CONJURA · OPEN PROBLEM

Subexponential Best Separable State with Imperfect Completeness

Constant completeness error rather than $1/n$

Status. Statement: AI-written from Boaz Barak, Pravesh K. Kothari, David Steurer, *Quantum entanglement, sum of squares, and the log rank conjecture*, arXiv preprint (quant-ph), v2 submitted 9 July 2017, not yet checked by a human. The perfect-completeness case $c = 1$ and the near-perfect case $c = 1 - 1/n$ are settled by the source (Theorem 1.3 together with Remarks 1.4 and 4.3); the case of a constant c strictly below 1 — the case asserted here — is open, and the paper lists it first among the open questions of its Section 8 and conjectures the affirmative answer.

Category. *Quantum.*

Conjecture (informal). *Given a quantum measurement on a pair of subsystems, deciding whether some non-entangled state passes it is not known to be doable faster than trying essentially everything, which costs exponential time in the dimension. This paper gives the first improvement: an algorithm running in time roughly two to the square root of the dimension, but only in the case where the yes-instances are perfect, meaning that some non-entangled state is accepted with probability exactly one. The authors observe that their proof also tolerates a completeness error of one over the dimension, and no more, because the rank one matrix their rounding procedure produces is only guaranteed to have norm about the square root of the dimension divided by the dimension, so anything larger than a roughly one-over-the-dimension error swamps it. They conjecture that the result nevertheless holds with a constant completeness error: for any two constants with the first strictly larger than the second and strictly below one, distinguishing the case that some non-entangled state is accepted with probability at least the first from the case that every non-entangled state is accepted with probability at most the second should also be possible in time two to roughly the square root of the dimension.*

1 The setting

Deciding whether a given quantum state is entangled is not known to be doable in time polynomial in the dimension, and the robust version, the Quantum Separability Problem, is NP hard for inverse-polynomial ε by Gharibian [Gha10], improving on Gurvits [Gur03]. The closely related Best Separable State problem $\mathrm{BSS}_{c,s}$ asks to distinguish the case that some separable state is accepted by a given measurement with probability at least c from the case that every separable state is accepted with probability at most s. Certifying the NO case makes the measurement an entanglement witness, which is how entanglement is certified experimentally.

BSS is NP hard when $c - s = 1/\mathrm{poly}(n)$ [BT09, Gur03], and Harrow and Montanaro [HM13] show that under the Exponential Time Hypothesis there is no $n^{o(\log n)}$ time algorithm for $\mathrm{BSS}_{1,1/2}$. The problem is the algorithmic face of the complexity class QMA(2): an algorithm for $\mathrm{BSS}_{c,s}$ decides languages in QMA(2) with completeness c and soundness s, so a quasi-polynomial time algorithm for $\mathrm{BSS}_{0.99,0.5}$ would give $\mathrm{QMA}(2) \subseteq \mathrm{EXP}$. Doherty, Parrilo and Spedalieri [DPS04] proposed a sum-of-squares algorithm; it is not known whether it solves $\mathrm{BSS}_{c,s}$ for constants $c > s$ in quasi-polynomial time, though Brandão, Christandl and Yard [BaCY11] showed quasi-polynomial time for the restricted class of 1-LOCC measurements, and Brandão and Harrow [BH15] obtained comparable performance by an ε-net search. Aaronson, Impagliazzo and Moshkovitz [AIM14] suggested that $\mathrm{BSS}_{c,s}$ for constants $s < c$ might admit a quasi-polynomial time algorithm.

This paper gives the first improvement over brute force for general measurements: a $2^{\tilde{O}(\sqrt{n})}$ time algorithm, based on $\tilde{O}(\sqrt{n})$ rounds of the sum-of-squares hierarchy, for $\mathrm{BSS}_{1,s}$ for every constant $s < 1$. The completeness side is perfect: the analysis runs the sum-of-squares program with the hard constraint that the rank one matrix $uv^\top$ lie exactly in the eigenspace $\mathcal{W}$ of $\mathcal{M}$ for eigenvalue 1. Remark 4.3 of the paper records the slack the argument has, and supplies the numbers: the proof would still go through if $uv^\top$ merely had small component orthogonal to $\mathcal{W}$, the rounding guarantees that the output rank one matrix $u_0 v_0^\top$ has norm at least k/n with $k = \tilde{O}(\sqrt{n})$, and it therefore suffices that $\|\Pi_{\mathcal{W}} uv^\top\|^2 \geq 1 - k^2/n^2$ — which is what yields the near-perfect completeness case $c = 1 - 1/n$. The

remark is framed there as an extension, not as a barrier. Comparing its numbers with the conjecture is our own inference, not a claim the paper makes: a tolerable completeness error of order k^2/n^2, that is $\tilde{O}(1/n)$, falls short of a constant error by a factor of order n, and we are not aware of anything in the published analysis that closes that gap. Section 8 lists removing the perfect or near-perfect completeness condition first among the questions the paper leaves open.

