Noncommutative Nullstellensätze and Perfect Games

Adam Bene Watts[*]   J. William Helton[†]   Igor Klep[‡]

December 2, 2021

Abstract

The foundations of classical Algebraic Geometry and Real Algebraic Geometry are the Nullstellensatz and Positivstellensatz. Over the last two decades the basic analogous theorems for matrix and operator theory (noncommutative variables) have emerged. This paper concerns commuting operator strategies for nonlocal games, recalls NC Nullstellensatz which are helpful, extends these, and applies them to a very broad collection of games. In the process it brings together results spread over different literatures, hence rather than being terse, our style is fairly expository.

The main results of this paper are two characterizations, based on Nullstellensatz, which apply to games with perfect commuting operator strategies. The first applies to all games and reduces the question of whether or not a game has a perfect commuting operator strategy to a question involving left ideals and sums of squares. Previously, Paulsen and others translated the study of perfect synchronous games to problems entirely involving a ∗-algebra. The characterization we present is analogous, but works for all games. The second characterization is based on a new Nullstellensatz we derive in this paper. It applies to a class of games we call torically determined games, special cases of which are XOR and linear system games. For these games we show the question of whether or not a game has a perfect commuting operator strategy reduces to instances of the subgroup membership problem and, for linear systems games, we further show this subgroup membership characterization is equivalent to the standard characterization of perfect commuting operator strategies in terms of solution groups. Both the general and torically determined games characterizations are amenable to computer algebra techniques, which we also develop.

For context we mention that Positivstellensätze are behind the standard NPA upper bound on the score players can achieve for a game using a commuting operator strategy. This paper develops analogous NC real algebraic geometry which bears on perfect games.

---

[*]University of Waterloo. `adam.benewatts1@uwaterloo.ca`
[†]University of California San Diego. `helton@math.ucsd.edu`
[‡]University of Ljubljana, Slovenia `igor.klep@fmf.uni-lj.si`

1

1   Introduction

A nonlocal game is a test performed between a verifier and k players, in which the verifier tests the players' ability to produce correlations without communicating. In a round of the game the verifier sends questions to the players and the players return responses to the verifier. The list of questions and responses is then scored according to a function known by both the verifier and the players before the game began. By convention, the score achieved lies in the interval $[0, 1]$. The players cooperate to try and achieve the highest possible score, with the challenge that the players can't communicate while the game is in progress and so don't know the questions sent to other players.

The optimal score the players can achieve on a nonlocal game $\mathcal{G}$ depends on the resources the players share. If the players share only classical randomness the optimal score they can achieve in expectation is called the the classical value of the game, denoted $\omega(\mathcal{G})$. If players share an arbitrary state in a (possibly infinite dimensional) Hilbert space and can make commuting measurements on it the optimal score they can achieve is called the commuting operator value of the game, denoted $\omega_{\mathrm{co}}^*(\mathcal{G})$. The supremum value achievable by players who make commuting measurements on a state in a finite dimensional entangled space is called the quantum value, denoted $\omega_{\mathrm{q}}^*(\mathcal{G})$. These three values can all differ, though the inequalities $\omega(\mathcal{G}) \leq \omega_{\mathrm{q}}^*(\mathcal{G}) \leq \omega_{\mathrm{co}}^*(\mathcal{G})$ are always satisfied.

Starting roughly in this century the classical subject of real algebraic geometry has been extended to matrix and operator (noncommutative) variables. Here inequalities and equalities are explained by being equivalent to algebraic formulas, often involving Sums of Squares (**SOS**). These go under the names of **Positivstellensatz** for inequalities and **Nullstellensatz** for equations. Of course finding quantum strategies for games leads to many such noncommutative (**NC**) inequalities and equalities.

In this paper we describe how the well developed NC real algebraic geometry theory applies and integrates with nonlocal games and commuting operator strategies for them. We show a connection between NC Nullstellensatz and whether or not a nonlocal game has a perfect commuting operator solution (i.e., $\omega_{\mathrm{co}}^*(\mathcal{G}) = 1$). This connection gives a new algebraic characterization which applies to all nonlocal games with commuting operator value exactly equal to one. This characterization provides a unified algebraic framework through which several previous results concerning the commuting operator value of nonlocal games can be understood. For a large class of games it also reduces the question of whether or not a game has perfect commuting operator value to an instance of the subgroup membership problem, providing a potential starting point for the investigation of several yet-to-be studied families of games.

For context, Positivstellensätze have long played a major role in the study of nonlocal games in that they are behind the standard [NPA08, DLTW08] upper bound on the commuting operator value of a game. Underlying this bound is one of the earliest NC Positivstellensätze, [HM04]. This paper turns its attention to developing the analogous NC real algebraic geometry which bears on perfect games.

In the remainder of this introduction we introduce some new terminology, review some previous results concerning the commuting operator value of nonlocal games, and then give formal statements of some of our main results.

Algebraic Description of the Commuting Operator Value   A commuting operator strategy for a nonlocal game is a description of how players can use commuting operator measurements to map questions sent by the verifier to responses. Formally, a (commuting operator) strategy can be specified by a Hilbert space $\mathcal{H}$, a state $\psi \in \mathcal{H}$ which is shared by the players and projectors

$\{E(\alpha)_a^i\}$ acting on $\mathcal{H}$, where α ranges over all players, i ranges over all questions, and a ranges over all responses. The projector $E(\alpha)_a^i$ can be read as "the projector corresponding to player α giving response a to question i".

Because the Hilbert space $\mathcal{H}$ on which they act is arbitrary, it is difficult to reason about the $E(\alpha)_a^i$ directly. Instead we introduce the universal game algebra $\mathscr{U}$, a $*$-algebra generated by variables $e(\alpha)_a^i$ which satisfy the same relations as the projectors $E(\alpha)_a^i$, for example, that $e(\alpha)_a^i$ and $e(\beta)_b^j$ commute for any $\alpha \neq \beta$.[1],[2] Commuting operator strategies can then be specified by tuples (π, ψ), consisting of a $*$-representation π mapping $\mathscr{U}$ to bounded operators on a Hilbert space $\mathcal{H}$, along with a state $\psi \in \mathcal{H}$. When specified in this way, it is understood that projectors $E(\alpha)_a^i$ are given by $\pi(e(\alpha)_a^i)$ and that ψ gives the state shared by the players.

Other Characterizations of Perfect Commuting-Operator Strategies   Several other papers have considered the problem of deciding whether or not a game has a perfect commuting operator strategy and given criteria which determine the existence of perfect commuting operator strategies for specific families of nonlocal games. We review some of those families of games and the associated characterizations below.

- Linear systems games are two player games based around system of m linear equations on n variables. In [CLS17] it was shown that deciding existence of a perfect commuting operator strategy for a binary linear systems game was equivalent to solving an instance of the word problem on a group called the solution group of the game.

- XOR games are k player games which, similarly to linear system games, test satisfiability of a system of m binary equations on kn variables.

  In [WH20] it was shown that deciding the existence of a perfect commuting operator strategy for an XOR game was equivalent to solving an instance of the subgroup membership problem on a group called the game group.

- Synchronous games are two player nonlocal games which include "consistency-checks", where Alice and Bob are sent the same question and win iff they send the same response. Other than these consistency checks, the questions and winning responses involved in a synchronous game are arbitrary. In [PSS+16] it was shown that there was a perfect commuting operator strategy for a coloring game iff a $*$-algebra associated with a single player's operators could be represented into a C^*-algebra with a faithful trace. In [HMPS17] and [KPS18] this was generalized to synchronous games.

Our Results   The main results of this paper are two theorems giving algebraic characterizations of games with perfect commuting operator strategies.

A key concept introduced on the way to proving these theorems is the notion of a game being determined by a set of elements $\mathcal{F} \subseteq \mathscr{U}$. Formally we say a game $\mathcal{G}$ is determined by a set of elements $\mathcal{F}$ if, for any commuting operator strategy (π, ψ), we have that (π, ψ) is a perfect commuting operator strategy for $\mathcal{G}$ iff $\pi(f)\psi = 0$ for all $f \in \mathcal{F}$. We also note that any game $\mathcal{G}$ is naturally determined by two sets of elements. The first, $\mathcal{N}$, consists of elements corresponding to projectors onto responses

---

[1]The $*$-algebra $\mathscr{U}$ is isomorphic to a group algebra and has appeared before in other contexts. For example, in [LMP+20] an algebra closely related to $\mathscr{U}$ was denoted $\mathcal{A}(X, A)$.

[2]A full set of relations for $\mathscr{U}$ is listed in Section 3.3.1.

which obtain a score less than 1 on questions asked by the verifier, while the second, $\mathcal{Y}$, consists of elements $y - 1$ with each element y corresponding to projectors onto responses which obtain a score of exactly 1. Details of this construction are given in Section 3.4.1.

Our first major theorem follows from combining the notion of sets of elements which determine a game with a result in noncommutative algebraic geometry known as a Nullstellensatz. To state the result formally, let $\mathfrak{L}(\mathcal{X})$ denote the left ideal of $\mathscr{U}$ generated by $\mathcal{X}$ for any set of elements $\mathcal{X} \subseteq \mathscr{U}$ and $\mathrm{SOS}_{\mathscr{U}}$ denote sums of squares in the algebra $\mathscr{U}$. Then the following result holds:

Theorem 1.1. *For a nonlocal game $\mathcal{G}$ determined by a set $\mathcal{F} \subseteq \mathscr{U}$ the following are equivalent:*

(i) *$\mathcal{G}$ has a perfect commuting operator strategy;*

(ii) *$-1 \notin \mathfrak{L}(\mathcal{F}) + \mathfrak{L}(\mathcal{F})^* + \mathrm{SOS}_{\mathscr{U}}$.*

Theorem 1.1 combined with the natural determining sets $\mathcal{N}$ and $\mathcal{Y}$, gives a fully algebraic characterization of nonlocal games with perfect commuting operator strategies. This characterization is analogous to the characterization of synchronous games given in [HMPS17], but works for all games. For the special case of synchronous games we show in Section 8 that the characterizations of Theorem 1.1 and [HMPS17] are equivalent.

The second major theorem focuses on a general class of games on which Theorem 1.1 can be simplified further. A game $\mathcal{G}$ is called a torically determined game if there exists a group G with $\mathscr{U} \cong \mathbb{C}[G]$ and $\mathcal{G}$ is determined by a set of elements

$$\mathcal{F} = \{\beta_i g_i - 1\} \tag{1.1}$$

with each $\beta_i \in \mathbb{C}$ and $g_i \in G$. We call the elements $\beta_i g_i$ clauses of $\mathcal{F}$, and let $\mathscr{H} = \{\beta_i g_i\}$ be the set of all the clauses of $\mathcal{F}$. We give the following characterization of torically determined games with perfect commuting operator strategies:

Theorem 1.2. *Let $\mathcal{G}$ be a game torically determined by a set of elements $\mathcal{F}$ with clauses $\mathscr{H}$. Then $\mathcal{G}$ has a perfect commuting operator strategy iff the following equivalent criteria are satisfied:*

(i) *$-1 \notin \mathfrak{L}(\mathcal{F}) + \mathfrak{L}(\mathcal{F})^*$;*

(ii) *The subgroup H of $\mathscr{U}$ generated by $\mathscr{H} \cup \mathscr{H}^*$ meets $\mathbb{C}$ only in 1.*

Condition (i) makes it clear Theorem 1.2 can be viewed as a version of Theorem 1.1 for torically determined games which holds without the SOS term. Additionally, condition (ii) reduces the characterization of perfect commuting operator strategies in terms of $*$-algebras given in Theorem 1.1 to one entirerly in terms of groups. In the paper we show that both linear systems games and XOR games are torically determined games, and that Theorem 1.2 recovers the algebraic characterizations of these games given in [CLS17, WH20] respectively. We also show that Theorem 1.2 lets us extend the algebraic characterization of both XOR and binary linear systems games to more general games based on linear equations Mod r for any integer r.[3]

Both Theorems 1.1 and 1.2 allow new algorithms for identifying nonlocal games with perfect commuting operator strategies. In this paper we discuss one such algorithm, based on Gröbner bases,

---

[3]In [CLS17] it was already observed that the characterization of binary linear systems games presented could be generalized to any system of equations mod p for any prime p. This generalization is given explicitly in [Gol21].

and give some sample applications. We note that, unlike the upper bounds coming from the ncSoS hierarchy, these Gröbner bases algorithms can both prove a game has commuting operator value strictly less than 1 and identify some games with commuting operator value exactly equal to 1.[4]

Recent Related Work In [LMP+20] the characterization of perfect commuting operator strategies for synchronous games in terms of representations of a ∗-algebra into a C^* algebra with a faithful trace was generalized to a class of games known as imitation games, and a purely algebraic characterization of perfect commuting operator strategies was giving for a subclass of imitation games known as mirror games. In this paper we do not try and reconcile these characterizations with Theorems 1.1 and 1.2, but we do note it as an interesting problem worth future study. In [Gol21] the solution group characterization of perfect commuting operator strategies for linear systems game given in [CLS17] was related to the C^*-algebra characterization of perfect commuting operator strategies for a synchronous variant of linear systems games presented in [KPS18]. The relationship between these algebraic objects is similar to the relationships presented in Sections 7 and 8 of this paper.

Paper Outline In Section 2 we review some general mathematical definitions necessary to understand the main results of the paper. In Section 3 we introduce terminology related to nonlocal games and define key algebraic objects. In Section 4 we introduce Nullstellensätze and prove Theorem 1.1. In Section 5 we simplify the Nullstellensätze from the previous section and prove Theorem 1.2, then apply it to XOR and Mod r games. Section 7 shows that Theorem 1.2 is equivalent to the characterization of linear systems games given in [CLS17]. Section 8 shows that, in the special case of synchronous games, Theorem 1.1 is equivalent to the characterization of synchronous games given in [HMPS17]. Section 6 introduces Gröbner basis algorithms for identifying games with perfect commuting operator value based on Theorems 1.1 and 1.2 and Section 8.3 gives an example application of our Nullstellensätze to quantum graph coloring.

There is a table of contents, an index and a list of notation at the end of the paper.

2 Math Background

Representations Given an algebra $\mathcal{A}$, a **representation** of $\mathcal{A}$ is a unital homomorphism $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$. When $\mathcal{A}$ is endowed with an involution ∗, then π is called a ∗-representation if $\pi(a^*) = \pi(a)^*$ for all $a \in \mathcal{A}$.

Free algebras Let $x = (x_1, \ldots, x_d)$ denote a tuple of noncommuting letters. Words in x form the **free monoid** $\langle x \rangle$, including the empty word denoted 1. A **noncommutative (nc) polynomial** is a linear combination of words; the algebra of nc polynomials is the **free algebra** $\mathbb{C}\langle x \rangle$. We endow it with the involution ∗ fixing $\mathbb{R} \cup \{x\}$.

Example 2.1. Any representation π of $\mathbb{C}\langle x \rangle$ is described by a tuple of operators $X \in \mathcal{B}(\mathcal{H})^d$ through $\pi(x_j) = X_j$. Then π is a ∗-representation if and only if the X_j are self-adjoint.

---

[4]The question of whether a game has perfect commuting operator value is undecidable [Slo20], meaning these algorithms (or any algorithms!) cannot always identify games with commuting operator value one, but there are many examples where they do.

Group algebras   Given an abstract group G, the **group algebra** $\mathbb{C}[G]$ has G as a vector space basis, and the multiplication is extended from the one in G by linearity/distributivity. Thus elements $p \in \mathbb{C}[G]$ are finite linear combinations

$$p = \sum_j s_j g_j, \tag{2.1}$$

where $s_j \in \mathbb{C}$ and $g_j \in G$. The involution on $\mathbb{C}[G]$ is complex conjugation on $\mathbb{C}$ and $g \mapsto g^{-1}$ for $g \in G$. Hence a $*$-representation of a group algebra $\pi : \mathbb{C}[G] \to \mathcal{B}(\mathcal{H})$ is a ring homomorphism such that $\pi(g)$ is a unitary operator for all $g \in G$.

Example 2.2. Each group algebra admits a left regular $*$-representation. Namely, let $\ell^2(G)$ be the Hilbert space with Hilbert space basis G. Then the left regular representation λ defined as

$$\lambda(g)(\sum_j a_j g_j) = \sum_j a_j g^{-1} g_j \qquad \text{for } \sum_j a_j g_j \in \ell^2(G).$$

Thus each $g \in G$ induces a unitary operator $\lambda(g) \in \mathcal{B}(\ell^2(G))$ and thus by linearity $\lambda : \mathbb{C}[G] \to \mathcal{B}(\ell^2(G))$ is a $*$-representation.

3   Nonlocal Game Definitions

This section gives an overview of all the terminology used to discuss nonlocal games in this paper. Section 3.1 gives a semi-formal introduction to the language used to describe nonlocal games. Section 3.2 gives technical definitions which are key to this paper. In Section 3.3 we introduce an algebraic framework which we will use to describe nonlocal games and their commuting operator strategies. In Section 3.4 we describe the condition that a nonlocal game has perfect commuting operator strategy in terms of some of the notation introduced in previous sections. Finally, in Section 3.5 we describe some well-know families of games using the language introduced in previous sections.

A reader already familiar with nonlocal games can skip Section 3.1 but should not skip Section 3.2 (or later sections) as conventions are set in those sections which will remain important throughout the paper.

3.1   General Notation

Nonlocal games describe experiments which test the correlations that can be produced by measurements of quantum systems. A nonlocal game involves a **referee** (also called the **verifier**) and k **players** (also called **provers**). In a round of the game, the verifer selects a vector of questions $\vec{i} = (i(1), i(2), \ldots, i(k))$ randomly from a set $\mathcal{Q}$ of possible question vectors, then sends player α question $i(\alpha)$. Each player responds with an answer $a(\alpha)$. The players cannot communicate with each other when choosing their answers. After receiving an answer from each player, the verfier computes a **score** $V(\vec{a} \, | \vec{i}) = V(a(1), a(2), \ldots, a(k) | i(1), i(2), \ldots, i(k))$ which depends on the questions selected and answers received. The players know the set of possible questions S and the scoring function V. Their goal is to chose a **strategy** for responding to each possible question which maximizes their score in expectation. The difficulty for the players lies in the fact that in a given round each

player only has partial information about the questions sent to other players. The set of all questions possible is finite; cardinality is denoted m.

For a given game G, the maximum expected score achievable by players is called the **value** of the game. The value depends on the resources available to the players. If players are restricted to classical strategies, the value is called the **classical value** and denoted $\omega(G)$. If players can make measurements on a shared quantum state (but still can't communicate) the value can be larger and is called the **entangled value**. More specifically, if the players shared state lives in a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_k$ and the i-th player makes a measurement on the i-th Hilbert space (*i.e.* all measurement operators used by the i-th player take the form $I_1 \otimes \cdots \otimes I_{i-1} \otimes X_i \otimes I_{i+1} \otimes \cdots \otimes I_k$ with X_i acting on $\mathcal{H}_i$) the supremum score the players can obtain is called the **quantum value**, denoted ω_{q}^*. In [SW08] it was shown that this value is equal to the supremum score the players can achieve making measurements on finite dimensional Hilbert spaces.

If the players state and Hilbert space is arbitrary and the only restriction placed on their measurements is all measurement operators for different players commute (enforcing no-communication), the maximum achievable score is called the **commuting operator value**, denoted ω_{co}^*. When the state shared by the players is finite dimensional the tensor product and commuting operator values of a game coincide. In the infinite dimensional case $\omega_{\mathrm{tp}}^* \leq \omega_{\mathrm{co}}^*$, and there exist games for which the inequality is strict [JNV$^+$20, Fri12, JNP$^+$11].

A notation summary is:

$$k := \#\text{players}, \quad n := \#\text{questions} \quad m := \#\text{responses per question}. \tag{3.1}$$

3.2 Basic Definitions

3.2.1 Commuting Operator Strategies

We start with a definition of a commuting operator strategy for nonlocal games. The setting is a separable Hilbert space $\mathcal{H}$, possibly infinite dimensional; measurements, described by bounded operators in $\mathcal{B}(\mathcal{H})$ and states, positive semidefinite $\rho \in \mathcal{B}(\mathcal{H})$ with trace 1. Such operators ρ are often called **density operators** or (normalized) **trace class operators**. Of course $\ell_\rho(W) = \mathrm{tr}(W\rho)$ defines a positive linear functional $\ell_\rho : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ with $\ell(I) = 1$. A **pure state** corresponds to rank one ρ, that is $\rho = \psi^*\psi$ with ψ a unit vector in $\mathcal{H}$. In this case ℓ_ρ is of the form $W \mapsto \psi^*W\psi$.

Definition 3.1. *A* **commuting operator strategy** *S for a k-player, n-question, m-response nonlocal game is defined by $(\mathcal{H}, \rho, \mathcal{E}(1), \mathcal{E}(2), \ldots, \mathcal{E}(k))$ where $\mathcal{H}$ is a separable Hilbert space, ρ a state, and each $\mathcal{E}(\alpha)$ for $\alpha \in [k]$ is a set of projectors acting on $\mathcal{H}$,*

$$\mathcal{E}(\alpha) = \{E(\alpha)_a^i \mid i \in [n], a \in [m]\} \tag{3.2}$$

which satisfy

$$[E(\alpha)_a^i, E(\beta)_b^k] = 0 \quad \forall\, \alpha \neq \beta, \tag{3.3a}$$

$$\sum_{a \in [m]} E(\alpha)_a^i = 1 \quad \forall\, \alpha \in [k], i \in [n]. \tag{3.3b}$$

Note that as a consequence of [Equation (3.3b)](#) we have $E(\alpha)_a^i E(\alpha)_b^i = 0$ and hence $[E(\alpha)_a^i, E(\alpha)_b^i] = 0$ for any α, i and $a \neq b$.

