Electronic Colloquium on Computational Complexity, Report No. 23 (2012)

Classical and quantum partition bound and detector inefficiency

S. Laplante
LRI, Université Paris-Sud 11

V. Lerays
LRI, Université Paris-Sud 11

J. Roland
ULB, QuIC, Ecole Polytechnique de Bruxelles

Abstract

In the standard setting of communication complexity, two players each have an input and they wish to compute some function of the joint inputs. This has been the object of much study and a wide variety of lower bound methods have been introduced to address the problem of showing lower bounds on communication. Recently, Jain and Klauck introduced the partition bound, which subsumes many of the known methods, in particular factorization norm (γ_2), discrepancy, and the rectangle (corruption) bound.

Physicists have considered a closely related scenario where two players share a predefined entangled state. Each is given a measurement as input, which they perform on their share of the system. The outcomes of the measurements follow a distribution which is predicted by quantum mechanics. Physicists want to rule out the possibility that there is a classical explanation for the distribution, through loopholes such as communication or detector inefficiency. In an experimental setting, Bell inequalities [Bel64] are used to distinguish truly quantum from classical behavior.

We present a new lower bound technique based on the notion of detector inefficiency (where some runs are discarded by either of the players) for the extended setting of simulating distributions, and show that it coincides with the partition bound in the special case of computing functions. As usual, the dual form is more feasible to use, and we show that it amounts to constructing an explicit Bell inequality. We also give a lower bound on quantum communication complexity which can be viewed as a quantum extension of the rectangle bound, effectively overcoming the necessity of a quantum minmax theorem.

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.

Finally, an important goal in physics is to devise robust Bell experiments that are impervious to noise and detector inefficiency. We make further progress towards this by giving a general tradeoff between communication, Bell inequality violation, and detector efficiency.

ISSN 1433-8092

1 Introduction

1.1 Communication complexity and the partition bound

Recently, Jain and Klauck [JK10] 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. The algebraic methods and discrepancy give lower bounds on quantum communication complexity, whereas the rectangle bound can show polynomial lower bounds on randomized communication complexity for problems known to have logarithmic quantum protocols.

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 [NS96, BCWdW01, BYJK08, GKK+08], most recently [KR11]. These 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 [Yao83], comes from strong duality of linear programming. This technique appears to be inherently non-applicable to quantum communication complexity (see for instance [dGdW02] which considers a similar question in the setting of query complexity), and the rectangle bound, as a result, is understood to be a strictly classical method for lower bounds.

Contrary to previous combinatorial type lower bounds, the partition bound is proven directly for randomized protocols, without first going to the distributional model. Although the partition bound re-introduces LP duality, the dual variables can no longer be interpreted as a (hard) distribution on the inputs. By the same token, it is harder to get intuition on how to obtain concrete lower bounds for explicit functions.

1.2 Bell experiments

Quantum information 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 quantum, or whether there is a purely classical explanation to the quantum 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 [Bel64] 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 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 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 δ, we say that the efficiency is $\eta = 1 - \delta$. (Here we assume that individual runs are independent of one another.) To close the detection loophope, 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, it 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 [DKLR11]. Here, we show that the partition bound also corresponds to a class of Bell inequalities.

1.3 Summary of results

We focus on detector efficiency and see that it is closely related to the partition bound. 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 [Mas02, BHMR03], 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.

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. To our knowledge this is the first quantum lower bound known to be tight.

Simulating distributions while allowing for runs to be discarded with some probability corresponds to a zero-error randomized protocol. (Jain and Klauck [JK10] also introduce a Las Vegas partition bound for zero-error protocols.) This 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 [LS09a, Theorem 60] (attributed to Harry Buhrman; see also Degorre et al. [DKLR11]). 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.

The following gives a brief summary of our main 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 Section 3.1). $R_0(\mathbf{p})$ denote 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. $R^\eta_\epsilon(\mathbf{p})$ and $Q^\eta_\epsilon(\mathbf{p})$ are defined similarly, except that the players are allowed to abort the protocol with probability at most $1 - \eta$, and when none of them aborts, the distribution they obtain should lie at distance at most ϵ from $\mathbf{p}$. One-way communication, where only Alice sends a message to Bob, is denoted $\rightarrow$. In the simultaneous messages model, each player sends a message to the referee, who does not know the inputs of either player, and has to produce the output. This is denoted by the superscript $\|$. Shared entanglement is indicated by the superscript $*$. For any distribution $\mathbf{p}$,

- Theorem 4: $\mathrm{prt}(\mathbf{p}) = \mathrm{eff}(\mathbf{p})$.
- Theorem 5: $Q^*_0(\mathbf{p}) \geq \frac{1}{2}\log(\mathrm{eff}^*(\mathbf{p}))$
- Theorem 6: $\gamma_2(\mathbf{p}) \leq 2\mathrm{eff}^*(\mathbf{p})$ and $\nu(\mathbf{p}) \leq 2\mathrm{eff}(\mathbf{p})$ (for any non-signaling $\mathbf{p}$).
- Theorem 8: $R^{*,\|}_0(\mathbf{p}) \leq O(\mathrm{eff}^*(\mathbf{p}))$ and $R^*_0(\mathbf{p}) \leq O(\sqrt{\mathrm{eff}^*(\mathbf{p})})$.

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 7.

- Theorems 10, 11: $\log(\mathrm{eff}^{*,\rightarrow}(\mathbf{p})) \leq Q^{\rightarrow}_0(\mathbf{p})$ and $Q^{\eta,*,\rightarrow}_0(\mathbf{p}) \leq \log(\mathrm{eff}^{*,\rightarrow}(\mathbf{p})) + O(1)$.

We can use smoothing to handle ϵ error, and demonstrate how this is done in practice in the examples given in the appendices. 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 5%). Gisin and Gisin show that the EPR correlations can be reproduced classically using only 75% detector efficiency [GG99].

Massar exhibits a Bell inequality that is more robust against detector inefficiency based on the distributed Deutsch Josza game [Mas02]. The Bell inequality is derived from the lower bound on communication complexity for this promise problem [BCW98, BCT99]. He shows an upper bound of $\text{eff}(\mathbf{p})$ 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.* [BHMR03, BHMR06] show how to get Bell inequalities with better resistance to detector inefficiency by considering multipartite scenarios where players share GHZ type entangled states. The 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.* [BRSdW11] 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 can use shared randomness and in the quantum case, they use shared entanglement. 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.* [DKLR11]. These bounds are shown to be closely related to the nuclear norm and factorization norm [LS09b], and the dual expressions are interpreted as Bell inequality violations.

2 Preliminaries

2.1 Classical partition bound

The partition bound of Jain and Klauck [JK10] is given as a linear program, following the approach that was introduced by Lovász [Lov90] and studied in more depth by Karchmer *et al.* [KKN95]. It differs from the rectangle and other combinatorial bounds in that it is formulated directly on the randomized protocol, as opposed to first applying Yao's minmax theorem to reduce to a deterministic protocol with distributional inputs. From a c-bit, ϵ-correct randomized protocol one can infer a distribution over rectangle partitions of size at most 2^c, where each rectangle is assigned an output value z. Set weights $w_{R,z}$ to be the probability that that rectangle R occurs with label z (the same rectangle may occur in different partitions, with different labels and different probabilities). This is a feasible solution to the following linear program.

Definition 1 (Partition bound [JK10])**.** *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be any partial function whose domain we write f^{-1}. Then $prt_\epsilon(f)$ is defined to be the optimal value of the LP:*

$$\begin{aligned} \text{prt}_\epsilon(f) = \min_{w_{R,z} \geq 0} \quad & \textstyle\sum_{R,z} w_{R,z} \\ \textit{subject to} \quad & \textstyle\sum_{R:(x,y)\in R} w_{R,f(x,y)} \geq 1-\epsilon \quad \forall x,y \in f^{-1} \\ & \textstyle\sum_z \sum_{R:(x,y)\in R} w_{R,z} = 1 \quad \forall x,y \in \mathcal{X}\times\mathcal{Y} \end{aligned}$$

Our feasible solution verifies all the constraints and the objective value is at most 2^c, therefore $R_\epsilon(f) \geq \log(\mathrm{prt}_\epsilon(f))$. Jain and Klauck show that the partition bound subsumes a large number of previously known techniques, in particular the factorization norm [LS09b], rectangle or corruption bound [Yao83], and discrepancy [CG85, BNS89].

