Classical and Quantum Partition Bound and Detector Inefficiency*

Sophie Laplante[1], Virginie Lerays[1], and Jérémie Roland[2]

[1] LRI, Université Paris-Sud 11
[2] ULB, QuIC, Ecole Polytechnique de Bruxelles

Abstract. We study randomized and quantum efficiency lower bounds in communication complexity. These arise from the study of zero-communication protocols in which players are allowed to abort. Our scenario is inspired by the physics setup of Bell experiments, where two players share a predefined entangled state but are not allowed to communicate. Each is given a measurement as input, which they perform on their share of the system. The outcomes of the measurements should follow a distribution predicted by quantum mechanics; however, in practice, the detectors may fail to produce an output in some of the runs. The efficiency of the experiment is the probability that neither of the detectors fails.

When the players share a quantum state, this leads to a new bound on quantum communication complexity (eff*) that subsumes the factorization norm. When players share randomness instead of a quantum state, the efficiency bound (eff), coincides with the partition bound of Jain and Klauck. This is one of the strongest lower bounds known for randomized communication complexity, which subsumes all the known combinatorial and algebraic methods including the rectangle (corruption) bound, the factorization norm, and discrepancy. The lower bound is formulated as a convex optimization problem. In practice, the dual form is more feasible to use, and we show that it amounts to constructing an explicit Bell inequality (for eff) or Tsirelson inequality (for eff*). For one-way communication, we show that the quantum one-way partition bound is tight for classical communication with shared entanglement up to arbitrarily small error.

1 Introduction

1.1 Communication Complexity and the Partition Bound

Recently, Jain and Klauck [1] proposed a new lower bound on randomized communication complexity which subsumes two families of methods: the algebraic methods, including the nuclear norm and factorization norm, and combinatorial methods, including discrepancy and the rectangle or corruption bound.

A longstanding open problem is whether there are total functions for which there is an exponential gap between classical and quantum communication complexities. Many partial results have been given [2,3,4,5], most recently [6]. These

* Full version available as arXiv:1203.4155 and ECCC TR12-023.

A. Czumaj et al. (Eds.): ICALP 2012, Part I, LNCS 7391, pp. 617–628, 2012.

strong randomized lower bounds all use the distributional model, in which the randomness of the protocol is replaced by randomness in the choice of inputs, which are sampled according to some hard distribution. The equivalence of the randomized and distributional models, due to Yao's minmax theorem [7], comes from strong duality of linear programming. This appears to be non-applicable to quantum communication complexity (see for instance [8] which considers a similar question in the setting of query complexity), and the rectangle bound, as a result, is understood to be an inherently classical method for lower bounds.

1.2 Bell Experiments

Quantum nonlocality gives us a different viewpoint from which to consider lower bounds for communication complexity. A fundamental question of quantum mechanics is to establish experimentally whether nature is truly *nonlocal*, as predicted by quantum mechanics, or whether there is a purely classical (i.e., *local*) explanation to the phenomena that have been observed in the lab. In an experimental setting, two players share an entangled state and each player is given a measurement to perform. The outcomes of the measurements are predicted by quantum mechanics and follow some probability distribution $p(a, b|x, y)$, where a is the outcome of Alice's measurement x, and b is the outcome of Bob's measurement y. (We write $\mathbf{p}$ for the distribution, and $p(a, b|x, y)$ for the individual probabilities.) A Bell test [9] consists of estimating all the probabilities $p(a, b|x, y)$ and computing a Bell functional, or linear function, on these values. The Bell functional $B(\mathbf{p})$ is chosen together with a threshold τ so that any local classical distribution $\mathbf{p}'$ verifies $B(\mathbf{p}') \leq \tau$, but the chosen distribution $\mathbf{p}$ violates this inequality: $B(\mathbf{p}) > \tau$.

Although there have been numerous experiments that have validated the predictions of quantum mechanics, none so far has been totally "loophole-free". A loophole can be introduced, for instance, when the state preparation and the measurements are imperfect, or when the detectors are partially inefficient so that no measurement is registered in some runs of the experiment, or if the entangled particles are so close that communication may have taken place in the course of a run of the experiment. In such cases, there are classical explanations for the results of the experiment. For instance, if the detectors were somehow coordinating their behavior, they may choose to discard a run, and though the conditional probability (conditioned on the run not having been discarded) may look quantum, the unconditional probability may very well be classical. This is called the detection loophole. When an experiment aborts with probability at most $1 - \eta$, we say that the efficiency is η. (Here we assume that individual runs are independent of one another.) To close the detection loophole, the efficiency has to be high enough so that the classical explanations are ruled out.

What can Bell tests tell us about communication complexity? Both are measures of how far a distribution is from the set of local distributions (those requiring no communication), and one would expect that if a Bell test shows a large violation for a distribution, simulating this distribution should require a lot of communication, and vice versa. Degorre et al. showed that the factorization norm amounted to finding large Bell inequality violations for a particular class of Bell inequalities [10]. Here, we show that the partition bound also corresponds to a class of Bell inequalities.

