Free randomness amplification using bipartite chain correlations

Andrzej Grudka,[1] Karol Horodecki,[2,3] Michał Horodecki,[2,4] Paweł Horodecki,[2,5] Marcin Pawłowski,[4,6] and Ravishankar Ramanathan[2]

[1]*Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland*
[2]*National Quantum Information Center of Gdańsk, 81-824 Sopot, Poland*
[3]*Institute of Informatics, University of Gdańsk, 80-952 Gdańsk, Poland*
[4]*Institute of Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*
[5]*Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland*
[6]*Department of Mathematics, University of Bristol, Bristol BS8 1TW, U.K.*

(Dated: June 24, 2013)

Motivation

It is known, that violation of Bell inequalities can lead to the so called device independent security [5–7]. To achieve security in device independent way, one needs to have private randomness at hand. It has been shown by Santha and Vasirani [3], that privacy of randomness can not be amplified using classical means only and having access to bits from specific source called further Santha-Vasirani (SV) source. The SV source is parametrized by a positive parameter ϵ. It is called ϵ-free if each of its subsequent bits conditionally on any external variable describing possible knowledge about them (including previous bits from the source) has bias that diverges from unbiased distribution by ϵ. Facing such a classical no-go, the natural question arises, with important philosophical consequences: Can privacy of randomness be amplified by quantum means? In [1] it has been shown, that if one has access to ϵ-free SV source (i.e. ϵ-free randomness) then one can obtain single bit that is $\epsilon' < \epsilon$-free for any $\epsilon' > 0$, providing $\epsilon < \frac{(\sqrt{2}-1)^2}{2}$. It is reached by measuring the so called N-th Chained Bell inequality [8] on a bipartite quantum state, with properly high n. Further, in [2], it is shown (existentially) that there is a procedure to obtain any ϵ'-free bit starting from any $\epsilon < 1/2$, based on measuring Mermin's inequality [9] on a 5-partite quantum state. In [11] we follow these results, showing new perspective on the subject, and then focusing on obtaining randomness from the N-th Chained Bell inequalities.

The results

In presented manuscript, we show the following three results:

1. We give characterization of the distributions of bits drown from SV source, showing that they are mixture of (certain) permutations of Bernoulli distribution with probability of success given by $1/2 + \epsilon$ where SV is assumed to be ϵ-free.

2. We recast the problem of amplification of randomness in the language of the families of probability distributions called here 'boxes', and easily rederive the result of [1] in this terms.

3. We close the problem of randomness extraction using Chain Bell inequalities. The threshold value of ϵ from which free randomness can be amplified, is shown to be 0.901. To this end, we explore the introduced boxes approach as well as the characterization of ϵ-free sources.

Explanation of the results

Here we explain the results that are available in [11]. First result.-

A source of bits is called a Santha-Vazirani (SV) source if for any random variable $X = (X_1, X_2, \ldots, X_n)$ produced by this source and for any $0 \leq i < n$ and $x_i = \{0, 1\}$, there holds

$$\frac{1}{2} - \epsilon \leq P(X_{i+1} = x_{i+1} | X_i = x_i, \ldots, X_1 = x_1) \leq \frac{1}{2} + \epsilon. \tag{1}$$

The model can be interpreted as each bit being obtained by the flip of a biased coin, the bias being fixed by an adversary who has knowledge of the history of the process. As such, the conditioning variables can be any set of pre-existing variables W that could be a possible cause of the succeeding bit X_{i+1}. Each bit produced by the source is ϵ-free in the sense that the probability distribution is ϵ away in variational distance from the uniform distribution.

Regarding characterization of the SV source, we first observe, that a joint probability distribution given in form of $p(x)p(y|x)$ such that $p(x)$ belongs to an allowed set of distributions S_X as well as $p(y|x)$ to some set S_Y is spanned by the probability distributions which are multiplications of extremal points of these two sets S_X and S_Y. Because of this multiplication rule, the resulting extremal distributions are Bernoulli distributions or their permutations, as we exemplify below. The rest of the proof goes by induction with respect to bits from the source. To exemplify this consider $p(x, y)$ to be distribution of two bits. By rule of total probability we can write it as follows:

$$\{p(x,y)\} = \Big(p(0)p(0|0), p(0)p(1|0), p(1)p(0|1), p(1)p(1|1)\Big) \tag{2}$$

