Hardness of approximation for quantum problems

Sevag Gharibian * Julia Kempe†

Abstract

The polynomial hierarchy plays a central role in classical complexity theory. Here, we define a quantum generalization of the polynomial hierarchy, and initiate its study. We show that not only are there natural complete problems for the second level of this quantum hierarchy, but that these problems are in fact strongly hard to approximate. Our results thus yield the first known hardness of approximation results for a quantum complexity class. Our approach is based on the use of dispersers, and is inspired by the classical results of Umans regarding hardness of approximation for the second level of the classical polynomial hierarchy [Umans, FOCS 1999].

Over the last decades, the Polynomial Hierarchy (PH) [MS72], a natural generalization of the class NP, has been the focus of much study in classical computational complexity. Of particular interest is the second level of PH, denoted Σ_2^p. Here, we say a problem is in Σ_2^p if it has an efficient verifier with the property that for any YES instance $x \in \{0,1\}^*$ of the problem, *there exists* a polynomial length proof y such that *for all* polynomial length proofs z, the verifier accepts x, y and z. Note the *alternation* from an existential quantifier over y to a for-all quantifier over z is crucial here — keeping only the existential quantifier reduces us to NP.

It turns out that the use of such alternating quantifiers makes Σ_2^p a powerful class which is believed to be *beyond* NP. For example, many natural and important problems are known to be in Σ_2^p but not in NP. Such problems range from "does the optimal assignment to a 3SAT instance satisfy *exactly k* clauses?" to extremely practically relevant problems related to circuit minimization, such as "given a boolean formula C in Disjunctive Normal Form (DNF), what is the smallest DNF formula C' equivalent to C?". Further, the study of Σ_2^p has led to a host of other fundamental theoretical results, such as the Karp-Lipton theorem, which states that NP $\not\subseteq$ $\mathrm{P}_{/\mathrm{poly}}$ unless PH collapses to Σ_2^p. Σ_2^p has even been used, for example, to prove that SAT cannot be solved simultaneously in linear time and logarithmic space [For00, FLvMV05]. For these reasons, Σ_2^p and more generally PH have occupied a central role in classical complexity theoretic research.

Moving to the quantum setting, the study of quantum proof systems and a natural quantum generalization of NP, the class Quantum Merlin Arthur (QMA) [KSV02], has been a very active area of research over the last decade. Roughly, a problem is in QMA if for any YES instance of the problem, there exists a polynomial size *quantum* proof convincing a *quantum* verifier of this fact with high probability. With the notion of quantum proofs in mind, we thus ask the natural question: *Can a* quantum *generalization of* Σ_2^p *be defined, and what types of problems might it contain and characterize?* Perhaps surprisingly, to date there are almost no known results in this direction.

Our results: In this work, we introduce a quantum generalization of Σ_2^p, which we call cq-Σ_2^p, and initiate its study. In particular, we study cq-Σ_2^p-completeness and moreover cq-Σ_2^p-hardness of approximation for two new problems we define. In order to state our first main result, Theorem 5 (our second similar result for the problem QIRR will appear in a technical version of this abstract), we begin by introducing the requisite definitions. First, the class cq-Σ_2^p is informally defined as:

Definition 1 (cq-Σ_2^p (informal))**.** *A problem* Π *is in* cq-Σ_2^p *if it has an efficient quantum verifier satisfying the following property for any input* $x \in \{0,1\}^*$*:*

- *If* x *is a YES instance of* Π*, then there exists a polynomial length* classical *proof* y *such that for all polynomial length* quantum *proofs* $|z\rangle$*, the verifier accepts* x*,* y *and* $|z\rangle$ *with high probability.*

*David R. Cheriton School of Computer Science and Institute for Quantum Computing, University of Waterloo.
†CNRS & LIAFA, University Paris Diderot - Paris 7, and Blavatnik School of Computer Science, Tel Aviv University.

- *If x is a NO instance of Π, then for all polynomial length* classical *proofs y, there exists a polynomial length* quantum *proof $|z\rangle$ such that the verifier rejects x, y and $|z\rangle$ with high probability.*

We believe this is a natural quantum generalization of Σ_2^p. Here, the prefix *cq* in cq-Σ_2^p derives from the fact that the existential proof is classical, while the for-all proof is quantum. One can also consider variations of this scheme such as qq-Σ_2^p, qc-Σ_2^p, or cc-Σ_2^p (with a quantum verifier), defined analogously. In this paper, however, our focus is on cq-Σ_2^p, as it is the natural setting for the computational problems for which we wish to prove hardness of approximation. Note also that unlike for Σ_2^p, the definition of cq-Σ_2^p is bounded error — this is due to the use of a quantum verifier for cq-Σ_2^p. This implies, for instance, that the quantum analogue of the classically non-trivial result BPP $\subseteq \Sigma_2^p$ [Sip83, Lau83], i.e. BQP $\subseteq$ cq-Σ_2^p, holds trivially. Finally, one can extend the definition of cq-Σ_2^p to an entire hierarchy of quantum classes analogous to PH by adding further levels of alternating quantifiers, attaining presumably different classes depending on whether the quantifier at any particular level runs over classical or quantum proofs.

