RANDOMNESS AMPLIFICATION WITHOUT MARKOV CONDITION

F. BRANDAO, A. GRUDKA, M. HORODECKI, K. HORODECKI, P. HORODECKI, M. PAWŁOWSKI, R. RAVISHANKAR, AND H. WOJEWÓDKA

ABSTRACT. We consider randomness amplification of ε-SV sources, using no-signalling correlations. Unlike in previous papers (see Colbeck et al., 1105.3195v3 (2013), Gallego et al., 1210.6514v1 (2012) or Brandao et al., 1310.4544v1 (2013)), we do not assume Markov condition and show that, nonetheless, randomness can be amplified. By Markov condition we mean that ε-SV sources and boxes may only be correlated with each other through the no-signaling eavesdropper Eve.

In many applications, like numerical simulations, cryptography or gambling, just to name a few, free randomness is desired due to the fact that a wide range of results is based on it. In practice, however, random sources are rarely private. That is why the problem of randomness amplification became useful and worth investigating. Overall, the idea is to use inputs from a partially random source and obtain perfectly random output bits.

In our research we consider an ε-SV source (named for Santha and Vazirani [9]), where ε is a parameter which indicates how far we are from full randomness. In the most general case, an ε-SV source is given by a probability distribution $p(\varphi_0, \ldots, \varphi_n)$ over bit strings such that, for every $1 \leq i \leq n$,

$$(\frac{1}{2} - \varepsilon) \leq P(\varphi_i | \varphi_0, \ldots, \varphi_{i-1}) \leq (\frac{1}{2} + \varepsilon).$$

Note that, when $\varepsilon = 0$, bits are fully random, while they are fully deterministic, when $\varepsilon = \frac{1}{2}$.

In our study we use a family of probability distributions, usually called a box, denoted by $P(x, y|u, v)$, where u, v and x, y are pairs of inputs and outputs, respectively.

To talk about randomness amplification, it is advisable to explain what is meant by no-signaling (NS) condition and correctness of quantum theory (QT). Suppose that Alice and Bob prepare input bits u and v, respectively. Their measurement outcomes are x and y. In the most general form, NS assumption means that $\sum_y P(x, y|u, v) = \sum_y P(x, y|u, v')$ and $\sum_x P(x, y|u, v) = \sum_x P(x, y|u', v)$, for every x, y, u, u', v, v'. By correctness of QT we understand that the joint probability distribution $P(x, y|u, v)$ can be obtained by performing measurements on some quantum state.

In classical information theory, randomness amplification is unattainable (see [9] for proof). However, quite recently exciting results appeared, which show that it becomes possible, if quantum correlations are used and NS principle is assumed.

In the research of randomness amplification, the paper of Colbeck and Renner [2] is certainly crucial. It is also a starting point for our idea. The authors consider the bipatrite scenario of the chained Bell inequality and prove that, if NS assumption and correctness of QT are satisfied, it is possible to amplify randomness of ε-SV sources, provided $\varepsilon < (\sqrt{2} - 1)^2/2 \approx 0.086$. The result may be improved, as it is done in [5]. Namely, based on the observation that extremal points of the set of probability distributions from an ε-SV source are certain permutations of Bernoulli distributions with parameter $(\frac{1}{2} - \varepsilon)$, randomness amplification is obtained for any $\varepsilon < 0.0961$. Moreover, the bound is tight, which means that above this threshold it is not possible to achieve randomness amplification using the chained Bell inequality.

In [3], authors show that, given an ε-SV source, with any $0 < \varepsilon < \frac{1}{2}$, and assuming NS, full randomness may be certified using quantum non-local correlations. However, it should be noted that, in [3], only one scenario of five-party Mermin inequality is considered. Moreover, unlike in protocol proposed in [2], the hashing function used to compute the final random bit is not explicitly provided and a large number of space-like separated devices is required.

So far, all papers have been based on the assumption that ε-SV sources and boxes may only be correlated with each other through the no-signaling eavesdropper Eve. To be precise, it is assumed that an ε-SV source, Eve's random variables (Z, W) and the box P constitute a Markov chain, which means that, given $(Z = z, W = w)$, the box $P(x, y|u, v, Z = z, W = w)$ is independent of the bits produced by the source. We call it the Markov condition.

