|\tau - \tau'\|_{\mathrm{tr}} \le \|\rho - \rho'\|_{\mathrm{tr}} \le 2\delta_b.$$

Thus, $\mathsf{E}_\mu\left[\left|\frac{r_{xy}}{r} - 1\right|\right] \le 2\delta_b$, and by Markov's inequality, $\Pr_\mu\left[\left|\frac{r_{xy}}{r} - 1\right| \ge 2\delta_b^{1/2}\right] \le \delta_b^{1/2}$.

■

We can now move to the second step of our proof of Theorem 3. Figure 2 presents a protocol $\mathcal{P}''$ with $t - t' + 1$ rounds of communication where the initial actions of Alice and Bob are derived from the protocol $\mathcal{P}'$ analyzed above.

Alice and Bob start with $K \triangleq \frac{10}{r}(\log\frac{1}{\delta})$ copies of σ as prior entanglement. We refer to these copies as $\sigma^1, \ldots, \sigma^K$.

Input: Alice gets $x \in X$ and Bob gets $y \in Y$.

Alice: Applies $\mathcal{M}_x$ to each σ^i. Let $\hat{S} \triangleq \{i : \mathcal{M}_x$ succeeded on $\sigma^i\}$. If $\hat{S}$ has less than $2\alpha K$ elements, Alice aborts the protocol; otherwise, she sends $S \subseteq \hat{S}$ to Bob, $|S| = 2\alpha K$.

Bob: Applies $\mathcal{M}_y$ to each σ_i for $i \in S$ and sends Alice the index i^* where he (and hence both) succeeded. If there is is no such i^* he aborts the protocol.

Alice and Bob now revert to protocol $\mathcal{P}$ after round t', and operate on the registers corresponding to σ^{i^*}.

Figure 2. The final protocol $\mathcal{P}''$

Claim 2 *(a) The number of bits sent by Alice in the first round is at most $k_a 2^{O(k_b/\delta^6)}$; the number of bits sent by Bob is at most $O(k_b/\delta^6)$.*

(b) If the inputs are chosen according to the distribution μ, the protocol $\mathcal{P}''$ computes f correctly with probability of error at most $\epsilon + \delta$.

Proof: Recall that $\delta_b = (\delta/10)^2$, $\beta = 2^{-O(k_b/\delta_b^3)}$ and $\delta_a = \delta_b\beta/2$ and $\alpha = 2^{-O(k_a/\delta_a^3)}$. By part (a) of Claim 1 it follows that $r \geq \alpha\beta/2$. The number of bits needed by Alice to encode her set S is at most

$$\log \binom{K}{2\alpha K} \leq 2\alpha K \log\left(\frac{e}{2\alpha}\right) = k_a 2^{O(k_b/\delta^6)}.$$

The number of bits sent by Bob is at most $\log 2\alpha K = O\left(\frac{k_b}{\delta^6}\right)$. This justifies part (a) of our claim.

For part (b), we will use Claim 1 to bound the probability of error $\mathcal{P}''$. Call a pair $(x, y) \in \mathcal{X} \times \mathcal{Y}$ *good* if $|\frac{r_{xy}}{r} - 1| \leq 2\delta_b^{1/2}$; let χ denote the indicator random variable for the event "(x, y) is good." Let χ' be the indicator random variable for the event "Alice and Bob do not abort protocol $\mathcal{P}''$." Note that if Alice and Bob do not abort protocol $\mathcal{P}''$, they enter round $t' + 1$ of protocol $\mathcal{P}$ with their registers in the state $\sigma'_{xy} \triangleq \frac{\mathcal{M}_x\mathcal{M}_y(\sigma)}{r_{xy}}$. Thus under distribution μ, the average probability of error of $\mathcal{P}''$ differs from the average probability of error ϵ of the original protocol $\mathcal{P}$ by at most

$$\begin{array}{l} \mathsf{E}_\mu\left[\chi\chi' \left\|\sigma'_{xy} - \sigma_{xy}\right\|_{\mathrm{tr}}\right] + \Pr[\chi = 0] + \\ \Pr[\chi = 1 \text{ and } \chi' = 0]. \end{array} \qquad (3)$$

