Strong parallel repetition for free entangled games, with any number of players

Kai-Min Chung∗ Xiaodi Wu† Henry Yuen‡
Academia Sinica MIT MIT
November 6, 2014

Abstract

We present a strong parallel repetition theorem for the entangled value of multi-player, one-round free games (games where the inputs come from a product distribution). Our result is the first parallel repetition theorem for entangled games involving more than two players. Furthermore, our theorem applies to games where the players are allowed to output (possibly entangled) quantum states as answers.

More specifically, let $G$ be a $k$-player free game, with entangled value $\text{val}^*(G) = 1 - \epsilon$. We show that the entangled value of the $n$-fold repetition of $G$, $\text{val}^*(G^\otimes n)$, is at most $(1 - \epsilon)^\Omega(n/k^2)$. In the traditional setting of $k = 2$ players, our parallel repetition theorem is optimal in terms of its dependence on $\epsilon$ and $n$. For an arbitrary number of players, our result is nearly optimal: for all $k$, we exhibit a $k$-player free game $G$ and $n > 1$ such that $\text{val}^*(G^\otimes n) \geq \text{val}^*(G)^{n/k}$. Hence, exponent of the repeated game value cannot be improved beyond $\Omega(n/k)$.

Our parallel repetition theorem improves on the prior results of Jain et al. and Chailloux and Scarpa in a number of ways: (1) our theorem applies to a larger class of games (arbitrary number of players, quantum outputs); (2) we demonstrate that strong parallel repetition holds for the entangled value of free games: i.e., the base of the repeated game value is $1 - \epsilon$, rather than $1 - \epsilon^2$; and (3) there is no dependence of the repeated game value on the input and output alphabets of $G$. In contrast, it is known that the repeated game value of classical free games must depend on the output size. Thus our results demonstrate a separation between the behavior of entangled games and classical games.

1 Introduction

The study of multi-player one-round games has been central to both theoretical computer science and quantum information. Games have served as an indispensable tool with which to study a diverse array of topics, from the hardness of approximation to cryptography; from delegated computation to Bell inequalities; from proof systems to the monogamy of entanglement. In particular, two-player games have received the most scrutiny. In a two-player game $G$, a referee samples a pair of questions $(x, y)$ from some distribution $\mu$, and sends question $x$ to one player (typically named Alice), and $y$ to the other (typically named Bob). Alice and Bob then utilize some non-communicating strategy to produce

∗E-mail: kmchung@iis.sinica.edu.tw
†E-mail: xiaodiwu@mit.edu
‡E-mail: hyuen@csail.mit.edu
answers $a$ and $b$, respectively, upon which the referee computes some predicate $V(x, y, a, b)$ to decide whether to accept or not. In this paper, we focus on the setting where Alice and Bob may utilize quantum entanglement as part of their strategy. The primary quantity of interest is the entangled value $\text{val}^*(G)$ of game $G$, which is the maximum success probability over all possible entangled strategies for the players.

Recently, there has been significant interest in the parallel repetition of entangled games [KV11, CS14a, CS14b, JPY14, DSV14]. More formally, the $n$-fold parallel repetition of a game $G$ is a game $G^\otimes n$ where the referee will sample $n$ independent pairs of questions $(x_1, y_1), \ldots, (x_n, y_n)$ from the distribution $\mu$. Alice receives $(x_1, \ldots, x_n)$ and Bob receives $(y_1, \ldots, y_n)$. They produce outputs $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$, respectively, and they win only if $V(x_i, y_i, a_i, b_i) = 1$ for all $i$. We call each $i$ a "coordinate" of $G^\otimes n$ or "repetition" of $G$.

Suppose we have a game $G$ where $\text{val}^*(G) = 1 - \epsilon$. Intuitively, one should expect that $\text{val}^*(G^\otimes n)$ should behave as $(1 - \epsilon)^n$. Indeed, this would be the case if the game $G$ were played $n$ times sequentially. However, there are counterexamples of games $G$ and $n > 1$ where $\text{val}^*(G^\otimes n) = \text{val}^*(G)$ (see Section 3). Despite such counterexamples, it has been shown that the classical value $\text{val}(G^\otimes n)$ (i.e. where the players are restricted to using classical strategies) of a repeated game $G^\otimes n$ goes down exponentially with $n$, for large enough $n$ [Raz98, Hol07]. This result is known as the Parallel Repetition Theorem, and is central in the study of hardness of approximation, probabilistically checkable proofs, and hardness amplification in classical theoretical computer science.

Recently, quantum analogues of the Parallel Repetition Theorem have been studied, and for certain types of games, it has been shown that the entangled game value also goes down exponentially with the number of repetitions. In particular, parallel repetition theorems have been shown for 2-player free games (see [CS14a, CS14b, JPY14]) and projection games (see [DSV14]). Free games are where the input distribution to the players is a product distribution (i.e. each players’ questions are chosen independently of each other). Projection games are where, for each answer of one designated player, there is at most one other answer for the other player that the referee would accept.

### 1.1 Our results

In this work, we further the study of the parallel repetition of entangled free games. We generalize prior results by showing a parallel repetition theorem for free games with an arbitrary number of players, and players that can send back (possibly entangled) quantum states, not just classical messages. Our main result is the following:

**Theorem 1.1 (Main Theorem)** Let $k \geq 2$ be an integer. Let $G$ be a $k$-player free game where the players answers can be quantum. Suppose that $\text{val}^*(G) = 1 - \epsilon$. Then

$$\text{val}^*(G^\otimes n) \leq (1 - \epsilon)^{\Omega(n/k^2)}.$$ 

In the case of 2-player games, such a theorem is known as strong parallel repetition, where the base of the repeated game value is $1 - \epsilon$ (as opposed to $1 - \epsilon^c$ for some $c > 1$), and the exponent is $\Omega(n)$. Furthermore, we prove that exponent $n/k^2$ is nearly optimal in terms of its dependence on $n$ and $k$:

**Theorem 1.2** For all $k \geq 2$, there exists a $k$-player free game $G$ and $n > 1$ where $\text{val}^*(G^\otimes n) \geq \text{val}^*(G)^{n/k}$.
We remark that, in the context of 2-player games, our parallel repetition theorem is optimal in the sense that we get $\text{val}^*(G^\otimes n) = (1 - \epsilon)^{\Omega(n)}$.

CQ Games. Our parallel repetition theorem applies to a class of games that is a generalization of the traditional notion of games that involve two players and have classical inputs and outputs. In this paper we introduce the class of $k$-player classical-quantum (CQ) games, where the players receive classical inputs, apply local unitary operators to their share of an entangled state, and return some qubits to the referee. The referee then makes a measurement on the answer qubits to decide whether to accept or reject. If we restrict the players’ unitaries to be permutation matrices, and the referee’s measurement to be diagonal in the standard basis, then we recover the class of classical games.

We believe the model of CQ games is worth deeper investigation. One motivation for the study of CQ games comes from the recent exciting work of Fitzsimons and Vidick [FV14], who demonstrated an efficient reduction transforming a local Hamiltonian $H = H_1 + \cdots + H_m$ acting on $n$ qubits to a 5-player CQ-game $G_H$ such that approximating $\text{val}^*(G_H)$ with inverse polynomial accuracy will decide whether the ground state energy of $H$ is a YES or NO instance of the QMA-complete problem LOCAL HAMILTONIANS. In this game, the referee sends $O(\log n)$-sized questions, and the players responds with $O(1)$-qubit states as answers. The significance of this is that it opens up the possibility of proving a “games” version of the Quantum PCP conjecture. This intriguing possibility calls for further study of the behavior of CQ games.

1.2 Prior work

We discuss how our result relates to prior results in parallel repetition, classical and quantum. Most relevant to our work are the results on free games. Jain, et al. [JPY14] and Chailloux and Scarpa [CS14a, CS14b] both proved that the entangled value of 2-player free games (with classical inputs and outputs) goes down exponentially with the number of repetitions. In particular, [CS14b] showed for such a game $G$ with $\text{val}^*(G) = 1 - \epsilon$, we have that $\text{val}^*(G^\otimes n) \leq (1 - \epsilon^2)^{\Omega(n/s)}$, where $s$ is the output length of the players. We improve upon this result in a number of ways: we can handle an arbitrary number of players; the output messages are not restricted to being classical; the base of the game value is $1 - \epsilon$ rather than $1 - \epsilon^2$; and finally we have no output alphabet dependence.

In a different line of work, Dinur, Steurer and Vidick show that projection games (with an arbitrary input distribution) also have an exponential decay in entangled value under parallel repetition: if $G$ be a 2-player projection game with classical inputs and outputs, and $\text{val}^*(G) = 1 - \epsilon$, then $\text{val}^*(G^\otimes n) \leq (1 - \epsilon^2)^{\Omega(n)}$ [DSV14]. This result is not comparable with our work, nor with the work of [CS14b, JPY14]. While [DSV14] can handle games with arbitrary input distributions, the games need to satisfy the projection property. On the other hand, the results on free games can handle arbitrary verification predicates, but the input distributions need to be product.

