Quantum de Finetti Theorems under Local Measurements with Applications

Fernando G.S.L. Brandão and Aram W. Harrow

Summary. In [1] we prove two new quantum versions of the de Finetti theorem, both showing that under tests formed by local measurements in each of the subsystems one can get a much improved error dependence on the dimension of the subsystems. We also obtain similar results for non-signalling probability distributions. We give the following applications of the results:

- We prove the optimality of the Chen-Drucker [2] $\mathsf{BellQMA}(\sqrt{n}\,\mathrm{polylog}(n))$ protocol for 3-SAT, under the assumption there is no subexponential-time algorithm for SAT: We show that any similar protocol in $\mathsf{BellQMA}(n^{1/2-\varepsilon}\,\mathrm{polylog}(n))$ would imply a $\exp((\tilde{O}(n^{1-2\varepsilon}))$-time algorithm for 3-SAT.

- We show that the maximum winning probability of free games (in which the questions to each prover are chosen independently) can be estimated in polynomial time by linear programming (for constant output alphabet). We also show that 3-SAT with m variables can be reduced to obtaining a constant error approximation of the maximum winning probability under entangled strategies of $O(\sqrt{m})$-player one-round non-local games, in which the players communicate $O(\sqrt{m})$ bits all together.

- We show that the optimization of certain polynomials over the hypersphere can be performed in quasipolynomial time in the number of variables n by considering $O(\log(n))$ rounds of the Sum-of-Squares (Parrilo/Lasserre) hierarchy of semidefinite programs. This can be considered an analogue to the hypersphere of a similar result by Powers and Reznick for the simplex [3]. We also give a quasipolynomial-time algorithm for deciding multipartite separability.

- We consider a result due to Aaronson [4] – showing that given an unknown n qubit state one can perform tomography that works well for most measurement settings by measuring only $O(n)$ independent and identically distributed (i.i.d.) copies of the state – and relax the assumption of having i.i.d copies of the state to merely the ability to select subsystems at random from a quantum multipartite state.

Background. An important technique in the study of entanglement are quantum versions of the de Finetti theorem, stating that an l-partite quantum state $\rho^{A_1 \cdots A_l}$ that is a reduced state of a permutation-symmetric state on $k \geq l$ subsystems is close (for $k \gg l$) to a convex combination of i.i.d. quantum states, i.e. $\rho^{A_1 \cdots A_l} \approx \int \mu(d\sigma)\sigma^{\otimes l}$ for a probability measure μ on quantum states. The quantum version appears very similar to the original de Finetti theorem [5], but it is much more remarkable. Not only it says that the correlations are arranged in an organized fashion (as a convex combination of i.i.d. states) but also that the state of l subsystems is close to a *separable*, non-entangled, state. A well-known property of entanglement is that it is monogamous: A quantum system cannot be highly entangled with a large number of other systems. The quantum de Finetti theorems provide a quantitative statement for the monogamy of entanglement; in a symmetric state all the subsystems are equally correlated with all the others and so any small number of subsystems can be only lightly entangled.

We now know several possible quantum versions of the de Finetti theorem [6–10]. A natural way to quantify the closeness to convex combinations of i.i.d. states is by the trace norm, in which case we know the bound must be at least linear in the local dimension of the state [7]. However in many applications this error is too large to be useful. One possible way forward is therefore to consider other ways of quantifying the approximation rather than the trace norm. There are two known quantum de Finetti theorems following this idea. The first is the exponential de Finetti theorem of Renner [8]. The second is the de Finetti theorem proved in Ref. [10]. Both results have found interesting applications [8, 11, 12] and [13]. These two results suggest that more quantum versions of the de Finetti theorem might exist. In [1] we show that this is indeed the case.

Another interesting approach to the study of quantum entanglement is to analyze its role in *quantum proof systems*. The goal there is to understand how useful are entangled states for convincing a verifier the truth of a mathematical statement. In [1] we consider two particular proof systems: The first is the setting of multiple provers that share entanglement and are only allowed to communicate with the verifier and not with each other [14]. The second is the setting of non-interactive multiple proof protocols with the assumption that the proofs are *not* entangled [15]. Both settings have been extensively studied in the past (see e.g. [16–26] and [2, 10, 27–38]), although there are still many interesting open questions concerning them.

