A New Proof of Nonsignalling Multiprover Parallel Repetition Theorem

Himanshu Tyagi[†] Shun Watanabe[‡]

***Abstract*—We present an information theoretic proof of the nonsignalling multiprover parallel repetition theorem, a recent extension of its two-prover variant that underlies many hardness of approximation results. The original proofs used de Finetti type decomposition for strategies. We present a new proof that is based on a technique we introduced recently for proving strong converse results in multiuser information theory and entails a change of measure after replacing hard information constraints with soft ones.**

I. Introduction

The parallel repetition theorem is an important tool in theoretical computer science which is used to prove hardness of approximation results. It shows roughly that if distributed provers can satisfy a random predicate with probability $v < 1$ without coordinating, then they can satisfy n independent copies of the same predicate only with probability going to 0 exponentially in n. Such a theorem for the two-prover case was shown in [8], with a simplified proof given in [4]. The precise form of the statement of such a theorem relies on the structure of the query distribution, the predicate, and the class of strategies allowed for the provers. In particular, in some applications we only need a parallel repetition theorem for nonsignalling strategies, a class of correlation that subsumes even quantum correlations.

While the validity of a multiprover parallel repetition theorem for the standard setting is unclear, recently such a theorem has been proved for the nonsignalling setting [6] (see, also, [1], [2]). The proof uses de Finetti type decomposition of strategies and a linear programming interpretation of the value function. In this paper, we provide a new proof of the same result that is completely "information theoretic". Our proof draws on the connection between the parallel repetition setting and that of multiuser rate-distortion theory. In particular, we rely on a change of measure approach developed recently in [9] for proving strong converse results in multiuser information theory. In this approach, we first replace the hard information constraints involving conditional independence by their soft counterparts involving bounds on KL divergences. Next, we change measure to that obtained by conditioning on the "winning" event. The n-fold problem is related to a single instance of the problem using a tensorization property of the resulting value function.

[†]Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore 560012, India. Email: htyagi@ece.iisc.ernet.in.
[‡]Department of Computer and Information Sciences, Tokyo University of Agriculture and Technology, Tokyo 184-8588, Japan. Email: shunwata@cc.tuat.ac.jp.

This paper is part review – we recall the formulation and results for two provers in Section II, followed by those for the multiprover setting in Section III. Our main contribution is a new proof of the multiprover parallel repetition theorem (Theorem 4) given in Section IV. The final section contains brief concluding remarks.

Notation. Given random variable $(X_1, ..., X_m)$, for a subset $\mathcal{A}$ of $\{1, ..., m\}$, we abbreviate the random variable $(X_i, i \in \mathcal{A})$ as $X_{\mathcal{A}}$. Similarly, for a tupple $(x_1, ..., x_m)$, denote $x_{\mathcal{A}} = (x_i, i \in \mathcal{A})$. For other notations, we basically follow [3].

II. Two-Prover Parallel Repetition Theorem

We begin by reviewing the two-prover setting. A two-prover game G consists of a verifier and two-provers $\mathcal{P}_1$ and $\mathcal{P}_2$. The verifier samples a query (X_1, X_2) according to a fixed joint distribution $\mathrm{P}_{X_1X_2}$ on finite alphabet $\mathcal{X}_1 \times \mathcal{X}_2$, and sends X_1 and X_2 to $\mathcal{P}_1$ and $\mathcal{P}_2$, respectively. Upon receiving the queries, $\mathcal{P}_1$ and $\mathcal{P}_2$ send responses $U_1 \in \mathcal{U}_1$ and $U_2 \in \mathcal{U}_2$, respectively, where U_i depends only on X_i. They may use any mappings f_i, $i = 1, 2$, of X_i to get U_i; for finite sets $\mathcal{U}$ and $\mathcal{X}$, denote by $\mathcal{F}(\mathcal{U}|\mathcal{X})$ the set of all mappings from $f : \mathcal{X} \to \mathcal{U}$. The provers win the game if $\omega(X_1, X_2, U_1, U_2) = 1$ for a prespecified predicate $\omega : \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{U}_1 \times \mathcal{U}_2 \to \{0, 1\}$. We will represent the game G by the pair $(\mathrm{P}_{X_1X_2}, \omega)$. The goal of the provers is to choose mappings (f_1, f_2) that maximize the winning probability. This maximum winning probability is termed the *value of the game* and is given by

$$\rho(G) := \max \big\{ \mathbb{E}[\omega(X_1, Y_1, f_1(X_1), f_2(X_2))] : f_1 \in \mathcal{F}(\mathcal{U}_1|\mathcal{X}_1), f_2 \in \mathcal{F}(\mathcal{U}_2|\mathcal{X}_2) \big\}.$$

In n parallel repetitions of the game, the verifier samples sequences of queries X_1^n and X_2^n according to the product distribution $\mathrm{P}^n_{X_1X_2}$. The provers now respond with sequences $U_1^n \in \mathcal{U}_1^n$ and $U_2^n \in \mathcal{U}_2^n$ where U_i^n depends only on X_i^n, $i = 1, 2$. They win the game if predicates for each coordinate are satisfied, namely the predicate $\omega^{\wedge n}$ for the parallel repetition game $G^{\wedge n}$ is given by

$$\omega^{\wedge n}(x_1^n, x_2^n, u_1^n, u_2^n) := \bigwedge_{j=1}^{n} \omega(x_{1j}, x_{2j}, u_{1j}, u_{2j}),$$

where $\bigwedge$ denotes the AND function. The value of $G^{\wedge n}$ is defined similarly as follows:

$$\rho(G^{\wedge n}) := \max \big\{ \mathbb{E}[\omega^{\wedge n}(X_1^n, X_2^n, f_1(X_1^n), f_2(X_2^n))] : f_1 \in \mathcal{F}(\mathcal{U}_1^n|\mathcal{X}_1^n), f_2 \in \mathcal{F}(\mathcal{U}_2^n|\mathcal{X}_2^n) \big\}.$$

As a simple attempt towards winning the parallel repetition game, provers may simply apply strategies for single instance of the game across each coordinate. In fact, they may use a different strategy for each coordinate. Clearly, any such attempt will have value less than $\rho(G)^n$. But can they do better by using other functions f_i that take into account the entire vector X_i^n and do not have a product structure across coordinates? At a high level, a parallel repetition theorem says that the answer is no: The exponential decay of value with n is unavoidable.

