Trading Isolation for Certifiable Randomness Expansion

by

Matthew Ryan Coudron

B.S. Mathematics, University of Minnesota (2011)

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degree of

Master of Science in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 2013

Author . . . .
Department of Electrical Engineering and Computer Science
August 30, 2013

Certified by . . . .
Peter Shor
Professor
Thesis Supervisor

Accepted by . . . .
Leslie A. Kolodziejski
Chairman, Department Committee on Graduate Theses

Trading Isolation for Certifiable Randomness Expansion

by

Matthew Ryan Coudron

Submitted to the Department of Electrical Engineering and Computer Science
on August 30, 2013, in partial fulfillment of the
requirements for the degree of
Master of Science in Electrical Engineering and Computer Science

Abstract

A source of random bits is an important resource in modern cryptography, algorithms and statistics. Can one ever be sure that a "random" source is truly random, or in the case of cryptography, secure against potential adversaries or eavesdroppers? Recently the study of non-local properties of entanglement has produced an interesting new perspective on this question, which we will refer to broadly as Certifiable Randomness Expansion (CRE). CRE refers generally to a process by which a source of information-theoretically certified randomness can be constructed based only on two simple assumptions: the prior existence of a short random seed and the ability to ensure that two or more black-box devices do not communicate (i.e. are non-signaling).

In this work we make progress on a conjecture of [Col09] which proposes a method for indefinite certifiable randomness expansion using a growing number of devices (we actually prove a slight modification of the original conjecture in which we use the CHSH game as a subroutine rather than the GHZ game as originally proposed). The proof requires a technique not used before in the study of randomness expansion, and inspired by the tools developed in [RUV12]. The result also establishes the existence of a protocol for constant factor CRE using a finite number of devices (here the constant factor can be much greater than 1). While much better expansion rates (polynomial, and even exponential) have been achieved with only two devices, our analysis requires techniques not used before in the study of randomness expansion, and represents progress towards a protocol which is provably secure against a quantum eavesdropper who knows the input to the protocol.

Thesis Supervisor: Peter Shor
Title: Professor

Acknowledgments

I am very grateful to Aram Harrow, Thomas Vidick, and Henry Yuen for many enlightening conversations regarding this work. A special thanks to my advisor Peter Shor for good advice, and patient counsel. As always, thanks to my family for constant encouragement, love and support.

Portions of the abstract and preliminary section of this paper are paraphrased from [CVY13], which was joint work with Thomas Vidick and Henry Yuen. This work makes extensive use of ideas cited from [RUV12].

This work was supported by the Center for Science of Information, an NSF Science and Technology Center, under grant CCF-0939370, and also supported by NSF grant CCF-0801525.

Contents

Chapter 1

Introduction

In his Ph.D. thesis, Colbeck [Col09], was the first to propose protocols for "Private Randomness Expansion", here referred to as Certifiable Randomness Expansion (CRE). These proposals sparked a series of works to refine and improve CRE protocols and their analysis [PAM10, CK11, VV11, FGS13, PM13]. Most of the protocols proposed by these works use only two non-signaling devices, and follow a basic format in which the devices are required to play a certain quantum game (such as the CHSH game, or GHZ game) many times in serial, reporting their output bits for one round to a referee before receiving the randomized input bits for the next round. At the end of all the rounds the referee may perform a test that the devices are expected to pass. A good protocol has the property that, conditioned on the devices passing the test, one can prove a lower bound on the entropy of the output. For more on the formal framework for such protocols see [CVY13].

The best known expansion rate for such two-device non-adaptive protocols is exponential [VV11]. That is, it can be certified that, conditioned on the devices passing the referee's test, the output has smoothed min-entropy which is exponential in the size of the random seed. In [VV11] it is further proved this the min-entropy of the output is secure against any quantum eavesdropper that has no knowledge of the seed. The analysis of [VV11] uses a concept called the "guessing game". Their proof shows that, if an eavesdropper could guess some information about the output of the devices running this protocol (conditioned on the devices passing the referee's test), then that eavesdropper can guess a lot of information about the random input seed. This is very unlikely since, by assumption, the random input seed is unknown to the eavesdropper.

Colbeck's original proposals for CRE protocols (section 5 of [Col09]) were based around serial repetition of the GHZ game. Essentially, he proposes that if one were to have three non-signaling devices play r rounds of the GHZ game (a game which requires three devices) in serial, with appropriately randomized input at every round, then the output (conditioned on the devices winning the GHZ game at every round) should have smoothed min-entropy proportional to r, secure even against an quantum eavesdropper that knows the input to the rounds. Even if true, this conjecture would not establish randomness *expansion* since the output is no larger than the input. Therefore, Colbeck further proposes a protocol in which these r rounds of serial GHZ are repeated simultaneously by n different triples of devices (all devices being jointly multi-partite non-signaling). Furthermore, each of the triples of devices must receive the same random input as the other triples throughout the course of the protocol. He conjectures that the output of these devices (conditioned on the devices winning every GHZ game) has smoothed min-entropy proportional to nr. This is, therefore, a proposal of a CRE protocol which has expansion factor linear in the number of devices used, and thus has an arbitrarily large expansion factor if one is allowed access to an arbitrary number of devices. The intuition behind this proposition is that, since each triple of devices produces randomness secure even against an eavesdropper who knows the input, the output of each triple must still have randomness even conditioned on the outputs of all the other device triples (which may be viewed as eavesdroppers).

This is an interesting and natural proposal. Nonetheless, it is difficult to prove such results using an analysis based on the "guessing game" because we can no longer assume that the eavesdropper has no knowledge of the input. Indeed, each device triple has full knowledge of the input used on every other device triple. A priori, this could allow them to correlate their answers arbitrarily and produce very low total output entropy while still passing the referee's test. We will show that, at least in one particular natural setting, no such cheating strategy is possible.

In this work we will give a proof of these conjectures with a couple modifications. Instead of using the GHZ game as a subroutine, we will use the CHSH game. This means that instead of device triples, we will speak of device pairs. In order to accommodate the optimal winning probability of the CHSH game the referee's test in the protocol will also change. Otherwise the protocol remains the same (for a precise statement refer to Definition 1.2.1 below). We will not explicitly prove security against quantum eavesdropper for this protocol in this work, though we note that, as discussed above, the indefinite expansion result which we do prove already requires an implicit notion of such security. We expect that security against a quantum eavesdropper (even one that knows the input to the protocol) can be derived from this analysis in a straightforward manner, but leave this for future work.

The main technical observation of this work is that, by applying an analysis similar to that in [RUV12] we can certify that the devices in the protocol must actually be performing a particular type of quantum measurement on a particular type of quantum state in order to pass the referee's test with high probability. With such specific knowledge we can show that the output of certain pairs of devices has high entropy, even conditioned on other devices in the protocol who know the input.

For the soundness condition of our result we will need to assume that the devices use a strategy in which the probability of passing the referee's test is greater than $1 - \frac{1}{\mathrm{poly}(r)}$. This assumption can be enforced through a form of polynomial amplification, but removing the assumption altogether would make the result cleaner, and is an interesting open problem. The smoothness parameter and probability bounds that we prove for this protocol are often inverse polynomial where one might hope that they could be made inverse exponential in r. Indeed, they are often only the inverse of a fractional power of r (like $\frac{1}{\sqrt[4]{r}}$). This parameter scaling may be inherent in applying the tools of [RUV12], and improving the scaling (by improving the analysis, or redesigning the protocol) is another very interesting open problem. Nonetheless, proving randomness expansion results of this form (whatever the parameter scaling) is a necessary and potentially useful conceptual step in improving our understanding of randomness expansion and quantum non-locality.

1.1 Preliminaries

Let X be a random variable that takes values in some discrete domain $\mathcal{D}$. Its min-entropy is defined as $H_\infty(X) = -\log \max_{x\in\mathcal{D}} \Pr(X = x)$

The conditional min-entropy is defined as

$$H_\infty(X|Y) = -\log\Big(\sum_y \Pr(Y = y) 2^{-H_\infty(X|Y=y)}\Big).$$

For two discrete random variables X, Y with the same domain, their statistical distance is $\|X - Y\|_1 = \sum_{x\in\mathcal{D}} |\Pr(X = x) - \Pr(Y = x)|$. When X and Y are defined by probability distributions P_x and P_y, we may also write $\|P_x - P_y\|_1$ to denote $\|X - Y\|_1$, the statistical distance between X and Y. For $\epsilon > 0$, the smoothed min-entropy of a discrete random variable X is defined as

$$H_\infty^\epsilon(X) = \sup_{\tilde{X}, \|\tilde{X}-X\|_1 \le \epsilon} H_\infty(\tilde{X}),$$

where the supremum is taken over all $\tilde{X}$ defined on $\mathcal{D}$. The smoothed conditional min-entropy is

$$H_\infty^\epsilon(X|Y) = \sup_{(\tilde{X},\tilde{Y}), \|(\tilde{X},\tilde{Y})-(X,Y)\|_1 \le \epsilon} H_\infty(\tilde{X}|\tilde{Y}).$$

The CHSH game. The CHSH game is a two-player game with two non-communicating players, Alice and Bob, who are given independent random inputs $x, y \in \{0, 1\}$ respectively. Their task is to produce outputs $a, b \in \{0, 1\}$ such that $a \oplus b = x \wedge y$. By enumerating over all deterministic strategies, it is not hard to see that the optimal classical winning probability of the CHSH game is $\omega_c(\text{CHSH}) = 3/4$. There is a simple quantum strategy based on the use of a single EPR pair which demonstrates that the optimal quantum winning probability is $\omega_q(\text{CHSH}) \ge \cos^2(\pi/8) \approx 85\%$, and in fact it is an optimal quantum strategy [Cir80, CN]. This "ideal", or "optimal" quantum strategy is illustrated in Table 1.1 which is taken from [RUV12].

