# Quantum Course Project-Local Games: Entanglement vs Communication

Yuval Efron, Hugh Goatcher

December 5, 2020

## 1 Introduction

The goal of this project is to explore the connections and trade-offs between entanglement and communication in various games. Specifically, the project surveys the state of art of parallel repetition of games in both the absence and presence of quantum entanglement. Additionally, this project begins to explore the power of allowing limited classical communication between Alice and Bob in parallel repetitions of games and how strategies involving classical communication relate to strategies without.

Concrete examples of questions concerning this topic which were explored (and ones we hope to explore) in both the entangled regime and the classical regime include:

1. Given $n$ instances of the CHSH game, can Alice and Bob beat[1] the trivial strategy of playing all $n$ games separately.
2. For the cases that the answer to the former question is no, is there a perfect parallel repetition theorem for some family of games in the discussed model?
3. How much do a classical Alice and Bob need to communicate in order to close the gap between the classical and the entangled case. How much communication is required in order to get their probability to win all games up to 1? The latter question is also interesting in the entangled case.
4. Can we come up with a game whose parallel repetition version benefits from allowing communication more than expected?

We will be talking about games in this paper. A game is played with multiple players and a referee. The players collectively come up with a strategy, and then are split apart and prevented from communicating. According to a distribution known beforehand to the players, the referee then sends questions to each player, and the players each respond with an answer. They then either win or lose according to some function of their questions and answers.

These games have historical significance in their use for showing the non-local properties of our universe. Bell [Bel64] proved that behaviour expected from our current theory of quantum mechanics and the idea that events in one location cannot be affected by simultaneous actions in a far off location are mutually inconsistent. Clauser, Horne, Shimony, and Holt [CHSH69] then used ideas from the work of Bell to come up with an experiment (or game) that could be used to verify these non-local properties. This game is widely known as the CHSH game. In this game there are two players who each get independent and uniformly randomly chosen bits as questions, they answer with a bit each, and they win if the XOR of their answers equals the AND of their questions. What makes this game particularly interesting is that if we assume our universe has no non-local effects (like those we would expect from quantum entanglement) then we can show that Alice and Bob cannot win this game with greater than 75% probability. On the other hand if we allow them to share quantum entanglement they can win with up to $\frac{2+\sqrt{2}}{4} \approx 85\%$ probability, as shown by Cirel'son [Cir80]. In fact, this game has been used to give evidence of the quantum nature of our world by running this experiment with quantum entanglement and succeeding consistently with higher than 75% probability. Another interesting property of the CHSH game as a non-local game is that it is a rigid game.

[1] In terms of the probability to win all games

What this means is that there is effectively only one optimal quantum strategy, and furthermore any strategy that attains near optimal success is, in some sense, close to this optimal strategy [MYS12]. Therefore if you are a referee for two computers playing the CHSH game and they are winning with near optimal success probability, then with high probability you know nearly exactly what they are doing beneath the hood.

This concept of using rigidity of games to verify the behaviour of the players can actually be used to verify that a quantum computer is performing any particular quantum computation. By forcing two isolated quantum computers to share entanglement and randomly switch between playing rigid games with quantum value 1 and reporting the state of the quantum computation, you can know with high probability that they accurately report the state of the computation and so know that they are performing it as instructed [Gri20].

One of the rigid games used in such applications is the $n$-fold parallel repetition of the Magic Square Game. The $n$-fold parallel repetition of a game is when the players play $n$ instances of the game simultaneously and win if they win all instances of the game. Trivially, the players can just play each of the games independently and if they could win a single version of the game with probability $p$, then they win the $n$-fold parallel repetition with probability $p^n$. It turns out that depending on the game and whether or not quantum strategies are used, players can sometimes outperform this trivial strategy. How much better they can perform though is a non-trivial question. Verbitsky [Ver94] showed that for a broad class of two-player games with subperfect classical winning strategies, the classical value tends to 0 as the number of repetitions tends to $\infty$. This was improved by Raz [Raz95] who showed that the value decays exponentially with the number of repetitions. An interesting result in the quantum setting has been shown by Cleve, Slofstra, Unger, and Upadhyay [CSUU07] for two-player XOR games, which are games for which the two players each return a bit, and whether they win or lose depends only on the questions they received and the XOR of their responses. They showed that for a set of two-player XOR games $G_1, ..., G_n$ (potentially different) that the probability of the players winning all of them played in parallel is equal to the product of the probabilities of them winning each game individually. For example, an optimal quantum strategy for the $n$-fold parallel repetition of the CHSH game would just be to repeat the quantum strategy for the CHSH game $n$ times.

# 2 Motivation

The CHSH game is the classic witness for the correctness of Bell's Theorem [Bel64]. In general, non-local games with 2 players have proved to be useful in several areas such as quantum mechanics, randomness expansion and hardness of approximation [Hås01, DS14a]. In the following subsections, we elaborate on some of these applications, and discuss how they relate to non-local games.

