

# A parallel repetition theorem for all entangled games

Henry Yuen\*

MIT

## Abstract

The behavior of games repeated in parallel, when played with quantumly entangled players, has received much attention in recent years. Quantum analogues of Raz's classical parallel repetition theorem have been proved for many special classes of games. However, for general entangled games no parallel repetition theorem was known.

We prove that the entangled value of a two-player game  $G$  repeated  $n$  times in parallel is at most  $c_G n^{-1/4} \log n$  for a constant  $c_G$  depending on  $G$ , provided that the entangled value of  $G$  is less than 1. In particular, this gives the first proof that the entangled value of a parallel repeated game must converge to 0 for *all* games whose entangled value is less than 1. Central to our proof is a combination of both classical and quantum correlated sampling.

## 1 Introduction

A two-player one-round game  $G$  is played between a referee and two isolated players (who we will call Alice and Bob), who communicate only with the referee and not between themselves. The referee first samples a question pair  $(x, y)$  from some distribution  $\mu$  and sends  $x$  to Alice and  $y$  to Bob. Alice and Bob respond with answers  $a$  and  $b$  respectively, and they win if  $V(x, y, a, b) = 1$  for some predicate  $V$ .

The maximum winning probability of Alice and Bob in a game  $G$  is a quantity that depends on what resources they are allowed to use. If their answers are a deterministic function of their received question (and perhaps some public random string), then we call their maximum winning probability the *classical value* of  $G$ , denoted by  $\text{val}(G)$ . However quantum mechanics allows Alice and Bob to share a resource called *entanglement*, which gives rise to correlations that cannot be reproduced with public randomness only. When Alice and Bob make use of entanglement to play a game  $G$ , we call their maximum winning probability the *entangled value* of  $G$ , denoted by  $\text{val}^*(G)$ . For all games, the classical value is at most the entangled value. Cast in the language of games, the famous Bell's Theorem states that there exist games  $G$  where those values are different:  $\text{val}^*(G) > \text{val}(G)$  [Bel64].

The Parallel Repetition Question is the following natural and basic question: given a game  $G$  with value less than 1, what is the value of the game  $G^n$ , wherein Alice and Bob play  $n$  independent instances of  $G$  played *in parallel*? More formally, in the game  $G^n$ , the referee samples  $n$  independent

---

\*hyuen@mit.edu

question pairs  $(x_1, y_1), \dots, (x_n, y_n)$  from  $\mu$ , and sends  $(x_1, \dots, x_n)$  to Alice, and sends  $(y_1, \dots, y_n)$  to Bob. Alice responds with answer tuple  $(a_1, \dots, a_n)$ , Bob responds with  $(b_1, \dots, b_n)$ , and the players win if for all coordinates  $i \in [n]$ ,  $V(x_i, y_i, a_i, b_i) = 1$ .

The difficulty in relating  $\text{val}(G^n)$  with  $\text{val}(G)$  and  $n$  is that even though each of the  $n$  instances of  $G$  in  $G^n$  are independent, Alice and Bob need not play each instance independently. For example, since Alice receives  $(x_1, \dots, x_n)$  all at once, she can use some question  $x_j$  to answer the  $i$ 'th game, and Bob can do something similar. Because of such strategies, for every  $k$  there are games  $G$  such that  $\text{val}(G^k) = \text{val}(G) < 1$ . This shows that the naive expectation that  $\text{val}(G^n) = \text{val}(G)^n$  is false.

The naive expectation is not too far from the truth, however: Raz's Parallel Repetition Theorem [Raz98] states that

$$\text{val}(G^n) \leq (1 - (1 - \text{val}(G))^3)^{c_G n},$$

where  $c_G$  is a constant depending on  $G$ . In particular, as  $n$  goes to infinity, the classical success probability goes to 0 exponentially fast in  $n$  (provided that  $\text{val}(G) < 1$ ). The proof is highly nontrivial, although it has been simplified and improved upon in recent years [Hol09, BG15]. Raz's Parallel Repetition Theorem has heavily influenced complexity theory, most notably in the areas of hardness of approximation [Hås01] and communication complexity [Jai11, BRWY13].

One open question, which we call the Quantum Parallel Repetition Conjecture, asks whether an analogue of Raz's Parallel Repetition Theorem holds in the setting of entangled players. The Quantum Parallel Repetition Conjecture has been resolved for many special cases of games, including free games [CS14, JPY14, CWY15], projection games [DSV14], XOR games [CSUU08], unique games [KRT08], anchored games [BVY15], and fortified games [BVY16]. However, the general case has remained elusive. Not only do we not know of a quantum analogue of Raz's Parallel Repetition Theorem, it hasn't even been shown that if  $\text{val}^*(G) < 1$ , then  $\text{val}^*(G^n)$  goes to 0 as  $n$  goes to infinity! Could quantum entanglement allow players to counteract the value-decreasing effect of parallel repetition?

In this paper we prove that for all nontrivial entangled games  $G$  (i.e.  $\text{val}^*(G) < 1$ ), the entangled value of  $G^n$  must converge to 0. This resolves a weaker version of the Quantum Parallel Repetition Conjecture for general games. Quantitatively, our result is the following:

**Theorem 1** (Main Theorem). *Let  $G$  be a game involving two entangled players with  $\text{val}^*(G) = 1 - \varepsilon$ . Then for all integer  $n > 0$ ,*

$$\text{val}^*(G^n) \leq c \cdot \frac{s_G \log n}{\varepsilon^{17} n^{1/4}}$$

where  $c$  is a universal constant and  $s_G$  is the bit-length of the players' answers in  $G$ .

This shows that the entangled value of  $G^n$  must decay at a polynomial rate with  $n$ . The full Quantum Parallel Repetition Conjecture states that the rate of decay is in fact exponential, and this remains an important open problem.

## 1.1 Previous work

There has been extensive work on the parallel repetition of entangled games. As stated earlier, past results have applied to various special classes of games, but there was no result that covered *all* games.

The results coming closest to the Quantum Parallel Repetition Conjecture are the work of Kempe and Vidick [KV11] and Bavarian, Vidick, and Yuen [BVY15, BVY16]. Rather than proving parallel repetition theorems for general games, these works prove general *gap amplification* theorems, which are closely related. Instead of showing that for games  $G$  where  $\text{val}^*(G) < 1$  that  $\text{val}^*(G^n)$  goes to 0 with  $n$ , the game  $G$  is first converted to another game  $H$  where analyzing  $\text{val}^*(H^n)$  is much more tractable. Gap amplification is a technique used in complexity theory and cryptography to amplify the difference between two cases of a problem (usually called the *completeness* and *soundness* cases).

Kempe and Vidick showed that given an arbitrary game  $G$ , one can efficiently transform it to another game  $H$  with the following properties: if the *classical* value of  $G$  is 1 (meaning that there is a perfect deterministic strategy), then  $\text{val}(H^n) = 1$  (and thus  $\text{val}^*(H^n) = 1$ ). If the *entangled* value of  $G$  is less than 1, then the entangled value of  $H^n$  decays at a polynomial rate  $n^{-\Omega(1)}$ . In this transformed game  $H$ , in addition to playing the game  $G$ , the referee will randomly choose to ask “consistency” questions to check that the players give the same answers on the same questions<sup>1</sup>. Thus [KV11] prove gap amplification for general games – with a caveat. Because of the random consistency checks in the game  $H$ , the “quantum completeness” is not preserved: even if  $\text{val}^*(G) = 1$ , it is not necessarily the case that  $\text{val}^*(H) = 1$ .

More recently, Bavarian, Vidick, and Yuen [BVY15, BVY16] gave better gap amplification results for entangled games<sup>2</sup>. They showed that for general games  $G$ , one can apply a simple transformation to obtain another game  $H$  with the following properties:

1. If  $\text{val}^*(G) = 1$ , then  $\text{val}^*(H^n) = 1$ .
2. If  $\text{val}^*(G) < 1$ , then  $\text{val}^*(H^n) \leq \exp(-\Omega(n))$ .

Note that the transformation from  $G$  to  $H$  preserves quantum completeness, and that when  $\text{val}^*(G) < 1$ , the entangled value of the repeated game decays *exponentially*. Like [KV11], the transformations of [BVY15, BVY16] construct  $H$  by adding auxiliary questions to the game  $G$ . The transformation given in [BVY15] is called *anchoring*, and the transformation in [BVY16] is called *fortification*. The latter transformation gives a quantum generalization of the fortification technique of [Mos14] for *classical games*. The quantitative aspects of repeated anchored games are different from those of fortified games, but both yield general gap amplification theorems for entangled games.

The results of Bavarian, Vidick and Yuen show that, while we do not know if the Quantum Parallel Repetition Conjecture holds for all games  $G$ , we *do* know that it holds for a class of games that effectively captures the general case, in fact with exponential decay similar to Raz’s theorem. Since the main application of parallel repetition in complexity theory and quantum information is gap amplification, the results of [BVY15, BVY16] effectively settle the Quantum Parallel Repetition Conjecture – as far as applications are concerned.

But as a scientific question, the original Quantum Parallel Repetition Conjecture is a fundamental and basic problem about the power of entanglement in games. Prior to this work, one might have wondered whether there exists a game  $G$  such that  $\text{val}^*(G) < 1$ , but there is some constant  $\delta$  such that for infinitely many  $n$  there is a nefarious entangled strategy for  $G^n$  with success probability at least  $\delta$ ? Here we prove that this cannot happen.

<sup>1</sup>This transformation is due to Feige and Kilian [FK00], who proved a similar result for classical games.

<sup>2</sup>They also obtain general gap amplification results for games with more than two players.

## 1.2 Proof overview

Theorem 1 is proved via reduction: if  $\text{val}^*(G^n)$  is too large, then from an optimal entangled strategy for  $G^n$  we can construct an entangled strategy for the single-shot game  $G$  that wins with probability strictly greater than  $\text{val}^*(G)$ , which would be a contradiction.

In more detail, suppose that  $\text{val}^*(G) = 1 - \varepsilon$ . If the success probability of the players in  $G^n$  is dramatically larger than our target bound (which in our case is  $\sim n^{-O(1)}$ ), then we can identify a set of coordinates  $C \subseteq [n]$  that is not too large, but has the property that for a uniformly random coordinate  $i \in [n] - C$ ,

$$\Pr(\text{Win game } i \mid \text{Win games in } C) > 1 - \varepsilon/2 \quad (1)$$

where here the probability is both over the randomness of the questions in  $G^n$ , the randomness of the players' entangled strategy, and the randomly chosen index  $i$ . Thus it would be advantageous if Alice and Bob could play the single-shot game  $G$  by "embedding" it in a randomly chosen  $i$ th coordinate of  $G^n$ , and playing  $G^n$  *conditioned* on the event that the games indexed by  $C$  have been won. If they could do this, then by (1), the probability they win the  $i$ th coordinate of  $G^n$ , and hence the original game  $G$ , is at least  $1 - \varepsilon/2 > \text{val}^*(G)$ , which would be a contradiction.