The first instance of parallel repetition theorem was shown by Raz [8] (see [4] for simpler proof).

Theorem 1 ([8])**.** *There exists a function $C : [0,1] \to [0,1]$ satisfying $C(t) < 1$ if $t < 1$ such that for any game G,*

$$\rho(G^{\wedge n}) \leq C(\rho(G))^{-\frac{n}{\log|\mathcal{U}_1||\mathcal{U}_2|}}.$$

The statement above holds for any game G with the same universal function $C(\cdot)$ and universal exponent that depends only on the cardinality of the response set $\mathcal{U}_1 \times \mathcal{U}_2$.

An important aspect of the setting above, which will be a prime focus here, is the role of randomness in response strategies. A simple derandomization argument shows that the value of games will not change if the pair (f_1, f_2) is generated randomly using shared randomness V that is independent of the query. Such strategies with shared randomness available to the provers can be described by channels

$$\begin{aligned} &\mathrm{P}_{U_1U_2|X_1X_2}(u_1, u_2|x_1, x_2) \\ &\quad = \sum_{\substack{f_1 \in \mathcal{F}(\mathcal{U}_1|\mathcal{X}_1) \\ f_2 \in \mathcal{F}(\mathcal{U}_2|\mathcal{X}_2)}} \mu(f_1, f_2)\delta_{f_1,f_2}(u_1, u_2|x_1, x_2) \end{aligned} \tag{1}$$

where μ is a distribution on $\mathcal{F}(\mathcal{U}_1|\mathcal{X}_1) \times \mathcal{F}(U_2|\mathcal{X}_2)$ and δ_{f_1,f_2} given by $\delta_{f_1,f_2}(u_1, u_2|x_1, x_2) := \mathbb{1}_{\{u_1=f_1(x_1), u_2=f_2(x_2)\}}$ is the deterministic strategy induced by functions f_1, f_2.

In physics, strategies of the form (1) are said to satisfy the *hidden variable theory*, a classical physics principle which says that if all the hidden variables are revealed then the state of the world will be deterministic. We denote the set of all such strategies by $\mathcal{P}_{\mathtt{HVT}} = \mathcal{P}_{\mathtt{HVT}}(\mathcal{U}_1 \times \mathcal{U}_2|\mathcal{X}_1 \times \mathcal{X}_2)$. With this new notation at our disposal and using the observation above that shared randomness does not improve the value of a game, we can express $\rho(G)$ alternatively as

$$\rho(G) = \max_{\mathrm{P}_{U_1U_2|X_1X_2} \in \mathcal{P}_{\mathtt{HVT}}} \mathbb{E}[\omega(X_1, X_2, U_1, U_2)].$$

Note that since strategies using shared randomness can perform at best as deterministic strategies, the same must be true for strategies using independent private randomness at the provers. Thus, yet another alternative form of $\rho(G)$ is given by

$$\begin{aligned} \rho(G) = \max \{&\mathbb{E}[\omega(X_1, X_2, U_1, U_2)] : \\ &\mathrm{P}_{U_1U_2|X_1X_2} \text{ s.t. } U_1 -\!\!\circ\!\!- X_1 -\!\!\circ\!\!- X_2 -\!\!\circ\!\!- U_2\}, \end{aligned} \tag{2}$$

namely we can consider maximization over Markov chains $U_1 -\!\!\circ\!\!- X_1 -\!\!\circ\!\!- X_2 -\!\!\circ\!\!- U_2$ with marginal of (X_1, X_2) fixed to $\mathrm{P}_{X_1X_2}$.

It is important to examine the limitation posed by restricting to strategies in $\mathcal{P}_{\mathtt{HVT}}$. In fact, a contentious debate in physics revolving around statistical modeling of quantum measurements was finally settled in the second half of the previous century through quantitative distinction between correlations allowed in hidden variable theory and more general *nonsignalling* correlation.

For our setting, we can define the class of *nonsignaling strategies* as follows.

Definition 1 (Nonsignalling strategies)**.** Let $\mathcal{P}_{\mathtt{NS}} = \mathcal{P}_{\mathtt{NS}}(\mathcal{U}_1 \times \mathcal{U}_2|\mathcal{X}_1 \times \mathcal{X}_2)$ be the set of all strategies $\mathrm{P}_{U_1U_2|X_1X_2}$ satisfying

$$\begin{aligned} \mathrm{P}_{U_1|X_1X_2}(u_1|x_1, x_2) &= \mathrm{P}_{U_1|X_1X_2}(u_1|x_1, x_2'), \\ \mathrm{P}_{U_2|X_1X_2}(u_2|x_1, x_2) &= \mathrm{P}_{U_2|X_1X_2}(u_2|x_1', x_2) \end{aligned} \tag{3}$$

for every $x_1 \neq x_1'$ and $x_2 \neq x_2'$. Equivalently, we can express these conditions as $I(U_1 \wedge X_2|X_1) = I(U_2 \wedge X_1|X_2) = 0$, namely the Markov relations $U_1 -\!\!\circ\!\!- X_1 -\!\!\circ\!\!- X_2$ and $U_2 -\!\!\circ\!\!- X_2 -\!\!\circ\!\!- X_1$ hold.

