Lecture 3

Testing a qubit under spatial assumptions

(Comment: To insert a comment, use the macro "\com{$\cdot$}"**)**

In this lecture we introduce a new assumption in addition to our overarching assumption that all parties in a protocol can be modeled using quantum mechanics; as argued in the previous lecture additional assumptions are necessary to develop a test for a qubit with classical verifier. In physical terms our new assumption consists in requiring that the device that is being tested is made of two parts that are "physically isolated," in the sense that no communication can take place between the two parts for the duration of the protocol. For the case where the protocol consists of a single round of interaction (a question from the verifier and an answer from the prover) one can imagine enforcing this assumption by e.g. placing the provers and verifier on a line $P_1 - V - P_2$ and ensuring that the round-trip interaction between the verifier and either prover takes place sufficiently fast that the verifier is confident, based on relativistic considerations (information does not travel faster than light), that no information can be exchanged between the provers between the times when they receive their question and have to send their answer. Mathematically, the assumption is reflected by modeling the device's Hilbert space $\mathcal{H}$ as $\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ and writing that each sub-device's observables act on its Hilbert space only. Following tradition we will use the symbols A and B to denote "registers" (a word loosely used to refer to the physical substrate modeled by the mathematical Hilbert space) associated with each device and, oftentimes personify the devices as "provers" or "players" with the lovely names of "Alice' and "Bob" respectively.

As we will see in this lecture as well as in the last third of the course this assumption of "localization" allows the verifier to gain much leverage over the device. Some intuition for this may be gained from thinking about a situation where a detective (the verifier) interrogates two suspects (the provers). Clearly the detective has more leverage over the suspects if she interrogates them in isolation and cross-examines their answers. Be warned however that this intuition only goes so far, because it only explains why interactive proofs with two provers may be more powerful than single-prover interactive proofs; it does not give insight into why specifically quantum aspects of the provers may manifest themselves in this framework. The fact that quantum mechanics allows a broader set of behavior for the provers than classical mechanics does is evidenced in the EPR paradox [EPR35], whose authors puzzle over the "non-local" nature of quantum mechanics. A precise framework for describing this non-locality was set in place by Bell [Bel64] who identified simple "inequalities" that separate classical from quantum behavior in bipartite scenario. Here we take the modern tack on Bell's inequalities and introduce them directly through the framework of nonlocal games.

3.1 Nonlocal games

A non-local game is a cooperative game of imperfect information between a referee and two players. The referee is a trusted party that executes the game by sending a question to each player, collecting answers from them, and deciding whether the players' answers satisfy a winning criterion. The rules of the game (the distribution on questions used by the referee, the possible answers, the winning criterion) are public and known to the players, who cooperate in order to maximize their chances of winning. The only source of uncertainty is that each player is only revealed their question, but not the other's; this point is what makes the difference between a single-player and a multi-player game.

Remark 3.1. To make the connection with interactive proof systems of the kind that we described in the previous lecture, somewhat informally a *multi-prover interactive proof system* for a language L is specified by a collection of non-local games $\{G_x\}_{x\in\{0,1\}^*}$, one for each possibe input x. These games should have the property that if $x \in L$ then there is a strategy for the players that succeeds with high probability (this is the completeness property) and if $x \notin L$ then no strategy will make them win with high probability (the soundness property).[1] In the notes we freely interchange between the terminology of non-local games, referees and players and that of interactive proofs, verifier and prover depending on context.

One may rightfully wonder what is the benefit of associating games, or interactive proof systems, to computational problems. One element that we can point out is that a game itself is a computational problem—is the maximum winning probability high (larger than some c) or low (smaller than some s)? By providing a different, "dynamic" perspective on e.g. a 3SAT formula the framework of games has historically been instrumental in proving results in hardness of approximation for constraint satisfaction problems. In a completely different direction, they are a natural setting for cryptography where they were introduced in the context of zero-knowledge proofs.

For the sake of concreteness let us see an example. Consider the language L that is the collection of all strings x such that x represents a satisfiable 3SAT formula φ.[2] For example, φ could be "$y_1 \wedge y_2 \wedge \overline{y_3}\,\mathrm{AND}\,\overline{y_2} \wedge y_3 \wedge y_4$," which is obviously satisfiable. Since it is in general believed to be hard to determine satisfiability of such a formula, let's make the provers work and design an interactive proof systems for the hypothesis "φ is satisfiable".[3]

Here is a first candidate, which involves a single prover:

1. The verifier sends φ to the prover.[4]
2. The prover returns a $\{0,1\}$-valued assignment $(y_1, y_2, \ldots)$ to all variables in φ.
3. The verifier accepts if and only if the assignment satisfies φ.

This proof system has completeness 1 (if there is a solution, a prover that sends it will be accepted with probability 1) and soundness 0 (if there is no solution, no prover has any chance of being accepted). Unfortunately, while the verifier is more efficient than solving the formula herself (by e.g. trying out all possible

[1] For a formal connection between interactive proofs and games one would also have to insist that the games be "uniformly generated" from x, and that the verifier in each game is described by a circuit of size $\mathrm{poly}(|x|)$.

[2] In the following we use the notation φ and x interchangeably: we think of x as a string of bits and φ as a formula, but we assume fixed an efficiently computable bijection between the two.

[3] We emphasize that the goal of the proof system is not to find a more efficient method to solve the formula itself, as someone —the prover— still has to do the work. The goal rather is to provide a different framework in which to think about the complexity of the computational problem "decide if φ is satisfiable".

[4] In the theory of interactive proof systems it is always assumed that the prover has access to the instance that is being decided, so this step is not necessary.

solutions) she still has to read a lot of information in order to make her decision.[5] In keeping with our goal of making verifiers more efficient, let's see a more succinct proof system with two provers. Let φ consist of equations $E_1, \ldots, E_m$ such that E_j has the form $y_{j_1}^{c_{j_1}} \wedge y_{j_2}^{c_{j_2}} \wedge y_{j_3}^{c_{j_3}}$ with $c_j \in \{0,1\}$ and for a variable y, $y^0 = y$ and $y^1 = (1-y)$.