Conventions:

$$\alpha, \beta \textbf{ variables label players}, \quad i, j \textbf{ variables label questions}, \text{ and}$$
$$a, b \textbf{ variables label responses}.$$

3.2.2 Games and their Commuting Operator Value

A k-player, n-question, m-response nonlocal game $\mathcal{G} = (V, \mu)$ is specified by a scoring function

$$V : [n]^k \times [m]^k \to [0, 1] \tag{3.4}$$

and a probability distribution μ on $[n]^k$. The **score** a strategy S obtains on a game $\mathcal{G} = (V, \mu)$ is given by

$$V(\mathcal{G}, S) = \sum_{\vec{i} \in [n]^k} \sum_{\vec{a} \in [m]^k} \mu\left(\vec{i}\right) V\left(\vec{i}, \vec{a}\right) \operatorname{Tr}\left[\prod_{\alpha \in [k]} E(\alpha)_{a(\alpha)}^{i(\alpha)} \rho\right] \tag{3.5}$$

The commuting operator value $\omega_{\mathrm{co}}^*(\mathcal{G})$ of a game is defined to be the supremum value achieved over commuting operator strategies, so

$$\omega_{\mathrm{co}}^*(\mathcal{G}) = \sup_{S \in \mathcal{S}_{\mathrm{co}}} V(\mathcal{G}, S). \tag{3.6}$$

where we have defined $\mathcal{S}_{\mathrm{co}}(k, n, m)$ to be the set of all k-player, n-question, m-response commuting operator strategies. Often k, n, m are implied from context, and we just write $\mathcal{S}_{\mathrm{co}}$.

3.3 The Algebraic Picture

In this paper we think of strategies $S \in \mathcal{S}_{\mathrm{co}}$ as arising from from representations of an algebra we call the universal game algebra. We define that algebra next.

3.3.1 Universal Game Algebra

Here we define the **Universal Game Algebra** $\mathscr{U}$ in terms of various generators and relations. These relations define a two sided ideal $\mathscr{I}$ which lives inside the $*$-algebra of all noncommutative polynomials in the generators. We call $\mathscr{I}$ the **Universal Game Ideal**. These relations reflect the algebraic properties of projectors or related algebraic objects.

Projection Generators Define $\mathscr{U}$ to be the $*$-algebra with generators $e(\alpha)_a^i$ which satisfy relations

$$[e(\alpha)_a^i, e(\beta)_b^j] = 0 \quad \forall\, i, j, a, b, \alpha \neq \beta, \tag{3.7a}$$

$$\left(e(\alpha)_a^i\right)^2 = \left(e(\alpha)_a^i\right)^* = e(\alpha)_a^i, \tag{3.7b}$$

$$e(\alpha)_a^i e(\alpha)_b^i = 0 \quad \forall\, i, a \neq b, \tag{3.7c}$$

$$\sum_a e(\alpha)_a^i = 1 \quad \forall\, \alpha, i, \tag{3.7d}$$

with $i, j \in [n]; a, b \in [m]$, and $\alpha \in [k]$. (Technically we should define a different Universal Algebra for every different value n, m and k, so $\mathscr{U} = \mathscr{U}(n, m, k)$. We frequently omit this detail when n, m and k are clear from context.)

Alternately, we can describe $\mathscr{U}$ as a quotient of the free $*$-algebra. Namely, let e denote the tuple

$$e = (e(\alpha)_a^i))_{i,a,\alpha},$$

and define the universal game ideal $\mathscr{I}$ to be the 2 sided ideal in the free algebra $\mathbb{C}\langle e \rangle$, defined by the polynomials

$$\left\{ [e(\alpha)_a^i, e(\beta)_b^j], \ \left(e(\alpha)_a^i \right)^2 - e(\alpha)_a^i, \ e(\alpha)_{a'}^i e(\alpha)_{b'}^i, \ \sum_a e(\alpha)_a^i - 1 \right\} \tag{3.8}$$

where the indices run through all $i, j, a, b, a' \neq b', \alpha \neq \beta$. Then $\mathscr{U} = \mathbb{C}\langle e \rangle / \mathscr{I}$; note that $\mathscr{U}$ comes equipped with an involution induced by $\left(e(\alpha)_a^i \right)^* = e(\alpha)_a^i$.

There are two common changes of variables we will use when describing the algebra $\mathscr{U}$.

Signature Matrix Generators The first change of variables is to generators satisfying the algebraic properties of signature matrices, defined by

$$x(\alpha)_a^i := 2e(\alpha)_a^i - 1. \tag{3.9}$$

These variables satisfy relations

$$x(\alpha)_a^i x(\beta)_b^j = x(\beta)_b^j x(\alpha)_a^i \quad \forall i, j, a, b, \alpha \neq \beta, \tag{3.10a}$$

$$(2x(\alpha)_a^i - 1)(2x(\alpha)_b^i - 1) = 0 \quad \forall i, a \neq b, \alpha \text{ and} \tag{3.10b}$$

$$\sum_a x(\alpha)_a^i = -(m - 2), \tag{3.10c}$$

$$\left(x(\alpha)_a^i \right)^* = x(\alpha)_a^i, \tag{3.10d}$$

$$\left(x(\alpha)_a^i \right)^2 = 1 \quad \forall i, a, \alpha. \tag{3.10e}$$

It is straightforward to check that the set of relations above gives a defining set of relations for the algebra $\mathscr{U}$ written in terms of the $x(\alpha)_a^i$.

Cyclic Unitary Generators The second change of variables is to cyclic unitary generators, defined by

$$c(\alpha)_j := \sum_a \exp\left(\frac{2\pi a i}{m} \right) e(\alpha)_a^j. \tag{3.11}$$

(In this subsection i refers to the imaginary unit, and j is used to index questions). These elements satisfy relations

$$c(\alpha)_j c(\beta)_{j'} = c(\beta)_{j'} c(\alpha)_j \quad \forall j, j', \alpha \neq \beta, \tag{3.12a}$$

$$\left(c(\alpha)_j \right)^* = \left(c(\alpha)_j \right)^{-1}, \tag{3.12b}$$

$$\left(c(\alpha)_j \right)^m = 1. \tag{3.12c}$$

9

Routine calculation using the inverse transformation

$$e(\alpha)_a^j = \frac{1}{m} \sum_b \left(\exp\left(\frac{-2\pi a i}{m} \right) c(\alpha)_j \right)^b \tag{3.13}$$

shows that Equations (3.12a) to (3.12c) also form a defining set of relations for $\mathscr{U}$.

We can also define a group G generated by elements $c(\alpha)_j$ which satisfy the relations defined in Equations (3.12a) to (3.12c). Then we can write that $\mathscr{U} = \mathbb{C}[G]$, making it clear that $\mathscr{U}$ is a group algebra.

Two Answer Games An notable special case occurs when the answer set of the game contains only 2 responses. In this case the cyclic observable and signature matrix change of variables are the same, since

$$c(\alpha)_i = e(\alpha)_0^i - e(\alpha)_1^i = 2e(\alpha)_0^i - 1 = x(\alpha)_0^i, \tag{3.14a}$$
$$x(\alpha)_0^i = -x(\alpha)_1^i. \tag{3.14b}$$

In this case we use the simplified notation $x_i^{(\alpha)} = c(\alpha)_i = x(\alpha)_0^i$.

3.3.2 Strategies as Representations of the Universal Game Algebra

Recall from Section 2 that a $*$-representation $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ is an algebraic structure preserving map, so images of generators of $\mathscr{U}$ consist of operators on $\mathcal{H}$ which respect the algebraic structure of $\mathscr{U}$, for example

$$\pi\big((e(\alpha)_a^i)^2\big) = \pi(e(\alpha)_a^i)^2.$$

Then we note that any $*$-representation $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ and state $\psi \in \mathcal{H}$ can be used to define a commuting operator strategy $S \in \mathcal{S}_{\mathrm{co}}$, simply by setting

$$E(\alpha)_a^i = \pi(e(\alpha)_a^i) \tag{3.15}$$

for all i, a, α and taking the Hilbert space $\mathcal{H}$ to be the target Hilbert space of the $*$-representation π. Similarly, any commuting operator strategy defined by a Hilbert space $\mathcal{H}$, state ψ, and projectors $E(\alpha)_a^i$ can be used to define a $*$-representation $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ by setting

$$\pi(e(\alpha)_a^i) = E(\alpha)_a^i \tag{3.16}$$

for all i, a, α. For this reason we view commuting operator strategies interchangeably with pairs (π, ψ) consisting of $*$-representations $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ and states $\psi \in \mathcal{H}$.

3.3.3 An Algebraic Definition of the Commuting Operator Value of a Game

For any game $\mathcal{G}$ define the game polynomial $\Phi_{\mathcal{G}} \in \mathscr{U}$ by

$$\Phi_{\mathcal{G}} = \sum_{\vec{i} \in [n]^k} \sum_{\vec{a} \in [m]^k} \mu\left(\vec{i}\right) V\left(\vec{i}, \vec{a}\right) \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \tag{3.17}$$

10

Then, recalling the view of strategies as representations introduced in Section 3.3.2,

$$\omega_{\mathrm{co}}^*(\mathcal{G}) = \sup_{\pi, \rho} \mathrm{tr}[\pi(\Phi_{\mathcal{G}})\rho] \tag{3.18}$$

where the supremum is taken over all $*$-representations π of $\mathscr{U}$ into bounded operators on a Hilbert space $\mathcal{H}$, and density operators $\rho \in \mathcal{B}(\mathcal{H})$.

A slightly different representation of ω_{co}^* which is useful is given in the next lemma.

Lemma 3.2. *The sup in Equation (3.18) is attained for some pair representation-density operator $(\hat{\pi}, \hat{\rho})$. Moreover, one can take $\hat{\rho}$ to be a pure state $\hat{\rho} = \hat{\psi}^* \hat{\psi}$, so*

$$\omega_{\mathrm{co}}^*(\mathcal{G}) = \max_{\pi, \psi} \psi^* \pi(\Phi_{\mathcal{G}}) \psi. \tag{3.19}$$

Here $\psi \in \mathcal{H}$ is a unit vector, and $\mathcal{H}$ is the Hilbert space into which π represents; without loss of generality $\mathcal{H}$ can be taken to be separable.

Proof. Firstly, it is well-known that the extreme points of the convex set of density operators $\rho \in \mathcal{B}(\mathcal{H})$ are exactly rank ones. This shows one can replace ρ by $\psi^* \psi$ for unit vectors ψ in Equation (3.18).

Given π, ψ as above, the map

$$\ell : \mathscr{U} \to \mathbb{C}, \quad a \mapsto \psi^* \pi(a) \psi \tag{3.20}$$

is a positive linear functional with $\ell(1) = 1$. Conversely, a normalized positive linear functional $\ell : \mathscr{U} \to \mathbb{C}$ yields through the Gelfand-Naimark-Segal (GNS) construction a representation π and unit vector ψ such that Equation (3.20) holds. Thus Equation (3.18) can be rewritten as

$$\omega_{\mathrm{co}}^*(\mathcal{G}) = \sup_{\ell} \ell(\Phi_{\mathcal{G}}). \tag{3.21}$$

The set of the normalized positive linear functionals on $\mathscr{U}$ is weak-$*$ compact by the Banach-Alaoglu theorem. Thus by continuity, the supremum in Equation (3.21) is attained. Hence the GNS construction as explained above yields Equation (3.19). Observe that since $\mathscr{U}$ is countably dimensional, the constructed Hilbert space $\mathcal{H}$ will be separable. $\square$

3.3.4 Valid and Invalid Response Sets

Now we introduce a few more objects which are useful for describing nonlocal games.

First, for any game $\mathcal{G}$, let the set $\mathcal{Q} \subseteq [n]^k$ contain all question vectors which can be sent to the players with nonzero probability. Formally,

$$\mathcal{Q} = \{\vec{i} \in [n]^k : \mu(\vec{i}) > 0\}. \tag{3.22}$$

Then, for each $\vec{i} \in \mathcal{Q}$, let $\mathcal{Y}(\vec{i})$ list the response vectors to each question vector which achieve a score of exactly 1, so

$$\mathcal{Y}(\vec{i}) = \{\vec{a} : V(\vec{i}, \vec{a}) = 1\}. \tag{3.23}$$

11

We say the set $\mathcal{Y}(\vec{i})$ contains all the valid or "winning" responses to the question vector $\vec{i}$. We also define the set of invalid responses or "losing" responses $\mathcal{N}(\vec{i})$ to be the complement of the set $\mathcal{Y}(\vec{i})$.

In this paper we assume that all games have a scoring function V whose image is either 0 or 1 and a distribution μ which is uniform over a set of allowed questions. For these games, specifying a question set $\mathcal{Q}$ and sets $\mathcal{Y}(\vec{i})$ (or $\mathcal{N}(\vec{i})$) for all $\vec{i} \in \mathcal{Q}$ completely specifies the game, since we can write

$$\Phi_{\mathcal{G}} = \frac{1}{|\mathcal{Q}|} \sum_{\vec{i} \in \mathcal{Q}} \sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)}. \tag{3.24}$$

3.4 Determining Perfect Commuting Operator Strategies for Games

A commuting operator strategy $S = (\pi, \psi)$ is called a perfect strategy for a game $\mathcal{G}$ if $V(\mathcal{G}, S) = 1$. In this section, we develop some terminology for describing perfect commuting operator strategies for nonlocal games.

We first introduce a general definition which will be used frequently in later sections.

Definition 3.3. *A game $\mathcal{G}$ is said to be **determined by** a set of elements $\mathcal{F} \subseteq \mathcal{U}$ (or, equivalently, $\mathcal{F}$ is said to be a determining set of $\mathcal{G}$) if it is true that any strategy $S = (\pi, \psi)$ satisfies $V(\mathcal{G}, S) = 1$ iff $\pi(f)\psi = 0$ for all $f \in \mathcal{F}$.*

3.4.1 Determining Sets of a Game

We next show that any game $\mathcal{G}$ has two natural determining sets, based on the valid and invalid response sets introduced in Section 3.3.4. We first define these sets, then show they are both determining sets for the game $\mathcal{G}$.

Definition 3.4. *For any game $\mathcal{G}$ with question set $\mathcal{Q}$ and valid responses $\mathcal{Y}(\vec{i})$, we introduce a companion set of valid elements of $\mathcal{U}$,*

$$\mathcal{Y} := \left\{ \sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha} e(\alpha)_{a(\alpha)}^{i(\alpha)} - 1 \right\}_{\vec{i} \in \mathcal{Q}}, \tag{3.25}$$

Similarly, define the invalid elements $\mathcal{N}$ by

$$\mathcal{N} := \left\{ \prod_{\alpha} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right\}_{(\vec{i}, \vec{a}) \in \mathcal{Q} \times \mathcal{N}(\vec{i})}. \tag{3.26}$$

Theorem 3.5. *Let $\mathcal{G}$ be a game and $\mathcal{Y}$, $\mathcal{N}$ be as in Definition 3.4. Then $\mathcal{G}$ is determined by both $\mathcal{Y}$ and $\mathcal{N}$.*

Proof. By definition, a strategy (π, ψ) for a nonlocal game is perfect iff

$$\psi^* \pi(\Phi_G)\psi = 1, \tag{3.27}$$

i.e.,

$$\psi^* \frac{1}{|\mathcal{Q}|} \sum_{\vec{i} \in \mathcal{Q}} \sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} \pi\left(e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) \psi = 1. \tag{3.28}$$

This equation has the form: the average of a function equals its maximum, so each term equals the maximum. We now exploit this: for all $\vec{i} \in \mathcal{Q}$ we have

$$\pi \left(\sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) \leq \pi \left(\sum_{\vec{a} \in [m]} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) = I \tag{3.29}$$

hence

$$\psi^* \pi \left(\sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) \psi \leq \psi^* \psi = 1 \tag{3.30}$$

and a game is perfect iff we have for all $\vec{i} \in \mathcal{Q}$:

$$\psi^* \pi \left(\sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) \psi = 1, \tag{3.31}$$

equivalently,

$$\psi^* \pi \left(\left(\sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) - 1 \right) \psi = 0. \tag{3.32}$$

Again using Equation (3.29), we see

$$\pi \left(\sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) - I \tag{3.33}$$

is negative semidefinite, hence Equation (3.32) implies

$$\pi \left(\left(\sum_{\vec{a} \in \mathcal{Y}(\vec{i})} \prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) - I \right) \psi = 0 \tag{3.34}$$

which finishes the first part of the proof.

To convert this condition from terms of $\mathcal{Y}$ to terms of $\mathcal{N}$ fix $\vec{i} \in \mathcal{Q}$ and use

$$\sum_{\vec{a} \in \mathcal{Y}(\vec{i}) \cup \mathcal{N}(\vec{i})} \psi^* \pi \left(\prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) \psi = \psi^* \psi = 1. \tag{3.35}$$

In words we are summing over all responses valid or invalid to question $\vec{i}$. Subtract Equation (3.31) from this to get $\sum_{\vec{a} \in \mathcal{N}(\vec{i})} = 0$. This is a sum of nonnegative terms, so each is 0:

$$\psi^* \pi \left(\prod_{\alpha \in [k]} e(\alpha)_{a(\alpha)}^{i(\alpha)} \right) \psi = 0 \quad \forall \, \vec{a} \in \mathcal{N}(\vec{i}) \tag{3.36}$$

13

Since operators $\pi\left(e(\alpha)_a^i\right)$ are positive semidefinite we get

$$\pi\left(\prod_{\alpha\in[k]} e(\alpha)_{a(\alpha)}^{i(\alpha)}\right)\psi = 0 \quad \forall\, \vec{a}\in\mathcal{N}(\vec{i}),$$

thus finishing the proof. $\qquad\square$

3.4.2 Torically Determined Games

While any game $\mathcal{G}$ is determined by the sets $\mathcal{Y}$ and $\mathcal{N}$, there are, in general, many other sets of elements in $\mathscr{U}$ that determine a game $\mathcal{G}$. An important class of games in this paper are torically determined games, which we define as games determined by a particularly nice set of binomial elements.

Definition 3.6. *A game $\mathcal{G}$ is called a **torically determined game** if there exists a group G with $\mathscr{U}\cong\mathbb{C}[G]$ and $\mathcal{G}$ is determined by a set of elements*

$$\mathcal{F} = \{\beta_i g_i - 1\} \tag{3.37}$$

*with each $\beta_i\in\mathbb{C}$ and $g_i\in G$. In this case we say $\mathcal{G}$ is **torically determined by** the set $\mathcal{F}$ and call the elements $\beta_i g_i$ clauses of $\mathcal{F}$.*

Traditionally, the term toric ideal refers to ideals generated by binomials, these being the difference of two monomials. The next lemma shows that our use of the term toric is consistent with this.

Lemma 3.7. *A game $\mathcal{G}$ which is determined by a set of elements of the form*

$$\mathcal{F}' = \{\beta_i g_i - \beta_i' g_i'\}_i \tag{3.38}$$

with all $\beta_i,\beta_i'\in\mathbb{C}$, and $g_i,g_i'\in G$ for some group G with $\mathscr{U}\cong\mathbb{C}[G]$ is also torically determined.

Proof. For all (π,ψ) we have

$$\pi(\beta_i g_i - \beta_i' g_i')\psi = 0 \qquad \Leftrightarrow \qquad (\,\pi(\beta_i(\beta_i')^{-1}g_i(g_i')^{-1} - 1)\psi = 0 \tag{3.39}$$

so $\mathcal{G}$ is also (torically) determined by the set

$$\mathcal{F} = \{\beta_i(\beta_i')^{-1}g_i(g_i')^{-1} - 1\}_i. \qquad\qquad\square$$

To provide some further intuition about the definition of torically determined games we introduce the concept of a relaxed game polynomial. Given a game $\mathcal{G}$ with game polynomial $\Phi_{\mathcal{G}}$, we define a **relaxed game polynomial** for the game to be any element $\tilde{\Phi}_{\mathcal{G}}\in\mathscr{U}$ with the property that for any representation π and state ψ such that

$$\pi(\Phi_{\mathcal{G}})\psi = \psi \tag{3.40}$$

we have

$$\pi(\tilde{\Phi}_{\mathcal{G}})\psi = \psi, \tag{3.41a}$$

$$\left|\phi^*\pi(\tilde{\Phi}_{\mathcal{G}})\phi\right| \leq 1 \qquad \text{for all} \ \ \|\phi\|\leq 1. \tag{3.41b}$$

14

Informally, scoring a strategy using a relaxed game polynomial produces the correct score if a strategy is perfect for the associated game, but may give the wrong score otherwise. In particular, a relaxed game polynomial need not be self-adjoint, and the "score" coming from the relaxed game polynomial may not even be real when a strategy is not perfect.

Then we note that a game $\mathcal{G}$ which is torically determined by a set of elements $\mathcal{F}$ with clauses $\mathcal{H}$ has a relaxed game polynomial of the form

$$\tilde{\Phi}_{\mathcal{G}} = \frac{1}{|\mathcal{H}|} \sum_{h \in \mathcal{H}} h. \tag{3.42}$$

Similarly, any game $\mathcal{G}$ with a relaxed game polynomial

$$\tilde{\Phi}_{\mathcal{G}} = \frac{1}{|\mathcal{H}|} \sum_{h \in \mathcal{H}} h \tag{3.43}$$

where each $h \in \mathcal{H}$ is of the form $\beta_i g_i$ with $\beta_i \in \mathbb{C}$, $|\beta_i| = 1$, and $g_i \in G$ for some group G with $\mathcal{U} \cong \mathbb{C}[G]$ is torically determined by the set of elements $\mathcal{F} = \mathcal{H} - 1$. Since $\tilde{\Phi}_{\mathcal{G}}$ is an average, the proof of both these statements follows from an argument very similar to the proof of Theorem 3.5.

3.5 XOR and Mod r Games

Now we practice using some of the machinery introduced in the previous section to describe XOR games, and a natural generalization which we call Mod r games. In this section we often describe games in a variety of ways (for example using game polynomials, valid or invalid response sets, and relaxed game polynomials) without proving that these definitions are equivalent. In all cases the proof of equivalence amounts to a routine calculation using the definitions given in Section 3.3.

3.5.1 XOR Games

XOR games are games with $m = 2$ responses which we interpret as a 0 or a 1. The valid responses $\mathcal{Y}(\vec{i})$ to each question vector $\vec{i}$ are all responses which sum to either 0 or sum to 1 mod 2. We can think of an XOR game with T possible questions, labeled $\vec{i}_t = (i_t(1), i_t(2), ..., i_t(k))$ for $t \in [T]$ as testing the satisfiability of a system of T equations, where each equation takes the form

$$\sum_{\alpha \in [k]} y_{i_t(\alpha)}^{(\alpha)} = s_t \pmod{2}, \tag{3.44}$$

the $y_{i_t(\alpha)}^{(\alpha)}$ are free variables taking values in $\{0, 1\}$, and each $s_t \in \{0, 1\}$ specifies the winning parity associated with each question vector $\vec{i}_t$.