1.3 Summary of Results

If we assume there is a c-bit classical communication protocol where Alice and Bob output a, b with distribution $p(a, b|x, y)$ when Alice's input is x and Bob's input is y, then there is a protocol without communication that outputs according to $\mathbf{p}$ (conditioned on the run not being discarded) that uses shared randomness and whose efficiency is 2^{-c}: both players guess a transcript, and if they disagree with the transcript, they abort. Otherwise they follow the protocol using the transcript. As others have noticed [11,12], one can immediately derive a lower bound: let η be the maximum efficiency of a protocol without communication that successfully simulates $\mathbf{p}$ with shared randomness. We define $\mathrm{eff}(\mathbf{p}) = 1/\eta$, and $\log(\mathrm{eff}(\mathbf{p}))$ is a lower bound on the communication complexity of simulating $\mathbf{p}$. Though this may sound naïve, this gives a surprisingly strong bound which coincides with the partition bound (in the special case of computing functions).

When we turn to the dual formulation, we get a natural physical interpretation, that of Bell inequalities. To prove a lower bound amounts to finding a good Bell inequality and proving a large violation. This is similar to finding a hard distribution and proving a lower bound in the distributional model of communication; but it is much stronger since the Bell functional is not required to have positive coefficients that sum to one.

Our approach leads naturally to a "quantum partition bound" which gives a lower bound on quantum communication complexity. Let $\mathrm{eff}^*(\mathbf{p}) = 1/\eta^*$, where η^* is the maximum efficiency of a protocol without communication that successfully simulates $\mathbf{p}$ with shared entanglement. In the one-way setting, our quantum partition bound is tight up to arbitrarily small error.

Simulating distributions while allowing for runs to be discarded with some probability is a stronger requirement than allowing a probability of error since the errors are flagged. Lee and Shraibman give a proof of the factorization norm (γ_2) lower bound on (quantum) communication complexity based on the best bias one can achieve with no communication [13, Theorem 60] (attributed to Buhrman; see also Degorre et al. [10]). In light of our formulation of the (quantum) partition bound, it is an easy consequence that the (quantum) partition bound is an upper bound on γ_2 (see e.g. [14] for definitions of the factorization norm γ_2 and the related nuclear norm ν, as well as [10] for their extensions to the communication complexity of distributions).

The following gives a summary of our results. Full definitions and statements are given in the main text. Let $\mathrm{prt}(\mathbf{p})$ be the partition bound for a distribution $\mathbf{p}$ (defined in Sect. 3.1). $R_0(\mathbf{p})$ denotes the communication complexity of simulating $\mathbf{p}$ exactly using shared randomness and classical communication, and $Q_0^*(\mathbf{p})$ denote the communication complexity of simulating $\mathbf{p}$ exactly using shared entanglement and quantum communication. One-way communication, where only Alice sends a message to Bob, is denoted $\rightarrow$. In the simultaneous messages model, denoted $\|$, each player sends a message to the referee, who does not know the inputs of either player, and has to produce the output. Shared entanglement is indicated by the superscript $*$. For any distribution $\mathbf{p}$,

- Theorem 2: $\mathrm{prt}(\mathbf{p}) = \mathrm{eff}(\mathbf{p})$,
- Theorem 3: $Q_0^*(\mathbf{p}) \geq \frac{1}{2}\log(\mathrm{eff}^*(\mathbf{p}))$,
- Theorem 4: $\gamma_2(\mathbf{p}) \leq 2\ \mathrm{eff}^*(\mathbf{p})$ and $\nu(\mathbf{p}) \leq 2\ \mathrm{eff}(\mathbf{p})$ (for nonsignaling $\mathbf{p}$),
- Theorem 5: $R_\varepsilon^{*,\|}(\mathbf{p}) \leq O(\mathrm{eff}^*(\mathbf{p}))$ and $R_\varepsilon^*(\mathbf{p}) \leq O(\sqrt{\mathrm{eff}^*(\mathbf{p})})$.

In the case of one-way communication, the upper bounds are much tighter. The one-sided efficiency measure, which we denote $\mathrm{eff}^{\rightarrow}$ is given in Definition 5.

- Theorem 6: $\frac{1}{2}\log(\mathrm{eff}^{*,\rightarrow}(\mathbf{p})) \leq Q_0^{*,\rightarrow}(\mathbf{p})$; $Q_\varepsilon^{*,\rightarrow}(\mathbf{p}) \leq \log(\mathrm{eff}^{*,\rightarrow}(\mathbf{p})) + O(1)$.

We can use smoothing to handle ϵ error, and demonstrate in the full paper how this is done in practice for some specific examples. For simplicity we have omitted these details in this summary. In the case of boolean functions, this is equivalent to relaxing the exactness constraints in the linear programs.

1.4 Related Work

The question of simulating quantum distributions in the presence of inefficient detectors has long been the object of study, since the reality of the experimental setups is that whenever the detectors can be placed far apart enough to prevent the communication loophole (typically in optics setups), the efficiency is extremely small (on the order of 10%). Gisin and Gisin show that the EPR correlations can be reproduced classically using only 75% detector efficiency [15].

