ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Aspects and Consequences of Multi-Party Non-Locality

Master Thesis

Helen Ebbe
Department of Mathematics, ETH Zürich

March 29, 2013

Advisor: Prof. Dr. Stefan Wolf

Faculty of Informatics, USI Lugano

Abstract

One consequence of quantum physics are non-local correlations. These correlations do not allow for signaling and can not be explained by preshared information. We show that some of these multi-partite correlations can be distilled – some of them with a classical adaptive protocol and others using partial communication. Therefore, some arbitrarily weak non-local correlations can have a *communication value* in the context of replacing classical communication. Further, to get trivial (probabilistic) communication complexity we can use (weak) multi-partite non-local correlations. We determine *how non-local* such a correlation must be in order to get trivial communication complexity.

Contents

Chapter 1

Introduction

We give a short introduction to the topic of *non-locality distillation* and *(probabilistic) communication complexity* and discuss their background and motivation. Further, we give an overview of this thesis.

1.1 Background and Motivation

Quantum mechanics is a branch of physics that is dealing with microscopic particles. There occur some "strange" behaviours – one of them is *non-locality*. Experiments on separated particles showed that the outcomes of the measurements on each particle are correlated, but cannot be explained by pre-shared (classical) information determining all the outcomes locally [1].

The effect of non-locality was first perceived by Einstein, Podolsky, and Rosen [18]. They raised the question "Can quantum-mechanical description of physical reality be considered complete?" Responding to that question, Bell [4] showed that quantum mechanics is incompatible with a *local hidden variable theory*.

These non-local correlations are not only used in physics but also in computer science, where they improve the efficiency of many computational tasks, as well as, in information theory, where strong non-local correlations lead to a collapse of communication complexity.

It is obvioues that strong non-local correlations are more useful for such tasks than weak correlations. Therefore, it would be very helpful to amplify weak non-local correlations with local wirings. The first distillation protocol that amplify non-local correlations for bipartite correlations was found by Forster, Winkler, and Wolf [19]. Later, there was found an adaptive protocol by Brunner and Skrzypczyk [8] that distills non-local correlations to its algebraic maximum.

In this thesis, we show that there also exists a distillation protocol for a special class of multi-party non-local correlations that is able to distill these correlations to its algebraic maximum. A much bigger class of multi-party non-local correlations is also distillable if we allow some parties to use communication channels.

Non-local correlations are very useful for determining the *communication complexity* of a Boolean function: Two parties want to minimize the amount of communications for achieving that one of the parties is able to calculate the function value. Van Dam [31] showed that the communication complexity of each Boolean function gets trivial if these two parties share a Popescu-Rohrlich box, which corresponds to a maximal non-local correlation.

Brassard *et al.* [2] introduced a *probabilistic* version of communication complexity where only one of the parties has to guess the correct function value with probability $p > 1/2$. They showed that every Boolean function has trivial probabilistic communication complexity for two parties who share an approximation of the PR box that works correctly with probability greater than 90.8%.

In this thesis we also raise the question how good an approximation of a full-correlation box must be in order to get trivial probabilistic communication complexity. We present solutions to this question for the generalizations of the extremal tripartite full-correlation boxes.

1.2 Outline

In Chapter 2, the reader is introduced to the basic definitions of n-partite boxes, locality, non-signaling, and a number of other notions.

We proceed, in Chapter 3, by determining the distances between the extremal tripartite boxes and the local polytope, as well as, the distance to the set of quantum behaviours. Further, we analyse full-correlation boxes. We show which conditions a full-correlation must fulfill to be an extremal box of the non-signaling polytope.

In Chapter 4 we have a look at two well-known bipartite non-locality distillation protocols and adapt the Brunner-Skrzypczyk protocol to a natural generalization of the PR box for n parties.

In Chapter 5 we present, based on the generalized Brunner-Skzypczyk protocol, a distillation protocol for a much bigger class of full-correlation boxes that allows some parties to use communication channels. Therefore, the distillation replaces communication channels that we would need for simulating the correlation from scratch.

Non-local boxes can be used to decrease the (probabilistic) communication complexity of functions. An analyse of the generalizations of the three extremal tripartite full-correlation boxes is done in Chapter 6.

At last, in Chapter 7, we briefly discuss our results and concern to further open questions.

Our results from Chapter 4 and 5 are partially submitted to ISIT 2013 [16].

Chapter 2

Preliminaries

In this chapter we fix the most important notations and definitions used throughout this thesis.

2.1 Notation

Definition 2.1 *We denote the NOT of a boolean variable a by $\bar{a}$. For the NOT of a longer term of boolean variables we use the sign $\neg$.*

Definition 2.2 *Let X be a set. Then $\mathcal{P}(X)$ denotes the power set of the set X.*

2.2 Properties of n-Partite Boxes

The definitions, used in this section, follows [26].

In this thesis we will often talk about *n-partite boxes*. An *n-partite box* is an n-partite input-output system, where the ith party inputs x_i and receives the output a_i. The behaviour of this system can be defined by the conditional probability distribution

$$P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right). \tag{2.1}$$

In general, the inputs and outputs are elements from arbitrarily finite sets, $a_i \in \{0, 1, ..., A_i - 1\}$ and $x_i \in \{0, 1, ..., X_i - 1\}$. But in this thesis we only concern to binary input and output bits. So for every party i the input x_i and output a_i belong to the set $\{0, 1\}$.

The conditional behaviour distribution $P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right)$ has to fulfill the *non-negativity conditions*:

$$P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) \geq 0 \tag{2.2}$$

for all inputs $x_1, x_2, ..., x_n$ and all outputs $a_1, a_2, ..., a_n$. It also has to fulfill the *normalization conditions*:

$$\sum_{x_1 x_2 ... x_n} P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) = 1 \tag{2.3}$$

for all inputs $x_1, x_2, ..., x_n$.

If appropriate, we represent an n-partite box by its probability distribution $P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right)$ in matrix notation [19] as

$$\begin{pmatrix} P\left(00...0|00...0\right) & P\left(00...1|00...0\right) & \cdots & P\left(11...1|00...0\right) \\ P\left(00...0|00...1\right) & P\left(00...1|00...1\right) & & P\left(11...1|00...1\right) \\ \vdots & & \ddots & \vdots \\ P\left(00...0|11...1\right) & P\left(00...1|11...1\right) & \cdots & P\left(11...1|11...1\right) \end{pmatrix}. \tag{2.4}$$

2.2.1 Locality

An n-partite box is said *local* if the output of party i depends only on its input. Such a box can be simulated by non-communicating parties that are only using shared randomness.

Definition 2.3 (Local n-Partite Box) *An n-partite box is said* local *if the conditional behaviour of the box can be written as*

$$P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) = \sum_i P(e_i) P(a_1|x_1 e_i) P(a_2|x_2 e_i) \cdots P(a_n|x_n e_i), \tag{2.5}$$

where e is a shared random variable and fulfills $\sum_i P(e_i) = 1$.

This definition shows that every local n-partite box can be written as a convex combination of other local n-partite boxes. So the local n-partite boxes form a polytope. The vertices (extremal points) of this polytope are *deterministic strategies* obtained by setting the probabilities $P(a_1|x_1)$, $P(a_2|x_2 e_i)$, ..., $P(a_n|x_n)$ always to 0 or 1 [7].

Definition 2.4 (Deterministic Strategy) *A* deterministic strategy *s is a conditional probability distribution of the form*

$$P_s\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) = P_s(a_1|x_1) P_s(a_2|x_2) \cdots P_s(a_n|x_n), \tag{2.6}$$

where $P_s(a_i|x_i) \in \{0, 1\}$ for all $i = 1, 2, ..., n$.

It is well-known that every point inside a polytope can be written as a convex combination of its vertices. Hence, every local box with conditional probability distribution $P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right)$ can be written as a convex combination of the deterministic strategies

$$P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) = \sum_s a_s \cdot P_s\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right), \tag{2.7}$$

where we sum over all possible strategies s and the parameters a_s have to fulfill $\sum_s a_s = 1$.

2.2.2 Non-Signaling

Since in physics (also in quantum mechanics) it is not possible to communicate faster than light, the n-partite boxes should have the property that for every party the output comes immediately out when the input is given. In this way we avoid to transmit instantaneously information from one party to another. We will call this property *non-signaling*.

Definition 2.5 (Non-Signaling) *An n-partite box with conditional probability distribution $P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right)$ is said* non-signaling *when the marginal distribution for each subset of parties $\{a_{k_1}, a_{k_2}, ..., a_{k_m}\}$ only depends on its corresponding inputs*

$$P\left(a_{k_1} a_{k_2} ... a_{k_m} | x_1 x_2 ... x_n\right) = P\left(a_{k_1} a_{k_2} ... a_{k_m} | x_{k_1} x_{k_2} ... x_{k_m}\right). \tag{2.8}$$

An equivalent condition to Condition 2.8 can be found in [26, 2]:

$$\sum_{a_k} P\left(a_1 ... a_k ... a_n | x_1 ... x_k ... x_n\right) = \sum_{a_k} P\left(a_1 ... a_k ... a_n | x_1 ... x'_k ... x_n\right) \tag{2.9}$$

for all $k \in \{1, 2, ..., n\}$, all $a_1, a_2, ... a_n$ and $x_1, x_2, ... x_{k-1}, x_k, x'_k, x_{k+1}, ..., x_n$

These linear equations characterize an affine set. Together with the properties of a conditional probability distribution, they also define a convex polytope.

Remark 2.6 *We have to note that the local-polytope is included in the non-signaling-polytope.*

2.3 Some Special n-Partite Boxes

Some kind of n-partite boxes are used very often in publications about nonlocality distillation and communication complexity. Since we want to enhance some of these results, we give a short overview about the most important boxes.

2.3.1 Popescu-Rohrlich Box

For showing that quantum mechanics is not maximally non-signaling, Popescu and Rohrlich [30] introduced a non-signaling box whose correlations can not be simulated with quantum states. In this thesis we will use the definition of the Popescu-Rohrlich box that is given in [3].

Definition 2.7 (Popescu-Rohrlich box) *The* Popescu-Rohrlich Box *(or short* PR box*) takes two inputs x_1, $x_2 \in \{0,1\}$ and produces two outputs a_1, $a_2 \in \{0,1\}$ according to the conditional distribution*

$$P^{PR}(a_1 a_2 | x_1 x_2) = \begin{cases} \frac{1}{2} & a_1 \oplus a_2 = x_1 x_2 \\ 0 & \textit{otherwise.} \end{cases} \tag{2.10}$$

Note that all non-local extremal boxes of the two-partite non-signaling polytope are equivalent to the PR box [2].

The definition of the PR box can be generalized in a natural way to more than two parties:

Definition 2.8 (n-Partite Popescu-Rohrlich Box) *The* n-partite Popescu-Rohrlich box *(or short* n-PR box*) takes n inputs $\vec{x} = (x_1, x_2, ..., x_n)$ and produces n outputs $\vec{a} = (a_1, a_2, ..., a_n)$ according to the conditional distribution*

$$P_n^{PR}(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = x_1 x_2 \cdot ... \cdot x_n \\ 0 & \textit{otherwise.} \end{cases} \tag{2.11}$$

Similar to [8], we define the even parity box and the family of correlated non-local boxes for n parties:

Definition 2.9 (Even Parity Box for n Parties) *The* even parity box for n parties *takes n inputs $\vec{x} = (x_1, x_2, ..., x_n)$ and produces n outputs $\vec{a} = (a_1, a_2, ..., a_n)$ according to the conditional distribution*

$$P^c(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = 0 \\ 0 & \textit{otherwise.} \end{cases} \tag{2.12}$$

Definition 2.10 (Family of Correlated Non-Local Boxes for n Parties) *The* family of correlated non-local boxes for n parties *is defined as follows:*

$$P_{n,\varepsilon}^{PR} = \varepsilon P_n^{PR} + (1-\varepsilon) P_n^c, \tag{2.13}$$

where $0 \leq \varepsilon \leq 1$.

2.3.2 Full-Correlation Box

The most general types of boxes for n parties are full-correlation boxes. The definition that we use is analogously to [3].

Definition 2.11 (Full-Correlation Box) *A* full-correlation box *is an n-partite box which takes n inputs and produces n outputs. We denote the n-tuple of the inputs as $\vec{x} = (x_1, x_2, ..., x_n)$, where each input $x_i \in \{0, 1, ..., 2^m - 1\}$. The n-tuple of the outputs is $\vec{a} = (a_1, a_2, ..., a_n)$, where each output $a_i \in \{0, 1\}$. The* full-correlation box *is characterized by the conditional distribution*

$$P(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \sum\limits_i a_i = f(\vec{x}) \text{ mod } 2 \\ 0 & \text{otherwise,} \end{cases} \tag{2.14}$$

where $f(\vec{x})$ is a Boolean function of the inputs.

A full-correlation box has the property that the outputs for any subset of $n - 1$ parties are completely random [3] .

2.4 Measures of Non-Locality

We have seen in Section 2.2 that not every non-signaling box has a local behaviour. Hence, we are interested to determine if a box is local or not. If a box is non-local, we also want to know *how non-local* the box is. Therefore, we introduce Bell-inequalities and a numerical method to determine the distance from the box to the local-polytope.

2.4.1 Bell-Inequalities

This section will follow the definitions in [25].

Since the local n-partite boxes form a polytope, we are able to find hyperplanes where the whole polytope can be placed on one side of the hyperplane. All linear inequalities that define such a hyperplane are called *Bell-inequalities*.

For the following definitions we write the conditional probability distribution of a n-partite box as a vector

$$p = (P(00...0|00...0), ..., P(11...1|00...0), P(00...0|00...1), ..., P(11...1|11...1)), \tag{2.15}$$

where p is an element of $\mathbb{R}^{2^{(n+1)}}$.

Definition 2.12 (Bell-Inequality) *A linear inequality $a^T x - b \leq 0$ is a* Bell-inequality *if*

$$a^T p - b \leq 0 \tag{2.16}$$

for all p that belongs to a conditional probability distribution of a local box.

We have to note that there exist infinitely many Bell-inequalities, but the local-polytope can also be characterized by a finite number of linear inequalities. These linear inequalities correspond to the facets of the polytope that are called *tight Bell inequalities*. Finding all facets of a polytope is a NP-hard problem [29].

2.4.2 CHSH-Inequality

One special Bell-inequality for bipartite boxes is the *CHSH-inequality* [11]. Therefore, we define the *correlation functions* of a box with the conditional probability distribution P

$$E_{xy}(P) = P(00|xy) + P(11|xy) - P(01|xy) - P(10|xy) \tag{2.17}$$

for $xy = 00, 01, 10, 11$. From the CHSH-inequality we know that the corresponding box is local if and only if its correlation functions satisfies the following inequality

$$-2 \leq E_{xy}(P) + E_{x\bar{y}}(P) + E_{\bar{x}y} - E_{\bar{x}\bar{y}}(P) \leq 2 \tag{2.18}$$

for all $xy = 00, 01, 10, 11$.

Example 2.13 (CHSH-Value of the PR Box) *The PR box violates the CHSH-inequality maximal with value 4 [30] and, therefore, it is not local.*

2.4.3 Distances to the Local Polytope

An other possibility to determine *how non-local* an n-partite box is, is to compute the distance between the conditional probability distribution of the box and the closest local box. Therefore, we define the conditional probability distribution of the box as a vector in $\mathbb{R}^{2^{(n+1)}}$ (see Equation 2.15). The distance function d can be defined by a metric on the vectorspace:

$$d(p, p') = \|p - p'\|, \tag{2.19}$$

where $p, p' \in \mathbb{R}^{2^{(n+1)}}$ and $\|\cdot\|$ is a metric on $\mathbb{R}^{2^{(n+1)}}$.

