MSc in Photonics

PHOTONICS**BCN**

Universitat Politècnica de Catalunya (UPC)
Universitat Autònoma de Barcelona (UAB)
Universitat de Barcelona (UB)
Institut de Ciències Fotòniques (ICFO)

http://www.photonicsbcn.eu

Master in Photonics

MASTER THESIS WORK

The communication cost of simulating POVMs over maximally entangled qubits

Ricard Ravell Rodríguez

Supervised by Prof. Dr. Antonio Acín, ICFO
and Dr. Gabriel Senno, ICFO

Presented on date 9th September 2019

Registered at

Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona

The communication cost of simulating POVMs over maximally entangled qubits

Ricard Ravell Rodríguez

ICFO, Mediterranean Technology Park, Avinguda Carl Friedrich Gauss, 3, 08860 Castelldefels, Barcelona

E-mail: ricard.ravell@icfo.eu

July 2019

Abstract. In [Toner and Bacon, Phys. Rev. Lett. 91, 187904 (2003)], 1 bit of communication was proven to be enough to simulate the statistics of local projective measurements over the maximally entangled state. Ever since then, the question of whether 1 bit is also enough for the case of generalized measurements has been open. In this thesis, we retort to inefficiency-resistant Bell functionals, a powerful technique to prove lower bounds communication complexity, to numerically study this question. The results obtained suggest that, indeed, as is the case with projective measurements, 1 bit of communication suffices to simulate POVMs over maximally entangled qubits.

Keywords: Bell theorem, quantum nonlocality, communication complexity, detection loophole.

1. Introduction

One of quantum theory's features which have puzzled scientists the most since its origin is nonlocality, the fact that measuring a property of a quantum system can instantaneously determine the results of another property measured on a distant system. Such kind of nonlocal influence was part of an important debate inside the scientific community. In their article of 1935 entitled "Can quantum-mechanical description of physical reality be considered complete?", Einstein, Podolsky and Rosen [8] argued that any theory making the same predictions as quantum theory and, at the same time, avoiding such spooky action at a distance, as they called these non-local influences, has to postulate the existence of "real properties" (or, hidden variables) which, when taken into account, allow for the complete local determination of the observations' outcomes. Since orthodox quantum theory does not include these, from the assumption of the impossibility of nonlocal causation one has to conclude its incompleteness. Decades later, in 1964, John S. Bell proved that the predictions of quantum mechanics can never be explained by a physical theory of local hidden variables, under the assumption of free will, going against EPR's intuition [2]. Besides producing a fundamental change in our perception of the universe, the study of Bell nonlocality [4] has led to new

technological applications, and now we know that nonlocal correlations are the key resource in most of quantum mechanics' advantages for informational and computational tasks; key distribution protocols [17], algorithms for distributed computation [13], or random number generators [10, 3] are examples of such applications [18].

Given the existence of quantum correlations that cannot be reproduced by classical, non-communicating devices, it is natural to study how much classical communication would that devices need in order to be able to reproduce them. In a celebrated result, Toner and Bacon [20] proved that 1 bit of communication suffices to simulate the correlations arising from projective measurements over the maximally entangled state. However, for generalized (i.e. POVMs) measurements, it is an open question whether a finite amount of communication suffices or not. This is precisely the problem we will study in this thesis.

To tackle the aforementioned problem we will retort to inefficiency-resistant Bell functionals. These are functionals on the space of probability distributions which are bounded above by 1 on all local distributions that can abort, i.e. local distributions with an additional abort outcome $\perp$ for each party. The reason for considering this type of Bell functionals is that the logarithm of the value they take on a given distribution is a lower bound on the distribution's communication complexity [12]. Moreover, this value coincides with the value given by the partition bound, the tightest lower bound on communication complexity discovered so far [12]. The plan will be to generate examples of these functionals and try to find POVMs measurements over a maximally entangled of 2 qubits such that the value that the resulting quantum distribution takes on the considered Bell functional (i.e. its 'violation') is above 2 (which, by the above reasoning, implies that its communication complexity is above 1). In order to generate the inefficieny-resistant Bell functionals, two methods will be used.

The first method consists on transforming the facets of the polytope of local distributions in an scenario with N inputs and K outputs per party (for different values of N and K), which are (by definition) Bell functionals, to inefficiency-resistant Bell functionals. The problem of enumerating the facets of the local polytope becomes infeasible already for small values of N and K. Hence, for the largest values of N and K considered in this thesis (see the Results section), we will retort to symmetries that will allow us to reduce the computational complexity of the problem.