Let us next take a step back and recall two classical problems crucial to our work here. In the NP-complete problem SET COVER, one is given a set of subsets $\{S_i\}$ whose union covers some ground set U, and we are asked for the smallest number of the S_i whose union still covers U. If, however, the S_i are represented *succinctly* as the on-set[1] of a 3-DNF formula ϕ_i, we obtain a much more difficult problem known as SUCCINCT SET COVER (SSC). SSC, along with a related problem IRREDUNDANT (IRR), are not just NP-hard, but are in fact Σ_2^p-complete (indeed, they even Σ_2^p-hard to approximate [Uma99]). Specifically, SSC and IRR are defined as:

Definition 2 (SUCCINCT SET COVER (SSC) [Uma99])**.** *Given a set $S = \{\phi_i\}$ of 3-DNF formulae such that $\bigvee_{i \in S} \phi_i$ is a tautology, what is the smallest subset $S' \subseteq S$ that remains a tautology?*

Definition 3 (IRREDUNDANT (IRR) [Uma99])**.** *Given a DNF formula $\phi = t_1 \vee t_2 \vee \cdots \vee t_n$, what is the smallest subset $S \subseteq \{t_i\}_{i=1}^n$ such that $\phi = \bigvee_{i \in S} t_i$?*

Our work introduces and studies quantum generalizations of SSC and IRR. In particular, analogous to the classically important task of circuit minimization, the quantum generalizations we define are arguably natural and related to what one might call "Hamiltonian minimization" — given a sum of Hermitian operators $H = \sum_i H_i$, what is the smallest subset of terms $\{H_i\}$ whose sum approximately preserves certain spectral properties of H? Such questions may be useful to physicists in a lab who wish to simulate the simplest Hamiltonian possible while retaining the desired characteristics of a complex Hamiltonian involving many interactions. We remark that at a high level, the connection to cq-Σ_2^p for the task of Hamiltonian minimization is as follows: The classical existential proof encodes the subset of terms $\{H_i\}$, while the quantum for-all proof encodes complex unit vectors which achieve certain energies against H. We now define our quantum version of SSC.

Definition 4. QUANTUM SUCCINCT SET COVER *(QSSC) (informal) Given a set of local Hamiltonians $\{H_i\}$ acting on N qubits and whose sum has smallest eigenvalue at least α, what is the smallest subset of the H_i whose sum has smallest eigenvalue at least α? Any subset satisfying this property is called a* cover.

Here, a *local Hamiltonian* is a sum of Hermitian operators, where each operator acts non-trivially on a constant number of qubits k for some fixed k. Intuitively, the goal in QSSC is to cover the entire Hilbert space using as few interaction terms H_i as possible. Hence, we associate the notion of a "cover" with obtaining large eigenvalues, as opposed to small ones, making QSSC a direct quantum analogue of SSC. We remark that since SSC is a classical constraint satisfaction problem, we believe the language of *quantum* constraint satisfaction, i.e. Hamiltonian constraints, is a natural avenue for defining QSSC. Our first result concerns QSSC, and is as follows.

Theorem 5. *QSSC is* cq-Σ_2^p*-complete, and moreover is* cq-Σ_2^p*-hard to approximate within N^ϵ for some $\epsilon > 0$ and for N the encoding size of the QSSC instance.*

[1] By *on-set*, we mean the set of assignments which cause ϕ_i to be true.

By *hard to approximate*, we mean that any problem in cq-Σ_2^p can be reduced to an instance of QSSC via a polynomial time mapping or Karp reduction such that the gap between the sizes of the optimal cover in the YES and NO cases scales as N^ϵ. In other words, it is cq-Σ_2^p-hard to determine whether the smallest cover size of an arbitrary instance of QSSC is at most g or at least g' for $g'/g \in O(N^\epsilon)$ (where $g' \geq g$).

Our second result is a similar hardness of approximation result for a quantum version of IRR we call QIRR — the reader is referred to the technical draft for further details.

Proof ideas: To show the hardness of approximation result of Theorem 5, we first demonstrate a gap-introducing reduction from an arbitrary cq-Σ_2^p problem to a problem we call QUANTUM MONOTONE MINIMUM WEIGHT WORD (QMMWW) using *dispersers* (see e.g., [SZ94]). We then show a gap-preserving reduction from QMMWW to QSSC (and further from QSSC to QIRR for our second result). We remark that our proofs are inspired by the classical work of Umans [Uma99, Hem02], who used dispersers to attain hardness of approximation results for Σ_2^p for the classical problems MMWW (the classical version of QMMWW), SSC and IRR.