In our work we focus on re-establishing the results given in [2] and [5], but in the case when the Markov condition is abandoned. Suprisingly, it turns out that allowing for correlation between an ε-SV source and a device does not change a lot and still randomness amplification may be obtained for ε, precisely $\varepsilon < 0.029$. Generally, the threshold is weaker than the optimal one obtained in [5] but it is still positive, which indicates that assuming the Markov condition is not the key reason for possibiliy of randomness amplification. However, if we additionally assume that the protocol does not abort if and only if the players see the source as fully random, we are able to obtain a fully private random bit for $\varepsilon < 0.0961$. This coincides with the optimal threshold value of ε which enables randomness amplification via the chained Bell inequality.

Further, we show that the results may be generalised to other scenarios. Instead of the chained Bell inequality, we can use any Bell inequality for which the quantum Bell value is close to its algebraic violation. Good examples of such Bell inequalities are Bell inequalities for quantum non-local games such as pseudo-telepathy games (see [4]) or Bell inequalities for Graph States (see [6]).

References

[1] Brandão, F. G. S. L., Ramanathan, R., Grudka, A., Horodecki, K., Horodecki, M. & Horodecki, P. (2013). *Robust Device-Independent Randomness Amplification with Few Devices*, arXiv:1310.4544v1 [quant-ph]

[2] Colbeck, R., Renner, R. (2013). *Free randomness can be amplified*, arXiv:1105.3195v3 [quant-ph]

[3] Gallego, R., Masanes, L., De La Torre, G., Dhara, C., Aolita, L. & Acin, A. (2012). *Full randomness from arbitrarily deterministic events*, arXiv:1210.6514v1 [quant-ph]

[4] Gisin, N., Méthot, A. A. & Scarani, V. (2006). *Pseudo-telepathy: input cardinality and Bell-type inequalities*, arXiv:quant-ph/0610175v1

[5] Grudka, A., Horodecki, K., Horodecki, M., Horodecki, P., Pawłowski, M. & Ramanathan, R. (2013). *Free randomness amplification using bipartite chain correlations*, arXiv:1303.5591

[6] Gühne, O., Tóth, G., Hyllus, P. & Briegel, H. J. (2005). *Bell Inequalities for Graph States*, arXiv:quant-ph/0410059v2

[7] Jones, N. S., Masanes, L. (2005). *Interconversion of Nonlocal Correlations*, arXiv:quant-ph/0506182

[8] Popescu, S., Rohrlich, D. (1994). *Nonlocality as an axiom*, Found. Phys. 24, 379

[9] Santha, M., Vazirani, U. V. (1984). *Generating Quasi-Random Sequences from Slightly-Random Sources*, Proceedings of the 25th IEEE Symposium on Foundations of Computer Science (FOCS'84), 434

FB: Department of Computer Science, University College London
E-mail address: `f.brandao@ucl.ac.uk`

AG: Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `ndrzej.grudka@amu.edu.pl`

MH: Institute of Theoretical Physics and Astrophysics, Gdańsk University, Wita Stwosza 57, 80-952 Gdańsk, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `fizmh@ug.edu.pl`

KH: Institute of Informatics, University of Gdask, 80-952 Gdańsk, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `khorodec@inf.ug.edu.pl`

PH: Faculty of Applied Physics and Mathematics, Technical University of Gdańsk, 80-233 Gdańsk, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `pawel@mif.pg.gda.pl`

MP: Institute of Theoretical Physics and Astrophysics, Gdańsk University, Wita Stwosza 57, 80-952 Gdańsk, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `dokmpa@.univ.gda.pl`

RR: Institute of Theoretical Physics and Astrophysics, Gdańsk University, Wita Stwosza 57, 80-952 Gdańsk, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `ravishankar.r.10@gmail.com`

HW: Institute of Theoretical Physics and Astrophysics, Gdańsk University, Wita Stwosza 57, 80-952 Gdańsk, Poland; National Quantum Information Centre of Gdańsk, Andersa 27, Sopot, 81-824, Poland
E-mail address: `hwojewod@ug.edu.pl`