SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

From Non-Local Games to Embeddings of Groups: Resolving Tsirelson's Problem

av

Emilia Dunfelt

2023 - M4

From Non-Local Games to Embeddings of Groups: Resolving Tsirelson's Problem

Emilia Dunfelt

Självständigt arbete i matematik 30 högskolepoäng, avancerad nivå

Handledare: Sven Raum

2023

Abstract

By considering whether the correlations arising from a two-player non-local game with measurements in a Hilbert space of the form $\mathcal{H}_A \otimes \mathcal{H}_B$ are the same as the correlations arising with commuting measurements in a Hilbert space $\mathcal{H}$, a Tsirelson problem is obtained. Due to recent results in this direction, all Tsirelson problems can now be considered to be resolved in the negative. William Sloftstra gave the first proof towards this resolution in [18]. The following text aims to present the theory of non-local games, correlation sets, and, most importantly, a proof of the Tsirelson problem originally given by Slofstra as well as a proof of the Tsirelson problem arising by considering finite-dimensional Hilbert spaces.

Acknowledgments

First and foremost, I would like to thank my supervisor, Sven Raum, for an abundance of good advice, immense patience, and many fruitful conversations along the way – be it online or by the whiteboard. Most of all, I am thankful for being introduced to this fascinating topic that will undoubtedly stay with me for many years to come. Finally, I extend much gratitude to my family for their endless support and motivation in the work on this thesis.

Table of contents

1. Introduction

The phenomenon known as quantum entanglement – when two or more particles, or quantum systems, are correlated in such a way that they can no longer be considered separate entities on a fundamental level – is arguably the most fascinating and valuable property of quantum mechanics, and by extension of quantum information theory. As intensive research in quantum mechanics and quantum information theory has revealed, this phenomenon stands unmatched in the classical counterpart of these fields.

In 1935, physicists Albert Einstein, Boris Podolsky, and Nathan Rosen [10] published a paper critiquing the implications of entanglement on physical reality. The phenomenon implied that quantum mechanics could exhibit *non-locality* in the sense that the actions of an observer of a system could produce instantaneous changes in physical properties over a massive distance. However, in 1964, John Bell suggested an experiment [2] that promised to settle the long-standing scientific debate: By entangling two particles, separating them spatially, measuring their properties, and then comparing the observed result to a statistical bound on the probabilities as predicted by quantum mechanics compared to classical mechanics, it would be possible to demonstrate non-locality in action. Not long after, several scientists conducted the first practical experiments verifying Bell's theoretical claims, experiments which were recently awarded the Nobel Prize in Physics in 2022 [23].

So-called *non-local games* can be used to model Bell experiments and is a valuable construct to study non-locality. These information-theoretical "games" take place between two or more players and a verifier. Each player receives a question from the verifier and then responds with an answer. If the question- and answer pairs satisfy a predefined criterion, the verifier concludes that the players win the game. The "catch" in this scenario is that the players cannot communicate once the verifier has distributed the questions. They are thus limited to deciding on a clever strategy before the game starts, based only on their knowledge of the game's rules. The players can share an entangled state in the quantum information theoretical scenario, and their strategy entails choosing a set of measurement operators. As Bell showed, non-local games exist such that the best quantum strategy results in a greater winning probability than any classical strategy.

In the context of a quantum non-local game, we can mathematically model the systems involved in several ways. The traditionally dominating model is the so-called *tensor-product model*, in which we consider each player's measurements to be operators on separate Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ in the context of a two-player non-local game. The entangled quantum state is then a state in the space given by $\mathcal{H}_A \otimes \mathcal{H}_B$. An alternative model is the

commuting-operator model in which we instead allow the players to pick measurement operators in a single Hilbert space $\mathcal{H}$, but in such a way that their operators are commuting.

As we will see, considering finite-dimensional Hilbert spaces, these two models are equivalent in that there are strategies in either model producing the same winning probabilities for any non-local game. A long-standing problem in quantum information theory is *Tsirelson's problem* which, in essence, asks if this is true also for infinite-dimensional Hilbert spaces. Perhaps surprisingly, although both models describe a quantum theoretical scenario in which the players share an entangled state, it was shown in [18] by William Slofstra that there are non-local games that can be played perfectly – i.e., with a winning probability of 1 – using a commuting-operator strategy but not with any tensor-product strategy. In this essay, we will concern ourselves with the proof of this statement.

Currently, this result lies purely in the realm of the theoretical. Similar to the early result by Bell, which suggested a separation between results achievable through classical strategies and those achievable through entangled strategies, our result suggests a separation of different quantum strategies. At the time of writing, this result is still awaiting the day of experimental verification. However, the theory of non-local games is still intensively studied and is seeing significant use in areas such as quantum key distribution and the development of cryptosystems capable of achieving perfect secrecy [1,11].

The main result considered in this text is thus the *embedding theorem* of [18] (Theorem 4.6), the proof of which we will ultimately reach in Section 6, where we also provide some concluding remarks on the future of this problem. This text aims to give a clear overview of the fundamental constructions involved in this proof and provide some of the necessary background on Tsirelson's problem. Starting in Section 3, we present the theory of non-local games and correlation sets of different strategies. We also present a proof of the Tsirelson problem concerning finite-dimensional Hilbert spaces, giving full details to the original sketch of this statement made in [20]. Here, we rely on some basic theory of operator algebras presented in Section 2. Section 4 presents the main results of [18], and we define the type of non-local game from which we can derive the separation of the two models. Section 5 introduces the critical constructions necessary for the proof of Theorem 4.6.

