An improved semidefinite programming hierarchy for testing entanglement

Aram W. Harrow, Anand Natarajan, and Xiaodi Wu

MIT Center for Theoretical Physics

I. INTRODUCTION

Entanglement is one of the key features that distinguishes quantum information from classical information. One particularly basic and important problem in the theory of entanglement is to determine whether a given mixed state ρ is entangled or separable. Via standard techniques of convex optimization, this problem is roughly equivalent to maximizing a linear function over the set of separable states [1]. Indeed, it has close relations with a variety of problems, including estimating channel capacities, analyzing two-prover proof systems, finding the ground-state energy in the mean-field approximation, finding the least entangled pure state in a subspace, etc. as well as problems not obviously related to quantum mechanics such as planted clique, the unique games problem and small-set expansion [2].

However, there is no simple test for determining whether a state is entangled. Indeed not only are tests such as the PPT (positive partial transpose) condition known to have arbitrarily large error [3], but computational hardness results show that any test implementable in time polynomial in the dimension must be highly inaccurate, given the plausible assumption that 3-SAT requires exponential time [2, 4]. These limitations indicate that separability tests cannot be as efficient as, say, a test for correlation, or a calculation of the largest eigenvalue of a matrix.

The main open question is whether algorithms exist that match these hardness results, or whether further hardness results can be found. The two leading algorithmic frameworks are ϵ-nets and semidefinite programming (SDP) hierarchies. There are two regimes in which these come close to matching the known hardness results. Let n denote the dimension of the states we examine. Informally speaking, the well-studied regimes are the constant-error regime, where there are both algorithms and hardness results with time $n^{\Theta(\log n)}$ (although important caveats exist, discussed below), and the $1/\operatorname{poly}(n)$ regime, where the algorithms and hardness results together suggest that the complexity is exponential in n.

In this paper we consider the regime of much lower error. Specifically, if ϵ is the error allowed, we will focus on the scaling of error with ϵ rather than n. In other settings, such as infinite translationally invariant Hamiltonians, it is possible for the complexity to grow rapidly with $1/\epsilon$ even for fixed local dimension [5]. Another example closer to the current work is [6], which showed that approximating quantum interactive proofs to high accuracy (specifically with the bits of precision polynomial in the message dimension) corresponds to the complexity class EXP rather than PSPACE. However, for separability testing we will show this is not the case.

Our main contribution is to describe a pair of classical algorithms for the separability problem. In the high-accuracy limit both run in time $\exp(\operatorname{poly}(n))\operatorname{poly}\log(1/\epsilon)$. One is based on quantifier elimination [7] and is simple, but does not appear to yield new insights into the problem. The second algorithm is based on an SDP hierarchy due to Doherty, Parrilo and Spedalieri (DPS) [8]. Like DPS, our algorithm runs in time $\operatorname{poly}(\binom{n+k-1}{k})$ for what is called the k^{th} "level" of the hierarchy. As k is increased our algorithm, like that of DPS, becomes more accurate. Indeed, for any fixed value of k our algorithm performs at least as well as that of DPS. However, unlike DPS, our hierarchy always converges exactly in a finite number of steps, which we can upper bound by $\exp(\operatorname{poly}(n))$. Taking into account numerical error yields an algorithm again running in time $\exp(\operatorname{poly}(n))\operatorname{poly}\log(1/\epsilon)$. Thus our algorithm is, for the first time, a single SDP hierarchy which matches or improves upon the best known performance of previous algorithms at each scale of ϵ.

The fact that our algorithm is a semidefinite program gives it further advantages. One very useful property of semidefinite programs is duality. In our algoirthm, both the primal and dual problems have useful interpretations in terms of quantum information. On the primal side, our algorithm can be viewed as searching over symmetric mixed states over an extended system obtained by adding copies of the individual subsystems. In this light, our convergence bounds can be viewed as new monogamy relations: we show that if a state is symmetric under exchange of subsystems and satisfies certain other conditions, then if there are enough copies of each subsystem, then none of the subsystems can be entangled with each other. On the dual side, every feasible point of the dual is an entanglement witness operator. Indeed, our algorithm yields a new class of entanglement witnesses, as discussed in section III.D of the full paper. Duality is also useful in practice, since a feasible solution to the dual can certify the correctness of the primal, and vice versa.

