CS286.2 Around the Quantum PCP Conjecture

Challenge problem

I would like participants in the class to form small groups of $2-4$, involving at least one student with a CS background and one with a Physics background, and think hard about the following challenge problem (in bold below). This is a general research question to which there is no definite answer, and any partial answer, suggestion, reformulation, refutation, exploration, will be given credit. Below I suggest some possible references as starting point; a possible outcome for this project is to pick one of the papers, read it in detail, and write a short report outlining its connection to the QPCP conjecture and your thoughts on how it could be used towards proving (or disproving) the conjecture. The references are far from exhaustive however. For each of them you may find more by reading the introduction, looking at the listed references, and also using Google scholar to find more recent papers citing these works. Good luck!

Towards the quantum PCP conjecture

Proving the quantum PCP conjecture is likely to be challenging. But the classical PCP theorem was not proved in one go either. In particular, in class we saw a complete proof of a "baby" version of the theorem, $\mathrm{NP} \subseteq \mathrm{PCP}(\mathrm{poly}, O(1))$. For the case of (QPCP, LH), such a version is discussed in [AAV13]: there it is shown that any $L \in \mathrm{QMA}$ can be verified by making a constant number of queries to an *exponentially long* classical proof. For the case of (QPCP, games), a baby version follows from [IV12, Vid13], where it is shown that all languages in NEXP, and in particular QMA, have a 3-player quantum game in which messages from the referee to the players are of polynomial length, and messages from the players to the referee are a single bit each. None of these baby versions is particularly satisfying, however, as both heavily rely on classical techniques, end up with a "classical" object (classical proof, classical game), and in fact prove much more than containment of QMA (IP = PSPACE in the first case, NEXP in the second).

The challenge I would like to propose is to come up with your own "baby" version of either QPCP conjecture that we discussed in class.

Challenge: State and prove your own "baby" version of either version of QPCP.

A possibility to address this challenge is to improve upon any of the two results discussed above, or give your own proof of a result of a similar flavor. But you should interpret the challenge as broadly as you wish, and a "baby" version of QPCP does not need to be along the same lines as the classical $\mathrm{PCP} \subseteq \mathrm{PCP}(\mathrm{poly}, O(1))$. The versions above consider relaxing the requirement on the length of the proof, for the (QPCP, LH) variant, or the length of the messages from referee to players, for the (QPCP, games) variant. Different variants can be thought after that relax other parameters. For instance,

1. Show that (QPCP, LH) trivially holds if: (i) Each local Hamiltonian is allowed to act on n qubits, or (ii) The qubits, instead of being of dimension 2, can be of dimension 2^n, or (iii) the gap $b-a$ is only required to be a constant (independent of n and m).

2. Show that (QPCP, games) trivially holds if: (i) There are n players, or (ii) There is a constant number of players, but messages from the players are allowed to be n-qubits long.

The observations above are very basic (check carefully that they do hold!), but they provide some starting points. The challenge can then be reformulated as follows: give *any* asymptotic improvement on any of the seven "baby QPCPs" discussed above. For instance, regarding 1.(i) show that any instance of LH on n qubits with gap $b-a=\Omega(\mathrm{poly}^{-1}(n))$ can be mapped to an instance of LH on $\mathrm{poly}(n)$ qubits in which each local Hamiltonian acts on $O(\sqrt{n})$ qubits and has gap $b-a=\Omega(m)$, where m is the number of Hamiltonians in the new instance. Or, regarding 2.(ii), give a game for LH on n qubits that has constant completeness-soundness gap, a constant number of players, and in which the total amount of communication from the provers to the verifier is sublinear in n.

Here are some other possible starting points for questions to look at (this is highly non-exhaustive, and I encourage you to look elsewhere for inspiration!):

- The paper [ABD$^+$09] shows that 3SAT on n variables can be proven with two unentangled quantum states, each of length $O(\sqrt{n}\,\mathrm{poly}\log n)$ qubits. Can the ideas be extended to prove n-qubit instances of LH with less than n qubit-long messages (possibly adding interaction, i.e. the setting of a quantum game)?