We are now able to define a measure of non-locality for the n-partite boxes.

Definition 2.14 (Measure of Non-Locality) *The* measure of non-locality *of an n-partite box with conditional probability distribution vector p is defined by*

$$NL(p) = \min_{p' \text{ local}} (\|p - p'\|). \tag{2.20}$$

To determine the measure of non-locality of an n-partite box with the conditional probability distribution vector p, we have to solve the following optimization problem:

$$\begin{aligned} \text{minimize } & \|p - \sum_s a_s \cdot p_s\left(a_1a_2...a_n|x_1x_2...x_n\right)\| \\ \text{such that } & \sum_s a_s = 1 \\ & a_s \geq 0 \text{ for all local strategies } s, \end{aligned} \tag{2.21}$$

where the $p_s\left(a_1a_2...a_n|x_1x_2...x_n\right)$ are the local strategies $P_s\left(a_1a_2...a_n|x_1x_2...x_n\right)$ written as a vector.

Remark 2.15 *Note that there is an unique measure of non-locality for a given norm, but if the norm is not uniform convex*[1] *then it is possible that more than one local box exist that is closest to the original box [17]. For example all L^p-norms for $1 < p < \infty$ are uniform convex [10].*

In this thesis we will use the L^1-norm which is defined by

$$\|p\|_1 = \sum_{i=1}^{2^{(n+1)}} |p_i|. \tag{2.22}$$

2.5 Quantum Bits

This introduction to quantum bits, entanglement, POVM measurements and quantum behaviour follows [20, 27].

It is well-known that a classical bit is in the state 0 or 1. Also a qubit has a state. This state is a superposition of the states $|0\rangle$ and $|1\rangle$ that correspond to the classical states 0 and 1.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.23}$$

where $|\alpha|^2 + |\beta|^2 = 1$. These two special states are known as *computational basis states* and form an orthonormal basis. We can write them as $|0\rangle = (1,0)^{\mathrm{T}}$ and $|1\rangle = (0,1)^{\mathrm{T}}$. If we measure the qubit $|\psi\rangle$, we get either the result 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$.

Definition 2.16 (Kronecker Product) *Let A be an m by n matrix and B be an p by q matrix. Then the* Kronecker product *is defined by*

$$A \otimes B = \begin{pmatrix} A_{11}B & A_{12}B & \cdots & A_{1n}B \\ A_{21}B & A_{22}B & & A_{2n}B \\ \vdots & & \ddots & \vdots \\ A_{m1}B & A_{m2}B & \cdots & A_{mn}B \end{pmatrix}. \tag{2.24}$$

[1] A norm $\|\cdot\|$ is uniform convex if $(\forall x, y, \|x\|, \|x\| \leq 1 \Rightarrow \|\frac{x+y}{2}\| \leq 1 - \varepsilon(\|x-y\|)$, where $\varepsilon\colon [0,2] \to [0,1]$ is a monotonically increasing function with $\varepsilon(r) > 0\ \forall r \geq 0)$

If we have n qubits in a system, then we describe a *pure state* again as a superposition of the computational basis of these n qubits. This basis can be written in the form $|x_1x_2...x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_n\rangle$ where $x_i \in \{0,1\}$ for all i.

$$|\psi\rangle = \sum_{x_1,x_2,...,x_n} \alpha_{x_1x_2...x_n}|x_1x_2...x_n\rangle, \tag{2.25}$$

where $\sum_{x_1,x_2,...,x_n} \alpha^2_{x_1x_2...x_n} = 1$. For every pure state $|\psi\rangle$ exists a *density matrix*

$$\rho = |\psi\rangle\langle\psi|. \tag{2.26}$$

There also exists systems whose state is not completely known, that means we have different states $|\psi_i\rangle$ that occurs with probability p_i. Such a system can be described by the following density matrix

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|. \tag{2.27}$$

where the probabilities p_i have to sum up to 1. Such a kind of state is called a *mixed state*.

2.5.1 Entanglement

We will call a state *entangled* if its density matrix can not be written as a convex combination of density matrices of pure states

$$\rho \neq \sum_i p_i\rho^i_1 \otimes \rho^i_2 \otimes ... \otimes \rho^i_n, \tag{2.28}$$

where $\sum_i p_i = 1$ and ρ^i_j are density matrices for the jth qubit of the system.

Otherwise we call the state *separable*.

2.5.2 POVM Measurements

The most general form of measurements are called *POVM measurements*. POVM stands for *Positive Operator-Valued Measure.*

For these kind of measurements we use POVM. A set of operators $\{E_m\}_m$ is called a POVM if

(a) each operator E_m is positive, and

(b) $\sum_m E_m = \mathbb{1}$.

After a POVM measurement, the probability of outcome m is given by

$$p(m) = \langle\psi|E_m|\psi\rangle = \mathrm{Tr}\left(E_m\rho_\psi\right). \tag{2.29}$$

2.5.3 Quantum Behaviour

Since we know POVM measurements, we are able to determine if a box can be realized by quantum states and measurements. Therefore, a box $P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right)$ has *quantum behaviour* if there exist POVM $\{E_{a_i}^{x_i}\}_{a_i}$ and a quantum state ρ such that

$$P\left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) = \mathrm{Tr}\left(E_{a_1}^{x_1} \otimes E_{a_2}^{x_2} \otimes ... \otimes E_{a_n}^{x_n} \rho\right). \qquad (2.30)$$

2.5.4 Tsirelson's Bound

Bell [4] showed that non-local behaviours occur in quantum mechanics. So the question came up *how non-local* quantum mechanics is. Cirel'son [9] proved that quantum mechanics is not able to violate the CHSH inequality by more than $2\sqrt{2}$

$$-2\sqrt{2} \leq E_{xy}(P) + E_{x\bar{y}}(P) + E_{\bar{x}y} - E_{\bar{x}\bar{y}}(P) \leq 2\sqrt{2}. \qquad (2.31)$$

If a box can be simulated by quantum mechanical correlations, then its correlation functions satisfy the above equation. This bound is called *Tsirelson's bound*.

Chapter 3

Multipartite Boxes

In this chapter we compute the distance from the extremal tripartite boxes of the non-signaling polytope to the local polytope and the set of quantum behaviours. Further, we analyse the class of n-partite full-correlation boxes. We give arguments that a full-correlation box must fulfill in order to be non-local or to be an extremal box of the n-partite non-signaling polytope.

3.1 Tripartite Extremal Boxes of the Non-Signaling Polytope

Pironio, Bancal, and Scarani [28] determined all kind of extremal tripartite boxes of the non-signaling polytope. In this section we refer to these 46 equivalence classes of extremal boxes. A representative of each equivalence class can be found in Appendix A.

3.1.1 Local and Quantum Approximations for the Tripartite Extremal Boxes

In the table below we determine the L^1-distance from the extremal tripartite boxes P of the non-signaling polytope [28] to the closest local behaviour and quantum behaviour that can be reached with one pure entangled quantum state. Note that obviously the distance to the closest quantum behaviour (that can be reached with a mixed state) is smaller or equal to the distance to the closest local behaviour. Since we have only one pure entangled quantum state, it is obvious that in this way not every quantum behaviour (and also local behaviour) can be simulated

If we have more than two participating parties, we have to distinguish between to different definitions of closest boxes C: in the first definition we minimize the sum of all entries of the matrix $|P - C|$

$$\min_{\text{C loc.}} \left(\sum_{i,j} |P_{i,j} - C_{i,j}| \right), \tag{3.1}$$

this corresponds to find a local box whose average success for all inputs is maximized. The other possibility is to minimize the biggest sum of a row of the matrix $|P - C|$

$$\min_{\text{C loc.}} \left(\max_{\text{rows i}} \left(\sum_{\text{columns j}} |P_{i,j} - C_{i,j}| \right) \right), \tag{3.2}$$

this corresponds to find a local box whose smallest input success probability is maximized. These kinds of distances are marked with a star (*).

			one pure entangled state	
No	local	local*	quantum	quantum*
1	0.0000	0.0000	0.0000	0.0000
2	4.0000	0.5000	2.3431	0.2929
3	2.0000	0.5000	3.0294	0.6159
4	2.0000	0.4000	4.3852	0.5970
5	2.0000	0.5000	3.5805	0.4897
6	2.0000	0.5000	3.1716	0.6603
7	2.0000	0.5000	3.5183	0.6596
8	2.0000	0.5000	1.6754	0.2929
9	2.5000	0.5000	3.7235	0.6256
10	2.0000	0.5000	2.1195	0.4024
11	2.0000	0.5000	2.9904	0.5622
12	2.0000	0.5000	3.1257	0.4726
13	2.3333	0.3566	2.4404	0.4613
14	2.0000	0.3333	3.3047	0.5370
15	2.0000	0.5000	2.1919	0.3685
16	2.3333	0.5000	3.6737	0.5858
17	2.0000	0.5000	2.7520	0.4707
18	2.0000	0.5000	2.3424	0.3605
19	2.0000	0.5000	2.6183	0.4527
20	2.6000	0.5000	3.5254	0.5895
21	2.0000	0.5000	1.7863	0.3357
22	2.3333	0.5000	1.4315	0.1877
23	2.5000	0.5000	3.2397	0.6618
24	2.0000	0.5000	3.0822	0.5772
25	2.6667	0.3333	3.8928	0.5605
26	2.0000	0.5000	2.7050	0.3585
27	2.0000	0.5000	2.9814	0.4773

			one pure entangled state	
No	local	local*	quantum	quantum*
28	2.0000	0.5000	2.7374	0.4574
29	2.6667	0.4000	2.9827	0.4247
30	2.4000	0.4000	2.1541	0.3495
31	2.4000	0.3000	1.6328	0.2342
32	2.4000	0.4000	3.2189	0.5569
33	2.6000	0.4000	3.1710	0.6002
34	2.5000	0.5000	1.3796	0.2082
35	2.5000	0.5000	3.2347	0.5723
36	2.2500	0.4000	1.7704	0.2878
37	2.5000	0.5000	3.1384	0.5751
38	2.0000	0.5000	3.1786	0.5222
39	2.0000	0.5000	2.2486	0.3154
40	2.0000	0.3333	2.9771	0.5279
41	2.0000	0.5000	3.0294	0.6152
42	2.0000	0.5000	3.0294	0.5858
43	2.2857	0.4571	2.5319	0.9483
44	2.0000	0.6000	2.0000	0.5000
45	4.0000	0.5000	4.0000	0.9880
46	4.0000	0.5000	2.3431	0.2929

3.2 Full-Correlation Boxes

In Section 2.3.2, we defined a *full-correlation box* by the probability distribution

$$P(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \sum_i a_i = f(\vec{x}) \bmod 2 \\ 0 & \text{otherwise,} \end{cases} \tag{3.3}$$

where $\vec{x} = (x_1, x_2, ..., x_n)$ is the n-tuple of the inputs, $\vec{a} = (a_1, a_2, ..., a_n)$ is the n-tuple of the outputs and $f(\vec{x})$ is a Boolean function of the input elements.

In the following sections, we show how such boxes can be constructed by n-PR boxes. Further, we give an argument to determine if a full-correlation box is non-local and if it is an extremal box of the non-signaling polytope. Therefore, we are able to determine some classes of extremal boxes in the multi-partite case.

3.2.1 Construction of Full-Correlation Boxes

Barrett and Pironio [3] showed that every full-correlation box can be simulated by PR boxes. The PR box simulation for all extremal tripartite full-correlation boxes are given in [2]. The construction for a 3-PR box that is defined by the Boolean function $f(x_1, x_2, x_3) = x_1 x_2 x_3$ can be seen in Figure 3.1.

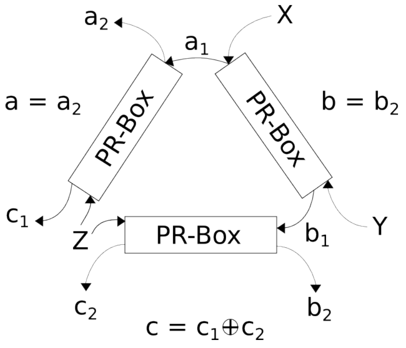

Figure 3.1: Simulation of a 3-PR box with three PR boxes

This construction can be generalized for all n-PR boxes. On Figure 3.2 one can see how an n-PR box can be inductively simulated.

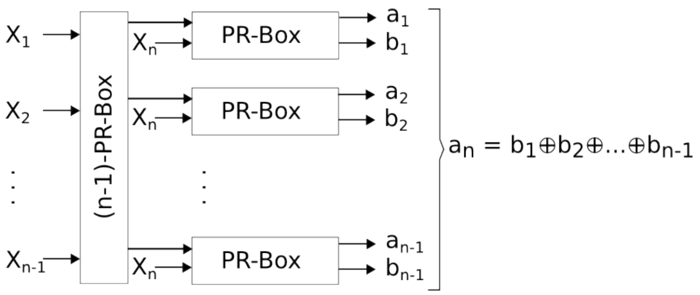

Figure 3.2: Simulation of a n-PR box with a $(n-1)$-PR box and $n-1$ PR boxes

Lemma 3.1 shows how an arbitrary full-correlation box can be simulated with n-PR boxes and local XOR operations.

Lemma 3.1 *If f is a boolean function of the inputs $x_1, x_2, ..., x_n$, then f can be written as*

$$f(x_1, ..., x_n) = \bigoplus_{I \in \mathcal{I}} \left(a_I \cdot \bigwedge_{i \in I} x_i \right), \tag{3.4}$$

where $\mathcal{I} = \mathcal{P}(\{1, 2, ..., n\})$ and $a_I \in \{0, 1\}$ for all $I \subseteq \mathcal{I}$.

Proof The constant, the AND and the XOR allow for implementing the universal Boolean functions AND and NOT. □

Hence, the full-correlation box associated to the Boolean function f can be constructed by $\sum_{I \in \mathcal{I}} a_I$ n-PR boxes. Indeed, for every $a_I = 1$, an n-PR box is needed, where the ith party inputs x_i if $i \in I$, and otherwise it inputs 1. Then, the box will output b_i^I. In the end, every party outputs $c_i = \bigoplus_{I \in \mathcal{I},\ a_I = 1} b_i^I$.

3.2.2 Non-Local Full-Correlation Boxes

If we write the Boolean function of a full-correlation box as in Lemma 3.1, it is easy to determine if a full-correlation box is local or non-local.

It is obvious that a full-correlation box is local if the associated Boolean function can be written as the XOR of a constant and single inputs of the box. Assume that the function consists of at least one AND-term with more than one input. This box can be reduced to the PR box that is non-local, if some of the parties input a constant into the box. Therefore, a full-correlation box is local if and only if the Boolean function can be written as the XOR of a constant and single inputs of the box

$$f(x_1, ..., x_n) = \bigoplus_{I \in \mathcal{I}} \left(a_I \cdot \bigwedge_{i \in I} x_i \right), \tag{3.5}$$

where $\mathcal{I} = \{\emptyset, \{x_1\}, \{x_2\}, ..., \{x_n\}\}$ and $a_I \in \{0, 1\}$ for all $I \subseteq \mathcal{I}$.