The first term in the above sum can be bounded as follows:

$$\begin{aligned} & \mathsf{E}_\mu\left[\chi\chi' \left\|\sigma'_{xy} - \sigma_{xy}\right\|_{\mathrm{tr}}\right] \\ = \quad & \mathsf{E}_\mu\left[\chi\chi' \left\|\frac{1}{r_{xy}}\mathcal{M}_x\mathcal{M}_y(\sigma) - \sigma_{xy}\right\|_{\mathrm{tr}}\right] \\ \leq \quad & \mathsf{E}_\mu\left[\chi\chi' \left\|\frac{1}{r}\mathcal{M}_x\mathcal{M}_y(\sigma) - \sigma_{xy}\right\|_{\mathrm{tr}}\right] + \\ & \mathsf{E}_\mu\left[\chi\chi' \left|1 - \frac{r_{xy}}{r}\right| \frac{1}{r_{xy}} \left\|\mathcal{M}_x\mathcal{M}_y(\sigma)\right\|_{\mathrm{tr}}\right] \\ \leq \quad & \left\|\frac{1}{r}\mathcal{M}_Y\mathcal{M}_X(\sigma) - \mathcal{X}\mathcal{Y}(\sigma)\right\|_{\mathrm{tr}} + \\ & \mathsf{E}_\mu\left[\chi\chi' \left|1 - \frac{r_{xy}}{r}\right| \frac{1}{r_{xy}} \left\|\mathcal{M}_x\mathcal{M}_y(\sigma)\right\|_{\mathrm{tr}}\right] \\ \leq \quad & 2\delta_b + 2\delta_b^{1/2}. \end{aligned}$$

For the second last inequality, we used the fact that in the states σ'_{xy} and σ_{xy}, the input registers of Alice and Bob contain x and y. For the last inequality, we used part (b) of Claim 1 and the definition of good (x, y). The second term of (3) is at most $\delta_b^{1/2}$ by part (c) of Claim 1. It remains to bound the last term of (3), which corresponds to the probability that Alice or Bob abort the protocol for some good (x, y).

Alice aborts: The probability of success of $\mathcal{M}_x$ for any one copy of σ is exactly α. Thus, the expected number of successes is αK, and by Chernoff's bound (see e.g. [AS00, Appendix A]), the probability that there are less than $2\alpha K$ successes is at most $\left(\frac{e}{4}\right)^{\alpha K} \leq \delta^{10}$.

Bob aborts: Bob aborts when the two parties do not simultaneously succeed in any of the K attempts, even though their probability of success was at least $r_{xy} \geq (1 - 2\delta_b^{1/2})r \geq r/2$ (recall that we are now considering a good pair (x, y)). The probability of this is at most $\left(1 - \frac{r}{2}\right)^K \leq \exp\left(-\frac{rK}{2}\right) \leq \delta^5$.

Thus overall, the average probability of error of $\mathcal{P}''$ is at most

$$\epsilon + 2\delta_b + 2\delta_b^{1/2} + \delta_b^{1/2} + \delta^{10} + \delta^5 \leq \epsilon + \delta.$$

■

This completes the proof of Theorem 3. ■

The following corollaries result from the above theorem. In what follows, let $Q^{1,A\to B,\mathrm{pub}}_{[\,]}(f)$ denote the communication complexity of one-round quantum protocols with prior entanglement and Alice communicating computing f with bounded average error under product distributions. We define $Q^{1,B\to A,\mathrm{pub}}_{[\,]}(f)$ analogously. We let $Q^{\mathrm{pub}}_{[\,]}(f)$ denote the round-independent communication complexity of quantum protocols with prior entanglement computing f with bounded average error under product distributions.

Corollary 3 (Privacy tradeoff) *For any function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, $L(f, A, B)2^{O(L(f,B,A))} \geq Q^{1,A\to B,\mathrm{pub}}_{[\,]}(f)$. Similarly, $L(f, B, A)2^{O(L(f,A,B))} \geq Q^{1,B\to A,\mathrm{pub}}_{[\,]}(f)$.*

Remark: It was shown by Kremer [Kre95] that $Q(f) \geq \Omega(\log D^1(f))$, where $D^1(f)$ is the one-round deterministic communication complexity of f. The above corollary can be viewed as the privacy analogue of that result. It is optimal as evidenced by the index function problem and the pointer chasing problem, both of which have communication complexity $O(\log n)$ [JRS02].

Corollary 4 (A weak direct sum result) *For any function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$, $Q^{\mathrm{pub}}_{[\,]}(f^{\oplus m}) \geq m \cdot \Omega(\log Q^{1,pub}_{[\,]}(f))$.*

Remark: Jain, Radhakrishnan, and Sen [JRS03] proved a direct sum result for classical constant round protocols. Their result was stronger because it avoided the logarithm. However, if we want a direct sum result independent of the number of rounds, the above is the best possible as evidenced by the index function problem and the pointer chasing problem [JRS02].

5 Entanglement reduction

We will need the following geometric result. It is similar to a result proved earlier in [JRS03].

