Constant-sized robust self-tests for states and measurements of unbounded dimension

Laura Mančinska, Jitendra Prakash, Christopher Schafhauser

Background

One of the key tasks in the development of quantum technologies is the certification of quantum devices. This ensures that the devices are performing according to their specification. One of the ways such certification may be carried out is by using *self-testing* methods which enable us to infer the quantum-mechanical description of a device merely from classical observations (measurement statistics). We can then treat these devices as black boxes as we need not trust the inner workings of the system, a scenario which one refers to as *device-independence*. Beginning with [MY04], in which the term was first coined, self-testing has found many applications, such as *device-independent quantum cryptography* [MY98, MY04], *delegated quantum computation* [CGJV19], *entanglement detection* [BvCA18a, BvCA18b], investigating the structure of the *quantum correlation set* [CS17, GKW$^+$18], and novel advances in *quantum complexity theory* [FJVY19, NV18, NW19]. Self-testing is also one of the ingredients behind the recent breakthrough result establishing that $\mathrm{MIP}^* = \mathrm{RE}$ [JNV$^+$20]; which further implies a negative answer to the celebrated *Connes' embedding problem* [Con76] from the theory of von Neumann algebras.

A general scenario of self-testing is the following. Suppose that spatially separated agents, Alice and Bob, share a quantum state ψ and each one of them has a quantum measurement device. The device has n measurement settings with k outcomes each. Alice and Bob randomly pick settings v and w, respectively. Alice gets an outcome i, and similarly, Bob gets an outcome j after performing their measurements. Performing such measurements many times and with all the settings, they can estimate $p(i, j|v, w)$ which is the conditional probability that they get outcomes i and j upon performing measurement v and w, respectively. For certain correlations $p(i, j|v, w)$, it is possible to *essentially* identify what the shared state ψ and the measurements must have been. We then say that the correlation $p(i, j|v, w)$ *self-tests* the state ψ and the corresponding measurements. In practice, Alice and Bob can never learn the correlation $p(i, j|v, w)$ exactly. In addition, any real-world devices are bound to have some imperfections. Therefore, we are interested in *robust* self-testing which guarantees that the only way to produce correlation close to $p(i, j|v, w)$ is by sharing a state close to ψ and performing measurements that are close to the reference ones.

Often times self-testing results are proven using ad-hoc techniques, which means that to obtain new results one essentially has to start from scratch. One notable exception is an approach that uses perturbative representation theory of groups to establish robust self-testing [Vid18, CS17, CMMN20]. The basic idea is that in the ideal case one deduces algebraic relations which the measurement operators must satisfy on the quantum state. One then associates a suitable finite group such that one gets a representation of the group. This transfers to the well-studied field of the representation theory of finite groups and the problem reduces to identifying suitable irreducible representations of the group. In the robust case, one gets approximate versions of the algebraic relations which yield "approximate" representations of the group (with respect to state-dependent distance). A key tool used in the approximate case is the Gowers–Hatami theorem [GK17, Gow17, Vid18] which relates an "approximate" representation of a group to a representation of that group in some suitable sense. A caveat to this approach is that, in general, it is far from clear what group should be associated to the algebraic relations identified and if this is at all possible. In fact, it would be more natural to associate an *algebra* rather than a group to these algebraic relations. Moreover, there are known families of non-local games whose optimal strategies do not have an apparent underlying group yet an underlying algebra can easily be identified (for example, consider binary constraint system games [CM14] beyond linear ones, synchronous games [PSS+16, HMPS19], graph homomorphism [MR16] and isomorphism games [AMR+19]).

One of our main contributions is that we showcase how the above general method for self-testing from this *group-theoretic* framework can be lifted to an *algebraic-theoretic* framework. Instead of seeking an appropriate group to associate with the algebraic relations, we simply work with the algebra generated by those relations. To accomplish this, a major step is to obtain some sort of analogue of Gowers–Hatami theorem for algebras. We showcase how this can be done for a particular algebra but the approach can be easily generalized. However, our analogue has a non-constructive (ϵ,δ)-dependence which is the most pressing question raised by the current work.

