CMSC 858: Algorithmic Lower Bounds
Fall 2022
CHSH Game Reductions

Rushil Dandamudi

December 8, 2022

In this lecture, we explore the CHSH game, a type of 2-player non-local game where quantum and classical players perform differently. Within the past few years, there have been single-player versions of this game relying on computational hardness assumptions. These single-player games are coined interactive proofs of quantumness (iPoQs). After walking through both problems and tools to analyze their hardness, I will prove a reduction from CHSH to an iPoQ. Finally, I explain how one would do the same for generalized CHSH games.

Contents

Scribe: Rushil Dandamudi
Group 4 **Date:** 11/26/2022

1 Background Presentation Notes

The following section covers the first presentation (background) for this final project.

1.1 The CHSH Game

The CHSH game is a 2-player 1-referee interactive game where players are only allowed to communicate before receiving input from the referee. This type of game with restricted communication is generally called a *non-local game*.
In the CHSH game, Alice and Bob each receive a random bit from the Referee and each output a bit to the Referee. Alice and Bob win if and only if the XOR of their outputs equals the AND of their inputs. In other words, the win condition for the CHSH game is – Alice and Bob must output different bits if and only if their inputs are both 1 ($x \wedge y = 1$ or $x + y = 2$)

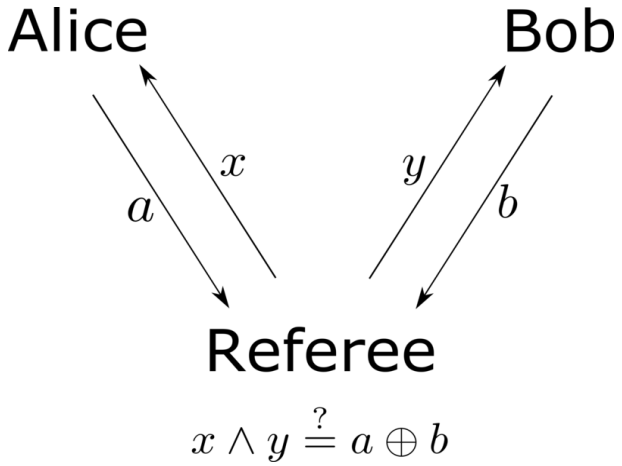


Figure 1: The CHSH game. Alice and Bob are the non-communicating players. x and y are inputs, a and b are outputs.

Definition 1 *A **non-local game** is one where the referee asks n players separate questions and collects their separate answers. The referee's win condition is a function of the inputs and answers. The main rule is the n players must not communicate after receiving their inputs from the referee. The players are allowed to discuss beforehand.*

All optimal quantum strategies require players to prepare entangled qubits during pre-game discussion. Experimentally, these non-local games are interesting because they provide simple, measurable evidence of quantum entanglement.
Note: Because non-local games are played with commuting operators, and be-

cause faster-than-light communication is impossible[1], any game can be viewed sequentially (i.e. Alice measures before Bob). For this reason, the analysis of a game can be illustrated by Bob's potential states after Alice's measurements.

Definition 2 ***Steering*** *is the process where one party's measurements on their qubit to intentionally manipulate the state of a separate party's entangled qubit.*

This always happens with entanglement, but if the first party is clever and intentional, they can predict and design a strategy for both players. For example, consider an attempt at making a single-player non-local game. If a Referee wanted to play the game with Bob and act as Alice, they would *steer* their entangled qubits to force Bob's to enter a particular state that matches potential states after Alice's measurement. This will be crucial later for the single-prover Interactive Proofs of Quantumness in section 2.3.

1.1.1 Related Problems

There are other tangential but related problems to the CHSH game. These are all non-local games, but are different and interesting to explore.

XOR Games Broadly speaking, the CHSH game is a type of XOR game.

Definition 3 *Any non-local game where the referee's win condition depends on the XOR of Alice and Bob's outputs is an* ***XOR game****.*

It is well studied and may generalize to any distribution of inputs and outputs, along with any desired XOR value $c = a \oplus b$.

