Hardness Amplification for Entangled Games via Anchoring

Mohammad Bavarian
Massachusetts Institute of Technology
Cambridge, MA, USA
bavarian@mit.edu

Thomas Vidick
California Institute of Technology
Pasadena, CA, USA
vidick@cms.caltech.edu

Henry Yuen
UC Berkeley
Berkeley, CA, USA
hyuen@cs.berkeley.edu

ABSTRACT

We study the parallel repetition of one-round games involving players that can use quantum entanglement. A major open question in this area is whether parallel repetition reduces the entangled value of a game at an exponential rate — in other words, does an analogue of Raz's parallel repetition theorem hold for games with players sharing quantum entanglement? Previous results only apply to special classes of games.

We introduce a class of games we call *anchored*. We then introduce a simple transformation on games called *anchoring*, inspired in part by the Feige-Kilian transformation, that turns *any* (multiplayer) game into an anchored game. Unlike the Feige-Kilian transformation, our anchoring transformation is completeness preserving.

We prove an exponential-decay parallel repetition theorem for anchored games that involve any number of entangled players. We also prove a threshold version of our parallel repetition theorem for anchored games.

Together, our parallel repetition theorems and anchoring transformation provide the first hardness amplification techniques for general entangled games. We give an application to the games version of the Quantum PCP Conjecture.

CCS CONCEPTS

• **Theory of computation → Quantum complexity theory**;

KEYWORDS

Entangled games, parallel repetition, hardness amplification

ACM Reference format:
Mohammad Bavarian, Thomas Vidick, and Henry Yuen. 2017. Hardness Amplification for Entangled Games via Anchoring. In *Proceedings of 49th Annual ACM SIGACT Symposium on the Theory of Computing, Montreal, Canada, June 2017 (STOC'17),* 14 pages.
DOI: 10.1145/3055399.3055433

1 INTRODUCTION

Hardness amplification is a central method in complexity theory and cryptography for reducing the soundness error of interactive proofs and argument systems. Often, it is easier to construct an interactive protocol with soundness error bounded away from 1, and then apply hardness amplification on the protocol to reduce the soundness error to an arbitrarily small δ. Furthermore, one would often like the hardness amplification method to maintain important structural features of the protocol, such as the number of rounds or the number of parties involved. The simplest operation which achieves this is *parallel repetition*, where multiple independent instances of the original protocol are executed in parallel. However, despite the independence between instances, the parties in the protocol may not treat them independently. Because of this, showing that parallel repetition reduces the soundness error is generally a difficult task, which has been the focus of a long line of research in complexity theory and cryptography [19, 22, 23, 25, 27, 39, 41].

In this paper, we study the parallel repetition of games involving players sharing entanglement. For simplicity we first consider two-player games. A two-player one-round game is specified by finite question sets $\mathcal{X}, \mathcal{Y}$, finite answer sets $\mathcal{A}, \mathcal{B}$, a probability distribution μ over $\mathcal{X}\times\mathcal{Y}$, and a verification predicate $V : \mathcal{X}\times\mathcal{Y}\times\mathcal{A}\times\mathcal{B} \to \{0, 1\}$ that determines the acceptable question and answer combinations. The game is played as follows: a referee samples questions $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to μ and sends x to the first player and y to the second. Each player replies with an answer, $a \in \mathcal{A}$ and $b \in \mathcal{B}$ respectively. The referee accepts if and only if $V(x, y, a, b) = 1$, in which case we say that the players win the game. The extension to three or more players is straightforward.

Multiplayer games arise naturally in settings ranging from hardness of approximation [24, 49] and interactive proof systems [7, 22] to the study of Bell inequalities and non-locality in quantum physics [6, 13].

The main quantity associated with a multiplayer game G is its *value*: the maximum acceptance probability achievable by the players, where the probability is taken over the questions, as chosen by the referee, and the players' answers. Different notions of value arise from different restrictions on allowed strategies for the players. The most important for us are the *classical value* (denoted by $\mathrm{val}(G)$) and the *entangled value* (denoted by $\mathrm{val}^*(G)$). The former is obtained by restricting the players to classical strategies, where each player's answer is a function of its question only[1]. The latter allows for quantum strategies, in which each player's answer is obtained as the outcome of a local measurement performed on a quantum state shared by the players. The use of quantum states *does not* allow communication between the players, but it does allow for correlations between their questions and answers that cannot be reproduced by any classical strategy [6].

We study the behavior of $\mathrm{val}(G)$ and $\mathrm{val}^*(G)$ under parallel repetition. In the n-fold parallel repetition G^n of a game G the referee samples $(x_1, y_1), \ldots, (x_n, y_n)$ independently from μ, and sends $(x_1, \ldots, x_n)$ to the first player and $(y_1, \ldots, y_n)$ to the second. The players respond with answer tuples $(a_1, \ldots, a_n)$ and

[1] Both private and shared randomness are in principle allowed, but easily seen not to help.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
STOC'17, Montreal, Canada
© 2017 ACM. 978-1-4503-4528-6/17/06…$15.00

DOI: 10.1145/3055399.3055433

$(b_1, \ldots, b_n)$ respectively, and they win if and only if their answers satisfy $V(x_i, y_i, a_i, b_i) = 1$ for all i.

Clearly, if the players play each instance of G in G^n independently of each other (i.e. according to a *product strategy*), their success probability is the n-th power of their success probability in G. The main obstacle to proving a parallel repetition theorem is that players need not employ product strategies – their answers for the i-th instance of G may depend on their questions in the j-th instance for $j \neq i$. Indeed, it is known that there are games G for which non-product strategies enable the players to win G^n with probability significantly greater than $\mathrm{val}(G)^n$ [20, 43].

Nevertheless, the parallel repetition theorem of Raz [41] establishes that if G is a two-player game such that $\mathrm{val}(G) < 1$ the value $\mathrm{val}(G^n)$ decays exponentially with n. Thus, Raz's theorem shows that parallel repetition is a good hardness amplification technique for two-player one-round games. The two following decades have seen a substantial amount of research on this question, connecting the problem of parallel repetition to topics such as the Unique Games conjecture, hardness of approximation, communication complexity, and more [3, 10, 24, 40].

Recently, there has been much interest in obtaining hardness amplification techniques for games involving players sharing entanglement — in particular, obtaining an analogue of Raz's theorem for entangled games. The study of entangled games has recently been a prominent focus of quantum complexity theory and quantum information, for its role in quantum interactive proofs [29, 45], quantum cryptography [47, 48], and for its aid in studying fundamental aspects of quantum entanglement [34, 35]. However, this has proved challenging, for a variety of reasons. For one, there is no *a priori* upper bound on the amount of entanglement needed to play a given game optimally. Secondly, our toolbox for analyzing quantum entanglement in multiprover interactive proofs is still quite limited. Thus, in addition to its application to hardness amplification, the question of parallel repetition for entangled games is a challenging proving ground for analyzing entanglement in the complexity theoretic setting.

In spite of much research—and partial results, as surveyed in Section 1.3—it remains an open question as to whether an analogue of Raz's theorem holds for entangled games. In this paper, we make progress on this question.

1.1 Our Results

We give the first hardness amplification method for general entangled games, involving any number of players. Prior to this work, parallel repetition theorems were only known for special classes of entangled two-player games, but not *all* games. Our main result can be summarized as follows; see Theorems 5.1 and 6.1 for precise statements.

Theorem 1.1 (Main theorem, informal). *There exists a polynomial-time transformation (called* anchoring*) that takes the description of an arbitrary k-player game G and returns a game $G_\perp$ with the following properties:*

(1) *(Classical hardness amplification)*
If $\mathrm{val}(G) = 1 - \varepsilon$ *then* $\mathrm{val}(G_\perp) = 1 - \frac{3}{4}\varepsilon$ *and* $\mathrm{val}(G_\perp^n) = \exp(-\Omega(\varepsilon^3 \cdot n))$.
(2) *(Quantum hardness amplification)*
If $\mathrm{val}^*(G) = 1 - \delta$ *then* $\mathrm{val}^*(G_\perp) = 1 - \frac{3}{4}\delta$ *and* $\mathrm{val}^*(G_\perp^n) = \exp(-\Omega(\delta^8 \cdot n))$.

The implied constants in the $\Omega(\cdot)$ only depend on the number of players k and the cardinality of the answer sets of G.

We obtain an efficient hardness amplification method from this theorem in the following way: suppose given a k-player game G whose entangled value is either 1 or at most $1 - \delta$. By letting $n = \mathrm{poly}(\log \beta^{-1}, \delta^{-1})$, the game $G_\perp^n$ (the n-fold repetition of the anchored game $G_\perp$) has value either 1 or at most β. An important aspect of our anchoring transformation is that it preserves *quantum completeness*, meaning that if $\mathrm{val}^*(G) = 1$, then $\mathrm{val}^*(G_\perp) = 1$. Similar game transformations in previous works (such as the one given by Feige and Kilian [19]) do *not* preserve quantum completeness, and thus cannot be used for hardness amplification in the same way.

We remark that our theorem applies to games with any number of players, with or without entanglement. Whether Raz's theorem can be extended to games with more than two players is a notorious open problem (even without entanglement).

We also obtain a *threshold* version of the theorem above, which states that the probability that the players win more than an $\mathrm{val}^*(G) + \gamma$ fraction of the n instances of $G_\perp$ in $G_\perp^n$ goes to 0 exponentially fast in n:

Theorem 1.2 (Threshold theorem, informal). *Let G be a k-player game with $\mathrm{val}^*(G) = 1 - \delta$, and $G_\perp$ the anchored version of G. Then for all integer $n \geq 1$ the probability that in the game $G_\perp^n$ the players can win more than $(1 - \frac{3}{4}\delta + \gamma)n$ instances of $G_\perp$ is at most $\exp(-\Omega(\gamma^9 n))$, where the implied constant only depends on the number of players k and the cardinality of the answer sets of G.*

The advantage of having a threshold theorem is that it also implies that parallel repetition reduces the *completeness error* in addition to the soundness error. This is useful in situations where we are trying to distinguish between, say, $\mathrm{val}^*(G) \geq 0.99$ and $\mathrm{val}^*(G) \leq 0.5$. The entangled value of $G_\perp^n$ in both cases is exponentially small. However, if the referee instead checks that the number of instances won in $G_\perp^n$ is above a certain threshold, then we can obtain a new game where either the value is exponentially close to 1 or exponentially close to 0. See Theorem 5.6 for a more precise statement.

Finally, we present an application of our threshold theorem to the so-called Quantum PCP Conjecture. The main application of Raz's parallel repetition theorem is to amplify the completeness/soundness gap of probabilistically checkable proofs, in order to obtain stronger hardness of approximation results (see, e.g., [24]). Similarly, our threshold bound would perform the same function for the multiprover games formulation of the Quantum PCP Conjecture. It is crucial that our threshold bound applies to games with any number of players; so far, it appears that the types of games that arise in approaches to the Quantum PCP Conjecture (games version) involve more than two players [29, 37]. We discuss this in more detail in Section 2.

1.2 The Anchoring Transformation

The idea of modifying the game to facilitate its analysis under parallel repetition originates in work of Feige and Kilian [19] which predates Raz's parallel repetition theorem. Feige and Kilian introduce a transformation that converts an arbitrary game G to a so-called *miss-match* game G_{FK}. The transformation is *value-preserving* in the sense that there is a precise affine relationship $\text{val}(G_{FK}) = (2 + \text{val}(G))/3$. Furthermore Feige and Kilian are able to show that the value of the n-fold repetition of G_{FK} decays *polynomially* in n whenever $\text{val}(G) < 1$. This enables them to establish a general hardness amplification result without having to prove a parallel repetition theorem for arbitrary games. This is sufficient for many applications, including to hardness of approximation, for which it is enough that the hardness amplification procedure be efficient and value-preserving.

Theorem 1.1 adopts a similar approach to that of Feige and Kilian by providing an arguably even simpler transformation, *anchoring*, which preserves both the classical and entangled value of a game and for which we are able to prove an exponential decay under parallel repetition. In contrast, the transformation considered by Feige and Kilian does not in general preserve the entangled value. We proceed to describe our transformation and then discuss the role it plays in facilitating the proof of our parallel repetition theorem.

Definition 1.3 (Basic anchoring). Let G be a two player game with question distribution μ on $\mathcal{X} \times \mathcal{Y}$, and verification predicate V. Let $0 < \alpha < 1$. In the α-anchored game $G_\perp$ the referee chooses a question pair $(x, y) \in \mathcal{X} \times \mathcal{Y}$ according to μ, and independently and with probability α replaces each of x and y with an auxiliary "anchor" symbol $\perp$ to obtain the pair $(x', y') \in (\mathcal{X} \cup \{\perp\}) \times (\mathcal{Y} \cup \{\perp\})$ which is sent to the players as their respective questions. If any of x', y' is $\perp$ the referee accepts regardless of the players' answers; otherwise, the referee checks the players' answers according to the predicate V.

