Randomness in nonlocal games between mistrustful players

Carl A. Miller
National Institute of Standards and Technology
100 Bureau Dr., Gaithersbug, MD 20899, USA

Yaoyun Shi
Department of Electrical Engineering and Computer Science
University of Michigan, Ann Arbor, MI 48109, USA

March 10, 2017

Abstract

If two quantum players at a nonlocal game G achieve a superclassical score, then their measurement outcomes must be at least partially random from the perspective of any third player. This is the basis for device-independent quantum cryptography. In this paper we address a related question: does a superclassical score at G guarantee that one player has created randomness from the perspective of the other player? We show that for complete-support games, the answer is yes: even if the second player is given the first player's input at the conclusion of the game, he cannot perfectly recover her output. This implies that some amount of *local* randomness (i.e., randomness possessed by only one player) can always be obtained when randomness is certified by nonlocal games. We discuss potential implications for cryptographic protocols between mistrustful parties.

1 Introduction

When two quantum parties Alice and Bob play a nonlocal game G and achieve a score that exceeds the best classical score $\omega_c(G)$, their outputs must be at least partially random. In other words, all Bell inequality violations certify the existence of randomness. This fact is at the center of protocols for device-independent quantum cryptography, where untrusted devices are used to perform cryptographic procedures. In particular, this notion of certification is the basis for device-independent *randomness expansion*, where a small random seed is converted into a much larger uniformly random output by repeating Bell violations [3, 19, 4, 27, 20, 10, 5, 6, 17, 16, 9, 1].

A natural question arises: is new randomness also generated by one player from the perspective of the other player? Specifically, if X denotes Alice's outputs, Z denotes the post-measurement state that Bob has at the conclusion of the game, and F denotes all side information (including Alice's input), is there a certified lower bound for the conditional entropy $H(X \mid ZF)$? Besides helping us understand the nature of certified randomness, this particular kind of randomness (local randomness) has applications in mutually mistrustful cryptographic settings, where Alice and Bob are cooperating but have different interests.

Quantifying local randomness (i.e., randomness that is only known to one player) is challenging because many of the known tools do not apply. Lower bounds for the total randomness (i.e, randomness from the perspective of an outside adversary) have been computed as a function of the degree of the Bell violation (see Figure 2 in [19]) but are not directly useful for certifying local randomness. One of the central challenges is that we are measuring randomness from the perspective of an active, rather than passive, adversary: Bob's guess at Alice's output occurs after Bob has carried out his part of the strategy for G. Current tools for device-independent randomness expansion are not designed to address the case where the adversary is a participant in the nonlocal game.

Does the generation of certified randomness always involve the generation of *local* certified randomness? The answer is not obvious: for example, in the non-signaling setting, Alice and Bob could share a PR-box[1] which generates 1 bit of certified randomness per use, but no new local randomness – Bob could perfectly guess Alice's output from his own if he were given Alice's input.

Motivated by the above, we prove the following result in this paper (see Theorem 14 for a formal statement).

Theorem 1 (Informal)**.** *For any complete-support game*[2] *G, there is a constant $C_G > 0$ such that the following holds. Suppose Alice and Bob use a strategy for G which achieves a score that is δ above the best classical score (with $\delta > 0$). Then, at the conclusion of the strategy and given Alice's input, Bob can guess her output with probability at most $(1 - \delta^2/C_G)$.*

We note that similar problems have been studied in the literature in settings different from ours. There has been other work showing upper bounds on the probability that a third party can guess Alice's output after a game (e.g., [18], [13]) and single-round games have appeared where Bob is sometimes given only Alice's input, and asked to produce her output (e.g., [14], [26], [29]). (We believe the novelty of our scenario in comparison to these papers is that when consider the randomness of Alice's output *after* Bob has performed his part of a quantum strategy, and thus has potentially lost information due to measurement.) Two recent papers also address randomness between multiple players, under assumptions about imperfect storage [12, 21].

In addition to the above, we prove a structural theorem for quantum strategies that allow perfect guessing by Bob. Not only do such strategies not achieve Bell inequalities, but they are also *essentially classical* in the following sense. Let D, E denote the quantum systems possessed by Alice and Bob, respectively

Theorem 2 (Informal)**.** *Suppose that Alice's and Bob's strategy is such that if the game G is played and then Bob is given Alice's input, he can perfectly guess her output. Then, there is an isometry mapping Bob's system to $E_1 \otimes E_2$ such that Bob's strategy for G involves only E_1, and all of Alice's observables commute with the reduced state on DE_1.*

(See Theorem 5 and Corollary 7 for a formal statement.) Thus, in the case of perfect guessing, the strategy is equivalent to one in which Alice's measurements have no effect on the shared state.

1.1 Structure of the paper

We begin with the case of perfect guessing. We formalize the concept of an essentially classical strategy, using a definition of equivalence between strategies which is similar to definitions used in results on quantum rigidity. We then give the proof of Theorem 2. It is known that two sets of mutually commuting measurements on a finite-dimensional space be expressed as the pullback of bipartite measurements. This fact is used along with matrix algebra arguments to show the necessary splitting of Bob's system into $E_1 \otimes E_2$.

Then we proceed with the proof of Theorem 1. It has been observed by previous work (e.g., [14], [28]) that if a measurement $\{P_i\}$ on a system D from bipartite state ρ_{DE} are highly predictable via measurements on E, then the measurement does not disturb the reduced state by much: $\sum_i P_i \rho_D P_i \sim \rho_D$. In this paper we give a simplified proof of that fact (Proposition 11). The interesting consequence for our purpose is that if Alice's measurements are highly predictable to Bob, then Alice can copy out her measurement outcomes in advance, thus making her strategy approximately classical. We take this a step further, and show that if Bob first performs his own measurement on E the resulting classical-quantum correlation is also approximately preserved by Alice's measurements (which is not necessarily true of the original entangled state ρ_{AB}). This is sufficient to show that an approximately-guessable strategy yields an approximately classical strategy.