Magic Square Game Another non-local game, the Magic Square game has the usual three parties but with a 3x3 square. The referee randomly selects a row and column i,j for Alice and Bob respectively. Alice and Bob must insert 0 or 1 into each location, and they win iff

1. The values in row i add to an even number.
2. The values in column j add to an odd number.
3. Alice and Bob's values are consistent (they agree at (i, j)).

In general Magic Square games, the square's dimension can be any size kxk.This problem has been studied throughout history (since at least 190 BCE) across the world (China, India, Persia, etc.) for different k.
Classical Value: A quick sketch can illuminate that there is no classical solution to such a problem. It is impossible to fill a 3x3 grid with 0s and 1s such that all rows add to even numbers and all columns add to odd numbers. In fact, out of the 9 locations, there will always be at best 1 location where Alice and

[1] Called the No-Communication Theorem.

Bob must disagree (to satisfy the first two properties). Thus, the classical value of this game is $8/9$.
Quantum Value: When Alice and Bob share an entangled state and perform some predetermined entangled measurements (where each grid location should correspond to a unique measurement value), they can succeed with probability 1 – better than the CHSH game.

One useful property of the Magic Square game is *pseudo-telepathy*[2].

Definition 4 *A game is **pseudo-telepathic** if its quantum value is 1, but classical value is less than 1.*

This allows for useful experiments! Assuming the quantum computer is fault tolerant and minimizing its noise, repeating a non-local game for quantum players should have success remain ≈ 1, whereas classical players would clearly scale down to some negligible value. Imagine the probability of $\frac{1}{x^n}$ as n approaches a large number of iterations.
Brassard et al.'s paper on pseudo-telepathic games[2] lists a variety and many fall under the class of games called Linear Constraint System games.

Linear Constraint System (LCS) Consider a binary linear system of the form $Mx = b$ where $M \in \mathbb{Z}_2^{m \times n}$ and $b \in \mathbb{Z}_2^m$. The referee prepares this system randomly and shares it with Alice and Bob. The referee gives a row r of the matrix to Alice and an index i of b to Bob. Alice must output a x that satisfies the constraint $M_r x = b_r$, and Bob must output a value for b_i. They win iff (1) they agree at i and (2) Alice's x satisfies the constraint.[8]

In his outstanding work, Arkhipov reduces from an incidence graph to all LCS games. Briefly, the mapping works by creating vertices and edges based on constraints in M and b. By reducing from graph-coloring an incidence graph to solving an LCS game, Arkhipov shows the NP-Hardness of these non-local games. He also shows that all pseudo-telepathic graphs contain a combination of Magic Square graphs and a related graph called the Magic Pentagram (10 variables instead of 9).

Theorem 1 *A linear constraint system is pseudo-telepathic iff the associated incidence graph is non-planar. Also, any pseudo-telepathic (non-planar) incidence graph must have at least 1 Magic Pentagram or Magic Square graph as a minor.[1]*

Other related but more related problems are elaborated in section 2.3.1.

1.2 Unconditional Hardness of Games

The Bell (resp. Tsirelson's) Inequality is used to bound the classical (resp. quantum) hardness of playing CHSH games. By upper bounding expectations,

we can upper bound probability of success (or easiness), which is equivalent to an "unconditional" lower bound in the hardness of the game.

1.2.1 Bell and Tsirelson's Inequalities

To capture the sum of expected correlations in an interesting way that is aligned with the game, we find the correlation between inputs and outputs for each case. To express anti-correlation, we use a negative sign as a coefficient for an expectation. If the probability for equal outputs given certain inputs is $p(a \oplus b = 0|x_i, y_j)$ then the corresponding expectation is written as $< X_i Y_j >$.

Theorem 2 *Let* $S =< X_0Y_0 > + < X_0Y_1 > + < X_1Y_0 > - < X_1Y_1 >$.

- $S_c \leq 2$ *(CHSH Inequality)[6]*
- $S_q \leq 2\sqrt{2}$ *(Tsirelon's Inequality)[4]*

1.2.2 Probability vs Expectation

It is known that the expectation of a measurement is can be related to the probability like so: $< X_i Y_j >= \frac{1}{2}(1 + p(a \oplus b = 0|x_i, y_j))$[3].