If the players are classical (i.e. use deterministic strategies), this embedding is performed in the following way. Alice and Bob are first given questions  $(X_i, Y_i)$  for the  $i$ 'th game. Based on their received question, Alice and Bob jointly sample a *dependency-breaking variable*  $R$ . The essential features of this dependency-breaking variable are:

1. **Usefulness**<sup>3</sup>:  $\mathbb{P}_{A_i B_i | R X_i Y_i W_C} = \mathbb{P}_{A_i | R X_i W_C} \cdot \mathbb{P}_{B_i | R Y_i W_C}$
2. **Sampleability**:  $\mathbb{P}_{R | X_i Y_i W} \approx \mathbb{P}_{R | X_i W_C} \approx \mathbb{P}_{R | Y_i W_C}$

where " $\approx$ " means closeness in statistical distance. Here,  $W_C$  denotes the event that the players win all the games in  $C$ .  $\mathbb{P}_{A_i B_i | R X_i Y_i W_C}$  denotes the probability distribution of Alice's and Bob's answers in the  $i$ th coordinate when playing  $G^n$ , conditioned on the dependency-breaking variable  $R$ , their received questions for the  $i$ th game  $(X_i, Y_i)$ , and the event  $W_C$ . The "Usefulness property" states that, the players' answers in the  $i$ th round are independent of each other, conditioned on  $R$ , their own questions, and  $W_C$ . Thus, given  $R$  distributed according to  $\mathbb{P}_{R | X_i Y_i W_C}$ , Alice can sample  $A_i$  on her own, because she possesses  $R$  and  $X_i$ , and similarly Bob can sample  $B_i$  on his own, because he possesses knowledge of  $R$  and  $Y_i$ . By (1), the probability that  $V(X_i, Y_i, A_i, B_i) = 1$  will be strictly greater than  $\text{val}^*(G)$ , wherein we would arrive at a contradiction.

As the name suggests, the "sampleability property" implies that Alice and Bob can (approximately) jointly sample the variable  $R$ . Even though the distribution  $\mathbb{P}_{R | X_i Y_i W_C}$  may depend on both players' questions, the sampleability property shows  $R$ , up to some error, only depends on  $X_i$  or  $Y_i$ , but not both. Using the *correlated sampling procedure* of [Hol09], Alice and Bob can jointly sample  $R$  from  $\mathbb{P}_{R | X_i Y_i W}$  with high probability.

---

<sup>3</sup>We will let  $\mathbb{P}$  denote the probability distribution that describes the joint distribution of the random variables relevant in an execution of the strategy for  $G^n$ , including the players' questions  $X_1, \dots, X_n, Y_1, \dots, Y_n$ , the players' answers  $A_1, \dots, A_n, B_1, \dots, B_n$ , and the dependency-breaking variable  $R$ .

At a high level, the proof of our quantum parallel repetition theorem is similar. However instead of sampling a dependency-breaking variable  $R$ , the players will need to sample a *dependency-breaking state*. It is an entangled state  $|\Psi_{x_i y_i}\rangle$  that depends on both Alice’s and Bob’s questions  $(x_i, y_i)$ , and satisfies similar Usefulness and Sampleability properties:

1. **Usefulness:** The distribution of measurement outcomes by making local measurements on  $|\Psi_{X_i Y_i}\rangle$  is equal to  $P_{A_i B_i | X_i Y_i W_C}$ .
2. **Sampleability:** There exist states  $|\Phi_{X_i}\rangle$  and  $|\Gamma_{Y_i}\rangle$  such that  $|\Psi_{X_i Y_i}\rangle \approx |\Phi_{X_i}\rangle \approx |\Gamma_{Y_i}\rangle$

where “ $\approx$ ” means closeness in  $\ell_2$  distance, and the statements hold on average over  $X_i Y_i$ .

The Usefulness property states that if on input  $(x_i, y_i)$ , Alice and Bob were to share the entangled state  $|\Psi_{x_i y_i}\rangle$ , then they could make local measurements to obtain outcomes distributed according to  $P_{A_i B_i | X_i Y_i W_C}$ , which would mean that their success probability would be  $\Pr(\text{Win } i \mid \text{Win } C)$ , which is greater than  $\text{val}^*(G)$ , an impossibility.

The Sampleability property implies that on input  $(x_i, y_i)$  Alice and Bob are actually able to approximately prepare the state  $|\Psi_{x_i y_i}\rangle$ . This is because of the *quantum correlated sampling procedure* of Dinur, Steurer, and Vidick, who used it to prove a parallel repetition theorem for entangled projection games [DSV14]. It is entirely analogous to Holenstein’s correlated sampling procedure: Alice has a description of a state  $|\Phi_{X_i}\rangle$  that’s close to  $|\Psi_{X_i Y_i}\rangle$ , and Bob has a description of a state  $|\Gamma_{Y_i}\rangle$  that is also close to  $|\Psi_{X_i Y_i}\rangle$ . Via local transformations on preshared quantum entanglement, Alice and Bob can generate an approximation of  $|\Psi_{X_i Y_i}\rangle$ . Combined with the Usefulness property, Alice and Bob are then able to win the  $i$ th game with too high probability.

It is not difficult to define states that satisfy the Usefulness property. Consider an execution of the entangled strategy for  $G^n$ . In the beginning, the players share some entangled state  $|\psi\rangle$ , and upon obtaining questions  $(x_1, \dots, x_n)$  and  $(y_1, \dots, y_n)$ , the players apply local measurements depending on these questions to  $|\psi\rangle$  to obtain answer tuples  $(a_1, \dots, a_n)$  and  $(b_1, \dots, b_n)$ . One can define an ensemble of states  $\{|\Psi_{x_i y_i}\rangle\}$  that are, roughly speaking, derived from the post-measurement state of the players *conditioned* on the players having won all the games in  $C$  (that is, conditioned on the event  $W_C$ ), *and* having received a specific question pair  $(x_i, y_i)$  in the  $i$ ’th coordinate. Such an ensemble of states would satisfy the Usefulness property.

However, the primary challenge is achieving Sampleability property, that is, to show the states  $|\Psi_{x_i y_i}\rangle$  only depend on one player’s question, but not both. One major obstacle to proving the Sampleability property is the following: in the players’ strategy for  $G^n$ , Bob (say) may elect to “print” his entire vector of questions  $(y_1, \dots, y_n)$  into the entangled state  $|\psi\rangle$ . He can do this by applying a local unitary operation controlled on his questions on some ancilla qubits in  $|\psi\rangle$ . We cannot say he does not do this, because the shared entangled state  $|\psi\rangle$  and the players’ measurements are completely arbitrary. But this implies that we cannot hope to prove that the post-measurement state is independent of  $y_i$ , conditioned on  $x_i$ .

Despite such barriers, we are able to define the  $|\Psi_{x_i y_i}\rangle$  in such a way that removes such adversarial dependencies on the players’ questions. Assuming (for contradiction) that the players’ probability of success is at least  $n^{-O(1)}$ , then we are able to prove that these states satisfy the Sampleability property. We build upon many previous works: we use the information theoretic framework of [CS14, JPY14], carefully combined with the operator analysis techniques from [DSV14]. The

definition of the dependency-breaking states  $|\Psi_{x_i, y_i}\rangle$  includes the classical dependency-breaking variables of [Hol09] used to prove Raz's parallel repetition theorem. Our final constructed strategy for the single-shot game  $G$  uses both classical and quantum correlated sampling procedures.

## 2 Preliminaries

### 2.1 Probability distributions

We largely adopt the notational conventions from [Hol09] for probability distributions. We let capital letters denote random variables and lower case letters denote specific samples. We will use subscripted sets to denote tuples, e.g.,  $X_{[n]} := (X_1, \dots, X_n)$ ,  $x_{[n]} = (x_1, \dots, x_n)$ , and if  $C \subset [n]$  is some subset then  $X_C$  will denote the sub-tuple of  $X_{[n]}$  indexed by  $C$ . We use  $P_X$  to denote the probability distribution of random variable  $X$ , and  $P_X(x)$  to denote the probability that  $X = x$  for some value  $x$ . For multiple random variables, e.g.,  $X, Y, Z$ ,  $P_{XYZ}(x, y, z)$  denotes their joint distribution with respect to some probability space understood from context.

We use  $P_{Y|X=x}(y)$  to denote the conditional distribution  $P_{YX}(y, x)/P_X(x)$ , which is defined when  $P_X(x) > 0$ . When conditioning on many variables, we usually use the shorthand  $P_{X|y,z}$  to denote the distribution  $P_{X|Y=y, Z=z}$ . For example, we write  $P_{V|\omega_{-i}, x_i, y_i}$  to denote  $P_{V|\Omega_{-i}=\omega_{-i}, X_i=x_i, Y_i=y_i}$ . For an event  $W$  we let  $P_{XY|W}$  denote the distribution conditioned on  $W$ . We use the notation  $\mathbb{E}_X f(x)$  and  $\mathbb{E}_{P_X} f(x)$  to denote the expectation  $\sum_x P_X(x)f(x)$ .

Let  $P_{X_0}$  be a distribution of  $\mathcal{X}$ , and for every  $x$  in the support of  $P_{X_0}$ , let  $P_{Y|X_1=x}$  be a conditional distribution defined over  $\mathcal{Y}$ . We define the distribution  $P_{X_0}P_{Y|X_1}$  over  $\mathcal{X} \times \mathcal{Y}$  as

$$(P_{X_0}P_{Y|X_1})(x, y) := P_{X_0}(x) \cdot P_{Y|X_1=x}(y).$$

Additionally, we write  $P_{X_0Z}P_{Y|X_1}$  to denote the distribution  $(P_{X_0Z}P_{Y|X_1})(x, z, y) := P_{X_0Z}(x, z) \cdot P_{Y|X_1=x}(y)$ .

For two random variables  $X_0$  and  $X_1$  over the same set  $\mathcal{X}$ , we use

$$\|P_{X_0} - P_{X_1}\| := \frac{1}{2} \sum_{x \in \mathcal{X}} |P_{X_0}(x) - P_{X_1}(x)|,$$

to denote the total variation distance between  $P_{X_0}$  and  $P_{X_1}$ .

### 2.2 Quantum information theory

For comprehensive references on quantum information we refer the reader to [NC10, Wil13].

For a vector  $|\psi\rangle$ , we use  $\| |\psi\rangle \|$  to denote its Euclidean length. For a matrix  $A$ , we will use  $\|A\|_1$  to denote its *trace norm*  $\text{Tr}(\sqrt{AA^\dagger})$ , and  $\|A\|_F$  to denote its *Frobenius norm*  $\sqrt{\text{Tr}(AA^\dagger)}$ . A density matrix is a positive semidefinite matrix with trace 1. The *fidelity* between two density matrices  $\rho$  and  $\sigma$  is defined as  $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ . For Hermitian matrices  $A, B$  we write  $A \preceq B$  to indicate that  $A - B$  is positive semidefinite. We use  $\mathbb{I}$  to denote the identity matrix. A *positive operator valued measurement* (POVM) with outcome set  $\mathcal{A}$  is a set of positive semidefinite matrices  $\{E^a\}$  labeled by  $a \in \mathcal{A}$  that sum to the identity.

