Some limits on non-local randomness expansion

Matt Coudron and Henry Yuen

December 12, 2012

1 Introduction

> God does not play dice.
> *–Albert Einstein*

> Einstein, stop telling God what to do.
> *–Niels Bohr*

One of the defining features of quantum mechanics is that quantum systems can exhibit non-local behavior that cannot be reproduced by any classical theory obeying locality (i.e. special relativity). Recently, non-locality has been a subject of special interest in quantum computing and in theoretical computer science; the attempt to pin down the power and limitations of non-local behavior has led to advances in the understanding of quantum cryptography, the complexity of quantum interactive proof systems, and the properties of quantum entanglement.

A beautiful new development in quantum information theory has been the concept of *certified randomness*, pioneered by Roger Colbeck in his Ph.D. thesis. The motivating question is this: is it possible to test that the output of a physical device is random? For example, there are companies that purportedly sell devices that generate random bits via quantum mechanical means – one would like to check that their purchased device is behaving as advertised! However, for most definitions of "test" and "random", this seems to be a hopeless task.

Surprisingly, with the help of non-locality, and *two* devices, we can meaningfully and rigorously test that the devices produce random bits! The idea is to separate the devices so that they cannot communicate with one another, and then test the devices for non-local behavior according to some protocol. If the devices pass the test, then they must be producing random bits *by necessity*. These random bits are then *certified*.

The protocols constructed in Colbeck's Ph.D. thesis [1], as well as [3], [4], are based on testing that the two devices win certain quantum games. One famous quantum game, which [3] and [4] use, is the *CHSH game*: two non-communicating players, Alice and Bob, are given random inputs $x, y \in \{0, 1\}$ respectively. Their task is to produce outputs $a, b \in \{0, 1\}$ such that $a \oplus b = x \wedge y$. It is easy to see that if Alice and Bob play according to a classical strategy, their maximum success probability is 75%. On the other hand, there is a quantum strategy strategy involving a shared

entangled state between Alice and Bob that allows them to win this game with probability $\approx 85\%$. The key insight is that if Alice and Bob are winning CHSH games with superclassical winning probability (i.e. greater than 75%), they must be randomized!

These protocols can do more than just certify randomness – they can *expand* it. The protocol presented in [3] uses n bits of randomness, and the devices produce $\Omega(n^2)$ bits of certified randomness (ostensibly generated via quantum means). In a breakthrough paper, Vazirani and Vidick [4] give a protocol that takes n bits of seed randomness and stretches it to $\exp(n)$ random bits. A striking property of the Vazirani-Vidick (VV) protocol is that its correctness does not depend on correctness of quantum mechanics! That is, as the referee operating the VV protocol, you do not need to believe in the validity of quantum mechanics in order to believe that the device outputs are random – you only need to trust that it is possible to prevent the devices from communicating, for example by spatially separating the boxes.

The natural next question is: how much randomness expansion can we get? Doubly exponential? An unbounded amount? We address the question of upper bounds on randomness expansion protocols in this work.

1.1 Our results

We obtain partial answers to the upper bound question, and also present a variant of the Vazirani-Vidick protocol that achieves better parameters. We refer to the two devices as Alice and Bob.

Upper bounds. We show that in restricted setting where the protocol is nonadaptive, performs its tests in a special "product" fashion, and can be passed by Alice and Bob with probability 1, the amount of certifiable randomness is at most doubly exponential in the seed length. This is proved by exhibiting a strategy for Alice and Bob to cheat and pass the tests without expanding the seed randomness by more than a doubly exponential amount.

We then consider a specialized protocol that is again nonadaptive, performs "product" tests, and the tests specifically are for the CHSH game. We prove that in the setting where Alice and Bob are not restricted to quantum strategies, but can use more general *non-signaling strategies*, they can employ a cheating strategy so that the protocol can only guarantee singly exponential randomness expansion!

This latter result shows that natural generalizations of the Vazirani-Vidick protocol, along with its analysis, are essentially *optimal*. This is because the VV analysis only use the fact that Alice and Bob are employing non-signaling strategies. Any asymptotic improvement to the randomness expansion of a VV-like protocol would necessarily require that quantum arguments be used!

Lower bounds. We present a partial converse to the first upper bound, by exhibiting a randomness expansion protocol that is nonadaptive, performs "product" tests, and can be passed by Alice and Bob with probability 1. In particular, we modify the VV protocol so that it uses another quantum game, called the Magic Square game, instead of the CHSH game. This protocol also guarantees singly exponential randomness expansion, but achieves better parameters. In particular, this protocol achieves constant **rate** (defined in Section 2), while the VV protocol has rate $\Omega(1/\text{polylog}(n))$, which tends to 0 as the seed length grows. The protocol and analysis also benefit by being cleaner.

1.2 Organization

We begin by giving some definitions in Section 2. Then, we present our upper bounds on specializations of non-adaptive protocols in Section 3. We then give our simplified variant of the Vazirani-Vidick protocol in Section 4. Finally, we conclude with some open problems.