SDP hierarchies are also used for discrete optimization problems, such as integer programming. In that case, it is known that the n^{th} level of most SDP hierarchies provides the exact answer to optimizations problems on n bits. By contrast, neither the DPS hierarchy nor the more general Sum-of-Squares SDP hierarchy will converge exactly at any finite level for general objective functions. Our result can be seen as a continuous analogue of the exact convergence achievable for discrete optimization.

The main idea of our algorithm is that entanglement testing can be viewed as a convex optimization problem, and thus the solution should obey the KKT (Karush-Kuhn-Tucker) conditions. Thus we can WLOG add these as constraints. It was shown in [9] that for general polynomial optimization problems, adding the KKT conditions yields an SDP hierarchy with finite convergence. Moreover, the number of levels necessary for convergence is a function only of the number of variables and the degrees of the objective and constraint polynomials. However, the proof of convergence presented in [9] gives a very high bound on the number of levels (triply exponential in n or worse). In contrast, we obtain a bound in the number of levels that is singly exponential in n. We use tools from algebraic geometry (Bézout's and Bertini's theorem) to show that generically, adding the KKT conditions reduces the feasible set of our optimization problem to isolated points. Then, using tools from computational algebra (Gröbner bases), we show that low levels of the SDP hierarchy can effectively search over this finite set. Although we use genericity in the analysis, our algorithm works for all inputs. We emphasize that our *proof* employs tools from algebraic geometry while our algorithm involves an elementary and simple modification of the DPS hierarchy.

While some of these techniques have been used to analyze SDP hierarchies in the past, they have generally not been applied to the problems arising in quantum information. We hope that they find future application to understanding entanglement witnesses, monogamy of entanglement and related phenomena.

Our main contribution is an improved version of the DPS hierarchy which we describe in section III. It is always at least as stringent as the DPS hierarchy, and in Theorem 1 we show that it outperforms DPS by converging exactly at a finite level, depending on the input dimension.

II. CONNECTIONS TO OTHER PROBLEMS

Define $\text{Sep}(n,k) := \text{conv}\{|\psi_1\rangle\langle\psi_1| \otimes \cdots \otimes |\psi_k\rangle\langle\psi_k| : |\psi_1\rangle, \ldots, |\psi_k\rangle \in B(\mathbb{C}^n)\}$, where $\text{conv}(S)$ denotes the convex hull of a set S (i.e. the set of all finite convex combinations of elements of S) and $B(V)$ denotes the set of unit vectors in a vector space V. States in $\text{Sep}(n,k)$ are called separable, and those not in $\text{Sep}(n,k)$ are entangled. Given a Hermitian matrix M, we define

$$h_{\text{Sep}(n,k)}(M) := \max\{\text{Tr}[M\rho] : \rho \in \text{Sep}(n,k)\}. \tag{1}$$

We will often abbreviate $\text{Sep} := \text{Sep}(n,2)$ where there is no ambiguity. More generally if K is a convex set, we can define $h_K(x) := \max\{\langle x, y\rangle : y \in K\}$. A classic result in convex optimization [1]

holds that approximating h_K is roughly equivalent in difficulty to the weak membership problem for K: namely, determining whether $x \in K$ or whether $\mathrm{dist}(x, K) > \epsilon$ given the promise that one of these holds. Thus, in what follows we will treat entanglement testing (i.e. the weak membership problem for Sep) as equivalent to the optimization problem in (1). For mathematical simplicity, we make a further reduction from h_{Sep} to the optimization problem $h_{\mathrm{ProdSym}(n,k)}$, defined in terms of the set $\mathrm{ProdSym}(n,k) := \mathrm{conv}\{(|\psi\rangle\langle\psi|)^{\otimes k} : |\psi\rangle \in B(\mathbb{C}^n)\}$. In Corollary 14 of [2] (see specifically explanation (2) there) it was proven that for any n^2-dimensional M there exists M' with dimension $4n^2$ satisfying $h_{\mathrm{ProdSym}(2n,2)}(M') = \frac{1}{4} h_{\mathrm{Sep}(n,2)}(M)$. Thus an algorithm for h_{ProdSym} implies an algorithm of similar complexity for h_{Sep}.