We will use the convention that, when  $|\psi\rangle$  is a pure state,  $\psi$  refers to the rank-1 density matrix  $|\psi\rangle\langle\psi|$ . We use subscripts to denote system labels; so  $\rho_{AB}$  will denote the density matrix on the

systems  $A$  and  $B$ . A *classical-quantum* state (or simply *cq-state*)  $\rho_{XE}$  is classical on  $X$  and quantum on  $E$  if it can be written as  $\rho_{XE} = \sum_x p(x)|x\rangle\langle x|_X \otimes \rho_{E|X=x}$  for some probability measure  $p(\cdot)$ . The state  $\rho_{E|X=x}$  is by definition the  $E$  part of the state  $\rho_{XE}$ , conditioned on the classical register  $X = x$ . We write  $\rho_{XE|X=x}$  to denote the state  $|x\rangle\langle x|_X \otimes \rho_{E|X=x}$ . We often write expressions such as  $\rho_{E|x}$  as shorthand for  $\rho_{E|X=x}$  when it is clear from context which registers are being conditioned on. This will be useful when there are many classical variables to be conditioned on.

The Fuchs-van de Graaf inequalities relate fidelity and trace norm as

$$1 - F(\rho, \sigma) \leq \frac{1}{2} \|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho, \sigma)^2}. \quad (2)$$

When dealing with pure states, we can tighten the relationship between the trace norm and the Euclidean distance:

**Fact 2.** For pure states  $|v\rangle$  and  $|w\rangle$ ,  $\| |v\rangle\langle v| - |w\rangle\langle w| \|_1 \leq 2 \| |v\rangle - |w\rangle \|$ .

**Ando's Identity.** For any symmetric pure state  $|\psi\rangle = \sum_j \sqrt{\lambda_j} |v_j\rangle |v_j\rangle$  for an orthonormal basis  $\{|v_j\rangle\}$  and arbitrary linear operators  $X, Y$ , we have

$$\langle \psi | X \otimes Y | \psi \rangle = \text{Tr}(X \sqrt{\rho} Y^\top \sqrt{\rho}),$$

where  $\rho = \sum \lambda_j |v_j\rangle\langle v_j|$  is the reduced density matrix of  $|\psi\rangle$  on either subsystem and the transpose is taken with respect to the basis  $\{|v_j\rangle\}$ .

**Information theoretic quantities.** For two positive semidefinite operators  $\rho, \sigma$ , the *relative entropy*  $S(\rho\|\sigma)$  is defined to be  $\text{Tr}(\rho(\log \rho - \log \sigma))$ . The *relative min-entropy*  $S_\infty(\rho\|\sigma)$  is defined as  $\min\{\lambda : \rho \preceq 2^\lambda \sigma\}$ .

Let  $\rho_{AB}$  be a bipartite state. The mutual information  $I(A : B)_\rho$  is defined as  $S(\rho_{AB}\|\rho_A \otimes \rho_B)$ . For a classical-quantum state  $\rho_{XAB}$  that is classical on  $X$  and quantum on  $AB$ , we write  $I(A; B|x)_\rho$  to indicate  $I(A; B)_{\rho_x}$ .

**Fact 3.** For all states  $\rho_{AB}, \sigma_A$ , and  $\tau_B$ , we have

$$S(\rho_{AB}\|\sigma_A \otimes \tau_B) \geq S(\rho_{AB}\|\rho_A \otimes \rho_B) = I(A; B)_\rho.$$

**Fact 4** (Pinsker's inequality). For all density matrices  $\rho, \sigma$ ,  $\frac{1}{2} \|\rho - \sigma\|_1^2 \leq S(\rho\|\sigma)$ .

**Lemma 5** ([JPY14], Fact II.8). Let  $\rho = \sum_z P_Z(z) |z\rangle\langle z| \otimes \rho_z$ , and  $\rho' = \sum_z P_{Z'}(z) |z\rangle\langle z| \otimes \rho'_z$ . Then  $S(\rho'\|\rho) = S(P_{Z'}\|P_Z) + \mathbb{E}_{Z'} [S(\rho'_z\|\rho_z)]$ . In particular,  $S(\rho'\|\rho) \geq \mathbb{E}_{Z'} [S(\rho'_z\|\rho_z)]$ .

We will also use the following Lemma from [CWY15, BVY15].

**Lemma 6** ([CWY15, BVY15], Quantum Raz's Lemma). Let  $\rho$  and  $\sigma$  be two cq-states with  $\rho_{XA} = \rho_{X_1 X_2 \dots X_n A}$  and  $\sigma = \sigma_{XA} = \sigma_{X_1} \otimes \sigma_{X_2} \otimes \dots \otimes \sigma_{X_n} \otimes \sigma_A$  with  $X = X_1 X_2 \dots X_n$  classical in both states. Then

$$\sum_{i=1}^n I(X_i : A)_\rho \leq S(\rho_{XA} \|\sigma_{XA}). \quad (3)$$

### 2.3 Classical and quantum correlated sampling

*Correlated sampling* is a key component of Holenstein's proof of the classical parallel repetition theorem.

**Lemma 7** (Classical correlated sampling [Hol09]). *Let  $P$  and  $Q$  be two probability distributions over a universe  $\mathcal{U}$  such that  $\|P - Q\|_1 \leq \varepsilon < 1$ . Then there exists a zero communication two-player protocol using shared randomness where the first player outputs an element  $p \in \mathcal{U}$  distributed according to  $P$ , the second player samples an element  $q \in \mathcal{U}$  distributed according to  $Q$ , and with probability at least  $1 - O(\varepsilon)$ , the two elements are identical (i.e.  $p = q$ ).*

We call the protocol in the Lemma above the *classical correlated sampling procedure*. The next lemma is the quantum extension of the correlated sampling lemma, proved by [DSV14] in order to obtain a parallel repetition theorem for entangled projection games, a class of two-player games. Their lemma is a robust version of the quantum state embezzlement procedure of [vDH03].

**Lemma 8** (Quantum correlated sampling [DSV14]). *Let  $d$  be an integer and  $\alpha > 0$ . Then there exists an integer  $d'$  depending on  $d$  and  $\alpha$ , and a collection of unitaries  $V_\psi, W_\psi$  acting on  $\mathbb{C}^{dd'}$  for every state  $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ , such that the following holds: for any two states  $|\varphi\rangle, |\theta\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ ,*

$$\|\bar{V}_\varphi \otimes W_\theta |E_{dd'}\rangle - |\varphi\rangle |E_{d'}\rangle\| \leq O(\max\{\alpha^{1/12}, \|\varphi - \theta\|^{1/6}\})$$

where  $|E_d\rangle \propto \sum_{j=1}^d \frac{1}{\sqrt{j}} |j\rangle |j\rangle$  is the  $d$ -dimensional embezzlement state.

We shall call the protocol in the Lemma above the *quantum correlated sampling procedure*.

## 3 Proof of the Main Theorem

Let  $G$  be a two-player one-round game with question distribution  $\mu$  and referee predicate  $V(x, y, a, b)$ . Let  $\mathcal{A}$  and  $\mathcal{B}$  denote the alphabets of Alice's and Bob's answers, respectively. Let  $\text{val}^*(G) = 1 - \varepsilon$ .

Consider an optimal entangled strategy for  $G^n$ , which consists of a shared entangled state  $|\psi\rangle^{E_A E_B} \in \mathbb{C}^d \otimes \mathbb{C}^d$  and measurement POVMs for Alice and Bob,  $\{A_{x_{[n]}}^{a_{[n]}}\}$  and  $\{B_{y_{[n]}}^{b_{[n]}}\}$  respectively. We will assume that  $|\psi\rangle$  is symmetric; i.e.,  $|\psi\rangle = \sum_i \sqrt{\lambda_i} |v_i\rangle |v_i\rangle$  for some orthonormal basis  $\{|v_i\rangle\}$ . This is without loss of generality, as we can always rotate (say) Bob's basis vectors to match Alice's basis vectors, and fold the unitary rotation into Bob's measurements. For  $i \in [n]$ , let  $W_i$  denote the event that the players win coordinate  $i$  using this optimal strategy. Let  $W = W_1 \wedge \dots \wedge W_n$  denote the event that the players win all coordinates. For a set  $C \subseteq [n]$ , let  $W_C = \bigwedge_{i \in C} W_i$ .

**Proposition 9.** *Suppose that  $\log 1/\Pr(W) \leq \varepsilon n/16 - \log 4/\varepsilon$ . Then there exists a set  $C \subseteq [n]$  of size at most  $t = \frac{8}{\varepsilon} (\log 4/\varepsilon + \log 1/\Pr(W))$  such that*

$$\Pr_{i \notin C}(W_i | W_C) \geq 1 - \varepsilon/2.$$

where  $i$  is chosen uniformly from  $[n] - C$ .

*Proof.* Set  $\delta = \varepsilon/8$ . Let  $W_{>1-\delta}$  denote the event that the players won more than  $(1 - \delta)n$  rounds. To show existence of such a set  $C$ , we will show that  $\mathbb{E}_C \Pr(\neg W_i | W_C) \leq \varepsilon/2$ , where  $C$  is a (multi)set



of  $t$  independently chosen indices in  $[n]$ . This implies that there exists a particular set  $C$  such that  $\Pr(\neg W_i | W_C) \leq \varepsilon/2$ , which concludes the claim.

First we write, for a fixed  $C$ ,

$$\begin{aligned} \Pr(\neg W_i | W_C) &= \Pr(\neg W_i | W_C, W_{>1-\delta}) \Pr(W_{>1-\delta} | W_C) + \\ &\quad \Pr(\neg W_i | W_C, \neg W_{>1-\delta}) \Pr(\neg W_{>1-\delta} | W_C). \end{aligned}$$

Observe that  $\Pr(\neg W_i | W_C \wedge W_{>1-\delta})$  is the probability that, conditioned on winning all rounds in  $C$ , the randomly selected coordinate  $i \in [n] - C$  happens to be one of the (at most)  $\delta n$  lost rounds. This is at most  $\delta n / (n - t) \leq \varepsilon/4$ , where we use our assumption on  $t$  from the Proposition statement. Now observe that

$$\begin{aligned} \mathbb{E}_C \Pr(\neg W_{>1-\delta} | W_C) &\leq \mathbb{E}_C \frac{\Pr(W_C | \neg W_{>1-\delta})}{\Pr(W_C)} \\ &\leq \frac{1}{\Pr(W)} (1 - \delta)^t \\ &\leq \varepsilon/4 \end{aligned}$$

where in the second line we used the fact that  $\Pr(W_C) \geq \Pr(W)$ . □

For the rest of the proof we will fix a set  $C$  given by Proposition 9.