The subtleties in the proof are in establishing the error terms that arise when Alice copies out multiple measures from her side of the state. We note that the proof crucially requires that the game G has complete support. An interesting further avenue is to explore how local randomness may break down if the condition is not satisfied.

In section 5 we discuss the implications of our result.

[1] That is, the unique 2-part non-signaling resource whose input bits a, b and output bits x, y always satisfy $x \oplus y = a \wedge b$

[2] That is, a game in which each input pair occurs with nonzero probability.

2 Preliminaries

For any finite-dimensional Hilbert space V, let $L(V)$ denote the vector space of linear automorphisms of V. For any $M, N \in L(V)$, we let $\langle M, N \rangle$ denote $\mathrm{Tr}[M^* N]$. If $S \subseteq V$ is a subspace of V, let $\mathbf{P}_S \in L(V)$ denote orthogonal projection onto V.

Throughout this paper we fix four disjoint finite sets $\mathcal{A}, \mathcal{B}, \mathcal{X}, \mathcal{Y}$, which denote, respectively, the first player's input alphabet, the second player's input alphabet, the first player's output alphabet, and the second player's output alphabet. A 2-*player (input-output) correlation* is a vector (p_{ab}^{xy}) of nonnegative reals, indexed by $a, b, x, y \in \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y}$, satisfying $\sum_{xy} p_{ab}^{xy} = 1$ for all pairs (a, b), and satisfying the condition that the quantities

$$p_a^x := \textstyle\sum_y p_{ab}^{xy}, \qquad p_b^y := \textstyle\sum_x p_{ab}^{xy} \tag{1}$$

are independent of b and a, respectively (no-signaling).

A 2-player game is a pair (q, H) where

$$q \colon \mathcal{A} \times \mathcal{B} \to [0, 1] \tag{2}$$

is a probability distribution and

$$H \colon \mathcal{A} \times \mathcal{B} \times \mathcal{X} \times \mathcal{Y} \to [0, 1] \tag{3}$$

is a function. If $q(a, b) \neq 0$ for all $a \in \mathcal{A}$ and $b \in \mathcal{B}$, the game is said to have a *complete support*. The expected score associated to such a game for a 2-player correlation (p_{ab}^{xy}) is

$$\sum_{a,b,x,y} q(a, b) H(a, b, x, y) p_{ab}^{xy}. \tag{4}$$

We will extend notation by writing $q(a) = \sum_b q(a, b)$, $q(b) = \sum_a q(a, b)$, and $P_q(a \mid b) = q(a, b)/q(b)$ (if $q(b) \neq 0$).

A 2-*player strategy* is a 5-tuple

$$\Gamma \quad = \quad (D, E, \{\{R_a^x\}_x\}_a, \{\{S_b^y\}_y\}_b, \gamma) \tag{5}$$

such that D, E are finite dimensional Hilbert spaces, $\{\{R_a^x\}_x\}_a$ is a family of $\mathcal{X}$-valued positive operator valued measures (POVMs) on D (indexed by $\mathcal{A}$), $\{\{S_b^y\}_y\}_b$ is a family of $\mathcal{Y}$-valued positive operator valued measures on E, and γ is a density operator on $D \otimes E$. The *second player states* ρ_{ab}^{xy} of Γ is defined by

$$\rho_{ab}^{xy} \quad := \quad \mathrm{Tr}_D \left[\sqrt{R_a^x \otimes S_b^y} \gamma \sqrt{R_a^x \otimes S_b^y} \right] \tag{6}$$

Define ρ_a^x by the same expression with S_b^y replaced by the identity operator. (These represent the pre-measurement states of the second-player.) Define $\rho := \mathrm{Tr}_D(\gamma) = \sum_x \rho_a^x$ for any a.

We say that the strategy Γ *achieves* the 2-player correlation (p_{ab}^{xy}) if $p_{ab}^{xy} = \mathrm{Tr}[\gamma(R_a^x \otimes S_b^y)]$ for all a, b, x, y. If a 2-player correlation (p_{ab}^{xy}) can be achieved by a 2-player strategy then we say that it is a *quantum* correlation.

If (p_{ab}^{xy}) is a convex combination of product distributions (i.e., distributions of the form $(q_a^x) \otimes (r_b^y)$ where $\sum_x q_a^x = 1$ and $\sum_y r_b^y = 1$) then we say that (p_{ab}^{xy}) is a *classical* correlation. Note that if the underlying state of a quantum strategy is separable (i.e., it is a convex combination of bipartite product states) then the correlation it achieves is classical. The maximum expected score that can be achieved for a game G by a classical correlation is denoted $\omega_c(G)$.

3 Perfect Guessing

3.1 Congruent strategies

It is necessary to identify pairs of strategies that are essentially the same from an operational standpoint. We use a definition that is similar to definitions from quantum self-testing (e.g., Definition 2.13 in [15]).

A *unitary embedding* from a 2-player strategy

$$\Gamma \quad = \quad (D, E, \{\{R_a^x\}_x\}_a, \{\{S_b^y\}_y\}_b, \gamma) \tag{7}$$

to another 2-player strategy

$$\overline{\Gamma} \quad = \quad (\overline{D}, \overline{E}, \{\{\overline{R}_a^x\}_x\}_a, \{\{\overline{S}_b^y\}_y\}_b, \overline{\gamma}) \tag{8}$$

is a pair of unitary embeddings $i\colon D \hookrightarrow \overline{D}$ and $j\colon E \hookrightarrow \overline{E}$ such that $\overline{\gamma} = (i \otimes j)\gamma(i \otimes j)^*$, $R_a^x = i^* \overline{R}_a^x i$, and $S_b^y = j^* \overline{S}_b^y j$.

