Noise-Tolerant Testing of High Entanglement of Formation

Rotem Arnon-Friedman[1]
ETH Zürich, Switzerland
http://rotemaf.info
rotema@itp.phys.ethz.ch

Henry Yuen[2]
UC Berkeley, USA
http://www.henryyuen.net
hyuen@cs.berkeley.edu

Abstract

In this work we construct tests that allow a classical user to certify high dimensional entanglement in uncharacterized and possibly noisy quantum devices. We present a family of non-local games $\{G_n\}$ that for all n certify states with entanglement of formation $\Omega(n)$. These tests can be derived from *any* bipartite non-local game with a classical-quantum gap. Furthermore, our tests are noise-tolerant in the sense that fault tolerant technologies are not needed to play the games; entanglement distributed over noisy channels can pass with high probability, making our tests relevant for realistic experimental settings. This is in contrast to, e.g., results on self-testing of high dimensional entanglement, which are only relevant when the noise rate goes to zero with the system's size n. As a corollary of our result, we supply a lower-bound on the entanglement cost of any state achieving a quantum advantage in a bipartite non-local game. Our proof techniques heavily rely on ideas from the work on classical and quantum parallel repetition theorems.

2012 ACM Subject Classification Theory of computation → Quantum complexity theory

Keywords and phrases device independence, quantum games, entanglement testing, noise tolerance

Digital Object Identifier 10.4230/LIPIcs.ICALP.2018.11

Related Version Full version hosted on arXiv at https://arxiv.org/abs/1712.09368.

Acknowledgements We thank Valerio Scarani for helpful pointers to the literature, Thomas Vidick for feedback on an earlier draft, and anonymous referees for helpful comments and pointing us to the work of [JPPG+10]. Work on this project initiated when RAF was visiting UC Berkeley.

1 Introduction

Non-local games offer a powerful method to experimentally study the properties and behavior of uncharacterized quantum systems. In a non-local game, an experimenter can play a game with two non-communicating players (representing spatially separated quantum systems) via classical interaction only. Based on the outcome of the game, the experimenter draws conclusions about, e.g., whether the players used an entangled quantum state to win the

[1] RAF is supported by the Swiss National Science Foundation (grant No. 200020-135048) via the National Centre of Competence in Research "Quantum Science and Technolog" and by the US Air Force Office of Scientific Research (grant No. FA9550-16-1-0245)
[2] HY is supported by ARO Grant W911NF-12-1-0541 and NSF Grant CCF-1410022.

45th International Colloquium on Automata, Languages, and Programming (ICALP 2018).
Editors: Ioannis Chatzigiannakis, Christos Kaklamanis, Dániel Marx, and Donald Sannella;
Article No. 11; pp. 11:1–11:12

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

game. This idea dates back to John Bell's seminal paper [7], in which he presents a game to test the non-classicality of nature. Today, such games are not only relevant for our understanding of the foundations of quantum physics but are at the heart of device-independent quantum information processing, where a classical user can certify that an unknown quantum device is performing a desired computational or cryptographic task (such as, e.g., device-independent quantum key distribution [4, 37, 45, 34, 2] or delegated quantum computation [42, 24, 22, 35, 17]).

In this work we ask the following question:

Is it possible to classically test for high dimensional entanglement, even in the presence of noise?

Whereas Bell's original test is a classical method to certify the *presence* of entanglement, we are instead interested in non-local games that would allow us to quantify the *amount*. In particular, we are interested in certifying the amount of entanglement of *noisy quantum systems*.

Designing noise-tolerant tests for high dimensional entanglement is an important and timely challenge for both computer science and physics. First, our understanding of complexity theory indicates that unless $\mathsf{BQP} \subseteq \mathsf{BPP}$ (i.e., quantum computers are classically simulable), general quantum computations must involve highly entangled states. Thus if we hope to achieve super-classical speedups in quantum computers, at the very least we must be able to generate high dimensional entanglement.

Second, we are seeing increasingly sophisticated experiments involving quantum information, from loophole-free Bell tests [26, 43, 23] to small scale quantum computers [10, 29]. However, full-fledged quantum fault tolerance appears to be a faraway prospect; in the near-term, our explorations of complex quantum states will be done using noisy gates and little (if any) error correction. Despite this obstacle, researchers have been enthusiastically proposing uses of noisy quantum computers, from approximate optimization to investigation of exotic physics phenomena. Interesting questions will emerge in tandem with these efforts, namely: how can one verify that a noisy quantum computer has succeeded in these proposed experiments? Finding noise-tolerant tests to certify high dimensional entanglement is a prerequisite step towards verifying other complex quantum behavior in this noisy regime.