For a choice of $\alpha = 1 - \frac{\sqrt{3}}{2}$ it holds that both $\text{val}(G_\perp) = \frac{3}{4}\text{val}(G) + \frac{1}{4}$ and $\text{val}^*(G_\perp) = \frac{3}{4}\text{val}^*(G) + \frac{1}{4}$. One can think of $G_\perp$ as playing the original game G with probability 3/4, and a trivial game with probability 1/4. The term "anchored" refers to the fact that question pairs chosen according to μ are all "anchored" by a common question $(\perp, \perp)$. Though the existence of this anchor question makes the game $G_\perp$ *easier* to play than the game G, it facilitates showing that the repeated game $G_\perp^n$ is *hard*. At a high level, the anchor questions provide a convenient way to handle the complicated correlations that may arise when the players use non-product strategies in the repeated game.

Our parallel repetition results more generally apply to a class of games we call *anchored*. The anchoring transformation of Theorem 1.1 produces games of this type; however, anchored games can be more general. We give a full definition of anchored games in Section 3. We note that the class of anchored games includes the class of *free games*, a class of games for which quantum parallel repetition theorems were previously shown in [11, 12, 28].

1.3 Related Work

We refer to the surveys by Feige and Raz [18, 42] for an extensive historical account of the classical parallel repetition theorem and its connections to the hardness of approximation and multiprover interactive proof systems, and instead focus on more recent results, specifically those pertaining to the quantum or multiplayer parallel repetition.

The first result on the parallel repetition of entangled-player games was obtained by Cleve et al. [14] for XOR games. This was extended to the case of unique games by Kempe, Regev and Toner [31]. Kempe and Vidick [32] studied a Feige-Kilian type repetition for the entangled value of two-player games, and obtained a polynomial rate of decay. The Feige-Kilian transformation does not in general preserve the entangled value, and their result does not provide a hardness amplification technique for arbitrary entangled games.

Dinur et al. [17] extend the analytical framework of Dinur and Steurer [16] to obtain an exponential-decay parallel repetition theorem for the entangled value of two-player projection games. However their techniques appear to heavily rely on symmetries of projection games, and it is unclear how to extend them to general games. Chailloux and Scarpa [11] and Jain et al. [28] prove exponential-decay parallel repetition for *free two-player games*, i.e. games with a product question distribution. Their analysis, as well as the follow-up work Chung et al. [12], is based on extending the information-theoretic approach of Raz and Holenstein.

Much less is known about the multiplayer setting than the quantum setting. The only parallel repetition bound that applies to all multiplayer games is due to Verbitsky [50], but the rate of decay proved there is very slow – it is essentially an inverse Ackermann-like function. Prior to this work, exponential-decay bounds were only known for multiplayer free games; this was long a folklore result.

Subsequent work. Since the original posting of this work, several relevant papers have emerged [5, 15, 26, 53]. First, [5] analyzed a different hardness amplification method called "fortification", which was first introduced by Moshkovitz [36] in the context of classical parallel repetition. They obtained exponential-decay parallel repetition bounds for quantum as well as multiplayer games, although with the caveat that decay only holds for a bounded number of rounds. Later, Yuen [53] showed that the entangled value of a *general* repeated game must decay to 0 polynomially fast (provided the base game has entangled value less than one), whereas no general decay bound was known for repeated entangled games. Finally, Dinur et al. [15] establish exponential-decay bounds for *expander games*, which includes anchored games and free games as a special case. However, although the multiplayer parallel repetition theorem of [15] is more general than the one proved in this paper, the proof for the special case of anchored games given here is simpler.

1.4 Organization

In Section 2 we give a brief discussion of the Quantum PCP Conjecture, and an application of our threshold theorem (Theorem 5.6) to it. In Section 3 we give an overview of the techniques underlying our main results, mainly focusing on the general ideas and leaving the specifics to each subsequent section. Section 4 introduces some preliminaries, including the definition of anchored games. In Section 5 we present the proof of the quantum parallel repetition theorem for anchored games, as well as the threshold theorem. In

Section 6 we present the result on the parallel repetition of multiplayer classical anchored games. We conclude in Section 7 by recounting a few open problems related to parallel repetition.

2 APPLICATION TO THE QUANTUM PCP CONJECTURE

Just as the the classical parallel repetition theorem is useful for proving hardness of approximation results, one might expect that a *quantum* parallel repetition theorem would be useful for proving *quantum* hardness of approximation results. However, we do not (yet) have a Quantum PCP theorem; as of writing this is an active field of research. Furthermore, while the classical PCP theorem has three equivalent formulations – one in terms of probabilistically checkable proofs, one in terms of hardness of approximation for constraint satisfaction problems (CSP), and one in terms of games – only two out of the three corresponding formulations of the Quantum PCP Conjecture are known to be equivalent.

The following is the formulation of the Quantum PCP Conjecture that is analogous to the classical CSP formulation. (We refer to the survey [2] for further background on the conjecture, including explanations of the standard technical terms we use below.)

Conjecture 2.1 (Quantum PCP Conjecture, constraint satisfaction formulation). *There exists a constant $0 < \gamma < 1$ and integer $k \geq 2$ and $d \geq 2$ for which the following problem is* QMA-*hard: Given $a, b \in [0,1]$ such that $a-b \geq \gamma$ and a k-local Hamiltonian $H = H_1 + \cdots + H_m$ acting on n qudits of local dimension d such that $0 \leq H \leq \mathbb{I}$, decide whether the smallest eigenvalue of H is at least a or at most b, promised that one is the case.*

This problem is known as the k-Local Hamiltonian problem with *constant promise gap*, where by promise gap we mean the gap γ between the thresholds a and b. The problem is only known to be QMA-hard for gaps γ that are inverse polynomial in n [33].

A *games* version of the conjecture is introduced in [21]:

Conjecture 2.2 (Quantum PCP Conjecture, games formulation). *There exists a constant $\gamma \in (0,1)$ and integers $s \geq 1, k \geq 2$ for which the following problem is* QMA-*hard: Given $a, b \in [0,1]$ such that $a - b \geq \gamma$, and a k-player game G where each player answers with s bits, decide whether* $\mathrm{val}^*(G) \geq a$ *or* $\mathrm{val}^*(G) \leq b$*, promised that one is the case.*

When $\mathrm{val}^*(\cdot)$ is replaced with $\mathrm{val}(\cdot)$, the above conjecture is exactly equivalent to the classical PCP theorem. For constant gap γ it was proved by [51] that the problem of approximating the entangled value of a game is at least NP-hard. For inverse polynomial γ the problem was shown QMA-hard [29], and very recently it was even shown to be NEXP-hard [30].

Though neither Conjecture 2.1 nor Conjecture 2.2 has been solved, we can nonetheless explore the consequences if they were true. We give a simple application of our parallel repetition for anchored games: assuming the truth of Conjecture 2.2, we can boost its hardness to any desired gap between completeness and soundness.

Proposition 2.3. *If Conjecture 2.2 is true, then for all $\delta > 0$ the following problem is* QMA-*hard: given a description of a k-player game G with answer size that depends only on δ, distinguish between* $\mathrm{val}^*(G) \geq 1-\delta$ *or* $\mathrm{val}^*(G) \leq \delta$*, promised that one is the case.*

Proof. Let $0 \leq b < a \leq 1$ be a promise gap satisfying the conditions of Conjecture 2.2. Define $a' = (1+3a)/4$, and $b' = (1+3b)/4$. Consider the following reduction: given a description of a k-player game G, promised that either $\mathrm{val}^*(G) \leq b$ or $\mathrm{val}^*(G) \geq a$, outputs the description of the following *threshold game* $G_\perp^{t,\geq\tau}$: the referee plays $G_\perp^t$, the t-fold repetition of $G_\perp$, the anchored version of G, but instead accepts iff the players win at least $\tau := (a' - \frac{a'-b'}{4})t$ games. We set parameters $\Delta = (a'-b')/4$ and $t = \frac{s}{c} \cdot \frac{2}{\Delta^9} \cdot \ln\frac{1}{\delta}$, where s is the length of the players' answers in G, and c is the universal constant from Theorem 5.6.

We get that if $\mathrm{val}^*(G) \geq a$, then $\mathrm{val}^*(G_\perp) \geq a'$. One strategy for $G_\perp^{t,\geq\tau}$ is for the players to play each coordinately independently using the optimal strategy for $G_\perp$. By a Chernoff-Hoeffding bound, the probability that they win at least τ games is at least

$$\mathrm{val}^*(G_\perp^{t,\geq\tau}) \geq 1 - \exp(-t\Delta^2/2) \geq 1-\delta.$$

Otherwise, $\mathrm{val}^*(G) \leq b$. Applying Theorem 5.6, we get that

$$\mathrm{val}^*(G_\perp^{t,\geq\tau}) \leq \left(1 - \Delta^9/2\right)^{c_k t/s} \leq \delta.$$

Observe that this reduction is efficient: the size of the description of $G_\perp^{t,\geq\tau}$ is $O(|G|^t)$; assuming the truth of Conjecture 2.2 this means that $a' - b' = \Omega(a-b) = \Omega(1)$, and thus since δ and s are constant, t is constant. The answer size of the new game is still $O(1)$. Thus the reduction runs in time polynomial in the input instance size, so if there were an algorithm that could distinguish between $\mathrm{val}^*(G_\perp^{t,\geq\tau}) \geq 1-\delta$ or $\mathrm{val}^*(G_\perp^{t,\geq\tau}) \leq \delta$, then this would distinguish between whether $\mathrm{val}^*(G) \geq a$ or $\mathrm{val}^*(G) \leq b$, respectively. □

We point out that we used two features of the anchoring transformation: first, that it allows us to analyze the repetition of arbitrary k-player games; second, it yields threshold theorems for parallel repetition.

3 TECHNICAL OVERVIEW

We give a technical overview of anchored games and their parallel repetition. For concreteness we focus on the case of two-player games. For the full definition of k-player anchored games, see Section 4.3.

Definition 3.1 (Two-player anchored games). Let G be a two-player game with question alphabet $\mathcal{X} \times \mathcal{Y}$ and distribution μ. For any $0 < \alpha \leq 1$ we say that G is α-anchored if there exists subsets $\mathcal{X}_\perp \subseteq \mathcal{X}$ and $\mathcal{Y}_\perp \subseteq \mathcal{Y}$ such that, denoting by μ the respective marginals of μ on both coordinates,

(1) Both $\mu(\mathcal{X}_\perp), \mu(Y_\perp) \geq \alpha$,
(2) Whenever $x \in \mathcal{X}_\perp$ or $y \in \mathcal{Y}_\perp$ it holds that $\mu(x,y) = \mu(x) \cdot \mu(y)$.

Informally, a game is *anchored* if each player independently has a significant probability of receiving a question from the set of "anchor questions" $\mathcal{X}_\perp$ and $\mathcal{Y}_\perp$. An alternative way of thinking about the class of anchored games is to consider the case where μ is uniform over a set of edges in a bipartite graph on vertex set $\mathcal{X} \times \mathcal{Y}$; then the condition is that the induced subgraph on $\mathcal{X}_\perp \times \mathcal{Y}_\perp$ is a complete bipartite graph that is connected to the rest of $\mathcal{X} \times \mathcal{Y}$ and has weight at least α. In other words, a game G is anchored if it contains a free game that is connected to the entire game.

It is easy to see that the games $G_\perp$ output by the anchoring transformation given in Definition 1.3 are α-anchored. Free games are automatically 1-anchored (set $\mathcal{X}_\perp = \mathcal{X}$ and $\mathcal{Y}_\perp = \mathcal{Y}$), but the class of anchored games is much broader; indeed assuming the Exponential Time Hypothesis it is unlikely that there exists a similar (efficient) reduction from general games to free games [1]. Additionally, since free games are anchored games, our parallel repetition theorems automatically reproduce the quantum and multiplayer parallel repetition of free games results of [11, 12, 28], albeit with worse parameters.

Dependency-breaking variables and states. Essentially all known proofs of parallel repetition proceed via reduction, showing how a "too good" strategy for the repeated game G^n can be "rounded" into a strategy for G with success probability strictly greater than val(G), yielding a contradiction.