The game polynomial of an XOR game takes the form

$$\Phi_{\mathcal{G}} = \frac{1}{2} + \frac{1}{2T} \sum_{t=1}^{T} (-1)^{s_t} \prod_{\alpha \in [k]} x_{i_t(\alpha)}^{(\alpha)} \tag{3.45}$$

with $T > 0$ some integer, the vector $\vec{i}_t \in [n]^k$ and the integer $s_t \in \{0, 1\}$ are arbitrary and the notation $i_t(\alpha)$ refers to the α-th entry of the vector $\vec{i}_t$. In anticipation of a connection to torically

15

determined games, we refer to each monomial

$$(-1)^{s_t} \prod_{\alpha \in [k]} x_{i_t(\alpha)}^{(\alpha)} \tag{3.46}$$

as a clause, so the game polynomial above corresponds to a T-clause XOR game.

When working with XOR games it is convenient to remove the constant factor in the game polynomial and rescale the remaining terms, producing a relaxed game polynomial

$$\tilde{\Phi}_{\mathcal{G}} = \frac{1}{T} \sum_{t=1}^{T} (-1)^{s_t} \prod_{\alpha \in [k]} x_{i_t(\alpha)}^{(\alpha)}. \tag{3.47}$$

This relaxed game polynomial computes a quantity known as the bias (meaning $\mathrm{tr}\left[\pi(\tilde{\Phi}_{\mathcal{G}})\rho\right]$ gives the bias achieved by the strategy defined by π, ρ). For this reason we also call the relaxed game polynomial for XOR games defined in this way the *bias polynomial* of an XOR game. Note that an XOR game can be completely specified by describing its bias polynomial. We also note that the bias polynomial formulation of XOR games makes it immediately clear that XOR games are torically determined games, by the discussion in Section 3.4.2 and the observation that elements $x_{i_t(\alpha)}^{(\alpha)}$ are also cyclic unitary generators as defined in Section 3.3.

3.5.2   Mod r Games

Mod r games are a natural generalization of XOR games where the players have m responses and the valid responses to any question vector $\vec{j}_t$ are responses which satisfy some linear equation mod r. Formally, we specify a T question Mod r game by a system of equations

$$\left\{ \sum_{\alpha \in [k]} d_t(\alpha) y_{j_t(\alpha)}^{(\alpha)} = s_t \quad (\mathrm{mod}\ r) \right\}_{t \in [T]}. \tag{3.48}$$

The $d_t(\alpha)$ and s_t are integers in $[r]$, while the $y_{j_t(\alpha)}^{(\alpha)}$ are free variables. Players' responses $a(1), a(2), \ldots, a(k)$ to question vector $\vec{j}_t$ are winning if setting $y_{j_t(\alpha)}^{(\alpha)} = a(\alpha)$ satisfies the t-th equation in the system of equations. We show in Theorem 3.8 that Mod r games are torically determined by a set of elements of the form

$$\mathcal{F} = \left\{ (\exp(-2\pi i/r))^{s_t} \prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)} - 1 \right\}_{t \in [T]} \tag{3.49}$$

and hence admit a relaxed game polynomial of the form

$$\tilde{\Phi}_{\mathcal{G}} = \frac{1}{T} \sum_{t=1}^{T} (\exp(-2\pi i/r))^{s_t} \prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)}, \tag{3.50}$$

with the $c(\alpha)_{j_t(\alpha)}$ cyclic unitaries of order m, as described in Section 3.3.1. We also note that a very similar result (Theorem 7.2) is proven for linear systems in Section 7.

16

Theorem 3.8. *A Mod r game specified by a system of equations*

$$\left\{ \sum_{\alpha \in [k]} d_t(\alpha) y_{j_t(\alpha)}^{(\alpha)} = s_t \pmod{r} \right\}_{t \in [T]} \tag{3.51}$$

is torically determined by a set of elements of the form

$$\mathcal{F} = \left\{ (\exp(-2\pi i/r))^{s_t} \prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)} - 1 \right\}_{t \in [T]} \tag{3.52}$$

Proof. First we write cyclic unitary generators in terms of projectors $e(\alpha)_a^i$ and expand out the resulting product to note

$$\prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)} = \sum_{\vec{a} \in [r]^k} \exp\left(\frac{2\pi i}{r} \sum_{\alpha \in [k]} d_t(\alpha) a(\alpha) \right) \prod_{\alpha} e(\alpha)_{a(\alpha)}^{j_t(\alpha)}. \tag{3.53}$$

Then we define

$$A(t) = \left\{ \vec{a} : \sum_{\alpha \in [k]} a(\alpha) d_t(\alpha) = s_t \right\} \tag{3.54}$$

to be the collection of response vectors which win on the question corresponding to clause $t \in [T]$ of the mod r game. Then, Equation (3.53) gives that, for any commuting operator strategy (π, ψ) the condition

$$\pi \left(\prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)} \right) \psi = \psi \tag{3.55}$$

is equivalent to the condition

$$\pi \left(\sum_{\vec{a} \in A(t)} \prod_{\alpha} e(\alpha)_{a(\alpha)}^{j_t(\alpha)} \right) \psi = \exp\left(\frac{2\pi i s_t}{r} \right) \psi \tag{3.56}$$

and thus the condition

$$\pi \left(\exp(-2\pi i/r))^{s_t} \prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)} \right) \psi = \psi \tag{3.57}$$

ensures the players' response is always winning for question $t \in [T]$. The result follows. $\qquad\square$

3.5.3 Example

To provide a concrete example of the various ways of characterizing perfect games we discuss the GHZ game. This is a 3 player XOR game with bias polynomial

$$\Phi_{GHZ} = \frac{1}{4} \left(x_0^{(1)} x_0^{(2)} x_0^{(3)} - x_1^{(1)} x_1^{(2)} x_0^{(3)} - x_1^{(1)} x_0^{(2)} x_1^{(3)} - x_0^{(1)} x_1^{(2)} x_1^{(3)} \right) \tag{3.58}$$

Then, equivalently, the GHZ game is determined by the set of elements

$$\{ x_0^{(1)} x_0^{(2)} x_0^{(3)} - 1, -x_1^{(1)} x_1^{(2)} x_0^{(3)} - 1, -x_1^{(1)} x_0^{(2)} x_1^{(3)} - 1, -x_0^{(1)} x_1^{(2)} x_1^{(3)} - 1 \} \tag{3.59}$$

and has a perfect commuting operator strategy iff there exists a Hilbert space $\mathcal{H}$, state $\psi \in \mathcal{H}$, and a $*$-representation $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ satisfying

$$\pi \left(x_0^{(1)} x_0^{(2)} x_0^{(3)} \right) \psi = \psi, \tag{3.60a}$$

$$\pi \left(x_0^{(1)} x_1^{(2)} x_1^{(3)} \right) \psi = \pi \left(x_1^{(1)} x_0^{(2)} x_1^{(3)} \right) \psi = \pi \left(x_1^{(1)} x_1^{(2)} x_0^{(3)} \right) \psi = -\psi. \tag{3.60b}$$

Such a representation can be found by taking $\mathcal{H}$ to be an eight dimensional Hilbert space, ψ a 3 qubit GHZ state, and letting π map elements $x_i^{(\alpha)}$ to the standard measurement operators for the GHZ game or, explicitly

$$\pi \left(x_0^{(1)} \right) = \sigma_X \otimes I \otimes I \qquad\qquad \pi \left(x_1^{(1)} \right) = \sigma_Y \otimes I \otimes I \tag{3.61a}$$

$$\pi \left(x_0^{(2)} \right) = I \otimes \sigma_X \otimes I \qquad\qquad \pi \left(x_1^{(2)} \right) = I \otimes \sigma_Y \otimes I \tag{3.61b}$$

$$\pi \left(x_0^{(3)} \right) = I \otimes I \otimes \sigma_X \qquad\qquad \pi \left(x_1^{(3)} \right) = I \otimes I \otimes \sigma_Y \tag{3.61c}$$

where σ_X and σ_Y are the Pauli X and Y operators, respectively, and I denotes a dimension 2 identity matrix.

While it is certainly easiest to describe the GHZ game using the game polynomial formulation, we can also describe perfect strategies for the game using the language of valid and invalid response sets. Using this language the question set of the GHZ game is given by $\mathcal{Q}_{GHZ} = \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$ with valid response sets

$$\mathcal{Y}_{GHZ}(0,0,0) = \{EVEN\}, \tag{3.62a}$$

$$\mathcal{Y}_{GHZ}(0,1,1) = \mathcal{Y}_{GHZ}(1,0,1) = \mathcal{Y}_{GHZ}(1,1,0) = \{ODD\}, \tag{3.62b}$$

where $\{EVEN\}$ and $\{ODD\}$ denote the set of all 3 bit response strings containing an even and odd number of ones, respectively. The invalid response sets are described similarly, but with $\{EVEN\}$ and $\{ODD\}$ swapped.

We can obtain projectors corresponding to a perfect strategy for the GHZ game using the same representation as above, with

$$E(1)_0^0 = \pi \left(e(1)_0^0 \right) = \pi \left(\frac{1}{2} \left(1 + x_0^{(1)} \right) \right), \tag{3.63a}$$

$$E(1)_1^0 = \pi \left(e(1)_1^0 \right) = \pi \left(\frac{1}{2} \left(1 - x_0^{(1)} \right) \right), \tag{3.63b}$$

and so on. We leave it as an exercise for the reader to check that the projectors defined in this way satisfy the valid and invalid response perfect game characterization conditions laid out in Theorem 3.5.

4 Nullstellensätze for Perfect Nonlocal Games

Nullstellensätze are algebraic certificates for polynomial equations to be solvable or, even stronger, for one set of polynomial equations to have solutions contained in the set of solutions to another. Solutions to a polynomial equation such as $X^2 = I$ are often called zeroes of the polynomial $p(x) := x^2 - 1$.

4.1 Three types of zeroes

For nc polynomials there are three natural types of zero: hard zeroes, directional zeroes and determinantal zeros. These have been studied in the mathematics community for several decades.

Let us illustrate directional zeroes since that is what we work with most in this paper. Given $f \in \mathbb{C}\langle x \rangle$ define the **directional zero set**

$$\mathcal{Z}_{\mathrm{dir}}(f) := \{(X, \psi) \mid X_j \in \mathcal{B}(\mathcal{H}),\ 0 \neq \psi \in \mathcal{H},\ f(X)\psi = 0 \text{ over all } \mathcal{H}\}. \tag{4.1}$$

In the language of representations we have

$$\mathcal{Z}_{\mathrm{dir}}(f) := \{(\pi, \psi) \mid \pi(f)\psi = 0,\ \pi : \mathbb{C}\langle x \rangle \to \mathcal{B}(\mathcal{H}) \text{ representation},\ 0 \neq \psi \in \mathcal{H}\}. \tag{4.2}$$

Quantum strategies need refinements of this set up; for one, we have not captured crucial algebraic relationships such as our whole world lives inside an algebra. Thus for an arbitrary algebra $\mathcal{A}$ and $f \in \mathcal{A}$ we define

$$\mathcal{Z}_{\mathrm{dir}}^{\mathcal{A}}(f) = \{(\pi, \psi) \mid \pi(f)\psi = 0,\ \pi : \mathcal{A} \to \mathcal{B}(\mathcal{H}) \text{ representation},\ 0 \neq \psi \in \mathcal{H}\}. \tag{4.3}$$

Essential to strategies is the intersection of this with $*$-representations in the context of $*$-algebras $\mathcal{A}$:

$$\mathcal{Z}_{\mathrm{dir}}^{\mathrm{re},\mathcal{A}}(f) = \mathcal{Z}_{\mathrm{dir}}^{\mathcal{A}}(f) \cap \{(\pi, \psi) \mid \pi\ *\text{-representation}\}. \tag{4.4}$$

So far we have motivated and given the definition of the set of directional zeroes. With motivation in the same spirit, we define hard and determinantal real zeros by

$$\mathcal{Z}_{\mathrm{hard}}^{\mathcal{A}}(f) = \{\pi \mid \pi(f) = 0,\ \pi : \mathcal{A} \to \mathcal{B}(\mathcal{H}) \text{ representation}\}$$
$$\mathcal{Z}_{\mathrm{det}}^{\mathcal{A}}(f) = \{\pi \mid \det[\pi(f)] = 0,\ \pi : \mathcal{A} \to \mathcal{B}(\mathcal{H}) \text{ representation with } \dim \mathcal{H} < \infty\}.$$

Directional and hard zeroes (cf. Section 8) are central to quantum games. The definition of determinantal zeros is included here for perspective only.

Of course one also has the $*$-representation version of these:

$$\mathcal{Z}_{\mathrm{hard}}^{\mathrm{re},\mathcal{A}} \quad \text{and} \quad \mathcal{Z}_{\mathrm{det}}^{\mathrm{re},\mathcal{A}}$$

Also for a subset $F \subseteq \mathbb{C}\langle x \rangle$ we define

$$\mathcal{Z}(F) = \bigcap_{f \in F} \mathcal{Z}(f).$$

19

4.1.1 Example

In Section 3.4 we described perfect commuting operator strategies for nonlocal games as $*$-representations of an algebra $\mathscr{U}$ which satisfied certain desiderata which we now re-describe using the language of nc polynomial zeros introduced in the section above. For concreteness, we consider the GHZ game introduced in Section 3.5.3.

As discussed in Section 3.5.3, the GHZ game is determined by a set of polynomials

$$\mathcal{F} = \{x_0^{(1)}x_0^{(2)}x_0^{(3)} - 1,\ x_0^{(1)}x_1^{(2)}x_1^{(3)} + 1,\ x_1^{(1)}x_0^{(2)}x_1^{(3)} + 1,\ x_1^{(1)}x_1^{(2)}x_0^{(3)} + 1\}. \tag{4.5}$$

Equivalently, in the language of directional zeros we see that the GHZ game has a perfect commuting operator strategy iff the directional zero set $\mathcal{Z}_{\mathrm{dir}}^{\mathrm{re},\mathscr{U}}(\mathcal{F})$ is nonempty. Furthermore, entries in this set correspond to representations and states (π, ψ) defining perfect commuting operator strategies.

For an example using hard zeros see Section 8.3.

4.2 A general noncommutative Nullstellensatz

Let $\mathcal{A}$ be a $*$-algebra. We equip $\mathcal{A}$ with a certain topology called the finest locally convex topology[5]. For our purposes one does not need to worry about it since we will soon move to a much less general "weak" Nullstellensatz. For a subset $C \subseteq \mathcal{A}$ let $\mathrm{cl}(C)$ denote the closure of C in the finest locally convex topology. We use SOS_C to denote all sums of u^*u with $u \in C$.

Results of Section 5 of [CHMN13], see also [CHK$^+$14], adapted to our use case are as follows.

Theorem 4.1. *Suppose that $\mathfrak{L}$ is the left ideal of $\mathcal{A}$ generated by $F \subseteq \mathcal{A}$. Then for $a \in \mathcal{A}$ the following are equivalent:*

(i) *$\pi(a)\psi = 0$ for every $*$-representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ for some (possibly infinite dimensional) Hilbert space $\mathcal{H}$ and vector $\psi \in \mathcal{H}$ such that $\pi(f)\psi = 0$ for all $f \in F$;*

(i)' *$\mathcal{Z}_{dir}^{\mathrm{re},\mathcal{A}}(F) \subseteq \mathcal{Z}_{dir}^{\mathrm{re},\mathcal{A}}(a)$;*

(ii) *$-a^*a \in \mathrm{cl}[\mathrm{SOS}_{\mathcal{A}} - \mathrm{SOS}_{\mathfrak{L}}]$;*

(iii) *$-a^*a \in \mathrm{cl}(\mathrm{SOS}_{\mathcal{A}} - \mathrm{cone}(S))$, where $S = \{f^*f \mid f \in F\}$;*

(iv) *$-a^*a \in \mathrm{cl}[\mathrm{SOS}_{\mathcal{A}} + \mathfrak{L} + \mathfrak{L}^*]$.*

When $\mathcal{A} = \mathbb{C}\langle x \rangle$ is the free algebra and $\mathfrak{L}$ is finitely generated, $*$-representations π into finite dimensional Hilbert spaces suffice in Item (i).

Corollary 4.2. *Suppose $\mathfrak{I} \subseteq \mathcal{A}$ is a $*$-closed two sided ideal. Then the following are equivalent for $a \in \mathcal{A}$:*

(i) *$\pi(a) = 0$ for every $*$-representation π such that $\pi(f) = 0$ for all $f \in \mathfrak{I}$;*

---

[5]This is the finest vector space topology whose every neighborhood of zero contains a convex balanced absorbing set. Equivalently, it is the coarsest topology for which every seminorm on $\mathcal{A}$ is continuous. In this case, every linear functional f on $\mathcal{A}$ is continuous since $|f|$ is a seminorm. Hence for a convex subset $C \subseteq \mathcal{A}$ we have

$$\mathrm{cl}(C) = \{c \in \mathcal{A} \mid \forall \text{ linear } \ell : \mathcal{A} \to \mathbb{C} \text{ with } \ell(C) \subseteq \mathbb{R}_{\geq 0} \text{ we have } \ell(c) \geq 0\}$$

by the Hahn-Banach separation theorem.

(i)' $\mathcal{Z}_{hard}^{\mathrm{re},\mathcal{A}}(\mathfrak{I}) \subseteq \mathcal{Z}_{hard}^{\mathrm{re},\mathcal{A}}(a)$;

(ii) $-a^*a \in \mathrm{cl}[\mathrm{SOS}_{\mathcal{A}} + \mathfrak{I}]$.

Proof. Items (i) and (i)' are equivalent by the definition on $\mathcal{Z}_{\mathrm{hard}}^{\mathrm{re},\mathcal{A}}$.

In the context of Theorem 4.1, $\mathfrak{L} := \mathfrak{I} = \mathfrak{L}^*$ is a left (and right) ideal, so the algebraic certificate in Item (ii) is

$$- a^*a \in \mathrm{cl}[\mathrm{SOS}_{\mathcal{A}} + \mathfrak{I}] = \mathrm{cl}[\mathrm{SOS}_{\mathcal{A}} + \mathfrak{L} + \mathfrak{L}^*]. \tag{4.6}$$

Thus if Item (ii) fails to hold, then by Theorem 4.1 there is a $*$-representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and $0 \neq \psi \in \mathcal{H}$ with with $\pi(\mathfrak{I})\psi = \{0\}$, and $\pi(a)\psi \neq 0$.

Now consider the Hilbert space $\tilde{\mathcal{H}} := [\pi(\mathcal{A})\psi] \subseteq \mathcal{H}$. By definition, $\pi(\mathcal{A})\check{\mathcal{H}} \subseteq \check{\mathcal{H}}$, so π induces a $*$-representation $\check{\pi} : \mathcal{A} \to \mathcal{B}(\check{\mathcal{H}})$. By construction, $\check{\pi}(\mathfrak{I}) = \{0\}$ (this uses that $\mathfrak{I}$ is a right ideal, too), but $\check{\pi}(a)\psi \neq 0$, so $\check{\pi}(a) \neq 0$. $\qquad\square$

Proof of Theorem 4.1. Here we give a proof which ties the parts of the theorem to corresponding theorems in [CHMN13]. This is unintuitive so in Section 4.2.1 we sketch the idea of the proof.

Item (i) and Item (i)' are equivalent by the definition on $\mathcal{Z}_{\mathrm{dir}}^{\mathrm{re},\mathcal{A}}$. The equivalence between Item (i) and Item (ii) is [CHMN13, Theorem 5.1]. The equivalence (i) $\Leftrightarrow$ (iv) is [CHMN13, Corollary 5.3]. Finally, (iii) $\Leftrightarrow$ (ii) now follows from [CHMN13, Proposition 5.2].

The finite dimensional assertion is proved constructively and this is the major part of [CHMN13]; see [CHMN13, Proposition 6.8 and Theorem 2.1]. $\qquad\square$

Remark. In general closures in Theorem 4.1 and Corollary 4.2 are needed as can be shown by employing the Weyl algebra.

4.2.1 Intuition behind the proof of Theorem 4.1

Here is a special case of Theorem 4.1, included here since a sketch of its proof supplies the readers intuition. Also this lesser level of generality is all that is needed here for quantum games, so this theorem is what gets referenced later.

Theorem 4.3. *Suppose*

(1) $\mathcal{A}$ *is a $*$-algebra, where* $\mathrm{SOS}_{\mathcal{A}}$ *is* **archimedean** *in the sense that for every $a \in \mathcal{A}$ there is $\eta \in \mathbb{N}$ with $\eta - a^*a \in \mathrm{SOS}_{\mathcal{A}}$;*[6]

(2) $\mathfrak{L} \subseteq \mathcal{A}$ *is a left ideal.*

Then the following are equivalent:

(i) *there exist a $*$-representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ and $0 \neq \psi \in \mathcal{H}$ satisfying*

$$\pi(f)\psi = 0 \tag{4.7}$$

for all $f \in \mathfrak{L}$;

(i)' $\mathcal{Z}_{dir}^{\mathrm{re},\mathcal{A}}(\mathfrak{L}) \neq \varnothing$;

---

[6]This notion of archimedean should not be confused with the algebra $\mathcal{A}$ being **archimedean closed**, meaning that for any $a \in \mathcal{A}$ with $a + \epsilon \in \mathrm{SOS}_{\mathcal{A}}$ for each $\epsilon \in \mathbb{R}_{>0}$ we also have $a \in \mathrm{SOS}_{\mathcal{A}}$.

(ii) $-1 \notin \mathrm{SOS}_{\mathcal{A}} + \mathfrak{L} + \mathfrak{L}^*$.

Proof. As before, Items (i) and (i)' are equivalent by the definition on $\mathcal{Z}_{\mathrm{dir}}^{\mathrm{re},\mathcal{A}}$. We thus establish (i) $\Leftrightarrow$ (ii).

Easy side: suppose $-1 \in \mathrm{SOS}_{\mathcal{A}} + \mathfrak{L} + \mathfrak{L}^*$. If π, ψ as in Equation (4.7) exist, then $-\psi^*\psi \geq \psi^* \mathrm{SOS}_{\mathcal{A}} \psi \geq 0$; contradiction.