We will see from Lemma 1.3.2 (also copied from [RUV12]) that this ideal strategy is, in

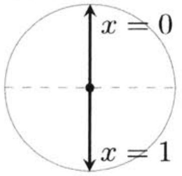
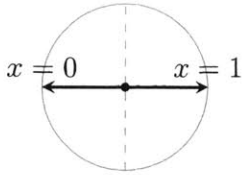
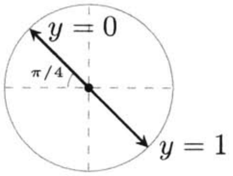
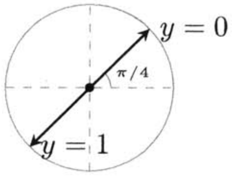
Alice's strategy		**Bob's strategy**	
$\underline{a=0}$	$\underline{a=1}$	$\underline{b=0}$	$\underline{b=1}$
$\|0\rangle\langle 0\| \mapsto x=0$	$\|+\rangle\langle +\| \to x=0$	$M^\dagger\|+\rangle\langle +\|M \to y=0$	$M^\dagger\|0\rangle\langle 0\|M \to y=0$
$\|1\rangle\langle 1\| \mapsto x=1$	$\|-\rangle\langle -\| \to x=1$	$M^\dagger\|-\rangle\langle -\|M \to y=1$	$M^\dagger\|1\rangle\langle 1\|M \to y=1$
			

Table 1.1: [This table taken from [RUV12]] An optimal quantum strategy for the CHSH game. Alice and Bob each have one qubit of a shared EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. On each input a or b, they make the two-outcome projective measurements listed above. Here, $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $M = \exp(-i\frac{\pi}{8}Y)$. Thus $R_0^A = Z$, $R_1^A = X$, $R_0^B = M^\dagger XM$ and $R_1^B = M^\dagger ZM$. The measurements are also illustrated on a cross-section through the xz-plane of the Bloch sphere.

a robust sense, the only strategy which can achieve the optimal winning probability for the CHSH game. This property of the CHSH game is often referred to as rigidity. This is the key idea which we will use in our analysis, in a manner similar to that pioneered by [RUV12].

1.2 The Main Result

Definition 1.2.1. *We define a family of protocols $(P_{r,n,h,\delta})$. Here, $P_{r,n,h,\delta}$ $(r, n \in \mathbb{N}, 1 > \delta, h > 0)$ is a protocol designed for n pairs of devices (D^l_A, D^l_B) for $l \in [n]$, and a referee. The protocol takes as input $2r$ uniform random bits, which we will denote with a vector $\vec{r} \in \{0,1\}^{2r}$, and proceeds in r rounds. At the i^{th} round the referee sends $x_i \equiv \vec{r}_{2i-1}$ to D^l_A (for all $l \in [n]$), and bit $y_i \equiv \vec{r}_{2i}$ to D^l_B (for all $l \in [n]$), and requests that each pair (D^l_A, D^l_B) play a CHSH game with those bits as input. The referee then collects the outputs of every pair of non-signaling devices and proceeds to the next round. The output from D^l_A at the i^{th} round will be denoted a^l_i and that from D^l_B, b^l_i.*

Let $Win_l \equiv 1\left[\left|\{i : a^l_i \oplus b^l_i = x_i y_i\}\right| \geq r(\text{OPT} - \delta)\right]$ be the event that the l^{th} pair of devices "win" at least an $\text{OPT} - \delta$ fraction of the r rounds played. The referee accepts if and only if

$$Win \equiv 1\left[\left|\{l : Win_l = 1\}\right| \geq (1-h)n\right] = 1. \tag{1.2.1}$$

Theorem 1.2.2. *Consider the protocol $P_{r,n,\frac{1}{r},\frac{1}{\sqrt[4]{r}}}$. For $r \geq 4$ this protocol has completeness $1 - 2\exp\left(-\frac{n}{4r^2}\right)$. Furthermore, if $\Pr(Win = 1) \geq 1 - \frac{1}{\sqrt[4]{r}}$, then*

$$H_\infty^{\Theta\left(\frac{1}{\sqrt[32]{r}}\right)}(Output|Win = 1) \geq \frac{nr}{16} \tag{1.2.2}$$

In particular, this implies that (following the convention of [CVY13] Definition 3.1) the family of protocols $(P_{r,n,\frac{1}{r},\frac{1}{\sqrt[4]{r}}})$ is a randomness amplifier with seed length $2r$, completeness $c(r) = 1 - 2\exp\left(-\frac{n}{4r^2}\right)$, soundness $s(r) = 1 - \frac{1}{\sqrt[4]{r}}$ against quantum strategies, smoothness $\epsilon(r) = \Theta\left(\frac{1}{\sqrt[32]{r}}\right)$, and expansion $g(n,r) = \frac{n}{32}$.

Note that the expansion $g(n,r)$ could, a priori, be a function of r, but in fact is only a function of n. Furthermore, $g(n,r)$ grows linearly with n regardless of the value of r, and this is the sense in which this family of protocols gives a scheme for indefinite randomness expansion, assuming access to arbitrarily many devices. Also note that Definition 3.1 of

[CVY13] technically only covers protocols using two devices, but it is natural and straight forward to generalize.

1.3 Rigidity, and sequential CHSH games

In this section we review some results and notation for studying rigidity of the CHSH game, and sequences of CHSH games. The material in this section is either cited or paraphrased from [RUV12] (see citations).

Definition 1.3.1 (Paraphrased from [RUV12]). *For convenience in studying the CHSH game we will define* $\mathrm{OPT} \equiv \cos^2(\pi/8)$.

For $\epsilon \geq 0$, *a quantum strategy for the CHSH game is* ϵ-structured *if the winning probability (with uniform random inputs) is at least* $\mathrm{OPT} - \frac{\epsilon}{8}$.

Lemma 1.3.2 (CHSH game rigidity: Reichardt, Unger, and Vazirani [RUV12]). *There exists a constant* $c > 0$ *such that the following statements hold. Consider a quantum strategy for the CHSH game, specified by Hilbert spaces* $\mathcal{H}_A$, $\mathcal{H}_B$ *and* $\mathcal{H}_C$, *a state* $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, *and reflections* $R^D_\alpha \in \mathcal{L}(\mathcal{H}_D)$ *for* $D \in \{A, B\}$ *and* $\alpha \in \{0, 1\}$. *Let* $\epsilon > 0$ *and assume that the strategy is* ϵ*-structured.*

Then there are extensions of the Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$, *and extensions of the reflections* R^D_α *by a direct sum with other reflections, so that the following properties hold:*

- *There is an isomorphism between Alice's extended space and* $\mathbf{C}^2 \otimes \hat{\mathcal{H}}_A$, *under which* $R^A_0 = Z \otimes \mathbf{1}$ *and* $\|(R^A_1 - X \otimes \mathbf{1})_A \otimes \mathbf{1}_{BC}|\psi\rangle\| < c\sqrt{\epsilon}$.

- *Bob's space is isomorphic to* $\mathbf{C}^2 \otimes \hat{\mathcal{H}}_B$, *with* $R^B_0 = Z \otimes \mathbf{1}$ *and* $\|(R^B_1 - X \otimes \mathbf{1})_B|\psi\rangle\| < c\sqrt{\epsilon}$.

- *Finally, letting*
$$|\psi^*\rangle = (I \otimes (HM))\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \ , \tag{1.3.1}$$
where $M = \exp(-i\frac{\pi}{8}Y)$ *as in Table 1.1, and H is the two by two Hadamard matrix, there exists a unit vector* $|\psi^\times\rangle \in \hat{\mathcal{H}}_A \otimes \hat{\mathcal{H}}_B \otimes \mathcal{H}_C$ *with* $\||\psi\rangle - |\psi^*\rangle \otimes |\psi^\times\rangle\| < c\sqrt{\epsilon}$.