Let S^n be a strategy for G^n that has a high success probability. By an inductive argument one can identify a set of coordinates C and an index i such that Pr(Players win round $i|W$) > val(G) + δ, where W is the event that the players' answers satisfy the predicate V in all instances of G indexed by C. Given a pair of questions (x, y) in G the strategy S embeds them in the i-th coordinate of a n-tuple of questions

$$x_{[n]}y_{[n]} = \begin{pmatrix} x_1, x_2, \ldots, x_{i-1}, x, x_{i+1}, \ldots, x_n \\ y_1, y_2, \ldots, y_{i-1}, y, y_{i+1}, \ldots, y_n \end{pmatrix}$$

that is distributed according to $\mathsf{P}_{X_{[n]}Y_{[n]}|X_i=x, Y_i=y, W}$. The players then simulate S^n on $x_{[n]}$ and $y_{[n]}$ respectively to obtain answers $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$, and return (a_i, b_i) as their answers in G. The strategy S succeeds with probability precisely Pr(Win $i|W$) in G, yielding the desired contradiction.

As S^n need not be a product strategy, conditioning on W may introduce correlations that make $\mathsf{P}_{X_{[n]}Y_{[n]}|X_i=x, Y_i=y, W}$ impossible to sample exactly. A key insight in Raz' proof of parallel repetition is that it is still possible for the players to *approximately* sample from this distribution. Drawing on the work of Razborov [44], Raz introduced a *dependency-breaking variable* Ω with the following properties:

(a) Given $\omega \sim \mathsf{P}_\Omega$ the players can locally sample $x_{[n]}$ and $y_{[n]}$ according to $\mathsf{P}_{X_{[n]}Y_{[n]}|X_i=x, Y_i=y, W}$,
(b) The players can jointly sample from P_Ω using shared randomness.

In [27] Ω is defined so that a sample ω fixes at least one of $\{x_{i'}, y_{i'}\}$ for each $i' \neq i$. It can then be shown that conditioned on x, Ω is nearly (though not exactly) independent of y, and vice-versa. In other words,

$$\mathsf{P}_{\Omega|X_i=x, W} \approx \mathsf{P}_{\Omega|X_i=x, Y_i=y, W} \approx \mathsf{P}_{\Omega|Y_i=y, W} \quad (1)$$

where "≈" denotes closeness in statistical distance. Eq. (1) suffices to guarantee that the players can *approximately* sample the same ω from $\mathsf{P}_{\Omega|X_i=x, Y_i=y, W}$ with high probability, achieving point (b) above. This sampling is accomplished through a technique called *correlated sampling*.

This argument relies heavily on the assumption that there are only two players who employ a deterministic strategy. With more than two players, it is not known how to design an appropriate dependency-breaking variable Ω that satisfies requirements (a) and (b) above: in order to be jointly sampleable, Ω needs to fix as few inputs as possible; in order to allow players to locally sample their inputs conditioned on Ω, the variable needs to fix as many inputs as possible. These two requirements are in direct conflict as soon as there are more than two players.

In the quantum case the rounding argument seems to require that Alice and Bob jointly sample a *dependency-breaking state* $|\Omega_{x,y}\rangle$, which again depends on both their inputs. Although it is technically more complicated, as a first approximation $|\Omega_{x,y}\rangle$ can be thought of as the players' post-measurement state, conditioned on W. Designing a state that simultaneously allows Alice and Bob to (a) simulate the execution of the i-th game in G^n conditioned on W, and (b) locally generate $|\Omega_{x,y}\rangle$ without communication is the main obstacle to proving a fully general parallel repetition theorem for entangled games.

It has long been known that in the free games case (i.e. games with product question distributions) these troubles with the dependency-breaking variable disappear, and consequently we have parallel repetition theorems for free games for the multiplayer and quantum settings [12]. With free games involving more than two players, it can be shown that

$$\mathsf{P}_{\Omega|X_i=x, Y_i=y, Z_i=z, \ldots, W} \approx \mathsf{P}_{\Omega|W}, \quad (2)$$

on average over question tuples $(x, y, z, \ldots)$. In the quantum case, [11, 12, 28] showed how to construct dependency-breaking states $|\Omega_{X_i=x, Y_i=y, W}\rangle$ and local unitaries U_x and V_y such that

$$(U_x \otimes V_y)|\Omega\rangle \approx |\Omega_{X_i=x, Y_i=y, W}\rangle \quad (3)$$

for some fixed quantum state $|\Omega\rangle$. This eliminates the need for the players to use correlated sampling, as they can simply share a sample from $\mathsf{P}_{\Omega|W}$ or the quantum state $|\Omega\rangle$ from the outset.

Breaking correlations in repeated anchored games. Rather than providing a complete extension of the framework of Raz and Holenstein to the multiplayer and quantum settings, we interpolate between the case of free games and the general setting by showing how the same framework of dependency-breaking variables and states can be extended to anchored games – without using correlated sampling. We introduce dependency-breaking variables Ω and states $|\Phi_{x,y}\rangle$ so that we can prove analogous statements to (2) and (3) in the anchored games setting.

The analysis for anchored games is more intricate than for free games. Proofs of the analogous statements for free games in [11, 12, 28] make crucial use of the fact that all possible question tuples are possible. An anchored game can be far from having this property. Instead, we use the anchors as a "home base" that is connected to all questions. Intuitively, no matter what question tuple $(x, y, z, \ldots)$ we are considering, it is only a few replacements away from the set of anchor questions. Thus the dependency of the variable Ω or state $|\Phi_{x,y}\rangle$ on the questions can be iteratively removed by "switching" each players' question to an anchor as

$$\mathsf{P}_{\Omega|X_i=x, Y_i=y, Z_i=z, W} \approx \mathsf{P}_{\Omega|X_i=x, Y_i=y, Z_i\in\perp, W}$$
$$\approx \mathsf{P}_{\Omega|X_i=x, Y_i\in\perp, Z_i\in\perp, W} \approx \mathsf{P}_{\Omega|X_i\in\perp, Y_i\in\perp, Z_i\in\perp, W},$$

where "$X_i \in \perp$" is shorthand for the event that $X_i \in \mathcal{X}_\perp$.

Dealing with quantum strategies adds another layer of complexity to the argument. The local unitaries U_x and V_y involved in (3) are quite important in the arguments of [11, 12, 28]. The difficulty in extending the argument for free games to the case of general games is to show that these local unitaries each only depend on the input to a single player. In fact with the definition of $|\Omega_{x,y}\rangle$ used in these works it appears likely that this statement does not hold, thus a different approach must be found.

When the game is anchored, however, we are able to use the anchor question in order to show the existence of unitaries U_x and V_y that achieve (3) and depend only on a single player's question each. Achieving this requires us to introduce dependency-breaking states $|\Omega_{x,y}\rangle$ that are more complicated than those used in the free games case; in particular they include information about the *classical* dependency-breaking variables of Raz and Holenstein.

We prove (3) for anchored games by proving a sequence of approximate equalities: first we show that for most x there exists U_x such that $(U_x \otimes \mathbb{I})|\Omega_{\perp,\perp}\rangle \approx |\Omega_{x,\perp}\rangle$, where $|\Omega_{\perp,\perp}\rangle$ denotes the dependency-breaking state in the case that both Alice and Bob receive the anchor question "$\perp$", and $|\Omega_{x,\perp}\rangle$ denotes the state when Alice receives x and Bob receives "$\perp$". Then we show that for all y such that $\mu(y|x) > 0$ there exists a unitary V_y such that $(\mathbb{I} \otimes V_y)|\Omega_{x,\perp}\rangle \approx |\Omega_{x,y}\rangle$. Accomplishing this step requires ideas and techniques going beyond those in the free games case. Interestingly, a crucial component of our proof is to argue the existence of a local unitary $R_{x,y}$ that depends on *both* inputs x and y. The unitary $R_{x,y}$ is not implemented by Alice or Bob in the simulation, but it is needed to show that V_y maps $|\Omega_{x,\perp}\rangle$ onto $|\Omega_{x,y}\rangle$.

One can view our work as pushing the limits of arguments for parallel repetition that do not require some form of correlated sampling, a procedure that seems inherently necessary to analyze the general case. Our results demonstrate that such procedure is not needed for the purpose of achieving strong gap amplification theorems for multiplayer and quantum games.

4 PRELIMINARIES

4.1 Probability Distributions

We largely adopt the notational conventions from [27] 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., $X_{[n]} := (X_1, \ldots, X_n)$, $x_{[n]} = (x_1, \ldots, x_n)$, 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 $\mathsf{P}_X(x)$ to denote the probability that $X = x$ for some value x. For multiple random variables, e.g., X, Y, Z, $\mathsf{P}_{XYZ}(x, y, z)$ denotes their joint distribution with respect to some probability space understood from context.

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

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

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

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

For two random variables X_0 and X_1 over the same set $\mathcal{X}$, $\mathsf{P}_{X_0} \approx_\varepsilon \mathsf{P}_{X_1}$ indicates that the total variation distance between P_{X_0} and P_{X_1},

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

is at most ε.

The following simple lemma will be used repeatedly.

Lemma 4.1. *Let Q_F and S_F be two probability distributions of some random variable F, and let $\mathsf{R}_{G|F}$ be a conditional probability distribution for some random variable G, conditioned on F. Then*

$$\|\mathsf{Q}_F\mathsf{R}_{G|F} - \mathsf{S}_F\mathsf{R}_{G|F}\| = \|\mathsf{Q}_F - \mathsf{S}_F\|.$$

4.2 Quantum Information Theory

For comprehensive references on quantum information we refer the reader to [38, 52].

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* $\mathrm{Tr}(\sqrt{AA^\dagger})$. A density matrix is a positive semidefinite matrix with trace 1. The *fidelity* between two density matrices ρ and σ is defined as $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$. The Fuchs-van de Graaf inequalities relate fidelity and trace norm as

$$1 - F(\rho, \sigma) \le \frac{1}{2}\|\rho - \sigma\|_1 \le \sqrt{1 - F(\rho, \sigma)^2}. \qquad (4)$$

For Hermitian matrices A, B we write $A \le B$ to indicate that $A - B$ is positive semidefinite. We use $\mathbb{I}$ to denote the identity matrix. For an operator X and a density matrix ρ, we write $X[\rho]$ for $X\rho X^\dagger$. 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, ψ refers to the rank-1 density matrix $|\psi\rangle\langle\psi|$. We use subscripts to denote system labels; so ρ_{AB} will denote the density matrix on the systems A and B. A *classical-quantum* state ρ_{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 ρ_{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.

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

Let ρ_{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 ρ_{XAB} that is classical on X and quantum on AB, we write $I(A;B|x)_\rho$ to indicate $I(A;B)_{\rho_x}$.

The following technical lemmas will be used in Section 5.

Proposition 4.2 (Pinsker's inequality). *For all density matrices ρ, σ, $\frac{1}{2}\|\rho - \sigma\|_1^2 \le S(\rho\|\sigma)$.*

Lemma 4.3 ([28], Fact II.8). *Let* $\rho = \sum_z \mathsf{P}_Z(z)|z\rangle\langle z|\otimes\rho_z$, *and* $\rho' = \sum_z \mathsf{P}_{Z'}(z)|z\rangle\langle z|\otimes\rho'_z$. *Then* $S(\rho'\|\rho) = S(\mathsf{P}_{Z'}\|\mathsf{P}_Z)+\mathbb{E}_{Z'}\left[S(\rho'_z\|\rho_z)\right]$. *In particular,* $S(\rho'\|\rho) \geq \mathbb{E}_{Z'}\left[S(\rho'_z\|\rho_z)\right]$.

We will also use the following Lemma from [12].[2]

Lemma 4.4 ([12], Quantum Raz's Lemma). *Let* ρ *and* σ *be two CQ states with* $\rho_{XA} = \rho_{X_1X_2\ldots X_nA}$ *and* $\sigma = \sigma_{XA} = \sigma_{X_1}\otimes\sigma_{X_2}\otimes\ldots\otimes\sigma_{X_n}\otimes\sigma_A$ *with* $X = X_1X_2\ldots X_n$ *classical in both states. Then*

$$\sum_{i=1}^{n} I(X_i\,:\,A)_\rho \leq S(\rho_{XA}\|\sigma_{XA}). \tag{5}$$

4.3 Games, Parallel Repetition, and Anchoring

We formally define k-player one-round games, their parallel repetition, and anchored games.

Multiplayer games. A k-player game $G = (\mathcal{X},\mathcal{A},\mu,V)$ is specified by a question set $\mathcal{X} = \mathcal{X}^1\times\mathcal{X}^2\times\cdots\times\mathcal{X}^k$, answer set $\mathcal{A} = \mathcal{A}^1\times\mathcal{A}^2\times\cdots\times\mathcal{A}^k$, a probability measure μ on $\mathcal{X}$, and a verification predicate $V:\mathcal{X}\times\mathcal{A}\to\{0,1\}$. Throughout this paper, we use superscripts in order to denote which player an input/output symbol is associated with. For example, we write x^1 to denote the input to the first player, and a^t to denote the output of the t-th player. Finally, to denote the tuple of questions/answers to all k players we write $x = (x^1,\ldots,x^k)$ and $a = (a^1,\ldots,a^k)$ respectively.