Harder side: suppose $-1 \notin \mathrm{SOS}_{\mathcal{A}} + \mathfrak{L} + \mathfrak{L}^*$. By the Hahn-Banach theorem (version due to Eidelheit-Kakutani [Bar02, Theorem III.1.7]) there is a linear functional $L : \mathcal{A} \to \mathbb{C}$ satisfying

$$L(1) = 1, \qquad L(\mathrm{SOS}_{\mathcal{A}} + \mathfrak{L} + \mathfrak{L}^*) \subseteq \mathbb{R}_{\geq 0}. \tag{4.8}$$

We remark that the strict separation is automatic since by archimedeanity $L(1) \neq 0$.

Since $\mathfrak{L}$ is a subspace, the second property of Equation (4.8) implies $L(\mathfrak{L}) = \{0\}$. Likewise, $L(f) \geq 0$ for any $f \in \mathrm{SOS}_{\mathcal{A}}$. We remark that $L(f)^* = L(f^*)$ for all $f \in \mathcal{A}$. Indeed, because $\mathcal{A}$ is archimedean, every self adjoint $g = g^* \in \mathcal{A}$ is bounded above: there is $\eta \in \mathbb{N}$ with $\eta - g \in \mathrm{SOS}_{\mathcal{A}}$. Thus $L(g) \in \mathbb{R}$. Then we write $h \in \mathcal{A}$ as a linear combination of self adjoints,

$$h = \frac{h + h^*}{2} + i\frac{h - h^*}{2i},$$

to get $L(h^*) = L(h)^*$.

Now perform the GNS construction. Define the bilinear form

$$\langle a \mid b \rangle := L(b^*a) \tag{4.9}$$

on $\mathcal{A}$. Set $N := \{a \in \mathcal{A} \mid L(a^*a)\} = 0$. By the Cauchy–Schwarz inequality for semi-scalar products,

$$0 \leq L(a^*r^*ra)^2 \leq L(a^*a)L(a^*r^*rr^*ra) = 0,$$

so N is a left ideal. Since $1 \notin N$, $N \neq \mathcal{A}$. Form the quotient space $\check{\mathcal{H}} = \mathcal{A}/N$. Then Equation (4.9) induces a scalar product on $\check{\mathcal{H}}$. We complete it to the Hilbert space $\mathcal{H}$. Let $\phi : \mathcal{A} \to \mathcal{H}$,

$$\phi(a) := a + N$$

be the quotient map and let $\psi := \phi(1)$.

Define a $*$-representation π of $\mathcal{A}$ on $\mathcal{H}$ by

$$\pi(a)(p + N) := ap + N.$$

Since N is a left ideal, this is well-defined. It is clear that π is a representation. It also intertwines the involution:

$$\langle \pi(a^*)(p + N) \mid q + N \rangle = \langle a^*p + N \mid q + N \rangle = L(q^*a^*p),$$
$$\langle p + N \mid \pi(a)(q + N) \rangle = \langle p + N \mid aq + N \rangle = L(q^*a^*p).$$

Finally, π maps into $\mathcal{B}(\mathcal{H})$. Assume $p \in \mathcal{A}$ is such that $\langle p + N \mid p + N \rangle = L(p^*p) = 1$, and let $a \in \mathcal{A}$. By archimedeanity, there is $\eta \in \mathbb{N}$ with $\eta - a^*a \in \mathrm{SOS}_{\mathcal{A}}$. Then we have

$$0 \leq \langle \pi(a)(p + N) \mid \pi(a)(p + N) \rangle$$
$$= \langle ap + N \mid ap + N \rangle = L(p^*a^*ap) \leq \eta L(p^*p) = \eta,$$

22

whence $\|\pi(a)\| \leq \sqrt{\eta}$. Thus $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ is a $*$-representation.

It remains to verify Equation (4.7). For $f \in \mathfrak{L}$ we have

$$\pi(f)\psi = \pi(f)(1 + N) = f + N.$$

Since $L(\mathfrak{L}) = \{0\}$ and $\mathfrak{L}^* \mathfrak{L} \subseteq \mathfrak{L}$, we have $\mathfrak{L} \subseteq N$. Thus $\pi(f)\psi = f + N = 0$, as desired. $\qquad\square$

Example 4.4. An appealing class of algebras for which this theorem applies are group algebras $\mathbb{C}[G]$. Indeed, for every group element $g \in \mathbb{C}[G]$ we have $1 - g^* g = 0 \in \mathrm{SOS}$. Since the set of bounded elements

$$H = \{f \in \mathbb{C}[G] \mid \exists \eta \in \mathbb{N} : \eta - f^* f \in \mathrm{SOS}\}$$

is a $*$-subalgebra [Vid59] containing G, we must have $H = \mathbb{C}[G]$ and thus SOS is archimedean in $\mathbb{C}[G]$.

Corollary 4.5. *Suppose $\mathcal{A}$ is a $*$-algebra, where $\mathrm{SOS}_\mathcal{A}$ is archimedean, and let $\mathfrak{I} \subseteq \mathcal{A}$ be a $*$-closed two sided ideal. Then the following are equivalent:*

(i) *there is a $*$-representation π such that $\pi(\mathfrak{I}) = \{0\}$;*

(i)' $\mathcal{Z}^{\mathrm{re},\mathcal{A}}_{hard}(\mathfrak{I}) \neq \varnothing$;

(ii) $-1 \notin \mathrm{SOS}_\mathcal{A} + \mathfrak{I}$.

Proof. The proof is the same as that of Corollary 4.2, just that we use Theorem 4.3 instead of Theorem 4.1. $\qquad\square$

4.3 Nullstellensätze and Perfect Games

Combining the Nullstellensatz of Section 4.2 with determining sets defined in Section 3.4 immediately gives a characterization of games with perfect commuting operator strategies in terms of left ideals and sums of squares of the universal game algebra $\mathscr{U}$.

Theorem 4.6. *For a nonlocal game $\mathcal{G}$ determined by a set $\mathcal{F} \subseteq \mathscr{U}$ the following are equivalent:*

(i) $\mathcal{G}$ *has a perfect commuting operator strategy;*

(ii) $-1 \notin \mathfrak{L}(\mathcal{F}) + \mathfrak{L}(\mathcal{F})^* + \mathrm{SOS}_\mathscr{U}$.

Proof. Immediate from Theorem 3.5 and Definition 3.3. $\qquad\square$

An immediate corollary of Theorem 4.6 comes from recalling the notions of determining sets $\mathcal{Y}, \mathcal{N}$ defined in Section 3.4.1.

Corollary 4.7. *Let $\mathcal{G}$ be a a nonlocal game, and $\mathcal{Y}, \mathcal{N}$ be the determining sets associated with the game. Then the following are equivalent:*

(i) $\omega^*_{\mathrm{co}}(\mathcal{G}) = 1$;

(ii) $-1 \notin \mathfrak{L}(\mathcal{Y}) + \mathfrak{L}(\mathcal{Y})^* + \mathrm{SOS}_\mathscr{U}$;

(iii) $-1 \notin \mathfrak{L}(\mathcal{N}) + \mathfrak{L}(\mathcal{N})^* + \mathrm{SOS}_\mathscr{U}$.

23

Proof. Immediate from Theorems 3.5 and 4.6. □

This corollary applies to all games (according to the definitions here) and characterizes which games do vs. do not have a quantum strategy. Unfortunately, the freedom given by the SOS terms in this algebraic certificate can make this theorem hard to use. Hence, we turn next to situations with no SOS term.

5 Nullstellensatz without SOS and Subgroup Membership

It is helpful to divide the perfect game condition into two sub questions. The first is checking whether $-1 \in \mathfrak{L} + \mathfrak{L}^*$ that is, whether

$$1 \in \mathfrak{L} + \mathfrak{L}^*.$$

Intuitively, this question feels "algebraic", and we will show in Section 5.2 that in special cases it reduces to a subgroup membership problem.

The second problem is checking whether

$$-1 \in \mathfrak{L} + \mathfrak{L}^* + \mathrm{SOS}_{\mathscr{U}} \tag{5.1}$$

given that

$$1 \notin \mathfrak{L} + \mathfrak{L}^*. \tag{5.2}$$

This question is more analytic, and adds substantial complexity to applications. In special cases we have that

$$1 \notin \mathfrak{L} + \mathfrak{L}^* \implies -1 \notin \mathfrak{L} + \mathfrak{L}^* + \mathrm{SOS}_{\mathscr{U}} \tag{5.3}$$

and hence the second problem is trivial. This seems closely related to the existence of projections which are conditional expectations and respect SOS. The next section investigates this link further.

5.1 Conditional Expectations and SOS Projections

We prepare to produce simpler a Nullstellensatz with no SOS terms. This uses existence of SOS projections and conditional expectations, notions we now study.

5.1.1 Definitions

Let $\mathcal{A}$ be ∗-algebra, and let $\mathcal{C} \subseteq \mathcal{A}$. Recall $\mathrm{SOS}_{\mathcal{C}}$ denotes all sums of squares of members of $\mathcal{C}$, i.e.,

$$\mathrm{SOS}_{\mathcal{C}} = \Big\{ \sum_i c_i^* c_i \mid c_i \in \mathcal{C} \Big\}.$$

If $\mathcal{C}$ is a ∗-subalgebra, then $\mathrm{SOS}_{\mathcal{C}} \subseteq \mathcal{C}$. A subtlety which is very important to us is: while $f \in \mathrm{SOS}_{\mathcal{A}}$ is in $\mathcal{C}$, f may not be in $\mathrm{SOS}_{\mathcal{C}}$. Similarly for $F \subseteq \mathcal{C}$ we let $\mathfrak{L}_{\mathcal{C}}(F) \subseteq \mathcal{C}$ denote the left ideal generated by F in the algebra $\mathcal{C}$. When there is no confusion we may omit $\mathcal{C}$ or F.

Definition 5.1. *Given a unital ∗-algebra $\mathcal{A}$, a (not necessarily unital) ∗-subalgebra $\mathcal{C}$ and a projection $\mathbb{E} : \mathcal{A} \to \mathcal{C}$ (i.e., $\mathbb{E}^2 = \mathbb{E}$) onto $\mathcal{C}$ satisfying $\mathbb{E}(a)^* = \mathbb{E}(a^*)$ for all $a \in \mathcal{A}$. Then $\mathbb{E}$ is called a*

(1) **SOS Projection** *if* $\mathbb{E}(\text{SOS}_\mathcal{A}) \subseteq \text{SOS}_\mathcal{C}$.

(2) **Conditional Expectation** *provided* $\mathcal{C}$ *is unital and* $\mathbb{E}$ *satisfies*

    (a) $\mathbb{E}(b_1 a b_2) = b_1 \mathbb{E}(a) b_2$ *for all* $a \in \mathcal{A}$, $b_1, b_2 \in \mathcal{C}$;

    (b) $\mathbb{E}(1_\mathcal{A}) = \mathbb{E}(1_\mathcal{B})$;

    (c) $\mathbb{E}(\text{SOS}_\mathcal{A}) \subseteq \text{SOS}_\mathcal{A} \cap \mathcal{C}$.

(3) **SOS Conditional Expectation** *if* $\mathbb{E}$ *is a conditional expectation that also satisfies the SOS projection property* $\mathbb{E}(\text{SOS}_\mathcal{A}) \subseteq \text{SOS}_\mathcal{C}$.

Conditional expectations will typically be denoted $\mathbb{E}$.

Remark. The bimodule property (a) in the definition of a conditional expectation can be replaced by the seemingly weaker one-sided version

    (a') $\mathbb{E}(ba) = b\mathbb{E}(a)$ for all $a \in \mathcal{A}$, $b \in \mathcal{C}$.

Indeed, given $a \in \mathcal{A}$ and $c \in \mathcal{C}$ we have

$$\mathbb{E}(ac) = \mathbb{E}\big((c^* a^*)^*\big) = \mathbb{E}\big((c^* a^*)\big)^* = \big(c^* \mathbb{E}(a^*)\big)^* = \mathbb{E}(a^*)^* c = \mathbb{E}(a)c,$$

as desired.

We now show existence of these mappings can simplify the nonlocal games Nullstellensatz.

5.1.2 Nullstellensatz

The next simple lemma explains the main use of SOS and conditional expectation property.

Lemma 5.2. *Given a unital $*$-algebra $\mathcal{A}$, a unital $*$-subalgebra $\mathcal{C}$ and $\mathfrak{L}$ a left ideal in $\mathcal{A}$. If an SOS conditional expectation $\mathbb{E} : \mathcal{A} \to \mathcal{C}$ exists, then*

(1) $L := \mathbb{E}(\mathfrak{L})$ *is a left ideal in $\mathcal{C}$;*

(2) $-1 \notin \mathfrak{L} + \mathfrak{L}^* + \text{SOS}_\mathcal{A}$ *iff* $-1 \notin L + L^* + \text{SOS}_\mathcal{C}$.

Proof. Suppose $b \in L$ and $c \in \mathcal{C}$. Then there is $\hat{b} \in \mathfrak{L}$ satisfying $\mathbb{E}(\hat{b}) = b$. These satisfy

$$cb = c\mathbb{E}(\hat{b}) = \mathbb{E}(c\hat{b}) \in \mathbb{E}(\mathfrak{L}) = L$$

establishing Item (1).

To prove the next item assume that $-1 \in \mathfrak{L} + \mathfrak{L}^* + \text{SOS}_\mathcal{A}$. Then

$$-1 = \mathbb{E}(-1) \in \mathbb{E}(\mathfrak{L} + \mathfrak{L}^* + \text{SOS}_\mathcal{A}) = L + L^* + \text{SOS}_\mathcal{C}. \tag{5.4}$$

The converse is obvious. $\qquad\square$

Corollary 5.3. *Let $\mathscr{A}$ be a $*$-algebra, $\mathcal{C}$ be a $*$-subalgebra of $\mathscr{A}$ and $F \subseteq \mathcal{C}$. Then, if a SOS conditional expectation $\mathbb{E} : \mathscr{A} \to \mathcal{C}$ exists then*

$$-1 \notin \mathfrak{L}(F)_\mathscr{A} + \mathfrak{L}(F)_\mathscr{A}^* + \text{SOS}_\mathcal{A} \quad \textit{iff} \quad -1 \notin \mathfrak{L}(F)_\mathcal{C} + \mathfrak{L}(F)_\mathcal{C}^* + \text{SOS}_\mathcal{C} \tag{5.5}$$

Proof. We show that $\mathbb{E}(\mathfrak{L}(F)_{\mathscr{A}}) = \mathfrak{L}(F)_{\mathcal{C}}$. Then the result is immediate from Lemma 5.2.

First, $\mathbb{E}$ is the identity map on $\mathcal{C}$, whence $\mathfrak{L}(F)_{\mathcal{C}} \subseteq \mathfrak{L}(F)_{\mathscr{A}}$ implies $\mathfrak{L}(F)_{\mathcal{C}} \subseteq \mathbb{E}(\mathfrak{L}(F)_{\mathscr{A}})$. To show the other inclusion note any element $p \in \mathfrak{L}(F)_{\mathscr{A}}$ can be written as $p = \sum_f a_f f$, with all $f \in F$ and $a_f \in \mathscr{A}$. Then (using the bimodule property of $\mathbb{E}$ in the second equality) we see

$$\mathbb{E}(p) = \sum_f \mathbb{E}(a_f f) = \mathbb{E}(a_f) f \in \mathfrak{L}(F)_{\mathcal{C}}, \tag{5.6}$$

hence $\mathbb{E}(\mathfrak{L}(F)_{\mathscr{A}}) \subseteq \mathfrak{L}(F)_{\mathcal{C}}$. Then $\mathbb{E}(\mathfrak{L}(F)_{\mathscr{A}}) = \mathfrak{L}(F)_{\mathcal{C}}$ and the proof is complete. $\qquad\square$

Now we prepare for finding a subalgebra $\mathcal{C}$ that makes Lemma 5.2 valuable.

Lemma 5.4. *Let $\mathscr{A}$ be a unital $*$-algebra and F be a set of elements in $\mathscr{A}$. Also let $\mathcal{C}$ denote the $*$-subalgebra of $\mathscr{A}$ generated by $\{F, 1\}$ and $\mathfrak{L}_{\mathcal{C}}$ be the left ideal in $\mathcal{C}$ generated by F. Finally, let $\mathcal{C}'$ be the subalgebra of $\mathscr{A}$ generated by F. Then the following hold.*

(1) *If $F = F^*$, then $\mathcal{C}' = \mathfrak{L}_C$.*

(2) *If 1 is not in the (non-unital) $*$-subalgebra $\mathcal{C}'$ generated by F, then*

$$-1 \notin \mathfrak{L}_{\mathcal{C}} + \mathfrak{L}_{\mathcal{C}}^* + \mathrm{SOS}_{\mathcal{C}}. \tag{5.7}$$

Proof. (1) By definition, $\mathfrak{L}_C \supseteq F$ and $\mathfrak{L}_C$ is closed under addition and multiplication. Since $F = F^*$, $\mathfrak{L}_C$ is also closed under the involution. It is thus contained in the $*$-algebra $\mathcal{C}'$. Conversely, since $F = F^*$, $\mathcal{C}'$ is the algebra generated by F and thus by definition contained in $\mathfrak{L}_C$.

(2) First note that any polynomial $p \in \mathcal{C}$ can be written as

$$p = p' + \alpha \tag{5.8}$$

where $\alpha \in \mathbb{C}$ and $p' \in \mathcal{C}'$. It follows that any polynomial $q \in \mathfrak{L}_{\mathcal{C}}$ can be written as a sum of terms of the form

$$q = (p' + \alpha) f \tag{5.9}$$

with $f \in F$. A similar description holds for any polynomial in $\mathfrak{L}_{\mathcal{C}}^*$. Additionally, any polynomial $p'' \in \mathrm{SOS}_{\mathcal{C}}$ can be written as

$$p'' = \sum_i (p_i + \alpha_i)^*(p_i + \alpha_i) \tag{5.10a}$$

$$= \sum_i (p_i^* p_i + \alpha_i^* p_i + \alpha_i p_i^*) + \sum_i |\alpha_i|^2 \tag{5.10b}$$

$$= \tilde{p} + \alpha'' \tag{5.10c}$$

with each $p_i \in \mathcal{C}'$; hence $\tilde{p} \in \mathcal{C}'$ and $\alpha'' \in \mathbb{R}_{\geq 0}$.

Now assume for contradiction that $-1 \in \mathfrak{L}_{\mathcal{C}} + \mathfrak{L}_{\mathcal{C}}^* + \mathrm{SOS}_{\mathcal{C}}$. Then, combining the above observations we can write

$$-1 = p' + \tilde{p} + \alpha'' \tag{5.11}$$

with $p', \tilde{p} \in \mathcal{C}'$ and $\alpha \in \mathbb{R}_{\geq 0}$. Rearranging Equation (5.11) gives

$$-(1 + \alpha'') = p' + \tilde{p} \in \mathcal{C}', \tag{5.12}$$

implying that $1 \in \mathcal{C}'$ since $1 + \alpha'' \in \mathbb{R}_{>0}$. $\qquad\square$

Combining Lemmas 5.2 and 5.4 results in the following "SOS free" Nullstellensatz.

Theorem 5.5. *Let $\mathscr{A}$ be a unital $*$-algebra with archimedean $\mathrm{SOS}_{\mathscr{A}}$, and let $F = F^* \subseteq \mathscr{A}$. Also let $\mathcal{C}$ be the $*$-subalgebra of $\mathscr{A}$ generated by $\{F, 1\}$. If there exists an SOS conditional expectation $\mathscr{A} \to \mathcal{C}$, then the following are equivalent:*

(i) *There exists a $*$-representation $\pi : \mathscr{A} \to \mathcal{B}(\mathcal{H})$ and vector $\psi \in \mathcal{H}$ with $\pi(f)\psi = 0$ for all $f \in F$;*

(i)' $\mathcal{Z}^{\mathrm{re},\mathscr{A}}_{dir}(F) \neq \varnothing$;

(ii) $-1 \notin \mathfrak{L}(F)_{\mathscr{A}} + \mathfrak{L}(F)^*_{\mathscr{A}} + \mathrm{SOS}_{\mathscr{A}}$;

(iii) $-1 \notin \mathfrak{L}(F)_{\mathcal{C}} + \mathfrak{L}(F)^*_{\mathcal{C}} + \mathrm{SOS}_{\mathcal{C}}$;

(iv) $1 \notin \mathfrak{L}(F)_{\mathscr{A}} + \mathfrak{L}(F)^*_{\mathscr{A}}$;

(v) $1 \notin \mathfrak{L}(F)_{\mathcal{C}} + \mathfrak{L}(F)^*_{\mathcal{C}}$;

(vi) 1 *is not in the (non-unital) $*$-subalgebra $\mathcal{C}'$ generated by F;*

(vii) $1 \notin \mathfrak{L}(F)_{\mathscr{A}}$;

(viii) $1 \notin \mathfrak{L}(F)_{\mathcal{C}}$.

Proof. Items (i), (i)' are equivalent by definition. We have (i) $\Leftrightarrow$ (ii) by the real Nullstellensatz Theorem 4.3, (ii) $\Rightarrow$ (iii) by set inclusion and (iii) $\Rightarrow$ (ii) by Corollary 5.3.

Next, (ii) $\Rightarrow$ (iv) $\Rightarrow$ (v) again by set inclusion. The equivalence (vi) $\Leftrightarrow$ (viii) follows from $\mathcal{C}' = \mathfrak{L}(F)_{\mathcal{C}}$, the implications (iv) $\Rightarrow$ (vii) $\Rightarrow$ (viii) are obvious, and (vi) $\Rightarrow$ (iii) by Lemma 5.4. $\square$

5.2 The Group Algebra Simplification

Obtaining SOS projections or conditional expectations is challenging. We now give a class of tractable situations and a Nullstellensatz appropriate for many games. The setting is a group algebra $\mathbb{C}[G]$ and $F \subseteq \mathscr{A}$, later to be chosen a set of binomials. Here G is a discrete group.

To an element $p \in \mathbb{C}[G]$,

$$p = \sum_{j}^{\gamma} s_j g_j$$

one associates the set $\mathrm{supp}(p) = \{g_1, \ldots, g_j\}$ of all group elements appearing in p, called the **support of p.** Similarly, $\mathrm{Mon}(p) = \{s_1 g_1, \ldots, s_\gamma g_\gamma\}$ is the set of monomials appearing in p. These notions are naturally extended to subsets $F \subseteq \mathbb{C}[G]$, e.g. $\mathrm{supp}(F) = \bigcup_{p \in F} \mathrm{supp}(p)$.

