Annotated Bibliography

Rahul Jain *
Computer Science Department and Institute for Quantum Computing
University of Waterloo †

The papers with a short abstract are mentioned below in the reverse chronological order.

1. "New bounds on classical and quantum one-way communication complexity." Submitted, 2008. (With Shengyu Zhang.)

   Abstract: In this paper we provide new bounds on classical and quantum distributional communication complexity in the two-party, one-way model of communication.

   In the classical one-way model, our bound extends the well known upper bound of Kremer, Nisan and Ron [KNR95] to include non-product distributions. Let $\epsilon \in (0, 1/2)$ be a constant. We show that for a boolean function $f : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ and a non-product distribution μ on $\mathcal{X} \times \mathcal{Y}$,

   $$D^{1,\mu}_{\epsilon}(f) = O((I(X : Y) + 1) \cdot \mathsf{V}C(f)),$$

   where $D^{1,\mu}_{\epsilon}(f)$ represents the one-way distributional communication complexity of f with error at most ϵ under μ; $\mathsf{V}C(f)$ represents the *Vapnik-Chervonenkis* dimension of f and $I(X : Y)$ represents the mutual information, under μ, between the random inputs of the two parties. For a non-boolean function $f : \mathcal{X} \times \mathcal{Y} \to \{1, \ldots, k\}$ ($k \geq 2$ an integer), we show a similar upper bound on $D^{1,\mu}_{\epsilon}(f)$ in terms of $k, I(X : Y)$ and the *pseudo-dimension* of $f' \triangleq \frac{f}{k}$, a generalization of the $\mathsf{V}C$-dimension for non-boolean functions.

   In the quantum one-way model we provide a lower bound on the distributional communication complexity, under product distributions, of a function f, in terms the well studied complexity measure of f referred to as the *rectangle bound* or the *corruption bound* of f. We show for a non-boolean total function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ and a product distribution μ on $\mathcal{X} \times \mathcal{Y}$,

   $$Q^{1,\mu}_{\epsilon^3/8}(f) = \Omega(\mathsf{rec}^{1,\mu}_{\epsilon}(f)),$$

   where $Q^{1,\mu}_{\epsilon^3/8}(f)$ represents the quantum one-way distributional communication complexity of f with error at most $\epsilon^3/8$ under μ and $\mathsf{rec}^{1,\mu}_{\epsilon}(f)$ represents the one-way rectangle bound of f with error at most ϵ under μ. Similarly for a non-boolean partial function $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z} \cup \{*\}$ and a product distribution μ on $\mathcal{X} \times \mathcal{Y}$, we show,

   $$Q^{1,\mu}_{\epsilon^6/(2 \cdot 15^4)}(f) = \Omega(\mathsf{rec}^{1,\mu}_{\epsilon}(f)).$$

2. "A separation between divergence and Holevo information for ensembles." In Proceedings of the 5th Annual Conference on Theory and Applications of Models of Computation (TAMC), 2008. Also available at arXiv:0712.3867. (With Ashwin Nayak and Yi Su.)

   Abstract: The notion of *Divergence information* $D(\mathcal{E})$ for an ensemble $\mathcal{E}$ was defined by Jain *et al* [JRS02] in the context of the substate theorem. There it was shown that for all ensembles $\mathcal{E}$, $D(\mathcal{E}) \leq \chi(\mathcal{E}) + 1$ where $\chi(\mathcal{E})$ is the Holevo-χ information of $\mathcal{E}$. We investigate the inequality in the

*Email: rjain@cs.uwaterloo.ca
†200 University Avenue West, Waterloo, ON, Canada, N2L 3G1.

other direction. We show that there exists an ensemble $\mathcal{E}$ of classical distributions, with its distributions having support on $[N]$, such that $\chi(\mathcal{E}) = \Omega(D(\mathcal{E}) \log \log N)$. This result implies strengthening of several results derived using the substate theorem for example the binding-concealing trade-offs for quantum string commitment in [Jai06].

3. "Entanglement-resistant two-prover interactive proof systems and non-adaptive private information retrieval systems.", Submitted, 2007. Also available at arXiv:0707.1729. (With Richard Cleve and Dmitry Gavinsky.)