The *classical value* of a game G is denoted by $\mathrm{val}(G)$ and defined as

$$\sup_{f^1,\ldots,f^k}\ \mathop{\mathbb{E}}_{(x^1,\ldots,x^k)\sim\mu}\left[V\left((x^1,\ldots,x^k),(f^1(x^1),\ldots,f^k(x^k)\right)\right]$$

where the supremum is over all functions $f_i:\mathcal{X}_i\to\mathcal{A}_i$; these correspond to deterministic strategies used by the players. It is easy to see that the classical value of a game is unchanged if we allow the strategies to take advantage of public or private randomness.

The *entangled value* of G is denoted by $\mathrm{val}^*(G)$ and defined as

$$\sup_{\substack{|\psi\rangle\in(\mathbb{C}^d)^{\otimes k}\\ M^1,\ldots,M^k}}\ \mathop{\mathbb{E}}_{(x^1,\ldots,x^k)\sim\mu}\ \sum_{\substack{(a^1,\ldots,a^k):\\ V\left((x^1,\ldots,x^k),(a^1,\ldots,a^k)\right)=1}} \langle\psi|M^1(x^1,a^1)\otimes\cdots\otimes M^k(x^k,a^k)|\psi\rangle \tag{6}$$

where the supremum is over all integer $d\geq 2$, k-partite pure states $|\psi\rangle$ in $(\mathbb{C}^d)^{\otimes k}$, and $M^1,\ldots,M^k$ for each player. Each M^t is a set of POVM measurements $\{M(x^t,a^t)\}_{a^t\in\mathcal{A}^t}$ acting on $\mathbb{C}^d$, one for each question $x^t\in\mathcal{X}^t$.

Repeated games. Let $G = (\mathcal{X},\mathcal{A},\mu,V)$ be a k-player game, with $\mathcal{X} = \mathcal{X}^1\times\cdots\times\mathcal{X}^k$ and $\mathcal{A} = \mathcal{A}^1\times\cdots\times\mathcal{A}^k$. Let $\mu^{\otimes n}$ denote the product probability distribution over $\mathcal{X}^{\otimes n} = \bigotimes_{i=1}^n\mathcal{X}_i$, where each $\mathcal{X}_i$ is a copy of $\mathcal{X}$. Similarly let $\mathcal{A}^{\otimes n} = \bigotimes_{i=1}^n\mathcal{A}_i$ where each $\mathcal{A}_i$ is a copy of $\mathcal{A}$. [3] Let $V^{\otimes n}:\mathcal{X}^{\otimes n}\times\mathcal{A}^{\otimes n}\to\{0,1\}$ denote the verification predicate that is 1 on question tuple $(x_1,\ldots,x_n)\in\mathcal{X}^{\otimes n}$ and answer tuple $(a_1,\ldots,a_n)\in\mathcal{A}^{\otimes n}$ iff for all i, $V(x_i,a_i)=1$. We define the n-fold parallel repetition of G to be the k-player game $G^n = (\mathcal{X}^{\otimes n},\mathcal{A}^{\otimes n},\mu^{\otimes n},V^{\otimes n})$.

When working with games with more than 2 players, we use subscripts to denote which game round/coordinate a question/answer symbol is associated with. For example, by x_i^t we mean the question to the t-th player in the i-th round. While this is overloading notation slightly (because superscripts are meant to indicate tuples), we use this convention for the sake of readability. When x^n refers to a tuple $(x_1,\ldots,x_n)$ and when x_i^t refers to the t-th player's question in the i-th coordinate should be clear from context.

Anchored games. We give the general definition of an anchored game.

Definition 4.5 (Multiplayer Anchored Games). A game $G = (\mathcal{X},\mathcal{A},\mu,V)$ is called α-anchored if there exists $\mathcal{X}_\perp^t\subseteq\mathcal{X}^t$ for all $t\in[k]$ where

(1) $\mu(\mathcal{X}_\perp^t)\geq\alpha$ for all $t\in[k]$, and
(2) for all $x\in\mathcal{X}$,

$$\mu(x) = \mu(x|_{\overline{F}_x})\cdot\prod_{t\in F_x}\mu(x^t) \tag{7}$$

where for all question tuples $x = (x^1,x^2,\ldots,x^k)\in\mathcal{X}$, $F_x\subseteq[n]$ denotes the set of coordinates of x that lie in the anchor, i.e.

$$F_x = \{t\in[k]\,:\,x^t\in\mathcal{X}_\perp^t\}$$

and $\overline{F}_x$ denotes the complement, i.e., $[n]-F_x$.

Here for a set $S\subseteq[n]$, $\mu(x|_S)$ denotes the marginal probability of the question tuple x restricted to the coordinates in S, i.e.

$$\mu(x|_S) = \sum_{x'|_S = x|_S}\mu(x').$$

When $k=2$ this definition coincides with the definition of two-player anchored games in Definition 3.1. Additionally, just like the two-player case, one can easily extend the anchoring transformation given in Definition 1.3 to arbitrary k-player games:

Proposition 4.6. *Let* $G = (\mathcal{X},\mathcal{A},\mu,V)$ *be a* k*-player game. Let* $G_\perp$ *be the* k*-player game where the referee samples* $(x^1,x^2,\ldots,x^k)$ *according to* μ*, replaces each* x^t *with an auxiliary symbol* $\perp$ *independently with probability* α*, and checks the players' answers according to* V *if all* $x^t\neq\perp$*, and otherwise the referee accepts. Then* $G_\perp$ *is an* α*-anchored game satisfying*

$$\begin{aligned}\mathrm{val}(G_\perp) &= 1-(1-\alpha)^k\cdot(1-\mathrm{val}(G))\\ \mathrm{val}^*(G_\perp) &= 1-(1-\alpha)^k\cdot(1-\mathrm{val}^*(G)).\end{aligned} \tag{8}$$

5 PARALLEL REPETITION OF ANCHORED GAMES WITH ENTANGLED PLAYERS

This section is devoted to the analysis of the entangled value of repeated anchored games. The main theorem we prove is the following:

Theorem 5.1. *Let* G *be a* k*-player* α*-anchored game satisfying* $\mathrm{val}^*(G) = 1-\varepsilon$. *Then*

$$\mathrm{val}^*(G^n)\leq\exp\left(-\Omega\left(\frac{\mathrm{poly}(\alpha^k)\cdot\varepsilon^8\cdot n}{\mathrm{poly}(k)\cdot s}\right)\right),$$

[2] Some versions of this lemma, though in a less compact form, also appear in [11, 28].
[3] We will use the tensor product notation ("$\bigotimes$") to denote product across coordinates in a repeated game, and the traditional product notation ("$\times$") to denote product across players.

where s is the total length of the answers output by the players.

For clarity we will focus on the $k = 2$ (two-player) case; we will describe how to extend the proof to arbitrary k at the end. We fix an α-anchored two-player game $G = (\mathcal{X} \times \mathcal{Y}, \mathcal{A} \times \mathcal{B}, \mu, V)$ with entangled value $\mathrm{val}^*(G) = 1 - \varepsilon$ and anchor sets $\mathcal{X}_\perp \subseteq \mathcal{X}, \mathcal{Y}_\perp \subseteq \mathcal{Y}$ for Alice and Bob, respectively. We also fix an optimal strategy for G^n, consisting of a shared entangled state $|\psi\rangle^{E_A E_B}$ and POVMs $\{A^{a^n}_{x^n}\}$ and $\{B^{b^n}_{y^n}\}$ for Alice and Bob respectively. Without loss of generality we assume that $|\psi\rangle$ is invariant under permutation of the two registers, i.e. there exist basis vectors $\{|v_j\rangle\}_j$ such that $|\psi\rangle = \sum_j \sqrt{\lambda_j} |v_j\rangle|v_j\rangle$.

5.1 Setup

We introduce the random variables, entangled states and operators that play an important role in the proof of Theorem 5.1. The section is divided into three parts: first we define the dependency-breaking variable Ω. Then we state useful lemmas about conditioned distributions. Finally we describe the states and operators used in the proof.

Dependency-breaking variables. Let $C \subseteq [n]$ a fixed set of coordinates for the repeated game G^n. We will assume that $C = \{m+1, m+2, \ldots, n\}$, 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 μ^n and (A^n, B^n) be defined from X^n and Y^n as follows:

$$\mathsf{P}_{A^n B^n | X^n = x^n, Y^n = y^n}(a^n, b^n) = \langle \psi | A^{a^n}_{x^n} \otimes B^{b^n}_{y^n} |\psi\rangle.$$

Let (X_C, Y_C) and $Z = (A_C, B_C)$ denote the players' questions and answers respectively associated with the coordinates indexed by C. For $i \in [n]$ let W_i denote the event that the players win round i while playing G^n. Let $W_C = \bigwedge_{i \in C} W_i$.

We use the same dependency-breaking variable Ω that is used in Holenstein's proof of parallel repetition. In those works, for all $i \in [n]$, Ω_i fixes at least one of X_i or Y_i (and sometimes both, if $i \in C$). Thus, conditioned on Ω, X^n and Y^n are independent of each other.

In more detail, let $D_1, \ldots, D_m$ be independent and uniformly distributed over $\{A, B\}$. Let $M_1, \ldots, M_m$ be independent random variables defined in the following way. If $D_i = A$, then M_i is coupled to X_i (that is, takes the same value as X_i). Otherwise, if $D_i = B$, then M_i is coupled to Y_i. Then $\Omega_i = (D_i, M_i)$, and $\Omega = (\Omega_1, \ldots, \Omega_m, X_C, Y_C)$.

Conditioned distributions. Define

$$\delta_C := \frac{1}{m}\left(\log 1/\Pr(W_C) + |C| \log |\mathcal{A}||\mathcal{B}|\right).$$

For notational convenience we often use the shorthand $X_i \in \perp$ and $Y_i \in \perp$ to stand for $X_i \in \mathcal{X}_\perp$ and $Y_i \in \mathcal{Y}_\perp$, respectively. The following lemma essentially follows from the classical arguments used in [27].

Lemma 5.2. *The following statements hold on, average over i chosen uniformly in* $[m]$*:*

(1) $\mathbb{E}_i \| \mathsf{P}_{D_i M_i X_i Y_i | W_C} - \mathsf{P}_{D_i M_i X_i Y_i} \| \le O(\sqrt{\delta_C})$
(2) $\mathbb{E}_i \| \mathsf{P}_{\Omega Z X_i Y_i | W_C} - \mathsf{P}_{\Omega Z | W_C} \mathsf{P}_{X_i Y_i | \Omega} \| \le O(\sqrt{\delta_C})$
(3) $\mathbb{E}_i \| \mathsf{P}_{X_i Y_i} \mathsf{P}_{\Omega_{-i} Z | X_i \in \perp, Y_i \in \perp, W_C} - \mathsf{P}_{X_i Y_i} \mathsf{P}_{\Omega_{-i} Z | X_i Y_i W_C} \| \le O(\sqrt{\delta_C}/\alpha^2)$
(4) $\mathbb{E}_i \left\| \mathsf{P}_{X_i Y_i} \mathsf{P}_{\Omega_{-i} Z | X_i Y_i W_C} - \mathsf{P}_{X_i Y_i \Omega_{-i} Z | W} \right\| \le O(\sqrt{\delta_C}/\alpha^2)$

Quantum states and operators. Recall that we have fixed an optimal strategy for Alice and Bob in the game G^n. This specifies a shared entangled state $|\psi\rangle$, and measurement operators $\{A^{a^n}_{x^n}\}$ for Alice and $\{B^{b^n}_{y^n}\}$ for Bob.

Operators. Define, for all a_C, b_C, x^n, y^n:

$$A^{a_C}_{x^n} := \sum_{a^n | a_C} A^{a^n}_{x^n}$$
$$B^{b_C}_{y^n} := \sum_{b^n | b_C} B^{b^n}_{y^n}$$

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). For all i, ω_{-i}, x_i, and y_i define:

$$A^{a_C}_{\omega_{-i}, x_i} = \mathop{\mathbb{E}}_{X^n | \omega_{-i}, x_i} A^{a_C}_{x^n}$$
$$B^{b_C}_{\omega_{-i}, y_i} = \mathop{\mathbb{E}}_{Y^n | \omega_{-i}, y_i} B^{b_C}_{y^n}$$

where recall that $\mathbb{E}_{X^n | \omega_{-i}, x_i}$ is shorthand for $\mathbb{E}_{X^n | \Omega_{-i} = \omega_{-i}, X_i = x_i}$. Intuitively, these operators represent the "average" measurement that Alice and Bob apply, conditioned on $\Omega_{-i} = \omega_{-i}$, and $X_i = x_i$ and $Y_i = y_i$. Next, define

$$A^{a_C}_{\omega_{-i}, \perp} := \mathop{\mathbb{E}}_{X^n | \Omega_{-i} = \omega_{-i} \wedge X_i \in \perp} A^{a_C}_{x^n}$$
$$B^{b_C}_{\omega_{-i}, \perp} := \mathop{\mathbb{E}}_{Y^n | \Omega_{-i} = \omega_{-i} \wedge Y_i \in \perp} B^{b_C}_{y^n}.$$

These operators represent the "average" measurement performed by Alice and Bob, conditioned on $\Omega_{-i} = \omega_{-i}$ and $M_i = \perp$. Finally, for all $x_i \in \mathcal{X}$ and $y_i \in \mathcal{Y}$, define

$$A^{a_C}_{\omega_{-i}, \perp/x_i} := \frac{1}{2} A^{a_C}_{\omega_{-i}, \perp} + \frac{1}{2} A^{a_C}_{\omega_{-i}, x_i}$$
$$dB^{b_C}_{\omega_{-i}, \perp/y_i} := \frac{1}{2} B^{b_C}_{\omega_{-i}, \perp} + \frac{1}{2} B^{b_C}_{\omega_{-i}, y_i}.$$

Intuitively, these operators represent the "average" measurements conditioned on $\Omega_{-i} = \omega_{-i}$ and when X_i is x_i with probability 1/2 and $\perp$ with probability 1/2 (or when $Y_i = y_i$ with probability 1/2 and $\perp$ with probability 1/2).