Note that these strategies include as a special case the "long Markov strategies" satisfying $U_1 -\!\!\circ\!\!- X_1 -\!\!\circ\!\!- X_2 -\!\!\circ\!\!- U_2$. This latter class performs as well as $\mathcal{P}_{\mathtt{HVT}}$. In fact, it is easy to verify that strategies in $\mathcal{P}_{\mathtt{HVT}}$ satisfy (3), which yields

$$\mathcal{P}_{\mathtt{HVT}} \subset \mathcal{P}_{\mathtt{NS}}. \tag{4}$$

In typical applications of parallel repetition theorem in complexity theory, it suffices to use a version of the theorem for nonsignalling strategies. In any case, the next question is of independent interest: Does parallel repetition theorem hold if we allow the broader class of nonsignalling strategies?

Specifically, denote by $\rho_{\mathtt{NS}}(G)$ the maximum probability of satisfying ω using nonsignalling strategies, i.e.,

$$\rho_{\mathtt{NS}}(G) := \max_{\mathrm{P}_{U_1U_2|X_1X_2} \in \mathcal{P}_{\mathtt{NS}}} \mathbb{E}[\omega(X_1, X_2, U_1, U_2)].$$

By (4), $\rho(G) \leq \rho_{\mathtt{NS}}(G)$. In fact, the inequality can be strict for some games (see [10, Example 1]).

Holenstein proved that the following version of parallel repetition theorem for nonsignaling strategies.

Theorem 2 ([4])**.** *There exists a function $C : [0,1] \to [0,1]$ satisfying $C(t) < 1$ if $t < 1$ such that for any game G,*

$$\rho_{\mathtt{NS}}(G^{\wedge n}) \leq C(\rho_{\mathtt{NS}}(G))^{-n}.$$

Note that now the exponent of parallel repetition theorem doesn't even depend on the cardinality of response set. Also, we remark that the proof of Theorem 2 in [4] is much simpler than the simplified proof of Theorem 1 in the same paper.

III. Multiprover Parallel Repetition Theorem

Moving to the multiprover setting, a multiprover game $G = (\mathrm{P}_{X_{\mathcal{M}}}, \omega)$ consists of a verifier and m provers $\mathcal{P}_1, \ldots, \mathcal{P}_m$. Denoting $\mathcal{M} = \{1, ..., m\}$ and $X_{\mathcal{M}} = (X_1, \ldots, X_m)$, the verifier samples a query $X_{\mathcal{M}}$ according to a fixed joint distribution $\mathrm{P}_{X_{\mathcal{M}}}$ and sends X_i to $\mathcal{P}_i$ for i in $\mathcal{M}$. Upon receiving the queries, each prover $\mathcal{P}_i$ sends a response $U_i \in \mathcal{U}_i$, $1 \leq i \leq m$, to the verifier. The provers win the game if $\omega(X_{\mathcal{M}}, U_{\mathcal{M}}) = 1$ for a given predicate $\omega : \mathcal{X}_{\mathcal{M}} \times \mathcal{U}_{\mathcal{M}} \to \{0,1\}$.

As in the previous section, the provers' strategy can be described by a channel $\mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}}$. The set of all strategies that can be described as convex combination of deterministic, local strategies is denoted by $\mathcal{P}_{\mathtt{HVT}} = \mathcal{P}_{\mathtt{HVT}}(\mathcal{U}_{\mathcal{M}}|\mathcal{X}_{\mathcal{M}})$ (cf. (1)). The value of the game that can be attained by strategies satisfying hidden variable theory is given by

$$\rho(G) = \max_{\mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}} \in \mathcal{P}_{\mathtt{HVT}}} \mathbb{E}[\omega(X_{\mathcal{M}}, U_{\mathcal{M}})].$$

The parallel repetition game $G^{\wedge n}$ is defined analogously to the two-player setting.

For the multi-prover setting, a nonsignaling strategy is a channel $\mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}}$ such that the following condition is satisfied:

$$\mathrm{P}_{U_{\mathcal{A}}|X_{\mathcal{M}}}(u_{\mathcal{A}}|x_{\mathcal{A}}, x_{\mathcal{A}^c}) = \mathrm{P}_{U_{\mathcal{A}}|X_{\mathcal{M}}}(u_{\mathcal{A}}|x_{\mathcal{A}}, x'_{\mathcal{A}^c}),$$

for all $x_{\mathcal{A}}, x_{\mathcal{A}^c}, x'_{\mathcal{A}^c}, u_{\mathcal{A}}$ and all subsets $\mathcal{A}$ of $\mathcal{M}$. Denoting the set of all nonsignaling strategies by $\mathcal{P}_{\mathtt{NS}} = \mathcal{P}_{\mathtt{NS}}(\mathcal{U}_{\mathcal{M}}|\mathcal{X}_{\mathcal{M}})$, the value of the game that can be attained by nonsignaling strategies is given by

$$\rho_{\mathtt{NS}}(G) = \max_{\mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}} \in \mathcal{P}_{\mathtt{NS}}} \mathbb{E}[\omega(X_{\mathcal{M}}, U_{\mathcal{M}})].$$

A general parallel repetition theorem for strategies in $\mathcal{P}_{\mathtt{HVT}}$ is not known. As we have mentioned at the end of the previous section, proving parallel repetition theorem for strategies in $\mathcal{P}_{\mathtt{NS}}$ is relatively easier than that for strategies in $\mathcal{P}_{\mathtt{HVT}}$; the former is known to hold under the condition that query distribution $\mathrm{P}_{X_{\mathcal{M}}}$ has full support [1], [2]. Remarkably, without the full support condition, a counterexample appeared in [5] for a parallel repetion theorem for $\mathcal{P}_{\mathtt{NS}}$. The counterexample rules out a parallel repetition theorem for $\mathcal{P}_{\mathtt{NS}}$ in general. In other words, $\rho_{\mathtt{NS}}(G) < 1$ is not sufficient to claim the exponential decay of winning probability in parallel repetition games. In fact, even preceding this counterexample, a parallel repetition theorem, i.e., exponential decay, was shown to hold if the value of the single game for a broader class of strategies, called *sub-nonsignalling* strategies, is strictly less than 1 [6].