Main results. A state ρ_{AB} is k-extendible if it is a reduction of a state $\rho_{AB_1\ldots B_k}$ which is permutation-symmetric in the B subsystems. The first main result of [1] reads

Theorem 1. *Let $\rho^{AB} \in \mathcal{D}(A \otimes B)$ be a k-extendible state and $\mu(m)$ a distribution over quantum operations $\{\Lambda_{A,m}\}_m$, with $\Lambda_{A,m} : \mathcal{D}(A) \to \mathcal{D}(X)$. Then*

$$\min_{\sigma \in \mathit{Sep}(A:B)} \max_{\Lambda_B \in \mathcal{M}} \mathop{\mathbb{E}}_{m \sim \mu} \left\| \Lambda_{A,m} \otimes \Lambda_B \left(\rho^{AB} - \sigma^{AB} \right) \right\|_1 \leq \sqrt{\frac{2 \ln |X|}{k}}. \tag{1}$$

We also prove a completely analogous result for non-signalling distributions. The most important aspect of the theorem is that the error term is independent of the subsystem dimensions of ρ^{AB}, and only depends on the output dimension of the family of quantum operations $\{\Lambda_{A,m}\}_m$. The de Finetti bound from Ref. [10] can be recovered (with an improved constant) as a special case of the theorem. The second main result of [1] is a generalization of the result of Ref. [10] to an arbitrary number of subsystems:

Theorem 2. *Let $\rho^{A_1 \ldots A_k} \in \mathcal{D}(A^{\otimes k})$ be permutation-invariant. Then for every there is a measure ν s.t.*

$$\max_{\Lambda_2, \ldots, \Lambda_l \in \mathcal{M}} \left\| (\mathbb{I} \otimes \Lambda_2 \otimes \ldots \otimes \Lambda_l) \left(\rho^{A_1 \ldots A_l} - \int \nu(d\sigma) \sigma^{\otimes l} \right) \right\|_1 \leq \sqrt{\frac{2 l^2 \ln |A|}{k - l}}. \tag{2}$$

The proof of both theorems are based on information theory and are significantly simpler and more direct than the arguments in [10].

Application 1: Multiple Unentangled Proofs. The first application concerns a protocol due to Chen and Drucker [2] in which a prover sends to a verifier $\sqrt{n}\,\mathrm{polylog}(n)$ unentangled quantum states, each composed of $\log(n)$ qubits, as a proof of the satisfiability of a 3-SAT instance with n variables and $O(n)$ clauses. The quantum verifier then checks the validity of the proof by performing local quantum measurements on each of the proofs and post-processing the outcomes. This result, based on the previous work [27, 28], is surprising since one can convince a verifier the satisfiability of a 3-SAT instance by sending only $\sqrt{n}\,\mathrm{polylog}(n)$ qubits! It is a natural question whether the total number of qubits could be decreased even further. We give strong evidence against any further reduction: We show that any similar protocol with $O(n^{1/2-\varepsilon})$ proofs, for any $\varepsilon > 0$, would imply in a $2^{\tilde{O}(n^{1-2\varepsilon})}$-time algorithm for 3-SAT, establishing the optimality of the protocol under the assumption [39] that there is no subexponential-time algorithms for SAT.

A related, but harder, problem is whether QMA(2) protocols can give at most a quadratic reduction in proof size with respect to QMA (by Ref. [29] we know QMA(2) gives at least a quadratic advantage over QMA, under plausible computational complexity assumptions). We conjecture that this is the case, and believe that our result gives evidence in favor of this conclusion, as well as a possible avenue towards proving it (i.e. using a further-improved de Finetti theorem).

Application 2: Non-local Games. The second application concerns the computational complexity of non-local games. We give two results in this direction. The first is algorithmic and concerns the class of free games, defined as games in which the questions to each prover are chosen independently. We show that the maximum winning probability of such games can be approximated within additive error ε in time $\exp\left(O(\log(|Q||A|)\log|Q|/\varepsilon^2)\right)$, with $|Q|$ and $|A|$ the number of questions and answers of the game, respectively, by solving a linear program. Although this is a purely classical result, we establish it by exploring a connection to non-local games: We show that for any two-player one-round free game, one can find another game on m players such that the maximum winning probability under non-signalling strategies, which can be computed by a linear program [40], gives a $(\ln|A|/(2m))^{1/2}$-additive approximation to the maximum winning probability of the original game. Since non-signalling strategies are at least as powerful as entangled strategies, the same result holds also for games in which the players share entanglement.

Using the relation above, we also show that 3-SAT on m variables can be reduced to obtaining a *constant-error* approximation of the maximum winning probability under entangled strategies of $O(\sqrt{m})$-player one-round non-local games, in which the players communicate $O(\sqrt{m})$ bits all together. Finally, we show how one would be able to get even NP-hardness of approximating the maximum winning probability under entangled strategies of a 4-player one-round game if one could strengthen the first new quantum de Finetti theorem (namely by changing the order of the expectation and the maximization in Eq. (1)). This gives a new approach to this problem, which is one of the most outstanding open questions concerning non-local games.

