Algorithms, Bounds, and Strategies for Entangled XOR Games

Adam Bene Watts, Aram W. Harrow, Gurtej Kanwar, and Anand Natarajan

Center for Theoretical Physics, MIT

March 15, 2022

Abstract

We study the complexity of computing the commuting-operator value $\omega^*$ of entangled XOR games with any number of players. We introduce necessary and sufficient criteria for an XOR game to have $\omega^* = 1$, and use these criteria to derive the following results:

1. An algorithm for symmetric games that decides in polynomial time whether $\omega^* = 1$ or $\omega^* < 1$, a task that was not previously known to be decidable, together with a simple tensor-product strategy that achieves value 1 in the former case. The only previous candidate algorithm for this problem was the Navascúes-Pironio-Acín (also known as noncommutative Sum of Squares or ncSoS) hierarchy, but no convergence bounds were known.

2. A family of games with three players and with $\omega^* < 1$, where it takes doubly exponential time for the ncSoS algorithm to witness this (in contrast with our algorithm which runs in polynomial time).

3. A family of games achieving a bias difference $2(\omega^* - \omega)$ arbitrarily close to the maximum possible value of 1 (and as a consequence, achieving an unbounded bias ratio), answering an open question of Briët and Vidick.

4. Existence of an unsatisfiable phase for random (non-symmetric) XOR games: that is, we show that there exists a constant $C_{\text{unsat}}^k$ depending only on the number $k$ of players, such that a random $k$-XOR game over an alphabet of size $n$ has $\omega^* < 1$ with high probability when the number of clauses is above $C_{\text{unsat}}^k n$.

5. A lower bound of $\Omega(n \log(n) / \log \log(n))$ on the number of levels in the ncSoS hierarchy required to detect unsatisfiability for most random 3-XOR games. This is in contrast with the classical case where the $n$-th level of the sum-of-squares hierarchy is equivalent to brute-force enumeration of all possible solutions.

*abenewat@mit.edu
†aram@mit.edu
‡gurtej@mit.edu
§anandn@mit.edu
## Contents

1 Background ........................................ 1
2 Results ......................................... 2
3 Future Work .................................. 4
4 Notation ....................................... 5
5 Technical Overview ............................... 6
   5.1 Strategies .................................. 7
      5.1.1 Classical Strategies ...................... 7
      5.1.2 Commuting-Operator Strategies ............ 8
   5.2 Refutations .................................. 9
   5.3 Games with no Parity-Permuted Refutations (noPREF Games) ........... 10
   5.4 Maximal Entanglement, Relative Phase (MERP) Strategies .............. 12
   5.5 MERP - PREF Duality .......................... 13
   5.6 Implications .................................. 13
6 Refutations ..................................... 14
   6.1 Upper Bound on Value ......................... 15
   6.2 Tools for Constructing Refutations ............ 18
      6.2.1 Combinatorics ............................ 18
      6.2.2 PREFs and Shuffle Gadgets ............... 19
   6.3 Algorithm for Symmetric Games .................. 25
7 MERP Strategies .................................. 26
   7.1 Generalizing GHZ ............................. 27
   7.2 MERP Strategy Value ......................... 28
   7.3 MERP - PREF Duality .......................... 29
8 Specific Games .................................. 31
   8.1 123 Game .................................... 32
      8.1.1 Value 1 Strategy ......................... 33
   8.2 Capped GHZ (CG) Games ....................... 34
   8.3 Asymptotically Perfect Difference (APD) Games ...................... 35
      8.3.1 Commuting-Operator Value ................. 36
      8.3.2 Classical Value ........................... 37
9 Random Games .................................. 39
   9.1 SAT Phase ................................... 40
   9.2 UNSAT Phase ................................ 40
   9.3 Lower Bound on Refutation Length (Sketch) ....................... 43
   9.4 Lower Bound on Refutation Length (Full Proof) .................... 47
A Explicit Refutation for Capped GHZ ................. 53
1 Background

Constraint satisfaction problems (CSPs) are a fundamental object of study in theoretical computer science. In quantum information theory, there are two natural analogues of CSPs, which both play important roles: local Hamiltonians and (our focus) non-local games. Non-local games originate from Bell’s pioneering 1964 paper, which showed how to test for quantum entanglement in a device with which we can interact only via classical inputs and outputs. In modern language, the tests developed by Bell are games: a referee presents two or more players with classical questions drawn from some distribution and demands answers from them. Each combination of question and answers receives some score and the players cooperate (but do not communicate) in order to maximize their expected score. These games are interesting because often the players can win the game with a higher probability if they share an entangled quantum state, so a high average score can certify the presence of quantum entanglement. Such tests are not only of scientific interest, but have had wide application to proof systems [7, 19], quantum key distribution [12, 1, 33], delegated computation [26], randomness generation [9] and elsewhere.

To be able to use a nonlocal game as a test for entanglement, it is essential to be able to approximately compute two quantities: the best possible expected score when the players share either classical correlations or entangled states, respectively called the “classical” and “quantum” (or “entangled”) values of the game, and denoted $\omega$ and $\omega^*$. To understand these quantities, think of a game with $k$ players as inducing a constraint satisfaction problem with a $k$-ary predicate. Each question in the game is mapped to a variable in the CSP, and each $k$-tuple of questions and set of accepted responses (a “clause”) asked by the referee corresponds to a constraint. Classically, a simple convexity argument shows that the players can always stick to deterministic strategies, where each question is assigned a fixed answer; thus, $\omega$ is in fact identical to the value of the CSP. Hence, thanks to various dichotomy theorems, we have a good understanding of the difficulty of computing $\omega$: in some cases, we know a $P$ algorithm, and for most others, we know it is $NP$-complete.

The quantum value $\omega^*$ is not as well understood. The main obstacle is that the set of entangled strategies is very rich: the “assignment” to each variable is no longer a value from a discrete set, but a linear operator over a Hilbert space of potentially unbounded dimension. As a result, we can say very little in terms of upper bounds on the complexity of computing $\omega^*$. In fact, it is not known whether even a constant-factor (additive) approximation to $\omega^*$ is Turing-computable. For general games, the best we can say is that it is recursively enumerable: there is an algorithm, called the NPA or ncSoS hierarchy [22, 10], that in the limit of infinite time converges from above to the quantum value, but with no bound on the speed of convergence. On the hardness side, more is known, and what we know is grounds for pessimism: we have been able to show hardness results for approximating $\omega^*$ matching (e.g. [34]) and in some cases exceeding (e.g. [19]) the classical case by constructing special games that force entangled players to use particular strategies. Moreover, families of games have been found for which deciding whether $\omega^*$ = 1 is uncomputable [28]. There are a few exceptions for which some positive results are known: for instance, the class of XOR games, in which the answers are bits and the payoff depends only on their XOR (for any given set of questions). In the classical case, these games are as hard as general games except in the “perfect completeness” regime: distinguishing $\geq 1 - \varepsilon$ satisfiability from $\leq \frac{1}{2} + \varepsilon$ satisfiability is $NP^*$-complete, but we can determine whether an XOR game is perfectly satisfiable in polynomial time using Gaussian elimination over $\mathbb{F}_2$. However, in the quantum case, it was shown by Tsirelon [5, 32] that for two-player XOR games, the lowest level of the ncSoS algorithm converges exactly to the quantum value, rendering it computable in polynomial time via semidefinite programming. (A similar technique was also applied to approximating the entangled value of unique games [21].) Yet these techniques seemed unlikely to generalize to three or more players: it is known that distinguishing $\geq 1 - \varepsilon$ satisfiability from $\leq \frac{1}{4} + \varepsilon$ for an entangled 3-player XOR game is $NP$-hard [34], and deciding the existence of perfect strategies for the closely-related family of linear systems games is uncomputable [28]. For a summary of these results, see Table 1.

Another question which has been very fruitful in the study of classical CSPs is understanding the typical value of a random instance. Research in this direction draws significantly on insights from statistical mechanics and has proven that there exist sharp satisfiable/unsatisfiable thresholds for random $k$-SAT and related games (often using the equivalent constraint-satisfaction formulation). But these techniques do not carry over to the quantum case. For random classical games, a basic method is to look at the expected number of winning responses (the “first moment method”) or the variance (the “second moment method”)
as we randomize the payoff function within some family such as random \( k \)-SAT or random \( k \)-XOR. This suffices, for example, to show that random 3-XOR games with \( n \) variables and \( Cn \) clauses are satisfiable with high probability if and only if \( C \lesssim 0.92 \) [11]. Since quantum strategies do not form a discrete (or even finite-dimensional) set, these methods are not possible. Nor is it obvious how to use more refined tools such as Shearer’s Lemma or the Lovasz Local Lemma, which address the question of when sets of overlapping constraints can be simultaneously satisfied. Indeed there are famous examples (such as the Magic Square game) of quantum “advantage” (i.e. the quantum value of a game is higher than the classical value) when there exist strategies for apparently contradictory constraints that succeed with probability 1. These suggest that the barriers to extending our classical intuition are not merely technical but reflect a genuinely different set of rules.

Table 1: Complexity of determining whether the value of various games is \( \geq c \) or \( \leq c - \varepsilon \).

| Game type | Classical value | Entangled value |
|-----------|----------------|-----------------|
| 2-XOR     | \( c = 1 \) in P | exact answer in P [5, 32] |
|           | \( c < 1 \) P or NP-complete depending on \( \varepsilon \) | |
| Unique Games | \( c = 1 \) in P | UGC-quality approximation in P [21] |
|           | \( c < 1 \) NP-complete assuming UGC | |
| \( k \)-XOR, \( k \geq 3 \) (symmetric) | \( c = 1 \) in P | \( c = 1 \) in P (this paper, Theorem 2.1) |
|           | \( c < 1 \) NP-complete | \( c < 1 \) NP-hard [34] |
| general   | \( c = 1, c < 1 \) both NP-complete | undecidable [29], recursively enumerable [22, 10] |

Unique Games and the Unique Games Conjecture (UGC) are a generalization of 2-XOR games that are defined in [31]. If the UGC holds, then it is NP-complete to achieve any approximation ratio better than that known to be achieved by existing algorithms. For \( k \)-XOR with \( k \geq 3 \) it is NP-complete to beat the trivial approximation.

2 Results

In this section we informally describe our main results, and then give precise theorem statements with links to proof sketches and full proofs later in the paper.

Our work introduces new techniques that let us make progress on the study of both worst-case complexity and random instances of XOR games with more than two players, in the regime where we are trying to decide whether \( \omega^* = 1 \). We think of a nonlocal game as a system of equations whose variables are linear operators, corresponding to the quantum measurements used by the players; a strategy is a solution to this system. Our main innovation is to consider a “dual” system of equations, whose solutions are objects that we call refutations. A refutation is a proof that the “primal” system of operator equations induced by the game is infeasible, and thus that \( \omega^* \neq 1 \). Surprisingly, for games that are symmetric under exchange of the players, we show that the dual system reduces to a set of linear equations over \( \mathbb{Z} \), which can be solved efficiently. This leads to our first result (Theorem 2.1), an algorithm for efficiently deciding whether \( \omega^* = 1 \) for a symmetric \( k \)-player XOR game, which brings the best known upper bound on this problem down from recursively enumerable [22, 10] to P. See Table 1 for a summary of how our result fits in with known upper and lower bounds. Subsequently, by taking the dual of the dual, we are able to explicitly construct a set of quantum strategies (we call these Maximal Entanglement, Relative Phase, or MERP, strategies) that attain value 1 for all symmetric games with \( \omega^* = 1 \) (Theorem 2.2). An explicit example shows that the symmetry assumption is indeed necessary for our algorithm to work: we exhibit a simple non-symmetric game called the 123 game, for which a simple, non-MERP strategy achieves \( \omega^* = 1 \), while our algorithm is unable to detect this (Theorem 2.3).

Our understanding of refutations and characterization of value-1 symmetric entangled games also lets us construct two specific families of games with interesting properties. The first, Capped GHZ (CG), is a family
where ncSoS takes $\exp(n)$ levels and $\exp(\exp(n))$ time to detect that $\omega^* < 1$ (Theorem 2.4), in contrast to our algorithm which runs in polynomial time. The second, Asymptotically Perfect Difference (APD), is an explicit, deterministic family of $k$-XOR games with $\omega^* = 1$ and classical value $\omega \to 1/2$ in the limit of large $k$ (Theorem 2.5). In comparison, there are randomized constructions of families of games whose bias ratio $\omega^{*-1/2}$ diverges for fixed $k \geq 3$ as $n \to \infty$ [24, 4]. However, known examples of these constructions involve both $\omega^* \to 1/2$ and $\omega \to 1/2$, potentially precluding experimental distinguishability. To our knowledge this is the first construction of a family of XOR games that asymptotically achieves a perfect bias difference, $2(\omega^* - \omega) \to 1$, addressing one of the main open questions presented in [4].

For random instances, we analyze the dual system to show the existence of an unsatisfiable (i.e. $\omega^* < 1$) phase as in the classical case (Theorem 2.6). We also relate our methods to the ncSoS hierarchy. For random instances, we show that in the unsatisfiable phase, a superlinear number of levels of ncSoS is necessary to certify that $\omega^* < 1$ (Theorem 2.7).

The theorem statements of these results are as follows. Proof sketches are in Section 5.

**Theorem 2.1.** There exists an algorithm that, given a $k$-player symmetric XOR game $G$ with alphabet size $n$ and $m$ clauses, decides in time $\text{poly}(n, m)^{1}$ whether $\omega^*(G) = 1$ or $\omega^*(G) < 1$.

**Proof.** Section 6.3. Sketch in 5.3. □

**Theorem 2.2.** For every $k$-XOR game $G$ for which the algorithm of Theorem 2.1 shows $\omega^*(G) = 1$, there exists a $k$-qubit tensor-product strategy achieving value 1, and a description of the strategy can be computed in polynomial time.

**Proof.** Section 7. Sketch in Sections 5.4 and 5.5. □

**Theorem 2.3.** There exists a 6-player XOR game $G$ with alphabet size 3 and 6 clauses, for which $\omega^*(G) = 1$ but the algorithm of Theorem 2.1 cannot detect this.

**Proof.** Section 8.1. □

**Theorem 2.4.** There exists a family of 3-XOR games with $\omega^* < 1$ but for which the minimum refutation length scales exponentially in the number of clauses $m$ and alphabet size $n$. For these games exponentially many levels of ncSoS are needed to witness that $\omega^* < 1$.

**Proof.** Section 8.2. □

**Theorem 2.5.** There exists a family of $k$-XOR games, parametrized by $K$, for which $\omega^*(G(K)) = 1$ and the classical value is bounded by

\[
\frac{1}{2} \leq \omega(G(K)) \leq \frac{1}{2} + \sqrt{\frac{K + 1}{2k + 1}} \leq \frac{1}{2} + \sqrt{\frac{\log k}{k}}.
\]

(1)

**Proof.** Section 8.3. □

**Theorem 2.6.** For every $k$, there exists a constant $C^\text{unsat}_k$ depending only on $k$ such that a random $k$-XOR game $G$ with $m \geq C^\text{unsat}_kn$ clauses has value $\omega^*(G) < 1$ with probability $1 - o(1)$.

**Proof.** Section 9.2. □

**Theorem 2.7.** For any constant $C$, the minimum length refutation of a random 3-XOR game with $m = Cn$ queries on an alphabet of size $n$ has length at least

\[
\frac{en \log(n)}{8C^2 \log(\log(n))} - o\left( \frac{n \log(n)}{\log(\log(n))} \right) \quad (2)
\]

with probability $1 - o(1)$ (as $n \to \infty$). Hence, either $\omega^* = 1$ or $\Omega(n \log(n)/\log(\log(n)))$ levels of the ncSoS hierarchy are needed to witness that $\omega^* < 1$ for such games.

\(^1\) Note that $m$ and $k$ do not scale independently for symmetric games. Any symmetric game may be specified by $m'$ base clauses that are then symmetrized via at most $k!$ permutations each, meaning $m \leq k! m'$. We could thus naively rewrite this runtime as $\text{poly}(n, k! m')$ to extract the $k$ dependence. Because the core information about the symmetric game is really only contained in the $m'$ clauses, one might expect that it is possible to remove the factor of $k!$, and we hope to address this in a future work.
Note that we can choose $C \geq C_{3}^{\text{unsat}}$ (with $C_{3}^{\text{unsat}}$ from Theorem 2.6) such that for large enough $n$, typical random instances will have $\omega^* < 1$ but ncSoS will require $\Omega(n \log(n)/\log(\log(n)))$ levels to detect this.

**Proof.** Section 9.3.

## 3 Future Work

We see four main directions in which our characterization of non-local XOR games could be extended.

First, our linear algebraic characterization of $\omega^* = 1$ games is incomplete: there exist games with $\omega^* = 1$ for which a MERP strategy cannot achieve value 1. We expect a strengthening of the $\text{PREF}$ condition may allow us to extend our decidability algorithm to detect these games. An approach to this conjecture is described in Section 6 and a conjectured element of this set of games is given in Section 8.1. Understanding the structure of such games would give further intuition about the behavior of optimal XOR commuting-operator strategies, in particular strategies which may require more entanglement than the simple explicit strategies in Theorem 2.2.

Second, our results leave open the possibility that determining whether $\omega^* = 1$ for nonsymmetric XOR games is outside $\mathcal{P}$ or even undecidable. In the realm of Binary Constraint System (BCS) games, [28] shows that determining whether a general BCS game has perfect value is undecidable. The structural similarity between BCS games and XOR games suggests that perhaps some of the group theoretic techniques of that work could be applied to XOR games to arrive at a similar conclusion. An interesting class of games which may serve as an intermediate class between XOR and BCS games are “incomplete” XOR games in which there are $k$ players but queries can involve $< k$ variables, effectively ignoring some players. Even for $k = 2$, Tsirelson’s semidefinite programming characterization of $\omega^*$ does not apply to incomplete XOR games, although in this case it is still easy to decide whether $\omega^* = 1$.

Thirdly, while in this work we have focused on computing the entangled game value $\omega^*$, our methods may also be useful from the perspective of Bell inequalities, in which the quantity of interest is the maximal violation achievable by an entangled strategy. While this has conventionally been measured in terms of the bias ratio $(\omega^* - 1/2)/(\omega - 1/2)$, the difference $2(\omega^* - \omega)$ is an equally natural measure of violation, and we hope that our techniques will render it more amenable to analysis. Indeed, in addition to the construction of Asymptotically Perfect Difference games mentioned above, our results have the following simple consequence: for symmetric games with $\omega^* = 1$, our characterization of the optimal strategies (MERP) together with the Grothendieck-type inequality of [3] imply that the bias ratio and difference are both bounded by constants depending only on $k$, and that for the difference, this constant is strictly less than one.

Finally, our results are almost entirely concerned with the question of whether $\omega^* = 1$ or $\omega^* < 1$. However, we note that the class of strategies appearing in Theorem 2.2 include the optimal strategy for the CHSH game [6], but not for all XOR games [23]. It is an interesting open question to find a natural characterization of games with $\omega^* < 1$ for which MERP strategies are optimal. In this setting there are still many classical tools which we do not know how to extend to the classical case. As an example, consider overconstrained games in which there are many more constraints than variables and we choose the signs of those constraints randomly. In the classical case, the value is shown to be close to 1/2 in Theorem 8.10 while in the quantum case we can only conclude that it is $< 1$ in Lemma 9.5.
## 4 Notation

Table 2 defines common notation used throughout the paper. This section is intended as a reference for the reader, while future sections provide more detailed technical definitions of these concepts.

| Symbol | Definition |
|--------|------------|
| $G$    | An XOR game. Consists of an indexed set of clauses. |
| $m$    | The number of queries or clauses in an XOR game. |
| $n$    | The question alphabet size or number of variables of an XOR game. |
| $k$    | The number of players in an XOR game. We often use the phrase “$k$-XOR game” to implicitly specify $k$. |
| $q_i$  | The $i$-th query of a game. Written as a length-$k$ vector. The $\alpha$-th entry $q_i^{(\alpha)} \in [n]$ specifies the question sent to player $\alpha$. |
| $s_i$  | The parity bit $\in \{-1, 1\}$ of the $i$-th query in a game. |
| $c_i = (q_i, s_i)$ | The $i$-th clause of a game. Written as a vector of length $k + 1$ that collectively represents the $i$-th query and $i$-th parity bit. |
| $\omega(G)$ | The classical value of XOR game $G$. |
| $\omega^*(G)$ | The commuting-operator value of XOR game $G$. |
| $A$    | The $m \times kn$, $\{0, 1\}$-valued game matrix for an XOR game. If $q_i^{(\alpha)} = j$ then $A_{i,(\alpha-1)n+j} = 1$, otherwise $A_{i,(\alpha-1)n+j} = 0$. |
| $\hat{s}$ | The length-$m$, $\{0, 1\}$-valued parity bit vector with entries $\hat{s}_i = \frac{1 + s_i}{2}$. |
| $G \sim (A, \hat{s})$ | The XOR game corresponding to game matrix $A$ and parity bit vector $\hat{s}$. |
| $\{O_{\pm 1}^\alpha(j)\}$ | The measurement made by the $\alpha$-th player upon receiving question $j \in [n]$. |
| $O^\alpha(j)$ | The strategy observable for player $\alpha$ on question $j$. Defined by the Hermitian operator $O^\alpha(j) := O_1^\alpha(j) - O_{-1}^\alpha(j)$. |
| $Q_i$  | The Hermitian operator representing the collective measurement made by the players of an XOR game upon receiving query $q_i$. Defined by $Q_i := \prod_\alpha O^\alpha(q_i^{(\alpha)})$. |
| $|\Psi\rangle$ | The shared state between the $k$ players of an XOR game. |
| $W$    | A word. In general a $k$-tuple with each element of the tuple a concatenation of questions (“letters”) drawn from $[n]$. We frequently refer to the $\alpha$-th entry of $W$ by $W^{(\alpha)}$, and the specific letter at row $i$ and offset $j$ by $w_{ij}$. |
| $W^\dagger$ | The reversed form of a word. |
| $\sim$ | Equivalence under neighboring pairs of letters canceling. |
| $\triangleq$ | Equivalence under $\sim$ and parity-preserving permutations. |

Table 2: Notation used throughout the paper.
5 Technical Overview

We begin by formally defining a $k$-XOR game and its classical and quantum values.

Definition 5.1. Define a clause $c = (q,s)$ to be any $(k+1)$-tuple consisting of a query $q \in [n]^k$ and parity bit $s \in \{-1,1\}$. In a $k$-XOR game $G$ associated with a set of clauses $M$, a verifier selects a clause $c_i = (q_i,s_i)$ uniformly at random from $M$. Next, the question $q_i^{(\alpha)}$ is sent to the $\alpha$-th player of the game, for all $\alpha \in [k]$. The players then each send back a single output $\hat{s}_i \in \{-1,1\}$, and win the game if their outputs multiply to $s_i$.

The key property of a game $G$ is its value – the maximum win probability achievable by players who cooperatively choose a strategy before the game starts, but cannot communicate while the game is being played. We distinguish various versions of the value by physical restrictions placed on the players.

Definition 5.2. For a given game $G$, the classical value $\omega(G)$ is the maximum win probability achievable by players sharing no entanglement.

The tensor-product value is the maximum win probability obtained by players who share a quantum state but are restricted to making measurements on distinct factors of a tensor-product Hilbert space.

Finally, the commuting-operator value $\omega^*(G)$ is the maximum win probability obtainable by players who may make any commuting measurements on a shared quantum state, not necessarily over a tensor-product Hilbert space. $\omega^*(G)$ is often also referred to as the field-theoretic value of $G$.

The commuting-operator value may differ from the tensor-product value of $G$ [28], and the question of whether it can differ from the closure of the set of values achievable by tensor product strategies remains open\(^2\). In this paper, we focus primarily on a description of the commuting-operator value but in many cases can show that it coincides with the tensor-product value.

For the purpose of analyzing both the classical and commuting-operator value of $k$-XOR games, we find it useful to define a linear algebraic representation for the game\(^3\). The linear algebraic view represents queries as a matrix and parity bits as a vector. In doing so, it abstracts away from the specifics of labels and player/query indices to reveal the underlying game structure.

Definition 5.3. Given a $k$-XOR game with $m$ queries and alphabet size $n$, define the game matrix $A$ as an $m \times kn$ matrix describing query-player-question incidence. Specifically, $A$ can be written as a segmented matrix with $k$ distinct column blocks of size $n$ each, where the $j$th column of block $\alpha$ consists of a 1 in row $i$ if the $\alpha$th player receives question $j$ for query $q_i$, and a 0 otherwise:

$$A_{i,(\alpha-1)n+j} := \begin{cases} 1 & \text{if } c_i^{(\alpha)} = j \\ 0 & \text{otherwise} \end{cases}. \quad (3)$$

For such a game, define the length-$m$ parity bit vector $\hat{s} \in \mathbb{F}_2^m$ by

$$\hat{s}_i := \begin{cases} 0 & \text{if } s_i = 1 \\ 1 & \text{if } s_i = -1 \end{cases}. \quad (4)$$

An XOR game $G$ is completely specified by providing the game matrix $A$ and parity bit vector $\hat{s}$: $G \sim (A, \hat{s})$. For example, the GHZ game [15] is defined by the clauses (here we use the labels $\{x, y\}$ for the questions instead of the typical $\{0, 1\}$):

$$G_{\text{GHZ}} := \left\{ \begin{bmatrix} x & y & y \\ x & y & x \\ 1 & -1 & -1 \end{bmatrix} \right\}. \quad (5)$$

And hard! For general games this question is known to be equivalent to Connes’ embedding conjecture [13].

