Optimal Robust Self-Testing by Binary Nonlocal XOR Games

Carl A. Miller[1] and Yaoyun Shi[2]

1 **Electrical Engineering and Computer Science Department**
University of Michigan
2260 Hayward St. Ann Arbor, MI 48109 USA carlmi@umich.edu
2 **Electrical Engineering and Computer Science Department**
University of Michigan
2260 Hayward St. Ann Arbor, MI 48109 USA shiyy@umich.edu

Abstract

Self-testing a quantum apparatus means verifying the existence of a certain quantum state as well as the effect of the associated measuring devices based only on the statistics of the measurement outcomes. Robust (i.e., error-tolerant) self-testing quantum apparatuses are critical building blocks for quantum cryptographic protocols that rely on imperfect or untrusted devices. We devise a general scheme for proving optimal robust self-testing properties for tests based on nonlocal binary XOR games. We offer some simplified proofs of known results on self-testing, and also prove some new results.

1998 ACM Subject Classification F.1.1 Models of Computation

Keywords and phrases self-testing, quantum cryptography, random number generation, nonlocal games

Digital Object Identifier 10.4230/LIPIcs.TQC.2013.254

1 Introduction

Consider a quantum apparatus with a classical input/output interface, and suppose that the internal behavior of the apparatus — the quantum state inside and the measurements selected by the classical input — cannot be trusted to conform to a desired specification. The apparatus is said to be *self-testing* [8], if there exists a self-test, i.e., a set of constraints on the input-output correlations, that once satisfied will guarantee the accuracy to the specification.

The notion of quantum self-testing was explicitly formulated by Mayers and Yao [8], who pointed out its importance for quantum cryptography: self-testing enables quantum cryptographic protocols that rely on imperfect or untrusted quantum devices. Such protocols were advanced in the recent thrust of research on *device-independent* quantum cryptography [1, 15, 9, 14, 6, 5, 18].

Multiple self-testing results are known. Such results are often based on nonlocal games. Popescu and Rohrlich [16] proved that any state that achieves a maximal violation of the CHSH inequality [3] must be equivalent to a direct sum of singlets. A self-testing result was proved for the GHZ paradox by Colbeck [4].

In order for self-testing to be practically useful, it must tolerate error. That is, an apparatus close to passing the self-test must be close to the specification. Robust self-testing results have been proved in [7, 10, 12, 11, 17]. These papers include two recent results which prove robust self-testing for the CHSH game [11, 17].

8th Conference on Theory of Quantum Computation, Communication and Cryptography.
Editors: Simone Severini and Fernando Brandao; pp. 254–262


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

Existing proofs of self-testing are fairly lengthy and technical, and appear specific to the underlying (class of) quantum states. Also, there is some variation in the error terms afforded by these results. Some of the results on nonlocal games show that if the score achieved is within ϵ of a passing score, the deviation of the apparatus from perfect behavior is no more than $C\sqrt{\epsilon}$. For other results (e.g., in [10, 11]) the error term is $C\epsilon^{1/4}$. It is natural to ask whether these error bounds can be tightened.

Most existing self-tests are based on binary nonlocal XOR games. In this paper, working within this class, we provide a simple criterion which determines whether a particular game is a robust self-test. The criterion guarantees an error term of $C\sqrt{\epsilon}$, which is easily seen to be the best possible (up to the constant C). The criterion is fairly simple to check, it encompasses known results on the CHSH game and the GHZ paradox, and it allows the proof of new results.

The starting point of our theory is the idea, first observed by Werner and Wolf [19], that the optimal score for a binary nonlocal XOR game can be expressed as the maximum of a certain multivariable sinusoidal function. In the present paper, we take the idea a step further and show that the robust self-testing property can be checked using the local and global properties of this function.

We will begin with some definitions and then state our main results. The results are stated initially for multiqubit states only, and a higher-dimensional generalization is given at the end of the paper. The proofs are sketched here—full proofs can be found in [13]. We offer some examples. We give a simple proof that the CHSH game is a robust self-test. (This result improves on the error term in [11], and it matches that of the independent work [17].) We also augment a recent paper [2] on randomness and quantum correlations by showing that a certain one-parameter family of games satisfies the robust self-testing condition.