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 [Bel64]. 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, independently of Bob, who outputs as a function of his input y. The local distributions $\mathcal{L}$ are any distribution over the local deterministic strategies. These correspond to taking convex combinations of the local deterministic distributions, and operationally are interpreted as using shared randomness ("local hidden variables") to decide on a local deterministic strategy.

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 $\perp \notin \mathcal{A} \cup \mathcal{B}$. When $\ell \in \mathcal{L}^\perp_{\mathrm{det}}$ or $\mathcal{L}^\perp$, $l(a, b|x, y)$ is not conditioned on $a, b \neq \perp$.

The quantum distributions, denoted $\mathbf{q} \in \mathcal{Q}$, are the ones that result from applying measurements to each part of a shared entangled bipartite state. Each player outputs the measurement outcome. If the players are allowed to abort, then 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 $f(x, y) = 1$, Alice and Bob output different bits. Let us further require Alice's marginal distribution to be uniform, likewise for Bob. Call the resulting distribution $\mathbf{p}_f$. If $\mathbf{p}_f$ were local, f could be computed with one bit of communication using shared randomness: Alice sends her output to Bob, and Bob XORs it with his output. If $\mathbf{p}_f$ were quantum, there would again be a 1-bit protocol with shared entanglement for f. We are usually interested in distributions requiring nontrivial communication complexity, and lie well beyond these sets.

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 each x, y. We will use the notation $|\mathbf{p} - \mathbf{p}'|_1 \leq \epsilon$ to mean that for any x, y, $\sum_{a,b} |p(a, b|x, y) - p'(a, b|x, y)| \leq \epsilon$.

$R^\eta_0(\mathbf{p})$ is the amount of communication needed to reproduce $\mathbf{p}$ exactly with a protocol which may abort with probability at most η for any input x, y (the probability that it aborts may depend on x, y). The probability produced by the protocol is conditioned on the event that neither player aborts. When the player aborts it outputs $\perp$.

For quantum communication, we use Q to denote quantum communication, and we use the superscript $*$ to denote the presence of shared entanglement. We use superscripts $\to$ 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 $Q^\eta_\epsilon(\mathbf{p}) \leq R^\eta_\epsilon(\mathbf{p})$ holds for any $\epsilon, \eta, \mathbf{p}$. Moreover, since one can always output at random instead of aborting, which introduces at most $1 - \eta$ error for each x, y, we have the following relation between $R_\epsilon(\mathbf{p})$ and $R^\eta_\epsilon(\mathbf{p})$.

Lemma 1. *For any ϵ, η and any distribution $\mathbf{p}$, we have $R_{\epsilon+(1-\eta)}(\mathbf{p}) \leq R^\eta_\epsilon(\mathbf{p})$.*

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 [New91].

3 Partition bound and detector inefficiency

3.1 The partition bound for distributions

We now give our extension of the partition bound to the setting where we wish to simulate a distribution $p(a,b|x,y)$ instead of computing a function. In this setting, protocols with shared randomness also lead to a distribution over rectangle partitions; however, since each player ouputs a value, the label associated with each rectangle is a local deterministic distribution, which we denote by ℓ. Here we give a more general definition, for protocols that use communication and allow the players to abort a run with some fixed probability $1-\eta$. The partition bound corresponds to the case $\eta = 1$ and the Las Vegas partition bound [JK10] is closely related to the case $\eta = 1/2$.

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 $\mathrm{prt}^\eta(\mathbf{p})$ to be the optimal value of the following linear program. The variables of the program are $w_{R,\ell}$, where R ranges over all the rectangles from $\mathcal{X}\times\mathcal{Y}$ and ℓ ranges over all the local deterministic distributions, with outputs in $\mathcal{A}\times\mathcal{B}$.*

$$\begin{aligned} \mathrm{prt}^\eta(\mathbf{p}) = \min_{w_{R,\ell}\geq 0} & \sum_{R,\ell\in\mathcal{L}_{\mathrm{det}}} w_{R,\ell} & \\ \textit{subject to} & \sum_{R,\ell\in\mathcal{L}_{\mathrm{det}}:x,y\in R} w_{R,\ell}\cdot l(a,b|x,y) = p(a,b|x,y)\cdot\eta_{x,y} & \forall x,y,a,b \in \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B} \\ & \eta \leq \eta_{x,y} \leq 1 & \forall x,y \in \mathcal{X}\times\mathcal{Y}. \end{aligned}$$

When $\eta = 1$ we write $\mathrm{prt}(\mathbf{p}) = \mathrm{prt}^1(\mathbf{p})$. In this case the linear program simplifies:

$$\begin{aligned} \mathrm{prt}(\mathbf{p}) = \min_{w_{R,\ell}\geq 0} & \sum_{R,\ell} w_{R,\ell} & \\ \textit{subject to} & \sum_{R,\ell:x,y\in R} w_{R,\ell}\cdot l(a,b|x,y) = p(a,b|x,y) & \forall x,y,a,b \in \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B} \end{aligned}$$

For randomized communication with error, we define $\mathrm{prt}^\eta_\epsilon(\mathbf{p}) = \min_{|p'-p|_1\leq\epsilon}\mathrm{prt}^\eta(\mathbf{p}')$.

Theorem 2. *For any distribution $\mathbf{p}$, $R^\eta_\epsilon(\mathbf{p}) \geq \log(\mathrm{prt}^\eta_\epsilon(\mathbf{p}))$.*

We have included a direct proof of the theorem in Appendix A, which for $\eta = 1$ is essentially the same as the original partition bound, sketched above, where output values z are replaced with local deterministic strategies ℓ. We will now turn to an alternative, arguably simpler, proof by introducing the efficiency bound.

3.2 The efficiency bound

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

Definition 3. *For any distribution $\mathbf{p}$ with inputs in $\mathcal{X}\times\mathcal{Y}$ and outputs in $\mathcal{A}\times\mathcal{B}$, define $\mathrm{eff}(\mathbf{p}) = 1/\zeta_{\mathrm{opt}}$, 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 $\mathcal{A}\cup\{\perp\}\times\mathcal{B}\cup\{\perp\}$.*

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

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

The first constraint expresses the fact that the local distribution, conditioned on both outputs differing from $\perp$, equals the target distribution, and the second is a normalization constraint. Note here that the efficiency ζ is the same for every input x, y. We could relax to $\zeta_{x,y} \geq \zeta$ to get another useful lower bound. However, this bound does not appear to coincide with the partition bound so we do not consider it in detail here.

Theorem 3. *[Mas02, BHMR03]* $R_\epsilon(\mathbf{p}) \geq \log \mathrm{eff}_\epsilon(\mathbf{p})$.

Proof (sketch). Let P be a randomized communication 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. We construct a distribution q_l over local deterministic protocols ℓ as follows: Alice and Bob pick a random 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. Note that since only one transcript can be valid for Alice and Bob simultaneously, the probability that neither player outputs $\perp$ is exactly 2^{-t}. Therefore, this satisfies the constraints of $\mathrm{eff}(\mathbf{p}')$ with $\zeta = 2^{-t}$. □

We are now ready to show that the two bounds are equal.

Theorem 4. *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). We can transform the LP for $\mathrm{prt}(\mathbf{p})$ into the LP for $\mathrm{eff}(\mathbf{p})$ by making the change of variables: $\zeta = \left(\sum_{R,\ell} w_{R,\ell}\right)^{-1}$ and $q_{\ell_R} = \zeta\ w_{R,\ell}$. □

We define $\mathrm{eff}^\eta(\mathbf{p})$ which is equal to $\mathrm{prt}^\eta(\mathbf{p})$. The details are given in Appendix B.

3.3 Lower bound for quantum communication complexity

By replacing the local distributions by quantum distributions we get a lower bound on quantum communication. Insomuch as the partition bound is an extension of the rectangle bound, this quantum analogue of the partition bound can be thought of as a lower bound on quantum communication complexity using an extension of the rectangle bound, effectively circumventing Yao's minmax theorem.

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

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

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

Theorem 5. $Q^*_\epsilon(\mathbf{p}) \geq \frac{1}{2} \log \mathrm{eff}^*_\epsilon(\mathbf{p})$.