1.1 What do we mean by certifying entanglement?

There are a variety of ways to formulate this task; our work is most directly motivated by recent work on *self-tests*, which are games that certify the presence of entanglement *of a specific form*. The works of [33, 14, 16, 20, 35] construct families of games $\{G_n\}$ where any optimal quantum strategy for G_n must use a large amount of entanglement, e.g., a tensor product of n EPR pairs. These self-testing results are also *robust*, in that near-optimal strategies must use states that are near a specific highly entangled state. However, these tests will also reject a natural class of highly entangled states such as $\sigma^{\otimes n}$ where σ has fidelity $1-\nu$ with a single EPR pair. Here, think of ν as a small (but fixed) noise parameter that represents the level of imperfection of a state preparation process.

Thus, even though $|EPR\rangle\langle EPR|^{\otimes n}$ can be used to pass the tests of [33, 14, 16, 20, 35] with high probability, the "similar-looking" state $\sigma^{\otimes n}$ will fail with high probability. A key observation we wish to emphasize in this paper is that robustness of a self-test is *not* equivalent to noise tolerance!

More formally, the robust self-tests in the above works show the following: let $\mathrm{qval}(G_n)$ denote the optimal quantum winning probability for the game G_n. Then there exists a

function $f(n,\varepsilon)$ and an *ideal state* ρ_n^* such that for all ε, any quantum strategy that achieves a winning probability of at least $\text{qval}(G_n)-\varepsilon$ must use a state ρ that is $f(n,\varepsilon)$-close to ρ_n^*. In these works, ρ_n^* is a state whose entanglement grows with n (like a maximally entangled state on n qubits). "Closeness" can be defined in terms of the fidelity of the two states up to local isometries acting on each of the players' systems.

Given a game G_n as above, an experiment to test the entanglement of an unknown state ρ can be the following: play the game G_n using ρ, and check whether the game is won.[3] In order to obtain a non-trivial guarantee about ρ, we require that $f(n,\varepsilon)<1$; one can think of this function as specifying the amount of experimental imperfection/noise that can be tolerated by the *test* itself. In the works of [33, 14, 16, 20], the function $f(n,\varepsilon)$ scales as $a\cdot n^b\cdot\varepsilon^c$ for constants a,b,c. Thus we get no guarantees about ρ unless ε scales as $1/\operatorname{poly}(n)$. In other words, as we increase the amount of entanglement we want to certify, the test becomes less tolerant of noise!

The strongest self-testing result (in this context) is presented in the work of Natarajan and Vidick [35]. There, a self-test for n EPR pairs is given where the associated function is $f(n,\varepsilon)=O(\sqrt{\varepsilon})$. While the closeness parameter is independent of the parameter n, such $f(n,\varepsilon)$ still requires that, in order to pass the test with high probability, the players share a state ρ that is *globally* $O(\sqrt{\varepsilon})$-close to $|EPR\rangle\langle EPR|^{\otimes n}$. Using a state like $\sigma^{\otimes n}$ where σ has $1-\nu$ fidelity with a single EPR pair would fail their test with high probability, because $\sigma^{\otimes n}$ has *exponentially small* fidelity $(1-\nu)^n\approx e^{-n/\nu}$ with $|EPR\rangle\langle EPR|^{\otimes n}$.

In this paper we seek an entanglement test that is both *sound* — meaning that any strategy that passes the test with good probability must have high entanglement — and also *noise tolerant*, meaning that they do not reject noisy implementations of an ideal strategy. The self-tests above are sound, but they are not noise tolerant. Part of the difficulty stems from the fact that it is not even clear how one should *formulate* the soundness guarantee of a desired noise-tolerant self-testing result.

1.2 Noise model

As discussed above, we wish to define a testing procedure that can also certify entanglement in noisy entangled states. While our work can be used to certify different types of noisy states, we briefly discuss a specific noise model here for the sake of concreteness. The noise model that we have in mind produces a state of the form $\sigma^{\otimes n}$ where each σ has fidelity $1-\nu$ with some optimal state defined via the considered non-local game. Such a state can be produced, e.g., by sending many copies of the optimal state via noisy channels.

We emphasize that by saying that this is the noise model that we consider we merely mean that we require that our tests will be able to certify the entanglement of $\sigma^{\otimes n}$. However, we do not assume that all of the states on which the procedure is applied must have this form (i.e., the soundness part of the statement is independent of the considered noise model).

1.3 Results and contributions

In this work, instead of trying to certify the presence of a specific state like in self-testing statements, we address the question of certifying an entanglement measure. This allows us to sidestep the difficulty of formulating a noise-tolerant self-testing result.

[3] In an experiment one actually needs to prepare many identical and independent copies of ρ and play the game G_n many times. Then the average winning probability can be calculated, and high amount of entanglement is certified (with high probability) if the average winning probability is at least $\text{qval}(G_n)-\varepsilon$.