## 2.1 Infinite randomness expansion

The first application of non local games is the ability to use verification of quantum computation in order to *expand* random bits using untrusted quantum computers. While if we have a trusted quantum computer we could easily get random bits by measuring $|+\rangle$ states in the standard basis, if the quantum computer is not trusted (maybe we don't even know if it is quantum) it may do any computation it desires and output potentially bits with very low entropy. Therefore having a way to ensure quantum computers are doing what you have asked them to do would help obtain random bits from untrusted quantum computers.

Before we mentioned that if a classical observer sees two quantum computers (or "provers") that are unable to communicate with each other but are succeeding at the CHSH game with near 85% probability, then they know that with high probability they are executing near the optimal quantum protocol for the CHSH game. This allows a classical player interacting with untrusted provers to test that they are producing randomness by repeatedly playing the CHSH game with them, as an optimal quantum strategy for CHSH produces at least one uniformly random bit.

It turns out though that the amount of randomness one can get from untrusted provers without reusing the output bits is much greater than the amount of randomness required as input from the classical player. This phenomena raises the notion of *randomness expansion*, in which a classical player could potentially use a small random seed and some number of untrusted quantum computers in order to play multiple CHSH games, forcing them to output more randomness than the initial seed contained. It has been shown by Vazirani and Vidick [VV11] that if we restrict the algorithms to a certain class of protocols, in which the trusted players questions to the provers do not depend on the provers' previous answers (such a protocol is called an *un-adaptive* protocol), then we can still get exponential expansion ($O(\log n)$ bits to $n$ bits), but we

cannot do better than a doubly exponential blowup in terms of randomness expansion (turning $m$ random bits to $2^{2^{O(m)}}$ close to random bits), shown by Coudron, Vidick, and Yuen [CVY13]. Later, Coudron and Yuen [CY14] presented an *adaptive* protocol (allowed to reuse output bits) involving 8 untrusted provers that allows one to expand $m$ random bits to $N$ exponentially (in $m$) close to uniform bits, where $N$ can be arbitrarily large.

### 2.2 Hardness of approximation

Dinur and Steurer [DS14b] show that for a particular class of games called *projection games*, the classical value of the $k$-fold parallel repetition of the projection game $G$ with classical value $\leq \rho$ is bounded above by

$$\left(\frac{2\sqrt{\rho}}{1+\rho}\right)^{k/2}.$$

This bound on the value of a class of games has as corollary that for every constant $c$, it is NP-hard to decide if the value of an instance of LABEL COVER of size $n$ has value 1 or at most $\frac{1}{(\log n)^c}$. In turn, they used this result for LABEL COVER to show that it is NP-hard to approximate instances of SET COVER of size $n$ to within $(1-\alpha)\ln n$.

## 3 Better communication protocols imply better quantum repetition theorems

In this section we elaborate on a particular result of Chung, Wu and Yuen [CWY14] that connects communication complexity to non-local games. For this, we need to a more precise and formal familiarity with non-local games.

### 3.1 Preliminaries

#### 3.1.1 2-player games

We start with a formal definition of 2-player games with a classical input and output. A 2-player game is a tuple $G = (\mathcal{X} \times \mathcal{Y}, \mathcal{A} \times \mathcal{B}, \mu, V)$, where:

1. $\mathcal{X}, \mathcal{Y}$ are finite alphabets. These are the *questions* spaces.
2. $\mathcal{A}, \mathcal{B}$ are finite alphabets. These are the *answer* spaces.
3. $\mu$ is a distribution over $\mathcal{X} \times \mathcal{Y}$.
4. $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$ is the verification predicate.

In a 2-player game, a referee samples $x = (x, y)$ from $\mu$ and sends $x$ to Alice and $y$ to Bob. The players (Alice and Bob) respectively produce answers $a, b$, and the referee accepts (and $A$ and $B$ win the game) if $V(x, y, a, b) = 1$. We say that a game is *free* if $\mu$ is a product distribution, i.e. the marginal distributions on $\mathcal{X}$ and $\mathcal{Y}$ are independent.

A quantum strategy for $G$ is a shared state $|\xi\rangle$, and two sets of measurements $\{M_{A,x} : x \in X\}$, $\{M_{B,y} : y \in Y\}$. On input $x$, Alice measures her part of $|\xi\rangle$ with $M_{A,x}$, gets an outcome $a$, and sends it to the referee. Similarly, Bob obtains an outcome $b$, and sends it to the referee. The entangled value, $val^*(G)$, of a game $G$ is defined as the supremum probability of the referee accepting over all possible finite dimensional quantum strategies for 2 players. The classical value of a game, $val(G)$, is similarly defined for classical strategies in which the players don't communicate and don't share any entanglement. The $n$-fold repetition of a game $G$ is denoted by $G^{\otimes n} = (\mathcal{X}^n \times \mathcal{Y}^n, \mathcal{A}^n \times \mathcal{B}^n, \mu^{\otimes n}, V^n)$, where $\mu^{\otimes n}$ is the product distribution over $n$ independent copies of $\mathcal{X} \times \mathcal{Y}$, and $V^n = \prod_{i=1}^{n} V(x_i, y_i, a_i, b_i)$.

