PHYSICS 491: Symmetry and Quantum Information April 4, 2017

Quantum correlations, non-local games, rigidity

Lecture 1 *Michael Walter, Stanford University*

These lecture notes are not proof-read and are offered for your convenience only. They include additional detail and references to supplementary reading material. I would be grateful if you email me about any mistakes and typos that you find.

Quantum mechanics can seem quite strange at times! We have phenomena such as superpositions ($|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$), entanglement ($|\phi\rangle_{AB} \neq |\phi\rangle_A \otimes |\phi\rangle_B$), incompatible measurements ($[X, Y] \neq 0$), etc. This "strangeness" manifests itself through the *correlations* predicted by quantum mechanics. A modern perspective of studying and comparing correlations is through the notions of a *nonlocal game*. You have met nonlocal games already in Physics 230, but we will discuss some interesting new aspects that you may not have seen before.

1.1 Nonlocal games

In a *nonlocal game*, we imagine that a number of *players* play against a *referee*. The referee hands them *questions* and the players reply with appropriate *answers* that win them the game. The players' goal is to collaborate and maximize their chances of winning. Before the game, the players meet and may agree upon a joint strategy – but then they move far apart from each other and cannot communicate with each other while the game is being played (this can be ensured by the laws of special relativity). The point then is the following: *Since the players are constrained by the laws of physics, we can concoct games where players utilizing a quantum strategy may have an advantage.* This way of reasoning about quantum correlations is eminently operational and quantitative, as we will see in the following.

The *GHZ (Greenberger-Horne-Zeilinger) game* is a famous example of a nonlocal game due to Mermin (1990); cf. Greenberger et al. (1990). Figure 1 illustrates the setup of the GHZ game. It involves three players – Alice, Bob, and Charlie. Each receives as questions a bit $x, y, z \in \{0,1\}$ and their answers are likewise bits $a, b, c \in \{0,1\}$. They win the game if the sum of their answers modulo 2 is as follows:

x	y	z	$a \oplus b \oplus c$
0	0	0	0
1	1	0	1
1	0	1	1
0	1	1	1

Note that not all bit strings xyz are questions that the referee asks. The winning condition can be succintly stated as follows: $a \oplus b \oplus c = x \vee y \vee z$. We write $\oplus$ for addition modulo 2 and $\vee$ for the logical OR. Those of you that have taken the Physics 230 final are already familiar with the rules of this game.

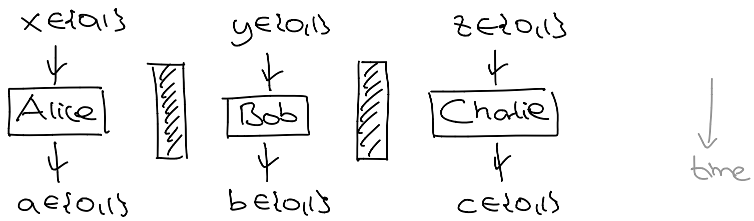

Figure 1: Setup of the three-player GHZ game. The winning condition is that $a \oplus b \oplus c = x \vee y \vee z$.

Classical strategies

It is easy to see that the GHZ game cannot be won if the players' strategies are described by a "local" and "realistic" theory. As in Physics 230, "local" means that each player's answer does only depend on its immediate surroundings, and "realistic" means that the theory must assign a pre-existing value to every possible measurement before the measurement is made. In our case, "measurements" correspond to "questions" and "outcomes" to "answers". Thus in a local and realistic theory we assume that

$$a = a(x), \quad b = b(y), \quad c = c(z).$$

When we say that the players may jointly agree on a strategy before the game is being played, we mean that they may select "question-answer functions" a, b, c in a correlated way. For example, when the players meet before the game is being played, they could flip a coin, resulting in some random $\lambda \in \{0,1\}$, and agree on the strategy $a(x) = x \oplus \lambda$, $b(y) = y \oplus \lambda$, $c(z) = z \oplus \lambda$. Thus, in mathematical terms, the functions a,b,c can be correlated random variables. Equivalently, we could say that λ is a "hidden variable", with some probability distribution $p_\lambda(0) = p_\lambda(1) = 1/2$, and consider $a = a(x,\lambda)$ as a deterministic function of both the input and the hidden variable. You will discuss this point of view in problem 1.1. If the players strategy can be described by classical mechanics then the above would provide an adequate model. Thus, strategies of this form are usually referred to as *local hidden variable strategies* or simply as *classical strategies*.