There is a rich history of study of parallel repetition in classical theoretical computer science, which we will not detail here. However, we point out several results that are relevant to our situation. The parallel repetition of classical free games was primarily studied in [BRR+09], who showed that for 2-player free games $G$ with classical value $1 - \epsilon$, $\text{val}(G^\otimes n) \leq (1 - 2^\epsilon)^{\Omega(n/s)}$, where $s$ is the output length of the players. When $G$ is a projection game, they obtain strong parallel repetition, or $\text{val}(G^\otimes n) \leq (1 - \epsilon)^{\Omega(n)}$.

Feige and Verbitsky demonstrated that a dependence of the exponent on the output alphabet is necessary for classical parallel repetition, even for free games [FV02]! That is, they demonstrated a 2-player free game $G$ and $n$ where $\text{val}(G^\otimes n) > \text{val}(G)^{O(n/s)}$, where $s$ is the output length of the players.
Thus, we obtain a separation between the behavior of the entangled value and classical value of games under repetition. Also, because the entangled value of a game upper bounds its classical value, our parallel repetition theorem implies that the entangled value of the Feige-Verbitsky game must satisfy \( \text{val}^*(G) \geq \text{val}(G)^{O(1/s)} \).

In [Hol07], a parallel repetition theorem is proved for non-signaling value of games, where players are now allowed to employ any strategy that respects the non-communication constraints (this includes strategies that cannot be achieved quantumly!). It is proved that for a 2-player game \( G \), \( \text{val}_{ns}(G^\otimes n) \leq (1-\epsilon^2)^{O(n)} \) – note the lack of output alphabet dependence. This indicates that the behavior of quantum games is closer to that of non-signaling games, than of classical games.

It was shown in [KR10] that the entangled value of games cannot, in general, satisfy strong parallel repetition, i.e. \( \text{val}^*(G^\otimes n) = (1-\epsilon)^{O(n)} \) if \( \text{val}^*(G) = 1-\epsilon \). That is, the exponent on \( \epsilon \) must be strictly greater than 1. Here, we do obtain strong parallel repetition, thus separating the behavior of entangled free games from entangled general games.

Finally, there has been little prior study of the parallel repetition of games with more than 2 players. Buhrman, et. al. studied this question for non-signaling players, and showed that the non-signaling value of repeated games goes down exponentially with the number of repetitions [BFS13]. Their parallel repetition theorem holds for games with full support, meaning that every possible combination of questions gets asked with positive probability; furthermore, the rate of decay also depends on the complete description of the game, not just the original game value and the number of repetitions. Rosen also studied \( k \)-player parallel repetition in a weaker version of the non-signaling model, and demonstrated an exponential rate of decay [Ros10]. To our knowledge, our result is the first to show quantum parallel repetition in the setting of games with more than 2 provers.

1.3 Proof overview

At first glance, the proof of our parallel repetition theorem appears to be a generalization the approach of [JPY14], which itself is a loose generalization of the proof of [Hol07]. However, it would be more accurate to view our approach as the quantum generalization of [BRR+09]. This view better highlights the commonalities and differences between classical and quantum parallel repetition (at least in the context of free games).

To explain this further, we first give a high-level outline of the proof of [BRR+09]. Let \( G \) be a 2-player free game with input distribution \( \mu \) and \( \text{val}(G) = 1-\epsilon \), and suppose for contradiction that \( \text{val}^*(G^\otimes n) > 2^{-\gamma n} \) for some small enough \( \gamma \). Then there is some “large-probability” event \( W \) such that, conditioned on \( W \), for a random coordinate \( i \), the probability that the players win game \( G \) in coordinate \( i \) is large, say \( 1-\epsilon/2 \). The goal is to transform this “too-good-to-be-true” strategy for \( G^\otimes n \) into a strategy for the base game \( G \) that wins with probability \( \approx 1 - \epsilon/2 > \text{val}^*(G) \), a contradiction. This base game strategy attempts to “smuggle” in the true inputs to \( G \) into one of these coordinates \( i \), and simulate the multi-game strategy conditioned on \( W \). However, conditioning on \( W \) may introduce unwanted correlations between the players’ inputs in coordinate \( i \).

The technical workhorse behind showing that this simulation succeeds is the so-called Raz’s Lemma. A simple version of Raz’s Lemma is the following: given independent random variables \( X_1, \ldots, X_n \) (think of these as the inputs to each of the coordinates of a repeated game), conditioning on an event \( W \) cannot simultaneously skew the distribution of all \( X_i \)’s by much. In fact, the average disturbance is small: \( \sum_i S((X_i)_W|X_i) \leq \log \frac{1}{\text{Pr}[W]} \), where \( S((X_i)_W|X_i) \) denotes the relative entropy between the distribution of \( X_i \) conditioned on \( W \) and the original distribution \( X_i \).
Roughly speaking, the proof in \cite{BRR+09} proceeds in three steps. Let $\mu_{W}^\otimes n$ denote $\mu^\otimes n$ conditioned on the event $W$.

1. Use Raz’s Lemma to conclude that, conditioned on the event $W$, for a random $i$, the marginal distribution of the $i$th coordinate in $\mu_{W}^\otimes n$ is close to the original distribution $\mu$. Such $i$’s are suitable for “smuggling” in our single-game inputs.

2. Let $(\vec{x}, \vec{y})$ distributed according to $\mu_{W}^\otimes n$. A version of Raz’s Lemma implies that, conditioned on the event $W$, for a random $i$, the correlation between $\vec{x}_i$ and $\vec{y}$ is small, and similarly for $\vec{y}_i$ and $\vec{x}$.

3. This implies that Alice and Bob can locally (approximately) sample $(\vec{x}, \vec{y})$ from $\mu_{W}^\otimes n$ conditioned on $W$ and $\vec{x}_i = x$ and $\vec{y}_i = y$, where $(x, y)$ are their true single-game inputs.

Once Alice and Bob are able to sample $(\vec{x}, \vec{y})$ from $\mu_{W}^\otimes n$ conditioned on $W$ and $\vec{x}_i = x$ and $\vec{y}_i = y$, they can win with probability $\approx 1 - \epsilon/2$. This is because in the classical setting, Alice and Bob’s strategies are deterministic functions of their inputs.

In the quantum setting, Alice and Bob’s strategies are no longer deterministic functions. Instead they share an entangled state $|\xi\rangle$ and apply local operations that depend on their inputs. Nonetheless, the proof of our quantum parallel repetition theorem mirrors the approach of \cite{BRR+09}. The setup is the same: there exists a “large-probability” event $W$ such that, conditioned on $W$, the players win the average coordinate $i$ with probability at least $1 - \epsilon/2$.

1. By the classical Raz’s Lemma, the distribution of the $i$th coordinate of $\mu_{W}^\otimes n$, for a random $i$, is close to $\mu$. (This is the same as in the classical proof).

2. Let $(\vec{x}, \vec{y})$ distributed according to $\mu_{W}^\otimes n$ and let $i$ be a random coordinate. Not only is the correlation between $\vec{x}_i$ and $\vec{y}$ small, but also the correlation between $\vec{x}_i$ (resp. $\vec{y}_i$) and the Bob’s share (resp. Alice’s share) of $|\xi_W\rangle$ is small, where $|\xi_W\rangle$ represents the original entanglement $|\xi\rangle$ conditioned on the event $W$. This follows from what we call Quantum Raz’s Lemma (see Lemma 4.13).

3. For coordinates $i$ where the correlation between $\vec{x}_i$ and Bob’s part of $|\xi_W\rangle$ and $\vec{y}$ is small (and similarly for $\vec{y}_i$ versus Alice’s part of $|\xi_W\rangle$ and $\vec{x}$), Quantum Strategy Sampling implies that on inputs $(x, y)$ drawn from $\mu$, Alice and Bob can apply local unitaries $U_x$ and $V_y$, respectively, on their share of $|\xi_W\rangle$ to obtain a state close to $|\xi_{W,x,y}\rangle$ — that is, $|\xi\rangle$ conditioned on both $W$ and $\vec{x}_i = x$ and $\vec{y}_i = y$.

Intuitively, once Alice and Bob obtain the state $|\xi_{W,x,y}\rangle$, they can apply their original strategy for the repeated game to play the base game with inputs $(x, y)$ smuggled into the $i$th coordinate, and win with probability greater than $1 - \epsilon$, a contradiction.