We need the next theorem and string of lemmas to obtain our Nullstellensatz aimed at a large class of games. Our first observation is that there is a natural SOS conditional expectation mapping from $\mathbb{C}[G]$ onto a type of envelope of a given set F.

Theorem 5.6. *Consider a group algebra $\mathbb{C}[G]$ and let $F \subseteq \mathbb{C}[G]$. Then there is an SOS conditional expectation $\mathbb{E} : \mathbb{C}[G] \to \mathbb{C}[\mathfrak{G}(\mathrm{supp}(F))]$.*

Proof. Since $\mathfrak{G}(\mathrm{supp}(F))$ is by definition a subgroup of G, this follows from [SS13]. For context, the map P is defined by

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in \mathfrak{G}(\mathrm{supp}(F))} a_g g.$$

It is an SOS conditional expectation by routine calculation; see [SS13, Example 5, Proposition 4] for details. $\qquad\square$

5.2.1 Relating the Subalgebra and Subgroup Membership Problems

In this section we restrict to sets F of binomials in a group algebra $\mathbb{C}[G]$ of the form $f = r - 1$ where each r is a monomial, $r = \beta g$ for some $g \in G$ and $\beta \in \mathbb{C}$. Our starting point is the following lemma, which gives a standard form for elements in $\mathrm{Alg}_{\mathbb{C}[G]}(F)$.

Lemma 5.7. *Consider a group algebra $\mathbb{C}[G]$ and let F be a set of elements in $\mathbb{C}[G]$ with each $f \in F$ of the form $f = r - 1$ with r a monomial and let H denote the subgroup of the invertible elements $\mathbb{C}[G]^{-1}$ in $\mathbb{C}[G]$ generated by $\mathrm{Mon}(F)$. Then any $p \in \mathrm{Alg}_{\mathbb{C}[G]}(F)$ can be written in the form*

$$p = \sum_{u,v \in H} \beta_{u,v}(u - v) \tag{5.13}$$

with $\beta_{u,v} \in \mathbb{C}$.

Proof. We induct on the length of products needed to express $p \in \mathrm{Alg}_{\mathbb{C}[G]}(F)$. If p is a linear combination of elements of F, say $p = \sum_j \beta_j(r_j - 1)$, this is immediate since $r_j, 1 \in H$.

As the set of expressions of the form given in Equation (5.13) is closed under linear combinations, for the induction step it suffices to consider the product of $u - v, u' - v'$ for $u, u', v, v' \in H$. But the product

$$(u - v)(u' - v') = (uu' - uv') + (vv' - vu')$$

is clearly of the form Equation (5.14) since $uu', uv', vv', vu' \in H$, thus finishing the proof. $\qquad\square$

Lemma 5.8. *Consider a group algebra $\mathbb{C}[G]$ and let F be a set of elements in $\mathbb{C}[G]$ with each $f \in F$ of the form $f = r - 1$ with r a monomial and let Δ denote the subgroup of $\mathbb{C}[G]^{-1}$ generated by $\mathrm{Mon}(F) \cup \mathrm{Mon}(F^*)$ Then any element p in the $*$-subalgebra generated by F, $p \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F)$, can be written in the form*

$$p = \sum_{u,v \in \Delta} \beta_{u,v}(u - v) \tag{5.14}$$

with $\beta_{u,v} \in \mathbb{C}$.

Proof. Immediate from Lemma 5.7. $\qquad\square$

Lemma 5.9. *Assume the hypotheses of Lemma 5.8 are in force. Then*

$$1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F) \quad \Leftrightarrow \quad \Delta \cap \mathbb{C} \supsetneq \{1\}. \tag{5.15}$$

Proof. First we note that the result is trivial if there exists an element $f = r - 1 \in F$ with $r^*r \neq 1$. That is, $r = \beta g$ with $|\beta| \neq 1$. Namely,

$$(r-1)^*(r-1) + (r-1) + (r-1)^* = r^*r - 1 = \beta^*\beta - 1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F) \tag{5.16}$$

and since $\beta^*\beta - 1 \neq 0$ we can conclude $1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F)$. At the same time $rr^* = \beta\beta^* \in \Delta \cap \mathbb{C}$ and $\beta\beta^* \neq 1$. This proves the result in this special case. In what follows we can assume $rr^* = 1$ for all $r - 1 \in F$.

($\Leftarrow$) First note that for all monomials r and r' we have

$$(r-1)(r'-1) + (r-1) + (r'-1) = rr' - 1. \tag{5.17}$$

Similarly,

$$(r-1)^* = r^* - 1 = r^{-1} - 1.$$

It follows that for any $r \in \Delta$ we have $r - 1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F)$. Then, if $1 \neq \beta \in \Delta \cap \mathbb{C}$, we have $\beta - 1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F)$, whence $1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F)$.

($\Rightarrow$) To prove the result in the other direction we assume for contradiction that $\beta \notin \Delta$ for all $\beta \in \mathbb{C} \setminus \{1\}$ and that $1 \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F)$. Then, using Lemma 5.8, we can write

$$1 = \sum_{u,v \in \Delta} \beta_{u,v}(u - v) = \sum_{u,v} \beta_{u,v} u - \sum_{u,v} \beta_{u,v} v = \sum_{u,v} \beta_{u,v} u - \sum_{u,v} \beta_{v,u} u \tag{5.18a}$$

$$= \sum_{u,v} u \left(\beta_{u,v} - \beta_{v,u} \right) = \sum_u u \sum_v \left(\beta_{u,v} - \beta_{v,u} \right) \tag{5.18b}$$

where we relabeled u and v in the last term in the sum on the first line. By assumption, $\beta \notin \Delta$ for all $\beta \in \mathbb{C} \setminus \{1\}$. Thus the terms $u \sum_v (\beta_{u,v} - \beta_{v,u})$ in the last equality of Equation (5.18b) are linearly independent since the underlying group elements of distinct $u \in \Delta$ are distinct. We conclude

$$\sum_v (\beta_{1,v} - \beta_{v,1}) = 1, \tag{5.19a}$$

$$\sum_v (\beta_{u,v} - \beta_{v,u}) = 0 \tag{5.19b}$$

for all $u \neq 1$. But this is a contradiction, since

$$\sum_v (\beta_{1,v} - \beta_{v,1}) + \sum_{u \neq 1} \sum_v (\beta_{u,v} - \beta_{v,u}) = \sum_{u,v} (\beta_{u,v} - \beta_{v,u}) = 0. \qquad \square$$

5.2.2 NC Left Nullstellensatz without SOS Terms

Now we combine the results in Sections 5.1 and 5.2.1 to obtain the following specialized Nullstellensatz.

Theorem 5.10. *Consider a group algebra $\mathbb{C}[G]$ and let F be a set of elements in $\mathbb{C}[G]$ with each $f \in F$ of the form $f = r - 1$ with r a monomial and let Δ denote the subgroup of $\mathbb{C}[G]^{-1}$ generated by $\mathrm{Mon}(F \cup F^*)$.*

Then the following are equivalent:

(i) *There exists a $*$-representation $\pi : \mathbb{C}[G] \to \mathcal{B}(\mathcal{H})$ and vector $\psi \in \mathcal{H}$ with $\pi(f)\psi = 0$ for all $f \in F$;*

(i)' $\mathcal{Z}_{dir}^{\mathrm{re},\mathbb{C}[G]}(F) \neq \varnothing$;

(ii) $-1 \notin \mathfrak{L}(F)_{\mathbb{C}[G]} + \mathfrak{L}(F)_{\mathbb{C}[G]}^* + \mathrm{SOS}_{\mathbb{C}[G]}$;

(iii) $1 \notin \mathfrak{L}(F)_{\mathbb{C}[G]} + \mathfrak{L}(F)_{\mathbb{C}[G]}^*$;

(iv) $1 \notin \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)} + \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)}^*$;

(v) $1 \notin \mathrm{Alg}_{\mathbb{C}[G]}^*(F)$;

(vi) $\Delta \cap \mathbb{C} = \{1\}$.

Moreover, if each $f \in F$ is of the form $f = \beta w - 1$ with $w \in G$ and $\beta \in \mathbb{C}$ with $|\beta| = 1$, then these statements are also equivalent to

(vii) $1 \notin \mathfrak{L}(F)_{\mathbb{C}[G]}$;

(viii) $1 \notin \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)}$.

Proof. We have (i) $\Leftrightarrow$ (i)' by definition, (i) $\Leftrightarrow$ (ii) by the real Nullstellensatz Theorem 4.3, and (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) by set inclusion.

To show (iv) $\Rightarrow$ (v), assume $1 \in \mathrm{Alg}_{\mathbb{C}[G]}^*(F)$, i.e.,

$$1 = p_1 f_1 + p_2 f_2^* \tag{5.20}$$

for some $f_j \in F$ and $p_i \in \mathrm{Alg}_{\mathbb{C}[G]}^*(F \cup \{1\})$. Write $f_2 = \beta_2 w_2 - 1$ for $\beta_2 \in \mathbb{C}$ and $w_2 \in G$. Then $f_2^* = \beta_2^* w_2^* - 1$, and

$$f_2^* f_2 + f_2 + f_2^* = |\beta_2|^2 - 1. \tag{5.21}$$

If $|\beta_2|^2 \neq 1$, then Equation (5.21) immediately implies

$$1 \in \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)} + \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)}^*.$$

If $|\beta_2|^2 = 1$, then from Equation (5.21) we deduce

$$f_2^* = -f_2^* f_2 - f_2 \in \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)}, \tag{5.22}$$

whence Equation (5.20) yields

$$1 = p_1 f_1 - p_2 f_2^* f_2 - p_2 f_2 \in \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)} \subseteq \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)} + \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)}^*,$$

as desired.

Next, items (v) and (vi) are equivalent by Lemma 5.9, and (v) $\Rightarrow$ (ii) by Lemma 5.4 and Corollary 5.3. Here we use that an SOS conditional expectation mapping $\mathbb{C}[G] \to \mathrm{Alg}_{\mathbb{C}[G]}^*(F \cup \{1\}) = \mathbb{C}[\mathfrak{G}(\mathrm{supp}(F))]$ exists by Theorem 5.6.

Finally, we tackle the moreover statement. Implications (iii) $\Rightarrow$ (vii) $\Rightarrow$ (viii) are obvious. To conclude we prove (viii) $\Rightarrow$ (iv). Thus assume $1 \in \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)} + \mathfrak{L}(F)_{\mathrm{Alg}_{\mathbb{C}[G]}^*(F)}^*$, i.e.,

$$1 = \sum p_i f_i + \sum g_j^* q_j \tag{5.23}$$

for some $p_i, q_j \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F \cup \{1\})$ and $f_i, g_j \in F$. Write $q_j = q_{j1}f_{j1} + q_{j2}g^*_{j2}$ for some $q_{ji} \in \mathrm{Alg}^*_{\mathbb{C}[G]}(F \cup \{1\})$ and $f_{j1}, g_{j2} \in F$. As in Equation (5.22) we write

$$g^*_{j2} = -g^*_{j2}g_{j2} - g_{j2} \in \mathfrak{L}(F)_{\mathrm{Alg}^*_{\mathbb{C}[G]}(F)}. \tag{5.24}$$

Using Equation (5.24) in Equation (5.23) leads to

$$
\begin{aligned}
1 &= \sum p_i f_i + \sum g^*_j q_j = \sum p_i f_i + \sum g^*_j(q_{j1}f_{j1} + q_{j2}g^*_{j2}) \\
&= \sum p_i f_i + \sum g^*_j q_{j1} f_{j1} - \sum g^*_j q_{j2} g^*_{j2} g_{j2} - \sum g^*_j q_{j2} g_{j2} \\
&\in \mathfrak{L}(F)_{\mathrm{Alg}^*_{\mathbb{C}[G]}(F)},
\end{aligned}
$$

as desired. $\qquad \square$

5.3 Nullstellensätze for Perfect Torically Determined Games

We now apply the simplified Nullstellensatz of this section to nonlocal games. We first recall the definition of torically determined games introduced in Section 3.4.2.

Definition 5.11 (repeated). *A game $\mathcal{G}$ is called a torically determined game if there exists a group G with $\mathscr{U} \cong \mathbb{C}[G]$ and $\mathcal{G}$ is determined by a set of elements*

$$\mathcal{F} = \{\beta_i g_i - 1\} \tag{5.25}$$

with each $\beta_i \in \mathbb{C}$ and $g_i \in G$. In this case we say $\mathcal{G}$ is torically determined by the set $\mathcal{F}$ and call the elements $\beta_i g_i$ clauses of $\mathcal{F}$.

We let the set $\mathscr{H}$ denote all the clauses of $\mathcal{F}$. Now the following characterization of torically determined games with perfect commuting operator strategies is a quick consequence of our Nullstellensatz Theorem 5.10.

Theorem 5.12. *Let $\mathcal{G}$ be a game which is torically determined by a set $\mathcal{F} = \mathscr{H} - 1$, and let H be the group of elements in $\mathscr{U}$ generated by $\mathscr{H} \cup \mathscr{H}^*$. Then $\mathcal{G}$ has a perfect commuting operator strategy iff the following equivalent criteria are satisfied:*

(i) $1 \notin \mathfrak{L}(\mathcal{F}) + \mathfrak{L}(\mathcal{F})^*$;

(ii) $H \cap \mathbb{C} = \{1\}$.

Moreover, if $|\beta| = 1$ for each each $h = \beta g \in \mathscr{H}$ then these statements are also equivalent to

(iii) $1 \notin \mathfrak{L}(\mathcal{F})$.

Proof. By definition, $\mathcal{G}$ has a perfect commuting operator strategy iff there exists a $*$-representation π mapping $\mathscr{U}$ into bounded operators on a Hilbert space $\mathcal{H}$ and a state ψ in $\mathcal{H}$ with $\pi(h - 1)\psi = 0$ for all clauses $h \in \mathscr{H}$. But this is equivalent to the statement $\mathcal{Z}^{\mathrm{re},\mathbb{C}[G]}_{\mathrm{dir}}(\mathcal{F}) \neq \varnothing$. Then the result follows directly from Theorem 5.10. $\qquad \square$

5.3.1   Torically Determined Games and the Subgroup Membership Problem

Condition (ii) of Theorem 5.12 relates existence of perfect commuting operator strategies to a question of membership of certain elements in a group. We now translate this question to a standard instance of the subgroup membership problem.

First, observe that if any clause $\beta_i g_i \in \mathscr{H}$ has $|\beta_i| \neq 1$ then the game $\mathcal{G}$ trivially cannot have a perfect commuting operator strategy, since

$$\beta g \left(\beta g\right)^* = |\beta|^2 \neq 1 \in H. \tag{5.26}$$

Then we restrict our attention to the case where $|\beta_i| = 1$ for all $\beta_i g_i \in \mathscr{H}$. Let B be the group generated by all the β_i under multiplication, and note B is an abelian group consisting of a subset of the unit circle. Then the statement $H \cap \mathbb{C} = \{1\}$ is equivalent to $H \cap B = \{1\}$, i.e., $\beta \notin H$ for any $1 \neq \beta \in B$. This is exactly equivalent to one (or several) instances of the subgroup membership problem.

For many games the group B is very simple, containing just a few elements. In this case, alternate notation can be used for elements $\beta \in B$ (for example, the J element used in [CLS17] or the σ element in [WH20]). We see an example of this next.

5.3.2   Mod r Games

We now apply the machinery described previously in this section to Mod r Games. From Section 3.5.2 we have that Mod r games are torically determined by a set of elements

$$\left\{ (\exp(-2\pi i/r))^{s_t} \prod_{\alpha \in [k]} \left(c(\alpha)_{j_t(\alpha)}(\alpha) \right)^{d_t(\alpha)} - 1 \right\}_{t \in [T]} \tag{5.27}$$

with the $c(\alpha)_{j_t(\alpha)}$ cyclic unitaries.

Following the notation introduced in Section 5.3.1 we define B to be the group generated by the set of elements $\{(\exp(-2\pi i/r))^{s_t}\}_{t \in [T]}$. We note that B is isomorphic to a subgroup of $\mathbb{Z}_r$ and for notational convenience introduce the element ζ as shorthand for $\exp(-2\pi i/r)$. Then we can write clauses $h_t \in \mathscr{H}$ as

$$h_t = \zeta^{s_t} \prod_{\alpha \in [k]} c(\alpha)_{j_t(\alpha)}. \tag{5.28}$$

It follows that a Mod m game has a perfect commuting operator strategy iff $\zeta^s \notin H$ for all $s \in \{1, 2, \ldots, r-1\}$.

We note that if r is prime there is an immediate simplification of this characterization, since $\zeta^s \in H \Leftrightarrow \zeta^{rs+1} = \zeta \in H$ and hence a game has a perfect commuting operator strategy iff $\zeta \notin H$. We also note that the Mod 2 game (i.e., XOR game) version of this condition is equivalent to Theorem 2.1 in [WH20].

6   Gröbner Basis Algorithm Tailored to Games

What arises in this paper are sums of left and two sided ideals. We present here a kludge for using a conventional two sided ideal nc Gröbner Basis (GB) algorithm to solve these mixed ideal problems.

While a special purpose algorithm could be more efficient, the procedure here can be very convenient in practice. It has certainly been valuable to the authors. We also alert the reader to Section 8.3 which applies Gröbner Bases plus a Nullstellensatz to synchronous games.

At the core of our algorithm is the following observation:

Proposition 6.1. *Consider an ideal $\mathfrak{I}$ and left ideal $\mathfrak{L}$ in a free algebra $\mathbb{C}\langle x\rangle$. For $f \in \mathbb{C}\langle x\rangle$, we have*

$$f \in \mathfrak{I} + \mathfrak{L} \quad \Longleftrightarrow \quad f\xi \in (\mathfrak{I} + \mathfrak{L}\xi)_{\mathbb{C}\langle x,\xi\rangle},$$

where $(\mathfrak{I} + \mathfrak{L}\xi)_{\mathbb{C}\langle x,\xi\rangle}$ denotes the two-sided ideal of $\mathbb{C}\langle x,\xi\rangle$ generated by $\mathfrak{I} + \mathfrak{L}\xi$. In particular,

$$1 \in \mathfrak{I} + \mathfrak{L} \quad \Longleftrightarrow \quad \xi \in (\mathfrak{I} + \mathfrak{L}\xi)_{\mathbb{C}\langle x,\xi\rangle}.$$

Proof. The forward implication is obvious, so assume $f\xi \in (\mathfrak{I} + \mathfrak{L}\xi)_{\mathbb{C}\langle x,\xi\rangle}$, i.e.,

$$f\xi = \sum_j f_j a_j g_j + \sum_i p_i s_i \xi q_i \tag{6.1}$$

for some $f_j, g_j, p_i, q_i \in \mathbb{C}\langle x,\xi\rangle$, $a_j \in \mathfrak{I}$ and $s_i \in \mathfrak{L}$.

Each element r in $\mathbb{C}\langle x,\xi\rangle$ can be written uniquely as $r = r_0 + r_1$, where $r_0 \in \mathbb{C}\langle x\rangle$ and $r_1 \in (\xi)_{\mathbb{C}\langle x,\xi\rangle}$. We keep only terms of degree ≥ 1 in ξ in Equation (6.1) to obtain

$$f\xi = \sum_j f_{j0} a_j g_{j1} + \sum_j f_{j1} a_j g_{j0} + \sum_i p_{i0} s_i \xi q_{i0}. \tag{6.2}$$

Now extract all terms that end in ξ to get

$$f\xi = \sum_j f_{j0} a_j \tilde{g}_{j1} \xi + \sum_i p_{i0} \hat{q}_{i0} s_i \xi \tag{6.3}$$

for some $\tilde{g}_{j1} \in \mathbb{C}\langle x\rangle$ and $\hat{q}_{i0} \in \Bbbk$. Cancelling ξ on the right in Equation (6.3) leads to $f \in \mathfrak{I} + \mathfrak{L}$. $\quad\square$

6.1 Gröbner Basis Algorithm

Algorithm Suppose $a_1, \ldots, a_m, b_1, \ldots, b_n \in \mathbb{C}\langle x\rangle$ are given, and let $\mathfrak{I} = (a_1, \ldots, a_m)$, $\mathfrak{L} = \mathbb{C}\langle x\rangle b_1 + \cdots + \mathbb{C}\langle x\rangle b_n$ be a two-sided and left ideal in $\mathbb{C}\langle x\rangle$, respectively. Add a new variable ξ, to form the two-sided ideal $(a_1, \ldots, a_m, b_1\xi, \ldots, b_n\xi)_{\mathbb{C}\langle x,\xi\rangle}$ and compute its Gröbner basis B, with respect to any admissible monomial order. Then

$$1 \in \mathfrak{I} + \mathfrak{L} \quad \text{iff} \quad 1 \in B \ \text{ or } \ \xi \in B.$$

Here $1 \in B$ iff $1 \in \mathfrak{I}$. $\quad\square$

Basics of NC GB We assume the reader has a familiarity with Gröbner Bases; a standard reference in the commutative setting is [CLO15], while [Mor86, Gre00] describe the appropriate nc analogs. NC GBs have properties very similar to those of for traditional commutative GB with the dramatic exception that an NC GB might not be finite.

Fixing a monomial order, a subset B of an ideal $\mathfrak{I} \subseteq \mathbb{C}\langle x\rangle$ is a GB if the set of leading terms $\mathrm{LT}(B)$ of elements of B generates the same ideal $\mathrm{LT}(\mathfrak{I})$ as all leading terms of $\mathfrak{I}$. Roughly speaking,

the nc Bucherger criterion [Mor86, Theorem 5.1] states that B is a GB iff each S-polynomial built off B can be expressed in terms of the elements of B with lower degrees. Thus algorithms for building NC GBs work by producing S-polynomials for pairs a_i, a_j of (not necessarily distinct) polynomials which are generators of $\mathfrak{I}$. S-polynomials are ones of the form

$$S_{i,j}(w_i, w_i', w_j, w_j') = \frac{1}{\mathrm{LC}(a_i)} w_i a_i w_i' - \frac{1}{\mathrm{LC}(a_j)} w_j a_j w_j' \tag{6.4}$$

for words w_i, w_i', w_j, w_j' in x satisfying

$$w_i \, \mathrm{LT}(a_i) w_i' = w_j \, \mathrm{LT}(a_j) w_j'. \tag{6.5}$$

Here $\mathrm{LC}(a)$ denotes the coefficient of the leading term of a.