We will not fully survey the applications of separability testing, but briefly mention two connections. First, $h_{\mathrm{Sep}(2^n,k)}$ is closely related to the complexity class $\mathsf{QMA_n(k)}$ in which k unentangled provers send n-qubit states to a verifier. If the verifier's measurement is M (which might be restricted, e.g. by being the result of a short quantum circuit) then the maximum acceptance probability is precisely $h_{\mathrm{Sep}(2^n,k)}(M)$. Thus the complexity of h_{Sep} is closely related to the complexity of multiple-Merlin proof systems. See [10] for a classical analogue of these proof systems, and a survey of recent open questions.

Second, h_{Sep} is closely related to the problems of estimating the $2 \to 4$ norm of a matrix, finding the least-expanding small set in a graph and estimating the optimum value of a unique game [11]. These problems in turn relate to the approximation complexity of constraint satisfaction problems, which are an extremely general class of discrete optimization problems. They are currently known only to be of intermediate complexity (i.e. only subexponential-time algorithms are known), and are the subject of intense research. One of leading approaches to these problems has been SDP hierarchies, but here too it is generally unknown how well these hierarchies perform or which features are important to their success.

III. ALGORITHM AND RESULTS

Our algorithm takes the form of a hierarchy of semidefinite programs. There are many ways to formulate the hierarchy; here we present a formulation suited for comparison with DPS. The level-r SDP of our hierarchy for h_{ProdSym} is

$$\begin{aligned} \max_{\rho} \quad & \langle \mathcal{P}(M \otimes \mathbb{1}^{\otimes r}), \rho \rangle \\ \text{such that} \quad & \rho \succeq 0, \langle \mathcal{P}(A_\alpha \otimes \Gamma_{ij}), \rho \rangle = 0 \ \forall i, j, \alpha. \end{aligned} \tag{2}$$

In this program, the variable ρ is a matrix in $\mathbb{R}^{(2n)^{d+r} \times (2n)^{d+r}}$, representing a density matrix $d + r$ parties. The symbol $\mathcal{P}$ indicates symmetrization under interchange of the parties. The main difference from DPS is the set of added constraints $\langle A_\alpha \otimes \Gamma_{ij}, \rho \rangle = 0$, which are the moment relaxations of the KKT conditions.

Our main result is the following convergence bound:

Theorem 1. *For all input M, the hierarchy (2) converges to the optimum value of $h_{\mathrm{ProdSym}}(M)$ at level $r = O(d^{\mathrm{poly}(n)})$.*

Corollary 1. *For all inputs M, $h_{\mathrm{ProdSym}}(M)$ and $h_{\mathrm{Sep}}(M)$ can be approximated up to additive error ϵ in time $O(d^{\mathrm{poly}(n)} \operatorname{poly} \log(1/\epsilon))$.*

[1] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, second corrected edition ed., Algorithms and Combinatorics, Vol. 2 (Springer, 1993) ISBN 3-540-56740-2, 0-387-56740-2 (U.S.).
[2] A. W. Harrow and A. Montanaro, J. ACM, **60**, 3:1 (2013), ISSN 0004-5411, 1001.0017.
[3] S. Beigi and P. W. Shor, J. Math. Phys., **51**, 042202 (2010), 0902.1806.
[4] F. L. Gall, S. Nakagawa, and H. Nishimura, Q. Inf. Comp., **12**, 589 (2012), 1108.4306.
[5] T. S. Cubitt, D. Perez-Garcia, and M. Wolf, "Undecidability of the spectral gap problem," (2014), in preparation.
[6] T. Ito, H. Kobayashi, and J. Watrous, in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, ITCS '12 (2012) pp. 266–275, ISBN 978-1-4503-1115-1, 1012.4427.
[7] S. Basu, R. Pollack, and M.-F. Roy, J. ACM, **43**, 1002 (1996), ISSN 0004-5411.
[8] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, "A complete family of separability criteria," (2003), arXiv:quant-ph/0308032.
[9] J. Nie, "An exact Jacobian SDP relaxation for polynomial optimization," (2010), arXiv:1006.2418.
[10] S. Aaronson, R. Impagliazzo, and D. Moshkovitz, in *Computational Complexity (CCC), 2014 IEEE 29th Conference on* (2014) pp. 44–55, 1401.6848.
[11] B. Barak, F. G. S. L. Brandão, A. W. Harrow, J. Kelner, D. Steurer, and Y. Zhou, in *Proceedings of the 44th symposium on Theory of Computing*, STOC '12 (2012) pp. 307–326, 1205.4484.