For notational convenience we often suppress the dependence on $(i, \omega_{-i}, z = (a_C, b_C))$ when it is clea from context. Thus, when we refer to an operator such as $A_{\perp/x}$, we really mean the operator $A^{a_C}_{\omega_{-i}, \perp/x_i}$.

States. For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, define the following (unnormalized) states:

$$|\Phi_{x,y}\rangle := \sqrt{A_x} \otimes \sqrt{B_y} |\psi\rangle$$
$$|\Phi_{x,\perp}\rangle := \sqrt{A_x} \otimes \sqrt{B_\perp} |\psi\rangle$$
$$|\Phi_{\perp/x,\perp}\rangle := \sqrt{A_{\perp/x}} \otimes \sqrt{B_\perp} |\psi\rangle$$
$$|\Phi_{\perp/x,y}\rangle := \sqrt{A_{\perp/x}} \otimes \sqrt{B_y} |\psi\rangle \quad (9)$$
$$|\Phi_{\perp,\perp}\rangle := \sqrt{A_\perp} \otimes \sqrt{B_\perp} |\psi\rangle$$

together with the normalization factors

$$\gamma_{x,y} := \left\||\Phi_{x,y}\rangle\right\| \qquad \gamma_{x,\perp} := \||\Phi_{x,\perp}\rangle\|$$
$$\gamma_{\perp/x,\perp} := \left\||\Phi_{\perp/x,\perp}\rangle\right\| \qquad \gamma_{\perp/x,y} := \left\||\Phi_{\perp/x,y}\rangle\right\|$$
$$\gamma_{\perp,\perp} := \||\Phi_{\perp,\perp}\rangle\|$$

Note that these normalization factors are the square-roots of the probabilities that a certain pair of answers $z = (a_C, b_C)$ occurred, given the specified inputs and the dependency-breaking variables. For example, revealing the depencies on ω_{-i} and z, we have

$$\gamma_{\substack{\omega_{-i},z\\x_i,y_i}} = \sqrt{\mathsf{P}_{Z|\omega_{-i},x_i,y_i}(z)}.$$

We denote the normalized states by $|\widetilde{\Phi}_{x,y}\rangle = |\Phi_{x,y}\rangle/\gamma_{x,y}$, $|\widetilde{\Phi}_{x,\perp}\rangle = |\Phi_{x,\perp}\rangle/\gamma_{x,\perp}$, $|\widetilde{\Phi}_{\perp/x,\perp}\rangle = |\Phi_{\perp,\perp}\rangle/\gamma_{\perp/x,\perp}$, $|\widetilde{\Phi}_{\perp/x,\perp/y}\rangle = |\Phi_{\perp/x,y}\rangle/\gamma_{\perp/x,y}$, and $|\widetilde{\Phi}_{\perp,\perp}\rangle = |\Phi_{\perp,\perp}\rangle/\gamma_{\perp,\perp}$.

5.2 Proof of the Parallel Repetition Theorem

Lemma 5.3. *Let G be an α-anchored two-player game. Let $C \subset [n]$ be a set of coordinates. Then*

$$\mathop{\mathbb{E}}_{i \notin C} \Pr(W_i|W_C) \le \mathrm{val}^*(G) + O(\delta_C^{1/8}/\alpha^2)$$

where the expectation is over a uniformly chosen $i \in [n]\backslash C$ and $\delta_C = \frac{1}{m}(\log 1/\Pr(W_C) + |C| \log|\mathcal{A}||\mathcal{B}|)$.

Proof. For every ω_{-i}, $z = (a_C, b_C)$, $x_i \in \mathcal{X}$, $y_i \in \mathcal{Y}$, $a_i \in \mathcal{A}$ and $b_i \in \mathcal{B}$, define

$$\hat{A}^{a_i}_{\omega_{-i},x_i} := \sum_{a^n|a_i,a_C} (A^{a_C}_{\omega_{-i},x_i})^{-1/2} A^{a^n}_{\omega_{-i},x_i} (A^{a_C}_{\omega_{-i},x_i})^{-1/2}$$
$$\hat{B}^{b_i}_{\omega_{-i},y_i} := \sum_{b^n|b_i,b_C} (B^{b_C}_{\omega_{-i},y_i})^{-1/2} B^{b^n}_{\omega_{-i},y_i} (B^{b_C}_{\omega_{-i},y_i})^{-1/2}$$

where $a^n|a_i, a_C$ (resp. $b^n|b_i, b_C$) denotes summing over tuples a^n that are consistent with a_C and a_i (resp. b^n that are consistent with b_C and b_i). Note that the $\{\hat{A}^{a_i}_{\omega_{-i},x_i}\}_{a_i}$ and $\{\hat{B}^{b_i}_{\omega_{-i},y_i}\}_{b_i}$ are positive semidefinite operators that sum to identity, so form valid POVMs.

Consider the following strategy to play game G. Alice and Bob share classical public randomness, and for every setting of i, ω_{-i}, z, the bipartite state $|\widetilde{\Phi}_{\substack{\omega_{-i},z\\\perp,\perp}}\rangle$. Upon receiving questions $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ respectively they perform the following:

1. Alice and Bob use public randomness to sample (i, ω_{-i}, z) conditioned on W_C.
2. Alice applies $U_{\omega_{-i},z,x}$ to her register of $|\widetilde{\Phi}_{\substack{\omega_{-i},z\\\perp,\perp}}\rangle$.
3. Bob applies $V_{\omega_{-i},z,y}$ to his register of $|\widetilde{\Phi}_{\substack{\omega_{-i},z\\\perp,\perp}}\rangle$.
4. Alice measures with POVM operators $\{\hat{A}^{a_i}_{\omega_{-i},x}\}$ and returns the outcome as her answer.
5. Bob measures with POVM operators $\{\hat{B}^{b_i}_{\omega_{-i},y}\}$ and returns the outcome as his answer.

Suppose that, upon receiving questions (x, y) and after jointly picking a uniformly random $i \in [m]$, Alice and Bob could jointly sample ω_{-i}, z from $\mathsf{P}_{\Omega_{-i}Z|W_C}$ and locally prepare the state $|\widetilde{\Phi}_{\substack{\omega_{-i},z\\x,y}}\rangle$. For a fixed (x, y), ω_{-i} and z, the distribution of outcomes (a_i, b_i) after measuring $\{\hat{A}^{a_i}_{\omega_{-i},x} \otimes \hat{B}^{b_i}_{\omega_{-i},y}\}_{a_i,b_i}$ will be identical to $\mathsf{P}_{A_iB_i|\omega_{-i},z,x,y}$ (where we mean conditioning on $X_i = x$ and $Y_i = y$). Averaging over $(x, y) \sim \mu$, i, ω_{-i}, and z, the above-defined strategy will win game G with probability at least $\mathbb{E}_i \Pr(W_i|W_C)$.

Next we show that Alice and Bob are able to *approximately* prepare $|\widetilde{\Phi}_{\substack{\omega_{-i},z\\x,y}}\rangle$ with high probability, and thus produce answers that are approximately distributed according to $\mathsf{P}_{A_iB_i|\omega_{-i},z,x,y}$, allowing them to win game G with probability greater than $1 - \varepsilon$ — a contradiction.

For the remainder of the proof, we will fix C and implicitly carry it around. Let $\delta = \delta_C$. We use the following lemma:

Lemma 5.4. *For every C, i, ω_{-i}, $z = (a_C, b_C)$, x_i and y_i there exists unitaries U_{ω_{-i},z,x_i} acting on E_A and V_{ω_{-i},z,y_i} acting on E_B such that*

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{X_iY_i,\Omega_{-i}Z|W} \left\|(U_{\omega_{-i},z,x_i} \otimes V_{\omega_{-i},z,y_i}) \left|\widetilde{\Phi}_{\substack{\omega_{-i},z\\\perp,\perp}}\right\rangle - \left|\widetilde{\Phi}_{\substack{\omega_{-i},z\\x_i,y_i}}\right\rangle\right\|^2 = O(\delta^{1/4}/\alpha^4).$$

The proof of Lemma 5.4 can be found in the full version of this paper [4]. Using the fact that for two pure states $|\psi\rangle$ and $|\phi\rangle$, $\|\psi - \phi\|_1 \le \sqrt{2}\| |\psi\rangle - |\phi\rangle\|$, as well as Jensen's inequality,

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{XY\Omega_{-i}Z|W_C} \left\|(U_{\omega_{-i},z,x} \otimes V_{\omega_{-i},z,y}) \left[\widetilde{\Phi}_{\substack{\omega_{-i},z\\\perp,\perp}}\right] - \widetilde{\Phi}_{\substack{\omega_{-i},z\\x,y}}\right\|_1 = O\left(\frac{\delta^{1/8}}{\alpha^2}\right), \tag{10}$$

where the second expectation is over (x, y) drawn from μ, and $(U \otimes V)[\widetilde{\Phi}]$ denotes $(U \otimes V)\widetilde{\Phi}(U \otimes V)^\dagger$. Conditioned on a given pair of questions (x, y) and the players sampling (i, ω_{-i}, z) in Step 1., the state that the players prepare after Step 3. in the protocol is precisely $(U_{\omega_{-i},z,x} \otimes V_{\omega_{-i},z,y})[\widetilde{\Phi}_{\substack{\omega_{-i},z\\\perp,\perp}}]$. Let $\mathcal{E}_{\substack{\omega_{-i},z\\x,y}}$ denote the quantum-classical channel on density matrices that performs the measurement $\{\hat{A}^{a_i}_{\omega_{-i},x} \otimes \hat{B}^{b_i}_{\omega_{-i},y}\}_{a_i,b_i}$, and outputs a classical register with the measurement outcome (a_i, b_i). Applying $\mathcal{E}_{\substack{\omega_{-i},z\\x,y}}$ to the expression inside the trace norm in (10), using that the trace norm is non-increasing under quantum operations,

$$\mathop{\mathbb{E}}_{i} \mathop{\mathbb{E}}_{XY\Omega_{-i}Z|W_C} \left\|\widetilde{\mathsf{P}}_{A_iB_i|\omega_{-i},v,x,y} - \mathsf{P}_{A_iB_i|\omega_{-i},v,x,y}\right\| \le O(\delta^{1/8}/\alpha^2).$$

where $\widetilde{\mathsf{P}}_{A_iB_i|\omega_i,z,x,y}(a_i, b_i)$ denotes the probability of outcome (a_i, b_i) in the above strategy, conditioned on questions (x, y) and the players sampling (i, ω_{-i}, z) in Step 1. Thus

$$\begin{aligned}
&\mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W_C} \cdot \mathsf{P}_{XY} \cdot \widetilde{\mathsf{P}}_{A_iB_i|\Omega_{-i}ZX_iY_i} \\
&\approx_{O(\delta^{1/8}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}Z|W_C} \cdot \mathsf{P}_{XY} \cdot \mathsf{P}_{A_iB_i|\Omega_{-i}ZX_iY_i} \\
&\approx_{O(\delta^{1/8}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{\Omega_{-i}ZX_iY_i|W_C} \cdot \mathsf{P}_{A_iB_i|\Omega_{-i}ZX_iY_i}
\end{aligned}$$

where the X_iY_i in the conditionals is shorthand for $X_i = x, Y_i = y$. The last approximate equality follows from Lemma 5.2. Marginalizing $\Omega_{-i}Z$, we get

$$\mathsf{P}_I \cdot \mathsf{P}_{XY} \cdot \widetilde{\mathsf{P}}_{A_iB_i|X_iY_i} \approx_{O(\delta^{1/8}/\alpha^2)} \mathsf{P}_I \cdot \mathsf{P}_{X_iY_iA_iB_i|W_C}. \tag{11}$$

Under the distribution $\mathsf{P}_{X_iY_iA_iB_i|W_C}$, the probability that $V(x_i, y_i, a_i, b_i)$ is 1 is precisely $\Pr(W_i|W_C)$. On the other hand, (11) implies that using the protocol described above the players win G with probability at least $\mathbb{E}_i \Pr(W_i|W_C) - O(\delta^{1/8}/\alpha^2)$. This concludes the proof of the lemma. □

Given Lemma 5.3, the proof of Theorem 5.1 (at least the two player case) follows using a standard inductive argument (see, e.g., the argument for Theorem 6.1 given in Section 6). In the next section, we sketch the changes necessary to adapt the proof to handle an arbitrary number of players.

