Certified Randomness Generation using Quantum Non-Locality

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

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

Advisor: Prof. Rajat Mittal
rmittal@cse.iitk.ac.in
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

April 2016

Abstract

This is the final report for the course project which we did at IIT Kanpur for the course CS682A: Quantum Computing. In this report, we explain briefly about Quantum Non-locality and some non-local game strategies and then go on to give a brief idea about an extremely intriguing application of Quantum Non-locality: Certified Randomness Generation. This is a major field of research in Quantum Cryptography and we primarily looked at the 2010 Nature article titled 'Random numbers certified by Bell's theorem' [4] by Pironio et.al.

Contents

1 Introduction **3**

1.1 Generation of Certifiable Randomness . . . 3

2 What we learned from the Project **3**

3 Local Realism and the EPR Paradox **4**

3.1 Locality . . . 4

3.2 Realism . . . 4

3.3 EPR Paradox . . . 4

4 Non local games **4**

4.1 Strategies and Values of Non local games . . . 5

4.1.1 Classical Strategies . . . 5

4.1.2 Quantum Strategies . . . 5

4.2 The CHSH game . . . 5

5 Overview of 'Random Numbers Certified by Bell's Theorem' **7**

5.1 Preliminaries . . . 7

5.1.1 Martingales . . . 7

5.1.2 Azuma Hoeffding inequality . . . 7

5.2 Description . . . 7

6 Directions for Future Research **8**

7 Acknowledgments **9**

1 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, 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 generation of certifiable randomness is an urgent practical problem. To tackle this problem, Bell inequalities [1] were used in a very novel way in [4]. Building upon [4], Vazirani and Vidick built a protocol for exponential randomness expansion in [6].

1.1 Generation of Certifiable 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. The Nature article titled "Random numbers certified by Bell's Theorem" [4] 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 generate certified private randomness.

2 What we learned from the Project

We first understood some instances of Quantum Non-locality, which included the Bell-CHSH inequality and some quantum non-local game strategies [3] which included the CHSH game which was a prerequisite to understand the Nature article 'Random Numbers certified by Bell's Theorem' [4]. Then we tried to understand the paper [4]. There were a lot of things which we didn't know but needed to understand the paper. We learnt about entropy in the information theory context, specifically Shannon entropy and the min-entropy. In the process of trying to understand the proof of the result stated in the paper, we read about Martingales, the Azuma-Hoeffding inequality, SDP and bits of 'random' stuff here and there. We enjoyed working thorough the project but we are not completely satisfied with the level of clarity we have over the paper [4] and intend to read it again in detail and fill in the gaps.

3 Local Realism and the EPR Paradox

Locality and Realism are two very fundamental concepts which are assumed to be true in everyday life but which cannot both be simultaneously true according to the laws of Quantum Mechanics.

3.1 Locality

This principle means that an event happening at one point in space cannot affect events which are happening at some other point in space instantaneously. This is a consequence of Einstein's No-signalling theorem which says that information or matter cannot travel from one point in space to another point faster than the speed of light.

3.2 Realism

Realism states that the results of any measurement exist independently of the measurement. For example, the momentum of an object exists even if we do not explicitly measure it.

3.3 EPR Paradox

The examples in this section were taken from [5]. Now, we describe the celebrated EPR paradox, which lead to the discovery of entanglement. Consider a bell state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. According to Quantum Mechanics, if we measure the first qubit in the $|0\rangle, |1\rangle$ basis, then we know the state of the second qubit in the $|0\rangle, |1\rangle$ basis. By the rotational invariance of the Bell state, we also know that measuring the first qubit in the $|+\rangle, |-\rangle$ basis gives us the exact state of the second qubit in the $|+\rangle, |-\rangle$ basis. What this means is that knowledge of the first qubit in any basis completely determines the state of the second qubit in the same basis.

Now suppose that the two qubits are very far away from each other, let us say they are 1 light year away from each other. According to the above arguments, if we measure the first qubit in the bit basis and get $|0\rangle$ and one second later, another experimenter measures the second qubit in the bit basis, then we are sure that the second qubit is in the state $|0\rangle$ as well. This means that the second qubit must have been in the $|0\rangle$ state for a definite one second.

A very crucial point to note here is that the above arguments work exactly the same not only for the $|0\rangle, |1\rangle$ basis but also for the $|+\rangle, |-\rangle$ basis. That is, the second qubit must have been in the $|+\rangle$ state for a full one second before it was measured. Assuming that locality is true, Einstein, Podolsky and Rosen concluded that since qubit 2 cannot have any information about the basis in which qubit 1 was measured, it's state in both the bit and the sign basis is simultaneously determined. But, Quantum Mechanics does not allow this. Therefore, EPR suggested that quantum mechanics is an incomplete theory and they tried to formulate local hidden variable theories which assumed the correctness of local realism.