The second method to generate candidate inefficiency-resistant Bell functionals consists of computing the dual of the eff linear program (see its definition in the Preliminaries section) for distributions (in general, nonquantum) having nontrivial communication complexity appearing the literature. The reason being that the solutions of the this linear program are, precisely, inefficiency-resistant Bell functionals.

This thesis is organized as follows. In section 2 we define the necessary concepts from the areas of Bell nonlocality and communication complexity. In section 3 we present the results we obtained. Finally, in section 4, we provide our conclusions and outline possible future lines of research.

2. Preliminaries

2.1. Quantum non-locality

A bipartite Bell experiment consists of two systems, which may have previously interacted, that are separated and each one of these systems is measured by an observer, Alice or Bob. Alice may choose a measurement x between many others, and may obtain an outcome a. Similarly for Bob but with y and b. From one run of the experiment to the other, these measurements and outcomes may vary. Thus, there is a probability distribution $p(a, b|x, y)$ which describes the probabilities for each pair of outcomes when a certain pair of measurements is performed.

We say that a probability distribution $p(a, b|x, y)$ is *local* if it can be written as

$$\mathbf{p} = \sum_{\lambda} q_\lambda \mathbf{d}_\lambda, \quad \text{with } q_\lambda \geq 0, \quad \sum_{\lambda} q_\lambda = 1 \tag{1}$$

where $\mathbf{d}_\lambda$ corresponds to a deterministic *behaviour*:

$$\mathbf{d}_\lambda(ab|xy) = \begin{cases} 1 & \text{if a} = a_x \text{ and b=}b_y \\ 0 & \text{otherwise.} \end{cases} \tag{2}$$

For N different measurements per party, each of them yielding K possible outcomes, there are K^{2N} deterministic behaviours. Thus, the set of local distributions, which we denote by $\mathcal{L}$, is the convex hull (i.e the set of convex combinations of) of a finite number of points (the deterministic distributions) and, hence, it is a polytope. By virtue of Minkowski's theorem, a polytope can, equivalently to the representation (1) as the convex hull of its vertices, be represented as the intersection of finitely many half-spaces. Hence, a distribution $\mathbf{p} \in \mathcal{L}$ iff

$$s^i \cdot p \leq S^i \qquad \forall i \in I, \tag{3}$$

where I indexes a finite set of linear functionals s^i over $\mathbb{R}^{N^2K^2}$. In the case of the local polytope $\mathcal{L}$, this functionals are known as *Bell functionals* and the corresponding inequalities as *Bell inequalities*. If $s \cdot p \leq S_l$ is a valid inequality for the polytope $\mathcal{L}$, then $F = \{l \in \mathcal{L} | s \cdot l \leq S_l\}$ is called a face of $\mathcal{L}$. Faces of dimension $\dim F = \dim \mathcal{L} - 1$ are called facets of $\mathcal{L}$ and the corresponding inequalities are called facet Bell inequalities. On the remainder of this thesis, we will denote the application of a Bell functional B on a distribution p as $B(p)$. If a distribution p is such that $B(p) > b$ for some Bell inequality $B(l) \leq b \ \forall \ l \in \mathcal{L}$, we say that p is *nonlocal*.

In quantum physics, the joint probabilites are computed using the Born's rule which is given by $p(ab|xy) = \langle \psi | A_{a|x} \otimes B_{b|y} | \psi \rangle$, where: $|\psi\rangle$ is a quantum state in some tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$; and, for every x, $\{A_{a|x}\}_a$ is a POVM (Positive operator-valued measurement) over $\mathcal{H}_A$ (i.e. $A_{a|x}$ are positive semi-definite operators satisfying $\sum_a A_{a|x} = \mathbb{I}$ for every x) and the same goes for Bob.

Bell's 1964 result [2] is the discovery of nonlocal quantum distributions. In the simplest scenario of two binary measurements per party, Clauser, Horm, Shimony and

Holt (CHSH) [6] discovered the Bell inequality $\langle a_0 b_0\rangle + \langle a_0 b_1\rangle + \langle a_1 b_0\rangle - \langle a_1 b_1\rangle \leq 2$, where $\langle a_x b_y\rangle = \sum_{a,b} abp(ab|xy)$, which is violated in quantum mechanics by measuring appropriate (local) qubit observables over the maximally entangled qubit state with a maximal value of $2\sqrt{2}$.