Here, $< X_i Y_j >$ represents the expected XOR of the outputs from Alice and Bob given they receive $x = i$ and $y = j$. For quantum players, this means they measure A_i and B_j, but for classical players they only perform their specific classical operations. The above formula comes from the fact that the expected correlation for A_i and B_j is $Tr(A_i B_j \rho)$ where rho is the outer product of Alice and Bob's initial joint state.

Definition 5 *In complexity theory, or specifically game theory, the probability a party wins a game like the non-local games described above is called the* ***value*** *of the game, where a value of a game G is written as* $\nu(G)$.

We can determine the quantum and classical values of the game using the above formula, the Bell/Tsirelson's inequalities and algebra – $\nu(G) = \frac{1}{2}(1 + \frac{S}{4})$. Plugging in the bounds, the classical value becomes .75 and quantum is .85.

Optimal Classical Strategy: The optimal strategy for Alice and Bob is for both to always output the same bit, say 0. Because the inputs are uniformly distributed, 3/4 of the time, the right answer is to output the same bit. Figure 2 can simply explain why.

Note: Because the CHSH and other non-local games serve to separate quantum and classical capabilities, a key component of their construction is the optimal quantum measurements, and we prove their optimality using Tsirelson's inequality. For classical players, we do not imagine their optimal measurements, but rather use the CHSH inequality to show their maximum likelihood of success. This will be important later in section 2.

$$a(x) + b(y) = xy \pmod 2$$

Strategy	x	y	a	b	a+b	xy
Always Send 0	0	0	0	0	0	0
	0	1	0	0	0	0
	1	0	0	0	0	0
	1	1	0	0	0	1
Always Send 1	0	0	1	1	0	0
	0	1	1	1	0	0
	1	0	1	1	0	0
	1	1	1	1	0	1
Same as Input	0	0	0	0	0	0
	0	1	0	1	1	0
	1	0	1	0	1	0
	1	1	1	1	0	1
Opposite of Input	0	0	1	1	0	0
	0	1	1	0	1	0
	1	0	0	1	1	0
	1	1	0	0	0	1

Figure 2: Possible strategies for classical players. Incorrect outputs are in red.

1.3 Interactive Proofs of Quantumness (iPoQs)

Interactive Proofs of Quantumness (iPoQs) are a type of Prover-Verifier security protocol where the Verifier poses questions to the Prover to determine whether the Prover is quantum (BQP-abilities) or classical (P-abilities). Analyzing the success-rate for a prover can illuminate to the verifier whether it is quantum or classical.

In Kahanamoku-Meyer et al., the authors create an iPoQ, Protocol-2, between a single prover-verifier system using *computational hardness of inverting* a Trapdoor Claw-Free Function (TCF) and *unconditional hardness of the CHSH game* [7]. By relying on the CHSH game, where quantum and classical parties have a clear (.10) gap, they create a protocol where quantum and classical provers also have the same gap in success-rate (.10).

Definition 6 *A **trapdoor claw-free function (TCF)** is a* k*-to-*1 *function that is computationally difficult to invert but efficiently invertible with a trapdoor (usually a bitstring). By default, TCF typically refers to a* 2*-to*1 *function.*