## 3.2 The result

Specifically, in this section we give an overview of the tools and techniques employed in order to prove the following result of Chung, Wu, and Yuen, proved in [CWY14].

**Theorem 3.1.** *Let $G$ be a 2-player free game with entangled value $1-\epsilon$, then for $n = \Omega(s\log(1/\epsilon)/\epsilon^{3/2})$,*

$$val^*(G^{\otimes n}) \leq (1-\epsilon^{3/2})^{\Omega(n/s)}$$

*Here, $s$ is the answer length of the players.*

This theorem is proven using the reduction approach, i.e. showing that a high winning probability for the repeated game implies a "too good" strategy for a single instance of the game, arriving at a contradiction. Specifically, the proof of the above theorem goes roughly as follows.

1. Assume that a "too good" quantum strategy $\mathcal{S}$ exists for the repeated game. The proof converts such a strategy into an *advice-based strategy* for the single instance of the game $G$, which wins with high probability. An advice-based strategy for the game $G$ constitutes a collection of states $\{\phi_{xy}\}$ for each possible pair of questions $x, y$. An advice-based strategy differs for a regular quantum strategy mainly in the shared state between $A$ and $B$. In a regular quantum strategy, the state shared by $A$ and $B$ is independent of their inputs, where as in an advice-based strategy, the state shared between $A$ and $B$ may depend on their respective inputs $x, y$. Such a strategy is clearly not a valid quantum strategy. This intermediate step is useful however due to the following reason.

2. The proof then shows that by using the fact that $\mathcal{S}$ has a very high winning probability, one can *round* the advice-based strategy into a true game strategy. Concretely, $A$ and $B$ can respectively apply local operations $U_x, V_y$ to some *input-independent* state $\phi$ in order to *approximate* $\phi_{xy}$, and then simulate the advice-based strategy, with some error.

One needs to pick the advice-based strategy $\{\phi_{xy}\}$ with great care, as it is very much not clear how could one approximate a given ideal advice-based strategy to a valid quantum strategy. Precisely here is where the link to communication complexity is established. Previous work [CS14, CS15] was able to overcome this obstacle by designing an advice-based strategy $\{\phi_{x,y}\}$ with the following properties:

1. The strategy wins the game $G$ with high probability.

2. There is a *low communication protocol* between $A$ and $B$ that produces $\phi_{xy}$ on respective inputs $x, y$.

The low communication property turns out to be crucial for $A$'s and $B$'s ability to approximate the advice-based strategy using a true quantum strategy. This work established the notion that efficient communication protocols can lead to smaller rounding error of advice-based strategies, and in turn lead to better quantum parallel quantum repetition theorems. However, there is a caveat to the work of [CS14, CS15], the analysis of their proof focuses on simple one-way communication protocols, and doesn't capture advice-based strategies that can be produced by a bi-directional quantum low communication protocol. The work of [CWY14] proves precisely that connection, that advice-based strategies that can be produced by low quantum communication protocols can be approximated by a true quantum strategy with small error.

In order to demonstrate the fact that arbitrary ideal advice-based strategies cannot be approximated by quantum strategies, we describe here a naive attempt for constructing an advice-based strategy, and then we give a high level overview of the construction of [CWY14].

### 3.2.1 A naive attempt

We begin by describing a naive candidate for an advice-based strategy for the game $G$. Prior to that, we again go over important notation. Let $G$ be a two player free game and let $(x, y)$ be an input sampled from $\mu_X \otimes \mu_Y$. Denote by $V$ the verification predicate of $G$, by $\mathcal{S}$ an optimal strategy for $G^{\otimes n}$, in which $A$ and $B$ share the state $|\xi\rangle$, and given their respective inputs, perform the local measurements $M^{\mathbf{x}}, N^{\mathbf{y}}$, where here $\mathbf{x} = (x_1, ..., x_n), \mathbf{y} = (y_1, ..., y_n)$ are the input vectors of Alice and Bob. Similarly, denote by $\mathbf{a}, \mathbf{b}$ the answer vectors of $A, B$, respectively. Denote by $|\xi_{\mathbf{xyab}}\rangle$ the unnormalized post measurement state shared between $A$ and $B$ on inputs $\mathbf{x}, \mathbf{y}$ and answers $\mathbf{a}, \mathbf{b}$. Below, $\alpha$ is a normalizing constant. $\mu^{\otimes n}$ is the input distribution

for $G^{\otimes n}$, and $V(\mathbf{x},\mathbf{y},\mathbf{ab}) = \prod_i V(x_i, y_i, a_i.b_i)$. Assume for the sake of contradiction that $val^*(G^{\otimes n}) > 2^{-\gamma n}$, for some small $\gamma$.