### 3.1 Dependency-breaking variables

We introduce the random variables that play an important role in the proof of Theorem 1. Let  $C \subseteq [n]$  be as given by Proposition 9. We fix  $C = \{m + 1, m + 2, \dots, n\}$ , where  $m = n - |C|$ , as this will easily be seen to hold without loss of generality. Let  $(X_{[n]}, Y_{[n]})$  be distributed according to  $\mu_{[n]}$  and  $(A_{[n]}, B_{[n]})$  be defined from  $X_{[n]}$  and  $Y_{[n]}$  as follows:

$$P_{A_{[n]}B_{[n]}|X_{[n]}Y_{[n]}}(a_{[n]}, b_{[n]}) = \langle \psi | A_{X_{[n]}}^{a_{[n]}} \otimes B_{Y_{[n]}}^{b_{[n]}} | \psi \rangle.$$

Let  $(X_C, Y_C)$  and  $Z = (A_C, B_C)$  be random variables that denote the players' questions and answers respectively associated with the coordinates indexed by  $C$ .

We use the random variables  $\Omega$  and  $R$  that are crucially used in Holenstein's proof of Raz's parallel repetition theorem. Let  $D_1, \dots, D_m$  be independent and uniformly distributed in  $\{Alice, Bob\}$ . Let  $M_1, \dots, M_m$  be independent random variables defined in the following way: for each  $i \in [m]$ ,

$$M_i = \begin{cases} X_i & \text{if } D_i = Alice \\ Y_i & \text{if } D_i = Bob \end{cases}$$

Now for  $i \in [m]$ , we define  $\Omega_i := (D_i, M_i)$ . We say that  $\Omega_i$  fixes Alice's input if  $D_i = Alice$ , and otherwise  $\Omega_i$  fixes Bob's input. We write  $\Omega$  to denote the random variable  $(\Omega_1, \dots, \Omega_m, X_C, Y_C)$ , where  $X_C Y_C$  are Alice and Bob's questions in the coordinates indexed by  $C$ . For  $i \in [m]$  we write  $\Omega_{-i}$  to denote the random variable  $\Omega$  with  $\Omega_i$  omitted.

**Proposition 10.** *Conditioned on  $\Omega$ ,  $X_{[n]}$  and  $Y_{[n]}$  are independent.*

Finally, we will define a *dependency-breaking variable*  $R := (\Omega, A_C, B_C)$ , where  $A_C$  and  $B_C$  are the players' answers in the coordinates indexed by  $C$ . For  $i \notin C$ , we let  $R_{-i} := (\Omega_{-i}, A_C, B_C)$ .  $R_i$  will refer to  $\Omega_i$ . We will use lowercase letters to denote instantiations of these random variables: e.g.,  $r_{-i}$ ,  $x_i$ , and  $y_i$  refer to specific values of  $R_{-i}$ ,  $X_i$ , and  $Y_i$ .

Throughout our proofs, all expectations are implicitly over the measure defined by  $P$ . For example, the expectation  $\mathbb{E}_{\Omega_{-i}Z|x_i,y_i}$  indicates  $\sum_{\omega_{-i},a_C,b_C} P_{\Omega_{-i}A_C B_C|x_i,y_i}(\omega_{-i},a_C,b_C)$ . Given an event such as  $W$  (winning all the coordinates) or  $W_C$  (winning all the coordinates in  $C$ ),  $P(W)$  and  $P(W_C)$  will mean the probability of these events with respect to the distribution  $P$ .

The following Lemma expresses the idea that, because  $W_C$  is an event that occurs with not-too-small probability, conditioning on it cannot skew the distribution of variables corresponding to an average coordinate by too much. This Lemma follows in a straightforward manner from the [Hol09].

**Lemma 11.** *The following statements hold on, average over  $i$  chosen uniformly in  $[m]$ :*

1.  $\mathbb{E}_i \|P_{R_i X_i Y_i | W_C} - P_{R_i X_i Y_i}\|_1 \leq O(\sqrt{\delta})$
2.  $\mathbb{E}_i \|P_{X_i Y_i R_{-i} | W_C} - P_{X_i Y_i} \cdot P_{R_{-i} | X_i W_C}\|_1 \leq O(\sqrt{\delta})$
3.  $\mathbb{E}_i \|P_{X_i Y_i R_{-i} | W_C} - P_{X_i Y_i} \cdot P_{R_{-i} | Y_i W_C}\|_1 \leq O(\sqrt{\delta})$

where  $\delta := \frac{1}{m} (\log 1/P(W_C) + |C| \log |\mathcal{A}||\mathcal{B}|)$ .

### 3.2 Two key Lemmas, and proof of the Main Theorem

For every  $i \in [n] - C$ , we will construct a collection of bipartite states  $\{|\Psi_{r_{-i},x_i,y_i}\rangle\} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$ , which we call dependency-breaking states, that are indexed by the dependency-breaking variable  $r_{-i}$  defined above, and questions  $(x_i, y_i)$ . The following lemmas state the important properties of this collection of states:

**Lemma 12 (Usefulness Lemma).** *For all  $r_{-i}, x_i, y_i$ , there exist POVMs  $\{\widehat{A}_{r_{-i},x_i}^{a_i}\}$  and  $\{\widehat{B}_{r_{-i},y_i}^{b_i}\}$  acting on  $\mathbb{C}^d$  such that*

$$P_{A_i B_i | r_{-i}, x_i, y_i}(a_i, b_i) = \text{Tr} \left( \widehat{A}_{r_{-i},x_i}^{a_i} \otimes \widehat{B}_{r_{-i},y_i}^{b_i} \Psi_{r_{-i},x_i,y_i} \right).$$

**Lemma 13 (Sampleability Lemma).** *There exists an integer  $d' \geq d$  such that for every  $i, r_{-i}, x_i, y_i$ , there exist local unitaries  $U_{r_{-i},x_i}, V_{r_{-i},y_i}$  acting on  $\mathbb{C}^{d'}$  such that*

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i} | x_i, y_i, W_C} \left\| U_{r_{-i},x_i} \otimes V_{r_{-i},y_i} |E_{dd'}\rangle - |\Psi_{r_{-i},x_i,y_i}\rangle |E_{d'}\rangle \right\| \right] \leq O((\delta^{1/4}/P(W_C))^{1/12})$$

where  $|E_{dd'}\rangle$  and  $|E_{d'}\rangle$  are  $dd'$  and  $d'$ -dimensional embezzlement states, respectively, and  $\delta$  is defined to be  $\frac{1}{m} (\log 1/P(W_C) + |C| \log |\mathcal{A}||\mathcal{B}|)$ .

Lemma 12 shows that the states  $|\Psi_{r_{-i},x_i,y_i}\rangle$  are *useful* to have; they allow Alice and Bob to produce answers in the  $i$ 'th coordinate whose statistics are consistent with the dependency-breaking variable  $r_{-i}$  and their inputs  $(x_i, y_i)$ . Lemma 13 shows that these states are *locally generatable* by Alice and Bob, when given joint access to preshared entanglement, the dependency-breaking variable  $r_{-i}$  and their own inputs  $x_i$  and  $y_i$  respectively.

Using these two Lemmas we can prove the Main Theorem.

*Proof of the Main Theorem.* Consider the following strategy for the game  $G$ . Alice and Bob share beforehand the embezzlement state  $|E_{dd'}\rangle$  of dimension  $dd'$  given by Lemma 13, and they also have access to shared randomness. Given inputs  $(x_i, y_i)$  distributed according to  $P_{X_i Y_i} = \mu$ :

1. Alice and Bob jointly sample a uniformly random  $i \in [n] - C$ .
2. Alice and Bob jointly, approximately sample  $R_{-i}$  from  $P_{R_{-i}|x_i, y_i, W_C}$  using the classical correlated sampling procedure.
3. Alice applies  $U_{r_{-i}, x_i}$  to her side of  $|E_{dd'}\rangle$
4. Bob applies  $V_{r_{-i}, y_i}$  to his side of  $|E_{dd'}\rangle$
5. Alice measures her side of the entanglement using  $\{\hat{A}_{r_{-i}, x_i}^{a_i}\}$  and outputs the outcome  $a_i$
6. Bob measures his side of the entanglement using  $\{\hat{B}_{r_{-i}, y_i}^{b_i}\}$  and outputs the outcome  $b_i$

We now analyze the success probability of this strategy. We will use  $\tilde{P}$  to denote the distribution of variables in the probability space associated with an execution of this strategy. For example, we will write  $\tilde{P}_{R_{-i}|X_i Y_i}$  to denote the distribution of  $R_{-i}$  conditioned on  $X_i Y_i$  that is sampled in Step 1. From Lemma 11 we have that on average over  $i$ ,  $P_{X_i Y_i R_{-i}|W_C} \approx P_{X_i Y_i} \cdot P_{R_{-i}|X_i W_C} \approx P_{X_i Y_i} \cdot P_{R_{-i}|Y_i W_C}$  where “ $\approx$ ” means closeness in statistical distance. By invoking the classical correlated sampling procedure of Lemma 7, we get

$$\mathbb{E}_i \|P_{X_i Y_i} \cdot \tilde{P}_{R_{-i}|X_i Y_i} - P_{X_i Y_i R_{-i}|W_C}\|_1 \leq O(\sqrt{\delta}).$$

After Step 3, Alice and Bob will possess a state  $|\Lambda_{r_{-i}, x_i, y_i}\rangle$  such that

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i}|x_i, y_i, W_C} \|\Lambda_{r_{-i}, x_i, y_i} - \Psi_{r_{-i}, x_i, y_i}\|_1 \right] \leq \eta$$

where  $\eta = O((\delta^{1/4}/P(W_C))^{1/12})$ . Consider the measurement process in Steps 4 and 5. Let  $\tilde{P}_{A_i B_i | r_{-i}, x_i, y_i}$  denote the distribution of measurement outcomes in this strategy, conditioned on their inputs and a sampled value of  $r_{-i}$ . By Lemma 12 and the fact that the trace norm is nonincreasing under quantum operations, we have that

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i}|x_i, y_i, W_C} \|\tilde{P}_{A_i B_i | x_i, y_i, r_{-i}} - P_{A_i B_i | x_i, y_i, r_{-i}}\|_1 \right] \leq \eta$$

or equivalently

$$\mathbb{E}_i \|P_{X_i Y_i} \cdot \tilde{P}_{R_{-i}|X_i Y_i W_C} \cdot \tilde{P}_{A_i B_i | x_i, y_i, r_{-i}} - P_{X_i Y_i} \cdot P_{R_{-i}|X_i Y_i W_C} \cdot P_{A_i B_i R_{-i}|X_i Y_i W_C}\|_1 \leq \eta.$$