Suppose now for sake of finding a contradiction that Alice, Bob, and Charlie can win the GHZ game perfectly. Then,

$$\begin{aligned} 1 &= 0 \oplus 1 \oplus 1 \oplus 1 \\ &= (a(0) \oplus b(0) \oplus c(0)) \oplus (a(1) \oplus b(1) \oplus c(0)) \oplus (a(1) \oplus b(0) \oplus c(1)) \oplus (a(0) \oplus b(1) \oplus c(1)) = 0. \end{aligned}$$

The last equality holds because $a(x) \oplus a(x) \equiv 0$ etc., whatever the value of $a(x)$. This is a contradiction! We conclude that there is no perfect classical winning variable strategy for the GHZ game. Suppose, e.g., that the referee selects each possible question xyz with equal probability 1/4. Then the game can be won with probability at most

$$p_{\text{win,cl}} = 3/4.$$

This winning probability can be achieved by, e.g., the trivial strategy $a(x) = b(y) = c(z) \equiv 1$.

Quantum strategies

In a *quantum strategy*, we imagine that the three players are described by quantum mechanics. Thus they start out by sharing an arbitrary joint state $|\psi\rangle_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, where $\mathcal{H}_A$ is the Hilbert space describing a quantum system in Alice' possession, etc., and upon receiving their questions $x, y, z \in \{0,1\}$ they will measure corresponding observables A_x, B_y, C_z on their respective Hilbert spaces. While it might not be immediately obvious, any classical strategy is also a quantum strategy, as you will show in problem 1.1.

It will be convenient to take the eigenvalues (i.e., measurement outcomes) of the observables to be in $\{\pm 1\}$ rather than in $\{0,1\}$. Provided the outcome of Alice's measurement of A_x is $(-1)^a$, she sends back a as the answer, etc. In this case, the eigenvalues of $A_x \otimes B_y \otimes C_z$ are $(-1)^{a+b+c} = (-1)^{a \oplus b \oplus c}$, that is, they correspond precisely to the the sum modulo two of the answers. Thus, a perfect quantum strategy is one where

$$\begin{aligned}
(A_0 \otimes B_0 \otimes C_0) |\psi\rangle_{ABC} &= + |\psi\rangle_{ABC}, \\
(A_1 \otimes B_1 \otimes C_0) |\psi\rangle_{ABC} &= - |\psi\rangle_{ABC}, \\
(A_1 \otimes B_0 \otimes C_1) |\psi\rangle_{ABC} &= - |\psi\rangle_{ABC}, \\
(A_0 \otimes B_1 \otimes C_1) |\psi\rangle_{ABC} &= - |\psi\rangle_{ABC},
\end{aligned} \tag{1.1}$$

In problem 1.1 you will verify that, more generally,

$$p_{\text{win},q} = \frac{1}{2} + \frac{1}{8} \langle \psi_{ABC} | A_0 \otimes B_0 \otimes C_0 - A_1 \otimes B_1 \otimes C_0 - A_1 \otimes B_0 \otimes C_1 - A_0 \otimes B_1 \otimes C_1 | \psi_{ABC} \rangle$$

is the probability of winning the GHZ game (for uniform choice of questions xyz).

Remarkably, there is a quantum strategy for the GHZ game that allows the players to win the game *every single time* (i.e., $p_{\text{win,q}} = 1$). Following Watrous (2006), the players share the three-qubit state

$$|\Gamma\rangle_{ABC} = \frac{1}{2} (|000\rangle - |110\rangle - |101\rangle - |011\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2, \tag{1.2}$$

where we imagine that the first qubit is in Alice's possession, the second in Bob's, and the third in Charlie's. Upon receiving $x = 0$, Alice measures the observable $A_0 = Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ on her qubit, while upon receiving $x = 1$ she measures the observable $A_1 = X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Bob and Charlie perform exactly the same strategy on their qubits. To see that this quantum strategy wins the GHZ game every single time, we only need to verify (1.1). Indeed:

$$\begin{aligned}
(Z \otimes Z \otimes Z) |\Gamma\rangle_{ABC} &= |\Gamma\rangle_{ABC}, \\
(X \otimes X \otimes Z) |\Gamma\rangle_{ABC} &= \frac{1}{2} (|110\rangle - |000\rangle - (-1) |011\rangle - (-1) |101\rangle) = - |\Gamma\rangle_{ABC},
\end{aligned}$$

and similarly $(X \otimes Z \otimes X) |\Gamma\rangle_{ABC} = (Z \otimes X \otimes X) |\Gamma\rangle_{ABC} = - |\Gamma\rangle_{ABC}$.

This shows that in a precise quantitative sense, quantum mechanics enables much stronger "non-local correlations" than what is possible using a local realistic theory.

Exercise. *This looks different from what you remember from the Physics 230 exam! It is a fun exercise to relate the strategy above to the one you remember from the Physics 230 exam.*

Device-independent quantum cryptography

When the three players perform the optimal strategy described above then not only do their answers satisfy the winning condition but their answers are in fact completely *random*, subject only to the constraint that $a \oplus b \oplus c$ must sum to the desired value $x \vee y \vee z$. In particular, $a, b \in \{0,1\}$ are two independent random bits. You can easily verify this by inspection: E.g., for $x = y = z = 0$, Alice, Bob, and Charlie each measure their local Z observable. The eigenvectors are $|abc\rangle$ and so it is clear from eq. (1.2) that we obtain $abc \in \{000, 110, 101, 011\}$ with equal probability 1/4. The randomness obtained in this way is also *private* in the following sense: Suppose that apart from Alice, Bob, Charlie, there is also an evil eavesdropper (Evan) who would like to learn about the random bits generated in this way. Their joint state will be described by a pure state $|\psi\rangle_{ABCE}$ (we may assume that this is a pure state – just hand all other systems to the eavesdropper; this will only give him more power). If Alice, Bob, and Charlie indeed share the state in eq. (1.2) (or for that matter *any* pure state) then it must be the case that $|\psi\rangle_{ABCE} = |\Gamma\rangle_{ABC} \otimes |\psi\rangle_E$. You will show this in problem 2.2. This means that Evan is completely decoupled from Alice, Bob and Charlie's state, and it follows that the random bits a and b are completely uncorrelated from the E system. All these means that the players' answers can be used to generate private randomess – the referee simply locks Alice, Bob, and Charlie (best thought of as quantum devices) into his laboratory, ensures that they cannot communicate, and interrogates them with questions. But of course, the referee cannot in general trust Alice, Bob, and Charlie to actually play the strategy above! So this observation might seem not very useful at first glance...

However, what if the optimal strategy for winning the GHZ game was actually unique? In this case, the referee could test Alice, Bob, and Charlie with randomly selected questions and check that they pass the test every time. After a while, the referee might be confident that the players are in fact able to win the GHZ game every time. But then, by uniqueness of the winning strategy, the referee should in fact know the precise strategy that Alice, Bob, and Charlie are pursuing! The referee in this case would *not* have to put any trust in Alice, Bob, Charlie – they would prove their worth by winning the GHZ game every time around. This remarkable idea for generating private random bits was first proposed by Colbeck (2009). (Note that we need private random bits in the first place to generate the random questions – thus this protocol proposes to achieve a task known as *randomness expansion*. Private random bits cannot be generated without an initial seed of random bits.) The argument sketched so far is of course not rigorous at all: ignoring questions of robustness, we need to take into account that Alice, Bob, Charlie may not behave the same way every time we play the game, may have a (quantum) memory, etc.

However, these challenges can be circumvented and secure randomness expansion protocols using completely untrusted devices do exist (see, e.g., Miller and Shi (2014) and the review Acín and Masanes (2016))! This general line of research is known as *device-independent quantum cryptography* (Mayers and Yao, 1998), since it does not rely on assumptions on the inner workings of the devices involved, but only on their observed correlations. Other applications of include device-independent quantum key distribution (Vazirani and Vidick, 2014) and the command of an adversarial quantum system (Reichardt et al., 2013).