The proof outline above is described in terms of $k = 2$ players, and is in fact a way to view the approach of \cite{JPY14}. Our proof is a simplification and generalization of theirs. First, many of the information theoretic calculations in \cite{JPY14} are abstracted away into two invocations of Raz’s Lemma (both the classical and quantum versions of it). Secondly, we generalize their Quantum Strategy Sampling technique to support an arbitrary number of players. Finally, as a pleasant consequence of our simplifications, our proof can handle games where the players’ outputs are quantum states.

\footnote{We note also that \cite{CS14b} use essentially the same Quantum Strategy Sampling technique.}
We say a few words about the quantitative aspects of our parallel repetition theorem. As mentioned previously, we show (a) the rate of decay does not depend on either the input or output alphabet size, and (b) the base of the game value is $1 - \epsilon$ (i.e. strong parallel repetition). To achieve (a), we do not need to condition on specific values of players’ outputs in order to construct our conditioned state $|\xi_W\rangle$. Such conditioning on the outputs is necessary in the classical case, as demonstrated by [FV02]. The analyses of [JY14, CS14b] also condition on output values; however, we show that this is not necessary: in constructing $|\xi_W\rangle$, we only condition on a subspace of accepting outputs, roughly speaking.

To achieve strong parallel repetition, we use the squared Bures metric to measure distances between quantum states. This distance measure allows us to translate between relative entropies and probabilities without suffering a quadratic loss; in particular, we avoid using the trace distance. This approach is similar to that of [BRR+09], which solely uses relative entropy in order to achieve optimal strong parallel repetition for free projection games.

Outline. We formally describe the model of CQ games in Section 2. In Section 3, we show that the repeated value of a game necessarily depends on the number of players. In Section 4, we list the quantum information theoretic facts we’ll need, and prove Quantum Raz’s Lemma along with a few technical lemmas. In Section 5, we prove our $k$-player quantum strategy sampling lemma. In Section 6, we prove our parallel repetition theorem.

2 The model

Here we introduce the model of $k$-player classical-quantum (CQ) games.

**Definition 2.1** Let $k \geq 2$. A $k$-player classical-quantum (CQ) game $G$ is a tuple $(\mathcal{X}, A, \mu, \{V_x\}_{x \in \mathcal{X}})$, where

1. $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_k$ with each $\mathcal{X}_j$ being a finite alphabet;

2. $A = A_1 \otimes A_2 \otimes \cdots \otimes A_k$, with each $A_j$ being a finite-dimensional complex Hilbert space;

3. $\mu$ is a probability distribution over $\mathcal{X}$;

4. For each $x \in \mathcal{X}$, $0 \preceq V_x \preceq \text{id}$ is a positive semidefinite operator that acts on the space $A$.

In a $k$-player CQ game $G = (\mathcal{X}, A, \mu, \{V_x\})$, the referee will sample a tuple of inputs $x = (x_1, \ldots, x_k) \in \mathcal{X}$ from the distribution $\mu$, and send question $x_j$ to player $j$. Player $j$ will apply a local unitary on her part of a shared entangled state, and send her qubits in the space $A_j$ to the referee. The referee then performs the binary measurement $\{V_x, \text{id} - V_x\}$ on the players’ answers, and accepts if the outcome corresponding to $V_x$ is observed. In the case that the referee accepts, we say the players win the game $G$.

We say that a CQ game is free if $\mu = \mu_1 \otimes \cdots \otimes \mu_k$, where $\mu_i$ is some distribution on $\mathcal{X}_i$ (i.e. $\mu$ is a product distribution). A strategy for a CQ game $G$ is a shared state $|\xi\rangle^{EA}$ (where $E$ and $A$ are $k$-partite spaces split between the $k$ players), and for each player $j$ a set of unitaries $\{U_{x_j}^j\}_{x_j \in \mathcal{X}_j}$, which act on the space $E_jA_j$. On input $x_j$, player $j$ applies the unitary $U_{x_j}^j$ to the $E_jA_j$ registers of $|\xi\rangle$, and then sends the $A_j$ register to the referee. The entangled value of a CQ game $G$ is defined
as the maximum probability a referee will accept over all possible (finite-dimensional) strategies for \( k \) players:

\[
\text{val}^*(G) = \max_{|\xi\rangle, \{\{U_{ij}\}_j\}_j} \mathbb{E}_{x \sim \mu} \left[ \left\| \sqrt{V_x} U^1_{i1} \otimes \cdots \otimes U^k_{ik} |\xi\rangle \right\|^2 \right].
\]

When we restrict ourselves to maximizing over classical strategies (i.e. the state \(|\xi\rangle = |0\rangle\) and the unitaries \( U^j_{ij} \) are permutation matrices), we get the classical value of game \( G \), denoted by \( \text{val}(G) \).

The \( n \)-fold repetition of a CQ game \( G = (\mathcal{A}, A, \mu, \{V_x\}) \) is denoted by \( G^\otimes n = (\mathcal{A}^n, B, \mu^\otimes n, \{W_{\bar{x}}\}_{\bar{x} \in \mathcal{A}^n}) \), where: \( B \) is the tensor product of \( n \) isomorphic copies of \( A; \mu^\otimes n(\bar{x}) = \prod_i \mu(\bar{x}_i); \) and \( W_{\bar{x}} = \bigotimes_{\ell \in [n]} V_{\bar{x}_\ell}^\ell \) with \( V_{\bar{x}_\ell}^\ell \) denoting the \( \bar{x}_\ell \) POVM element acting on the \( \ell \)th copy of \( A \) in \( B \).

The model of CQ games is a strict generalization of the standard notion of games with entangled provers, where the inputs and outputs of the players are classical, and the verification predicate is some function of the inputs and outputs.

### 3 A lower bound

In this section we demonstrate a \( k \)-player free CQ game \( G \) such that \( \text{val}(G) = \text{val}^*(G) = 1/2 \), but \( \text{val}^*(G^\otimes n) = \text{val}(G^\otimes n) = 1/2 \) for \( n \leq k \). This implies that in general, the dependence of the exponent of parallel repetition on the number of players is necessary (for both the classical and entangled value). This is a generalization of Feige’s “non-interactive agreement” example of a 2-player game \( F \) such that \( \text{val}(F^\otimes 2) = \text{val}(F) \).

**Theorem 3.1** There exists a \( k \)-player free CQ game \( G \) and \( n > 1 \) such that \( \text{val}^*(G^\otimes n) = \text{val}(G^\otimes n) \geq \text{val}^*(G)^{n/k} = \text{val}(G)^{n/k} \).

**Proof.** Consider the \( k \)-player game \( G \) where each player \( j \) receives uniformly random bit \( x_j \) independent of the others. Each player \( j \) has to output a pair \((i_j, a_j) \in [k] \times \{0, 1\}\). The players win if there exists an \( i \) such that \( i = i_1 = \cdots = i_k \), and \( x_i = a_{i_k}^\otimes \), the parity of the bits in the set \( \{a_1, \ldots, a_k\} - \{a_i\} \).

To prove this theorem it suffices to show that the non-signaling value of \( G \), \( \text{val}_{ns}(G) \), is 1/2, and the classical value of the game, \( \text{val}(G^\otimes n) \), is still 1/2. This is because, for any game \( F \), \( \text{val}_{ns}(F) \geq \text{val}^*(F) \geq \text{val}(F) \) [BFS13].

It is clear that \( \text{val}_{ns}(G) \geq \text{val}^*(G) \geq \text{val}(G) \geq 1/2 \); a classical strategy achieving this is for every player to deterministically output \((1, 0)\). We now show that \( \text{val}_{ns}(G) \leq 1/2 \). Let \( \mathcal{A} = [k] \times \{0, 1\} \). A non-signaling strategy for \( G \) is a conditional probability distribution \( p((i_1, a_1), \ldots, (i_k, a_k)|x_1, \ldots, x_k) \), that satisfies the following conditions: for all subsets \( I \subseteq [k] \), the complement \( J = [k] - I \),

\[
\sum_{\alpha_j \in \mathcal{A}^J} p(\alpha_I, \alpha_J|x_I, x_J) = \sum_{\alpha_j \in \mathcal{A}^J} p(\alpha_I, \alpha_J|x_I, x'_J) \quad \text{for all } x_J, x'_J \in \{0, 1\}^J \text{ and } \alpha_I \in \mathcal{A}^I,
\]

where for a set \( S \), \( \alpha_S \) is a set of tuples \((i, a)\) indexed by elements in \( S \), and \( x_S \) indicates a set of bits indexed by elements of \( S \).
The probability that strategy $p$ wins game $G$ is

$$\mathbb{E}_{x_1,\ldots,x_k} \left[ \sum_{i,i',a_1,\ldots,a_k} \sum_{x_i = a_i} p((i, a_1), \ldots, (i', a_k) | x_1, \ldots, x_k) \right]$$

$$= \mathbb{E}_{x_1,\ldots,x_k} \left[ \sum_{y} \sum_{i,i',a_1,\ldots,a_k} \sum_{x_i = y} p((i, a_1), \ldots, (i', a_k) | x_1, \ldots, y, \ldots, x_k) \right]$$

Applying the non-signaling constraints to the sum $\sum_{i} \sum_{a_1,\ldots,a_k} \sum_{x_i = y} p(\cdots)$ for when $y = 0$, then we get

$$\sum_{i} \sum_{a_1,\ldots,a_k} \sum_{x_i = 0} p((i, a_1), \ldots, (i', a_k) | x_1, \ldots, 0, \ldots, x_k)$$

$$= \sum_{i} \sum_{a_1,\ldots,a_k} \sum_{x_i = 0} p((i, a_1), \ldots, (i', a_k) | x_1, \ldots, 1, \ldots, x_k)$$

$$\leq 1 - \sum_{i} \sum_{a_1,\ldots,a_k} \sum_{x_i = 1} p((i, a_1), \ldots, (i', a_k) | x_1, \ldots, 1, \ldots, x_k).$$

But this implies that the non-signaling game value is at most $1/2$.