By Lemma 11 we have  $\mathbb{E}_i \|P_{X_i Y_i | W_C} - P_{X_i Y_i}\| \leq \sqrt{\delta}$ . By triangle inequality and that  $\tilde{P}_{X_i Y_i} = P_{X_i Y_i}$ , we have

$$\mathbb{E}_i \|\tilde{P}_{X_i Y_i R_{-i} A_i B_i} - P_{X_i Y_i R_{-i} A_i B_i | W_C}\|_1 \leq O(\eta).$$

Note that  $\tilde{P}_{X_i Y_i R_{-i} A_i B_i}$  represents the probability distribution of all the variables present in the strategy above. Let  $W_i$  denote the probability the players win the  $i$ th coordinate. Thus we get

$$\mathbb{E}_i |\tilde{P}(W_i) - P(W_i|W_C)| \leq O(\eta). \quad (4)$$

Assume that

$$P(W) \geq \frac{cs \log n}{\varepsilon^{17} n^{1/4}}$$

where  $c > 0$  is a universal constant, and  $s$  is the bit-length of the players' answers. Since  $P(W_C) \geq P(W)$ , and using our bound on  $|C|$  (from Proposition 9) and our bound on  $\delta$  (from Lemma 11), this implies that the right hand side of (4) is at most  $\varepsilon/4$  (for an appropriate choice of  $c$ ). This implies that

$$\begin{aligned} \mathbb{E}_i \tilde{P}(W_i) &\geq \mathbb{E}_i P(W_i|W_C) - \varepsilon/4 \\ &\geq 1 - \varepsilon/2 - \varepsilon/4 \\ &> \text{val}^*(G) \end{aligned}$$

where in the second line we used the bound from Proposition 9. However, this implies that there exists an  $i$  such that  $\tilde{P}(W_i) > \text{val}^*(G)$ , which is a contradiction. Therefore  $P(W) \leq \frac{cs \log n}{\varepsilon^{17} n^{1/4}}$ .  $\square$

## 4 Proofs of the two Key Lemmas

Now we turn to proving the two key lemmas above, the Usefulness Lemma and the Sampleability Lemma.

### 4.1 Quantum states and operators

In this subsection we define the states  $|\Psi_{r_{-i}, x_i, y_i}\rangle$  and measurement operators  $\{\hat{A}_{r_{-i}, x_i}^{a_i}\}$  and  $\{\hat{B}_{r_{-i}, y_i}^{b_i}\}$ . Recall that the dependency-breaking variable  $R$  consists of the set of fixed questions  $\Omega = (X_C, Y_C, \Omega_1, \dots, \Omega_m)$  and fixed answers  $Z = (A_C, B_C)$  for the coordinates in  $C$ .

**Coarse-grained measurements.** We first *coarsen* the measurement POVMs  $\{A_{x_{[n]}}^{a_{[n]}}\}$  and  $\{B_{y_{[n]}}^{b_{[n]}}\}$  that constitute Alice and Bob's strategy in  $G^n$  to construct a set of *intermediate measurements*, which essentially produce answers for the games in set  $C$ , conditioned on a setting of  $\Omega$ .

Fix  $i, \omega, a_C, b_C, x_i, y_i$ . Define

$$A_{\omega_{-i}, x_i}^{a_C} = \sum_{a_{[n]}|a_C} \mathbb{E}_{X_{[n]}|\omega_{-i}, x_i} A_{x_{[n]}}^{a_{[n]}} \quad B_{\omega_{-i}, y_i}^{b_C} = \sum_{b_{[n]}|b_C} \mathbb{E}_{Y_{[n]}|\omega_{-i}, y_i} B_{y_{[n]}}^{b_{[n]}}$$

where  $a_{[n]}|a_C$  (resp.  $b_{[n]}|b_C$ ) indicates summing over all tuples  $a_{[n]}$  consistent with the suffix  $a_C$  (resp.  $b_{[n]}$  consistent with suffix  $b_C$ ) and recall that  $\mathbb{E}_{X_{[n]}|\omega_{-i}, x_i}$  is shorthand for  $\sum_{x_{[n]}} P_{X_{[n]}|\Omega_{-i}=\omega_{-i}, X_i=x_i}(x_{[n]})$ . We also define

$$A_{\omega}^{a_C} = \mathbb{E}_{X_{[n]}|\omega} A_{x_{[n]}}^{a_C} \quad B_{\omega}^{b_C} = \mathbb{E}_{Y_{[n]}|\omega} B_{y_{[n]}}^{b_C}.$$

Let  $\rho$  denote the reduced density matrix of  $|\psi\rangle$  on Alice's side. Since we have assumed that  $|\psi\rangle$  is symmetric,  $\rho$  is also the reduced density matrix on Bob's side. For all  $i, \omega, x_i, y_i, a_C, b_C$ , let  $U_{\omega-i, x_i, a_C}, U_{\omega, a_C}, V_{\omega-i, y_i, b_C}$ , and  $V_{\omega, b_C}$  be unitaries such that

$$\begin{aligned} U_{\omega-i, x_i, a_C} (A_{\omega-i, x_i}^{a_C})^{1/2} \sqrt{\rho} & & V_{\omega-i, y_i, b_C} (B_{\omega-i, y_i}^{b_C})^{1/2} \sqrt{\rho} \\ U_{\omega, a_C} (A_{\omega}^{a_C})^{1/2} \sqrt{\rho} & & V_{\omega, b_C} (B_{\omega}^{b_C})^{1/2} \sqrt{\rho} \end{aligned}$$

are positive semidefinite. Such unitaries can be found via singular value decompositions. For notational convenience, let

$$\begin{aligned} S_{\omega-i, x_i, a_C} &= U_{\omega-i, x_i, a_C} (A_{\omega-i, x_i}^{a_C})^{1/2} & T_{\omega-i, y_i, b_C} &= V_{\omega-i, y_i, b_C} (B_{\omega-i, y_i}^{b_C})^{1/2} \\ S_{\omega, a_C} &= U_{\omega, a_C} (A_{\omega}^{a_C})^{1/2} & T_{\omega, b_C} &= V_{\omega, b_C} (B_{\omega}^{b_C})^{1/2} \end{aligned}$$

**Fine-grained measurements.** Now we can define the *fine-grained measurements* that Alice and Bob can apply to obtain answers for the  $i$ 'th game. Define

$$\widehat{A}_{r-i, x_i}^{a_i} = S_{\omega-i, x_i, a_C}^{-1} A_{\omega-i, x_i}^{a_C, a_i} S_{\omega-i, x_i, a_C}^{-1} \quad \widehat{B}_{r-i, y_i}^{b_i} = T_{\omega-i, y_i, b_C}^{-1} B_{\omega-i, y_i}^{b_C, b_i} T_{\omega-i, y_i, b_C}^{-1}$$

where

$$A_{\omega-i, x_i}^{a_C, a_i} = \sum_{a_{[n]} | a_C, a_i} \mathbb{E}_{X_{[n]} | \omega-i, x_i} A_{x_{[n]}}^{a_{[n]}} \quad B_{\omega-i, y_i}^{b_C, b_i} = \sum_{b_{[n]} | b_C, b_i} \mathbb{E}_{Y_{[n]} | \omega-i, y_i} B_{y_{[n]}}^{b_{[n]}}$$

and  $a_{[n]} | a_C, a_i$  (resp.  $b_{[n]} | b_C, b_i$ ) denotes summing over all  $a_{[n]}$  consistent with  $a_C$  and  $a_i$  (resp. all  $b_{[n]}$  consistent with  $b_C$  and  $b_i$ ). It is easy to verify that the sets  $\{\widehat{A}_{r-i, x_i}^{a_i}\}_{a_i \in \mathcal{A}}$  and  $\{\widehat{B}_{r-i, y_i}^{b_i}\}_{b_i \in \mathcal{B}}$  form POVMs. Here, for a square matrix  $A$ ,  $A^{-1}$  denotes its generalized inverse.

**States.** Now we are ready to define the states. Fix  $i, r-i = (\omega-i, a_C, b_C)$ , and  $x_i, y_i$ . Then let

$$|\Psi_{r-i, x_i, y_i}\rangle = \frac{S_{\omega-i, a_C, x_i} \otimes T_{\omega-i, b_C, y_i} |\psi\rangle}{\|S_{\omega-i, a_C, x_i} \otimes T_{\omega-i, b_C, y_i} |\psi\rangle\|}.$$

Observe that the normalization  $\|S_{\omega-i, a_C, x_i} \otimes T_{\omega-i, b_C, y_i} |\psi\rangle\|^2$  is equal to  $\mathbb{P}_{A_C B_C | \omega-i, x_i, y_i}(a_C, b_C)$ .

## 4.2 Proof of Usefulness Lemma (Lemma 12)

This Lemma follows from a simple calculation: for every  $x_i, y_i, a_i, b_i, r-i$ :

$$\begin{aligned} & \text{Tr} \left( \widehat{A}_{r-i, x_i}^{a_i} \otimes \widehat{B}_{r-i, y_i}^{b_i} \Psi_{r-i, x_i, y_i} \right) \\ &= \frac{1}{\|S_{\omega-i, a_C, x_i} \otimes T_{\omega-i, b_C, y_i} |\psi\rangle\|^2} \text{Tr} \left( A_{\omega-i, x_i}^{a_C, a_i} \otimes B_{\omega-i, y_i}^{b_C, b_i} |\psi\rangle\langle\psi| \right) \\ &= \frac{1}{\mathbb{P}_{A_C B_C | \omega-i, x_i, y_i}(a_C, b_C)} \sum_{a_{[n]} | a_C, a_i} \sum_{b_{[n]} | b_C, b_i} \mathbb{E}_{X_{[n]} Y_{[n]} | \omega-i, x_i, y_i} \text{Tr} \left( A_{x_{[n]}}^{a_{[n]}} \otimes B_{y_{[n]}}^{b_{[n]}} |\psi\rangle\langle\psi| \right) \\ &= \frac{\mathbb{P}_{A_i B_i A_C B_C | \omega-i, x_i, y_i}(a_i, b_i, a_C, b_C)}{\mathbb{P}_{A_C B_C | \omega-i, x_i, y_i}(a_C, b_C)} \\ &= \mathbb{P}_{A_i B_i | r-i, x_i, y_i}(a_i, b_i). \end{aligned}$$

In the second equality we used that conditioned on  $\Omega, X_{[n]}$  and  $Y_{[n]}$  are independent, so therefore  $\mathbb{E}_{X_{[n]} | \omega-i, x_i} \mathbb{E}_{Y_{[n]} | \omega-i, y_i} = \mathbb{E}_{X_{[n]} Y_{[n]} | \omega-i, x_i, y_i}$ . In the last equality we used that  $r-i = (\omega-i, a_C, b_C)$ . This concludes the Usefulness Lemma.

### 4.3 Proof of the Sampleability Lemma (Lemma 13)

**Overview.** Here we give some intuition. We first analyze an ensemble of states  $\{|\Gamma_{x_i, x_C, a_C}\rangle\}$  (for now we omit mention of the dependency-breaking variable  $R$  for simplicity). These are indexed by Alice's questions in the  $i$ 'th coordinate, her questions in the  $C$  coordinates, as well as her answers in the  $C$  coordinates. The state  $|\Gamma_{x_i, x_C, a_C}\rangle$  roughly represents the state of the players where only Alice has applied her measurements – Bob hasn't done anything yet.