\(^2\)There seems to exist an interesting parallel between this linear algebraic representation of an XOR game and the linear algebraic specification of a BCS game. While interesting, it is not explored in this work aside from its brief mention here and in Section 3.
We translate the GHZ queries into $A_{GHZ}$ and parity bits into $\hat{s}_{GHZ}$ by:

$$\Rightarrow A_{GHZ} := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}^T \leftarrow (Alice, x)$$  
$$\quad \leftarrow (Alice, y)$$  
$$\quad \leftarrow (Bob, x)$$  
$$\quad \leftarrow (Bob, y)$$  
$$\quad \leftarrow (Charlie, x)$$  
$$\quad \leftarrow (Charlie, y)$$

(6)

$$= \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \hat{s}_{GHZ} := \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$  

(7)

Many of our results apply to two special classes of XOR games: symmetric XOR games and random XOR games.

**Definition 5.4.** A symmetric $k$-XOR game is an XOR game that additionally satisfies a clause symmetry property: for every clause $c_i = (q_i, s_i)$ in the game, the game must also contain all clauses $c'_i = (q'_i, s_i)$ where $q'_i$ is a permutation of the questions in $q_i$, and the parity bit is unchanged.

**Definition 5.5.** A random $k$-XOR game on $m$ clauses and $n$ variables is an XOR game with the $m$ clauses chosen independently at random from a uniform distribution over $[n]^k \times \{-1, 1\}$.

### 5.1 Strategies

We next introduce both classical and commuting-operator strategies and state claims regarding their value and constraints on when these strategies play perfectly given an X OR game. These claims are proved in Section 7.3. For any game, constructing a strategy and computing its value lower-bounds the value of the game. In the commuting-operator case, this is generally intractable and motivates the subsequent refutations picture.

#### 5.1.1 Classical Strategies

For any game, the optimal classical strategy can be taken to be a deterministic assignment of answers. In the case of XOR games we will see that it is natural to view this assignment as a vector in $F_2^{kn}$.

**Definition 5.6.** A deterministic classical strategy dictates that player $\alpha$ outputs $\eta(\alpha, j) \in \{-1, 1\}$ when they receive question $j$ from the verifier. Note that valid outputs must satisfy

$$\eta^2(\alpha, j) = 1.$$  

(8)

To exploit the linear algebraic picture, it is useful to define a length-$kn$ classical strategy vector $\hat{\eta} \in F_2^{kn}$ analogous to the parity bit vector. It is defined by the relation

$$\eta(\alpha, j) = (-1)^{\hat{\eta}_{h(\alpha-1)+j}} = \cos \left( \pi \hat{\eta}_{h(\alpha-1)+j} \right).$$  

(9)

Here the cos anticipates a generalization that we will see in the quantum case when we construct MERP strategies.

**Claim 5.7.** If the players play a game $G \sim (A, \hat{s})$ following strategy $\hat{\eta}$, the vector $\hat{o} = A\hat{\eta}$ determines their output, i.e. query $i$ has answer $(-1)^{\hat{o}_i}$. The value of classical strategy $\hat{\eta}$ is

$$v(G, \hat{\eta}) := \frac{1}{m} \sum_{i=1}^{m} \frac{1 + (-1)^{\hat{o}_i - \hat{s}_i}}{2} = \frac{1}{2} + \frac{1}{2m} \left( \sum_{i=1}^{m} \cos(\pi [(A\hat{\eta})_i - \hat{s}_i]) \right),$$  

(10)

where again we have used an apparently unnecessary cos, anticipating a quantum generalization. We also treat $F_2$ and $\{0, 1\}$ as equivalent here.
These observations lead to a well known procedure using Gaussian elimination to find a classical value-1 strategy or determine that no such strategy exists.

**Definition 5.8.** Define the classical constraint equations for game $G$ by

$$A\hat{\eta} = \hat{s} \tag{11}$$

over $\mathbb{F}_2$. Equivalently,

$$\prod_{\alpha=1}^{k} \eta(\alpha, q^{(\alpha)}_i) = s_i, \forall i \in [m]. \tag{12}$$

**Claim 5.9.** Every solution $\hat{\eta}$ to (11) corresponds to a strategy $\eta$ achieving value 1 on game $G \sim (A, \hat{s})$, and vice versa. In other words, a game $G$ has classical value 1 iff (11) has a solution.

When $\omega(G) < 1$, on the other hand, there does not exist an efficient algorithm for finding optimal classical strategies (assuming $P \neq NP$) \cite{18}.

### 5.1.2 Commuting-Operator Strategies

**Definition 5.10.** Consider a $k$-XOR game with $n$ variables. For each $j \in [n]$, let the Positive-Operator Valued Measure (POVM) $\{O^\alpha_1(j), O^\alpha_{-1}(j)\}$ give the $\alpha$-th player’s commuting-operator strategy upon receiving question $j$ from the verifier. These POVMs act on some shared state $|\Psi\rangle$, and different players’ POVM elements commute due to the no-communication requirement on the players.

Using the Naimark dilation theorem, we can restrict our players’ strategies to be Projection-Valued Measures (PVMs). We make this restriction for the remainder of the paper. This allows us to define the following observables.

**Definition 5.11.** Given a strategy $\{O^\alpha_1(j), O^\alpha_{-1}(j)\}$, define the strategy observable

$$O^\alpha(j) := O^\alpha_1(j) - O^\alpha_{-1}(j).$$

Since $\{O^\alpha_1(j), O^\alpha_{-1}(j)\}$ is a PVM, $O^\alpha(j)$ is a Hermitian operator. Indeed commuting-operator strategies are equivalent to imposing the constraints for $\alpha \neq \beta$

$$[O^\alpha(j), O^\beta(j')] = 0 \quad \text{(operators held by distinct players commute)} \tag{13a}$$

$$O^\alpha(j)^2 = I \quad \text{(square identity, analogous to (8))} \tag{13b}$$

The condition for commuting-operator strategies to achieve value 1 is the following generalization of (11).

**Definition 5.12.** For a $k$-XOR game $G$, define the commuting-operator constraint equations:

$$Q_i |\Psi\rangle := \left( \prod_{\alpha} O^{\alpha}(q^{(\alpha)}_i) \right) |\Psi\rangle = s_i |\Psi\rangle, \forall i \in [m] \tag{14}$$

These equations stipulate that applying the strategy observables for a given question to the shared state $|\Psi\rangle$ produces the correct output for that question.

**Claim 5.13.** A game $G$ has commuting operator value 1 iff there exists some state and strategy observables that satisfy (13) and (14).

While there is an efficient algorithm to solve the classical constraint equations, no such algorithm is known to exist for the commuting-operator constraint equations. This difficulty forces us to consider alternative techniques for characterizing the commuting-operator value of XOR games.
5.2 Refutations

In addition to lower bounding the value of a game by constructing strategies for it, we can also upper bound a game’s value by showing no high-value strategy can exist. In particular, we construct proofs that a game cannot have value 1, which we call refutations. Classically, refutations are well understood, and emerge naturally from the dual to the classical constraint equations.

Definition 5.14. Define a classical refutation \( y \in \mathbb{F}_2^n \) as any vector satisfying the equations dual to (11),

\[
\begin{bmatrix}
A^T \\
S^T
\end{bmatrix}
\begin{bmatrix}
y \\
1
\end{bmatrix} = 0
\]

where once again the algebra is over \( \mathbb{F}_2 \).

Fact 5.15. Either a classical refutation \( y \) exists satisfying (15) or a classical strategy \( \hat{\eta} \) exists satisfying (11).

The proof is standard but because dualities like Fact 5.15 play a major role in our paper, we review it here.

Proof. By the definition of \( \text{im} \) and \( \ker \), we have \( \text{im} \ A \subseteq (\ker A^T)^\perp \). The rank-nullity theorem implies that \( \dim \text{im} \ A = \dim(\ker A^T)^\perp \), meaning that in fact

\[
\text{im} \ A = (\ker A^T)^\perp.
\]

(16)

Therefore

\[
\hat{s} \not\in \text{im} \ A \iff \hat{s} \not\in (\ker A^T)^\perp \iff \exists y \in \ker A^T, \ s^T y \neq 0.
\]

(17)

Another way to view \( y \) as a refutation is by interpreting it as the indicator vector of a subset of clauses.

Recall from (12) that clause \( i \) corresponds to the equation \( \prod_{\alpha} \eta(\alpha, q_i^{(\alpha)}) = s_i \) over the variables \( \eta(\cdot, \cdot) \). If \( y \) satisfies (15) then multiplying the equations corresponding to clauses with \( y_i = 1 \) yields

\[
\prod_{i:y_i=1} \prod_{\alpha \in [k]} \eta(\alpha, q_i^{(\alpha)}) = \prod_{i:y_i=1} s_i
\]

(18)

From \( A^T y = 0 \) and (8) it follows that the LHS of (18) equals 1. From \( s^T y = 1 \) it follows that the RHS of (18) equals \(-1\). Thus the existence of \( y \) satisfying (15) means there is no \( \eta \) satisfying (12).

In this paper we consider the commuting-operator analogue of classical refutations. We would like to construct a dual to (14), meaning a characterization of certificates for the unsatisfiability of (14). As there is no analogue to the linear algebraic methods used in the classical case, we will instead attempt to generalize (18).

Cleve and Mittal [8] make use of a noncommutative generalization of (18), which they call the substitution method, to exhibit refutations of some Binary Constraint System games. We will use a similar method for XOR games in which we multiply together constraints of the form (14) to obtain a contradiction. Our contribution will be to give a simple characterization of when such refutations exist in the case of symmetric \( k \)-XOR games and in some cases, random asymmetric 3-XOR games. Indeed, our characterization will resemble the classical dual equations (15) although the route by which we obtain it is quite different.

To explain this in more detail, we introduce some definitions.

Definition 5.16. Let \( Z_1 \) and \( Z_2 \) be two operators formed from products of strategy observables. We say \( Z_1 \) is equivalent to \( Z_2 \), written \( Z_1 \sim Z_2 \), if \( Z_1 = Z_2 \) is an identity for all strategy observables satisfying (13).

Definitions 5.12 and 5.16 then motivate the definition of a (quantum) refutation, analogous to Definition 5.14. From now on, “refutation” will be a quantum refutation unless otherwise specified.

Definition 5.17. Let \( G \) be some \( k \)-XOR game with \( m \) clauses. A refutation for \( G \) is defined to be a sequence \( (i_1, i_2, \ldots, i_k) \in [m]^k \) satisfying

\[
Q_{i_1} Q_{i_2} \ldots Q_{i_k} \sim I \quad \text{and} \quad s_{i_1} s_{i_2} \ldots s_{i_k} = -1.
\]

(19)
Refutations certify that \( \omega^* < 1 \), analogous to the way that classical refutations certify that \( \omega < 1 \). In Theorem 6.1, we show that in fact any game with \( \omega^* < 1 \) has a refutation. The proof of this fact relies on a connection between refutations and the ncSoS hierarchy analogous to a connection made by Grigoriev [16] between classical refutations and the SoS hierarchy.

It is not obvious that one can find refutations more easily than one can find strategies. However, we next establish a necessary condition for a game to admit a refutation, and thus an easily-identified subclass of XOR games that certainly do not have a refutation meaning they have \( \omega^* = 1 \).

### 5.3 Games with no Parity-Permuted Refutations (noPREF Games)

noPREF games are a subclass of entangled XOR games for which it is easy to show no refutation can exist. To motivate their construction and prove some properties about them, we must first redefine refutations from a combinatorial perspective. A more complete treatment of these ideas is given in Section 6.

**Definition 5.18** (Combinatorial Construction of Refutations, informal). For a k-XOR game \( G \), consider the combinatorial version of the query \( q_i^\alpha \) to be a vector with \( k \) coordinates (the player indices) with letter \( q_i^\alpha \) at coordinate \( \alpha \). Define the set of words contained in \( G \) to be all vectors formed by concatenating the queries of \( G \) coordinate-wise (by player). The sign of a word contained in \( G \)

\[
W = q_{i_1}q_{i_2} \ldots q_{i_\ell}
\]

is defined as

\[
s_W := s_{i_1}s_{i_2} \ldots s_{i_\ell}.
\]

We will refer to each coordinate of the word as a wire. The identity \( I \) under the concatenating action is the word that is blank on every wire.

Define an equivalence relation generated by all wire-by-wire permutations of the following base relations (in this setting the product of two vectors indicates their coordinate-wise concatenation).

1. (Repeated elements cancel) : \[\begin{bmatrix} j \\ \vdots \\ j \end{bmatrix} \sim \begin{bmatrix} \vdots \\ \vdots \end{bmatrix} \quad \forall \ j \in [n]\]

2. (Elements on different wires commute) : 
\[
\begin{bmatrix} j \\ \vdots \end{bmatrix} \sim \begin{bmatrix} \vdots \\ \vdots \end{bmatrix} \quad \begin{bmatrix} j' \\ \vdots \end{bmatrix} \sim \begin{bmatrix} \vdots \\ \vdots \end{bmatrix} \quad \forall \ j, j' \in [n]
\]

A refutation is defined to be a sequence \((i_1, i_2, i_3, \ldots, i_\ell) \in [m]^\ell\) for which

\[
q_{i_1}q_{i_2} \ldots q_{i_\ell} \sim I \quad \text{and} \quad s_{i_1}s_{i_2} \ldots s_{i_\ell} = -1.
\]

We claim that this definition of a refutation is equivalent to the one given in Section 5.2. Intuitively, such a construction explicitly manipulates the operator identities required by each clause of \( G \) in a way that exploits the operator requirements of (13) to produce a refutation as in Definition 5.17. We prove this fact in Section 6. We next motivate the noPREF class of games by making the following key observation.

**Observation 5.19.** All elements contained in queries at even positions in a refutation must cancel with queries at odd positions.

To exploit this observation, we find it useful to define a broader equivalence relation \( \mathcal{L} \sim \) that allows for a parity-preserving permutation on each wire before canceling and commuting letters.

**Definition 5.20** (Informal). We say k-XOR word \( W_A \) is parity-permuted equivalent to \( W_B \)—denoted \( W_A \sim \mathcal{L} W_B \)—if \( W_A \sim W_B' \) where some permutations of the even positions and odd positions on each wire of \( W_B \) can produce \( W_B' \).

---

\(^4\) We overload the notation \( q_i \) here to indicate both the definitional and combinatorial version of a query, with the relevant meaning clear from context.
Since this is just a broadening of the equivalence given in Definition 5.18, \( W_1 \sim W_2 \implies W_1 \not\sim W_2 \).
With this equivalence relation in hand, we can state a necessary condition for the existence of a refutation of a game \( G \).

**Definition 5.21.** A game \( G \) contains a **Parity-Permuted Refutation (PREF)** if the game \( G \) contains a word which is \( \not\sim I \) with sign \(-1\).

The set of **PREF Games** are the set of XOR games that contain PREFs. The set of **noPREF Games** are the set of XOR games that do not.

**Theorem 5.22** (Necessary condition for refutation). If a game \( G \) admits a refutation, it contains a PREF.

*Proof (sketch).* This follows essentially immediately from the observation that \( \sim \) implies \( \not\sim \). \( \square \)

**Corollary 5.23.** Every noPREF game has commuting-operator value 1.

*Proof.* This follows directly from Theorem 5.22 and the completeness of refutations (Theorem 6.1). \( \square \)

The significance of noPREF games is made clear by the two following theorems. For both, a short proof sketch is given, while the full proofs are delegated to Section 6.

**Theorem 5.24** (Informal). There exists a poly-time algorithm that decides membership in the set of noPREF games.

*Proof (sketch).* The key observation here is that a game \( G \sim (A, \hat{s}) \) contains a PREF if and only if there is a solution to the set of equations

\[
A^T z = 0 \quad (23)
\]
\[
\hat{s}^T z = 1 \pmod{2} \quad (24)
\]

for some \( z \in \mathbb{Z}^m \). If (23) and (24) can be satisfied, the game \( G \) contains a PREF built by interleaving the multisets of clauses

\[
\mathcal{O} = \{ q_i \text{ with multiplicity } |z_i| \forall i : z_i > 0 \} \quad (25a)
\]
\[
\mathcal{E} = \{ q_i \text{ with multiplicity } |z_i| \forall i : z_i < 0 \} \quad (25b)
\]

such that their elements are placed in odd and even positions, respectively. The reverse direction requires a technical lemma relating the even and odd clauses of a PREF. Then standard techniques for solving linear Diophantine equations complete the proof. \( \square \)

The vector \( z \) defined in the proof of Theorem 5.24 is sometimes referred to as a PREF specification due to (25).

**Theorem 5.25** (Informal). The noPREF characterization is complete for symmetric games. That is, every value 1 symmetric game is in the noPREF set.

*Proof (sketch).* We use the structure of symmetric games to construct shuffle gadgets – short words that move letters from one wire to another when they are appended onto an existing word. We then show shuffle gadgets are sufficient to construct a refutation given a PREF contained in the game. This shows that containing a PREF is both necessary and sufficient for a symmetric game to have a refutation. Then a symmetric game is either in the set of noPREF games or has value \(<1\).

Theorems 5.24 and 5.25 together show that the class of symmetric value 1 games has a poly-time deterministic algorithm, while previously the question of whether such games took value 1 was not known to be decidable. This progress is due to the noPREF characterization of games.

Given that noPREF games form a large class of value 1 games, it is reasonable to try to construct a commuting-operator strategy to play them. We can ask if there exists a strategy dual to the PREF criteria, similar to what we have described in the classical and commuting-operator cases. In particular, we ask if a

---

\(^5\) Or a MERP refutation, for reasons described in Section 5.5.
game $G$ not satisfying (23) and (24) guarantees existence of a solution to the constraint equations indicating some simple family of strategies can achieve value 1 for $G$.

Somewhat miraculously, the answer to this question turns out to be yes. We proceed by first defining this class of strategies, then showing that their constraint equations are dual to the PREF criteria for any game.

### 5.4 Maximal Entanglement, Relative Phase (MERP) Strategies

We introduce a family of “Maximal Entanglement, Relative Phase” (MERP) strategies: a useful subfamily of the set of tensor-product (and thus commuting-operator) strategies. MERP strategies are a generalization of the GHZ strategy to arbitrary games. Crucially, determining whether a MERP strategy achieves value 1 for a game, and if so a construction for such a strategy, can be described in time polynomial in $m$, $n$, and $k$.\(^6\)

Furthermore, the conditions for a MERP strategy to achieve value 1 are dual to the PREF condition for a game, meaning MERP achieves value 1 on any noPREF game. In particular, this means MERP strategies achieve tensor-product value 1 on any symmetric XOR game with $\omega^* = 1$ (Theorem 5.25) as well as on a family of non-symmetric games (APD games, Section 8.3) with $\omega^* = 1$ and classical value $\omega \to \frac{1}{2}$.

We begin with the definition of a MERP strategy for a game $G$.

**Definition 5.26 (MERP).** Given a $k$-XOR game $G$ with $m$ clauses, a **MERP strategy** for $G$ is a tensor-product strategy in which:

1. The $k$ players share the maximally entangled state $|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle^\otimes k + |1\rangle^\otimes k)$, with player $\alpha$ having access to the $\alpha$-th qubit of the state.

2. Upon receiving question $j$ from the verifier, player $\alpha$ rotates his qubit by an angle $\theta(\alpha, j)$ about the $Z$ axis, then measures his qubit in the $X$ basis and sends his observed outcome to the verifier.

Explicitly, we define the states $|\theta(\alpha, j)\pm\rangle := \frac{1}{\sqrt{2}} (|0\rangle \pm e^{i\theta(\alpha, j)} |1\rangle)$ and pick strategy observables $O^\theta(j) := |\theta(\alpha, j)_+\rangle\langle\theta(\alpha, j)_+| - |\theta(\alpha, j)_-\rangle\langle\theta(\alpha, j)_-|$.\(^\text{(28)}\)

There exists a useful parallel between MERP strategies and classical strategies, which we summarize below. Almost identically to the classical value (10),

**Claim 5.27.** Let the length-$kn$ **MERP strategy vector** for a given MERP strategy be defined by

\[ \hat{\theta}_{(\alpha-1)n+j} := \frac{1}{\pi} \theta(\alpha, j). \]

The value achieved by that MERP strategy on game $G$ is:

\[ v^{\text{MERP}}(G, \hat{\theta}) := \frac{1}{2} + \frac{1}{2m} \left( \sum_{i=1}^{m} \cos \left( \pi \left[ (A\hat{\theta})_i - \hat{s}_i \right] \right) \right). \]

**Proof.** Explicit calculation. Done in full in Section 7.2.\(\square\)

Claim 5.27 allows us to write down the constraint equations for MERP strategies to achieve $v^{\text{MERP}} = 1$.\(^\text{6}\) For symmetric games, $m \sim \exp\{k\}$, so in this case one can decide MERP value 1 and describe a strategy in time polynomial in $m$ and $n$.\(^\text{6}\)
Definition 5.28. Define the MERP constraint equations for game $G$ by

$$A\hat{\theta} = \hat{s} \pmod{2}$$

(31)

with $\hat{\theta} \in \mathbb{Q}^{kn}$.

(We could have equivalently required $\hat{\theta}$ to be in $\mathbb{R}^{kn}$. This is because $A, \hat{s}$ have integer entries and so any real solution to (31) will also be rational.)

Claim 5.29. A MERP strategy achieves $v^{\text{MERP}} = 1$ on a game $G$ iff its MERP constraint equations have a solution. A solution $\hat{\theta}$ corresponds to the MERP strategy in which player $\alpha$ uses $\theta(\alpha, j) = \pi\hat{\theta}_{(\alpha-1)n+j}$.

Intuitively, MERP provides an explicit construction allowing players to return an arbitrary phase on each input, rather than the classical 0 or $\pi$. The MERP constraint equations then ensure that for each question the returned phases sum to $\pi\hat{s}_i$ up to multiples of $2\pi$. For any game, Claim 5.29 allows us to efficiently determine whether some MERP strategy achieves value 1 via Gaussian elimination over $\mathbb{Q}$. We often refer to this optimal MERP strategy for a game $G$ as simply the MERP strategy for $G$.

5.5 MERP - PREF Duality

The set of games for which MERP achieves value 1 is exactly the set noPREF. As in the classical and commuting-operator cases, the MERP constraint equations (31) are dual to the PREF conditions:

Theorem 5.30. For any game $G$, either there exists a PREF specification, or a MERP strategy with value 1.

Proof. Technical proof in the style of a Theorem of Alternatives, analogous to Fact 5.15. See Section 7.3. $\square$

Because of Theorem 5.30 we also refer to a PREF specification $z$ as a MERP refutation.

Figure 1 summarizes the extensions of the classical duality relations presented in this paper. The general quantum duality provides a complex but complete description of games with $\omega^* = 1$. The PREF conditions are efficient to compute, but are only necessary conditions for constructing commuting-operator refutations, and thus the dual, MERP value 1, holds true for only a subset of all $\omega^* = 1$ games. We can make a stronger statement about symmetric games: PREFs are both necessary and sufficient for a symmetric game to have a refutation, so the duality ensures MERP achieves value 1 for all symmetric games with $\omega^* = 1$.

5.6 Implications

Finally we can use our main results to analyze some particular families of games and partially characterize the XOR game landscape.

In the $\omega^* = 1$ regime, we construct a family of games that generalize the GHZ game, termed the Asymptotically Perfect Difference (APD) family. Members are parameterized by scale $K$, with the $K$-th member having $k = 2^K - 1$ players, and $K = 2$ reproducing GHZ. The APD family is contained in the noPREF set ($\omega^* = 1$) and has perfect difference in the asymptotic limit,

$$\lim_{K \to \infty} 2(\omega^* - \omega) = 1.$$  

(32)

This demonstrates that XOR games include a subset for which (at least asymptotically) the best classical strategy is no better than random while a tensor-product strategy (MERP) can play perfectly. Details of this construction are given in Section 8.3. We also give, in Section 8.1, the construction for a (nonsymmetric) game for which $\omega^* = 1$ but which falls outside the noPREF set, which shows the incompleteness of the PREF criteria.