3.2.3 Extremal Boxes of the Non-Signaling Polytope

In this section we determine which full-correlation boxes are extremal boxes of the non-signaling polytope.

We already know from Lemma 3.1 that all n-partite full-correlation boxes can be simulated by n-partite PR boxes. We define the set of all (non-local) n-PR boxes that are needed to simulate the full-correlation box: Let

$$\mathcal{J} := \{I \in \mathcal{I} \mid a_I = 1 \text{ and } |I| \geq 2\}. \tag{3.6}$$

This set can be partitioned into disjoint subsets $\{J_1, J_2, ..., J_{n_\mathcal{J}}\}$ such that all $A \in J_i$ and $B \in J_j$ fulfill $A \cap B = \emptyset$ for all $i \neq j$. We define the maximal number of such subsets as $n_\mathcal{J}$.

Theorem 3.2 (Extremal Full-Correlation Boxes) *Let P be a given n-partite full-correlation box associated to the Boolean function f that is depending on k input variables. Then P is an extremal box of the non-signaling polytope if and only if $n_\mathcal{J} = 1$ and $k = n$ holds.*

Lemma 3.3 *Let P be a given n-partite full-correlation box with associated function f that is depending on k input variables. If $k \neq n$ then P can be written as a convex combination of other non-signaling boxes and, therefore, the box P is not an extremal box of the non-signaling polytope.*

Proof P can be written as a convex combination of the following two non-signaling boxes:

$$P^1(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{k-1}} & \bigoplus_{i=1}^{k} a_i = f(x_1, x_2, ..., x_k) \text{ and } \bigoplus_{i=k+1}^{n} a_i = 0 \\ 0 & \text{otherwise,} \end{cases} \tag{3.7}$$

and

$$P^2(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{k-1}} & \bigoplus_{i=1}^{k} a_i = 1 \oplus f(x_1, x_2, ..., x_k) \text{ and } \bigoplus_{i=k+1}^{n} a_i = 1 \\ 0 & \text{otherwise.} \end{cases} \tag{3.8}$$

So $P = \frac{1}{2}P^1 + \frac{1}{2}P^2$. Therefore, the box P is not an extremal box of the non-signaling polytope. □

Lemma 3.4 *Let P be a given n-partite full-correlation box with associated function f that is depending on k input variables. Let $k = n$. If $n_{\mathcal{J}} \geq 2$ then the box P is not extremal.*

Proof Since $n_{\mathcal{J}}$ is at least 2, we are able to split the Boolean function f in two other Boolean functions, f_1 and f_2, such that they do not depend on the same input variables. Without loss of generality, we assume that f_1 depends on the input variables $x_1, x_2, ..., x_m$ and f_2 depends on $x_{m+1}, ..., x_n$ $(m < n)$. Therefore, f can be written as $f(x_1, ..., x_n) = f_1(x_1, ..., x_m) \oplus f_2(x_{m+1}, ..., x_n)$. So the box P can be written as a convex combination of the following two boxes:

$$P^1(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-2}} & \bigoplus_{i=1}^{m} a_i = f_1(x_1, x_2, ..., x_m) \text{ and } \bigoplus_{i=m+1}^{n} a_i = f_2(x_{m+1}, ..., x_n) \\ 0 & \text{otherwise,} \end{cases} \tag{3.9}$$

and

$$P^2(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-2}} & \bigoplus_{i=1}^{m} a_i = \neg f_1(x_1, x_2, ..., x_m) \text{ and } \bigoplus_{i=m+1}^{n} a_i = \neg f_2(x_{m+1}, ..., x_n) \\ 0 & \text{otherwise.} \end{cases} \tag{3.10}$$

So $P = \frac{1}{2}P^1 + \frac{1}{2}P^2$. Therefore, the box P is not an extremal box of the non-signaling polytope.

Lemma 3.5 *Let P be a given n-partite full-correlation box with associated function f that is depending on k input variables. If $k = n$ and $n_{\mathcal{J}} = 1$ then the box P is extremal.*

Proof Statement follows directly from Lemmas 3.6 and 3.7. □

Lemma 3.6 (Existence of an Extremal n-Partite Full-Correlation Box) *Every n-PR box is extremal.*

Proof The proof is based on the same argument as in [22] for showing that *any non-locality implies some secrecy*. Assume that the n-PR box P can be written as a convex combination of two other non-signaling boxes P^1 and P^2

$$P = \varepsilon P^1 + (1-\varepsilon)P^2, \tag{3.11}$$

where $0 < \varepsilon < 1$. It is obvious that both of the boxes must fulfill that the XOR of their output elements is equal to the AND of their input elements

$$\text{Prob}\left[\bigoplus_{i=1}^{n} A_i = \prod_{i=1}^{n} X_i \mid X_i = x_i \; \forall \; 1 \le i \le n\right] = 1, \tag{3.12}$$

for all input elements $x_i \in \{0,1\}$. We will show that all possible biases, $p_i := \text{Prob}\left[A_i = 0 | X_k = 0 \text{ for all } k\right]$ for all $1 \le i \le n-1$ such that the box is non-signaling, must be $p_i = 1/2$. Therefore, P cannot be written as a convex combination of other non-signaling boxes.

Assume without loss of generality that all $p_i \ge 1/2$ for all $1 \le i \le n-1$. Because of Equation 3.12, the bias p_n can be computed from the biases p_i for $i \in \{1,2,...,n-1\}$. Since our box is still non-signaling, all biases are independent of the other parties inputs. We determine step by step the biases $p_i' := \text{Prob}\left[A_i = 0 | X_i = 1\right]$ for all i and get that $p_i' = p_i$. If not all biases are $1/2$ then this is a contradiction to Equation 3.12 for the input $(1,1,...,1)$. □

Lemma 3.7 *Let P^1 and P^2 be extremal m and k-partite full-correlation boxes with associated functions f_1 and f_2, where f_1 depends on the input variables $x_1, x_2, ..., x_m$ and f_2 depends on $x_l, x_{l+1}, ..., x_{l+k-1}$ ($l \le m$). Let f_1 and f_2 be two Boolean functions with no common AND-term. Then the box P with associated function $f(x_1, ..., x_{l+k-1}) = f_1(x_1, ..., x_m) \oplus f_2(x_l, ..., x_{l+k-1})$ is also extremal.*

Proof P^1 and P^2 are both extremal boxes and, therefore, we are able to verify this property with the argument from [22]. To show that the new box with associated function f is also an extremal box, we use the above property, as well as the property that these two boxes have at least one common input element. So the biases of the two functions are coupled.

We assume that the box with associated function f can be written as a convex combination of two other non-signaling boxes P_1 and P_2

$$P = \varepsilon P_1 + (1-\varepsilon)P_2, \tag{3.13}$$

where $0 < \varepsilon < 1$. As before, it is obvious that both of the boxes must fulfill that the XOR of their output elements is equal to the XOR of the Boolean functions f_1 and f_2

$$\text{Prob}\left[\bigoplus_{i=1}^{n} A_i = f_1(X_1, ..., X_m) \oplus f_2(X_l, ..., X_{l+k+1}) \mid X_i = x_i \; \forall \; i\right] = 1, \quad (3.14)$$

for all input elements $x_i \in \{0, 1\}$.

We will show that all possible biases, $p_i := \text{Prob}\,[A_i = 0|X_k = 0 \text{ for all } k]$ for all $1 \leq i \leq m-1$ and $m+1 \leq i \leq n-1$ such that the box is non-signaling, must be $p_i = 1/2$. Therefore, P cannot be written as a convex combination of other non-signaling boxes.

Since P^1 and P^2 are extremal boxes, we know that if there exist biases $\neq 1/2$, there exist at least one input for that the box get signaling to be still correct. Because the boxes does not have a common AND-term, there exist at least one input that is just affected from one box (because if it is affected by both boxes, it is correct since we take the XOR of two wrong outputs and so the box must not be signaling). So we showed that all p_i must be equal to $1/2$ to be non-signaling. □

Remark 3.8 *Note that the n-partite full-correlation box associated to the function $f(x_1, ..., x_n) = \prod_{i=1}^{n} x_i \oplus x_1$ is also an extremal box, since it can be constructed with an n-PR and an $(n-1)$-PR box by flipping the input bit x_1.*

Proof (Proof of Theorem 3.2) The statement follows from Lemmas 3.3, 3.4, and 3.5. □

In the same way we are also able to prove that we can construct from every extremal full-correlation box another extremal box that is not a full-correlation box.

Remark 3.9 *Let P be a given extremal n-partite full-correlation box with associated function f. Then the following $(n+1)$-partite box P^* is also extremal:*

$$P^*(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^n} & \bigoplus_{i=1}^{n} a_i = f(x_1, x_2, ..., x_n) \textit{ and } a_{n+1} = c \\ 0 & \textit{otherwise,} \end{cases} \quad (3.15)$$

where $c \in \{0, 1\}$.

3.2.4 Relation between Full-Correlation Boxes and the Local Polytope

We show that for every non-local full-correlation box exists a closest local box that is also a full-correlation box.

Definition 3.10 (Closest Local Full-Correlation Box) *Let P be the joint probability distribution of a non-local box. Then the joint probability distribution of the* closest local full-correlation box closef(P) *is defined by*

$$\|P - \text{closef}(P)\|_1 = \min_{P' \text{ loc. Full-Corr. box}} \left(\|P - P'\|_1\right). \tag{3.16}$$

Lemma 3.11 *Let P be the joint probability distribution of an n-partite full-correlation box. Then the closest local full-correlation box would be one of the closest local boxes, that means*

$$\|P - \text{closef}(P)\|_1 = \min(\|P - \sum_s a_s \cdot P_s \left(a_1 a_2 ... a_n | x_1 x_2 ... x_n\right) \|_1), \tag{3.17}$$

where s is a deterministic strategy and the a_i's fulfill $\sum_s a_s = 1$.

Proof It is obvious that every deterministic local strategy can fulfill at most the same number of input-output behaviours (XOR of the outputs equal to a Boolean function of the inputs) as the closest local full-correlation box. So every local box has at least the same distance from the given full-correlation box as the closest local full-correlation box. □

Chapter 4

Non-Local Distillation Without Communication

In this chapter we discuss protocols based on the XOR protocol [19] and the Brunner-Skrzypczyk protocol [8] for distilling multi-party non-locality.

4.1 Distillation based on the XOR Protocol

In this section we concern to non-adaptive distillation protocols based on the XOR protocol for distilling multi-party non-locality.

4.1.1 XOR Protocol

In this section we present the results from Forster, Winler, and Wolf [19].

Protocol 4.1 (XOR Protocol) *Alice and Bob shares n boxes. Alice inputs x and Bob inputs y in all n boxes. So the boxes compute in parallel Alice's and Bob's outputs $(a_1, a_2, ..., a_n)$ and $(b_1, b_2, ..., b_n)$, respectively. In the end Alice outputs $a = \bigoplus_{i=1}^{n} a_i$ and Bob outputs $b = \bigoplus_{i=1}^{n} b_i$.*

The following theorem is proved in [19]:

Theorem 4.2 *If we take $n > 1$ correlated non-local boxes P_{ε}^{PR} and $0 < \varepsilon < 1/2$, then the protocol is a non-locality distillation protocol.*

Remark 4.3 (Detailed Results) *The CHSH-value of the correlated non-local box P_{ε}^{PR} is $CHSH\big(P_{\varepsilon}^{PR}\big) = 3 - (1 - 2\varepsilon) > 2$. If we take n copies of the box P_{ε}^{PR} $0 < \varepsilon < 1/2$ then the CHSH-value of our distilled box $P_{\varepsilon'}^{PR}$ will be $CHSH\big(P_{\varepsilon}^{PR}\big) = 3 - (1 - 2\varepsilon)^n$. So the protocol can distill non-locality up to the CHSH-value of 3.*

4.1.2 XOR Protocol Applied to Extremal Boxes of the Tripartite Non-Signaling Polytope

We apply the XOR protocol and some similar protocol to the extremal boxes of the tripartite non-signaling polytope. With similar protocol we mean that some parties output the XOR of a constant and their output from the original XOR protocol.

In this way the boxes 2, 3, 4, 5, 6, 7 ,8, 41, 42, 44, and 45 from [28] can be distilled in a given range, but not to the algebraic maximum.

In the next section we will generalize this procedure to all full-correlation boxes for a much bigger class of similar XOR protocols.

4.1.3 XOR Protocol Applied to Full-Correlation Boxes

We prove in this section that every full-correlation box that is non-local can be distilled in a given range.

Before we can present our main results, we have to make some definitions.

Definition 4.4 (Family of Local Combinated Full-Correlation Boxes) *Let P be a non-local full-correlation box with closest local full-correlation box closef(P). Then we define the* family of local combinated Full Correlation boxes *of box P as*

$$P_{\varepsilon}^{P} = \varepsilon P + (1-\varepsilon)\mathrm{closef}(P) \tag{4.1}$$

Remark 4.5 *Let P be a given joint behaviour distribution of an n-partite full-correlation box and let P^* be the closest local full-correlation box. We assume that the measure of non-locality of P is $\mathrm{NL}(P) = \|P - P^*\|_1 = d$. Then the measure of non-locality of a local combinated full-correlation box P_{ε}^{P} $0 < \varepsilon < 1$ is given by*

$$\begin{aligned}\mathrm{NL}(P_{\varepsilon}^{P}) &= \|\varepsilon P + (1-\varepsilon)P^* - P^*\|_1 \\ &= \|\varepsilon P - \varepsilon P^*\|_1 \\ &= \varepsilon\|P - P^*\|_1 \\ &= \varepsilon d \end{aligned} \tag{4.2}$$

Protocol 4.6 (Generalized XOR Protocol for Full-Correlation Boxes) *This protocol works as follows (see Fig. 4.1). All n parties share three boxes, where we denote x_i as the value that the ith party inputs to all three boxes. The output bit of the first box for the ith party is then a_i^1, the output bit of the second box is a_i^2 and the output bit of the third box is a_i^3. Finally the ith party outputs $a_i = a_i^1 \oplus a_i^2 \oplus a_i^3$.*

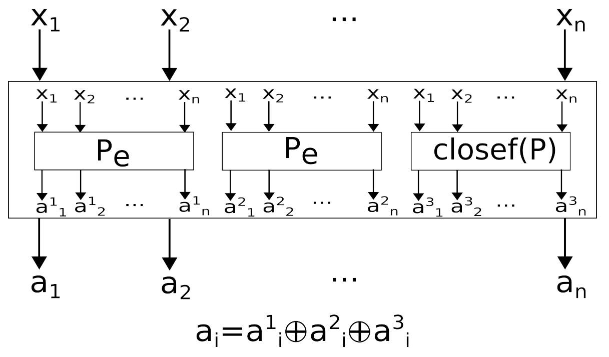

Figure 4.1: Distillation based on the XOR protocol

Theorem 4.7 *Given an n-partite full-correlation box with joint behaviour P the generalized XOR protocol for n-partite full-correlation boxes takes two copies of an arbitrarily box P^P_ε with $0 < \varepsilon < 1/2$ and a $closef(P)$ box to a local combinated Full-Correaltion box $P^P_{\varepsilon'}$ with $\varepsilon' > \varepsilon$, thus distilling non-locality. Moreover, in the asymptotic regime of many copies, any P^P_ε with $0 < \varepsilon < 1/2$ is distilled arbitrarily closely to $P^P_{1/2}$.*

The procedure of the proof is the same as in [8].