At each step in construction of a GB, one considers a collection of polynomials $\hat{B}$. If the "remainder" of an S-polynomial after division by $\hat{B}$ is nonzero, one adds it to $\hat{B}$ and repeats the process. Ultimately (maybe in an infinite number of steps) $\hat{B}$ grows to a GB B.

Left ideals have what we call left GB. Algorithms for producing left GBs are very similar to algorithms for producing GBs for 2 sided ideals. Now common multiples must be made by multiplying on the left (not the right), and the key matches are

$$w_i \, \mathrm{LT}(a_i) = w_j \, \mathrm{LT}(a_j) \tag{6.6}$$

for words w_i, w_j in x.

We refer the reader to [MR98, Xiu12] for excellent references on this.

Justification   Now behold a few properties of our GB.

(1) The set of polynomials in B which do not contain ξ is itself a Gröbner basis for $\mathfrak{I}$.

(2) The set of polynomials in B which do contain ξ, after ξ is removed, is itself a Left Gröbner basis for $\mathfrak{L}$. Moreover, the left S-polynomials which occur in the left GB algorithm for $\mathfrak{L}$ are the "same" as those which occur in the standard two sided ideal GB algorithm for $\mathfrak{L}\xi$; thus their run times are similar.

(3) The "natural generators" $x_i^2 - 1$, $x_i y_j - y_j x_i$, etc., are themselves a GB for the universal game ideal, $\mathscr{I}$. This is easily checked, say with a computer, by focusing on the subset of all polynomials involving only two variables x_i, y_j.

6.2   Examples of GBs

In the forthcoming examples we use the natural graded lexicographic order defined by

$$x_i < y_j < z_k < \xi \qquad \text{and} \quad x_0 < x_1 < \cdots, \quad \text{etc.}$$

Example 6.2. Consider the CHSH game. It has a perfect commuting operator strategy iff there exist signature matrices X_0, X_1, Y_0, Y_1 with Xs commuting with Ys so that for some state ψ we have

$$\begin{aligned} X_0 Y_0 \psi &= \psi \\ X_0 Y_1 \psi &= \psi \\ X_1 Y_0 \psi &= \psi \\ X_1 Y_1 \psi &= -\psi. \end{aligned} \tag{6.7}$$

The universal game ideal $\mathscr{I}$ for a 2-player, 2-question game, such as CHSH, with answers denoted x_0, x_1, y_0, y_1 lies in the free algebra $\Bbbk\langle x_0, x_1, y_0, y_1 \rangle$ and is generated by the 4 signature properties $x_i^2 - 1, y_j^2 - 1$ and 4 commuting relations $x_i y_j - y_j x_i$. The GB for $\mathscr{I}$ is itself, by Item (3).

So take $\mathfrak{I} = \mathscr{I}$ and take $\mathfrak{L}$ generated by $x_0 y_0 - 1$, $x_0 y_1 - 1$, $x_1 y_0 - 1$, $x_1 y_1 + 1$. This encodes the CHSH game. The Gröbner basis B for $(\mathscr{I} + \mathfrak{L}\xi)_{\Bbbk\langle x_0, x_1, y_0, y_1, \xi \rangle}$ is given by the defining relations for $\mathscr{I}$ and ξ. Since $\xi \in B$, by Proposition 6.1 we have $1 \in \mathscr{I} + \mathfrak{L}$, whence Equation (6.7) does not have a solution.

6.3 Construction of solutions to the game equations

Next we show how to attempt finding solutions to the game equations once we have a GB. We do this with an example.

Example 6.3 (GHZ 3 player game). We seek symmetries x_i, y_i, z_i, $0 \le i \le 1$, with x's commuting with y's and z's, and y's commuting with z's, so that the four operators

$$-1 - x_0 y_0 z_1, \ -1 - x_0 y_1 z_0, \ -1 - x_1 y_0 z_0, \ 1 - x_1 y_1 z_1 \tag{6.8}$$

have a common nonzero kernel vector.

In the free algebra $\mathbb{C}\langle x, y, z \rangle$ consider its ideal $\mathfrak{I}$ encoding the signature relations $x_i^2 = x_i, y_j^2 = y_j, z_j^2 = z_j$ and commuting relations $x_i y_j = y_j x_i, x_i z_j = z_j x_i, z_i y_j = y_j z_i$, and its left ideal $\mathfrak{L}$ generated by the polynomials in Equation (6.8). The Gröbner basis B for $(\mathfrak{I} + \mathfrak{L}\xi)_{\mathbb{C}\langle x, y, z, \xi \rangle}$ is given by:

the signature relations, commuting relations, and the following 18 polynomials (all of whom are divisible by ξ on the right)

$$\begin{aligned}
& y_0\xi + x_0 z_1\xi, \ z_1\xi + x_0 y_0\xi, \ x_0\xi + y_0 z_1\xi, \ y_1\xi + x_0 z_0\xi, \ z_0\xi + x_0 y_1\xi, \\
& x_0\xi + y_1 z_0\xi, \ y_0\xi + x_1 z_0\xi, \ z_0\xi + x_1 y_0\xi, \ x_1\xi + y_0 z_0\xi, \ -y_1\xi + x_1 z_1\xi, \\
& -z_1\xi + x_1 y_1\xi, \ -x_1\xi + y_1 z_1\xi, \ x_0 x_1\xi + y_1 y_0\xi, \ -x_0 x_1\xi + z_0 z_1\xi, \\
& -x_1 x_0\xi + z_1 z_0\xi, \ -x_0 x_1\xi + y_0 y_1\xi, \ x_0 x_1\xi + x_1 x_0\xi, \ -y_1 z_0\xi + x_1 x_0 x_1\xi.
\end{aligned} \tag{6.9}$$

We shall use B to construct a solution to our system. Let

$$V_0 = \mathbb{C}\langle x, y, z, \xi \rangle / (\mathfrak{I} + \mathfrak{L}\xi),$$

and let $f \mapsto \overline{f}$ denote the quotient map $\mathbb{C}\langle x, y, z, \xi \rangle \to V_0$. The subspace

$$V := \overline{\mathbb{C}\langle x, y, z \rangle \xi} \subseteq V_0$$

is eight dimensional, spanned by $B = \{\xi, \ x_0\xi, \ x_1\xi, \ y_0\xi, \ y_1\xi, \ z_0\xi, \ z_1\xi, \ x_0 x_1\xi\}$.

Each of the nc variables x_i, y_i, z_i acts on V from the left, and with respect to the basis B we

obtain matrix representations as follows:

$$\widehat{x}_0 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \widehat{x}_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\widehat{y}_0 = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}, \quad \widehat{y}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\widehat{z}_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad \widehat{z}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \end{pmatrix}.$$

It is easy to verify that these solve the system Equation (6.8) with common kernel vector e_1.

Remark. For a 3-XOR game, if the restricted GNS construction (as in Example 6.3) gives a finite-dimensional space of dim > 8, then the solution to the game may not be unique. Indeed, MERP is one solution; it has dim 8. Other solutions may show up in the GNS construction via it block diagonalizing and the other solutions being blocks. These blocks might all be unitarily equivalent to the MERP solution; otherwise the game has multiple solutions.

The problem of establishing uniqueness of solution to the game has been studied and there is a standard technique available. cf [CMMN20]. It can be tried on a game for which the bias and optimal value satisfy

$$\omega^* - \Phi_{\mathcal{G}} = SOS$$

exactly (as opposed to approximately as in [NPA08, DLTW08, HM04]). Optimality implies there exists a state ψ making

$$0 = (\omega^* - \Phi_{\mathcal{G}})\psi = SOS\psi.$$

Thus we get algebraic equations $s_j\psi = 0$ corresponding to $SOS = \sum_j s_j^* s_j$. For some games it is possible to show from these equations have only one solution (that is, a unique $*$-representation) and from this show that the game has a unique optimal strategy.

7 Linear Systems Games

Linear systems games are some of the first games to have their perfect commuting operator strategies characterized algebraically. This characterization, given in [CLS17], shows that perfect commuting operator strategies for linear systems games arise from representations of a group called the solution group of the game. As a result of this characterization, deciding existence of perfect commuting

operator strategies for linear systems games was shown to be equivalent to solving an instance of the word problem.

In this section, we reconcile this characterization of linear systems games with the Nullstellensatz framework described in this paper. In particular, we derive the linear systems game characterization given in [CLS17] using Theorem 5.12 as a starting point.

To begin, we recap the definition of linear systems games.

Definition 7.1. *A linear systems game $\mathcal{G}$ is a two player game based on a system of m linear equations in n variables computed mod r. A question to Alice is an integer $i \in [m]$ selecting an equation in the linear system equation. A question to Bob selects a variable $j \in [n]$. Alice's response consists of a vector $\vec{a}_i = (a_{i_1}, a_{i_2}, \ldots, a_{i_k}) \in [r]^k$ containing values for all the variables contained in the i-th equation, with $i_1, \ldots i_k$ indexing the variables. Bob's response is a single variable $b_j \in [r]$. The players win each round provided variables $(a_{i_1}, a_{i_2}, \ldots, a_{i_k})$ satisfy the i-th equation and $a_{i_t} = b_j$ whenever $i_t = j$.*

Following the notation laid out in Section 3.2 note the game algebra $\mathcal{U}$ is generated by elements $e(1)^i_{\vec{a}_i}$ and $e(2)^j_{b_j}$ with $\vec{a}_j$ ranging over all possible vectors of responses to question i and b_j ranging over all possible values Bob can give for variable b_j.

Next, we identify elements of $\mathcal{U}$ which correspond to the value Alice gives to a single variable in the system of equations. For any $i \in [m]$ let $T(i) = \{t_1, t_2, \ldots, t_k\}$ list all the variables contained in the i-th equation in the system of equations associated with the game. Then, for any $t \in T(i)$ and $r' \in [r]$ define

$$e(1)^i_{a_t=r'} = \sum_{\vec{a}_i : a_t = r'} e(1)^i_{\vec{a}_i}. \tag{7.1}$$

It is easy to check that the elements $e(1)^i_{a_t=r'}$ also satisfy the relations of projectors,

$$\left(e(1)^i_{a_t=r'}\right)^2 = \left(e(1)^i_{a_t=r'}\right)^* = e(1)^i_{a_t=r'}, \tag{7.2a}$$

$$\sum_{r' \in [r]} e(1)^i_{a_t=r'} = 1. \tag{7.2b}$$

Additionally, orthogonality of the $e(1)^i_{\vec{a}_i}$ elements gives that for any $i \in [m]$, $t_1, t_2 \in T(i)$, and $r_1, r_2 \in [r]$ we have

$$e(1)^i_{a_{t_1}=r_1} e(1)^i_{a_{t_2}=r_2} = e(1)^i_{a_{t_2}=r_2} e(1)^i_{a_{t_1}=r_1} = \sum_{\substack{\vec{a}_i : a_{t_1}=r_1 \\ \text{and } a_{t_2}=r_2}} e(1)^i_{\vec{a}_i} \tag{7.3}$$

Finally we note that, also by orthogonality of the $e(1)^i_{\vec{a}_i}$ elements we have for any i with $T(i) = \{t_1, \ldots, t_k\}$ and $\vec{a}_i = (r_{t_1}, r_{t_2}, \ldots, r_{t_k})$ that

$$\prod_{t \in T(i)} e(1)^i_{a_t=r_t} = e(1)^i_{\vec{a}_i}. \tag{7.4}$$

From here we can define cyclic unitary generators analogously to in Section 3.3, with

$$c(1)_t^{(j)} := \sum_{r'=1}^{r} \exp\left(\frac{2\pi r' i}{r}\right) e(1)_{a_t=r'}^j, \tag{7.5a}$$

$$c(2)_j := \sum_{a=1}^{r} \exp\left(\frac{2\pi a i}{r}\right) e(2)_a^j. \tag{7.5b}$$

These unitary generators satisfy the same relations as the generators defined in Section 3.3, namely,

$$\left(c(1)_t^{(i)}\right)^r = (c(2)_j)^r = 1, \tag{7.6a}$$

$$\left(c(1)_t^{(i)}\right)^* c(1)_t^{(i)} = (c(2)_j)^* c(2)_j = 1, \tag{7.6b}$$

$$c(1)_t^{(i)} c(2)_j = c(2)_j c(1)_t^{(i)} \quad \forall\, i \in [m],\ j, t \in [n]. \tag{7.6c}$$

In addition, Equation (7.4) gives that

$$c(1)_{t_1}^{(i)} c(1)_{t_2}^{(i)} = c(1)_{t_2}^{(i)} c(1)_{t_1}^{(i)} \quad \forall\, i \in [m],\ t_1, t_2 \in T(i). \tag{7.6d}$$

We can then define G_{ls} to be the group generated by the $c(1)_t^{(i)}$ and $c(2)_j$.

Now we show that linear systems games are torically determined games.

Theorem 7.2. *Let $\mathcal{G}_{ls}$ be a linear systems game based on a system of m equations. For any $j \in [m]$ write the j-th equation of the system as*

$$\sum_{t \in T(j)} d_t^{(j)} y_t = s_j \pmod{r} \tag{7.7}$$

where $T(j)$ indexes all the variables y_t contained in the j-th equation of the system and $d_t^{(j)}, s_j \in [r]$. Then $\mathcal{G}_{ls}$ is a torically determined game, determined by the elements

$$\mathcal{F} = \left\{ \exp\left(-\frac{2\pi s_j i}{r}\right) \prod_{t \in T(j)} \left(c(1)_t^{(j)}\right)^{d_t^{(j)}} - 1 \right\}_{j \in [m]} \bigcup \left\{ c(1)_t^{(j)} \left(c(2)_t\right)^* - 1 \right\}_{t \in [n], j \in [m]}. \tag{7.8}$$

Proof. First we note that expanding out the product and applying Equation (7.4) gives

$$\prod_{t \in T(j)} \left(c(1)_t^{(j)}\right)^{d_t^{(j)}} = \prod_{t \in T(j)} \left(\sum_{r'=1}^{r} \exp\left(\frac{2\pi d_t^{(j)} r' i}{r}\right) e(1)_{a_t=r'}^j\right) \tag{7.9}$$

$$= \sum_{\vec{a}_j} \exp\left(\frac{2\pi i}{r} \sum_{t \in T(j)} d_t^{(j)} a_t^{(j)}\right) e(1)_{\vec{a}_j}^j \tag{7.10}$$

where we wrote $\vec{a}_j = (a_{t_1}^{(j)}, a_{t_2}^{(j)}, \ldots, a_{t_k}^{(j)})$ for $\{t_1, t_2, \ldots, t_k\} \in T(j)$. Then define

$$A(j) = \left\{ \vec{a}_j : \sum_{t \in T(j)} d_t^{(j)} a_t^{(j)} = s_j \pmod{r} \right\} \tag{7.11}$$

38

to be the collection of winning responses Alice can send to question j. Then as a consequence of Equation (7.10), we have for any commuting operator strategy (π, ψ) that the condition

$$\pi \left(\prod_{t \in T(j)} \left(c(1)_t^{(j)} \right)^{d_t^{(j)}} \right) \psi = \exp \left(\frac{2\pi i s_j}{r} \right) \psi \tag{7.12a}$$

is equivalent to

$$\pi \left(\sum_{\vec{a}_j \in A(j)} \pi(e(1)_{\vec{a}_j}^j) \right) \psi = \psi. \tag{7.12b}$$

Hence the condition

$$\pi \left(\exp \left(-\frac{2\pi s_j i}{r} \right) \prod_{t \in T(j)} \left(c(1)_t^{(j)} \right)^{d_t^{(j)}} - 1 \right) \psi = 0 \tag{7.13}$$

for all $j \in [m]$ ensures that Alice's responses in the game $\mathcal{G}_{ls}$ are always winning. Similarly, the condition

$$\pi \left(c(1)_t^{(j)} \left(c(2)_t \right)^* \right) \psi = \psi \tag{7.14}$$

ensures that

$$\sum_{r' \in [r]} \pi \left(e(1)_{a_t = r'}^j e(2)_{r'}^t \right) \psi = \psi \tag{7.15}$$

and thus Bob's responses are also always winning. Thus it is clear that $\mathcal{G}_{ls}$ is determined by $\mathcal{F}$.

It remains to show that all the elements of $\mathcal{F}$ are of the correct form. But we have that the elements $c(1)_t^{(j)}$ and $c(t)_2$ generate the elements $e(1)_{a_t = r'}^j$ and $e(2)_a^j$ through the same inverse transformation as given for the cyclic unitary generators in Section 3.3.1. And we also know that the elements $e(1)_{a_t = r'}^j$ generate the elements $e(1)_{\vec{a}_i}^j$ by Equation (7.4). Then $\mathscr{U} = \mathbb{C}[G_{ls}]$ and the result is clear. $\qquad\square$

Theorem 7.2 reduces the question of whether or not a game has a perfect commuting operator strategy to an instance of the subgroup membership problem. The next theorem lets us reduce further to the standard formulation in terms of the word problem. We prepare with a few definitions, following wherever possible the conventions laid out in Section 5.3.1.

Definition 7.3. *Let $\mathcal{G}_{ls}$ be a linear systems game based on a system of m equations defined as in Theorem 7.2 and introduce to shorthand $\zeta = \exp\left(-\frac{2\pi i}{r} \right)$ to simplify notation. Then define the following groups:*

(1) *G_{ls}^{aug} to be the subgroup of $\mathbb{C}[G_{ls}]$ generated by the elements $G_{ls} \cup \{\zeta\}$;*

(2) *$H_{ls} < G_{ls}^{aug}$ to be the subgroup of G_{ls}^{aug} generated by the set of elements*

$$\left\{ \zeta^{s_i} \prod_{t \in T(i)} \left(c(1)_t^{(i)} \right)^{d_t^{(i)}} \right\}_{i \in [m]} \bigcup \left\{ c(2)_t \left(c(1)_t^{(i)} \right)^{-1} \right\}_{i \in [m], t \in [r]} ; \tag{7.16}$$

(3) $G_{ls}^{aug}(2)$ to be the subgroup of G_{ls}^{aug} generated by the elements

$$\{c(2)_t\}_{t\in[r]} \cup \{\zeta\}; \tag{7.17}$$

(4) $N_{ls}(2)$ to be the normal subgroup of $G_{ls}^{aug}(2)$ generated by the elements

$$\left\{ \zeta^{s_i} \prod_{t\in T(i)} (c(2)_t)^{d_t^{(i)}} \right\}_{i\in[m]} \bigcup \left\{ c(2)_t c(2)_{t'} c(2)_t^{-1} c(2)_{t'}^{-1} \right\}_{t,t'\in T(i), i\in[m]}. \tag{7.18}$$

Theorem 7.4. *A linear system game $\mathcal{G}_{ls}$, defined as in Theorem 7.2, has a perfect commuting operator strategy iff any of the equivalent conditions are satisfied:*

(i) $\zeta^s \notin H_{ls}$ *for all* $s \in [r-1]$;

(ii) $\zeta^s \notin N_{ls}(2)$ *for all* $s \in [r-1]$;

(iii) *Letting $[\zeta^s]$ denote the image of $\zeta^s \in G_{ls}^{aug}(2)$ in the group $G_{ls}^{aug}(2)/N_{ls}(2)$, then $[\zeta^s] \neq 1$ for all* $s \in [r-1]$.

Proof. We first note that condition (i) is equivalent to the existence of a perfect commuting operator strategy by Theorem 7.2 and Theorem 5.12.

To show (i) $\Rightarrow$ (ii) we show $N_{ls}(2)$ is contained in H_{ls}. First note that for any $i \in [m]$ we have

$$\left(\zeta^{s_i} \prod_{t\in T(i)} \left(c(1)_t^{(i)}\right)^{d_t^{(i)}} \right) \prod_{t\in T(i)} \left(\left(c(1)_t^{(i)}\right)^{-1} c(2)_t \right)^{d_t^{(i)}} = \zeta^{s_i} \prod_{t\in T(i)} (c(2)_t)^{d_t^{(i)}} \in H_{ls} \tag{7.19}$$

and, for any $i \in [m]$ and $t_1, t_2 \in T(i)$ we can multiply together generators of the group H_{ls} to find

$$\left(c(2)_{t_1} \left(c(1)_{t_1}^{(i)}\right)^{-1} \right) \left(c(2)_{t_2} \left(c(1)_{t_2}^{(i)}\right)^{-1} \right) \left(c(2)_{t_1} \left(c(1)_{t_1}^{(i)}\right)^{-1} \right)^{-1} \left(c(2)_{t_2} \left(c(1)_t^{(i)}\right)^{-1} \right)^{-1}$$

$$= \left(c(2)_{t_1} c(2)_{t_2} c(2)_{t_1}^{-1} c(2)_{t_2}^{-1} \right) \left(\left(c(1)_{t_1}^{(i)}\right)^{-1} \left(c(1)_{t_2}^{(i)}\right)^{-1} c(1)_{t_1}^{(i)} c(1)_{t_2}^{(i)} \right). \tag{7.20a}$$

Now we cancel the $c(1)_{t_1}^{(i)}$ terms using Equation (7.6d) to get

$$c(2)_{t_1} c(2)_{t_2} c(2)_{t_1}^{-1} c(2)_{t_2}^{-1} \in H_{ls}. \tag{7.20b}$$

Finally, we note that for any elements $w(2) \in H_{ls} \cap G_{ls}^{aug}(2)$ and $c(2)_t$ generating $G_{ls}^{aug}(2)$ we have

$$\left(c(2)_t \left(c(1)_t^{(i)}\right)^{-1} \right) w(2) \left(c(2)_t \left(c(1)_t^{(i)}\right)^{-1} \right)^{-1} = c(2)_t w(2) c(2)_t^{-1} \in H_{ls} \tag{7.21}$$

and thus, the normal closure in $G_{ls}^{aug}(2)$ of any element in $H_{ls} \cap G_{ls}^{aug}(2)$ is also contained in H_{ls} (recall that the element ζ is central). We conclude that $N_{ls}(2) \subseteq H_{ls}$, as desired.