Additionally, if Γ is such that $D = D_1 \otimes D_2$, and $R_a^x = G_a^x \otimes I$ for all a, x, then we will call the strategy given by

$$(D_1, E, \{\{G_a^x\}_a\}_x, \{\{S_b^y\}_y\}_b, \mathrm{Tr}_{D_2}\gamma) \tag{9}$$

a *partial trace* of Γ. We can similarly define a partial trace on the second subspace E if it is a tensor product space.

We will say that two strategies Γ and Γ' are *congruent* if there exists a sequence of strategies $\Gamma = \Gamma_1, \ldots, \Gamma_n = \Gamma'$ such that for each $i \in \{1, \ldots, n-1\}$, either Γ_{i+1} is a partial trace of Γ_i, or vice versa, or there is a unitary embedding of Γ_i into Γ_{i+1}, or vice versa. This is an equivalence relation. Note that if two strategies are congruent then they achieve the same correlation.

3.2 Essentially classical strategies

We are ready to define the key concept in this paper and to state formally our main theorem.

Definition 3. *A quantum strategy (5) is said to be* essentially classical *if it is congruent to one where γ commutes with R_a^x for all x and a.*

We are interested in strategies after the application of which Bob can predict Alice's output given her input. This is formalized as follows. If $\chi_1, \ldots, \chi_n$ are positive semidefinite operators on some finite dimensional Hilbert space V, then we say that $\{\chi_1, \ldots, \chi_n\}$ is *perfectly distinguishable* if χ_i and χ_j have orthogonal support for any $i = j$. This is equivalent to the condition that there exists a projective measurement on V which perfectly identifies the state from the set $\{\chi_1, \ldots, \chi_n\}$.

Definition 4. *A quantum strategy (5)* allows perfect guessing *(by Bob) if for any a, b, y, $\{\rho_{ab}^{xy}\}_x$ is perfectly distinguishable.*

Theorem 5 (Main Theorem)**.** *If a strategy for a complete-support game allows perfect guessing, then it is essentially classical.*

(We note that the converse of the statement is not true. This is because even in a classical strategy, Alice's output may depend on some local randomness, which Bob cannot perfectly predict.)

Before giving the proof of this result, we note the following proposition, which taken together with Theorem 5 implies that any strategy that permits perfect guessing yields a classical correlation.

Proposition 6. *The correlation achieved by an essentially classical strategy must be classical.*

Proof. We need only to consider the case that γ commutes with R_a^x for all a, x. For each $a \in \mathcal{A}$, let $V_a = \mathbb{C}^{\mathcal{X}}$, and let $\Phi_a \colon L(D) \to L(V_a \otimes D)$ be the nondestructive measurement defined by

$$\Phi_a(T) \quad = \quad \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes \sqrt{R_a^x} T \sqrt{R_a^x}. \tag{10}$$

Note that by the commutativity assumption, such operation leaves the state of DE unchanged.

Without loss of generality, assume $\mathcal{A} = \{1, 2, \ldots, n\}$. Let $\Lambda \in L(V_1 \otimes \ldots \otimes V_n \otimes D \otimes E)$ be the state that arises from applying the superoperators $\Phi_1, \ldots, \Phi_n$, in order, to γ. For any $a \in \{1, \ldots, n\}$, the reduced state $\Lambda^{V_a E}$ is precisely the same as the result of taking the state γ, applying the measurement $\{R_a^x\}_x$ to D, and recording the result in V_a. Alice and Bob can therefore generate the correlation (p_{ab}^{xy}) from the marginal state $\Lambda^{V_1 \cdots V_n E}$ alone (if Alice possesses $V_1, \ldots, V_n$ and Bob possesses E). Since this state is classical on Alice's side, and therefore separable, the result follows. □

Corollary 7. *If a strategy for a complete-support game allows perfect guessing, the correlation achieved must be classical.* □

3.3 Proving Theorem 5

The proof will proceed as follows. First, we show that Alice's measurements $R_a := \{R_a^x\}_x$ induce projective measurements $Q_a := \{Q_a^x\}_x$ on Bob's system. Next, we argue that Q_a commutes with Bob's own measurement $S_b := \{S_b^y\}_y$ for any b. This allows us to isometrically decompose Bob's system into two subsystems $E_1 \otimes E_2$, such that S_b acts trivially on E_2, while E_2 alone can be used to predict x given a. The latter property allows us to arrive at the conclusion that R_a commutes with γ_{DE_1}.

We will need the following lemma, which is commonly used in studying two-player quantum strategies. The proof was sketched in [24] (see also Theorem 1 in [22]).

Lemma 8. *Let V be a finite-dimensional Hilbert space and let $\{M_j\}$ and $\{N_k\}$ be sets of positive semidefinite operators on V such that $M_j N_k = N_k M_j$ for all j, k. Then, there exists a unitary embedding $i \colon V \hookrightarrow V_1 \otimes V_2$ and positive semidefinite operators $\{\overline{M}_j\}$ on V_1 and $\{\overline{N}_k\}$ on V_2 such that $M_j = i^*(\overline{M}_j \otimes \mathbb{I})i$ and $N_k = i^*(\mathbb{I} \otimes \overline{N}_k)i$ for all j, k.*

Proof of Theorem 5: Express Γ as in (5). Without loss of generality, we may assume that Supp $\rho = E$. By the assumption that Γ allows perfect guessing, for any a, the second-player states $\{\rho_a^x\}_x$ must be perfectly distinguishable (since otherwise the post-measurement states $\{\rho_{ab}^{xy}\}_x$ would not be). Therefore, we can find projective measurements $\{\{Q_a^x\}_x\}_a$ on E such that

$$Q_a^x \rho Q_a^x = \rho_a^x. \tag{11}$$

Note that for any fixed a, if the measurements $\{R_a^x\}_a$ and $\{Q_a^x\}_a$ are applied to γ, the outcome is always the same.