2 Definitions

For our purposes, a *binary nonlocal XOR game* is simply a function $f\colon \{0,1\}^n \to \mathbb{R}$. The function f describes a scoring rule for the game: if the input sequence is $(i_1, i_2, \ldots, i_n)$, and the output sequence satisfies $\oplus_k o_k = 0$, then the score is $f(i_1, i_2, \ldots, i_n)$; if the input sequence is $(i_1, i_2, \ldots, i_n)$ and the output sequence satisfies $\oplus_k o_k = 1$, then the score is $-f(i_1, i_2, \ldots, i_n)$.

To any nonlocal game f, let us associate a polynomial $P_f\colon \mathbb{C}^n \to \mathbb{C}$ like so: for any n-tuple $(\lambda_1, \ldots, \lambda_n)$ of complex numbers, let $P_f(\lambda_1, \ldots, \lambda_n)$ be equal to

$$\sum_{(i_1,\ldots,i_n)\in\{0,1\}^n} f(i_1, \ldots, i_n)\lambda_1^{i_1}\lambda_2^{i_2}\cdots\lambda_n^{i_n}. \tag{1}$$

For example, if g is the CHSH game ($g(1,1) = -1$, $g(0,0) = g(0,1) = g(1,0) = 1$) then

$$P_g = 1 + \lambda_1 + \lambda_2 - \lambda_1\lambda_2. \tag{2}$$

Additionally, for any binary nonlocal XOR game $f\colon \{0,1\}^n \to \mathbb{R}$, and any real numbers $\theta_0, \theta_1, \ldots, \theta_n$, let $Z_f(\theta_0, \ldots, \theta_n)$ denote the quantity

$$\sum_{(i_k)\in\{0,1\}^n} f(i_1, \ldots, i_n)\cos\left(\theta_0 + \sum_k i_k\theta_k\right). \tag{3}$$

Thus,

$$Z_g(\theta_0, \theta_1, \theta_2) = \cos(\theta_0) + \cos(\theta_0 + \theta_1) + \cos(\theta_0 + \theta_2) - \cos(\theta_0 + \theta_1 + \theta_2). \tag{4}$$

Note that the function Z_f is 2π-periodic in every variable.

The two quantities P_f and Z_f are related by the following identity.

$$Z_f(\theta_0, \ldots, \theta_n) \quad = \quad \mathrm{Re}[e^{i\theta_0} P_f(e^{i\theta_1}, \ldots, e^{i\theta_n})]. \tag{5}$$

Note also that

$$\left|P_f\left(e^{i\theta_1}, \ldots, e^{i\theta_n}\right)\right| \quad = \quad \max_{t\in[-\pi,\pi]} Z_f(t, \theta_1, \ldots, \theta_n). \tag{6}$$

3 Quantum strategies

For our purposes, a *quantum strategy* for a binary n-player nonlocal game is a pure state

$$|\psi\rangle \in \mathcal{Q}_1 \otimes \mathcal{Q}_2 \otimes \ldots \otimes \mathcal{Q}_n, \tag{7}$$

where each $\mathcal{Q}_j$ is a finite-dimensional Hilbert space, together with two projective measurements

$$\left\{P_j^{(0,+)}, P_j^{(0,-)}\right\}, \left\{P_j^{(1,+)}, P_j^{(1,-)}\right\} \tag{8}$$

on the space $\mathcal{Q}_j$. These measurements can be more compactly expressed as Hermitian operators:

$$M_j^{(0)} \quad := \quad P_j^{(0,+)} - P_j^{(0,-)} \tag{9}$$

$$M_j^{(1)} \quad := \quad P_j^{(1,+)} - P_j^{(1,-)} \tag{10}$$

The *score* for such a strategy is

$$\langle\psi| \sum_{(i_k)} f(i_1, \ldots, i_n) M_1^{(i_1)} \otimes \ldots \otimes M_n^{(i_n)} |\psi\rangle . \tag{11}$$

Let us use the term *qubit strategy* to refer to a strategy whose Hilbert spaces $\mathcal{Q}_j$ are all copies of $\mathbb{C}^2$ and whose projection operators $P_j^{(i,*)}$ are all one-dimensional projectors.

For any nonlocal game f, let q_f denote the highest possible score for f that can be achieved by a qubit strategy. This quantity has a relationship to the functions Z_f and P_f which was proved in [19]. For the benefit of our exposition, we include a proof here.