5.3 Extending the Argument to More Than Two Players

We extend the argument from the previous sections to games with $k > 2$ entangled players. We describe the required modifications to the case of $k = 3$; the only hurdle in handling larger number of players is notational. Furthermore we restrict our attention to the repetition of the game $G_\perp$ obtained by applying the anchor transformation to a game G.

Let G be an arbitrary game involving three players Alice, Bob and Charlie. The players' questions are denoted by X, Y, Z, and their outputs are denoted as A, B, C. We will let $\mu(x, y, z)$ denote the question distribution of the game G. Let $G_\perp$ be the anchoring transformation applied to G (for some α), and let $\mu_\perp(x, y, z)$ denote the question distribution of $G_\perp$. We analyze the behavior of $\mathrm{val}^*(G_\perp^n)$. Consider an optimal strategy for $G_\perp^n$, involving a tripartite state $|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$ and POVM for each of the players: $\{A_{x^n}^{a^n}\}$ for Alice, $\{B_{y^n}^{b^n}\}$ for Bob, and $\{C_{z^n}^{c^n}\}$ for Charlie. The entangled state $|\psi\rangle$ is supported on three registers E_A, E_B, and E_C.

The subset of coordinates that we condition on winning (formerly called C) will be denoted by S. The answers to rounds in S that we condition on will be denoted together as $Q = (A_S, B_S, C_S)$ (formerly called $Z = (A_C, B_C)$).

The idea behind the proof of the multiplayer extension is to reduce to the two-player case by "combining" two of the three players and treating them as a single player.

Dependency-breaking variable. The dependency-breaking variable Ω is constructed so that for each coordinate $i \notin S$, Ω_i fixes 2 out of 3 questions. That is, D_i is uniformly distributed over $\{\{A, B\}, \{A, C\}, \{B, C\}\}$. The variable D_i indicates which questions M_i is coupled to. For example, if $D_i = \{A, B\}$, then M_i is coupled to the pair (X_i, Y_i). The dependency breaking variable satisfies the property that for all ω, for all i, $\mathsf{P}_{X_i Y_i Z_i|\Omega=\omega}(x, y, z) = \mathsf{P}_{X_i|\Omega=\omega}(x) \cdot \mathsf{P}_{Y_i|\Omega=\omega}(y) \cdot \mathsf{P}_{Z_i|\Omega=\omega}(z)$.

Operators and states. We define the states and operators in a nearly identical way to the two-player case. We also introduce operators corresponding to the third player, $C_{\omega_{-i}, z_i}^{c_S}, C_{\omega_{-i}, \perp}^{c_S}, C_{\omega_{-i}, \perp/(x_i, y_i)}^{c_S}$, etc., defined in the obvious manner.

The states are also defined in a similar way:

$$|\Phi_{x,y,z}\rangle = \sqrt{A_x} \otimes \sqrt{B_y} \otimes \sqrt{C_z}|\psi\rangle$$

where x, y, and z can be "normal" questions from $\mathcal{X}$, $\mathcal{Y}$, or $\mathcal{Z}$, or they can be $\perp$ or a hybrid such as $\perp/x$.

The analogue of Lemma 5.4 in the three-player setting is the following. We use simplified notation to maximize clarity, and suppress mention of i, ω_{-i}, and $q = (a_S, b_S, c_S)$.

Lemma 5.5. *For all $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$, there exist unitaries U_x, V_y, and W_z acting on E_A, E_B, and E_C respectively such that*

$$\mathop{\mathbb{E}}_{XYZ} \left\| (U_x \otimes V_y \otimes W_z)|\Phi_{\perp,\perp,\perp}\rangle - |\Phi_{x,y,z}\rangle \right\|^2 = O(\delta^{1/4}/\alpha^{2k}).$$

Proof sketch. Lemma 5.5, as in the two-player case, is proved in two steps. The first step is to establish the existence of unitaries U_x, V_y, and W_z such that $U_x|\Phi_{\perp,\perp,\perp}\rangle \approx |\Phi_{x,\perp,\perp}\rangle$, $V_x|\Phi_{\perp,\perp,\perp}\rangle \approx |\Phi_{\perp,y,\perp}\rangle$, and $W_z|\Phi_{\perp,\perp,\perp}\rangle \approx |\Phi_{\perp,\perp,z}\rangle$, with the unitaries acting on the appropriate spaces.

To prove, say, the existence of U_x, we treat Bob and Charlie as a single player – call him "SuperBob" – and use the analysis from the two-player case where the game G is a two player game involving Alice and SuperBob. Using the same reasoning as in the two-player case, we get that

$$\mathop{\mathbb{E}}_{XY} \left\| (U_x \otimes V_y \otimes \mathbb{I})|\Phi_{\perp,\perp,\perp}\rangle - |\Phi_{x,y,\perp}\rangle \right\|^2 = O(\delta^{1/4}/\alpha^{2k}).$$

It then only remains to show that, on average over (x, y, z), $(\mathbb{I} \otimes \mathbb{I} \otimes W_z)|\Phi_{x,y,\perp}\rangle$ is close to $|\Phi_{x,y,z}\rangle$:

$$\begin{aligned}
&\left\| W_z|\Phi_{x,y,\perp}\rangle - |\Phi_{x,y,z}\rangle \right\| \\
&= \left\| W_z C_\perp C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle - C_z C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle \right\| \\
&= \left\| H_{x,y,z} \otimes W_z C_\perp C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle - H_{x,y,z} \otimes C_z C_{\perp/z}^{-1/2}|\Phi_{x,y,\perp/z}\rangle \right\| \\
&\approx \left\| W_z C_\perp C_{\perp/z}^{-1/2}|\Phi_{\perp,\perp,\perp/z}\rangle - C_z C_{\perp/z}^{-1/2}|\Phi_{\perp,\perp,\perp/z}\rangle \right\| \\
&= \| W_z|\Phi_{\perp,\perp,\perp}\rangle - |\Phi_{\perp,\perp,z}\rangle \| \\
&\approx 0,
\end{aligned}$$

where $H_{x,y,z}$ is a unitary acting on $E_A E_B$ jointly such that

$$H_{x,y,z}|\Phi_{x,y,\perp/z}\rangle \approx |\Phi_{\perp,\perp,\perp/z}\rangle.$$

□

The main theorem for the case of $k > 2$ entangled players follows from Lemma 5.5 using the same steps as in the two-player case.

5.4 A Threshold Theorem

We also observe that our proof nearly immediately yields a *threshold* version of our parallel repetition theorem: we can give an exponentially small bound on the probability that the players are able to win significantly more than a $(1 - \varepsilon)n$ coordinates in the repeated game $G_\perp^n$, where $\mathrm{val}^*(G_\perp) = 1 - \varepsilon$. In [40], Rao shows how a Lemma of the form Lemma 5.3 yields not only a parallel repetition theorem, but also gives a concentration bound. Using essentially the same argument, we get the following theorem:

Theorem 5.6. *Let G be an α-anchored k-player game with $\mathrm{val}^*(G) \leq 1 - \varepsilon$. Then for all integer $n \geq 1$ the probability that in the game G^n the players can win more than $(1 - \varepsilon + \gamma)n$ games is at most*

$$\left(1 - \gamma^9/2\right)^{c\,\alpha^{8k}\,n/s}$$

where c is a universal constant and s is the length of the players' answers.

6 CLASSICAL MULTIPLAYER GAMES

Perhaps the most well-known open problem about the classical parallel repetition of games is whether an analogue of Raz's theorem holds for games with more than two players. While the two-player case already presented a number of non-trivial difficulties, proving a parallel repetition theorem for three or more players is believed to require substantially new ideas.[4]

In this section we show that multiplayer anchored games satisfy a classical parallel repetition theorem. Thus, the anchoring transformation along with parallel repetition yields a general hardness amplification technique for classical multiplayer games involving any number of players.[5]

Theorem 6.1. *Let $G = (\mathcal{X}, \mathcal{A}, \mu, V)$ be a k-player α-anchored game such that* $\mathrm{val}(G) \leq 1 - \varepsilon$. *Then*

$$\mathrm{val}(G^n) \leq \exp\left(-\frac{\alpha^{2k} \cdot \varepsilon^3 \cdot n}{384 \cdot s \cdot k^2}\right), \tag{12}$$

where $s = \log |\mathcal{A}|$.

For the remainder of this section we fix a k-player α-anchored game $G = (\mathcal{X}, \mathcal{A}, \mu, V)$, an integer n, and a deterministic strategy for the k players in the repeated game G^n that achieves success probability $\mathrm{val}(G^n)$. In Section 6.1 we introduce the notation, random variables and basic lemmas for the proof. The proof of Theorem 6.1 itself is given in Section 6.2.

6.1 Breaking Classical Multipartite Correlations

We refer to Section 4.3 for basic notation related to multiplayer games.

Let $C \subseteq [n]$ a fixed set of coordinates for the repeated game G^n of size $|C| = n-m$. It will be convenient to fix $C = \{m+1, m+2, \ldots, n\}$; the symmetry of the problem will make it clear that this is without loss of generality. Let $\mathrm{Z} = A_C = (A_C^1, A_C^2, \ldots, A_C^k)$ denote the players' answers associated with the coordinates indexed by C.

For $t \in [k]$ let $\mathcal{Y}^t = (\mathcal{X}^t \setminus \mathcal{X}_\perp^t) \cup \{\perp\}$, and define a random variable

$$Y^t = \begin{cases} X^t, & X^t \in \mathcal{X}^t \setminus \mathcal{X}_\perp^t \\ \perp, & X^t \in \mathcal{X}_\perp^t \end{cases}. \tag{13}$$

Let $\mathcal{Y} = \mathcal{Y}^1 \times \mathcal{Y}^2 \times \ldots \times \mathcal{Y}^k$ and $Y = (Y^1, Y^2, \ldots, Y^k)$. For G^n we write

$$Y^{\otimes n} = \left(\left(Y_1^1, \ldots, Y_1^k\right), \left(Y_2^1, \ldots, Y_2^k\right), \ldots, \left(Y_n^1, \ldots, Y_n^k\right)\right).$$

Note that each k-tuple Y_i is a deterministic function of X_i. Furthermore, we will write Y_i^{-t} to denote Y_i with the t-th coordinate Y_i^t omitted.

[4] This is mainly because the Raz/Holenstein framework, if extended to a multiplayer parallel repetition theorem in full generality, would likely also yield new lower bound techniques for multiparty communication complexity, an area that has long resisted progress (especially for the important multiparty direct sum/product problems).

[5] There are other ways to perform hardness amplification of classical multiplayer games, including transforming a k-player game G into an equivalent two-player projection game G' (where one player simulates the original k players, and the second player is used to consistently check the answers of the new "super-player"), and then applying Raz's parallel repetition theorem to G'. However, this k-to-2 transformation does not preserve quantum completeness, in general, which may be a useful feature. The anchoring transformation, on the other hand, preserves quantum completeness, and simultaneously supports both classical and quantum hardness parallel repetition.

For $i \in [n]$ let D_i be a subset of $[k]$ of size $k-1$ chosen uniformly at random, and $\overline{D}_i \in [k]$ its complement in $[k]$. Let $M_i = Y_i^{D_i}$ denote the coordinates of Y associated to indices in D_i. Define the *dependence-breaking random variable* Ω_i as

$$\Omega_i = \begin{cases} (D_i, M_i) & i \in \overline{C} \\ X_i & i \in C \end{cases}. \tag{14}$$

The importance of Ω is captured in the following lemma.