We have that the states

$$\rho_{ab}^{xy} \quad = \quad \overline{S_b^y} Q_a^x \rho Q_a^x \quad \overline{S_b^y} \tag{12}$$

$$\rho_{ab}^{x'y} \quad = \quad \overline{S_b^y} Q_a^{x'} \rho Q_a^{x'} \quad \overline{S_b^y} \tag{13}$$

have orthogonal support for any $x = x'$. Since Supp $\rho = E$, we have $c\mathbb{I} \leq \rho$ for some $c > 0$. Therefore,

$$\left\langle \quad \overline{S_b^y} c Q_a^x \quad \overline{S_b^y}, \quad \overline{S_b^y} c Q_a^{x'} \quad \overline{S_b^y} \right\rangle \quad = \quad 0, \tag{14}$$

which implies, using the cyclicity of the trace function,

$$\left\| Q_a^x S_b^y Q_a^{x'} \right\|_2 \quad = \quad 0. \tag{15}$$

Therefore, the measurements $\{Q_a^x\}_x$ and $\{S_b^y\}_y$ commute for any a, b.

By Lemma 8, we can find a unitary embedding $i\colon E \hookrightarrow E_1 \otimes E_2$ and such that $S_b^y = i^*(\overline{S}_b^y \otimes \mathbb{I})i$ and $Q_a^x = i^*(\mathbb{I} \otimes \overline{Q}_a^x)i$, for measurements $\{\overline{S}_b^y\}_y$ and $\{\overline{Q}_a^x\}_x$. With

$$\overline{\gamma} = (\mathbb{I}_D \otimes i)\gamma(\mathbb{I}_D \otimes i^*), \tag{16}$$

the strategy Γ embeds into the strategy

$$\Gamma' := \left(D, E_1 \otimes E_2, \{\{R_a^x\}_x\}_a, \{\overline{S}_b^y \otimes \mathbb{I}_{E_2}\}_y\}_b, \overline{\gamma}\right).$$

For any fixed a, the state $\overline{\gamma}$ is such that applying the measurement $\{R_a^x\}_x$ to the system D and the measurement $\{\overline{Q}_a^x\}_x$ to the system E_2 always yields the same outcome. In particular, if we let

$$\tau_a^x \quad = \quad \mathrm{Tr}_{E_2}\left(\overline{Q}_a^x \overline{\gamma}\right), \tag{17}$$

then $\mathrm{Tr}[R_a^{x'}\tau_a^x]$ will always be equal to 1 if $x = x'$ and equal to 0 otherwise. Therefore $\{R_a^x\}_x$ commutes with the operators $\{\tau_a^x\}_x$, and thus also with their sum $\sum_x \tau_a^x = \mathrm{Tr}_{E_2}\overline{\gamma}$.

Thus if we trace out the strategy Γ' over the system E_2, we obtain a strategy (congruent to the original strategy Γ) in which Alice's measurement operators commute with the shared state. □

4 Approximate Guessing

Definition 9. *Let $\{\rho_i\}_{i=1}^n$ denote a finite set of positive semidefinite operators on a finite dimensional Hilbert space V. Then, let*

$$\mathrm{Dist}\{\rho_i\} \quad = \quad \max_i \quad \mathrm{Tr}(T_i\rho_i), \tag{18}$$

where the maximum is taken over all POVMs $\{T_i\}_{i=1}^n$ on V.

Note that if $\sum_i \mathrm{Tr}(\rho_i) = 1$, and each ρ_i is nonzero, then this quantity has the following interpretation: if Alice gives Bob a state from the set $\{\rho_i/\mathrm{Tr}(\rho_i)\}$ at random according to the distribution $(\mathrm{Tr}(\rho_i))_i$, then $\mathrm{Dist}\{\rho_i\}$ is the optimal probability that Bob can correctly guess the state. This quantity is well-studied (see, e.g., [23]).

Definition 10. *Let $\Phi\colon L(V) \to L(V)$ denote a completely positive trace-preserving map over a finite-dimensional Hilbert space V. Let $\beta \in L(V)$ denote a density operator on V. Then we say that Φ **is ϵ-commutative with β if***

$$\|\Phi(\beta) - \beta\|_1 \quad \leq \quad \epsilon. \tag{19}$$

Note that this relation obeys a natural triangle inequality: if Φ_1 is ϵ_1-commutative with β, and Φ_2 is ϵ_2-commutative with β, then

$$\begin{aligned} \|\Phi_2(\Phi_1(\beta)) - \rho\|_1 &\leq \|\Phi_2(\Phi_1(\beta)) - \Phi_2(\beta)\|_1 + \|\Phi_2(\beta) - \beta\|_1 \\ &\leq \|\Phi_1(\beta) - \beta\|_1 + \epsilon_2 \\ &\leq \epsilon_1 + \epsilon_2. \end{aligned}$$

The following proposition will be an important building block. Our proof is a significant simplification of a method from Lemma 29 in [28]. (See also Lemma 2 in [14] for a related result.)

Proposition 11. *Let $\Lambda \in L(A \otimes B)$ be a density operator and $\{F_i\}_{i=1}^n$ a projective measurement on A such that the induced states $\Lambda_i^B := \mathrm{Tr}_A(F_i\Lambda)$ satisfy*

$$\mathrm{Dist}\{\Lambda_i^B\} \quad = \quad 1 - \delta. \tag{20}$$

Then, the superoperator $X \mapsto \sum_i F_i X F_i$ is $(2\sqrt{\delta} + \delta)$-commutative with $\Lambda^A := \mathrm{Tr}_B\Lambda$.