Protocol-2

Scribe: Rushil Dandamudi
Group 4 **Date:** 11/26/2022

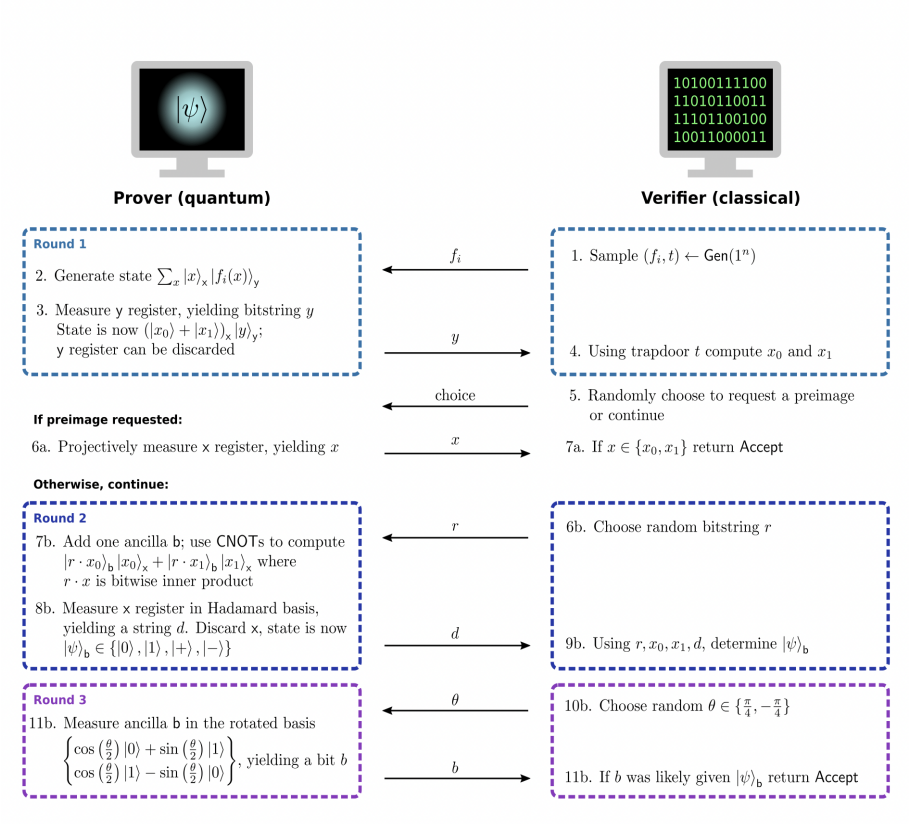


Figure 3: Protocol-2 Details. In the textual description above, 1. refers to Round 1, 2. to 6-7a, 3. to 6-7b, 4. to 8-9b, and 5. to Round 3.

1. The Verifier, V, prepares a TCF, saves the trapdoor and informs the prover of the function. The honest (quantum) Prover, P, should prepare a state that captures all inputs and outputs for this function (superposition). Measuring the output register would collapse the superposition onto a single output, which P should output to V. Now, P has committed to a particular TCF image, y. Because the TCF is 2-to-1, P's input register, a superposition of all inputs mapping to y, should capture 2 pre-images.

2. V flips a coin – if it is 0, P must output one pre-image of y. P can easily do this by measuring (and collapsing) its input register.

3. If it is 1, V sends a random bitstring r. P must create a new qubit, h, and compute in superposition $\mathsf{r} \cdot \mathsf{x}_\mathsf{i}$ for $\mathsf{i} = \{0, 1\}$. Now, this new qubit stores a hardcore bit of both pre-images, which is computationally difficult to learn based on the TCF's security. Based on the values of $\mathsf{r} \cdot \mathsf{x}_\mathsf{i}$, it is either in $\theta \in \{0, \pi/2, \pi/4\}$, where θ represents the angle of the state.

4. After using a QFT (Hadamard) on the input register and measuring it, P outputs the result to V. This process *steers* the new "hardcore" qubit, h, into one of 4 states – $\theta \in \{0, \pi/2, \pi/4, 3\pi/4\}$.

5. The final step is for V to request a random one of two measurements of h and P passes if its measurement is likely given the V's expected h. (V can compute h using parameters, $\theta = f(x_0, x_1, r, d)$, because it can use the trapdoor to compute both pre-images).

Although the authors prove security using a reduction from the TCF's security, there is no explicit reduction from the CHSH game. An optimal classical (resp. honest quantum) prover succeeds (tight bound) with .75 (resp. .85). Because these probabilities match the CHSH game, it is reasonable to assume the reduction exists. I will prove this in the next *section*.

1.4 Generalized CHSH ($G_{m_1 m_2 n_1 n_2}$)

For each choices of measurement operators per player, or more measurement outcomes per operator, a new inequality and game can be created. In her paper, Stephanie Wehner computes generalized bounds on the sum of the expected correlations for a games where Alice and Bob have the same number of inputs and only 2 outputs (G_{mm22})[10].