To study the $\omega^* < 1$ regime, we consider the behavior of randomly generated XOR games with a large number of clauses. We prove Theorem 2.6 by explicitly constructing a refutation for such games using insights developed in previous sections. Interestingly, we also show such games have a minimal length refutation that

\footnote{Despite the language, we do not wish to suggest that there is a single optimal MERP strategy. Instead one should imagine some convention being used to specify a unique MERP strategy from the set of optimal ones.}
Figure 1: We extend the well-understood duality relation for classical XOR games (left) to a more complex set of dualities characterizing perfect strategies for entangled XOR games (right). The arrows indicate implications, with the red, unfilled arrows holding for symmetric games only. The dashed red arrows follow from the other arrows for symmetric games.

scales like $\Omega(n \log(n)/\log(\log(n)))$, which implies that it takes the ncSoS algorithm superexponential time to show that these games have $\omega^* < 1$ (Lemma 6.4 and Theorem 2.7). These results can be seen as quantum analogues of Grigoriev’s [16] integrality gap instances for classical XOR games. Finally, we try to push the potentially superexponential runtime of ncSoS to its extremes. We demonstrate a family of symmetric games, called the Capped GHZ family, that provably have $\omega^* < 1$, but have minimum refutation length exponential in the number of clauses (Section 8.2). For games in this family the ncSoS algorithm requires time doubly exponential to prove that their commuting-operator value is $< 1$ while the noPREF criterion can be used to conclude this fact in polynomial time.

6 Refutations

Refutations are a powerful tool for differentiating between XOR games with perfect commuting-operator strategies ($\omega^* = 1$) and those with $\omega^*$ bounded away from 1. In Section 6.1, we prove Theorem 6.1 and Theorem 6.2, relating refutations to the commuting-operator value of XOR games:

**Theorem 6.1.** An XOR game $G$ has commuting-operator value $\omega^*(G) = 1$ if and only if it admits no refutations.

**Theorem 6.2.** Let $G$ be an XOR game consisting of $m$ queries, with $G$ yielding a length-$\ell$ refutation. The commuting-operator value of the game is bounded above by

$$\omega^*(G) \leq 1 - \frac{\pi^2}{4m\ell^2}. \quad (33)$$

Informally, Theorem 6.1 gives completeness and soundness of refutations when used as a proof system for checking if a game has $\omega^* < 1$. Theorem 6.2 improves the soundness.

We previously introduced the notion of the combinatorial view of refutations (Definition 5.18) and containing a PREF as a necessary condition for a game to have a refutation (Corollary 5.23). Section 6.2 presents the combinatorial view in more detail, and proves that a PREF specification and existence of a particular
set of “shift gadgets” is a sufficient condition for a refutation to exist. Finally, Section 6.3 demonstrates that for symmetric XOR games, all desired “shift gadgets” are automatically available, meaning that a refutation exists if and only if a PREF specification exists, thus providing an efficient technique to decide whether any symmetric XOR game has perfect commuting-operator value.

6.1 Upper Bound on Value

We begin by proving Theorem 6.1. The main tool we use is the non-commuting Sum of Squares (ncSoS) hierarchy, also known as the NPA hierarchy [22, 10]. Given a game \( G \), each level in the ncSoS hierarchy is a semidefinite program depending on \( G \) whose solution gives an upper bound on the value \( \omega^*(G) \); higher levels correspond to larger semidefinite programs and tighter upper bounds. While we refer the reader to the references cited above for a full description, we include here a definition of the key object used in constructing the hierarchy: the pseudoexpectation operator.

**Definition 6.3.** Given an XOR game \( G \), a degree-\( d \) pseudoexpectation operator or pseudodistribution is a linear function \( \tilde{E} [\cdot] \) that maps formal polynomials of degree at most \( d \) over the strategy observables \( O^\alpha(j) \) to complex numbers. A pseudoexpectation \( \tilde{E} [\cdot] \) is valid if

- for all polynomials \( p \) of degree at most \( d/2 \), \( \tilde{E} [p^\dagger p] \geq 0 \),
- for all polynomials \( p_1, p_2 \) with \( \deg(p_1 p_2) \leq d - 2 \) and indices \( \alpha \in [k] \) and \( j \in [n] \),
  \[
  \tilde{E} \left[ p_1 \left\{ (O^\alpha(j))^2 - I \right\} p_2 \right] = 0. \tag{34}
  \]
- for all polynomials \( p_1, p_2 \) with \( \deg(p_1 p_2) \leq d - 2 \) and indices \( \alpha \neq \alpha' \in [k] \) and \( j, j' \in [n] \),
  \[
  \tilde{E} \left[ p_1 \left\{ O^\alpha(j)O^{\alpha'}(j') - O^{\alpha'}(j')O^\alpha(j) \right\} p_2 \right] = 0. \tag{35}
  \]

Intuitively speaking, these requirements state that any algebraic manipulations allowed by (13) are also allowed under the pseudoexpectation, as long as they never result in a polynomial of degree greater than \( d \). We further say that a pseudoexpectation satisfies a clause \( c_i = (q_i, s_i) \) if for all polynomials \( p_1, p_2 \) with degrees summing to \( \leq d - k \), \( \tilde{E} [p_1(Q_i - s_i I) p_2] = 0 \).

The full ncSoS algorithm involves optimizing over all valid pseudoexpectation operators that satisfy clauses in the game; it can be shown that this optimization reduces to a semidefinite program in matrices whose dimension is the number of monomials of degree at most \( d/2 \) in the observables \( O^\alpha(j) \). In the special case of determining whether the game value is 1, it reduces to checking for the existence of such a pseudoexpectation operator.

In [16], Grigoriev showed a connection between refutations of classical games and pseudodistributions which appear to satisfy all clauses of a classical XOR game. In our analysis, we will adapt some of these arguments to the quantum setting. In particular, Lemma 6.4 gives a quantum analogue of Grigoriev’s central insight that, in the special case of deciding whether the game value is 1, the sum-of-squares hierarchy reduces to checking for the existence of a refutation.

In addition to being key to the proof of Theorem 6.1, Lemma 6.4 also gives a bound on the time it takes the ncSoS algorithm to show a XOR game has value \( \leq 1 \) in terms of the minimum length refutation admitted by the game.

**Lemma 6.4.** For any \( k \)-XOR game \( G \) with no refutation of length \( \leq 2\ell \) there exists a degree-\( k\ell \) pseudodistribution whose pseudoexpectation satisfies every clause in \( G \). Consequently, it takes time at least \( \Omega((nk)^{k\ell}) \) for the ncSoS algorithm to prove \( \omega^*(G) \neq 1 \).

**Proof.** To construct this pseudodistribution, we follow a procedure of Grigoriev [16]. For each clause \( c_i = (q_i, s_i) \), define

\[
\tilde{E} [Q_i] = \tilde{E} \left[\prod_\alpha O^\alpha(q_i^{(\alpha)}) \right] := s_i, \tag{36}
\]

Proof. To construct this pseudodistribution, we follow a procedure of Grigoriev [16]. For each clause \( c_i = (q_i, s_i) \), define

\[
\tilde{E} [Q_i] = \tilde{E} \left[\prod_\alpha O^\alpha(q_i^{(\alpha)}) \right] := s_i, \tag{36}
\]
and for any word\(^8\) \(w\) which can be obtained as a product of \(N \leq \ell\) queries,

\[
w := \prod_{x=1}^{N} Q_{i_x},
\]

(37)

define the pseudoexpectation of \(w\) to be the product of the parity bits \(s_{i_x}\) associated with each query \(Q_{i_x}\) in the operator construction:

\[
\tilde{E}[w] := \prod_{x=1}^{N} s_{i_x}.
\]

(38)

We need to argue that this prescription is well-defined, i.e. that (37) and (38) never assign two different values to the same \(\tilde{E}[w]\). Suppose to the contrary that \(w = \prod_{x \in [M]} Q_{i_x} = \prod_{y \in [N]} Q_{j_y}\) with \(M, N \leq \ell\) but that \(\prod_{x \in [M]} s_{i_x} = \prod_{y \in [N]} s_{j_y}\). Since (38) can only take on the values \(\pm 1\) we have \(\prod_{x \in [M]} s_{i_x} \cdot \prod_{y \in [N]} s_{j_y} = -1\). Also each \(Q_i\) is Hermitian, so

\[
1 = w w^\dagger = Q_{i_1} \cdots Q_{i_N} Q_{j_M} \cdots Q_{j_1}.
\]

(39)

This constructs a refutation of length \(M + N \leq 2\ell\), contradicting our hypothesis that no such refutation exists. We conclude that \(\tilde{E}[w]\) is well-defined for the choices of \(w\) resulting from (37).

For all other words (i.e. those that cannot be obtained as products of queries or have length \(> \ell\)), set their pseudoexpectation to 0. Finally, extend the definition by linearity to sums and scalar multiples of operator products.

Moreover, \(\tilde{E}[\cdot]\) induces an equivalence relation on words: we say that words \(w_a \tilde{\sim} w_b\) if \(\tilde{E}[w_a^\dagger w_b] \neq 0\). This relation therefore partitions the set of words into equivalence classes \(C_1, C_2, \ldots\). We pick a representative element \(w_i\) for each class \(C_i\). A key feature of the equivalence relation is that for \(w_a, w_b \in C_i\),

\[
w_a \tilde{\sim} w_b \implies \tilde{E}[w_a^\dagger w_b] = \tilde{E}[w_i^\dagger w_i] \tilde{E}[w_i^\dagger w_b].
\]

(40)

To show that \(\tilde{E}[\cdot]\) is a pseudodistribution, it suffices to show that for any polynomial \(p\) of degree at most \(k\ell/2\) in the operators \(O^a(j), \tilde{E}[p^\dagger p] \geq 0\). Group the monomials in \(p\) according to the equivalence classes, so that \(p = p_1 + p_2 + \ldots\) where each \(p_i\) is a sum of terms from equivalence class \(C_i\). It follows that

\[
\tilde{E}[p^\dagger p] = \sum_i \sum_j \tilde{E}[p_i^\dagger p_j] = \sum_i \tilde{E}[p_i^\dagger p_i].
\]

(41)

So we have reduced the problem to showing that \(\tilde{E}[q^\dagger q] \geq 0\) for any polynomial \(q\), all of whose terms belong to the same equivalence class. Write \(q\) as a linear combination of words in equivalence class \(C_i\),

\[
q = \alpha_1 w_1 + \cdots + \alpha_s w_s.
\]

(42)

Then

\[
\tilde{E}[q^\dagger q] = \tilde{E} \left[ \sum_{a,b=1}^{s} \alpha_a^* \alpha_b w_a^\dagger w_b \right]
\]

(43)

\[
= \sum_{a,b=1}^{s} \alpha_a^* \alpha_b \tilde{E}[w_a^\dagger w_b]
\]

(44)

\[
(40) = \sum_{a,b=1}^{s} \alpha_a^* \alpha_b \left( \tilde{E}[w_a^\dagger w_a] \right)^\dagger \tilde{E}[w_a^\dagger w_a]
\]

(45)

\[
= \sum_{a} \alpha_a \tilde{E}[w_a^\dagger w_a]^2
\]

(46)

\[
\geq 0.
\]

(47)

\(^8\) In this context, we borrow this terminology from the combinatorial picture to indicate any product of strategy observables.
The existence of this pseudodistribution implies that the ncSoS algorithm would need to run to level at least \( k\ell \) in the ncSoS hierarchy to show \( G \) has commuting-operator value \( < 1 \). This can be converted to a lower bound on the runtime by standard results in semidefinite programing.

Finally, we state and prove the duality between refutations and \( \omega^* = 1 \).

**Theorem 6.1 (restated).** An XOR game \( G \) has commuting-operator value \( \omega^*(G) = 1 \) if and only if it admits no refutations.

**Proof.** In one direction, Definition 5.12 immediately implies that if the game has commuting value 1, then there are no refutations.

In the other direction, suppose there are no refutations. Then, by Lemma 6.4 and taking \( \ell \to \infty \) we see there exists a pseudodistribution under which every clause is satisfied, and this pseudodistribution satisfies the constraints of all levels of the ncSoS hierarchy [22]. Since it is known that the ncSoS hierarchy converges to the commuting value of the game, it follows that this value is 1. \( \square \)

Classical refutations prove that a constraint satisfaction problem is not feasible, and so if there are \( m \) constraints they trivially yield an upper bound of \( 1 - 1/m \). In the commuting-operator case, even this statement is not obvious. In particular, one could worry that a game with a quantum refutation still admits a sequence of commuting-operator strategies with limiting value 1.

However, here we prove Theorem 6.2, showing that even in the commuting-operator case, refutations yield explicit upper bounds on \( \omega^*(G) \) that are strictly less than 1. An argument similar to the one presented here was known previously, and used to derive a comparable result in Section 5 of [8].

**Theorem 6.2 (restated).** Let \( G \) be an XOR game consisting of \( m \) queries, with \( G \) yielding a length-\( \ell \) refutation. The commuting-operator value of the game is bounded above by

\[
\omega^*(G) \leq 1 - \frac{\pi^2}{4m\ell^2}. \tag{48}
\]

**Proof.** Recall from Definition 5.12 that the Hermitian operator \( Q_i \) is defined for some XOR game \( G \), and represents the collective measurements made by the players upon receiving query \( q_i \). It has eigenvalues \( \pm 1 \), which correspond to the value of the XOR’d bit received by the verifier. Define \( \tilde{Q}_i := s_i Q_i \), so the 1 eigenspace of \( \tilde{Q}_i \) corresponds to measurement outcomes on which the players win the game given query \( q_i \), and the \(-1\) eigenspace corresponds to measurement outcomes on which the players lose the game. Let \( (i_1, i_2, \ldots, i_\ell) \) be the assumed refutation for \( G \). Letting \( |\Psi\rangle \) be the state shared by the players, we have

\[
\tilde{Q}_{i_1} \tilde{Q}_{i_2} \cdots \tilde{Q}_{i_\ell} |\Psi\rangle = (s_{i_1} s_{i_2} \cdots s_{i_\ell}) Q_{i_1} Q_{i_2} \cdots Q_{i_\ell} |\Psi\rangle = -1 |\Psi\rangle. \tag{49}
\]

On the other hand, if we let \( P_i = \frac{1 - \tilde{Q}_i}{2} \) be the projector on to the \(-1\) eigenspace of \( \tilde{Q}_i \), then the losing probability is

\[
\delta := \frac{1}{m} \sum_{i=1}^{m} \text{Tr} \left[ P_i |\Psi\rangle \langle \Psi| \right] \tag{50}
\]

We now follow an argument similar to the union bound proof of [14]. Let \( \angle(|\alpha\rangle, |\beta\rangle) = \arccos |\langle \alpha | \beta \rangle| \) and observe that it satisfies the triangle inequality, i.e. \( \angle(|\alpha\rangle, |\gamma\rangle) \leq \angle(|\alpha\rangle, |\beta\rangle) + \angle(|\beta\rangle, |\gamma\rangle) \). Then

\[
\pi \leq \sum_{x=1}^{\ell} \angle \left( |\Psi\rangle, Q_{i_x} |\Psi\rangle \right) \quad \text{Note that } Q_{i_x} \text{ is unitary.} \tag{51}
\]

\[
= \sum_{x=1}^{\ell} \arccos \left( 1 - 2 \text{Tr} \left[ P_{i_x} |\Psi\rangle \langle \Psi| \right] \right) \tag{52}
\]

\[
\leq \sum_{x=1}^{\ell} 2 \sqrt{\text{Tr} \left[ P_{i_x} |\Psi\rangle \langle \Psi| \right]} \tag{53}
\]

\[
\leq 2 \sum_{x=1}^{\ell} \sqrt{m\delta} \tag{54}
\]

\[
= 2\ell \sqrt{m\delta}. \tag{55}
\]
6.2 Tools for Constructing Refutations

Having demonstrated the utility of refutations, we return to the combinatorial picture of refutations and prove necessary and sufficient conditions for an XOR game to contain a refutation.

6.2.1 Combinatorics

We now formally reintroduce $k$-XOR games from a combinatorial standpoint. Several definitions mirror those in Section 5.2 but are presented here in a slightly different form to enable discussion of combinatorial proofs.

**Definition 6.5.** A $k$-XOR game on $m$ clauses with $n$ questions is defined to be a set of $m_k$-tuples, consisting of elements of $[n]$, with $m$ associated parity bits. An individual $k$-tuple is called a query, and is denoted by

$$q_i = \begin{bmatrix} q_i^{(1)} \\ q_i^{(2)} \\ \vdots \\ q_i^{(k)} \end{bmatrix}.$$  

**Definition 6.6.** A word $W$ on alphabet $[n]$ is a $k$-tuple of the form

$$W = \begin{bmatrix} w_{i_1}^{(1)} \ w_{i_2}^{(1)} \cdots w_{i_\ell}^{(1)} \\ w_{i_1}^{(2)} \ w_{i_2}^{(2)} \cdots w_{i_\ell}^{(2)} \\ \vdots \\ w_{i_1}^{(k)} \ w_{i_2}^{(k)} \cdots w_{i_\ell}^{(k)} \end{bmatrix}$$

with all $w_{ij} \in [n]$. Each row of $W$ is referred to as a wire of the word, and the $\alpha$-th row is sometimes denoted by $W^{(\alpha)}$. When all wires have length $\ell$, (so $\ell_1 = \ell_2 = \cdots = \ell_k = \ell$) we say $W$ has length $\ell$.

The product of two words is defined to be their coordinate-wise concatenation. The notation $q_{i_1} q_{i_2} \cdots q_{i_\ell}$ then refers to the length $\ell$ word given by

$$q_{i_1} q_{i_2} \cdots q_{i_\ell} = \begin{bmatrix} q_{i_1}^{(1)} \ q_{i_2}^{(1)} \cdots q_{i_\ell}^{(1)} \\ q_{i_1}^{(2)} \ q_{i_2}^{(2)} \cdots q_{i_\ell}^{(2)} \\ \vdots \\ q_{i_1}^{(k)} \ q_{i_2}^{(k)} \cdots q_{i_\ell}^{(k)} \end{bmatrix}. $$

Finally, define the identity word $I$ to be the empty $k$-tuple, which satisfies

$$IW = IW = W$$

for any word $W$.

**Definition 6.7.** A game $G$ contains a word $W$ with sign $s_W \in \{\pm 1\}$ if

$$W = q_{i_1} q_{i_2} \cdots q_{i_\ell} \text{ and } s_W = s_{i_1} s_{i_2} \cdots s_{i_\ell},$$

for some $(i_1, i_2, \ldots, i_\ell) \in [m]^{\ell}$.

**Definition 6.8.** Relations are used to express equivalence between words. There are two basic types (shown here for 3-XOR, and defined analogously for $k$-XOR).
1. (Commute Relations):
\[
\begin{bmatrix}
j \\
j' \\
j''
\end{bmatrix} \sim \begin{bmatrix}
j'' \\
j' \\
j
\end{bmatrix} \sim \begin{bmatrix}
j' \\
j'' \\
j
\end{bmatrix} \sim \begin{bmatrix}
j'' \\
j \\
j'
\end{bmatrix} \quad \forall j,j',j'' \in [n]
\] (62)

2. (Cancellation Relations):
\[
\begin{bmatrix}
j^2
\end{bmatrix} \sim \begin{bmatrix}
j^2
\end{bmatrix} \sim \begin{bmatrix}
j^2
\end{bmatrix} \sim I \quad \forall j \in [n]
\] (63)

The relationship property is associative (as suggested by the notation), so more complicated equivalences can be constructed by concatenating the ones above.

**Definition 6.9.** Given a k-XOR game \( G \), a length \( \ell \) refutation for that game is a length \( \ell \) word \( W \) contained in \( G \) with sign \(-1\) and
\[
W \sim I.
\] (64)

### 6.2.2 PREFs and Shuffle Gadgets

The key difference between entangled and classical strategies is that in the entangled case, the strategy observables do not all commute with each other. In other words, strings of queries can be acted on nontrivially by permutations. In this section we consider equivalence under a restricted class of parity-preserving permutations, and use the fact that at least one element of a class equivalent to some refutation must be contained in a game for it to admit a refutation, giving a tractable necessary condition for a refutation to exist. We then define gadgets that perform these permutations while preserving the associated parity bits. The result will be a useful set of sufficient conditions for a refutation to exist.

We recall the formal definitions related to these equivalence classes.

**Definition 5.20 (repeated).** Given two 1-XOR words \( W_1, W_2 \), we say that \( W_1 \) is parity-permuted equivalent to \( W_2 \)—denoted \( W_1 \overset{p}{=} W_2 \)—if there exists a permutation \( \pi \) mapping even indices to even indices and odd indices to odd indices such that \( W_1 \sim \pi(W_2) \).

For k-XOR words \( W_A, W_B \), we say \( W_A \overset{p}{\sim} W_B \) if \( W_A^{(\alpha)} \overset{p}{\sim} W_B^{(\alpha)} \) for all \( \alpha \in [k] \).

From the definition, we see that \( \overset{p}{=\sim} \) is necessary for \( \sim \), i.e.
\[
W_1 \sim W_2 \implies W_1 \overset{p}{=} W_2.
\] (65)

We can then conclude that a game \( G \) contains a refutation only if it contains a word \( W \overset{p}{=} I \) with sign \(-1\). To make this necessary condition more useful to us, we will move from an operational definition of the \( \overset{p}{=} \) relation to a structural one. This is done by talking about the even and odd subsets of a given word. The relevant definitions are given below.

**Definition 6.10.** Two multisets of queries \( \mathcal{T}_1 \) and \( \mathcal{T}_2 \) are said to be multiplicity equivalent if all player-question combinations occur with the same multiplicity in both sets. That is, \( \mathcal{T}_1 \) and \( \mathcal{T}_2 \) are multiplicity equivalent iff
\[
\left| \left\{ q \in \mathcal{T}_1 : q^{(\alpha)} = j \right\} \right| = \left| \left\{ q' \in \mathcal{T}_2 : q'^{(\alpha)} = j \right\} \right| \quad \forall \alpha, j.
\] (66)

**Definition 6.11.** Given a word contained in a game \( G \)
\[
W = q_1 q_2 \ldots q_x
\] (67)
define its even and odd multisets \( \mathcal{E} \) and \( \mathcal{O} \) in the natural way, so \(^9\)
\[
\mathcal{E} := \biguplus_{x \text{ even}} q_x \quad \text{and} \quad \mathcal{O} := \biguplus_{x \text{ odd}} q_x.
\] (68)

\(^9\) Here and beyond we use the multiset operation \( \biguplus \) to indicate union with addition of multiplicities. When applied to single elements we mean to treat each element as a single-element multiset.
The key feature of the multiplicity equivalence condition is that a word contained in a game $G$ is \( \triangleq I \) iff its even and odd multisets are multiplicity equivalent. A slightly more general form of this statement is proved below.

**Lemma 6.12.** Given two words $W_1$ and $W_2$ contained in $G$, the following are equivalent:

1. $W_1 \triangleq W_2$.
2. The even and odd multisets of the word $W_1W_2^{-1}$ are multiplicity equivalent.

**Proof.** This proof is easiest if we generalize from the concept of even and odd multisets of clauses to even and odd multisets of variable-player combinations. In particular, given a word $W$ (not necessarily contained in a game $G$), its even and odd variable multisets are defined by

\[
\mathcal{E}'(W) := \bigcup_{i \text{ even, } \alpha} (w_{i, \alpha}, \alpha) \quad (69)
\]

\[
\mathcal{O}'(W) := \bigcup_{i \text{ odd, } \alpha} (w_{i, \alpha}, \alpha) \quad (70)
\]

where the tuple notion tracks the fact that variables given to different players are treated as distinct. To prove Lemma 6.12, we must now claim some basic facts about $\mathcal{E}'$ and $\mathcal{O}'$.

(A) For a word $W$ contained in $G$, the even and odd multisets of $W$ are multiplicity equivalent iff

\[
\mathcal{E}'(W) = \mathcal{O}'(W). \quad (71)
\]

(B) Applying a parity preserving permutation to a word $W$ does not change $\mathcal{E}'(W)$ or $\mathcal{O}'(W)$.