Lemma 2 *Suppose M, N are positive integers with $M = \theta(N^{2/3} \log N)$. Let the underlying Hilbert space be $\mathbb{C}^M$. There exist $16N$ subspaces $V_{ij} \leq \mathbb{C}^M$, $1 \leq i \leq N$, $1 \leq$*

$j \leq 16$, each of dimension $\frac{M}{16}$, such that if we define Π_{ij} to be the orthogonal projection onto V_{ij} and $\rho_{ij} \triangleq \frac{16}{M} \cdot \Pi_{ij}$, then

1. *$\forall i, j$ $\mathsf{Tr}(\Pi_{ij}\rho_{ij}) = 1$.*
2. *$\forall i, j, i', j'$, $i \neq i'$, $\mathsf{Tr}(\Pi_{ij}\rho_{i'j'}) < 1/4$.*
3. *$\forall i, j, j'$, $j \neq j'$, $\mathsf{Tr}(\Pi_{ij}\rho_{ij'}) = 0$.*
4. *$\forall i$, $I_M = \sum_{j=1}^{16} \Pi_{ij}$, where I_M is the identity operator on $\mathbb{C}^M$.*
5. *For all subspaces W of dimension at most $N^{1/6}$, for all families of density matrices $\{\sigma_{ij}\}_{i \in [N], 1 \leq j \leq 16}$, σ_{ij} supported in W,*

$$|\{i : \exists j,\ 1 \leq j \leq 16,\ \mathsf{Tr}(\Pi_{ij}\sigma_{ij}) > 9/16\}| \leq N/4.$$

Proof:(**Sketch**) The proof follows by combining the proofs of Theorem 5 and Lemma 7 of [JRS03]. ■

We shall also need the following easy proposition.

Proposition 2 *Let $|\phi\rangle_{AB}$ be a bipartite pure quantum state. Define $e \triangleq E(|\phi\rangle)$. Then there is a bipartite pure quantum state $|\phi'\rangle_{AB}$ having Schmidt rank at most 2^{100e} such that $\||\phi\rangle\langle\phi| - |\phi'\rangle\langle\phi'|\|_{\mathrm{tr}} \leq 1/20$.*

Proof: Let $|\phi\rangle_{AB} = \sum_i \sqrt{\lambda_i}|a_i\rangle_A|b_i\rangle_B$ be the Schmidt decomposition of $|\phi\rangle$, $\lambda_i \geq 0$, $\sum_i \lambda_i = 1$. Define a set $\mathsf{Good} \triangleq \{i : \lambda_i \geq 2^{-100e}\}$. Since $e = -\sum_i \lambda_i \log \lambda_i$, by Markov's inequality $\sum_{i \in \mathsf{Good}} \lambda_i \geq 99/100$. Define the bipartite pure state $|\phi'\rangle_{AB} \triangleq \sum_{i \in \mathsf{Good}} \sqrt{\lambda_i}|a_i\rangle_A|b_i\rangle_B$ normalized. The Schmidt rank of $|\phi'\rangle_{AB}$ is at most 2^{100e} and $\||\phi\rangle\langle\phi| - |\phi'\rangle\langle\phi'|\|_{\mathrm{tr}} \leq 1/20$. ■

We are now ready to prove our impossibility result about black-box reduction of prior entanglement.

Theorem 4 (No black-box red. of prior entan.) *Let EQ_n denote the equality function on n-bit strings. There exists a one-round quantum protocol $\mathcal{P}$ for EQ_n with $\frac{2n}{3} + \log n + \theta(1)$ EPR pairs of prior entanglement and communicating 4 bits such that, there is no similar protocol $\mathcal{P}'$ that starts with a prior entangled state $|\phi\rangle$, $E(|\phi\rangle) \leq \frac{n}{600}$.*

Proof: We use the notation of Lemma 2 with $M \triangleq 2^m$ and $N \triangleq 2^n$. Let $0 \leq i \leq 2^n - 1$ i.e. $i \in \{0,1\}^n$. Choose $m = \frac{2n}{3} + \log n + \theta(1)$. Let $\mathcal{P}$ be a one-round protocol with m EPR pairs of prior entanglement. In $\mathcal{P}$, on input i Alice measures her EPR halves according to the von Neumann measurement $\{\Pi_j\}_{1 \leq j \leq 16}$ and sends the result j as a 4-bit classical message to Bob. The state of Bob's EPR halves now becomes ρ_{ij}. On input i' and message j', Bob performs the two-outcome measurement $\{\Pi_{i'j'}, I_M - \Pi_{i'j'}\}$ on his EPR halves. Therefore in $\mathcal{P}$, Bob outputs 1 with probability 1 if $i' = i$ and with probability at most $1/4$ if $i' \neq i$. Thus, $\mathcal{P}$ is a protocol for EQ_n.