Now, for $x = 0$, we have decomposition

$$p(0|0) = \alpha_0 p_+ + (1-\alpha_0)p_-, \quad p(1|0) = \alpha_0 p_- + (1-\alpha_0)p_+. \tag{3}$$

where $p_+ = 1/2 + \epsilon$ and $p_- = 1/2 - \epsilon$ - the two extremal distributions of S_X. For $x = 1$ we have some other decomposition

$$p(0|1) = \alpha_1 p_+ + (1-\alpha_1)p_-, \quad p(1|1) = \alpha_1 p_- + (1-\alpha_1)p_+ \tag{4}$$

since again p_+ and p_- are distributions of S_Y. We can directly check that

$$\begin{aligned}&\big(p(0)p(0|0), p(0)p(1|0), p(1)p(0|1), p(1)p(1|1)\big) = \\ &\alpha_0\alpha_1\big(p(0)p_+, p(0)p_-, p(1)p_+, p(1)p_-\big) + \\ &\alpha_0(1-\alpha_1)\big(p(0)p_+, p(0)p_-, p(1)p_-, p(1)p_+\big) + \\ &(1-\alpha_0)\alpha_1\big(p(0)p_-, p(0)p_+, p(1)p_+, p(1)p_-\big) + \\ &(1-\alpha_0)(1-\alpha_1)\big(p(0)p_-, p(0)p_+, p(1)p_-, p(1)p_+\big)\end{aligned} \tag{5}$$

Now we further decompose the distribution $(p(0), p(1))$ into extremal points of S_X which are in this case the same as those of S_Y: (p_+, p_-) and (p_-, p_+). Therefore $\{p(x, y)\}$ is mixture of the eight probability distributions

$$\begin{aligned}&\big(p_+p_+, p_+p_-, p_-p_+, p_-p_-\big), \quad \big(p_+p_+, p_+p_-, p_-p_-, p_-p_+\big), \\ &\big(p_+p_-, p_+p_+, p_-p_+, p_-p_-\big), \quad \big(p_+p_-, p_+p_+, p_-p_-, p_-p_+\big), \\ &\big(p_-p_+, p_-p_-, p_+p_+, p_+p_-\big), \quad \big(p_-p_+, p_-p_-, p_+p_-, p_+p_+\big), \\ &\big(p_-p_-, p_-p_+, p_+p_+, p_+p_-\big), \quad \big(p_-p_-, p_-p_+, p_+p_-, p_+p_+\big),\end{aligned} \tag{6}$$

where the ordering is as follows:

$$\big(p(0,0), p(0,1), p(1,0), p(1,1)\big). \tag{7}$$

Note that the first distribution is precisely the Bernoulli distribution, with probability of 0 in single trial being $p = p_+$. This distribution is memoryless. The other distributions are not memoryless, but are related to the Bernoulli distribution by permutation of probabilities (not bits). Note that only 8 out of 24 permutations appear. Not all permutations appear, because the bits from SV source have 'history', i.e. they are ordered in condition of SV source, which implies order in constructing the joint probability distribution of n such bits, yielding a tree structure, and in turn specific permutations.

The second result.-

Regarding second result, we re-derive result of [1] in the way, that can be generally applied. We choose a Bell inequality, which to be measured, with certain cardinality of measurements to be done, and certain cardinality of outputs for each measurement. One of the output of its measurement is taken as a bit with higher randomness. Measuring such a Bell inequality on quantum state yields then a box B, of certain dimensions. This box, being quantum, has some value of violation of the Bell inequality B_Q. Eve tries to cheat Alice and Bob, by using the most local box she can, so that still when they measure the box with number of measurement taken from SV source, they would observe quantum value B_Q. We then consider different mixtures of the *extremal* boxes i.e. that are vertices of the whole polytope of non-signaling boxes of dimension same as B, and check how much randomness gives each of them. To be more specific now, consider as Bell inequality the N-th Chain inequality [8].