1.2 Rigidity of the GHZ game

For the remainder of the lecture, we will content ourselves with showing that the winning strategy for the GHZ game is indeed essentially unique (Colbeck and Kent, 2011). We say that the GHZ game is *rigid* – or that it is a *self-test* for the state (1.2).

Remark. *The CHSH game which you might remember from Physics 230 is likewise rigid; see Tsirel'son (1987), Summers and Werner (1987), Popescu and Rohrlich (1992), McKague et al. (2012), Reichardt et al. (2013). (Here, optimal quantum winning probability is $1/2 + 1/2\sqrt{2} < 1$!) Robust rigidity results for general XOR games are contained in Slofstra (2011), Miller and Shi (2013),* *Ostrev (2015). Rigidity is also closely related to the question of how much entanglement is needed to win a nonlocal game (e.g., Slofstra, 2011). Surveying some of these results would make for great (but challenging) course projects.*

To prove the rigidity result, we first observe that in the three-qubit strategy discussed above, the state $|\Gamma\rangle_{ABC}$ is already uniquely determined by the measurement operators: Indeed, any eigenvector of $Z \otimes Z \otimes Z$ is necessarily of the form $\alpha|000\rangle + \beta|110\rangle + \gamma|101\rangle + \delta|011\rangle$, and the other three conditions are only satisfied if $\alpha = -\beta = -\gamma = -\delta = 1/2$, up to overall phase.

Let us now consider a general optimal strategy given by operators A_x, B_y, C_z with $A_x^2 = \mathbb{1}$ etc. and a state $|\psi\rangle_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ such that eq. (1.1) are satisfied. The basic strategy to prove the rigidity theorem will be to uncover some *hidden symmetries* in the problem to reduce to the case of three qubits:

Claim 1.1. *In any optimal strategy, the observables must anticommute: "$\{A_0, A_1\} = 0$, $\{B_0, B_1\} = 0$, $\{C_0, C_1\} = 0$" (see below for fine-print).*

We will prove this claim later, but let us see first see how this allows us to identify three qubits.

How to find a qubit?

Consider, e.g., the pair of observables A_0, A_1. They satisfy $A_0^2 = A_1^2 = \mathbb{1}$ and $\{A_0, A_1\} = 0$. Hence, $A_2 = -\frac{i}{2}[A_0, A_1] = -iA_0A_1 = iA_1A_0$ is such that

$$[A_1, A_2] = A_1A_2 - A_2A_1 = iA_1A_1A_0 + iA_0A_1A_1 = 2iA_0,$$

and similarly $[A_2, A_0] = 2iA_1$. This means that A_0, A_1, A_2 transform like the Pauli matrices X, Y, Z! It follows that the Hilbert space decomposes into irreducible representations of $SU(2)$:

$$\mathcal{H}_A = V_{j_1} \oplus V_{j_2} \oplus \cdots = \bigoplus_{j=0,1/2,1,\dots} V_j \otimes \mathbb{C}^{m_j},$$

where m_j counts the number of times the spin-j representation V_j appears in $\mathcal{H}_A$. We claim that, since $\{A_0, A_1\} = 0$, this representation of $SU(2)$ has to be $j = 1/2$! Indeed, $A_2^2 = -iA_0A_1iA_1A_0 = 1$ and so

$$\frac{1}{4}(A_0^2 + A_1^2 + A_2^2) = \frac{3}{4} = \frac{1}{2}(\frac{1}{2} + 1)$$

acts by a scalar. Comparing with $j(j+1)$ we find that $j = 1/2$ (cf. remark 5.4).

Therefore, $\mathcal{H}_A \cong \mathbb{C}^2 \otimes \mathcal{H}_{A'}$, where $\mathcal{H}_{A'}$ is some auxiliary Hilbert space of dimension $m_{1/2}$, and A_0, A_1 act by

$$Z \otimes \mathbb{1}, X \otimes \mathbb{1}.$$

Exercise. *Can you find an argument that avoids using the representation theory of $SU(2)$?*

The same argument works for Bob and Charlie's pairs of observables. Thus the total Hilbert space decomposes as

$$\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \cong (\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathcal{H}_{A'} \otimes \mathcal{H}_{B'} \otimes \mathcal{H}_{C'})$$

and the measurement operators act as in the three-qubit solution. We saw above that in the three-qubit solution the state is uniquely determined by the measurement operators. Thus,

$$|\psi\rangle_{ABC} = |\Gamma\rangle \otimes |\gamma\rangle_{A'B'C'},$$

where $|\Gamma\rangle$ is the three-qubit state from eq. (1.2) and $|\gamma\rangle_{A'B'C'}$ some auxiliary state (which is irrelevant because the observables do not act on it). This is the desired rigidity result.

