How Non-Local are n Noisy Popescu-Rohrlich Machines?

Matthias Fitzi*, Esther Hänggi*, Valerio Scarani† and Stefan Wolf*

*Computer Science Department, ETH Zürich, Switzerland [1]
†Centre for Quantum Technologies and Department of Physics, National University of Singapore, Singapore [2]

Abstract. We show that the local part of n symmetric ε-PRMs is of order $\Theta(\varepsilon^{\lceil n/2 \rceil})$ and that the local part of n maximally biased (asymmetric) δ-PRMs is exactly $(3\delta)^n$.

Keywords: Local part, non-local box, non-signaling
PACS: 03.65.Ud,03.67.-a,87.19.lo

INTRODUCTION

The behavior of a bipartite input/output system $P_{XY|UV}$ is *non-local* if it cannot be explained by pre-shared information. For example, the measurement choice/outcome behavior of certain *entangled* quantum states is non-local. As an application, non-locality can imply device-independent unconditional secrecy in quantum cryptography [1]: hidden parameters that do not exist cannot be known by the adversary; and the stronger the non-locality the more secret is the respective information. Non-local correlations can also be seen as a resource to fulfill distributed tasks [2].

Non-locality of a binary input/output system is typically characterized by the Popescu-Rohrlich Machine (PRM) [3] that, on inputs X and Y, produces random outputs U and V such that $X \oplus Y = U \cdot V$. Quantum mechanically, PRM behavior can only be simulated with an accuracy of roughly 85% [4] whereas the classical limit is 75% [5].

The question of how much non-locality there is in a given system's behavior — where non-locality is quantified by partitioning the behavior into a local part of maximal weight and the remaining non-local part — has first been asked in [6] (see also [7]). We study here the local part of (a number of) imperfect PRMs, e.g., the local part of a perfect PRM is zero. Our main result is that the local part of n symmetric ε-PRMs is of order $\Theta(\varepsilon^{\lceil n/2 \rceil})$ and that the local part of n maximally biased δ-PRMs is exactly $(3\delta)^n$ (see also [8]).

DEFINITIONS

Note that we restrict ourselves to bipartite systems although generalizations to more parties are possible. These bipartite systems take an input and yield an output from a

[1] Supported by the Swiss National Science Foundation.
[2] Supported by the National Research Foundation and Ministry of Education, Singapore.

well-defined alphabet on each side (i.e., to each party) and can be characterized by a conditional probability distribution $P_{XY|UV}(x,y,u,v)$ where U and V are the inputs, and X and Y are the outputs on the respective sides.

DEFINITION 1 *A bipartite conditional probability distribution $P_{XY|UV}(x,y,u,v)$ is called* non-signaling *if the two parties cannot use it to transmit information, i.e.,*

$$\sum_x P_{XY|UV}(x,y,u,v) = \sum_x P_{XY|UV}(x,y,u',v) \ \forall y,v$$

and similar when the role of the two parties are reversed. It is called local deterministic *if it can be written as*

$$P_{XY|UV} = \delta_{x,f(u)} \cdot \delta_{y,g(v)} \ ,$$

where $f : U \to X$ and $g : V \to Y$ and δ is the Kronecker symbol; and it is local *if it is a convex combination of local deterministic probability distributions.*

We will only consider non-signaling probability distributions in this paper. Note that the space of all non-signaling probability distributions over a certain input/output alphabet is convex. All local probability distributions can be simulated by two distant parties using a pre-agreed strategy and shared randomness — the shared randomness determines which local deterministic probability distribution to use, and respective output is then a deterministic function of the input (on the same side).

DEFINITION 2 *Given a bipartite non-signaling probability distribution $P_{XY|UV}$, the maximum p, $0 \leq p \leq 1$, such that $P_{XY|UV}$ can be written as the convex combination of a local and a non-signaling probability distribution is called its* local part*:*

$$P_{XY|UV} = p \cdot P_{local} + (1-p) \cdot P_{ns} \ .$$

A probability distribution is local if and only if its local part is equal to one. However, in the special case of probability distributions taking binary input and giving binary output, there is a simple inequality which can be used to determine if a probability distribution is local.