4 Non local games

Non local games as have been described in [3] are cooperative games of incomplete information. Let Alice and Bob denote the two cooperative parties, out of the three parties involved. The third is a referee or a verifier. Let S and T be two non empty finite sets, with a probability distribution π over S x T. The referee selects a pair of questions $(s,\, t)$ randomly according to π and sends s to Alice and t to Bob. Alice then replies with the answer a, $a \in A$ and Bob with b, $b \in B$, where A and B are also finite non empty sets. Additionally, there is a predicate V defined on S x T x A x B. π and V define the game completely.

Alice, Bob and the referee know A, B, S, T, π and V before the game starts. Alice and Bob are not allowed to communicate once the game commences, but they may agree to some strategy before it. Since a and b are decided on the basis of s and t, $V(s,\, t,\, a,\, b)$ can be denoted as $V(a,\, b \mid s,\, t)$. They win the game if $V(a,\, b \mid s,\, t) = 1$, else they lose.

4.1 Strategies and Values of Non local games

Alice and Bob can form strategies for a game to maximize their probability of winning. The maximum probability so obtained is the value of that non local game. We describe the two classes of strategies used for non local games:

4.1.1 Classical Strategies

The classical value of a game is the maximum probability one can achieve considering all classical strategies. Deterministic strategies are ones where we can express a as a function of s and b as a function of t. Probabilistic strategies can be expressed using a convex combination of classical strategies, thus to calculate the classical value of a game, we only need to consider deterministic strategies. Mathematically,

$$\omega_c\ (G(\pi,\, V)) = \max_{a,b} \sum_{s,t} \pi(s,\, t)\ V(a(s),\, b(t) \mid s,\, t)$$

4.1.2 Quantum Strategies

Quantum strategies consist of an initial entangled state $|\psi\rangle$ which is shared by Alice and Bob. Alice performs the measurement on her part of $|\psi\rangle$ given $s \in S$ to obtain $a \in A$, while while Bob on his part to get $b \in B$ given $t \in T$.

Consider two set of positive semi-definite n x n matrices, $\{X_s^a\colon \sum_a X_s^a = I\}$ and $\{Y_t^b\colon \sum_b Y_t^b = I\}$ where the former describes the measurement performed by Alice on her part of $|\psi\rangle$, while the latter is the corresponding set for Bob given questions s & t respectively. The probability of getting the specified answers with inputs $s \in S$ and $t \in T$ is $\langle\psi|\, X_s^a \otimes Y_t^b\, |\psi\rangle$.

Thus the quantum value of any game G can be given by

$\omega_q\ (G(\pi,\, V)) = \max \sum_{s,t} \pi(s,\, t) \sum_{a,b} \langle\psi|\, X_s^a \otimes Y_t^b\, |\psi\rangle\ V(a,\, b \mid s,\, t)$ *over all quantum strategies*

Note: The value n is not theoretically bounded, hence one cannot be certain if the quantum value is always achieved by some strategy or not.

4.2 The CHSH game

Quantum entanglement causes non classical correlations, and this fact is used in important areas like Quantum teleportation, Super Dense Coding, etc. We will now demonstrate how the same phenomenon can be used to develop quantum strategies which outperform the classical ones.

The CHSH game is related to the CHSH inequality which we will describe later. In terms of the notions of non local games described above, here $S = T = A = B = \{0,\, 1\}$ and π is the uniform distribution over S x T. Also, V = ($a \oplus b == s \wedge t$).

The classical value of this game is 0.75. To prove this, we observe that Alice only knows s, while Bob only knows b, so a will be a function of s and will not depend on t, and vice-versa for b. The best possible deterministic classical strategy that can be used by Alice and Bob is that they output the same bit, either 0 or 1 irrespective of the inputs, since $s.t$ will evaluate to 0 for $\frac{3}{4}$ of the cases, and having equal values of a and b for these will make their XOR value to 0, this giving them a success rate of 0.75 in deterministic case. As has been stated above, we only need to consider deterministic cases.

This figure and the text with the figure is taken from [6]

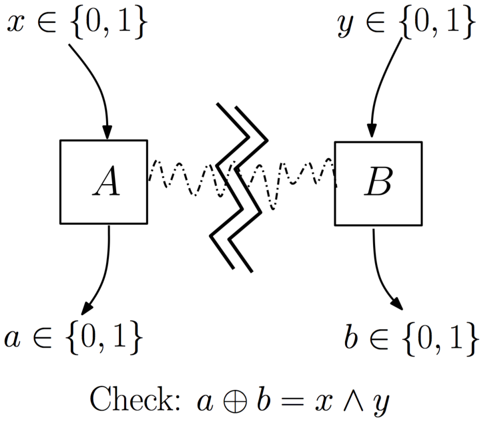

Figure 1: The CHSH game. Any pair of boxes A, B is characterized by a distribution $p(a, b|x, y)$ which is required to be *no-signaling*: the marginal distribution of b is independent of x, and that of a is independent of y.