Sub-nonsignaling strategies $\mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}}$, which we define next, need not be conditional distributions and are only required to be subnormalized, namely we only need them to be nonnegative and satisfying $\sum_{u_{\mathcal{M}}} \mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}}(u_{\mathcal{M}}|x_{\mathcal{M}}) \leq 1$. Both total variation distances and KL divergence can be applied to such subnormalized distribution. We remark that the marginal P_Y and the conditional distribution $\mathrm{P}_{Y|X}$, respectively, for a subnormalized distribution P_{XY} are defined as $\mathrm{P}_Y(y) = \sum_x \mathrm{P}_{XY}(x,y)$ and $\mathrm{P}_{Y|X}(y|x) = \mathrm{P}_{XY}(x,y)/\mathrm{P}_X(x)$. While P_Y, too, is a subnormalized distribution, $\mathrm{P}_{Y|X}$ will be a (normalized) distribution.

Definition 2 (Sub-nonsignalling strategies)**.** The set $\mathcal{P}_{\mathtt{SNS}}$ of sub-nonsignalling strategies consists of subnormalized $\mathrm{P}_{U_{\mathcal{M}}|X_{\mathcal{M}}}$ such that, for each subsets $\mathcal{A}$ of $\mathcal{M}$, there exists a channel $\mathrm{Q}_{U_{\mathcal{A}}|X_{\mathcal{A}}}$ satisfying:

$$\mathrm{P}_{U_{\mathcal{A}}|X_{\mathcal{M}}}(u_{\mathcal{A}}|x_{\mathcal{A}}, x_{\mathcal{A}^c}) \leq \mathrm{Q}_{U_{\mathcal{A}}|X_{\mathcal{A}}}(u_{\mathcal{A}}|x_{\mathcal{A}}), \qquad (5)$$

for all $x_{\mathcal{A}}, x_{\mathcal{A}^c}, u_{\mathcal{A}}$.

Note that nonsignalling strategies are those for which the inequality condition above is replaced with identity. Heuristically, sub-nonsignalling strategies may be regarded as the class of strategies close to nonsignalling strategies in statistical distance. Another heuristic was suggested in [6] which interpreted sub-nonsignalling strategies as nonsignalling strategies with additional $x_{\mathcal{M}}$ dependent power to randomly abstain from responding. In fact, we can find a sub-nonsignalling strategy close to a distribution for which all conditional distributions $\mathrm{P}_{U_{\mathcal{A}}|X_{\mathcal{M}}}$ are close to some conditional distributions $\mathrm{Q}_{U_{\mathcal{A}}|X_{\mathcal{A}}}$.[1]

Lemma 3 ([6, Lemma 5.2])**.** *Let $\mathrm{P}_{X_{\mathcal{M}}}$ be a query distribution on $\mathcal{X}_{\mathcal{M}}$, and let $\mathrm{P}_{\tilde{U}_{\mathcal{M}}\tilde{X}_{\mathcal{M}}}$ be a probability distribution on $\mathcal{U}_{\mathcal{M}} \times \mathcal{X}_{\mathcal{M}}$. Suppose that for each $\mathcal{A} \subsetneq \mathcal{M}$ there exists a conditional distribution $\mathrm{Q}_{U_{\mathcal{A}}|X_{\mathcal{A}}}$ such that*

$$d_{\mathtt{var}}(\mathrm{P}_{\tilde{U}_{\mathcal{A}}\tilde{X}_{\mathcal{M}}}, \mathrm{P}_{X_{\mathcal{M}}}\mathrm{Q}_{U_{\mathcal{A}}|X_{\mathcal{A}}}) \leq \varepsilon_{\mathcal{A}}.$$

Then, there exists a sub-nonsignaling $\mathrm{P}'_{U_{\mathcal{M}}|X_{\mathcal{M}}}$ such that

$$d_{\mathtt{var}}(\mathrm{P}_{\tilde{U}_{\mathcal{M}}\tilde{X}_{\mathcal{M}}}, \mathrm{P}_{X_{\mathcal{M}}}\mathrm{P}'_{U_{\mathcal{M}}|X_{\mathcal{M}}}) \leq \varepsilon_{\emptyset} + 2 \sum_{\emptyset \neq \mathcal{A} \subsetneq \mathcal{M}} \varepsilon_{\mathcal{A}}.$$

By definition, the value of the game that is attained by sub-nonsignaling strategies satisfy $\rho_{\mathtt{SNS}}(G) \geq \rho_{\mathtt{NS}}(G)$. For two-prover games, $\rho_{\mathtt{SNS}}(G)$ was shown in [6] to coincide with $\rho_{\mathtt{NS}}(G)$. However, equality may not hold for multiprover games, in general. Interestingly, when the query distribution $\mathrm{P}_{X_{\mathcal{M}}}$ has full support, there exists a constant $\Gamma = \Gamma(\mathrm{P}_{X_{\mathcal{M}}})$ such that, for $\varepsilon > 0$, $(cf.$ [6])

$$\rho_{\mathtt{NS}}(G) < 1 - \varepsilon \Longrightarrow \rho_{\mathtt{SNS}}(G) < 1 - \frac{\varepsilon}{\Gamma}. \qquad (6)$$