(C) For any two words $W_1 \sim W_2$, we have

\[
\mathcal{E}'(W_1) \sqcup \mathcal{O}'(W_2) = \mathcal{E}'(W_2) \sqcup \mathcal{O}'(W_1). \quad (72)
\]

Claims (A) and (B) come directly from the definition of $\mathcal{E}'$ and $\mathcal{O}'$. To prove claim (C) we consider two words $W_1 \sim W_2$. If we never used a cancellation relation, we would immediately have

\[
\mathcal{E}'(W_1) = \mathcal{E}'(W_2) \text{ and } \mathcal{O}'(W_1) = \mathcal{O}'(W_2). \quad (73)
\]

Now a cancellation on a word always occurs between an element at an even position and one at an odd one, that is, it removes elements equally from $\mathcal{E}'$ and $\mathcal{O}'$. Letting $C_1$ be the multiset of elements removed from $\mathcal{E}'(W_1)$ (and equivalently $\mathcal{O}'(W_1)$) by cancellation, with $C_2$ defined similarly for $W_2$, we find

\[
(\mathcal{E}'(W_1) \setminus C_1) \sqcup (\mathcal{O}'(W_2) \setminus C_2) = (\mathcal{E}'(W_2) \setminus C_2) \sqcup (\mathcal{O}'(W_1) \setminus C_1) \quad (74)
\]

\[
\iff \mathcal{E}'(W_1) \sqcup \mathcal{O}'(W_2) = \mathcal{E}'(W_2) \sqcup \mathcal{O}'(W_1). \quad (75)
\]

Now, to prove Lemma 6.12 we note

\[
W_1 \triangleq W_2 \quad (76)
\]

\[
\iff \exists \text{ parity preserving } \pi : \pi(W_1) \sim W_2 \quad (77) \text{ (definition)}
\]

\[
\iff \mathcal{E}'(\pi(W_1)) \sqcup \mathcal{O}'(W_2) = \mathcal{E}'(W_2) \sqcup \mathcal{O}'(\pi(W_1)) \quad (C) \quad (78)
\]

\[
\iff \mathcal{E}'(W_1) \sqcup \mathcal{O}'(W_2) = \mathcal{E}'(W_2) \sqcup \mathcal{O}'(W_1) \quad (B) \quad (79)
\]

\[
\iff \mathcal{E}'(W_1W_2^{-1}) = \mathcal{O}'(W_1W_2^{-1}) \quad (\text{reordering word}) \quad (80)
\]

\[
\iff \text{The even and odd subsets of } W_1W_2^{-1} \text{ are multiplicity equivalent.} \quad (A) \quad (81)
\]

(80) is a somewhat subtle step, but follows formally (for example) from a proof by cases considering even and odd length words $W_1$ and $W_2$ and noting that the length of $W_1$ and $W_2$ must be equivalent mod 2. □
Definition 5.21 (restated). A game G contains a Parity-Permuted Refutation (PREF) if the queries of the game can be combined to form two multiplicity equivalent multisets for which the parity bits corresponding to the queries multiply to $-1$. Equivalently (Lemma 6.12), the game G contains a word which is $\triangleleft I$ with sign $-1$.

The set of PREF Games are the set of XOR games that contain PREFs. The set of noPREF Games are the set of XOR games that do not.

We can finally restate and prove our necessary condition formally:

Theorem 5.22 (restated) (Necessary condition for refutation). If a game G admits a refutation, it contains a PREF.

Proof. By definition, a refutation $R$ admitted by game $G$ must be $\sim I$ and therefore $R \triangleleft I$. $R$ must also have sign $-1$. By Definition 5.21, game $G$ then contains a PREF.

Phrasing this necessary condition in terms of even and odd multiplicity equivalent multisets then provides an efficient means of computing whether or not a game satisfies this PREF criterion (Section 6.3).

----------------

We next consider the structural requirements on refutations to derive a stronger condition that is sufficient for a game to admit a refutation. As a first step we show that we can map between words which are $\triangleleft$ to each other using a restricted class of permutations.

Lemma 6.13. Let $W = w_1 w_2 \ldots w_{2\ell}$ be a 1-XOR word of even length such that $W \triangleleft I$; i.e. there exists a parity-preserving permutation $\pi \in S_{2\ell}$ such that $\pi(W) \sim I$. Then there exists a permutation $\pi' \in S_{2\ell}$, also satisfying $\pi'(W) \sim I$, also parity-preserving, and with an additional “pair preserving” property. This means that it permutes the pairs $(1, 2), (3, 4), \ldots, (2\ell - 1, 2\ell)$ without separating or reordering the elements in each pair:

$$\pi'(2i - 1) = \pi'(2i) - 1 \quad \forall i \in [\ell].$$

Proof. Every letter in $\pi(W)$ will cancel with a unique other letter. We call a letter even or odd based on the parity of its location in $\pi(W)$. Deleting a canceled pair does not change the parity of any other location, and $\pi$ also preserves the parities. Thus the letter in location $2i$ will cancel a letter in some odd position, which we call $2f(i) - 1$ (i.e. $w_{2i} = w_{2f(i)-1}$). Since each odd letter cancels exactly one even letter, $f$ is a permutation of $[\ell]$. Next we decompose $f$ into disjoint cycles: $f = (i_1, i_2, \ldots, i_{\ell})(i_{\ell+1}, \ldots, i_2)\ldots(i_{\ell+1}, \ldots, i_{\ell})$ where $\ell_c = \ell$. We claim that, written in two-line notation,

$$t' := \begin{pmatrix} 1 & 2 & \ldots & \ell_c \\ i_1 & i_2 & \ldots & i_{\ell_c} \end{pmatrix}$$

is a permutation of the pairs satisfying the desired properties. This map from $f$ to $t'$ is known as the Foata correspondence. Let $\pi'$ be the corresponding pair-preserving permutation of $[2\ell]$. Then

$$\pi'(w) = w_{2i_1-1} w_{2i_1} w_{2i_2-1} w_{2i_2} \cdots w_{2i_{\ell_c}-1} w_{2i_{\ell_c}} w_{2i_{\ell_c+1}-1} \cdots w_{2i_2}.$$  

We can see that $\pi'(w)$ fully cancels following the pattern marked by the square brackets, with each cancellation using the fact that $w_{2i} = w_{2f(i)-1}$.

A pair (and hence parity) preserving permutation $\pi' \in S_{2\ell}$ can be specified uniquely by some $\pi \in S_\ell$, given the relation

$$\pi(i) = \pi'(2i)/2.$$  

We will frequently use of this alternate description of pair-preserving permutations, in a way made formal in Definition 6.18.

Before introducing this formally, we will the concept of a shuffle.
Definition 6.14. A function $f: [\ell] \rightarrow [\ell]$ is called a shuffle function if the sequence
\[
f^{-1}(1), f^{-1}(2), \ldots, f^{-1}(\ell)
\]
can be partitioned into two increasing subsequences. That is, for any shuffle function $f$, there exist disjoint increasing sequences $s_A$ and $s_B$ with $|s_A| + |s_B| = \ell$ and $f^{-1}$ increasing on $s_A$ and $s_B$.

Operationally, the set of shuffle functions are the set of permutations which can be obtained by partitioning the elements of $[\ell]$ into two sets, considering those sets as increasing sequences, and then mixing those sequences using a dovetail (riffle) shuffle.

Definition 6.15. Let $A$ be an arbitrary set, and let $t = (a_1, a_2, \ldots, a_\ell)$ be a sequence consisting of elements of $A$. Define the set of shuffles of $t$
\[
\text{shuffle}(t) := \{(a_{f(1)}, a_{f(2)}, \ldots, a_{f(\ell)}): f \text{ a shuffle function}\}
\]
and let this function act on sets in the natural way, so
\[
\text{shuffle}(T) := \bigcup_{t \in T} \text{shuffle}(t)
\]
where $T \subseteq A^*$ and $A^* = \bigcup_{n \geq 0} A^n$ is the set of all sequences of elements of $A$.

Shuffles are a subset of the set of permutations. However, a standard result \cite{2} regarding dovetail shuffles states that any permutation can be expressed as a short sequence of dovetail shuffles. Since our definition of shuffles contains a choice of partition that generalizes dovetail shuffles, the same result applies to our family of shuffles.

Lemma 6.16 (Theorem 1 of \cite{2}). Let $t$ be any sequence of length $\ell$, $p \geq \lceil \log(\ell) \rceil$, and let $t'$ be any permutation of $t$. Then
\[
t' \in \text{shuffle}^p(t).
\]

Our next goal is constructing a gadget from $k$-XOR clauses that allows us to shuffle pairs of letters on any wire of a word without changing the overall parity bit. The construction of this gadget relies on a simpler “shift gadget” which allows us to move words between wires. This definition and construction are given below.

Definition 6.17. For any string of letters $y = y_1y_2\ldots y_\ell$, a $1 \rightarrow 2$ shift gadget for $y$ is a word $S^{1\rightarrow 2}(y)$ that equals the identity on all wires except the first two, and is equal to $y^{-1} := y_\ell\ldots y_2y_1$ on wire 1, i.e. a word of the form
\[
q_{i_1}q_{i_2}\ldots q_{i_\ell} := S^{1\rightarrow 2}(y) \sim \begin{bmatrix} y^{-1} \\ h(y) \end{bmatrix},
\]
for some arbitrary string of letters $h(y)$. For $\alpha, \beta \in [k]$, define $\alpha \rightarrow \beta$ shift gadgets analogously.

Note that any shift gadget has a natural inverse
\[
q_{i_1}q_{i_{\ell-1}}\ldots q_{i_1} := S^{1\rightarrow 2}(y) \sim \begin{bmatrix} y \\ h^{-1}(y) \end{bmatrix} = (S^{1\rightarrow 2}(y))^{-1}.
\]

Intuitively, $S^{1\rightarrow 2}(y)$ removes $y$ from the first wire and “saves” it on the second wire in the form of the string $h(y)$. $S^{1\rightarrow 2}(y)$ then “loads” $y$ back onto the first wire while removing $y'$ from the second wire. We now use these shift gadgets to construct a gadget that shuffles pairs of letters.

Definition 6.18. Define unpack : $([n]^2)^{\ell/2} \rightarrow [n]^\ell$ to map sequences of pairs into an “unpacked” sequence in the natural way, so that
\[
\text{unpack}((t_1, t_2), (t_3, t_4), \ldots, (t_{\ell-1}, t_\ell)) = (t_1, t_2, \ldots, t_\ell).
\]
Note that any permutation $\pi' \in S_\ell$ is pair preserving iff it satisfies
\[
\pi' = \text{unpack} \circ \pi \circ \text{unpack}^{-1}
\]
for some $\pi \in S_{\ell/2}$. 

22
Lemma 6.19 (Shuffle Gadget). Let \( t = (t_1,t_2,\ldots,t_{\ell/2}) \) be a length \( \ell/2 \) sequence of pairs of letters, with each \( t_i := (t_i^{(1)},t_i^{(2)}) \in [n]^2 \). Let \( G \) be an XOR game that contains all shift gadgets in the set \(^{10}\)

\[
\{ S^{(1)}_i(t_i^{(1)},t_i^{(2)}) : \alpha \in \{\alpha_1,\alpha_2\}, i \in [\ell/2] \},
\]

where \( \alpha_1 \neq \alpha_2 \) are elements of \([k]\setminus\{1\}\) and each shuffle gadget has length at most \( K \). Then, for all \( t' \in \text{shuffle}(t) \), \( G \) contains a word \( W \) with sign \( s_W = +1 \), length at most \( K\ell \), and

\[
W \sim \left[ \text{unpack}(t)^{-1} \text{unpack}(t') \right].
\]

Proof. Let \( f \) be the shuffle function satisfying \( f(t) = t' \in \text{shuffle}(t) \). Since \( f \) is a shuffle function we can choose disjoint sequences \( s_A \) and \( s_B \) with \( s_A \cup s_B = [\ell/2] \) and \( f^{-1} \) increasing on both. We construct a word of the desired form by first saving the pairs in \( s_A \) and \( s_B \) onto wires \( \alpha_1 \) and \( \alpha_2 \), respectively, then loading them back onto the first wire, interleaving in the appropriate order.

For any sequence \( s \), let \( s^r \) be shorthand for that sequence written in reverse order. Define the function \( g : [\ell/2] \to \{\alpha_1,\alpha_2\} \) by

\[
g(i) = \begin{cases} 
\alpha_1 & \text{if } i \in s_A \\
\alpha_2 & \text{if } i \in s_B 
\end{cases}
\]

Then the word \( W \) given below satisfies the lemma:

\[
W = \prod_{i=1}^{\ell/2} \left( S^{(1)}_i g(i) (t_i^{(1)},t_i^{(2)}) \right) \prod_{i=1}^{\ell/2} \left( S^{(1)}_i g(f^{-1}(i)) (f(i)^{(1)},f(i)^{(2)}) \right)
\]

\[
\sim \left[ \prod_{i \in s_A} h(t_i^{(1)},t_i^{(2)})^{-1} \right] \left[ \prod_{i \in s_B} h(t_i^{(1)},t_i^{(2)})^{-1} \right] = \left[ \text{unpack}(t)^{-1} \text{unpack}(t') \right].
\]

By assumption, \( G \) contains each shift gadget used in the construction of \( W \), and each shift gadget has length at most \( K \). Therefore \( W \) is contained in \( G \) and has length at most \( 2K(\ell/2) = K\ell \). For each shift gadget used, its inverse is also used. By construction, the sign of each shift gadget is the same as its inverse, so the overall sign of \( W \) is \( s_W = +1 \).

Note 6.20. For any game \( G \) and sequence of pairs \( t \) that meets the conditions of Lemma 6.19, \( G \) will also meet the conditions for any sequence of pairs \( u = \pi(t) \) produced through permutation \( \pi \) of \( t \). Then, under the assumptions of Lemma 6.19 we get “for free” that a word is contained in \( G \) with sign \( +1 \) and has the form

\[
\left[ \text{unpack}(\pi(t))^{-1} \text{unpack}(f(\pi(t))) \right]
\]

with \( \pi \) any permutation on pairs and \( f \) any shuffle function (see Definition 6.14).

Combining our newly constructed shuffle gadget with our understanding of parity preserving permutations allows us to derive a set of sufficient conditions for a game \( G \) to contain a refutation. These will be used in a critical way in Section 6.3.

Lemma 6.21. Let \( G \) be a \( k \)-XOR game containing a length \( \ell \) word \( W \) whose first wire is given by

\[
W_1 = [w_{11} w_{12} \ldots w_{1\ell}] \not\in I.
\]

Also let \( G \) contain all shift gadgets in the set

\[
\{ S^{(1)}_i (w_{1(2i-1)},w_{1(2i)}) : \alpha \in \{\alpha_1,\alpha_2\}, i \in [\ell/2] \},
\]

\(^{10}\) There is nothing special about player 1 here but we state the lemma in terms of player 1 for notational simplicity.
where \( \alpha_1 \neq \alpha_2 \in [k] \setminus \{1\} \) and each gadget has length at most \( K \).

Then \( G \) contains a word with sign +1 and length at most \( K \ell \log(\ell) \) whose first wire is given by

\[
W_1^{-1} = [w_{1\ell} w_{1(l-1)} \ldots w_{11}].
\]

and which is \( \sim I \) on all wires other than the first.

**Proof.** By Lemma 6.13 there exists a permutation \( \pi \) on \([\ell/2]\) satisfying

\[
\text{unpack } \circ \pi ((w_{11} w_{12}), (w_{13} w_{14}), \ldots, (w_{1(l-1)} w_{1\ell})) \sim I.
\]

By Lemma 6.16, there then exists a sequence \((f_1, f_2, \ldots, f_p)\) of \( p \leq \log(\ell) \) shuffle functions with

\[
f_p \ldots f_2 f_1 = \pi.
\]

Now let \( \pi' \) be an arbitrary permutation of \([\ell/2]\), \( f' \) be an arbitrary shuffle of \([\ell/2]\), and define the word \( Y(\pi', f') \) to have first coordinate

\[
Y_1(\pi', f') := \text{unpack } \circ \pi' ((w_{11} w_{12}), \ldots, (w_{1(l-1)} w_{1\ell}))^{-1} \text{unpack } \circ f' (\pi' ((w_{11} w_{12}), \ldots, (w_{1(l-1)} w_{1\ell})))
\]

and all remaining \( k - 1 \) coordinates the identity. By Lemma 6.19 and Note 6.20, we have that \( G \) contains a word with sign +1 and length at most \( K\ell \) which is \( \sim Y(\pi', f') \).

By concatenating a carefully chosen string of these words, we see \( G \) also contains a word with sign +1 and length at most \( K \ell \log(\ell) \) which is

\[
\sim Y(e, f_1) Y(f_1, f_2) Y(f_2 f_1, f_3) \ldots Y(f_{k-1} f_{k-2} \ldots f_1, f_k) \sim W_1^{-1}.
\]

Lemma 6.21 suggests we can construct refutations for a game \( G \) by finding a word contained in \( G \) which is \( \not\sim I \) and has sign \(-1\), and then checking to see if \( G \) contains the necessary shift gadgets. First, we demonstrate that the first two wires of some permutation of such a word can be made to cancel without using any shift gadgets, then determine a sufficient set of shift gadgets required thereafter.

**Lemma 6.22.** Let game \( G \) contain word \( W' = q_{i_1} q_{i_2} \ldots q_{i_\ell} \not\sim I \). There exists a permutation \( \pi \in S_\ell \) such that

\[
W := q_{\pi(i_1)} q_{\pi(i_2)} \ldots q_{\pi(i_\ell)} \not\sim I
\]

and both \( W^{(1)} \sim I \) and \( W^{(2)} \sim I \) with \( W^{(2)} = x_{1} x_{2} x_{2} \ldots x_{l/2} x_{l/2} \) where \( x_i \in [n] \).

**Proof.** By Lemma 6.12, we have that the even and odd multisets of \( W' , E \) and \( O \) respectively, are multiplicity equivalent. Thus, for each \( \alpha \in [k] \), there exists a bijection \( f_\alpha : E \leftrightarrow O \) that maps a query \((q^{(1)}, \ldots, q^{(k)}) \in E\) to a query \((q'^{(1)}, \ldots, q'^{(k)}) \in O\) such that \( q'^{(\alpha)} = q^{(\alpha)} \). From the bijections \( f_1, f_2 \), we will define a new map \( f : E \cup O \rightarrow E \cup O \) that maps each query \( q \in E \) to \( f_1(q) \in O \) and each \( q' \in O \) to \( f_2^{-1}(q') \in E \). Since \( f_1 \) and \( f_2 \) are bijections, so is \( f \). Applying the Foata correspondence, as in Lemma 6.13, to the permutation of \( E \cup O \) associated with \( f \) yields a sequence of queries that make a word \( W \) with the property that the first two wires completely cancel to identity and wire 2 takes the desired form, i.e.

\[
W = \begin{bmatrix}
[w_{11} w_{12} \ldots w_{1(l-1)} w_{1\ell}] \\
[w_{31} w_{32} \ldots w_{3(l-1)} w_{32\ell}] \\
\vdots \\
W^{(3)} \\
\cdots \\
W^{(k)}
\end{bmatrix} \sim \begin{bmatrix}
W^{(3)} \\
\cdots \\
W^{(k)}
\end{bmatrix}
\]

where \( W^{(3)}, \ldots, W^{(k)} \) are even-length strings of letters. \( \square \)
For a refutation to exist we then simply need to be able to shuffle the pairs on the remaining wires $3, \ldots, k$.

**Theorem 6.23** (Sufficient condition for refutation). Let $G$ be a PR game which by definition contains some word $W' \notin I$ of some even length $\ell$. Let $W \notin I$ be the pairwise permuted word as in Lemma 6.22. If $G$ contains all shift gadgets in the set
\[ \left\{ S^{\alpha \rightarrow \alpha'}(W_{2i-1}^{(\alpha)} W_{2i}^{(\alpha)}) : \alpha \in \{3, \ldots, k\}, \alpha' \in \{1, 2\}, i \in [\ell/2] \right\} \]  
(105)
then $G$ contains a refutation.

**Proof.** By the definition of a PR game (Definition 5.21), $G$ contains the word $W$ with sign $-1$. By Lemma 6.21, $G$ contains all words $W''_\alpha$ with $\alpha$-th wire given by $(W''_\alpha)^{(\alpha)} = (W^{(\alpha)})^{-1}$, all other wires $\sim I$, and sign $+1$. Therefore $G$ contains the word
\[ R := W \prod_{\alpha} W''_\alpha \sim I \]  
(106)
with sign $s_R = -1$, which is a refutation. \qed

It turns out that for the special case of symmetric XOR games, the symmetric structure guarantees existence of all required shift gadgets automatically. Theorems 6.23 and 5.22 then give that a symmetric game contains a PREF if and only if it contains a refutation. Further, whether a game contains a PREF is an efficiently decidable criterion. A formal definition of symmetric XOR games and a proof of these facts are demonstrated in Section 6.3.

### 6.3 Algorithm for Symmetric Games

We begin with a formal definition of symmetric games.

**Definition 6.24.** A $k$-XOR game $G$ is **symmetric** if whenever it contains a clause $c = (q^{(1)}, q^{(2)}, \ldots, q^{(k)}, s)$, it also contains all clauses $c' = (q^{(\pi(1))}, q^{(\pi(2))}, \ldots, q^{(\pi(k))}, s)$, where $\pi : [k] \rightarrow [k]$ permutes the query while the parity bit $s$ is unchanged.

**Definition 6.25.** A **random symmetric** $k$-XOR game $G_{sym}$ on $m = k!/m'$ clauses is a game constructed by randomly generating $m'$ clauses, then including all clauses related by permutations (as above) in $G_{sym}$.

For symmetric games, we can now prove that all required shift gadgets are certainly included.

**Lemma 6.26.** Let $W$ be a word contained in symmetric game $G$ of even length $\ell$ with second wire of the form $W^{(2)} = x_1 x_2 x_2 \ldots x_\ell x_\ell$, where $x_i \in [n]$. For any wire $\alpha \in \{3, \ldots, k\}$ and pairs of letters $y_1, y_2$ that appear at adjacent positions $2i - 1, 2i$ in $W^{(\alpha)}$, there exists shift gadgets from $\alpha \rightarrow 2$ and from $\alpha \rightarrow 1$ for $y_1 y_2$ with length $O(1)$.

**Proof.** Since the game is symmetric, it suffices to show the existence of the gadget for $\alpha \rightarrow 2$. Let the queries containing $y_1, y_2$ in $W$ be $q_1 = (q^{(1)}_1, q^{(2)}_1, \ldots, y_1, \ldots)$ and $q_2 = (q^{(1)}_2, q^{(2)}_2, \ldots, y_2, \ldots)$, respectively. Then by the assumption of symmetry, all permutations of these queries exist in the given game. We can thus construct the shift gadget $S^{\alpha \rightarrow 2}(y_1 y_2)$ by the product of four clauses as follows:

\[ S^{\alpha \rightarrow 2}(y_1 y_2) = \begin{pmatrix} (1) & q_1^{(1)} & q_1^{(2)} & q_1^{(1)} & h(y_1 y_2) \\ q_1^{(2)} & y_2 & q_1^{(1)} & q_1^{(2)} \\ \vdots & \vdots & \vdots & \vdots \\ y_2 & q_2 & q_1 & y_1 \end{pmatrix} = \begin{pmatrix} h(y_1 y_2) \\ y_2 y_1 \end{pmatrix}, \]  
(107)

where $h(y_1 y_2) := q_2^{(2)} y_2 y_1 q_1^{(2)}$ and the equality holds because $y_1$ and $y_2$ appear at an odd and following even position of $W$ so by the form of the second wire $q_1^{(2)} = q_2^{(2)}$. \qed
We now prove Theorem 2.1, by showing that the PREF criterion is both necessary and sufficient for a symmetric game to have a refutation, and can also be expressed as a system of linear Diophantine equations and thus solved efficiently.

**Theorem 2.1 (restated).** There exists an algorithm that, given a \( k \)-player symmetric XOR game \( G \) with alphabet size \( n \) and \( m \) clauses, decides in time \( \text{poly}(n,m) \) whether \( \omega^\ast(G) = 1 \) or \( \omega^\ast(G) < 1 \).

**Proof.** By Theorem 6.1, deciding whether the commuting-operator value is 1 is equivalent to deciding whether the game admits a refutation (of any length). By Theorem 5.22 for a game to admit a refutation it is necessary that it contains a PREF. Further, Theorem 6.23 and Lemma 6.26 together show that for a symmetric game to admit a refutation it is also sufficient to contain a PREF. Thus for a symmetric game, deciding whether \( \omega^\ast = 1 \) reduces to determining whether or not the game contains a PREF.

We can now rephrase the condition for a game to contain a PREF as a system of linear Diophantine equations. For each query in the game \( q_i = (q_i^{(1)}, \ldots, q_i^{(k)}) \), let \( z_i \) be an integer-valued variable representing the number of times query \( i \) appears in the even multiset of the PREF minus the number of times it appears in the odd multiset. The condition that these \( z_i \) in fact correspond to multiplicity equivalent sets can then be stated as a system of linear Diophantine equations,

\[
A^T z = 0 \quad (108)
\]

where \( A \) is the game matrix as defined in Definition 5.3 and we have collected the \( z_i \) into a vector \( z \in \mathbb{Z}^m \).

The condition that the signs of the clauses in the PREF multiply to \(-1\) can be expressed as an additional linear Diophantine equation in terms of \( z \) and parity bit vector \( \hat{s} \) (Definition 5.3):

\[
\hat{s}^T z = 1 \pmod{2} \quad (109)
\]

By applying a standard algorithm, such as the one described in Chapter 5 of [27], this system can be solved in time polynomial in the size of the system, measured as the number of bits necessary to specify the system of equations. This means a runtime that is \( \text{poly}(n,m) \).

**Note 6.27.** Finding a solution to (108) and (109) tells us not only that a refutation exists but also bounds its length. In particular, by following the steps of the preceding proof, it can be shown that for a symmetric game with \( \omega^\ast(G) < 1 \), the minimum-length refutation has length \( L \) satisfying

\[
\Omega(\|z\|_1) \leq L \leq O(k\|z\|_1 \log \|z\|_1),
\]

where \( z \) is a solution to (108) and (109) minimizing \( \|z\|_1 \).