We present a family of simple non-local games $\{G_n\}$ where each game G_n certifies that the shared state of the players has $\Omega(n)$ bits of *entanglement of formation*. The entanglement of formation, denoted by $E_F(\rho)$, is a well-studied entanglement measure for bipartite mixed states that, in the case of pure states, is equal to the entanglement entropy. As the name suggests, the entanglement of formation captures, roughly speaking, the amount of entanglement needed in order to produce a given state ρ. It is also closely related to another important, perhaps more well known, entanglement measure which will be of use below – the *entanglement cost* $E_C(\rho)$. The entanglement cost of a mixed state roughly describes how many EPR pairs are needed to create ρ via local operations and classical communication [9]. We provide a more thorough discussion of the entanglement measures relevant for our work in Section 1.4.

The family of non-local games that we consider are the so called *threshold games*. Before stating our main result, we define these games. Let G be a two-player non-local game with classical value[4] $\mathrm{cval}(G)$ and quantum value $\mathrm{qval}(G)$. Given an integer $n \geq 1$ and a noise threshold $0 \leq \nu < \mathrm{qval}(G) - \mathrm{cval}(G)$, define the threshold game $G^n_{\mathrm{qval}(G)-\nu}$ to be a game where the two-players now play n independent instances of G in parallel, and win if they win at least $\mathrm{qval}(G) - \nu$ fraction of instances of G.

The main theorem of this paper is as follows:

▶ **Theorem 1** (Main theorem). *Let G be a two-player game with a classical-quantum gap: i.e., $\Delta := \mathrm{qval}(G) - \mathrm{cval}(G) > 0$. Let $0 \leq \nu < \Delta$ be a noise parameter.*

Completeness (Noise tolerance). *Let $n \geq 1$ be an integer. Consider a quantum strategy for G that succeeds with probability $\mathrm{qval}(G) - \eta$ for $0 \leq \eta < \nu$. Playing this strategy n times independently in parallel in the threshold game $G^n_{\mathrm{qval}(G)-\nu}$ succeeds with probability at least $1 - \exp(-(\nu - \eta)^2 n/3)$.*[5]

Soundness (Entanglement certification). *There exist constants $0 < c_1, c_2 < 1$ such that for sufficiently large $n > \frac{1}{c_1}$, any strategy that wins the threshold game $G^n_{\mathrm{qval}(G)-\nu}$ with probability $\kappa \geq \exp(-c_1 n)$ must use a quantum state ρ such that its entanglement of formation satisfies $E_F(\rho) \geq c_2 \kappa^2 n$.*

The constants c_1, c_2 depend only on Δ, ν, and the number of possible answers in G.

To gain a better understanding of our theorem we now give an example. Consider the famous CHSH game, which has classical value $\mathrm{cval}(CHSH) = 3/4$ and quantum value $\mathrm{qval}(CHSH) \approx 0.854$. Any strategy for winning a single instance of CHSH with probability $\mathrm{qval}(CHSH) - \eta$ for some parameter $0 \leq \eta < 0.1$ must use some entangled state σ. An "honest" strategy for playing the threshold game $CHSH^n_{.854-2\eta}$ would be to play each instance of $CHSH$ independently using $\sigma^{\otimes n}$ as the entangled resource state. Via a simple Chernoff-Hoeffding bound it is easy to see that this strategy will pass $CHSH^n_{.854-2\eta}$ with overwhelming probability. Thus this game is noise-tolerant. The entanglement of formation of $\sigma^{\otimes n}$ is indeed $\Omega(n)$.

But what about other strategies? Is there a state with entanglement of formation $o(n)$ that can be used to win $CHSH^n_{.854-2\eta}$ sufficiently well? Theorem 1 shows that this is not possible.

---

[4] The classical value of a game is the maximum winning probability when the players employ classical strategies, i.e., do not use entanglement. Similarly, the quantum value of a game is the optimal winning probability when using quantum strategies.

[5] Alternatively, a simpler (but slightly weaker) statement is that playing a strategy the succeeds with probability $\mathrm{qval}(G) - \nu$ in G n times independently in parallel succeeds in the threshold game $G^n_{\mathrm{qval}(G)-\nu}$ with probability $\frac{1}{2}$. This is sufficient for an experiment certifying entanglement.

