Epsilon-net method for optimizations over separable states

Yaoyun Shi and Xiaodi Wu

Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, USA

Abstract

We give algorithms for the optimization problem: $\max_\rho \langle Q, \rho\rangle$, where Q is a Hermitian matrix, and the variable ρ is a bipartite *separable* quantum state. This problem lies at the heart of several problems in quantum computation and information, such as the complexity of QMA(2). While the problem is NP-hard, our algorithms are better than brute force for several instances of interest. In particular, they give PSPACE upper bounds on promise problems admitting a QMA(2) protocol in which the verifier performs only logarithmic number of elementary gates that act on both proofs, as well as the promise problem of deciding if a bipartite local Hamiltonian's ground energy is large or small. For $Q \geq 0$, our algorithm runs in time exponential in $\|Q\|_F$. While the existence of such an algorithm was first proved recently by Brandão, Christandl and Yard [*Proceedings of the 43rd annual ACM Symposium on Theory of Computation*, 343–352, 2011], our algorithm is conceptually simpler.

Entanglement is an essential ingredient in many ingenious applications of quantum information processing. Understanding and exploiting entanglement remains a central theme in quantum information processing research [HHH+09]. Denote by $\mathrm{SepD}\left(\mathcal{A}_1 \otimes \mathcal{A}_2\right)$ the set of separable (i.e, unentangled) density operators over the space $\mathcal{A}_1 \otimes \mathcal{A}_2$. A fundamental question known as the *weak membership* problem for separability is to decide, given the classical description of a quantum state ρ over $\mathcal{A}_1 \otimes \mathcal{A}_2$, whether ρ is inside or ϵ far away in trace distance from $\mathrm{SepD}\left(\mathcal{A}_1 \otimes \mathcal{A}_2\right)$. Unfortunately, this basic problem turns out to be intractable. In 2003, Gurvits [Gur03] proved the NP-hardness of the problem when ϵ is inverse exponential in the dimension of $\mathcal{A}_1 \otimes \mathcal{A}_2$. The dependence on ϵ was later improved to inverse polynomial [Ioa07, Gha10].

In this paper we study a closely related problem to the weak membership problem discussed above. More precisely, we consider the linear optimization problem over separable states.

Problem 1. Given a Hermitian matrix Q over $\mathcal{A}_1 \otimes \mathcal{A}_2$ (of dimension $d \times d$), compute the optimum value, denoted by $\mathrm{OptSep}(Q)$, of the optimization problem

$$\max \langle Q, X\rangle \text{ subject to } X \in \mathrm{SepD}\left(\mathcal{A}_1 \otimes \mathcal{A}_2\right).$$

It is well-known in convex optimization [GLS93, Ioa07] that the weak membership problem and the weak linear optimization, a special case of Problem 1, over certain convex set, such as $\mathrm{SepD}\left(\mathcal{A}_1 \otimes \mathcal{A}_2\right)$, are equivalent up to polynomial loss in precision and polynomial-time overhead. Thus the hardness result on the weak membership problem for separability passes directly to Problem 1.

Besides the connection with the weak membership problem for separability, Problem 1 can also be understood from many other aspects. Firstly, as the objective function is the inner-product of a Hermitian matrix and a quantum state, which represents the average value of some physical observable, the optimal value of Problem 1 inherently possesses certain physical meaning. Secondly, in the study of the tensor product space [DF92], the value $\mathrm{OptSep}(Q)$ is precisely the *injective norm* of Q in $\mathcal{L}(\mathcal{A}_1) \otimes \mathcal{L}(\mathcal{A}_2)$, where $\mathcal{L}(\mathcal{A})$ denote the Banach space of operators on $\mathcal{A}$ with the operator norm. Finally, one may be equally motivated from the study in operations research. Problem 1 appeared in an equivalent form in [LQNY09] as "bi-quadratic optimization over unit spheres". Subsequent works [HLZ10, So11] demonstrated that Problem 1 is just a special case of a more general class of optimization problems called homogenous polynomial optimization with quadratic constraints, which is currently an active research topic in operation research.

Another motivation to study Problem 1 is the recent interest on the complexity class QMA(2). The class QMA [KSV02] is the quantum counterpart of the classical complexity class NP (or more precisely, MA).