2.2. The detection loophole

In the context of experimental tests of quantum nonlocality, people have studied (what are now known as) *loopholes*, i.e experimental situations that may allow classical, non-communicating devices to generate nonlocal correlations. For instance, if, in an optical setup, the detectors were somehow coordinating their behavior, they may choose to discard a run (i.e. not to click), and though the conditional probability (conditioned on the run not having been discarded) may look quantum, the unconditional probability may very well be classical (i.e local). This is called the detection loophole. When an experiment aborts with probability at most $1-\eta$, we say that the efficiency is η. To close the detection loophole, the efficiency has to be high enough so that the classical explanations are ruled out. It is thus important to study, given a target distribution p (say, one maximally violating the above CHSH inequality), what is the efficiency required for the detectors above which no local explanation p, which exploits the detection loophole is possible, that is

$$\max\{\eta : \exists\ l \in \mathcal{L}^{\perp}, l(a,b|x,y) = \eta p(a,b|x,y) + (1-\eta)a(a,b|x,y)\ \forall a,b,x,y\} \qquad (4)$$

where $\mathcal{L}^{\perp}$ denotes the set of local distributions with one additional outcome per party, the abort outcome $\perp$ (corresponding to the 'no-click' events), and $a \in \mathcal{L}^{\perp}$. Intuitevely, the smallest the value of this quantity the more suceptible to the detection loophole the correlations are. The inverse of (4), which can be expressed by the following linear program,

$$\begin{aligned}
\mathrm{eff}(p) = \min_{\eta,\mu_l \geq 0} \quad & \frac{1}{\eta} && (5)\\
\text{subject to} \quad & \sum_{l \in \mathcal{L}^{\perp}_{det}} \mu_l l(a,b|x,y) = \eta p(a,b|x,y) \quad \text{for } a \neq \perp \text{ and } b \neq \perp && (6)\\
& \sum_{l \in \mathcal{L}^{\perp}_{det}} \mu_l = 1 && (7)
\end{aligned}$$

is a measure of nonlocality, i.e. the higher $\mathrm{eff}(p)$ the further from the local polytope is p. Notice that a distribution p is nonlocal iff $\mathrm{eff}(p) > 1$. As every linear programm, (5) has a dual:

$$\begin{aligned}
\mathrm{eff}(p) = \max_{B} \quad & B(p) && (8)\\
\text{subject to} \quad & B(l) \leq 1 \quad \forall l \in \mathcal{L}^{\perp}_{det}. && (9)
\end{aligned}$$

The solutions of (8) are Bell functionals which are bounded above by 1 on the set $\mathcal{L}^{\perp}$ and whose coefficients for the abort events are all 0. This class of Bell functionals is known as 'inefficiency-resistant Bell functionals' [13].

2.3. Inefficiency-resistant Bell functionals and communication complexity

Communication complexity theory, introduced by Andrew Yao in 1979 [21], studies the communication requirements in the distributed computation of functions. More formally, given a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, the communication complexity of f, denoted $CC(f)$, is the number of bits, in the worst case of the inputs, that have to be exchanged between Alice holding input $x \in \{0,1\}^n$ and Bob holding input $y \in \{0,1\}^n$ in order for him to output $f(x,y)$. The standard scenario of functions easily generalizes to the simulation of probability distributions. In this setting, Alice gets input x, Bob gets input y, and after exchanging bits, Alice has to output a and Bob b such that the joint distribution is some given $p(a,b|x,y)$. This allows us to recast the theory of non-locality in the language of communication complexity: local distributions are those that can be simulated with zero bits of communication and access to some shared randomness λ, i.e. $CC(l) = 0$ for all $l \in \mathcal{L}$. Several techniques to prove lower bounds in communication complexity are known (see, e.g. [11]). In [12], it was shown than one of the strongest techniques, the partition bound, coincides with the log of (8). We thus have:

Proposition 1 [12]. For any distribution p, $CC(p) \geq \log(eff(p))$.

Proposition 1 implies that if we find an inefficiency-resistant Bell functional B and a quantum distribution q obtained by measuring POVMs over a pair of maximally entangled qubits and such that $B(q)>2$, we would have proven that 1 bit of communication is not enough to simulate generalized measurements over the singlet.