Consider the state:

$$|\theta\rangle = \frac{1}{\sqrt{\alpha}} \sum_{\mathbf{x},\mathbf{y}} \sqrt{\mu^{\otimes n}(\mathbf{x},\mathbf{y})} |\mathbf{x}\rangle \otimes |\mathbf{y}\rangle \otimes \sum_{\mathbf{a},\mathbf{b}: V(\mathbf{x},\mathbf{y},\mathbf{a},\mathbf{b})=1} |\xi_{\mathbf{xyab}}\rangle \otimes |\mathbf{a}\rangle \otimes |\mathbf{b}\rangle$$

The above state describes the superposition on all possible post execution of $\mathcal{S}$ configurations of the system (Alice's and Bob's inputs, outputs, and shared state) conditioned on the assumption that they won the game.

Now consider the following advice-based strategy $\mathcal{T}$ for $G$ (a single instance!) that employs $|\theta\rangle$:

1. Alice and Bob share $|\theta\rangle$, with Alice holding $|\mathbf{x}\rangle$, $|\mathbf{a}\rangle$, and her half of $|\xi_{\mathbf{xyab}}\rangle$, with Bob holding the rest of the qubits.

2. On input $(x, y)$ sampled from $\mu$, some fixed coordinate $i \in [n]$ is chosen, and then they both measure the $i$-th qubit of their shared state $|\theta\rangle$. This measurement produces answers $x'$ and $y'$, and assume that $x' = x, y' = y$. Now we define $|\theta_{xy}\rangle$ to be exactly the resulting state after the above measurement when the measurement outputs were $x$ and $y$. But now, by construction of $|\theta\rangle$, measuring the $i$-th qubit of the state $|\theta_{xy}\rangle$ is guaranteed to output $a, b$ such that $V(x, y, a, b) = 1$.

Thus, ideally, the advice-based strategy defined by $\{|\theta_{xy}\rangle\}$ is an ideal strategy. However, this strategy cannot be rounded to a quantum strategy with small error. For this reason, a more delicate advice strategy is required, in this case, one which stems from an efficient communication protocol for Grover search.

### 3.2.2 Advice-based strategy from a low communication protocol

We next describe a quantum communication protocol that constructs an advice-based strategy $|\phi_{xy}\rangle$ which can be rounded with small error to be a valid quantum strategy.

First, consider the state:

$$|\psi\rangle = \sum_{\mathbf{x},\mathbf{y}} \sqrt{\mu^{\otimes n}(\mathbf{x},\mathbf{y})} |\mathbf{x}\rangle \otimes |\mathbf{y}\rangle \otimes \sum_{\mathbf{a},\mathbf{b}} |\xi_{\mathbf{xyab}}\rangle \otimes |\mathbf{a}\rangle \otimes |\mathbf{b}\rangle$$

It is important to note that since we are going over all possible inputs and outputs, this state can be produced with no communication at all. Again here, Alice holds $|\mathbf{x}\rangle$ and $|\mathbf{a}\rangle$ and her half of $|\xi_{\mathbf{xyab}}\rangle$. Bob holds the rest of the qubits. Now comes in the communication protocol. The input for this protocol would be $\mathbf{x}, \mathbf{a}$ for Alice, and $\mathbf{y}, \mathbf{b}$ for Bob. Their goal is find out whether they have won the game for the given questions and answers. In other words, their goal is to look for the existence of a coordinate $i \in [n]$ such that $V(\mathbf{x}_i, \mathbf{y}_i, \mathbf{a}_i, \mathbf{b}_i) = 0$, i.e., a losing coordinate. Thus their goal is to solve a search problem on the strings they received. Solving this problem with classical communication requires $\Omega(n)$ bits of communication. A quantum communication protocol however can employ Grover search in order to solve this search problem with $\tilde{O}(\sqrt{n})$ communication.

This protocol is performed on the states $|\mathbf{x}\rangle, |\mathbf{y}\rangle, |\mathbf{a}\rangle, |\mathbf{b}\rangle$. One can assume without loss of generality that Alice simulates the query protocol of Grover search. Denote the state shared by Alice and Bob at the end of performing the protocol by $|\psi^*\rangle$. Furthermore, denote by $|\phi\rangle$ the shared stated between Alice and Bob assuming Alice found no losing coordinate, i.e. with high probability (since Grover search is correct with high probability), Alice and Bob win the game on their respective questions and answers. It can be shown that if the Grover search performed correctly and didn't commit an error, then we would have that $|\phi\rangle = |\theta\rangle$, which is exactly the ideal state we discussed before, from which we saw how to produce an ideal advice-based strategy. However, since Grover search doesn't always succeed, it doesn't hold that $|\phi\rangle = |\theta\rangle$. However, one can make sure that Grover search errors with an exponentially small probability, which makes sure that $|\phi\rangle$ is a very good approximation of $|\theta\rangle$. All that is left to do is to thus treat $|\phi\rangle$ as if it were $|\theta\rangle$ and construct an advice-based strategy from it in the same manner as in the naive approach.

The rest of the proof involves showing that the above advice-based strategy can be rounded to be a valid quantum strategy for $G$, while introducing a small amount of error. Then, showing that the resulting quantum strategy for $G$ has too high of a winning probability, thus arriving at a contradiction. For a full proof of this result, see [CWY14].