▶ Proposition 1. Let $f\colon \{0,1\}^n \to \mathbb{R}$ be a nonlocal binary XOR game. Then,

$$q_f = \max_{|\lambda_1|=\ldots=|\lambda_n|=1} |P_f(\lambda_1, \ldots, \lambda_n)| \tag{12}$$

and

$$q_f = \max_{\theta_0,\ldots,\theta_n\in[-\pi,\pi]} Z_f(\theta_0, \ldots \theta_n). \tag{13}$$

Proof. Let $\left(\psi, \left\{\{M_j^{(0)}, M_j^{(1)}\}\right\}_j\right)$ be a qubit strategy for f. Each of the operators $M_j^{(i)}$ is a Hermitian operator on a 2-dimensional space that has eigenvalues in the set $\{-1, +1\}$. After an appropriate change of basis, we may make the assumption that

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad M_j^{(1)} = \begin{bmatrix} 0 & e^{i\theta_j} \\ e^{-i\theta_j} & 0 \end{bmatrix} \tag{14}$$

for some $\theta_0, \ldots, \theta_n \in [-\pi, \pi]$.

The score for this quantum strategy is clearly bounded by the operator norm of the operator

$$\mathbf{M} := \sum_{(i_k)} f(i_1, \ldots, i_n) M_1^{(i_1)} \otimes \ldots \otimes M_n^{(i_n)} \tag{15}$$

The operator $\mathbf{M}$ is on a Hilbert space which has basis $\{|a_1 a_2 \ldots a_n\rangle \mid a_i \in \{0,1\}\}$. If we take the elements of this basis in lexicographical order, the resulting matrix expression is a reverse-diagonal matrix:

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & * \\ 0 & 0 & \ldots & * & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & * & \ldots & 0 & 0 \\ * & 0 & \ldots & 0 & 0 \end{bmatrix} \tag{16}$$

The entries along the reverse diagonal are given by the expressions

$$P_f\left(e^{i(-1)^{a_1}\theta_1}, \ldots, e^{i(-1)^{a_n}\theta_n}\right) \tag{17}$$

for $(a_k) \in \{0,1\}^n$.

Using the simple observation that the eigenvalues of any matrix of the form

$$\begin{bmatrix} & & & & & & z_1 \\ & & & & & z_2 & \\ & & & & \iddots & & \\ & & & z_n & & & \\ & & \overline{z_n} & & & & \\ & \iddots & & & & & \\ \overline{z_2} & & & & & & \\ \overline{z_1} & & & & & & \end{bmatrix}, \tag{18}$$

are $\pm|z_1|, \pm|z_2|, \ldots, \pm|z_n|$, we find that the operator norm of $\mathbf{M}$ is

$$\max_{(a_i)\in\{0,1\}^n} \left| P_f\left(e^{i(-1)^{a_1}\theta_1}, \ldots e^{i(-1)^{a_n}\theta_n}\right)\right|. \tag{19}$$

Formula (12) follows. Formula (13) follows also via equality (5). ◀

4 Self-testing

Let f be a binary nonlocal XOR game. Let us say that f is a *self-test* if the following condition holds:

(*) There is a single optimal qubit strategy $(\phi, \{M_j^{(0)}, M_j^{(1)}\}_j)$ such that for any other optimal qubit strategy $(\psi, \{N_j^{(0)}, N_j^{(1)}\}_j)$, there exist unitary matrices $U_j \colon \mathbb{C}^2 \to \mathbb{C}^2$ such that

$$(U_1 \otimes U_2 \otimes \ldots \otimes U_n)\psi = \phi \tag{20}$$

and

$$U_j N_j^{(i)} U_j^\dagger = M_j^{(i)} \tag{21}$$

for all $i \in \{0,1\}$, $j \in \{1, 2, \ldots, n\}$.

▶ Proposition 2. Let $f\colon \{0,1\}^n \to \mathbb{R}$ be a nonlocal binary XOR game. Then f is a self-test if and only if the following two conditions hold:

1. There exists a maximum $(\alpha_0, \ldots, \alpha_n)$ of f such that none of $\alpha_1, \ldots, \alpha_n$ is a multiple of π.
2. Every other maximum of f is congruent modulo 2π to either $(\alpha_0, \ldots, \alpha_n)$ or $(-\alpha_0, \ldots, -\alpha_n)$.