We list several features of Theorem 1:

1. It holds for *any* two-player game G. In other words, any game with a classical-quantum gap can be "lifted" to another game that tests for large entanglement in a noise-tolerant manner.
2. The players are able to pass our test with high probability by holding a tensor product of noisy few-qubit states (such as $\sigma^{\otimes n}$ where σ has fidelity $1-\nu$ with an EPR pair for any amount). The theorem gives non-trivial guarantees for any $0 \leq \nu < \mathrm{qval}(G) - \mathrm{cval}(G)$, i.e., it is robust to *any* amount of noise up to the classical limit.
3. It gives non-trivial guarantees even for strategies whose success probability is far from optimal; for any constant κ, Theorem 1 still guarantees that $E_F(\rho) \in \Omega(n)$.[6]

Theorem 1 thus shows that by playing the simple threshold game $G^n_{\mathrm{qval}(G)-\nu}$ with an uncharacterized device we can classically test for large amounts of entanglement (as measured by the entanglement of formation), even when the device is highly noisy, as current devices are. As far as we are aware, previous results [33, 14, 16, 35, 18] cannot be used to derive conclusions which are quantitively strong as Theorem 1, even when considering more complex games and proof techniques.[7]

Our main theorem presented above can be easily used to derive another quantitive relation between the advantage in a non-local game G and the *entanglement cost* required to achieve this advantage. Specifically, we prove the following.

▶ **Theorem 2.** *Let G be a two-player game with a classical-quantum gap: i.e., $\Delta := \mathrm{qval}(G) - \mathrm{cval}(G) > 0$. Let $0 \leq \nu < \Delta$ be a noise parameter. Then, for any state σ that can be used to win G with probability at least $\mathrm{qval}(G) - \nu$, its entanglement cost satisfies $E_C(\sigma) \geq c_2/4$, where c_2 is the constant from Theorem 1.*

Put in other words: the minimum entanglement cost[8] needed to obtain a super-classical success probability in a non-local game only depends on the classical-quantum gap as well as the number of possible answers in the game.

As we explain in Section 1.4, even given the full description of a state σ, calculating $E_C(\sigma)$ is not easy and no "single letter" formula is known to describe it. Theorem 2 gives a simple lower bound on $E_C(\sigma)$ in terms of σ's advantage in any non-local game G.

The only lower-bound with a similar flavour which was known before is the one given in [46]. There, a (tight) relation between $E_F(\sigma)$ and σ's winning probability in the CHSH game was derived. Self-testing results can, of course, also be used to achieve similar bounds (by taking into account the continuity of the considered entanglement measures), but so far most of the results are non-trivial for a very limited amount of noise and only apply to specific two-player games. In contrast, Theorem 2 holds for any non-local game and amount of noise.

1.4 Why entanglement of formation?

In this section we motivate and explain the relations between the entanglement measures certified by our tests in Theorem 1 and Theorem 2.

[6] However, the constants c_1 and c_2 are probably not optimal and can be improved.

[7] This is not to say that our work supersedes the mentioned works; these derived self-testing statements which certify the *state* and not just its *entanglement* as we do here.

[8] For any σ, $E_F(\sigma) \geq E_C(\sigma)$. Thus, Theorem 2 could have been phrased in terms of the entanglement of formation as well.

Myriad entanglement measurements have been studied by researchers, each possessing various properties [38, 28]. For pure bipartite states $|\psi\rangle^{\mathsf{AB}}$, the coarsest quantity describing entanglement is the *entanglement rank*, which is simply the Schmidt rank of $|\psi\rangle$. However, this is not a very useful measure of entanglement as one can have a state arbitrarily close to a product state, yet have high entanglement rank.

A more natural measure of entanglement is the *entanglement entropy* $E(\psi)$, which is the von Neumann entropy of the reduced density matrix of $|\psi\rangle$ on system A or equivalently B [8, 39]. In fact, the entanglement entropy is the *unique* entanglement measure for pure bipartite states that satisfies a few natural axioms, such as monotonicity under local operations and classical communication (LOCC) and asymptotic continuity [28].

For mixed states the situation is more complicated — there is no clear "best" entanglement measure. The most natural and operational entanglement measures are considered to be the *entanglement cost* E_C and the *distillable entanglement* E_D. In fact, for any entanglement measure M satisfying some natural properties we have that $E_D \leq M \leq E_C$ [28]. Thus the entanglement cost and distillable entanglement are in a sense "extremal" entanglement measures. For pure states, both E_C and E_D are equal to the entanglement entropy.

In the following we focus on E_C. Informally, the entanglement cost of a bipartite quantum state ρ_{AB} describes the number of maximally entangled states required to produce ρ using only LOCC. As LOCC cannot increase entanglement, the pre-shared maximally entangled states describe the sole source of entanglement in such a process and hence quantify how entangled ρ is in a meaningful way.[9]

Formally, the entanglement cost is defined as the following asymptotic quantity:

$$E_C(\rho) = \inf\left\{ r : \lim_{n\to\infty} \left(\inf_{\Lambda} \|\rho^{\otimes n} - \Lambda(\Phi^+_{2^{rn}})\|_1 \right) = 0 \right\} ,$$

where the infimum ranges over all LOCC maps Λ and $\Phi^+_{2^{rn}}$ is the maximally entangled state of rank 2^{rn}. That is, it is the maximal possible rate r at which one can convert $\Phi^+_{2^{rn}}$ into $\rho^{\otimes n}$ with vanishing error in the limit $n \to \infty$.

