A multiprover interactive proof system for the local Hamiltonian problem

Joseph Fitzsimons* Thomas Vidick†

Abstract

We give a quantum interactive proof system for the local Hamiltonian problem on n qubits in which (i) the verifier has a single round of interaction with five entangled provers, (ii) the verifier sends a classical message on $O(\log n)$ bits to each prover, who replies with a constant number of qubits, and (iii) completeness and soundness are separated by an inverse polynomial in n. As the same class of proof systems, without entanglement between the provers, is included in QCMA, our result provides the first indication that quantum multiprover interactive proof systems with entangled provers may be strictly more powerful than unentangled-prover interactive proof systems. A distinguishing feature of our protocol is that the completeness property requires honest provers to share a large entangled state, obtained as the encoding of the ground state of the local Hamiltonian via an error-correcting code. Our result can be interpreted as a first step towards a multiprover variant of the quantum PCP conjecture.

The proof that the local Hamiltonian (LH) problem is QMA-complete [13] shows that any language that admits efficiently verifiable quantum proofs of membership also has proofs that are of a very special form: they are the lowest-energy state of a *local* Hamiltonian $H = \sum_i H_i$. What makes this statement particularly nontrivial is the locality of the Hamiltonian. Although the original proof may be a highly complex state displaying arbitrary entanglement that is difficult, if not impossible, to detect locally, its *existence* can be certified by the local Hamiltonian.

Kitaev's hardness result provides a particularly simple format into which any polynomial-time quantum verification procedure can be efficiently transformed: (i) receive a quantum state $|\Psi\rangle$; (ii) select a local term H_j uniformly at random and estimate the energy of $|\Psi\rangle$ with respect to H_j; (iii) repeat until a sufficiently accurate estimate for the total energy has been computed. Here (ii) is the key step that is simplified by Kitaev's result: instead of applying a generic quantum circuit, the verifier only needs to access, and measure, a constant number of qubits of $|\Psi\rangle$. Steps (i) and (iii) also deserve attention. Since Kitaev's QMA-hardness proof for LH requires an approximation of the energy accurate up to an additive factor inverse polynomial in the total number of qubits, the number of repetitions required in (iii) is also polynomial, making for a lengthy verification procedure. The famous quantum PCP conjecture claims that (iii) can be drastically improved: there should exist a more robust encoding for which obtaining constant-factor approximations remains QMA-hard, hence a constant number of repetitions would suffice. Although the conjecture has captured the imagination of many researchers [1, 6, 9] very little is known [2].

In this submission we investigate step (i) and ask the following question: can quantum proofs, and in particular ground states of local Hamiltonians, be encoded in a format that can be verified *without ever having to store the complete proof* — instead relying on untrustworthy quantum server(s) to provide the few qubits to be measured in step (ii)? The question is nontrivial as the servers, more traditionally called provers, have full control over the qubits they provide: instead of being contrived to send a complete proof to the verifier, who would only then selects the few qubits to be measured, we ask whether the order of interaction can be reversed: first the verifier should specify which qubits it wants to see, and then only the qubits are provided by the provers. Is there a way for the verification procedure to guarantee that different qubits, associated with distinct queries, can be "patched" into a global proof?

Before stating our results more formally, we note that the question can be formulated in terms of quantum interactive proof systems, and in fact follows very closely the line of work that led to the original proof of the PCP

* Singapore University of Technology and Design and Centre for Quantum Technologies, National University of Singapore, Singapore. Email: joe.fitzsimons@nus.edu.sg.

† California Institute of Technology, Pasadena, CA, USA. Email: vidick@cms.caltech.edu.

theorem [4, 3] from classical complexity theory. This line of work was stimulated by the progressive discovery that the possibility for *interaction* could substantially increase the power of polynomial-time verifiers: from the class MA, which characterizes purely static verification procedures, through the class IP $=$ PSPACE [16] associated with interactions with a single prover, to MIP $=$ NEXP [5] as soon as there are two or more non-communicating provers. It is this last equality which, once appropriately scaled down, led to the first formulations of the PCP theorem in terms of hardness of approximation [7] that the quantum PCP conjecture aims to port to the quantum setting. Our results can be interpreted as an attempt to devise a new route towards the quantum PCP conjecture that mimics an approach that has been successful in the classical setting.[1]

Results

Our main result is the design of an interactive proof system for the local Hamiltonian problem. Formally,

Theorem 1. *Let k be an integer. There exists constants $C, c > 0$ depending on k only such that the following holds. Let $H = \sum_{i=1}^{m} H_i$ be an instance of the k-local Hamiltonian problem on n qubits, such that the number of constraints is $m = \mathrm{poly}(n)$. There exists a one-round interactive protocol between a quantum polynomial-time verifier and $r = 5$ entangled quantum provers such that:*