1. The verifier selects $j \in \{1, \ldots, m\}$ uniformly at random and $k \in \{1,2,3\}$ uniformly at random. She sends j to the first prover and j_k to the second, where j_k is the index of the k-th variable on which clause E_j acts in some canonical ordering. (Importantly, this ordering hides k, i.e. the prover only knows that its variable appears in *some* clause, but not which clause or which position the variable appears in it.)

2. The first prover returns a triple $(a_1, a_2, a_3) \in \{\pm 1\}$. The second prover returns a value $b \in \{\pm 1\}$.

3. The verifier accepts if and only if *(consistency check:)* $a_k = b$ and *(equation check:)* (a_1, a_2, a_3) satisfy clause E_j.

We make the following claim regarding completeness and soundness of this proof system:

Claim 3.2. *The two-prover proof system described above has completeness* 1 *and soundness at most* $1 - \frac{1}{3m}$*, where* m *is the number of clauses in the input formula.*

Note that while our proof system brought us gains in terms of communication, the soundness has degraded quite substantially, from 0 to $1 - \frac{1}{3m}$. It is possible to obtain improved variants of this proof system that have roughly similar communication complexity but much better soundness, say $\frac{1}{100}$ or even less. However, this requires much more work and is essentially the content of the *PCP theorem*, to which we will return in the last part of the course.

Proof. The completeness is easy to verify. For soundness, consider an arbitrary strategy for the two provers that succeeds with some probability p. In order to analyze this strategy we first need to accomplish the usual modeling step: how do we represent a two-prover strategy? The most "naïve" way to do so is to use a representation of each prover as a function from questions to answers and declare that the provers' joint strategy is the combination (direct product) of these functions: the first prover, Alice, employs a function $f_A : \{1, \ldots, m\} \to \{0,1\}^3$ and the second prover, Bob, a function $f_B : \{1, \ldots, n\} \to \{0,1\}$; their joint strategy is simply the function $f = (f_A, f_B)$ that goes from pairs of questions (x, y) in the protocol to pairs of answers (a, b). If one gives a little more thought to the question then it is not at all obvious that this is the right answer. Nevertheless, let's postpone any further thinking for now and finish the proof of the claim using this model for the provers.

Fix a strategy (f_A, f_B) of this form for the provers. We distinguish two cases. Either the strategies "match", meaning that for any clause E_j it holds that

$$f_A(j) = (f_B(j_1), f_B(j_2), f_B(j_3)) , \tag{3.1}$$

where y_{j_1}, y_{j_2}, y_{j_3} are the three variables involved in E_j. In this case we interpret the list of values $f_B(1), \ldots, f_B(n)$ as an assignment to the n variables of φ. Since by assumption φ is not satisfiable there must exist a j such that $(f_B(j_1), f_B(j_2), f_B(j_3))$ do not satisfy clause E_j. By (3.1), $f_A(j)$ does not satisfy E_j

[5] It is possible to argue that for a proof system of this form it is necessary for the prover to send a total number of bits that scales linearly with the length of an NP (i.e. non-interactive) proof for the same statement, see e.g. [GVW01].

either. Hence whenever the verifier sends a question of the form (j,k) for $k \in \{j_1, j_2, j_3\}$ the provers fail in the equation check.

In the second case, the strategies do not match, i.e. there is a pair $(j,k) \in \{1,\ldots,m\} \times \{1,2,3\}$ such that the k-th entry of $(f_A(j))$ does not match $f_B(j_k)$. In this case the provers fail in the consistency check when the question (j,k) is sent.

In all cases there is at least one question on which the provers must fail one of the verifier's checks. Since there are $3m$ possible questions in total and the verifier's distribution on them in uniform this completes the proof of the claim. □

3.2 Non-local strategies

In the proof of Claim 3.2 we were faced with the problem of modeling precisely how the assumption that the provers do not communicate affects the class of strategies that they may employ. While we dodged the question there, let's turn to it more seriously now. First of all, note that the object we are trying to represent is a family of bipartite conditional probability distributions $\{p(\cdot,\cdot|x,y)\}_{x,y\in\mathcal{X}\times\mathcal{Y}}$ over $\mathcal{A}\times\mathcal{B}$, where $\mathcal{X},\mathcal{Y}$ and $\mathcal{A},\mathcal{B}$ are finite sets of questions and answers respectively associated with each player. The question then is, *what families of bipartite conditional distributions can be generated by non-communicating provers?* (equivalently, players, devices, etc.)

3.2.1 Classical and non-signaling correlations

Let's examine two extremes. The first extreme is to require that each prover performs an entirely local computation. In this case the first prover's answer a_1 to their question x_1 is determined by a function $f_1 : \mathcal{X} \to \mathcal{A}$, and similarly for the second prover. This is the answer that we adopted in the proof of Claim 3.2. More generally, being familiar with randomized computation we could allow each prover to make use of a randomized computation, in which case their respective input-output behavior can be modeled by a family of conditional distributions $\{p_{\mathsf{A}}(\cdot|x)\}_{x\in\mathcal{X}}$ on $\mathcal{A}$, and similarly for the second prover. The joint distributions of answers that they provide to the verifier would then be required to factorize as

$$\forall (x,y) \in \mathcal{X}\times\mathcal{Y}\,, \quad \forall (a,b) \in \mathcal{A}\times\mathcal{B}\,, \qquad p(a,b|x,y) \;=\; p_{\mathsf{A}}(a|x)p_{\mathsf{B}}(b|y)\,. \tag{3.2}$$

Since we allowed randomness it may also be natural to allow the randomness to be shared, i.e. allow the more general class of distributions that can be represented as

$$\forall (x,y) \in \mathcal{X}\times\mathcal{Y}\,, \quad \forall (a,b) \in \mathcal{A}\times\mathcal{B}\,, \qquad p(a,b|x,y) \;=\; \int_\lambda p_{\mathsf{A}}(a|x,\lambda)p_{\mathsf{B}}(b|y,\lambda)d\lambda\,, \tag{3.3}$$

where λ ranges over any measurable set and for each λ, $\{p_{\mathsf{A}}(\cdot|x,\lambda)\}_{x\in\mathcal{X}}$ is a family of conditional distributions on $\mathcal{A}$, and similarly for the other prover. It is not hard to see that the proof of Claim 3.2 generalizes to this case: briefly, this is because for a strategy of the form (3.3) to succeed with probability p in the protocol it is necessary that the product strategy obtained by fixing λ succeeds with probability p for at least some choice of λ.