2.4. NPA hierarchy for optimization problems

As previously stated, after obtaining the inefficiency resistant Bell functionals we will calculate their quantum violation. When the dimension of the quantum states is fixed, as in the case we are considering (recall we will be working with qubits), the standard technique to find the maximal violation of a given Bell functional, introduced in [14] and known as 'seesaw' algorithm, is to fix one of the players' measurements, say, Bob, optimize over Alice's measurements, and iterate this procedure with the newly found measurements for the other player. This method, however in many cases efficient, is not guaranteed to reach the global maximum (i.e., it can get stuck in a local maximum). To cope with this issue, we will retort to the NPA hierarchy.

The NPA hierarchy, introduced by Navascués, Pironio and Acín [15], is a sequence of semi-definite programs (SDP) $\{P_i\}_i$ approximating the set of quantum correlations (with no restriction on the dimension) from the outside and converging to it in the limit of i going to infinity. That is, the sets $\{Q_i\}$ of feasible points of the SDPs $\{P_i\}_i$ include the quantum set and get closer and closer to it as i (known as, the *level* of the hierarchy) increases. Therefore, the maximal value of a given Bell functional in the i-th level of the hierarchy is an upper bound to its maximal quantum violation (and, hence, also to its maximal quantum violation with qubits).

3. Results

In this section we report on the results obtained during this master project. As stated in the Introduction, the question we are interested in is whether, as is the case for projective measurements, 1 bit of communication suffices to classically simulate the statistics of POVMs over a pair of maximally entangled qubits. As is the case with every problem in communication complexity, to prove an upper bound of 1 bit (i.e. to prove that 1 bit suffices), one has to give a communication protocol that works for any valid input, in this case, any set of POVMs for Alice and Bob and, in the worst case, uses 1 bit of communication. On the other hand, to prove that 1 bit of communication is not enough, it suffices to find a particular set of POVMs such that the resulting quantum distribution has a communication complexity higher than 1 bit. For this thesis we decided to pursue this second path, not only because it is simpler and, hence, more appropriate for the duration of a master, but also because we were hoping to benefit from the power of inefficiency-resistant Bell functionals as lower bounds for the communication complexity of quantum distributions (recall that the logarithm of the value that a quantum distribution take on an inefficiency-resistant Bell functional is a lower bound on its communication complexity). Therefore, we set out to find a inefficiency-resistant Bell functional and a *qubit distribution* whose value on the functional is above 2.

As we briefly discussed in the Introduction, to find the above-mentioned inefficieny-resistant Bell functionals we followed two strategies. The first consisted on enumerating the facets of the local polytope for different bipartite Bell scenarios (i.e. for different number of inputs and outputs for Alice and Bob), and the second on obtaining them as solutions to the dual of the efficiency linear program (see (8)) for appropriately chosen distributions. After finding the inequalities, our plan was to study their maximal quantum violation with POVMs over a pair of maximally entangled qubits. However, given that searching over the space of all POVMs is computationally very costly and that the available methods are not guaranteed to converge, we decided to first compute the violation in the first levels of the NPA hierarchy (which, as explained in the Preliminaries section, gives an upper bound on its quantum violation).

Unfortunately, for all the Bell functionals that we found, their value already on the first level of the NPA hierarchy is (although sometimes above 1) always below 2. We interpret this an indication that, as is the case for projective measurements, 1 bit of classical communication is, in fact, enough to simulate POVMs over qubits as well (we will say more about this in the Conclusions). Nevertheless, in this section we report on the functionals found and the values obtained in the NPA for the two different methods mentioned above.

3.1. First method: Facets transformation

The steps of this method can be summarized as follows:

(i) Compute the facets of the local polytope for a scenario with N inputs per party and K outcomes per input.

(ii) Extend the Bell functionals defining the facets to a scenario with one more outcome per party (the 'abort' outcome) putting 0 in the coefficients corresponding to this new outcome.

(iii) Divide all the coefficients of the new functionals by the maximal value that each functional takes (if nonzero) on the set of local distributions in the N inputs and $K+1$ outputs scenario. This two steps transform the standard Bell functionals obtained in Step 1 for the (N, K) scenario to inefficiency-resistant Bell functionals for the scenario $(N, K+1)$.

(iv) Compute the maximal value that the resulting inefficieny-resistant Bell functional takes on the firsts levels of the NPA hierarchy.

For the computations carried out with this method, a hierarchy of Python classes was developed ‡. We anticipate it will be of further use by the members of ICFO's QIT group working in the topic of nonlocality.

In Table 1 we summarize the results obtained with this method for different number of inputs N and outcomes per input K.