Massar exhibits a Bell inequality that is more robust against detector inefficiency based on the distributed Deutsch Josza game [11]. The Bell inequality is derived from the lower bound on communication complexity for this promise problem [16,17]. Massar shows an upper bound of $\mathrm{eff}(\mathbf{p})$ on expected communication complexity of simulating $\mathbf{p}$. He also states, but does not claim to prove, that a lower bound can be obtained as the logarithm of the efficiency. Buhrman et al. [12,18] show how to get Bell inequalities with better resistance to detector inefficiency by considering multipartite scenarios where players share GHZ type entangled states. Their technique is based on the rectangle bound and they derive a general tradeoff between monochromatic rectangle size, efficiency, and communication. They show a general lower bound on multiparty communication complexity which is exactly as we describe above.

Buhrman et al. [19] show gaps between quantum and classical winning probability for games where the players are each given inputs and attempt, without communication, to produce outputs that satisfy some predicate. In the classical case they use shared randomness and entanglement in the quantum case. Winning probabilities are linear so these translate to large Bell inequality violations.

Lower bounds for communication complexity of simulating distributions were first studied in a systematic way by Degorre et al. [10]. These bounds are shown to be closely related to the nuclear norm and factorization norm [14], and the dual expressions are interpreted as Bell inequality violations. Jain and Klauck define a Las Vegas partition bound where protocols are allowed to abort [1].

2 Preliminaries

2.1 Classical Partition Bound

The partition bound of Jain and Klauck [1] is given as a linear program, following the approach of Lovász [20] and studied in more depth by Karchmer et al. [21].

Definition 1 (Partition bound [1]). *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be any partial function whose domain we write f^{-1}. Then $\mathrm{prt}_\epsilon(f)$ is defined to be the optimal value of the following linear program, where R ranges over the rectangles from $\mathcal{X} \times \mathcal{Y}$ and z ranges over the set $\mathcal{Z}$:*

$$\mathrm{prt}_\epsilon(f) = \min_{w_{R,z} \geq 0} \sum_{R,z} w_{R,z} \ \textit{subject to} \sum_{R:(x,y)\in R} w_{R,f(x,y)} \geq 1 - \epsilon \quad \forall x,y \in f^{-1}$$
$$\sum_{z} \sum_{R:(x,y)\in R} w_{R,z} = 1 \quad \forall x,y \in \mathcal{X} \times \mathcal{Y} \ .$$

Jain and Klauck [1] show that $R_\epsilon(f) \geq \log(\mathrm{prt}_\epsilon(f))$. The partition bound subsumes almost all previously known techniques [1], in particular the factorization norm [14], rectangle or corruption bound [7], and discrepancy [22,23].

2.2 Local and Quantum Distributions

Given a distribution $\mathbf{p}$, how much communication is required if Alice is given $x \in \mathcal{X}$, Bob is given $y \in \mathcal{Y}$, and their goal is to output $a, b \in \mathcal{A} \times \mathcal{B}$ with probability $p(a, b|x, y)$?

Some classes of distributions are of interest and have been widely studied in quantum information theory since the seminal paper of Bell [9]. The local deterministic distributions, denoted $\ell \in \mathcal{L}_{\mathrm{det}}$, are the ones where Alice outputs according to a deterministic strategy, i.e., a (deterministic) function of x, and Bob independently outputs as a function of y. The local distributions $\mathcal{L}$ are any distribution over the local deterministic strategies. Mathematically this corresponds to taking convex combinations of the local deterministic distributions, and operationally to zero-communication protocols with shared randomness.

We will also consider local strategies that are allowed to output $\perp$ when the players abort the protocol. We will use the notation $\mathcal{L}^{\perp}_{\mathrm{det}}$ and $\mathcal{L}^{\perp}$ to denote these strategies, where $\perp$ is added to the possible outputs for both players, and $\perp \notin \mathcal{A} \cup \mathcal{B}$. Therefore, when $\ell \in \mathcal{L}^{\perp}_{\mathrm{det}}$ or $\mathcal{L}^{\perp}$, $l(a, b|x, y)$ is not conditioned on $a, b \neq \perp$ since $\perp$ is a valid output for such distributions.

The quantum distributions, denoted $\mathbf{q} \in \mathcal{Q}$, result from applying measurements to a shared quantum state. Each player outputs the measurement outcome. In communication complexity, these are zero-communication protocols with shared entanglement. When players are allowed to abort, the corresponding set of distributions is denoted $\mathcal{Q}^{\perp}$.

Consider a boolean function $f : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ whose communication complexity we wish to study. First, we split the output so that if $f(x, y) = 0$, Alice and Bob are required to output the same bit, and if $f(x,y)=1$, they output different bits. Let us further require Alice's marginal distribution to be uniform, likewise for Bob. Call the resulting distribution $\mathbf{p}_f$. Computing f reduces to computing $\mathbf{p}_f$ and Alice sending her outcome to Bob. For any f, p_f is nonsignaling, that is, the marginals $p(a|x,y)=p(a|xy')$ for any a,x,y,y', and $p(b|x,y)=p(b|x',y)$ for any b,x,x',y.