PROPOSITION 1 (Bell [5]) *A bipartite probability distribution $P_{XY|UV}$ taking binary input and giving binary output is non-local if, for uniform inputs,*

$$P(X \oplus Y = U \cdot V) > 0.75 \ .$$

Note that, up to relabelling of the inputs and outputs, the above condition is in fact equivalent to non-locality. After [9], we denote the condition $X \oplus Y = U \cdot V$ by *CHSH-condition*.

For more than two inputs and outputs, the following Lemma 1 will be of use.

LEMMA 1 *Consider two non-signaling probability distributions $P_{XY|UV}$ and $P_{ns,1}$. The former one can be written as $P_{XY|UV} = p \cdot P_{ns,1} + (1-p) \cdot P_{ns,2}$ (where $P_{ns,2}$ is a second non-signaling probability distribution) if and only if*

$$p \cdot P_{ns,1}(x,y,u,v) \leq P_{XY|UV}(x,y,u,v) \ \forall x,y,u,v \ .$$

Proof. FORWARD DIRECTION: Since both $P_{XY|UV}$ and $P_{ns,1}$, are normalized and non-signaling, $P_{ns,2}$ is also normalized and non-signaling (both properties are linear). Now, since $P_{ns,2}(x,y,u,v) = (1/(1-p))(P_{XY|UV}(x,y,u,v) - p \cdot P_{ns,1}(x,y,u,v))$, which is larger than zero by assumption, the forward direction follows. REVERSE DIRECTION: Assume that $p \cdot P_{ns,1}(x,y,u,v) > P_{XY|UV}(x,y,u,v)$ for some x,y,u,v. Then $P_{ns,2}(x,y,u,v) < 0$ and thus $P_{ns,2}$ is not a probability distribution. □

We will study in this paper two particular non-signaling probability distributions:

DEFINITION 3 *A* symmetric ε-PRM *(denoted by $P^{1,\varepsilon}_{XY|UV}$ for one ε-PRM) and a* maximally biased δ-PRM *are bipartite conditional probability distribution given by the probability tables below.*

ε-PRM=

		U	0		1	
V	Y \ X		0	1	0	1
0	0		$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$
	1		$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$
1	0		$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$
	1		$\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{1}{2}-\frac{\varepsilon}{2}$	$\frac{\varepsilon}{2}$

δ-PRM=

		U	0		1	
V	Y \ X		0	1	0	1
0	0		$\frac{1}{2}-\frac{\delta}{2}$	0	$\frac{1}{2}-\frac{\delta}{2}$	0
	1		δ	$\frac{1}{2}-\frac{\delta}{2}$	δ	$\frac{1}{2}-\frac{\delta}{2}$
1	0		$\frac{1}{2}-\frac{\delta}{2}$	0	0	$\frac{1}{2}-\frac{\delta}{2}$
	1		δ	$\frac{1}{2}-\frac{\delta}{2}$	$\frac{1}{2}+\frac{\delta}{2}$	0

SYMMETRIC ε-PRMS

We now study the case of symmetric ε-PRMs ($\varepsilon \in [0, 0.25]$), i.e., PRMs that fulfill the CHSH-condition with probability $1-\varepsilon$ for all inputs and unbiased output bits.

By Lemma 1, we can write any non-signaling probability distribution as

$$P_{XY|UV} = p_i \cdot P_{ld,i} + (1 - \sum_i p_i) \cdot P_{ns}$$

where $P_{ld,i}$ are the different local deterministic strategies fixed by the input and output size. Together with the definition of the local part this implies the following two lemmas.