We demonstrate an explicit refutation construction using the symmetric game shift gadgets in the context of the Capped GHZ game in Appendix A.

Finally, note that this linear algebraic description of the necessary PREF criterion for an entangled refutation parallels the classical condition for refutation (Definition 5.14). The only distinction is that (108) is considered an equation over \( \mathbb{F}_2 \) for classical games and over \( \mathbb{Z} \) for entangled games. As described in Section 7.3, these Diophantine equations then give rise to a dual condition similar to the classical picture: a MERP strategy achieves value 1 exactly when these equations do not admit a solution.

## 7 MERP Strategies

Section 5.4 introduced the family of Maximal Entanglement, Relative Phase (MERP) strategies. The primary feature of the MERP strategies is that deciding whether \( v^\text{MERP} = 1 \) and computing the accompanying MERP strategy vector may be done efficiently via Gaussian elimination. Beyond computability, the MERP strategies actually achieve value 1 on a large class of games where that is possible. Specifically, MERP achieves value 1 exactly where a PREF does not exist (noPREF games), including all symmetric value 1 games. This MERP - PREF duality is analogous to the duality between a classical linear algebraic refutation and the construction of a classical value 1 strategy.

Here, we motivate the definition of MERP strategies (Section 7.1) and prove their value defined in Claim 5.27 (Section 7.2). We then investigate the duality between MERP value 1 and PREFs (Section 7.3).
7.1 Generalizing GHZ

The MERP family of strategies is motivated by the GHZ strategy for solving the GHZ game. We begin by reviewing the GHZ game and value 1 strategy.

Definition 7.1. Recall that the GHZ game is defined by the clauses

\[
G_{\text{GHZ}} := \left\{ \begin{bmatrix} x \\ y \\ x \\ y \end{bmatrix}, \begin{bmatrix} y \\ x \\ y \\ x \end{bmatrix}, \begin{bmatrix} y \\ x \\ y \\ x \end{bmatrix}, \begin{bmatrix} x \\ y \\ y \\ x \end{bmatrix}, \begin{bmatrix} x \\ y \\ y \\ x \end{bmatrix} \right\}. \tag{110}
\]

The GHZ strategy [15], defined as follows, achieves value 1 for this game.

Definition 7.2. Define the GHZ Strategy for \( G_{\text{GHZ}} \) to be the tensor-product strategy in which:

1. The \( k = 3 \) players share the maximally entangled state

\[
|\Psi\rangle = \frac{1}{\sqrt{2}} [ |000\rangle + |111\rangle ] \tag{111}
\]

with player \( \alpha \) having access to the \( \alpha \)-th qubit of the state.

2. Upon receiving symbol \( j \) from the verifier, player \( \alpha \) rotates his qubit by an angle

\[
\theta(\alpha,j) = \begin{cases} 0 & \text{if } j = x \\ \frac{\pi}{2} & \text{if } j = y \end{cases} \tag{112}
\]

about the Z axis, then measures his qubit in the X basis and sends his observed outcome to the verifier. Defining the states \( |\theta(\alpha,j)\rangle_\pm \) by

\[
|\theta(\alpha,j)\rangle_+ = \frac{1}{\sqrt{2}} \left[ |0\rangle + e^{i\theta(\alpha,j)} |1\rangle \right] \quad \text{and} \quad |\theta(\alpha,j)\rangle_- = \frac{1}{\sqrt{2}} \left[ |0\rangle - e^{i\theta(\alpha,j)} |1\rangle \right] \tag{113, 114}
\]

the GHZ strategy may be given by the strategy observables

\[
O^\alpha(j) := |\theta(\alpha,j)\rangle_+ \langle \theta(\alpha,j)\rangle_+ - |\theta(\alpha,j)\rangle_- \langle \theta(\alpha,j)\rangle_- . \tag{115}
\]

We now consider why this strategy is successful. Recall that a \( \varphi \) rotation in the Z basis is represented by the operator

\[
e^{i\varphi/2} |0\rangle\langle 0| + e^{-i\varphi/2} |1\rangle\langle 1|. \tag{116}
\]

Thus the rotations \( \varphi_1, \varphi_2, \varphi_3 \) applied by the players to their shared state \( |\Psi\rangle \) results in

\[
|\Psi_\varphi\rangle := \frac{1}{\sqrt{2}} \left[ e^{-i\varphi} |000\rangle + e^{i\varphi} |111\rangle \right] \tag{117}
\]

\[
\varphi := \varphi_1 + \varphi_2 + \varphi_3. \tag{118}
\]

Note that \( X \otimes X \otimes X |\Psi_\varphi\rangle = |\Psi_{-\varphi}\rangle \). This gives expected value of the measurements performed by the three players,

\[
\langle \Psi_\varphi | X \otimes X \otimes X |\Psi_\varphi\rangle = \frac{e^{i\varphi} + e^{-i\varphi}}{2} = \cos \varphi. \tag{119}
\]

Thus the relative phase between the kets \( |000\rangle \) and \( |111\rangle \) introduced by the Z rotations determines the probabilities that the players output +1 or −1. For the GHZ game, the prescription for Z rotations given in (112) results in relative phase \( \varphi = 0 \) for the first clause and \( \varphi = \pi \) for the remaining three clauses, exactly matching the desired outputs.
This description of GHZ motivates the MERP family as a generalization. For a game $G$, the MERP construction assigns a distinct angle to each player-question combination such that the relative phase for each query in $G$ gives optimal probability of winning. The set of games for which MERP can achieve value 1 is exactly the set for which the game admits independently setting the relative phase for each query to $\pi \hat{s}_i$. This is exactly the statement of Claim 5.29.

We proceed by recalling the definition of a MERP strategy in light of the GHZ analogue, proving our value claim, and finally demonstrating the duality with PREF games.

### 7.2 MERP Strategy Value

Recall the definition of a MERP strategy:

**Definition 5.26 (restated).** Given a $k$-XOR game $G$ with $m$ clauses, a **MERP strategy** for $G$ is a tensor-product strategy in which:

1. The $k$ players share the maximally entangled state

   $$|\Psi\rangle = \frac{1}{\sqrt{2}} \left[ |0\rangle^\otimes k + |1\rangle^\otimes k \right]$$

   with player $\alpha$ having access to the $\alpha$-th qubit of the state.

2. Upon receiving question $j$ from the verifier, player $\alpha$ rotates his qubit by an angle $\theta(\alpha, j)$ about the $Z$ axis, then measures his qubit in the $X$ basis and sends his observed outcome to the verifier.

   Explicitly, we define the states

   $$|\theta(\alpha, j)\pm\rangle := \frac{1}{\sqrt{2}} \left[ |1\rangle \pm e^{-i\theta(\alpha, j)} |0\rangle \right]$$

   and pick strategy observables

   $$O^\alpha(j) := |\theta(\alpha, j)+\rangle \langle \theta(\alpha, j)+| - |\theta(\alpha, j)−\rangle \langle \theta(\alpha, j)−|.$$  

We now demonstrate that a MERP strategy achieves the claimed tensor-product (and thus commuting-operator) value by explicit calculation.

**Claim 5.27 (restated).** The value achieved by that MERP strategy on game $G$ is:

$$v^{MERP}(G, \hat{\theta}) := \frac{1}{2} + \frac{1}{2m} \left( \sum_{i=1}^{m} \cos \left( \pi \left( A\hat{\theta}_i - \hat{s}_i \right) \right) \right)$$

$$= \frac{1}{2} + \frac{1}{2m} \left( \sum_{i=1}^{m} \cos \left( \sum_{\alpha=1}^{k} \theta(\alpha, q_i^{(\alpha)}) - \pi \hat{s}_i \right) \right).$$

**Proof.** Consider a particular clause $c_i = (q_i, s_i)$. We calculate the probability that a MERP strategy parameterized by $\theta(\alpha, q_i^{(\alpha)})$ returns output $s_i$ correctly.

If players $1, \ldots, k$ apply rotations by $\varphi_1, \ldots, \varphi_k$ to their qubits in state $|\Psi\rangle = \frac{1}{\sqrt{2}} \left[ |0\rangle^\otimes k + |1\rangle^\otimes k \right]$ then they will be left with

$$|\psi_{\varphi}\rangle := \frac{1}{\sqrt{2}} \left[ e^{i\varphi} |0\rangle^\otimes k + e^{-i\varphi} |1\rangle^\otimes k \right]$$

$$\varphi := \varphi_1 + \ldots + \varphi_k.$$  

Note that $X^\otimes k |\psi_{\varphi}\rangle = |\psi_{-\varphi}\rangle$. The expected value of the product of the $k$ measurements is then

$$\langle \psi_{\varphi} | X^\otimes k | \psi_{\varphi}\rangle = \frac{e^{i\varphi} + e^{-i\varphi}}{2} = \cos \varphi.$$  

28
We now plug in the values from the clause and the corresponding angles in the MERP strategy. The angles are \( \varphi_\alpha = \theta(\alpha, q^*_\alpha) \) so that
\[
\varphi = \sum_{\alpha \in [k]} \theta(\alpha, q^*_\alpha) = (A\hat{\theta})_i.
\] (128)
The probability of obtaining the correct answer for the clause is
\[
\frac{1 + s_i \langle \Psi^k \mid X^\otimes k \mid \Psi^k \rangle}{2} = \frac{1 + \cos(\varphi - \pi \hat{s}_i)}{2}.
\] (129)
Averaging over all clauses and substituting (128) for \( \varphi \) we obtain (123) and (124).

\section*{7.3 MERP - PREF Duality}

It is well-known that the structure of the game matrix over \( \mathbb{F}_2 \) gives insight into the classical value of an XOR game. The construction of a classical value 1 strategy is dual to the existence of a classical refutation. In much the same way, the construction of a commuting-operator value 1 MERP strategy is dual to the existence of a PREF.

MERP is restricted to achieving value 1 on only a subset of commuting-operator value 1 XOR games. By the duality to PREF this subset is exactly those games that our algorithm can decide have value 1. In particular, this means that all symmetric games with value 1 can be played optimally using MERP, making it a powerful family of strategies.

We begin with a review of the classical value 1 - refutation duality, which informs our later proof of the MERP - PREF duality. From Claim 5.7, we have the value of a classical strategy
\[
v(G, \hat{\eta}) = \frac{1}{2} + \frac{1}{2m} \left( \sum_i \cos(\pi [(A\hat{\eta})_i - \hat{s}_i]) \right)
\] (130)
where the vector algebra is taken over \( \mathbb{F}_2 \). Using this linear algebraic form for the value, we can prove Claim 5.9.

\textbf{Claim 5.9 (restated).} Every solution \( \hat{\eta} \in \mathbb{F}_2^n \) to
\[
A\hat{\eta} = \hat{s}
\] (11)
corresponds to a strategy \( \eta \) achieving value 1 on game \( G \sim (A, \hat{s}) \), and vice versa. In particular, a game \( G \) has classical value 1 iff (11) has a solution.

\textbf{Proof.} If a solution \( \hat{\eta} \) exists,
\[
v(G, \hat{\eta}) = \frac{1}{2} + \frac{1}{2m} \left( \sum_i \cos(\pi [(A\hat{\eta})_i - \hat{s}_i]) \right)
\] (131)
\[
= \frac{1}{2} + \frac{1}{2m} \left( \sum_i \cos(0) \right) = 1.
\] (132)
Conversely, to achieve value 1, we must have the argument of every cosine equal to some multiple of \( 2\pi \). Therefore we need \( A\hat{\eta} - \hat{s} = 0 \) over \( \mathbb{F}_2 \).

Recall that this classical value 1 constraint has a dual set of equations, such that there exists a classical refutation that solves the dual equations if and only if the classical value 1 constraints are not satisfiable.

\textbf{Fact 5.15 (restated).} Either a classical refutation \( y \) exists satisfying
\[
\begin{bmatrix} A^T \\ \hat{s}^T \end{bmatrix} y = \begin{bmatrix} 0 \\ 1 \end{bmatrix}
\] (15)
or a classical strategy \( \hat{\eta} \) exists satisfying (11).
We use an analogous duality relation to prove the MERP - PREF duality shortly. Before that, we mention one more consequence of this characterization of classical value 1 games – a linear algebraic specification, in terms of game matrix $A$, of the set of $\hat{s}$ for which the game $G \sim (A, \hat{s})$ has $\omega(G) = 1$.

**Definition 7.3.** Define the vector space $Y_2 \subseteq \mathbb{F}_2^{kn}$ by

$$Y_2 := \{ A\hat{\eta} : \hat{\eta} \in \mathbb{F}_2^{kn} \} = \text{im}_2(A) \quad (133)$$

Define the dimension of this vector space as

$$\sigma_2 := \dim Y_2. \quad (134)$$

**Corollary 7.4.** Given a game matrix $A$, the set of possible accompanying $\hat{s}$ that produce a game $G \sim (A, \hat{s})$ with classical value 1 is exactly the $2^{\sigma_2}$ parity-bit vectors in $Y_2$.

**Proof.** This follows immediately from Claim 5.9. \qed

The main use of Corollary 7.4 is to characterize the classical value of games with randomly chosen $s_i$ (Section 8.3).

We now use an analogue of Fact 5.15 to demonstrate that the set of games on which MERP achieves commuting-operator value 1 is exactly the complement of those for which a PREF specification exists. First, recall the MERP constraint equations that define the set of games for which MERP achieves value 1.

**Claim 5.29 (restated).** A MERP strategy achieves $v^{\text{MERP}} = 1$ on a game $G$ iff its MERP constraint equations

$$A\hat{\theta} = \hat{s} \pmod{2} \quad (135)$$

have a solution $\hat{\theta} \in \mathbb{Q}^{kn}$.

**Proof.** If a solution $\hat{\theta}$ exists, (123) gives the MERP value using this strategy vector:

$$v^{\text{MERP}}(G, \hat{\theta}) = \frac{1}{2} + \frac{1}{2m} \left( \sum_{i=1}^{m} \cos(0) \right) = 1. \quad (136)$$

Conversely, the only way to achieve value $m$ inside the sum over cosines is for the argument to each cosine to be a multiple of $2\pi$. This is only possible if $(A\hat{\theta})_i - \hat{s}_i = 0 \pmod{2}$ for each $i$. \qed

**Theorem 5.30 (restated).** Either there exists a MERP refutation $z \in \mathbb{Z}^m$ satisfying the PREF equations

$$A^T z = 0 \quad (137)$$

$$\hat{s}^T z = 1 \pmod{2} \quad (138)$$

or a MERP strategy with value 1 exists for game $G \sim (A, \hat{s})$.

**Proof.** We begin by reformattting the linear Diophantine equations (137) and (138) to remove the modulo 2 and collect the PREF constraints into a single matrix equation

$$\begin{bmatrix} A^T & 0 \\ \hat{s}^T & 2 \end{bmatrix} \begin{bmatrix} z \\ z' \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (139)$$

with $z' \in \mathbb{Z}$.

By [27, Corollary 4.1a], the dual to (139) is the system of constraints

$$\begin{bmatrix} A & \hat{s} \\ 0 & 2 \end{bmatrix} \begin{bmatrix} w \\ w' \end{bmatrix} \in \mathbb{Z}^{m+1} \quad \text{and} \quad (140)$$

$$\begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} w \\ w' \end{bmatrix} \notin \mathbb{Z}. \quad (141)$$
Here “dual” means that (140) and (141) are satisfiable iff (139) is unsatisfiable. The bottom rows of (140) and (141) can be satisfied iff
\[ w' = a + \frac{1}{2}, \, a \in \mathbb{Z}. \] (142)
The top row of (140) then becomes:
\[ Aw + \hat{s}w' = a' \in \mathbb{Z}^m \] (143)
\[ \iff A(2w) + (2a + 1)\hat{s} = 2a' \] (144)
\[ \iff A(2w) = \hat{s} \pmod{2}. \] (145)
Setting \( \hat{\theta} = 2w \) and picking arbitrary \( a \in \mathbb{Z} \), (142) and (145) can be satisfied iff there is a solution to
\[ A\hat{\theta} = \hat{s} \pmod{2}, \hat{\theta} \in \mathbb{Q}^n. \] (146)

Theorem 5.30 tells us that every game that we can decide has value 1 using the algorithm of Section 6.3 also has an accompanying MERP strategy with value 1. Further, we demonstrated in that section that a symmetric game contains a PREF iff it has value \( \omega^* < 1 \). We conclude that for symmetric games, the MERP family of strategies achieves value 1 everywhere it is possible to do so.

Following the classical case, it is also illuminating to note a linear algebraic specification, in terms of game matrix \( A \), of the \( \hat{s} \) for which a MERP strategy can achieve value 1 on game \( G \sim (A, \hat{s}) \). First, we define a mapping between the space in which the image of \( A \) lives, \( \text{im}_Q(A) \subseteq \mathbb{Q}^m \), and the space in which the parity bits live, \( \hat{s} \in \mathbb{F}_2^m \).

**Definition 7.5.** Define a mapping \( \varphi_2 : \mathbb{Q}^m \to \mathbb{F}_2^m \) by
\[ \varphi_2(z) := \begin{cases} z \pmod{2} & \text{if } z \in \mathbb{Z}^m \\ 0 & \text{otherwise.} \end{cases} \]

Now, we can define an analogue to \( Y_2 \), here considering \( A \) as a map over \( \mathbb{Q} \) and naturally extending \( \varphi_2 \) to act on subsets of \( \mathbb{Q}^m \).

**Definition 7.6.** Define the vector space \( Y_Q \subseteq \mathbb{F}_2^m \) by
\[ Y_Q := \varphi_2(\text{im}_Q(A)). \] (147)

We then find that, accounting for the \( \varphi_2 \) technicality due to the mod 2 involved in computing an overall output, the set of games with MERP value 1 is the image of \( A \) over \( \mathbb{Q} \).

**Corollary 7.7.** Given a game matrix \( A \), the set of possible accompanying \( \hat{s} \) that produce a game \( G \sim (A, \hat{s}) \) with MERP value 1 is exactly the parity bit vectors in \( Y_Q \).

**Proof.** This follows directly from Claim 5.29. \( \square \)

In this sense, Corollary 7.7 demonstrates that the advantage of MERP over a classical strategy is simply exploiting entanglement to enable the players to “output” values in \( \mathbb{Q} \) instead of \( \mathbb{F}_2 \).

### 8 Specific Games

In this section we use the machinery of the previous sections to construct some games with interesting properties.

The first is a simple game, the 123 Game, which illustrates conditions under which the PREF condition can be fooled. It is a relatively small (6 player, 6 query) non-symmetric game which does contain a PREF,
but still does not contain any refutations. We show this by giving an explicit value 1 strategy for the 123 Game.

The second is a family of games, called Capped GHZ (CG), which are designed to be hard instances for the ncSoS algorithm. In particular, the CG game on $n$ variables (denoted $CG_n$) is a symmetric game with value strictly less than 1, meaning the decision algorithm of Section 6.3 can show the game has value $< 1$ in poly time, but with a minimum refutation of length at least exponential in $n$. This shows a doubly exponential improvement in the runtime of our decision algorithm as compared to the ncSoS algorithm, and an exponential improvement over the previous best known ncSoS lower bounds for this problem \[17\]12. This game construction is based primarily on the theorems of Section 6, which outline the relationship between refutations and ncSoS runtime, as well as our decision algorithm.

Finally, we construct a family of games with commuting-operator value 1 and a low classical value. These games are called Asymptotically Perfect Difference (APD) games, and are parameterized by $K$. The classical value of the $K$-th APD game (APD$_K$) approaches $1/2$, which is the lowest possible, in the limit of large $K$. The existence of such a family was posed as an open question in [4]. The construction of these games is based primarily on the difference between the linear equations defining MERP value 1 and classical value 1, which is discussed in Section 7.3.

These games are summarized in the following table, with a full discussion of each in the subsequent sections.

| Game     | $n$ | $m$ | $k$ | $\omega^*$ | $\omega$     | minimum refutation length |
|----------|-----|-----|-----|-------------|---------------|--------------------------|
| 123 Game | 3   | 6   | 6   | 1           | 5/6           | –                        |
| CG$_n$   | $n$ | $3n-1$ | 3   | $< 1 - 1/\exp(n)$ | $1 - 1/m$    | $2^{n+1} - 2$        |
| APD$_K$  | 2   | $2^K$ | $2^K - 1$ | 1           | $1/2 + \sqrt{K/2^K}$ | –                        |

Table 3: Overview of the games constructed in this section. Quantities of note are denoted in bold.

8.1 123 Game

We begin with a discussion of the intuition behind the 123 game, then follow with an explicit value 1 strategy. It is instructive to begin by analyzing the “Small 123 Game”.

**Definition 8.1.** Define the Small 123 Game to be the $k = 3$ player game with $n = 3$ and $m = 6$ clauses

\[
G_{123}^{\text{small}} := \left\{ \begin{array}{ccc} 1 & 1 & 3 \\ 1 & 2 & 3 \\ 1 & 3 & -1 \end{array} \right\}.
\]

(148)

In this form, it is clear the Small 123 Game has $\omega^*(G_{123}^{\text{small}}) < 1$, since placing its clauses in the order presented forms a refutation.

The game matrix $A$ has a one-dimensional left nullspace (corresponding to the space of candidate PREF specifications $z$ satisfying $A^T z = 0$):

\[
z \propto \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}^T.
\]

(149)

Any odd multiples of this basis vector produce a PREF specification $z$.

We now add players to this game while preserving this PREF specification, until we exclude all refutations formed by permutations of a single copy of each of the clauses. To preserve the PREF specification, for each question $j$ given to a new player, we ensure $j$ is given to the player once in an even clause (2, 4, or 6) and once in an odd clause (1, 3, or 5). We must add three players to exclude all possible reorderings of the

12In fact, to our knowledge, our results are the first exponential degree lower bound for the ncSoS hierarchy applied to any problem.
length-6 refutation given by the clauses of the Small 123 Game, and in doing so end up with the “123 Game” (clauses reordered to expose the game structure):

**Definition 8.2.** Define the 123 Game by the following set of clauses:

\[
G_{123} := \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 2 & 3 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 1 & 2 \\ -1 & 1 \end{bmatrix} \right\}.
\]

(150)

The 123-game has been constructed to make it difficult to reorder valid PREF specifications into refutations (for instance, it can be shown that no permutation of the valid length-6 PREF specifications corresponds to a valid refutation).

In Section 6.3 we demonstrated that symmetric games have a refutation whenever they contain a PREF by construction of all required shift gadgets. In the (non-symmetric) 123 Game, there are no obvious shift gadgets present. This structure gives some intuition for why one would expect this game to have value 1 even though it has a PREF. In the next section we prove that this intuition is correct; the 123-Game does in fact have value 1.

### 8.1.1 Value 1 Strategy

We define a simple strategy: measure in the Z basis if sent a 1, X if sent a 2, and Y if sent a 3.\(^\text{13}\) If each player plays the 123 Game uses this strategy, it results in the following set of query observables:

\[
Q_{123} := \left\{ \begin{bmatrix} Z & X & Y \\ Z & X & Y \\ Z & Y & X \end{bmatrix}, \begin{bmatrix} Z & X & Y \\ Z & X & Y \\ Z & Y & X \end{bmatrix}, \begin{bmatrix} Z & X & Y \\ Z & X & Y \\ Z & Y & X \end{bmatrix} \right\}.
\]

(151)

We also define a state on which these measurement can be made.\(^\text{14}\)

\[
|\psi_{123}\rangle := \frac{1}{\sqrt{8}} \left( |000000\rangle + |111111\rangle - \left[ |001001\rangle + |001010\rangle + |010001\rangle + |010101\rangle + |101011\rangle + |101101\rangle \right] \right)
\]

(152)

**Theorem 8.3.** The strategy observables in \(Q_{123}\) measured on the state \(|\psi_{123}\rangle\) win the 123 Game with probability 1. (The 123 Game has value 1.)

**Proof.** For every string in \(|\psi_{123}\rangle\), its compliment is also in \(|\psi_{123}\rangle\) with the same sign. Additionally, every string in \(|\psi_{123}\rangle\) has even Hamming weight. Overall, we may then conclude

\[
XXXXXX |\psi_{123}\rangle = ZZZZZZ |\psi_{123}\rangle = |\psi_{123}\rangle
\]

and hence

\[
YYYYYY |\psi_{123}\rangle = (i)^6 XXXXX \left[ ZZZZZZ |\psi_{123}\rangle \right] = -|\psi_{123}\rangle.
\]

\(^\text{13}\) This is motivated by the observation that the 123 game provably does not have a refutation if we assume the measurements for different questions anticommute. We plan on addressing this intuition formally in an upcoming paper.