# 4 Local games in the presence of communication

In this section we discuss potential research avenues regarding the relationship between non-local games, quantum entanglement, and communication. We define a new model of non-local games, in which the two players, Alice and Bob, receive $n$ instances of some game $G$, and are tasked with winning all games. The difference from a regular repeated game is that we now allow Alice and Bob to engage in a short conversation (of say $k$ bits) regarding their input questions before answering. We consider what kind of benefits this could provide. For example if $G$ is the CHSH game, can this communication help them perform better than the naive strategy of communicating the input bit for $k$ games, and so effectively cancelling (winning with probability 1) $k$ games out the $n$, and playing the rest $n-k$ games with an optimal non-communication strategy? This addition of communication can be introduced to both the classical setting, and the quantum setting, in which Alice and Bob are allowed to share entanglement. To the best of our knowledge, such a model hasn't been studied previously.

## 4.1 Model definition

For simplicity, we discuss here mostly the classical model of non-local games, in which players don't posses shared entangled states. See the beginning of section 3.1 for a formal definition of a non-local game, and the definition of a repeated non-local game. We now define what is a *bounded communication strategy* for a repeated game $G^{\otimes n}$. A bounded communication strategy of length $k$ is defined by a deterministic communication protocol $\Pi$ of at most $k$ bits between Alice and Bob. On input vectors $\mathbf{x}, \mathbf{y}$ respectively, Alice and Bob perform $\Pi(\mathbf{x}, \mathbf{y})$, and then output answer vectors $\mathbf{a}, \mathbf{b}$, respectively, based on their input vectors and the information each of them learned from the execution of $\Pi$. We call $n$ parallel instances of a game $G$ an $n$-repeated game.

## 4.2 Observations

We started with asking the simple question of what can be done with a single bit of communication? Using a computer program that brute forces over all possible strategies, we came to the conclusion that, e.g., for the CHSH game, adding a single bit of communication from Alice to Bob to a 2-repeated game of CHSH offers no advantage over playing a single instance of CHSH. Next, we considered the game defined by Feige in [Fei91], in which on respective inputs $(x, y)$ which are independent random bits, Alice and Bob are required to both output $(1, X)$ or both output $(2, Y)$, i.e. they must decide to guess the input of Alice, or the input of Bob. Clearly, they can win this game with probability 0.5, by always choosing to guess, e.g., Alice's input, and one can observe that they can not win with higher probability, since one of the players is required to guess a uniformly random bit.

Now consider the 2-repeated version of this game, denote the inputs by $(x_1, x_2)$ and $(y_1, y_2)$, and consider the following strategy: On the first game Alice and Bob respectively output $(1, x_1), (1, y_2)$, and on the second game they respectively output $(2, x_1), (2, y_2)$. Clearly, the game is won if $x_1 = y_2$, which occurs with probability half. Thus this game demonstrates a strange phenomena, in which the value of the 2-repeated game is equal to the value of a single instance of the game. We thought that this unique property of the game would make it a good candidate for exhibiting an advantage over a single instance of the game when we allow Alice to send a single bit to Bob in the 2-repeated game. However, it turns out that this is not case, i.e., allowing Alice to send one bit of information about her inputs to Bob in the 2-repeated case doesn't increase the value of the game above 0.5.

The property shared by both the game described above, and the CHSH game, is that for both for each output of Alice, there is at most a single answer Bob can give to win the game. Furthermore, the CHSH game has the property of being a *unique game*, a formal definition follows.

**Definition 4.1.** *Given a non-local game $G = (\mathcal{X} \times \mathcal{Y}, \mathcal{A} \times \mathcal{B}, \mu, V)$, we say that $G$ is* unique *if on any given pair of respective inputs $(x, y)$ the following holds: For all $a \in \mathcal{A}$ there exists exactly one $b \in \mathcal{B}$ such that $V(x, y, a, b) = 1$.*

At this point, it seemed as if these types of games might not be the right place to look for a game in which the introduction of communication exhibits a non-trivial advantage for the 2-repeated game over a single instance of the game. For this purpose, let us consider the following game, which we call 2-wildcard $(2WC)$.

**Definition 4.2.** *The $2WC$ non-local game is defined as follows. $\mathcal{X} = \mathcal{Y} = \mathcal{A} = \mathcal{B} = \mathbb{Z}_3$, $\mu = \mu_A \otimes \mu_B$, where both $\mu_A$ and $\mu_B$ are the uniform distribution over $\mathbb{Z}_3$. the verification predicate $V$ is given by $V(x, y, a, b) = 1$ iff one of the following holds: $x = 2$ or $x \neq 2$ and $a + b = xy \mod 3$.*

First, we consider the value of this game in the classical setting, with no communication.