Proof. By assumption, there exists a POVM $\{G_i\}$ on B such that

$$\sum_i \mathrm{Tr}[(F_i \otimes G_i)\Lambda] \quad = \quad 1 - \delta. \tag{21}$$

By standard arguments, we can assume without loss of generality that that $\{G_i\}$ is a projective measurement and that Λ is pure.[3]

There is a linear map $M\colon \mathbb{C}^s \to \mathbb{C}^r$ such that $\mathrm{Tr}_A\Lambda = M^*M$ and $\rho = \mathrm{Tr}_B\Lambda = MM^*$. Upon choosing an appropriate basis for A and B, we can write M with a block form determined by the spans of $\{F_i\}$ and $\{G_j\}$:

$$M \quad = \quad \left[\begin{array}{c|c|c|c} M_{11} & M_{12} & \cdots & M_{1n} \\ \hline M_{21} & M_{22} & \cdots & M_{2n} \\ \hline \vdots & & \ddots & \\ \hline M_{n1} & M_{n2} & \cdots & M_{nn} \end{array}\right]. \tag{22}$$

Let

$$\overline{M} \quad = \quad \left[\begin{array}{c|c|c|c} M_{11} & 0 & \cdots & 0 \\ \hline 0 & M_{22} & \cdots & 0 \\ \hline \vdots & & \ddots & \\ \hline 0 & 0 & \cdots & M_{nn} \end{array}\right]. \tag{23}$$

Note that the probability of obtaining outcome F_i for the measurement on A and outcome G_j for the measurement on B is given by the quantity $\|M_{ij}\|_2^2$, and the probability that the outcomes of the measurements disagree is exactly $\left\|M - \overline{M}\right\|_2^2$. We have

$$\left\|M - \overline{M}\right\|_2^2 \quad = \quad \delta. \tag{24}$$

Additionally, we can compare $\overline{MM}^*$ to the post-measurement state $\sum_i F_i\rho F_i$. The latter quantity is given by

$$\left[\begin{array}{c|c|c|c} \sum_k M_{1k}M_{1k}^* & 0 & \cdots & 0 \\ \hline 0 & \sum_k M_{2k}M_{2k}^* & \cdots & 0 \\ \hline \vdots & & \ddots & \\ \hline 0 & 0 & \cdots & \sum_k M_{nk}M_{nk}^* \end{array}\right],$$

and therefore the difference $(\sum_i F_i\rho F_i - \overline{MM}^*)$ is equal to

$$\left[\begin{array}{c|c|c|c} \sum_{k\neq 1} M_{1k}M_{1k}^* & 0 & \cdots & 0 \\ \hline 0 & \sum_{k\neq 2} M_{2k}M_{2k}^* & \cdots & 0 \\ \hline \vdots & & \ddots & \\ \hline 0 & 0 & \cdots & \sum_{k\neq n} M_{nk}M_{nk}^*, \end{array}\right]$$

which is a positive semidefinite operator whose trace is exactly $\sum_{i\neq j}\|M_{ij}\|_2^2 = \delta$. Thus,

$$\sum_i F_i\rho F_i - \overline{MM}^* \quad _1 \quad = \quad \delta. \tag{25}$$

[3]We can construct an enlargement $B \subseteq \overline{B}$ such that $\mathbf{P}_B\overline{G}_i\mathbf{P}_B = G_i$ for some projective measurement $\{\overline{G}_i\}$ on $\overline{B}$, and we can construct an additional Hilbert space E and a pure state $\overline{\Lambda} \in L(A \otimes B \otimes E)$ such that $\mathrm{Tr}_E\overline{\Lambda} = \Lambda$. The joint probability distribution of the measurements $\{F_i\}$ and $\{\overline{G}_i \otimes I_E\}$ on $\overline{\Lambda}$ are the same as those of $\{F_i\}$ and $\{G_i\}$ on Λ.

Therefore we have the following, using the Cauchy-Schwarz inequality:

$$\begin{aligned}
& \rho - \sum_i F_i \rho F_i \Big\|_1 \\
= \; & MM^* - \sum_i F_i \rho F_i \Big\|_1 \\
= \; & M(M-\overline{M}^*) + (M-\overline{M})\overline{M}^* + \overline{MM}^* - \sum_i F_i \rho F_i \Big\|_1 \\
\leq \; & \|M(M-\overline{M}^*)\|_1 + \|(M-\overline{M})\overline{M}^*\|_1 \\
& + \|\overline{MM}^* - \sum_i F_i \rho F_i\|_1 \\
\leq \; & \|M\|_2 \, \|M-\overline{M}^*\|_2 + \|M-\overline{M}\|_2 \, \|\overline{M}^*\|_2 + \delta \\
\leq \; & 1 \cdot \sqrt{\delta} + \sqrt{\delta} \cdot 1 + \delta \\
\leq \; & 2\sqrt{\delta} + \delta,
\end{aligned}$$

as desired. □

Corollary 12. *Let $\Lambda \in L(A \otimes B \otimes C)$ be a density operator which is classical*[4] *on C. Suppose that $\{F_i\}_{i=1}^n$ is a projective measurement on A such that the induced states $\Lambda_i^{BC} := \mathrm{Tr}_A(F_i \Lambda)$ satisfy*

$$\mathrm{Dist}\{\Lambda_i^{BC}\} \;=\; 1 - \delta. \tag{26}$$

Then, the superoperator $X \mapsto \sum_i (F_i \otimes I) X (F_i \otimes I)$ is $(2\sqrt{\delta} + \delta)$-commutative with Λ^{AC}.