Computing $E_C(\rho)$ is considered to be a difficult task in general. Due to this reason one usually considers a closely related entanglement measure called the *entanglement of formation*. It is formally defined as follows [9]:

$$E_F(\rho) = \inf\left\{ \sum_i p_i E(\Psi_i) : \rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i| \right\} .$$

That is, $E_F(\rho)$ is the minimum average entanglement entropy over all pure-state decompositions of ρ.

The entanglement of formation derives its relevance from its relation to the entanglement cost $E_C(\rho)$ discussed above. It describes the rate in which maximally entangled states are converted to ρ using a specific type of LOCC protocols [51] (whereas $E_C(\rho)$ is the minimum over all LOCC protocols). Furthermore, [25] showed that the entanglement cost is equal to the *regularised* entanglement of formation:

$$E_C(\rho) = E_F^{\infty}(\rho) = \lim_{n\to\infty} (E_F(\rho^{\otimes n})/n).$$

[9] Another way of thinking about the operational meaning of entanglement cost is by considering the task of entanglement dilution. There, the goal is to start with initial noiseless entanglement and dilute it to create a target state ρ using LOCC.

For some time it was conjectured that the entanglement of formation is additive and hence $E_C(\rho) = E_F(\rho)$. Today it is known that this is not the case and that the limit in the above equation is needed in general [11].

It is not known how to compute $E_F^\infty(\rho)$ for general ρ, in part because of the infinite limit. The "single-letter" quantity $E_F(\rho)$ does not appear to be much easier to compute because of the minimisation over all possible decompositions of ρ. To date, it can be done only for states with high symmetry [44, 48] or of low dimension [49, 50, 3]. One can imagine that the task of calculating or bounding $E_F(\rho)$ only becomes harder if one does not have full information about ρ as in the scenario considered in the current work.

In the light of the above, one can see our work as giving a way to lower bound those complex entanglement measures for an unknown state ρ in a device-independent manner. Of course, this is not a general method that works for all states ρ, but rather it works for any state ρ that can be used to gain an advantage in non-local games (or, in other words, violate some Bell inequality). Specifically, Theorem 1 gives a lower bound on E_F for high dimensional (while perhaps noisy) states that can be used to pass the threshold game $G^n_{\mathrm{qval}(G)-\nu}$ for some two-player game G. Theorem 2 gives a lower bound on E_C for any state achieving a quantum advantage in a two-player game G. In particular, for any given state one can choose the game G such that the lower bounds on E_F and E_C are maximal.

1.5 Proof technique

The proof idea is simple: if the entanglement of formation of the players' shared state in the threshold game $G^n_{\mathrm{qval}(G)-\nu}$ is $o(n)$ and the players win with non-negligible probability, then this strategy can be transformed into a strategy for the original game G that uses *no* entanglement, yet still wins with probability strictly greater than $\mathrm{cval}(G)$, which would be a contradiction.

This is argued as follows. Consider a two-player game G where the first player receives a question x and produces answer a, and the second player receives question y and responds with answer b. The players win if $V(x, y, a, b) = 1$ for some predicate V. Let $\mathrm{qval}(G) > \mathrm{cval}(G)$.

Now suppose there is a quantum strategy that wins $G^n_{\mathrm{qval}(G)-\nu}$ with decent probability. A simple probabilistic argument implies that conditioned on an event E of winning roughly $\mathrm{qval}(G) - \nu$ fraction of some subset $S \subseteq [n]$ of instances, the players will win the j'th instance with probability close to $\mathrm{qval}(G)$, for an average $j \in [n]$. Another way of phrasing this statement is: Let $(\mathbf{X}_j, \mathbf{Y}_j)$ denote the questions to the two players in the j'th instance of G, and let $(\mathbf{A}_j, \mathbf{B}_j)$ denote their answers. Let $\mathsf{P}_{\mathbf{X}_j\mathbf{Y}_j\mathbf{A}_j\mathbf{B}_j|E}$ denote the joint distribution of questions and answers of the j'th coordinate in this hypothetical strategy, conditioned on the event E. Then sampling a tuple $(\mathbf{X}_j, \mathbf{Y}_j, \mathbf{A}_j, \mathbf{B}_j)$ from $\mathsf{P}_{\mathbf{X}_j\mathbf{Y}_j\mathbf{A}_j\mathbf{B}_j|E}$ will satisfy the game predicate V with probability $\mathrm{qval}(G) - \varepsilon > \mathrm{cval}(G)$.