2.3 Communication Complexity Measures

$R_\epsilon(\mathbf{p})$ is the minimum amount of communication necessary to reproduce the distribution $\mathbf{p}$ in the worst case, up to ϵ in total variation distance for all x,y. We write $|\mathbf{p}-\mathbf{p}'|_1\le\epsilon$ to mean that for any x,y, $\sum_{a,b}|p(a,b|x,y)-p'(a,b|x,y)|\le\epsilon$. We use Q to denote quantum communication, and the superscript $*$ denotes the presence of shared entanglement. We use superscripts $\rightarrow$ for one-way communication (i.e, when only Alice can send a message to Bob), and $\|$ for simultaneous messages (i.e., when Alice and Bob cannot communicate to each other, but are only allowed to send a message to a third party who should produce the final output of the protocol). The usual relation $Q^*_\epsilon(\mathbf{p})\le R_\epsilon(\mathbf{p})$ holds for any $\epsilon,\mathbf{p}$.

For all the models of randomized communication, we assume shared randomness between the players. Except in the case of simultaneous messages, this is the same as private randomness up to a logarithmic additive term [24]. (Ref. [10] sketches how to adapt Newman's theorem to the case of distributions.)

3 Partition Bound and Detector Inefficiency

3.1 The Partition Bound for Distributions

We extend the partition bound to the more general setting of simulating a distribution $p(a,b|x,y)$ instead of computing a function.

Definition 2. *For any distribution $\mathbf{p}=p(a,b|x,y)$, over inputs $x\in\mathcal{X},y\in\mathcal{Y}$ and outputs $a\in\mathcal{A},b\in\mathcal{B}$, define* $\mathrm{prt}(\mathbf{p})$ *to be the optimal value of the following linear program. The variables of the program are $w_{R,\ell}$, where R ranges over the rectangles from $\mathcal{X}\times\mathcal{Y}$ and ℓ ranges over the local deterministic distributions with outputs in $\mathcal{A}\times\mathcal{B}$.*

$$\mathrm{prt}(\mathbf{p}) = \min_{w_{R,\ell}\ge 0}\sum_{R,\ell} w_{R,\ell}$$

$$\textit{subject to}\quad \sum_{R,\ell:x,y\in R} w_{R,\ell}\cdot l(a,b|x,y)=p(a,b|x,y)\quad \forall x,y,a,b\in\mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B}\ .$$

For randomized communication with error, $\mathrm{prt}_\epsilon(\mathbf{p})=\min_{|p'-p|_1\le\epsilon}\mathrm{prt}(\mathbf{p}')$.

In the special case of a distribution $\mathbf{p}_f$ arising from a function f, we have as expected $\mathrm{prt}_\epsilon(\mathbf{p}_f)=\mathrm{prt}_\epsilon(f)$. For the general case of a distribution $\mathbf{p}$, we can show that $R_\varepsilon(\mathbf{p})\ge\log\mathrm{prt}_\varepsilon(\mathbf{p})$. Rather than proving this directly, we will first show that this partition bound is equivalent to another bound based on the notion of efficiency.

3.2 The Efficiency Bound

For any distribution $\mathbf{p}$, $\mathrm{eff}(\mathbf{p})$ is the inverse of the maximum efficiency sufficient to simulate it classically with shared randomness, without communication.

Definition 3. *For any distribution* $\mathbf{p}$ *with inputs* $\mathcal{X} \times \mathcal{Y}$ *and outputs in* $\mathcal{A} \times \mathcal{B}$, $\mathrm{eff}(\mathbf{p}) = 1/\zeta_{\mathrm{opt}}$, *where* ζ_{opt} *is the optimal value of the following linear program. The variables are* ζ *and* q_ℓ, *where* ℓ *ranges over local deterministic protocols with inputs taken from* $\mathcal{X} \times \mathcal{Y}$ *and outputs in* $\mathcal{A} \cup \{\perp\} \times \mathcal{B} \cup \{\perp\}$.

$$\begin{aligned} \zeta_{\mathrm{opt}} &= \max_{\zeta, q_\ell \geq 0} \zeta \\ \textit{subject to} & \sum_{\ell \in \mathcal{L}^{\perp}_{\mathrm{det}}} q_\ell l(a,b|x,y) = \zeta p(a,b|x,y) \qquad \forall x,y,a,b \in \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B} \\ & \sum_{\ell \in \mathcal{L}^{\perp}_{\mathrm{det}}} q_\ell = 1 \ . \end{aligned}$$

For randomized communication with error, define $\mathrm{eff}_\epsilon(\mathbf{p}) = \min_{|p'-p|_1 \leq \epsilon} \mathrm{eff}(\mathbf{p}')$.

The first constraint says that the local distribution, conditioned on both outputs differing from $\perp$, equals $\mathbf{p}$, and the second is a normalization constraint. Note that the efficiency ζ is the same for every input x, y. This is surprisingly important and the relaxation $\zeta_{x,y} \geq \zeta$ does not appear to coincide with the partition bound. Other more realistic variants (for the Bell setting), such as players aborting independently of one another, could be considered as well. We note that this would not result in a linear program.