Proof. Suppose that f satisfies both of these conditions. Let

$$\phi = \frac{1}{\sqrt{2}} \left(|00\ldots0\rangle + \frac{P_f(\alpha_1, \ldots, \alpha_n)}{|P_f(\alpha_1, \ldots, \alpha_n)|} |11\ldots1\rangle \right).$$

Suppose that $(\psi, \{\{M_j^{(0)}, M_j^{(1)}\}\}_j)$ is an optimal qubit strategy for f. After a unitary change of basis, we may assume that the operators $M_j^{(i)}$ have the form

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad M_j^{(1)} = \begin{bmatrix} 0 & e^{i\theta_j} \\ e^{-i\theta_j} & 0 \end{bmatrix}, \tag{22}$$

with $(\theta_j) \in [-\pi, \pi]^n$, and we may make the additional assumption that the vectors $(\alpha_1, \ldots, \alpha_n)$ and $(\theta_1, \ldots, \theta_n)$ lie in the same quadrant. (That is, for every $j \in \{1, 2, \ldots, n\}$, $\theta_j \alpha_j \geq 0$.)

Again we let

$$\mathbf{M} = \sum_{(i_k)} f(i_1, \ldots, i_n) M_1^{(i_1)} \otimes \ldots \otimes M_n^{(i_n)}. \tag{23}$$

Since the chosen strategy is optimal, by formula (19) we must have $(\theta_1, \ldots, \theta_n) = (\alpha_1, \ldots, \alpha_n)$. Moreover, the vector ψ must lie in the eigenspace corresponding to the largest eigenvalue of $\mathbf{M}$. This eigenspace is spanned by ϕ. We conclude that f is a self-test.

It is easy to show that if f fails to satisfy either of the two conditions of the theorem, then there exist multiple optimal strategies for f which are inequivalent. ◀

The reader may note one consequence of this proof: if a binary XOR game f is a self-test, then all optimal qubit-strategies for f use states that are equivalent to the GHZ state $\frac{1}{\sqrt{2}}(|00\ldots0\rangle + |11\ldots1\rangle)$.

5 Robustness

Let us say that two qubit strategies $(\psi, \{\{N_j^{(0)}, N_j^{(1)}\}\}_j)$ and $(\gamma, \{\{S_j^{(0)}, S_j^{(1)}\}\}_j)$ are δ-*close* if

$$\|\psi - \gamma\| \leq \delta \tag{24}$$

and

$$\left\| N_j^{(i)} - S_j^{(i)} \right\| \leq \delta \tag{25}$$

for all $j \in \{1, 2, \ldots, n\}$ and $i \in \{0, 1\}$. Let us say that a binary nonlocal XOR game $f\colon \{0,1\}^n \to \mathbb{R}$ is a *second-order robust self-test* if both condition (*) and the following condition hold:

(**) There exists a constant $C > 0$ such that any qubit strategy whose score is within ϵ of the optimal score is $(C\sqrt{\epsilon})$-close to an optimal qubit strategy.

The next proposition uses the concept of a Hessian matrix. For any twice-differentiable function $G\colon \mathbb{R}^m \to \mathbb{R}$ and any element $\mathbf{c} = (c_1, \ldots, c_m) \in \mathbb{R}^m$, let

$$\mathrm{Hess}_{\mathbf{c}}(G) = \left[\frac{\partial^2 G}{\partial x_i \partial x_j}(\mathbf{c}) \right]_{i,j}. \tag{26}$$

The Hessian matrix can be used to calculate the second derivatives of the function G in any direction. When the function G is such that the Hessians at all of its maxima are nonsingular (meaning that all second-derivatives at maxima are negative) the function has the property that near-maxima tend to lie close to true maxima. This fact is the basis for the following proposition, which is proved in full detail in the supplementary information of [13].

▶ Proposition 3. Let $f\colon \{0,1\}^n \to \mathbb{R}$ be a binary nonlocal XOR game. Then f is a second-order robust self-test if and only if the conditions of Proposition 2 are satisfied and the Hessian matrix of Z_f at $(\alpha_0, \ldots, \alpha_n)$ is nonsingular. ◀

Proof sketch. Let $\mathbb{T}$ be the set of all n-qubit strategies $\left(\psi, \left\{\{M_j^{(0)}, M_j^{(1)}\}\right\}_j\right)$ which are such that the operators $M_j^{(i)}$ have the form

$$M_j^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad M_j^{(1)} = \begin{bmatrix} 0 & e^{i\theta_j} \\ e^{-i\theta_j} & 0 \end{bmatrix} \tag{27}$$

$(j = 1, \ldots, n)$ and the state ψ has the form

$$\psi \quad = \quad \frac{1}{\sqrt{2}} \left(|00\ldots0\rangle + e^{i\theta_0} |11\ldots1\rangle \right) \tag{28}$$

with $\theta_j \in [-\pi, \pi]$. Direct calculation shows that the score for such a strategy is given by $Z_f(\theta_0, \ldots, \theta_n)$. The Hessian assumption implies that f is a second-order robust self-test within the class $\mathbb{T}$.