   Abstract: Two-prover classical interactive proof systems are known to be very powerful and include NEXP. In fact for every language in NEXP, there is a two-prover one-round protocol with constant bit answers by the provers [CHyTW04]. However if the provers are allowed to share *quantum entanglement*, it can potentially give them both extra power and also help them cheat. Understanding the power of entangled provers is an important question and is widely open.

   We make progress in this direction. We show that, for any language in NP, there is a two entangled prover, one-round, interactive proof system with single bit answers by the provers. This is currently the strongest expressive power of any known constant-bit answer, multi-prover interactive proof system. Our result is based on an *oracularizing* property of certain private information retrieval systems, which may be of independent interest.

4. " Direct product theorems for communication complexity via subdistribution bounds." In proceedings of The 40th ACM Symposium on Theory of Computing (STOC), 2008. Also available at ECCC report number TR07-064. (With Hartmut Klauck and Ashwin Nayak.)

   Abstract: A basic question in complexity theory is whether the computational resources required for solving k independent instances of the same problem scale as k times the resources required for one instance. The *Direct product* property for a resource states that if $o(kc)$ resource is provided for solving k independent instances, where c is the resource required for solving one-instance, then the overall success for all the k instances is exponentially small in k. We investigate this question for classical communication complexity.

   We define a new measure, the *subdistribution bound*, which is a generalization of the well-studied rectangle or corruption bound in communication complexity. We prove that the one-way version of this bound tightly captures the one-way public-coin randomized communication complexity of any relation. More importantly, we show that for any relation, this bound satisfies the strong direct product property under product distributions, for both one- and two-way communication. This way we recover and generalize, in a unified manner, several recent results on the direct product question, including those due to Klauck *et al.* [KvdW04], Beame *et al.* [BPSW07], Gavinsky [Gav06], and de Wolf [dW05].

   The simplicity and broad applicability of our technique is perhaps an indication of its potential to solve yet more challenging questions regarding the direct product problem.

5. "The communication complexity of correlation." In Proceedings of 22nd IEEE Conference on Computational Complexity (CCC), 2007. Also available at ECCC report number TR06-151, 2007. (With Prahladh Harsha and David McAllester and Jaikumar Radhakrishnan.)

   Abstract: We examine the communication required for generating random variables remotely. One party Alice will be given a distribution D, and she has to send a message to Bob, who is then required to generate a value with distribution exactly D. Alice and Bob are allowed to share random bits generated without the knowledge of D. There are two settings based on how the distribution D provided to Alice is chosen.

   Average case: D is itself chosen randomly from some set (the set and distribution are known in advance) and we wish to minimize the expected communication in order for Alice to generate a value y, with distribution D. We characterize the communication required in this case based on the mutual information between the the input to Alice and the output Bob is required to generate.

Worst case: D is chosen from a set of distributions $\mathcal{D}$, and we wish to devise a protocol so that the expected communication (the randomness comes from the shared random string and Alice's coin tosses) is small for each $D \in \mathcal{D}$. We characterize the communication required in this case in terms of the channel capacity associated with the set $\mathcal{D}$.

Prior to this work, only the limit (or asymptotic) versions of these results were known, where Alice is given a sequence of distributions $\langle D_1, D_2, \ldots, D_n \rangle$, and Bob is required to generate n values $\langle y_1, y_2, \ldots, y_n \rangle$, where y_i is distributed according to D_i. In these works the amortized cost (per D_i) was studied as n tends to infinity. In the case, when the D_i's are iid and some error is allowed, Winter [Win02] characterized the cost in terms of mutual information. In the case where D_i's are only known to come from some set $\mathcal{D}$ and we require worst case bounds, the Reverse Shannon Theorem of Bennett, Shor, Smolin and Thapliyal [BSST02] characterizes the limiting amortized cost in terms of the channel capacity.

Our results, are for the *one-shot* case and immediately imply the limit versions shown earlier. An essential ingredient in our proofs is a *rejection sampling* procedure that relates the relative entropy between two distributions to the communication complexity of generating one distribution from the other.