Furthermore, if $\mathcal{H}_A$ *and* $\mathcal{H}_B$ *are finite-dimensional, then the isomorphisms into* $\mathbf{C}^2 \otimes \hat{\mathcal{H}}_A$ *and into* $\mathbf{C}^2 \otimes \hat{\mathcal{H}}_B$ *depend only on* R^A_0, R^A_1 *and on* R^B_0, R^B_1, *respectively.*

We now establish some notation for CHSH games played in sequence, one following the next, such that devices cannot communicate between games. Each game is understood to have a uniform random inputs, independent from all previous games.

Definition 1.3.3 (Paraphrased from [RUV12]). *A strategy $\mathcal{S}$ for two provers, Alice and Bob, to play n sequential CHSH games consists of the provers' Hilbert spaces, their initial state and the reflections they use to play each game. Fix the following notation:*

Transcripts: *Denote questions asked to Alice by $a_1, \ldots, a_n$, questions asked to Bob by $b_1, \ldots, b_n$, and possible answers by $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$, respectively. Write $h_j^A = (a_1, \ldots, a_j, x_1, \ldots, x_j)$, $h_j^B = (b_1, \ldots, b_j, y_1, \ldots, y_j)$ and $h_j = (h_j^A, h_j^B)$, a full transcript for games* 1 *through j.*

Hilbert spaces: *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be the two provers' Hilbert spaces, and $\mathcal{H}_C$ any external space.*

Reflection and projection operators: *In game j, for questions a_j and b_j, let $R_{a_j}^A(h_{j-1}^A)$ and $R_{b_j}^B(h_{j-1}^B)$ be the reflections specifying Alice and Bob's respective strategies. Let $P_j^A(h_j^A) = \frac{1}{2}(\mathbf{1} + (-1)^{x_j} R_{a_j}^A(h_{j-1}^A))$ and $P_j^B(h_j^B) = \frac{1}{2}(\mathbf{1} + (-1)^{y_j} R_{b_j}^B(h_{j-1}^B))$.*

States: *Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ be the provers' initial shared state, and let $|\psi(h_{j-1})\rangle$ be the shared state at beginning of game j conditioned on the transcript h_{j-1}*

Random variables: *We use A_j, B_j, X_j, Y_j to denote the random variables for the questions and answers in game j, and H_j for the transcript up through game j. A_j and B_j are distributed independently and uniformly at random. Conditioned on the transcript h_{j-1} for the first $j-1$ games and the questions a_j and b_j, X_j and Y_j are distributed according to $\Pr[X_j = x_j, Y_j = y_j | H_{j-1} = h_{j-1}, A_j = a_j, B_j = b_j] = \| P_j^A(h_j^A) \otimes P_j^B(h_j^B) |\psi(h_{j-1})\rangle \|^2$.*

Chapter 2

Proofs

2.1 Outline of Proof

Now let us consider a sequence of r rounds of CHSH played in serial with the same pair of non-signaling players with uniform random, independent inputs at each round. We will use the terminology of section 1.3 above. Let W_i be the random variable indicating a "win" in round i. That is, $W_i = 1 \oplus X_i \oplus Y_i \oplus A_i B_i$. Let $W \equiv \sum_{i=1}^{r} W_i$ be the random variable counting the number of "wins" in the serial protocol. In the following lemma $\mathbb{E}[W_i|H_{i-1}]$ denotes a conditional expectation, and is therefore a random variable, which is equal to the winning probability of the i^{th} round conditioned on H_{i-1}, the transcript of all previous games. We define $S \equiv \sum_{j=1}^{r} \mathbb{E}[W_j|H_{j-1}]$

We now present a result about testing for individual ϵ-structured games within a sequence of CHSH games. This result is similar in spirit and in proof to those in section 5.7 of [RUV12], though it is tailored to our purpose and does not appear there in this form.

Lemma 2.1.1. *For $\delta_1, \delta_2 > 0$,*

$$\Pr\left(W \geq (\text{OPT} - \delta_1)r \textit{ and } S \leq (\text{OPT} - \delta_2)r\right) \leq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right)$$

We will now consider the parallel randomness amplification scheme $P_{r,n,h,\delta}$ of Definition 1.2.1. In light of the many pairs of devices present in the protocol $P_{r,n,h,\delta}$ we will update the notation of Section 1.3. There we defined a number of terms regarding the strategies and outputs of a single pair of devices (D_A, D_B) playing a sequence of CHSH games each with independent uniform random inputs. We now give each pair of devices (D^l_A, D^l_B) in protocol $P_{r,n,h,\delta}$ its own copy of the notation defined in Section 1.3. We will denote this by adding a superscript l to the notation referring to outputs or strategies of the device pair (D^l_A, D^l_B). Thus, X^l_j is the output of device D^l_A at round j, H^l_j is the random variable taking the value of the transcript for the first j rounds of use of device pair (D^l_A, D^l_B), $R^{A,l}_{a^l_j}(h^{A,l}_{j-1})$ is the reflection applied by D^l_A at the j^{th} round given that $H^{A,l}_{j-1} = h^{A,l}_{j-1}$ and $A^l_j = a^l_j$, and so on.

Furthermore, we will similarly update the notation of Lemma 2.1.1. Let W^l_i be the binary random variable indicating a "win" by devices (D^l_A, D^l_B) at round i. That is, $W^l_i = 1 \oplus X^l_j \oplus Y^l_j \oplus A^l_j B^l_j$. Let $S_l \equiv \sum_{i=1}^r \mathbb{E}[W^l_j | H^l_{j-1}]$.

Here we pause to highlight a subtle but important point. Note that, WLOG, we may assume that $R^{A,l}_{a^l_j}(h^{A,l}_{j-1})$ (resp. $R^{B,l}_{b^l_j}(h^{B,l}_{j-1})$) are deterministic functions of a^l_j and $h^{A,l}_{j-1}$ (resp. b^l_j and $h^{B,l}_{j-1}$), not random variables. The reason for this is that, we have assumed that all the devices (which are multi-partite non-signaling) must employ a quantum strategy, and furthermore, any shared randomness used by the devices before the beginning of the protocol can be instead encoded in their shared quantum state without changing the outcome probabilities. Thus, the shared quantum state (shared between all $2n$ devices in the protocol), and the reflections, which are deterministic functions of past transcripts and current inputs, represent the most general quantum strategy. We will assume this, and it will be important in order for the entire analysis to remain well defined.

The following lemma will ultimately allow us to establish, with high probability, the existence of many ϵ-structured individual games across all n pairs of devices (conditioned on the entire protocol passing).

Lemma 2.1.2. *Imagine a single use of protocol P_{r,n,h,δ_1}. If*

$$\Pr\left(|\{l : S_l \geq (\text{OPT} - \delta_2) r\}| \geq (1-s)n | Win = 1 \right) \leq 1 - d$$

Then,

$$(ds - h)\Pr(Win = 1) \leq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right)$$

As one might guess from the statement, the proof of Lemma 2.1.2 makes critical use of Lemma 2.1.1.

The idea behind the proof of Theorem 1.2.2 is to use Lemma 2.1.2, and the guarantee $\Pr(Win = 1) \geq 1 - \frac{1}{\sqrt[4]{r}}$ to prove existence of many values $(l, i) \in [n] \times [r]$ ($\Theta(nr)$ such values) such that round i played by the l^{th} device pair is τ-structured (with $\tau = \Theta\left(\frac{1}{\sqrt[16]{r}}\right)$) nearly all the time. Further analysis will reveal that the distribution of outputs a_i^l at such rounds satisfies the assumed property in Lemma 2.1.3 below. An application of Lemma 2.1.3 then completes the poof of Theorem 1.2.2.