\(^\text{14}\) This state was found through simple trial and error.
It remains to check the outcomes for the last 3 queries. Explicit calculation gives
\[ Z_{XYZX} |000000\rangle = (-1) |0\rangle |1\rangle (-i) |1\rangle (-1) |0\rangle |1\rangle (-i) |1\rangle = - |011011\rangle. \]  
(155)
as well as
\[ Z_{XYZX} |111111\rangle = |1\rangle |0\rangle i |0\rangle |1\rangle |0\rangle i |0\rangle = - |100100\rangle \]  
(156)
Similarly, we can check
\[ Z_{XYZX} |001010\rangle = (-1) |0\rangle |1\rangle i |0\rangle (-1) |0\rangle |0\rangle (-i) |1\rangle = |010001\rangle. \]  
(157)
and
\[ Z_{XYZX} |110101\rangle = |1\rangle |0\rangle (-i) |1\rangle |1\rangle |1\rangle |0\rangle = |101110\rangle. \]  
(158)
Putting this all together we see
\[ Z_{XYZX} |\psi_{123}\rangle = |\psi_{123}\rangle, \]  
(159)
with similar (permuted) arguments holding for \( XYZYZX \) and \( YZXXYZ \).

8.2 Capped GHZ (CG) Games

We begin by considering a family of symmetric games with commuting-operator value \(< 1\). The key property of this family is that to detect that \( \omega^* < 1 \) requires an exponentially high level in the ncSoS hierarchy, whereas the algorithm presented in Section 6.3 can do so in polynomial time.

**Definition 8.4.** Define the \( n \)-th order **Capped GHZ game** as the 3-XOR game with alphabet size \( n \) and \( m = 3n - 1 \) clauses defined by

\[ CG_n := \left\{ \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix}, \begin{bmatrix} 2 \\ 2 \\ +1 \end{bmatrix}, \begin{bmatrix} 2 \\ 3 \\ +1 \end{bmatrix}, \begin{bmatrix} 3 \\ 2 \\ +1 \end{bmatrix}, \ldots, \begin{bmatrix} (n-1) \\ n \\ +1 \end{bmatrix}, \begin{bmatrix} n \\ n \\ +1 \end{bmatrix}, \begin{bmatrix} n \\ n \\ +1 \end{bmatrix} \right\}. \]  
(160)

We claim \( \omega^*(CG_n) < 1 \), and that it requires level at least \( 2^n + 1 - 2 \) in the ncSoS hierarchy to detect this fact. Define the \( i \)-th triple of \( CG_n \) to be the clause set

\[ A_i := \left\{ \begin{bmatrix} i \\ (i+1) \\ +1 \end{bmatrix}, \begin{bmatrix} (i+1) \\ i \\ +1 \end{bmatrix}, \begin{bmatrix} (i+1) \\ (i+1) \\ +1 \end{bmatrix} \right\}. \]  
(161)

The clauses

\[ \begin{bmatrix} 1 \\ 1 \\ -1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} n \\ n \\ +1 \end{bmatrix} \]  
(162)
are called the caps (upper and lower) of the game and, for notational convenience, are referred to by \( A_0 \) and \( A_n \). Our first claim shows that any refutation for \( CG_n \) must include both the upper and lower caps.

**Lemma 8.5.** Let \( E, O \) be minimal multiplicity equivalent multisets of queries taken from \( CG_n \), so \( E \sim O \) and no clause appears in both \( E \) and \( O \). If \( E \uplus O \) contains some \( x \in A_j \) with \( j \notin \{0,n\} \), then \( E \uplus O \) also contains clauses drawn from \( A_{j-1} \) and \( A_{j+1} \).
Proof. Without loss of generality, assume
\[
x = \begin{bmatrix} j \\ (j + 1) \\ (j + 1) \\ +1 \end{bmatrix} \in \mathcal{E}.
\] (163)
We then proceed by contradiction. If no clause from \(A_{j-1}\) is contained in \(O\) then the multiplicity of letter \(j\) for wire 1 in \(O\) cannot match \(\mathcal{E}\), and the contradiction is immediate.

To prove the second claim, assume \(x\) occurs in \(\mathcal{E}\) with multiplicity \(\lambda\), and no terms from \(A_{j+1}\) are contained in \(O\). Then, in order to match the \((j + 1)\) multiplicity on the 2nd and 3rd wires, clauses
\[
y_1 = \begin{bmatrix} (j + 1) \\ j \\ (j + 1) \\ +1 \end{bmatrix} \text{ and } y_2 = \begin{bmatrix} (j + 1) \\ j \\ (j + 1) \\ +1 \end{bmatrix}
\] (164)
must both occur in \(O\) with multiplicity \(\lambda\). Then we find \((j + 1)\) occurs on the first wire of \(\mathcal{E}\) with multiplicity 0, and on the first wire of \(O\) with multiplicity \(2\lambda\). Then \(\mathcal{E}\) and \(O\) cannot be multiplicity equivalent, and this contradiction proves our result.

A bound on the minimum length refutations for \(CG_n\) follows in a straightforward manner from Lemma 8.5.

**Theorem 8.6.** The minimal length refutation for \(CG_n\) has length at least \(2^{n+1} - 2\).

**Proof.** We show the minimal sized multiplicity equivalent multisets \(\mathcal{E}\) and \(O\) formed by elements of \(CG_n\) have size at least \(2^{n+1} - 2\). By Lemma 8.5 the lower cap \(A_0\) of \(CG_n\) is contained in either \(\mathcal{E}\) or \(O\). Without loss of generality, assume it is contained in \(\mathcal{E}\).

Then \(\mathcal{E}\) contains letter 1 on every wire, and by minimality we know \(A_0 \cap O = \emptyset\). Since \(\mathcal{E}\) and \(O\) are multiplicity equivalent multisets, we conclude \(A_1 \subseteq O\). But then \(O\) has two 2s on each wire, and by minimality \(A_1 \cap \mathcal{E} = \emptyset\). So we conclude \((A_2^2) \in \mathcal{E}\), where the notation \(A_2^2\) denotes the multiset containing two copies of each element of \(A_2\), and containment of one multiset in another implies containment of each element with at least its multiplicity. Continuing in this vein, we see (assuming even \(n\) for the assignment of \(A_n\) below, though this does not affect the counting):
\[
A_0 \uplus (A_2)^2 \uplus (A_4)^8 \ldots \uplus (A_n)^{2^{n-1}} \subseteq \mathcal{E} \text{ and } A_1 \uplus (A_2)^4 \uplus (A_4)^{16} \ldots \uplus (A_{n-1})^{2^{n-2}} \subseteq O.
\] (165)

The total number of clauses contained in \(\mathcal{E} \uplus O\) is then given by
\[
1 + 3(2^0) + 3(2^1) + \ldots + 3(2^{n-2}) + 2^{n-1} = 1 + 3(2^{n-1} - 1) + 2^{n-1}
\] (166)
\[
= 2^{n+1} - 2.
\] (167)
Any refutation gives rise to even and odd multiplicity equivalent multisets \(\mathcal{E}\) and \(O\), and the above demonstrates that their combined size must be \(\geq 2^{n+1} - 2\), proving the lower bound on refutation length.

Theorem 8.6 shows that there exists a pseudodistribution on the clauses of \(CG_n\) which appears to have value 1 to a level exponential in the ncSoS hierarchy (proving Theorem 2.4). The minimal length multisets constructed in the proof of Theorem 8.6 are in fact multiplicity equivalent and the parity bits multiply to \(-1\) (there is exactly one copy of \(A_0\), which is the only question with \(s_i = -1\)) meaning \(CG_n\) contains a PREF. Since \(CG_n\) is a symmetric game, these two properties are sufficient to ensure a refutation exists (Section 6.3) giving \(\omega^*(CG_n) < 1\).

### 8.3 Asymptotically Perfect Difference (APD) Games

We next construct a family of \(k\)-XOR games, parameterized by \(K \in \mathbb{N}\), with \(k = 2^K - 1\), \(m = 2^K\) clauses, and asymptotically perfect difference: each game in the family is a noPREF game, meaning
\[
\omega^*(\text{APD}_K) = 1,
\] (168)
while
\[ \omega(\text{APD}_K) \sim \frac{1}{2} + \sqrt{\frac{K}{2^K}} \sim \frac{1}{2} + \sqrt{\log k} \]  
indicating that the difference is asymptotically as large as possible,
\[ \lim_{K \to \infty} 2(\omega^*(\text{APD}_K) - \omega(\text{APD}_K)) = 1. \]

**Definition 8.7.** Define the *Asymptotically Perfect Difference* family of XOR games parameterized by a scale \( K \in \mathbb{N} \) as the set of games with alphabet size \( n = 2 \), \( k = 2^K - 1 \) players, and \( m = 2^K \) clauses:

\[ \text{APD}_K := \{ [q_i] : q_i(\alpha) = B^{\alpha,i}_{(K)} + 1 \}. \]

The \( s_i \) are defined to adversarially minimize \( \omega(\text{APD}_K) \) and the matrix \( B_{(K)} \in \{0,1\}^{2^K \times 2^K} \) is recursively defined by

\[ B_{(0)} = [1] \]
\[ B_{(K+1)} = [\bar{B}_{(K)} \ B_{(K)}] \]

with \( \bar{B} \) produced by switching 0 \( \leftrightarrow \) 1 for all entries of \( B \). Equivalently, \( \bar{B} = J - B \), with \( J \) the all-ones matrix.

Note that by the game definition, the \( m \times kn = (2^K) \times (2*(2^K-1)) \) game matrix \( A_{(K)} \) for \( \text{APD}_K \) consists of the first \( 2^K - 1 \) columns of \( B_{(K)} \) interleaved with the first \( 2^K - 1 \) columns of \( \bar{B}_{(K)} \):

\[ A_{(K)} = [B_{(K)}^{-1} \ B_{(K)}^{-1} \ B_{(K)}^{-2} \ \ldots \ \ B_{(K)}^{-2^{K-1}} \ \bar{B}_{(K)}^{-2^{K-1}}]. \]

The pairs of columns in \( A_{(K)} \) corresponding to the two possible outputs from each player are complementary, making \( A_{(K)} \) a valid game matrix.

Note that \( \text{APD}_2 \) is exactly the GHZ game, so the APD family is a particular many-player generalization of GHZ:

\[ B_{(2)} = \begin{bmatrix} \bar{B}_{(1)} & B_{(1)} \\ B_{(1)} & \bar{B}_{(1)} \end{bmatrix} \]
\[ = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \]
\[ \implies A_{(2)} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}. \]

Exchanging columns 3 \( \leftrightarrow \) 6 and 4 \( \leftrightarrow \) 5, corresponding to a relabeling of players and inputs, gives \( A_{\text{GHZ}} \) as defined in (5). The choice of parity bits in GHZ is known to minimize the classical value, exactly matching the definition of \( \text{APD}_2 \).

We now prove our claims about the commuting-operator and classical values of APD games.

### 8.3.1 Commuting-Operator Value

**Lemma 8.8.** For all \( K \), \( B_{(K)} \) has trivial kernel.

**Proof.** We proceed by induction.

1. **Base case:** \( B_{(0)} = [1] \) has trivial kernel by inspection.
2. **Induction step:** Assume $B_{(K)}$ has trivial kernel, i.e. $B_{(K)}x = 0 \implies x = 0$. We now demonstrate that $B_{(K+1)}$ has trivial kernel by contradiction.

Assume to the contrary that $B_{(K+1)}x = 0$ for $x \neq 0$. We can expand the blocks of this equation:

$$B_{(K+1)}x = \begin{bmatrix} \bar{B}_{(K)} & B_{(K)} \\ B_{(K)} & B_{(K)} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = 0.$$  \hspace{1cm} (178)

By the bottom block,

$$B_{(K)}x_1 + B_{(K)}x_2 = 0 \quad \text{(179)}$$
$$B_{(K)}(x_1 + x_2) = 0 \quad \text{(180)}$$
$$\implies x_2 = -x_1. \quad \text{(Induction hypothesis)} \hspace{1cm} (181)$$

Using this relation in the top block, we have

$$0 = \bar{B}_{(K)}x_1 - B_{(K)}x_1 = (J - B_{(K)} - B_{(K)}) x_1 \quad \text{(182)}$$
$$2B_{(K)}x_1 = Jx_1 \quad \text{(183)}$$
$$2B_{(K)}x_1 = \begin{bmatrix} \sum_i x_i \\ \vdots \end{bmatrix}. \quad \text{(184)}$$

Noting that the bottom row of $B_{(K)}$ is always the all-ones vector by the definition, we can consider the bottom element of (185)

$$2 \sum_i x_i = \sum_i x_i \quad \text{(186)}$$
$$\implies \sum_i x_i = 0. \quad \text{(187)}$$

This means $Jx_1 = 0$, which together with (184) gives:

$$B_{(K)}x_1 = 0. \quad \text{(188)}$$

By the induction hypothesis, this must mean $x_1 = 0 = x_2$, contradicting $x \neq 0$. \hfill \Box

**Theorem 8.9.** For all $K$, $\text{APD}_K$ is a noPREF game, and thus has a MERP strategy with value 1 and $\omega^*(\text{APD}_K) = 1$. The same holds for any choice of $\hat{s}$.

**Proof.** First, we demonstrate that $(A_{(K)})^T$ has trivial kernel.

We have from Lemma 8.8 that $B_{(K)}$ has trivial kernel, and thus its rank is $m = 2^K$. $A_{(K)}$ includes all columns of $B_{(K)}$ except the last, the all-ones vector. $A_{(K)}$ also includes columns of $\bar{B}_{(K)}$. Adding a column of $B_{(K)}$ to the corresponding column of $\bar{B}_{(K)}$ produces the all-ones vector, so it must be in the column-span of $A_{(K)}$ as well. Finally, this means the column span of $A_{(K)}$ includes the column span of $B_{(K)}$ and so the rank must be $m$. By the rank-nullity theorem, matrix $(A_{(K)})^T$ has trivial kernel.

The PREF constraints are unsatisfiable, so $\text{APD}_K$ is a noPREF game. By Theorem 5.30, $\text{APD}_K$ has a MERP strategy with value 1 and $\omega^*(\text{APD}_K) = 1$. \hfill \Box

### 8.3.2 Classical Value

We extend the motivating classical results presented in Section 7.3 to analyze the classical value of the APD family. Corollary 7.4 demonstrates that the set of outputs achievable by a deterministic classical strategy is given exactly by $\mathcal{Y}_2 := \text{im}_{\mathbb{F}_2^m}(A)$. Recalling that $\sigma_2 = \dim \mathcal{Y}_2$, we see that when $\sigma_2 \ll m$, the set of deterministically achievable outputs is much smaller than the total space of possible parity bit vectors, and so we should be able to find a vector $\hat{s} \in \mathbb{F}_2^m$ with large Hamming distance from all outputs in $\mathcal{Y}_2$. In this section the probabilistic method is used to formalize this argument.

37
Theorem 8.10. Let \( A \) be an XOR game matrix, for which \( \sigma_2 \leq \delta m \). Then there exists a parity bit vector \( \hat{s} \in \mathbb{F}_2^m \) for which the game \( G \sim (A, \hat{s}) \) has value at most

\[
\frac{1}{2} + \sqrt{\frac{\delta}{2}}
\]  

(189)

Proof. This argument is a close variant of the usual Hamming bound on error-correcting codes. Let \( S \) denote the set of \( \hat{s} \) within distance \( m(1/2 - \varepsilon) \) of some point in \( \mathcal{Y}_2 \). Using the fact that \( |\mathcal{Y}_2| = 2^{\sigma_2} \leq 2^{\delta m} \) we have

\[
|S| \leq 2^{\delta m} \sum_{k \leq m(1/2 - \varepsilon)} \binom{m}{k}.
\]  

(190)

We bound the sum over binomial coefficients with the Chernoff bound to obtain

\[
|S| \leq 2^{\delta m} 2^m (1 - 2\varepsilon^2).
\]  

(191)

Then for any \( \varepsilon > \sqrt{\delta/2} \) there exists a \( \hat{s} \) with distance \( \geq m(1/2 - \varepsilon) \) from any point in \( \mathcal{Y}_2 \). This corresponds to value \( 1/2 + \varepsilon \).

We now consider the specific case of the APD game and demonstrate the asymptotic limit of the classical value.

Lemma 8.11. Given \( K \in \mathbb{N} \), the APD game \( \text{APD}_K \) has \( \sigma_2(\text{APD}_K) = K + 1 \).

Proof. Recall that \( \sigma_2 \) is the dimension of \( \mathcal{Y}_2 \), the image of \( A_K \) viewed as a map taking \( \mathbb{F}_2^{kn} \to \mathbb{F}_2^m \). Equivalently, \( \mathcal{Y}_2 \) is the column span of \( A_K \) taken over \( \mathbb{F}_2 \), and for this proof we use this view. By the same argument as Theorem 8.9, the column span of \( A_K \) is identical to the column span of \( B_K \). We prove this Lemma by induction over the \( B_K \):

1. Base case: \( B(0) = [1] \) giving \( \sigma_2 = 1 \) by inspection.

2. Induction step: Assume \( \sigma_2(\text{APD}_K) = K + 1 \), meaning the dimension of the column span of \( B_K \) over \( \mathbb{F}_2 \) is \( K + 1 \). We can write \( B_{K+1} \) in block format:

\[
B_{K+1} = \begin{bmatrix} B_K & B_K \\ B_K & B_K \end{bmatrix} = \begin{bmatrix} (J - B_K) & B_K \\ B_K & B_K \end{bmatrix} = \begin{bmatrix} (J + B_K) & B_K \\ B_K & B_K \end{bmatrix} \quad \text{(over } \mathbb{F}_2) \tag{192}
\]

All columns in the right block of (192) take the form \([x \ x]^T\), so their span is

\[
S := \left\{ [r \ r]^T : r \in \mathcal{Y}_2(\text{APD}_K) \right\}.
\]  

(193)

On the other hand, all columns in the left block take the form \([1 \oplus x \ x]^T = [1 \ 0]^T + [x \ x]^T\). The form of the right block span guarantees \([1 \ 0]^T\) is linearly independent from the right columns. Thus the total column span is

\[
\mathcal{Y}_2(\text{APD}_{K+1}) = S \cup \left( S + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \tag{194}
\]

and \( \sigma_2(\text{APD}_{K+1}) = \sigma_2(\text{APD}_K) + 1 = (K + 1) + 1 \), completing the induction step.

Theorem 2.5 (restated). The APD family has classical value

\[
\frac{1}{2} \leq \omega(\text{APD}_K) \leq \frac{1}{2} + \sqrt{\frac{K+1}{2^{K+1}}} \leq \frac{1}{2} + \sqrt{\frac{\log k}{k}}.
\]  

(195)
Proof. The lower bound of $\frac{1}{2}$ applies to all XOR games since a random assignment will satisfy half the clauses in expectation.

For the first upper bound, note that for APD family, $m = 2^K$ and from Lemma 8.11, $\sigma_2 = K + 1$. Then Theorem 8.10 yields the bound

$$\omega(\text{APD}_K) \leq \frac{1}{2} + \sqrt{\frac{\sigma_2}{2m}} = \frac{1}{2} + \sqrt{\frac{K + 1}{2^{K+1}}} \leq \frac{1}{2} + \sqrt{\frac{K}{2^K}}.$$ (196)

The last bound in the theorem statement is obtained by noting that $K = 2^k$.

Finally, we conclude by mentioning that even though the APD construction may require an exponential time to choose the adversarial $s_i$, one can achieve the same asymptotic difference with high probability by choosing the $s_i$ uniformly at random. This is implicit in the proof of Theorem 8.10, which implies that a randomly chosen $s$ has value $\geq 1/2 + \varepsilon$ with probability $\leq 2^{(d-2\varepsilon^3)m}$. Note as well that $\omega^* = 1$ for any choice of $s_i$, according to Theorem 8.9.

9 Random Games

The previous sections give a complete characterization of symmetric games with commuting-operator value 1. However, as demonstrated by the final example of the previous Section (8.1), non-symmetric games remain, in general, hard to characterize. One area where we can make some progress is in understanding the value of randomly generated XOR games. We will work in a model, specified in Definition 5.5, where each clause is sampled uniformly with replacement from the set of all possible clauses.

The classical value of random CSPs\textsuperscript{15} in this model has been intensely studied for several predicates including XOR, and it is useful to summarize the classical results. While determining the exact classical value of a random $k$-XOR instance for $k \geq 3$ remains hard, union bound arguments can give probabilistic bounds on the classical value of random $k$-XOR instances, in terms of the number of variables $n$ and the number of clauses $m$. Combining these with second moment-type arguments and combinatorial analysis has revealed the existence of SAT and UNSAT phases for random instances in the limit of large $n$, which are separated by a sharp threshold in $m$ [25]. For $k = 3$, this threshold occurs at $m/n \approx 0.92$ [11]. When $m/n$ is below the threshold, a random 3-XOR instance has value 1 with probability approaching 1 as $n \to \infty$, while when $m/n$ is above the threshold, a random instance has value 1 with probability approaching 0, and in fact, in the UNSAT phase, it is known that the value is close to 1/2. In addition to the true value, one can study the performance of the SoS algorithm on random instances. A key result in this direction is that of Grigoriev [16], who showed the existence of a region in the UNSAT phase with classical value close to 1/2, but for which the classical SoS algorithm reports a classical value of 1 until a high level in the SoS hierarchy. In the language we have developed thus far, he showed this by proving that random XOR games with appropriately chosen $m$ and $n$ do not admit any short-length classical refutations. One can interpret this result as showing the existence of a phase which is both UNSAT and computationally intractable.

The goal of this section is to prove a quantum analogue of these results. We are limited in one important sense: classically, the existence of an UNSAT phase with value close to 1/2 is shown via a union bound on the set of possible classical strategies, but this tool is no longer available to us for quantum strategies. Using our refutation-based technology, the best we can say is that the commuting-operator value of a game is bounded a small distance away from 1 (see Section 6.1). At the same time, the quantum case presents us with an opportunity to go beyond what is possible classically: while the classical SoS algorithm has a natural upper bound at level $kn$, no such bound exists for the ncSoS algorithm. We could thus potentially improve on Grigoriev’s result to prove a superexponential lower bound on the runtime of ncSoS.

We work subject to these considerations. In one direction, we know that for any $G$, $\omega^*(G) \geq \omega(G)$, and so we immediately get an entangled SAT phase for 3-XOR games with $m \leq 0.92n$. In the other direction we show the existence of an entangled UNSAT phase: specifically, we show that there exists a constant $C_k$ depending only on the number of players $k$ such that random games with more than $C_k n$ queries have

\textsuperscript{15}As noted in Section 1, CSPs and games are closely related. Classically, the difference between a CSP and the associated symmetric game is that each player in a game may play according to a different assignment of the variables; thus, the value of a CSP is always less than or equal to the classical value of the associated symmetric game.
commuting-operator value \(<1\) with high probability. For 3-XOR games we find \(C_3 \lesssim 4\). Our bounds on the entangled SAT and UNSAT phases are only a constant factor apart, leaving open the possibility of a sharp threshold behavior as in the classical case.

Further, in analogy with Grigoriev’s results, we also show that random XOR games with \(m = O(n)\) queries have, w.h.p., no refutation with length less than \(\Omega(n \log(n)/\log(\log(n)))\). By Lemma 6.4, this implies ncSoS takes superexponential time to show these games have value \(<1\).

9.1 SAT Phase

To start, we will show how the existence of a SAT phase for \(k\)-XOR viewed as a CSP implies the existence of such a phase for \(k\)-player XOR games. This is a simple consequence of the connection between games and CSPs.

**Lemma 9.1.** For every \(k\)-XOR game \(G\) with \(m\) clauses and \(n\) variables, there exists a corresponding \(k\)-XOR CSP instance \(\Phi_G\) with the same number of clauses and variables, such that if \(\text{val}(\Phi_G) = 1\), then \(\omega(G) = 1\). Moreover, when \(G\) is chosen at random according to the distribution in Definition 5.5, the induced definition over \(\Phi_G\) is the one generated by uniformly sampling \(m\) clauses over \(n\) variables with replacement.

**Proof.** For each clause \((q_{i1}, \ldots, q_{i\ell}, s_i) \in G\), create a clause \(x_{i1} x_{i2} \ldots x_{i\ell} = s_i\) in \(\Phi_G\), where the variables \(x_i\) are taken over \(\{\pm 1\}\). (We allow \(\Phi_G\) to contain repeated clauses.) It is clear that \(\Phi_G\) has the same number of clauses and variables as in \(G\), and that if \(G\) is random then \(\Phi_G\) is distributed as in the lemma statement.

If \(\Phi\) has value 1, let \(x\) be a satisfying assignment for \(\Phi\). Then the classical strategy when all players play according to \(x\) is a strategy for \(G\) achieving value 1. Hence \(\text{val}(\Phi_G) = 1\) implies that \(\omega(G) = 1\).

**Corollary 9.2.** For every \(k\), there exists a constant \(B_k\) such that for any \(b \leq B_k\), a random \(k\)-XOR game with \(m = bn\) clauses will have \(\omega(G) = \omega^*(G) = 1\) with probability approaching 1 as \(n \to \infty\).

