Randomness Certification & Generation using Quantum Non-Locality

Preliminary Project Report for CS682A

Advisor: Prof. Rajat Mittal*

Kunal Kapila
Dept. of Mathematics & Statistics
Indian Institute of Technology, Kanpur
kunalkap@iitk.ac.in

Talla Aravind Reddy
Dept. of Computer Science & Engineering
Indian Institute of Technology, Kanpur
arareddy@iitk.ac.in

ABSTRACT

Quantum Non-locality has drastically changed our understanding of nature. In this project, we aim to understand Quantum Non-locality and we will look at two very closely related and intriguing applications of Quantum Non-locality: Certification and Generation of Randomness. This is a major field of research in Quantum Cryptography.

Introduction

Randomness is at the heart of Quantum Mechanics which is in turn at the heart of physical reality. Therefore, understanding the nature of randomness is a very fundamental question from both physical and philosophical views. Randomness is also immensely indispensable in computation. It is used in several distinct areas of computation like Fast Information Acquisition, Cryptography, Primality Testing, Distributed Computation etc. In cryptographic applications, it is of paramount importance for the user to make sure that no other person (including the manufacturer of the randomness generating device) knows the random numbers generated. Thus, one can easily see that randomness certification is an urgent practical problem. To tackle this problem, Bell inequalities[1] were used in a very novel way in [3]. Building upon [3], Vazirani and Vidick built a quantum safe protocol for generation of random numbers in [5].

Certification of Randomness

It is a highly non-trivial task to characterize random numbers mathematically. Generation of random numbers relies on unpredictable physical processes. Inaccuracies in the theoretical modelling of such processes limit the reliability of random number generators. We will be reading the Nature article titled "Random numbers certified by Bell's Theorem"[3] which, inspired by earlier work on non-locality and device independent quantum information processing, shows that the non-local correlations of entangled quantum particles can be used to certify the presence of randomness in a given string of numbers.

Quantum-Secure Randomness Generation

For this part of the project, we will be primarily reading from the STOC 2012 article titled "Certifiable Quantum Dice" by Vazirani and Vidick[5]. In this paper, a protocol is introduced through which a pair of Quantum Mechanical Devices may be used to generate n bits that are close in statistical distance from n uniformly distributed bits, starting from a random seed of uniform bits. Crucially, this protocol is valid even from the point of view of a quantum adversary who may have had prior access to the devices, and may be having other devices which are entangled with them. We will also learn a lot about Classical random number generation protocols and Randomness extractors[4] as this is a crucial part in understanding the above protocol and it's security proof.

Aim of the Project

We intend to first understand Quantum Non-locality, which includes Bell inequalities [1] and non-local game strategies [2]. Then, we intend to understand how certification of randomness is possible by using Quantum Non-locality from [3]. We will conclude by understand the protocol of [5] and it's Complexity Proof.

References

[1] J. Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3):195–200, 1964.

[2] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. *Proceedings of the Annual IEEE Conference on Computational Complexity*, 19:236–249, 2004.

[3] S. Pironio, A. Acin, S. Massar, A. B. De La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 04 2010.

[4] L. Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, 48(4):860–879, 2001.

[5] U. Vazirani and T. Vidick. Certifiable quantum dice. In *Proceedings of the Forty-fourth Annual ACM Symposium on Theory of Computing*, STOC '12, pages 61–76, New York, NY, USA, 2012. ACM.

---

*

Department of Computer Science & Engineering,
Indian Institute of Technology, Kanpur
rmittal@cse.iitk.ac.in