Now consider the repeated game $G^{\otimes k}$. We now give a strategy for the players such that $\text{val}(G^{\otimes k}) = 1/2$. Therefore $\text{val}^*(G^{\otimes k})$ (and $\text{val}_{ns}(G^{\otimes k})$) is at least $1/2$.

In the repeated game, each player $j$ receives a uniformly random vector of inputs $(x_1^j, x_2^j, \ldots, x_j^k)$. For the $\ell$th repetition, player $j$ will output the pair $(\ell, x_{j}^k)$. The probability that the players win the first coordinate is $1/2$. Conditioned on the first coordinate winning, we have that $x_1^1 \oplus x_2^2 \oplus \cdots \oplus x_k^k = 0$. But then this ensures that the players win the rest of the coordinates with certainty.

4 Preliminaries

We assume familiarity with the basics of quantum information and computation. For a comprehensive reference, we refer the reader to [NC10] [WH13]. For a pure state $|\psi\rangle$, we will let $\psi$ denote the density matrix $|\psi\rangle\langle\psi|$. If $|\psi\rangle^{AB}$ is a bipartite state, then $\psi^A$ will be the reduced density matrix of $\psi^{AB}$ on space $A$. A density matrix $\rho^{XA}$ is a classical-quantum (CQ) state if $\rho^{XA} = \sum_x p(x) |x\rangle\langle x| \otimes \rho^A_x$, where $p(x)$ is a probability distribution and $\rho^A_x$ is an arbitrary density matrix on space $A$. For a probability distribution $\mu$, $x \sim \mu$ indicates $x$ is drawn from $\mu$. For a classical state $\rho^X = \sum_x \mu(x) |x\rangle\langle x|$, we write $x \sim \rho^X$ to denote $x \sim \mu$.

4.1 Properties of the squared Bures metric

For two positive semidefinite operators $\rho, \sigma$, let the fidelity between $\rho$ and $\sigma$ be denoted by $F(\rho, \sigma) := \text{tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}$. The fidelity distance measure has the well-known property that for pure states $|\psi\rangle$ and
Proof. We adapt the proof from [CS14b]. For one, it does not satisfy a triangle inequality. However, one can convert fidelity into other measures that are metrics. One such measure is the Bures metric, defined as $d_B(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)}$. In this paper, we will use the squared Bures metric, denoted by $d_B^2(\rho, \sigma) := d_B(\rho, \sigma)^2$, as the primary distance measure between quantum states. It satisfies many pleasant properties, including the following:

**Fact 4.1 (Triangle inequality)** Let $n \geq 2$ and let $\rho_1, \ldots, \rho_{n+1}$ be density matrices. Then

$$K(\rho_1, \rho_{n+1}) \leq n \sum_i K(\rho_i, \rho_{i+1}).$$

**Proof.** We adapt the proof from [CS14b]. For $i \in [n]$ let $\alpha_i = \arccos(F(\rho_i, \rho_{i+1}))$. Let $\alpha = \arccos(F(\rho_1, \rho_{n+1}))$. Then, since $\arccos(F(\cdot, \cdot))$ is a distance measure for quantum states, we have $\alpha \leq \sum_i \alpha_i$. Then we have

$$K(\rho_1, \rho_{n+1}) = 1 - \cos(\alpha) \leq n^2(1 - \cos(\alpha/n)) \leq n \sum_i (1 - \cos(\alpha_i)) = n \sum_i K(\rho_i, \rho_{i+1}).$$

**Fact 4.2 (Contractivity under quantum operations)** Let $\mathcal{E}$ be a quantum operation, and let $\rho$ and $\sigma$ be density matrices. Then $K(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq K(\rho, \sigma)$.

**Fact 4.3 (Unitary invariance)** Let $U$ be unitary, and let $\rho$ and $\sigma$ be density matrices. Then $K(U \rho U^\dagger, U \sigma U^\dagger) = K(\rho, \sigma)$.

**Fact 4.4 (Convexity)** Let $\{A_i\}$ and $\{B_i\}$ be finite collections of positive semidefinite operators, and let $\{p_i\}$ be a probability distribution. Then $K(\sum_i p_i A_i \sum_i p_i B_i) \leq \sum_i p_i K(A_i, B_i)$.

### 4.2 Quantum information theory

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 entropy of $\rho$ is denoted by $H(\rho) := -\text{tr}(\rho \log \rho)$. For a tripartite state $\rho^{ABC}$, the conditional mutual information $I(A:B|C)$ is defined as $H(A) - H(A|B)$.

**Fact 4.5 ([JRS03])** Let $\rho$ and $\sigma$ be density matrices. Then $S(\rho\|\sigma) \geq K(\rho, \sigma)$.

**Fact 4.6 ([JRS03])** Let $\mu$ be a probability distribution on $\mathcal{X}$. Let $\rho = \sum_{x \in \mathcal{X}} \mu(x) |x\rangle \langle x| \otimes \rho_x^A$. Then $I(X : A) = E_{x \sim \mu} [S(\rho_x\|\rho)]$.

**Fact 4.7 ([JPY14], Fact II.11)** Let $\rho^{XY}$ and $\sigma^{XY}$ be quantum states. Then $S(\rho^{XY}\|\sigma^{XY}) \geq S(\rho^X\|\sigma^X)$.

**Fact 4.8** Let $\rho^{XY}$ and $\sigma^{XY} = \sigma^X \otimes \sigma^Y$ be quantum states. Then $S(\rho^{XY}\|\sigma^{XY}) \geq S(\rho^X\|\sigma^X) + S(\rho^Y\|\sigma^Y)$.

**Fact 4.9 ([JPY14], Fact II.8)** Let $\rho = \sum_x \mu(x) |x\rangle \langle x| \otimes \rho_x$, and $\rho^* = \sum_x \mu^*(x) |x\rangle \langle x| \otimes \rho_x^1$. Then $S(\rho^1\|\rho) = S(\mu^1\|\mu) + E_{x \sim \mu^1} [S(\rho_x^1\|\rho_x)]$.

**Lemma 4.10 ([JPY14], Lemma II.13)** Let $\rho = pp_0 + (1 - p)\rho_1$. Then $S_\infty(\rho_0\|\rho) \leq \log 1/p$. 


4.3 Some technical lemmas

The following lemma is due to [BRR+09]:

**Lemma 4.11** ([BRR+09], Lemma 3.3) Let \( P = (p, 1-p) \) and \( Q = (q, 1-q) \) be binary distributions. If \( S(P\|Q) \leq \delta \), and \( p < \delta \), then \( q \leq 4\delta \).

The following adapts Lemma 4.11 to use the distance measure \( K \) instead:

**Lemma 4.12** Let \( P = (p, 1-p) \) and \( Q = (q, 1-q) \) be binary distributions. If \( K(P, Q) \leq \delta \), and \( p < \delta \), then \( q \leq 4\delta \).