2 Definitions

Definition 2.1. *A **nonadaptive protocol** with m rounds is a game with two non-signaling players $\mathcal{A}$ and $\mathcal{B}$ and a referee $\mathcal{R}$. At the beginning of the game, the referee has a random seed $s \in \{0,1\}^n$. He uses a pair of question functions (Q_A, Q_B) to generate the input sequences $\vec{X} = Q_A(s), \vec{Y} = Q_B(s)$. For each round $i \in [m]$ in the game, the referee will give inputs $\vec{X}_i$ and $\vec{Y}_i$ to $\mathcal{A}$ and $\mathcal{B}$ respectively, and collect their respective outputs $A_i, B_i \in \Sigma$. At the end of the protocol, the referee will apply a test $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B})$ to decide whether to accept or reject. The output of the protocol is the pair of sequences $(\vec{A}, \vec{B})$.*

Definition 2.2. *Let $N = 2^n$. For a pair of question functions $Q = (Q_A, Q_B)$, define the **input matrix** $M(Q) \in (\Sigma \times \Sigma)^{m \times N}$ to be such that $M(Q)_{i,s} = (Q_A(s)_i, Q_B(s)_i)$.*

Without loss of generality, we can imagine that the referee selects the input sequences $\vec{X}$ and $\vec{Y}$ by choosing a column of $M(Q)$ uniformly at random.

Definition 2.3 (Min Entropy)**.** *Let X be a discrete random variable. The min-entropy of X, denoted $H_\infty(X)$, is defined as* $\min_x \log(1/\Pr[X = x])$.

Definition 2.4 (Non-signaling distribution)**.** *A joint probability distribution $p(A, B, X, Y)$ over random variables A, B, X, Y is **non-signaling** with respect to $(A, X), (B, Y)$ iff the following properties hold:*

1. *For all $a \in \mathrm{Supp}(A), x \in \mathrm{Supp}(X), y \in \mathrm{Supp}(Y)$, $p(a \mid x, y) = p(a \mid x)$.*
2. *For all $b \in \mathrm{Supp}(B), x \in \mathrm{Supp}(X), y \in \mathrm{Supp}(Y)$, $p(b \mid x, y) = p(b \mid y)$.*

Definition 2.5 (Quantum distribution)**.** *A non-signaling distribution $p(A, B, X, Y)$ with respect to $(A, X), (B, Y)$ is a **quantum distribution** iff there exists an $d \in \mathbb{N}$ such that a $2d$-qubit shared entangled state $|\psi\rangle \in \mathbb{C}^{2^d} \otimes \mathbb{C}^{2^d}$, and a set of measurement operators $\{M_a^x\}$ on the first d qubits, and $\{M_b^y\}$ on the second d qubits, with the property that $p(a, b \mid x, y) = \langle\psi| M_a^x \otimes M_b^y |\psi\rangle$.*

Let S be a strategy for $\mathcal{A}$ and $\mathcal{B}$ in a nonadaptive protocol. Let $\mathrm{WIN}(S)$ denotes the event that $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B}) = 1$, if $\mathcal{A}$ and $\mathcal{B}$ play according to strategy S.

Definition 2.6. *A $(c, s, m, f(n), \epsilon)$-**non-signaling randomness expansion protocol** is a nonadaptive protocol with m rounds and n bits of seed randomness such that the following holds:*

- *(Completeness) There exists a non-signaling strategy S (not necessarily quantum) such that if $\mathcal{A}$ and $\mathcal{B}$ play according to S, then*

$$\Pr[\mathrm{WIN}(S)] \geq c,$$

- *(Soundness) For every non-signaling strategy S, if* $\Pr[\mathrm{WIN}(S)] \geq s$, *then* $H_\infty(\vec{A}, \vec{B} \mid \vec{X}, \vec{Y}, \mathrm{WIN}(S)) \geq f(n)$.

Definition 2.7. *A $(c, s, m, f(n))$-**quantum randomness expansion protocol** is a nonadaptive protocol with m rounds and n bits of seed randomness such that the following holds:*

- *(Completeness) There exists a quantum strategy S such that if $\mathcal{A}$ and $\mathcal{B}$ play according to S, then*
$$\Pr[\mathrm{WIN}(S)] \geq c,$$
- *(Soundness) For every quantum strategy S, if* $\Pr[\mathrm{WIN}(S)] \geq s$, *then* $H_\infty(\vec{A}, \vec{B} \mid \vec{X}, \vec{Y}, \mathrm{WIN}) \geq f(n)$.

Definition 2.8 (Randomness expansion rate)**.** *Let P be a $(c, s, m, f(n))$-randomness expansion protocol (either quantum or non-signaling). The **rate** of P is defined to be $(f(n) - n)/m$.*

Informally, the rate of a randomness expansion protocol is a measure of how much "bit per buck" you get out of the protocol. The higher the rate, the more randomness is produced on average per round. This is an important quantity to consider, especially for those who are renting randomness expansion boxes by the hour.

Definition 2.9. *Consider a nonadaptive protocol where the referee's test R is of a special form: there exists a subtest $T : \Sigma^4 \to \{0,1\}$ and a function $g : \{0,1\}^m \to \{0,1\}$ such that $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B}) = g\left(T(\vec{X}_1, \vec{Y}_1, \vec{A}_1, \vec{B}_1), ..., T(\vec{X}_i, \vec{Y}_i, \vec{A}_i, \vec{B}_i), ..., T(\vec{X}_m, \vec{Y}_m, \vec{A}_m, \vec{B}_m)\right)$. Call this a **product protocol**.*

Definition 2.10. *We now define a simplified product protocol in which $g(\vec{v}) \equiv$ **AND** $\vec{v} = \prod_i v_i$, so that $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B}) = \prod_i T(\vec{X}_i, \vec{Y}_i, \vec{A}_i, \vec{B}_i)$. Call this an **"AND" protocol**.*