- "Perturbative gadgets" allow one to modify an instance of LH and change its properties: for instance, map an instance of 3-LH to an instance of 2-LH (see [JF08, BDLT08] and references in/to these works for starting points). Can you use such gadgets in the "large locality" regime, to e.g reduce a constant-gap instance of LH with n-qubit Hamiltonians to one with $o(n)$-qubit Hamiltonians?

- Ran Raz has a suggestively named paper [Raz05] from 2005, in which he shows that languages in NEXP have a special form of interactive proof system that uses quantum information to be more efficient than could classical proof systems for NEXP of the same form (as far as we know). This paper has not received much attention, and was published before all the discussions on the quantum PCP conjecture. Can Raz's paper be revisited in light of the conjecture? Can you improve his construction to show that QMA, instead of NP, has a proof system of a similar type as a (scaled-down) variant of his construction?

- There are a fair number of QMA-complete problems known; see [Boo12] for a survey (see also [CS12] for some interesting variations on LH). Some of these problems may give inspiration for better starting points than the local Hamiltonian problem; for instance some of them may more naturally lend themselves to the construction of a multiplayer game than LH.

- The different variants of QPCP assert the QMA-hardness of a certain problem for which we already know that NP-hardness holds. A natural intermediate step would be to show QCMA-hardness for these problems. Since QCMA is based on classical proofs, the reductions (e.g. Dinur's gap amplification) may be much easier to carry through. A difficulty is that we do not have natural complete problems for QCMA. However, very recently a problem related to LH was shown to be QCMA-complete [GS14] and could be a good starting point: can you answer any of the challenge improvements suggested above, for the QCMA-complete problem described in [GS14], instead of the QMA-complete problem LH?

- In class we described two main variants of the quantum PCP conjecture: the CSP/LH variant and the games variant. (You can read more about the first variant in this survey [AAV13], and about the second

in a recent paper [FV14].) I claimed that there is no relationship known between the conjectures. Nevertheless we can make the following simple observation: Suppose (QPCP, LH variant) holds. Then there exists a n-player game for LH (where n is the number of qubits in the LH instance) in which the verifier only ever talks to a constant number of players, only receives a constant number of qubits from each player he talks to, and has a constant completeness/soundness gap. Hence (QPCP, LH) implies (QPCP, games)...but with n players.

1. Prove the above observation. Can you improve it by reducing the number of players (and possibly increasing the amount of interaction between the verifier and each of them)?
2. Can you find an analogue "naive" reduction in the other direction: what is the most non-trivial version of (QPCP, LH) that you could derive assuming that (QPCP, games) holds?

References

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. The quantum PCP conjecture. Technical report, arXiv:1309.7495, 2013. Appeared as guest column in ACM SIGACT News archive Volume 44 Issue 2, June 2013, Pages 47–79.

[ABD+09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009.

[BDLT08] Sergey Bravyi, David P. DiVincenzo, Daniel Loss, and Barbara M. Terhal. Quantum simulation of many-body hamiltonians using perturbation theory with bounded-strength interactions. *Phys. Rev. Lett.*, 101:070503, Aug 2008.

[Boo12] Adam Bookatz. Qma-complete problems. Technical report, arXiv:1212.6312, 2012.

[CS12] A. Chailloux and O. Sattath. The complexity of the separable hamiltonian problem. In *Proc. 27th IEEE Conf. on Computational Complexity (CCC'12)*, pages 32–41, June 2012.

[FV14] Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local Hamiltonian problem, 2014. To appear in the proceedings of the 6th Conference on Innovations in Theoretical Computer Science (ITCS'15).

[GS14] Sevag Gharibian and Jamie Sikora. Ground state connectivity of local hamiltonians. Technical report, arXiv:1409.3182, 2014.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. *Proc. 53rd FOCS*, pages 243–252, 2012.

[JF08] Stephen P. Jordan and Edward Farhi. Perturbative gadgets at arbitrary orders. *Phys. Rev. A*, 77:062329, Jun 2008.

[Raz05] Ran Raz. Quantum information and the pcp theorem. Technical report, arXiv:quant-ph/0504075, 2005.

[Vid13] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Proc. 54th FOCS*, 2013.