Theorem 3 *Let* $S = \sum_{i=0}^{m-1} < X_i Y_i > + \sum_{i=0}^{m-1} < X_{i+1} Y_i >$*, where* $< X_n Y_{m-1} > = - < X_0 Y_{m-1} >$.

- $S_c^{(mmnn)} \leq 2m - 2$ *(classical)*
- $S_q^{(mmnn)} \leq 2m \cos(\frac{\pi}{2m})$ *(quantum)*

This is consistent with previous findings. For example for the CHSH game (G_{2222}), $S_c \leq 2$ and $S_q \leq 2\sqrt{2}$. While the bounds were derived from SDP strategies, intuitively they make some sense. For classical settings, 2 is maximum expected classical overlap between measurements, so this means $\frac{2m-2}{2} = m - 1$ expectations remain after considering the measurements can comply with at most $m - 1$ correlations out of $2m$. While the intuition isn't as clear for inequalities that include all m^2 permutations, the true bound for this seems to be $m(m-2) + 2$.

For quantum settings, the $2m$ coefficient clearly comes from the $2m$ terms in the sum of expectations S. The $\cos(\frac{\pi}{2m})$ term represents the maximum overlap (angle similarity) between 2 measurement vectors amongst $2m$ in a space of $(-\pi/2, \pi/2]$.

This means, if I were interested in a modified inequality with a different set of inputs to sum expected outputs over, say a set of m^2 for m^2 permutations of inputs, then the bound would be $S_q \leq m^2 \cos(\pi/2m)$

2 In-Depth Report (Findings)

The following section covers the second presentation (new findings) for this final project. After constructing and analyzing Protocol-2, a natural question is – what is the quantum and classical hardness of breaking Protocol-3?

2.1 Protocol-k ($k = 3$)

When there are 3 inputs per player, corresponding to at most 3 measurements a player could use, this corresponds to CHSH-iPoQ with a new type of TCF. This TCF is called a *3-to-1* TCF. Clearly, from the name, this TCF has 3 pre-images for each image, unlike the standard 2 for a typical (*2-to-1*) TCF.

Overall, the protocol is the same as Protocol-2, however in step 8b., the potential states for the "hardcore" qubit now has an angle depending on (x_0, x_1, x_2, r, d) instead of (x_0, x_1, r, d)). This means the prover steers towards different states than those in Protocol-2. I list them below:

- $B_1 = \{0, \pi/2\}$
- $B_2 = \{\frac{-\pi}{7}, \frac{5\pi}{14}\}$
- $B_3 = \{\frac{\pi}{7}, \frac{-5\pi}{14}\}$

2.2 G_{3322}

Win Condition: $I(x+y=3) = a \oplus b$. I is the indicator function that outputs 1 if the condition is true and 0 otherwise. This is decided by the table below. The third column is decided by checking which of Alice's measurement vector is closer to Bob's (correlated or anti-correlated).

x	y	$I(E[a \oplus b] < 0)$
0	0	0
0	1	0
0	2	0
1	0	0
1	1	0
1	2	1
2	0	0
2	1	1
2	2	0

Table 1: Correlation of *quantum* Alice and Bob's Outputs given they follow prescribed, optimal measurements. Here, the third column represents the sign of the expectation of their XOR'ed measurements (whether their outputs are more likely to be same or different).

Alice's Measurements: Alice's angles in G_{3322} are analogous to these steered states in Protocol-3 (see steering explanation in section 1.1). Explicitly,

these measurements are equivalent to Alice and Bob starting with a maximally entangled state[2] and Alice measuring in one of the three bases (pairs of orthogonal vectors) listed above. Alice's answer, a, is 0 if the measurement collapses to the left angle, and 1 for the right angle.

Bob's Measurements: Bob's angles, $\{0, \pm.16\pi\}$, are determined via numerical optimization. The optimization problem is to find 3 vectors with angles within $(-\pi/2, \pi/2]$ that maximize the correlation inequality (saturate the bound) for G_{3322}.