Definition 2.11 (CHSH game)**.** *The **CHSH game** is a two-player game with two non-communicating players, Alice and Bob, who are given random inputs $x, y \in \{0,1\}$ respectively. Their task is to produce outputs $a, b \in \{0,1\}$ such that $a \oplus b = x \wedge y$.*

Definition 2.12. *Consider a product protocol in which $\vec{X}, \vec{Y}, \vec{A}, \vec{B} \in \{0,1\}^m$, and $T(X, Y, A, B) = 1 \oplus X \wedge Y \oplus A \oplus B$. Note that $T(X, Y, A, B) = 1$ if and only inputs X, Y and outputs A, B satisfy the success criterion for the CHSH game. We will refer to such a protocol as a **CHSH product protocol**.*

3 Nonadaptive Upper Bounds

The following theorem gives a sense in which doubly exponential randomness expansion is a natural upper bound on certain randomness expansion protocols.

Theorem 3.1. *Let P be a $(1, s, m, f(n))$-quantum randomness expansion "AND" protocol. Then $f(n) \leq |\Sigma|^{2^{n+1}} \cdot (2 \log |\Sigma|)$.*

Proof. If $m \leq |\Sigma|^{2^{n+1}}$, then the theorem statement is trivially true. Suppose $m > |\Sigma|^{2^{n+1}}$. Now we present a cheating quantum strategy S' that passes the referee's test with probability 1, but the output Shannon entropy is at most $|\Sigma|^{2^{n+1}} \cdot (2 \log |\Sigma|)$ (and hence the output min-entropy is bounded by the same amount).

Since P has completeness 1, there exists a strategy S such that $\Pr[\mathrm{WIN}(S) = 1]$. In the background, $\mathcal{A}$ and $\mathcal{B}$ will maintain a concurrent simulation of strategy S, where at each round i, $\mathcal{A}$ and $\mathcal{B}$ relay the referee's inputs X_i and Y_i to strategy S, and secretly record the outputs $\hat{A}_i$ and $\hat{B}_i$ determined by S.

At each round i, $\mathcal{A}$ and $\mathcal{B}$ examine the input matrix $M(Q)$. If $M(Q)_{i,*} = M(Q)_{j,*}$ for some $j < i$ (i.e. the ith row of the input matrix is identical to a previous row), $\mathcal{A}$ and $\mathcal{B}$ will simply repeat the outputs A_j and B_j, respectively – call these rounds the **repeat rounds**. Otherwise, $\mathcal{A}$ and $\mathcal{B}$ will produce outputs $\hat{A}_i$ and $\hat{B}_i$ according to strategy S – call these the **honest rounds**.

We claim that if $\mathcal{A}$ and $\mathcal{B}$ play according to this strategy, they will win with probability 1. It is clear that for the honest rounds i, $\Pr[T(X_i, Y_i, A_i, B_i) = 1] = 1$. But this is also true in the repeat rounds. Let i be such a round. Let $j < i$ be the smallest such that $M(Q)_{i,*} = M(Q)_{j,*}$. Note that at round j, $\mathcal{A}$ and $\mathcal{B}$ played according to S, so $\Pr[T(X_j, Y_j, A_j, B_j) = 1] = 1$.

It follows that regardless of the value of the referee's random seed, $X_i = X_j$ and $Y_i = Y_j$. S' mandates that $A_i = A_j$ and $B_i = B_j$ in this case. Thus, $T(X_i, Y_i, A_i, B_i) = T(X_j, Y_j, A_j, B_j)$, so $\Pr[T(X_i, Y_i, A_i, B_i) = 1] = \Pr[T(X_j, Y_j, A_j, B_j) = 1] = 1$. Thus $\Pr[\prod_i T(\vec{X}_i, \vec{Y}_i, \vec{A}_i, \vec{B}_i) = 1] = 1$.

Finally, we show that the output Shannon entropy is at most $|\Sigma|^{2^{n+1}}$. Let i be a repeat round. It is clear that $H(A_i, B_i \mid A_{<i}, B_{<i}, X, Y) = 0$, because $A_i = A_j$ and $B_i = B_j$ as random variables for some $j < i$. For a honest round i, $H(A_i, B_i \mid A_{<i}, B_{<i}, X, Y) \leq H(A_i, B_i) \leq 2 \log |\Sigma|$.

Noting the dimensions of $M(Q)$, we see that there can be at most $|\Sigma|^{2^{n+1}}$ distinct rows in $M(Q)$, and hence there at most $|\Sigma|^{2^{n+1}}$ honest rounds. By using the chain rule for Shannon entropy,

$$\begin{aligned} H(A, B \mid X, Y) &= \sum_i H(A_i, B_i \mid A_{<i}, B_{<i}, X, Y) \\ &= \sum_{i \text{ honest}} H(A_i, B_i \mid A_{<i}, B_{<i}, X, Y) + \sum_{i \text{ repeat}} H(A_i, B_i \mid A_{<i}, B_{<i}, X, Y) \\ &\leq |\Sigma|^{2^{n+1}} \cdot (2 \log |\Sigma|). \end{aligned}$$

We now note that the Shannon entropy of a random variable is an upper bound for the min-entropy of a random variable, and the theorem statement follows.