Lemma 2.1.3. *Suppose, for some $\delta > 0$, that we have a probability distribution $P(x_1, ..., x_n)$ on n-bit strings $\vec{x} = (x_1, ..., x_n) \in \{0,1\}^n$ such that for all $i \in [n]$*

$$||P(x_1, .., x_i) - P(x_1, ..., x_{i-1}) \cdot P_{\frac{1}{2}}(x_i)||_1 \leq \delta$$

Here, $P_{\frac{1}{2}}$ is the uniform distribution on a single bit. It follows that

$$H_\infty^{6\sqrt{\delta}}(\vec{x}) \geq -\log\left(\frac{1}{1 - 3\sqrt{\delta}}\right) - \frac{n}{4}\log\left(\frac{1}{2} + \sqrt{\delta}\right)$$

2.2 The Proof

Suppose that we choose parameters $d, s, h, \delta_1, \delta_2 \geq 0$ such that

$$(ds - h)\Pr(Win = 1) \geq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right) \tag{2.2.1}$$

Then it follows by Lemma 2.1.2 that

$$\begin{aligned}
&\mathbb{E}\left[\sum_{l=1}^{n}\sum_{i=1}^{r}\mathbb{E}[W_i^l|H_{i-1}^l]\right] \geq \Pr(Win = 1)\mathbb{E}\left[\sum_{l=1}^{n}\sum_{i=1}^{r}\mathbb{E}[W_i^l|H_{i-1}^l]|Win = 1\right] \\
&\geq \Pr(Win = 1)\Pr\left(|\{l : S_l \geq (\text{OPT} - \delta_2)r\}| \geq (1-s)n|\, Win = 1\right)(1-s)n(\text{OPT} - \delta_2)r \\
&\geq \Pr(Win = 1)(1-d)(1-s)(\text{OPT} - \delta_2)nr
\end{aligned} \tag{2.2.2}$$

We know, by optimality of OPT as the maximal winning probability for the CHSH game, and the fact that every round (l, i) is given a uniformly random input conditioned on H_{i-1}^l that for all $(l, i) \in [n] \times [r]$, $\mathbb{E}[W_i^l|H_{i-1}^l] \leq \text{OPT}$ (here $\mathbb{E}[W_i^l|H_{i-1}^l]$ is a random variable and this inequality holds with probability 1). Therefore, also, $\mathbb{E}[\mathbb{E}[W_i^l|H_{i-1}^l]] \leq \text{OPT}$. It follows by Markov's inequality and equation (2.2.2) that, for any $0 < \gamma_1 \leq 1$ there can be at most $\gamma_1 nr$ values $(l, i) \in [n] \times [r]$ such that

$$\begin{aligned}
&\left(\text{OPT} - \mathbb{E}\left[\mathbb{E}[W_i^l|H_{i-1}^l]\right]\right) \geq \frac{1}{\gamma_1}\left(\text{OPT} - \Pr(Win = 1)(1-d)(1-s)(\text{OPT} - \delta_2)\right) \\
&= \frac{\text{OPT}}{\gamma_1}\left(1 - \Pr(Win = 1)(1-d)(1-s)\left(1 - \frac{\delta_2}{\text{OPT}}\right)\right)
\end{aligned} \tag{2.2.3}$$

We now define

$$G \equiv \left\{(l, i) \in [n] \times [r] : \left(\text{OPT} - \mathbb{E}\left[\mathbb{E}[W_i^l|H_{i-1}^l]\right]\right) \leq B_1\right\} \tag{2.2.4}$$

Where, for notational simplicity we have set

$$B_1 \equiv \frac{\text{OPT}}{\gamma_1}\left(1 - \Pr(Win = 1)(1-d)(1-s)\left(1 - \frac{\delta_2}{\text{OPT}}\right)\right)$$

By the above argument it follows that $|G| \geq \lfloor (1-\gamma_1)nr \rfloor$. For any $(l,i) \in G$ it follows by Markov's inequality that for any $0 < \gamma_2 \leq 1$

$$\Pr\left(H_{i-1}^l \in \left\{h_{i-1}^l : \left(\text{OPT} - \mathbb{E}[W_i^l | H_{i-1}^l = h_{i-1}^l]\right) > \frac{B_1}{\gamma_2}\right\}\right) \\ \leq \gamma_2 \tag{2.2.5}$$

Note, in the above equation, that, for any value of h_{i-1}^l, $\mathbb{E}[W_i^l | H_{i-1}^l = h_{i-1}^l]$ is a constant by definition. Reorganizing the above equation gives:

$$\Pr\left(H_{i-1}^l \in \left\{h_{i-1}^l : \mathbb{E}[W_i^l | H_{i-1}^l = h_{i-1}^l] \geq B_2\right\}\right) \\ > 1 - \gamma_2 \tag{2.2.6}$$

where we have

$$B_2 \equiv \text{OPT}\left(1 - \frac{1}{\gamma_2\gamma_1}\left(1 - \Pr(Win = 1)(1-d)(1-s)\left(1 - \frac{\delta_2}{\text{OPT}}\right)\right)\right)$$

Let $P\left(\{x_i^l : (l,i) \in G\}\right)$ be the probability distribution of the Alice outputs for the rounds $(l,i) \in G$. We define an order on the elements of G as follows: for $(l,i),(l',i') \in G$ we say $(l',i') \geq (l,i)$ if $l' > l$, or $l' = l$ and $i \geq i'$. Otherwise we say $(l,i) > (l',i')$.

Lemma 2.2.1. *Define*

$$\epsilon \equiv 8\frac{\text{OPT}}{\gamma_2\gamma_1}\left(1 - \Pr(Win = 1)(1-d)(1-s)\left(1 - \frac{\delta_2}{\text{OPT}}\right)\right)$$

.

For every $(l', i') \in G$

$$\left\| P\left(\left\{x_i^l : (l,i) \in G \textit{ and } (l,i) \leq (l',i')\right\}\right) - P\left(\left\{x_i^l : (l,i) \in G \textit{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right) \right\|_1 \leq 4\left(\gamma_2 + 4c\sqrt{\epsilon}\right) \tag{2.2.7}$$

We are now ready to prove the main result, Theorem 1.2.2.

2.2.1 Proof of Theorem 1.2.2

Restatement of Theorem 1.2.2

Consider the protocol $P_{r,n,\frac{1}{r},\frac{1}{\sqrt[4]{r}}}$. For $r \geq 4$ this protocol has completeness $1 - 2\exp\left(-\frac{n}{4r^2}\right)$. Furthermore, if $\Pr\left(Win = 1\right) \geq 1 - \frac{1}{\sqrt[4]{r}}$, then

$$H_{\infty}^{\Theta\left(\frac{1}{\sqrt[32]{r}}\right)}\left(Output|Win = 1\right) \geq \frac{nr}{16} \tag{2.2.8}$$

In particular, this implies that (following the convention of [CVY13] Definition 3.1) the family of protocols $(P_{r,n,\frac{1}{r},\frac{1}{\sqrt[4]{r}}})$ is a randomness amplifier with seed length $2r$, completeness $c(r) = 1 - 2\exp\left(-\frac{n}{4r^2}\right)$, soundness $s(r) = 1 - \frac{1}{\sqrt[4]{r}}$ against quantum strategies, smoothness $\epsilon(r) = \Theta\left(\frac{1}{\sqrt[32]{r}}\right)$, and expansion $g(n,r) = \frac{n}{32}$.

Proof of of Theorem 1.2.2

Proof. First we analyze completeness. Suppose that each pair of devices (D_A^l, D_B^l) uses the optimal CHSH strategy (presented in Table 1.1) at each of the r rounds. Then

$$\begin{aligned}
&\Pr\left(Win_l = 1\right) = \Pr\left(\sum_{i=1}^{r} W_i^l \geq r(\text{OPT} - \frac{1}{\sqrt[4]{r}})\right) \\
&\geq \Pr\left(\frac{1}{r}\left(\sum_{i=1}^{r} W_i^l - \mathbb{E}\left[\sum_{i=1}^{r} W_i^l\right]\right) = \left(\frac{1}{r}\sum_{i=1}^{r} W_i^l - \text{OPT}\right) \geq \frac{1}{\sqrt[4]{r}}\right) \\
&\geq 1 - \exp\left(-2\sqrt{r}\right)
\end{aligned} \tag{2.2.9}$$

Where the last inequality follows by Hoeffding's inequality. When all the devices are using the optimal CHSH strategy at all rounds, the random variables Win_l are independent since the states being measured by different pairs of devices are in tensor product with each other. Thus,

$$\begin{aligned}
&\Pr\left(Win = 1\right) = \Pr\left(\sum_{l=1}^{n} Win_l \geq (1 - \frac{1}{r})n\right) \geq 1 - \Pr\left(\sum_{l=1}^{n} Win_l \leq (1 - \frac{1}{r})n\right) \\
&\geq 1 - \Pr\left(\frac{1}{n}\left|\sum_{l=1}^{n} Win_l - \mathbb{E}\left[\sum_{l=1}^{n} Win_l\right]\right| \geq \left(\frac{1}{r} - \exp\left(-2\sqrt{r}\right)\right) \geq \frac{1}{2r}\right) \\
&\geq 1 - 2\exp\left(-\frac{n}{4r^2}\right)
\end{aligned} \tag{2.2.10}$$

The last inequality once again uses Hoeffding's inequality. Here we have assumed that r is sufficiently large that $\exp\left(-2\sqrt{r}\right) \leq \frac{1}{2r}$ ($r \geq 4$ suffices for this).