2.3 Extremal Inequalities

Previously, I described the hardness of the CHSH game and its generalized modifications using an inequality to upper bound optimal correlations/strategies. However, there is a better, more geometric interpretation for any *Bell* inequality for these CHSH-esque games.

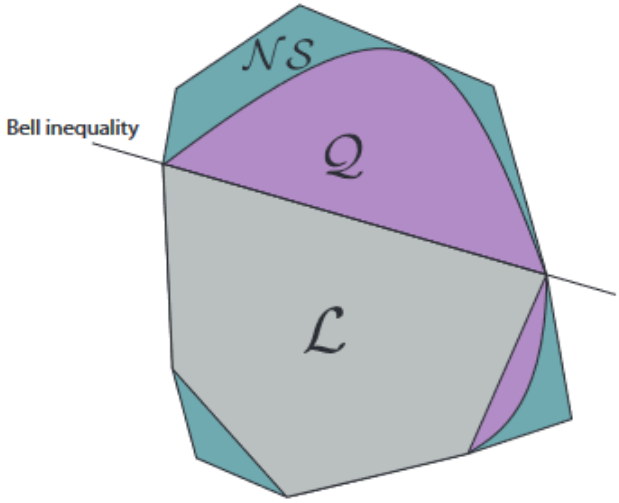
2.3.1 Determining Extremal Inequalities

Let each strategy, or distribution of outputs given inputs, for Alice and Bob in a CHSH-esque game be represented as a point in d-dimensional space. Grouping all distributions that can be described classically, we get a convex set, or a polytope (see Figure 4) in d-dimensional space. Each face/facet of this polytope represents a set of equivalent Bell inequalities. Two inequalities are equivalent if simple relabelling and/or scaling maps from one to the other. For G_{2222} there is only one nontrivial facet. The trivial facet (all probabilities must be non-negative and ≤ 1 isn't of interest because these properties must be satisfied by quantum states too.[5]

While the challenge of computing all of these inequalities is a challenging search problem. Asymptotically, this problem is NP-Complete. The reverse problem, verifying an inequality lies in a facet, is co-NP Complete. These problems are reduced from SAT and 3-colorability.[9] Because computing the maximum *value* of a game requires SDP but with exponentially large inputs, this task is in EXP. For games like CHSH, however, the XOR operations simplify the game and the computation falls to PSPACE.[3]

From Collins and Gisin's work, it is known the maximal value for G_{3322} is most likely reachable by the maximally entangled state. While the measurements they suggest do not align with those emulated by the TCF's steering in Protocol-3, if the emulated angles θ are offset by Collins and Gisin's optimal, θ_{opt}, by δ, offsetting their optimal angles for Bob by δ should yield a two sets of measurements, $(\{A_i\}, \{B_j\})$, equivalent to the optimal suggestions for Alice and Bob. However, as indicated below, Protocol-3 is more complex than imagined.

[2]Explaining maximally entangled states is out of scope. The takeaway is that measuring one qubit in a maximally entangled pair of qubits will result in the other qubit steering to the same state. This means that Bob's qubit mimics Alice's, steering to the same angle.



Sketch of the no-signaling ($\mathcal{NS}$), quantum ($\mathcal{Q}$), and local ($\mathcal{L}$) sets. Notice the strict inclusions $\mathcal{L} \subset \mathcal{Q} \subset \mathcal{NS}$. Moreover, $\mathcal{NS}$ and $\mathcal{L}$ are polytopes, *i.e.*, they can be defined as the convex combination of a finite number of extremal points. The set $\mathcal{Q}$ is convex, but not a polytope. The hyperplanes delimiting the set $\mathcal{L}$ correspond to Bell inequalities.

Figure 4: Polytope diagram describing the 3 sets of inequalities. NS describes the correlations impossible even for quantum computers, requiring faster-than-light communication.[3]

2.3.2 G_{3322} bounds

The following bounds are numerically determined – they may not hold true for larger m.