While the extension of NP to allow multiple provers trivially reduces to NP itself, the power of QMA(2), the extension for QMA with multiple *unentangled* provers, remains far from being well understood. The study of the multiple-prover model was initiated in [KMY01, KMY03], where QMA(k) denotes the complexity class for the *k*-prover case. Much attention was attracted to this model because of the discovery that NP admits *logarithmic*-size unentangled quantum proofs [BT09] (with weak soundness). This result was surprising because single prover quantum logarithm-size proofs only characterize BQP [MW05]. It seems adding one unentangled prover increases the power of the model substantially. There are several subsequent works on refining the initial protocol either with improved completeness and soundness bounds [Bei10, ABD+09, CF11, GNN11] or with less powerful verifiers [CD10]. Recently it was proved that QMA(2)=QMA(poly) [HM10] by using the so-called *product test* protocol that determines whether a multipartite state is a product state when two copies of it are given. There is another line of research on the power of unentangled quantum proofs with restricted verifiers. Two complexity classes BellQMA and LOCCQMA, referring to the restricted verifiers that perform only nonadaptive or adaptive local measurements respectively, were defined in [ABD+09] and studied in [Bra08, BCY11]. It has been shown [BCY11] that LOCCQMA(m) is equal to QMA for constant m.

Despite much effort, no nontrivial upper bound of QMA(2) is known. The best known upper bound QMA(2)$\subseteq$NEXP follows trivially by nondeterministically guessing the two proofs. It would be surprising if QMA(2) $=$ NEXP. Thus it is reasonable to seek a better upper bound such as EXP or even PSPACE. It is not hard to see that simulating QMA(2) amounts to distinguishing between two promises of OptSep(Q), although one has the freedom to choose the appropriate Q. Problem 1 was also studied in [BCY11] for the same purpose.

Hardness result. There are several approaches to prove the hardness of Problem 1. The first is to make use of the NP-hardness of the weak membership problem and the folk theorem in convex optimization as mentioned above. However, one may directly reduce the CLIQUE problem to Problem 1 [deK08, LQNY09]. There is also a stronger hardness result [HM10] on the exact running time of algorithms solving Problem 1 conditioned on the Exponential Time Hypothesis (ETH) [IP01]. The hardness results extend naturally to the approximation version of Problem 1. It is known that OptSep(Q) remains to be NP-hard to compute even if an inverse polynomial additive error is allowed. Nevertheless, it is wide open whether the hardness result remains if one allows even a larger additive error.

From the perspective of operations research, the hardness of Problem 1 is a consequence of not being a convex optimization problem. In this case although efficient methods, compared with brute-force, for finding a local optimum usually exist, on the other hand finding the global one is fraught with difficulty. This is because one needs to enumerate all possible local optima before one can determine the global optimum in the worst case.

Our contributions. In this paper we provide efficient algorithms for Problem 1 in either time or space for several Qs of interest. As the hardness result implies that enumeration is likely to be inevitable in the worst case, our idea is to enumerate via epsilon-nets more "cleverly" with the help of certain structure of Q.

When the total number of points to enumerate is not large, one can represent and hence enumerate each point in polynomial space. If the additional computation for each point can also be done in polynomial space, one immediately gets a polynomial-space implementation for the whole algorithm by composing those two components naturally. We make use of the relation NC(poly)=PSPACE [Bor77] to obtain space-efficient implementation for the additional computation, which in our cases basically includes the following two parts. The first part helps to make sure the enumeration procedure works correctly. This is because these epsilon-nets of interest in our algorithm are not standard, additional effort is necessary to generate them. This part turns into a simple application of the so-called *multiplicative matrix weight update* (MMW) method [AHK05, WK06, Kal07] to computing a min-max form, which is known to admit efficient parallel algorithms under certain conditions. The second part contains the real computation that in our case only consists of fundamental matrix operations. It is well known those operations admit efficient parallel algorithms [Gat93]. As a result,the additional computation can be implemented in polynomial space in our case. We summarize below the main results obtained by applying the above ideas.

1. The first property exploited is the so-called *decomposability* of Q which refers to whether Q can be decomposed in the form $Q = \sum_{i=1}^{M} Q_i^1 \otimes Q_i^2$ with small M. Intuitively, if one substitutes this Q's decomposition into $\langle Q, \rho_1 \otimes \rho_2 \rangle$ and treat $\langle Q_1^1, \rho_1 \rangle, \cdots, \langle Q_M^1, \rho_1 \rangle, \langle Q_1^2, \rho_2 \rangle, \cdots, \langle Q_M^2, \rho_2 \rangle$ as variables, the optimization problem becomes quadratic and M corresponds to the number of second-order terms in the objective function. By plugging the values of $\langle Q_1^1, \rho_1 \rangle, \cdots, \langle Q_M^1, \rho_1 \rangle$ into the objective function, the optimization problem reduces to be a semidefinite program, and thus can be efficiently solved. Since this approach naturally extends to the k-partite case for $k \geq 2$, we obtain the following general result.