Proof We define $P^* = closef(P)$ and start with the initial three box state of the protocol which is given by

$$P^P_\varepsilon P^P_\varepsilon P^* = \varepsilon^2 P^P P^P P^* + \varepsilon\,(1-\varepsilon)\left(P^P P^* P^* + P^* P^P P^*\right) + (1-\varepsilon)^2 P^* P^* P^* \tag{4.3}$$

Since P and P^* are joint behaviour distributions of full-correlation boxes we are able to write them as

$$P(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = f(\vec{x}) \\ 0 & \text{otherwise} \end{cases} \tag{4.4}$$

and

$$P^*(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_i a_i = g(\vec{x}) \\ 0 & \text{otherwise,} \end{cases} \tag{4.5}$$

where $f(\vec{x})$ and$g(\vec{x})$ are Boolean function of the input elements.

Now we apply the above distillation protocol and get the final box. As in [8] we use the notation $P^1_i P^2_i P^3_i \longrightarrow P_f$ which means that the protocol takes three initial boxes, P^1_i, P^2_i and P^3_i, to one copy of the final box P_f.

- $P^P P^P P^* \longrightarrow P^*$: For the first box we have $\bigoplus_{i=1}^n a_i^1 = f(x_1, x_2, ..., x_n)$, for the second $\bigoplus_{i=1}^n a_i^2 = f(x_1, x_2, ..., x_n)$ and for the third $\bigoplus_{i=1}^n a_i^3 = g(x_1, x_2, ..., x_n)$. So the outputs satisfy the relation $\bigoplus_{i=1}^n a_i = \bigoplus_{i=1}^n a_i^1 \oplus \bigoplus_{i=1}^n a_i^2 \oplus \bigoplus_{i=1}^n a_i^3 = f(x_1, x_2, ..., x_n) \oplus f(x_1, x_2, ..., x_n) \oplus g(x_1, x_2, ..., x_n) = g(x_1, x_2, ..., x_n)$.

- $P^P P^* P^* \longrightarrow P^P$: For the first box we have $\bigoplus_{i=1}^n a_i^1 = f(x_1, x_2, ..., x_n)$, for the second $\bigoplus_{i=1}^n a_i^2 = g(x_1, x_2, ..., x_n)$ and for the third $\bigoplus_{i=1}^n a_i^3 = g(x_1, x_2, ..., x_n)$. Therefore, we get $\bigoplus_{i=1}^n a_i = f(x_1, x_2, ..., x_n) \oplus g(x_1, x_2, ..., x_n) \oplus g(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$.

- $P^* P^P P^* \longrightarrow P^P$: For the first box we have $\bigoplus_{i=1}^n a_i^1 = g(x_1, x_2, ..., x_n)$, for the second $\bigoplus_{i=1}^n a_i^2 = f(x_1, x_2, ..., x_n)$ and for the third $\bigoplus_{i=1}^n a_i^3 = g(x_1, x_2, ..., x_n)$. So the final outputs satisfy $\bigoplus_{i=1}^n a_i = g(x_1, x_2, ..., x_n) \oplus f(x_1, x_2, ..., x_n) \oplus g(x_1, x_2, ..., x_n) = f(x_1, x_2, ..., x_n)$.

- $P^* P^* P^* \longrightarrow P^*$: Here we have for the first box $\bigoplus_{i=1}^n a_i^1 = g(x_1, x_2, ..., x_n)$, for the second $\bigoplus_{i=1}^n a_i^2 = g(x_1, x_2, ..., x_n)$ and for the third $\bigoplus_{i=1}^n a_i^3 = g(x_1, x_2, ..., x_n)$. So we get $\bigoplus_{i=1}^n a_i = g(x_1, x_2, ..., x_n) \oplus g(x_1, x_2, ..., x_n) \oplus g(x_1, x_2, ..., x_n) = g(x_1, x_2, ..., x_n)$.

After the application of the distillation protocol we get the final box, which is given by

$$P_{\varepsilon'}^P = \left(2\varepsilon - 2\varepsilon^2\right) P + \left(1 - \left(2\varepsilon - 2\varepsilon^2\right)\right) P^* \tag{4.6}$$

Hence, $\varepsilon' = 2\varepsilon - 2\varepsilon^2$. We are now able to determine what kind of boxes can be distilled by this protocol. If the protocol distills the box P_ε^P to $P_{\varepsilon'}^P$ then ε has to fulfill $\varepsilon' > \varepsilon$. We observe that all $0 < \varepsilon < 1/2$ fulfill this condition, and therefore, the protocol distills any box of the family of local combinated full-correlation boxes with $0 < \varepsilon < 1/2$.

We show that in the asymptotic regime of many copies, any P_ε^P with $0 < \varepsilon < 1/2$ is distilled arbitrarily closely to $P_{1/2}^P$. We are starting with 2^m copies of the box P_ε^P (since P^* is a local box we are able to simulate it as many we need) and get finally the box $P_{\varepsilon_m}^P$, where ε_m is the mth iteration of the map

$$T(\varepsilon) = 2\varepsilon - 2\varepsilon^2. \tag{4.7}$$

The fixed points of this map are $\varepsilon = 0$ and $\varepsilon = 1/2$. To analyse the stability of these two fixed points we calculate the eigenvalues of the Jacobian (since the map is one-dimensional the Jacobian is a real value and not a matrix). For the box P^* ($\varepsilon = 0$) we find $\frac{\mathrm{d}T}{\mathrm{d}\varepsilon}|_{\varepsilon=0} = 2 > 1$, so this box is repulsive. For the other box $P_{1/2}^P$ we find $\frac{\mathrm{d}T}{\mathrm{d}\varepsilon}|_{\varepsilon=1/2} = 0 < 1$, so this box is attractive. □

Remark 4.8 *Note that the original XOR protocol is also contained in the generalization. For that we define $P = P^{PR}$ and $P^* = P^c$.*

For bipartite boxes were shown that the XOR protocol is the best non-adaptive protocol to distill non-local of boxes [21]. It is a open question, if these protocols above also are the best non-adaptive protocols for multipartite non-local (full-correlation) boxes.

4.2 Distillation based on the Brunner-Skrzypczyk Protocol

In this section we have a look at a distillation protocol based on the Brunner-Skrzypczyk protocol [8] for distilling multi-party non-locality.

4.2.1 Brunner-Skrzypczyk Protocol

In this section we present the results from [8]. Brunner and Skrzypczyk presented a protocol that is deterministically distilling non-locality. This protocol works optimal for correlated non-local boxes and in the asymptotic limit all these boxes will be distilled to the PR-box.

The Brunner-Skrzypczyk protocol (or short BS protocol) works as follows:

Protocol 4.9 (BS Protocol) *Alice and Bob share two boxes. Alice inputs in box i x_i and Bob input in box i y_i. The outputs of box i are then denoted by a_i and b_i. Alice proceeds as follows: $x_1 = x$, $x_2 = xa_1$ and Bob proceeds as Alice: $y_1 = y$, $y_2 = yb_1$. In the end they output: $a = a_1 \oplus a_2$ and $b = b_1 \ominus b_2$.*

The following theorem is proved in [8]:

Theorem 4.10 *The BS protocol takes two copies of an arbitrarily box P_{ε}^{PR} with $0 < \varepsilon < 1$ to a bipartite correlated non-local box $P_{\varepsilon'}^{PR}$ with $\varepsilon' > \varepsilon$, thus distilling non-locality. Moreover, in the asymptotic regime of many copies, any P_{ε}^{PR} with $0 < \varepsilon$ is distilled arbitrarily closely to the PR box.*

4.2.2 Generalization of the Brunner-Skrzypczyk Protocol for n-PR Boxes

We present a non-locality distillation protocol for generalized n-partite PR boxes that is similar to the Brunner-Skrzypczyk protocol. It works also deterministically for correlated non-local boxes for n parties (Def. 2.10).

Protocol 4.11 (Generalized BS Protocol for n-PR Boxes) *The protocol works as follows (see Fig. 4.2). All n parties share two boxes, where we denote x_i as the value that the ith party inputs to the first box and y_i the value that the ith party inputs to the second box. The output bit of the first box for the ith party is then a_i and the output bit of the second box is b_i. The n parties proceed as follows: $y_i = x_i\bar{a}_i$ and they output finally $c_i = a_i \oplus b_i$.*

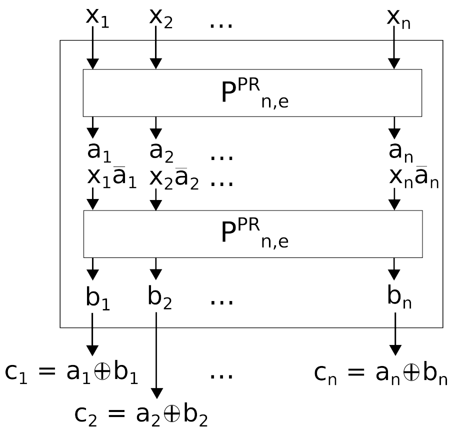

Figure 4.2: Generalized BS protocol for n-PR boxes

With this protocol we are also able to distill a large class of boxes arbitrarily closely to the n-PR box:

Theorem 4.12 *The Generalized BS protocol takes two copies of an arbitrarily box $P^{PR}_{n,\varepsilon}$ with $0 < \varepsilon < 1$ to a n-partite correlated non-local box $P^{PR}_{n,\varepsilon'}$ with $\varepsilon' > \varepsilon$, thus distilling non-locality. Moreover, in the asymptotic regime of many copies, any $P^{PR}_{n,\varepsilon}$ with $0 < \varepsilon$ is distilled arbitrarily closely to the n-PR box.*

Since the protocol and theorem are a generalization of [8], the proof works almost in the same manner.

Proof We start with the initial two box state of the protocol which is given by

$$P^{PR}_{n,\varepsilon}P^{PR}_{n,\varepsilon} = \varepsilon^2 P^{PR}_n P^{PR}_n + \varepsilon\,(1-\varepsilon)\left(P^{PR}_n P^c_n + P^c_n P^{PR}_n\right) + (1-\varepsilon)^2 P^c_n P^c_n \tag{4.8}$$

Now, we apply the above distillation protocol and get the final box. As in [8], we use the notation $P_i P'_i \longrightarrow P_f$ which means that the protocol takes two initial boxes, P_i and P'_i, to one copy of the final box P_f.

- $P^{PR}_n P^{PR}_n \longrightarrow P^{PR}_n$: For the first box we have $\bigoplus_{i=1}^n a_i = \bigwedge_{i=1}^n x_i$, implying $a_1 = \bigoplus_{i=2}^n a_i \oplus \bigwedge_{i=1}^n x_i$. For the second box we have $\bigoplus_{i=1}^n b_i = \bigwedge_{i=1}^n x_i \bar{a}_i = \bigwedge_{i=1}^n x_i \wedge \bigwedge_{i=2}^n \bar{a}_i \wedge \neg(\bigoplus_{i=2}^n a_i \oplus \bigwedge_{i=1}^n x_i) = 0$. So the outputs satisfy the relation $\bigoplus_{i_1}^n c_i = \bigoplus_{i=1}^n a_i \oplus b_i = \bigwedge_{i=1}^n x_i$.

- $P^{PR}_n P^c_n \longrightarrow P^{PR}_n$: For the first box we have $\bigoplus_{i=1}^n a_i = \bigwedge_{i=1}^n x_i$. For the second box we have $\bigoplus_{i=1}^n a_i = 0$ independently of the inputs. Therefore, we get $\bigoplus_{i_1}^n c_i = \bigoplus_{i=1}^n a_i \oplus b_i = \bigwedge_{i=1}^n x_i$.

- $P^c_n P^{PR}_n \longrightarrow 2^{1-n} P^{PR}_n + \left(1 - 2^{1-n}\right) P^c_n$: For the first box we have $\bigoplus_{i=1}^n a_i = 0$, implying $a_1 = \bigoplus_{i=2}^n a_i$, where $a_2, a_3, ..., a_n$ are random. For the second box we have

$$\bigoplus_{i=1}^{n} b_i = \bigwedge_{i=1}^{n} x_i \bar{a}_i = \bigwedge_{i=1}^{n} x_i \wedge \bigwedge_{i=2}^{n} \bar{a}_i \wedge \neg\left(\bigoplus_{i=2}^{n} a_i\right)$$

$$= \begin{cases} \bigwedge_{i=1}^{n} x_i & \text{Prob } \frac{1}{2^{n-1}}, \text{ all } a_i = 0 \\ 0 & \text{Prob } 1 - \frac{1}{2^{n-1}}, \text{ otherwise.} \end{cases}$$

So the final outputs satisfy $\bigoplus_{i_1}^{n} c_i = \bigoplus_{i=1}^{n} a_i \oplus b_i = \bigoplus_{i=1}^{n} b_i$.

- $P_n^c P_n^c \longrightarrow P_n^c$: Here we have for the first box $\bigoplus_{i=1}^{n} a_i = 0$ and for the second box $\bigoplus_{i=1}^{n} b_i = 0$. So we get $\bigoplus_{i_1}^{n} c_i = \bigoplus_{i=1}^{n} a_i \oplus b_i = 0$.

After the application of the distillation protocol we get the final box, which is given by

$$P_{n,\varepsilon'}^{PR} = \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right) P_n^{PR} + 1 - \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right) P_n^c \tag{4.9}$$

Hence, $\varepsilon' = \varepsilon/2^{n-1}\left(2^{n-1} + 1 - \varepsilon\right)$. We are now able to determine what kind of boxes can be distilled by this protocol. If the protocol distills the box $P_{n,\varepsilon}^{PR}$ to $P_{n,\varepsilon'}^{PR}$, then ε has to fulfill $\varepsilon' > \varepsilon$. We observe that all $0 < \varepsilon < 1$ fulfill this condition and, therefore, the protocol distills any box of the family of of correlated non-local boxes (see Def. 2.10).

We show that in the asymptotic regime of many copies, any $P_{n,\varepsilon}^{PR}$ with $0 < \varepsilon < 1$ is distilled arbitrarily closely to the n-PR box. We are starting with 2^m copies of the box $P_{n,\varepsilon}^{PR}$ and get finally the box P_{n,ε_m}^{PR}, where ε_m is the mth iteration of the map

$$T_n(\varepsilon) = \frac{\varepsilon}{2^{n-1}}\left(2^{n-1} + 1 - \varepsilon\right). \tag{4.10}$$

The fixed points of this map are $\varepsilon = 0$ and $\varepsilon = 1$. To analyse the stability of these two fixed points we calculate the eigenvalues of the Jacobian (since the map is one-dimensional the Jacobian is a real value and not a matrix). For the box P_n^c ($\varepsilon = 0$) we find $\frac{\mathrm{d}T}{\mathrm{d}\varepsilon}|_{\varepsilon=0} = 1 + 1/2^{n-1} > 1$, so this box is repulsive. For the other box P_n^{PR} we find $\frac{\mathrm{d}T}{\mathrm{d}\varepsilon}|_{\varepsilon=1} = 1 + 1/2^{n-1} - 1/2^{n-2} < 1$, so this box is attractive. □

We showed that in the asymptotic regime of many copies the n-PR boxes can be distilled arbitrary closely by the generalized BS protocol. It raise the question, if there are also other n-partite full-correlation boxes that can be distilled arbitrary close by the generalized BS protocol. We will show that this is not possible.