□

Lemma 3.2. *There exists a non-signaling strategy that wins a single CHSH game with probability 1.*

Proof. Labeling the inputs to the game as X and Y respectively, imagine that the players $\mathcal{A}$ and $\mathcal{B}$ select their outputs (A and B, resp.) according to the following distribution (which we will show is non-signaling):

If $X \wedge Y = 1$ they select outputs $(A, B) = (1, 0)$, or $(A, B) = (0, 1)$ each with probability $\frac{1}{2}$. If $X \wedge Y = 0$ they select ouputs $(A, B) = (0, 0)$, or $(A, B) = (1, 1)$, again each with probability $\frac{1}{2}$. It now follows easily that, regardless of the values of A,B, X, and Y we have

$$p(A \mid X, Y) = p(A \mid X) = \frac{1}{2}$$

and

$$p(B \mid X, Y) = p(B \mid Y) = \frac{1}{2}$$

Thus, the above strategy is non-signaling by definition.

□

Theorem 3.3. *Let P be a $(c, s, m, f(n))$-non-signaling randomness expansion CHSH "AND" protocol. Then $f(n) \leq 2^{2n+2}$.*

Proof. By assumption $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B}) = \prod_i T(\vec{X}_i, \vec{Y}_i, \vec{A}_i, \vec{B}_i) = \prod_i \left(1 \oplus \vec{X}_i \wedge \vec{Y}_i \oplus \vec{A}_i \oplus \vec{B}_i\right)$. We will now give a strategy that can be used by the non-signaling players $\mathcal{A}$ and $\mathcal{B}$ to ensure that $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B}) = 1$ with probability 1. The strategy will have the additional property that all of the output pairs $(\vec{A}_i, \vec{B}_i)$, except for at most 2^n values of i, are deterministic functions of the outputs (as random variables) of a particular set of 2^{2n} previous games. We will see that this proves the desired result.

Let us consider the rows of the input matrix $M(Q) \in (\{0, 1\}^2)^{m \times 2^n}$ as vectors $M(Q)_{i,*} \in \mathbb{F}_2^{2 \cdot 2^n} = \mathbb{F}_2^{2^{n+1}}$. Note that the input matrix $M(Q)$, and all of its columns, are deterministic objects known to $\mathcal{A}$, $\mathcal{B}$, and $\mathcal{R}$ before the protocol begins. Of course, $\mathcal{R}$'s random seed determines which column of $M(Q)$ is chosen as input, and is known only to $\mathcal{R}$ at the beginning of the protocol. During the course of the protocol non-signaling players $\mathcal{A}$ and $\mathcal{B}$ will keep track of dependencies among the rows of $M(Q)$ by updating a set I. At the beginning of the protocol $I = \phi$. When $\mathcal{A}$ and $\mathcal{B}$ receive the i^{th} input, they first check to see if row $M(Q)_{i,*}$ is linearly indepedent (as a vector in $\mathbb{F}_2^{2^{n+1}}$) from $\{M(Q)_{j,*} : j < i\}$. If so, they will update I by adding the number i to it (note that $\mathcal{A}$ and $\mathcal{B}$ can do this indepedently and without communicating; in this sense there are actually two sets I, owned by $\mathcal{A}$ and $\mathcal{B}$ respectively, but these sets will always be identical since they are updated by $\mathcal{A}$ and $\mathcal{B}$ in an identical manner).

Additionally, if $M(Q)_{i,*}$ is linearly indepedent from $\{M(Q)_{j,*} : j < i\}$, $\mathcal{A}$ and $\mathcal{B}$ will use the non-signaling strategy described in Lemma 3.2 to play the CHSH game with inputs $\vec{X}_i$, and $\vec{Y}_i$ respectively (note that, while the rows of M do not depend on $\mathcal{R}$'s random seed, the specific inputs do; see Definition2.1, and Definition 2.2). This strategy produces outputs A and B and we know that $T(\vec{X}_i, \vec{Y}_i, A, B) = 1 \oplus \vec{X}_i \wedge \vec{Y}_i \oplus A \oplus B = 1$ with probability 1. $\mathcal{A}$ and $\mathcal{B}$ then report A and B respectively as their outputs to $\mathcal{R}$ for the i^{th} round (so $\vec{A}_i = A$ and $\vec{B}_i = B$). Before moving on to the next round $\mathcal{A}$ and $\mathcal{B}$ now play a series of private games and store the outcomes without reporting them to $\mathcal{R}$. For every $j \in I$ with $j < i$ (starting from the smallest such j and proceeding to the highest), and $\mathcal{A}$ and $\mathcal{B}$ will play the CHSH game using the non-signaling strategy defined in

Lemma 3.2 with inputs $\vec{X}_i$, $\vec{Y}_j$ and store the outputs. We will denote $\mathcal{A}$'s output for this game by A_{ij} and $\mathcal{B}$'s by B_{ij}. We know that, with probability 1, $T(\vec{X}_i, \vec{Y}_j, A, B) = 1 \oplus \vec{X}_i \wedge \vec{Y}_j \oplus A_{ij} \oplus B_{ij} = 1$. $\mathcal{A}$ and $\mathcal{B}$ perform the same process with inputs $\vec{X}_j$ and $\vec{Y}_i$ as well, and denote their outputs A_{ji} and B_{ji} respectively. After all of this is done, they move on to next input pair given by $\mathcal{R}$.