Before we state the parallel repetition theorem for sub-nonsignalling strategies, we switch to a slightly more general formulation where in the n parallel repeptiton game, instead of winning all the games, we are interested in quantifying the probability that the provers win more than a fraction Δ of the game. This formulation is closer to the rate-distortion theory formulation of information theory and appeared, for instance, in [7]. Specifically, for $0 < \Delta \leq 1$, consider

$$\rho_{\mathtt{SNS}}(G^n, \Delta) := \max\left\{ \Pr\left(N_\omega(X^n_{\mathcal{M}}, U^n_{\mathcal{M}}) \geq n\Delta\right) : \mathrm{P}_{U^n_{\mathcal{M}}|X^n_{\mathcal{M}}} \in \mathcal{P}_{\mathtt{SNS}}(\mathcal{U}^n_{\mathcal{M}}|\mathcal{X}^n_{\mathcal{M}})\right\}, \qquad (7)$$

where $N_\omega(x^n_{\mathcal{M}}, u^n_{\mathcal{M}}) := \sum_{j=1}^n \omega(x_{\mathcal{M},j}, u_{\mathcal{M},j})$. Since $\omega(x_{\mathcal{M},j}, u_{\mathcal{M},j})$ is the indicator for a win in the jth coordinate, $N_\omega(x^n_{\mathcal{M}}, u^n_{\mathcal{M}})$ denotes the total number of wins. Analogously, $\mathcal{P}_{\mathtt{NS}}$ is defined by restricting the maximum in (7) to nonsignalling strategies; our original definition $\rho_{\mathtt{NS}}(G^{\wedge n})$ coincides with $\rho_{\mathtt{NS}}(G^n, 1)$.

[1]Lemma 3 is a multiprover extension of [4, Lemma 9.5] which showed that in the two-prover setting we can find a nonsignalling $\mathrm{P}'_{U_{\mathcal{M}}|X_{\mathcal{M}}}$.

We now recall the multiprover parallel repetition theorem from [6].

Theorem 4. *Let $G = (\mathrm{P}_{X_{\mathcal{M}}}, \omega)$ be a multiprover game with $\rho_{\mathtt{SNS}}(G) < 1$. For any $\Delta \geq \rho_{\mathtt{SNS}}(G) + \nu$ with $0 < \nu \leq 1 - \rho_{\mathtt{SNS}}(G)$, we have*

$$\rho_{\mathtt{SNS}}(G^n, \Delta) \leq \exp\left(- n\frac{\nu^2}{C_m}\right),$$

where the constant $C_m = \mathcal{O}(2^{2m})$ depends only on $m = |\mathcal{M}|$.

For multiprover games with full support query distributions, Theorem 4 together with (6) implies the parallel repetition theorem for nonsignaling strategies, shown first in [2].

The proof of the multiprover parallel repetition theorem for nonsignaling strategies and full support query distribution in [2] entails extending the proof approach for the two-prover setting in [4]. An alternative proof was provided in [1] by using a technique based on de Finetti theorem. At a high level, this technique allows us to restrict attention to convex combinations of product strategies. In [6], the parallel repetition theorem for sub-nonsignaling strategies, namely Theorem 4, was proved by using another variant of de Finetti theorem.

In the next section, we provide an alternative proof of Theorem 4. Our proof is based on a technique recently developed by the authors in [9] to prove strong converse theorems for multi-user information theory problems. A crucial observation is that the parallel repetition theorem can be regarded as an exponential strong converse of a multi-user rate-distortion problem with no communication. In contrast to the proof in [6] that uses a structural decomposition of strategies, our proof is completely "information theoretic".

IV. A New Proof of Theorem 4

Our proof looks at the expected number of wins instead of the probability of winning. For a given multiprover game $G = (\mathrm{P}_{X_{\mathcal{M}}}, \omega)$ and $\delta \geq 0$, define

$$\eta_{\mathtt{NS}}(G, \delta) := \max\big\{\mathbb{E}[\omega(\tilde{X}_{\mathcal{M}}, \tilde{U}_{\mathcal{M}})] : \\ I(\tilde{U}_{\mathcal{A}} \wedge \tilde{X}_{\mathcal{A}^c}|\tilde{X}_{\mathcal{A}}) + D(\mathrm{P}_{\tilde{X}_{\mathcal{M}}}\|\mathrm{P}_{X_{\mathcal{M}}}) \leq \delta, \forall \mathcal{A} \subsetneq \mathcal{M}.\big\}$$

Note that the maximum is over the set of distributions, which we call *δ-approximate nonsignaling distributions*, that satisfy the information structure only approximately. In particular, we have replaced the hard information constraints required by nonsignalling strategies by their soft counterparts expressed by bounds on KL diveregence. Below we shall see two properties of $\eta_{\mathtt{NS}}(G, \delta)$: it tensorizes and can be bounded above roughly by $\rho_{\mathtt{SNS}}(G)$. We note that a linear programming based notion of approximate nonsignaling strategies was used in [4], [2], [1], [6]. Our divergence based notion of approximation is amenable to tensorization and facilitates an information theoretic proof.

Under the changed measure obtained by conditioning on $\mathcal{C}$, the expected number of wins is more than $n\Delta$. Also, this new measure satisfies the soft information constraint bound with δ equal to the exponent of probability of $\mathcal{C}$. Thus, $\eta_{\mathtt{NS}}(G^n, \delta)$ must be more than $n\Delta$. Using the properties of $\eta_{\mathtt{NS}}(G^n, \delta)$ mentioned earlier, we can bound it above roughly by $n\rho_{\mathtt{SNS}}(G)$, which shows that Δ must be roughly bounded above by $\rho_{\mathtt{SNS}}(G)$. The required bound for exponent is obtained by the contrapositive statement.

Formal arguments follow. We begin with the tensorization property.