The second extreme is to allow the most general family of bipartite conditional distributions that does not "imply communication". A natural formalization of the latter requirement, usually referred to as the "non-signaling assumption" on p, is that for every a, x and y, y',

$$\sum_b p(a,b|x,y) \;=\; \sum_b p(a,b|x,y')\,. \tag{3.4}$$

In words, the answer a given by the first prover should have a marginal distribution that is independent of the question y given to the second prover. Of course, a symmetric condition should hold with the provers' roles exchanged.

At first it may seem that these two extreme classes "ought to" be the same. Are there distributions that satisfy (3.4) but are not of the form (3.3)? The answer is yes. Here is a simple example: let $\mathcal{X} = \mathcal{Y} = \mathcal{A} = \mathcal{B} = \{0,1\}$. For $(x,y) \neq (1,1)$ let $p(\cdot,\cdot|x,y)$ be uniform over $\{(0,0),(1,1)\}$. For $(x,y) = (1,1)$ let $p(\cdot,\cdot|x,y)$ be uniform over $\{(0,1),(1,0)\}$. It is easy to see that this distribution cannot be expressed in factorized form, or even as a convex combination of factorized forms as in (3.3). (Showing this is a good exercise which we leave to the reader.[6]) However, the distribution clearly satisfies (3.4) since all marginals are uniform. We will see another example in Section 3.3.1.

Having observed that there are at least two possible models for the "non-communicating provers," which one is it most appropriate? Conventionally we call the first model "classical" because it can be realized physically using local computation only, together with possibly a source of shared randomness. The second model is called "non-signaling" and is considered non-physical even though it does not strictly violate the no-communication assumption, because we do not have a credible physical theory in which arbitrary distributions in that model can be generated at locations that are space-time isolated (in other words, there is no physical theory that allows us to describe an experiment which would be able to generate any kind of correlation that is in principle allowed by special relativity; there are other constraints that relativity itself does not provide a means to model). Interestingly, the kind of correlations that can be generated by *quantum* provers lies strictly in-between the two extremes. Let's explore those correlations next.

3.2.2 Quantum (tensor product) correlations

The most natural way to measure spatial isolation in non-relativistic quantum mechanics is to associate a distinct Hilbert space with each device (or prover), $\mathcal{H}_\mathsf{A}$ for Alice and $\mathcal{H}_\mathsf{B}$ for Bob, such that the joint Hilbert space is $\mathcal{H} = \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. Upon receiving a question x the first prover performs a POVM $\{A_a^x\}_{a\in\mathcal{A}}$ on $\mathcal{H}_\mathsf{A}$ to obtain an outcome a that it sends back to the verifier; similarly, the second prover performs a POVM $\{B_b^y\}_{b\in\mathcal{B}}$ to obtain its answer b. The class of correlations that can be generated in this model is all families of bipartite conditional distributions that take the form

$$p(a,b|x,y) \;=\; \langle\psi| A_a^x \otimes B_b^y |\psi\rangle \;, \tag{3.5}$$

where A_a^x and B_b^y are as above and $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ is an arbitrary state. We will succinctly write $(|\psi\rangle, A, B)$ to represent a triple of a bipartite state and families of POVM measurements on each subsystem as above, and refer to such a triple as a *strategy* for a given two-player game.

Definition 3.3. Given a two-player one-round[7] game G with question sets $\mathcal{X}$ and $\mathcal{Y}$ and answer sets $\mathcal{A}$ and $\mathcal{B}$, a *strategy* for G is a triple $(|\psi\rangle, A, B)$ where $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ is a quantum state on the tensor product of finite-dimensional Hilbert spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ and $A = \{A^x\}$ and $B = \{B^y\}$ are collections of POVM $\{A_a^x\}$ and $\{A_b^y\}$ on $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ respectively, for every $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.

As a sanity check we can verify that (3.5) allows us to recover (3.3). To see this, set $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ to be separable Hilbert spaces with a basis indexed by all possible values of λ,[8] $|\psi\rangle = \sum_{\lambda\in\Omega} \sqrt{p_\lambda} |\lambda\rangle_\mathsf{A} |\lambda\rangle_\mathsf{B}$,

[6] Hint: "fix the randomness" and consider the values that each prover returns to each of their two possible questions. Show that these four values together cannot all lie exclusively among the allowed pairs for all four possible pairs of questions.

[7] A non-local game, just as an interactive proof system, can in principle involve multiple rounds of interaction. Here we always always restrict ourselves to the single-round case, that is simpler to analyze and captures everything that we need.

[8] Assume for simplicity that the probability space is countable.

$A_a^x = \sum_\lambda p_{\mathsf{A}}(a|x,\lambda)|\lambda\rangle\langle\lambda|_{\mathsf{A}}$, and similarly for B_b^y. One immediately verifies that these define valid POVM and that they lead to the desired correlation (3.3). Moreover, the POVM condition $\sum_b B_b^y = \mathrm{Id}$ for all y implies that the correlations (3.5) always satisfy the no-signaling condition (3.4). However, the model is strictly more general than the classical model (3.3), as we show next by identifying a non-local game in which the use of quantum correlations leads to a strictly higher winning probability than classical correlations could. (It is also possible to show that it is not as general as the non-signalling model, as the example of a non-signaling correlation given above cannot be realized in quantum mechanics.)

3.3 Binary Linear System Games

For this section we borrow some material from the lecture notes by Richard Cleve available at this url.

Binary linear system games, or BLS games for short, are a class of two-player one-round games introduced in [CM14] and inspired by Mermin's proofs of Bell's theorem [Mer90, Mer93]. These games capture the flavor of the "clause-vs-variable" game considered in the previous section, except that the underlying formula involves parity constraints of the form $y_{j_1} \oplus \cdots \oplus y_{j_\ell} = c_j$ as opposed to the disjunctions we had for the case of 3SAT.