Suppose $\mathcal{A}$ and $\mathcal{B}$ encounter a row $M(Q)_{i,*}$ of $M(Q)$ that is linearly dependent on the rows $\{M(Q)_{j,*} : j < i\}$. It is easy to prove by induction that (with the current set I) the set $\{M(Q)_{j,*} : j \in I\}$ forms an indepedent basis (over $\mathbb{F}_2^{2^{n+1}}$) for $\{M(Q)_{j,*} : j \leq i\}$. Thus, there exists a subset $J \subset I$ such that $M(Q)_{i,*} = \sum_{j \in J} M(Q)_{j,*}$, and it follows that, regardless of the value of random seed chosen by $\mathcal{R}$, $(\vec{X}_i, \vec{Y}_i) = \sum_{j \in J} (\vec{X}_j, \vec{Y}_j) = (\sum_{j \in J} \vec{X}_j, \sum_{j \in J} \vec{Y}_j)$. Knowing this, $\mathcal{A}$ and $\mathcal{B}$ now wish to produce output values A and B respectively (without communicating), such that

$$\begin{aligned} &T(\vec{X}_i, \vec{Y}_i, A, B) = 1 \oplus \vec{X}_i \wedge \vec{Y}_i \oplus A \oplus B = 1 \\ &\iff A \oplus B = \vec{X}_i \wedge \vec{Y}_i = \sum_{j \in J} \vec{X}_j \wedge \sum_{j \in J} \vec{Y}_j = \sum_{(k,j) \in J^2} \vec{X}_k \wedge \vec{Y}_j \end{aligned} \tag{1}$$

To accomplish this, $\mathcal{A}$ outputs $A = \sum_{(k,j) \in J^2} A_{kj}$ and $\mathcal{B}$ outputs $B = \sum_{(k,j) \in J^2} B_{kj}$, where the values of the summands have been previously stored as described above. We thus know that, for each $(k, j) \in J^2 \subset I^2$

$$T(\vec{X}_k, \vec{Y}_j, A_{kj}, B_{kj}) = 1 \oplus \vec{X}_k \wedge \vec{Y}_j \oplus A_{kj} \oplus B_{kj} = 1 \iff A_{kj} \oplus B_{kj} = \vec{X}_k \wedge \vec{Y}_j \tag{2}$$

It follows that

$$\begin{aligned} A \oplus B &= \sum_{(k,j) \in J^2} A_{kj} \oplus \sum_{(k,j) \in J^2} B_{kj} = \sum_{(k,j) \in J^2} A_{kj} \oplus B_{kj} \\ &= \sum_{(k,j) \in J^2} \vec{X}_k \wedge \vec{Y}_j = \sum_{j \in J} \vec{X}_j \wedge \sum_{j \in J} \vec{Y}_j = \vec{X}_i \wedge \vec{Y}_i \\ &\iff T(\vec{X}_i, \vec{Y}_i, A, B) = 1 \oplus \vec{X}_i \wedge \vec{Y}_i \oplus A \oplus B = 1 \end{aligned} \tag{3}$$

as desired.

Thus, by following this strategy for every row $M(Q)_{i,*}$ of $M(Q)$ we have shown that $T(\vec{X}_i, \vec{Y}_i, \vec{A}_i, \vec{B}_i) = 1 \oplus \vec{X}_i \wedge \vec{Y}_i \oplus \vec{A}_i \oplus \vec{B}_i = 1$ for all $i \in [m]$ with probability 1. It follows that $R(\vec{X}, \vec{Y}, \vec{A}, \vec{B}) = 1$ with probability 1. Furthermore, every output in the entire protocol is a deterministic function of the set of outputs $\{A_{i,j}, B_{i,j} : (i, j) \in I^2\}$ (Here I denotes the value of the set I at the end of the protocol after all the relevant indices have been added). Since this set contains exactly $|I^2| = |I|^2$ random variables, each of which has the range $\{0, 1\}$, the entire set can have entropy at most $|I|^2$.

It follows easily that $H_\infty(\vec{A},\vec{B} \mid \vec{X},\vec{Y},\text{WIN}(S)) \leq H(\vec{A},\vec{B} \mid \vec{X},\vec{Y},\text{WIN}(S)) \leq H(\vec{A},\vec{B}) \leq |I|^2$. Thus, we must have $f(n) \leq |I|^2$.

We now note that, since all of the rows of $M(Q)$ lie in $\mathbb{F}_2^{2^{n+1}}$, which is a 2^{n+1}-dimensional vector space, any set of $2^{n+1}+1$ or more rows of $M(Q)$ must be linearly dependent. It follows easily that if, during the course of the protocol, I ever grows to contain 2^{n+1} indices, then it will never grow further for the rest of the protocol. Thus, at the end of the protocol we have $|I| \leq 2^{n+1}$. It follows that $f(n) \leq |I|^2 \leq 2^{2n+2}$ and we are done.

□

Corollary 3.4. *Let P be a $(c,s,m,f(n))$-non-signaling randomness expansion CHSH product protocol with $c > 0$. Then $f(n) \leq 2^{n+1}$.*

Proof. In the proof of Theorem 3.3 we saw that $\mathcal{A}$ and $\mathcal{B}$ a have non-signaling strategy that allows them to pass each inidividual CHSH test with probability 1, and produce at most 2^{n+1} bits of entropy in their outputs. We now want a similar proof which allows $\mathcal{A}$ and $\mathcal{B}$ to win against any CHSH product test (rather than just the AND) test. Suppose that the test is given by

$$R(\vec{X},\vec{Y},\vec{A},\vec{B}) = g\left(T(\vec{X}_1,\vec{Y}_1,\vec{A}_1,\vec{B}_1),...,T(\vec{X}_i,\vec{Y}_i,\vec{A}_i,\vec{B}_i),...,T(\vec{X}_m,\vec{Y}_m,\vec{A}_m,\vec{B}_m)\right)$$

for some function $g : \{0,1\}^m \to \{0,1\}$. Since $c > 0$ we know that $\mathcal{R}$ cannot reject every vector of wins and losses, so there must exist some $v \in \{0,1\}^m$ such that $g(v) = 1$.