To show that (ii) $\Rightarrow$ (i) we assume $\zeta^s \in H_{\mathrm{ls}}$ for some $s \in [r-1]$. Then, there exists elements $w(1)_1, \ldots, w(1)_L$ and $v(1,2)_1, \ldots, v(1,2)_{L+1}$ with each $w(1)_\ell$ equal to a product of elements or inverses of elements in the set

$$\left\{ \zeta^{s_i} \prod_{t \in T(i)} \left(c(1)_t^{(i)} \right)^{d_t^{(i)}} \right\}_{i \in [m]} \tag{7.22}$$

each $v(1,2)_{\ell'}$ equal to a product of elements or inverses of elements in the set

$$\left\{ c(2)_t \left(c(1)_t^{(i)} \right)^{-1} \right\}_{i \in [m], t \in [r]} \tag{7.23}$$

and

$$\zeta^s = v(1,2)_1 w(1)_1 v(1,2)_2 w(1)_2 \cdots v(1,2)_L w(1)_L v(1,2)_{L+1}. \tag{7.24}$$

Then let the elements $w(2)_\ell$ for $\ell \in \{1, 2, ..., L\}$ be obtained by choosing some product of elements drawn from the set defined in Equation (7.22) and equal to $w(1)_\ell$, then making the replacement

$$\zeta^{s_i} \prod_{t \in T(i)} \left(c(1)_t^{(i)} \right)^{d_t^{(i)}} \to \zeta^{s_i} \prod_{t \in T(i)} (c(2)_t)^{d_t^{(i)}} \tag{7.25}$$

to each element in the product.[7] Similarly let elements $v(1)_1, \ldots, v(1)_{L+1}$ be obtained from $v(1,2)_\ell$ by the replacement

$$c(2)_t \left(c(1)_t^{(i)} \right)^{-1} \to \left(c(1)_t^{(i)} \right)^{-1} \tag{7.26}$$

and elements $v(2)_1, \ldots, v(2)_{L+1}$ be obtained via the replacement

$$c(2)_t \left(c(1)_t^{(i)} \right)^{-1} \to c(2)_t \tag{7.27}$$

applied to some fixed products of elements from Equation (7.23) equal to $v(1,2)_\ell$.

Then commuting $c(1)_t$ and $c(2)_t$ elements gives

$$\zeta^s = v(1,2)_1 w(1)_1 v(1,2)_2 w(1)_2 \cdots v(1,2)_L w(1)_L v(1,2)_{L+1}$$
$$= v(1)_1 w(1)_1 v(1)_2 w(1)_2 \cdots v(1)_L w(1)_L v(1)_{L+1} v(2)_1 v(2)_2 \cdots v(2)_{L+1}. \tag{7.28}$$
$$\tag{7.29}$$

From this we conclude

$$v(2)_1 v(2)_2 \cdots v(2)_{L+1} = 1 \tag{7.30}$$

since the word $v(2)_1 v(2)_2 \cdots v(2)_{L+1}$ contains only $c(2)_t$ elements (and no product of $c(2)_t$ elements and their inverses can be to equal ζ or to any product of $c(1)_t$ elements) and hence

$$v(1)_1 w(1)_1 v(1)_2 w(1)_2 \cdots v(1)_L w(1)_L v(1)_{L+1} = \zeta^s. \tag{7.31}$$

---

[7] Note we have not shown this definition of $w(2)_\ell$ is unique, i.e. we have not shown that this replacement defines a homomorphism, but we will not need to for the current proof.

But then we also have

$$v(2)_1 w(2)_1 v(2)_2 w(2)_2 \cdots v(2)_L w(2)_L v(2)_{L+1} = \zeta^s \tag{7.32}$$

since the relations between $c(2)_t$ elements are the same as those between the $c(1)_t^{(i)}$ elements. Then the calculation

$$\zeta^s = \left(\prod_{\ell \in [L]} v(2)_\ell w(2)_\ell \right) v(2)_{L+1} \tag{7.33a}$$

$$= \left(\prod_{\ell \in [L]} \left(\prod_{\ell' < \ell} v(2)_{\ell'} \right) w(2)_\ell \left(\prod_{\ell' < \ell} v(2)_{\ell'} \right)^{-1} \right) v(2)_1 v(2)_2 \cdots v(2)_{L+1} \tag{7.33b}$$

$$= \left(\prod_{\ell \in [L]} \left(\prod_{\ell' < \ell} v(2)_{\ell'} \right) w(2)_\ell \left(\prod_{\ell' < \ell} v(2)_{\ell'} \right)^{-1} \right) \in N_{\mathrm{ls}}(2) \tag{7.33c}$$

shows $\zeta^s \in N_{\mathrm{ls}}(2)$, as desired.

Finally we note (ii) $\Leftrightarrow$ (iii) by the definition of a quotient group. $\qquad \square$

8 Nullstellensatz applied to Synchronous Games

As discussed in the introduction, a two player game is called synchronous if it includes "consistency-checks" where Alice and Bob are sent the same question and win iff they send the same response. Below we give a formal definition of synchronous games using the scoring function and probability distribution description of games introduced in Section 3.2.2.

Definition 8.1. *A two player, n question, m response game $\mathcal{G}$ defined by scoring function V and question distribution μ is called a* **synchronous game** *iff, for all $i \in [n]$ we have*

$$\mu(i, i) > 0 \tag{8.1}$$

and

$$V(a, b | i, i) = \delta_{a,b} \tag{8.2}$$

where $\delta_{a,b}$ denotes the Kronecker delta function.

An immediate consequence of Definition 8.1 in terms of the notion of invalid determining set introduced in Section 3.4.1 is the following claim.[8]

Claim 8.2. *Let $\mathcal{G}$ be a synchronous game and $\mathcal{N}$ be the invalid elements of $\mathcal{G}$. Then we have*

$$e(1)_a^i e(2)_b^i \in \mathfrak{L}(\mathcal{N}) \tag{8.3}$$

for all $i \in [n]$ and $a, b \in [m]$ with $a \neq b$.

---

[8]We note this claim can hold true for a larger class of games than synchronous ones. In most of this section the only property of synchronous games which will be used is that they satisfy Equation (8.3). Thus, most of the techniques of this section apply to a slightly larger class of games than synchronous ones.

Proof. Immediate since for all for all $i \in [n]$ and $a, b \in [m]$ with $a \neq b$ we have $V(a, b|i, i) = 0$ and $\mu(i, i) > 0$ by definition of a synchronous game, hence $e(1)_a^i e(2)_b^i \in \mathcal{N}$ by the definition of $\mathcal{N}$. $\qquad\square$

Synchronous games can be studied using the standard techniques of this paper, where we consider representations of the algebra $\mathscr{U}$ which satisfy directional zero constraints. However, Paulsen with various collaborators [PSS$^+$16] [HMPS17, Theorem 3.2], found an equivalent simpler formulation using a 'smaller' algebra which we denote $\mathscr{U}(1)$, and using hard zeroes arising from an ideal $\mathfrak{I}(\operatorname{synch} \mathcal{B}(1))$ of $\mathscr{U}(1)$. Also the papers [PSS$^+$16, KPS18] show that the synchronous value of a game is given by the trace of a bilinear function on $\mathscr{U}(1)$. The first goal in this section is to show how this reconciles with our Nullstellensätze. This is the substance of Theorem 8.3 in Section 8.1.

Next in Section 8.2 we turn to the tracial Nullstellensatz and recall that the theory of Null- and Positivstellensätze appropriate to tracial situations go back to [KS08] and is well developed in subsequent papers which are summarized in [BKP16, Chapter 5]; see also [KP16].

Finally, in Section 8.3 we demonstrate (on a graph coloring problem) a computer algorithm based on Gröbner Bases plus Nullstellensatz.

8.1 Synchronous two player games in terms of an algebra

In what follows let:

(1) $\mathscr{U}$ be the universal game algebra;

(2) $\mathfrak{L}(\mathcal{N})$ be the left ideal of $\mathscr{U}$ generated by the set $\left\{ \prod_\alpha e(\alpha)_{a(\alpha)}^{i(\alpha)} : (\vec{i}, \vec{a}) \in \mathcal{N} \right\}$;

(3) $\mathfrak{L}(\operatorname{synch} \mathcal{B})$ be the left ideal of $\mathscr{U}$ generated by the set

$$\left\{ \prod_\alpha e(1)_{a(\alpha)}^{i(\alpha)} : (\vec{i}, \vec{a}) \in \mathcal{N} \right\} \cup \left\{ \prod_\alpha e(2)_{a(\alpha)}^{i(\alpha)} : (\vec{i}, \vec{a}) \in \mathcal{N} \right\} \cup \left\{ e(1)_a^i - e(2)_a^i : i \in [n], a \in [m] \right\};$$

(4) $\mathscr{U}(1)$ be the subalgebra of $\mathscr{U}$ generated by $e(1)_a^i$ only;

(5) $\mathfrak{I}(\operatorname{synch} \mathcal{B}(1))$ be the two sided ideal of $\mathscr{U}(1)$ generated by $\left\{ \prod_\alpha e(1)_{a(\alpha)}^{i(\alpha)} : (\vec{i}, \vec{a}) \in \mathcal{N} \right\}$.

Now we state the objective of this section.

Theorem 8.3. *A synchronous game characterized by a set $\mathcal{N}$ of invalid responses has a perfect commuting operator strategy iff any of the equivalent conditions are satisfied:*

(i) *There exists a $*$-representation $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ and a state $\psi \in \mathcal{H}$ satisfying*

$$\pi(\mathfrak{L}(\mathcal{N}))\psi = \{0\}; \tag{8.4}$$

(i)' $\mathcal{Z}_{dir}^{\operatorname{re}, \mathscr{U}}(\mathcal{N}) \neq \varnothing$;

(ii) *There exists a $*$-representation $\pi : \mathscr{U} \to \mathcal{B}(\mathcal{H})$ and a state $\psi \in \mathcal{H}$ satisfying*

$$\pi(\mathfrak{L}(\operatorname{synch} \mathcal{B}))\psi = \{0\}; \tag{8.5}$$

(ii)' $\mathcal{Z}_{dir}^{\mathrm{re},\mathscr{U}}(\mathrm{synch}\,\mathcal{B}) \neq \varnothing$;

(iii) *There exists a $*$-representation $\pi' : \mathscr{U}(1) \to \mathcal{B}(\mathcal{H})$ and a tracial state $\psi \in \mathcal{H}$ satisfying*

$$\pi'(\mathfrak{I}(\mathrm{synch}\,\mathcal{B}(1))\psi = \{0\}; \tag{8.6}$$

(iv) *There exists a $*$-representation π' of $\mathscr{U}(1)$ mapping into a tracial von Neumann algebra $\mathcal{W} \subseteq \mathcal{B}(\mathcal{H})$ satisfying*

$$\pi'(\mathfrak{I}(\mathrm{synch}\,\mathcal{B}(1))) = \{0\}; \tag{8.7}$$

The proof of (i), (ii), (iii) is based on several lemmas which we now give. The core of the proofs of the lemmas come from [PSS$^+$16] but we include a self contained account for clarities sake.

Lemma 8.4. *If the set of invalid responses $\mathcal{N}$ comes from a synchronous game, we have $\mathfrak{L}(\mathcal{N}) = \mathfrak{L}(\mathrm{synch}\,\mathcal{B})$.*

Proof. We first show that $e(1)_a^i - e(2)_a^i \in \mathfrak{L}(\mathcal{N})$. Because $\mathcal{N}$ corresponds to a synchronous game, we have

$$e(1)_a^i e(2)_b^i \in \mathcal{N} \subseteq \mathfrak{L}(\mathcal{N}) \tag{8.8}$$

for all $b \neq a$. Then we also have

$$\mathfrak{L}(\mathcal{N}) \ni \sum_{b \neq a} e(1)_a^i e(2)_b^i = e(1)_a^i \sum_{b \neq a} e(2)_b^i = e(1)_a^i(1 - e(2)_a^i) \tag{8.9a}$$

$$= e(1)_a^i - e(1)_a^i e(2)_a^i. \tag{8.9b}$$

Similarly, summing over the $e(1)$ terms (and recalling that $e(1)$ and $e(2)$ commute) gives:

$$\sum_{b \neq a} e(1)_b^i e(2)_a^i = e(2)_a^i(1 - e(1)_a^i) = e(2)_a^i - e(1)_a^i e(2)_a^i \in \mathfrak{L}(\mathcal{N}). \tag{8.10}$$

Subtracting Equation (8.10) from Equation (8.9b) gives

$$e(1)_a^i - e(2)_a^i \in \mathfrak{L}(\mathcal{N}). \tag{8.11}$$

Next note that for any $e(1)_a^i e(2)_b^j \in \mathcal{N}$ we have

$$e(1)_a^i e(1)_b^j = e(1)_a^i\big(e(1)_b^j - e(2)_b^j\big) + e(1)_a^i e(2)_b^j \in \mathfrak{L}(\mathcal{N}). \tag{8.12}$$

A similar argument shows $e(2)_a^i e(2)_b^j \in \mathfrak{L}(\mathcal{N})$. Then all the generators of $\mathfrak{L}(\mathrm{synch}\,\mathcal{B})$ are contained in $\mathfrak{L}(\mathcal{N})$ and we conclude $\mathfrak{L}(\mathrm{synch}\,\mathcal{B}) \subseteq \mathfrak{L}(\mathcal{N})$.

To prove the converse we observe that for any $e(1)_a^i e(2)_b^j \in \mathcal{N}$ we have

$$e(1)_a^i e(2)_b^j = e(1)_a^i e(1)_b^j - e(1)_a^i\big(e(1)_b^j - e(2)_b^j\big) \in \mathfrak{L}(\mathrm{synch}\,\mathcal{B}), \tag{8.13}$$

which gives $\mathfrak{L}(\mathcal{N}) \subseteq \mathfrak{L}(\mathrm{synch}\,\mathcal{B})$ and completes the proof. $\qquad\square$

Lemma 8.5. $\mathfrak{I}(\text{synch}\,\mathcal{B}(1)) \subseteq \mathfrak{L}(\text{synch}\,\mathcal{B})$.

Proof. First consider a monomial $m(1) = e(1)_{a_1}^{i_1}\cdots e(1)_{a_t}^{i_t} \in \mathscr{U}(1)$ and note

$$e(1)_{a_1}^{i_1}\cdots e(1)_{a_t}^{i_t} = e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}}(e(1)_{a_t}^{i_t} - e(2)_{a_t}^{i_t}) + e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}}e(2)_{a_t}^{i_t} \tag{8.14a}$$

$$= e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}}(e(1)_{a_t}^{i_t} - e(2)_{a_t}^{i_t}) + e(2)_{a_t}^{i_t}e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}}, \tag{8.14b}$$

whence

$$e(1)_{a_1}^{i_1}\cdots e(1)_{a_t}^{i_t} - e(2)_{a_t}^{i_t}e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}} \in \mathfrak{L}(\text{synch}\,\mathcal{B}).$$

Applying this inductively we see

$$e(1)_{a_1}^{i_1}\cdots e(1)_{a_t}^{i_t} - e(2)_{a_t}^{i_t}e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}} \tag{8.15a}$$

$$+ e(2)_{a_t}^{i_t}\left(e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}} - e(2)_{a_{t-1}}^{i_{t-1}}e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-2}}^{i_{t-2}}\right) \tag{8.15b}$$

$$+ e(2)_{a_t}^{i_t}e(2)_{a_{t-1}}^{i_{t-1}}\left(e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-1}}^{i_{t-1}} - e(1)_{a_{t-2}}^{i_{t-2}}e(1)_{a_1}^{i_1}\cdots e(1)_{a_{t-3}}^{i_{t-3}}\right) \tag{8.15c}$$

$$+ \cdots \tag{8.15d}$$

$$= e(1)_{a_1}^{i_1}\cdots e(1)_{a_t}^{i_t} - e(2)_{a_t}^{i_t}e(2)_{a_{t-1}}^{i_{t-1}}\cdots e(2)_{t_1}^{i_1} \in \mathfrak{L}(\text{synch}\,\mathcal{B}). \tag{8.15e}$$

We can write this last expression compactly as $m(1) - m(2)^* \in \mathfrak{L}(\text{synch}\,\mathcal{B})$, where we understand $m(2)$ to be the polynomial $m(1)$ with all $e(1)$ replaced by $e(2)$. By linearity this observation immediately extends to general polynomials, so we have $p(1) - p(2)^* \in \mathfrak{L}(\text{synch}\,\mathcal{B})$ for any polynomial $p(1)$ formed entirely from $e(1)$.

For any polynomial $p \in \mathfrak{I}(\text{synch}\,\mathcal{B}(1))$ we can write $p = s(1)t(1)$ where $s(1) \in \mathfrak{L}(\text{synch}\,\mathcal{B})$ and $t(1) \in \mathscr{U}(1)$ is an arbitrary polynomial consisting only of $e(1)$ generators. Then we observe:

$$p = s(1)t(1) = s(1)(t(1) - t(2)^*) + t(2)^*s(1) \in \mathfrak{L}(\text{synch}\,\mathcal{B}) \tag{8.16}$$

and we are done. $\qquad\qquad\square$

Also important in this section are tracial linear mappings on an algebra, defined to be linear mappings $\tau : \mathscr{A} \to \mathbb{C}$ satisfying

$$\tau(ab) = \tau(ba) \tag{8.17}$$

for all $a, b \in \mathscr{A}$. A state ψ is called a tracial state (for some operator algebra $\mathscr{A}$) if the linear mapping it induces is tracial, so

$$\psi^*ab\psi = \psi^*ba\psi \tag{8.18}$$

for all operators $a, b \in \mathscr{A}$. We show, using an argument very similar to the one given in the proof of Lemma 8.5, that any linear mapping vanishing on $\mathfrak{L}(\text{synch}\,\mathcal{B})$ and $\mathfrak{R}(\text{synch}\,\mathcal{B})$ must be tracial on $\mathscr{U}(1)$.

Lemma 8.6. *Given a linear mapping $\tau : \mathscr{U} \to \mathbb{C}$ on $\mathscr{U}$ satisfying*

$$\tau(\mathfrak{L}(\text{synch}\,\mathcal{B})) = 0 = \tau(\mathfrak{R}(\text{synch}\,\mathcal{B})), \tag{8.19}$$

then τ is tracial on $\mathscr{U}(1)$; i.e. for any $a, b \in \mathscr{U}(1)$,

$$\tau(ab) = \tau(ba). \tag{8.20}$$

Note: If τ is symmetric, then since synch $\mathcal{B}$ is a $*$-closed set, we have

$$\tau(\mathfrak{L}(\text{synch}\,\mathcal{B})) = 0 \implies \tau(\mathfrak{R}(\text{synch}\,\mathcal{B})) = 0.$$

Proof. Consider monomials $w, \tilde{w} \in \mathscr{U}(1)$. Since w is generated by $e(1)_a^i$, we can write $w = w'e(1)_a^i$ and then observe

$$\tilde{w}w'\left(e(1)_a^i - e(2)_a^i\right) \in \mathfrak{L}(\text{synch}\,\mathcal{B}), \tag{8.21a}$$

$$\left(e(1)_a^i - e(2)_a^i\right)\tilde{w}w' \in \mathfrak{R}(\text{synch}\,\mathcal{B}). \tag{8.21b}$$

Then

$$\tau(\tilde{w}w'e(1)_a^i) = \tau(\tilde{w}w'e(2)_a^i) = \tau(e(2)_a^i\tilde{w}w') = \tau(e(1)_a^i\tilde{w}w') \tag{8.22}$$

where we use Equation (8.21a) for the first equality, that elements of $\mathscr{U}(1)$ and $\mathscr{U}(2)$ commute for the second equality, and Equation (8.21b) for the equality. Repeating this argument shows that for any elements $w, \tilde{w} \in \text{synch}\,\mathcal{B}(1)$ we have

$$\tau(w\tilde{w}) = \tau(\tilde{w}w) \tag{8.23}$$

and the proof is complete. $\square$

Now comes the proof of the main theorem of this section.

Proof of Theorem 8.3. Item (i) is equivalent to existence of a perfect commuting operator strategy by definition (see Section 3.4).

Item (ii) is equivalent to Item (i) by Lemma 8.4.

To prove Item (ii) $\Rightarrow$ Item (iii) we let π be any representation satisfying Item (ii), and define π' to be the restriction of π to $\mathscr{U}(1)$. Clearly $\pi' : \mathscr{U}(1) \to \mathcal{B}(\mathcal{H})$ and

$$\pi'(\mathfrak{I}(\text{synch}\,\mathcal{B}(1)))\psi = \pi(\mathfrak{I}(\text{synch}\,\mathcal{B}(1)))\psi \subseteq \pi(\mathfrak{L}(\text{synch}\,\mathcal{B}))\psi = \{0\}, \tag{8.24}$$

where the inclusion follows from Lemma 8.5. To show the state ψ is tracial on $\pi'(\mathscr{U}(1))$ note the linear mapping defined by

$$\tau(w) = \psi^*\pi(w)\psi \tag{8.25}$$

vanishes on $\mathfrak{L}(\text{synch}\,\mathcal{B})$ (and hence $\mathfrak{R}(\text{synch}\,\mathcal{B})$) by Item (ii) and so τ is tracial on $\mathscr{U}(1)$ by Lemma 8.6.