Lemma 5. *For a given multiprover game $G = (\mathrm{P}_{X_{\mathcal{M}}}, \omega)$, $n \in \mathbb{N}$ and $\delta \geq 0$, we have*

$$\eta_{\mathtt{NS}}(G^n, n\delta) = n \cdot \eta_{\mathtt{NS}}(G, \delta).$$

Proof. The inequality $\eta_{\mathtt{NS}}(G^n, n\delta) \geq n\eta_{\mathtt{NS}}(G, \delta)$ holds by definition. For the other direction, fix a $n\delta$-approximate nonsignalling distribution $\mathrm{P}_{\tilde{U}^n_{\mathcal{M}}\tilde{X}^n_{\mathcal{M}}}$. We have

$$\begin{aligned}\mathbb{E}[N_\omega(\tilde{X}_{\mathcal{M}}, \tilde{U}_{\mathcal{M}})] &= \sum_{j=1}^n \mathbb{E}[\omega(\tilde{X}_{\mathcal{M},j}, \tilde{U}_{\mathcal{M},j})] \\ &= n\mathbb{E}[\omega(\tilde{X}_{\mathcal{M},J}, \tilde{U}_{\mathcal{M},J})], \end{aligned} \quad (8)$$

where J is distributed uniformly on $\{1, \ldots, n\}$. Furthermore,

$$\begin{aligned} n\delta &\geq I(\tilde{U}^n_{\mathcal{A}} \wedge \tilde{X}^n_{\mathcal{A}^c}|\tilde{X}^n_{\mathcal{A}}) + D(\mathrm{P}_{\tilde{X}^n_{\mathcal{M}}}\|\mathrm{P}_{X^n_{\mathcal{M}}}) \\ &\geq n\big[H(\tilde{X}_{\mathcal{A}^c,J}|\tilde{X}_{\mathcal{A},J}) + D(\mathrm{P}_{\tilde{X}_{\mathcal{M},J}}\|\mathrm{P}_{X_{\mathcal{M}}})\big] \\ &\quad - \sum_{j=1}^n H(\tilde{X}_{\mathcal{A}^c,j}|\tilde{X}^n_{\mathcal{A}}, \tilde{U}^n_{\mathcal{A}}) \\ &\geq n\big[H(\tilde{X}_{\mathcal{A}^c,J}|\tilde{X}_{\mathcal{A},J}) + D(\mathrm{P}_{\tilde{X}_{\mathcal{M},J}}\|\mathrm{P}_{X_{\mathcal{M}}})\big] \\ &\quad - \sum_{j=1}^n H(\tilde{X}_{\mathcal{A}^c,j}|\tilde{X}_{\mathcal{A},j}, \tilde{U}_{\mathcal{A},j}) \\ &= n\big[H(\tilde{X}_{\mathcal{A}^c,J}|\tilde{X}_{\mathcal{A},J}) + D(\mathrm{P}_{\tilde{X}_{\mathcal{M},J}}\|\mathrm{P}_{X_{\mathcal{M}}})\big] \\ &\quad - nH(\tilde{X}_{\mathcal{A}^c,J}|\tilde{X}_{\mathcal{A},J}, \tilde{U}_{\mathcal{A},J}, J) \\ &\geq n\big[I(\tilde{U}_{\mathcal{A},J} \wedge \tilde{X}_{\mathcal{A}^c,J}|\tilde{X}_{\mathcal{A},J}) + D(\mathrm{P}_{\tilde{X}_{\mathcal{M},J}}\|\mathrm{P}_{X_{\mathcal{M}}})\big], \end{aligned}$$

where the first inequality follows from [9, Proposition 1] and the second and the third inequalities hold since conditioning decreases entropy. Thus, $\mathrm{P}_{\tilde{U}_{\mathcal{M},J},\tilde{X}_{\mathcal{M},J}}$ is a δ-approximate nonsignalling distribution and the claim follows by (8). ☐

Next, we relate $\eta_{\mathtt{NS}}(G, \delta)$ and $\rho_{\mathtt{SNS}}(G)$ using Lemma 3.

Lemma 6. *For a given multiprover game $G = (\mathrm{P}_{X_{\mathcal{M}}}, \omega)$ and $\delta \geq 0$, we have*

$$\eta_{\mathtt{NS}}(G, \delta) \leq \rho_{\mathtt{SNS}}(G) + C'_m\sqrt{(2\ln 2)\delta},$$

where the constant $C'_m = \mathcal{O}(2^m)$ depends only on $m = |\mathcal{M}|$.

Proof. Consider a δ-approximate nonsignalling distribution $\mathrm{P}_{\tilde{U}_{\mathcal{M}}\tilde{X}_{\mathcal{M}}}$. For any $\mathcal{A} \subsetneq \mathcal{M}$, since $I(\tilde{U}_{\mathcal{A}} \wedge \tilde{X}_{\mathcal{A}^c}|\tilde{X}_{\mathcal{A}}) = D(\mathrm{P}_{\tilde{U}_{\mathcal{A}}\tilde{X}_{\mathcal{M}}}\|\mathrm{P}_{\tilde{X}_{\mathcal{M}}}\mathrm{P}_{\tilde{U}_{\mathcal{A}}|\tilde{X}_{\mathcal{A}}}) \leq \delta$ and $D(\mathrm{P}_{\tilde{X}_{\mathcal{M}}}\|\mathrm{P}_{X_{\mathcal{M}}}) \leq \delta$, by using Pinsker's inequality [3] and the triangle inequality, we get

$$d_{\mathtt{var}}(\mathrm{P}_{\tilde{U}_{\mathcal{A}}\tilde{X}_{\mathcal{M}}}, \mathrm{P}_{X_{\mathcal{M}}}\mathrm{P}_{\tilde{U}_{\mathcal{A}}|\tilde{X}_{\mathcal{A}}}) \leq \sqrt{(2\ln 2)\delta}.$$