- *The verifier sends $O(\log n)$-bit classical messages to each prover,*
- *The provers respond with at most k qubits each,*
- *If there exists a state $|\Gamma\rangle$ such that $\langle\Gamma|H|\Gamma\rangle \leq am$ then there is a strategy for the provers that is accepted with probability at least $1 - a/2$,*
- *If for every state $|\Psi\rangle$, $\langle\Psi|H|\Psi\rangle \geq bm$ then any strategy is accepted with probability at most $1 - Cb/n^c$.*

In terms of interactive proofs, our result can be scaled up to obtain the first formal separation between quantum multiprover interactive proof systems with and without entanglement between the provers. Let $\mathrm{QMIP}^*(r,t,c,s)$ be the class of languages that have quantum interactive-proof systems with r provers, t rounds of interaction, completeness c and soundness s, and $\mathrm{QMA}_{\mathrm{EXP}}$ the exponential-witness size version of QMA (see the full version [8] for formal definitions). The scaled-up version of the local Hamiltonian problem, over exponentially many qubits, is $\mathrm{QMA}_{\mathrm{EXP}}$-complete for $k = 2$, a that is exponentially small (in the input length) and b at least an inverse polynomial [11]. Thus as an immediate consequence of Theorem 1 we obtain the following:

Corollary 2. *There exists a polynomial q such that* $\mathrm{QMA}_{\mathrm{EXP}} \subseteq \mathrm{QMIP}^*(5,1,1-2^{-(q+1)},1-2^{-q})$*, and hence* $\mathrm{QMIP}(5,1,1-2^{-(q+1)},1-2^{-q}) \subsetneq \mathrm{QMIP}^*(5,1,1-2^{-(q+1)},1-2^{-q})$ *unless* $\mathrm{NEXP} = \mathrm{QMA}_{\mathrm{EXP}}$.

Corollary 2 provides the first indication that entanglement *increases* the complexity of entangled (quantum) games compared to their non-entangled counterparts, at least in the range of inverse-exponential approximations.[2] The corollary follows from the fact that $\mathrm{QMIP}(5,1,1-2^{-(q+1)},1-2^{-q}) \subseteq \mathrm{NEXP}$ [14] and $\mathrm{NEXP} \subseteq \mathrm{MIP}^*(3,1,1,1-1/\mathrm{poly})$ [10] together with the observation $\mathrm{MIP}^*(3,1,1,1-1/\mathrm{poly}) \subseteq \mathrm{QMIP}^*(5,1,1-2^{-(q+1)},1-2^{-q})$. The same corollary holds with QMIP replaced by the larger class $\mathrm{QMIP}^{(l.e.)}$ of languages having quantum multiprover interactive proof systems in which the provers share an entangled state on at most a polynomial number of qubits, which is also known to be included in NEXP [14]. Hence under the assumption that $\mathrm{NEXP} \neq \mathrm{QMA}_{\mathrm{EXP}}$ it also holds that, in our proof system, honest provers *need* an exponential number of qubits of entanglement in order to achieve a success probability equal to the completeness.

We note that even though it is known that $\mathrm{MIP}^* = \mathrm{QMIP}^*$ [15] the above corollary falls short of proving a separation between MIP $=$ NEXP and MIP^*. The reason is that the transformation from a QMIP^* to a MIP^* protocol in [15] requires the completeness and soundness parameters of the QMIP^* protocol to be separated by an inverse polynomial in the input size, whereas our construction only gives an inverse exponential separation.

[1] We stress that our results have no formal bearing on the quantum PCP conjecture itself, and we will not discuss their relationship further in this brief abstract; see the full version [8] for more details.

[2] Prior works had already demonstrated the "practical usefulness" of shared entanglement to simplify *existing* proof systems, showing that it could be used to reduce the number of rounds of interaction [12] or remove the need for quantum messages [15].

Proof idea

Consider first the following natural attempt at designing a protocol for the local Hamiltonian problem, that mimics the classical construction of a two-prover protocol for 3SAT. Without going into details, the idea is to ask the first prover for an assignment to all variables appearing in a randomly chosen clause and the second prover for an assignment to a single of the three variables. The provers' answers are cross-checked to ensure that the first provers' answers lead to a globally consistent assignment. In the quantum setting such "cross-checking" runs into an immediate obstacle: any given qubit of the proof can be placed in the hands of one prover only, but it cannot be duplicated! This first attempt does not have *completeness*: even satisfiable instances of LH may not imply a good strategy for the provers.