The chained Bell inequality considers the bipartite scenario of two spatially separated parties Alice and Bob who each choose from a set of N measurement settings: $x \in \{0, \ldots, N-1\}_A$ for Alice and $y \in \{0, \ldots, N-1\}_B$ for Bob. Each measurement results in a binary outcome $a \in \{0, 1\}$ for Alice and $b \in \{0, 1\}$ for Bob. The chained Bell inequality is then written as

$$\sum_{x=y||x=y+1} P(a \oplus b = 1|x, y) + P(a \oplus b = 0|0, N-1) \geq 1, \tag{8}$$

where $\oplus$ denotes addition modulo 2. Notice that out of the N^2 possible measurement pairs, only the $2N$ neighboring pairs where $x = y$ or $x = y + 1$ (sum modulo N) forming a chain are considered in the inequality and the LHV bound is obtained from the fact that perfect correlations in the outcomes for the $2N - 1$ pairs in the sum automatically implies perfect correlation for the pair $\{0, N-1\}$. Quantum mechanics violates this inequality obtaining a value of $2N \sin^2(\frac{\pi}{4N})$ which for large N tends to the algebraic limit of 0. This optimal quantum value is obtained by measuring on the maximally entangled state $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with the measurement settings defined by the bases $\{|0_k\rangle, |1_k\rangle\}$ (for $k = x, y$). Here $|0_k\rangle = \cos\frac{\phi_k}{2}|0\rangle + \sin\frac{\phi_k}{2}|1\rangle$, $|1_k\rangle = \sin\frac{\phi_k}{2}|0\rangle - \cos\frac{\phi_k}{2}|1\rangle$ with the angles $\phi_k = \frac{\pi k}{2N}$.

It is straightforward to see, that taking into account that Alice and Bob uses SV source to measure the above Bell inequality (i.e. their choices are not fully random), it changes into the following form:

$$\begin{aligned}&\sum_{x=y||x=y+1} P(x, y|w)P(a \oplus b = 1|x, y) + \\ &P(0, N-1|w)P(a \oplus b = 0|0, N-1) \geq p_{\min}\end{aligned} \tag{9}$$

where w is within the set of space-time variables with which the imperfectly free SV source may be correlated (and which may be thought of as held by the adversary Eve). The bound $p_{\min} = \min_{x,y} P(x, y|w)$ is the minimum probability of a pair of measurement settings chosen by Alice and Bob, ideally $p_{\min}^{ideal} = \frac{1}{2N}$ (for $\epsilon = 0$).

Fortunately, by [10], for the polytope defined by Chained Bell inequality, all boxes that gives full randomness violate maximally (giving 0), and all other extremal boxes do not violate it giving at least value p_{min}. Let us denote the box, which Eve sends to Alice and Bob by B',

and consider its decomposition into extremal boxes B_i:

$$B' = \sum_i p_i B_i = \sum_{i\in I} p_i B_i^r + \sum_{j\in J} p_j B_j^{nr} \qquad (10)$$

where B_i^r are extremal boxes with full randomness among all extremal boxes B_i and B_j^{nr} are those without randomness ($I \cup J$ gives all indices in the sum on the LHS). Let us denote $\sum_{j\in J} p_j = \delta$. Taking the value of the N-th Chain inequality on both sides, recalling that Eve should report value that Alice and Bob observe i.e. β_Q, hence denoting $\beta(X)$ the value of the Chain inequality on box X, we get

$$\beta_Q = (1-\delta)\sum_{i\in I} \frac{p_i}{(1-\delta)}\beta(B_i^r) + \delta \sum_{j\in J} \frac{p_j}{\delta}\beta(B_j^r) \qquad (11)$$

But $\beta(B_i^r) = 0$ for boxes with randomness, and $\beta(B_j^{nr})$ equals at least p_{min}. Thus the best attack for Eve is to satisfy:

$$\beta_Q \geq \delta p_{min} \qquad (12)$$

Now if $\frac{\beta_Q}{p_{min}}$ goes to 0, we have that δ vanishes, yielding asymptotically perfect security, since the the only fraction of non-random boxes in (10) disappears.