Next, we will prove the following three statements (roughly speaking): (1) $\mathsf{P}_{\mathbf{X}_j\mathbf{Y}_j|E} \approx \mathsf{P}_{\mathbf{X}_j\mathbf{Y}_j}$, (2) $\mathsf{P}_{\mathbf{A}_j|\mathbf{X}_j\mathbf{Y}_jE} \approx \mathsf{P}_{\mathbf{A}_j|\mathbf{X}_jE}$, and (3) $\mathsf{P}_{\mathbf{B}_j|\mathbf{X}_j\mathbf{Y}_j\mathbf{A}_jE} \approx \mathsf{P}_{\mathbf{B}_j|\mathbf{Y}_jE}$, where "$\approx$" denotes closeness in statistical distance. Notice that without the conditioning event E, the first item would be trivial and the second item would follow exactly from the non-signaling condition between the players. To prove the third item, we use the fact that the hypothetical strategy for the threshold game uses $o(n)$ bits of entanglement; intuitively this implies that each instance of G can only use $o(1)$ bits of entanglement.

Putting these three items together, we obtain a classical strategy for G: the first player receives question $\mathbf{X}_j$, and samples an answer $\mathbf{A}_j$ from the distribution $\mathsf{P}_{\mathbf{A}_j|\mathbf{X}_jE}$. The second player receives question $\mathbf{Y}_j$ and samples from $\mathsf{P}_{\mathbf{B}_j|\mathbf{Y}_jE}$. The joint distribution of their questions and answers will be close to $\mathsf{P}_{\mathbf{X}_j\mathbf{Y}_j\mathbf{A}_j\mathbf{B}_j|E}$, but that implies that they will win G with probability $\mathrm{qval}(G) - \varepsilon > \mathrm{cval}(G)$, which is a contradiction.

The proof strategy and the techniques used are heavily inspired by the proofs of the *parallel repetition theorem* in classical complexity theory [41, 27, 40], and subsequently the work on the *quantum parallel repetition problem*. This problem asks for a bound on $\mathrm{qval}(G^n)$ if $\mathrm{qval}(G) < 1$, where G^n is like the threshold game except we demand that the players win *all* instances of G. It is conjectured that $\mathrm{qval}(G^n)$ decays exponentially with n, although the best general upper bound is that $\mathrm{qval}(G^n)$ decays polynomially with n when $\mathrm{qval}(G) < 1$ [52]. Nearly all of the works that study the quantum parallel repetition problem [30, 15, 5, 6] share the proof strategy of transforming a "too-good-to-be-true" strategy for the repeated game G^n into a "too-good-to-be-true" strategy for the single game G, namely a quantum strategy with success probability better than $\mathrm{qval}(G)$, a contradiction. These works all use information-theoretic machinery in the proof, and in this work we use the same tools.

The full proof can be found at `https://arxiv.org/abs/1712.09368`.

1.6 Related work

Our work is the first that addresses directly the question of certifying the entanglement of formation of high dimensional states in a noise-tolerant way (while the case of a single CHSH game was already considered in [46] as mentioned above).

Any robust self-testing result can be used to certify any continuous entanglement measures (e.g. the entanglement of formation); but as explained before, such results cannot accommodate the kinds of noise considered here. In addition to the self-testing results mentioned before [33, 14, 16, 20, 35, 18], the only other self-testing result that certifies asymptotically growing amounts of entanglement is from the work of Reichardt, Unger and Vazirani [42], who show how to verify quantum computations using classical resources only. At the heart of their result is a *sequential* protocol where the experimenter plays many rounds of the CHSH game with the two players in order to certify the presence of many EPR pairs. However, like the other self-testing results, the protocol of [42] is also not noise-tolerant in the sense considered here.

If one cares just about certifying high *entanglement rank* of a state (rather than certifying an entanglement measure such as E_F, or precisely characterizing the state as in self-testing), then we can combine the following two independent results to address the question of noise-tolerant, device-independent testing of asymptotically growing amounts of entanglement: The work of [40] shows that the *classical* value of a threshold game $G^n_{\mathrm{cval}(G)+\delta}$ decays exponentially fast with n (if $\mathrm{cval}(G) < 1$). The work of [31] shows that the maximum quantum success probability in a game F using dimension-d entanglement is at most $d\,\mathrm{cval}(F)$. Letting F be a threshold game, we obtain that d must be exponentially large in any quantum strategy whose winning probability is say at least a small constant. Since the threshold game is noise-tolerant (i.e. it can be won with high probability with noisy strategies), this gives a noise-tolerant test for *entanglement rank*. This same argument can be modified to show that the 1/2-*Rényi entropy* of the state[10] must be linear in n.