Theorem 4.13 *The n-PR boxes are the only non-local full-correlation boxes that in the asymptotic regime of many copies can be distilled arbitrary closely by the generalized BS protocol.*

Proof It is enough to show that the only non-local full-correlation box which is unaffected by the BS-protocol are the n-PR boxes since ε' is a continuous function of ε in the proof of Theorem 4.12.

We know from Lemma 3.1 that the general form of a Boolean function f looks like

$$f(x_1,...,x_n) = \bigoplus_{I\in\mathcal{I}} \left(a_I \cdot \bigwedge_{i\in I} x_i \right), \tag{4.11}$$

where $\mathcal{I} = \mathcal{P}\left(\{1,2,...,n\}\right)$ and $a_I \in \{0,1\}$ for all $I \subseteq \mathcal{I}$. If the BS protocol is applied to the full-correlation box with the associated function f, we get the new full-correlation box with the associated function

$$g(x_1,x_2,...,x_n) = f\left(x_1,x_2,...,x_n\right) \oplus f\left(x_1\bar{b}_1, x_2\bar{b}_2,...,x_n\bar{b}_n\right), \tag{4.12}$$

where $b_1 \oplus b_2 \oplus ... \oplus b_n = f(x_1,x_2,...,x_n)$. Since we are only interested in full-correlation boxes that are not affected by the BS protocol, the associated function f has to fulfill

$$f\left(x_1\bar{b}_1, x_2\bar{b}_2,...,x_n\bar{b}_n\right) = 0. \tag{4.13}$$

where $b_1 \oplus b_2 \oplus ... \oplus b_n = f(x_1,x_2,...,x_n)$. In the next step we substitute b_1 in the function and get

$$f\left(x_1 \cdot \left(1 \oplus b_2 \oplus ... \oplus b_n \oplus f\left(x_1,x_2,...,x_n\right)\right), x_2\bar{b}_2,...,x_n\bar{b}_n\right) = 0. \tag{4.14}$$

In Section 2.3.2, we have remarked that all $b_2, b_3, ..., b_n$ are completely random, this property will now be utilized. We test our function in a strategic way with different input elements and fix $x_1 = 0$:

Step	Input	Conclusion
1	00...00	$f(0,0,...,0,0) = a_I = 0$, $I = \emptyset$
2	00...01	$f(0,0,...,0,\bar{b}_n) = a_I\bar{b}_n = 0$, where $I = \{n\}$ and b_n arbitrarily $\Rightarrow a_I = 0$
3	00...10	$f(0,0,...,\bar{b}_{n-1},0) = a_I\bar{b}_{n-1} = 0$, where $I = \{n-1\}$ and b_{n-1} arbitrarily $\Rightarrow a_I = 0$
4	00...11	$f(0,0,...,\bar{b}_{n-1},\bar{b}_n) = a_I\bar{b}_{n-1}\bar{b}_n = 0$, where $I = \{n-1,n\}$ and b_{n-1}, b_n arbitrarily $\Rightarrow a_I = 0$
⋮	⋮	⋮
2^{n-1}	01...11	$f(0,\bar{b}_2,...,\bar{b}_{n-1},\bar{b}_n) = a_I\bar{b}_2 \cdot ... \cdot \bar{b}_n = 0$, where $I = \{2,3,...,n\}$ and $b_2, b_3, ..., b_n$ arbitrarily $\Rightarrow a_I = 0$

If we do the same procedure for every indice we get that

$$f(x_1, x_2, ..., x_n) = a_I x_1 x_2 \cdot ... \cdot x_n, \tag{4.15}$$

where $I = \{1, 2, ..., n\}$ and $a_I \in \{0, 1\}$.

If $a_I = 1$ we get the n-PR box and we already know from Thm 4.12 that this kind of box can be distilled by the generalized BS protocol. If $a_I = 0$ we get a local box which is not interesting to distill. □

Chapter 5

Non-Local Distillation With Partial Communication

In Chapter 4 we have seen that the n-partite PR boxes are the only kind of full-correlation boxes that in the asymptotic regime of many copies can be distilled arbitrarily closely by the generalized BS protocol. Since the generalized BS protocol does not work for other full-correlation boxes[1], we are looking for distillation protocols based on the generalized BS protocol but also allowing communication between some of the parties. That means we allow some parties to use one-way communication channels which can be used as often as they like[2]. We will show that the number of these one-way communication channels is lesser than the number of one-way communication channels we need to get the behaviour from scratch.

5.1 Idea

To give an understanding of the basic idea we start with an example:

We have a look at the box

$$P(abc|xyz) = \begin{cases} \frac{1}{4} & a \oplus b \oplus c = xy \oplus xz \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

As we have seen in Theorem 4.13 the generalized BS protocol does not work for this box.

But we know that this box can be simulated by two PR boxes (see Fig. 5.1 a)). We assume as in the Chapter 4 that there are correlated non-local boxes for

[1] This does not mean that there exists no other distillation protocol that would be able to do this. But so far the authors do not know such a distillation protocol.

[2] This makes sense because in the asymptotic region of many copies we apply the protocol very often and we will need the channel in every application of the protocol.

two parties (Def. 2.10) instead of two PR boxes. If we would be able to isolate both of these boxes we could apply to each of them the generalized BS protocol (see Fig. 5.1 a)). Since the original box cannot simulate the two correlated non-local boxes, we cannot isolate them. But if we allow an one-way communication channel from the third party to the first party, we are obviously able to simulate a perfect PR box between these two parties by communication (we do not have to distill the non-perfect PR box between them) and the non-perfect PR between the first party and second party can by simulated by the original box and the one-way communication channel. For that the parties input $(x, y, 0)$ to the original box and further, the third party sends his output to the first party. So the new output for the first party is the XOR of the third parties output and its output. Now, we are able to apply the Brunner-Skrzypzyk protocol to the isolated box (see Fig. 5.1 b)). If we would simulate the perfect original box only with one-way communication channels we would need two of them.

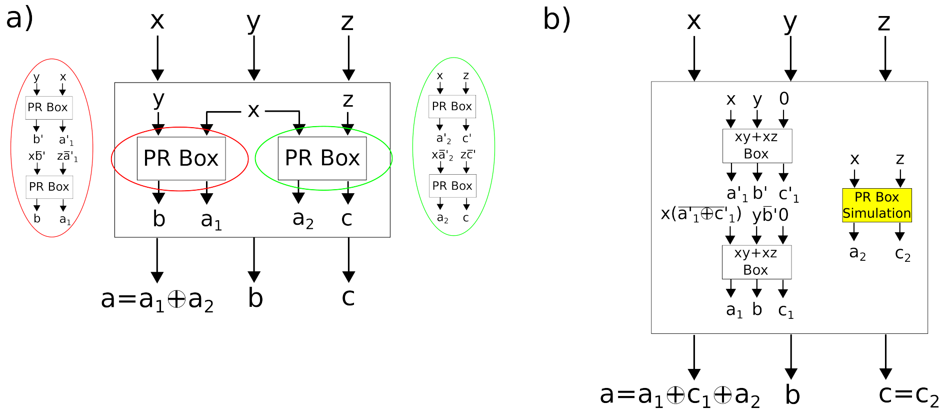

Figure 5.1: a) Isolation of the PR boxes and application of the generalized BS protocol to both of them b) Generalized BS protocol with a one-way communication channel from the third party to the first party

5.2 Distillation With Partial Coomunication

Before we are able to generalize the example to an arbitrary full-correlation box, we repeat how an arbitrary full-correlation box can be constructed. For that we need Lemma 3.1 which says that a Boolean function f with input elements $x_1, x_2, ..., x_n$ can be written as

$$f(x_1, ..., x_n) = \bigoplus_{I \in \mathcal{I}} \left(a_I \cdot \bigwedge_{i \in I} x_i \right), \tag{5.2}$$

where $\mathcal{I} = \mathcal{P}(\{1, 2, ..., n\})$ and $a_I \in \{0, 1\}$ for all $I \in \mathcal{I}$.

Hence, it is obvious that the full-correlation box associated to the Boolean function f can be constructed by $\sum_{I\in\mathcal{I}} a_I$ n-PR boxes. Indeed, for every $a_I = 1$, an n-PR box is needed, where the ith party inputs x_i if $i \in I$, and otherwise it inputs 1. Then, the box will output b_i^I. In the end, every party outputs $c_i = \bigoplus_{I\in\mathcal{I},\ a_I=1} b_i^I$. For an example, see Fig. 5.2. Note that the n-PR boxes belonging to a_I where $|I| \leq 1$ are local and can be simulated by local operations and shared randomness.

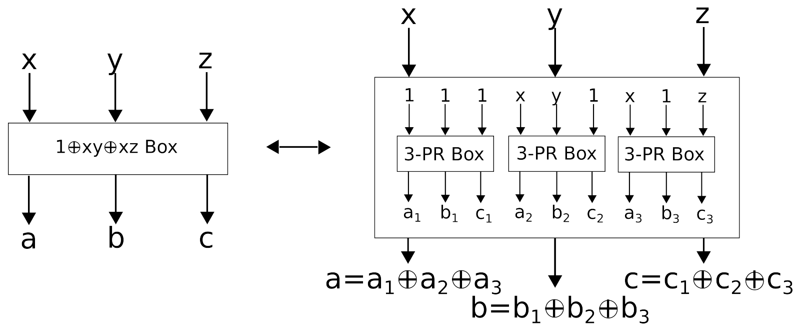

Figure 5.2: Construction of the $1 \oplus xy \oplus xz$ box

We already know that all n-partite full-correlation boxes can be simulated by n-partite PR boxes. As in Section 3.2.3 we define the set of all n-PR boxes that are needed to simulate the full-correlation box: Let

$$\mathcal{J} := \{I \in \mathcal{I} \,|\, a_I = 1 \text{ and } |I| \geq 2\}. \tag{5.3}$$

This set can be partitioned into disjoint subsets $\{J_1, J_2, ..., J_{n_\mathcal{J}}\}$ such that all $A \in J_i$ and $B \in J_j$ fulfill $A \cap B = \emptyset$ for all $i \neq j$. We define the maximal number of such subsets as $n_\mathcal{J}$. Later, we will see that it is important to know how many of the variables in a non-local box appear only in this non-local box, for that we define $m_I = |I \setminus \bigcup_{J\in\mathcal{J}\setminus I} J|$ for all $I \in \mathcal{J}$.

5.2.1 Simulation of a Full-Correlation Box With Classical Communication Channels

Theorem 5.1 shows how many one-way communication channels are needed to simulate an n-partite full-correlation box.

Theorem 5.1 (Number of One-Way Communication Channels) *Let f be the Boolean function associated to an n-partite full-correlation box, and let f be defined as in Lemma 3.1. If $n_\mathcal{J} = 1$, then the number $N_{comm}^{scratch}$ of one-way communication* *channels to simulate the full-correlation box from scratch is*

$$N_{\text{comm}}^{\text{scratch}} = \left| \bigcup_{I \in \mathcal{J}} I \right| - 1. \tag{5.4}$$

Proof We prove the statement by induction. We ignore the local part of the Boolean function f (i.e. the terms of single variables) and start with the case when the function f depends on two variables. The case $|\mathcal{J}| = 2$ is equivalent to a PR-box. From [28], we know that it can be simulated by one one-way communication channel. Now we assume that the claim is true for $|\mathcal{J}| \leq n$. Assume we have a function with $|\mathcal{J}| = n + 1$ that still fulfills the assumption of the theorem. We substitute 1 for x_i, where x_i is the input which is an element of a minimal number of elements of $\mathcal{J}$. This new function still fulfills the assumption of the theorem. We also know that $|\mathcal{J}| = n$ and, therefore, we need $n - 1$ communication channels to simulate the associated box. We combine all these n function values into one variable. The original function can be written with two variables. Therefore, we are back in the case $|\mathcal{J}| = 2$. Together, we need n one-way communication channels to simulate a function with $|\mathcal{J}| = n + 1$. □

5.2.2 Distillation Protocol

We construct an n-partite box where the outputs depend on the outputs of two full-correlation boxes for less than n parties. These two boxes are defined by

$$P_1(a_1...a_{k_2}|x_1...x_{k_2}) = \begin{cases} \frac{1}{2^{k_2-1}} & \bigoplus_{i=1}^{k_2} a_i = g_1(x_1, ..., x_{k_2}) \\ 0 & \text{otherwise,} \end{cases} \tag{5.5}$$

where g_1 is a Boolean function which depends on all of its input variables and $k_2 < n$. The second box is defined as

$$P_2(b_{k_1}...b_n|x_{k_1}...x_n) = \begin{cases} \frac{1}{2^{n-k_1}} & \bigoplus_{i=k_1}^{n} b_i = \prod_{i=k_1}^{k_3} x_i \\ 0 & \text{otherwise,} \end{cases} \tag{5.6}$$

where $0 < k_1 < k_2 < k_3 \leq n$. These two boxes can be calculated in parallel. Finally the constructed box outputs to party i

$$c_i = \begin{cases} a_i & i \in \{1, 2, ..., k_1 - 1\} \\ a_i \oplus b_i & i \in \{k_1, k_1 + 1, ..., k_2\} \\ b_i & i \in \{k_2 + 1, k_2 + 2, ..., n\}. \end{cases} \tag{5.7}$$

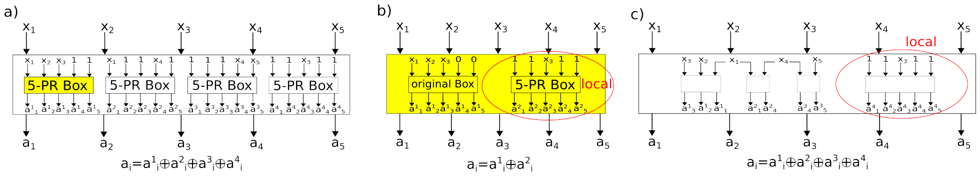

Figure 5.3: a) Simulating the full-correlation box with four 5-PR boxes. b) How to simulate the first 5-PR box with the original full-correlation box and a local box. c) Simulation of the full-correlation box with n-PR boxes without a constant input and a local box.

Lemma 5.2 *The constructed box is equivalent (i.e. the joint probabilities are equal) to the full-correlation box defined by*

$$P(\vec{c}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^{n} c_i = g_1(x_1, ..., x_{k_2}) \oplus \prod_{i=k_1}^{k_3} x_i \\ 0 & otherwise. \end{cases} \tag{5.8}$$

Proof The statement follows directly from the property of the full-correlation box that the set of outputs of any subset of $n-1$ parties (or smaller) is completely random [3], and the property that the XOR conserves randomness in case of independence. □

Theorem 5.3 and Corollary 5.4 state that a general class of full-correlation boxes can be simulated by distillation and classical one-way communication channels. The number of these one-way channels is then smaller than the number of one-way communication channels we need if we do not apply a distillation protocol, i.e. operate from scratch.

Theorem 5.3 (Distillation With Communication) *Let f be a Boolean function associated to an n-partite full correlation box, and let f be written as in Lemma 3.1. If f fulfills $n_{\mathcal{J}} = 1$, then:*

(i) The full-correlation box can be constructed from generalized PR-boxes shared between a different number of parties such that in at most one generalized PR box some parties input all the time a constant.