As an important application of our one-shot protocol, we also derive a *direct sum* result for two-way distributional communication complexity under product distributions. For any relation f and a product distribution μ on $\mathcal{X} \times \mathcal{Y}$, we show the following,

$$D_{\epsilon}^{\mu^t,k}(f^t) \geq \frac{t}{2}\left(\delta D_{\epsilon+\delta}^{\mu,k}(f) - O(k)\right).$$

Here, $D_{\epsilon}^{\mu,k}(f)$ represents the distributional complexity for computing f with k-round protocols with error at most ϵ, f^t represents t independent copies of f and μ^t represents t independent copies of μ. Our result substantially improves the previous such result shown by Jain *et al.* [JRS03].

6. " On parallel composition of zero-knowledge proofs with black-box quantum simulators." Submitted, available at arXiv:quant-ph/0607211, 2006. (With Alexandra Kolla, Gatis Midrijanis and Ben Reichardt.)

   Abstract: *Zero knowledge* protocols are known to be very powerful. Assuming the existence of *one-way* functions there exists zero-knowledge protocols for all of IP. However contrastingly, Goldreich and Krawczyk [OK90] showed that if a language L has a constant round zero-knowledge *Arthur-Merlin* (AM) protocol with negligible soundness error and a black box simulator, then L is in BPP.

   We consider the same question in the quantum setting. Quantum simulators are known to be very powerful [Wat06] and it is known that all languages in quantum zero-knowledge have a 3-round QAM protocol [Wat02]. Let L be a language decided by a constant-round QAM protocol with negligible soundness error and all but possibly the last message being classical. We prove that if this protocol is zero knowledge with a black-box quantum simulator, then L is in BQP. Our result also applies to any language having a three-round classical interactive proof with negligible soundness error and a black-box quantum simulator. These results in particular disallow parallel composition of certain protocols in order to reduce soundness error while maintaining zero knowledge with a black-box quantum simulator, unless $\mathsf{BQP} = \mathsf{NP}$.

   Our proof goes via a reduction to quantum black-box search. We show that the existence of a black-box simulator when $L \notin \mathsf{BQP}$ would imply an impossibly-good quantum search algorithm.

7. " Accessible versus Holevo information for a binary random variable." Submitted, 2006, available at arXiv:quant-ph/0603278. (With Ashwin Nayak.)

   Abstract: The *accessible information* $I_{\mathrm{acc}}(\mathcal{E})$ of an ensemble $\mathcal{E}$ is the maximum mutual information between a random variable encoded into quantum states, and the probabilistic outcome of a quantum measurement of the encoding. Accessible information is extremely difficult to characterize analytically; even bounds on it are hard to place. The celebrated *Holevo bound* states that accessible information cannot exceed $\chi(\mathcal{E})$, the quantum mutual information between the random variable

and its encoding. However, for general ensembles, the gap between the $I_{\rm acc}(\mathcal{E})$ and $\chi(\mathcal{E})$ may be arbitrarily large.

We consider the special case of a binary random variable, which often serves as a stepping stone towards other results in information theory and communication complexity. We show that for a binary ensemble $\mathcal{E} \triangleq \{(p, \rho_0), (1-p, \rho_1)\}$, $I_{\rm acc}(\mathcal{E}) \geq \max\{H(p) - \sqrt{4p(1-p) - \chi(\mathcal{E})^2}, \frac{\chi(\mathcal{E})^2}{4 \ln 2}\}$. This is the first explicit lower bound for $I_{\rm acc}(\mathcal{E})$ in a binary ensemble $\mathcal{E}$, in terms of $\chi(\mathcal{E})$. In previous works due Jozsa, Robb and Wootters [JRW94], Fuchs and Caves [FC94] and Hall [Hal97] on the same question, the lower bounds on $I_{\rm acc}(\mathcal{E})$ were either not explicit or not in terms of $\chi(\mathcal{E})$.

8. " An approach from classical information theory to lower bounds for smooth codes." Submitted, 2006, available at arXiv:cs/0607042.