Table 1. Largest values that the transformed functionals for the different scenarios studied take on the first level of the NPA hierarchy. The larger number of outcomes in the scenario $\{N = 3, K = 4\}$ made the facet enumeration infeasible. For this reason, we decided to leverage the techniques developed in [1] to only enumerate the symmetric subset of the facets. The facets of the local polytope in the $\{N = 4, K = 2\}$ scenario were obtained from [7].

Scenario	Max. NPA violation of transformed functionals
$N = 3$ and $K = 2$	1.59
$N = 3$ and $K = 4$ (symmetric)	1.34
$N = 4$ and $K = 2$	1.61

3.2. Second method: Dual of eff

The steps of this method can be summarized as follows:

(i) Compute the (dual of the) efficiency linear program (see (8)) for each of the candidate distributions (see below). Recall that the solutions to this linear program are inefficiency-resistant Bell functionals.

(ii) Compute the maximal value that the resulting inefficieny-resistant Bell functional takes on the firsts levels of the NPA hierarchy.

‡ Ricard Ravell Rodríguez and Gabriel Senno. Python library for Bell nonlocality. https://github.com/gsenno/nonlocality

The candidate distributions came from two sources:

(i) *communication complexity problems for which there is a quantum advantage over classical communication complexity.* In [13], quantum distributions are constructed from quantum communication protocols and inefficiency-resistant Bell functionals, which the distributions violate, are extracted from the dual of the efficiency linear program from (8). The quantum distributions in that construction, however, only violate the Bell inequalities for a sufficiently big number of inputs. Moreover, the dimension of the quantum states grows with the input size. In this thesis, we wanted to test whether the resulting inefficiency-resistant Bell functionals, which we know have quantum violations, can be violated with qubits.
The distributions in this category are p_{DISJ_n}, $p_{EQ'_n}$, p_{VSP_n} and p_{GHD_n}, where: the input sets are binary strings of length n (hence, there are 2^n inputs per player); the outputs are bits; $DISJ_n(x,y) = 1$ if $|\{i : x_i = 1 = y_i\}| = 0$ and 0 otherwise; $EQ'_n(x,y) = 1$ if the Hamming distance between x and y is 2^{n-1} and 0 otherwise; $GHD_n(x,y) = 1$ if $\sum_i (-1)^{x[i]+y[i]} \geq 2^{n/2}$ and 0 otherwise; $VSP_n(\cdot,\cdot)$ is the discretized version of the (continuous) Vector in Subspace Problem (see [5, Section 3.6]); and, finally, $p_{f_n}(a,b|x,y) = 1/2$ if $a \oplus b = f_n(x,y)$ (with $\oplus$ the bitwise XOR) and 0 otherwise.
We could only test the $n = 2$ case as, already for $n = 3$, the size of the local polytope makes the problem unfeasible even for ICFO QIT's cluster. The results obtained for these distributions were:

Table 2. eff values and maximal NPA violation of the corresponding inefficiency-resistant Bell functional for the candidate distributions. The values of the third column being less than 2 implies that the corresponding functionals are, unfortunately, not useful for our purposes. These results also imply that: 1) p_{DISJ_2}, $p_{EQ'_2}$ and p_{VSP_2} are nonlocal distributions, as expected. They are also nonquantum, as the corresponding values in the third column are smaller than in the second. p_{GHD_2}, on the other hand, is local, which is something we did not expect (as we know from [13] that, for sufficiently large n, p_{GHD_n} is nonlocal). There is also some numerical error in eff($p_{EQ'_2}$) because the distribution is non-signaling and from [13] we know that eff should be ≤ 4.

Distribution p	eff(p)	NPA violation for the solution to eff
$DISJ_2$	3.99	1.66
EQ'_2	4.01	1.62
VSP_2	3.66	1.65
GHD_2	1	1

(ii) *quantum information protocols for nonclassical tasks.* We extracted quantum nonlocal distributions appearing in self-testing and randomness extraction protocols and computed their efficiency value using (8). This distributions were selected because they make nontrivial use of POVMs over maximally entangled qubit (that is, POVMs are necessary to achieve the desired characteristic in the corresponding

quantum information protocol). The result of eff for these distributions not only gave us a lower bound on their communication complexity (which is what we were interested in) but also, by definition, a lower bound on the inverse of the efficiency required in an experimental setup aimed at testing such protocols, which is of independent interest.

Table 3. eff values and maximal NPA violation of the corresponding inefficiency-resistant Bell functional for the distributions appearing in [19, Section IV.A] and in [9]. The values of the third column being less than 2 implies that the corresponding functionals are, unfortunately, not useful for our purposes.