Theorem 1 ([11,12]). $R_\epsilon(\mathbf{p}) \geq \log \mathrm{eff}_\epsilon(\mathbf{p})$.

Proof (sketch). Let P be a randomized protocol for a distribution $\mathbf{p}'$ with $|\mathbf{p} - \mathbf{p}'|_1 \leq \epsilon$, using t bits of communication. We assume that the total number of bits exchanged is independent of the execution of the protocol, introducing dummy bits at the end of the protocol if necessary. Let q_l be the following distribution over local deterministic protocols ℓ: Alice and Bob pick a transcript $T \in \{0,1\}^t$ using shared randomness. If T is consistent with P, Alice outputs according to P, otherwise she outputs $\perp$; similarly for Bob. Only one transcript is valid for Alice and Bob simultaneously, so the probability that neither player outputs $\perp$ is exactly 2^{-t}. This satisfies the constraints of $\mathrm{eff}(\mathbf{p}')$ with $\zeta = 2^{-t}$. □

Theorem 2. *For any distribution* $\mathbf{p}$, $\mathrm{eff}(\mathbf{p}) = \mathrm{prt}(\mathbf{p})$.

Proof. In the partition bound, a pair (ℓ, R), where ℓ is a local distribution with outputs in $\mathcal{A} \times \mathcal{B}$ and R is a rectangle, defines a local distribution ℓ_R with outputs in $(\mathcal{A} \cup \{\perp\}) \times (\mathcal{B} \cup \{\perp\})$, where Alice outputs as in ℓ if $x \in R$, and outputs $\perp$ otherwise (similarly for Bob). Let $(a_0, b_0) \in \mathcal{A} \times \mathcal{B}$ be an arbitrary pair of outputs. In the efficiency bound, a distribution $\ell \in \mathcal{L}^{\perp}_{\mathrm{det}}$ defines both a rectangle being the set of inputs where neither Alice nor Bob abort, and a local distribution $\ell' \in \mathcal{L}_{\mathrm{det}}$ where Alice outputs as ℓ if the output is different from

$\perp$ and a_0 otherwise (similarly for Bob with b_0). We can transform the linear program for $\mathrm{prt}(\mathbf{p})$ into the linear program for $\mathrm{eff}(\mathbf{p})$ by making the change of variables: $\zeta = \left(\sum_{R,\ell} w_{R,\ell}\right)^{-1}$ and $q_{\ell_R} = \zeta\, w_{R,\ell}$. $\square$

3.3 Lower Bound for Quantum Communication Complexity

By replacing local distributions by quantum distributions we get a strong new lower bound on quantum communication that subsumes the factorization norm.

Definition 4. *For any distribution* $\mathbf{p}$ *with inputs* $\mathcal{X} \times \mathcal{Y}$ *and outputs* $\mathcal{A} \times \mathcal{B}$, $\mathrm{eff}^*(\mathbf{p}) = 1/\eta^*$, *with* η^* *the optimal value of the following (non-linear) program.*

$$\max_{\zeta, \mathbf{q} \in \mathcal{Q}^{\perp}} \zeta \quad \textit{subject to} \quad q(a,b|x,y) = \zeta p(a,b|x,y) \quad \forall x,y,a,b \in \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B}\ .$$

As before, we let $\mathrm{eff}^*_\epsilon(\mathbf{p}) = \min_{|p'-p|_1 \leq \epsilon} \mathrm{eff}^*(\mathbf{p}')$.

Theorem 3. $Q^*_\epsilon(\mathbf{p}) \geq \frac{1}{2} \log \mathrm{eff}^*_\epsilon(\mathbf{p})$.

The proof follows the lines of the proof for eff, except that we first use teleportation to replace quantum communication by entanglement-assisted classical communication.

Since the local distributions form a subset of the quantum distributions, $\mathrm{eff}^*(\mathbf{p}) \leq \mathrm{eff}(\mathbf{p})$ for any $\mathbf{p}$. We can show that the efficiency is bounded below by the factorization norm.

Theorem 4. *For any nonsignaling* $\mathbf{p}$, $\nu(\mathbf{p}) \leq 2\ \mathrm{eff}(\mathbf{p})$ *and* $\gamma_2(\mathbf{p}) \leq 2\ \mathrm{eff}^*(\mathbf{p})$.

The proof is provided in the long version of the article, and is based on the fact that a reject outcome can be replaced by a random outcome.

3.4 Proving Concrete Lower Bounds Using the Dual

To prove lower bounds, we use the dual formulation, and give a feasible solution.

Lemma 1 (Dual formulation). *For any distribution* $\mathbf{p}$,

$$\begin{aligned} \mathrm{eff}(\mathbf{p}) = \max_{B_{abxy}} & \sum_{a,b,x,y \in \mathcal{A}\times\mathcal{B}\times\mathcal{X}\times\mathcal{Y}} B_{abxy} p(a,b|x,y) \\ \textit{subject to} & \sum_{a,b,x,y \in \mathcal{A}\times\mathcal{B}\times\mathcal{X}\times\mathcal{Y}} B_{abxy} l(ab|xy) \leq 1 \qquad \forall \ell \in \mathcal{L}_{\mathrm{det}}^{\perp}\ . \end{aligned}$$

For $\mathrm{eff}^*(\mathbf{p})$ *the expression is identical save for replacing* ℓ *by* $\mathbf{q} \in \mathcal{Q}^{\perp}$.