   Abstract: Let $\mathcal{C} : \{0,1\}^n \mapsto \{0,1\}^m$ be a code encoding an n-bit string into an m-bit string. Such a code is called a (q, c, ϵ) *smooth code* if there exists a probabilistic decoding algorithm which while decoding any bit of the input, makes at most q probes on the code word, the probability with which it looks at any location is at most c/m and the error made by the decoding algorithm is at most ϵ. Smooth codes were introduced by Katz and Trevisan [KT00] in connection with *locally decodable codes*. For 2-probe smooth codes Kerenidis and de Wolf [KdW03] have shown that $m \geq 2^{\Omega(n)}$ in case c and ϵ are constants. Although the final result is about classical codes, their proof goes through *quantum* information theoretic arguments. These arguments do not seem to extend to codes with higher number of probes.

   Using very different classical information theoretic arguments, we show that for 2-probe codes if $\epsilon \leq \frac{c^2}{8n^2}$, then $m \geq 2^{\frac{n}{320c^2}-1}$. While our bounds fall short of the bounds shown by Kerenidis and de Wolf, we hope that the techniques used in this paper extend to match the bounds shown using quantum arguments. More so, we hope that they extend to show bounds for codes with greater number of probes for which the quantum arguments of Kerenidis and de Wolf break down.

9. "Resource requirements of private quantum channels and consequence for oblivious remote state preparation." Submitted, 2006, available at quant-ph/0507075.

   Abstract: Shannon [Sha48, Sha49] in celebrated works had shown that n bits of shared key is necessary and sufficient to transmit n-bit classical information in an information-theoretically secure way. Ambainis, Mosca, Tapp and de Wolf in [AMTdW00] considered a more general setting, referred to as *Private quantum channels*, in which instead of classical information, quantum states are required to be transmitted and only one-way communication is allowed. They show that in this case $2n$ bits of shared key is necessary and sufficient to transmit an n-qubit state. We consider the most general setting in which we allow for all possible combinations i.e. we let the input to be transmitted, the message sent and the shared resources to be classical/quantum. We develop a general framework by which we are able to show simultaneously optimal bounds on communication/shared resources in all of these cases and this includes the results of Shannon and Ambainis *et al*.

   Our arguments also imply resource bounds for the problem of *Oblivious remote state preparation* (ORSP). In this problem Alice is required to transfer a quantum state, completely known to her, to Bob using classical communication and quantum entanglement. The protocol should be such that the honest Bob gets to know nothing more about the transfered state, other than a copy of it in a designated quantum register. We show that in an ORSP protocol for transferring an n-qubit state, the entropy of the communication must be $2n$ and the *entanglement measure* of the shared resource must be n. This generalizes on the result of Leung and Shor [LS03] who show a lower bound of $2n$ on the length of communication.

10. "Stronger impossibility results for quantum string commitment.", Journal of Cryptology (JoC), 2008, available at quant-ph/0506001.

    Abstract:

    String commitment schemes are similar to the well studied *bit commitment* schemes in cryptography with the difference that the committing party, say Alice is supposed to commit a long string

instead of a single bit, to another party say Bob. Similar to bit commitment schemes, such schemes are supposed to be *binding*, i.e Alice cannot change her choice after committing and *concealing* i.e. Bob cannot find Alice's committed string before Alice reveals it. Strong impossibility results are known for bit commitment schemes both in the classical and quantum settings, for example due to Mayer [May97] and Lo and Chau [LC97, LC98]. In fact for approximate quantum bit commitment schemes, trade-offs between the *degrees* of cheating of Alice and Bob, referred to as *binding-concealing* trade-offs are known as well for example due to Spekkens and Rudolph [SR02].

Recently, Buhrman, Christandl, Hayden, Lo and Wehner [BCH$^+$06] have shown similar binding-concealing trade-offs for quantum string commitment schemes (QSC), both in the scenario of single execution of the protocol and in the asymptotic regime of sufficiently large number of parallel executions of the protocol. We show stronger trade-off in the scenario of single execution of a QSC protocol which also immediately imply the trade-off shown by Buhrman *et al.* in the asymptotic regime of multiple parallel executions of a QSC protocol. We show our results by making a central use of the important information theoretic tool called the *substate theorem* due to Jain, Radhakrishnan and Sen [JRS02]. Our techniques are quite different from that of [BCH$^+$06] and may be of independent interest.

