Two Results about Quantum Messages[*]

Hartmut Klauck[1] and Supartha Podder[2]

[1] Centre for Quantum Technologies and Nanyang Technological University
hklauck@gmail.com

[2] Centre for Quantum Technologies and National University of Singapore
supartha@gmail.com

The comparison of communication protocols using quantum messages with protocols using classical messages is a central topic in information and communication theory. It is always good to understand such questions well in the simplest settings where they arise. An example is the setting of one-way communication complexity, which is rich enough to lead to many interesting questions, yet accessible enough for us to prove results about questions like the relationship between different computational modes, e.g. quantum versus classical or nondeterministic versus deterministic.

1 One-way Communication Complexity

Perhaps the simplest question one can ask about the power of quantum messages is the relationship between quantum and classical one-way protocols. Alice sends a message to Bob in order to compute the value of a function $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$. Essentially, Alice communicates a quantum state and Bob performs a measurement, both depending on their respective inputs. Though deceptively simple, this scenario is not at all fully understood. Let us just mention the following open problem: what is the largest complexity gap between quantum and classical protocols of this kind for computing a total Boolean function? The largest gap known is a factor of 2, as shown by Winter [11], but for all we know there could be examples where the gap is exponential, as it indeed is for certain partial functions (i.e., functions that are only defined on a subset of $\{0,1\}^n \times \{0,1\}^m$) [5].

An interesting bound on such speedups can be found by investigating the effect of replacing quantum by classical messages. Suppose a total Boolean function f has a quantum one-way protocol with communication c, namely Alice sends c qubits to Bob, who can decide f with error $1/3$ by measuring Alice's message. We allow Alice and Bob to share an arbitrary input-independent entangled state. Extending Nayak's random access code bound [8] Klauck [7] showed that $Q^{A\to B,*}(f) \geq \Omega(VC(f))$, where $Q^{A\to B,*}(f)$ denotes the entanglement-assisted quantum one-way complexity of f, and $VC(f)$ the Vapnik-Chervonenkis dimension of the communication matrix of f. Together with Sauer's Lemma [9] this implies that $D^{A\to B}(f) \leq O(Q^{A\to B,*}(f) \cdot m)$, where m is the length of Bob's input.

[*] This paper has been published in MFCS 2014. Full version under arXiv:1402.4312.

A result such as the above is much more interesting in the case of partial functions. Aaronson [1] showed a weaker result for partial functions in the following way: Bob tries to learn Alice's message. He starts with a guess (the totally mixed state) and keeps a classical description of his guess. Alice also always knows what Bob's guess is. Bob can simulate quantum measurements by brute-force calculation: for any measurement operator Bob can simply calculate the result from his classical description. Alice can do the same. Since Bob has some 2^m measurements he is possibly interested in, Alice can just tell him on which of these he will be wrong. Bob can then adjust his quantum state accordingly, and Aaronson's main argument is that he does not have to do this too often before he reaches an approximation of the message state. Note that Bob might never learn the message state if it so happens that all measurements are approximately correct on his guess. But if he makes a certain number of adjustments he will learn the message state and no further adjustments are needed.

Let us state Aaronson's result from [1].

Fact 1. *$D^{A\to B}(f) \leq O(Q^{A\to B}(f) \cdot \log(Q^{A\to B}(f)) \cdot m)$ for all partial Boolean $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$.*

Aaronson [2] later also proved the following result, that removes the log-factor at the expense of having the randomized complexity on the left hand side.

Fact 2. *$R^{A\to B}(f) \leq O(Q^{A\to B}(f) \cdot m)$ for all partial Boolean $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$.*

Our first result is the following improvement of the above statements.

Result 1. *$D^{A\to B}(f) \leq O(Q^{A\to B,*}(f) \cdot m)$ for all partial Boolean $f : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$.*

Hence we remove the log-factor, and we allow the quantum communication complexity on the right hand side to feature prior entanglement between Alice and Bob. Arguably, looking into the entanglement-assisted case (which is interesting for our second main result) led us to consider a more systematic progress measure than in Aaronson's proof, namely the relative entropy between the current guess and the target state. Using this measure in turn allowed us to analyze a different update rule for Bob's guess states that also works for protocols with error 1/3, instead of the extremely small error used in [1], which is the cause of the lost log-factor. While an improvement by a mere logarithmic factor might seem unimportant, we note that having tight bounds for such basic questions is generally desirable, e.g., Nayak's bound for random access codes [8] is an improvement by a logarithmic factor over previous work.