Proof (sketch). Let Q be a t qubit communication protocol for $\mathbf{p}'$ with $|\mathbf{p}' - \mathbf{p}|_1 \leq \epsilon$. We use teleportation and classical communication to send every qubit, hence obtaining an entanglement-assisted protocol using at most $2t$ bits of classical communication. We also introduce dummy bits so that the number of bits exchanged is exactly $2t$, independently of the execution of the protocol. Then proceed as before: guess a classical transcript and abort if the transcript is not valid. Otherwise output according to the protocol. The result is a protocol using zero communication and entanglement with efficiency 2^{-2t}, satisfying the constraints of the program. □

Since the local distributions form a subset of the quantum distributions, $\mathrm{eff}^*(\mathbf{p}) \leq \mathrm{eff}(\mathbf{p})$ for any $\mathbf{p}$.

3.4 Upper bound for the factorization norm

Jain and Klauck have shown that the partition bound is an upper bound on γ_2 for boolean functions (in fact they show that the weaker smooth rectangle bound is an upper bound on γ_2 as well) [JK10]. The lower bounds ν and γ_2 were extended to nonsignaling distributions by Degorre et al [DKLR11]. Nonsignaling distributions are superset of quantum distributions for which the marginal distributions are independent of the other player's input.

Definition 5 (Non-signaling distributions)**.** *A bipartite, conditional distribution* $\mathbf{p}$ *is non-signaling if*

$$\begin{aligned} \forall a, x, y, y', \quad & \textstyle\sum_b p(a,b|x,y) = \sum_b p(a,b|x,y'), \\ \forall b, x, x', y, \quad & \textstyle\sum_a p(a,b|x,y) = \sum_a p(a,b|x',y). \end{aligned}$$

Definition 6 ([DKLR11])**.** *For any non-signaling distribution* $\mathbf{p}$*,*

- $\nu(\mathbf{p}) = \min\{\sum_i |\, q_i \,| \colon \exists \mathbf{p}_i \in \mathcal{L}, q_i \in \mathbb{R}, \mathbf{p} = \sum_i q_i \mathbf{p}_i\}$,
- $\gamma_2(\mathbf{p}) = \min\{\sum_i |\, q_i \,| \colon \exists \mathbf{p}_i \in \mathcal{Q}, q_i \in \mathbb{R}, \mathbf{p} = \sum_i q_i \mathbf{p}_i\}$,

It was shown that for any Boolean function f, the factorization norm $\gamma_2(f) = \Theta(\gamma_2(\mathbf{p}_f))$, and similarly for the nuclear norm, $\nu(f) = \Theta(\gamma_2(\mathbf{p}_f))$ [DKLR11]. (The definition of $\mathbf{p}_f$ is given in Section 2.2.)

Theorem 6. *For any nonsignaling* $\mathbf{p}$*,* $\nu(\mathbf{p}) \leq 2\mathrm{eff}(\mathbf{p})$ *and* $\gamma_2(\mathbf{p}) \leq 2\mathrm{eff}^*(\mathbf{p})$*.*

Proof. We sketch the proof for γ_2 vs eff^*. The proof for ν vs. eff is similar.

Let $\zeta, \mathbf{q}$ be an optimal solution for $\mathrm{eff}^*(\mathbf{p})$. Then $q(a,b|x,y) = \zeta p(a,b|x,y) \forall x,y,a,b \in \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B}$, where $\mathbf{q}$ outputs $\perp$ with probability $1-\zeta$ for every x, y. Define $\tilde{\mathbf{q}} \in \mathcal{Q}$ as the distribution where the players output according to $\mathbf{q}$ unless their outcome is $\perp$, in which case they output independently from the other player, uniformly at random from $\mathcal{A}$ or $\mathcal{B}$. We can write $\tilde{q}(a,b|x,y) = q(a,b|x,y) + (1-\zeta) r(a,b|x,y)$ where $\mathbf{r}$ is the distribution $\tilde{\mathbf{q}}$ conditioned on one of the players having output $\perp$ when they ran $\mathbf{q}$. Notice that $\mathbf{r}$ is local (it is a distribution over product distributions). Therefore, on $\mathcal{A}\times\mathcal{B}$, $\mathbf{p} = \frac{1}{\zeta}\mathbf{q} = \frac{1}{\zeta}\tilde{\mathbf{q}} - \frac{1-\zeta}{\zeta}\mathbf{r}$. This is an affine combination of quantum distributions (that do not output $\perp$) so $\gamma_2(\mathbf{p}) \leq |\frac{1}{\zeta}| + |-\frac{1-\zeta}{\zeta}| = 2\mathrm{eff}^*(\mathbf{p}) - 1$. □

For Boolean function, the gap between ν and γ_2 is known to be at most a multiplicative constant (by Grothendieck's inequality). However there is no immediate way to conclude similarly for eff vs. eff^*. Since these are stronger bounds, determining the largest possible gap between these measures could lead to further evidence towards the existence, or not, of exponential gaps between quantum and classical communication complexity for total boolean functions.

3.5 Proving concrete lower bounds using the dual

To prove lower bounds on communication complexity, it is helpful to use the dual formulation, where it suffices to give a feasible solution.

Lemma 7 (Dual formulation of the efficiency bounds)**.** *For any distribution* $\mathbf{p}$*,*

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

The first part is shown using linear programming duality and the second 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 $B(\mathbf{p}) = \sum_{a,b,x,y} B_{abxy} p(a,b|x,y)$ such 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 in such a way that they correlate well with the distribution $\mathbf{p}$ and badly with local strategies. For $B(\ell)$ to be small for local strategies, we can apply a small weight or even a penalty (negative weight) when the local strategy is incorrect. For $B(\mathbf{p})$ to be large, we can assign a positive coefficient when the outcome is correct, or if it should occur with high probability. Weights can be zero when the input is not contributing to the hardness of the problem.

We give an example in Appendix C for a distribution based on the Hidden Matching problem [BYJK08, GKK+08, BRSdW11]. In Appendix D, we study the Khot Vishnoi game for which there is a large Bell inequality violation [KV05, BRSdW11]. We reformulate it as a distribution which can be simulated with shared entanglement and no communication, and give a randomized communication lower bound of $\log(n)$ for this distribution. The proofs use many of the techniques Burhman *et al.* used to establish large Bell inequality violations [BRSdW11].

4 Upper bounds for one- and two-way communication

The efficiency and partition bounds subsume many known lower bound techniques for randomized communication complexity. How close are they to being tight? An upper bound on randomized communication is proven by Massar [Mas02]. We give a similar bound for quantum communication complexity in terms of eff^*.

Theorem 8. *For any distribution* $\mathbf{p}$ *with outputs in* $\mathcal{A}, \mathcal{B}$*,*

- *[Mas02]* $R^{\eta,\|}(\mathbf{p}) \leq \log(\frac{1}{1-\eta})\mathrm{eff}(\mathbf{p}) \log(\#(\mathcal{A} \times \mathcal{B}))$
- $R^{*,\eta,\|}(\mathbf{p}) \leq \frac{1}{2}\log(\frac{1}{1-\eta})\mathrm{eff}^*(\mathbf{p}) \log(\#(\mathcal{A} \times \mathcal{B}))$
- $R^{*,\eta}(\mathbf{p}) \leq O\left(\sqrt{\log(\frac{1}{1-\eta})\mathrm{eff}^*(\mathbf{p})}\right)$

Proof. For the first item, let P be a zero-error, zero-communication protocol with shared randomness for $\mathbf{p}$ which has efficiency $\zeta = \frac{1}{\mathrm{eff}(\mathbf{p})}$. Alice and Bob run the protocol $N = \lceil \log(\frac{1}{1-\eta})\frac{1}{\zeta} \rceil$ times and send their outcome to the referee in each run. If the referee finds a valid run (neither player aborts), he produces the corresponding outputs; otherwise he aborts. Since each run has a probability η of producing a valid run, the probability that the referee aborts is $(1-\zeta)^N \leq e^{-\zeta N} \leq 1 - \eta$.

For the second item, the proof is the same but the players share entanglement to run the protocol with shared entanglement and efficiency $\frac{1}{\mathrm{eff}^*(\mathbf{p})}$.

If multiple rounds of communication are allowed, then a quadratic speedup is possible in the quantum case by using a protocol for disjointness [BCW98, HdW02, AA05] on the input u, v of length N, 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. In the case of the partition bound, we consider only rectangles of the form $X \times Y$ with $Y = \mathcal{Y}$. In the case of the efficiency bound, this amounts to only letting Alice abort the protocol. We give the results for quantum communication since the rectangle bound is already known to be tight for randomized communication complexity [JKN08]. The set of local (resp. quantum) distributions where only Alice can abort is denoted $\mathcal{L}^{\perp A}_{\mathrm{det}}$ (resp. $\mathcal{Q}^{\perp A}$).