Next, by applying Lemma 3 with $\varepsilon_{\mathcal{A}} = \sqrt{(2\ln 2)\delta}$, there exists a sub-nonsignaling strategy $\mathrm{P}'_{U_\mathcal{M}|X_\mathcal{M}}$ such that

$$d_{\mathtt{var}}(\mathrm{P}_{\tilde{U}_\mathcal{M}\tilde{X}_\mathcal{M}}, \mathrm{P}_{X_\mathcal{M}}\mathrm{P}'_{U_\mathcal{M}|X_\mathcal{M}}) \le (2^{|\mathcal{M}|+1}-3)\sqrt{(2\ln 2)\delta}.$$

Finally, since ω is bounded by 1, we have

$$\begin{aligned}&\mathbb{E}_{\mathrm{P}_{\tilde{X}_\mathcal{M}\tilde{U}_\mathcal{M}}}[\omega(X_\mathcal{M}, U_\mathcal{M})]\\ &\le \mathbb{E}_{\mathrm{P}_{X_\mathcal{M}}\mathrm{P}'_{\tilde{U}_\mathcal{M}|\tilde{X}_\mathcal{M}}}[\omega(X_\mathcal{M}, U_\mathcal{M})]\\ &\qquad + 2d_{\mathtt{var}}(\mathrm{P}_{\tilde{U}_\mathcal{M}\tilde{X}_\mathcal{M}}, \mathrm{P}_{X_\mathcal{M}}\mathrm{P}'_{U_\mathcal{M}|X_\mathcal{M}})\\ &\le \rho_{\mathtt{SNS}}(G) + 2(2^{|\mathcal{M}|+1}-3)\sqrt{(2\ln 2)\delta},\end{aligned}$$

where the final inequality uses the fact that $\mathrm{P}'_{\tilde{U}_\mathcal{M}|\tilde{X}_\mathcal{M}}$ is sub-nonsignalling. We obtain the claimed bound with $C'_m = 2(2^{m+1}-3)$ since $\mathrm{P}_{\tilde{U}_\mathcal{M}\tilde{X}_\mathcal{M}}$ was an arbitrary δ-approximate nonsignalling distribution. □

We have all the tools for the proof of Theorem 4 in place.

Proof of Theorem 4: If $\rho_{\mathtt{SNS}}(G^n, \Delta) > \exp(-n\delta)$, we can find a sub-nonsignalling strategy $\mathrm{P}_{U^n_\mathcal{M}|X^n_\mathcal{M}}$ such that $\mathbb{P}\left(N_\omega(U_\mathcal{M}, X^n_\mathcal{M}) \ge n\Delta\right) > \exp(-n\delta)$ for some $\delta > 0$. Denoting

$$\mathcal{C} = \left\{(u^n_\mathcal{M}, x^n_\mathcal{M}) : N_\omega(x^n_\mathcal{M}, u^n_\mathcal{M}) \ge n\Delta\right\},$$

we change the measure by conditioning on the event $(U^n_\mathcal{M}, X^n_\mathcal{M}) \in \mathcal{C}$ as follows:[2]

$$\mathrm{P}_{\tilde{U}^n_\mathcal{M}\tilde{X}^n_\mathcal{M}}(u^n_\mathcal{M}, x^n_\mathcal{M}) = \frac{\mathrm{P}_{U^n_\mathcal{M}X^n_\mathcal{M}}(u^n_\mathcal{M}, x^n_\mathcal{M})\mathbf{1}[(u^n_\mathcal{M}, x^n_\mathcal{M}) \in \mathcal{C})]}{\mathrm{P}_{U^n_\mathcal{M}X^n_\mathcal{M}}(\mathcal{C})}.$$

Then, by a simple calculation, we have

$$D(\mathrm{P}_{\tilde{U}^n_\mathcal{M}\tilde{X}^n_\mathcal{M}} \| \mathrm{P}_{U^n_\mathcal{M}X^n_\mathcal{M}}) = \log\frac{1}{\mathrm{P}_{U^n_\mathcal{M}X^n_\mathcal{M}}(\mathcal{C})} \le n\delta.$$

Furthermore, for each $\mathcal{A} \subsetneq \mathcal{M}$, denoting by $\mathrm{Q}_{U^n_\mathcal{A}|X^n_\mathcal{A}}$ the dominating conditional distribution for the sub-nonsignaling strategy $\mathrm{P}_{U^n_\mathcal{A}|X^n_\mathcal{A}}$ (cf. (5)), we have

$$\begin{aligned}&I(\tilde{U}^n_\mathcal{A} \wedge \tilde{X}^n_{\mathcal{A}^c}|\tilde{X}^n_\mathcal{A}) + D(\mathrm{P}_{\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{X^n_\mathcal{M}})\\ &\le I(\tilde{U}^n_\mathcal{A} \wedge \tilde{X}^n_{\mathcal{A}^c}|\tilde{X}^n_\mathcal{A}) + D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}|\tilde{X}^n_\mathcal{A}}\|\mathrm{Q}_{U^n_\mathcal{A}|X^n_\mathcal{A}}|\mathrm{P}_{\tilde{X}^n_\mathcal{A}})\\ &\quad + D(\mathrm{P}_{\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{X^n_\mathcal{M}})\\ &= D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}|\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{\tilde{U}^n_\mathcal{A}|\tilde{X}^n_\mathcal{A}}|\mathrm{P}_{\tilde{X}^n_\mathcal{M}}) + D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}|\tilde{X}^n_\mathcal{A}}\|\mathrm{Q}_{U^n_\mathcal{A}|X^n_\mathcal{A}}|\mathrm{P}_{\tilde{X}^n_\mathcal{M}})\\ &\quad + D(\mathrm{P}_{\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{X^n_\mathcal{M}})\\ &= D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}|\tilde{X}^n_\mathcal{M}}\|\mathrm{Q}_{U^n_\mathcal{A}|X^n_\mathcal{A}}|\mathrm{P}_{\tilde{X}^n_\mathcal{M}}) + D(\mathrm{P}_{\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{X^n_\mathcal{M}})\\ &\le D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}|\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{U^n_\mathcal{A}|X^n_\mathcal{M}}|\mathrm{P}_{\tilde{X}^n_\mathcal{M}}) + D(\mathrm{P}_{\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{X^n_\mathcal{M}})\\ &= D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{U^n_\mathcal{A}X^n_\mathcal{M}})\\ &\le D(\mathrm{P}_{\tilde{U}^n_\mathcal{A}\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{U^n_\mathcal{A}X^n_\mathcal{M}})\\ &\quad + D(\mathrm{P}_{\tilde{U}^n_{\mathcal{A}^c}|\tilde{U}^n_\mathcal{A}\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{U^n_{\mathcal{A}^c}|U^n_\mathcal{A}X^n_\mathcal{M}}|\mathrm{P}_{\tilde{U}^n_\mathcal{A}\tilde{X}^n_\mathcal{M}})\\ &= D(\mathrm{P}_{\tilde{U}^n_\mathcal{M}\tilde{X}^n_\mathcal{M}}\|\mathrm{P}_{U^n_\mathcal{M}X^n_\mathcal{M}})\\ &\le n\delta,\end{aligned}$$