Theorem 1 (Informal)**.** *Given any Hermitian Q and its decomposition, OptSep(Q) can be approximated with an additive error δ in quasi-polynomial time*[1] *in d and $1/\delta$ if kM is bounded by poly-logarithms of d.*

By exploiting the space-efficient algorithm design strategy above, this algorithm can also be made space-efficient. To facilitate the later applications to complexity classes, we choose the input size to be some n such that $d = \exp(\mathrm{poly}(n))$.

Corollary 1 (Informal)**.** If $kM/\delta \in O(\mathrm{poly}(n))$, OptSep$(Q)$ can be approximated with an additive error δ in PSPACE.

As a direct application, we prove the following variant of QMA(2) belongs to PSPACE. Note the complexity class QMA(2)$[\mathrm{poly}(n), O(\log(n))]$ refers to the model where the verifier only performs $O(\log(n))$ elementary gates that act on both proofs at the same time and a polynomial number of other elementary gates.

Corollary 2. QMA(2)$[\mathrm{poly}(n), O(\log(n))] \subseteq$ PSPACE.

This result establishes the first PSPACE upper bound for a variant of QMA(2) where the verifier is allowed to generate some quantum entanglement between two proofs. In contrast, previous results are all about variants with nonadaptive or adaptive local measurements, such as BellQMA(2) [ABD+09, Bra08, CD10] or LOCCQMA(2) [ABD+09, BCY11].

We also initiate the study of Problem 1 for a k-partite local Hamiltonian Q. Recall that a promise version of this problem in the one party case, namely the *local-Hamiltonian problem*, is QMA-complete problem [KSV02]. Our definition extends the original local Hamiltonian problem to its k-partite version. However, as will be clear in the main section, the k-partite local Hamiltonian problem is no longer necessarily QMA(k)-complete. On the other side, our enumeration algorithm based on the decomposability of Q works extremely well in this case. As a result, we obtain the following corollary.

Corollary 3 (Informal)**.** For a k-partite local Hamiltonian Q, OptSep(Q) can be approximated with an additive error δ in quasi-polynomial time in $d, 1/\delta$; the k-partite local Hamiltonian problem is in PSPACE.

2. The second structure made use of is the eigenspace of Q of large eigenvalues. As a result, we establish an algorithm solving Problem 1 with running time exponential in $\|Q\|_{\mathrm{F}}$.

Theorem 2 (Informal)**.** *For a positive semidefinite Q, OptSep(Q) can be approximated with an additive error δ in time* $\exp(O(\log(d) + \delta^{-2}\|Q\|_F^2 \ln(\|Q\|_F/\delta)))$.

A similar running time $\exp(O(\log^2(d)\delta^{-2}\|Q\|_{\mathrm{F}}^2))$ was obtained in [BCY11] using some known results in quantum information theory (i.e., the semidefinite programming for finding symmetric extension [DPS04] and an improved quantum de Finetti-type bound.) In contrast, our algorithm only uses fundamental operations of matrices and epsilon-nets. To approximate with precision δ, it suffices to consider the eigenspace of Q of eigenvalues greater than δ and a dimension bounded by $\|Q\|_{\mathrm{F}}^2/\delta^2$. Nevertheless, naively enumerating density operators over that subspace does not work since one cannot detect the separability of those density operators. We circumvent this difficulty by making use of the Schmidt decomposition of bipartite pure states. We note, however, that other results in [BCY11] do not follow from our algorithm, and our method cannot be seen as a replacement of the kernel technique therein. Furthermore, our method does not extend to the k-partite case, as there is no Schmidt decomposition in that case.

[1] Quasi-polynomial time is upper bounded by $2^{O((\log n)^c)}$ for some fixed c, where n is the input size.

Acknowledgement

We thank Zhengfeng Ji and John Watrous for helpful discussions. This research was supported in part by National Basic Research Program of China Awards 2011CBA00300 and 2011CBA00301, and by NSF of United States Award 1017335.

References

[ABD+09] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman and P. Shor, The Power of Unentanglement. *Theory of Computing*, 5, pp. 1-42, 2009.

[AHK05] S. Arora, E. Hazan, and S. Kale. The multiplicative weights update method: a meta algorithm and applications, 2005.

[Bei10] S. Beigi. NP vs QMAlog(2). *Quantum Information and Computation*, 54(1&2):0141–0151, 2010.

[Bor77] Allan Borodin. On relating time and space to size and depth. *SIAM Journal on Computing*, 6(4):733–744, 1977.

[BT09] H. Blier and A. Tapp, All languages in NP have very short quantum proofs. *Proceedings of the ICQNM*, pp. 34-37, 2009.

[Bra08] F. G. S. L. Brandão. *Entanglement Theory and the Quantum Simulation of Many-Body Physics*. PhD thesis, Imperial College, 2008.