Our test lower bounds a stronger entanglement measure, the entanglement of formation, which in the pure state case is the entanglement entropy and therefore a lower bound on the 1/2-Rényi entropy. There can be arbitrarily large gaps between the von Neumann entropy and the 1/2-Rényi entropy of a pure state.

[10] The 1/2-Rényi entropy of a pure state $|\psi\rangle$ is $2\log(\sum_i \lambda_i^{1/2})$ where λ_i are the eigenvalues of the reduced density matrix of $|\psi\rangle$ on either side.

The broader goal of certifying the dimension of a quantum system in a device-independent manner has been heavily studied under the heading of *dimension witnesses*. Much of the work on dimension witnesses has focused on finding Bell inequalities such that achieving the optimal violation requires an entangled state of a certain dimension [12, 36, 13]. Many of these works construct and design dimension witnesses using a combination of analytical and numerical techniques.

1.7 Future work

Some open problems and future directions include:

1. Quantitatively improve our results. The constants c_1, c_2 in Theorem 1 are small; for the CHSH game, the constant c_1 is on the order of 10^{-6} and thus in order for our Theorem to give any guarantees, $\sim 10^6$ CHSH games would have to be played. Even though recent experiments are capable of producing such a large amount of states (in [32], for example, order of 10^{10} signals were produced), an improvement of the constants can lead to the ability of certifying *much* more entanglement in such experiments. Our analysis is likely far from tight and significant quantitative improvements can probably be gained by tailoring the analysis to a specific game, such as the CHSH game.
2. To get a non-trivial bound on the entanglement of formation, this requires that the success probability κ is at least $\sim 1/\sqrt{n}$. Can this dependence on κ be improved?
3. Can one prove a version of Theorem 1 for some non-local games G that allows one to lower bound other measures of entanglement, such as distillable entanglement[11] or quantum conditional entropy? The results of [47, 21] indicate that this cannot be done for arbitrary amount of noise for all games since there are Bell inequalities that can be violated while using states with un-distillable entanglement or positive conditional entropy.
4. Can one prove a self-testing result for a growing number of EPR pairs that is also noise-tolerant in the sense described above? A concrete goal would be to characterize all near-optimal strategies for the threshold game $CHSH^n_{.854-\nu}$. The results of [19] hint that by sticking to the current measures of distance considered in self-testing results any characterization of near-optimal strategies for $CHSH^n_{.854-\nu}$, in the regime of high amount of noise, must include also non-entangled states. Hence, we do not expect self-testing results (as they are phrased today) to allow for certification of entanglement in the presence of arbitrary noise using threshold games.

References

1 Rotem Arnon-Friedman and Jean-Daniel Bancal. Device-independent certification of one-shot distillable entanglement. *arXiv*, 2017.

2 Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *arXiv preprint arXiv:1607.01797*, 2016.

3 Koenraad Audenaert, Frank Verstraete, and Bart De Moor. Variational characterizations of separability and entanglement of formation. *Physical Review A*, 64(5):052304, 2001.

4 Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, 2005.

[11] In a related work by Jean-Daniel Bancal together with one of the current authors a device-independent protocol certifying a lower bound on the one shot distillable entanglement is given. The considered setting and type of statement are different than the ones presented here. For further details see [1].

5 Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Parallel repetition via fortification: analytic view and the quantum case. *arXiv preprint arXiv:1603.05349*, 2016.

6 Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Hardness amplification for entangled games via anchoring. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 303–316, 2017.

7 John S Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3), 1964.

8 Charles H Bennett, Herbert J Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53(4):2046, 1996.

9 Charles H Bennett, David P DiVincenzo, John A Smolin, and William K Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824, 1996.

10 Sergio Boixo, Sergei V Isakov, Vadim N Smelyanskiy, Ryan Babbush, Nan Ding, Zhang Jiang, John M Martinis, and Hartmut Neven. Characterizing quantum supremacy in near-term devices. *arXiv preprint arXiv:1608.00263*, 2016.

11 Fernando GSL Brandao and Michał Horodecki. On Hastings' counterexamples to the minimum output entropy additivity conjecture. *Open Systems & Information Dynamics*, 17(01):31–52, 2010.

12 Nicolas Brunner, Stefano Pironio, Antonio Acin, Nicolas Gisin, André Allan Méthot, and Valerio Scarani. Testing the dimension of Hilbert spaces. *Physical review letters*, 100(21):210503, 2008.

13 Yu Cai, Jean-Daniel Bancal, Jacquiline Romero, and Valerio Scarani. A new device-independent dimension witness and its experimental implementation. *Journal of Physics A: Mathematical and Theoretical*, 49(30):305301, 2016.