Lemma 6.2. *(Local Sampling) Let X, Z, Ω be as above. Then $\mathsf{P}_{X_{-i}|X_i\Omega_{-i}\mathrm{Z}}$ is a product distribution across the players:*

$$\mathsf{P}_{X_{-i}|X_i\Omega_{-i}\mathrm{Z}} = \prod_{t=1}^{k} \mathsf{P}_{X_{-i}^t|\Omega_{-i}^t \mathrm{Z}^t X_i^t}.$$

Proof. Conditioned on $M_i = Y_i^{D_i}$ each $X_i = (X_i^1, X_i^2, \ldots, X_i^k)$ is a product distribution, hence $\mathsf{P}_{X_{-i}|\Omega_{-i}X_i}$ is product. Since for $t \in [k]$ Z^t is a deterministic function of X^t the same holds of $\mathsf{P}_{X_{-i}|\Omega_{-i}\mathrm{Z}X_i}$. □

Lemma 6.2 crucially relies on the sets D_j being of size $k-1$: if two or more of the players' questions are unconstrained in a coordinate it is no longer necessarily true that $\mathsf{P}_{X_{-i}|\Omega_{-i}\mathrm{Z}X_i}$ is product across all players.

Let $W = W_C = \bigwedge_{i=1}^{C} W_i$ denote the event that the players' answers Z to questions in the coordinates indexed by C satisfy the predicate V. Let

$$\delta = \frac{|C| \log |\mathcal{A}| + \log \frac{1}{\Pr(W_C)}}{m}. \tag{15}$$

The following lemma and its corollary are direct consequences of analogous lemmas used in the analysis of repeated two-player games, as stated in e.g. [27, Lem. 5] and [27, Cor. 6]. They do not depend on the structure of the game, and only rely on W being an event defined only on (X_C, Z).

Lemma 6.3. *We have*

(i) $$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_iY_i\Omega_i|W} - \mathsf{P}_{X_iY_i\Omega_i}\| \leq \sqrt{\delta}.$$

(ii) $$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_iY_i\mathrm{Z}\Omega_{-i}|W} - \mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_i\mathrm{Z}\Omega_{-i}|W}\| \leq \sqrt{\delta}$$

(iii) $$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{Y_i\mathrm{Z}\Omega|W} - \mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{\mathrm{Z}\Omega|W}\| \leq \sqrt{\delta}.$$

Proof. Item (i) follows directly from [27, Lem. 5] by taking $U_i = X_iY_i\Omega_i$. For (ii) apply [27, Cor. 6] with $U_i = X_i$ and $T = (Y_1, Y_2, \ldots, Y_m, X_C)$ to get

$$\mathop{\mathbb{E}}_{i\in[m]} \|\mathsf{P}_{X_i\mathrm{Z}Y_{[m]}X_C|W} - \mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_i\mathrm{Z}Y_{[m]\setminus\{i\}}X_C|W}\| \leq \sqrt{\delta}, \tag{16}$$

which is stronger than (ii); (ii) follows by marginalizing $Y_i^{\overline{D}_i}$ in each term. Finally, the same corollary applied with $U_i = Y_i$ and $T = \Omega$ shows (iii). □

Corollary 6.4.

$$\mathop{\mathbb{E}}_{i\in[m]} \sum_{t=1}^{k} \|\mathsf{P}_{Y_i}\mathsf{P}_{\mathrm{Z}\Omega_{-i}|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{\mathrm{Z}\Omega_{-i}|WY_i^{-t}}\| \leq 3k \cdot \sqrt{\delta}.$$

Proof. We have $\mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega|W} = \mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{\Omega_i|W}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}$. Applying Lemma 4.1 with $\mathsf{Q}_F = \mathsf{P}_{\Omega_i|W}$, $\mathsf{S}_F = \mathsf{P}_{\Omega_i}$, and $\mathsf{R}_{G|F} = \mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}$, we see that

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in[m]}\|\mathsf{P}_{Y_i|\Omega_i}\mathsf{P}_{Z\Omega|W} - \mathsf{P}_{Y_i\Omega_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}\|\\ &= \mathop{\mathbb{E}}_{i\in[m]}\|\mathsf{P}_{\Omega_i|W} - \mathsf{P}_{\Omega_i}\| \le \sqrt{\delta},\end{aligned}$$

where the last inequality follows from Lemma 6.3, item (i). Combining the above with item (iii) of the same Lemma, we have

$$\mathop{\mathbb{E}}_{i\in[m]}\|\mathsf{P}_{Y_iZ\Omega|W} - \mathsf{P}_{Y_i\Omega_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}\| \le 2\sqrt{\delta}. \tag{17}$$

Noting that Ω_i is determined by Y_i (the D_i are completely independent of everything else), (17) implies

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in[m]}\mathop{\mathbb{E}}_{t\in[k]}\|\mathsf{P}_{Y_iZ\Omega_{-i}|W} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i^{-t}}\|\\ &= \mathop{\mathbb{E}}_{i\in[m]}\|\mathsf{P}_{Y_iZ\Omega_{-i}|W} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|W\Omega_i}\|\\ &\le 2\sqrt{\delta}.\end{aligned}$$

Finally, notice that Lemmas 4.1 and 6.3 imply $\mathbb{E}_{i\in[m]}\|\mathsf{P}_{Y_iZ\Omega_{-i}|W} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i}\| = \mathbb{E}_{i\in[m]}\|\mathsf{P}_{Y_i} - \mathsf{P}_{Y_i|W}\| \le \sqrt{\delta}$; the desired result follows. ◻

6.2 Proof of the Parallel Repetition Theorem

This section is devoted to the proof of Theorem 6.1. The main ingredient of the proof is given in the next proposition.

Proposition 6.5. *Let $C \subseteq [n]$ and X, Z, Ω_{-i} be defined as in Section 6.1. Then*

$$\mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| \le (6k\alpha^{-k}+1)\sqrt{\delta}, \tag{18}$$

where δ is defined in (15).

Theorem 6.1 follows from this proposition in a relatively standard fashion; this is done at the end of this section. Let us now prove Proposition 6.5 assuming a certain technical statement, Lemma 6.6. This lemma is proved immediately after.

Proof of Proposition 6.5. First observe that

$$\begin{aligned}&\left\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|\\ &= \left\|\mathsf{P}_{X_iY_i\Omega_{-i}Z|W} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|\end{aligned}$$

as Y_i is a deterministic function of X_i. Applying Lemma 6.3, item (ii) we get

$$\mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{X_iY_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_i\Omega_{-i}Z|W}\right\| \le \sqrt{\delta}.$$

The latter distribution can be written as $\mathsf{P}_{Y_i|W}\mathsf{P}_{X_i|Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i}$. Applying Lemma 4.1 with $\mathsf{Q}_F = \mathsf{P}_{Y_i|W}$ and $\mathsf{S}_F = \mathsf{P}_{Y_i}$ we see that

$$\left\|\mathsf{P}_{X_i|Y_i}\mathsf{P}_{Y_i\Omega_{-i}Z|W} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|WY_i}\right\| = \left\|\mathsf{P}_{Y_i|W} - \mathsf{P}_{Y_i}\right\|,$$

which is bounded by $\sqrt{\delta}$ on average over i by Lemma 6.3, item (i). Hence

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|\\ &\le 2\sqrt{\delta} + \mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|\\ &= 2\sqrt{\delta} + \mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|,\end{aligned}$$

where the equality follows from Lemma 4.1 applied with $\mathsf{R}_{G|F} = \mathsf{P}_{X_i|Y_i}$. Applying the triangle inequality,

$$\begin{aligned}&\mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{X_iY_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|\\ &= \mathop{\mathbb{E}}_{i\in[m]}\left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\|\\ &\le \mathop{\mathbb{E}}_{i\in[m]}\sum_{t=1}^{k}\left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{<t}=\perp^{t-1},Y_i^{\ge t}} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{\le t}=\perp^t,Y_i^{>t}}\right\| \qquad (19)\\ &\le 6k\alpha^{-k}\cdot\sqrt{\delta}, \qquad (20)\end{aligned}$$

where (19) is proved by Lemma 6.6 below and (20) follows from Corollary 6.4. ◻

Lemma 6.6. *Let $S \subset [k]$ and $t \in \overline{S}$. Then*

$$\begin{aligned}&\left\|\mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^S=\perp^S,Y_i^{\overline{S}}} - \mathsf{P}_{Y_i}\mathsf{P}_{\Omega_{-i}Z|WY_i^{S\cup\{t\}}=\perp^{S\cup\{t\}},Y_i^{\overline{S}\setminus\{t\}}}\right\|\\ &\le 2\alpha^{-(|S|+1)}\cdot\left\|\mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i} - \mathsf{P}_{Y_i}\mathsf{P}_{Z\Omega_{-i}|WY_i^{-t}}\right\|. \qquad (21)\end{aligned}$$

Proof. In the proof for ease of notation we omit the subscript i and write Y instead of Y_i. After relabeling we may assume $S = \{1, 2, \ldots, r-1\}$ and $t = r$ where $1 \le r < k$. Expanding the expectation over Y explicitly we can rewrite the left-hand side of (21) as

$$\left\|\mathsf{P}_Y\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{\ge r},y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{\le r}=\perp^r}\right)\right\|. \tag{22}$$

Next we use a symmetrization argument to bound the above expression. Consider a random variable $\hat{Y}$ that is a copy of Y, and is coupled to Y in the following way: $\hat{Y}^{-r} = Y^{-r}$, and conditioned on any setting of $Y^r = y^r$, $\hat{Y}^r$ and Y^r are independent. Using the fact that $\Pr[\hat{Y}^r = \perp] \ge \alpha$ conditioned on any value of $Y^{-r} = U^{-r} = y^{-r}$, we get that the expression in (22) is at most

$$\begin{aligned}&\alpha^{-1}\left\|\mathsf{P}_{Y^{-r}}\mathsf{P}_{Y^r|Y^{-r}}\mathsf{P}_{\hat{Y}^r|Y^{-r}}\cdot\right.\\ &\left.\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^r,y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},\hat{y}^r,y^{<r}=\perp^{r-1}}\right)\right\|.\end{aligned}$$

Using the triangle inequality and symmetry of Y and $\hat{Y}$, this expression can be bounded by

$$2\alpha^{-1}\cdot\left\|\mathsf{P}_Y\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^r,y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{<r}=\perp^{r-1}}\right)\right\|,$$

which after noting that the quantity $\|\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^r,y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{\le r}=\perp^r}\|$ is independent of the variable $Y^{<r}$, can be rewritten as

$$2\alpha^{-1}\cdot\left\|\mathsf{P}_{Y^{\ge r}}\cdot\left(\mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^r,y^{<r}=\perp^{r-1}} - \mathsf{P}_{\Omega_{-i}Z|W,y^{>r},y^{<r}=\perp^{r-1}}\right)\right\|.$$

Using that the event that $Y^{<r} = \perp^{r-1}$ occurs with probability at least α^{r-1} and $\mathsf{P}_{Y^{\ge r}|Y^{<r}=\perp^{r-1}} = \mathsf{P}_{Y^{\ge r}}$ by the anchor property, we

can finally bound (22) by

$$2\alpha^{-r} \cdot \|\mathsf{P}_Y \mathsf{P}_{Z\Omega_{-i}|WY} - \mathsf{P}_Y \mathsf{P}_{Z\Omega_{-i}|WY^{-r}}\|,$$

which is the desired result. □

We prove Theorem 6.1 by iteratively applying Proposition 6.5 as follows.

Proof of Theorem 6.1. Let $C_0 = \emptyset$ and $\delta_0 = 0$. While $(6k\alpha^{-k} + 1)\sqrt{\delta_s} \leq \varepsilon/2$, by Proposition 6.5, we can choose $i \in \overline{C}_s$ with $\left\|\mathsf{P}_{X_i\Omega_{-i}Z|W} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W,Y_i=\perp^k}\right\| \leq \varepsilon/2$. Set $C_{s+1} = C_s \cup \{i\}$ and $\delta_{s+1} = (|C_{s+1}|\log|\mathcal{A}| + \log 1/\Pr(W_{C_{s+1}}))/m$. First we show that throughout this process the bound

$$\Pr[W_{C_s}] \leq (1-\varepsilon/2)^{|C_s|} \tag{23}$$

holds. Since by the choice of i one has

$$\left\|\mathsf{P}_{X_i\Omega_{-i}Z|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}\right\| \leq \varepsilon/2,$$

to establish (23) it will suffice to show that

$$\Pr(W_i|W_C) \leq \mathrm{val}(G) + \left\|\mathsf{P}_{X_i\Omega_{-i}Z|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}\right\|. \tag{24}$$

The proof of (24) is based on a rounding argument. Consider the following strategy for G: First, the players use shared randomness to obtain a common sample from $\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}$. After receiving her question x_t^*, player $t \in [k]$ samples questions for the remaining coordinates according to $\mathsf{P}_{X_{-i}^t|\Omega_{-i}^t Z^t X_i^t}$, forming the tuple $X^t = (X_{-i}^t, x_t^*)$. She determines her answer $a_i^t \in \mathcal{A}_i^t$ according to the strategy for G^n. The distribution over questions X implemented by players following this strategy is

$$\mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C Y_i=\perp^k}\prod_{t=1}^{k}\mathsf{P}_{X_{-i}^t|\Omega_{-i}^t Z^t X_i^t},$$

which by Lemma 6.2 is equal to

$$\mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C Y_i=\perp^k}\mathsf{P}_{X_{-i}|\Omega_{-i}Z}.$$

On the other hand from the definition of Ω_{-i} we have

$$\mathsf{P}_{X\Omega_{-i}Z|W_C} = \mathsf{P}_{X_i\Omega_{-i}Z|W_C}\mathsf{P}_{X_{-i}|\Omega_{-i}ZW_C} = \mathsf{P}_{X_i\Omega_{-i}Z|W_C}\mathsf{P}_{X_{-i}|\Omega_{-i}Z}.$$

Applying Lemma 4.1 with $R = \mathsf{P}_{X_{-i}|\Omega_{-i}Z}$ it follows that

$$\left\|\mathsf{P}_{XZ\Omega_{-i}|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C Y_i=\perp^k}\mathsf{P}_{X_{-i}|\Omega_{-i}Z}\right\| = \left\|\mathsf{P}_{X_i\Omega_{-i}Z|W_C} - \mathsf{P}_{X_i}\mathsf{P}_{\Omega_{-i}Z|W_C,Y_i=\perp^k}\right\|.$$

Now by definition the winning probability of the extracted strategy for G is at most $\mathrm{val}(G)$, and (24) follows.