(ii) The number $N_{comm}^{distill}$ of necessary one-way communication channels for simulating the full-correlation box with using the generalized BS protocol is

$$N_{\text{comm}}^{\text{distill}} \leq \begin{cases} n - 1 - \max_{I \in \mathcal{J}}(m_I) & \max_{I \in \mathcal{J}}(m_I) \neq n \\ 0 & \max_{I \in \mathcal{J}}(m_I) = n. \end{cases} \tag{5.9}$$

Proof In this proof, we replace full-correlation boxes with $a_I = 1$ for $|I| \leq 1$ by the full-correlation box with $a_I = 0$ for $|I| \leq 1$, and all other a_I for all $I \in \mathcal{I} \setminus \{\emptyset\}$ keep their values. We can do this by taking the XOR of the original box and the local box with $a_I = 1$ for $|I| \leq 1$. To get our original box back in the end, we take again the XOR of the changed box and the local box.

We start to prove part (i) of the theorem. The idea is to replace the boxes step by step. In the first step, we are beginning with a n-PR box with the associated set I. To that end, we are looking for another n-PR box with associated set J such that $I \cap J \neq \emptyset$ (this is possible because of the assumption of the theorem). Because of Lemma 5.2, we are able to replace these two boxes by two smaller boxes. We substitute the first box by an $|I \setminus J|$-PR box with inputs I. The second box is substituted by an $(n - |I|)$-box, where we input J and for the parties $\{1, 2, ..., n\} \setminus (I \cup J)$, we input 1.

Assume that we have, in this way, replaced some n-PR boxes by new boxes. Again, we are looking for an n-PR box which is not yet replaced, and whose input elements intersect with the input elements of the new box. We are making the same steps as before to replace these two boxes. In the end, we have replaced all n-PR boxes to a new box with the claimed properties (see Fig. 5.4).

We prove part (ii) of the theorem. For this part, we assume that the replacement is made according to part (i). We have replaced the original n-PR boxes such that the general PR box with constant element does not correspond to the original n-PR box belonging to the biggest m_I. This is possible, since we can replace this box first. We are now able to isolate the box belonging to the biggest m_I. Therefore, we allow all parties that appear at least twice as well as the parties that input all the time a constant to communicate their inputs and outputs to a party which acts also in the isolated box. We have isolated the general PR box, and we are able to apply the generalized BS protocol to this box. All the other generalized PR boxes that appear in the abstraction of part (i) in the theorem can be simulated by the communication of the parties and shared randomness. So we will need $\max_{I \in \mathcal{J}}(m_I)$ one-way-communication channels less than when we start from scratch. □

Corollary 5.4 *Let f be a Boolean function associated to an n-partite full correlation box, and let f be written as in Lemma 3.1. If f fulfills that $n_{\mathcal{J}} = 1$ and $\max_{I \in \mathcal{J}}(m_I) > n - |\bigcup_{I \in \mathcal{J}} I|$, then*

$$N_{\text{comm}}^{\text{distill}} < N_{\text{comm}}^{\text{scratch}} . \tag{5.10}$$

Proof The statement follows directly from Theorems 5.1 and 5.3. □

Remark 5.5 *If the assumptions of Theorem 5.3 are not fulfilled, we will need the same number of one-way communication canals as in the classical case. That is because we are not able to abstract the boxes in the way we are doing in Theorem*

5.3 a). So every output appears at least twice and so we are no longer able to isolate one of the boxes with lesser communication than in the classical way!

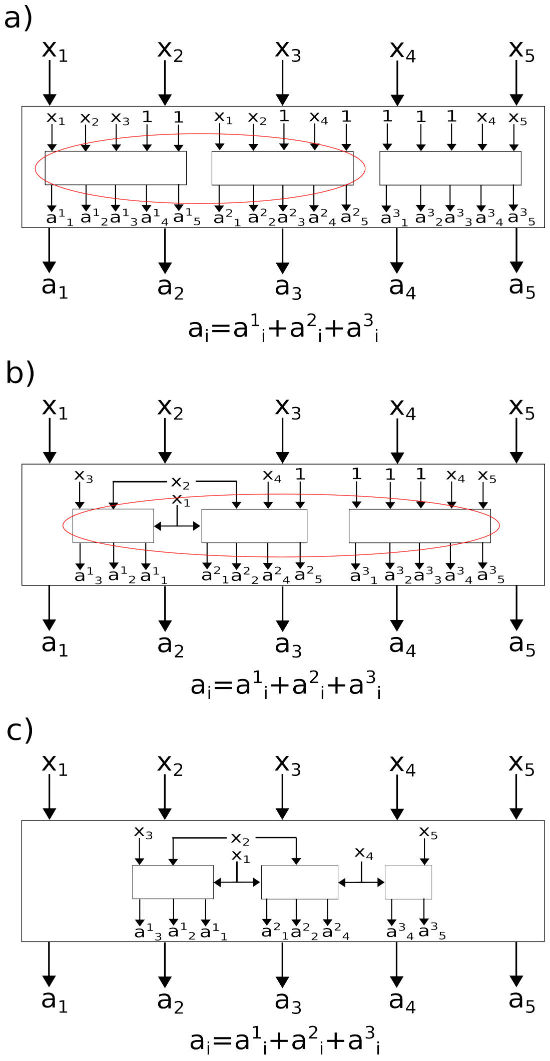
a)
x1 x2 x3 x4 x5
x1 x2 x3 1 1 x1 x2 1 x4 1 1 1 1 x4 x5
a¹1 a¹2 a¹3 a¹4 a¹5 a²1 a²2 a²3 a²4 a²5 a³1 a³2 a³3 a³4 a³5
a1 a2 a3 a4 a5
ai=a¹i+a²i+a³i
b)
x1 x2 x3 x4 x5
x3 x2 x1 x4 1 1 1 1 x4 x5
a¹3 a¹2 a¹1 a²1 a²2 a²4 a²5 a³1 a³2 a³3 a³4 a³5
a1 a2 a3 a4 a5
ai=a¹i+a²i+a³i
c)
x1 x2 x3 x4 x5
x3 x2 x1 x4 x5
a¹3 a¹2 a¹1 a²1 a²2 a²4 a³4 a³5
a1 a2 a3 a4 a5
ai=a¹i+a²i+a³i

Figure 5.4: Approach of Thm 5.3 (i)

Corollary 5.6 *Every extremal full-correlation box with associated Boolean function f such that $\max_{I\in\mathcal{J}}(m_I) > 0$ fulfills*

$$N_{\text{comm}}^{\text{distill}} < N_{\text{comm}}^{\text{scratch}} . \tag{5.11}$$

Proof The statement follows from Theorem 3.2 and Corollary 5.4. □

5.3 Example

In this example we want to distill some boxes up to the following full-correlation box:

$$P(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^{5} a_i = x_1x_2x_3 \oplus x_1x_4 \oplus x_4x_5 \oplus x_3 \\ 0 & \text{otherwise.} \end{cases} \tag{5.12}$$

Therefore, we determine first the above-defined sets and constants. Let $\mathcal{I} = \mathcal{P}(\{1,2,3\})$. From Lemma 3.1, we know that all $a_I = 1$ for $I \in \{\{1,2,3\},\{1,4\},\{4,5\},\{3\}\}$, and otherwise $a_I = 0$. This means that the given full-correlation box can be simulated by four 5-PR boxes with some constant inputs, where one of these boxes is local (see Fig. 5.3 a)). We are also able to assign the set $\mathcal{J}$ of non-local n-PR boxes that are needed to simulate the full-correlation box:

$$\mathcal{J} = \{\{1,2,3\},\{1,4\},\{4,5\}\} \tag{5.13}$$

Each of these three non-local 5-PR boxes can be obtained from the original box by taking the XOR of the original box and the local 5-PR box when every party inputs its bits except for the parties that input the constant 1 to the 5-PR box, they input 0 in both boxes (see Fig. 5.3 b)). If we apply Theorem 5.3 (i), then we know that the non-local part of the original full-correlation box can be simulated by three connected n-PR boxes with no constant input.

Since we know $\mathcal{J}$, the number of required one-way communication channels for simulating the full-correlation box can be calculated with Theorem 5.1:

$$N_{\text{comm}}^{\text{distill}} = \left| \bigcup_{I \in \mathcal{J}} I \right| - 1 = 4. \tag{5.14}$$

Obviously, this box is not local. To determine the distance (measured in the L^1-norm), we can use a linear program and get that the distance is 20, and the closest local box (not unique) is given by

$$P^L(\vec{a}|\vec{x}) = \begin{cases} \frac{1}{2^{n-1}} & \bigoplus_{i=1}^{5} a_i = x_3 \\ 0 & \text{otherwise.} \end{cases} \tag{5.15}$$

We start with the second part of the example, where we show in detail how we distill a box from the family $P_\varepsilon = \varepsilon P + (1-\varepsilon)P^L$, where $0 < \varepsilon < 1$, up to $P(\vec{a}|\vec{x})$.

We want to distill this box arbitrarily closely to the full-correlation box above. For that, we determine first which of the parties have to communicate. Therefore, we calculate the number of parties that only belong to one of the non-local 5-PR boxes: $m_{\{1,2,3\}} = 2$, $m_{\{1,4\}} = 1$, and $m_{\{4,5\}} = 1$. This means that we isolate the box that belongs to the 5-PR box with three arbitrary inputs. This can be done in the same way as before: We input $(x_1, x_2, x_3, 0, 0)$ in P_ε and the local box and take then the XOR of its outputs. Then, we use one-way communication channels from Party 5 to 4 and one from 4 to 1. Remember that the communication channels can be used as often as the parties want. Hence, we are able to simulate perfectly the two 2-PR box, and the non-perfect 3-PR box can be isolated by communicating the inputs and outputs of the two 2-PR box to Party 1 (see Fig. 5.3 c)). We have isolated the box $P_{3,\varepsilon}^{PR}$ that is known to be distillable up to P_3^{PR} by the generalized BS protocol. In this way, we are able to distill the box P_ε up to the full-correlation box in the beginning.

We get that the number of one-way communication channels that is needed for this kind of distillation is $N_{\text{comm}}^{\text{distill}} = 2$, i.e., less than $N_{\text{comm}}^{\text{scratch}} = 4$.

Chapter 6

Multi-Party Probabilistic Communication Complexity

This chapter is about communication complexity and the question, "How much do non-local boxes decrease the communication complexity of Boolean functions?"

Assume that there are n parties that want to compute a Boolean function $f(x_1, ..., x_n)$, where x_i is a vector of bits known only by the ith party. Their task is to minimize the amount of communication required between the n parties with the goal that one of the parties, say the first party, learns the function value.

Yao [32] and Kushilevitz [23] were the first who formulated this problem and found some bounds for classical two-party problems. Cleve, Buhrmann [12], de Wolf [15], and Brassard [5] allowed the parties to use entangled quantum states. They showed that in this way, the communication complexity of some functions decreases, but that for computing the inner-product function, the parties still need the same amount of communication [13, 14].

Van Dam [31] showed that if two parties share PR boxes, the communication complexity gets *trivial* for every Boolean function. That means that only the second party has to send a bit to the first party, so the first party is able to compute the function value. Note that *trivial communication complexity* does not mean that there is no need of communication, since that would mean that the box must be signaling!

6.1 Probabilistic Communication Complexity in the Bipartite Case

In contrast to the above definition of communication complexity, Brassard *et al.* [6] introduced a probabilistic version of communication complexity.

Assume we have two parties, Alice and Bob, and they want to compute the function $f(x,y)$. Their task is to minimize the amount of communication required between Alice and Bob with the goal that Alice guesses the function value of $f(x,y)$ for all x and y correct with probability $p > 1/2$ bounded away from $1/2$.

In [6], is shown that in any world in which it is possible, without communication, to implement an approximation to the PR box that works correctly for every input with probability greater than $(3+\sqrt{6})/6 \approx 90.8\%$, every Boolean function has trivial probabilistic communication complexity.

Since we need the proof of this claim in a further section, we repeat the most important definitions and lemmas from [6].

Definition 6.1 (Distributed Bit) *A bit c is* distributed *if Alice has bit a and Bob bit b such that $c = a \oplus b$.*

Definition 6.2 (f is Distributively Computed) *A Boolean function f is* distributively computed *by Alice and Bob if, given inputs x and y, they can produce a distributed bit equal to $f(x,y)$.*

Definition 6.3 (Protocol has Bias) *A* protocol has a bias *for a Boolean function f if f can be distributively computed by the protocol without any communication and with probability strictly greater than 1/2 for every input.*

Lemma 6.4 *Provided Alice and Bob are allowed to share random variables, all protocols for Boolean functions have a bias.*

Definition 6.5 (Bounded Bias) *A protocol has a* bounded bias *for a Boolean function f if f can be distributively computed by the protocol without any communication and with probability bounded away from 1/2 for every input.*

Lemma 6.6 *Any Boolean function that has a protocol with bounded bias, has trivial communication complexity.*

Definition 6.7 (Non-Local Majority Problem) *The* non-local majority *problem consist in computing the distributed majority of three distributed bits. Let Alice have the bits x_1, x_2, x_3 and let Bob have y_1, y_2, y_3. The task for Alice and Bob is to compute a and b such that*

$$a \oplus b = \mathrm{Maj}\left(x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3\right), \tag{6.1}$$

where $Maj(u,v,w)$ denotes the bit occuring the most among u, v, and w.

Lemma 6.8 *For any q such that $5/6 < q \leq 1$, if Alice and Bob can compute non-local majority with probability at least q, every protocol for a Boolean function has bounded bias.*

Definition 6.9 (Non-Local Equality Problem) *The* non-local equality *problem consist in distributively deciding if three distributed bits are equal. Let Alice have the bits x_1, x_2, x_3 and let Bob have y_1, y_2, y_3. The task for Alice and Bob is to compute a and b such that*

$$a \oplus b = \begin{cases} 1 & \text{if } x_1 \oplus y_1 = x_2 \oplus y_2 = x_3 \oplus y_3 \\ 0 & \text{otherwise.} \end{cases} \tag{6.2}$$

Lemma 6.10 *Non-local equality can be computed using only two (perfect) PR boxes.*

Lemma 6.11 *Non-local majority can be computed using only two (perfect) PR boxes.*

6.2 Probabilistic Communication Complexity in the Multi-Partite Case

In the section before was analysed with which probability a PR box must be approximated to get trivial communication complexity. In this section we analyse some extremal multipartite full-correlation boxes of the non-signaling polytope.

In [24] were already shown that if the n-partite Svetlichny box, an n-partite full-correlation box with associated function $f(x_1, ..., x_n) = \bigoplus_{i=1}^{n-1} \bigoplus_{j=i+1}^{n} x_i x_j$, can be approximated with probability 93.7%, then the communication complexity gets trivial.

We start with generalizing Lemma 6.4 to n parties.

Lemma 6.12 *Provided all parties are allowed to share random variables, all protocols for Boolean functions are biased.*

Proof Let f be an arbitrarily Boolean function and let each party $i \in \{2, 3, ..., n\}$ shares a random variable z_i with the first party of the same size as the ith party's input. After receiving their inputs $\{x_1, x_2, ..., x_n\}$ (input x_i has length n_i), the first party computes its output $a_1 = f(x_1, z_2, z_3, ..., z_n)$ and the other parties outputs $a_i = 0$ if $x_i = z_i$ and otherwise they output a uniformly distributed random bit a_i. If $x_i = z_i$ for all i the distributed bit between the n parties is correct. In all other cases the probability that the distributed bit is correct is 1/2. The total probability to get a correct distributed bit is $1/2^{n_2+n_3+...+n_n} + (1 - 1/2^{n_2+n_3+...+n_n})1/2 > 1/2$. □

Also the definitions of the *non-local majority* problem and the *non-local equality* problem can be generalized in a natural way to n parties.