It is then natural to consider splitting the proof (e.g. the ground state of the LH instance) qubits into two (or more) sets S_1 and S_2, and only asking prover i for qubits coming from set S_i. While this leads to a game which does have perfect completeness, the fact that the sets need to be specified a priori can prevent the *soundness* property from holding. To see why, consider the simple example of a one-dimensional nearest-neighbor Hamiltonian in which each term is a projection on the orthogonal complement of an EPR pair split across two adjacent qubits. This Hamiltonian is highly frustrated, but the provers can succeed in the corresponding protocol, in which S_1 (resp. S_2) is the set of all even-numbered (resp. odd-numbered) qubits, with probability 1 by systematically sending back their respective half of a single EPR pair, independently of the verifier's question!

We suggest a diferent protocol to overcome these difficulties. Our main goal is to ensure that, when a prover is asked for its share of a certain qubit i, or j, of the proof, the actual qubits that it sends back to the verifier do indeed correspond to distinct physical qubits — that they do not "overlap", or even correspond to the same physical qubit (as was the case in the above example). To enforce this, instead of asking the (honest) provers to directly split the qubits of the original proof we ask them to share an *encoding* of the proof: each "logical" qubit of $|\Psi\rangle$ should be individually encoded into five "physical" qubits using a quantum error-correcting code. Each of five provers should then be given one of the five shares associated with each of the original proof's qubits.

Given this (presumed) splitting of the proof, the verifier performs each of the following two tests with probability $1/2$. In the first test he asks each of the five provers for its corresponding share of each qubit on which a randomly chosen H_j acts and estimates the energy of the (decoded) qubits with respect to H_j. In the second test the verifier again chooses a term H_j uniformly at random; let $S_j = \{i_1, \dots, i_k\}$ be the qubits on which it acts. He selects an index $\ell \in \{1, \dots, k\}$ at random and asks four out of the five provers (again chosen at random) for their respective share of qubit i_ℓ only. To the last prover he asks for its respective shares of all qubits in S_j (so the last prover cannot distinguish whether it is this test or the first that is being performed). The verifier checks that all shares that he received associated with qubit i_ℓ lie in the codespace, and rejects the provers if not.

In this second test the messages sent back by the first four provers only depend on qubit i_ℓ. The key point is that, informally, given their four respective answer qubits there can exist at most one additional qubit that is entangled with them in a way that completes a valid codeword. Indeed (and again informally), if there were two such qubits it would imply that it is possible for the "environment" to entangle itself with a codeword through acting on a single qubit and without being detected by the code — this possibility is excluded as long as the code is required to correct (or even just detect) all single-qubit errors. Thus this additional test enforces that the qubit sent back by the fifth prover in response to query i_ℓ is uniquely specified by the query i_ℓ; this is acheived by "locking" the qubit with the other four provers' answers via the codespace.

Although the above provides some intuition, proving soundness of the protocol remains technically challenging. We need to show how, from prover strategies that are successful in the protocol, can be extracted (at least in principle) a complete proof $|\Psi\rangle$ serving as a witness for the minimum energy of the Hamiltonian H. Formally each prover's strategy is specified by a pair of unitaries, one for each type of query from the verifier. The difficulty in proving that these unitaries are "compatible" and can be composed so as to reconstruct $|\Psi\rangle$ from the provers' entangled registers — indeed, note a prover may apply an arbitrary transformation to its private space before answering any of the verifier's queries. Our proof specifies an explicit circuit, based on the provers' unitaries, for reconstructing $|\Psi\rangle$ from their initial entangled state. The depth of this circuit is linear in the number of qubits, and it is ultimately this which leads to the polynomial dependence of the soundness parameter on the number of qubits in the proof.

References

[1] S. Aaronson. The quantum PCP manifesto, 2006. Blog entry available at http://www.scottaaronson.com/blog/?p=139.

[2] D. Aharonov, I. Arad, and T. 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.

[3] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[4] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[5] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Comput. Complexity*, 1:3–40, 1991.

[6] F. G. Brandao and A. W. Harrow. Product-state approximations to quantum ground states. In *Proc. 45th STOC*, 2013.

[7] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Interactive proofs and the hardness of approximating cliques. *J. ACM*, 43(2):268–292, 1996.

[8] J. Fitzsimons and T. Vidick. A multiprover interactive proof system for the local Hamiltonian problem. Technical report, arXiv:1409.0260, 2014.

[9] M. H. Freedman and M. B. Hastings. Quantum systems on non-k-hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs. *arXiv preprint arXiv:1301.1363*, 2013.

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

[11] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, May 2006.

[12] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18:273–307, 2009.

[13] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[14] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[15] B. Reichardt, F. Unger, and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *Nature*, 496(7446):456–460, 2013.

[16] A. Shamir. IP = PSPACE. *J. ACM*, 39(4):869–877, 1992.