**Proof.** The analogous statement for \(k\)-XOR CSP instances is proved in Theorem 16 of [25]. Let \(B_k\) be the threshold appearing in that theorem. By Lemma 9.1, if we sample a random \(k\)-XOR game \(G\) with \(m = bn\) clauses, then the associated CSP instance \(\Phi_G\) will be a random CSP instance with \(bn\) clauses, and thus have value 1 with probability approaching 1. Hence, \(\omega(G) = \omega^*(G) = 1\) with probability approaching 1 as well.

For \(k = 3\), the constant \(B_k\) can be computed to be \(\approx 0.92\) [11].

9.2 UNSAT Phase

Since we are considering general random XOR games, we cannot appeal to the shift gadgets available by symmetry. Instead we use probabilistic analysis to show that such gadgets exist with high probability, given enough clauses. Below we give the analysis for the specific case of random 3-XOR games. The analysis for general \(k\) proceeds identically, with different constants depending on the number of players.

**Lemma 9.3.** Let \(G\) be a randomly generated 3-XOR game defined by the set \(M\) of queries and associated parity bits, with \(|M| = m \geq 3.3n\). Then with probability \(1 - o(1)\), there exists a set \(N_{3,1} \subseteq [n]\) with \(|N_{3,1}| > 0.95n\) such that for all \(a, b \in N_{3,1}\), \(G\) contains a shift gadget

\[
S^{3-1}(ab).
\]

**Proof.** Consider a bipartite graph between two sets of \(n\) vertices. Label one set of vertices by \(([n], 3)\), and the other by \(([n], 2)\). Add an edge between \((j, 3)\) and \((j', 2)\) iff there exists a query

\[
\begin{bmatrix}
  r \\
  j' \\
  j
\end{bmatrix} \in M
\]

where \(r \in [n]\) is arbitrary. Label the edge by the index of the query corresponding to it. Our key observation is that that \(S^{3-1}(ab)\) can be constructed from the queries corresponding to a walk from \((a, 3)\) to \((b, 3)\) in the graph.
Because queries are randomly generated, edges in this graph are randomly generated as well. So our graph is a $G_{n,n,m}$ Erdős–Rényi random bipartite graph. A technical result (Lemma 9.4) gives that this graph is at least as connected as $\hat{G}_{n,n,p}$ - a random bipartite graph in which each edge is present independently with probability $p = m/n^2 - \epsilon/n = (3.3 - \epsilon)/n$, where $\epsilon$ is an arbitrary small constant.

Finally, applying a Galton-Watson style argument to this random graph shows [20, Theorem 9] that with probability $1 - o(1)$ it contains a “giant component” that touches at least $\gamma n$ vertices of $(\lceil n \rceil, 3)$, where $\gamma$ is the unique solution in the interval $(0, 1]$ to the equation

$$\gamma + \exp \left( p m (\exp(-p n \gamma) - 1) \right) = 1 \implies \gamma > 0.95.$$ 

Lemma 9.4 (Relating random graph models). Let $G \sim G_{N,N,m}$ with $m = CN$. Further let $\hat{G} \sim \hat{G}_{N,N,p}$ with $p = (C - \epsilon)/N$, for arbitrary small constant $\epsilon$. For any value $Z$, if $\hat{G}$ contains a connected component of size $Z$ with probability $1 - o(1)$ then $G$ also contains a connected component of size $Z$ with probability $1 - o(1)$.

Proof. We couple the distributions used to generate $\hat{G}$ and $G$. In particular, a graph $G$ can be generated by choosing a graph $\hat{G}$, then randomly adding or removing edges until the graph has exactly $m$ edges. As long as we only add edges, this process will only increase the size of the largest connected component in the graph. Letting $E(\hat{G})$ be the set of edges of a graph $\hat{G}$, we find

$$\mathbb{E}[|E(\hat{G})|] = N^2 p = (C - \epsilon)N$$

and so

$$\mathbb{P}\{ |E(\hat{G})| > m \} \leq \exp(-c^2 N/3) = o(1)$$

by a Chernoff bound.

Lemma 9.3 tells us that, given a large enough number of queries, most variables can be shuffled in exactly the manner described in Section 6.2.2. If we consider only queries involving these variables, we should then be able to construct refutations from PREFs using exactly the techniques described in the latter half of that section. In fact, we only need to restrict to those variables on $k - 2$ of the wires, since cancellations on the first two wires are automatic (see, in particular, the proof of Lemma 6.22).

If a large enough number of queries remain one would expect that they admit a PREF with high probability. This fact is proved below.

Lemma 9.5. For any $k$-XOR game $G$ with $m$ queries, alphabet size $n$ and

$$m - kn = \delta > 0,$$  \hspace{1cm} (197)

if the parity bits for $G$ are picked randomly then $G$ has a PREF with probability at least $1 - 2^{-\delta}$.

Proof. By definition, a PREF specification is any vector $z \in \mathbb{Z}^m$ satisfying

$$A^T z = 0 \text{ and } \hat{s}^T z = 1.$$  \hspace{1cm} (198)\hspace{1cm} (199)

When $m > kn$, the matrix $A^T$ has rank $\leq kn$. By the rank-nullity theorem, the kernel of $A^T$ has dimension $\geq m - kn$, and so the are at least $\delta$ linearly independent vectors $z$ satisfying (198). If the parity bits are chosen randomly, each of these vectors $z$ satisfy (199) with probability 1/2, and the result follows.

Finally, we use our lemmas to prove the specific $k = 3$ case of the random game threshold.

Theorem 2.6 (repeated). Let $G$ be a random 3-XOR game with $m = \lceil 3.3n \rceil$ clauses on an alphabet of size $n$. Then, with probability $1 - o(1)$, $G$ has value $< 1$.  

41
Proof. Let \( N_{3,1} \) be defined as in Lemma 9.3, and extend this definition to \( N_{3,2} \) analogously. Define
\[
N_3 := N_{3,1} \cap N_{3,2}.
\] (200)

Let \( \gamma \) be defined as in Lemma 9.3. A union bound then gives that the expected size of of \( N_3 \) is bounded below by
\[
(1 - 2(1 - \gamma)) > 0.9n.
\]

Finally we let \( M \) be the set of queries for \( G \), then define
\[
M' := \{(q^{(1)}, q^{(2)}, q^{(3)}) \in M : q^{(3)} \in N_3\}.
\]

If \( N_3 \) were independent of \( M' \), we could conclude
\[
\mathbb{E}[|M'|] = \frac{m|N_3|}{n} > 3.01n
\] (201)

and then, by concentration,
\[
P\{|M'| < 3.009\} \lesssim \exp(-n) = o(1).
\] (202)

\( M \) and \( N_3 \) are not independent, but a technical lemma (Lemma 9.6) shows their correlation can only increase the size of \( M' \), hence (202) remains valid.

Now consider a game \( G' \) consisting of only the clauses of \( G \) with queries in \( M' \). \( M' \) has been constructed such that \( G' \) has shuffle gadgets for any wire of a pair of queries drawn from \( M' \). Furthermore \(|M'| - 3n \geq 0.009n\) with high probability, so by Lemma 6.21 and Lemma 9.5, we can then conclude \( G' \) contains a complete refutation with probability \( 1 - o(1) \). Since \( G' \) contains a subset of the clauses of \( G \), this also means \( G \) contains a complete refutation with probability \( 1 - o(1) \).

Lemma 9.6. Let \( G \) be a random 3-XOR game on \( m \) clauses, and let \( N_3 \) and \( M' \) be defined as in the proof of Theorem 2.6. If there exists some constant \( \delta \) for which
\[
\mathbb{E}[|N_3|] \geq \delta n
\]

with probability \( 1 - o(1) \), then we have, for any \( \epsilon > 0 \) that
\[
\mathbb{E}[|M'|] \geq (\delta - \epsilon)m
\]

with probability \( 1 - o(1) \) as well.

Proof. We first move from the random game \( G \) to the random game \( \hat{G} \), in which the total number of clauses isn’t fixed, but rather every possible clause appears in the game with probability\(^{16}17\)
\[
\frac{m - \epsilon_1}{2n^3}.
\] (203)

We also define the variables \( \hat{N}_3, \hat{M} \) and \( \hat{M}' \), which depend on \( \hat{G} \) in exactly the same way the unhatted variables depends on \( G \). By an argument identical to the one used in the proof of Lemma 9.4, lower bounds on the size of \( \hat{M}' \) will carry over to lower bounds on the size of \( M' \) for \( G \) with high probability.

The techniques used to bound the size of \( N_3 \) work equally well on \( \hat{N}_3 \), and so
\[
|\hat{N}_3| \geq (\delta - \epsilon_1 - \epsilon_2)n
\] (204)

with probability \( 1 - o(1) \).

Now we let \( A \) be some arbitrary subset of \([n]\) of size \([(\delta - \epsilon_1 - \epsilon_2)n]\), and define
\[
\hat{M}(A) = \{(q^{(1)}, q^{(2)}, q^{(3)}) \in \hat{M} : q^{(3)} \in A\}.
\]

\(^{16}\)Note the factor of 2 in the denominator comes from the choice of parity bit.

\(^{17}\)Here and below we use \( \epsilon_i \) to indicate arbitrary small constants.
Since $A$ is arbitrary, it is immediate that

$$\mathbb{E} \left[ |\hat{M}(A)| \right] = (\delta - \epsilon_1 - \epsilon_2)m$$

(205)

and (by concentration)

$$\mathbb{P} \left\{ |\hat{M}(A)| < (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \right\} = o(1).$$

(206)

Finally, we define the indicator random variables $I_q$ to take on value 1 if $q \in \hat{M}$, and 0 otherwise. Our key observation is that

$$\mathbb{E} \left[ I_q \mid A \subseteq N_3 \right] = \mathbb{E} [I_q] \left( \frac{\mathbb{P} \{ A \subseteq N_3 \mid I_q = 1 \}}{\mathbb{P} \{ A \subseteq N_3 \}} \right) \geq \mathbb{E} [I_q]$$

(207)

(208)

and this remains true even after conditioning on the outcomes of other $I_q$’s.

The indicator for the event

$$\left\{ |\hat{M}(A)| < (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \right\}$$

(209)

is a decreasing function of the $I_q$’s, and so we can conclude

$$\mathbb{P} \left\{ |\hat{M}(A)| \leq (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \mid A \subseteq N_3 \right\} \leq \mathbb{P} \left\{ |\hat{M}(A)| < (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \right\}$$

(210)

Putting this all together, we find

$$\mathbb{P} \left\{ |\hat{M}'| \leq (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \right\} \leq \mathbb{P} \left\{ |\hat{M}(A)| < (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \mid A \subseteq N_3 \right\} \leq \mathbb{P} \left\{ |\hat{M}(A)| < (\delta - \epsilon_1 - \epsilon_2 - \epsilon_3)m \right\}$$

(211)

(212)

(213)

(where the first line follows from definition of $M'$). Since $|\hat{M}'|$ is a lower bound for $|M'|$ with high probability, we can set $\epsilon = \epsilon_1 + \epsilon_2 + \epsilon_3$ and conclude the result.

9.3 Lower Bound on Refutation Length (Sketch)

In this section we sketch the proof of the following theorem, which gives a lower bound that holds with high probability for the length of refutations of random 3-XOR games. Aside from the immediate implications of the theorem, this result is also significant because its proof uses a counting technique not found elsewhere in the paper.

**Theorem 2.7 (restated).** For any constant $C$, the minimum length refutation of a random 3-XOR game with $m = Cn$ queries on an alphabet of size $n$ has length at least

$$\frac{en \log(n)}{8C^2 \log(\log(n))} - o \left( \frac{n \log(n)}{\log(\log(n))} \right)$$

(214)

with probability $1 - o(1)$ (as $n \to \infty$). Hence, either $\omega^* = 1$ or $\Omega(n \log(n)/\log(\log(n)))$ levels of the ncSoS hierarchy are needed to witness that $\omega^* < 1$ for such games.

This significance of this result is twofold. Firstly, it gives a lower bound on refutation lengths which matches the length of refutations constructed using the methods of Section 6.3 to a factor of $O(\log(\log(n)))$. 

43
This suggests that the algorithm described in Section 6.3 is a near-optimal method for constructing refutations for symmetric XOR games.\footnote{Strictly speaking, this conclusion is motivated only for 3-XOR games. That being said, for larger \( k \), Theorem 2.7 still gives a lower bound which is tight to a factor of \( C_4 \log(n) \), and it is reasonable to expect that, with additional work, this lower bound could be tightened further.} Secondly, combining Theorem 2.7 with Lemma 6.4 show that an ncSoS proof that a random 3-XOR game has value \( < 1 \) requires going to level \( \Omega(n \log(n)/\log(\log(n))) \) in the ncSoS hierarchy. This results in a runtime which is superexponential in \( n \), and longer than the worst possible case for classical (commuting) SoS applied to XOR games (or boolean CSPs in general).

Theorem 2.7 is proved using a careful application of the first moment method. The full analysis is somewhat involved, and so we spend some time discussing the key ideas required for the proof. The proof hinges on enumerating possible refutations in a somewhat non-intuitive way. Rather than building up a refutation of length \( \ell \) query by query, we will instead write down all possible sequences of \( \ell \) queries, and consider all the ways those queries could cancel to form a refutation. The key definition required to make this counting work is that of a cancellation pattern.

**Definition 9.7.** A length \( \ell \) one wire cancellation pattern is a partition of \([\ell]\) into \( \ell/2 \) pairs of the form \((a_1, b_1), \ldots, (a_{\ell/2}, b_{\ell/2})\) with

\[
a_i < b_i \quad \text{and} \quad a_i < a_j \implies b_i > b_j
\]

\( \forall \, i, j \in [\ell/2] \) (no cancellation patterns exist for odd \( \ell \)). When discussing \( k \)-XOR games, a length \( \ell \) cancellation pattern refers to an ordered list containing \( k \) one wire cancellation patterns.

**Definition 9.8.** Given a length \( \ell \) cancellation pattern, the locations of that cancellation pattern are elements of \([\ell]\), corresponding to the positions at which queries can appear in the cancellation. The sites of the cancellation pattern are specified by coordinates \((\alpha, i) \in [k] \otimes [\ell]\), and represent the places where individual questions appear. Site \((\alpha_1, i_1)\) is said to cancel site \((\alpha_2, i_2)\) iff \( \alpha_1 = \alpha_2 \) and the pair \((i_1, i_2)\) is contained in the \( \alpha_1 \)-th cancellation pattern. In this case, the pair of sites \(((\alpha_1, i_1), (\alpha_2, i_2))\) is referred to as a cancellation.

**Definition 9.9.** Using matrix notation to specify individual letters in a word, a cancellation pattern is valid on a word \( W \) iff

\[
w_{\alpha_1, i_1} = w_{\alpha_2, i_2}
\]

for all sites \((\alpha_1, i_1)\) and \((\alpha_2, i_2)\) which cancel one another.

By definition, a word cancels to the identity iff there exists at least one cancellation pattern which is valid on the word. It is also straightforward to give a combinatorial bound on the number of possible length \( \ell \) cancellation patterns.

**Claim 9.10.** The number of possible cancellation patterns on a single wire with \( \ell \) locations is given by the \( \ell/2 \)-th Catalan number, denoted by \( C_{\ell/2} \). The number of possible cancellation patterns on a length \( \ell \) word formed from \( k \)-XOR queries is then given by

\[
(C_{\ell/2})^k \leq 2^{\ell^2}.
\]

**Proof.** Direct from the definition of Catalan numbers, and standard bounds on their size. See [30] for an extensive discussion.

To illustrate the benefit of working in terms of cancellation patterns, we prove a simple theorem, regarding the existence of a restricted class of refutations.

**Theorem 9.11.** Let \( m \in o(n^{k/2}) \). Then, as \( n \to \infty \), a random \( k \)-XOR game with \( m \) queries on an alphabet of size \( n \) will contain a refutation in which every query is used at most once with probability at most \( o(1) \).

**Proof.** We apply the first moment method. There are \( \ell^m \) ways of creating a word of length \( \ell \) from the queries, and at most \( 2^{\ell^2} \) cancellation patterns on the word. Since queries are all independent and randomly
chosen, each cancellation pattern on a length $\ell$ word is valid with probability $(1/n)^{k\ell/2}$. Then the probability of a valid cancellation of any length is given by (using $(m)(m-1)...(m-2r) \leq m^{2r}$)

$$
\sum_{r=1}^{m/2} \left[ (2r)! \binom{m}{2r} (C_r)^k (1/n)^{kr} \right] \leq \sum_{r=1}^{m/2} \left[ 2^k \left( m/n^{k/2} \right)^{2r} \right] \in o(1).
$$

(218)

We now take a small detour, and use techniques similar to the one above to reprove a result of Grigoriev [16]. This is done to illustrate the power of these techniques, but also for completeness, as we will use Grigoriev’s result in our proof of Theorem 2.7.

**Theorem 9.12** (Originally proved in [16]). Let $G$ be a random 3-XOR game on the set of queries $M$, with $|M| = m = Cn$ and alphabet size $n$. Define a classical refutation to be a subset of queries $T \subseteq M$ such that

$$
|\{ q \in T \mid q^{(\alpha)} = j \}| = 2m \forall j \in [n], \alpha \in \{1, 2, 3\}
$$

(219)

(if written as a word, $T$ would contain each $j \in [n]$ an even number of times on each wire). Then, with probability $1 - o(1)$ as $n \to \infty$ the shortest classical refutation contained in $m$ has length at least $en/C^2$.

**Proof.** We again use the first moment method, paralleling the argument used in the proof of Theorem 9.11. We find $(C^n)$ ways of choosing $\ell$ queries from $M$, and $((\ell - 1)!!)^3$ ways of pairing up letters on all rows once $\ell$ queries have been chosen (if $\ell$ is even). As before, each pair of letters is equivalent independently with probability $(1/n)$ and so by the union bound the probability of a classical refutation of length less than $\ell$ is bounded by

$$
\sum_{r=1}^{\ell/2} \left[ \frac{C^n}{2r} ((2r - 1)!!)^3 (1/n)^{3r} \right] \leq \sum_{r=1}^{\ell/2} \left[ (Cn)^{2r} (2^r r!) (1/n)^{3r} \right]
$$

$$
= \sum_{r=1}^{\ell/2} \left[ r! (2C^2/n)^r \right]
$$

(221)

$$
\leq \sum_{r=1}^{\ell/2} \left[ e\sqrt{\pi} (2C^2 r/(en))^r \right].
$$

(222)

Noting this sum is $o(1)$ provided $\ell C^2/en < 1$ completes the proof.

Returning to the informal proof of Theorem 2.7, the natural approach is to try to generalize the proof of Theorem 9.11 by allowing repeated queries and repeating the union bound analysis. Unfortunately, when queries are repeated not all cancellations are valid independent of one another, which makes it dramatically more difficult to compute the probability of a given cancellation pattern being valid. To accommodate this, we require additional terminology for discussing the different types of cancellations that can occur when a cancellation interacts with a word containing repeated queries. This is introduced below, along with a brief discussion of how these cancellations are accounted for in the full proof.

**Definition 9.13.** Given a cancellation pattern on a word made up of queries from a random $k$-XOR game, define:

- **The set of independent cancellations** to be a maximal set of cancellations so that each cancellation is valid independent of all others in the set with probability $1/n$.

- **The set of dependent cancellations** to be the set of cancellations which are valid with probability 1 if all independent cancellations are valid.

- **The set of self cancellations** to be the set of all cancellations which are valid with probability 1 independent of all other cancellations (these occur when a query is canceled with itself).
A full cancellation pattern is a cancellation pattern where cancellations are specified to be independent, dependent or self ahead of time, and this full cancellation pattern is valid on a word iff the sets defined above are compatible with the way the cancellations are labeled ahead of time.

Note there is some freedom in which cancellations are chosen as dependent vs. independent. This ambiguity allows us to simplify the full proof, and is left in intentionally.\textsuperscript{19} Semi-formally, we can now give the proof of Theorem 2.7 as follows:

\textit{Proof (semi-formal).} Our goal is to show that, under the conditions of Theorem 2.7, any cancellation pattern on a word consisting of a small number of queries is valid with vanishing probability. We restrict our attention to minimum length refutations: refutations for which no subset of queries can be removed while leaving a valid refutation.

We then attempt a union bound argument in which we identify the various ways queries can interact with cancellation patterns in the refutation. We begin by segmenting the queries in the refutation into maximal strings of queries connected via dependent or self cancellations. We call these phrases. By definition, the phrases themselves must be connected by independent cancellations.

We can bound the number of ways of building a phrase of length \( k \). The first query in a phrase can be picked arbitrarily from a set of size \( m \). After that, a query connected to a known query by a self-cancellation is fixed exactly, and concentration inequalities can be used to show that a query connected to a fixed query via a dependent cancellation is drawn from a set of size at most \( m \log(n)/n \).\textsuperscript{20} Then the ways of choosing queries such that they form the given phrase is bounded by

\[
m \left( \frac{m \log(n)}{n} \right)^{k-1}.
\]

We next place some restrictions on the number and type of phrases that can occur in a refutation. By minimality, each phrase must contain at least one site involved in an independent cancellation (otherwise the phrase is “redundant”); then by parity each phrase must contain two. We also get a bound on the number of queries appearing an odd number of times. Removing all queries that occur an even number of times, and leaving only one copy of each query that occurs an odd number will produce a classical refutation. Theorem 9.12 then tells us that with probability \( 1 - o(1) \), any valid refutation must have \( en/C^2 \) queries which occur an odd number of times.

We then use a result from the technical proof: for \( p \) phrases and \( s \) sites with independent cancellations,

\[
s \geq 2p + en/4C^2.
\]

Using (223) to bound the number of ways each phrase occurs, and a factor of \( 1/\sqrt{n} \) per site in an independent cancellation (making \( 1/n \) per independent cancellation) we find that any full length-\( \ell \) cancellation pattern is valid on some word of \( \ell \) queries with probability at most

\[
m^p \left( \frac{m \log(n)}{n} \right)^{\ell-p} \left( \frac{1}{n} \right)^{s/2} \leq m^p \left( \frac{m \log(n)}{n} \right)^{\ell-p} \left( \frac{1}{n} \right)^{p+en/8C^2}
\]

\[
\leq \left( \frac{1}{\log(n)} \right)^p \left( \frac{1}{n} \right)^{en/8C^2} (C \log(n))^{\ell}
\]

\[
\leq \left( \frac{1}{n} \right)^{en/8C^2} (C \log(n))^{\ell}.
\]

Adding in a union bound over all possible length \( \ell \) full cancellation patterns, we find the probability of a

\textsuperscript{19}Of course, it could also be removed by fixing a convention for the cancellations which are labeled independent (i.e. choosing the lexicographically minimal set).

\textsuperscript{20}Proved in Lemma 9.16
valid length $\ell$ cancellation pattern existing is at most

\[
C_{\ell/2}^{3/2} 3^{\ell/2} \left( \frac{1}{n} \right)^{en/8C^2} \leq 12^{3/2} \left( \frac{1}{n} \right)^{en/8C^2} (C \log(n))^\ell
\]

\[
\leq \left( \frac{1}{n} \right)^{en/8C^2} (42C \log(n))^\ell.
\]

Setting $m/n = C$ and following through the geometric series we find the probability of a refutation of length less than or equal to $\ell$ existing is at most

\[
\frac{42C \log(n)^{\ell+1}}{n^{en/8C^2} + o(1)}
\]

where the $o(1)$ term comes from the use of results 9.12 and 9.16 in our proof. It follows that the total probability of refutation is $o(1)$ unless

\[
\ell \geq \frac{en \log(n)}{8C^2 \log(42C \log(n))} - 1
\]

completing the proof of Theorem 2.7.

While the proof above was hopefully convincing, it wasn’t completely formal. A more careful proof that clearly discusses the various events the union bound is constructed over is given below.

### 9.4 Lower Bound on Refutation Length (Full Proof)

For the most part, the key ideas used in the proof of Theorem 2.7 are well covered in Section 9.3. The remaining details are primarily technical, but somewhat involved. We begin by formalizing the definition of a **phrase**, used informally above.

**Definition 9.14.** Consider a full cancellation pattern consisting of dependent, self and independent cancellations. Let $G$ be a graph with vertices corresponding to dependent or self cancellations in the cancellation pattern. Add an edge between vertices if the corresponding cancellations overlap at some location. The sets of cancellations corresponding to connected components in this graph are called **phrases**.

Our analysis will require language specific to the ways in which queries and phrases can occur in a refutation. That language is introduced below.

**Definition 9.15.** Given a refutation, we define the following sets:

- $L_r$ is the set of locations located at the leftmost point in some phrase. We call queries at these locations **roots**.
- $L_c$ is the set of all locations in phrases which are not the leftmost point of a phrase. Queries at these locations are called **constrained queries**.
- $P$ is the set of all phrases in the cancellation pattern.
- $P_r \subseteq P$ is the set of all phrases for which every location in the phrase contains only self or dependent cancellations. Phrases in $P_r$ are called **redundant phrases**.
- $S$ is the set of all sites in independent cancellations.

Redundant phrases are so named because removing all queries contained in them still leaves a valid refutation. For this reason **minimal length refutations** are defined to be refutations that do not contain any redundant phrases.