[2]Although $\mathrm{P}_{U_\mathcal{M}X_\mathcal{M}}$ is only a subnormalized distribution, the changed measure $\mathrm{P}_{\tilde{U}_\mathcal{M}\tilde{X}_\mathcal{M}}$ is a distribution.

where the second inequality follows from the sub-nonsignaling condition (5) and the third inequality uses the fact that $\mathrm{P}_{U^n_{\mathcal{A}^c}|U^n_\mathcal{A}X^n_\mathcal{M}}$ is a conditional distribution. The above bound implies that the changed measure $\mathrm{P}_{\tilde{U}^n_\mathcal{M}\tilde{X}^n_\mathcal{M}}$ is δ-approximate nonsignalig distribution. Furthermore, since $N_\omega(\tilde{X}_\mathcal{M}, \tilde{U}^n_\mathcal{M}) \ge n\Delta$ holds with probability 1 under the changed measure $\mathrm{P}_{\tilde{U}^n_\mathcal{M}\tilde{X}^n_\mathcal{M}}$, we have

$$n\Delta \le \mathbb{E}[N_\omega(\tilde{U}^n_\mathcal{M}, \tilde{X}^n_\mathcal{M})] \le \eta_{\mathtt{NS}}(G^n, n\delta),$$

which together with Lemma 5 and Lemma 6 implies

$$\Delta \le \eta_{\mathtt{NS}}(G, \delta) \le \rho_{\mathtt{SNS}}(G) + C'_m\sqrt{(2\ln 2)\delta}.$$

By considering contraposition, if

$$\Delta > \rho_{\mathtt{SNS}}(G) + C'_m\sqrt{(2\ln 2)\delta}, \tag{9}$$

then we have $\rho_{\mathtt{SNS}}(G^n, \Delta) \le \exp(-n\delta)$. Thus, by setting $\delta = \frac{\nu^2}{(2\ln 2)(C'_m+1)^2}$, $\Delta \ge \rho_{\mathtt{SNS}}(G) + \nu$ implies (9), and we have the claim of the theorem. □

V. Discussion

A multiprover parallel repetition theorem for standard strategies, i.e., strategies satisfying the hidden variable theory, is not available. In fact, our initial attempt in this work was to provide an alternative proof of the two-prover parallel repetition theorem for the standard strategies. We tried to prove a counterpart of the tensorization property, Lemma 5, for standard strategies. However, our preliminary attempt failed, mainly because it was difficult to identify a suitable soft constraint for the long Markov chain in (2). Nonetheless, we do believe that our measure change approach can be used to obtain a parallel repetition theorem for standard strategies, perhaps by proving an approximate tensorization property of the value function with suitable soft constraints.

References

[1] R. Arnon-Friedman, R. Renner, and T. Vidick, "Non-signaling parallel repetition using de Finetti reductions," *IEEE Trans. Inf. Theory*, vol. 62, no. 3, pp. 1440–1457, November 2016.

[2] H. Buhrman, S. Fehr, and C. Schaffner, "On the parallel repetition of multi-player games: The no-signaling case," in *Leibniz International Proceedings in Informatics*, 2014, pp. 24–35.

[3] I. Csiszár and J. Körner, *Information theory: Coding theorems for discrete memoryless channels. 2nd edition*. Cambridge University Press, 2011.

[4] T. Holenstein, "Parallel repetition: Simplifications and the no-signaling case," *Theory of Computing*, vol. 5, pp. 141–172, 2009.

[5] J. Homgren and L. Yang, "(A counterexample to) Parallel repetition for non-signaling multi-player games," 2018, http://people.csail.mit.edu/holmgren/papers/ns-parrep.pdf.

[6] C. Lancien and A. Winter, "Parallel repetition and concentration for (sub-)no-signalling games via a flexible constrained de Finetti reduction." *Chicago J. Theor. Comput. Sci.*, no. 11, pp. 1–22, 2016.

[7] A. Rao, "Parallel repetition in projection games and a concentration bound," *SIAM J. Comput.*, vol. 40, no. 6, pp. 1871–1891, 2011.

[8] R. Raz, "A parallel repetition theorem," *SIAM J. Comput.*, vol. 27, no. 3, pp. 763–803, 1998.

[9] H. Tyagi and S. Watanabe, "Strong converse using change of measure arguments," *arXiv:1805.04625*, 2018.

[10] ——, "A new proof of nonsignaling multiprover parallel repetition theorem," *arXiv*, 2019.