Let $\mathbb{S}$ be the set of all n-qubit strategies $\left(\phi, \left\{\{M_j^{(0)}, M_j^{(1)}\}\right\}_j\right)$ such that the operators $M_j^{(i)}$ have the form (27) and the state ϕ is permitted to be any n-qubit state satisfying $\langle \phi \,|\, 00\ldots0\rangle \geq 0$. Then, it can be shown that there exists a constant $K > 0$ such that any n-qubit strategy in $\mathbb{S}$ which achieves a score of $q_f - \epsilon$ must be $(K\sqrt{\epsilon})$-close to some n-qubit strategy in $\mathbb{T}$ which achieves an equal or higher score. As a consequence, robust self-testing holds within the class $\mathbb{S}$ as well. The proof is then completed by the observation that any qubit strategy is equivalent under local unitary transformations to a strategy in $\mathbb{S}$. ◀

6 Examples

It is easy to show that the function Z_g (4) corresponding to the CHSH game has two maxima: $(-\frac{\pi}{4}, \frac{\pi}{2}, \frac{\pi}{2})$ and $(\frac{\pi}{4}, -\frac{\pi}{2}, -\frac{\pi}{2})$. The Hessian matrices at these maxima are both equal to

$$\left(-\frac{1}{\sqrt{2}}\right) \begin{bmatrix} 4 & 2 & 2 \\ 2 & 2 & 1 \\ 2 & 1 & 2 \end{bmatrix}, \tag{29}$$

which is a nonsingular matrix. Therefore, the CHSH game is a second-order robust self-test.

Let d be the 3-player GHZ game:

$$\begin{aligned} Z_d(\theta_0, \theta_1, \theta_2, \theta_3) \quad = \quad & \cos(\theta_0) - \cos(\theta_0 + \theta_1 + \theta_2) \\ & - \cos(\theta_0 + \theta_2 + \theta_3) - \cos(\theta_0 + \theta_1 + \theta_3). \end{aligned}$$

It easy to show that the maxima of this function are $(0, \pm\frac{\pi}{2}, \pm\frac{\pi}{2}, \pm\frac{\pi}{2})$, and that the Hessian matrices at these maxima are nonsingular. Therefore the GHZ game is also a self-test that satisfies second-order robustness. (This fact can also be proved using the results on self-testing graph states in [10].)

Let us see how Proposition 3 can be used to prove new results. The recent paper [2] by Acin *et al.* considers a family of nonlocal games $\{h_\alpha \colon \{0,1\}^2 \to \mathbb{R}\}_{\alpha>1}$ defined by

$$\begin{aligned} h_\alpha(0,0) &= \alpha \quad & h_\alpha(0,1) &= \alpha \\ h_\alpha(1,0) &= 1 \quad & h_\alpha(1,1) &= -1. \end{aligned} \tag{30}$$

The authors characterize the qubit-devices that achieve an optimal score at these games, and show that these devices achieve more randomness than optimal devices for the standard CHSH inequality. The games h_α may therefore be suitable for randomness expansion. However in randomness expansion protocols, it is only possible to approximately determine the expected score of a device. Thus it is important to ask whether the games from this family satisfy robust self-testing.

With the aid of the theory in [2], one can show that the function $Z_{h_\alpha}(\theta_0, \theta_1, \theta_2)$ has two maxima in $[-\pi, \pi]^3$, and the Hessian matrices at these maxima are

$$-(1+\alpha^2)^{-1/2} \begin{bmatrix} 2\alpha^2+2 & \alpha^2+1 & 2 \\ \alpha^2+1 & \alpha^2+1 & 1 \\ 2 & 1 & 2 \end{bmatrix} \tag{31}$$

which is nonsingular for any $\alpha > 1$. Therefore, each of the games in the family $\{h_\alpha\}_{\alpha>1}$ is a second-order robust self-test.