**Claim 4.3.** $val(2WC) = \frac{7}{9}$.

*Proof.* Consider the following strategy in which Alice always outputs $a = 0$, and Bob outputs $b = 0$ on $y \in \{0, 1\}$, and on $y = 2$ Bob outputs $b = 2$. One can very easily go over all 9 cases and see that Alice and Bob lose only on $x = y = 1$, and $x = 0, y = 2$. This proves that $val(G) \geq \frac{7}{9}$. To prove that $val(G) \leq \frac{7}{9}$, let $f, g$ be any two strategies employed by Alice and Bob, respectively. Now, consider the following equations, all mod 3. Note that these equations exactly describe the winning conditions for different input pairs.

$$\begin{aligned} f(0) + g(0) &= 0 \\ f(0) + g(1) &= 0 \\ f(0) + g(2) &= 0 \\ f(1) + g(0) &= 0 \\ f(1) + g(1) &= 1 \\ f(1) + g(2) &= 2 \end{aligned}$$

If the first, second, fourth and fifth equations are all satisfied, one can deduce that $f(0) - f(1) = 0$ and that $f(0) - f(1) = 2$, which is a contradiction, which means that one of these equations is false. Assume w.l.o.g that its the first equation. Now note that from the second and third equations one can obtain $g(2) - g(1) = 0$, and from the sixth and fifth equations one can obtain that $g(2) - g(1) = 1$, which is also a contradiction. Thus at least 2 of these 6 equations are false. One can check to see that the choice of which of the four equations discussed for the first contradiction actually does not hold is indeed without loss of generality. Thus, no matter what pair of strategies is chosen between Alice and Bob, they always lose at least two instances out of the possible 9. thus their winning probability is at most $\frac{7}{9}$. ■

Now, before we dive into the communication variant of this game, we want to discuss what is the 'correct' amount of communication one should give the players in order to test the power that communication introduces. In this project, our goal is to check whether one can use communication in a non-trivial manner, where the trivial manner is simply Alice sending Bob some of her inputs to win a fraction of the games automatically.

Thus, our question in the beginning of this sub-section of what is the power of a single bit of communication might appear as misleading, since in the above game the input space is of size 3, all inputs are equally likely, thus the entropy of the input distribution of Alice is 1.5. So it would seem at first that in order to 'cancel' a single game in a repeated instance of $2WC$, Alice needs to send a trinary bit to Bob. However, a more careful look at the problem reveals that Alice can actually do so using a single binary bit. Consider the 2-repeated version of the game, and say that Alice wants to inform Bob of her first coordinate input. If Alice received $x_1 = 0$, she'll send 0, otherwise she'll send 1. Note that since the input 2 is a wildcard, with this information Bob can always guarantee a win in the first game. Because either he knows Alice's input in the first coordinate (0 or 1 case) or either Alice holds the wildcard 2, in which case Bob wins anyway. Thus the first game is effectively cancelled.

So now the challenge we tackle here is whether one can do anything better with a single bit of communication from Alice to Bob, other than just cancelling a single game? We answer this question in the affirmative. Formally, we prove the following. In the following $val^1(2WC^{\otimes 2})$ refers to the value of the 2-repeated version of $2WC$ with classical players in which Alice sends one bit of information to Bob.

**Claim 4.4.** $val^1(2WC^{\otimes 2}) \geq \frac{1}{3} + \frac{2}{3} \cdot \frac{7}{9}$

*Proof.* Consider the following strategy from Bob and Alice. Regarding her output strategy, Alice chooses the same strategy as in the no communication case, $a = 0$ always.

Regarding Alice's bit of communication, Alice sends 1 to Bob if $(x_1, x_2) \in \{(1,1),(1,2),(2,1)\}$, and otherwise sends 0.

Bob does the following, if Bob received 1 from Alice, Bob picks appropriate winning answers $b_1, b_2$ assuming that Alice holds $(1,1)$, and outputs them. Note that since 2 is a wildcard, Alice and Bob always win the game in this case, and this case occurs with probability $\frac{1}{3}$.

Otherwise, if Bob received 0 from Alice, then Bob outputs $b_1 = b_2 = 0$. Let us do a case analysis for the winning probability in this case:

1. If Alice's input satisfies $(x_1, x_2) \in \{(0,0),(0,2),(2,0),(2,2)\}$ then by definition of the game, Alice's strategy, and the fact that 2 is a wildcard, we get that Alice and Bob win the game. These account for $\frac{2}{3}$ of the cases where Alice sends a 0.

2. If $(x_1, x_2) = (1,0)$ then they win iff Bob received $y_1 = 0$, since in that case both Bob and Alice output zeroes. This gives another $\frac{1}{18}$ of the cases where Alice sends a 0 where they win. Symmetrically, they win another $\frac{1}{18}$ of the cases where Alice sends a 0 for when $(x_1, x_2) = (0,1)$.

In total, Alice and Bob win the game in $\frac{7}{9}$ of the cases of when Bob gets 0 from Alice. So in total their winning probability with this strategy is $\frac{1}{3} + \frac{2}{3} \cdot \frac{7}{9}$, which concludes the proof. ■

## 4.3 Conjecture

The above observations led us to consider the question of whether communication can help *unique* games at all? In particular, we began pondering on the following conjecture.