Definition 7. *Define* $\text{eff}^{\rightarrow}$ *and* $\text{eff}^{*,\rightarrow}$ *as*

$$
\begin{aligned}
(\text{eff}^{\rightarrow}(\mathbf{p}))^{-1} = & \max_{\zeta, q_\ell \geq 0} \zeta \\
& \textit{subject to} \sum_{\ell \in \mathcal{L}_{\text{det}}^{\perp A}} q_\ell l(a,b|x,y) = \zeta p(a,b|x,y) \qquad \forall a \in \mathcal{A}, b \in B, x, y \in \mathcal{X} \times \mathcal{Y} \\
& \sum_{\ell \in \mathcal{L}_{\text{det}}^{\perp A}} q_\ell = 1; \\
(\text{eff}^{*,\rightarrow}(\mathbf{p}))^{-1} = & \max_{\zeta, \mathbf{q} \in \mathcal{Q}^{\perp A}} \zeta \\
& \textit{subject to } q(a,b|x,y) = \zeta p(a,b|x,y) \qquad \forall a \in \mathcal{A}, b \in B, x, y \in \mathcal{X} \times \mathcal{Y}.
\end{aligned}
$$

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

Lemma 9 (Dual formulation for one-way efficiency)**.** *For any* $\mathbf{p}$*,*

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

Theorem 10. $R_0^{\rightarrow}(\mathbf{p}) \geq \log \text{eff}^{\rightarrow}(\mathbf{p})$ *and* $Q_0^{\rightarrow}(\mathbf{p}) \geq \log \text{eff}^{*,\rightarrow}(\mathbf{p})$.

The proof is similar to the two-way case. Here we show that the quantum partition bound is tight, up to arbitrarily small inefficiency.

Theorem 11. *For any distribution* $\mathbf{p}$ *and efficiency* $\eta < 1$*,* $Q_0^{*,\eta,\rightarrow}(\mathbf{p}) \leq \log(\text{eff}^{*,\rightarrow}(\mathbf{p})) + \log\log(1/(1-\eta))$.

Proof. Let $(\zeta, \mathbf{q})$ be an optimal solution for $\text{eff}^{*,\rightarrow}(\mathbf{p})$. 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 $N = \lceil \log(\frac{1}{1-\eta}) \frac{1}{\zeta} \rceil$ 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 $\Pr_{\mathbf{q}}[a_i = \perp (\forall i)] = (1-\zeta)^N \leq e^{-\zeta N} \leq 1 - \eta$. The protocol then requires $\log N = -\log \zeta + \log\log(\frac{1}{1-\eta})$ bits of communication. □

Finally, we show that $R_0^{\eta,\rightarrow}$ depends on η by at most an additive constant. The same is also true in the quantum model.

Lemma 12. *For any distribution* $\mathbf{p}$ *and efficiencies* $0 < \eta \leq \eta' < 1$*,* $R_0^{\eta,\rightarrow}(\mathbf{p}) \leq R_0^{\eta',\rightarrow}(\mathbf{p}) \leq R_0^{\eta,\rightarrow}(\mathbf{p}) - \log \eta + \log\log(1/(1-\eta'))$.

Proof (sketch). The proof is as above, except that we start from a protocol for $\mathbf{p}$ with efficiency η instead of a quantum distribution. Note that Alice only needs to send the communication corresponding to the original protocol for the successful attempt. □

As an application, we show in Appendix C that $R_\epsilon^{\rightarrow}(\text{HM}) = \Omega(\sqrt{n})$. for a quantum distribution HM based on the Hidden Matching problem. Vértesi *et al.* show that there is a distribution with boolean outputs $\mathbf{p} \in \mathcal{Q}$, based on partially entangled states, such that (in our language) $\text{eff}^{\rightarrow}(\mathbf{p}) = \Omega(2^n)$ [VPB10]. Therefore, $R_0^{\rightarrow}(\mathbf{p}) = n$. Since the states are nearly separable, however $R_\epsilon^{\rightarrow}(\mathbf{p}) = 0$ for small enough ϵ.

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 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.* [BHMR06]. 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 [BPA+08, VPB10]. 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 communication gives a lower bound on the dimension. For the detection loophole, one can also consider more realistic models of inefficiency. The inefficiency might depend on the measurements, or we might assume that the players abort independently. (The latter is a standard assumption among experimentalists, who do not tend to view inefficiency as adversarial.)

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 there 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 [CSWY01]. It was recently shown that information complexity is an upper bound on discrepancy [BW11]. We would like to see connections one way or the other between information complexity and the partition bound (also an upper bound on discrepancy).

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 to be sure than finding a good Bell inequality, that can nevertheless be approached via semidefinite programming relaxations [NPA08, DLTW08]. 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.

6 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

[AA05] S. Aaronson and A. Ambainis. Quantum search of spatial regions. *Theory of Computing*, 1:47–79, 2005. arXiv:quant-ph/0303041, doi:10.4086/toc.2005.v001a004.

[BCT99] G. Brassard, R. Cleve, and A. Tapp. Cost of exactly simulating quantum entanglement with classical communication. *Phys. Rev. Lett.*, 83:1874–1877, 1999. arXiv:quant-ph/9901035, doi:10.1103/PhysRevLett.83.1874.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs classical communication and computation. In *Proc. 30th STOC*, pages 63–68, 1998. arXiv:quant-ph/9802040, doi:10.1145/276698.276713.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Phys. Rev. Lett.*, 87(16):167902, 2001. doi:10.1103/PhysRevLett.87.167902.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

[BHMR03] H. Buhrman, P. Høyer, S. Massar, and H. Röhrig. Combinatorics and quantum nonlocality. *Phys. Rev. Lett.*, 91, 2003. arXiv:quant-ph/0209052, doi:10.1103/PhysRevLett.91.047903.

[BHMR06] H. Buhrman, P. Høyer, S. Massar, and H. Röhrig. Multipartite nonlocal quantum correlations resistant to imperfections. *Phys. Rev. A*, 73, 2006. doi:10.1103/PhysRevA.73.012321.

[BNS89] L. Babai, N. Nisan, and M. Szegedy. Multiparty protocols and logspace-hard pseudorandom sequences. In *Proc. 21st STOC*, pages 1–11, 1989. doi:10.1145/73007.73008.

[BPA+08] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. Méthot, and V. Scarani. Testing the dimension of Hilbert spaces. *Phys. Rev. Lett.*, 100:210503, 2008. arXiv:0802.0760, doi:10.1103/PhysRevLett.100.210503.

[BRSdW11] H. Buhrman, O. Regev, G. Scarpa, and R. de Wolf. Near-optimal and explicit Bell inequality violations. In *Proc. 26th CCC*, pages 157–166, 2011. arXiv:1012.5043, doi:10.1109/CCC.2011.30.

[BW11] M. Braverman and O. Weinstein. A discrepancy lower bound for information complexity. Technical Report 164, ECCC, 2011. arXiv:1112.2000.

[BYJK08] Z. Bar-Yossef, T.S. Jayram, and I. Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM J. Comput.*, 38(1):366–384, 2008. doi:10.1145/1007352.1007379.

[CG85] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. In *Proc. 26th FOCS*, pages 429–442, 1985. doi:10.1109/SFCS.1985.62.

[CSWY01] A. Chakrabarti, Y. Shi, A. Wirth, and A. Yao. Informational complexity and the direct sum problem for simultaneous message complexity. In *Proc. 42nd FOCS*, pages 270–278, 2001. doi:10.1109/SFCS.2001.959901.

[dGdW02] M. de Graaf and R. de Wolf. On quantum versions of the Yao principle. In *Proc. 19th STACS*, pages 347–358, 2002. doi:10.1007/3-540-45841-7_28.

[DKLR11] J. Degorre, M. Kaplan, S. Laplante, and J. Roland. The communication complexity of non-signaling distributions. *Quantum Information and Computation*, 11(7 –8):649–676, 2011. arXiv:0804.4859.

[DLTW08] A. C. Doherty, Y.-. Liang, B. Toner, and S. Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *Proc. 23rd CCC*, pages 199–210, 2008. arXiv:0803.4373, doi:10.1109/CCC.2008.26.

[dW08] R. de Wolf. A brief introduction to Fourier analysis on the boolean cube. *Theory of Computing Library–Graduate Surveys*, 1:1–20, 2008. doi:10.4086/toc.gs.2008.001.