By definition, p_{min} is the minimal probability of the distribution $P(\mathbf{x},\mathbf{y})$ with which Alice and Bob will measure the Chain inequality. They need to choose out of N^2 measurements, that is they will have have to specify $\mathbf{x}$ and $\mathbf{y}$ from range 1,...,N each, but accept it only in $2N$ cases. Each number has probability of occurring at least $p_-^{2\log N}$ where $p_- = 1/2 - \epsilon$, since to describe both the numbers of measurement $\mathbf{x}$ and $\mathbf{y}$, they spend $2\log N$ bits from SV source. Thus

$$p_{\min} = \frac{p_-^{2\log N}}{p_-^{2\log N} + ||P(\mathbf{x},\mathbf{y})||_{2N-1}}, \qquad (13)$$

where $||P(\mathbf{x},\mathbf{y})||_{2N-1}$ is the $(2N-1)^{th}$ Ky Fan norm of the probability distribution $P(\mathbf{x},\mathbf{y})$ generated by the source, i.e., the sum of the $2N-1$ largest probabilities. The denominator of the above expression can be bounded from above by $2Np_+^{2\log N}$ where $p_+ = (\frac{1}{2}+\epsilon)$, since $p_+^{2\log N}$ is the largest probability of occurrence of a bit string of length $2\log N$ generated by the source. We therefore have:

$$\delta p_{\min} \geq \delta \frac{p_-^{2\log N}}{2^{\log N+1} p_+^{2\log N}}. \qquad (14)$$

Setting this inequality in RHS of (12), we obtain that the fraction of non-random boxes δ approaches 0 (and perfect randomness is obtained) as we increase the number of measurement settings N provided

$$\lim_{\log N\to\infty} \frac{\pi^2}{8}\frac{p_+^{2\log N}}{N p_-^{2\log N}} = 0, \qquad (15)$$

giving $\frac{(\frac{1}{2}+\epsilon)^2}{2(\frac{1}{2}-\epsilon)^2} < 1$, thus recovering $\epsilon < \frac{(\sqrt{2}-1)^2}{2} \approx 0.086$, which is the result of [1].

The third result.-

Finally we use the characterization of the SV source to compute exact threshold value of ϵ which allows for (asymptotically) perfect security amplification. We do this as follows. We want to find for which ϵ, the expression $\frac{\beta_Q}{p_{min}}$, vanishes with large N, yielding vanishing δ according to (12), which implies asymptotically fully private randomness. Thus we need to lower bound p_{min} and in turn, to upper bound the Ky Fan norm that we have in its denominator. This is achieved by the fact, that norm is convex, hence

$$||P(\mathbf{x},\mathbf{y})||_{\mathbf{2N-1}} \leq \sum_{\mathbf{i}} \mathbf{q_i} ||\mathbf{P_i}(\mathbf{x},\mathbf{y})||_{\mathbf{2N-1}} \qquad (16)$$

where P_i are extremal distributions in the set of distributions satisfying SV source. Hence, by characterization, each P_i is permutation of Bernoulli distribution, and thus have the same Ky Fan norm as the Bernoulli (BE) distribution itself:

$$||P(\mathbf{x},\mathbf{y})||_{\mathbf{2N-1}} \leq ||\mathbf{BE}(\mathbf{x},\mathbf{y})||_{\mathbf{2N-1}} \qquad (17)$$

After some algebra, we find asymptotically exact bound on RHS of the above inequality, which proves that ϵ from which Alice and Bob can start to get asymptotically secure random bit is 0.0961. Interestingly, again by elementary algebra we find, that this value is the highest ϵ for which full randomness amplification based on Chained Bell inequality holds, hence it is a threshold value for this way of obtaining full randomness.

[1] R. Colbeck and R. Renner, Nature Physics **8**, 450 (2012).
[2] R. Gallego, L. Masanes, G. de la Torre, C. Dhara, L. Aolita and A. Acin, arXiv:1210.6514 (2012).
[3] M. Santha and U. V. Vazirani, Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS-84), 434 (1984).
[4] R. Colbeck, PhD dissertation, University of Cambridge (2007).
[5] A. Acin, S. Massar and S. Pironio, Phys. Rev. Lett. **108**, 100402 (2012).
[6] J. Barrett, L. Hardy and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[7] E. Hänggi, R. Renner and S. Wolf, EUROCRYPT 2010, 216 (2010).
[8] S. L. Braunstein and C. M. Caves, Annals of Physics **202**, 22 (1990).
[9] N. D. Mermin, Phys. Rev. Lett. **65**, 3373 (1990).
[10] N. S. Jones and L. Masanes, Phys. Rev. A **72**, 052312 (2005).
[11] A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, M. Pawłowski and Ravishankar Ramanathan arXiv:1303.5591