Definition 3.4. A BLS game is specified by integers $m, n \geq 1$, a matrix $E \in \{0,1\}^{m\times n}$ and a vector $c \in \{\pm 1\}^m$. (This information is available to both the referee and the players in the game.) The game proceeds as follows:

1. The referee samples $j \in \{1,\ldots,m\}$ uniformly at random and sends j to the first player. Let ℓ be the number of nonzero entries in the j-th row of E. The referee samples $k \in \{1,\ldots,\ell\}$ uniformly at random and sends the index of the k-th nonzero entry of the j-th row of E to the second player.

2. The referee expects answers $(a_1,\ldots,a_\ell) \in \{\pm 1\}^\ell$ from the first player and $b \in \{\pm 1\}$ from the second.[9]

3. The referee declares that the players win if and only if both the following conditions hold: *(consistency check:)* $a_k = b$ and *(equation check:)* $\prod_i a_i = c_j$.

The class of BLS games has many interesting properties. In particular, there is a direct correspondence between the existence of perfect strategies in different models and certain kinds of 'solutions' to the system of equations implied by E and c. (Precisely, for $j \in \{1,\ldots,m\}$ the j-th row of E and c can be interpreted as a constraint $y_1^{E_{j,1}} \cdots y_n^{E_{j,n}} = c_j$ on n variables $y_1,\ldots,y_n \in \{\pm 1\}$.) For the case of classical strategies, following the proof of Claim 3.2 we easily see that the game has a perfect strategy if and only if the system of equations has a solution over $\{\pm 1\}$, which in this case can be determined by Gaussian elimination. For quantum strategies in the model introduced above (i.e. the "tensor product model" (3.5)) there is a correspondence between perfect strategies and "operator solutions" to the system of equations. This correspondence will allow us to make use of a specific BLS game called the "Magic Square game" in order to develop our first test of a qubit that can be executed by an entirely classical verifier. We introduce the Magic Square game in the next section.

Remark 3.5. The correspondence between strategies and (operator) solutions goes further than the classical and tensor product models. In particular one can say interesting things about quantum strategies in an extended model called the "commuting-operator model", but we don't discuss this here. See for example [CLS17] and follow-up works.

[9] For later convenience we adopt a multiplicative $\{\pm 1\}$ convention for the variables, instead of the more usual $\{0,1\}$ convention.

3.3.1 An example: the Magic Square game

The Magic Square game is the following BLS game with 6 constraints on 9 variables. The constraints are best visualized by picturing the variables arranged in the entries of a 3×3 square, as follows:

$$\begin{array}{ccc|c} y_1 & y_2 & y_3 & +1 \\ y_4 & y_5 & y_6 & +1 \\ y_7 & y_8 & y_9 & +1 \\ \hline +1 & +1 & -1 & \end{array}$$

As indicated on the picture the 6 constraints are that the product of all variables in any given row should equal $+1$ and that the product of all variables in any column should equal $+1$ *except* for the last column, where it should equal -1.

This system of equations does not have a solution (make sure you can show this!), and so the associated BLS game, as described in Definition 3.4, does not have a perfect classical strategy: it is not hard to see that the maximum success probability that classical players can achieve is $\frac{17}{18}$, matching the bound of Claim 3.2.

A remarkable fact is that there is a perfect quantum strategy for this game ("perfect" means that the strategy succeeds with probability 1 in the game). This is remarkable because, as we just saw, the underlying system of equations *does not have a solution*! Yet quantum players are able to *always* give answers that are accepted by the referee. For this to be possible these answers necessarily have to be generated "on the fly", freshly every time a question is asked: if this were not the case then the same proof as that of Claim 3.2 would apply. Quantum provers are able to win with certainty, yet there is no way to extract a satisfying assignment from them. What feature of the system of equations makes this possible? Can quantum provers win *any* BLS game with probability 1, irrespective of any truth value of the underlying system of equations?

To gain insight into this question let us describe an explicit quantum strategy for the players that succeeds with probability 1. The key observation is that even though as we saw the system of equations associated with the magic square does not have a solution with values in $\{\pm 1\}$, it has an *operator solution*

$$\begin{array}{ccc} I \otimes \sigma_Z & \sigma_Z \otimes I & \sigma_Z \otimes \sigma_Z \\ \sigma_X \otimes I & I \otimes \sigma_X & \sigma_X \otimes \sigma_X \\ \sigma_X \otimes \sigma_Z & \sigma_Z \otimes \sigma_X & \sigma_Y \otimes \sigma_Y \end{array} \tag{3.6}$$

where $\sigma_Y = i\sigma_X\sigma_Z$. Observe that in each row or column the three observables always commute; moreover, the product of the three observables in each row or column is always $+I$ except for the last column, where it is $-I$. This is what we mean by "operator solution".

Definition 3.6. An operator solution to a BLS (E, c) is a collection of binary observables $Y_1, \ldots, Y_n$ on the same Hilbert space $\mathcal{H}$ such that for each equation (specified by a row of E) $y_{j_1} \cdots y_{j_\ell} = c_j$ the observables $Y_{j_1}, \ldots, Y_{j_\ell}$ commute and their product equals $c_j \,\mathrm{Id}$.

It is not too hard to show that for any BCS, an operator solution immediately translates into a perfect quantum strategy for it.