We now analyze the soundness of the protocol. We assume that $\Pr\left(Win = 1\right) \geq 1 - \frac{1}{\sqrt[4]{r}}$. Setting $h = \frac{1}{r}$, and $\delta_1 = \frac{1}{\sqrt[4]{r}}$, we note that we are considering the P_{r,n,h,δ_1} protocol. Further setting $\delta_2 = \frac{2}{\sqrt[4]{r}}$, $d = \frac{1}{\sqrt[4]{r}}$, and $s = \frac{1}{\sqrt[4]{r}}$ it is easy to see that (for sufficiently large r)

$$(ds - h)\Pr(Win = 1) \geq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right) \tag{2.2.11}$$

Now set $\gamma_1 = \frac{1}{2}$, and $\gamma_2 = \frac{1}{\sqrt[8]{r}}$. It follows by Lemma 2.2.1 that if we set

$$\epsilon \equiv 8\frac{\mathrm{OPT}}{\gamma_2\gamma_1}\left(1 - \Pr(Win = 1)(1-d)(1-s)\left(1 - \frac{\delta_2}{\mathrm{OPT}}\right)\right) \tag{2.2.12}$$

then we have that, for every $(l', i') \in G$ (G here is as defined in equation (2.2.4))

$$\left\| P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) - P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right) \right\|_1 \leq 4\left(\gamma_2 + 4c\sqrt{\epsilon}\right) \tag{2.2.13}$$

A simple calculation gives that $\epsilon = \Theta\left(\frac{1}{\sqrt[8]{r}}\right)$, and thus

$$4\left(\gamma_2 + 4c\sqrt{\epsilon}\right) = \Theta\left(\frac{1}{\sqrt[16]{r}}\right) \tag{2.2.14}$$

Since $|G| \geq (1-\gamma_1)nr$ it follows by Lemma 2.1.3 that

$$H_\infty^{6\sqrt{\Theta\left(\frac{1}{\sqrt[16]{r}}\right)}}\left(\{x_i^l : (l,i) \in G\}\right) \geq -\log\left(\frac{1}{1 - 3\sqrt{\Theta\left(\frac{1}{\sqrt[16]{r}}\right)}}\right) - \frac{(1-\gamma_1)nr}{4}\log\left(\frac{1}{2} + \sqrt{\Theta\left(\frac{1}{\sqrt[16]{r}}\right)}\right) \tag{2.2.15}$$

So,

$$\begin{aligned} &H_\infty^{\frac{\Theta\left(\frac{1}{\sqrt[32]{r}}\right)}{\Pr(Win=1)}}\left(\{x_i^l : (l,i) \in G\} \mid Win = 1\right) \\ &\geq -\log(\Pr(Win = 1)) - \log\left(\frac{1}{1 - 3\Theta\left(\frac{1}{\sqrt[32]{r}}\right)}\right) - \frac{(1-\gamma_1)nr}{4}\log\left(\frac{1}{2} + \Theta\left(\frac{1}{\sqrt[32]{r}}\right)\right) \end{aligned} \tag{2.2.16}$$

Since $\Pr(Win = 1) \geq 1 - \frac{1}{\sqrt[4]{r}}$ and $\{x_i^l : (l,i) \in G\}$ is a subset of the entire output we have that, for sufficiently large r

$$H_\infty^{\Theta\left(\frac{1}{\sqrt[32]{r}}\right)}(Output|Win = 1) \geq \frac{nr}{16} \tag{2.2.17}$$

□

2.2.2 Proof of Lemma 2.2.1

Restatement of Lemma 2.2.1

Define

$$\epsilon \equiv 8\frac{\mathrm{OPT}}{\gamma_2\gamma_1}\left(1 - \Pr(Win = 1)(1-d)(1-s)\left(1 - \frac{\delta_2}{\mathrm{OPT}}\right)\right)$$

.

For every $(l', i') \in G$

$$\left\|P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) - P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right)\right\|_1$$
$$\leq 4\left(\gamma_2 + 4c\sqrt{\epsilon}\right) \tag{2.2.18}$$

Proof of Lemma 2.2.1

Proof. The main idea of the proof is as follows. Given a particular $(l', i') \in G$, we will consider a new strategy for the devices in which only the conditional measurements(and the quantum state) used at round (l', i') have been modified. The modifications will be such that the new strategy always outputs an independent uniform bit (conditioned on the past) at round (l', i'). We will show that each of the modifications made are small, and thus that the output distribution of the modified strategy is close to the original output distribution.

Fix a particular $(l', i') \in G$. From equation (2.2.5) we know that

$$\Pr\left(H_{i'-1}^{l'} \notin Good_{i'}^{l'}\right) \leq \gamma_2 \tag{2.2.19}$$

Where we have defined

$$Good_{i'}^{l'} \equiv \left\{h_{i'-1}^{l'} : \mathbb{E}[W_{i'}^{l'} | H_{i'-1}^{l'} = h_{i'-1}^{l'}] \geq B_2\right\} \tag{2.2.20}$$

So, for each $h_{i'-1}^{l'} \notin Good_{i'}^{l'}$ we modify $R_a^{A,l'}(h_{i'-1}^{A,l'})$ (resp. $R_b^{B,l'}(h_{i'-1}^{B,l'})$) for both values of a (resp. b), as well as $|\psi(h_{i'-1}^{l'})\rangle$ so that they match the ideal strategy for the CHSH game (illustrated in Table 1.1). We call the distribution of the outputs $\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\}$ corresponding to this new strategy $P'\left(\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\}\right)$. Since this new strategy is unchanged whenever $h_{i'-1}^{l'} \in Good_{i'}^{l'}$, we have that

$$\begin{aligned}
&\left\| P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) - P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right)\right\|_1 \\
&\leq \Pr\left(H_{i'-1}^{l'} \in Good_{i'}^{l'}\right) \left\| P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\} | H_{i'-1}^{l'} \in Good_{i'}^{l'}\right)\right. \\
&\left. - P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\} | H_{i'-1}^{l'} \in Good_{i'}^{l'}\right)\right\|_1 \\
&+ \Pr\left(H_{i'-1}^{l'} \notin Good_{i'}^{l'}\right) \left\| P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\} | H_{i'-1}^{l'} \notin Good_{i'}^{l'}\right)\right. \\
&\left. - P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\} | H_{i'-1}^{l'} \notin Good_{i'}^{l'}\right)\right\|_1 \\
&\leq \Pr\left(H_{i'-1}^{l'} \in Good_{i'}^{l'}\right) \cdot 0 + \Pr\left(H_{i'-1}^{l'} \notin Good_{i'}^{l'}\right) \cdot 2 \leq 2\gamma_2
\end{aligned} \tag{2.2.21}$$

Note that in the above $\Pr\left(H_{i'-1}^{l'} \in Good_{i'}^{l'}\right) = P\left(H_{i'-1}^{l'} \in Good_{i'}^{l'}\right) = P''\left(H_{i'-1}^{l'} \in Good_{i'}^{l'}\right)$ is well defined, since P and P' are identical probability distributions on

$$\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}.$$

We now further modify the strategy in the following way:

For each $h_{i'-1}^{l'} \in Good_{i'}^{l'}$ we know from the definition of $Good_{i'}^{l'}$ and the definition of ϵ that

$$\mathbb{E}[W_{i'}^{l'} | H_{i'-1}^{l'} = h_{i'-1}^{l'}] \geq \text{OPT} - \frac{\epsilon}{8} \tag{2.2.22}$$

Note that the input to round (l',i') is still uniform and independent conditioned on the event $H_{i'-1}^{l'} = h_{i'-1}^{l'}$. It follows by Lemma 1.3.2 that there are extensions of the Hilbert spaces $\mathcal{H}_{i'}^{A,l'}(h_{i'-1}^{l'}), \mathcal{H}_{i'}^{B,l'}(h_{i'-1}^{l'})$, and extensions of the reflections $R_a^{D,l'}(h_{i'-1}^{A,l'})$ by a direct sum with other reflections (for $D \in \{A,B\}$ and $a \in \{0,1\}$), so that the following properties hold:

- There is an isomorphism between $D_A^{l'}$'s extended space and $\mathbf{C}^2 \otimes \hat{\mathcal{H}}_{i'}^{A,l'}(h_{i'-1}^{l'})$, under which $R_0^{A,l'}(h_{i'-1}^{A,l'}) = Z \otimes \mathbf{1}$ and $\|(R_1^{A,l'}(h_{i'-1}^{A,l'}) - X \otimes \mathbf{1})_A \otimes \mathbf{1}_{BC} |\psi\rangle(h_{i'-1}^{l'})\| < c\sqrt{\epsilon}$.
- There is an isomorphism between $D_B^{l'}$'s extended space and $\mathbf{C}^2 \otimes \hat{\mathcal{H}}_{i'}^{B,l'}(h_{i'-1}^{l'})$, under which $R_0^{B,l'}(h_{i'-1}^{B,l'}) = Z \otimes \mathbf{1}$ and $\|(R_1^{B,l'}(h_{i'-1}^{B,l'}) - X \otimes \mathbf{1})_B |\psi\rangle(h_{i'-1}^{l'})\| < c\sqrt{\epsilon}$.
- Finally, letting
$$|\psi^*\rangle = (I \otimes (HM))\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \ , \tag{2.2.23}$$
where $M = \exp(-i\frac{\pi}{8}Y)$ as in Table 1.1, and H is the two by two Hadamard matrix, there exists a unit vector $|\psi^\times\rangle \in \hat{\mathcal{H}}_{i'}^{A,l'}(h_{i'-1}^{l'}) \otimes \hat{\mathcal{H}}_{i'}^{B,l'}(h_{i'-1}^{l'}) \otimes \hat{\mathcal{H}}_{i'}^{C,l'}(h_{i'-1}^{l'})$ such that after applying both aforementioned isomorphisms,
$$\| |\psi\rangle(h_{i'-1}^{l'}) - |\psi^*\rangle \otimes |\psi^\times\rangle \| < c\sqrt{\epsilon} \tag{2.2.24}$$

In other words, the quantum strategy used by devices $D_A^{l'}$ and $D_B^{l'}$ at the i'^{th} round, conditioned on $H_{i'-1}^{l'} = h_{i'-1}^{l'}$ is very close to the ideal strategy for the CHSH game. Therefore, we will modify the strategy so that it is exactly the ideal strategy for the CHSH game. That is, we will replace $|\psi\rangle(h_{i'-1}^{l'})$ with $|\psi^*\rangle \otimes |\psi^\times\rangle$. It follows by the definition of the trace norm and the triangle inequality that we still have

$$\begin{aligned}
&||(R_0^{A,l'}(h_{i'-1}^{A,l'}) - Z \otimes \mathbf{1})_A \otimes \mathbf{1}_{BC}|\psi^*\rangle \otimes |\psi^\times\rangle|| < c\sqrt{\epsilon}\\
&||(R_1^{A,l'}(h_{i'-1}^{A,l'}) - X \otimes \mathbf{1})_A \otimes \mathbf{1}_{BC}|\psi^*\rangle \otimes |\psi^\times\rangle|| < 2c\sqrt{\epsilon}\\
&||(R_0^{B,l'}(h_{i'-1}^{B,l'}) - Z \otimes \mathbf{1})_B \otimes \mathbf{1}_{AC}|\psi^*\rangle \otimes |\psi^\times\rangle|| < c\sqrt{\epsilon}\\
&||(R_1^{B,l'}(h_{i'-1}^{B,l'}) - X \otimes \mathbf{1})_B \otimes \mathbf{1}_{AC}|\psi^*\rangle \otimes |\psi^\times\rangle|| < 2c\sqrt{\epsilon}
\end{aligned} \tag{2.2.25}$$

We now alter the values of $R_a^{D,l'}(h_{i'-1}^{A,l'})$ (for $D \in \{A, B\}$ and $a \in \{0,1\}$) so that we instead have,

$$\begin{aligned}
&||(R_0^{A,l'}(h_{i'-1}^{A,l'}) - Z \otimes \mathbf{1})_A \otimes \mathbf{1}_{BC}|\psi^*\rangle \otimes |\psi^\times\rangle|| = 0\\
&||(R_1^{A,l'}(h_{i'-1}^{A,l'}) - X \otimes \mathbf{1})_A \otimes \mathbf{1}_{BC}|\psi^*\rangle \otimes |\psi^\times\rangle|| = 0\\
&||(R_0^{B,l'}(h_{i'-1}^{B,l'}) - Z \otimes \mathbf{1})_B \otimes \mathbf{1}_{AC}|\psi^*\rangle \otimes |\psi^\times\rangle|| = 0\\
&||(R_1^{B,l'}(h_{i'-1}^{B,l'}) - X \otimes \mathbf{1})_B \otimes \mathbf{1}_{AC}|\psi^*\rangle \otimes |\psi^\times\rangle|| = 0
\end{aligned} \tag{2.2.26}$$

Note that, since the isomorphisms from Lemma 1.3.2 are invertible by definition, there is a well defined way to do this. With all of these modifications to the state and the measurements, the devices $D_A^{l'}$ and $D_B^{l'}$ now use exactly the ideal strategy for the CHSH game at the i'^{th} round, conditioned on $H_{i'-1}^{l'} = h_{i'-1}^{l'}$.

We make these modifications for every value of $h_{i'-1}^{l'} \in Good_{i'}^{l'}$, and we call the distribution of the outputs $\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\}$ resulting from this modified quantum strategy $P''\left(\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\}\right)$. Note that this modified quantum strategy now has the property that the devices $D_A^{l'}$ and $D_B^{l'}$ use exactly the ideal strategy for the CHSH game at the i'^{th} round, conditioned on $H_{i'-1}^{l'} = h_{i'-1}^{l'}$, for all $h_{i'-1}^{l'} \in Good_{i'}^{l'}$ by this most recent modification, and also for all $h_{i'-1}^{l'} \notin Good_{i'}^{l'}$ by the earlier modification that took us from P to P'. It follows that

$$P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) = P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right) \tag{2.2.27}$$

Note that because, in this new strategy, devices $D_A^{l'}$ and $D_B^{l'}$ always use an ideal strategy for the CHSH game at round i' the output of $D_A^{l'}$ at round i' is a uniform random bit independent of past transcript, and also independent of the outputs of the other device pairs D_A^l and D_B^l, where $l \neq l'$. We have implicitly used this fact in establishing equation (2.2.27).

Furthermore, it follows from equations 2.2.26 and equation 2.2.24, through a simple application of triangle inequality, that for any value $h_{i'-1}^{l'} \in Good_{i'}^{l'}$ we have

$$\begin{aligned}
&\Big\| P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\} | H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) \\
&- P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\} | H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) \Big\|_1 \\
&\leq 8c\sqrt{\epsilon}
\end{aligned} \tag{2.2.28}$$

Here the constant factor of 8 comes from the fact that we are including all of the bounds in equations equations 2.2.26 and equation 2.2.24 into our triangle inequality calculation. We could probably use fewer of these bounds a get a smaller constant factor, but we will not worry about that here.

Of course, for $h_{i'-1}^{l'} \notin Good_{i'}^{l'}$ we have

$$
\begin{aligned}
&P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\} | H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) \\
&= P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\} | H_{i'-1}^{l'} = h_{i'-1}^{l'}\right)
\end{aligned}
$$

since we didn't modify the quantum strategy at all between P' and P'' in that event. Putting all this together we get

$$
\begin{aligned}
&\Big\| P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\}\right) \\
&-P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\}\right)\Big\|_1 \\
&= \sum_{h_{i'-1}^{l'}} \Pr\left(H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) \Big\| P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\} | H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) \\
&-P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\} | H_{i'-1}^{l'} = h_{i'-1}^{l'}\right)\Big\|_1 \\
&\le \sum_{h_{i'-1}^{l'}} \Pr\left(H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) 8c\sqrt{\epsilon} \\
&\le 8c\sqrt{\epsilon} \qquad (2.2.29)
\end{aligned}
$$

Note that in the above $\Pr\left(H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) = P'\left(H_{i'-1}^{l'} = h_{i'-1}^{l'}\right) = P''\left(H_{i'-1}^{l'} = h_{i'-1}^{l'}\right)$ is well defined, since P' and P'' are identical probability distributions on

$$
\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}.
$$

We are now ready for the final calculation. Using equations 2.2.21, 2.2.27 and 2.2.29 along with the triangle inequality we see that

$$
\begin{aligned}
&\left\| P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\}\right) - P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right)\right\|_1 \\
&\le \left\| P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\}\right) - P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \le (l',i')\right\}\right)\left(x_{i'}^{l'}\right)\right\|_1
\end{aligned}
$$

$$
\begin{aligned}
&+\left\|P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) - P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right)\left(x_{i'}^{l'}\right)\right\|_1 \\
&+\Big\|P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) \\
&-P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right)\Big\|_1 \\
&+\Big\|P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right) \\
&-P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) < (l',i')\right\}\right) \cdot P_{\frac{1}{2}}\left(x_{i'}^{l'}\right)\Big\|_1 \\
&\leq 2\gamma_2 + 8c\sqrt{\epsilon} + 0 + \Big\|P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) \\
&-P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right)\Big\|_1 \\
&\leq 2\gamma_2 + 8c\sqrt{\epsilon} + \Big\|P\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) \\
&-P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right)\left(x_{i'}^{l'}\right)\Big\|_1 \\
&+\left\|P'\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right) - P''\left(\left\{x_i^l : (l,i) \in G \text{ and } (l,i) \leq (l',i')\right\}\right)\left(x_{i'}^{l'}\right)\right\|_1 \\
&\leq 2(2\gamma_2 + 8c\sqrt{\epsilon}) = 4(\gamma_2 + 4c\sqrt{\epsilon})
\end{aligned}
$$

□

2.2.3 Proof of Lemma 2.1.1

Restatement of Lemma 2.1.1

For $\delta_1, \delta_2 > 0$,

$$\Pr\left(W \geq (\textsc{opt} - \delta_1)r \text{ and } S \leq (\textsc{opt} - \delta_2)r\right) \leq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right)$$

Note that Lemma 2.1.1 was originally stated using notation for sequential CHSH games with a single pair of devices, and therefore the notation does not include the superscript l. However, the same statement and proof would, of course, apply if we added the superscript l for any $l \in [n]$.