We now prove a few basic properties about the structure of refutations constructed from random queries.
Lemma 9.16. Let $m = Cn$ for some constant $C$. Then, with probability $1 - o(1)$, all refutations for a random 3-XOR game on $m$ queries with $n$ variables will satisfy

1. The refutation contains at least $\frac{en}{C^2}$ distinct queries occurring an odd number of times.

2. The cancellations can be labeled so that $|S| \geq 2|P| + \frac{en}{4C^2}$.

3. For all queries $q_i$: the refutation implies that $q_i$ cancels with at most $C\log(n)$ other queries on each wire.

Proof. We prove 1 by appealing to [16]. Note we can obtain a classical refutation from a quantum refutation by taking a single copy of each query repeated an odd number of times. Then, we know from [16] (alternately Theorem 9.12) that there are $\frac{en}{C^2}$ distinct queries repeated an odd number of times in the quantum refutation.

To prove 2, we first note that every distinct query occurring an odd number of times must be involved in at least three independent cancellations (one per wire) across all locations where it appears, resulting in a total count of $3\frac{en}{C^2}$ cancellations. We will show that we can relabel independent and dependent cancellations such that at least $1/4$ of these independent cancellations are all contained in at most $\frac{en}{4C^2}$ phrases.

To do so, we begin by making a list of all queries occurring an odd number of times in our refutation, and consider a cancellation pattern on which only the self-cancellations have been fixed. We refer to a phrase induced by these self cancellations as a subphrase. We now extract a query from the list, pick an odd length subphrase involving that query (this subphrase may have length one), and mark three non-self cancellations coming from that subphrase as independent (one per wire). Next, we remove from our list any queries connected to this subphrase by the newly labeled independent cancellations. Removing the connected queries from the list ensures that any non-self cancellations involving elements remaining on our list will be independent from the cancellations we have labeled so far. We then repeat this process until we have exhausted all queries on our list, and then label the remaining cancellations in any valid manner.

Over this process, we remove at most three additional queries from the list for every subphrase we identify, so when we have exhausted all queries on this list (but before we have labeled any dependent cancellations), we will have at $\frac{en}{4C^2}$ subphrases containing at least $3\frac{en}{4C^2}$ independent cancellations. Each of these subphrases is contained in a phrase (since all locations are connected via self-cancellations) and labeling the remaining cancellations cannot change the cancellations already labeled as independent, so we have found at least $3\frac{en}{4C^2}$ independent cancellations contained in at most $\frac{en}{4C^2}$ phrases.

From here the proof of 2 is straightforward: by minimality, each phrase contains must contain at least one independent cancellation, and hence by parity each phrase must contain two. Furthermore, we have already identified a special set of at most $\frac{en}{4C^2}$ phrases which contain at least $3\frac{en}{4C^2}$ independent cancellations. Letting $p_1$ be the number of phrases identified so far, and $p_2$ be the number of phrases not contained in the set already identified, we see

$$|S| \geq 2p_2 + \frac{3en}{4C^2} \geq 2(p_2 + p_1) + \frac{en}{4C^2} = 2|P| + \frac{en}{4C^2}$$

(232)

as desired.

Finally, 3 follows from concentration of measure. We define $y(j)$ to be the random variable counting the number of queries with letter $j$ on the top wire, so

$$y(j) = \left|\{i : q_i^{(1)} = j\}\right|.$$  

(233)

It is then clear that

$$\mathbb{E}[y(j)] = m/n = C.$$  

(234)

By a Chernoff bound

$$\mathbb{P}\{y(j) \geq C\log(n)\} \leq e^{-(\log^2(n) - 1)C/3n} \leq 1/n^{C\log(n)/3} = o(1)$$

(235)

(236)

and so a union bound argument gives the result for large $n$. 

\[\square\]
The proof of Theorem 2.7 will follow from our observations in Lemma 9.16 and first moment arguments. To make clear the analysis, we first present a simple algorithm for generating minimal length refutations with length $\ell$ from a random set of queries $G$.

**Algorithm 9.17 (Refutation generator).**

**input:** A set of $m$ queries, with $m = Cn$, and parameter $\ell$

**output:** A minimal refutation of length $\ell$, or failure

1. Initialize $\ell$ locations where queries might be placed.
2. Randomly generate a cancellation pattern consisting of self, dependent and independent cancellations on the $\ell$ locations. Identify the phrases in this cancellation pattern.
3. If there is any redundant phrase, return *failure: not minimal*.
4. Randomly map queries to locations.
   (a) If the independent cancellations require there to be more than $C \log(n)$ queries which agree on any wire, or if the cancellation pattern would imply $|S| \leq 2|P| + en/4C^2$, return *failure: improbable cancellation*.
   (b) If self-cancellations occur between non-identical queries, or dependent cancellations are not implied by independent cancellations, return *failure: improper labeling*.
5. If any independent cancellations occur between queries which disagree on the wire where the cancellation is occurring, return *failure: invalid cancellation*.
6. Otherwise, return *success* along with the cancellation pattern and query mapping.

We prove Theorem 2.7 by proving two basic facts about Algorithm 9.17. Firstly, we show that, with high probability$^{21}$, there exists a random seed for which Algorithm 9.17 finds a refutation provided one exists. Secondly, we show the expected number of paths on which Algorithm 9.17 returns success is small unless $\ell$ is sufficiently large. We will prove these claims separately.

**Theorem 9.18 (Correctness).** Algorithm 9.17 only returns success when it finds a valid minimum length refutation. Furthermore, when the input queries are randomly selected, with probability $1 - o(1)$ the algorithm has a positive probability of finding all valid length $\ell$ refutations.

**Proof.** The first claim is clear from inspection of the algorithm. The second follows from Lemma 9.16 and further inspection. In particular, the only refutations not found by the algorithm are those which require greater than $C \log(n)$ queries to agree on a wire, or those with a cancellation pattern for which

$$|S| \leq 2|P| + en/4C^2.$$  \hfill (237)

Lemma 9.16 tells us that these cases occur with probability $o(1)$ for randomly chosen queries.

**Theorem 9.19.** Given a randomly chosen set of $m = Cn$ queries as input, the expected number of minimal length $\ell$ refutations which can be found by Algorithm 9.17 is upper bounded by

$$(1/n)^{c'/2C^2} (4C \log(n))^\ell.$$  \hfill (238)

In particular, we expect to find no refutations until

$$\ell = \Omega(n \log(n) / \log(\log(n))).$$  \hfill (239)

$^{21}$It should be stressed that this with high probability refers to the randomness associated with choosing the queries provided as input to the algorithm, not the randomness associated with the algorithm’s run.
Proof. We give an overcounting of the number of possible paths Algorithm 9.17 can take. We first note that a path can be completely specified by a choice of cancellation pattern and mapping of queries to locations.

Using our rough bound on the Catalan numbers, there are at most \( C_{\ell/2}^3 \leq \frac{4^{\ell/2}}{\ell/2} \) different ways of pairing up all sites for cancellations. Since each cancellation can be one of three types, we find a total of

\[ 3^{\ell/2} \frac{4^\ell}{\ell/2} \leq 42^\ell \]  

possible cancellation patterns.

We next give a rough (over)counting of the number of ways queries can be mapped to locations such that the cancellation pattern is not rejected in step 4 of the algorithm.

In particular, we allow arbitrary queries to be mapped to locations in \( L_r \). After this mapping, we note all remaining locations are in \( L_c \). Assuming the cancellation pattern was not rejected in step 4a, a location connected to a fixed query by a self cancellation can only have a single query mapped to it, and a location connected to a fixed query by a dependent cancellation can have at most \( C_{\log(n)} \) queries mapped. In total then, we find

\[ \frac{m}{|P|} \left( C \log(n) \right)^{|L_c|} = \frac{m}{|P|} \left( C \log(n) \right)^{|L_c|} \]  

possible mappings from queries to locations.

Finally, we bound the probability that our given query assignment doesn’t fail in step 5 of the algorithm. Noting independent cancellations are, by definition, independent we find the probability of failure is given by

\[ \left( \frac{1}{n} \right)^{|S|/2} \]  

Since our cancellation pattern doesn’t contain any redundant phrases, and was not rejected as improbable by the algorithm we also have

\[ |S| \geq 2|P| + \frac{en}{4C^2}. \]  

The overall expected number of successes for a given cancellation pattern can then be bounded by:

\[ \frac{m}{|P|} \left( \frac{C \log(n)}{n} \right)^{|L_c|} \left( \frac{1}{n} \right)^{|P|+\frac{en}{8C^2}} \leq \left( \frac{1}{\log(n)} \right)^{\frac{|P|}{\log(n)}} \left( \frac{1}{n} \right)^{\frac{en}{8C^2}} \left( C \log(n) \right) \frac{\ell}{\log(n)} \]

resulting in an overall bound on the expected number of successes for any length \( \ell \) of

\[ \left( \frac{1}{n} \right)^{\frac{en}{8C^2}} \left( 42C \log(n) \right)^\ell. \]  

Summing the geometric series, the expected total number of refutations of length less than \( \ell \) can then be bounded above by

\[ \left( \frac{1}{n} \right)^{\frac{en}{8C^2}} \frac{(42C \log(n))^{\ell+1} - 1}{(42C \log(n)) - 1}. \]  

We see this is \( o(1) \) unless

\[ \ell \geq \frac{en \log(n)}{8C^2 \log(\log(n))} - o \left( \frac{n \log(n)}{\log(\log(n))} \right), \]  

and the desired result follows from Markov’s inequality. \( \square \)

\( ^{22} \)As a word of caution: it should be noted the \( \left( \frac{en \log(n)}{(8C^2 \log(\log(n)))} \right) \) only dominates when \( C \) is taken to be a constant with respect to \( n \). When \( C \) scales with \( n \) the above analysis will still work, but requires more care in computing the final bound.
To close this section, we note Theorem 2.7 is immediate from Theorems 9.18 and 9.19.

References

[1] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. Physical review letters, 95(1):010503, 2005, arXiv:quant-ph/0405101.

[2] D. Bayer and P. Diaconis. Trailing the dovetail shuffle to its lair. The Annals of Applied Probability, 2(2):294–313, 1992.

[3] J. Briët, H. Buhrman, T. Lee, and T. Vidick. Multipartite entanglement in XOR games. Quantum Info. Comput., 13(3-4):334–360, Mar. 2013, arXiv:0911.4007.

[4] J. Briët and T. Vidick. Explicit lower and upper bounds on the entangled value of multiplayer XOR games. Communications in Mathematical Physics, 321(1):181–207, 2013, arXiv:1108.5647.

[5] B. S. Cirel’son. Quantum generalizations of Bell’s inequality. Letters in Mathematical Physics, 4(2):93–100, 1980.

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett., 23:880–884, Oct 1969.

[7] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In CCC ’04, pages 236–249, 2004, arXiv:quant-ph/0404076.

[8] R. Cleve and R. Mittal. Characterization of binary constraint system games. In International Colloquium on Automata, Languages, and Programming, pages 320–331. Springer, 2014.

[9] R. Colbeck. Quantum And Relativistic Protocols For Secure Multi-Party Computation. PhD thesis, University of Cambridge, 2006, arXiv:0911.3814.

[10] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner. The quantum moment problem and bounds on entangled multi-prover games. In CCC ’08, pages 199–210, 2008, arXiv:0803.4373.

[11] O. Dubois and J. Mandler. The 3-XORSAT threshold. Comptes Rendus Mathématique, 335(11):963–966, 2002.

[12] A. K. Ekert. Quantum cryptography based on Bell’s theorem. Physical review letters, 67(6):661, 1991.

[13] T. Fritz, T. Netzer, and A. Thom. Can you compute the operator norm? Proceedings of the American Mathematical Society, 142(12):4265–4276, 2014, arXiv:1207.0975.

[14] J. Gao. Quantum union bounds for sequential projective measurements. Physical Review A, 92(5):052331, 2015, arXiv:1410.5688.

[15] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell’s theorem without inequalities. American Journal of Physics, 58(12):1131–1143, 1990.

[16] D. Grigoriev. Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity. Theoretical Computer Science, 259:613–622, 2001.

[17] A. Harrow, A. Natarajan, and X. Wu. Limitations of semidefinite programs for separable states and entangled games. 2016, arXiv:1612.09306.

[18] J. Håstad. Some optimal inapproximability results. Journal of the ACM (JACM), 48(4):798–859, 2001.

[19] Z. Ji. Classical verification of quantum proofs. In Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, pages 885–898. ACM, 2016.

[20] T. Johansson. The giant component of the random bipartite graph. Master’s thesis, Chalmers University of Technology, 2012.
[21] J. Kempe, O. Regev, and B. Toner. Unique games with entangled provers are easy. *SIAM Journal on Computing*, 39(7):3207–3229, 2010, arXiv:0710.0655.

[22] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.*, 10(7):073013, 2008, arXiv:0803.4290.

[23] D. Ostrev and T. Vidick. Entanglement of approximate quantum strategies in XOR games, 2016, arXiv:1609.01652.

[24] D. Pérez-García, M. M. Wolf, C. Palazuelos, I. Villanueva, and M. Junge. Unbounded violation of tripartite Bell inequalities. *Communications in Mathematical Physics*, 279(2):455–486, 2008, arXiv:quant-ph/0702189.

[25] B. Pittel and G. B. Sorkin. The satisfiability threshold for k-xorsat. *Combinatorics, Probability and Computing*, 25(2):236–268, 2016, arXiv:1212.1905.

[26] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[27] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, Chichester, 1986.

[28] W. Slofstra. Tsirelson’s problem and an embedding theorem for groups arising from non-local games, 2016, arXiv:1606.03140.

[29] W. Slofstra. The set of quantum correlations is not closed, 2017, arXiv:1703.08618.

[30] R. P. Stanley. *Enumerative Combinatorics, vol. 2*. Cambridge University Press, 1999. Exercise 6.36 and references therein.

[31] L. Trevisan. On Khot’s unique games conjecture. *Bulletin (New Series) of the American Mathematical Society*, 49(1), 2012.

[32] B. S. Tsirel’son. Quantum analogues of the Bell inequalities. The case of two spatially separated domains. *Journal of Mathematical Sciences*, 36(4):557–570, 1987.

[33] U. Vazirani and T. Vidick. Fully device-independent quantum key distribution. *Physical review letters*, 113(14):140501, 2014.

[34] T. Vidick. Three-player entangled XOR games are NP-hard to approximate. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, FOCS ’13, pages 766–775. IEEE Computer Society, 2013, arXiv:1302.1242.
A  Explicit Refutation for Capped GHZ

While the results of Section 6.3 prove that a refutation must exist for every symmetric game with a PREF specification, which includes all games in the Capped GHZ family, it is illuminating to follow a concrete demonstration of the methods of that section. We focus on the 3rd order Capped GHZ game and explicitly use the PREF specification and shuffling technology to construct a refutation.

The 3rd order Capped GHZ is defined by

\[
CG_3 := \left\{ \begin{array}{cccccccc}
1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\
1 & 2 & 2 & 2 & 1 & 3 & 3 & 3 \\
-1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\
\end{array} \right\}.
\]

(250)

By the arguments of the previous section, \( z = (-1 \ 1 \ 1 \ 1 \ -2 \ -2 \ -2 \ 4)^T \) is a PREF specification for this game. This PREF specification allows us to write down a word \( W \Leftrightarrow I \) by filling all even positions with \(|z|\) copies of queries that have \( z_i > 0 \) and filling all odd positions with \(|z|\) copies of queries that have \( z_i < 0 \),

\[
W := \left[ \begin{array}{cccccccc}
1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\
1 & 2 & 3 & 1 & 2 & 2 & 3 & 3 \\
1 & 2 & 3 & 2 & 1 & 2 & 3 & 3 \\
1 & 2 & 2 & 3 & 3 & 1 & 3 & 2 \\
\end{array} \right].
\]

(251)

Now, following the procedure of Section 6.3, we determine the parity-preserving permutation that causes the first two rows to cancel. The first row even letters can be mapped to canceling odd letters by the bijection

\[
f_1 : \mathcal{E} \to \mathcal{O}
\]

defined by

\[
\pi_1 := (3 \ 5)
\]

(252)

and thus the query permutation written in two-line notation

\[
1 \ 2 \ 3 \ 3 \ 3 \ 2 \ 3 \ 1 \\
1 \ 1 \ 3 \ 3 \ 2 \ 2 \ 2 \ 2
\]

(253)

while the second row even letters can likewise be mapped via the bijection

\[
f_2 : \mathcal{E} \to \mathcal{O}
\]

defined by

\[
\pi_2 := (1 \ 6 \ 2)
\]

(254)

and thus the query permutation written in two-line notation

\[
1 \ 2 \ 2 \ 3 \ 3 \ 1 \\
1 \ 1 \ 3 \ 3 \ 2 \ 2
\]

(255)

The combined bijection \( f : \mathcal{E} \cup \mathcal{O} \to \mathcal{E} \cup \mathcal{O} \) given by

\[
f(E_i) := O_{\pi_1(i)}
\]

(256)

and thus the query permutation written in two-line notation

\[
\pi := \left( \begin{array}{ccccccccccc}
\mathcal{O}_1 & \mathcal{E}_1 & \mathcal{O}_2 & \mathcal{E}_2 & \mathcal{O}_3 & \mathcal{E}_3 & \mathcal{O}_4 & \mathcal{E}_4 & \mathcal{O}_5 & \mathcal{E}_5 & \mathcal{O}_6 & \mathcal{E}_6 & \mathcal{O}_7 & \mathcal{E}_7 \\
\mathcal{O}_1 & \mathcal{E}_2 & \mathcal{O}_6 & \mathcal{E}_6 & \mathcal{O}_1 & \mathcal{E}_1 & \mathcal{O}_3 & \mathcal{E}_3 & \mathcal{O}_5 & \mathcal{E}_5 & \mathcal{O}_4 & \mathcal{E}_4 & \mathcal{O}_7 & \mathcal{E}_7
\end{array} \right).
\]

(257)

(258)

Applying this permutation to \( W \) produces the desired form:

\[
\pi(W) = \left[ \begin{array}{ccccccccccccc}
1 & 2 & 3 & 3 & 1 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\
1 & 1 & 3 & 3 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\
1 & 2 & 3 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 3 & 2 & 3 & 3 \\
\end{array} \right].
\]

(260)

and

\[
\sim \left[ \begin{array}{cccccccc}
1 & 2 & 3 & 3 & 3 & 2 & 3 & 1 \\
1 & 2 & 3 & 3 & 2 & 3 & 2 & 3
\end{array} \right].
\]

(261)
We must now use shuffling technology to concatenate to \(\pi(W)\) additional queries that rearrange the bottom wire such that it also cancels. We begin by identifying the needed shuffle functions, then describe their construction in terms of shift gadgets. Finally, we expand out the resulting refutation to demonstrate that the shuffle technology indeed works as expected.

The third wire of \(\pi(W)\) may be canceled by the pairwise permutation \(\pi' = (134)\). This can be produced by the composition of two shuffle functions:

\[
\pi' = f_b f_a \\
\begin{align*}
  f_a &:= (1243) \\
  f_b &:= (12).
\end{align*}
\]

Both shuffle functions can be implemented via a set of shift gadgets that “save” pairs from the 3rd wire onto the 1st and 2nd followed by a set of shift gadgets that “load” those pairs back onto the 3rd wire shuffled by the relevant shuffle function. Explicitly, we can perform the first shuffle by enacting the following saves and loads:

1. Save (2 3) → wire 1.
2. Save (2 3) → wire 1.
3. Save (3 3) → wire 1.
4. Save (3 1) → wire 2.
5. Save (3 2) → wire 1.
6. Save (3 3) → wire 2.
7. Save (1 2) → wire 1.
8. Load from wires 1 and 2 in the order 2, 2, 1, 1, 1, 1, 1.

After the saves, the 1st wire is \(~h(23)h(23)h(33)h(32)h(12)~\) and the 2nd wire is \(~h(31)h(33)~\), where \(h(ab)\) indicates the “saved” form of the pair \((ab)\), while the 3rd wire is \(~I~\). Loading in the specified order then reinstates the property that the 1st and 2nd wires cancel to \(I\) while the 3rd wire becomes \(~33|31|12|32|33|23|23~\). We may then perform the second shuffle by enacting the following saves and loads:

1. Save (2 3) → wire 1.
2. Save (2 3) → wire 1.
3. Save (3 3) → wire 1.
4. Save (3 2) → wire 1.
5. Save (1 2) → wire 1.
6. Save (3 1) → wire 1.
7. Save (3 3) → wire 2.
8. Load from wires 1 and 2 in the order 1, 2, 1, 1, 1, 1, 1.

After the saves, the 1st wire is \(~h(23)h(23)h(33)h(32)h(12)h(31)~\) and the 2nd wire is \(~h(33)~\), while the 3rd wire is \(~I~\). Loading in the specified order then reinstates the property that the 1st and 2nd wires cancel to \(I\) while the 3rd wire becomes \(~31|33|12|32|33|23|23~\).
Combining the construction of these two shuffle functions finally produces the desired refutation:

\[ R := \pi(W) \]

\[
\begin{align*}
&\frac{\text{(first two wires canceled)}}{\begin{align*}
S^{3 \to 1}_{(23)} & S^{3 \to 1}_{(33)} S^{3 \to 2}_{(31)} S^{3 \to 1}_{(22)} S^{3 \to 2}_{(33)} S^{3 \to 1}_{(12)} \quad \text{(saves for } f_a) \\
S^{3 \to 1}_{(23)} & S^{3 \to 1}_{(33)} S^{3 \to 1}_{(31)} S^{3 \to 1}_{(12)} S^{3 \to 1}_{(22)} S^{3 \to 2}_{(33)} \quad \text{(loads for } f_a) \\
S^{3 \to 1}_{(23)} & S^{3 \to 2}_{(33)} S^{3 \to 2}_{(31)} S^{3 \to 1}_{(12)} S^{3 \to 1}_{(22)} S^{3 \to 1}_{(33)} \quad \text{(saves for } f_b) \\
S^{3 \to 1}_{(31)} & S^{3 \to 1}_{(33)} S^{3 \to 2}_{(12)} S^{3 \to 2}_{(32)} S^{3 \to 1}_{(33)} S^{3 \to 1}_{(23)} \quad \text{(loads for } f_b)
\end{align*}}
\]

(265)

We simplify by canceling neighboring inverses and using the fact that the shuffle gadget \( S^{3 \to 1}_{(33)} \) and its inverse act on an identical pair, and thus can be chosen to be the identity to find

\[ R = \pi(W) S^{3 \to 1}_{(23)} S^{3 \to 1}_{(33)} S^{3 \to 2}_{(31)} S^{3 \to 1}_{(22)} S^{3 \to 2}_{(33)} S^{3 \to 1}_{(12)} S^{3 \to 1}_{(22)} S^{3 \to 1}_{(23)} S^{3 \to 1}_{(33)}. \]

(266)

We next construct the needed shuffle gadgets using the neighboring queries in \( W \) giving rise to each pairing \((23), (31)\), etc. For example, \( S^{3 \to 2}_{(31)} \) can be constructed using permutations of the neighboring queries

\[
\begin{bmatrix} 3 \\ 2 \\ 3 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}
\]

associated with the pair \((31)\) on the third wire of \( \pi(W) \):

\[ S^{3 \to 2}_{(31)} := \begin{bmatrix} 2 & 2 & 3 & 3 \\ 2 & 1 & 3 & 2 \\ 1 & 2 & 2 & 3 \end{bmatrix}. \]

(267)

\[ \sim \begin{bmatrix} 2 & 1 & 3 & 2 \\ 1 & 3 \end{bmatrix}. \]

(268)

This gadget serves to cancel the pair \((31)\) on the third wire and “save” it in the form \( h(31) = (2 \ 1 \ 3 \ 2) \) on the second wire. Recall that reversing the queries of this gadget gives the “load” form \( S^{3 \to 2}_{(31)} \). Crucially, these constructions are only possible because neighboring pairs in \( \pi(W) \) are guaranteed to have a cancellation in the second wire, which, exploiting the symmetric nature of the game, allows us to simplify the third wire of the shuffle gadget.

Expanding (266) allows us to conclude \( R \sim I \) by inspection.

\[
R = \begin{bmatrix} 1 & 2 & 2 & 3 & 3 & 1 & 3 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 1 & 3 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 2 & 3 & 3 & 3 & 2 & 3 & 1 & 3 & 3 & 2 & 3 & 2 & 3 & 3 \\ 3 & 3 & 2 & 3 & 3 & 3 & 3 & 2 & 3 & 3 & 2 & 2 & 3 & 3 & 3 & 3 \end{bmatrix}
\]

(269)

The only query with parity bit \( s_i = -1 \) is \( x_0 = [1 \quad 1 \quad 1]^T \), the all-zeros query. This query appears an odd number of times in \( W \) because \( W \) was constructed using the \textsc{pref} specification \( z \). By definition, the shuffle gadgets have parity bits that multiply to 1. Thus, by construction, the associated product of parity bits for refutation \( R \) is \(-1\), and therefore \( \omega^*(CG_3) < 1 \).