Theorem 4 *Let* $S =< X_0Y_0 > + < X_0Y_1 > + < X_0Y_2 > + < X_1Y_0 > + < X_1Y_1 > - < X_1Y_2 > + < X_2Y_0 > - < X_2Y_1 > + < X_2Y_2 >$.

- $S_c^{(3322)} \leq 5 = m(m-2)+2 \rightarrow \nu(G_{3322}) = \frac{1}{2}(1+\frac{5}{3^2}) = .78$
- $S_q^{(3322)} \leq 3\sqrt{3} = m^2\cos(\frac{\pi}{2m}) \rightarrow \nu(G_{3322}) = \frac{1}{2}(1+\frac{3\sqrt{3}}{3^2}) = .93$

2.4 Hardness Reductions

2.4.1 $G_{2222} \rightarrow$ Protocol-2

Although the original work by [7] proves security of their protocol to validate their iPoQ, their security proof is a reduction from the hardness of finding 2

pre-images for a TCF. In reality, the security of their protocol stems from both TCF security (inversion hardness) and the CHSH game. There is one reduction missing, seemingly trivial, that could aid with security proofs for Protocol-3.

I will construct an instance of Protocol-2 from a G_{2222} instance (x, y). Let the instance for Protocol-2 by written as (P-2, V-2) where P-2 and V-2 are *classical* prover and verifier algorithms for Protocol-2. Let the referee R moderate *classical* Alice (A) and Bob (B). R acts as V-2 while A and B jointly act as P-2.

1. R follows the initial procedure for Protocol-2 normally, preparing a TCF with a trapdoor and informing P-2 about the function.

2. Once P-2 commits to an image of the TCF by sending it to V-2 (or R), R selects an r and sends it to P-2.

3. Recall R (or V-2) can use the trapdoor to determine x_0, x_1, the pre-images of the image from P-2. R chooses a bitstring r based on the following criteria – given nothing, it seems random, but given x, $r \cdot (x_0 \oplus x_1) = x$.

   Randomness Preservation / Indistinguishability: This is possible because x is random, while the XOR of the pre-images is computationally difficult to recover (indistinguishable from random). Therefore, when P-2 receives r from V-2, it is indistinguishable from random.

   Completeness / Equivalence with Game: Recall the angle steering the state in G_{2222} should depend on x. In Protocol-2, with linear algebra, it is clear that $r \cdot (x_0 \oplus x_1)$ directly determines the basis for the hardcore qubit h. In other words, x is equivalent to $r \cdot (x_0 \oplus x_1)$, so R choosing r in such a way is ideal.

4. P-2 uses the r and outputs a d to indicate to V-2 the hardcore qubit's state.[3]

5. A reads d and outputs $a := (x)(d \cdot (x_0 \oplus x_1)) + (1 - x)(r \cdot x_0)$ to R as its output for G_{2222}.

   Here, Bob's input hasn't occurred yet, so it is safe for Alice to read d and even use the trapdoor to compute the pre-images for outputting a. There is no communication with Bob.

6. R sends $y = m$ (m is the measurement angle from V-2 in Protocol-2 in the last round) to B. B outputs the same output as P-2 $b := b$.

   Although b depends on all variables affecting a, they are computationally hidden by either random bitstrings (r) or TCF security.

Now, I will show a successful P-2, ($p[pass] \approx .85$), can simulate non-local (quantum) correlations by helping Alice and Bob win G_{2222} with $\approx .85$ chance. If b from P-2 is correct with $.85$ chance, that means the bit matches the expected

[3] We should be careful with our language and not mention any quantum operations under the hood (i.e. quantum fourier transform). It is an unsafe assumption when the prover is classical/an adversary. The only safe assumption is the inputs and outputs.

measurement given Bob's input $y = m$. The expected measurement is determined by the steered state, hardcore qubit, h, which is steered by the choice of r and d. Because (by algebra) the steered state is $\theta \in \{0, \pi/2\}$ if $x = r \cdot (x_0 \oplus x_1) = 0$ and $\theta \in \{\pm\pi/4\}$ otherwise, Alice's input behavior matches the optimal behavior in G_{2222}. By linear algebra, Alice outputting a described above steers it in the expected way. If Alice's input is $x = 0$, she outputs $d \cdot (x_0 \oplus x_1)$, which is 1 if h's angle is $\frac{-\pi}{4}$ and 0 for $\frac{\pi}{4}$. These angles match the exact qubit angle Bob would receive if $x, a = (0, 0)$ or $(0, 1)$ in G_{2222}. Similarly, the argument is true for $x = 1$. Thus, Alice and Bob's inputs and outputs directly correlate with the intended distribution for G_{2222}.