7 General quantum strategies

Now suppose that we consider quantum strategies of arbitrary finite dimension. Whenever there are two Hermitian operators $M^{(0)}, M^{(1)}$ on a single finite-dimensional Hilbert space $\mathcal{Q}$, each having eigenvalues in the set $\{-1, 1\}$, there exists a decomposition

$$\mathcal{Q} = \bigoplus_{\ell=1}^{m} \mathcal{Q}_\ell \tag{32}$$

which is respected by both of the operators $M^{(0)}, M^{(1)}$, with $\dim \mathcal{Q}_\ell \leq 2$. This allows us to reduce general quantum strategies to n-qubit strategies. In particular, this implies that for any binary nonlocal XOR game f, the maximum score achievable by qubit strategies (q_f) is the maximum score achievable by any quantum strategy.

The following generalization of Proposition 3 follows from the above decomposition. (See [13].)

▶ Proposition 4. Let $f \colon \{0,1\}^n \to \mathbb{R}$ be a binary nonlocal XOR game which satisfies the conditions of Proposition 2 and, additionally, satisfies the condition that the Hessian matrices of the maxima of Z_f are all nonsingular. Then, there exists a constant $K > 0$ and an n-qubit state $\chi \in \left(\mathbb{C}^2\right)^{\otimes n}$ such that the following holds: for any quantum strategy

$$\Phi \in \mathcal{Q}_1 \otimes \ldots \otimes \mathcal{Q}_n \tag{33}$$

$$M_j^{(i)} \colon \mathcal{Q}_j \to \mathcal{Q}_j \tag{34}$$

achieving a score of $q_f - \epsilon$, there exist unitary embeddings $U_j \colon \mathcal{Q}_j \to \mathbb{C}^2 \otimes \mathcal{Q}'_j$ and a vector $\Gamma \in \mathcal{Q}'_1 \otimes \ldots \otimes \mathcal{Q}'_n$ such that

$$\left\| (U_1 \otimes \cdots \otimes U_n)\, \Phi - \chi \otimes \Gamma \right\| \leq K\sqrt{\epsilon}. \quad \blacktriangleleft \tag{35}$$

As in the 2-dimensional case, we can take the state χ to be the n-qubit GHZ state.

8 Conclusion

We have provided some general results which allow for easy proofs of robust self-testing in the context of nonlocal binary XOR games. A natural question is whether our results could be generalized to a larger class of games. A possible next step would be to consider games in which the score is based on the XOR of a subset of the outputs (as in the tests used [10]). It would also be interesting to explore further applications to randomness expansion.

Acknowledgements. The authors thank Ryan Landay and Evan Noon for discussions that helped with the development of this material. This research was supported in part by the National Basic Research Program of China under Awards 2011CBA00300 and 2011CBA00301, and the NSF of the United States under Awards 1017335 and 1216729.

References

1 A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

2 A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108:100402, 2012.

3 J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, October 1969.

4 R. Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006. arXiv:0911.3814.

5 R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

6 E. Hänggi. *Device-independent quantum key distribution*. PhD thesis, ETH Zurich, December 17 2010. arXiv:1012.3878.

7 F. Magniez, D. Mayers, M. Mosca, and H. Ollivier. Self-testing of quantum circuits. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part I*, volume 4051 of *Lecture Notes in Computer Science*, pages 72–83. Springer, 2006.

8 D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, pages 503–509, 1998.

9 M. McKague. Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices. *New Journal of Physics*, 11(10):103037, 2009.

10 M. McKague. Self-testing graph states. arXiv:1010.1989, 2010.

11 M. McKague, T. Z. Yang, and V. Scarani. Robust self-testing of the singlet. arXiv:1203.2976v1, 2012.

12 C. Miller and Y. Shi. Randomness expansion from the Greenberger-Horne-Zeilinger paradox, 2011. Attached as an appendix to arXiv:1207.1819v4.

13 C. Miller and Y. Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. arXiv:1207.1819v4, 2012.

14 S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010.

15 S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

16 S. Popescu and D. Rohrlich. Which states violate Bell's inequality maximally? *Physics Letters A*, 169(6):411–414, 1992.

17 B. Reichardt, F. Unger, and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. arXiv:1209.0448, 2012.

18 U. Vazirani and T. Vidick. Certifiable quantum dice. *Phil. Trans. R. Soc. A*, 370:3432, 7 2012.

19 R. Werner and M. Wolf. All-multipartite Bell-correlation inequalities for two dichotomic observables per site. *Physical Review A*, 64(3), 2001.