Distribution	Efficiency Value	NPA violation for the solution to eff
randomness extraction [9]	1.29	1.66
selftesting POVM [19]	1.31	1.54

4. Conclusions and future work

In this thesis we set out to study the question of whether 1 bit of communication is enough to classically simulate the statistics of local POVMs over maximally entangled qubits. For that purpose, our strategy was to numerically search for inefficiency-resistant Bell functionals, as the logarithm of value they take on quantum distributions is a lower bound on their communication complexity. As we did not find any distribution coming from POVMs over maximally entangled qubits giving a violation of an inefficiency-resistant Bell inequality with a value above 2, we cannot claim a positive answer to the above question. However, giving the diversity of origins for the Bell functionals considered, we interpret our results as an indication that, as is the case for projective measurements, 1 bit of communication might in fact be enough for the simulation of any bipartite quantum distribution over maximally entangled qubits.

Of course, the next step in this research program is to prove the above-mentioned conjecture. For this goal, we expect that the results of [16] about simulating POVMs with projective measurements might be of use. However, as we know that, if the Hilbert space dimension is kept fixed, not every POVM can be simulated by a projective measurement (take, for example, the ones used in [9]), the simulation will have to be such that it holds for maximally entangled qubits but not in general.

5. Acknowledgments

We would like to thank Alejandro Pozas-Kerstjens for helpful discussions and Erik Woodhead for the support he gave us in using his common-lisp library for computations with the NPA hierarchy§.

§ https://github.com/ewoodhead/npa-hierarchy

6. References

[1] Jean-Daniel Bancal, Nicolas Gisin, and Stefano Pironio. Looking for symmetric bell inequalities. *Journal of Physics A: Mathematical and Theoretical*, 43(38):385303, 2010.

[2] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique*, 1(3):195–200, nov 1964.

[3] Manabendra Nath Bera, Antonio Acín, Marek Kuś, Morgan W Mitchell, and Maciej Lewenstein. Randomness in quantum mechanics: philosophy, physics and technology. *Reports on Progress in Physics*, 80(12):124001, nov 2017.

[4] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419–478, apr 2014.

[5] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald De Wolf. Nonlocality and communication complexity. *Reviews of modern physics*, 82(1):665, 2010.

[6] John F. Clauser and Michael A. Horne. Experimental consequences of objective local theories. *Phys. Rev. D*, 10(2):526–535, July 1974.

[7] E Zambrini Cruzeiro and N Gisin. Complete list of tight bell inequalities for two parties with four binary settings. *Physical Review A*, 99(2):022104, 2019.

[8] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, may 1935.

[9] S Gómez, A Mattar, ES Gómez, D Cavalcanti, O Jiménez Farías, A Acín, and G Lima. Experimental nonlocality-based randomness generation with nonprojective measurements. *Physical Review A*, 97(4):040102, 2018.

[10] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1), feb 2017.

[11] Eyal Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 2006.

[12] S. Laplante, V. Lerays, and J. Roland. Classical and quantum partition bound and detector inefficiency. In *Proceedings of the 39th International Colloquium on Automata, Languages and Programming*, pages 617–628, 2012.

[13] Sophie Laplante, Mathieu Laurière, Alexandre Nolin, Jérémie Roland, and Gabriel Senno. Robust bell inequalities from communication complexity. *Quantum*, 2:72, 2018.

[14] Yeong-Cherng Liang and Andrew C Doherty. Bounds on quantum correlations in bell-inequality experiments. *Physical Review A*, 75(4):042103, 2007.

[15] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[16] Michał Oszmaniec, Leonardo Guerini, Peter Wittek, and Antonio Acín. Simulating positive-operator-valued measures with projective measurements. *Physical review letters*, 119(19):190501, 2017.

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

[18] A. Shenoy-Hejamadi, A. Pathak, and S. Radhakrishna. Quantum cryptography: Key distribution and beyond. *Quanta*, 6(1):1, jun 2017.

[19] Armin Tavakoli, Massimiliano Smania, Tamás Vértesi, Nicolas Brunner, and Mohamed Bourennane. Self-testing non-projective quantum measurements. *arXiv preprint arXiv:1811.12712*, 2018.

[20] B. F. Toner and D. Bacon. Communication cost of simulating Bell correlations. *Physical Review Letters*, 91(18):187904, 2003.

[21] A. C. C. Yao. Some complexity questions related to distributed computing. In *Proc. 11th STOC*, pages 209–213, 1979.