Since g is known to everyone before the beginning of the protocol, $\mathcal{B}$ can find such a v deterministically before the start of the protocol (for example, choose the smallest v, comparing binary strings as integers, such that $g(v) = 1$). With this v, we will now have $\mathcal{A}$ and $\mathcal{B}$ pursue exactly the same strategy that they did in Thoerem 3.3 except that, just before reporting the answer to the i^{th} round, $\mathcal{B}$ will look at v_i. If $v_i = 1$ then $\mathcal{B}$ will report the answer he has measured using the strategy from Theorem 3.3 (and we will thus know that $T(\vec{X}_i,\vec{Y}_i,\vec{A}_i,\vec{B}_i) = 1$). If $v_i = 0$ then $\mathcal{B}$ will report the opposite of the answer he would have if he had used the strategy from Theorem 3.3, and we will know that $T(\vec{X}_i,\vec{Y}_i,\vec{A}_i,\vec{B}_i) = 1 + 1 = 0$.

Playing this way, it is clear that at the end of the protocol, we will have

$$R(\vec{X},\vec{Y},\vec{A},\vec{B}) = g\left(T(\vec{X}_1,\vec{Y}_1,\vec{A}_1,\vec{B}_1),...,T(\vec{X}_i,\vec{Y}_i,\vec{A}_i,\vec{B}_i),...,T(\vec{X}_m,\vec{Y}_m,\vec{A}_m,\vec{B}_m)\right) = g(v) = 1$$

and thus $\mathcal{A}$ and $\mathcal{B}$ will pass $\mathcal{R}$'s test with probability 1. Furthermore, since $\mathcal{A}$ and $\mathcal{B}$ have only applied determinisitc functions (depending only v which was known to all before the algorithm) to the outputs that they would have produced using the strategy from Theorem 3.3, we see that their outputs in this strategy can still only have 2^{n+1} bits of entropy. It follows that $f(n) \leq 2^{n+1}$. □

4 A Randomness Expansion Scheme based on the Magic Square Game

4.1 Introduction

In the preceding section, we saw an argument for why randomness expansion protocols that 1) have perfect completeness, 2) use nonadaptive inputs, and 3) check that the boxes $\mathcal{A}$ and $\mathcal{B}$ win *all* of the rounds – which we formally defined to be quantum randomness "AND" protocols – are subject to a doubly-exponential upper bound on the randomness expansion. In other words, if the protocol is of the form described, and only uses n bits of seed, there is a strategy for the boxes to pass the protocol and produce no more than $\exp(\exp(O(n)))$ bits of min-entropy.

We now show a partial converse, that there *exist* randomness expansion schemes of this form. While our scheme does not match the upper bound, it still produces an exponential amount of randomness. We modify the Vazirani-Vidick (VV) protocol to perform tests based on the **Magic Square Game**, and stretches n seed bits to produce $\exp(O(n))$ bits of min-entropy. The VV protocol tests are based on the CHSH game, which cannot be won perfectly, even by quantum players. Consequently, the VV protocol has to break up the rounds into *blocks*, and test that the CHSH correlations are satisfied within each block, that is, the players won $\approx 85\%$ of the rounds in each block. Ultimately, they have a protocol with $O(\ell \log^2 \ell)$ rounds, using $\Theta(\log \ell)$ bits of seed, that is guaranteed to produce $\Omega(\ell)$ bits of min-entropy, so the rate is $\Omega(1/\text{polylog}(\ell))$.

The Magic Square-variant of the VV protocol achieves much better rate: it runs in $O(\ell)$ rounds using $\Theta(\log \ell)$ bits of seed, producing $\Omega(\ell)$ bits of entropy, so we achieve $\Omega(1)$ rate for the protocol – much more "bit for our buck"! Furthermore, the analysis of the Magic Square variant is slightly cleaner than the CHSH variant.

4.2 The Magic Square Game

We describe the Magic Square game, also known as the Mermin-Peres magic square game.

Consider a 3×3 matrix, and suppose that one is asked to fill in each entry with 1 or 0, with the constraint that each row must have even parity and each column must have odd parity. Clearly, there is no such assignment that satisfies all the constraints, because while the row constraints imply that the sum of the entries has even parity, while the column constraints imply that the sum has odd parity, a contradiction.

Now consider the following 2 player game: the referee chooses an $x \in [6]$ uniformly at random, interpreted as choosing a row or column of a 3×3 matrix at random. Then, the referee chooses a $y \in [3] \times [3]$ that corresponds to a random entry in the row/colum x. For example, conditioned on $x = 1$, then y is uniform over the set $\{(1,1),(1,2),(1,3)\}$, the entries in the first row. We will call this the **Magic Square input distribution**.

The referee sends x to Alice, and solicits Alice for an assignment $a \in \{0,1\}^3$ to the entries in that row/column. Simultaneously, the referee sends y to Bob and solicits Bob for an assignment $b \in \{0,1\}$ to entry y. The referee checks that Alice's answer satisfies the parity constraint, and

Alice's answer is consistent with Bob's.