Definition 6.13 (Non-Local n-Partite Majority Problem) *The* non-local n-partite majority *problem consist in computing the distributed majority of n distributed bits. Let the ith party have the bits x_i^1, x_i^2, x_i^3. The task for the n parties is to compute a_i's such that*

$$\bigoplus_{i=1}^{n} a_i = \mathrm{Maj}\left(\bigoplus_{i=1}^{n} x_i^1, \bigoplus_{i=1}^{n} x_i^2, \bigoplus_{i=1}^{n} x_i^3\right), \tag{6.3}$$

where $Maj(u,v,w)$ denotes the bit occuring the most among u, v, and w.

Lemma 6.8 can also be applied to the non-local n-partite majority problem.

Definition 6.14 (Non-Local n-Partite Equality Problem) *The* non-local n-partite equality *problem consist in distributively deciding if three distributed bits are equal. Let the ith party have the bits x_i^1, x_i^2, x_i^3. The task for the n parties is to compute the a_i's such that*

$$\bigoplus_{i=1}^{n} a_i = \begin{cases} 1 & \text{if } \bigoplus_{i=1}^{n} x_i^1 = \bigoplus_{i=1}^{n} x_i^2 = \bigoplus_{i=1}^{n} x_i^3 \\ 0 & \text{otherwise.} \end{cases} \tag{6.4}$$

With the same construction as in the proof of Lemma 6.11, we are able to construct a non-local n-partite majority box with local operations and a non-local n-partite equality box.

Remark 6.15 *As in [6], Equation 6.4 is equivalent to*

$$\bigoplus_{i=1}^{n} a_i = \left(\bigoplus_{i=1}^{n} x_i^1 = \bigoplus_{i=1}^{n} x_i^2\right) \wedge \left(\bigoplus_{i=1}^{n} x_i^2 = \bigoplus_{i=1}^{n} x_i^3\right). \tag{6.5}$$

If we substitute $x'_1 = \bar{x}_1^1 \oplus x_1^2$, $x''_1 = \bar{x}_1^2 \oplus x_1^3$ and for all other i's $x'_i = x_i^1 \oplus x_i^2$ and $x''_i = x_i^2 \oplus x_i^3$ then we get

$$\begin{aligned} \bigoplus_{i=1}^{n} a_i &= \left(\bigoplus_{i=1}^{n} x'_i\right) \wedge \left(\bigoplus_{i=1}^{n} x''_i\right) && (6.6)\\ &= \bigoplus_{i=1}^{n} x'_i x''_i \oplus \bigoplus_{i \neq j} x'_i x''_j. && (6.7) \end{aligned}$$

The term $\bigoplus_{i=1}^{n} x'_i x''_i$ can be computed by local operations.

Now we analyse the probabilistic communication complexity of a Boolean function with n inputs elements using PR boxes or generalizations of the extremal tripartite full-correlation boxes.

6.2.1 PR Boxes

Assume n parties want to compute a Boolean function with n input elements using PR boxes. If they could simulate a (non-perfect) non-local n-partite majority box with (non-perfect) PR boxes, then we get trivial (probabilistic) communication complexity. Therefore, we are simulating equation 6.7 with PR boxes. For doing this, each pair of parties (say party i and j) has to share a PR box that they are using twice (they input $x'_i x''_j$ and $x'_j x''_i$). In total are $N = n(n-1)$ PR boxes used.

We assume that we only have approximations of PR boxes that work correctly with probability p. We want to determine p in order go get trivial probabilistic communication complexity.

If an even number of PR boxes output wrong bits then the simulated non-local n-partite equation box is still working well. So we have to solve the equation

$$\begin{aligned}
\frac{5}{6} &< \sum_{\substack{i=0\\ i \text{ even}}}^{n(n-1)} \binom{n(n-1)}{i} p^{n(n-1)-i}(1-p)^i && (6.8)\\
&= \sum_{i=0}^{\frac{1}{2}n(n-1)} \binom{n(n-1)}{2i} p^{n(n-1)-2i}(1-p)^{2i} && (6.9)\\
&= \frac{1}{2}\left[\left((1-2p)^2\right)^{\frac{1}{2}n(n-1)} + 1\right] && (6.10)\\
&= \frac{1}{2}\left[(1-2p)^{n(n-1)} + 1\right] && (6.11)
\end{aligned}$$

and get the solution $p > \frac{1}{2}\left(1 + \sqrt[N]{\frac{2}{3}}\right)$, where $N = n(n-1)$. To get from Equation 6.9 to 6.10 we applied the Binomial theorem.

6.2.2 n-PR Boxes

We are again simulating equation 6.7 with n-PR boxes. For doing this, all parties have to share an n-PR box that they are using $n(n-1)$ times, since the have to simulate each of the non-local terms in equation 6.7. In total are $N = n(n-1)$ PR boxes used.

We assume that we only have approximations of n-PR boxes that work correctly with probability p. We want to determine p in order to get trivial probabilistic communication complexity.

If an even number of PR boxes output wrong bits then the simulated non-local n-partite equation box is still working well. So we have to solve the equation

$$\frac{5}{6} < \sum_{\substack{i=0 \\ i \text{ even}}}^{n(n-1)} \binom{n(n-1)}{i} p^{n(n-1)-i}(1-p)^i \tag{6.12}$$

and get the solution $p > \frac{1}{2}\left(1 + \sqrt[N]{\frac{2}{3}}\right)$, where $N = n(n-1)$.

6.2.3 Svetlichny Boxes

In [24] were already shown that the non-local n-partite equality box can be simulated with three n-partite Svetlichny boxes, $f(x_1, ..., x_n) = \bigoplus_{i=1}^{n-1} \bigoplus_{j=i+1}^{n} x_i x_j$, independent of the number of parties. So if the n-partite Svetlichny boxes can be approximated with probability $p > \frac{1}{2}\left(1 + \sqrt[3]{\frac{2}{3}}\right) \approx 93.7\%$, then the communication complexity gets trivial.

6.2.4 $X(Y \oplus Z)$-Box

We try to simulate the n-partite non-local equation box with generalizations of the $X(Y \oplus Z)$-box $f(x_1, ..., x_n) = x_1 \wedge (\bigoplus_{i=2}^{n} x_i)$. But only using this box does not work. So we assume that the same kind of boxes with permuted parties are also available. This make sense, since if we would be able to produce such a box, there is no physical reason why we should not also be able to produce a permutation of it.

We are again simulating equation 6.7 with generalizations of the $X(Y \oplus Z)$-box and permutations. For doing this, all parties have to share every kind of the permutations of the generalization of the $X(Y \oplus Z)$-box (there exist n such boxes). Every of these boxes is then used twice. For example, the input for the box with associated function $f(x_1, ..., x_n) = x_1 \wedge (\bigoplus_{i=2}^{n} x_i)$ is the first time $(x_1', x_2'', ..., x_n'')$ and the second time $(x_1'', x_2', ..., x_n')$. So we use the boxes in total $N = 2n$ times.

We assume that we only have approximations of the $X(Y \oplus Z)$-boxes that works correctly with probability p. We want to determine p in order go get trivial probabilistic communication complexity.

If an even number of these boxes output wrong bits, then the simulated non-local n-partite equation box is still working well. So we have to solve the equation

$$\frac{5}{6} < \sum_{\substack{i=0 \\ i \text{ even}}}^{2n} \binom{2n}{i} p^{2n-i}(1-p)^i \tag{6.13}$$

and get the solution $p > \frac{1}{2}\left(1 + \sqrt[N]{\frac{2}{3}}\right)$, where $N = 2n$.

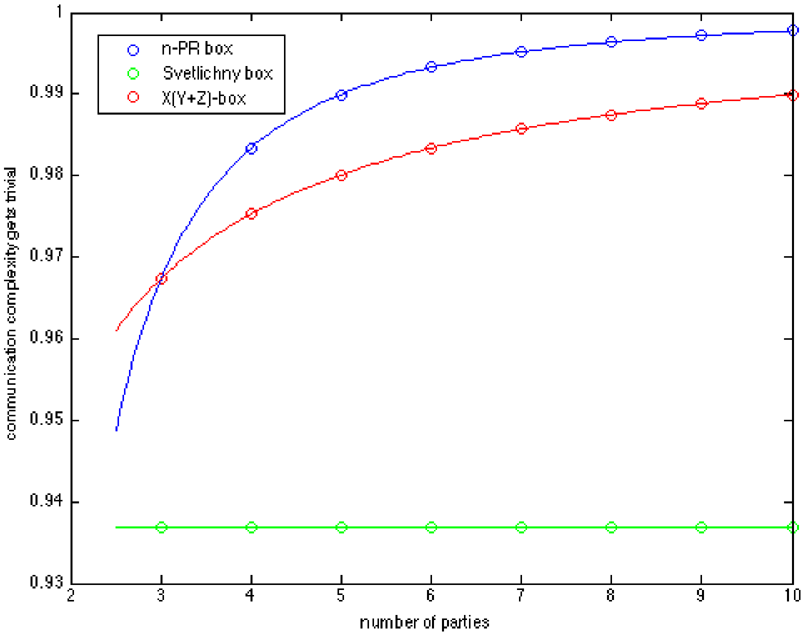

Figure 6.1: Graph shows when communication complexity gets trivial

6.3 Comparison of the Bounds

For the four types of boxes above were analysed, when communication complexity gets trivial. We compare this bounds. Since every full-correlation box can be simulated by PR boxes, we analyse how exact an approximation of the PR boxes must be in order to simulate the approximation of the full-correlation box.

n-PR Box

In Section 3.2.1, we have seen that an n-PR box can be simulated with $n(n-1)/2$ PR boxes. The detailed construction can be seen in Fig. 3.2.

We assume that we have approximations of the PR boxes that work correctly with probability p and determine how good this construction approximate the n-PR box.

3-PR Box

The 3-PR box can be simulated with 3 PR boxes as seen in the figure below.

We enumerate the three boxes; the box between the first and second party is number one, the box between the first and the third party is number two,

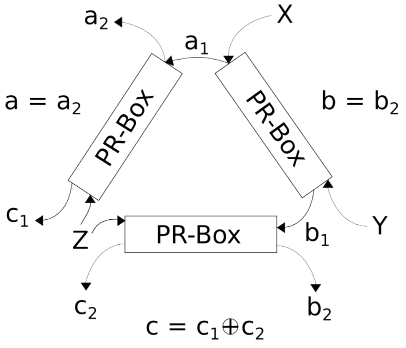

Figure 6.2: Simulation of a 3-PR box with three PR boxes

and the last is number three.

Assuming that each approximation of the PR box works correctly with probability p, we get the following result:

- box 1, 2, 3 correct or only box 1 correct: simulation works for all inputs correct (probability $= p^3 + p(1-p)^2$)
- only box 3 or box 2 not correct: simulation works for no input correct (probability $= 2p^2(1-p)$)
- only box 1 not correct or no box correct: simulation works for input $z = 1$ not correct (probability $= p^2(1-p) + (1-p)^3$)
- only box 2 or box 3 correct: simulation works for input $z = 0$ not correct (probability $= 2p(1-p)^2$)

Therefore, the simulated n-PR box works correctly for every input with probability

$$p' = p^3 + p(1-p)^2 + \min\left\{p^2(1-p) + (1-p)^3, 2p(1-p)^2\right\}. \tag{6.14}$$

Since $0 \le p \le 1$ we get

$$p' = p^3 + 2p(1-p)^2 + (1-p)^3. \tag{6.15}$$

Using an approximation of a 3-PR box, the communication complexity gets trivial if the approximation works correctly with probability $p' > \frac{1}{2}\left(1 + \sqrt[6]{\frac{2}{3}}\right)$. Therefore, the approximations of the PR boxes, we use to simulate the approximations of the 3-PR box, must work correct with probability $p > 0.9889$.

Estimate

Since it would be too complex to analyse it in detail, we do an estimate. Assume we simulate an n-PR box in the same recursive way as in Fig. 3.2. If the $n-1$-PR box works correctly and only an even number of the PR boxes work not correctly, then the simulated box still works well. Therefore, if the PR boxes work correctly with probability p, the constructed n-PR box works well with probability at least

$$p' = \prod_{k=1}^{\frac{1}{2}n(n-1)} \left(\sum_{\substack{i=0 \\ i \text{ even}}}^{k} \binom{k}{i} p^{k-i}(1-p)^{i} \right). \tag{6.16}$$

Svetlichny Box

A Svetlichny box can be simulated by $\frac{n(n-1)}{2}$ PR boxes. Each pair of parties shares a PR box, where both parties input their input bit. At the end, all parties compute the XOR of their $n-1$ output bits.

We assume that we have approximations of the PR boxes that work correctly with probability p. If an even number of the approximations do not work well, then the total simulation of the Svetlichny box still works well. Therefore, we have to solve the following equation

$$\frac{1}{2}\left(1+\sqrt[3]{\frac{2}{3}}\right) \leq \sum_{\substack{i=0 \\ i \text{ even}}}^{\frac{1}{2}n(n-1)} \binom{\frac{n(n-1)}{2}}{i} p^{\frac{1}{2}n(n-1)-i}(1-p)^{i}. \tag{6.17}$$

$X(Y \oplus Z)$-Box

An $X(Y \oplus Y)$-box can be simulated by $n-1$ PR boxes. The first party shares with each other party one PR box, where both input their bit. At the end, the first party computes the XOR of the output bits.

We assume that we have approximations of the PR boxes that work correctly with probability p. If an even number of the approximations do not work well, then the total simulation of the $X(Y \oplus Z)$-box still works well. Therefore, we have to solve the following equation

$$\frac{1}{2}\left(1+\sqrt[2n]{\frac{2}{3}}\right) \leq \sum_{\substack{i=0 \\ i \text{ even}}}^{n-1} \binom{n-1}{i} p^{n-1-i}(1-p)^{i}. \tag{6.18}$$

Comparing the Bounds

In the first analyse, the Svetlichny box seemed to be the best box for decreasing the communication complexity to trivial, since using this box, the communication complexity gets trivial if we can approximate this box with probability 93.7% independent of the number of parties.

Since every full-correlation box can be simulated with PR boxes, we compare the communication complexity of these boxes by comparing how good an approximation of a PR box must be in order to simulate an approximation of the full-correlation box to get trivial communication complexity. Obviously, we get that it would be best to use simple PR boxes. Amazingly, we find that simulating a Svetlichny box is still better than simulating one of the other full-correlation boxes, but the benefit to do this is low.

In the table below can be seen how good an approximation of a full-correlation box must be in order to get trivial communication complexity using the simulated full-correlation box.

	3	4	5	10	20
PR	0.9673	0.9834	0.9900	0.9978	0.9995
n-PR	0.9889	-	-	-	-
Svetlichny	0.9780	0.9889	0.9932	0.9985	0.9996
$X(Y \oplus Z)$-box	0.9834	0.9916	0.9950	0.9989	0.9997

Chapter 7

Discussion

In this thesis we focused on two main topics: *multiparty non-locality distillation with and without partial communication* and *probabilistic communication complexity in the multipartite case*. Therefore, we first analysed full-correlation boxes, especially when they are extremal boxes of the non-signaling polytope.