Proof. Let $\overline{C}$ be a Hilbert space which is isomorphic to C, and let $\overline{\Lambda} \in L(A \otimes B \otimes C \otimes \overline{C})$ be the state that arises from Λ by copying out along the standard basis: $|c_i\rangle \mapsto |c_i \overline{c_i}\rangle$. This copying leaves the state ABC unaffected, so assumption (26) still applies. Thus by Proposition 11, the operator $X \mapsto \sum_i (F_i \otimes I) X (F_i \otimes I)$ is $(2\sqrt{\delta} + \delta)$-commutative with $\Lambda^{A\overline{C}}$, and the same holds for the isomorphic state Λ^{AC}. □

Proposition 13. *Let*

$$\Gamma \;=\; (D, E, \{\{R_a^x\}_x\}_a, \{\{S_b^y\}_y\}_b, \gamma) \tag{27}$$

be a two-player strategy. Let

$$\delta \;=\; 1 - \frac{1}{|\mathcal{A}||\mathcal{B}|} \sum_{aby} \mathrm{Dist}\{\rho_{ab}^{xy} \mid x \in \mathcal{X}\}. \tag{28}$$

Then, there exists a classical correlation $(\overline{p}_{ab}^{xy})$ such that

$$\frac{1}{|\mathcal{A}||\mathcal{B}|} \sum_{abxy} |p_{ab}^{xy} - \overline{p}_{ab}^{xy}| \;\leq\; \sqrt{3\delta}\,|\mathcal{A}|\,. \tag{29}$$

Proof. We can assume without loss of generality that the measurements $\{\{R_a^x\}_x\}_a$ are all projective. We begin with the same strategy as in the proof of Proposition 6. For each $a \in \mathcal{A}$, let $V_a = \mathbb{C}^{\mathcal{X}}$, and let $\Phi_a \colon L(D) \to L(V_a \otimes D)$ be the nondestructive measurement defined by

$$\Phi_a(T) \;=\; \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes R_a^x T R_a^x. \tag{30}$$

[4] That is, $\Lambda = \sum_k \Lambda_k \otimes |c_k\rangle\langle c_k|$ for some orthonormal basis $\{c_1, \ldots, c_k\} \subseteq C$.

Let $\Phi_a^{V_a} = \mathrm{Tr}_D \circ \Phi_a$ and let $\Phi_a^D = \mathrm{Tr}_{V_a} \circ \Phi_a$. Likewise let $W_b = \mathbb{C}^{\mathcal{Y}}$ for each $b \in \mathcal{B}$, let $\Psi_b \colon L(D) \to L(W_b \otimes D)$ be the nondestructive measurement defined by

$$\Psi_b(T) \quad = \quad \sum_{y \in \mathcal{Y}} |y\rangle\langle y| \otimes \quad \overline{S_b^y} T \quad \overline{S_b^y}. \tag{31}$$

Let $\Psi_b^{W_b} = \mathrm{Tr}_E \circ \Psi_b$ and $\Psi_b^E = \mathrm{Tr}_{W_b} \circ \Psi_b$.

Assume without loss of generality that $\mathcal{A} = \{1, 2, \ldots, n\}$. Let $\Lambda \in L(V_1 \otimes \ldots \otimes V_n \otimes D \otimes E)$ be the state that arises from applying the superoperators $\Phi_1 \otimes I_E, \ldots, \Phi_n \otimes I_E$, in order, to γ. Let $(\overline{p}_{ab}^{xy})$ be the correlation that arises from Alice and Bob sharing the reduced state $\Lambda^{V_1 \cdots V_n E}$, Alice obtaining her output on input a from the register V_a, and Bob obtaining his output from his prescribed measurements $\{\{S_b^y\}_y\}_b$ to E. Since the state $\Lambda^{V_1 \cdots V_n E}$ is a separable state over the bipartition $(V_1 \ldots V_n \mid E)$, the correlation $(\overline{p}_{ab}^{xy})$ is classical.

If Alice and Bob share the measured state $(I_D \otimes \Psi_b)(\gamma)$ partitioned as $(D \mid EW_b)$, then the probability that Bob can guess Alice's outcome when she measures with $\{R_a^x\}_x$ is given by

$$\delta_{ab} \quad := \quad 1 - \sum_y \mathrm{Dist}\{\rho_{ab}^{xy} \mid x \in \mathcal{X}\}. \tag{32}$$

By Corollary 12, the operator $(\Phi_a^D \otimes I_{W_b})$ is $(2\sqrt{\delta_{ab}} + \delta_{ab})$-commutative with $(I_D \otimes \Psi_b^{W_b})\gamma$.

We wish to compare (p_{ab}^{xy}) and $(\overline{p}_{ab}^{xy})$. For any a, b the probability vector $(\overline{p}_{ab}^{xy})_{xy}$ describes the joint distribution of the registers $V_a W_b$ under the density operator

$$((\Phi_a^{V_a} \circ \Phi_{a-1}^D \circ \Phi_{a-2}^D \circ \cdots \circ \Phi_1^D) \otimes \Psi_b^{W_b})\gamma, \tag{33}$$

which by the previous paragraph is within trace-distance $\sum_{i=1}^{a-1}(2\sqrt{\delta_{ab}} + \delta_{ab})$ from the distribution described by $(p_{ab}^{xy})_{xy}$:

$$(\Phi_a^{V_a} \otimes \Psi_b^{W_b})\gamma. \tag{34}$$

Thus we have the following, in which we use the Cauchy-Schwarz inequality:

$$\begin{aligned}
\sum_{abxy} |p_{ab}^{xy} - \overline{p}_{ab}^{xy}| \quad &\leq \quad \sum_{ab} \quad \sum_{i=1}^{a-1} (2 \quad \overline{\delta_{ib}} + \delta_{ib}) && (35)\\
&= \quad \sum_{ab} (n-a)(2 \quad \overline{\delta_{ab}} + \delta_{ab}). && (36)\\
&\leq \quad \sum_{ab} (n-a)3 \quad \overline{\delta_{ab}} && (37)\\
&\leq \quad 3\sqrt{\sum_{ab} (n-a)^2}\sqrt{\sum_{ab} \delta_{ab}} && (38)\\
&= \quad 3\sqrt{\sum_{ab} (n-a)^2} \quad \overline{n|\mathcal{B}|\delta} && (39)\\
&= \quad 3\sqrt{|\mathcal{B}| \sum_{a} (n-a)^2} \quad \overline{n|\mathcal{B}|\delta} && (40)\\
&= \quad 3|\mathcal{B}|\sqrt{\sum_{a} (n-a)^2}\sqrt{n\delta} && (41)\\
&\leq \quad 3|\mathcal{B}| \quad \overline{n^3/3}\sqrt{n\delta}, && (42)
\end{aligned}$$

which simplifies to the desired bound. □

Proposition 13 is useful for addressing any game (q, H) where the distribution q is uniform (i.e., $q(a,b) = 1/(|\mathcal{A}||\mathcal{B}|)$.) We prove the following theorem which applies to more general games.