Proof of Lemma 2.1.1

Proof. The idea for this proof is to show that the serial protocol has a martingale structure, and then use Azuma's inequality to obtain the desired result.

For every j define $\Delta_j \equiv W_j - \mathbb{E}[W_j|H_{j-1}]$, so we clearly have $\mathbb{E}\left[\Delta_j|H_{j-1}\right] = \mathbb{E}[W_j|H_{j-1}] - \mathbb{E}[W_j|H_{j-1}] = 0$ (is identically zero as a random variable).

We now define $\Phi_i \equiv \sum_{j=1}^{i} \Delta_j$. Note that we have $\Phi_r = \sum_{j=1}^{r} \Delta_j = \sum_{j=1}^{r} W_j - \sum_{j=1}^{r} \mathbb{E}[W_j|H_{j-1}] = W - \sum_{j=1}^{r} \mathbb{E}[W_j|H_{j-1}]$.

Now note that for any $i \in [r-1]$

$$\mathbb{E}\left[\Phi_{i+1}|\Phi_i,\ldots,\Phi_1\right] - \Phi_i = \mathbb{E}\left[\Phi_{i+1} - \Phi_i|\Phi_i,\ldots,\Phi_1\right] = \mathbb{E}\left[\Delta_{i+1}|\Phi_i,\ldots,\Phi_1\right] = \mathbb{E}\left[\Delta_{i+1}|\Delta_i,\ldots,\Delta_1\right]$$

$$= \sum_{h_i \in \{0,1\}^{4i}} \mathbb{E}\left[\Delta_{i+1}|H_i = h_i\right] \cdot \mathbb{E}\left[1\left[H_i = h_i\right]|\Delta_i,\ldots,\Delta_1\right] = 0$$

Here $1\left[H_i = h_i\right]$ is the indicator variable which is 1 if $H_i = h_i$ and 0 otherwise. The third equality follows because the values of $\Phi_i,\ldots,\Phi_1$ can be calculated deterministically given the values of $\Delta_i,\ldots,\Delta_1$ and vice versa. The final equality follows because, since we established earlier that $\mathbb{E}\left[\Delta_{i+1}|H_i\right] \equiv 0$ (is identically zero as a random variable), it follows that $\mathbb{E}\left[\Delta_{i+1}|H_i = h_i\right] = 0$ for every value of h_i that occurs with non-zero probability.

Thus, by definition, we have that the sequence of random variables Φ_i is a martingale. Note that if we define $\Phi_0 \equiv 0$, we may include it at the beginning of the martingale sequence Φ_i without changing the martingale structure (since $\mathbb{E}\left[\Phi_1|\Phi_0 = 0\right] = \mathbb{E}\left[\Phi_1\right] = 0$). Further note that $|\Phi_i - \Phi_{i-1}| = |\Delta_i| \leq 2$. It follows by Azuma's inequality that

$$\Pr\left(|\Phi_r - \Phi_0| \geq t\right) = \Pr\left(|\Phi_r| \geq t\right) = \Pr\left(\left|W - \sum_{j=1}^{r} \mathbb{E}[W_j|H_{j-1}]\right| \geq t\right) \leq 2\exp\left(\frac{-t^2}{2\sum_{i=1}^{r} 2^2}\right)$$
$$= 2\exp\left(\frac{-t^2}{8r}\right) \qquad (2.2.30)$$

It follows that,

$$\begin{aligned}&\Pr\left(W \geq (\textsc{opt} - \delta_1)r \text{ and } S \leq (\textsc{opt} - \delta_2)r\right)\\&\leq \Pr\left(\left|W - \sum_{j=1}^{r} \mathbb{E}[W_j|H_{j-1}]\right| = |W - S| \geq (\delta_2 - \delta_1)r\right)\\&\leq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right)\end{aligned} \tag{2.2.31}$$

□

2.2.4 Proof of Lemma 2.1.2

Restatement of Lemma 2.1.2

Imagine a single use of protocol P_{r,n,h,δ_1}. If

$$\Pr\left(|\{l : S_l \geq (\textsc{opt} - \delta_2)r\}| \geq (1-s)n|\, Win = 1\right) \leq 1 - d$$

Then,

$$(ds - h)\Pr\left(Win = 1\right) \leq 2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right)$$

Proof of Lemma 2.1.2

Proof. Recall that

$$Win \equiv 1\left[|\{l : Win_l = 1\}| \geq (1-h)n\right] = 1. \tag{2.2.32}$$

By linearity of expectation we have that

$$\frac{1}{n}\sum_{l=1}^{n}\Pr(Win_l = 1|Win = 1) = \frac{1}{n}\mathbb{E}\left[\sum_{l=1}^{n}\frac{1}{\Pr(Win = 1)}\cdot 1\,[Win = Win_l = 1]\right]$$
$$\geq (1-h)\cdot\mathbb{E}\left[\frac{1}{\Pr(Win = 1)}\cdot 1\,[|\{l : Win_l = 1\}| \geq (1-h)n]\right] = (1-h)\frac{\Pr(Win = 1)}{\Pr(Win = 1)} = 1-h$$

So,

$$\frac{1}{n}\sum_{l=1}^{n}(1 - \Pr(Win_l = 1|Win = 1)) \leq h \tag{2.2.33}$$

Also by linearity of expectation

$$\frac{1}{n}\sum_{l=1}^{n}\Pr(S_l \geq (\text{OPT} - \delta_2)r|Win = 1) = \frac{1}{n}\sum_{l=1}^{n}\frac{1}{\Pr(Win = 1)}\mathbb{E}\left[1\left[S_l \geq (\text{OPT} - \delta_2)r \text{ and } Win = 1\right]\right]$$
$$\leq \frac{1}{\Pr(Win = 1)}\mathbb{E}\left[1\left[|\{l : S_l \geq (\text{OPT} - \delta_2)r\}| \geq (1-s)n \text{ and } Win = 1\right]\right]$$
$$+ (1-s)\frac{1}{\Pr(Win = 1)}\mathbb{E}\left[1\left[|\{l : S_l \geq (\text{OPT} - \delta_2)r\}| \leq (1-s)n \text{ and } Win = 1\right]\right]$$
$$= \Pr\left(|\{l : S_l \geq (\text{OPT} - \delta_2)r\}| \geq (1-s)n|\, Win = 1\right)$$
$$+ (1-s)\left(1 - \Pr\left(|\{l : S_l \geq (\text{OPT} - \delta_2)r\}| \geq (1-s)n|\, Win = 1\right)\right) \leq (1-d) + (1-s)d = 1 - ds$$

So,

$$1 - \frac{1}{n}\sum_{l=1}^{n}\Pr(S_l \geq (\text{OPT} - \delta_2)r|Win = 1) = \frac{1}{n}\sum_{l=1}^{n}(1 - \Pr(S_l \geq (\text{OPT} - \delta_2)r|Win = 1))$$
$$= \frac{1}{n}\sum_{l=1}^{n}\Pr(S_l \leq (\text{OPT} - \delta_2)r|Win = 1) \geq ds \tag{2.2.34}$$

It follows by combining equations 2.2.33 and 2.2.34 that there exists an $l' \in [n]$ such that

$$\begin{aligned}
&\Pr\left(Win_{l'} = 1 \text{ and } S_{l'} \leq (\textsc{opt} - \delta_2)r \middle| Win = 1\right) \\
&\geq \Pr(S_{l'} \leq (\textsc{opt} - \delta_2)r | Win = 1) - (1 - \Pr(Win_{l'} = 1 | Win = 1)) \\
&\geq \frac{1}{n}\sum_{l=1}^{n} (\Pr(S_l \leq (\textsc{opt} - \delta_2)r | Win = 1) - (1 - \Pr(Win_l = 1 | Win = 1))) \\
&\geq ds - h \qquad (2.2.35)
\end{aligned}$$

By combining equation 2.2.35 with Lemma 2.1.1 we get

$$\begin{aligned}
&2\exp\left(\frac{-r(\delta_2 - \delta_1)^2}{8}\right) \geq \Pr\left(Win_{l'} = 1 \text{ and } S_{l'} \leq (\textsc{opt} - \delta_2)r \middle| Win = 1\right) \cdot \Pr(Win = 1) \\
&\geq \Pr(Win = 1)(ds - h) \qquad (2.2.36)
\end{aligned}$$