Distillation of Multiparty Non-Locality

In Chapter 4 we showed that all full-correlation boxes can be distilled in a given range (but not to the algebraic maximum) with a protocol similar to the XOR protocol. For bipartite non-local boxes it is well-known that the XOR protocol is the best non-adaptive protocol for distilling non-locality, so the question is raised if these new multipartite protocols also are the best non-adaptive protocols for distilling multi-party non-locality.

Further, we adapted the Brunner-Skrzypczyk protocol for the natural generalization of the Popescu-Rohrlich Box and showed that this protocol is able to distill these boxes to its algebraic maximum. There is no other full-correlation box that can be distilled to its algebraic maximum by such a protocol. It is still an open question if there are (adaptive) protocols that distill these boxes to its algebraic maximum.

Distillation of Multiparty Non-Locality with Partial Communication

Since we have not found a classical distillation protocol to distill all full-correlation boxes to its algebraic maximum, we allowed some parties to use classical communication channels.

We showed that a much bigger class of correlations, including all extremal multipartite correlations, can be distilled from arbitrarily weak to maximal strength by the generalized Brunner-Skrzypczyk protocol with partial communication, i.e., using only a subset of the channels required for the creation of the same correlation from scratch (less than if no weak box can be used). In other words, we showed that arbitrarily weak non-local correlations can replace communication between a subset of parties.

Probabilistic Communication Complexity

We used the same construction as Brassard *et al.* [6] to determine when probabilistic communication complexity gets trivial using PR boxes, n-PR boxes, Svetlichny boxes and $X(Y \oplus Z)$-boxes. In contrast to the other boxes, the Svetlichny box must only be approximated with probability 93.7% to get trivial communication complexity independent of the number of parties. All other boxes need a better approximation that is increasing with the number of parties.

Since all these boxes can be simulated with PR boxes, we compare the different bounds by analysing how exactly an approximation of the PR box must be in order to simulate the approximation of the full-correlation box. Therefore, we came to the result that it also is best to use only PR boxes in the multipartite case. Further, in this analysis the probability to get trivial communication complexity for the Svetlichny box is no longer a constant and increases almost identically as the probability for the $X(Y \oplus Z)$-box.

The construction from Brassard *et al.* [6] gives a bound when communication complexity gets trivial using PR boxes. It is still an open question if it is also a lower bound or if there exists constructions that earlier collapse communication complexity. Maybe one can find a link between, “Why is quantum physics not more non-local?” and communication complexity.

Appendix A

Extremal Boxes of the Tripartite Non-Signaling Polytope

In [28] are all tripartite extremal boxes of the non-signaling polytope determined. Here we present their results again.

There are 53856 extremal boxes of the non-signaling polytope that can be classified by 46 equivalence classes. Two boxes are in the same equivalence class if they are identical after relabeling of the parties, inputs, and outputs.

We describe for each equivalence class a representative in the following list.

In contrast to section 2.1, $x, y, z \in \{0, 1\}$ denote the inputs of each party and a, b, $c \in \{-1, 1\}$ denote the outputs. To get the probability distribution of the boxes from the list, we have to calculate

$$\begin{aligned} P(abc|xyz) &= \frac{1}{8}[1 + a\langle A_x\rangle + b\langle B_y\rangle + c\langle C_z\rangle + ab\langle A_xB_y\rangle \\ &\quad +ac\langle A_xC_z\rangle + bc\langle B_yC_z\rangle + abc\langle A_xB_yC_z\rangle], \end{aligned} \tag{A.1}$$

where $\langle A_x\rangle = P(a = 1|x) - P(a = -1|x)$ is the expectation value of the outcome a for the input x, $\langle A_xB_y\rangle = P(ab = 1|xy) - P(ab = -1|xy)$ is the expectation value of the product ab for the inputs x and y, and so on.

	$\langle A_x \rangle$		$\langle B_y \rangle$		$\langle C_z \rangle$		$\langle A_x B_y \rangle$				$\langle A_x C_z \rangle$				$\langle B_y C_z \rangle$				$\langle A_x B_y C_z \rangle$								
No	0	1	0	1	0	1	00	01	10	11	00	01	10	11	00	01	10	11	000	001	010	011	100	101	110	111	n_R
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	64
2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	-1	1	1	1	-1	1	1	1	-1	96
3	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	-1	384
4	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	-1	0	0	128
5	0	0	0	0	0	0	1	0	0	1	1	0	0	0	1	0	0	0	0	0	0	1	0	-1	0	0	384
6	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	-1	384
7	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	1	-1	0	0	192
8	0	0	0	0	0	0	1	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	-1	192
9	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	1	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$-\frac{1}{2}$	0	0	1	-1	1	1	0	0	384
10	$\frac{1}{2}$	0	0	0	0	0	0	0	1	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	1	1	1	-1	0	0	0	0	768
11	$\frac{1}{2}$	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	1	0	0	1	$\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$\frac{1}{2}$	0	1	-1	0	768
12	$\frac{1}{2}$	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	1	1	0	0	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	0	0	1	-1	1536
13	$\frac{1}{3}$	0	$\frac{1}{3}$	0	$\frac{1}{3}$	0	1	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$-\frac{1}{3}$	$\frac{1}{3}$	0	$\frac{2}{3}$	-1	$\frac{2}{3}$	1	1	0	1536
14	$\frac{1}{3}$	0	$\frac{1}{3}$	0	0	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	0	0	1	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	1	-1	$\frac{1}{3}$	1	0	0	3072
15	$\frac{1}{2}$	$\frac{1}{4}$	0	0	0	0	0	0	$\frac{3}{4}$	$\frac{1}{4}$	0	0	$\frac{3}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	1	1	1	-1	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	1536
16	$\frac{1}{3}$	0	$\frac{1}{3}$	0	0	0	1	0	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$-\frac{1}{3}$	0	0	1	-1	1	1	$\frac{2}{3}$	0	1536
17	$\frac{1}{3}$	0	0	0	0	0	0	0	1	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	1	1	1	-1	0	0	$\frac{2}{3}$	0	3072
18	$\frac{1}{2}$	0	0	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$-\frac{1}{2}$	1	1	1	-1	$\frac{1}{2}$	0	$-\frac{1}{2}$	0	1536
19	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	1	1	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	1	-1	1536
20	$\frac{2}{5}$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{1}{5}$	0	0	$\frac{3}{5}$	0	0	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{2}{5}$	$-\frac{2}{5}$	$\frac{1}{5}$	$-\frac{1}{5}$	$\frac{2}{5}$	$\frac{2}{5}$	$-\frac{2}{5}$	0	1	1	1	-1	$\frac{4}{5}$	0	1536
21	$\frac{1}{2}$	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	$-\frac{1}{2}$	1	1	$-\frac{1}{2}$	1	$-\frac{1}{2}$	$-\frac{1}{2}$	-1	512
22	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	1	1	$\frac{1}{3}$	1	$\frac{1}{3}$	$\frac{1}{3}$	-1	512
23	$\frac{2}{3}$	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{2}{3}$	0	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	0	0	$\frac{2}{3}$	$\frac{2}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	1	1	1	-1	$\frac{1}{3}$	$-\frac{1}{3}$	1536

	$\langle A_x \rangle$		$\langle B_y \rangle$		$\langle C_z \rangle$		$\langle A_x B_y \rangle$				$\langle A_x C_z \rangle$				$\langle B_y C_z \rangle$				$\langle A_x B_y C_z \rangle$								
No	0	1	0	1	0	1	00	01	10	11	00	01	10	11	00	01	10	11	000	001	010	011	100	101	110	111	n_R
24	$\frac{1}{3}$	$\frac{1}{3}$	0	0	0	0	$\frac{2}{3}$	$\frac{2}{3}$	0	0	$\frac{2}{3}$	0	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	1	1	1	-1	1536
25	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	1	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	-1	-1	$\frac{1}{3}$	-1	$\frac{1}{3}$	-1	1536
26	$\frac{1}{3}$	$\frac{1}{3}$	0	0	0	0	$\frac{2}{3}$	0	0	0	$\frac{2}{3}$	0	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1	1	-1	1536
27	$\frac{1}{2}$	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	1	1	1	-1	1536
28	$\frac{1}{3}$	$\frac{1}{3}$	0	0	0	0	$\frac{2}{3}$	0	0	0	$\frac{2}{3}$	0	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	-1	1	1	1	-1	1536
29	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	1	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	1	$-\frac{1}{3}$	$-\frac{1}{3}$	$-\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	-1	$\frac{1}{3}$	-1	-1	-1	512
30	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	1	1	$\frac{1}{5}$	1	$\frac{1}{5}$	1	$-\frac{3}{5}$	1536
31	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	$\frac{1}{5}$	1	$-\frac{3}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	$-\frac{3}{5}$	1	256
32	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	1	1	1	$\frac{1}{5}$	$-\frac{3}{5}$	$\frac{1}{5}$	1	$-\frac{3}{5}$	3072
33	$\frac{3}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{3}{5}$	$-\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{3}{5}$	$-\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	$-\frac{3}{5}$	$-\frac{1}{5}$	$\frac{3}{5}$	$\frac{3}{5}$	-1	1	1	1	$\frac{1}{5}$	1536
34	$\frac{1}{3}$	0	$\frac{1}{3}$	0	$\frac{1}{3}$	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$-\frac{1}{3}$	1	$\frac{2}{3}$	$\frac{2}{3}$	-1	$-\frac{2}{3}$	1	1	0	512
35	$\frac{1}{3}$	0	$\frac{1}{3}$	0	0	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$-\frac{1}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	1	-1	1	1	$-\frac{2}{3}$	0	3072
36	$\frac{1}{4}$	0	$\frac{1}{4}$	0	0	0	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	1	1	$\frac{3}{4}$	$-\frac{3}{4}$	$\frac{3}{4}$	$-\frac{3}{4}$	0	-1	1536
37	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	0	0	$\frac{1}{2}$	0	0	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{2}$	0	1	1	1	-1	1	$\frac{1}{2}$	3072
38	$\frac{1}{3}$	0	0	0	0	0	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	1	1	1	-1	$\frac{2}{3}$	$\frac{2}{3}$	$-\frac{2}{3}$	0	3072
39	$\frac{1}{3}$	0	0	0	0	0	0	0	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{1}{3}$	1	1	1	-1	$\frac{2}{3}$	$-\frac{2}{3}$	$-\frac{2}{3}$	0	1536
40	$\frac{1}{2}$	0	0	0	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	0	0	0	0	0	0	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	1	-1	-1	1	384
41	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	-1	384
42	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	-1	1	1	768
43	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{7}$	$\frac{1}{7}$	3/7	$-\frac{1}{7}$	$-\frac{1}{7}$	$-\frac{1}{7}$	3/7	$-\frac{1}{7}$	$-\frac{1}{7}$	$-\frac{1}{7}$	$-\frac{1}{7}$	$-\frac{1}{7}$	$-\frac{1}{7}$	$-\frac{1}{7}$	$\frac{1}{7}$	$\frac{5}{7}$	$\frac{5}{7}$	-1	-1	-1	-1	-1	1536
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	-1	128
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	-1	-1	1	48
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	-1	1	-1	-1	-1	16

Bibliography

[1] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell's theorem. *Physical Review Letters*, 47:460–463, Aug 1981.

[2] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu, and David Roberts. Nonlocal correlations as an information-theoretic resource. *Physical Review A*, 71:022101, Feb 2005.

[3] Jonathan Barrett and Stefano Pironio. Popescu-rohrlich correlations as a unit of nonlocality. *Physical Review Letters*, 95:140401, Sep 2005.

[4] John S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1, 1964.

[5] Gilles Brassard. Quantum communication complexity. *Foundations of Physics*, 33:1593–1616, 2003.

[6] Gilles Brassard, Harry Buhrman, Noah Linden, André Allan Méthot, Alain Tapp, and Falk Unger. Limit on nonlocality in any world in which communication complexity is not trivial. *Physical Review Letters*, 96:250401, Jun 2006.

[7] Nicolas Brunner, Valerio Scarani, and Nicolas Gisin. Bell-type inequalities for non-local resources. *Journal of Mathematical Physics*, 47, Mar 2006.

[8] Nicolas Brunner and Paul Skrzypczyk. Nonlocality distillation and postquantum theories with trivial communication complexity. *Physical Review Letters*, 102:160403, Apr 2009.

[9] Boris S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4, Mar 1980.

[10] James A. Clarkson. Uniformly convex spaces. *Transactions of the American Mathematical Society*, 40, 1936.

[11] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, Oct 1969.

[12] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Physical Review A*, 56:1201–1204, Aug 1997.

[13] Richard Cleve, Wim Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In ColinP. Williams, editor, *Quantum Computing and Quantum Communications*, volume 1509 of *Lecture Notes in Computer Science*, pages 61–74. Springer Berlin Heidelberg, 1999.

[14] Richard Cleve, Wim van Dam, Michael Nielsen, and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Proceedings of 1st NASA QCQC Conference, Volume 1509 of Lecture Notes In Computer Science*, pages 61–74. Springer, 1998.

[15] Ronald de Wolf. Quantum communication and complexity. *Theoretical Computer Science*, 287(1):337 – 353, 2002. Natural Computing.

[16] Helen Ebbe and Stefan Wolf. Distillation of multi-party non-locality with and without partial communication. *arXiv preprint quant-ph/1301.5875*, Jan 2013.

[17] Manfred Einsiedler and Thomas Ward. Lecture notes in functional analysis. Jul 2012.

[18] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, May 1935.

[19] Manuel Forster, Severin Winkler, and Stefan Wolf. Distilling nonlocality. *Physical Review Letters*, 102:120401, Mar 2009.

[20] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865–942, Jun 2009.

[21] Peter Høyer and Jibran Rashid. Optimal protocols for nonlocality distillation. *Physical Review A*, 82:042118, Oct 2010.

[22] Esther Hänggi, Renato Renner, and Stefan Wolf. Quantum cryptography based solely on bell's theorem. *EUROCRYPT 2010*, Jan 2010.

[23] Eyal Kushilevitz. Communication complexity. volume 44 of *Advances in Computers*, pages 331 – 360. Elsevier, 1997.

[24] Samuel Marcovitch and Benni Reznik. Implications of communication complexity in multipartite systems. *Physical Review A*, 77:032120, Mar 2008.

[25] Lluis Masanes. Tight Bell inequality for d-outcome measurements correlations. *Quantum Information and Computation*, 3, Oct 2002.

[26] Lluis Masanes, Antonio Acin, and Nicolas Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, Jan 2006.

[27] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[28] Stefano Pironio, Jean-Daniel Bancal, and Valerio Scarani. Extremal correlations of the tripartite no-signaling polytope. *Journal of Physics A: Mathematical and Theoretical*, 44:065303, Jan 2011.

[29] Itamar Pitowski. Quantum probability, quantum logic. *Lecture Notes in Physics*, 321, 1989.

[30] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24, Mar 1994.

[31] Wim Van Dam. Implausible consequences of superstrong nonlocality. *arXiv preprint quant-ph/0501159*, 2005.

[32] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing(preliminary report). In *Proceedings of the eleventh annual ACM symposium on Theory of computing*, STOC '79, pages 209–213, New York, NY, USA, 1979. ACM.