From the foregoing discussion, it is easy to see that there is no classical strategy for Alice and Bob to successfully pass the referee's test with probability 1; in fact, the best classical strategy wins with probability at most 17/18. However, there *is* a quantum strategy for Alice and Bob to win with probability 1. We refer the reader to [2] for details on this quantum strategy.

4.3 Simplifying the VV protocol

We now describe a randomness expansion scheme based on the Magic Square game. The Magic Square input distribution over $[6] \times ([3] \times [3])$ is the one described in the foregoing section. For Alice's answer $a \in \{0,1\}^3$ and Bob's answer $b \in \{0,1\}$, the Magic Square win condition $R(x, y, a, b)$ is satisfied iff a satisfies the parity condition (depending on whether x corresponded to a row or a column) and a is consistent with b.

Magic Square Randomness Expansion Protocol

Let ℓ, Δ be given as input, and let $m = \Delta\ell$.
Choose $T \subseteq [m]$ uniformly at random by selecting each position independently with probability $1/\ell$.
for $i = 1 \dots m$ **do**
    if $i \in T$ **then**
        Choose x, y from the Magic Square input distribution.
        Distribute x to $\mathcal{A}$ and y to $\mathcal{B}$.
        Collect outputs $a \in \{0,1\}^3, b \in \{0,1\}$ from $\mathcal{A}$ and $\mathcal{B}$, respectively.
    else
        Set $x = y = 1$ and distribute to $\mathcal{A}$ and $\mathcal{B}$.
        Collect outputs $a \in \{0,1\}^3, b \in \{0,1\}$ from $\mathcal{A}$ and $\mathcal{B}$, respectively.
    end if
    If the Magic Square win condition is not satisfied, abort.
end for
If the protocol has not aborted, accept.

Call the rounds in T as "Bell rounds", ones where the inputs to the boxes are randomized. This protocol uses $O(\Delta \log \ell)$ bits of randomness. We will prove that this protocol generates $\Omega(\ell)$ bits of min-entropy. The improvement in the randomness rate over the original VV protocol comes from the fact that the input sequences consist of blocks of size $\Omega(\log^2 \ell)$ (and their test checks that the players won $\approx 85\%$ of the rounds *within each block*), but they still prove that the output has $\Omega(\ell)$ bits of entropy, so their randomness rate goes to 0 with ℓ.

Theorem 4.1. *There exists a constant $C > 1$ such that the following holds. Let $\epsilon > 0$. Set $\Delta = 10^3 \lceil \log(1/\epsilon) \rceil$ and $\ell = Cn$. Suppose $\mathcal{A}$ and $\mathcal{B}$ are two non-signaling players that execute Magic Square Randomness Expansion protocol. Then,*

- *Either $H_\infty^\epsilon(B \mid \text{WIN}) \geq n$,*

- *Or* $\Pr[\text{WIN}] \leq \epsilon$,

where B denotes the output of $\mathcal{B}$ in the protocol, and WIN *denotes the event that the Magic Square win condition is satisfied for all rounds.*

The proof of this theorem closely mirrors the analysis in the VV paper. We briefly sketch the argument. It proceeds by contradiction: suppose that the boxes $\mathcal{A}$ and $\mathcal{B}$ were able to pass the protocol with probability greater than ϵ but the output min-entropy is small. Then, it must be that there is a Bell round i_0 where the output of $\mathcal{B}$ in round i_0 is nearly deterministic, conditioned on some past values. This follows from Claim 6 in the VV paper:

Claim 4.2 (Claim 6 in VV)**.** *There exists a constant $C > 1$ such that the following holds. Let n be such that $m = C\Delta n$. Let $2^{-Cn} < \epsilon < 1/5$. Suppose that the boxes utilize a strategy S to play the Magic Square protocol, and that 1) $H_\infty^\epsilon(B \mid \text{WIN}) \leq n$ and 2) $\Pr[\text{WIN}] \geq \epsilon$. Then for all large enough n there exists a round i_0 that is a Bell round and an output sequence $b \in \{0,1\}^*$ of $\mathcal{B}$ such that the following holds:*

- *b is a possible winning output sequence of $\mathcal{B}$:*

$$\Pr[B = b, \text{WIN}] > 0,$$

- *$\mathcal{B}$'s output in the i_0th Bell round is essentially deterministic:*

$$\Pr[B_{i_0} \mid \text{WIN}_{<i_0}, B_{<i_0} = b_{<i_0}] \geq 0.99,$$

- *The* WIN *condition is satisfied with high probability in the i_0th Bell round:*

$$\Pr[\text{WIN}_{i_0} \mid \text{WIN}_{<i_0}, B_{<i_0} = b_{<i_0}] \geq 0.9,$$

where B_j denotes the output of $\mathcal{B}$ at round j, $B_{<j}$ denotes the output of $\mathcal{B}$ up to round j, WIN_j *denotes the event that the Magic Square win condition is satisfied for round j, and* $\text{WIN}_{<j}$ *denotes the event that the Magic Square win condition is satisfied up to and including round $j-1$.*

We now reduce to a particular guessing game, in which two non-signaling players Clara and David receive random inputs, and Clara has to guess David's input. Given that there is a "nearly deterministic" round i_0 (conditioned on some past values) in the Magic Square protocol, we devise a strategy for Clara to guess David's input with probability better than chance, which violates the non-signaling assumption on Clara and David. This will establish Theorem 4.1.

Before describing the reduction itself, we describe the guessing game in more detail.