Results

In this work, we prove that certain quantum strategies constructed from projections which sum up to some particular scalar times identity can be robustly self-tested from the quantum correlations that they induce. Specifically, we begin with $d \times d$ projections $\widetilde{P}_1, \ldots, \widetilde{P}_n$ ($n \geq 3$) such that $\widetilde{P}_1 + \cdots + \widetilde{P}_n = xI_d = (b/d)I_d$ (where $\gcd(b, d) = 1$) for some specific scalar $x \in \mathbb{R}$. The scalar x and the projections $\widetilde{P}_1, \ldots, \widetilde{P}_n$ have the property that whenever $P_1, \ldots, P_n$ are any other projections such that $P_1 + \cdots + P_n = xI$, then $P_i = I \otimes \widetilde{P}_i$ for all $1 \leq i \leq n$ in some basis. In other words, $\widetilde{P}_1, \ldots, \widetilde{P}_n$ constitute an *irreducible* set up to unitary equivalence. For example,

Example 1. Take any $n \geq 3$ and consider n unit vectors $\xi_1, \ldots, \xi_n$ in $\mathbb{R}^{n-1}$ which form the vertices of a regular n-simplex centered at the origin. Then their corresponding projections $\widetilde{P}_i = \xi_i \xi_i^*$ form an irreducible representation of the relation $P_1 + \cdots + P_n = \frac{n}{n-1} I$ [KRS02].

It turns out that for each $n \geq 3$ there is a countable set Λ_n of rationals x for which there exists a unique, up to unitary equivalence and taking direct sums, set of n finite-dimensional projections whose sum is xI. In particular, $\Lambda_3 = \{\frac{3}{2}\}$ while for $n \geq 4$ we have $\Lambda_n = \{x_k\}_{k=0}^{\infty}$ where $x_0 = 0$, and $x_k = 1 + \frac{1}{n-1-x_{k-1}}$ for all $k \geq 1$. The description of admissible scalars x, construction of projections summing up to scalar x , and their representation theory is given in [KRS02].

For $n \geq 3$ and $x \in \Lambda_n$, and $\widetilde{P}_1, \ldots, \widetilde{P}_n$ as above, we define a quantum strategy

$$\widetilde{\mathscr{S}_{n,x}} = (\varphi_d \in \mathbb{C}^d \otimes \mathbb{C}^d, \{\widetilde{P}_v, I_d - \widetilde{P}_v\}_{v=1}^n, \{\widetilde{P}_w^T, I_d - \widetilde{P}_w^T\}_{w=1}^n),$$

where $\varphi_d = \frac{1}{\sqrt{d}} \sum_i e_i \otimes e_i$ is the maximally entangled state. Let $\widetilde{p}_{n,x}$ denote the quantum correlation induced by $\widetilde{\mathscr{S}_{n,x}}$.

Our main result states that if we have a a quantum strategy $\mathscr{S}$ which induces a quantum correlation p close to the ideal correlation $\widetilde{p}_{n,x}$, then the strategy $\mathscr{S}$ must be close to the ideal quantum strategy $\widetilde{\mathscr{S}_{n,x}}$, in the sense made precise as follows.

Theorem. *Let $n \geq 3$, $x \in \Lambda_n$ and let $\widetilde{P}_1, \ldots, \widetilde{P}_n$ be projections as above. For any $\epsilon \geq 0$, there exists a $\delta \geq 0$ such that the following holds. Let p be a quantum correlation induced from an arbitrary quantum strategy*

$$\mathscr{S} = (\psi \in \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}, \{E_v, I_{d_A} - E_v\}_{v=1}^n, \{F_w, I_{d_B} - F_w\}_{w=1}^n),$$

such that $\|\widetilde{p}_{n,x} - p\| \leq \delta$. Then $\mathscr{S}$ is approximately related to $\widetilde{\mathscr{S}_{n,x}}$ via a local isometry, that is, there exist isometries $V_A \colon \mathbb{C}^{d_A} \to \mathbb{C}^d \otimes \mathbb{C}^{r_A}$ and $V_B \colon \mathbb{C}^{d_B} \to \mathbb{C}^d \otimes \mathbb{C}^{r_B}$ for some $r_A, r_B \in \mathbb{N}$ and a quantum state

$\psi_{\text{junk}} \in \mathbb{C}^{r_A} \otimes \mathbb{C}^{r_B}$ *such that for all* $1 \leq v, w \leq n$,

$$(V_A \otimes V_B)(E_v \otimes F_w)\psi \approx_\epsilon (\widetilde{P}_v \otimes \widetilde{P}_w^T)\varphi_d \otimes \psi_{\text{junk}},$$
$$(V_A \otimes V_B)\psi \approx_\epsilon \varphi_d \otimes \psi_{\text{junk}}.$$

For the proof, we show that Alice's measurements form an "approximate" representation of the relation $p_1 + \cdots + p_n = xI$, that is, the measurements are approximately projective $\|E_v - E_v^2\|_{\rho_A} \approx 0$, and $\|(E_1 + \cdots + E_n) - xI_{d_A}\|_{\rho_A} \approx 0$. (Here $\|.\|_{\rho_A}$ is the state-dependent norm defined by $\|X\|_{\rho_A}^2 := \mathrm{Tr}(X^* X \rho_A)$ where $\rho_A := \mathrm{Tr}_B(\psi\psi^*)$.) The key ingredient which relates an "approximate" representation to an exact one via an isometry is the following analogue of Gowers–Hatami. The proof exploits the simple representation theory of the algebra generated by projections $\{\widetilde{P}_v\}_{v=1}^n$.