**Proof.** If \( q \leq p \), then we are done. Assume otherwise. We have that \( \delta \geq K(P, Q) = 1 - F(P, Q) \geq (1 - F(P, Q)^2)/2 \), because \( 0 \leq F(P, Q) \leq 1 \). \( F(P, Q)^2 = (\sqrt{pq} + \sqrt{(1-p)(1-q)})^2 = pq + 1 - p - q + pq + 2\sqrt{pq(1-p)(1-q)} \), and thus

\[
2\delta \geq p + q - 2pq - 2\sqrt{pq(1-p)(1-q)} \\
\geq p + q - 2pq - 2\sqrt{pq} \\
= (\sqrt{p} - \sqrt{q})^2 - 2pq \\
\geq (\sqrt{p} - \sqrt{q})^2 - 2\delta,
\]

where in the last line we used the assumption that \( p \leq \delta \). Then \( 2\sqrt{\delta} \geq |\sqrt{p} - \sqrt{q}| \geq \sqrt{q} \), and thus \( q \leq 4\delta \). \( \blacksquare \)

Finally, we prove a quantum analogue of Raz’s Lemma, which is the central tool behind many information-theoretic proofs of parallel repetition theorems [Raz98, Hol07, BRR+09]:

**Lemma 4.13 (Quantum Raz’s Lemma)** Let \( \psi^{XA} = \left( \sum_x \mu(x) |x\rangle \langle x|^X \right) \otimes \psi^A \) be a CQ-state, classical on \( X \) and quantum on \( A \), where \( X \) is \( n \)-partite. Furthermore, suppose that \( \mu(x) = \prod_i \mu_i(x_i) \). Let \( \varphi^{XA} = \sum_x \sigma(x) |x\rangle \langle x|^X \otimes \varphi^A_x \) be such that \( S(\varphi||\psi) \leq t \). Then,

\[
\sum_i I(X_i : A)_\varphi \leq 2t.
\]

**Proof.** First observe the following manipulations:

\[
t \geq S(\varphi^{XA}||\psi^{XA}) \\
= S(\varphi^{XA}||\psi^X \otimes \psi^A) \\
\geq S(\varphi^{XA}||\varphi^X \otimes \varphi^A) \\
= I(X : A)_\varphi \\
= H(X)_\varphi - H(X|A)_\varphi \\
\geq H(X)_\varphi - \sum_i H(X_i|A)_\varphi.
\]
We focus on $H(X)\varphi$ now. Using that relative entropy is always non-negative:

$$-H(X)\varphi + \sum_i H(X_i)\varphi \leq -H(X)\varphi + \sum_i S(\varphi^{X_i}\|\psi^{X_i}) + H(X_i)\varphi$$

$$= -H(X)\varphi - \sum_i \text{tr}(\varphi^{X_i} \log \psi^{X_i})$$

$$= -H(X)\varphi - \text{tr}(\varphi^X \log \psi^X)$$

$$= S(\varphi^X\|\psi^X)$$

$$\leq t.$$  

Continuing, we have

$$t \geq -t + \sum_i H(X_i)\varphi - H(X_i|A)\varphi = -t + \sum_i I(X_i : A)\varphi.$$  

5 Quantum Strategy Sampling

In this section we prove our $k$-player Quantum Strategy Sampling lemma, generalizing the technique of [CS14b, JPY14].

We give some intuition for quantum strategy sampling, in the case of 2 players. Suppose that there is a family of “advice states” $\{\varphi_{xy}\}_{x,y}$, one for every possible input $x$ of Alice and $y$ of Bob. Alice possesses one half of $\varphi_{xy}$, and Bob the other half. Think of these states as being “advice” states that help Alice and Bob win with high probability, if on input $(x, y)$, Alice and Bob happened to share $\varphi_{xy}$ as shared entanglement. However, in a real game strategy, Alice and Bob only possesses a state $|\xi\rangle$ that’s independent of their inputs. Informally, the Quantum Strategy Sampling lemma states that, if the mutual information between Alice’s input and Bob’s half of $\varphi_{xy}$ is small, and the mutual information between Bob’s input and Alice’s half of $\varphi_{xy}$ is small, then in fact Alice and Bob can start with some state $|\xi\rangle$, apply local unitaries that depend on their inputs, and obtain a state that is approximately $\varphi_{xy}$. That is, the “advice”-based strategy is “locally sampled” from a real quantum strategy.

Lemma 5.1 ([JPY14]) Let $\mu$ be a probability distribution on $\mathcal{X}$. Let

$$|\varphi\rangle := \sum_{x \in \mathcal{X}} \sqrt{\mu(x)} |xx\rangle^{XX'} \otimes |\varphi_x\rangle^{AB}.$$  

Let $|\varphi_x\rangle := |xx\rangle^{XX'} \otimes |\varphi_x\rangle^{AB}$. Then there exists unitary operators $\{U_x\}_{x \in \mathcal{X}}$ acting on $XX'A$ such that

$$\mathbb{E}_{x \leftarrow \mu} \left[ K(\varphi_x, U_x \varphi U_x^\dagger) \right] \leq I(X : B)_\varphi.$$  

Proof. We follow the proof in [JPY14]. Denote the reduced states of Bob by $\rho_x := \text{tr}_{XX'A}(\varphi_x)$ and $\rho := \text{tr}_{XX'A}(\varphi)$. By Facts 4.5 and 4.6 we get that

$$I(X : B)_\varphi = \mathbb{E}_{x \leftarrow \mu} [S(\rho_x\|\rho)] \geq \mathbb{E}_{x \leftarrow \mu} [K(\rho_x, \rho)].$$

By Uhlmann’s Theorem, for each $x \in \mathcal{X}$ there exists $U_x$ such that $|\langle \varphi_x| (U_x \otimes \text{id}_B) |\varphi\rangle | = F(\rho_x, \rho)$. Furthermore, this is equal to $F(\varphi_x, U_x \otimes \text{id}_B \varphi U_x^\dagger \otimes \text{id}_B)$. We thus obtain the claim.
Lemma 5.2 Let \( \{|\varphi_a\rangle\}_{a \in A} \) be a finite collection of pure states. Let \( \mu \) and \( \tau \) be probability distributions over \( A \) such that \( S(\mu||\tau) \leq \epsilon \). Then

\[
K\left( \mathbb{E}_{a \sim \mu} [|\varphi_a\rangle\langle\varphi_a|], \mathbb{E}_{a \sim \tau} [|\varphi_a\rangle\langle\varphi_a|] \right) \leq \epsilon.
\]

Proof. Consider the states \( |\psi^\mu\rangle = \sum_{a \in A} \sqrt{\mu(a)} |aa\rangle^{AA'} \otimes |\varphi_a\rangle \) and \( |\psi^\tau\rangle = \sum_{a \in A} \sqrt{\tau(a)} |aa\rangle^{AA'} \otimes |\varphi_a\rangle \). Let \( \rho^\mu = \text{tr}_{A'}(|\psi^\mu\rangle\langle\psi^\mu|) \) and \( \rho^\tau = \text{tr}_{A'}(|\psi^\tau\rangle\langle\psi^\tau|) \). Then notice that \( \mathbb{E}_{a \sim \mu} [|\varphi_a\rangle\langle\varphi_a|] = \text{tr}_{A'}(\rho^\mu) \) and \( \mathbb{E}_{a \sim \tau} [|\varphi_a\rangle\langle\varphi_a|] = \text{tr}_{A'}(\rho^\tau) \), respectively. We then have that, considering the partial trace as a quantum operation, \( K(\mathbb{E}_{a \sim \mu} [|\varphi_a\rangle\langle\varphi_a|], \mathbb{E}_{a \sim \tau} [|\varphi_a\rangle\langle\varphi_a|]) \leq K(\rho^\mu, \rho^\tau) \). By Uhlmann’s Theorem, this is at most \( 1 - |\langle \psi^\mu | \psi^\tau \rangle| = 1 - \sum_{a \in A} \sqrt{\mu(a) \tau(a)} \). By Fact \( 4.5 \), this is at most \( S(\mu||\tau) \leq \epsilon \). \( \blacksquare \)

Lemma 5.3 (Quantum Strategy Sampling) Let \( k \geq 1 \). Let \( \mu \) be a probability distribution over \( \mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_k \), where the \( \mathcal{X}_i \) are finite alphabets. Let

\[
|\varphi\rangle := \sum_{x \in \mathcal{X}} \sqrt{\mu(x)} |x\rangle^{XX'} \otimes |\psi_x\rangle^{AB}
\]

where \( X = X_1 \cdots X_k \), \( X' = X'_1 \cdots X'_k \), and \( A = A_1 \cdots A_k \) are \( k \)-partite registers. Then for all \( i \in [k] \) there exist operators \( \{U^i_{\varphi}\}_{\varphi \in \mathcal{X}_i} \) acting on \( X_iX'_iA_i \) such that

\[
K\left( \mathbb{E}_{x \sim \mu} [X_iX'_iA_iB \varphi], \mathbb{E}_{x \sim \tau} [(U^i_{\varphi})^\dagger \otimes \chi_i] \right) \leq 4k \sum_{i} I(X_i : X_{-i}X'_{-i}A_{-i}B),
\]

where \( A_{-i}, X_{-i}, \) and \( X'_{-i} \) denote the \( A, X, \) and \( X' \) registers excluding the \( i \)th coordinate, respectively, and for all \( x \in \mathcal{X}, \varphi \in \mathcal{X}_i \), define

\[
|\varphi_{x_{>i}}\rangle := |x_{>i}x_{>i}\rangle^{X_{>i}X'_{>i}} \otimes \left( \sum_{x_{<i}} \sqrt{\mu(x_{<i}|x_{>i})} |x_{<i}x_{<i}\rangle^{X_{<i}X'_{<i}} \otimes |\psi_x\rangle \right)
\]

and

\[
|\varphi_{x_i}\rangle := |x_ix_i\rangle^{X_iX'_i} \otimes \left( \sum_{x_{-i}} \sqrt{\mu(x_{-i}|x_{i})} |x_{-i}x_{-i}\rangle^{X_{-i}X'_{-i}} \otimes |\psi_x\rangle \right).
\]