[GG99] B. Gisin and N. Gisin. A local hidden variable model of quantum correlation exploiting the detection loophole. *Phys. Lett. A*, 260:323–327, 1999. arXiv:quant-ph/9905018, doi:10.1016/S0375-9601(99)00519-8.

[GKK+08] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separation for one-way quantum communication complexity, with applications to cryptography. *SIAM J. Comput.*, 38(5):1695–1708, 2008. doi:10.1145/1250790.1250866.

[HdW02] P. Høyer and R. de Wolf. Improved quantum communication complexity bounds for disjointness and equality. In *Proc. 19th STACS*, pages 299–310, 2002. doi:10.1007/3-540-45841-7_24.

[JK10] R. Jain and H. Klauck. The partition bound for classical complexity and query complexity. In *Proc. 25th CCC*, pages 247–258, 2010. arXiv:0910.4266, doi:10.1109/CCC.2010.31.

[JKN08] R. Jain, H. Klauck, and A. Nayak. Direct product theorems for communication complexity via subdistribution bounds. In *Proc. 40th STOC*, pages 599–608, 2008. doi:10.1145/1374376.1374462.

[KKN95] M. Karchmer, E. Kushilevitz, and N. Nisan. Fractional covers and communication complexity. *SIAM J. Discrete Math.*, 8(1):76–92, 1995. doi:10.1109/SCT.1992.215401.

[KR11] B. Klartag and O. Regev. Quantum one-way communication can be exponentially stronger than classical communication. In *Proc. 43rd STOC*, 2011. arXiv:1009.3640, doi:10.1145/1993636.1993642.

[KV05] S. Khot and N. Vishnoi. The unique games conjecture, integrality gap for cut problems and embeddability of negative type metrics into l_1. In *Proc. 46th FOCS*, pages 53–62, 2005. doi:10.1109/SFCS.2005.74.

[Lov90] L. Lovász. *Communication Complexity: a Survey, in: Paths, Flows, and VLSI Layout.* Springer, B.H. Korte edition, 1990.

[LS09a] T. Lee and A. Shraibman. Lower bounds in communication complexity. *Foundations and Trends in Theoretical Computer Science*, 3(4):263–399, 2009. doi:10.1561/0400000040.

[LS09b] N. Linial and A. Shraibman. Lower bounds in communication complexity based on factorization norms. *Random Structures and Algorithms*, 34(3):368–394, 2009. doi:10.1002/rsa.20232.

[Mas02] S. Massar. Non locality, closing the detection loophole and communication complexity. *Phys. Rev. A*, 65, 2002. arXiv:quant-ph/0109008, doi:10.1103/PhysRevA.65.032121.

[New91] I. Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):61–71, 1991. doi:10.1016/0020-0190(91)90157-D.

[NPA08] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008. arXiv:0803.4290, doi:10.1088/1367-2630/10/7/073013.

[NS96] I. Newman and M. Szegedy. Public vs. private coin flips in one round communication games. In *Proc. 28th STOC*, pages 561–570, 1996. doi:10.1145/237814.238004.

[VPB10] T. Vértesi, S. Pironio, and N. Brunner. Closing the detection loophole in Bell experiments using qudits. *Phys. Rev. Lett.*, 104:060401, 2010. arXiv:0909.3171, doi:10.1103/PhysRevLett.104.060401.

[Yao83] A. C. Yao. Lower bounds by probabilistic arguments. In *Proc. 24th FOCS*, pages 420–428, 1983. doi:10.1109/SFCS.1983.30.

A Proof of Theorem 2

We give the proof that for any distribution $\mathbf{p}$, $R^{\eta}_{\epsilon}(\mathbf{p}) \geq \log(\mathrm{prt}^{\eta}_{\epsilon}(\mathbf{p}))$.

Proof of Theorem 2. Let $\mathcal{P}$ be a protocol that simulates $\mathbf{p}$ with η detector efficiency and c bits of communication in the worst case, up to ϵ error in total variation distance. Let $\mathbf{p}'$ be the distribution produced by $\mathcal{P}$. We can think of $\mathcal{P}$ as a probability distribution over fully deterministic protocols $\{P_i\}$, where P_i is chosen with probability $q(i)$. Each deterministic protocol P_i further decomposes into 2^c rectangles $\{R_{i,j}\}$ and in each rectangle, the players apply a local strategy $\ell_{i,j}$ defined over inputs in R and outputs in $\mathcal{A} \cup \{\perp\} \times \mathcal{B} \cup \{\perp\}$.

From this we construct a feasible solution to the linear program for $\mathrm{prt}^\eta(\mathbf{p}')$. For any rectangle $R \subseteq X \times Y$ and any local distribution l defined over inputs R and outputs in $\mathcal{A} \cup \{\perp\} \times \mathcal{B} \cup \{\perp\}$, we set

$$w_{R,\ell} = \sum_{i,j:R=R_{i,j} \text{ and } \ell=\ell_{i,j}} q(i).$$

Intuitively, $w_{R,\ell}$ is the probability of finding rectangle R paired together with local strategy ℓ when choosing a deterministic protocol from $\mathcal{P}$. Each pair R, l might appear in several of the deterministic protocols in $\mathcal{P}$, so we take the sum of the probabilities where this pair occurs.

First we claim that the objective function is 2^c.

$$\begin{aligned}
\sum_{R,\ell} w_{R,\ell} &= \sum_{R,\ell} \sum_{i,j:R=R_{i,j} \text{ and } \ell=\ell_{i,j}} q(i) \\
&= \sum_{i,j} \sum_{R_{i,j},\ell_{i,j}} q(i) \\
&= 2^c \sum_i q(i) \\
&= 2^c.
\end{aligned}$$

Now, we claim that all the constraints are verified. For the first constraint, fix any $a, b, x, y \in \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y}$. By assumption, $\mathcal{P}$ outputs according to $p'(a, b|x, y)$, conditioned on having output a value in $A \times B$. Let us explicitly calculate the (unconditional) probability that $\mathcal{P}$ outputs a, b on input x, y. With probability $w_{R,\ell}$, $\mathcal{P}$ outputs according to the local strategy l applied on a rectangle R containing x, y. So the probability of outputting a, b is $\sum_{R:x,y \in R,\ell} w_{R,\ell} \cdot l(a, b|x, y)$. The conditional probability is obtained by dividing by the probability of outputting some $a', b' \in \mathcal{A} \times \mathcal{B}$ on input x, y. This is precisely the quantity $\eta_{x,y}$.

The second constraint follows from the efficiency of $\mathcal{P}$. This completes the proof.

□

B Efficiency bound for protocols with η efficiency

In order to prove lower bounds on simulating $\mathbf{p}$ with efficiency $\eta < 1$, we define the following generalization of $\mathrm{eff}(\mathbf{p})$.

Definition 8. *For any distribution* $\mathbf{p}$ *with inputs in* $X \times Y$ *and outputs* $A \times B$*, define* $\mathrm{eff}^\eta(\mathbf{p}) = 1/\zeta_{\mathrm{opt}}$*, where* ζ_{opt} *is the optimal value of the following linear program. The variables are* ζ, ζ_{xy} *and* q_ℓ*, where* ℓ *ranges over all local deterministic protocols with inputs taken from* $\mathcal{X} \times \mathcal{Y}$ *and outputs in* $\mathcal{A} \cup \{\perp\} \times \mathcal{B} \cup \{\perp\}$*.*

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

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

This provides a lower bound for $R^\eta_\epsilon(\mathbf{p})$, which is equivalent to the lower bound obtained from $\mathrm{prt}^\eta_\epsilon(\mathbf{p})$ (we omit the proofs of these statements as they closely follow the lines of the special case $\eta = 1$).

Lemma 13. *For any distribution* $\mathbf{p}$*, we have* $R^\eta_\epsilon(\mathbf{p}) \geq \log \mathrm{eff}^\eta_\epsilon(\mathbf{p})$.

Theorem 14. *For any distribution* $\mathbf{p}$, $\mathrm{eff}_\epsilon^\eta(\mathbf{p}) = \mathrm{prt}_\epsilon^\eta(\mathbf{p})$.

We can also study the maximum η such that $\mathbf{p}$ can be simulated with efficiency $\eta_{xy} \geq \eta$ on input x, y, without any communication. We denote the inverse of this quantity by $\mathrm{eff}^{\mathrm{nc}}(\mathbf{p})$.