11. "Communication complexity of remote state preparation with entanglement.". Quantum Information and Computation (QIC), 2005.

    Abstract: In the problem of *Remote state preparation*, recently studied in several papers [Lo00, BHL$^+$05, BDS$^+$01], Alice who knows the complete description of a quantum state ρ, transfers it to Bob using classical communication and quantum entanglement. At the end of the protocol, Bob should be able to output a quantum state ρ' which has high fidelity with ρ. We study the communication complexity of this problem. Let Alice get the input states from the set $\{\rho_i : i \in [N]\}$. We consider a notion of *maximum possible information* $T(E) \stackrel{\Delta}{=} \max_\mu \chi(E_\mu)$ of the encoding $E : i \rightarrow \rho_i$, where μ is a distribution on $[N]$, E_μ is the ensemble $\{(\mu(i), \rho_i) : i \in [N]\}$ and χ represents the Holevo-χ information. Making critical use of the substate theorem [JRS02], we show that in the presence of entanglement, $T(E)$ tightly characterizes the communication complexity of this problem.

12. "Prior entanglement, message compression and privacy in quantum communication." In Proceedings of 20th IEEE Conference on Computational Complexity (CCC), 2005. (With Jaikumar Radhakrishnan and Pranab Sen.)

    Abstract: The *Direct sum* question in communication complexity asks whether to compute k independent instances of a task takes the same communication as k times the communication required to solve a single instance of the same task? It is a very fundamental question and is open for most models of communication.

    In this paper we settle this question for one-way and *Simultaneous message passing* (SMP) models for both quantum and classical protocols. For any relation f, we show $Q_\epsilon^{1,pub}(f^k) = k\Omega(Q_\epsilon^{1,pub}(f))$, where $Q_\epsilon^{1,pub}(f)$ represents the one-way quantum communication complexity of computing f in the presence of entanglement with error at most ϵ and f^k represents k-copies of f. For classical protocols we similarly show, $R_\epsilon^{1,pub}(f^k) = \Omega(kR_\epsilon^{1,pub}(f))$, where $R^{1,pub}(f)$ represents randomized public coins one-way classical communication complexity of f. We show similar direct sum results for quantum and classical SMP protocols. We also obtain *weak direct sum* results for two-way quantum and classical randomized protocols relating two-way communication complexity of k-copies of f to one-way communication complexity of f.

    We obtain our direct sum results via various message compression results in different settings by making a critical use of the important information theoretic tool called the substate theorem by Jain *et al.* [JRS02]. We present some applications of our results to show space-time trade-offs for some problems like the *Approximate Nearest Neighbor* in the *quantum data structure* model.

    Another question which is widely open for quantum communication protocols is bounding the amount of entanglement used by them. For classical protocols this question was well settled long

ago by Newman [New91] who showed that the amount of shared randomness can always be reduced to $O(\log n)$ in a *black-box* fashion, i.e. without changing the operations of communicating parties. We show that however for quantum protocols, entanglement **cannot** be reduced in this black-box fashion indicating that quantum entanglement is a much more complicated resource than classical randomness.

13. "A lower bound for bounded round quantum communication complexity of set disjointness." In Proceedings of 43rd IEEE Symposium on Foundations of Computer Science (FOCS), pages 220–229, 2003. (With Jaikumar Radhakrishnan and Pranab Sen.)

    Abstract: *Set disjointness* is a very well studied problem both in the classical and quantum communication complexity because of its connections to *circuit complexity* and *non-deterministic* communication complexity. In this paper we show lower bounds for multi-party bounded round quantum communication complexity of set disjointness like functions. For two-party k-round quantum communication complexity of the set disjointness problem, this implies a lower bound of $\Omega(n/k^2)$. For $k = 1$, our lower bound matches the $\Omega(n)$ lower bound observed by Buhrman and de Wolf [BdW01], and for $2 \leq k \ll n^{1/4}$, improves the celebrated lower bound of $\Omega(\sqrt{n})$ shown by Razborov [Raz02].