Anticommutations from correlations (proof of the claim)

We first note that the optimality condition eq. (1.1) can be written as

$$\begin{aligned}A_0|\psi\rangle &= +B_0C_0|\psi\rangle\\ A_0|\psi\rangle &= -B_1C_1|\psi\rangle\\ A_1|\psi\rangle &= -B_1C_0|\psi\rangle\\ A_1|\psi\rangle &= -B_0C_1|\psi\rangle\,.\end{aligned}$$

Here and in the following we write A_0 instead of $A_0\otimes\mathbb{1}_B\otimes\mathbb{1}_C$ to make the formulas more transparent. From the first two and last two equations, respectively,

$$\begin{aligned}A_0|\psi\rangle &= +\frac{1}{2}\left(B_0C_0 - B_1C_1\right)|\psi\rangle\\ A_1|\psi\rangle &= -\frac{1}{2}\left(B_1C_0 + B_0C_1\right)|\psi\rangle\end{aligned}$$

Hence,

$$\begin{aligned}A_0A_1|\psi\rangle &= -\frac{1}{4}\left(B_1C_0+B_0C_1\right)\left(B_0C_0-B_1C_1\right)|\psi\rangle = -\frac{1}{4}\left(B_1B_0 - C_0C_1 + C_1C_0 - B_0B_1\right)|\psi\rangle\,,\\ A_1A_0|\psi\rangle &= -\frac{1}{4}\left(B_0C_0-B_1C_1\right)\left(B_1C_0+B_0C_1\right)|\psi\rangle = -\frac{1}{4}\left(B_0B_1 - C_1C_0 + C_0C_1 - B_1B_0\right)|\psi\rangle\end{aligned}$$

and so

$$\{A_0,A_1\}|\psi\rangle = 0.$$

How can we show that $\{A_0,A_1\}=0$?

This is in fact not exactly true – hence the "quotes" in claim 1.1. But what is true is that $\{A_0,A_1\}=0$ on a subspace $\tilde{\mathcal{H}}_A$ of $\mathcal{H}_A$ such that $|\psi\rangle_{ABC}\in\tilde{\mathcal{H}}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C$. Indeed, we can expand

$$|\psi\rangle_{ABC} = \sum_i s_i\,|e_i\rangle_A\otimes|f_i\rangle_{BC}$$

where the $|e_i\rangle$ and $|f_i\rangle$ are orthonormal and $s_i>0$. If there are $\dim\tilde{\mathcal{H}}_A$ terms then the $|e_i\rangle$ form a complete basis of $\mathcal{H}_A$ and so $\{A_0,A_1\}|\psi\rangle=0$ implies that $\{A_0,A_1\}=0$. Otherwise, we can restrict to the subspace $\tilde{\mathcal{H}}_A := \operatorname{span}\{|e_i\rangle_A\}$ – this is called the *Schmidt decomposition* and we will discuss it in more detail in a future lecture. In the latter case, $|\psi\rangle_{ABC}\in\tilde{\mathcal{H}}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C$, the operators A_x are block diagonal with respect to $\tilde{\mathcal{H}}_A\oplus\tilde{\mathcal{H}}_a^\perp$, and $\{A_0,A_1\}=0$ on $\tilde{\mathcal{H}}_A$. We can proceed likewise for B_y and C_z.