Definition 9. *For any distribution* $\mathbf{p}$ *with inputs in* $X \times Y$ *and outputs* $A \times B$, *define* $\mathrm{eff}^{\mathrm{nc}}(\mathbf{p}) = 1/\eta$, *where* η *is the maximum* η *such that* $R^\eta(\mathbf{p}) = 0$.

This quantity can be seen as a relaxation of $\mathrm{eff}(\mathbf{p})$, where we no longer require the inefficiency to be the same for all inputs. Indeed, it can be rewritten as follows.

Lemma 15. *For any distribution* $\mathbf{p}$, *we have* $\mathrm{eff}^{\mathrm{nc}}(\mathbf{p}) = 1/\zeta_{\mathrm{opt}}$, *where* ζ_{opt} *is the optimal value of the following linear program.*

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

By comparing the linear programs for the different quantities, we immediately obtain the following relations:

Lemma 16. *For any distribution* $\mathbf{p}$, *we have* $\eta \cdot \mathrm{eff}^{\mathrm{nc}}(\mathbf{p}) \leq \mathrm{eff}^\eta(\mathbf{p}) \leq \eta \cdot \mathrm{eff}(\mathbf{p})$.

C Lower bound for a Hidden Matching distribution

We apply the partition bound method on the Hidden Matching probability distribution that we define here. The Hidden Matching distribution is based on the Hidden Matching problem of [BYJK08] adapted to the setting of distributions by Buhrman et al [BRSdW11]. We use many of the ideas and techniques from the latter to give this "proof of concept" of the partition bound. Some added tricks are needed to get the partition lower bound to go through.

Definition 10 (Hidden Matching distribution)**.** *Alice receives* $x \in \{0,1\}^n$ *and Bob receives a matching* M *over vertices* $\{1, \ldots, n\}$. *Alice has to output* $a \in \{0,1\}^{\log(n)}$ *and Bob has to output* $d \in \{0,1\}$ *and* $(i,j) \in M$ *according to the following distribution, which we call the* Hidden Matching distribution*:*

$$\mathrm{HM}(a,d,i,j|x,M) = \begin{cases} \frac{2}{n^2} & \text{if } \langle a, i \oplus j \rangle \oplus d = x_i \oplus x_j \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 17 ([BRSdW11])**.** $\mathrm{HM} \in \mathcal{Q}$, *that is,* $Q_0(\mathrm{HM}) = 0$.

Theorem 18. *There exists a constant* $\mathcal{C} > 0$ *such that, for any* $0 \leq \epsilon < \frac{1}{2}$, *we have* $R_\epsilon^{\rightarrow}(\mathrm{HM}) \geq \frac{\sqrt{n-1}}{2\mathcal{C}} - \log(n) + \log(\frac{1}{2} - \epsilon)$.

From the one-way version of Lemma 1, we obtain as a corollary:

Corollary 19. *There exists a constant* $\mathcal{C} > 0$ *such that, for any* $0 < \eta \leq 1$ *and* $0 \leq \epsilon < \eta - \frac{1}{2}$, *we have* $R_\epsilon^{\eta,\rightarrow}(\mathrm{HM}) \geq \frac{\sqrt{n-1}}{2\mathcal{C}} - \log(n) + \log(\eta - \epsilon - \frac{1}{2})$.

We give a bound on $\text{eff}^{\rightarrow}_{\epsilon}(\text{HM}) = \min_{\{p':|p'-\text{HM}|_1\leq\epsilon\}}(\text{eff}^{\rightarrow}(\mathbf{p}'))$. To give an upper bound on the Bell value of local deterministic strategies that may output $\perp$, we will use the fact that the larger the rectangle where neither player aborts, the smaller the success probability of a local deterministic strategy.

To express the success probability of ℓ, we will use B-coefficients which will be positive when the ℓ-answer is good and negative if it is not. Normalizing these coefficients, we will obtain an expression of the form : the size of the rectangle times the difference between the probability that the answer is good and the probability that it is not. We can bound this value using the fact that each local and deterministic strategy can only win with a small probability.

However, this idea is not sufficient because even if the success probability decreases when the rectangle size increases, the rectangle size appears as a multiplicative factor in our expression, and if R is very large, our expression can be too large. To fix this, we subtract from the Bs some constant that we will call μ. It will be useful just for the large rectangles.

We first recall an application of KKL inequality as explained in [dW08] which we use in the proof.

Lemma 20. *Let A be a subset of $\{0,1\}^n$. Let S be a subset of $\{1\dots n\}$. We define $\beta_S = \mathbb{E}_{x\in A}\left((-1)^{S\cdot x}\right)$ where $S\cdot x = \sum_{i\in S} x_i$. Let $\mathcal{S}_2$ be the set of subsets of $\{1\dots n\}$ of size 2. There exists an absolute constant $\mathcal{C}$ such that*

$$\sum_{S\in\mathcal{S}_2}\beta_S^2 \leq \mathcal{C}\log\left(\frac{2^n}{|A|}\right)^2.$$

We now prove the theorem.

Proof. Let $\mathbf{p}'$ be such that $|\mathbf{p}'-\text{HM}|_1\leq\epsilon$. We lower bound $\text{eff}^{\rightarrow}(\mathbf{p}')$ using the dual of $\text{eff}^{\rightarrow}$ (Lemma 7).

$$\begin{aligned}\text{eff}^{\rightarrow}(\mathbf{p}') = \max_{B_{x,M,a,d,i,j}} &\sum_{x,M,a,d,i,j} B_{x,M,a,d,i,j}\cdot p'(a,d,i,j|x,M)\\ \text{subject to } &\sum_{x\in X(\ell),M,a,d,i,j} B_{x,M,a,d,i,j}\cdot l(a,d,i,j|x,M)\leq 1 \qquad \forall \ell\in\mathcal{L}_{\text{det}}^{\perp A},\end{aligned}$$

where we let $X(\ell)$ be the set of inputs for which Alice does not abort when following the local deterministic strategy ℓ.

We exhibit coefficients that satisfy the constraints and give us a good lower bound for the objective function for each $\mathbf{p}'$ close to $\mathbf{p}$.

$$\begin{aligned}\mu_{x,M} &= -\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^{n+1}|\mathcal{M}_n|}\\ \Phi'_{x,M,a,d,i,j} &= \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n|\mathcal{M}_n|}\delta_{(i,j)\in M}\cdot(-1)^{\langle a,i\oplus j\rangle\oplus d\oplus x_i\oplus x_j}\\ B_{x,M,a,d,i,j} &= \Phi'_{x,M,a,d,i,j}+\mu_{x,M}\end{aligned}$$

where δ is the Kronecker function, and $\mathcal{M}_n$ is the set of matchings over edges $\{1,\dots n\}$.

Verifying the constraints. Let $\ell\in\mathcal{L}_{det}$ and $X = X(\ell)$. The strategy ℓ partitions the set X into $\bigcup_a X_a$ where Alice outputs a, and $\mathcal{M}_n$ into $\bigcup_{d,i,j} R_{d,i,j}$ where Bob outputs (d,i,j) because ℓ is local and deterministic.

First, we want to bound from above the value:

$$\sum_{x\in X,M,a,d,i,j}\Phi'_{x,M,a,d,i,j}\cdot l(a,d,i,j|x,M) = \sum_a\sum_{x\in X_a}\sum_{i,j,d}\sum_{M\in R_{i,j,d}}\Phi'_{x,M,a,d,i,j}.$$

Let us first see what happens on small rectangles.

Claim 1. *If* $|X_a| \leq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}$ *then* $\sum_{x\in X_a}\sum_{i,j,d}\sum_{M\in R_{i,j,d}}\Phi'_{x,M,a,d,i,j} \leq \frac{1}{n}$.

$$\begin{aligned}
&\sum_{x\in X_a}\sum_{i,j,d}\sum_{M\in R_{i,j,d}}\Phi'_{x,M,a,d,i,j}\\
&= \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}\sum_{x\in X_a, M\in\mathcal{M}_n}\left(\sum_{d,i,j|l(a,d,i,j|x,M)=1}\frac{(-1)^{x_i\oplus x_j\oplus d\oplus\langle a,i\oplus j\rangle}}{|\mathcal{M}_n|}\delta_{(i,j)\in M}\right)\\
&\leq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}|X_a|.
\end{aligned}$$

So, if $|X_a| \leq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}$ then this sum is less than $\frac{1}{n}$. This conlcudes the claim.
Now let us consider the case of the large rectangles.