2 The Power of Quantum Proofs

We now turn to the second result of our paper, which is philosophically the more interesting. Interactive proof systems are a fundamental concept in computer science. Quantum proofs have a number of disadvantages: reading them may destroy them, errors may occur during verification, verification needs some sort of quantum machine, and it may be much harder to provide them than classical proofs. The main hope is that quantum proofs can in some situations be verified using fewer resources than classical proofs. Until now such a hope has not been verified formally. In the fully interactive setting Jain et al. have shown that the set of languages recognizable in polynomial time with the help of a quantum prover is equal to the set where the prover and verifier are classical (i.e., IP=QIP [6]).

The question remains open in the noninteractive setting. Aharonov and Naveh [4] first asked whether the proofs that are in quantum states can ever be easier to verify than classical proofs (by quantum machines) in the absence of interaction, i.e., whether the class QMA is larger than its analogue with classical proofs but quantum verifiers, known as QCMA. An indication that quantum proofs may be powerful was given by Watrous [10], who described an efficient QMA black-box algorithm for deciding nonmembership in a subgroup. However, Aaronson and Kuperberg [3] later showed how to solve the same problem efficiently using a classical witness, giving a QCMA black-box algorithm for the problem. They also introduced a quantum problem, for which they show that QMA black-box algorithms are more efficient than QCMA black-box algorithms. Using a quantum problem to show hardness for algorithms using classical proofs seems unfair though, and a similar separation has remained open for Boolean problems.

In our second main result we compare the two modes of noninteractive proofs and quantum verification for a Boolean function in the setting of one-way communication complexity. More precisely we exhibit a partial Boolean function f, such that the following holds. f can be computed in a protocol where a prover who knows x, y can provide a quantum proof to Alice, and Alice sends quantum message to Bob, such that the total message length (proof plus message Alice to Bob) is $O(\log n)$. In the setting where a prover Merlin (still knowing all inputs) sends a classical proof to Alice, who sends a quantum message to Bob, the total communication is $\Omega(\sqrt{n}/\log n)$.

Result 2. *There is a partial Boolean function f such that $QMA^{A\to B}(f) = O(\log n)$, while $QCMA^{A\to B,*}(f) = \Omega(\sqrt{n}/\log n)$.*

We note that this is the first known exponential gap between computing a Boolean function in a QCMA- and a QMA-mode in any model of computation.

For the lower bound we use that once a classical proof that applies to a large set of 1-inputs proof has been fixed, we are left with a quantum one-way protocol for a partial function that accepts those 1-inputs with high probability, yet rejects all 0-inputs with high probability. Our first result then lets us obtain a deterministic protocol for this partial function. The lower bound then follows from showing that *any* such partial function must have large deterministic one-way communication complexity.

References

1. S. Aaronson. Limitations of quantum advice and one-way communication. *Theory of Computing*, 1:1–28, 2005. Earlier version in Complexity'04. quant-ph/0402095.
2. S. Aaronson. The learnability of quantum states. *Proceedings of the Royal Society of London*, A463(2088), 2007. quant-ph/0608142.
3. S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3(1):129–157, 2007.
4. D. Aharonov and T. Naveh. Quantum NP - a survey. quant-ph/0210077, 2002.
5. D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2008.
6. R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. *J. ACM*, 58(6), 2011.
7. H. Klauck. On quantum and probabilistic communication: Las Vegas and one-way protocols. In *Proceedings of 32nd ACM STOC*, pages 644–651, 2000.
8. A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of 40th IEEE FOCS*, pages 369–376, 1999. quant-ph/9904093.
9. N. Sauer. On the density of families of sets. *J. Combin. Theory Ser. A*, 13:145–147, 1972.
10. J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings of 41st IEEE FOCS*, pages 537–546, 2000. quant-ph/0011023.
11. A. Winter. Quantum and classical message identification via quantum channels. In *Festschrift A.S. Holevo 60*, pages 171–188, 2004.