Theorem 14. *Let $G = (q, H)$ be a complete-support game and let*

$$\Gamma \quad = \quad (D, E, \{\{R_a^x\}_x\}_a, \{\{S_b^y\}_y\}_b, \gamma) \tag{43}$$

be a two-player strategy. Let

$$\epsilon \quad = \quad 1 - \sum_{ab} q(a,b) \sum_y \mathrm{Dist}\{\rho_{ab}^{xy} \mid x \in \mathcal{X}\}. \tag{44}$$

Then, the score achieved by Γ exceeds the best classical score $\omega_c(G)$ by at most $C_G\sqrt{\epsilon}$, where

$$C_G \quad = \quad (3/2) \overline{\sum_{ab} q(b) \left(P_q(a \mid b)\right)^{-1}}. \tag{45}$$

Proof. Define $\overline{p}_{ab}^{xy}$ and δ_{ab} as in Proposition 13. We have the following (again using the Cauchy-Schwartz inequality):

$$\sum_{abxy} q(a,b)|p_{ab}^{xy} - \overline{p}_{ab}^{xy}| \tag{46}$$

$$\leq \quad \sum_{ab} q(a,b) \sum_{i=1}^{a-1} (2 \quad \overline{\delta_{ib}} + \delta_{ib}) \tag{47}$$

$$\leq \quad \sum_{ab} q(a,b) \sum_{i=1}^{a-1} 3 \quad \overline{\delta_{ib}} \tag{48}$$

$$= \quad \sum_{ab} \left(\sum_{k=a+1}^{n} q(k,b) \right) 3 \quad \overline{\delta_{ab}} \tag{49}$$

$$= \quad \sum_{ab} \left(\frac{\sum_{k=a+1}^{n} q(k,b)}{\overline{q(a,b)}} \right) 3 \quad \overline{q(a,b)\delta_{ab}} \tag{50}$$

$$\leq \quad 3 \sqrt{\sum_{ab} \frac{(\sum_{k=a+1}^{n} q(k,b))^2}{q(a,b)}} \quad \overline{\sum_{ab} q(a,b)\delta_{ab}} \tag{51}$$

$$\leq \quad 3 \sqrt{\sum_{ab} \frac{(\sum_{k=a+1}^{n} q(k,b))^2}{q(a,b)}} \sqrt{\epsilon} \tag{52}$$

$$\leq \quad 3 \sqrt{\sum_{ab} \frac{q(b)^2}{q(a,b)}} \sqrt{\epsilon} \tag{53}$$

$$\leq \quad 2C_G\sqrt{\epsilon} \tag{54}$$

Note that for any probability vectors $\mathbf{t} = (t_1, \ldots, t_m)$ and $\mathbf{s} = (s_1, \ldots, s_m)$ and any arbitrary vector $(u_1, \ldots, u_m) \in [0,1]^m$, we have

$$\sum_i u_i(t_i - s_i) \leq \frac{1}{2} \quad \|t_i - u_i\|. \tag{55}$$

Applying this fact to the probability vectors $(q(a,b)p_{ab}^{xy})_{abxy}$ and $(q(a,b)\overline{p}_{ab}^{xy})_{abxy}$ and the vector $(H(a,b,x,y))_{abxy}$ implies that the difference between the score achieved by (p_{ab}^{xy}) and the score achieved by $(\overline{p}_{ab}^{xy})$ is no more than half the quantity (54), which yields the desired result. □

5 Discussion

When two players achieve a superclassical score at a nonlocal game, their outputs must be at least partially unpredictable to an outside party, even if that party knows the inputs that were given. This fact is one of the bases for randomness expansion from untrusted devices [3], where a user referees a nonlocal game repeatedly with 2 or more untrusted players (or, equivalently, 2 or more untrusted quantum devices) to expand a small uniformly random seed S into a large output string T that is uniform conditioned on S. The players can exhibit arbitrary quantum behavior, but it is assumed that they are prevented from communicating with the adversary. At the center of some of the discussions of randomness expansion (e.g., [19]) is the fact that the min-entropy of the outputs of the players can be lower bounded by an increasing function of the score achieved at the game.

In this paper we have proven an analogous result for the case where one player in a game wishes to generate randomness that is unknown to the other player — in other words, we have achieved (one-shot) *blind* randomness expansion. (The second party, Bob, is "blind" to the randomness generated by Alice.) We have also proven a general rate curve for any game G, which relates the score achieve at G to the predictability of Alice's output from the perspective of Bob – specifically, if G is a complete support game and Alice and Bob achieve score w, then Bob's probability of guessing her output given her input is at most

$$f_G(\omega) \quad = \quad \begin{cases} 1 - (w - \omega_c(G))^2 / C_G & \text{if } w \geq \omega_c(G) \\ 1 & \text{otherwise,} \end{cases} \tag{56}$$

where C_G denotes the constant defined in equation (45).

A possible next step would be to prove a multi-shot version of Theorem 14, e.g., a proof that Alice's outputs across multiple rounds have high smooth min-entropy from Bob's perspective. With the use of a quantum-proof randomness extractor (e.g., [8]) this would imply that Alice has the ability to generate uniformly random bits, known only to her, through interactions with Bob. In the device-independent setting, this would mean that one device could be be reused in multiple iterations of randomness expansion without affecting the security guarantee, and in particular would decrease the minimum number of quantum devices needed to perform unbounded randomness expansion from four (as in [17, 2]) down to three.