We prove Item (iii) $\Rightarrow$ Item (i). Using π', ψ we define the positive linear functional

$$\ell' : \mathscr{U}(1) \to \mathbb{C}, \quad f \mapsto \psi^*\pi'(f)\psi.$$

Next extend ℓ' to a linear functional ℓ on $\mathscr{U}$ by mapping a monomial

$$w(e(1))u(e(2)) \mapsto \ell\big(w(e(1))u(e(1))^*\big).$$

It is obvious that ℓ is symmetric in the sense that $\ell(f^*) = \ell(f)^*$ for all $f \in \mathscr{U}(1)$. To check that ℓ is positive, let $f = \sum_{i,j} \beta_{ij} w_i(e(1))u_j(e(2)) \in \mathscr{U}$. Then

$$f^*f = \sum_{i,j}\sum_{k,l} \beta_{ij}^*\beta_{kl} w_i(e(1))^*w_k(e(1))u_j(e(2))^*u_l(e(2)),$$

whence

$$\ell(f^*f) = \sum_{i,j}\sum_{k,l} \beta_{ij}^*\beta_{kl}\ell'(w_i(e(1))^*w_k(e(1))u_l(e(1))^*u_j(e(1))). \tag{8.26}$$

Set

$$\check{f} = \sum_{i,j} \beta_{ij}w_i(e(1))u_j(e(1))^* \in \mathscr{U}(1).$$

Then

$$\check{f}^*\check{f} = \sum_{i,j}\sum_{k,l} \beta_{ij}^*\beta_{kl}u_j(e(1))w_i(e(1))^*w_k(e(1))u_l(e(1))^*,$$

and

$$\ell'(\check{f}^*\check{f}) = \sum_{i,j}\sum_{k,l} \beta_{ij}^*\beta_{kl}\ell'(u_j(e(1))w_i(e(1))^*w_k(e(1))u_l(e(1))^*). \tag{8.27}$$

Since ℓ' is tracial,

$$\ell'(u_j(e(1))w_i(e(1))^*w_k(e(1))u_l(e(1))^*) = \ell'(w_i(e(1))^*w_k(e(1))u_l(e(1))^*u_j(e(1))).$$

This implies the values in Equation (8.26) and Equation (8.27) are the same, so

$$\ell(f^*f) = \ell'(\check{f}^*\check{f}) \geq 0.$$

It remains to show that $\ell(\mathfrak{L}(\mathcal{N})) = \{0\}$. Elements in $\mathfrak{L}(\mathcal{N})$ are linear combinations of monomials of the form

$$w(e(1))u(e(2))e(1)_a^i e(2)_b^j = w(e(1))e(1)_a^i u(e(2))e(2)_b^j \tag{8.28}$$

with $((i,j),(a,b)) \in \mathcal{N}$. Applying ℓ to Equation (8.28) gives

$$\ell(w(e(1))e(1)_a^i u(e(2))e(2)_b^j) = \ell'(w(e(1))e(1)_a^i e(1)_b^j u(e(1))^*)$$

But $e(1)_a^i e(1)_b^j \in \mathcal{N}$, whence $w(e(1))e(1)_a^i e(1)_b^j u(e(1))^* \in \mathfrak{I}(\operatorname{synch}\mathcal{B}(1))$, so

$$\ell'(w(e(1))e(1)_a^i e(1)_b^j u(e(1))^*) = 0,$$

as desired. We have proved that $\ell(-1) = -1$ and $\ell(\operatorname{SOS}_{\mathscr{U}} + \mathfrak{L}(\mathcal{N}) + \mathfrak{L}(\mathcal{N})^*) \subseteq \mathbb{R}_{\geq 0}$, whence $-1 \notin \operatorname{SOS}_{\mathscr{U}} + \mathfrak{L}(\mathcal{N}) + \mathfrak{L}(\mathcal{N})^*$. Then Theorem 4.3 implies Item (i).

We next show Item (iii) $\Rightarrow$ Item (iv). Define the Hilbert space $\check{\mathcal{H}} := [\pi'(\mathscr{U}(1))\psi] \subseteq \mathcal{H}$. By definition, $\pi'(\mathscr{U}(1))\check{\mathcal{H}} \subseteq \check{\mathcal{H}}$, so π' induces a $*$-representation $\check{\pi}' : \mathscr{U}(1) \to \mathcal{B}(\check{\mathcal{H}})$. By construction, $\check{\pi}'(\mathfrak{I}(\operatorname{synch}\mathcal{B}(1))) = \{0\}$, as desired in Item (iv).

Finally, to go from Item (iv) to Item (iii), start with the tracial von Neumann algebra $\mathcal{W}$ with trace τ as in Item (iv) and perform a GNS construction. There is a Hilbert space $\mathcal{K}$, unit vector $\xi \in \mathcal{K}$, and a $*$-representation $\pi'' : \mathcal{W} \to \mathcal{B}(\mathcal{K})$ so that

$$\tau(a) = \langle \pi''(a)\xi, \xi \rangle, \quad a \in \mathcal{W}.$$

Since τ is a trace, ξ is a tracial state for $\pi''(\mathcal{W})$. Then the $*$-representation $\pi'' \circ \pi' : \mathscr{U}(1) \to \mathcal{B}(\mathcal{K})$ together with $\xi \in \mathcal{K}$ satisfy Item (iii).

$\square$

8.2 Tracial Nullstellensatz

Now we discuss a Nullstellensatz suited to synchronous games by virtue of handling traces. The earliest tracial Positivstellensatz is in [KS08], done in the context of the Connes' embedding conjecture. An exposition of this and the (dual) tracial moment problem is the book [BKP16, Chapter 5] with more extensive results along the lines of the theorem below, for example in [KP16, Proposition 4.2 and later] and more moment theory in [BK12]. Moments with with informative quantum games situations are also in the recent paper [Rus21].

Suppose $\mathcal{A}$ is a $*$-algebra. The **commutator** of $a, b \in \mathcal{A}$ is

$$[a, b] := ab - ba,$$

and we call a, b **cyclically equivalent**, $a \overset{\text{cyc}}{\sim} b$, if $a - b$ is a sum of commutators. Define

$$\widetilde{\text{SOS}} := \{a \in \mathcal{A} \mid \exists b \in \text{SOS} : a \overset{\text{cyc}}{\sim} b\}.$$

Elements of $\widetilde{\text{SOS}}$ are trace positive under all $*$-representations of $\mathcal{A}$ in tracial von Neumann algebra.

Theorem 8.7. *Suppose*

(1) $\mathcal{A}$ *is a $*$-algebra, where* $\widetilde{\text{SOS}}$ *is* **archimedean** *in the sense that for every* $a \in \mathcal{A}$ *there is* $\eta \in \mathbb{N}$ *with* $\eta - a^*a \in \widetilde{\text{SOS}}$*;*

(2) $\mathfrak{L} \subseteq \mathcal{A}$ *is a left ideal.*

Then the following are equivalent:

(i) *there exist a $*$-representation* $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ *and tracial state* $0 \neq \psi \in \mathcal{H}$ *satisfying*

$$\pi(f)\psi = 0 \tag{8.29}$$

for all $f \in \mathfrak{L}$*;*

(ii) *there exist a $*$-representation* $\pi : \mathcal{A} \to \mathcal{F}$ *into a tracial von Neumann algebra* $(\mathcal{F}, \tau)$ *satisfying*

$$\tau(\pi(f)) = 0 \tag{8.30}$$

for all $f \in \mathfrak{L}$*;*

(iii) $-1 \notin \widetilde{\text{SOS}} + \mathfrak{L} + \mathfrak{L}^*$.

Proof. The equivalence of Items (i) and (ii) is established via the GNS representation as in the proof of Theorem 8.3. The implication (ii) $\Rightarrow$ (iii) is easy. Namely, if $-1 \in \widetilde{\text{SOS}} + \mathfrak{L} + \mathfrak{L}^*$, and $(\mathcal{F}, \tau)$ as in (ii) exist, then

$$-1 = \tau(-1) \in \tau(\widetilde{\text{SOS}} + \mathfrak{L} + \mathfrak{L}^*) = \tau(\widetilde{\text{SOS}}) + \tau(\mathfrak{L}) + \tau(\mathfrak{L})^* = \tau(\widetilde{\text{SOS}}) \subseteq \mathbb{R}_{\geq 0},$$

a contradiction.

For the harder side (iii) $\Rightarrow$ (ii) we only give a sketch since it is very similar to that in the proof of Theorem 4.3. Suppose $-1 \notin \widetilde{\text{SOS}} + \mathfrak{L} + \mathfrak{L}^*$. By the Hahn-Banach theorem (version due to Eidelheit-Kakutani) there is a linear functional $L : \mathcal{A} \to \mathbb{C}$ satisfying

$$L(1) = 1, \qquad L(\widetilde{\text{SOS}} + \mathfrak{L} + \mathfrak{L}^*) \subseteq \mathbb{R}_{\geq 0}. \tag{8.31}$$

Since $\mathfrak{L}$ is a subspace, the second property of Equation (8.31) implies $L(\mathfrak{L}) = \{0\}$. Likewise, $\widetilde{\text{SOS}}$ contains all commutators and $L(\widetilde{\text{SOS}}) \subseteq \mathbb{R}_{\geq 0}$, whence $L(f) \geq 0$ for any $f \in \text{SOS}_\mathcal{A}$ and L is tracial. Further, $L(f)^* = L(f^*)$ for all $f \in \mathcal{A}$. Then the GNS construction yields the desired conclusion. $\square$

8.3 Quantum graph coloring

As an example of how one can use Theorem 8.3 we look at quantum coloring of graphs. It is often formulated as a synchronous game. We start by recalling the coloring setup then we illustrate a general approach through an example.

Given a graph $G = (V, E)$, where V is the set of vertices and $E \subseteq V \times V$ its edges, we say G admits a **quantum c-coloring** [PSS$^+$16], if to each vertex $i \in V$ one can assign projections e_a^i, $a \in \{1, \ldots, c\}$ so that

$$\sum_a e_a^i = 1, \tag{8.32}$$

and for each edge $(i, j) \in E$, we have

$$e_a^i e_a^j = 0, \quad \forall a. \tag{8.33}$$

In algebraic terms, G admits a quantum c-coloring if the the universal game algebra $\mathscr{U}(1)$ generated by $e(1)_a^i := e_a^i$, where i indexes the vertices and $a \in \{1, \ldots, c\}$ admit a $*$-representation π that vanishes on the polynomials $e_a^i e_a^j$ from Equation (8.33).

8.3.1 Quantum graph coloring as a synchronous game

We shall be brief here and refer to [PSS$^+$16, Section 2] for a thorough discussion of graph coloring and the connection to synchronous games.

A game is specified by a graph G. The verifier's questions amount to giving vertex i to Alice and vertex j to Bob; a perfect strategy consists of a vector ψ and k projectors $e(1)_{\tilde{a}}^i$ for Alice and $e(2)_{\tilde{b}}^i$ for Bob meeting the (universal game) constraints of Equation (3.7) and $e(1)_a^i e(2)_a^j = 0$ if vertices i and j are joined by an edge. These give the probability of Alice and Bob answering question (i, j) with colors $a, b \in 1, \ldots, c$ via the formula

$$p(a, b|i, j) := \psi^* e(1)_a^i e(2)_b^j \psi.$$

A synchronous strategy means for i any vertex, $p(a, b|i, i) = 0$ if $a \neq b$. This is equivalent to $e(1)_a^i \psi = e(2)_a^i \psi$ for $a = 1, \ldots, c$. Theorem 8.3 now converts solving this system of equations to the finding tracial representations of $\mathscr{U}(1)$ vanishing on synch $\mathcal{B}(1)$. In our forthcoming example, we show there are no representations much less tracial ones, so no 4-coloring exists.

8.3.2 Example

Consider the graph $G = (V, E)$ given in Figure 1. It is obtained from a five cycle by adding two apexes (denoted 6 and 7 in the figure), i.e., two vertices connected to all the other vertices.
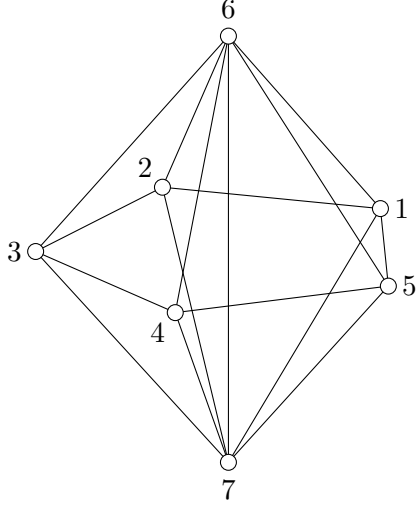
Figure 1: Pentagonal bipyramid

Observe that the chromatic number of G is five, so G does admit a quantum five coloring. We claim that G does not admit a quantum four coloring. For this we apply our Nullstellensatz Theorem 4.3 to the quantum 4-coloring Equations (8.32) and (8.33).

Generate the ideal

$$\mathfrak{I}_1 = (e_a^i e_a^j \mid (i,j) \in E, \ a \in \{1,\ldots,4\}) \subseteq \mathscr{U}(1). \tag{8.34}$$

By Corollary 4.5, the graph G admits a quantum 4-coloring iff

$$-1 \notin \mathrm{SOS}_{\mathscr{U}(1)} + \mathfrak{I}_1. \tag{8.35}$$

We show there are quadratic elements s_j in $\mathscr{U}(1)$ so that

$$1 + \sum s_j^* s_j \in \mathfrak{I}_1. \tag{8.36}$$

To search for these elements s_j we employ NC Gröbner basis combined with semidefinite programming.

Firstly, we lift our problem into the free algebra $\mathbb{C}\langle e \rangle$, where e denotes the tuple $e = (e_a^i)$. For this let $\Pi : \mathbb{C}\langle e \rangle \to \mathscr{U}(1)$ denote the canonical epimorphism, and let $\mathfrak{I} = \Pi^{-1}(\mathfrak{I}_1)$. Next one computes a GB for $\mathfrak{I}$; with respect to a lex order it has 350 elements of degree ≤ 3.

To search for nc polynomials s_j of degree d so that

$$1 + \sum s_j^* s_j \in \mathfrak{I}, \tag{8.37}$$

one employs the Gram matrix method and semidefinite programming [BKP16]. That is, letting W_d be the set of all monomials of degree $\leq d$ in $\mathbb{C}\langle e \rangle$ (listed w.r.t. some ordering), Equation (8.37) is equivalent to the existence of a positive semidefinite matrix M so that

$$1 + W_d^* M W_d \in \mathfrak{I}. \tag{8.38}$$

Since ideal membership can be described using linear equations in terms of the entries of M (given a Gröbner basis), Equation (8.38) immediately transforms into a semidefinite program (SDP).

In our example, Equation (8.38) is infeasible for $d = 1$ and does have a solution for $d = 2$. Reducing W_d modulo the GB (which one can do without loss of generality to help reduce the size of the SDP) yields an SDP of size 272×272. Observing that $W_d^* M W_d = \text{tr}(M W_d W_d^*)$ and reducing entries of $W_d W_d^*$ modulo the GB, Equation (8.38) converts into a set of linear equations on the entries of M which are sparse and can thus be efficiently solved. We are then left with an SDP of manageable size. Solving the SDP using a standard solver with trivial objective function yielded a floating point positive definite solution M with minimal eigenvalue of $\approx 10^{-2}$. By choosing a fine enough rationalization [PP08, CKP15] we thus obtain a symbolic (i.e., in exact arithmetic) positive definite solution M of Equation (8.38), establishing that G does not admit a quantum 4-coloring.

References

[Bar02]   Alexander Barvinok. *A course in convexity*, volume 54 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002. [p. 22]

[BK12]   Sabine Burgdorf and Igor Klep. The truncated tracial moment problem. *J. Operator Theory*, 68(1):141–163, 2012. [p. 48]

[BKP16]   Sabine Burgdorf, Igor Klep, and Janez Povh. *Optimization of polynomials in non-commuting variables*. SpringerBriefs in Mathematics. Springer, [Cham], 2016. [pp. 43, 48, 50]

[CHK⁺14]   Jakob Cimpric, J. William Helton, Igor Klep, Scott McCullough, and Christopher Nelson. On real one-sided ideals in a free algebra. *J. Pure Appl. Algebra*, 218(2):269–284, 2014. [p. 20]

[CHMN13]   Jakob Cimpric, J. William Helton, Scott McCullough, and Christopher Nelson. A non-commutative real Nullstellensatz corresponds to a noncommutative real ideal: algorithms. *Proc. Lond. Math. Soc.*, 3(5):1060–1086, 2013. [pp. 20, 21]

[CKP15]   Kristijan Cafuta, Igor Klep, and Janez Povh. Rational sums of Hermitian squares of free noncommutative polynomials. *Ars Math. Contemp.*, 9(2):243–259, 2015. [Paging previously given as 253–269]. [p. 51]

[CLO15]   David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. [p. 33]

[CLS17]   Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *J. Math. Phys.*, 58(1):012202, 2017. [pp. 3, 4, 5, 32, 36, 37]

[CMMN20]   David Cui, Arthur Mehta, Hamoon Mousavi, and Seyed Sajjad Nezhadi. A generalization of CHSH and the algebraic structure of optimal strategies. *Quantum*, 4:346, 2020. [p. 36]

[DLTW08]   Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *2008 23rd Annual IEEE Conference on Computational Complexity*, pages 199–210. IEEE, 2008. [pp. 2, 36]

[Fri12]   Tobias Fritz. Tsirelson's problem and Kirchberg's conjecture. *Rev. Math. Phys.*, 24(5):1250012, 67, 2012. [p. 7]

[Gol21]   Adina Goldberg. Synchronous linear constraint system games. *J. Math. Phys.*, 62(3):032201, 2021. [pp. 4, 5]

[Gre00]   Edward L. Green. Multiplicative bases, Gröbner bases, and right Gröbner bases. *J. Symbolic Comput.*, 29(4-5):601–623, 2000. [p. 33]

[HM04]   J. William Helton and Scott McCullough. A Positivstellensatz for noncommutative polynomials. *Trans. Amer. Math. Soc.*, 356(9):3721– 3737, 2004. [pp. 2, 36]

[HMPS17]   J. William Helton, Kyle P. Meyer, Vern I. Paulsen, and Matthew Satriano. Algebras, synchronous games and chromatic numbers of graphs. *Preprint*, 2017. https://arxiv.org/abs/1703.00960. [pp. 3, 4, 5, 43]

[JNP+11]   Marius Junge, Miguel Navascués, Carlos Palazuelos, David Perez-Garcia, Volkher B. Scholz, and Reinhard F. Werner. Connes embedding problem and Tsirelson's problem. *J. Math. Phys.*, 52(1):012102, 12, 2011. [p. 7]

[JNV+20]   Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE. *Preprint*, 2020. https://arxiv.org/abs/2001.04383. [p. 7]

[KP16]   Igor Klep and Janez Povh. Constrained trace-optimization of polynomials in freely noncommuting variables. *J. Global Optim.*, 64(2):325–348, 2016. [pp. 43, 48]

[KPS18]   Se-Jin Kim, Vern Paulsen, and Christopher Schafhauser. A synchronous game for binary constraint systems. *J. Math. Phys.*, 59(3):032201, 2018. [pp. 3, 5, 43]

[KS08]   Igor Klep and Markus Schweighofer. Connes' embedding conjecture and sums of Hermitian squares. *Adv. Math.*, 217(4):1816–1837, 2008. [pp. 43, 48]

[LMP+20]   Martino Lupini, Laura Mančinska, Vern I Paulsen, David E Roberson, Giannicola Scarpa, Simone Severini, Ivan G Todorov, and Andreas Winter. Perfect strategies for non-local games. *Mathematical Physics, Analysis and Geometry*, 23(1):1–31, 2020. [pp. 3, 5]

[Mor86]   Ferdinando Mora. Groebner bases for noncommutative polynomial rings. In *Algebraic algorithms and error correcting codes (Grenoble, 1985)*, volume 229 of *Lecture Notes in Comput. Sci.*, pages 353–362. Springer, Berlin, 1986. [pp. 33, 34]

[MR98]   Klaus Madlener and Birgit Reinert. String rewriting and Groebner bases – a general approach to monoid and group rings. *Technical report Zentrum Fur Computeralgebra Technische Universität Kaiserslautern*, page 55, May 1998. [p. 34]

[NPA08]   Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.*, 10(7):073013, 2008. [pp. 2, 36]

[PP08]   Helfried Peyrl and Pablo A. Parrilo. Computing sum of squares decompositions with rational coefficients. *Theoret. Comput. Sci.*, 409(2):269–281, 2008. [p. 51]

[PSS⁺16] Vern I. Paulsen, Simone Severini, Daniel Stahlke, Ivan G Todorov, and Andreas Winter. Estimating quantum chromatic numbers. *J. Funct. Anal.*, 270(6):2188–2222, 2016. [pp. 3, 43, 44, 49]

[Rus21] Travis B. Russel. A synchronous NPA hierarchy with applications. *Preprint*, 2021. https://arxiv.org/abs/2105.01555. [p. 48]

[Slo20] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *J. Amer. Math. Soc.*, 33(1):1–56, 2020. [p. 5]

[SS13] Yurii Savchuk and Konrad Schmüdgen. Unbounded induced representations of *-algebras. *Algebr. Represent. Theory*, 16(2):309–376, 2013. [p. 28]

[SW08] Volkher B. Scholz and Reinhard F. Werner. Tsirelson's problem. *Preprint*, 2008. https://arxiv.org/abs/0812.4305. [p. 7]

[Vid59] Ivan Vidav. On some *regular rings. *Acad. Serbe Sci. Publ. Inst. Math.*, 13:73–80, 1959. [p. 23]

[WH20] Adam Bene Watts and J. William Helton. 3XOR games with perfect commuting operator strategies have perfect tensor product strategies and are decidable in polynomial time. *Preprint*, 2020. https://arxiv.org/abs/2010.16290. [pp. 3, 4, 32]

[Xiu12] Xingqiang Xiu. *Non-commutative Gröbner bases and applications*. PhD thesis, 2012. [p. 34]

Contents

Index

Table of Notation

$\mathbb{C}\langle x \rangle$	free algebra on x + variants.
$\mathfrak{I}$	capital gothic letters for two-sided ideals AND
$\mathfrak{I}(generators)_{algebra}$	to be explicit in terms of gens/algebra
$\mathfrak{L}, \mathfrak{R}$	capital gothic letters for left/right ideals AND
$\mathfrak{L}(generators)_{algebra}$	to be explicit in terms of gens/algebra
$\mathcal{E}(\alpha)$	The set of projectors used by player α in a nonlocal game.
$E(\alpha)^i_a$	The projector in a nonlocal game strategy corresponding to player α giving a response a to question i.
$e(\alpha)^i_a$	Formal variables satisfying the same relations as $E(\alpha)^i_a$
$X(\alpha)^i_a$	The signature matrix $2E(\alpha)^i_a - 1$.
$x(\alpha)^i_a$	The formal variable in $\mathscr{U}$ corresponding to $X(\alpha)^i_a$.
$\mathscr{U}$	The universal game algebra formed by the $e(\alpha)^i_a$
$\mathscr{I}$	universal game ideal
$\mathcal{A}$, etc.	C^*-algebras
$\mathbb{E}$	conditional expectation
$\mathrm{Alg}_{\mathcal{A}}(blah)$	subalgebra of $\mathcal{A}$ generated by $blah$
$\mathrm{Alg}^*_{\mathcal{A}}(blah)$	$*$-subalgebra of $\mathcal{A}$ generated by $blah$
$\mathcal{A}^{-1}$	invertible elements in an algebra $\mathcal{A}$
$\mathcal{Y}(\vec{i})$	Set of answers corresponding to "valid responses" to question $\vec{i}$.
$\mathcal{N}(\vec{i})$	Set of answers corresponding to "invalid responses" to question $\vec{i}$
$\mathcal{Y}$	Set of elements $e(\alpha)^i_a$ corresponding to "valid responses - 1".
$\mathcal{N}$	Set of elements $e(\alpha)^i_a$ corresponding to "invalid responses".

Table 1: Table of Notation