The first equality (for eff) uses linear programming duality and the second (for eff^*) can be shown using Lagrange multipliers.

Concretely, how does one go about finding a feasible solution to the dual? Consider a distribution $\mathbf{p}$ for which we would like to find a lower bound. We construct a Bell inequality $B(\mathbf{p}) = \sum_{a,b,x,y} B_{abxy} p(a,b|x,y)$ so that $B(\mathbf{p})$ is large, and $B(\ell)$ is small for every $\ell \in \mathcal{L}^{\perp}$. The goal is to balance the coefficients so that they correlate well with the distribution $\mathbf{p}$ and badly with local strategies.

In the full paper, we give an example for a distribution based on the Hidden Matching problem [4,5,19]; we also study the Khot Vishnoi game for which there is a large Bell inequality violation [25,19]. We reformulate it as a quantum distribution $\mathbf{p} \in \mathcal{Q}$ (that is, $Q_0(\mathbf{p}) = 0$) and prove a lower bound $R_0(\mathbf{p}) = \Omega(\log(n))$. The proofs use many of the techniques Burhman et al. used to establish large Bell inequality violations [19].

4 Upper Bounds for One- and Two-Way Communication

The efficiency bound subsumes most known lower bound techniques for randomized communication complexity. How close is it to being tight? An upper bound on randomized communication is proven by Massar [11]. We give a similar bound for quantum communication complexity in terms of eff^*.

Theorem 5. *For any distribution* $\mathbf{p}$ *with outputs in* $\mathcal{A}, \mathcal{B}$*,*

1. $R_\epsilon^{\|}(\mathbf{p}) \le \mathrm{eff}(\mathbf{p}) \log(\frac{1}{\epsilon}) \log(\#(\mathcal{A} \times \mathcal{B}))$ *[11],*
2. $R_\epsilon^{*,\|}(\mathbf{p}) \le \mathrm{eff}^*(\mathbf{p}) \log(\frac{1}{\epsilon}) \log(\#(\mathcal{A} \times \mathcal{B}))$*,*
3. $R_\epsilon^{*}(\mathbf{p}) \le O\left(\sqrt{\mathrm{eff}^*(\mathbf{p}) \log(\frac{1}{\epsilon})}\right)$.

Proof (Sketch). For the first two items, the players simulate a zero-communication protocol $\lceil \log(\frac{1}{\epsilon}) \mathrm{eff}(\mathbf{p}) \rceil$ times and send the outcomes to the referee, who outputs a non-aborting run. For the third item, a quadratic speedup is possible by using a quantum protocol for disjointness [16,26,27] on the input u, v, where u_i is 0 if Alice aborts in the ith run and 0 otherwise, similarly for v with Bob. □

The partition and efficiency bounds can easily be tailored to the case of one-way communication protocols. For the partition bound, we consider only rectangles of the form $X \times Y$ with $Y = \mathcal{Y}$. For the efficiency bound, this amounts to only letting Alice abort the protocol. The set of local (resp. quantum) distributions where only Alice can abort is denoted $\mathcal{L}_{\mathrm{det}}^{\perp A}$ (resp. $\mathcal{Q}^{\perp A}$).

Definition 5. *Define* $\mathrm{eff}^{\rightarrow}$ *in the same way as* eff*, replacing* $\mathcal{L}_{\mathrm{det}}^{\perp}$ *with* $\mathcal{L}_{\mathrm{det}}^{\perp A}$ *; and* $\mathrm{eff}^{*,\rightarrow}$*, by replacing* $\mathcal{Q}^{\perp}$ *with* $\mathcal{Q}^{\perp A}$ *in the definition of* eff^**.*

The dual can also be interpreted as violations of Bell inequalities.

Lemma 2 (Dual formulation for one-way efficiency). *The dual for the one-way efficiency is as in the dual for* eff*, replacing* $\mathcal{L}_{\mathrm{det}}^{\perp}$ *with* $\mathcal{L}_{\mathrm{det}}^{\perp A}$*.*

Theorem 6. $R_0^{\rightarrow}(\mathbf{p}) \ge \log \mathrm{eff}^{\rightarrow}(\mathbf{p})$ *and* $Q_0^{*,\rightarrow}(\mathbf{p}) \ge \frac{1}{2} \log \mathrm{eff}^{*,\rightarrow}(\mathbf{p})$.

The proof is similar to the two-way case. Here we show that the one-way partition bound is tight, up to arbitrarily small error. We give the results for quantum communication since the rectangle bound is already known to be tight for randomized communication complexity [28].

Theorem 7. $Q_\epsilon^{*,\rightarrow}(\mathbf{p}) \leq \log(\mathrm{eff}^{*,\rightarrow}(\mathbf{p})) + \log\log(1/(\epsilon))$.