**Conjecture 4.5.** *Let $G$ be a unique game over a binary input and answer alphabets $(\{0,1\})^2$ in which the inputs to Alice and Bob are uniformly random and independent. Denote the value of the $n$-repeated game with a single bit of communication from Alice to Bob( $val^1(G^{\otimes n})$) by $p$. Then it holds that $val(G^{\otimes n-1}) = p$. Here, $val(G^{\otimes n-1})$ is the value of $n-1$-repeated version of $G$, with no communication.*

We considered several approaches to tackle this conjecture, on which we elaborate below.

**Bobs best strategy.** Consider an optimal strategy for the game $G^{\otimes n}$ with 1 bit of communication. Such a strategy is characterized by functions $A : \{0,1\}^n \to \{0,1\}^n$, which denotes Alice's strategy, $f : \{0,1\}^n \to \{0,1\}$ which denotes the bit that Alice sends to Bob, and $B : \{0,1\}^{n+1} \to \{0,1\}^n$, which denotes Bob's strategy based on his input and the bit he received from Alice.

Now, consider the game $G^{\otimes n-1}$ on inputs $x, y$ respectively. Intuitively, what can Alice and Bob do in order to have winning probability $p$? We'll start with Alice. Alice had no information regarding Bob's input even in the $G^{\otimes n}$ version with communication, thus for her the choice seems to be obvious, and we define her strategy $A^*$ for the $G^{\otimes n-1}$ game as follows: On input $x \in \{0,1\}^{n-1}$, Alice chooses a bit $x_n$ uniformly at random, computes $A(x, x_n)$ and outputs the first $n-1$ bits of the result (the bits that correspond to the answers of the games she is actually playing).

Next, we move on to Bob, now Bob's proposed strategy is more tricky, since in the strategy $B$, Bob depends on the communication from Alice in order to make his decision. Without it, Bob has *strictly* less information then he had in the $n$-repeated game about Alice's input. So, intuitively, the best Bob can hope for, knowing that Alice is simulating her strategy $A$ is to try an simulate his strategy $B$ to the best of his ability. Specifically, to output the most probable answers that $B$ would have outputted given the information Bob currently has. Formally, Bob is going to do the following.

Denote by $f_1 \subseteq \{0,1\}^n$ the set of inputs $x$ on which $f(x) = 1$. Similarly denote $f_0$. Assume w.l.o.g. that $|f_1| > |f_0|$, denote $p_1 = \frac{|f_1|}{2^n}$, and $p_0 = 1 - p_1$. Then, Bob will compute which strategy he would've been most likely to play. Each of his possible answer vectors start with value 0, then he computes the value of $B(y,0,1)$ (the communication bit is the last bit) and adds to its value $\frac{p_1}{2}$. He does the same for $B(y,1,1)$, $B(y,0,0)$, and $B(y,1,0)$.

Then Bob goes over all possible answer vectors $b \in \{0,1\}^{n-1}$, picks the one with the highest value, and outputs it.

[2]It turns out that all such non-trivial games are the CHSH game, up to some form of equivalence

Possible slight variations on this could be that Alice and Bob preemptively choose which will be the "extra game" or the game that they only pretend to play, Alice strategically chooses what her extra input bit is instead of randomly, and Bob strategically chooses among his 4 possible responses.

Unfortunately, we were not able to find a good way to analyze the winning probability of this strategy, although intuitively this type of strategy seems like the most straightforward approach to derive a strategy for $n-1$ games from a strategy for $n$ games with one bit of communication.

**Modifying the strategy closer to a dictator** Another attempt at proving this conjecture is trying to view a strategy for $(n-1)$-repeated version of the game as a strategy for our $n$-repeated version of the game in which $f = x_i$ for some $i \in [n]$. Concretely, the case where Alice sends Bob her input on one of the games and thus guarantees a win in that specific game.

Our goal would thus be to try and show that any strategy $(A, f, B)$ for the $n$-repeated version of the game with winning probability $p$ can be turned into a strategy $(A', f', B')$ with winning probability $p$ in which $f' = x_i$ for some $i \in [n]$. For a given Boolean function $g$, denote for each $i \in [n]$ by $Agr_i^{f_1}$ the set $\{x \in \{0,1\}^n \mid x_i = 1, f(x) = 1\}$. We similarly define $Agr_i^{f_0}$ for each $i \in [n]$.

Now, in order to achieve our goal it suffices to prove the following: Any strategy $(A, f, B)$ for the $n$-repeated version of the game with winning probability $p$ (in which $f$ is not a dictator function) can be turned into a strategy $(A', f', B')$ with winning probability $p$ in which $f$ and $f'$ differ on exactly one input, and the change of the value on said input either increased the size of $Agr_n^{f_0}$ or $Agr_n^{f_1}$, or more intuitively we make the communication function of Alice slightly closer to a function which just sends one of her inputs, so that we can inductively reduce a strategy to a trivial strategy as mentioned before.

So let $(A, f, B)$ be some strategy and let $x$ be some input such that $x_n = 1$ but $f(x) = 0$ and define $f'$ to equal $f$ on all inputs except for $x$ on which $f'(x) = 1$.

Now, if we don't change the strategies $A, B$ it could be that the winning probability of Alice and Bob decreased since Bob's answers might have changed on inputs when Alice got $x$ as input since we changed $f'$. Changing Bob's strategy $B$ can introduce even more complications since then it could potentially effect the winning probability on all possible inputs of Alice.