Lemma 3.7. *Suppose given an operator solution $Y_1, \ldots, Y_n$ to a BLS (E, c) such that each Y_j is a binary observable on a finite-dimensional Hilbert space $\mathcal{H}$. Then the following strategy succeeds with probability* 1 *in the BLS game:*

- *The players share the* maximally entangled *state*

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_i |i\rangle_A \otimes |i\rangle_B \in \mathcal{H}_A \otimes \mathcal{H}_B \,, \tag{3.7}$$

  where d is the dimension of $\mathcal{H}$, each of $\mathcal{H}_A$ and $\mathcal{H}_B$ is a copy of $\mathcal{H}$, and $\{|i\rangle\}$ an orthonormal basis for it.[10]
- *On question j, Alice sequentially measures the observables $Y_{j_1}, Y_{j_2}, \ldots, Y_{j_\ell}$ on her share of $|\psi\rangle$, where $j_1, \ldots, j_\ell$ are the indices of the nonzero entries of the j-th row of E. She obtains outcomes $a_1, \ldots, a_\ell$ that she returns as her answer.*
- *On question $k \in \{1 \ldots, n\}$ Bob measures the observable Y_k^T on his share of $|\psi\rangle$. He obtains an outcome $b \in \{\pm 1\}$ that he returns as his answer.*

Proof. First we note that the strategy described in the lemma is valid: since by definition of an operator solution the observables $Y_{j_1}, Y_{j_2}, \ldots, Y_{j_\ell}$ always commute it is possible for Alice to measure them simultaneously.

The following relation holds the key to the proof: for any operators A on $\mathcal{H}_\mathsf{A}$ and B on $\mathcal{H}_\mathsf{B}$ it holds that

$$\langle\psi|A \otimes B|\psi\rangle \;=\; \frac{1}{d}\mathrm{Tr}(AB^T) \,, \tag{3.8}$$

where $|\psi\rangle$ is as in (3.7). This relation follows easily from the relation $(\mathrm{Id} \otimes B)|\psi\rangle = (B^T \otimes \mathrm{Id})|\psi\rangle$ that we saw in the previous lecture and the fact that the reduced density matrix of $|\psi\rangle$ on either subsystem is the totally mixed stated $d^{-1}\,\mathrm{Id}$. Using this relation it is a matter of direct calculation to verify that the prover's answers always satisfy the verifier's checks in the game. In more detail,

- For the consistency check, we note that the probability that the two players return consistent answers on question (j,k) is

$$\frac{1}{2} + \frac{1}{2}\langle\psi|Y_{j_k} \otimes Y_{j_k}^T|\psi\rangle \;=\; \frac{1}{2} + \frac{1}{2}\frac{1}{d}\mathrm{Tr}\big(Y_{j_k}^2\big) \;=\; 1 \,,$$

  where the first equality follows from (3.8) and the second holds since Y_{j_k} is a binary observable so $Y_{j_k}^2 = \mathrm{Id}$.
- For the equation check, we note that the probability that Alice's answers satisfy the check for the j-th equation is

$$\frac{1}{2} + \frac{c_j}{2}\langle\psi|Y_{j_1} \cdots Y_{j_\ell} \otimes \mathrm{Id}\,|\psi\rangle \;=\; \frac{1}{2} + \frac{c_j}{2}\langle\psi|c_j\,\mathrm{Id} \otimes \mathrm{Id}\,|\psi\rangle \;=\; 1 \,,$$

  where the first equality holds since $Y_{j_1} \cdots Y_{j_\ell} = c_j\,\mathrm{Id}$ by definition of an operator solution.

□

Remark 3.8. The reader will have noticed that in Lemma 3.7 we carefully added the assumption that the operator solution is finite-dimensional, and indeed this seems necessary for the state $|\psi\rangle$ to be well-defined. It is possible to show that infinite-dimensional operator solutions to a BLS correspond to *commuting-operator* strategies for the associated game, and conversely; this correspondence is established in [CLS17]. Commuting-operator strategies are a strict superset of tensor-product strategies

Combining Lemma 3.7 with the operator solution to the magic square given by (3.6) we obtain a perfect strategy for the magic square game that uses two qubits per player, and two EPR pairs shared between them. Since we saw that the magic square does not have a perfect strategy this strategy gives us another example of a non-signaling correlation that is not classical.

[10] The maximally entangled state is a natural generalization of the EPR pair which can be defined on any tensor product of (finite-dimensional) isomorphic Hilbert spaces.

3.3.2 Characterization of optimal strategies

The following converse to Lemma 3.7 is shown in [CM14].

Lemma 3.9. *Suppose given a BLS (E, c) and a strategy $(|\psi\rangle, A, B)$ for the associated game that succeeds with probability 1. Then the BLS has a finite-dimensional operator solution.*

Proof. We give the proof for the special case of the Magic Square game, as the general case is similar. We start with the modeling step: a strategy $(|\psi\rangle, A, B)$ for the magic square game is given by a bipartite state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ for finite-dimensional $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ as well as the following measurements. For the first player (Alice), for each row or column x there is a 9-outcome projective measurement $\{A_a^x : a \in \{\pm 1\}^3\}$ on $\mathcal{H}_\mathsf{A}$. For the second player (Bob), for each variable (square) y there is an observable B_y on $\mathcal{H}_\mathsf{B}$. Note that here we assumed that the measurements made by each player are projective, which is without loss of generality by applying Naimark's theorem and enlarging the spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_\mathsf{B}$ if necessary.

To each of Alice's questions we can associate three observables that correspond to the three bits of her answer. For example, for question $j = 1$ (first row) we can define

$$A_1 = \sum_{a_1,a_2,a_3 \in \{\pm 1\}} a_1 \, A^1_{a_1 a_2 a_3} \, , \quad A_2 = \sum_{a_1,a_2,a_3 \in \{\pm 1\}} a_2 \, A^1_{a_1 a_2 a_3} \, , \quad A_3 = \sum_{a_1,a_2,a_3 \in \{\pm 1\}} a_3 \, A^1_{a_1 a_2 a_3} \, .$$

We can similarly proceed to define $A_4, \ldots, A_9$ from the rows and $A'_1, \ldots, A'_9$ from the columns. Next we show that success with probability 1 in the consistency checks implies that

$$\forall y \in \{1, \ldots, 9\} \, , \qquad A_y = A'_y = B_y^T \, . \tag{3.9}$$

Take for example the consistency check on question $(1, 2)$ (first row to Alice, second entry to Bob). It is easy to show that success in that check implies that

$$\langle \psi | A_2 \otimes B_2^T | \psi \rangle = 1 \, . \tag{3.10}$$

We use the following claim.