Proof. Let $(\zeta, \mathbf{q})$ be an optimal solution for $\mathrm{eff}^{*,\rightarrow}(\mathbf{p})$. For any x, y, if we sample a, b according to $\mathbf{q}$, $\Pr_{\mathbf{q}}[a \neq \perp | x] = \zeta$ and $\Pr_{\mathbf{q}}[a, b | x, y] = \zeta p(a, b | x, y)$ for all $a, b \neq \perp$ and all x, y. Let Alice and Bob simulate this quantum distribution $N = \lceil \log(\frac{1}{\epsilon})\frac{1}{\zeta} \rceil$ times, keeping a record of the outputs (a_i, b_i) for $i \in [N]$. Since this distribution is quantum, this requires no communication (only shared entanglement). Alice then communicates an index $i \in [N]$ such that $a_i \neq \perp$, if such an index exists, or just a random index if $a_i = \perp$ for all $i \in [N]$. Alice and Bob output (a_i, b_i) corresponding to this index.

The correctness of the protocol follows from the fact that $\Pr_{\mathbf{q}}[a_i = \perp (\forall i)] = (1-\zeta)^N \leq e^{-\zeta N} \leq \epsilon$. The protocol then requires $\log N$ bits of communication. □

5 Conclusion and Open Problems

There are many questions to explore. In experimental setups, in particular with optics, one is faced with the very real problem that in most runs of an experiment, no outcome is recorded. The frequency with which apparatus don't yield an outcome is called detector inefficiency. Can we find explicit Bell inequalities for quantum distributions that are very resistant to detector inefficiency? For experimental purposes, it is also important for the distribution to be feasible to implement. One way to achieve this could be to prove stronger bounds for the inequalities based on the GHZ paradox given by Buhrman et al. [18]. Their analysis is based on a tradeoff derived from the rectangle bound. It may be possible to give sharper bounds with our techniques. Another is to consider asymmetric Bell inequalities and dimension witnesses [29,30]. Here, Alice prepares a state and Bob makes a measurement. The goal is to have a Bell inequality demonstrating that Alice's system has to be large. The dimension is exponential in the size of Alice's message to Bob, so proving a lower bound on one-way communication complexity gives a lower bound on the dimension. In order to close the detection loophole, one can also consider more realistic models of inefficiency, where the failure to produce a measurement outcome is the result of either the entangled state not being produced, or the detector of each player failing independently. This could be exploited by defining a stronger version of the partition/efficiency bound that also takes into account the probabilities of events where only one of the players produces a valid outcome. While such a variation of the efficiency bound is meaningful for Bell tests, we have not considered it here as it might not be a lower bound on communication complexity.

We would like to see more applications. For the Khot Vishnoi distribution, we are not aware of any nontrivial upper bound so there is a gap to be improved.

A family of lower bound techniques still not subsumed by the partition bound are the information theoretic bounds such as information complexity [31]. It was recently shown that information complexity is an upper bound on discrepancy [32], and this upper bound was subsequently extended to a relaxation of the partition bound [33]. This *relaxed* partition bound also subsumes most algebraic and combinatorial lower bound techniques, with the notable exception of the partition bound itself, and we would therefore like to see connections one way or the other between information complexity and the partition bound.

Finally, the quantum partition bound is of particular interest. It is hard to apply since it is not linear, and it amounts to finding a Tsirelson inequality, a harder task than finding a good Bell inequality, that can nevertheless be approached via semidefinite programming [34,35]. On the other hand, it is a very strong bound and one can hope to get a better upper bound on quantum communication complexity. Finding tight bounds complexity would be an important step to proving the existence, or not, of exponential gaps for total functions.

Acknowledgements. We wish to particularly thank Raghav Kulkarni and Iordanis Kerenidis for many fruitful discussions. Research funded in part by the EU grant QCS, ANR Jeune Chercheur CRYQ, ANR Blanc QRAC and EU ANR Chist-ERA DIQIP.

References

1. Jain, R., Klauck, H.: The partition bound for classical complexity and query complexity. In: Proc. 25th CCC 2010, pp. 247–258 (2010)
2. Newman, I., Szegedy, M.: Public vs. private coin flips in one round communication games. In: Proc. 28th STOC 1996, pp. 561–570 (1996)
3. Buhrman, H., Cleve, R., Watrous, J., de Wolf, R.: Quantum fingerprinting. Phys. Rev. Lett. 87(16), 167902 (2001)
4. Bar-Yossef, Z., Jayram, T.S., Kerenidis, I.: Exponential separation of quantum and classical one-way communication complexity. SIAM J. Comput. 38(1), 366–384 (2008)
5. Gavinsky, D., Kempe, J., Kerenidis, I., Raz, R., de Wolf, R.: Exponential separation for one-way quantum communication complexity, with applications to cryptography. SIAM J. Comput. 38(5), 1695–1708 (2008)
6. Klartag, B., Regev, O.: Quantum one-way communication can be exponentially stronger than classical communication. In: Proc. 43rd STOC 2011, pp. 31–40 (2011)
7. Yao, A.C.: Lower bounds by probabilistic arguments. In: Proc. 24th FOCS 1983, pp. 420–428 (1983)
8. de Graaf, M., de Wolf, R.: On Quantum Versions of the Yao Principle. In: Alt, H., Ferreira, A. (eds.) STACS 2002. LNCS, vol. 2285, pp. 347–358. Springer, Heidelberg (2002)
9. Bell, J.S.: On the Einstein Podolsky Rosen paradox. Physics 1, 195 (1964)
10. Degorre, J., Kaplan, M., Laplante, S., Roland, J.: The communication complexity of non-signaling distributions. Quantum Information and Computation 11(7-8), 649–676 (2011)
11. Massar, S.: Non locality, closing the detection loophole and communication complexity. Phys. Rev. A 65, 032121 (2002)
12. Buhrman, H., Høyer, P., Massar, S., Röhrig, H.: Combinatorics and quantum nonlocality. Phys. Rev. Lett. 91, 048301 (2003)
13. Lee, T., Shraibman, A.: Lower bounds in communication complexity. Foundations and Trends in Theoretical Computer Science 3(4), 263–399 (2009)