Let now C be the final set of coordinates when the above-described process stops; at this point we must have

$$\delta = \frac{|C|\log|\mathcal{A}| + \log\frac{1}{\Pr(W_C)}}{n-|C|} > \frac{\alpha^{2k}\varepsilon^2}{48\cdot k^2}.$$

If $|C| \geq n/2$ we are already done by (23). Suppose

$$\frac{|C|\log|\mathcal{A}| + \log(\frac{1}{\Pr[W_C]})}{n} > \frac{\alpha^{2k}\epsilon^2}{96\cdot k^2}.$$

If $\log(\frac{1}{\Pr(W_C)}) \geq \frac{n\cdot\alpha^{2k}\epsilon^2}{192\cdot k^2}$ we are again done; hence, we can assume

$$\frac{|C|\log|\mathcal{A}|}{n} > \frac{\alpha^{2k}\epsilon^2}{192\cdot k^2}.$$

Now plugging the lower bound on the size of C in (23) we get

$$\mathrm{val}(G^n) \leq \Pr(W_C) \leq \exp\left(-\frac{\alpha^{2k}\cdot\varepsilon^3\cdot n}{384\cdot k^2\cdot s}\right)$$

where $s = \log|\mathcal{A}|$, which completes the proof. □

7 OPEN PROBLEMS

Many interesting problems about the parallel repetition of multiplayer and entangled games remain open. Perhaps the most obvious and pressing is the problem of obtaining a complete extension of Raz's theorem for general entangled two-player games. For example, obtaining a fully quantum analogue of Raz's theorem, as was the case for Raz's theorem itself, is likely to have important implications in the setting of communication complexity. One promising candidate approach could be to leverage the recent ideas related to quantum information complexity [9, 46].

Similarly, the problem of obtaining a parallel repetition with exponential decay for *general multiplayer* games remain a fascinating challenge. In our view, however, this problem (even classically) seems more challenging than the two-player entangled case, as its difficulties are related to communication complexity and circuit complexity lower bounds.

One limitation of our result is that it is essentially most suitable in the case of games with value close to 1, in the sense that if $\mathrm{val}(G), \mathrm{val}^*(G)$ are already *subconstant*, our bounds do not take advantage of this fact. Indeed, even if G originally has a value close to 0, the anchoring operation itself pushes the value up to $\Omega(1)$. It remains open to find a hardness amplification result that replicates the strength of similar theorems obtained recently in the classical setting [8, 16].

ACKNOWLEDGMENTS.

We thank Mark Braverman and Ankit Garg for useful discussions. MB was supported by NSF under CCF-0939370 and CCF-1420956. TV was supported by NSF CAREER Grant CCF-1553477, AFOSR YIP award number FA9550-16-1-0495, and the IQIM, an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028). HY was supported by Simons Foundation grant #360893, and National Science Foundation Grants 1122374 and 1218547.

REFERENCES

[1] Scott Aaronson, Russell Impagliazzo, and Dana Moshkovitz. 2014. Am with multiple merlins. In *Computational Complexity (CCC), 2014 IEEE 29th Conference on.* IEEE, 44–55.
[2] Dorit Aharonov, Itai Arad, and Thomas Vidick. 2013. Guest column: the quantum PCP conjecture. *Acm sigact news* 44, 2 (2013), 47–79.
[3] Boaz Barak, Moritz Hardt, Ishay Haviv, Anup Rao, Oded Regev, and David Steurer. 2008. Rounding parallel repetitions of unique games. In *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on.* IEEE, 374–383.
[4] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. 2015. Anchoring games for parallel repetition. *arXiv preprint arXiv:1509.07466* (2015).
[5] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. 2016. Parallel repetition via fortification: analytic view and the quantum case. *arXiv preprint arXiv:1603.05349* (2016).
[6] John S Bell. 1964. On the Einstein-Podolsky-Rosen paradox. *Physics* 1, 3 (1964).
[7] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. 1988. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of Symposium on Theory of computing (STOC).*

[8] Mark Braverman and Ankit Garg. 2015. Small Value Parallel Repetition for General Games. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing (STOC).*

[9] Mark Braverman, Ankit Garg, Young Kun Ko, Jieming Mao, and Dave Touchette. 2015. Near-optimal bounds on bounded-round quantum communication complexity of disjointness. In *Proceedings of Foundations of Computer Science (FOCS)—to appear.*

[10] Mark Braverman, Anup Rao, Omri Weinstein, and Amir Yehudayoff. 2013. Direct products in communication complexity. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on.* IEEE, 746–755.

[11] André Chailloux and Giannicola Scarpa. 2014. Parallel Repetition of Entangled Games with Exponential Decay via the Superposed Information Cost. In *41st International Colloquium on Automata, Languages, and Programming - (ICALP).* 296–307.

[12] Kai-Min Chung, Xiaodi Wu, and Henry Yuen. 2015. Parallel Repetition for Entangled k-player Games via Fast Quantum Search. In *30th Conference on Computational Complexity.* 512.

[13] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. 1969. Proposed experiment to test local hidden-variable theories. *Physical Review Letters* 23, 15 (1969), 880–884.

[14] Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. 2008. Perfect parallel repetition theorem for quantum XOR proof systems. *Computational Complexity* 17, 2 (2008), 282–299.

[15] Irit Dinur, Prahladh Harsha, Rakesh Venkat, and Henry Yuen. 2016. Multiplayer parallel repetition for expander games. *arXiv preprint arXiv:1610.08349* (2016).

[16] Irit Dinur and David Steurer. 2014. Analytical approach to parallel repetition. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing.* ACM, 624–633.

[17] Irit Dinur, David Steurer, and Thomas Vidick. 2014. A Parallel Repetition Theorem for Entangled Projection Games. In *the 29th Conference on Computational Complexity, CCC.* 197–208.

[18] Uriel Feige. 1995. Error Reduction by Parallel Repetition: The State of the Art. *Technical Report CS95-32 of the Weizmann Institute* (1995).

[19] Uriel Feige and Joe Kilian. 2000. Two-Prover Protocols—Low Error at Affordable Rates. *SIAM J. Comput.* 30, 1 (2000), 324–346.

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

[21] Joseph Fitzsimons and Thomas Vidick. 2015. A multiprover interactive proof system for the local Hamiltonian problem. In *Proceedings of the Conference on Innovations in Theoretical Computer Science.* ACM, 103–112.

[22] Lance Fortnow, John Rompel, and Michael Sipser. 1988. On the power of multipower interactive protocols. In *Proceedings of Structure in Complexity Theory Conference (CCC).* 156–161.

[23] Iftach Haitner. 2009. A parallel repetition theorem for any interactive argument. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on.* IEEE, 241–250.

[24] Johan Håstad. 2001. Some optimal inapproximability results. *Journal of the ACM (JACM)* 48, 4 (2001).

[25] Johan Håstad, Rafael Pass, Douglas Wikström, and Krzysztof Pietrzak. 2010. An efficient parallel repetition theorem. In *Theory of Cryptography Conference.* Springer, 1–18.

[26] Jan Hazła, Thomas Holenstein, and Anup Rao. 2016. Forbidden Subgraph Bounds for Parallel Repetition and the Density Hales-Jewett Theorem. *arXiv preprint arXiv:1604.05757* (2016).

[27] Thomas Holenstein. 2009. Parallel Repetition: Simplification and the No-Signaling Case. 5, 1 (2009), 141–172. DOI: https://doi.org/10.4086/toc.2009.v005a008

[28] Rahul Jain, Attila Pereszlényi, and Penghui Yao. 2014. A Parallel Repetition Theorem for Entangled Two-Player One-Round Games under Product Distributions. In *the 29th Conference on Computational Complexity, CCC.*

[29] Zhengfeng Ji. 2015. Classical verification of quantum proofs. *arXiv preprint arXiv:1505.07432* (2015).

[30] Zhengfeng Ji. 2016. Compression of Quantum Multi-Prover Interactive Proofs. *arXiv preprint arXiv:1610.03133* (2016).

[31] Julia Kempe, Oded Regev, and Ben Toner. 2008. Unique games with entangled provers are easy. In *Proceedings of Foundations of Computer Science (FOCS).*

[32] Julia Kempe and Thomas Vidick. 2011. Parallel repetition of entangled games. In *Proceedings of the forty-third annual ACM symposium on Theory of computing (STOC).* 353–362.

[33] Alexei Yu Kitaev, Alexander Shen, and Mikhail N Vyalyi. 2002. *Classical and quantum computation.* Vol. 47. American Mathematical Society Providence.

[34] Dominic Mayers and Andrew Yao. 1998. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science.* IEEE, 503–509.

[35] Carl A Miller and Yaoyun Shi. 2013. Optimal Robust Self-Testing by Binary Nonlocal XOR Games. In *8th Conference on the Theory of Quantum Computation, Communication and Cryptography.* 254.

[36] Dana Moshkovitz. 2014. Parallel repetition from fortification. In *Foundations of Computer Science (FOCS), 2014 IEEE 55th Annual Symposium on.* IEEE, 414–423.

[37] Anand Natarajan and Thomas Vidick. 2015. Constant-Soundness Interactive Proofs for Local Hamiltonians. *arXiv preprint arXiv:1512.02090* (2015).

[38] Michael A Nielsen and Isaac L Chuang. 2010. *Quantum computation and quantum information.* Cambridge university press.

[39] Rafael Pass and Muthuramakrishnan Venkitasubramaniam. 2007. An efficient parallel repetition theorem for Arthur-Merlin games. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing.* ACM, 420–429.

[40] Anup Rao. 2011. Parallel repetition in projection games and a concentration bound. *SIAM J. Comput.* 40, 6 (2011), 1871–1891.

[41] Ran Raz. 1998. A parallel repetition theorem. *SIAM J. Comput.* 27, 3 (1998), 763–803.

[42] Ran Raz. 2010. Parallel Repetition of Two Prover Games (Invited Survey). In *2010 25th Annual IEEE Conference on Computational Complexity.* IEEE, 3–6.

[43] Ran Raz. 2011. A counterexample to strong parallel repetition. *SIAM J. Comput.* 40, 3 (2011), 771–777.

[44] Alexander A. Razborov. 1992. On the distributional complexity of disjointness. *Theoretical Computer Science* 106, 2 (1992), 385–390.

[45] Ben W Reichardt, Falk Unger, and Umesh Vazirani. 2013. Classical command of quantum systems. *Nature* 496, 7446 (2013), 456–460.

[46] Dave Touchette. 2014. Quantum information complexity and amortized communication. *arXiv preprint arXiv:1404.3733* (2014).

[47] Umesh Vazirani and Thomas Vidick. 2012. Certifiable quantum dice. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 370, 1971 (2012), 3432–3448.

[48] Umesh Vazirani and Thomas Vidick. 2014. Fully device-independent quantum key distribution. *Physical review letters* 113, 14 (2014), 140501.

[49] Vijay V Vazirani. 2013. *Approximation algorithms.* Springer Science & Business Media.

[50] Oleg Verbitsky. 1996. Towards the parallel repetition conjecture. *Theoretical Computer Science* 157, 2 (1996), 277–282.

[51] Thomas Vidick. 2013. Three-player entangled XOR games are NP-hard to approximate. In *Proceedings of the 54th Annual Symposium on Foundations of Computer Science.* IEEE, 766–775.

[52] Mark M Wilde. 2013. *Quantum information theory.* Cambridge University Press.

[53] Henry Yuen. 2016. A Parallel Repetition Theorem for All Entangled Games. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy.* 77:1–77:13.