4.4 The Guessing Game

The guessing game is as follows: Clara and David are non-signaling players, and are given inputs x and y from the Magic Square input distribution. They both win if Clara outputs David's input.

Clearly, the maximum winning probability is 1/3: Clara's best strategy is to randomly guess an entry in her given row.

The following is an adaptation of Lemma 5 in the VV paper to the Magic Square game, showing that the conditions provided by Claim 4.2 are enough to allow Clara and David to beat the guessing game.

Claim 4.3. *Let $\beta, \gamma > 0$ be such that $\beta + \gamma < 1/5$. Suppose a given pair of boxes $\mathcal{A}$ and $\mathcal{B}$ taking inputs x, y from the Magic Square input distribution produce outputs $a \in \{0,1\}^3, b \in \{0,1\}$. Suppose the following conditions hold:*

1. *$\mathcal{B}$'s output is nearly deterministic: there exists a $b^* \in \{0,1\}$ such that $\Pr[B = b^*] \geq 1 - \gamma$; and*
2. *The boxes output satisfy the Magic Square win condition with high probability: $\Pr[\text{WIN}] \geq 1 - \beta$.*

Then there is a strategy for two non-signaling players Clara and David, using boxes $\mathcal{A}$ and $\mathcal{B}$, to win the guessing game with probability strictly greater than $1/3$.

Proof. Consider the following strategy: On input x, Clara runs $\mathcal{A}$ on x and records its output as $a = (a_1, a_2, a_3)$. On input y, David runs $\mathcal{B}$ on y (and doesn't need to record any output). Clara then uniformly selects an index i such that $a_i = b^*$, and outputs the coordinate of the ith entry in the row/column denoted by x (i.e. outputs an element of $[3] \times [3]$). If there is no such index, Clara then aborts the protocol.

Without loss of generality, assume that the Magic Square win condition is the following: the parity of a row must be $1 \oplus b^*$ and the parity of a column must be b^*. Condition on $B = b^*$ and WIN. If x corresponds to a row, it must be the case that two of the three a_i's equal b^*. If x is a column, it must be the case that either one or three a_i's equal b^*. In that case, with probability at least $(1/2)(1/2 + 1/3) = 5/12$ Clara will guess y correctly. Taking into account the conditioning,

$$\begin{aligned}\Pr[\text{Clara guesses } y] &\geq \Pr[\text{Clara guesses } y \mid B = b^*, \text{WIN}] \cdot \Pr[B = b^*, \text{WIN}] \\ &\geq \frac{5}{12} \cdot (1 - \beta - \gamma) \\ &> 1/3,\end{aligned}$$

where the last inequality follows from our condition on β and γ. □

We finish by showing the reduction to the guessing game.

4.5 Reduction to the guessing game

Suppose that there is a strategy S for the Magic Square protocol where the output entropy is low but $\mathcal{A}$ and $\mathcal{B}$ win with non-negligible probability. Take an output sequence $b^* \in \{0,1\}^*$ with the properties promised by Claim 4.2. The players Clara and David can take the boxes $\mathcal{A}$ and $\mathcal{B}$

respectively, and repeatedly simulate the Magic Square randomness expansion protocol up to and including round $i_0 - 1$, until the conditions $\text{WIN}_{<i_0}$ and $B_{<i_0} = b_{<i_0}$ are met. This is possible because $\Pr[B = b^*, \text{WIN}] > 0$.

Once they have achieved this state, the boxes $\mathcal{A}$ and $\mathcal{B}$ are now *primed* for use in the guessing game. Clara and David will abscond with the primed boxes $\mathcal{A}$ and $\mathcal{B}$ and separate themselves. They then play the guessing game above. Observe that the conditions of Claim 4.3 are met: since i_0 is a Bell round, $\mathcal{A}$ and $\mathcal{B}$ will receive inputs from the Magic Square input distribution. Furthermore, b^* is a nearly deterministic output sequence, the boxes win with high probability, and $\beta + \gamma < 0.11 < 1/5$.

Then, by Claim 4.3, Clara and Bob will win the guessing game with impossible probability. Thus, Theorem 4.1 holds.

5 Open Questions

The most obvious open problem is to prove upper bounds for more general protocols, say, all non-adaptive ones, without assuming anything about the nature of the referee tests. An even more ambitious goal would be to prove upper bounds for adaptive protocols, where the inputs to the devices might depend on the players' outputs. It seems completely plausible that this might be a means of attaining *infinite* expansion!

However, tackling these problems seem to require techniques beyond those presented here, which crucially use the fact that the tests are structured. It appears that more general methods, such as information theoretic arguments, will be needed.

Acknowledgements. We wish to thank Scott Aaronson for teaching his excellent class, Quantum Complexity Theory, without which this project would not have happened. Finally, we would like to give profuse thanks to Thomas Vidick for having many helpful discussions with us.

References

[1] R. Colbeck, *Quantum and Relativistic Protocols For Secure Multi-Party Computation*. Ph.D. thesis, Trinity college, University of Cambridge, November 2009.

[2] R. Cleve, P. Hoyer, B. Toner, J. Watrous. Consequences and Limits of Nonlocal Strategies. *Computational Complexity*, 2004 (236-249).

[3] S. Pironio, A. Acin, S. Massar, et al. Random Numbers Certified by Bell's Theorem. *Nature*, 464(7291):10, 2010.

[4] U. Vazirani, V. Vidick. Certifiable quantum dice - Or, exponential randomness expansion. *Philosophical Transactions of the Royal Society A*. (2010) 370, 3432-3448.