Claim 3.10. *Suppose that $|\psi\rangle$ is a bipartite state A, B observables such that $\langle \psi | A \otimes B | \psi \rangle = 1$. Let $|\psi\rangle = \sum_t \lambda_t |u_t\rangle |v_t\rangle$ be the Schmidt decomposition of $|\psi\rangle$, with $\lambda_t > 0$ for all t and $\{|u_t\rangle\}$ and $\{|v_t\rangle\}$ orthonormal families. Let $S_A = Span\{|u_t\rangle\} \subseteq \mathcal{H}_\mathsf{A}$ and $S_B = Span\{|v_t\rangle\} \subseteq \mathcal{H}_\mathsf{B}$. Then S_A is stable by A and S_B is stable by B. Moreover, letting A_S denote the matrix of the restriction of A to S_A in the basis $\{|u_t\rangle\}$ and similarly for B, it holds that $A_S = B_S^T$.*

Proof sketch. Let $K = \sum_t \lambda_t |u_t\rangle\langle v_t|$. Then the equality $\langle \psi | A \otimes B | \psi \rangle = 1$ is equivalent to $AKB^T = K$. Identifying left and right eigenspaces we see that A and B must each preserve the eigenspaces of K associated with any given eigenvalue. Thus $AKB^T = K$ decomposes in block form $\oplus_\lambda A_\lambda B_\lambda^T = \mathrm{Id}_\lambda$, where for each block we indicated with a subscript λ the restriction of each operator to the eigenspace of K associated with eigenvalue λ. This shows the claim. □

Using Claim 3.10 and the implications of the form (3.10) for the consistency checks, (3.9) follows, where the operators and the transpose should be understood to be written with respect to the Schmidt bases of $|\psi\rangle$. To conclude we claim that $B_1^T, \ldots, B_9^T$ (precisely, their restriction to the support of $|\psi\rangle$ on $\mathcal{H}_\mathsf{B}$) are an operator solution to the Magic Square. Commutation in each row or column follows from (3.9) and the definition of the A_y (which by definition commute by rows) and A'_y (by columns). The constraints follow from the fact that e.g. for the first row, $\langle \psi | A_1 A_2 A_3 \otimes \mathrm{Id} \, | \psi \rangle = +1$, which using Claim 3.10 implies that $A_1 A_2 A_3 = \mathrm{Id}$ and hence $B_1^T B_2^T B_3^T = \mathrm{Id}$. (Of course we could remove the transpose signs and still have a valid solution.) □

3.4 A nonlocal test for a qubit

We now have everything that we need in order to give our first classical-verifier test for a qubit (in fact, as we will see, for two qubits!). To motivate this, observe that the proof of Lemma 3.9 says a bit more than is stated in the lemma itself: not only did we show that the Magic Square has an operator solution, we also exhibited such a solution directly from the second player's observables in the game. Let's show the following simple fact.

Claim 3.11. *Suppose given an operator solution $Y_1, \ldots, Y_9$ to the magic square. Then Y_2 and Y_4 anti-commute.*

Proof. We first rewrite the product $Y_2 Y_4$ by rows to obtain

$$\begin{aligned} Y_2 Y_4 &= Y_1 Y_3 \cdot Y_6 Y_5 \\ &= Y_1 \cdot Y_9 \cdot Y_5 \,, \end{aligned}$$

where the second line is by the last column constraint. Next we write the product $Y_4 Y_2$ by columns:

$$\begin{aligned} Y_4 Y_2 &= Y_1 Y_7 \cdot Y_8 Y_5 \\ &= Y_1 \cdot (-Y_9) \cdot Y_5 \,, \end{aligned}$$

where the second line is by the last row constraint. Combining both equations it follows that $Y_2 Y_4 = -Y_4 Y_2$, as claimed. □

The following lemma is immediate from the proof of Lemma 3.9 and Claim 3.11. We state the lemma using the language of "self-testing" from the previous lecture.

Lemma 3.12. *Suppose that two non-communicating quantum devices A and B generate correlations*

$$p(a,b|x,y) \;=\; \langle \psi | A_a^x \otimes B_b^y | \psi \rangle$$

that perfectly satisfy the referee's tests in the Magic Square game. Let S_B denote the support of the reduced density ρ_B of $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ on $\mathcal{H}_B$. Then the observables $B_1, \ldots, B_9$ stabilize S_B, and their restriction to that space form an operator solution to the Magic Square. In particular, the device's joint state $|\psi\rangle_{AB}$ together with observables B_2 and B_4 of device B associated with inputs $y = 2$ and $y = 4$ respectively form a qubit $(|\psi\rangle, B_2, B_4)$.

Proof. The first part of the lemma follows from the proof of Lemma 3.9. By Claim 3.11 the observables associated to $y = 2$ and $y = 4$ anti-commute. □

The preceding lemma shows that two of device B's observables, B_2 and B_4, must anti-commute. As we saw in Lemma 1.2[11] this means that up to an isomorphism on the device's space these observables must take the form $B_2 \simeq \sigma_Z \otimes \mathrm{Id}$ and $B_4 \simeq \sigma_Z \otimes \mathrm{Id}$, which is exactly the form that they take in the solution given in (3.6). What about the other observables? In other words, are the constraints that underlie the Magic Square game *rigid*?

[11] Here we can apply the "state-independent" version of the qubit lemma because Lemma 3.12 states that the observables themselves, or rather their restriction to the support of $|\psi\rangle$, satisfy the operator constraints.

Lemma 3.13. *Under the same assumptions as Lemma 3.12 there is a unitary U on the space $\mathcal{H}_B$ associated with device B such that the observables $U^\dagger B_k U$ for $k \in \{1,\ldots,9\}$ take the form described in* (3.6)*. in particular, the dimension of (the span of the support of $|\psi\rangle$ on) $\mathcal{H}_B$ is a multiple of* 4*.*

Proof. The main ingredient in this proof is the qubit lemma, Lemma 1.2, together with Claim 1.6 which allows us to argue that observables that commute with σ_Z and σ_X on a copy of $\mathbb{C}^2$ must act as identity on $\mathbb{C}^2$.