In the quantum case, Alice and Bob share the qubit $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. We will use the property of $|\psi\rangle$ that it is rotationally invariant, i.e. for any given vector $|u\rangle$, and the corresponding vector $|u^\perp\rangle$, we can write $|\psi\rangle = \frac{|uu\rangle + |u^\perp u^\perp\rangle}{\sqrt{2}}$. Alice and Bob will select the measurement basis in which they measure the entangled state according to the given input s and t. If $s = 0$, Alice will take $|u\rangle = cos(0)\,|0\rangle + sin(0)\,|1\rangle$, else $|u\rangle = cos(\frac{\pi}{4})\,|0\rangle + sin(\frac{\pi}{4})\,|1\rangle$. After she measures the qubit in the specified basis, the corresponding part of the qubit for Bob gets fixed. Now if $t = 0$, Bob measures in the $|v\rangle = cos(\frac{\pi}{8})\,|0\rangle + sin(\frac{\pi}{8})\,|1\rangle$ basis, but if $t = 1$, Bob will measure his part of the qubit in $cos(\frac{-\pi}{8})\,|0\rangle + sin(\frac{-\pi}{8})\,|1\rangle$ basis.

With probability $cos^2(\frac{\pi}{8}) = 0.85$, Alice and Bob will win the game. To see why these choice of basis results in such a quantum value of the game, we will use the result that if Alice measures some qubit in $|u\rangle$, $|u^\perp\rangle$ basis, then when Bob measures the same qubit in $|v\rangle$, $|v^\perp\rangle$ basis, with the relation, $|v\rangle = cos(\theta)\,|u\rangle + sin(\theta)\,|u^\perp\rangle$, then Bob will measure $|u\rangle$ with probability $cos^2(\theta)$, and will measure $|u^\perp\rangle$ with probability $sin^2(\theta)$.

If the three cases when $s.t = 0$, we have an angle of $\frac{\pi}{8}$ between the basis vectors of Alice and Bob, and thus, we will get the same bit as output with a probability of $cos^2(\frac{\pi}{8})$. In the 4th case, we have the angle between the two basis states to be $\frac{3\pi}{8}$, this they will get the same output with probability $cos^2(\frac{3\pi}{8}) = sin^2(\frac{\pi}{8})$, and will get different outputs with a probability of $cos^2(\frac{\pi}{8})$, this giving an XOR value of 1, same as the product of s and t. Thus, in all cases, we get a winning probability of $cos^2(\frac{\pi}{8})$.

5 Overview of 'Random Numbers Certified by Bell's Theorem'

5.1 Preliminaries

To understand the proofs of the bounds obtained in the paper, it is essential to understand the concept of Martingales and Azuma Hoeffding inequality which was applied on martingales satisfying certain properties.

5.1.1 Martingales

A Martingale is a sequence of random variables such that the conditional expected value of on observation at some time k, given all observations up to some earlier time j, is equal to the value of the observation at time j.
Mathematically, $E(Z_k \mid W_1, W_2, ..., W_j) = Z_j$.
We say that $\{Z_k, k \geq 1\}$ is a martingale with respect to $\{W_j\}$.

5.1.2 Azuma Hoeffding inequality

For martingales that have bounded differences, $\mid Z_k - Z_{k-1} \mid < c_k$, for all k, then for some t

$$P(Z_N - Z_0 \geq t) \leq exp(\frac{-t^2}{2\sum_{k=1}^{N} c_k^2})$$

There are other versions of the inequality, which won't be used in the understanding of this paper.

5.2 Description

The goal of the paper is to show that non-local correlations of quantum states can be used to generate certified private randomness. To do this, they show that:
The observed outputs violate a Bell inequality $\implies$ They are not predetermined and that they arise from entangled quantum systems that possess intrinsic randomness.The Bell inequality violation is quantified using the CHSH correlation function[2]

$$I = \sum_{x,y}(-1)^{xy}[P(a = b|xy) - P(a \neq b|xy)]$$

This can be shown to be

$$I = 2\sum_{x,y} P(a \oplus b = x \wedge y) - 4$$

Further,

$$I = 8\omega - 4$$

where ω is the winning probability of the CHSH game defined earlier.
So, in the case of local hidden variable theories, we have I ≤ 2.