Theorem. *(Informal) Suppose positive semi-definite matrices* $E_1, \ldots, E_n \in \mathbb{M}_{d_A}$ *are "approximate" projections and form an "approximate" representation (with respect to* ρ_A*) of the relation* $p_1 + \cdots + p_n = xI$*. Then, there exists an isometry* $V\colon \mathbb{C}^{d_A} \to \mathbb{C}^d \otimes \mathbb{C}^{r_A}$ *such that for all* $1 \leq v \leq n$*, we have* $\|E_v - V^*(\widetilde{P}_v \otimes I_s)V\|_{\rho_A} \approx 0$.

Before we discuss the implications of our main theorem, let us take a look at the following special case:

Example 2. Let $n = 4$. For any $k \in \mathbb{N}$, there exists four rank k projections $\widetilde{P}_{k,1}, \widetilde{P}_{k,2}, \widetilde{P}_{k,3}, \widetilde{P}_{k,4}$ in $\mathbb{M}_{2k+1}$ such that $\widetilde{P}_{k,1} + \widetilde{P}_{k,2} + \widetilde{P}_{k,3} + \widetilde{P}_{k,4} = \frac{4k}{2k+1} I_{2k+1}$ [KRS02]. By our main theorem, we can robustly self-test each of the strategies

$$\widetilde{\mathscr{S}_k} = (\varphi_{2k+1}, \{\widetilde{P}_{k,v}, I_{2k+1} - \widetilde{P}_{k,v}\}_{v=1}^4, \{\widetilde{P}_{k,w}^T, I_{2k+1} - \widetilde{P}_{k,w}^T\}_{w=1}^4),$$

from the correlations $\widetilde{p}_{4,k}$ that each strategy induces.

In comparison to measurements, self-testing of quantum states is relatively well understood. For example, we know that any (pure) bipartite entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$ can be self-tested from a correlation with 3 inputs and d outputs [CGS17]. For applications, it would be efficient to have small-sized correlations that robustly self-test states with large dimensions. The only family of *constant-size* self-tests for states (or measurements) of arbitrarily large dimension has been reported just last year in [Fu19]. They show that for each $d \in \mathscr{D}$, where $\mathscr{D}$ is an infinite subset of the primes, the maximally entangled state $\varphi_{4(d-1)}$ can be robustly self-tested from correlations with roughly 100 questions per party. Example 2 yields the following corollary which complements the result in [Fu19], but with correlations of significantly smaller size:

Corollary 3. *For each odd dimension* $d \geq 3$*, the maximally entangled state* φ_d *can be robustly self-tested by quantum correlations with four inputs and two outputs.*

Furthermore, we also robustly self-test the measurements in Example 2. To the best of our knowledge, this is the first example of self-testing of measurements with rank higher than one. In addition, this is the first example, where measurements of arbitrarily large dimension are self-tested from constant-size correlations.

Corollary 4. *Given any natural number* k *there exist four projections of rank* k *which can be robustly self-tested by quantum correlations with four inputs and two outputs.*

Most of the known self-tests for *infinite families* of measurements are for tensor-products of Pauli matrices (for example, [NV17, Col17]) or Clifford unitaries [CGJV19]. There are a few results which are different from these, for instance, [SSKA19]. Our main theorem yields another example of an infinite family of measurements that goes beyond a tensor-product of Paulis or Clifford unitaries.

References

[AMR$^+$19] Albert Atserias, Laura Mančinska, David E. Roberson, Robert Šámal, Simone Severini, and Antonios Varvitsiotis. Quantum and non-signalling graph isomorphisms. *Journal of Combinatorial Theory, Series B*, 136:289 – 328, 2019.

[BvCA18a] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Device-independent entanglement certification of all entangled states. *Phys. Rev. Lett.*, 121:180503, Oct 2018.