14 Rui Chao, Ben W Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *arXiv preprint arXiv:1610.00771*, 2016.

15 Kai-Min Chung, Xiaodi Wu, and Henry Yuen. Parallel repetition for entangled k-player games via fast quantum search. In *the 30th Conference on Computational Complexity (CCC)*, pages 512–536, 2015.

16 Andrea Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Information and Computation*, 17(9-10):831–865, 2017.

17 Andrea Coladangelo, Alex Grilo, Stacey Jeffery, and Thomas Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. *arXiv preprint arXiv:1708.07359*, 2017.

18 Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint arXiv:1709.09267*, 2017.

19 Tim Coopmans. Robust self-testing of (almost) all pure two-qubit states. Master's thesis, Universiteit van Amsterdam, 2017.

20 Matthew Coudron and Anand Natarajan. The parallel-repeated magic square game is rigid. *arXiv preprint arXiv:1609.06306*, 2016.

21 Nicolai Friis, Sridhar Bulusu, and Reinhold A Bertlmann. Geometry of two-qubit states with negative conditional entropy. *Journal of Physics A: Mathematical and Theoretical*, 50(12):125301, 2017.

22 Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17(8):083040, 2015.

23 Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Physical review letters*, 115(25):250401, 2015.

24 Michal Hajdušek, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Device-independent verifiable blind quantum computation. *arXiv preprint arXiv:1502.02563*, 2015.

25 Patrick M Hayden, Michal Horodecki, and Barbara M Terhal. The asymptotic entanglement cost of preparing a quantum state. *Journal of Physics A: Mathematical and General*, 34(35):6891, 2001.

26 Bas Hensen, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, RFL Vermeulen, RN Schouten, C Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

27 Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. *Theory of Computing*, 5(8):141–172, 2009. doi:10.4086/toc.2009.v005a008.

28 Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

29 IBM. IBM quantum experience. URL: https://www.research.ibm.com/ibm-q/.

30 Rahul Jain, Attila Pereszlényi, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. In *Proceedings of Conference on Computational Complexity (CCC)*, pages 209–216, 2014.

31 Marius Junge, Carlos Palazuelos, David Pérez-García, Ignacio Villanueva, and Michael M Wolf. Unbounded violations of bipartite Bell inequalities via operator space theory. *Communications in Mathematical Physics*, 300(3):715–739, 2010.

32 Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li, et al. High speed self-testing quantum random number generation without detection loophole. In *Frontiers in Optics*, pages FTh2E–1. Optical Society of America, 2017.

33 Matthew McKague. Self-testing in parallel. *New Journal of Physics*, 18(4):045013, 2016.

34 Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 417–426. ACM, 2014.

35 Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015. ACM, 2017.

36 Károly F Pál and Tamás Vértesi. Quantum bounds on Bell inequalities. *Physical Review A*, 79(2):022120, 2009.

37 Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

38 Martin B Plenio and Shashank Virmani. An introduction to entanglement measures. *arXiv preprint quant-ph/0504163*, 2005.

39 Sandu Popescu and Daniel Rohrlich. Thermodynamics and the measure of entanglement. *Physical Review A*, 56(5):R3319, 1997.

40 Anup Rao. Parallel repetition in projection games and a concentration bound. *SIAM Journal on Computing*, 40(6):1871–1891, 2011.

41 Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

42 Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

43 Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.

44 Barbara M Terhal and Karl Gerd H Vollbrecht. Entanglement of formation for isotropic states. *Physical Review Letters*, 85(12):2625, 2000.

45 Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical review letters*, 113(14):140501, 2014.

46 Frank Verstraete and Michael M Wolf. Entanglement versus Bell violations and their behavior under local filtering operations. *Physical review letters*, 89(17):170401, 2002.

47 Tamás Vértesi and Nicolas Brunner. Disproving the Peres conjecture: Bell nonlocality from bipartite bound entanglement. *arXiv preprint arXiv:1405.4502*, 2014.

48 Karl Gerd H Vollbrecht and Reinhard F Werner. Entanglement measures under symmetry. *Physical Review A*, 64(6):062307, 2001.

49 William K Wootters. Entanglement of formation of an arbitrary state of two qubits. *Physical Review Letters*, 80(10):2245, 1998.

50 William K Wootters. Entanglement of formation and concurrence. *Quantum Information & Computation*, 1(1):27–44, 2001.

51 William K. Wootters. Entanglement of formation. In Prem Kumar, Giacomo M D'Ariano, and Osamu Hirota, editors, *Quantum Communication, Computing and Measurement 2*, pages 69–74. Springer, 2002.

52 Henry Yuen. A parallel repetition theorem for all entangled games. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 77:1–77:13, 2016.