First note that the proof of Lemma 3.12 immediately extends to show that any two observables not in the same row or column anti-commute. Furthermore, by definition the condition that the 9 observables $B_1,\ldots,B_9$ form an operator solution to the Magic Square implies that all observables in the same row or column must commute. Using this condition and the characterization of B_2 and B_4 given in Lemma 3.12 it follows from Claim 1.6 that $B_1 \simeq \mathrm{Id}\otimes B_1'$ and $B_5 \simeq \mathrm{Id}\otimes B_5'$, for some observable B_1' and B_5' on $\mathcal{H}'$ that anti-commute. Using Lemma 1.2 again it follows that there is an isometry U' on $\mathcal{H}'$ such that as operators on $\mathcal{H}'$, $B_1' \simeq \sigma_Z \otimes \mathrm{Id}$ and $B_5' \simeq \sigma_X \otimes \mathrm{Id}$, with the identity acting on some new ancilla space $\mathcal{H}''$ such that $\mathcal{H}' \simeq \mathbb{C}^2 \otimes \mathcal{H}''$. Combining U and U' together, we have shown that there is an isomorphism $U'U$ under which

$$\begin{array}{ll} B_1 \simeq \mathrm{Id}\otimes\sigma_Z\otimes\mathrm{Id} & B_2 \simeq \sigma_Z\otimes\mathrm{Id}\otimes\mathrm{Id} \\ B_4 \simeq \sigma_X\otimes\mathrm{Id}\otimes\mathrm{Id} & B_5 \simeq \mathrm{Id}\otimes\sigma_X\otimes\mathrm{Id} \end{array}.$$

The remaining entries of the table are immediately filled in from the row and column constraints, which uniquely determine them. □

As a last step we show that we can also characterize the entangled state used by any strategy. Interestingly, this characterization comes as a consequence of the characterization of the observables, which we obtained without talking much about the state. This is based on the following general lemma, that we will often make use of.

Lemma 3.14. *Let $|\psi\rangle_{ABE} \in (\mathbb{C}^2)_A^{\otimes n} \otimes (\mathbb{C}^2)_B^{\otimes n} \otimes \mathcal{H}_E$ be such that for every $i \in \{1,\ldots,n\}$ it holds that*

$$\left(\sigma_{X,i}\right)_A \otimes \left(\sigma_{X,i}\right)_B |\psi\rangle_{ABE} \;=\; \left(\sigma_{Z,i}\right)_A \otimes \left(\sigma_{Z,i}\right)_B |\psi\rangle_{ABE} \;=\; |\psi\rangle_{ABE}\,,$$

where the Pauli operators act on the i-th copy of $\mathbb{C}^2$ in register A and B respectively. Then $|\psi\rangle_{ABE} = |\phi^+\rangle_{AB}^{\otimes n} \otimes |aux\rangle$, for some state $|aux\rangle$ on $\mathcal{H}$.

Proof. Note that $\sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z$ commute, hence are simultaneously diagonalizable. The proof immediately follows from the observation that the only simultaneous eigenvalue-1 eigenstate of $\sigma_X \otimes \sigma_X$ and $\sigma_Z \otimes \sigma_Z$ is the EPR pair $|\phi^+\rangle$. □

Exercise 3.1. Show that the conclusion of Lemma 3.14 holds under the following weaker assumption: $|\psi\rangle_{\mathsf{ABE}} \in (\mathbb{C}^2)_{\mathsf{A}}^{\otimes n} \otimes \mathcal{H}_{\mathsf{B}}^{\otimes n} \otimes \mathcal{H}_{\mathsf{E}}$ with $\mathcal{H}_{\mathsf{B}}$ arbitrary, and for every $i \in \{1,\ldots,n\}$,

$$\left(\sigma_{X,i}\right)_{\mathsf{A}} \otimes \left(X_i\right)_{\mathsf{B}} |\psi\rangle_{\mathsf{ABE}} \;=\; \left(\sigma_{Z,i}\right)_{\mathsf{A}} \otimes \left(Z_i\right)_{\mathsf{B}} |\psi\rangle_{\mathsf{ABE}} \;=\; |\psi\rangle_{\mathsf{ABE}}\,,$$

with X_i and Z_i arbitrary binary observables on $\mathcal{H}_{\mathsf{B}}$ (in particular, we are not assuming any a priori qubit structure on $\mathcal{H}_{\mathsf{B}}$). *[Hint: Remember Claim 2.7]*

3.4.1 Consequences

The characterization of perfect strategies given in Lemma 3.13 together with Lemma 3.14 have some nice consequences. First of all, they imply that the Magic Square game tests not one, but two qubits: any perfect strategy must have a 4-qubit entangled state, two qubits per player, and Bob's observables specify two qubits, e.g. B_2 and B_4 for the first and B_1 and B_5 for the second. We even have access to more: for example, we know that when Bob is asked question 9 the observable he applies is $\sigma_Y \otimes \sigma_Y$. Although we clearly have some distance to go, these are first steps towards testing that Bob implements a certain computation; for now, we are able to test that he applies specific observables.

Another consequence of the characterization has to do with the problem of randomness certification. At this point we know that, in any perfect strategy, whenever Bob is asked question 2 he measures the first qubit of an EPR pair in the standard basis. This has the following implications:

1. The answer reported by Bob on question 2 (and, in fact, on *any* question) is a uniformly random bit. In particular, no deterministic strategy can succeed in the game! We knew this already, because deterministic strategies are classical. As such, any game for which quantum strategies can succeed with strictly higher probability than classical strategies can serve as a "test for randomness".

2. More importantly, the randomness that is generated by Bob at each execution of the game is "fresh" and "private". What we mean by this is that Bob's random bit is (1) independent of any information at the verifier's side, including Bob's question, and (2) uncorrelated to the environment. Indeed, since Bob's bit is the result of a measurement of half an EPR pair, the only party that can obtain correlated information is Alice, who holds the other half of the EPR pair. By the rigidity theorem this EPR pair *must* be in control of Alice: she needs it for them to succeed in the game. Therefore the verifier has the guarantee that the bit she obtains (1) cannot have been "planted" *a priori* in the devices, and (2) cannot be learned, even partially, by any third party distinct from A and B, even if the party could a priori have kept entanglement with the devices—this is because, using the notation of Lemma 3.14, the third party would only at best have access to the entirety of system E, which is uncorrelated with AB.