[BCY11] F. G. S. L. Brandão, M. Christandl, and J. Yard. A quasipolynomial-time algorithm for the quantum separability problem. *Proceedings of the 43rd annual ACM Symposium on Theory of Computation (STOC'11)* ,pp. 343, 2011.

[CD10] J. Chen and A. Drucker. Short multi-prover quantum proofs for SAT without entangled measurements. arXiv:1011.0716, 2010.

[CF11] A. Chiesa and M. Forbes. Improved Soundness for QMA with Multiple Provers. arXiv:1108.2098, 2011.

[DF92] A. Defant and K. Floret. *Tensor norms and operator ideals*, North Holland, 1992.

[DPS04] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. A complete family of separability criteria. *Phys. Rev. A*, 69:022308, 2004.

[Gat93] J. von zur Gathen. Parallel linear algebra. In J. Reif, editor, *Synthesis of Parallel Algorithms*, chapter 13. Morgan Kaufmann Publishers, Inc., 1993.

[Gha10] S. Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information and Computation* , 10:343, 2010.

[GLS93] M. Grötschel, L. Lovász, and A. Schrijver. *Geometric algorithms and combinatorial optimization*. Springer-Verlag, 1993.

[GNN11] F. L. Gall, S. Nakagawa and H. Nishimura. On QMA Protocols with Two Short Quantum Proofs. arXiv:1108.4306 , 2011.

[Gur03] L. Gurvits. Classical complexity and quantum entanglement. *Journal of Computer and System Sciences*, 69:448, 2004.

[GW10] G. Gutoski and X. Wu. Parallel approximation of min-max problems with applications to classical and quantum zero-sum games. arXiv:1011.2787v2.

[HHH+09] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865, 2009

[HLZ10] S. He, Z. Li and S. Zhang. Approximation Algorithms for Homogeneous Polynomial Optimization with Quadratic Constraints. *Mathematical Programming*, Series B 125(2), 353–383, 2010.

[HM10] A. Harrow and A. Montanaro. An efficient test for product states, with applications to quantum Merlin-Arthur games. *Proceedings of IEEE 51st Annual Symposium on Foundations of Computer Science (FOCS'10)*, p. 633, 2010.

[Ioa07] L. M. Ioannou. Computational complexity of the quantum separability problem. *Quantum Information and Computation*, 7:335, 2007.

[IP01] R. Impagliazzo and R. Paturi. On the complexity of k-SAT. *Journal of Computer and System Sciences*, 62(367), 2001.

[JW09] R. Jain and J. Watrous. Parallel approximation of non-interactive zero-sum quantum games. In *Proceedings of the 24th IEEE Conference on Computational Complexity*, pages 243–253, 2009.

[Kal07] S. Kale. *Efficient algorithms using the multiplicative weights update method*. PhD thesis, Princeton University, 2007.

[deK08] E. de Klerk. The Complexity of Optimizing over a Simplex, Hypercube or Sphere: a Short Survey. *Central European Journal of Operations Research* 16(2), 111–125, 2008.

[KMY01] H. Kobayashi, K. Matsumoto and T. Yamakami, Quantum Certificate Verification: Single versus Multiple Quantum Certificates, quant-ph/0110006.

[KMY03] H. Kobayashi, K. Matsumoto and T. Yamakami, Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur?, *Lecture Notes in Computer Science*, vol. 2906, pp. 189-198, 2003.

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

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

[LQNY09] C. Ling, L. Qi, J. Nie and Y. Ye, Bi-Quadratic Optimization over Unit Spheres and Semidefinite Programming Relaxations. *SIAM Journal on Optimization*, Vol. 20, No. 3, pp.1286–1310, 2009.

[MW05] C. Marriott and J. Watrous, Quantum Arthur-Merlin Games, *Computational Complexity*, 14(2): 122-152, 2005

[MWW09] W. Matthews, S. Wehner, and A. Winter. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding. *Comm. Math. Phys.*, 291, 2009

[NC00] Michael Nielsen and Issac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[So11] A. M. So. Deterministic Approximation Algorithms for Sphere Constrained Homogeneous Polynomial Optimization Problems. *Mathematical Programming*, to appear 2011.

[Wat08] J. Watrous. *Lecture Notes on Theory of Quantum Information*. 2008.

[WK06] M. Warmuth and D. Kuzmin. Online variance minimization. In *Proceedings of the 19th Annual Conference on Learning Theory*, volume 4005 of *Lecture Notes in Computer Science*, pages 514–528. Springer, 2006.

[Wu10a] X. Wu. Equilibrium value method for the proof of QIP=PSPACE. arXiv:1004.0264v4 [quant-ph], 2010.