□

2.2.5 Proof of Lemma 2.1.3

Restatement of Lemma 2.1.3

Suppose, for some $\delta > 0$, that we have a probability distribution $P(x_1, ..., x_n)$ on n-bit strings $\vec{x} = (x_1, ..., x_n) \in \{0,1\}^n$ such that for all $i \in [n]$

$$\|P(x_1, .., x_i) - P(x_1, ..., x_{i-1}) \cdot P_{\frac{1}{2}}(x_i)\|_1 \leq \delta$$

Here, $P_{\frac{1}{2}}$ is the uniform distribution on a single bit. It follows that

$$H_{\infty}^{6\sqrt{\delta}}(\vec{x}) \geq -\log\left(\frac{1}{1 - 3\sqrt{\delta}}\right) - \frac{n}{4}\log\left(\frac{1}{2} + \sqrt{\delta}\right)$$

Proof of Lemma 2.1.3

Proof. Note that

$$
\begin{aligned}
\delta &\geq \|P(x_1,..,x_i) - P(x_1,...,x_{i-1}) \cdot P_{\frac{1}{2}}(x_i)\|_1 \\
&= \sum_{(x_1,...,x_{i-1}) \in \{0,1\}^{i-1}} \sum_{x_i \in \{0,1\}} \left| P(x_1,..,x_i) - P(x_1,...,x_{i-1}) \cdot P_{\frac{1}{2}}(x_i) \right| \\
&= \sum_{(x_1,...,x_{i-1}) \in \{0,1\}^{i-1}} \sum_{x_i \in \{0,1\}} \left| P(x_1,..,x_{i-1}) \cdot P(x_i|x_1,...,x_{i-1}) - P(x_1,...,x_{i-1}) \cdot P_{\frac{1}{2}}(x_i) \right| \\
&= \sum_{(x_1,...,x_{i-1}) \in \{0,1\}^{i-1}} P(x_1,..,x_{i-1}) \cdot \|P(x_i|x_1,...,x_{i-1}) - P_{\frac{1}{2}}(x_i)\|_1 \qquad (2.2.37)
\end{aligned}
$$

Let us denote the probability distribution $P(x_i = x|x_1 = y_1, ..., x_{i-1} = y_{i-1})$ by $P_{y_1,...,y_{i-1}}(x)$. Given a string $\vec{y} = (y_1, ..., y_n) \in \{0,1\}^n$, we say that $\vec{y}$ is γ-Bad at site i if $\|P_{y_1,...,y_{i-1}}(x) - P_{\frac{1}{2}}(x)\|_1 \geq \gamma$, and γ-Good otherwise.

So for any i, and for $\vec{y}$ sampled from the distribution P, we see from the above equation and Markov's inequality that

$$
\mathbb{E}\left[I\left[\vec{y} \text{ is } \sqrt{\delta}\text{-Bad at site } i\right]\right] = \Pr\left(\vec{y} \text{ is } \sqrt{\delta}\text{-Bad at site } i\right) \leq \sqrt{\delta}
$$

By linearity of expectation we have that

$$
\mathbb{E}\left[\sum_{i=1}^{n} I\left[\vec{y} \text{ is } \sqrt{\delta}\text{-Bad at site } i\right]\right]
$$

$$
= \sum_{i=1}^{n} \mathbb{E}\left[I\left[\vec{y} \text{ is } \sqrt{\delta}\text{-Bad at site } i\right]\right] \leq n\sqrt{\delta}
$$

Once again using Markov's inequality we have that

$$
\Pr\left(\vec{y} \text{ is } \sqrt{\delta}\text{-Bad at more than } \lfloor n/2 \rfloor \text{ sites}\right) \leq \frac{n}{\lfloor n/2 \rfloor}\sqrt{\delta} \leq 3\sqrt{\delta}
$$

If $\vec{y}$ is not $\sqrt{\delta}$-Bad at more than $\lfloor n/2 \rfloor$ sites, then it is $\sqrt{\delta}$-Good at more than $\lfloor n/2 \rfloor$ sites. This means that, for more than $\lfloor n/2 \rfloor$ sites i we have $\|P_{y_1,...,y_{i-1}}(x) - P_{\frac{1}{2}}(x)\|_1 \leq \sqrt{\delta}$, and thus $\left|P_{y_1,...,y_{i-1}}(x = y_i) - \frac{1}{2}\right| \leq \sqrt{\delta}$, so $P_{y_1,...,y_{i-1}}(x = y_i) \leq \frac{1}{2} + \sqrt{\delta}$. It follows that (for $\vec{x}$

chosen according to the probability distribution P):

$$\Pr(\vec{x} = \vec{y}) = \prod_{i=1}^{n} P(x_i = y_i | x_1 = y_1, ..., x_{i-1} = y_{i-1}) = \prod_{i=1}^{n} P_{y_1,...,y_{i-1}}(x_i = y_i) \leq \left(\frac{1}{2} + \sqrt{\delta}\right)^{\lfloor n/2 \rfloor}$$

Thus, in order to modify the distribution on $\vec{x}$ induced by P to produce another distribution P' with $H_\infty(P') \geq -\log\left(\frac{1}{1-3\sqrt{\delta}}\left(\frac{1}{2} + \sqrt{\delta}\right)^{\lfloor n/2 \rfloor}\right) \geq -\log\left(\frac{1}{1-3\sqrt{\delta}}\right) - \frac{n}{4}\log\left(\frac{1}{2} + \sqrt{\delta}\right)$ we only need to take all the probability mass at any $\vec{y}$ that is $\sqrt{\delta}$-Bad at more than $\lfloor n/2 \rfloor$ sites and redistribute it over the remaining values of $\vec{y}$ in a manner proportional to the probability mass already at those values of $\vec{y}$. The above work shows that we move a total $3\sqrt{\delta}$ units of probability mass during this process, since there are only $3\sqrt{\delta}$ units of probability mass at all the "Bad" values of $\vec{y}$ combined. Moreover, it is evident that this process is equivalent to deleting the probability mass at all values of $\vec{y}$ that are $\sqrt{\delta}$-Bad at more than $\lfloor n/2 \rfloor$ sites, and re-normalizing the remaining probability mass to be a distribution. Since all the remaining values of $\vec{y}$ are $\sqrt{\delta}$-Good at at least $\lfloor n/2 \rfloor$ sites, it follows that the probability distribution P' which is produced this way has

$$\max_{\vec{y}} P'(\vec{x} = \vec{y}) \leq \frac{1}{1 - 3\sqrt{\delta}}\left(\frac{1}{2} + \sqrt{\delta}\right)^{\lfloor n/2 \rfloor}$$

and the Min-Entropy bound on P' follows (here the $\frac{1}{1-3\sqrt{\delta}}$ factor represents the largest possible renormalization factor). Moreover, we moved at most $3\sqrt{\delta}$ probability mass to transform P into P', so $||P - P'||_1 \leq 6\sqrt{\delta}$. Thus,

$$H_\infty^{6\sqrt{\delta}}(P) \equiv H_\infty^{6\sqrt{\delta}}(\vec{x}) \geq -\log\left(\frac{1}{1 - 3\sqrt{\delta}}\right) - \frac{n}{4}\log\left(\frac{1}{2} + \sqrt{\delta}\right)$$

□

Bibliography

[Cir80] B. S. Cirel'Son. Quantum generalizations of bell's inequality b.s. cirel'son. 4:93–100, 1980.

[CK11] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and ...*, pages 1–11, 2011.

[CN] I. Chuang and M. Nielsen. *Quantum Computation and Quantum Information.*

[Col09] R. Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, (December), 2009.

[CVY13] M. Coudron, T. Vidick, and H. Yuen. Robust Randomness Amplifiers: Upper and Lower Bounds. *arXiv preprint arXiv:1305.6626*, (0844626):1–28, 2013.

[FGS13] S. Fehr, R. Gelles, and C. Schaffner. Security and composability of randomness expansion from Bell inequalities. *Physical Review A*, pages 1–12, 2013.

[PAM10] S. Pironio, A. Acín, and S. Massar. Random numbers certified by Bell's theorem. *Nature*, pages 1–26, 2010.

[PM13] S. Pironio and S. Massar. Security of practical private randomness generation. *Physical Review A*, pages 1–18, 2013.

[RUV12] B. Reichardt, F. Unger, and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. *arXiv preprint arXiv:1209.0448*, 2012.

[VV11] U. Vazirani and T. Vidick. Certifiable Quantum Dice-Or, testable exponential randomness expansion. *Arxiv preprint arXiv:1111.6054*, pages 1–21, 2011.