Fix a  $y_i, x_C, a_C$ . For average  $x_i, x'_i$  that are independently sampled from the marginal distribution  $P_{X_i|Y_i=y_i}$ , we will show that

$$\| |\Gamma_{x_i, x_C, a_C}\rangle - |\Gamma_{x'_i, x_C, a_C}\rangle \| \sim \frac{1}{n}.$$

To handle issues such as Alice “printing” her input onto the state  $|\psi\rangle$  (as discussed in the introduction), the definition of  $|\Gamma_{x_i, x_C, a_C}\rangle$  requires local unitaries that “undo” such overt actions of Alice and Bob – this is accomplished by the unitaries  $U$  and  $V$  defined in Section 4.1.

Then, we consider what happens when we apply Bob's measurement to both states  $|\Gamma_{x_i, x_C, a_C}\rangle$  and  $|\Gamma_{x'_i, x_C, a_C}\rangle$ , and condition on obtaining answers  $b_C$  for the  $C$  coordinates. His measurement will depend on the questions  $y_i$  and  $y_C$ . The post-measurement states will be precisely  $|\Psi_{x_i, y_i, x_C, y_C, a_C, b_C}\rangle$  and  $|\Psi_{x'_i, y_i, x_C, y_C, a_C, b_C}\rangle$ . The distance between these states will be, roughly speaking, the distance between  $|\Gamma_{x_i, x_C, a_C}\rangle$  and  $|\Gamma_{x'_i, x_C, a_C}\rangle$  divided by the probability of Bob obtaining outcome  $b_C$  conditioned on Alice obtaining  $a_C$ . If we average this distance over all choices of  $x_C, y_C, a_C, b_C$  that imply the event  $W_C$ , we get that the average distance between  $|\Psi_{x_i, y_i, x_C, y_C, a_C, b_C}\rangle$  and  $|\Psi_{x'_i, y_i, x_C, y_C, a_C, b_C}\rangle$  is approximately  $\frac{1}{nP(W_C)}$ . If  $P(W)$  is much greater than  $1/n$ , then this distance is small. We then invoke quantum correlated sampling (Lemma 8), and that proves the Sampleability Lemma.

**Proof.** We introduce the following state:

$$\xi_{\Omega X_{[n]} E_A E_B A_C} = \sum_{\omega, x_{[n]}, a_C} P_{\Omega X_{[n]}}(\omega, x_{[n]}) |\omega x_{[n]}\rangle\langle\omega x_{[n]}| \otimes \sqrt{A_{x_{[n]}}^{a_C}} |\psi\rangle\langle\psi| \sqrt{A_{x_{[n]}}^{a_C}} \otimes |a_C\rangle\langle a_C|.$$

If we trace out the  $E_A$  register, we have that

$$\begin{aligned} \xi_{\Omega X_{[n]} E_B A_C} &= \sum_{\omega, x_{[n]}, a_C} P_{\Omega X_{[n]}}(\omega, x_{[n]}) |\omega x_{[n]}\rangle\langle\omega x_{[n]}| \otimes \sqrt{\rho} \overline{A_{x_{[n]}}^{a_C}} \sqrt{\rho} \otimes |a_C\rangle\langle a_C| \\ &\preceq \sum_{\omega, x_{[n]}, a_C} P_{\Omega X_{[n]}}(\omega, x_{[n]}) |\omega x_{[n]}\rangle\langle\omega x_{[n]}| \otimes \sqrt{\rho} \overline{A_{x_{[n]}}^{a_C}} \sqrt{\rho} \otimes \mathbf{I} \\ &= \sum_{\omega, x_{[n]}} P_{\Omega X_{[n]}}(\omega, x_{[n]}) |\omega x_{[n]}\rangle\langle\omega x_{[n]}| \otimes \rho \otimes \mathbf{I}, \end{aligned}$$

where  $\rho$  is the reduced density matrix of  $|\psi\rangle = \sum_j \sqrt{\lambda_j} |v_j\rangle |v_j\rangle$  on  $E_B$ ,  $\overline{A_{x_{[n]}}^{a_C}}$  denotes the entry-wise complex conjugate of  $A_{x_{[n]}}^{a_C}$  with respect to the basis  $\{|v_j\rangle\}$ , and the last equality uses  $\sum_{a_C} \overline{A_{x_{[n]}}^{a_C}} = \mathbf{I}$ . From the definition of  $S_\infty$  we have

$$\begin{aligned} |C| \cdot \log |\mathcal{A}| &\geq S_\infty \left( \xi_{\Omega X_{[n]} E_B A_C} \left\| \xi_{\Omega X_{[n]}} \otimes \xi_{E_B} \otimes \frac{\mathbf{I}}{\text{Tr}(\mathbf{I})} \right\| \right) \\ &\geq S \left( \xi_{\Omega X_{[n]} E_B A_C} \left\| \xi_{\Omega X_{[n]}} \otimes \xi_{E_B} \otimes \frac{\mathbf{I}}{\text{Tr}(\mathbf{I})} \right\| \right) \quad (S(\cdot\|\cdot) \leq S_\infty(\cdot\|\cdot)) \end{aligned}$$

$$\geq \mathbb{E}_{\Omega, A_C} S \left( \zeta_{X_{[n]} E_B | \omega, a_C} \left\| \zeta_{X_{[n]} | \omega} \otimes \zeta_{E_B} \right\| \right) \quad (\text{Lemma 5})$$

Now we apply Quantum Raz's Lemma:

$$\mathbb{E}_{\Omega, A_C} \mathbb{E}_i I(X_i; E_B | \omega, a_C)_{\zeta} \leq \frac{|C| \cdot \log |\mathcal{A}|}{m} \leq \delta \quad (5)$$

where recall that we defined  $\delta = (|C| \log |\mathcal{A}| \cdot |B|) / m$ . Applying the inequalities of Pinsker and Jensen, we obtain

$$\mathbb{E}_{\Omega, A_C} \mathbb{E}_i \mathbb{E}_{X_i | \omega, a_C} \left\| \zeta_{E_B | \omega, x_i, a_C} - \zeta_{E_B | \omega, a_C} \right\|_1 \leq \sqrt{\delta}. \quad (6)$$

These marginal density matrices have a nice description. Fix  $i, \omega, x_i, a_C$ . First we note that the state  $\zeta_{E_B | \omega, x_i, a_C}$  does not depend on  $\omega_i$ , because we are already conditioning on  $x_i$ . Thus we can write it as  $\zeta_{E_B | \omega_{-i}, x_i, a_C}$ . Then

$$\begin{aligned} \zeta_{E_B | \omega_{-i}, a_C, x_i} &= \frac{1}{\mathbb{P}_{A_C | \omega_{-i}, x_i}(a_C)} \sum_{x_{[n]}} \mathbb{P}_{X_{[n]} | \omega_{-i}, x_i}(x_{[n]}) \sqrt{\bar{\rho} A_{x_{[n]}}^{a_C}} \sqrt{\bar{\rho}} \\ &= \frac{1}{\mathbb{P}_{A_C | \omega_{-i}, x_i}(a_C)} \sqrt{\bar{\rho}} \left( \sum_{x_{[n]}} \mathbb{P}_{X_{[n]} | \omega_{-i}, x_i}(x_{[n]}) \overline{A_{x_{[n]}}^{a_C}} \right) \sqrt{\bar{\rho}} \\ &= \frac{1}{\mathbb{P}_{A_C | \omega_{-i}, x_i}(a_C)} \sqrt{\bar{\rho} \overline{A_{\omega_{-i}, x_i}^{a_C}}} \sqrt{\bar{\rho}}. \end{aligned}$$

Similarly,

$$\zeta_{E_B | \omega, a_C} = \frac{1}{\mathbb{P}_{A_C | \omega}(a_C)} \sqrt{\bar{\rho} \overline{A_{\omega}^{a_C}}} \sqrt{\bar{\rho}}.$$

For all  $\omega, x_i, a_C$ , define the following (unnormalized) states:

$$|\Gamma_{\omega_{-i}, x_i, a_C}\rangle = S_{\omega_{-i}, x_i, a_C} \otimes \mathbb{I} |\psi\rangle \quad |\Gamma_{\omega, a_C}\rangle = S_{\omega, a_C} \otimes \mathbb{I} |\psi\rangle \quad (7)$$

where the  $S$  operators were defined in Section 4.1. Let  $\gamma_{\omega_{-i}, x_i, a_C} = (\mathbb{P}_{A_C | \omega_{-i}, x_i}(a_C))^{1/2} = \|\Gamma_{\omega_{-i}, x_i, a_C}\|$  and  $\gamma_{\omega, a_C} = (\mathbb{P}_{A_C | \omega}(a_C))^{1/2} = \|\Gamma_{\omega, a_C}\|$  denote their norms. We will write

$$|\tilde{\Gamma}_{\omega_{-i}, x_i, a_C}\rangle = \gamma_{\omega_{-i}, x_i, a_C}^{-1} |\Gamma_{\omega_{-i}, x_i, a_C}\rangle \quad |\tilde{\Gamma}_{\omega, a_C}\rangle = \gamma_{\omega, a_C}^{-1} |\Gamma_{\omega, a_C}\rangle$$

to denote the normalized states.

For notational convenience we will suppress mention of  $\omega_{-i}$  and  $z = (a_C, b_C)$ , and implicitly carry them around. Thus, for example, when we write  $|\Gamma_{x_i}\rangle$  and  $|\Gamma_{\omega_i}\rangle$ , we implicitly mean  $|\Gamma_{\omega_{-i}, x_i, a_C}\rangle$  and  $|\Gamma_{\omega, a_C}\rangle$ , respectively.