Note that for all \( i, |\varphi\rangle = \sum_{x_i} \sqrt{\mu(x_i)} |\varphi_{x_i}\rangle \). Then by Lemma \( 5.1 \) we get that there exists \( \{U^i_{\varphi}\}_{\varphi \in \mathcal{X}_i} \) such that

\[
\mathbb{E}_{x \sim \mu} [K(\varphi_{x_i}, U^i_{\varphi}(\varphi))] \leq I(X_i : X_{-i}X'_{-i}A_{-i}B),
\]

where \( U^i_{\varphi} \) is the CP map that maps \( \sigma \mapsto U^i_{\varphi}(\sigma \otimes |\varphi_x\rangle \langle \varphi_x|) \). For notational convenience let \( \epsilon_i = I(X_i : X_{-i}X'_{-i}A_{-i}B) \). Define the following states: \( \rho_0 = \mathbb{E}_{x \sim \mu} [\varphi_x] \), and for all \( i \in [k] \), \( \rho_i = \mathbb{E}_{x \sim \mu} [U^i_{\varphi_{x_i}}(\varphi_{x_i})] \).

12
where $\mathcal{U}_{x \leq i}$ denotes the CP map $\sigma \mapsto \left( \bigotimes_{j \leq i} U_{x_j}^j \right) \sigma \left( \bigotimes_{j \leq i} U_{x_j}^j \right)^\dagger$. Then by the triangle inequality for the squared Bures metric (Fact 4.1),

$$K(\rho_0, \rho_n) \leq k \sum_{i=0}^{k-1} K(\rho_i, \rho_{i+1}).$$

We now just have to upper bound each term $K(\rho_i, \rho_{i+1})$:

$$K \left( \mathbb{E}_{x \leftarrow \mu_i} \mathcal{U}_{x \leq i} ([\varphi_{x > i}]), \mathbb{E}_{x \leftarrow \nu_{i+1}} \mathcal{U}_{x \leq i+1} ([\varphi_{x > i+1}]) \right)$$

$$\leq \mathbb{E}_{x \leftarrow \mu_i} \mathbb{E}_{x > i} \mathcal{U}_{x \leq i} \left( \mathbb{E}_{x > i} \mathcal{U}_{x > i+1} ([\varphi_{x > i+1}]) \right)$$

$$= K \left( \mathbb{E}_{x > i} \mathcal{U}_{x > i+1} ([\varphi_{x > i+1}]) \right).$$

The second and third lines follow from the convexity and unitary invariance of the squared Bures metric, respectively (Facts 4.4 and Fact 4.3). Consider the operation $\mathcal{E}$ that measures the registers $X_{>i+1} = X_{i+2} \ldots X_k$ in the standard basis. Then $\mathcal{E}[\mathbb{E}_{x > i+1} \mathcal{U}_{x > i+1} ([\varphi_{x > i+1}])] = \mathbb{E}_{x > i} \mathcal{U}_{x > i} ([\varphi_{x > i}])$ and $\mathcal{E}(\varphi) = \mathbb{E}_{x > i+1} \mathcal{U}_{x > i+1} ([\varphi_{x > i+1}])$. Then since the squared Bures metric is contractive under quantum operations (Fact 4.2), we have $K(\rho_i, \rho_{i+1})$ is at most

$$K \left( \mathbb{E}_{x \leftarrow \mu_i} \varphi_{x > i}, \mathbb{E}_{x \leftarrow \mu_{i+1}} \mathcal{U}_{x > i+1} ([\varphi_{x > i+1}]) \right)$$

$$\leq \mathbb{E}_{x \leftarrow \mu_i} \mathbb{E}_{x > i} \varphi_{x > i} \mathcal{U}_{x > i+1} ([\varphi_{x > i+1}])$$

$$\leq \epsilon_{i+1}.$$ 

To complete the proof, we use the triangle inequality once more:

$$K \left( \mathbb{E}_{x \leftarrow \mu} \varphi_x, \mathbb{E}_{x \leftarrow \mu} \mathcal{U}_x ([\varphi_x]) \right)$$

$$\leq 2 K \left( \mathbb{E}_{x \leftarrow \mu} \varphi_x, \mathbb{E}_{x \leftarrow \nu} \mathcal{U}_x ([\varphi_x]) \right) + 2 K \left( \mathbb{E}_{x \leftarrow \nu_0} \mathcal{U}_x ([\varphi_x]), \mathbb{E}_{x \leftarrow \mu} \mathcal{U}_x ([\varphi_x]) \right)$$

$$\leq 2 k \sum_i \epsilon_i + 2 k \sum_i \epsilon_i$$

$$\leq 4 k \sum_i \epsilon_i.$$

where $\mathcal{U}_x$ is the composition of $\mathcal{U}_{x_i}$ for all $i \in [k]$. Here we used Lemma 5.2 in the second line, and the fact that $S(\mu || \nu_k) = I(X_1 : X_2 : \cdots : X_k)_\mu$, which is the multipartite mutual information between the coordinates of $X$. It is a known fact (see, e.g., [YHH+09]) that the multipartite mutual information can be written in terms of the (standard) bipartite mutual information like so:

$$I(X_1 : X_2 : \cdots : X_k)_\mu \leq I(X_1 : X_2)_\mu + I(X_1 X_2 : X_3)_\mu + \cdots + I(X_1 X_2 \cdots X_{k-1} : X_k)_\mu,$$

but by the data processing inequality, we have that for all $i$, $I(X_1 \cdots X_{i-1} : X_i)_\mu \leq I(X_i : X_i X'_{i-1} A_{i-1})_\phi = \epsilon_i.$
6 Proof of the parallel repetition theorem

**Notation.** Let \(G = (\mathcal{X}, A, \mu, \{V_u\}_{u \in \mathcal{X}})\) be a \(k\)-player CQ-game. In what follows, we will think of \(x \in \mathcal{X}^n\) as \(n \times k\) matrices, where the \(i\)th row indicates the inputs of all \(k\) players in the \(i\)th coordinate, and the \(j\)th column indicates the inputs of the \(j\)th player. Thus \(x(i,\cdot)\) indicates the \(i\)th row of \(x\), and \(x(\cdot,j)\) indicates the \(j\)th column. When we write \(x_S\) for some subset \(S \subseteq [n]\), we mean the submatrix of \(x\) consisting of the rows indexed by \(i \in S\).

Let \(X\) be an \(n \times k\)-partite register. Then we will also format \(X\) as a \(n \times k\) matrix, so \(X_{(i,\cdot)}\) and \(X_{(\cdot,j)}\) have the natural meaning. For a subset \(S \subseteq [n]\), \(X_S\) denotes the registers corresponding to the rows of \(X\) indexed by \(S\). For an index \(j\), \(X_S(j)\) denotes the \(j\)th column of the rows indexed by \(S\). \(X_{(s,-j)}\) denotes the submatrix of \(X\) corresponding to rows indexed by \(i \in S\), and all columns except for the \(j\)th one.

Consider the repeated game \(G^\otimes n\), and let \(C \subseteq [n]\). Fix a strategy \(S\) for \(G^\otimes n\); then \(\Pr[\text{Win } C]\) is the probability that, under \(S\), the answers of the \(k\) players in coordinates indexed by \(C\) pass the referee’s verification procedure, over a random input \(x\) drawn from \(\mu^\otimes n\).

**Lemma 6.1** Let \(G = (\mathcal{X}, A, \mu, \{V_u\}_{u \in \mathcal{X}})\) be a \(k\)-player CQ-game such that \(\val^*(G) = 1 - \epsilon\), and let \(n \geq 1\). Fix a strategy for the repeated game \(G^\otimes n\). For all \(C \subseteq [n]\) such that \(|C| \leq n/2\), either \(\Pr[\text{Win } C] < 2^{-n}\), or there exists an \(i \notin C\) such that

\[\Pr[\text{Win } i \mid \text{Win } C] \leq 1 - \epsilon/6,\]

where \(\gamma = c\epsilon/k^2\) for some constant \(c\).