14. "A direct sum theorem in communication complexity via message compression." In Proceedings of 30th International Colloquium on Automata, Languages and Programming (ICALP), pages 300–315, 2003. Invited to a special issue of Theoretical Computer Science (TCS) on ICALP 2003. (With Jaikumar Radhakrishnan and Pranab Sen.)

    Abstract: In this paper we consider the *direct sum* question in two-party bounded error randomized multiple-round communication protocols. For any relation $f \subseteq \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ and a product distribution μ on $\mathcal{X} \times \mathcal{Y}$, we show the following:

    $$D_{\epsilon}^{\mu^t,k}(f^t) \geq t(\frac{\delta^2}{2k} D_{\epsilon+2\delta}^{\mu,k}(f) - 2)$$

    Here, $D_{\epsilon}^{\mu,k}(f)$ represents the distributional complexity of computing f with k-round protocols with error at most ϵ under μ, f^t represents t independent copies of f and μ^t represents t independent copies of μ.

    Our main technical result is a *compression* theorem saying that, for any *product* probability distribution μ over the inputs, a k-round private coin bounded error protocol for a relation f with *information cost* c can be converted into a k-round deterministic protocol for f with bounded distributional error and communication cost $O(kc)$. Here by distributional error we mean expected error, expectation being taken over the inputs (which are chosen according to the distribution μ.) This can be thought of as analogous to the message compression theorem of Shannon in the context of communication complexity. We prove this result using the *substate theorem* of Jain *et al.* [JRS02] about relative entropy and a *rejection sampling* argument. Our direct sum result follows from this compression result via other information theoretic arguments. This result extends and generalizes a result of Chakrabarti, Shi, Wirth and Yao [CSWY01] who showed a similar direct sum result for one round and simultaneous message protocols for distributional complexity of boolean functions, under the *uniform* distribution on the inputs.

    We also consider the message compression question in quantum communication. Using a probabilistic argument, we show that quantum messages **cannot** be compressed in this manner even if they carry small information, highlighting the fact that quantum communication is a fundamentally different resource.

15. "The quantum communication complexity of the pointer chasing problem: the bit version." In Proceedings of 22nd conference on the Foundations of Software Technology and Theoretical Computer Science (FSTTCS), pp. 218–229, 2002. (With Jaikumar Radhakrishnan and Pranab Sen.)

    Abstract: In this paper we consider the two-party quantum communication complexity of the bit version of the *pointer chasing problem*. The pointer chasing problem is a very well studied problem in communication complexity for understanding rounds v/s communication trade-offs. We show

that in any quantum protocol for this problem, the two players must exchange $\Omega(\frac{n}{k^2})$ qubits when the wrong player starts. This improves the previous best bound of $\Omega(\frac{n}{2^{2^{O(k)}}})$ in Klauck, Nayak, Ta-Shma and Zuckerman [KNTZ01] and comes significantly close to the best known upper bound $O(k \log n + \frac{n}{k}(\log^{\lceil k/2 \rceil}(n) + \log k))$ [KNTZ01]. Our proof uses a *round elimination* argument with correlated input generation making better use of the information theoretic tools than the previous works.

16. "Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states." In Proceedings of 43rd IEEE Symposium on Foundations of Computer Science (FOCS), pp. 429–438, 2002. Journal version in Journal of the ACM (JACM). To appear. Also available at arXiv:0705.2437. (With Jaikumar Radhakrishnan and Pranab Sen.)

    Abstract: In this paper, we prove the following theorem about relative entropy of quantum states.

    > *Substate theorem:* Let ρ and σ be quantum states in the same Hilbert space with relative entropy $S(\rho\|\sigma) \stackrel{\Delta}{=} \text{Tr}\, \rho(\log \rho - \log \sigma) = c$. Then for all $\epsilon > 0$, there is a state ρ' such that the trace distance $\|\rho' - \rho\|_{\text{tr}} \stackrel{\Delta}{=} \text{Tr}\, \sqrt{(\rho' - \rho)^2} \leq \epsilon$, and $\rho'/2^{O(c/\epsilon^2)} \leq \sigma$.