Application 3: Polynomial Optimization. We consider the connection [41–43] between quantum de Finetti theorems and the optimization over separable states, on one hand, and polynomial optimization and the Sum-of-Squares (Parrilo/Lasserre) hierachy, one other hand, and prove that the optimization of certain degree-d polynomials over the n-dimensional hypersphere can be performed in quasipolynomial-time in the number of variables by considering $O(\log(n)d^2)$ rounds of the Sum-of-Squares hierarchy of semidefinite programs. This result can be considered as an extension to the hypersphere of similar results for the simplex [3].

Application 4: Separability Testing. Another application is to give an algorithm for deciding separability of multipartite states which is quasi-polynomial in the local dimensions of the subsystems. Given a multipartite state $\rho_{A_1,\ldots,A_l}$, we prove one can decide whether it is fully separable or ε-away from separable in time $\exp\left(O\left(\left(\sum_k \ln|A_k|\right)^2 l^2\varepsilon^{-2}\right)\right)$, with distance measured either by the one-way LOCC norm [44] or by a multipartite version of the Frobenius norm introduced in [45]. This generalizes the findings of [13] from bipartite states to general multipartite states.

Application 5: Efficient State Tomography. A final application of the new de Finetti theorems is to quantum state tomography. The starting point is a result due to Aaronson [4], based on computational learning theory, showing that given an unknown n-qubit state one can perform tomography that works well for most measurement settings by measuring only $O(n)$ i.i.d. copies of the state. Theorem 2 allows us to relax the assumption of having i.i.d. copies of the state (which can never be fully certified), showing that the same conclusions holds true for arbitrary quantum states, as long as one can selects a few of its subsystems at random and performs the original scheme on them.

[1] Fernando G.S.L. Brandão and Aram W. Harrow. Quantum de Finetti theorems under local measurements and applications, 2012. arXiv:1210.6367.

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

[3] Victoria Powers and Bruce Reznick. A new bound for Pólya's theorem with applications to polynomials positive on polyhedra. *Journal of Pure and Applied Algebra*, 164(1–2):221–229, 2001.

[4] S. Aaronson. The learnability of quantum states. *Proc. R. Soc. A*, 463:2088, 2007. arXiv:quant-ph/0608142.

[5] P. Diaconis and D. Freedman. Finite exchangeable sequences. *Annals of Probability*, 8:745–764, 1980.

[6] Robert Koenig and Renato Renner. A de Finetti representation for finite symmetric quantum states. *J. Math. Phys.*, 46(12):122108, 2005. arXiv:quant-ph/0410229.

[7] Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. *Commun. Math. Phys.*, 273:473–498, 2007. arXiv:quant-ph/0602130.

[8] R. Renner. Symmetry implies independence. *Nature Physics*, 3:645–649, 2007. arXiv:quant-ph/0703069.

[9] Miguel Navascues, Masaki Owari, and Martin B. Plenio. The power of symmetric extensions for entanglement detection. *Phys. Rev. A*, 80:052306, 2009. arXiv:0906.2731.

[10] F. G. S. L. Brandão, M. Christandl, and J. Yard. Faithful squashed entanglement. *Commun. Math. Phys.*, 306(3):805–830, 2011. arXiv:1010.1750.

[11] R. Renner. *Security of quantum key distribution*. PhD thesis, ETHZ, Zurich, 2005. arXiv:quant-ph/0512258.

[12] Fernando G.S.L. Brandão and Martin B. Plenio. A generalization of quantum Stein's lemma. *Commun. Math. Phys.*, 295:791, 2010. arXiv:0904.0281.

[13] Fernando G.S.L. Brandão, Matthias Christandl, and Jon Yard. A quasipolynomial-time algorithm for the quantum separability problem. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 343–352, 2011. arXiv:1011.2751.

[14] Hirotada Kobayashi and Keiji Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *J. Comput. Syst. Sci.*, 66(3):429–450, May 2003. arXiv:cs/0102013.

[15] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *ISAAC*, volume 2906, pages 189–198, 2003. arXiv:quant-ph/0306051.

[16] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *CCC '04*, pages 236–249, 2004. arXiv:quant-ph/0404076.

[17] Stephanie Wehner. Entanglement in interactive proof systems with binary answers. In *STACS'06*, pages 162–171, 2006. arXiv:quant-ph/0508201.