Why it matters. The version of Best Separable State that bears on quantum complexity and on practice is the two-sided-error one, where the accepting separable state is only required to pass with probability bounded away from one by a constant: perfect completeness is a fragile promise, and the motivation the paper itself gives for studying BSS — noisy, experimentally realizable measurements used as entanglement witnesses — lives in the constant-error regime. Settling this in the affirmative would give the first subexponential algorithm for constant-gap BSS, that is for QMA(2) with two-sided error, which is precisely the regime in which a quasi-polynomial algorithm would give QMA(2) $\subseteq$ EXP. Settling it in the negative would be more striking still, since it would separate the constant-completeness problem from the perfect-completeness one and show that the $2^{\tilde{O}(\sqrt{n})}$ algorithm depends essentially on an exact algebraic promise rather than on the geometry of the separable cone.

Progress to date. The paper proves the case $c = 1$ (Theorem 1.3) and states in Remark 1.4 that all the proofs extend to near perfect completeness, $c = 1 - 1/n$. Remark 4.3 supplies the quantitative reason: the analysis of Theorem 4.1 guarantees that the rounded rank one matrix has norm at least k/n with $k = \tilde{O}(\sqrt{n})$, so it suffices that the projection of $uv^\top$ onto $\mathcal{W}$ have squared norm at least $1 - k^2/n^2$, a completeness error of order $\tilde{O}(1/n)$. Nothing in the paper closes the remaining factor of order n up to a constant error, and no partial result at any intermediate completeness error, such as $1/\mathrm{polylog}(n)$ or $1/n^{0.9}$, is reported.

2 Notation and parameters

- $n \in \mathbb{N}$ is the local dimension; the joint system has dimension $m = n^2$, and $\mathbb{C}^{n^2}$ is identified with $\mathbb{C}^n \otimes \mathbb{C}^n$ by identifying the vector indexed by $[n] \times [n]$ with the $n \times n$ matrix of its

coordinates. Brute force over the separable states costs $2^{O(n)}$.

- For $u \in \mathbb{C}^n$, u^* denotes the conjugate transpose; for Hermitian A, B, $A \preceq B$ means $B - A$ is positive semidefinite; I is the identity matrix.
- Tr denotes the trace.
- c and s are the completeness and soundness thresholds, $0 \le s < c < 1$, both constants independent of n. The paper proves the case $c = 1$ and extends to $c = 1 - 1/n$; the conjecture is the case where c is a constant strictly below 1.
- $C = C(c, s)$ is the constant hidden in the running time $2^{\tilde{O}(\sqrt{n})}$; it may depend on c and s but not on n or $\mathcal{M}$.

3 The conjecture

Definition 1 (Quantum state). A *quantum state* on a system of m elementary states is an $m \times m$ complex Hermitian positive semidefinite matrix ρ with $\operatorname{Tr} \rho = 1$. It is *pure* if $\rho = ww^*$ for a unit vector $w \in \mathbb{C}^m$.

Definition 2 (Measurement operator). A *measurement operator* on a system of m elementary states is an $m \times m$ complex Hermitian matrix $\mathcal{M}$ with $0 \preceq \mathcal{M} \preceq I$. The probability that $\mathcal{M}$ accepts a state ρ is $\operatorname{Tr}(\rho \mathcal{M})$.

Definition 3 (Separable state). Take $m = n^2$ and identify $[m]$ with $[n] \times [n]$ as above. A pure state $\rho = ww^*$ on $\mathbb{C}^m$ is *separable* if the vector $w \in \mathbb{C}^m$, viewed as an $n \times n$ matrix, equals uv^* for some $u, v \in \mathbb{C}^n$. A general state ρ is *separable* if it is a convex combination of separable pure states, that is $\rho = \mathbb{E}\,(uv^*)(uv^*)^*$ for some distribution over pairs of unit vectors $u, v \in \mathbb{C}^n$. A state that is not separable is *entangled*.

Definition 4 (The promise problem $\mathrm{BSS}_{c,s}$). Let $0 \le s < c \le 1$. An instance of $\mathrm{BSS}_{c,s}$ is an $n^2 \times n^2$ measurement operator

$\mathcal{M}$. It is a YES instance if there exists a separable state ρ on $\mathbb{C}^{n^2}$ with $\mathrm{Tr}(\rho\mathcal{M}) \geq c$, and a NO instance if every separable state ρ on $\mathbb{C}^{n^2}$ satisfies $\mathrm{Tr}(\rho\mathcal{M}) \leq s$. Instances that are neither carry no promise.