    It states that if the relative entropy of ρ and σ is c, then there is a state ρ' close to ρ, i.e. with small trace distance $\|\rho' - \rho\|_{\text{tr}}$, that when scaled down by a factor $2^{O(c)}$ 'sits inside', or becomes a 'substate' of, σ. This result has several applications in quantum communication complexity and cryptography. Using the substate theorem, we derive a privacy trade-off for the *set membership problem* in the two-party quantum communication model. Here Alice is given a subset $A \subseteq [n]$, Bob an input $i \in [n]$, and they need to determine if $i \in A$.

    > *Privacy trade-off for set membership:* In any two-party quantum communication protocol for the set membership problem, if Bob reveals only k bits of information about his input, then Alice must reveal at least $n/2^{O(k)}$ bits of information about her input.

    This result also implies same trade-off for the quantum communication between Alice and Bob and generalizes on the result of Nayak [Nay99] who studied the one-way quantum communication complexity of the same problem when there is no communication from Bob.

    We also use it to give optimal lower bounds for the k-round bounded error quantum communication complexity of the *pointer chasing* problem, when the wrong player starts, and all the $\log n$ bits of the kth pointer are desired. The pointer chasing problem is a very well studied problem both in the classical and quantum communication settings for studying rounds v/s communication trade-offs in communication complexity.

17. "Better lower bounds for locally decodable codes." In Proceedings of 17th IEEE Conference on Computational Complexity (CCC), 2002. Journal version in Random Structures and Algorithms, 2004. (With Amit Deshpande, Satyanarayana V. Lokam, Jaikumar Radhakrishnan, Kavitha Telikapalli.)

    Abstract: An error-correcting code is said to be *locally decodable* if a randomized algorithm can recover any single bit of a message by reading only a small number of symbols of a possibly corrupted encoding of the message. Katz and Trevisan [KT00] showed that any such code $C : \{0,1\} \to \Sigma^m$ with a decoding algorithm that makes at most q probes must satisfy $m = \Omega((n/\log|\Sigma|)^{q/(q-1)})$. They assumed that the decoding algorithm is non-adaptive, that is the location to which a probe is made does not depend on the result of the earlier probes and leave the same question in the adaptive setting open. We settle it and show that in fact the same lower bound holds even if the decoding algorithm is adaptive.

Manuscripts:

1. "Distinguishing sets of quantum states." 2005. Available at arXiv:quant-ph/0506205.

    Abstract: Given two sets of quantum states we give necessary and sufficient conditions for distinguishing them well using a quantum measurement. We show that they can be distinguished with

probability ϵ using a quantum measurement if and only if their *convex hulls* are separated in trace distance by 2ϵ. The same fact is also independently shown by Gutoski and Watrous in [GW05] who use it crucially in an application concerning *quantum interactive proofs with competing provers*.

References

[AMTdW00] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[BCH+06] H. Buhrman, M. Christandl, P. Hayden, H.K. Lo, and Wehner S. On the (im)possibility of quantum string commitment. In *Phys. Rev. Lett.*, volume 97(250501), 2006.

[BDS+01] C.H. Bennett, D.P. DiVincenzo, P.W. Shor, J.A. Smolin, B.M. Terkal, and W.K. Wootters. Remote state preparation. In *Phys. Rev. Letters*, volume 87, 2001.

[BdW01] H. Buhrman and R. de Wolf. Communication complexity lower bounds by polynomials. In *Proceedings of the 16th IEEE Conference on Computational Complexity*, pages 120–130, 2001.

[BHL+05] C.H. Bennett, P. Hayden, W. Leung, P.W. Shor, and A. Winter. Remote preparation of quantum states. In *IEEE Transaction on Information theory*, volume 51, pages 56–74, 2005.

[BPSW07] Paul Beame, Toniann Pitassi, Nathan Segerlind, and Avi Wigderson. A direct sum theorem for corruption and a lower bound for the multiparty communication complexity of set disjointness. *Computational Complexity*, 2007. To appear.

[BSST02] C.H. Bennett, P.W. Shor, J.A. Smolin, and A.V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem. In *IEEE Transactions on Information Theory*, volume 48(10), pages 2637–2655, 2002.

[CHyTW04] R. Cleve, P. Hø yer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Conference on Computational Complexity*, pages 236–249, 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 33rd Annual ACM Symposium on Theory of Computing*, 2001.