The recent entropy accumulation theorem [9] proves lower bounds on smooth min-entropy in various scenarios where a Bell inequality is violated. It will be interesting to see if it can be generalized to cover blind randomness expansion as well. (The current results apply under a Markov assumption which is not satisfied in our case.)

A corollary of our result is that, for any complete-support game G, the range of scores that certify randomness against a third party are exactly the same as the range of scores that certify randomness for one player against the second — in both cases, any superclassical score is adequate. We point out, however, that the certified min-entropy can be different. A simple example of this is the Magic Square game, where Alice and Bob are given inputs $a, b \in \{1, 2, 3\}$ respectively, and must produce outputs $(x_1, x_2, x_3), (y_1, y_2, y_3) \in \{0, 1\}^3$ respectively which satisfy

$$x_1 \oplus x_2 \oplus x_3 \quad = \quad 0, \tag{57}$$

$$y_1 \oplus y_2 \oplus y_3 \quad = \quad 1, \tag{58}$$

$$x_b \quad = \quad y_a. \tag{59}$$

Self-testing [30] for the Magic Square game implies that if Alice and Bob achieve a perfect score, Alice's output contains two bits of perfect randomness from the perspective of a third party, but only one perfect bit of randomness from the perspective of Bob. Optimizing the relationship between the game score and min-entropy in the blind scenario is an open problem.

A potentially useful aspect of Corollary 7 is that it contains a notion of *certified erasure* of information. For the example of the Magic Square game mentioned above, if Bob were asked before his turn to guess Alice's output given her input, he could do this perfectly. (The optimal strategy for for the Magic Square game uses a maximally entangled state and projective measurements, so each party's measurement outcomes

can be perfectly guessed by the other player.) Contrary to this, when Bob is compelled to carry out his part of the strategy before Alice's input is revealed, he loses the ability to perfectly guess Alice's output. Requiring a superclassical score from Alice and Bob amounts to forcing Bob to erase information. Different variants of certified erasure are a topic of current study [25, 12, 21]. An interesting research avenue is to determine the minimal assumptions under which certified erasure is possible.

Finally, we note that the scenario in which the second player tries to guess the first player's output after computing his own output fits the general framework of *sequential nonlocal correlations* [11]. In [7] such correlations are used for ordinary (non-blind) randomness expansion. A next step is to explore how our techniques could be applied to more general sequential nonlocal games.

Acknowledgments. We are indebted to Laura Mancinska for discussions that helped us to prove our robust result (Theorem 14). The first author also thanks Jedrzej Kaniewski, Marcin Pawlowski and Stefano Pironio for helpful information. This research was supported in part by US NSF Awards 1500095, 1216729, 1526928, and 1318070.

References

[1] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. arXiv:1607.01797, 2016.

[2] Kai-Min Chung, Xiaodi Wu, and Yaoyun Shi. Physical randomness extractors: Generating random numbers with minimal assumptions. arXiv:1402.4797, presented at QIP 2014, 2014.

[3] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006. arXiv:0911.3814.

[4] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[5] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust randomness amplifiers: Upper and lower bounds. In *Proceedings of APPROX 2013 and RANDOM 2013*, volume 8096 of *Lecture Notes in Computer Science*, pages 468–483. Springer, 2013.

[6] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 427–436, 2014.

[7] F. J. Curchod, M. Johansson, M. J. Hoban, P. Wittek, and A. Acin. Unbounded randomness certification using sequences of measurements. arXiv:1510.03394v1, October 2015.

[8] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan's extractor in the presence of quantum side information. *SIAM J. Comput*, 41(4):915–940, 2012.

[9] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. arXiv:1607.01796, 2016.

[10] Serge Fehr, Ran Gelles, and Christian Schaffner. Security and composability of randomness expansion from Bell inequalities. *Phys. Rev. A*, 87:012335, Jan 2013.

[11] Rodrigo Gallego, Lars Erik Wurflinger, Rafael Chaves, Antonio Acin, and Miguel Navascues. Nonlocality in sequential correlation scenarios. *New Journal of Physics*, 16(033037), 2014.

[12] Jedrzej Kaniewski and Stephanie Wehner. Device-independent two-party cryptography secure against sequential attacks. *New Journal of Physics*, 18, May 2016.

[13] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. *SIAM Journal on Computing*, 40(3):848–877, 2011.

[14] Laura Mancinska. Maximally entangled states in pseudo-telepathy games. arXiv:1506.07080, June 2015.

[15] Matthew McKague. Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016.

[16] Carl A. Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol, 2015. arXiv:1411.6608.

[17] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63(4):33:1–33:63, October 2016.

[18] Marcin Pawlowski. Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations. *Physical Review A*, 82:032313, 2010.

[19] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010.

[20] Stefano Pironio and Serge Massar. Security of practical private randomness generation. *Phys. Rev. A*, 87:012336, Jan 2013.

[21] Jeremy Riberio, Le Phuc Thinh, Jedrzej Kaniewski, Jonas Helsen, and Stephanie Wehner. Device-independence for two-party cryptography and position verification. arXiv:1606.08750, June 2016.

[22] V. B. Scholz and R. F. Werner. Tsirelson's problem. arXiv:0812.4305v1, 2008.

[23] Dominique Spehner. Quantum correlations and distinguishability of quantum states. *Journal of Mathematical Physics*, 55(7):075211, 2014.

[24] Boris Tsirelson. Bell inequalities and operator algebras. http://www.tau.ac.il/∼tsirel/download/bellopalg.pdf.

[25] Dominique Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6):49:1–49:76, December 2015.

[26] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[27] Umesh V. Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In Howard J. Karloff and Toniann Pitassi, editors, *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 61–76. ACM, 2012.

[28] Thomas Vidick. *The Complexity of Entangled Games*. PhD thesis, University of California, Berkeley, 2011.

[29] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Proceedings - Annuel IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 766–755, 2013.

[30] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, 93:062121, Jun 2016.