14. Linial, N., Shraibman, A.: Lower bounds in communication complexity based on factorization norms. Random Structures and Algorithms 34(3), 368–394 (2009)
15. Gisin, B., Gisin, N.: A local hidden variable model of quantum correlation exploiting the detection loophole. Phys. Lett. A 260, 323–327 (1999)
16. Buhrman, H., Cleve, R., Wigderson, A.: Quantum vs classical communication and computation. In: Proc. 30th STOC 1998, pp. 63–68 (1998)
17. Brassard, G., Cleve, R., Tapp, A.: Cost of exactly simulating quantum entanglement with classical communication. Phys. Rev. Lett. 83, 1874–1877 (1999)
18. Buhrman, H., Høyer, P., Massar, S., Röhrig, H.: Multipartite nonlocal quantum correlations resistant to imperfections. Phys. Rev. A 73, 012321 (2006)
19. Buhrman, H., Regev, O., Scarpa, G., de Wolf, R.: Near-optimal and explicit Bell inequality violations. In: Proc. 26th CCC 2011, pp. 157–166 (2011)
20. Lovász, L.: Communication Complexity: a Survey. In: Paths, Flows, and VLSI Layout, B.H. Korte edition. Springer (1990)
21. Karchmer, M., Kushilevitz, E., Nisan, N.: Fractional covers and communication complexity. SIAM J. Discrete Math. 8(1), 76–92 (1995)
22. Chor, B., Goldreich, O.: Unbiased bits from sources of weak randomness and probabilistic communication complexity. In: Proc. 26th FOCS 1985, pp. 429–442 (1985)
23. Babai, L., Nisan, N., Szegedy, M.: Multiparty protocols and logspace-hard pseudorandom sequences. In: Proc. 21st STOC 1989, pp. 1–11 (1989)
24. Newman, I.: Private vs. common random bits in communication complexity. Information Processing Letters 39(2), 61–71 (1991)
25. Khot, S., Vishnoi, N.: The unique games conjecture, integrality gap for cut problems and embeddability of negative type metrics into l_1. In: Proc. 46th FOCS 2005, pp. 53–62 (2005)
26. Høyer, P., de Wolf, R.: Improved Quantum Communication Complexity Bounds for Disjointness and Equality. In: Alt, H., Ferreira, A. (eds.) STACS 2002. LNCS, vol. 2285, pp. 299–310. Springer, Heidelberg (2002)
27. Aaronson, S., Ambainis, A.: Quantum search of spatial regions. Theory of Computing 1, 47–79 (2005)
28. Jain, R., Klauck, H., Nayak, A.: Direct product theorems for communication complexity via subdistribution bounds. In: Proc. 40th STOC 2008, pp. 599–608 (2008)
29. Brunner, N., Pironio, S., Acín, A., Gisin, N., Méthot, A., Scarani, V.: Testing the dimension of Hilbert spaces. Phys. Rev. Lett. 100, 210503 (2008)
30. Vértesi, T., Pironio, S., Brunner, N.: Closing the detection loophole in Bell experiments using qudits. Phys. Rev. Lett. 104, 060401 (2010)
31. Chakrabarti, A., Shi, Y., Wirth, A., Yao, A.: Informational complexity and the direct sum problem for simultaneous message complexity. In: Proc. 42nd FOCS 2001, pp. 270–278 (2001)
32. Braverman, M., Weinstein, O.: A discrepancy lower bound for information complexity. Technical Report 12-164, ECCC (2011)
33. Kerenidis, I., Laplante, S., Lerays, V., Roland, J., Xiao, D.: Lower bounds on information complexity via zero-communication protocols and applications. Technical Report 12-038, ECCC (2012)
34. Navascués, M., Pironio, S., Acín, A.: A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. New Journal of Physics 10(7), 073013 (2008)
35. Doherty, A.C., Liang, Y.-C., Toner, B., Wehner, S.: The quantum moment problem and bounds on entangled multi-prover games. In: Proc. 23rd CCC 2008, pp. 199–210 (2008)