The experiment is repeated n times to get an estimate of the Bell violation. For each trial, the measurement choices (x, y) are generated using an identical and independent probability distribution $P(xy)$. We use $r = (a_1, b_1; \ldots; a_n, b_n)$ to denote the final output string and $s = (x_1, y_1; \ldots; x_n, y_n)$ to denote the input string for n runs of the experiment.We use the estimator

$$\hat{I} = \frac{1}{n}\sum_{x,y} \frac{(-1)^{xy}[N(a = b|xy) - N(a \neq b|xy)]}{P(xy)}$$

determined by using the observed data.

Randomness of the output string is quantified by using min entropy

$$H_\infty(R|S) = -log_2[max_r P(r|s)]$$

The authors show that the min entropy of the outputs r is bounded by

$$H_\infty(R|S) \geq nf(\hat{I} - \epsilon) \ldots \ldots (1)$$

with probability greater than $1 - \delta$, where $\epsilon = O(\sqrt{-log\delta/(q^2 n)})$ is a statistical parameter and $q = min_{x,y} P(xy)$ is the probability of the least probable input pair. To obtain $f(I)$, semi-definite programming is used. The graph for $f(I)$ is shown below.

This figure and the text with the figure is taken from [4]

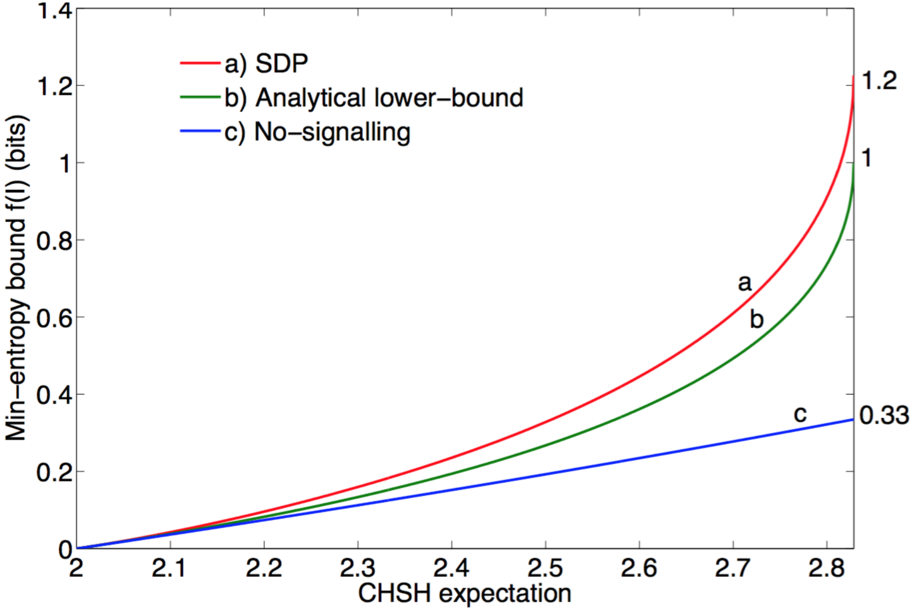

Figure 2: Plot of the function $f(I)$. The function $f(I)$ can be interpreted as a bound on the min-entropy per use of the system for a given CHSH expectation I, in the asymptotic limit of large n where finite statistics effects (the parameter ϵ in (3)) can be neglected. The function $f(I)$ (curve a) is derived through semidefinite programming using the techniques of [22,23] (semidefinite programming is a numerical method that is guaranteed to converge to the exact result). Curve b corresponds to the analytical lower-bound $f(I) \geq -\log_2 \left[1 - \log_2 \left(1 + \sqrt{2 - \frac{I^2}{4}}\right)\right]$. Curve c corresponds to the minimal value $f(I) = -\log_2 (3/2 - I/4)$ of the min-entropy implied by the no-signalling principle alone. The function $f(I)$ starts at zero at the local threshold value $I = 2$. Systems that violate the CHSH inequality ($I > 2$), on the other hand, satisfy $f(I) > 0$, i.e., have a positive min-entropy.

6 Directions for Future Research

We have learnt a lot from this course project. We have gained a basic understanding of Quantum non-local games and also have gained a decent understanding of the results of the paper [4] . There have been many follow up works based on [4]. [6] was specifically built upon this to achieve an exponential randomness expansion scheme. We want to understand [6] and also device independent Quantum Cryptography more clearly.

7 Acknowledgments

We are very grateful to Prof. Rajat Mittal for giving us the freedom to pursue the topic of our choice for the project and also for guiding us throughout the duration of the project. We are also very thankful to all the other students in the course for attending our mid-term presentation and their valuable feedback.

References

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

[2] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[3] 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.

[4] 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.

[5] U. Vazirani. Course notes: Quantum mechanics and quantum computation cs191-x.

[6] 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.