LEMMA 2 *The local part is the optimal value of the linear program:*

$$\textit{max:} \sum_i p_i \quad \textit{s.t.} \quad \sum_i p_i \cdot P_{l-d,i}(x,y,u,v) \leq P_{XY|UV}(x,y,u,v) \quad \textit{and} \quad p_i \geq 0 \ .$$

LEMMA 3 *The local part of $P^{1,\varepsilon}_{XY|UV}$ is 4ε.*

Now, consider the case of two independent symmetric ε-PRMs. We can write these two machines as one single machine taking 2 input bits and giving 2 output bits on each side:

$$\begin{aligned} P^{2,\varepsilon}_{XY|UV}(x,y,u,v) &= P^{2,\varepsilon}_{XY|UV}((x_1x_2),(y_1y_2),(u_1u_2),(v_1v_2)) \\ &= P^{1,\varepsilon}_{XY|UV}(x_1,y_1,u_1,v_1) \cdot P^{1,\varepsilon}_{XY|UV}(x_2,y_2,u_2,v_2) \ . \end{aligned}$$

Obviously it is always possible to write each of the two machines separately as a combination of one local and one non-local machine. This would give a local weight of $(4\varepsilon)^2$. However, the local part might be larger and, indeed, Lemma 2 and 3 show that the local part of two symmetric ε-PRMs is the same as the local part of one single symmetric ε-PRM.

LEMMA 4 $P^{2,\varepsilon}_{XY|UV} = (4\varepsilon)\cdot P^{2,local}_{XY|UV} + (1-4\varepsilon)\cdot P^{2,0}_{XY|UV}$.

This shows that it is neither possible to use two symmetric ε-PRMs in parallel to create a better ε-PRM, nor to create a more secure bit from the outputs of two ε-PRMsby applying a function (where we assume that the inputs are public).

We now consider the case of any number n of independent symmetric ε-PRMs.

LEMMA 5 *For every local deterministic strategy for n PRMs, there always exist inputs u and v such that $x_i \oplus y_i \neq u_i \cdot v_i$ for at least $n/2$ of the indices i.*

Proof. Assume, wlog, that $x(\vec{0}) = \vec{0}$. Consider the case $u = \vec{0}$. For at most k out of the n instances to fail, $y(v)$ must have Hamming weight at most k (independently of v). Now, consider $y(\bar{x}(\vec{1}))$: For all n instances to be correct for Input $u = \vec{1}$, $y(\bar{x}(\vec{1}))$ must be equal to $x(\vec{1})$ exactly at the positions where $x(\vec{1})$ is '1,' i.e., $y(\bar{x}(\vec{1})) = \vec{1}$. Thus, for at most k instances to fail, $y(\bar{x}(\vec{1}))$ must have Hamming weight at least $n-k$. Since $k < n/2$, this contradicts the fact that $y(v)$ must have Hamming weight at most k. □

THEOREM 1 *The local part of n symmetric ε-PRMs is of order $\Theta(\varepsilon^{\lceil \frac{n}{2} \rceil})$.*

Proof. It is easy to see that this order can be reached as a local part of $(4\varepsilon)^{\lceil \frac{n}{2} \rceil}$ can be achieved by combining the ε-PRMs in pairs. On the other hand, Lemma 5 implies that it is of order $O(\varepsilon^{\lceil \frac{n}{2} \rceil})$. □

MAXIMALLY BIASED δ-PRMS

Consider a PRM which fullfills the CHSH-condition in three out of the four input-cases with proability $1-\delta$ and in the fourth case perfectly, and where the output bit X is maximally biased towards zero.

A simple maximization shows that the local part of one maximally biased δ-PRM is 3δ. More generally, it is possible to show

THEOREM 2 *The local part of n maximally biased δ-PRMs is $(3\delta)^n$.*

REFERENCES

1. J. Barrett, L. Hardy, and A. Kent, *Physical Review Letters* **95**, 010503 (2005).
2. W. van Dam (2005), `quant-ph/0501159`.
3. S. Popescu, and D. Rohrlich, *Foundations of Physics* **24**, 379–385 (1994).
4. B. S. Cirel'son, *Letters in Mathematical Physics* **4**, 93–100 (1980).
5. J. S. Bell, *Physics* **1**, 195–200 (1964).
6. A. C. Elitzur, S. Popescu, and D. Rohrlich, *Physics Letters A* **162**, 25–28 (1992).
7. V. Scarani, *Physical Review A* **77**, 042112 (2008).
8. M. Fitzi, E. Hänggi, V. Scarani, and S. Wolf (2008), `quant-ph/0811.1649`.
9. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Physical Review Letters* **23**, 880–884 (1969).