Claim 2. *If* $|X_a| \geq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}$ *then* $\sum_{x\in X_a}\sum_{i,j,d}\sum_{M\in R_{i,j,d}}\Phi'_{x,M,a,d,i,j} \leq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}\frac{|X_a|}{2}$.

$$\begin{aligned}
&\sum_{x\in X_a}\sum_{i,j,d}\sum_{M\in R_{i,j,d}}\Phi'_{x,M,a,d,i,j}\\
&= \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}\sum_{i,j}\sum_{x\in X_a}\sum_{d}\sum_{M\in R_{d,i,j}}\frac{(-1)^{x_i\oplus x_j\oplus d\oplus\langle a,i\oplus j\rangle}}{|\mathcal{M}_n|}\delta_{(i,j)\in M}\\
&= \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}\sum_{i,j}|X_a|\beta^a_{i,j}\left(\sum_{d}\sum_{M\in R_{d,i,j}}\frac{(-1)^{\langle a,i\oplus j\rangle\oplus d}}{|\mathcal{M}_n|}\delta_{(i,j)\in M}\right).\\
&\leq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}|X_a|\sqrt{\sum_{i,j}|\beta^a_{i,j}|^2}\sqrt{\sum_{i,j}|q^a_{i,j}|^2}.
\end{aligned}$$

where $\beta^a_{i,j} = \mathbb{E}_{x\in X_a}((-1)^{x_i\oplus x_j})$ and $q^a_{i,j} = \sum_d\sum_{M\in R_{d,i,j}}\frac{(-1)^{\langle a,i\oplus j\rangle\oplus d}}{|\mathcal{M}_n|}\delta_{(i,j)\in M}$ and the last line follows from the Cauchy-Schwarz inequality.

Furthermore,

$$\begin{aligned}
|q^a_{i,j}| &\leq \sum_d\sum_{M\in R_{d,i,j}}\frac{\delta_{(i,j)\in M}}{|\mathcal{M}_n|}\\
&= \mathrm{Prob}_{M\in\mathcal{M}_n}(l \text{ outputs}(i,j)\in M)\\
&\leq \frac{1}{n-1}.
\end{aligned}$$

and

$$\sum_{i,j}|q^a_{i,j}| \leq 1$$

so

$$\sqrt{\sum_{i,j}|q^a_{i,j}|^2} \leq \frac{1}{\sqrt{n-1}}$$

On the other hand, the KKL inequality gives us (with $A = X_a$):

$$\sqrt{\sum_{i,j}|\beta^a_{i,j}|^2} \leq \mathcal{C}\times\log\left(\frac{2^n}{|X_a|}\right).$$

Hence,

$$\begin{aligned}\sum_{x\in X_a}\sum_{i,j,d}\sum_{M\in R_{i,j,d}}\Phi'_{x,M,a,d,i,j} &\leq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}|X_a|\mathcal{C}\log\left(\frac{2^n}{|X_a|}\right)\times\frac{1}{\sqrt{n-1}}\\ &\leq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}|X_a|\frac{1}{2},\end{aligned}$$

because $|X_a|\geq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}$ implies that $\mathcal{C}\log\left(\frac{2^n}{|X_a|}\right)\frac{1}{\sqrt{n-1}}\leq\frac{1}{2}$.

From Claims 1 and 2, we obtain:

$$\begin{aligned}&\sum_{x\in X,M,a,d,i,j}B_{x,M}\cdot l(a,d,i,j,|,x,M)\\ &= \sum_{x\in X,M}\mu_{x,M}+\sum_{x\in X,M,a,d,i,j}\Phi'_{x,M,a,d,i,j}\times l(a,d,i,j|x,M)\\ &\leq \sum_{x\in X,M}\mu_{x,M}+\sum_{a||X_a|\leq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\frac{1}{n}+\sum_{a||X_a|\geq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\left(\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}|X_a|\frac{1}{2}\right)\\ &\leq \sum_a|X_a|(-\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^{n+1}})+\sum_{a||X_a|\leq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\frac{1}{n}+\sum_{a||X_a|\geq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^{n+1}}|X_a|\\ &\leq \sum_{a||X_a|\leq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\frac{1}{n}+\sum_{a||X_a|\geq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^n}\left(\frac{1}{2}|X_a|-\frac{1}{2}|X_a|\right)\\ &\leq \sum_{a||X_a|\leq 2^{n-\frac{\sqrt{n-1}}{2\mathcal{C}}}}\frac{1}{n}\\ &\leq 1.\end{aligned}$$

Value of the objective function. Let $\mathbf{p}'$ be a distribution such that $|\mathbf{p}'-\mathrm{HM}|_1\leq\epsilon$. For any x,M,a,d,i,j, we define $\epsilon_{x,M,a,d,i,j}|p'(a,d,i,j|x,M)-\mathrm{HM}(a,d,i,j|x,M)|$ and for any x,M, we have

$$\sum_{a,d,i,j}\epsilon_{x,M,a,d,i,j}\leq\epsilon.$$

We have:

$$\sum_{x,M,a,d,i,j}\mu_{x,M}\cdot p'(a,d,i,j|x,M)=\sum_{x,M}\mu_{x,M}=-\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n2^{n+1}}2^n=-\frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{2n}$$

Then, we have:

$$
\begin{aligned}
&\sum_{M,a,d,i,j} \Phi'_{x,M,a,d,i,j} \cdot p'(a,d,i,j,|x,M) \\
&= 2^{\frac{\sqrt{n-1}}{2\mathcal{C}}} \sum_{x,M} \sum_{a,d,i,j} \frac{(-1)^{x_i \oplus x_j \oplus d \oplus \langle a, i \oplus j \rangle}}{n 2^n |\mathcal{M}_n|} \delta_{(i,j) \in M} p'(a,d,i,j|x,M) \\
&\geq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n 2^n |\mathcal{M}_n|} \sum_{x,M} \Big(\sum_{a,d,i,j : x_i \oplus x_j = d \oplus \langle a, i \oplus j \rangle} \delta_{(i,j) \in M} (\mathrm{HM}(a,d,i,j|x,M) - \epsilon_{x,M,a,d,i,j}) \\
&+ \sum_{a,d,i,j : x_i \oplus x_j \neq d \oplus \langle a, i \oplus j \rangle} \delta_{(i,j) \in M} (-\mathrm{HM}(a,d,i,j|x,M) - \epsilon_{x,M,a,d,i,j}) \Big) \\
&= \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n} - \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n 2^n |\mathcal{M}_n|} \sum_{x,M,a,d,i,j} \epsilon_{x,M,a,d,i,j} \delta_{(i,j) \in M} \\
&\geq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n} - \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n} \epsilon.
\end{aligned}
$$

Finally we have,

$$
\sum_{x,M,a,d,i,j} B_{x,M,a,d,i,j} \cdot p'(a,d,i,j|x,M) \geq \frac{2^{\frac{\sqrt{n-1}}{2\mathcal{C}}}}{n} (\frac{1}{2} - \epsilon).
$$

We obtain $\frac{\sqrt{n-1}}{2\mathcal{C}} - \log(n) + \log(\frac{1}{2} - \epsilon)$ as a lower bound for the Hidden Matching probability distribution. □

D Lower bound for the Khot Vishnoi game

Buhrman *et al.* introduce the Khot Vishnoi game to exhibit a Bell inequality violation [KV05, BRSdW11]. They present a quantum protocol without any communication that wins the game with a good probability whereas for any classical protocol the winning probability is small. Here, we define the probability distribution that is exactly simulated by their quantum protocol and we show that it requires at least $\frac{\delta}{1-\delta} \log(n) + \log((1-2\delta)^2 - \epsilon)$ bits of communication to be simulated classically with ϵ error, for any $0 \leq \delta \leq \frac{1}{2}$.

Definition 11. *Let $\{0,1\}^n$ be the group of all n-bit strings with $\oplus$, let H be the subgroup containing the n Hadamard codewords. For $a \in \{0,1\}^n$ we define $v^a = (\frac{(-1)^{a_i}}{\sqrt{n}})_{i \in [n]}$ which corresponds to the following quantum state: $\frac{1}{\sqrt{n}}(-1)^{a_i}|i\rangle$. Alice and Bob, each receive a coset of H and they have to output an element (a,b) of their coset with probability $\frac{\langle v^a, v^b \rangle^2}{n}$. Then*

$$
\mathrm{KV}(a,b|U,V) = \begin{cases} \frac{\langle v^a, v^b \rangle^2}{n} & \text{if } a \in U \text{ and } b \in V \\ 0 & \text{otherwise} \end{cases}
$$

Theorem 21 ([BRSdW11])**.** $\mathrm{KV} \in \mathcal{Q}$*, that is,* $Q_0(\mathrm{KV}) = 1$.