Statement of the rigidity theorem

What have we proved? In mathematical terms, we have established the following theorem:

Theorem 1.2 (Rigidity for the GHZ game)**.** *Consider an optimal strategy for the GHZ game given by operators A_x, B_y, C_z with $A_x^2=\mathbb{1}_A$ etc. and a state $|\psi\rangle_{ABC}\in\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_C$. Then there exist isometries $V_A\colon\mathbb{C}^2\otimes\mathcal{H}_{A'}\to\mathcal{H}_A$, $V_B\colon\mathbb{C}^2\otimes\mathcal{H}_{B'}\to\mathcal{H}_B$, $V_C\colon\mathbb{C}^2\otimes\mathcal{H}_{C'}\to\mathcal{H}_C$ such that*

(i) $|\psi\rangle_{ABC} = (V_A\otimes V_B\otimes V_C)(|\Gamma\rangle\otimes|\gamma\rangle)$ *for some* $|\gamma\rangle\in\mathcal{H}_{A'}\otimes\mathcal{H}_{B'}\otimes\mathcal{H}'C$.

(ii) $V_A^\dagger A_0 V_A = Z \otimes \mathbb{1}_{A'}$, $V_A^\dagger A_1 V_A = X \otimes \mathbb{1}_{A'}$, *and similarly for* B_y *and* C_z*.*

In the coming lectures, we will revisit many of the techniques used above in a more systematic way. I would suggest that you come back to this lecture at the end of the term – at this point you should be well equipped to write up a complete proof of theorem 1.2.

Outlook

There are many further aspects of nonlocal games related to what we discussed in this lecture. For example, how do winning probabilities and optimal strategies behave when one plays many instances of a game – either in multiple rounds (sequentially) or even at the same time (in parallel)? It is clear that if p is the optimal winning probability for a single instance then for n instances the winning probability is at least p^n – but we might be able to do better by using strategies that exploit correlations or entanglement in a clever way! Indeed, the maximal classical winning probability for a single instance of the CHSH game is 3/4 – while for two instances it is $10/16 > 9/16 = (3/4)^2$ (Barrett et al., 2002). On the other hand, it is proved in Cleve et al. (2007) not only for the CHSH game but for arbitrary *XOR games* (games where the winning condition only depends on the sum modulo two of the answers, $a \oplus b \oplus \dots$) that the optimal quantum winning probability for n instances is equal to p^n – this is known as a perfect *parallel repetition theorem*. Surveying some of the papers in this area could also make for a good course project.

Bibliography

N. David Mermin. Quantum mysteries revisited, *American Journal of Physics*, 58(8):731–734, 1990.

Daniel M. Greenberger, Michael A. Horne, Abner Shimony, and Anton Zeilinger. Bell's theorem without inequalities, *American Journal of Physics*, 58(12):1131–1143, 1990.

John Watrous. Bell inequalities and nonlocality. 2006. URL `https://cs.uwaterloo.ca/~watrous/CPSC519/LectureNotes/20.pdf`.

Roger Colbeck. *Quantum and relativistic protocols for secure multi-party computation.* PhD thesis, 2009. arXiv:0911.3814.

Carl A. Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol. 2014. arXiv:1411.6608.

Antonio Acín and Lluis Masanes. Certified randomness in quantum physics, *Nature*, 540(7632): 213–219, 2016.

Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pages 503–509. IEEE, 1998. arXiv:quant-ph/9809039.

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

Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems, *Nature*, 496(7446):456–460, 2013. arXiv:1209.0448.

Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices, *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011. arXiv:1011.4474.

Boris S. Tsirel'son. Quantum analogues of the Bell inequalities. the case of two spatially separated domains, *Journal of mathematical sciences*, 36(4):557–570, 1987.

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.

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

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.

William Slofstra. Lower bounds on the entanglement needed to play xor non-local games, *Journal of Mathematical Physics*, 52(10):102202, 2011.

Carl A. Miller and Yaoyun Shi. Optimal robust self-testing by binary nonlocal XOR games. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 22. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2013. arXiv:1207.1819.

Dimiter Ostrev. The structure of optimal and nearly-optimal quantum strategies for non-local XOR games. 2015. arXiv:1506.00607.

Jonathan Barrett, Daniel Collins, Lucien Hardy, Adrian Kent, and Sandu Popescu. Quantum nonlocality, bell inequalities, and the memory loophole, *Physical Review A*, 66(4):042111, 2002. arXiv:quant-ph/0205016.

Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. In *Computational Complexity, 2007. CCC'07. Twenty-Second Annual IEEE Conference on*, pages 109–114. IEEE, 2007. arXiv:quant-ph/0608146.