These observations are important for cryptography, where the use of high-quality randomness that is uncorrelated from any possible eavesdropper or adversary is an essential resource. Indeed, the observations we just made form the basis for the so-called "device-independent" analysis of quantum cryptography protocols.

Remark 3.15. We presented the fact that the Magic Square game tests two qubits, instead of one, as a "feature". But what if one only cares about a single qubit, is there a simple test for this? There is such a test, but it is not an BLS game: it is the CHSH game. The proof that this game tests a qubit was recognized early on, see e.g. [SW87] or [MYS12] for a more modern treatment. Unfortunately the game does not have "quantum completeness 1", in the sense that the optimal quantum strategy for it achieves a success probability that is greater than the optimal classical, but less than 1 (precisely, it is $\cos^2 \pi/8 \approx 0.85$). This makes it less convenient to use as a building block in larger protocols, and so here we will stick with the Magic Square game that is the simplest value-1 game which self-tests at least one qubit that we know of.

An important drawback of our analysis so far is that it is limited to the case of perfect strategies, i.e. strategies that succeed with probability 1 in the game. In practice one may only reasonably assume, after multiple executions of the game, that a given strategy succeeds with some probability that is close to one, $1-\varepsilon$ for some $\varepsilon \geq 0$ that can be made small but not 0. In the next section we discuss how the results can be extended to that case.

3.4.2 The approximate case

The following theorem gives the flavor of an approximate version of the lemmas from the previous section. It is taken from [CS17], where more general statements are shown for any BLS that satisfies appropriate conditions. (A similar result specialized to the case of the Magic Square game is shown in [WBMS16].)

Theorem 3.16. *Suppose that a strategy $(|\psi\rangle, A, B)$ succeeds with probability $1-\varepsilon$ in the Magic Square game, for some $\varepsilon \geq 0$. Then there are isometries $V_D : \mathcal{H}_D \to \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}_{D'}$ for $D \in \{A, B\}$ such that*

$$\left\| V_A \otimes V_B |\psi\rangle_{AB} - |\phi^+\rangle \otimes |\phi^+\rangle \otimes |aux\rangle \right\|^2 = O\left(\sqrt{\varepsilon}\right) ,$$

for some state $|aux\rangle$ on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$, and

$$\left\| \mathrm{Id}_A \otimes \left(V_B B_2 - (\sigma_Z \otimes \mathrm{Id} \otimes \mathrm{Id}) V_B\right) |\psi\rangle_{AB} \right\|^2 = O(\varepsilon) ,$$
$$\left\| \mathrm{Id}_A \otimes \left(V_B B_4 - (\sigma_X \otimes \mathrm{Id} \otimes \mathrm{Id}) V_B\right) |\psi\rangle_{AB} \right\|^2 = O(\varepsilon) ,$$

and similar relations hold for the remaining seven observables on Bob's side.

Note that the theorem only characterizes the player's observables "up to isometry", as opposed to "up to isomorphism" as we were able to in the perfect case (Lemma 3.13). As discussed in the previous lecture (Section 2.3) this is unavoidable in general.

Later we will see a general method to derive statements such as Theorem 3.16 based on the use of approximate group representation theory. For now, we let it serve as a good illustration of the kind of statements we aim to prove in this course. It is worth reflecting on the strength of what we have achieved: using only classical data and a single physical assumption (our model for spatial isolation based on the use of tensor products) we have arrived at a very simple test that can be used to fully characterize the quantum state of a 16-dimensional system (4 qubits) as well as elementary operations performed on it. This conclusion is much stronger than the "standard" conclusion that motivates the study of Bell inequalities in the first place: that they require entanglement.[12] There is no equivalent to this in classical theory!

[12] Note that the fact that the isometries V_A and V_B are "local", each acting only on one half of the total Hilbert space, is important because it means that they couldn't have artificially create the entanglement present in $|\phi^+\rangle \otimes |\phi^+\rangle$: that entanglement must "exist" even independently of the application of the isometry, which only serves to "package" it in the neat form of two EPR pairs. Of course, the state $|aux\rangle$ may or may not contain entanglement itself.

Bibliography

[AV12] Dorit Aharonov and Umesh Vazirani. Is quantum mechanics falsifiable? A computational perspective on the foundations of quantum mechanics. *arXiv preprint arXiv:1206.3686*, 2012.

[Bel64] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[Bre06] Frédéric Brechenmacher. *Histoire du théorème de Jordan de la décomposition matricielle (1870-1930). Formes de représentation et méthodes de décomposition.* PhD thesis, 2006.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In *International Colloquium on Automata, Languages, and Programming*, pages 320–331. Springer, 2014.

[CR20] Rui Chao and Ben W Reichardt. Quantum dimension test using the uncertainty principle. *arXiv preprint arXiv:2002.12432*, 2020.

[CRSV17] Rui Chao, Ben W Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping qubits. *arXiv preprint arXiv:1701.01062*, 2017.

[CRSV18] Rui Chao, Ben W Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *Quantum*, 2:92, 2018.

[CS17] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint arXiv:1709.09267*, 2017.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[GVW01] Oded Goldreich, Salil Vadhan, and Avi Wigderson. On interactive proofs with a laconic prover. In *International Colloquium on Automata, Languages, and Programming*, pages 334–345. Springer, 2001.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*= RE. *arXiv preprint arXiv:2001.04383*, 2020.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267. IEEE, 2018.

[Mer90] N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical review letters*, 65(27):3373, 1990.

[Mer93] N David Mermin. Hidden variables and the two theorems of john bell. *Reviews of Modern Physics*, 65(3):803, 1993.

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[NC02] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[SW87] Stephen J Summers and Reinhard Werner. Maximal violation of bell's inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, 110(2):247–259, 1987.

[VW16] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1-2):1–215, 2016.

[WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93(6):062121, 2016.