Fix  $x_i$ , and consider the following:

$$\begin{aligned} &\| |\tilde{\Gamma}_{x_i}\rangle - |\tilde{\Gamma}_{\omega_i}\rangle \|^2 \\ &= \left( \langle \tilde{\Gamma}_{x_i} | - \langle \tilde{\Gamma}_{\omega_i} | \right) \left( |\tilde{\Gamma}_{x_i}\rangle - |\tilde{\Gamma}_{\omega_i}\rangle \right) \\ &= \langle \psi | (\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i})^\dagger (\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i}) \otimes \mathbb{I} | \psi \rangle \end{aligned}$$

$$\begin{aligned}
&= \text{Tr} \left( \sqrt{\rho} (\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i})^\dagger (\gamma_{x_i}^{-1} S_{x_i} - \gamma_{\omega_i}^{-1} S_{\omega_i}) \sqrt{\rho} \right) \quad (\text{Ando's Identity}) \\
&= \|\gamma_{x_i}^{-1} S_{x_i} \sqrt{\rho} - \gamma_{\omega_i}^{-1} S_{\omega_i} \sqrt{\rho}\|_F^2.
\end{aligned}$$

Next we use the Powers-Størmer inequality [PS70], which states that for positive semidefinite operators  $A, B$ , we have  $\|A - B\|_F^2 \leq \|A^2 - B^2\|_1$ . Since  $S_{x_i} \sqrt{\rho}$  and  $S_{\omega_i} \sqrt{\rho}$  are by construction positive semidefinite, the above is bounded by

$$\leq \|\gamma_{x_i}^{-2} S_{x_i} \rho S_{x_i}^\dagger - \gamma_{\omega_i}^{-2} S_{\omega_i} \rho S_{\omega_i}^\dagger\|_1. \quad (8)$$

We can write  $S_{x_i} \rho S_{x_i}^\dagger = U_{x_i} (A_{x_i})^{1/2} \rho (A_{x_i})^{1/2} U_{x_i}^\dagger = \sqrt{\rho} A_{x_i} \sqrt{\rho}$  and  $S_{\omega_i} \rho S_{\omega_i}^\dagger = \sqrt{\rho} A_{\omega_i} \sqrt{\rho}$ . Next we observe that for any square matrix  $A$ ,  $\|A\|_1 = \|\bar{A}\|_1$ , where  $\bar{A}$  denotes the entry-wise complex conjugate in some basis. By taking the complex conjugate with respect to the basis that diagonalizes  $\rho$ , we have that (8) is equal to

$$\|\gamma_{x_i}^{-2} \sqrt{\rho} \bar{A}_{x_i} \sqrt{\rho} - \gamma_{\omega_i}^{-2} \sqrt{\rho} \bar{A}_{\omega_i} \sqrt{\rho}\|_1. \quad (9)$$

We see that (9), averaged over  $i, \omega, a_C$  and  $x_i$  is exactly the quantity bounded in (6). Applying Jensen's inequality, we have

$$\delta^{1/4} \geq \mathbb{E}_i \mathbb{E}_{\Omega_{AC} X_i} \|\tilde{\Gamma}_{\omega_{-i}, x_i, a_C} - \tilde{\Gamma}_{\omega, a_C}\| \quad (10)$$

$$\geq \mathbb{E}_i \mathbb{E}_{\Omega_{AC} X_i} \|\tilde{\Gamma}\langle\tilde{\Gamma}|\omega_{-i}, x_i, a_C - \tilde{\Gamma}\langle\tilde{\Gamma}|\omega, a_C\|_1 \quad (11)$$

where in the second line we used Fact 2, and we write  $|\tilde{\Gamma}\langle\tilde{\Gamma}|\omega_{-i}, x_i, a_C$  instead of  $|\tilde{\Gamma}_{\omega_{-i}, x_i, a_C}\langle\tilde{\Gamma}_{\omega_{-i}, x_i, a_C}|$  to save space.

Define the cq-states

$$\Phi_{\Omega X_i E_A E_B A_C}^i = \sum_{\omega, a_C, x_i} P_{\Omega_{AC} X_i}(\omega, a_C, x_i) |\omega x_i\rangle\langle\omega x_i| \otimes |\tilde{\Gamma}\langle\tilde{\Gamma}|\omega_{-i}, x_i, a_C \otimes |a_C\rangle\langle a_C|$$

and

$$\hat{\Phi}_{\Omega X_i E_A E_B A_C}^i = \sum_{\omega, a_C, x_i} P_{\Omega_{AC} X_i}(\omega, a_C, x_i) |\omega x_i\rangle\langle\omega x_i| \otimes |\tilde{\Gamma}\langle\tilde{\Gamma}|\omega, a_C \otimes |a_C\rangle\langle a_C|$$

so that the bound in (11) is equivalent to

$$\mathbb{E}_i \left\| \Phi_{\Omega X_i E_A E_B A_C}^i - \hat{\Phi}_{\Omega X_i E_A E_B A_C}^i \right\|_1 \leq \delta^{1/4} \quad (12)$$

We define the quantum operation  $\mathcal{E}$  acting on registers  $\Omega E_B$  as follows: for all  $\omega$  and density matrices  $\tau$ ,

$$\mathcal{E} : |\omega\rangle\langle\omega| \otimes \tau \mapsto |\omega\rangle\langle\omega| \otimes \sum_{b_C} T_{\omega, b_C} \tau T_{\omega, b_C}^\dagger \otimes |b_C\rangle\langle b_C|.$$

In other words, the quantum operation  $\mathcal{E}$  will, controlled on  $\Omega$ , apply the measurement corresponding to the  $T_{\omega, b_C}$  operators (defined in Section 4.1) to the  $E_B$  part of the state, and save the measurement outcomes in an ancilla register.

The operation  $\mathcal{E}$  is an isometry, so we have that

$$\mathbb{E}_i \left\| \mathcal{E} \left( \Phi_{\Omega X_i E_A E_B A_C}^i \right) - \mathcal{E} \left( \hat{\Phi}_{\Omega X_i E_A E_B A_C}^i \right) \right\|_1 \leq \delta^{1/4}. \quad (13)$$



Let us examine what happens when we apply  $\mathcal{E}$  to  $\Phi_{\Omega X_i E_A E_B A_C}^i$ :

$$\begin{aligned}
& \mathcal{E} \left( \Phi_{\Omega X_i E_A E_B A_C}^i \right) \\
&= \mathbb{E}_{\Omega A_C X_i} |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{b_C} T_{\omega, b_C} |\tilde{\Gamma}_{\omega-i, x_i, a_C}\rangle\langle\tilde{\Gamma}_{\omega-i, x_i, a_C}| T_{\omega, b_C}^\dagger \otimes |a_C b_C\rangle\langle a_C b_C| \\
&= \mathbb{E}_{\Omega X_i} \sum_{a_C} P_{A_C|\omega, x_i}(a_C) |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{b_C} \frac{T_{\omega, b_C} |\Gamma_{\omega-i, x_i, a_C}\rangle\langle\Gamma_{\omega-i, x_i, a_C}| T_{\omega, b_C}^\dagger}{P_{A_C|\omega-i, x_i}(a_C)} \otimes |a_C b_C\rangle\langle a_C b_C| \\
&= \mathbb{E}_{\Omega X_i} |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{a_C, b_C} T_{\omega, b_C} |\Gamma_{\omega-i, x_i, a_C}\rangle\langle\Gamma_{\omega-i, x_i, a_C}| T_{\omega, b_C}^\dagger \otimes |a_C b_C\rangle\langle a_C b_C|
\end{aligned}$$

where in the second equality we used that the normalization of  $|\tilde{\Gamma}\rangle\langle\tilde{\Gamma}|$  is equal to  $P_{A_C|\omega-i, x_i}(a_C)$ , and that  $P_{A_C|\omega, x_i}(a_C) = P_{A_C|\omega-i, x_i}(a_C)$ . Similarly, we have that

$$\mathcal{E} \left( \hat{\Phi}_{\Omega X_i E_A E_B A_C}^i \right) = \mathbb{E}_{\Omega X_i} |\omega x_i\rangle\langle\omega x_i| \otimes \sum_{a_C, b_C} T_{\omega, b_C} |\Gamma_{\omega, a_C}\rangle\langle\Gamma_{\omega, a_C}| T_{\omega, b_C}^\dagger \otimes |a_C b_C\rangle\langle a_C b_C|.$$

Define  $\Lambda_{\Omega X_i E_A E_B A_C B_C}^i = \mathcal{E} \left( \Phi_{\Omega X_i E_A E_B A_C}^i \right)$  and  $\hat{\Lambda}_{\Omega X_i E_A E_B A_C B_C}^i = \mathcal{E} \left( \hat{\Phi}_{\Omega X_i E_A E_B A_C}^i \right)$ . In both these states, the event of  $W_C$  is well defined: the registers  $X_C Y_C$  (which are part of the dependency-breaking variable  $\Omega$ ) and  $A_C B_C$  are classical. Furthermore, we claim that the probability of the event  $W_C$  in  $\Lambda^i$  and  $\hat{\Lambda}^i$  are equal to the probability of  $W_C$  in the actual repeated strategy. Let

$$\Pi = \sum_{\substack{x_C, y_C, a_C, b_C: \\ V(x_C, y_C, a_C, b_C)=1}} |x_C y_C a_C b_C\rangle\langle x_C y_C a_C b_C|$$

be the projector onto the subspace corresponding to the event  $W_C$ . Then for all  $i$

$$\begin{aligned}
& \text{Tr} \left( \Pi \Lambda^i \right) \\
&= \sum_{\omega, x_i} P_{\Omega X_i}(\omega x_i) \sum_{\substack{a_C, b_C: \\ V(x_C, y_C, a_C, b_C)=1}} \langle \Gamma_{\omega-i, x_i, a_C} | T_{\omega, b_C}^\dagger T_{\omega, b_C} | \Gamma_{\omega-i, x_i, a_C} \rangle \\
&= \sum_{\omega, x_i} P_{\Omega X_i}(\omega x_i) \sum_{\substack{a_C, b_C: \\ V(x_C, y_C, a_C, b_C)=1}} \langle \psi | (S_{\omega-i, x_i, a_C} \otimes T_{\omega, b_C})^\dagger (S_{\omega-i, x_i, a_C} \otimes T_{\omega, b_C}) | \psi \rangle \\
&= \sum_{\omega, x_i} P_{\Omega X_i}(\omega x_i) \sum_{\substack{a_C, b_C: \\ V(x_C, y_C, a_C, b_C)=1}} \langle \psi | \left( \sqrt{A_{\omega-i, x_i}^{a_C}} \otimes \sqrt{B_{\omega}^{b_C}} \right)^\dagger \left( \sqrt{A_{\omega-i, x_i}^{a_C}} \otimes \sqrt{B_{\omega}^{b_C}} \right) | \psi \rangle.
\end{aligned}$$

Using the definitions of  $A_{\omega-i, x_i}^{a_C}$  and  $B_{\omega}^{b_C}$  we see that this quantity is identical to  $P(W_C)$ . Similar reasoning shows that  $\text{Tr} \left( \Pi \hat{\Lambda}^i \right) = P(W_C)$ .