[dW05] Ronald de Wolf. Random access codes, direct product theorems, and multiparty communication complexity. Private communication, 2005.

[FC94] Christopher A. Fuchs and Carlton M. Caves. Ensemble-dependent bounds for accessible information in quantum mechanics. *Phys. Rev. Lett.*, 73(23):3047–3050, December 1994.

[Gav06] Dmitry Gavinsky. On the role of shared entanglement. Technical report, arXive:quant-ph/0604052, 2006.

[GW05] G. Gutoski and J. Watrous. Quantum interactive proofs with competing provers. In *Proceedings of the 22nd Annual Symposium on Theoretical Aspects of Computer Science*, 2005.

[Hal97] Michael J.W. Hall. Quantum information and correlation bounds. *Phys. Rev. A*, 55(1):100–113, 1997.

[Jai06] R. Jain. Stronger impossibility results for quantum string commitment. Technical report, arXiv:quant-ph/0506001, 2006.

[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 International Conference on Automata, Languages and Programming*, pages 300–315, 2003. Invited to a special issue of Theoretical Computer Science (TCS) on ICALP 2003.

[JRW94] Richard Jozsa, Daniel Robb, and William K. Wootters. Lower bound for accessible information in quantum mechanics. *Phys. Rev. A*, 49(2):668–677, February 1994.

[KdW03] I. Kerenedis and R. de Wolf. Exponential lower bound for 2-query locally decodable codes via quantum argument. In *Proceedings of the 35th ACM Symposium on Theory of Computing*, pages 106–115, 2003.

[KNR95] I. Kremer, N. Nisan, and D. Ron. On randomized one-round communication complexity. In *Proceedings of The 27th ACM Symposium on Theory of Computing (STOC)*, pages 596–605, 1995.

[KNTZ01] H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman. Interaction in quantum communication and the complexity of set disjointness. In *Proceedings of the 33rd Annual ACM Symposium on Theory of Computing*, pages 124–133, 2001.

[KT00] J. Katz and L. Trevisan. On the efficiency of local decoding procedures for error correcting codes. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing*, pages 80–86, 2000.

[KvdW04] Hartmut Klauck, Robert Špalek, and Ronald de Wolf. Quantum and classical strong direct product theorems and optimal time-space tradeoffs. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 12–21, 2004.

[LC97] H.-K. Lo and H.F. Chau. Is quantum bit commitment really possible? In *Phys. Rev. Lett.*, volume 78, pages 3410–3413, 1997.

[LC98] H.-K. Lo and H.F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. In *Physica D*, volume 120, pages 177–187, 1998.

[Lo00] H.-K. Lo. Classical communication cost in distributed quantum information processing - a generalization of quantum communication complexity. In *Phys. Rev. A*, volume 62, 2000.

[LS03] D.W. Leung and P.W. Shor. Oblivious remote state preparation. In *Phys. Rev. Lett.*, volume 90(127905), 2003.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. In *Phys. Rev. Letters*, volume 78, pages 3414–3417, 1997.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40rd Annual IEEE Symposium on Foundations of Computer Science*, pages 369–376, 1999.

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

[OK90] Goldreich O. and H. Krawczyk. On the composition of zero-knowledge proof systems. In *Proceedings of the 17th International Colloquium on Automata Languages and Programming (ICALP)*, 1990.

[Raz02] A. A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya Math*, 6, 2002. In Russian. To appear. English version at quant-ph/0204025.

[Sha48] C.E. Shannon. A mathematical theory of communication. In *Bell systems technical journal*, volume 27, pages 623–656, 1948.

[Sha49] C.E. Shannon. Communication theory of secrecy systems. In *Bell systems technical journal*, volume 28, pages 656–715, 1949.

[SR02] R. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. In *Phys. Rev. A*, volume 65 (012310), 2002.

[Wat02] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, pages 459–468, 2002.

[Wat06] J. Watrous. Zero-knowledge against quantum attacks. In *Proc. 38th ACM Symposium on Theory of Computing*, 2006.

[Win02] A. Winter. Compression of sources of probability distributions and density operators. Technical report, arXiv:quant-ph/0208131, 2002.