**Proof.** Consider a strategy for game \(G^\otimes n\) where the shared state between the \(k\) players is \(|\xi\rangle^E_A\) (where \(A\) is a \(n \times k\)-partite register, and \(E\) is a \(k\)-partite register) and each player \(j \in [k]\) possesses a set of unitaries \(\{W^j_{x_{(j)}}, x_{(j)}\}\) where, on input \(x_{(j)} \in \mathcal{X}^n_j\), player \(j\) applies \(W^j_{x_{(j)}}\) to the \(E_j A_{(j)}\) registers of the shared state \(|\xi\rangle\). For all \(x \in \mathcal{X}^n\), let \(|\xi_x\rangle^E_A = (\bigotimes_j W^j_{x_{(j)}}) |\xi\rangle^E_A\).

Let \(C \subseteq [n]\). Let

\[|\psi\rangle^{XX'EAB} := \sum_{x \in \mathcal{X}^n} \sqrt{\mu^\otimes n(x)} |xx\rangle^{XX'} \otimes \sum_{b \in \{0,1\}^C} \sqrt{V^b_{xc}} |\xi_x\rangle^E_A \otimes |b\rangle^B,\]

where \(X, X'\) are \(n \times k\)-partite registers, and \(V^b_{xc}\) denotes \(\bigotimes_{i \in C : b_i = 0} V^i_{x_{(i)} \cdot} \bigotimes_{i \in C : b_i = 1} (\id - V^i_{x_{(i)} \cdot})\), where by \(V^i_u\) for \(u \in \mathcal{X}\), we mean the POVM element \(V_u\) acting on the registers \(A_{(i)}\).

Let \(\lambda = \Pr[\text{Win } C]\), the probability of obtaining outcome 0 when measuring the \(B\) register of \(\psi\) in the standard basis – call this event \(\mathcal{W}\). Let

\[|\varphi\rangle^{XX'EAB} := \frac{1}{\sqrt{\lambda}} \sum_{x \in \mathcal{X}^n} \sqrt{\mu^\otimes n(x)} |xx\rangle^{XX'} \otimes \sqrt{V^0_{xc}} |\xi_x\rangle^E_A \otimes |0\rangle^B,\]

where \(V^0_{xc} = \bigotimes_{i \in C} V^i_{x_{(i)} \cdot}\).

Let \(S \subseteq [n]\). When we write a state such as \(\varphi_{xS}\) (or \(\psi_{xS}\)), we mean the pure state \(|\varphi\rangle\) (or \(|\psi\rangle\)) conditioned on \(X_S\) (and \(X'_S\)) register being equal to \(x_S\).
If $\lambda < 2^{-\gamma n}$, we are done. Otherwise, assume that $\lambda \geq 2^{-\gamma n}$. Let $\overline{C} = [n] - C$. Note that $\lambda \varphi^{X/E} + (1 - \lambda)\theta = \psi^{X/E}$ for some state $\theta$. Then,

$$\log 1/\lambda \geq S_{\infty}(\varphi^{X/E} \| \psi^{X/E}) \quad \text{(Fact 4.10)}$$
$$\geq S_{\infty}(\varphi^{X/E} \| \psi^{X/E})$$
$$\geq \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ S(\varphi^{x_C} \| \psi^{x_C}) \right] \quad \text{(Fact 4.9), (6.1)}$$

We first show that the distribution of individual coordinates $i \notin C$, conditioned on inputs in $C$ and the event $W$, is only affected by a small amount (on average). Starting from line (6.1),

$$\log 1/\lambda \geq \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ S(\varphi^{x_C} \| \psi^{x_C}) \right] \quad \text{(Fact 4.7)}$$
$$\geq \sum_{i \notin C} \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ S(\varphi^{x_C} \| \psi^{x_C}) \right], \quad \text{(Fact 4.8) (6.2)}$$

where we used the fact that $\psi^{x_C} = \psi^{x_C}$.

Now we argue that, for every player $j$ and for most coordinates $i \notin C$, conditioning on inputs in $C$ and the event $W$ does not introduce much correlation between $X(i,j)$ (i.e. player $j$’s input for the $i$th coordinate) and the other players’ quantum states and inputs. Fix a $j \in [k]$. Define

$$Z_{-j} = X'_i(\overline{C},-j)X_{i,-j}E_{-j}A_{i,-j}.$$ Applying Fact 4.7 to line (6.1), we have that

$$\log 1/\lambda \geq \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ S(\varphi^{x_C} \| \psi^{x_C}) \right].$$

Furthermore, observe that $\psi^{x_C}Z_{-j} = \psi^{x_C} \otimes \psi^{Z_{-j}}$, because player $j$ only performs a local operation on $X_{i,j}E_{j}A_{j}$, and the input distribution $\mu$ of game $G$ is a product distribution on $\mathcal{X}$. Hence the states $\varphi^{x_C}Z_{-j}$ and $\psi^{x_C}Z_{-j}$ satisfy the conditions of Quantum Raz’s Lemma, and we get

$$2 \log 1/\lambda \geq \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ \sum_{i \notin C} I(X(i,j) : Z_{-j} \varphi^{x_C}) \right].$$ (6.3)

Lines (6.2) and (6.3) yield:

(i) $\mathbb{E}_{i \in \overline{C}} \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ S(\varphi^{x_C} \| \psi^{x_C}) \right] \leq (\log 1/\lambda)/|\overline{C}|$,

(ii) For all $j \in [k]$, $\mathbb{E}_{i \in \overline{C}} \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ I(X(i,j) : Z_{-j} \varphi^{x_C}) \right] \leq (2 \log 1/\lambda)/|\overline{C}|$.

In the above, the index $i$ is chosen uniformly at random from $\overline{C}$. Let $\delta = (2 \log 1/\lambda)/|\overline{C}|$. For each setting of $x_C$ and $i$ we use Lemma 5.3 on the pure state $\varphi^{x_C}$ to obtain for each player $j$ a set of unitaries $\{U_{i,x_C}^{j, u}\}_{u \in \mathcal{X}_j}$ such that

$$\mathbb{E}_{i \in \overline{C}} \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ K \left( \mathbb{E}_{x_{(i,j)}} \varphi^{x_{(i,j)}} \left[ \mathbb{E}_{x_{(i,j)}} \varphi^{x_{(i,j)}} \left[ U_{i,x_C}^{j, u} \varphi^{x_C} \right] \right] \right) \right]$$
$$\leq \mathbb{E}_{i \in \overline{C}} \mathbb{E}_{x_C \leftarrow \varphi^{x_C}} \left[ 4k \sum_{j} I(X(i,j) : Z_{-j} \varphi^{x_C}) \right] \leq 4k^2 \delta.$$
where we let $U_{i,x_{C},x_{(i)}} = \bigotimes_{j} U_{i,x_{C},x_{(i,j)}}$ and let $U_{i,x_{C},x_{(i)}}$ be the CP map that maps $\varphi \mapsto U_{i,x_{C},x_{(i)}} \varphi U_{i,x_{C},x_{(i)}}^\dagger$.

We now describe a protocol for the $k$ players to play game $G$. The players receive $u \in \mathcal{X}$, drawn from the product distribution $\mu$. Player $j$ receives $u_j \in \mathcal{X}_j$. For each value of $x_{C}$, the players share the state $\varphi_{x_{C}}^X \otimes \mathcal{E}_A$. Note that these states are still pure, because we have conditioned on specific settings of $X_C$. Player $j$ has access to the $X_{(j)}' \otimes X_{(j)} E_j A_{(j)}$ part of each state. The players also have access to common shared randomness.

**Protocol A**

**Input:** $u \in \mathcal{X}$. Player $j$ receives $u_j$.

**Preshared entanglement:** $\{ \varphi_{x_{C}}^X \otimes \mathcal{E}_A \}_{x_{C}}$

**Strategy for player $j$:**

1. Use shared randomness to pick an index $i \in \mathcal{C}$ uniformly at random.
2. Use shared randomness to sample an $x_{C} \leftarrow \varphi_{x_{C}}^X$.
3. Apply the local unitary $U_{i,x_{C},u_j}$ on the $X_{(j)}' \otimes X_{(j)} E_j A_{(j)}$ registers of $\varphi_{x_{C}}^X$.
4. Output the $A_{(i,j)}$ part of $\varphi_{x_{C}}^X$.