Let  $\Lambda_{\Omega X_i E_A E_B A_C B_C | W_C}^i = (\Pi \Lambda^i \Pi) / P(W_C)$  and  $\hat{\Lambda}_{\Omega X_i E_A E_B A_C B_C | W_C}^i = (\Pi \hat{\Lambda}^i \Pi) / P(W_C)$  denote  $\Lambda^i$  and  $\hat{\Lambda}^i$  conditioned on the event  $W_C$ . So we have

$$\mathbb{E}_i \left\| \Lambda_{\Omega X_i E_A E_B A_C B_C | W_C}^i - \hat{\Lambda}_{\Omega X_i E_A E_B A_C B_C | W_C}^i \right\|_1 \leq \frac{\delta^{1/4}}{P(W_C)}. \quad (14)$$

Let us bundle together the  $\Omega$  and  $A_C B_C$  registers into  $R$ . For all  $r = (\omega, a_C, b_C)$  and  $x_i$ , define

$$|\Psi_{r,x_i}\rangle = \frac{S_{\omega,-i,x_i,a_C} \otimes T_{\omega,b_C} |\psi\rangle}{\|S_{\omega,-i,x_i,a_C} \otimes T_{\omega,b_C} |\psi\rangle\|} \quad |\Psi_r\rangle = \frac{S_{\omega,a_C} \otimes T_{\omega,b_C} |\psi\rangle}{\|S_{\omega,a_C} \otimes T_{\omega,b_C} |\psi\rangle\|}$$

Then we see that

$$\Lambda_{RX_i E_A E_B | W_C}^i = \mathbb{E}_{RX_i | W_C} |rx_i\rangle\langle rx_i| \otimes |\Psi_{r,x_i}\rangle\langle\Psi_{r,x_i}|$$

and

$$\widehat{\Lambda}_{RX_i E_A E_B | W_C}^i = \mathbb{E}_{R | W_C} |r\rangle\langle r| \otimes \mathbb{E}_{X_i | \omega} |x_i\rangle\langle x_i| \otimes |\Psi_r\rangle\langle\Psi_r|.$$

We see that  $\Lambda_{RX_i E_A E_B | W_C}^i$  and  $\widehat{\Lambda}_{RX_i E_A E_B | W_C}^i$  are both cq-states that are classical on  $RX_i$  and quantum on  $E_A E_B$ . The inequality in (14) implies that the trace distance between the classical parts of  $\Lambda_{W_C}^i$  and  $\widehat{\Lambda}_{W_C}^i$  is at most  $\delta^{1/4}/P(W_C)$ . Thus we can change the classical part of  $\widehat{\Lambda}_{W_C}^i$  to match the classical part of  $\Lambda_{W_C}^i$  by at most doubling the error:

$$\mathbb{E}_i \left\| \mathbb{E}_{RX_i | W_C} |rx_i\rangle\langle rx_i| \otimes (|\Psi_{r,x_i}\rangle\langle\Psi_{r,x_i}| - |\Psi_r\rangle\langle\Psi_r|) \right\|_1 \leq 2 \frac{\delta^{1/4}}{P(W_C)}.$$

which implies that

$$\mathbb{E}_i \mathbb{E}_{RX_i | W_C} \| |\Psi_{r,x_i}\rangle\langle\Psi_{r,x_i}| - |\Psi_r\rangle\langle\Psi_r| \|_1 \leq \frac{2\delta^{1/4}}{P(W_C)}.$$

By Lemma 11,  $\mathbb{E}_i \|P_{\Omega_i X_i | W_C} - P_{\Omega_i X_i}\|_1 \leq \sqrt{\delta}$ . Applying that to the above, we get

$$\mathbb{E}_i \mathbb{E}_{\Omega_i X_i} \left[ \mathbb{E}_{R_{-i} | \omega_i, x_i, W_C} \| |\Psi_{r,x_i}\rangle\langle\Psi_{r,x_i}| - |\Psi_r\rangle\langle\Psi_r| \|_1 \right] \leq \frac{2\delta^{1/4}}{P(W_C)} + \sqrt{\delta}$$

where the middle expectation over  $\Omega_i X_i$  is over the *prior* distribution (i.e. before conditioning on the event  $W_C$ ). Now observe that in this prior distribution,  $\Omega_i$  fixes  $Y_i$  with probability 1/2, so we in fact get

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i} | x_i, y_i, W_C} \| |\Psi_{r_{-i}, x_i, y_i}\rangle\langle\Psi_{r_{-i}, x_i, y_i}| - |\Psi_{r_{-i}, y_i}\rangle\langle\Psi_{r_{-i}, y_i}| \|_1 \right] \leq \frac{4\delta^{1/4}}{P(W_C)} + 2\sqrt{\delta}$$

where the states  $|\Psi_{r_{-i}, x_i, y_i}\rangle$  were defined in Section 4.1, and  $|\Psi_{r_{-i}, y_i}\rangle$  is  $|\Psi_r\rangle$  where  $r = (r_{-i}, \omega_i)$  and  $\omega_i$  fixes  $Y_i = y_i$ . Applying the Fuchs-van der Graaf inequality, we obtain a bound in terms of Euclidean distance:

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i} | x_i, y_i, W_C} \| |\Psi_{r_{-i}, x_i, y_i}\rangle - |\Psi_{r_{-i}, y_i}\rangle \| \right] \leq O\left((\delta^{1/4}/P(W_C))^{1/2}\right) \quad (15)$$

Similar reasoning implies that

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i} | x_i, y_i, W_C} \| |\Psi_{r_{-i}, x_i, y_i}\rangle - |\Psi_{r_{-i}, x_i}\rangle \| \right] \leq O\left((\delta^{1/4}/P(W_C))^{1/2}\right) \quad (16)$$

where  $|\Psi_{r_{-i},x_i}\rangle$  is  $|\Psi_r\rangle$  where  $r = (r_{-i}, \omega_i)$  and  $\omega_i$  fixes  $X_i = x_i$ . By triangle inequality, we have

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i}|x_i, y_i, W_C} \left\| |\Psi_{r_{-i}, y_i}\rangle - |\Psi_{r_{-i}, x_i}\rangle \right\| \right] \leq O\left((\delta^{1/4}/P(W_C))^{1/2}\right). \quad (17)$$

Let  $\eta := O((\delta^{1/4}/P(W_C))^{1/2})$ . Fix  $r_{-i}, x_i, y_i$ . Since  $r_{-i}$  is public, Alice knows  $r_{-i}, x_i$ , and thus knows a classical description of the state  $|\Psi_{r_{-i}, x_i}\rangle$ . Similarly, Bob knows a classical description of the state  $|\Psi_{r_{-i}, y_i}\rangle$ . By the Quantum Correlated Sampling Lemma of [DSV14] with parameter  $\alpha = \eta^6$ , there exists a dimension  $d'$  that depends only on  $d$  and  $\alpha$ , and unitaries  $U_{r_{-i}, x_i}$  and  $V_{r_{-i}, y_i}$  such that

$$\|U_{r_{-i}, x_i} \otimes V_{r_{-i}, y_i} |E_{dd'}\rangle - |\Psi_{r_{-i}, x_i}\rangle |E_{d'}\rangle\| \leq O(\max\{\alpha^{1/12}, \|\Psi_{r_{-i}, x_i}\rangle - |\Psi_{r_{-i}, y_i}\rangle\|^{1/6}\}).$$

We can average this over  $i, x_i, y_i$ , and  $r_{-i}$  to get that

$$\begin{aligned} & \mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i}|x_i, y_i, W_C} \left\| U_{r_{-i}, x_i} \otimes V_{r_{-i}, y_i} |E_{dd'}\rangle - |\Psi_{r_{-i}, x_i}\rangle |E_{d'}\rangle \right\| \right] \\ & \leq \mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i}|x_i, y_i, W_C} O(\max\{\alpha^{1/12}, \|\Psi_{r_{-i}, x_i}\rangle - |\Psi_{r_{-i}, y_i}\rangle\|^{1/6}\}) \right] \\ & \leq O(\alpha^{1/24}) \\ & = O(\eta^{1/12}) \end{aligned}$$

where in the second inequality we used the following fact: for an nonnegative random variable  $X$  with mean  $\mu = \mathbb{E} X$ , we can bound the expectation  $\mathbb{E} \max\{\sqrt{\mu}, X\} \leq O(\sqrt{\mu})$ . Using the bound (16), we get

$$\mathbb{E}_i \mathbb{E}_{X_i Y_i} \left[ \mathbb{E}_{R_{-i}|x_i, y_i, W_C} \left\| U_{r_{-i}, x_i} \otimes V_{r_{-i}, y_i} |E_{dd'}\rangle - |\Psi_{r_{-i}, x_i, y_i}\rangle |E_{d'}\rangle \right\| \right] \leq O(\eta^{1/12})$$

as desired.

**Acknowledgments.** This work was supported by Simons Foundation grant 360893 and National Science Foundation Grant 1218547. The author thanks both the Institute of Mathematical Sciences at the National University of Singapore, and the Weizmann Institute of Science for hospitable stays during which this research was conducted. The author also thanks Corinna Li, Mohammad Bavarian, Govind Ramnarayan, and anonymous referees for helpful feedback and discussions.

## References

- [Bel64] John S Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3), 1964.
- [BG15] Mark Braverman and Ankit Garg. Small value parallel repetition for general games. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing (STOC)*, 2015.
- [BRWY13] Mark Braverman, Anup Rao, Omri Weinstein, and Amir Yehudayoff. Direct products in communication complexity. In *2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 746–755. IEEE, 2013.

- [BVY15] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Anchoring games for parallel repetition. *arXiv preprint arXiv:1509.07466*, 2015.
- [BVY16] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Parallel repetition via fortification: analytic view and the quantum case. *arXiv preprint arXiv:1603.05349*, 2016.
- [CS14] André Chailloux and Giannicola Scarpa. Parallel repetition of entangled games with exponential decay via the superposed information cost. In *Automata, Languages, and Programming*, pages 296–307. Springer, 2014.
- [CSUU08] Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. *Computational Complexity*, 17(2):282–299, 2008.
- [CWY15] Kai-Min Chung, Xiaodi Wu, and Henry Yuen. Parallel repetition for entangled k-player games via fast quantum search. In *the 30th Conference on Computational Complexity (CCC)*, pages 512–536, 2015.
- [DSV14] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. In *the 29th Conference on Computational Complexity (CCC)*, pages 197–208, 2014.
- [FK00] Uriel Feige and Joe Kilian. Two-prover protocols—low error at affordable rates. *SIAM Journal on Computing*, 30(1):324–346, 2000.
- [Hås01] Johan Håstad. Some optimal inapproximability results. *Journal of the ACM (JACM)*, 48(4), 2001.
- [Hol09] Thomas Holenstein. Parallel repetition: Simplification and the no-signaling case. *Theory of Computing*, 5(8):141–172, 2009.
- [Jai11] Rahul Jain. New strong direct product results in communication complexity. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 18, page 2, 2011.
- [JPY14] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. In *Proceedings of Conference on Computational Complexity (CCC)*, pages 209–216, 2014.
- [KRT08] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy. In *Proceedings of Foundations of Computer Science (FOCS)*, 2008.
- [KV11] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the forty-third annual ACM symposium on Theory of computing (STOC)*, pages 353–362, 2011.
- [Mos14] Dana Moshkovitz. Parallel repetition from fortification. In *2014 IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 414–423. IEEE, 2014.
- [NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

- [PS70] Robert T Powers and Erling Størmer. Free states of the canonical anticommutation relations. *Communications in Mathematical Physics*, 16(1):1–33, 1970.
- [Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.
- [vDH03] Wim van Dam and Patrick Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003.
- [Wil13] Mark M Wilde. *Quantum information theory*. Cambridge University Press, 2013.