[BvCA18b] J. Bowles, I. Šupić, D. Cavalcanti, and A. Acín. Self-testing of pauli observables for device-independent entanglement certification. *Phys. Rev. A*, 98:042336, Oct 2018.

[CGJV19] A. Coladangelo, A. B. Grilo, S. Jeffery, and T. Vidick. Verifier-on-a-leash: new schemes for verifiable delegated quantum computation, with quasilinear resources. In *Advances in cryptology—EUROCRYPT 2019. Part III*, volume 11478 of *Lecture Notes in Comput. Sci.*, pages 247–277. Springer, Cham, 2019.

[CGS17] A. Coladangelo, K. T. Goh, and V. Scarani. All pure bipartite entangled states can be self-tested. *Nature Communications*, 8(1), May 2017.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In *Proceedings of the 41st International Colloquium on Automata, Languages, and Programming*, ICALP '14, pages 320–331. 2014.

[CMMN20] D. Cui, A. Mehta, H. Mousavi, and S. S. Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4:346, October 2020.

[Col17] A. Coladangelo. Parallel self-testing of (tilted) EPR pairs via copies of (tilted) CHSH and the magic square game. *Quantum Inf. Comput.*, 17(9-10):831–865, 2017.

[Con76] A. Connes. Classification of injective factors. Cases II_1, II_∞, III_λ, $\lambda \neq 1$. *Ann. of Math. (2)*, 104(1):73–115, 1976.

[CS17] A. Coladangelo and J. Stark. Robust self-testing for linear constraint system games. *arXiv e-prints*, page arXiv:1709.09267, September 2017.

[FJVY19] J. Fitzsimons, Z. Ji, T. Vidick, and H. Yuen. Quantum proof systems for iterated exponential time, and beyond. In *STOC'19—Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 473–480. ACM, New York, 2019.

[Fu19] H. Fu. Constant-sized correlations are sufficient to robustly self-test maximally entangled states with unbounded dimension. *arXiv e-prints*, page arXiv:1911.01494, November 2019.

[GK17] U. T. Gauèrs and O. Khatami. Inverse and stability theorems for approximate representations of finite groups. *Mat. Sb.*, 208(12):70–106, 2017.

[GKW$^+$18] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y-C. Liang, and V. Scarani. Geometry of the set of quantum correlations. *Phys. Rev. A*, 97:022104, Feb 2018.

[Gow17] W. T. Gowers. Generalizations of Fourier analysis, and how to apply them. *Bull. Amer. Math. Soc. (N.S.)*, 54(1):1–44, 2017.

[HMPS19] J. W. Helton, K. P. Meyer, V. I. Paulsen, and M. Satriano. Algebras, synchronous games, and chromatic numbers of graphs. *New York J. Math.*, 25:328–361, 2019.

[JNV$^+$20] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen. MIP*=RE. *arXiv e-prints*, page arXiv:2001.04383, January 2020.

[KRS02] S. A. Kruglyak, V. I. Rabanovich, and Yu. S. Samoĭlenko. On sums of projections. *Funktsional. Anal. i Prilozhen.*, 36(3):20–35, 96, 2002.

[MR16] Laura Mančinska and David E. Roberson. Quantum homomorphisms. *Journal of Combinatorial Theory, Series B*, 118:228 – 267, 2016.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 503–509, 1998.

[MY04] D. Mayers and A. Yao. Self testing quantum apparatus. *Quantum Inf. Comput.*, 4(4):273–286, 2004.

[NV17] A. Natarajan and T. Vidick. A quantum linearity test for robustly verifying entanglement. In *STOC'17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015. ACM, New York, 2017.

[NV18] A. Natarajan and T. Vidick. Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *59th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2018*, pages 731–742. IEEE Computer Soc., Los Alamitos, CA, 2018.

[NW19] A. Natarajan and J. Wright. NEEXP is contained in MIP*. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, November 2019.

[PSS$^+$16] V. I. Paulsen, S. Severini, D. Stahlke, I. G. Todorov, and A. Winter. Estimating quantum chromatic numbers. *J. Funct. Anal.*, 270(6):2188–2222, 2016.

[SSKA19] S. Sarkar, D. Saha, J. Kaniewski, and R. Augusiak. Self-testing quantum systems of arbitrary local dimension with minimal number of measurements. *arXiv e-prints*, page arXiv:1909.12722, September 2019.

[Vid18] T. Vidick. Quantum multiplayer games, testing and rigidity. `http://users.cms.caltech.edu/~vidick/notes/ucsd/ucsd_games.pdf`, 2018. [Online; accessed 15-November-2020].