Figure 1: Protocol for game $G$

We now relate the winning probability of this protocol with the quantity $\omega = \mathbb{E}_{i \notin C} \Pr [\text{Win } i \mid \text{Win } C]$. First, observe that for $i \notin C$:

$$
\Pr [\text{Win } i \mid \text{Win } C] = \frac{1}{\lambda} \Pr [\text{Win } C \cup \{ i \}]
= \frac{1}{\lambda} \mathbb{E}_{x \sim \mu \oplus \eta} \left\| \sqrt{V^i_{x_{(i)}}} \sqrt{V_{x_{C}}} \left| \xi_x \right\| \right|^2
= \left\| \sqrt{V^i_{x_{(i)}}} \right\| \mathbb{E}_{x \sim \mu \oplus \eta} \left\| \sqrt{V_{x_{C}}} \left| \varphi_{x_{(i)}} \right\| \right|^2.
$$

Let $\kappa$ denote the winning probability of Protocol A. This is equal to

$$
\kappa = \mathbb{E}_{u \sim \mu} \mathbb{E}_{i \sim \varphi_{x_{C}}} \left\| \sqrt{V^i_{u}} U_{i,x_{C},u} \left| \varphi_{x_{C}} \right\| \right|^2
= \mathbb{E}_{i \sim \varphi_{x_{C}}} \left\| \sqrt{V^i_{u}} U_{i,x_{C},u} \left| \varphi_{x_{C}} \right\| \right|^2
\geq \mathbb{E}_{i \sim \varphi_{x_{C}}} \mathbb{E}_{u \sim \varphi_{x_{C}}} \left\| \sqrt{V^i_{u}} U_{i,x_{C},u} \left| \varphi_{x_{C}} \right\| \right|^2 - 4\delta.
$$

where we use line (6.2) and appeal to Lemma 4.14. Let

$$
\tau := \mathbb{E}_{i \sim \varphi_{x_{C}}} \mathbb{E}_{u \sim \varphi_{x_{C}}} \left\| \sqrt{V^i_{u}} U_{i,x_{C},u} \left| \varphi_{x_{C}} \right\| \right|^2.
$$
Consider the quantum operation $E_i$ that, given a state $\varphi$, (1) measures the $X_{(i, \cdot)}$ in the standard basis; (2) conditioned on the outcome $X_{(i, \cdot)} = x_{(i, \cdot)}$, measures the $A_{(i, \cdot)}$ registers using $V^i_{x_{(i, \cdot)}}$ measurement; and (3) outputs a classical binary random variable $F$ indicating the verification measurement outcome (outcome 0 corresponds to “accept” and outcome 1 corresponds to “reject”). Let

$$F_0 = \mathbb{E}_i \mathbb{E}_x \mathbb{E}_{x'} \mathbb{E}_{x'_C} \mathbb{E}_{x_{(i, \cdot)}} \left[ \varphi_{x_{(i, \cdot)}}, \varphi_{x_{(i, \cdot)}}, \varphi_{x_C}, \varphi_{x'_C} \right],$$

and let

$$F_1 = \mathbb{E}_i \mathbb{E}_x \mathbb{E}_{x'} \mathbb{E}_{x'_C} \mathbb{E}_{x_{(i, \cdot)}} \left[ \mathcal{U}_{x_C, u} \left( \varphi_{x_C} \right) \right].$$

Note that $\Pr[F_0 = 0] = \omega$, and $\Pr[F_1 = 0] = \tau$.

By the convexity of the squared Bures metric (Fact 4.2) and Lemma 5.3,

$$K(F_0, F_1) \leq \mathbb{E}_i \mathbb{E}_x \left[ K \left( \mathcal{E}_i \left( \mathbb{E}_x \left[ \varphi_{x_{(i, \cdot)}}, \varphi_{x_C}, \varphi_{x'_C} \right] \right), \mathcal{E}_i \left( \mathbb{E}_{x'} \left[ \mathcal{U}_{x_C, u} \left( \varphi_{x_C} \right) \right] \right) \right] \leq 4k^2 \delta.$$

By assumption, $\log 1/\lambda < \gamma n$, and $|C| \geq n/2$. Thus, $\delta \leq 4\gamma$. By choosing $\gamma = \delta n/k^2$ for some small enough constant $\epsilon$, we can get that $\delta \leq \epsilon/24$ and $K(F_0, F_1) \leq \epsilon/6$. If $\omega \leq 1 - \epsilon/6$, we are done. Otherwise, by Lemma 4.12, $\Pr[F_1 = 0] \geq \omega - \epsilon/6$.

This means that $\kappa \geq \omega - \epsilon/6 - 4\delta \geq \omega - \epsilon/2$. On the other hand we have $\kappa \leq \text{val}^*(G)$, so thus $\omega \leq \text{val}^*(G) + \epsilon/2$ – and hence by averaging there exists an $i \notin C$ such that $\Pr[\text{Win } i | \text{Win } C] \leq \text{val}^*(G) + \epsilon/2$. This concludes the proof.

**Theorem 6.2** \text{val}^*(G^{\otimes n}) \leq (1 - \epsilon)^{\Omega(n/k^2)}.

**Proof.** For any subset $C \subseteq [n]$, we have that $\text{val}^*(G^{\otimes n}) \leq \Pr[\text{Win } C]$. We construct a $C$ iteratively as follows. As long as there exists a subset $i \notin C$ such that $\Pr[\text{Win } i | \text{Win } C] \leq 1 - \epsilon/6$, we add it to $C$. If at some point $\Pr[\text{Win } C] \leq 2^{-\gamma n}$, we are done, because this is at most $2^{-\gamma n} = (1 - \epsilon)^{\Omega(n/k^2)}$. Otherwise, if we cannot find any such $i$ to add, then it must be that $|C| > n/2$. But then, by Bayes’ rule, we have that $\Pr[\text{Win } C] \leq (1 - \epsilon/6)^{|C|} \leq (1 - \epsilon)^{\Omega(n)}$.

In either case, $\text{val}^*(G^{\otimes n}) \leq (1 - \epsilon)^{\Omega(n/k^2)}$.

**Acknowledgments.** HY is supported by an NSF Graduate Fellowship Grant No. 112374 and National Science Foundation Grant No. 1218547. XW is funded by ARO contract W911NF-12-1-0486 and by the NSF Waterman Award of Scott Aaronson. Part of this research was conducted while XW was a Research Fellow and HY was a graduate student visitor at the Simons Institute for the Theory of Computing, University of California, Berkeley.
References

[BFS13] H. Buhrman, S. Fehr, and C. Schaffner. On the parallel repetition of multi-player games: The no-signaling case. *arXiv preprint arXiv:1312.7455*, 2013.

[BRR⁺09] B. Barak, A. Rao, R. Raz, R. Rosen, and R. Shaltiel. Strong parallel repetition theorem for free projection games. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 352–365. Springer, 2009.

[CS14a] A. Chailloux and G. Scarpa. Parallel repetition of entangled games with exponential decay via the superposed information cost. In J. Esparza, P. Fraigniaud, T. Husfeldt, and E. Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 296–307. Springer, 2014. ISBN 978-3-662-43947-0. doi:10.1007/978-3-662-43948-7.25.

[CS14b] A. Chailloux and G. Scarpa. Parallel repetition of free entangled games: Simplification and improvements. *arXiv preprint arXiv:1410.4397*, 2014.

[DSV14] I. Dinur, D. Steurer, and T. Vidick. A parallel repetition theorem for entangled projection games. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 197–208. 2014. doi:10.1109/CCC.2014.28.

[FV02] U. Feige and O. Verbitsky. Error reduction by parallel repetition: a negative result. *Combinatorica*, 22(4):461–478, 2002.

[FV14] J. Fitzsimons and T. Vidick. A multiprover interactive proof system for the local hamiltonian problem. *arXiv preprint arXiv:1409.0260*, 2014.

[Hol07] T. Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 411–419. ACM, 2007.

[JPY14] R. Jain, A. Pereszlényi, and P. Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. In *IEEE 29th Conference on Computational Complexity, CCC 2014, Vancouver, BC, Canada, June 11-13, 2014*, pages 209–216. 2014. doi:10.1109/CCC.2014.29.

[JRS03] R. Jain, J. Radhakrishnan, and P. Sen. A lower bound for the bounded round quantum communication complexity of set disjointness. In *Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on*, pages 220–229. IEEE, 2003.

[KR10] J. Kempe and O. Regev. No strong parallel repetition with entangled and non-signaling provers. In *Computational Complexity (CCC), 2010 IEEE 25th Annual Conference on*, pages 7–15. IEEE, 2010.

[KV11] J. Kempe and T. Vidick. Parallel repetition of entangled games. In *Proceedings of the forty-third annual ACM symposium on Theory of computing*, pages 353–362. ACM, 2011.
[NC10] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[Raz98] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[Ros10] R. Rosen. A k-provers parallel repetition theorem for a version of no-signaling model. *Discrete Math., Alg. and Appl.*, 2(4):457–468, 2010.

[Wil13] M. M. Wilde. *Quantum information theory*. Cambridge University Press, 2013.

[YHH+09] D. Yang, K. Horodecki, M. Horodecki, P. Horodecki, J. Oppenheim, and W. Song. Squashed entanglement for multipartite states and entanglement measures based on the mixed convex roof. *Information Theory, IEEE Transactions on*, 55(7):3375–3387, 2009.