Theorem 22. *For any $0 \leq \delta \leq \frac{1}{2}$ and $0 \leq \epsilon < (1-2\delta)^2$, we have $R_\epsilon(\mathrm{KV}) \geq \frac{\delta}{1-\delta} \log(n) + \log((1-2\delta)^2 - \epsilon)$.*

By applying Lemma 1, we get the following bound on communication with η efficiency.

Corollary 23. *For any $0 \leq \delta < \frac{1}{2}$, efficiency $0 < \eta \leq 1$, and error $\epsilon < (1-2\delta)^2 - (1-\eta)$,*

$$
R^\eta_\epsilon(\mathrm{KV}) \geq \frac{\delta}{1-\delta} \log(n) + \log((1-2\delta)^2 - \epsilon - (1-\eta)).
$$

Proof. As in the proof of Theorem 18, we will use the dual version of the efficiency bound (Lemma 7). Recall that $\mathrm{eff}_\epsilon(\mathrm{KV})$ is defined as the solution of:

$$\min_{\{p':|p'-KV|_1\leq\epsilon\}} \max \sum_{(U,V)\in p'^{-1},(a,b)} B_{U,V,a,b}p'(a,b|U,V)$$
$$\text{subject to} \sum_{(U,V)\in p'^{-1}\cap R(\ell)} \left(\sum_{a,b} B_{U,V,a,b}\cdot l(a,b|U,V)\right) \leq 1 \qquad \forall \ell \in \mathcal{L}^{\perp}_{\mathrm{det}},$$

where $R(\ell)$ is the rectangle on which neither of the players abort when they follow the local deterministic strategy ℓ.

Fix $\delta \leq \frac{1}{2}$. For $x \in \{0,1\}^n$, we denote by $\delta(x)$ the probability of generating x where each bit of x is set to 1 with probability δ independently of the other bits. For each coset U, we fix arbitrarily a representative u_0. Let $k_n = n^{\frac{\delta}{1-\delta}}$. The coefficients of the Bell inequality are defined as:

$$B_{U,V,a,b} = k_n \frac{\delta(u_0 \oplus v_0)}{2^n} \delta_{a\in U}\delta_{b\in V}\delta_{a\oplus u_0 = b\oplus v_0}$$

Verifying the constraints. We need to show that for any local deterministic distribution $\ell \in \mathcal{L}^{\perp}_{\mathrm{det}}$ with $R = R(\ell)$, we have

$$\sum_{(U,V)\in R} \left(\sum_{a,b} B_{U,V,a,b} \times l(a,b|U,V)\right) \quad \leq \quad 1$$

Let ℓ be a deterministic strategy for Alice and Bob which outputs elements of the cosets. From Alice's point of view, the strategy is just a choice of an element in each coset that we can represent by $A : \{0,1\}^n \to \{0,1\}$ such that $A(x) = 1$ if x is the chosen element of the coset he belongs to. Similarly, we represent Bob's strategy by B. With this notation, our constraint is:

$$\forall A, B : \{0,1\}^n \to \{0,1\}, \forall R,$$
$$\textstyle\sum_{(u_0,v_0)\in R} \left(\sum_{a,b} \frac{\delta(u_0\oplus v_0)}{2^n} \times A(a)B(b)\delta_{a\in u_0+H}\delta_{b\in v_0+H}\delta_{a\oplus u_0 = b\oplus v_0}\right) \leq \frac{1}{k_n}$$

Since all the coefficients are positive,

$$\begin{aligned}
&\sum_{(u_0,v_0)\in R}\left(\sum_{a,b}\frac{\delta(u_0\oplus v_0)}{2^n}\times A(a)B(b)\delta_{a\in u_0+H}\delta_{b\in v_0+H}\delta_{a\oplus u_0=b\oplus v_0}\right)\\
\leq\ &\sum_{(u_0,v_0)\in\{0,1\}^n}\left(\sum_{a,b}\frac{\delta(u_0\oplus v_0)}{2^n}\times A(a)B(b)\delta_{a\in u_0+H}\delta_{b\in v_0+H}\delta_{a\oplus u_0=b\oplus v_0}\right)\\
=\ &\sum_{(u_0,v_0)\in\{0,1\}^n}\left(\sum_{(h,h')\in H}\frac{\delta(u_0\oplus v_0)}{2^n}\times A(u_0\oplus h)B(v_0\oplus h')\delta_{h=h'}\right)\\
=\ &\sum_{(u_0,v_0)\in\{0,1\}^n}\left(\sum_{h\in H}\frac{\delta(u_0\oplus v_0)}{2^n}\times A(u_0\oplus h)B(v_0\oplus h)\right)\\
=\ &n\times\sum_{(u_0,v_0)\in\{0,1\}^n}\frac{\delta(u_0\oplus v_0)}{2^n}\times A(u_0)B(v_0)\\
=\ &n\times\sum_{(u_0,z_0)\in\{0,1\}^n}\frac{\delta(z_0)}{2^n}\times A(u_0)B(u_0\oplus z_0)\\
=\ &n\mathbb{E}_{u_0 unif,z_0\sim\delta}(A(u_0)B(u_0\oplus z_0))
\end{aligned}$$

As shown in [BRSdW11, Thm7], this value is bounded from above by $\frac{1}{k_n}$.

Value of the objective function. Let $\mathbf{p}'$ be such that $|\mathbf{p}'-\mathrm{KV}|_1\leq\epsilon$. Then $\forall u_0,v_0,u,v$, we define $\epsilon_{u_0,v_0,u,v}=|\mathrm{KV}(u,v|u_0,v_0)-p'(u,v|u_0,v_0)|$, where $\forall u_0,v_0$, $\sum_{u,v}\epsilon_{u_0,v_0,u,v}\leq\epsilon$.

We have

$$\begin{aligned}
&k_n\sum_{u_0,v_0,u,v}\frac{\delta(u_0\oplus v_0)}{2^n}\delta_{u\oplus u_0=v\oplus v_0}\delta_{u\in u_0+H}\delta_{v\in v_0+H}p'(u,v|u_0,v_0)\\
=\ &k_n\sum_{u_0,v_0}\sum_{h,h'\in H}\frac{\delta(u_0\oplus v_0)}{2^n}\delta_{h=h'}p'(u_0\oplus h,v_0\oplus h'|u_0,v_0)\\
\geq\ &k_n\sum_{u_0,v_0}\sum_{h}\frac{\delta(u_0\oplus v_0)}{2^n}\left(\frac{\langle v^{u_0\oplus h},v^{v_0\oplus h}\rangle^2}{n}-\epsilon_{u_0,v_0,u_0\oplus h,v_0\oplus h}\right)\\
=\ &k_n\sum_{u_0,v_0}\sum_{h}\frac{\delta(u_0\oplus v_0)}{2^n}\left(\frac{(1-2\frac{d(u_0\oplus h,v_0\oplus h)}{n})^2}{n}-\epsilon_{u_0,v_0,u_0\oplus h,v_0\oplus h}\right)\\
\geq\ &k_n\sum_{u_0,v_0}\sum_{h}\frac{\delta(u_0\oplus v_0)}{2^n}\frac{(1-2\frac{d(u_0\oplus h,v_0\oplus h)}{n})^2}{n}-k_n\epsilon\sum_{u_0,v_0}\frac{\delta(u_0\oplus v_0)}{2^n}\\
=\ &k_n\sum_{u_0,z_0}\frac{\delta(z_0)}{2^n}(1-2\frac{d(z_0,0)}{n})^2-k_n\epsilon\\
=\ &k_n\left(\sum_{z_0}\delta(z_0)(1-2\frac{d(z_0,0)}{n})^2-\epsilon\right)\\
\geq\ &k_n\left(\sum_{z_0}\delta(z_0)(1-2\frac{d(z_0,0)}{n})\right)^2-k_n\epsilon\\
=\ &k_n\left((1-2\delta)^2-\epsilon\right).
\end{aligned}$$

We conclude that $R_\epsilon(\mathrm{KV}) \geq \log((1-2\delta)^2 - \epsilon) + \frac{\delta}{1-\delta}\log(n)$. □

ECCC ISSN 1433-8092

http://eccc.hpi-web.de