[18] Miguel Navascués, Stefano Pironio, and Antonio Acin. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.*, 10(7):073013, 2008. arXiv:0803.4290.

[19] Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *CCC '08*, pages 199–210, 2008. arXiv:0803.4373.

[20] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. *SIAM J. Comput.*, 39(7):3207–3229, July 2010. arXiv:0710.0655.

[21] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. *SIAM J. Comput.*, 40(3):848–877, 2011. arXiv:0704.2903.

[22] Tsuyoshi Ito, Hirotada Kobayashi, Daniel Preda, Xiaoming Sun, and Andrew C. C. Yao. Generalized tsirelson inequalities, commuting-operator provers, and multi-prover interactive proof systems. In *CCC '08*, pages 187–198, 2008. arXiv:0712.2163.

[23] Tsuyoshi Ito, Hirotada Kobayashi, and Keiji Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *CCC '09*, pages 217–228, 2009. arXiv:0810.0693.

[24] Richard Cleve, Dmitry Gavinsky, and Rahul Jain. Entanglement-resistant two-prover interactive proof systems and non-adaptive pir's. *Quantum Info. Comput.*, 9(7):648–656, July 2009. arXiv:0707.1729.

[25] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *STOC '11*, pages 353–362, 2011. arXiv:1012.4728.

[26] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled

provers. In *FOCS '12*, 2012. arXiv:1207.0550.

[27] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009. arXiv:0804.0802.

[28] Hugue Blier and Alain Tapp. All languages in NP have very short quantum proofs. In *First International Conference on Quantum, Nano, and Micro Technologies*, pages 34–37, Los Alamitos, CA, USA, 2009. IEEE Computer Society. arXiv:0709.0738.

[29] Aram W. Harrow and Ashley Montanaro. An efficient test for product states, with applications to quantum Merlin-Arthur games. In *FOCS '10*, pages 633–642, 2010. arXiv:1001.0017.

[30] F.G.S.L. Brandão. *Entanglement Theory and the Quantum Simulation of Many-Body Physics*. PhD thesis, Imperial College London, 2008. arXiv:0810.0026.

[31] S. Beigi. NP vs QMA_log(2). *Quant. Inf. Comp.*, 10(1&2):0141–0151, 2010. arXiv:0810.5109.

[32] Francois Le Gall, Shota Nakagawa, and Harumichi Nishimura. On QMA protocols with two short quantum proofs. *Quant. Inf. Comp.*, 12:0589, 2012. arXiv:1108.4306.

[33] A. Chiesa and M. Forbes. Improved soundness for QMA with multiple provers, 2011. arXiv:1108.2098.

[34] S. Gharibian, J. Sikora, and S. Upadhyay. QMA variants with polynomially many provers, 2011. arXiv:1108.0617.

[35] M. McKague. On the power of quantum computation over real Hilbert spaces, 2011. arXiv:1109.0795.

[36] André Chailloux and Or Sattath. The complexity of the separable Hamiltonian problem, 2011. arXiv:1111.5247.

[37] A. Pereszlenyi. Multi-prover quantum merlin-arthur proof systems with small gap, 2012. arXiv:1205.2761.

[38] Y. Shi and X. Wu. Epsilon-net method for optimizations over separable states, 2011. arXiv:1112.0808.

[39] R. Impagliazzo, R. Paturi, and F. Zane. Which problems have strongly exponential complexity? In *FOCS'98*, pages 653–662. IEEE, 1998.

[40] Tsuyoshi Ito. Polynomial-space approximation of no-signaling provers. In *ICALP'10*, pages 140–151, 2010. arXiv:0908.2363.

[41] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. Complete family of separability criteria. *Phys. Rev. A*, 69:022308, Feb 2004. arXiv:quant-ph/0308032.

[42] Boaz Barak, Fernando G.S.L. Brandão, Aram W. Harrow, Jonathan Kelner, David Steurer, and Yuan Zhou. Hypercontractivity, sum-of-squares proofs, and their applications. In *STOC '12*, STOC '12, pages 307–326, 2012. arXiv:1205.4484.

[43] Andrew C. Doherty and Stephanie Wehner. Convergence of sdp hierarchies for polynomial optimization on the hypersphere, 2012. arXiv:1210.5048.

[44] F.G.S.L. Brandão and M. Christandl. Detection of multiparticle entanglement: Quantifying the search for symmetric extensions, 2011. arXiv:1105.5720.

[45] Cecilia Lancien and Andreas Winter. Distinguishing multi-partite states by local measurements, 2012. arXiv:1206.2884.