Conjecture 1 (subexponential BSS with constant completeness error). *For all constants c, s with $0 \leq s < c < 1$ there exist a finite constant $C = C(c,s)$ and a randomized algorithm $\mathcal{A}$ with the following property. On input an $n^2 \times n^2$ measurement operator $\mathcal{M}$ (Definition 2), the algorithm $\mathcal{A}$ halts after at most*

$$2^{C\sqrt{n}\,(\log n)^C}$$

steps and decides the promise problem $\mathrm{BSS}_{c,s}$ of Definition 4: it outputs YES with probability at least $2/3$ whenever there exists a separable state ρ on $\mathbb{C}^{n^2}$ with $\mathrm{Tr}(\rho\mathcal{M}) \geq c$, and outputs NO with probability at least $2/3$ whenever every separable state ρ on $\mathbb{C}^{n^2}$ satisfies $\mathrm{Tr}(\rho\mathcal{M}) \leq s$. (Its output is unconstrained on inputs satisfying neither condition.) Here the entries of $\mathcal{M}$ are given as complex numbers with rational real and imaginary parts of bit length at most $\mathrm{poly}(n)$ — an encoding fixed here for definiteness, not a condition taken from the paper, which specifies none.

Remark 1 (why randomized). The paper's own algorithm is randomized: its Lemma 7.1 locates the reweighting direction by showing that a random unit vector succeeds with probability $2^{-O(k)}$, and no derandomization is given. Since Remark 1.4 conjectures that the paper's results extend, a randomized $2^{\tilde{O}(\sqrt{n})}$ algorithm should suffice to settle Conjecture 1, and the statement is written to allow one; a deterministic algorithm settles it a fortiori.

Remark 2 (the quantifier over c and s). The paper writes of "the setting where in the YES case $\mathrm{Tr}(\rho\mathcal{M}) = 1 - \varepsilon$ for some absolute constant ε", which read literally is an existential over ε. Conjecture 1 states the universal form, for all constants $0 \leq s < c < 1$, on the grounds that Remark 1.4 frames the question as whether the paper's results extend and that Theorem 1.3, the result being extended, is universally quantified over the soundness parameter; a single

unspecified ε would be an odd thing to conjecture. A reviewer who prefers the weaker existential reading should say so.

Remark 3 (algorithmic versus sum-of-squares form). What the paper conjectures is that its own proofs extend, which is formally stronger than the existence of some $2^{\tilde{O}(\sqrt{n})}$ algorithm: it asserts that the specific sum-of-squares algorithm of its Section 4, with $\tilde{O}(\sqrt{n})$ rounds, works. Stated above is the algorithmic consequence, since pinning down "the same algorithm" would require reproducing the paper's program. A solver who wants to match the paper exactly should aim at the sum-of-squares version.

4 Bibliography

[AIM14] Scott Aaronson, Russell Impagliazzo, and Dana Moshkovitz. *AM with multiple merlins.* Electronic Colloquium on Computational Complexity (ECCC) 21, 12, 2014.

[BaCY11] Fernando G.S.L. Brandão, Matthias Christandl, and Jon Yard. *A quasipolynomial-time algorithm for the quantum separability problem.* Proceedings of the Forty-third Annual ACM Symposium on Theory of Computing, STOC '11, ACM, pp. 343–352, 2011.

[BH15] Fernando G. S. L. Brandão and Aram Wettroth Harrow. *Estimating operator norms using covering nets.* CoRR abs/1509.05065, 2015.

[BT09] Hugue Blier and Alain Tapp. *All languages in np have very short quantum proofs.* Quantum, Nano and Micro Technologies, 2009. ICQNM'09. Third International Conference on, IEEE, pp. 34–37, 2009.

[DPS04] Andrew C Doherty, Pablo A Parrilo, and Federico M Spedalieri. *Complete family of separability criteria.* Physical Review A 69, no. 2, 022308, 2004.

[Gha10] Sevag Gharibian. *Strong np-hardness of the quantum separability problem.* Quantum Information & Computation 10, no. 3, 343–360, 2010.

[Gur03] Leonid Gurvits. *Classical deterministic complexity of edmonds' problem and quantum entanglement.* Proceedings of the thirty-fifth annual ACM symposium on Theory of computing, ACM, pp. 10–19, 2003.

[HM13] Aram Wettroth Harrow and Ashley Montanaro. *Testing product states, quantum merlin-arthur games and tensor optimization.* J. ACM 60, no. 1, 3, 2013.