To sum, intuitively the reduction follows because:

1. The distribution of steered states matches G_{3322}. (Alice's behavior is the same)
2. Bob's inputs (measurement angle and steered qubit) matches G_{3322}. (Bob's behavior is the same)
3. Alice and Bob's inputs are computationally hidden from each other (no-communication)

2.4.2 Sub-Optimality of Protocol-3

Although it seems the steered states in Protocol-3 match Alice's measurements in G_{3322}, the distribution does not match, this results in a sub-optimal value for the game $< .93$. Normally, the referee would send input uniformly random to Alice and Bob, causing each state to be uniformaly random. For Protocol-3, the distribution is:

x	$\{\theta\}$	$p(\theta)$
0	$\{0, \pi/2\}$	10/16
1	$\{\frac{\pi}{7}, \frac{-5\pi}{14}\}$	3/16
2	$\{\frac{-\pi}{7}, \frac{5\pi}{14}\}$	3/16

Table 2: The distribution of the inputs/steered states for Protocol-3. Probabilities represent match with union of the angles in the set. For individual probabilities, divide by 2.

This causes the optimal measurement angles listed above, to allow the prover to succeed with probability .84. On the other hand, the best classical strategy seems to win with probability .56. It is unclear whether this bound for classical players is tight (**soundness** or true best probability for an adversary). But using numerical optimization, I have determined .84 as the **completeness**, or optimal probability for a quantum prover.

Even if I were to modify G to G'_{3322} where the referee sends inputs to Alice matching the above distribution, her angles are still sub-optimal. Their shift from θ_{opt} is not consistent (δ mentioned above does not have a singular value).

So, it is impossible to use the TCF's steered states to reach the maximum value deemed by the inequalities.

Therefore, it is not possible to get a direct reduction from even G'_{3322} to Protocol-3. While it may be possible to prove security of Protocol-3 and show some gap between quantum and classical provers, proper reduction from G_{3322} requires more massaging.

References

[1] Alex Arkhipov. Extending and Characterizing Quantum Magic Games. arXiv:1209.3819, 2012.

[2] Brassard, G., Broadbent, A. & Tapp, A. Quantum Pseudo-Telepathy. Found Phys 35, 1877–1907 (2005). https://doi.org/10.1007/s10701-005-7353-4

[3] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner Rev. Mod. Phys. 86, 419 – Published 18 April 2014; Erratum Rev. Mod. Phys. 86, 839 (2014)

[4] B.S. Cirel'son, "Quantum generalizations of Bell's inequality." Letters in Mathematical Physics 4, 93-100 (1980).

[5] Daniel Collins and Nicolas Gisin 2004 J. Phys. A: Math. Gen. 37 1775 https://iopscience.iop.org/article/10.1088/0305-4470/37/5/021/meta

[6] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt Phys. Rev. Lett. 23, 880 – Published 13 October 1969; Erratum Phys. Rev. Lett. 24, 549 (1970)

[7] Kahanamoku-Meyer, G.D., Choi, S., Vazirani, U.V. et al. Classically verifiable quantum advantage from a computational Bell test. Nat. Phys. 18, 918–924 (2022). https://doi.org/10.1038/s41567-022-01643-7

[8] Mermin (1990). Simple unified form for the major no-hidden-variables theorems. Physical review letters, 65 27, 3373-3376 .

[9] Pitowsky, I. Correlation polytopes: Their geometry and complexity. Mathematical Programming 50, 395–414 (1991). https://doi.org/10.1007/BF01594946

[10] Wehner, S. (2005). Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. Physical Review A, 73, 22110.