It seems as if the more promising direction is trying to find a way to amend Alice's strategy in a way that ensures a winning probability of $p$ still with $f'$. Unfortunately, we were not able to find such a strategy.

## 4.4 Open problems

Introducing communication to the setting of non-local games raises a massive amount of questions about the connections between parallel repetition, communication complexity, and quantum entanglement. The potential research avenues are practically endless. We name a few such open questions which are of particular interest to us, and hopefully the broader community as well.

1. **Communication vs entanglement for CHSH.** It's known that there is a gap between $val(CHSH^{\otimes n})$ (the classical value) and $val^*(CHSH^{\otimes n})$ (quantum value). How much communication does one need to introduce to the classical version in order to close that gap? How much communication is needed in order to bring either one of these values up to one?

2. **One-directional vs bi-directional communication.** So far in our attempts we explored only one-way communication, namely from Alice to Bob. What power, if any, does bi-directional introduce over one-way communication for non-local games?

3. **Unique games vs non-unique games.** We gave an example for a non-unique game for which communication helps more than trivially cancelling games. Can one give such an example for unique games? Or maybe unique games can not benefit from communication in a non-trivial way? In general what *characterizes* the family of games for which the introduction of communication helps in a non-trivial way in the classical setting/the quantum setting?

4. **Alphabet size, input distribution.** How do the sizes of the input/output alphabet sets relates to the whether communication displays a non-trivial advantage? If at all? The same question can be asked about the input distribution $\mu$, we have considered only product, independent, uniform distributions in this project, but one can design games with very complex input distributions.

5. **Classical vs Quantum communication.** So far we have only considered classical communication between Alice and Bob. Of course one can also discuss the introduction of quantum communication between the players. This, however, requires a different definition of what is the "trivial advantage" that quantum communication introduces, since quantum communication may be able to do more than just cancelling games.

6. **Communication for a slower decay.** As mentioned in the introduction, there is a theorem of Raz [Raz95] that shows that for each game $G$, the value of its $n$-repeated version decays exponentially with $n$. Can the introduction of communication to the model overcome this phenomena? To be a little more precise, is there a game $G$ for which if Alice and Bob play $G^{\otimes n}$, while communicating $f(n)$ (e.g. $f(n) = n/2$) bits, then the value of $G^{\otimes n}$ in this model decays only polynomially fast?

# References


[Bel64] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[Cir80] B. S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[CS14] André Chailloux and Giannicola Scarpa. Parallel repetition of entangled games with exponential decay via the superposed information cost. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming - 41st International Colloquium, ICALP 2014, Copenhagen, Denmark, July 8-11, 2014, Proceedings, Part I*, volume 8572 of *Lecture Notes in Computer Science*, pages 296–307. Springer, 2014.

[CS15] André Chailloux and Giannicola Scarpa. Parallel repetition of free entangled games: Simplification and improvements, 2015.

[CSUU07] Richard Cleve, William Slofstra, Falk Unger, and Sarvagya Upadhyay. Perfect parallel repetition theorem for quantum xor proof systems. In *CCC*, pages 109–114, 07 2007.

[CVY13] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust randomness amplifiers: Upper and lower bounds. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*, pages 468–483. Springer, 2013.

[CWY14] Kai-Min Chung, Xiaodi Wu, and Henry Yuen. Parallel repetition for entangled k-player games via fast quantum search. *arXiv preprint arXiv:1501.00033*, 2014.

[CY14] Matthew Coudron and Henry Yuen. Infinite randomness expansion with a constant number of devices. In David B. Shmoys, editor, *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 427–436. ACM, 2014.

[DS14a] Irit Dinur and David Steurer. Analytical approach to parallel repetition. In David B. Shmoys, editor, *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 624–633. ACM, 2014.

[DS14b] Irit Dinur and David Steurer. Analytical approach to parallel repetition, 2014.

[Fei91] Uriel Feige. On the success probability of the two provers in one-round proof systems. In *Proceedings of the Sixth Annual Structure in Complexity Theory Conference, Chicago, Illinois, USA, June 30 - July 3, 1991*, pages 116–123. IEEE Computer Society, 1991.

[Gri20] Alex B. Grilo. A simple protocol for verifiable delegation of quantum computation in one round, 2020.

[Hås01] Johan Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, 2001.

[MYS12] M McKague, T H Yang, and V Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, Oct 2012.

[Raz95] Ran Raz. A parallel repetition theorem. In *Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '95, page 447–456, New York, NY, USA, 1995. Association for Computing Machinery.

[Ver94] Oleg Verbitsky. Towards the parallel repetition conjecture. In *Proceedings of the Ninth Annual Structure in Complexity Theory Conference, Amsterdam, The Netherlands, June 28 - July 1, 1994*, pages 304–307. IEEE Computer Society, 1994.

[VV11] Umesh V. Vazirani and Thomas Vidick. Certifiable quantum dice - or, testable exponential randomness expansion, 2011.