Suppose there exists a protocol $\mathcal{P}'$ similar to $\mathcal{P}$ that starts with an input independent shared state $|\phi'\rangle_{AB}$ on $m + m$ qubits. Suppose $E(|\phi\rangle) \leq n/10$. By Proposition 2, there is a bipartite pure state $|\phi''\rangle_{AB}$ on $m + m$ qubits having Schmidt rank at most $2^{n/6}$ such that $\||\phi'\rangle\langle\phi'| - |\phi''\rangle\langle\phi''|\|_{\mathrm{tr}} \leq 1/20$. Consider the protocol $\mathcal{P}''$ similar to $\mathcal{P}'$ starting with $|\phi''\rangle_{AB}$ as prior entanglement. Since $\mathcal{P}''$ is similar to $\mathcal{P}'$, it is also a one-round protocol with 4 classical bits of communication. Let σ_{ij} be the state of Bob's share of prior entanglement qubits after the first round of communication from Alice when Alice's input is i and her message is j. Since the Schmidt rank of $|\phi''\rangle$ is at most $2^{n/6}$, the σ_{ij}, $0 \leq i \leq 2^n - 1$, $1 \leq j \leq 16$ have support in a $2^{n/6}$-dimensional space. Let p_{ij} be the probability with which Alice sends message j when her input is i. It follows that for all i, $\sum_{j=1}^{16} p_j \mathsf{Tr} M_{ij}\sigma_{ij} \geq \frac{3}{4} - \frac{1}{20} - \frac{1}{20} = \frac{13}{20}$. This implies that for all i there exists a j, $1 \leq j \leq 16$, such that $\mathsf{Tr} M_{ij}\sigma_{ij} \geq 13/20 > 9/16$. From Lemma 2 this is not possible, and hence no such protocol $\mathcal{P}'$ exists. ■

Acknowledgment: We thank the referees for their comments and suggestions. We are grateful to Harold Ollivier for his comments on the proof of Theorem 4.

References

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998. Also quant-ph/9806029.

[ANTV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

[AS00] N. Alon and J. Spencer. *The probabilistic method*. John Wiley and Sons, 2000.

[BCJ$^+$93] C. Bennett, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. In *Physical Review Letters*, volume 70, pages 1895–1899, 1993.

[BCKO93] R. Bar-Yehuda, B. Chor, E. Kushilevitz, and A. Orlitsky. Privacy, additional information, and communication. *IEEE Transactions on Information Theory*, 39(6):1930–1943, 1993.

[BJKS02] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 209–218, 2002.

[BW92] C. Bennett and S. Wiesner. Communication via one and two particle operators on Einstein-Podolsky-Rosen states. In *Physical Review Letters*, volume 69, pages 2881–2884, 1992.

[CR04] A. Chakrabarti and O. Regev. An optimal randomised cell probe lower bound for approximate nearest neighbour searching. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science*, 2004.

[CSWY01] A. Chakrabarti, Y. Shi, A. Wirth, and A. Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 270–278, 2001.

[CvDNT98] R. Cleve, Wim van Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Proceedings of the 1st NASA International Conference on Quantum Computing and Quantum Communications*, Lecture Notes in Computer Science, vol. 1509, pages 61–74. Springer-Verlag, 1998. Also quant-ph/9708019.

[JRS02] R. Jain, J. Radhakrishnan, and P. Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 429–438, 2002.

[JRS03] R. Jain, J. Radhakrishnan, and P. Sen. A direct sum theorem in communication complexity via message compression. In *Proceedings of the 30th International Colloquium on Automata, Languages and Programming*, Lecture Notes in Computer Science, vol. 2719, pages 300–315. Springer-Verlag, 2003. Also cs.CC/0304020.

[Kla02] H. Klauck. On quantum and approximate privacy. In *Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, vol. 2285, pages 335–346. Springer-Verlag, 2002. Also quant-ph/0110038.

[Kre95] I. Kremer. Quantum communication. Master's thesis, Hebrew University, Jerusalem, 1995.

[New91] I. Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[PT04] M. Patrascu and M. Thorup. Space-time tradeoffs for the predecessor problem. Unpublished manuscript, private communication, October, 2004.

[Sen03] P. Sen. Lower bounds for predecessor searching in the cell probe model. In *Proceedings of the 18th Annual IEEE Conference on Computational Complexity*, pages 73–83, 2003.

[SV01] P. Sen and S. Venkatesh. Lower bounds in the quantum cell probe model. In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming*, Lecture Notes in Computer Science, vol. 2076, pages 358–369. Springer-Verlag, 2001.