Of these reductions, the most difficult aspect of our work is the gap-preserving reduction from QMMWW to QSSC (as well as the further reduction from QSSC to QIRR). Here, due to the continuous spaces in which quantum states live, as well as the non-commutativity inherent in quantum mechanics, an intricate balancing act involving carefully defined local Hamiltonian terms is needed to adapt Umans' ideas to the quantum setting. In particular, the reduction requires a precise analysis of spectra of sums of non-commuting local Hamiltonians, for which we require heavier machinery, such as the specific structure of Kitaev's local Hamiltonian construction [KSV02] and the projection lemma of Kempe, Kitaev, and Regev [KKR06].

We hence now focus on outlining our gap-preserving reduction from QMMWW to QSSC. Roughly, the input to QMMWW is a quantum circuit V which has both classical and quantum input registers, and the question QMMWW asks is: What is the smallest Hamming weight classical input $x \in \{0,1\}^n$ "accepted" by V? To reduce this to an instance of QSSC, we first apply Kitaev's construction to obtain a local Hamiltonian H_V which achieves large energy on accepting assignments, and small energy on non-accepting or invalid assignments. To then "cover" the portion of the Hilbert space corresponding to the low energy space of H_V, we introduce two other types of local Hamiltonian terms: (1) There are n terms of the first type, one per classical input bit to V, whose job it is to cover specific classical assignments which are rejected by V. In particular, these terms are designed so that the number of them required to help form a cover is directly related to the smallest Hamming weight string accepted by V. (2) The second type of local Hamiltonian term is designed to cover the space of all invalid ancilla and clock states. Due to the non-commuting nature of the Hamiltonians involved, we must carefully analyze the spectrum of any proposed cover in order to rigorously complete the reduction — part of this requires the projection lemma of Reference [KKR06].

Previous and related work: To the best of our knowledge, our work is the first to obtain hardness of approximation results for a quantum complexity class. The related question of whether a *quantum* PCP theorem holds is currently one of the biggest open problems in quantum complexity theory (see, e.g., [AALV09, Aar06]). Regarding quantum variants of PH, the only previous work we are aware of is that of Yamakami [Yam02], whose results and definition are largely unrelated to ours (e.g., complete problems are not studied).

Significance of results: Our results are significant in three respects: First, the classical polynomial hierarchy plays an important role in classical complexity theory, both as a generalization of NP and as a proof tool in itself. It is hoped that the scheme we propose here for generalizing PH to the quantum setting will find similar applications in quantum complexity theory. Second, the problems we show to be cq-Σ_2^p-complete here are arguably natural, and in embodying a generalization of classical circuit minimization, may be related to real scenarios in a lab. Further, although the alternation between classical and quantum quantifiers in cq-Σ_2^p may a priori seem odd, the notion of relating a classical proof to, say, subsets of local Hamiltonian terms, and the quantum proof to quantum states achieving certain energies is in itself quite natural, and in our opinion justifies the study of such a combination of quantifiers. Third, our results are the first known hardness of approximation results for a quantum complexity class. Given that whether a quantum PCP theorem holds remains a challenging open question, it is all the more interesting that one is able to prove such hardness of approximation results in a quantum setting using an entirely different tool, namely that of dispersers.

References

[AALV09] D. Aharonov, I. Arad, Z. Landau, and U. Vazirani. The detectibility lemma and quantum gap amplification. In *Proc. 41st ACM Syposium on Theory of Computing (STOC 2009)*, volume 287, pages 417–426, 2009.

[Aar06] S. Aaronson. The quantum PCP manifesto, 2006. http://scottaaronson.com/blog/?p=139.

[FLvMV05] L. Fortnow, R. Lipton, D. van Melkebeek, and A. Viglas. Time-space lower bounds for satisfiability. *Journal of the ACM*, 52:835–865, 2005.

[For00] L. Fortnow. Time-space tradeoffs for satisfiability. *Journal of Computer and System Sciences*, 60(2):337–353, 2000.

[Hem02] L. Hemaspaandra. SIGACT news complexity theory column 38. *ACM SIGACT News*, 33(4), 2002. Guest column by M. Schaefer and C. Umans.

[KKR06] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. 35(5):1070–1097, 2006.

[KSV02] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[Lau83] C. Lautemann. BPP and the polynomial time hierarchy. *Information Processing Letters*, 17:215–218, 1983.

[MS72] A. Meyer and L. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential time. In *Proceedings of the 13th Symposium on Foundations of Computer Science*, pages 125–129, 1972.

[Sip83] M. Sipser. A complexity theoretic approach to randomness. In *Proc. of the 15th Symposium on Theory of computing*, pages 330–335. ACM Press, 1983.

[SZ94] A. Srinivasan and D. Zuckerman. Computing with very weak random sources. In *Proceedings of the 35th Symposium on Foundations of Computer Science*, pages 264–275, 1994.

[Uma99] C. Umans. Hardness of approximating Σ_2^p minimization problems. In *Proceedings of the 40th Symposium on Foundations of Computer Science*, pages 465–474, 1999.

[Yam02] T. Yamakami. Quantum NP and a quantum hierarchy. In *Proceedings of the 2nd IFIP International Conference on Theoretical Computer Science*, pages 323–336. Kluwer Academic Publishers, 2002.