A reader already familiar with the theory of non-local games may readily rely on Sections 4 to 6 for the main result, necessary constructions, and proof of the main statement. For the reader seeking the complete picture, however, starting from the beginning of Section 3 is recommended, consulting Section 2 and Appendix A on quantum computing as necessary.

2. Algebra prerequisites

The following section presents the unfamiliar reader with some fundamental concepts in the theory of C^*-algebras. After presenting the necessary definitions of the area, our first goal is to prove the structure theorem of finite-dimensional C^*-algebras, which, although this text generally does not dwell on the finite-dimensional case for long, is needed to answer the Tsirelson problem for finite-dimensional Hilbert spaces, as seen in Section 3.3. We also briefly introduce the GNS construction, based on the presentation in [17], and the notion of the universal C^*-algebra. Last, we introduce a few purely group theoretical constructions needed to prove our main result in Section 4.2, namely Theorem 4.6.

§ 2.1. General concepts. Recall that an *algebra* is a vector space $\mathcal{A}$ together with an associative bilinear multiplication map $m : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ defined by $(a, b) \mapsto ab$. A *subalgebra* is a vector subspace closed under this multiplication map. If $\mathcal{A}$ is endowed with a norm $||\cdot||$, then $\mathcal{A}$ is said to be a *normed algebra*. If $\mathcal{A}$ contains a unit, then we say that it is a *unital* algebra.

Definition 2.1. Let $\mathcal{A}$ be an algebra with a conjugate-linear map $a \mapsto a^*$ such that $a^{**} = a$ and $(ab)^* = b^*a^*$ for all $a, b \in \mathcal{A}$. Then the map is called an *involution*, and the pair $(\mathcal{A}, *)$ is called a $*$-algebra.

A subset $S \subseteq \mathcal{A}$ such that $S^* = S$ is said to be *self-adjoint*. A self-adjoint subalgebra of $\mathcal{A}$ is a $*$-*subalgebra*.

As the attentive reader has probably recognized, the involution $*$ can be seen as a generalization of taking the adjoint of a matrix in a matrix algebra such as $M_n(\mathbb{C})$. Thus, this can be considered our canonical example of a $*$-algebra. Another familiar example is $\mathbb{C}$ with complex conjugation. Often, we will simply consider the set of bounded linear operators on a Hilbert space $\mathcal{H}$, denoted by $\mathcal{B}(\mathcal{H})$, with the involution $A \mapsto A^*$.

We now define a few basic properties of elements of $*$-algebras:

Definition 2.2. Let $\mathcal{A}$ be a $*$-algebra, and let $a \in \mathcal{A}$. The element a is said to be

- *self-adjoint* if $a^* = a$,
- *normal* if $a^*a = aa^*$,
- a *projection* if $a = a^* = a^2$, and
- *unitary* if $a^*a = aa^* = 1$.

A projection p in a finite-dimensional C^*-algebra $\mathcal{A}$ is said to be *minimal* if $p\mathcal{A}p = \mathbb{C}p$.

Note that by this definition, a projection is necessarily also self-adjoint, and a

unitary is also normal. These are all properties that we easily recognize in elements of our previously mentioned examples of $*$-algebras.

Definition 2.3. Let $\varphi : \mathcal{A} \to \mathcal{B}$ be a homomorphism of $*$-algebras such that $\varphi(a^*) = \varphi(a)^*$. Then, φ is said to be a $*$-*homomorphism*. If it is bijective, it is said to be a $*$-*isomorphism*.

In the general field of quantum mechanics and the mathematical modeling of such systems, the concept of C^*-algebras is instrumental. In Appendix A, we give the standard description of quantum computing and quantum mechanics in terms of Hilbert spaces, unit vectors, and unitary operators. However, there is an equivalent formulation of the same concepts in terms of C^*-algebras, pure states, and self-adjoint elements, respectively.

We spend the remainder of this section exploring these concepts in greater detail.

Definition 2.4. Let $\mathcal{A}$ be a $*$-algebra with a complete sub-multiplicative norm such that $||a^*|| = ||a||$ and

$$||a^* a|| = ||a||^2 \tag{2.1.1}$$

for all $a \in \mathcal{A}$. Then $\mathcal{A}$ is said to be a C^*-*algebra*, and the property (2.1.1) is called the C^*-*identity*.

All of our previous examples of $*$-algebras are in fact also C^*-algebras, with the usual norms.

Definition 2.5. Let φ be a linear functional on a C^*-algebra $\mathcal{A}$. Then φ is said to be *positive* if $\varphi(a) \geq 0$ for all positive $a \in \mathcal{A}$, i.e., all $a \in \mathcal{A}$ such that $a = bb^*$ for some $b \in \mathcal{A}$

Definition 2.6. Let $\mathcal{A}$ be a C^*-algebra. A *state* on is $\mathcal{A}$ positive linear functional on $\mathcal{A}$ of norm one. The set of states on $\mathcal{A}$ is denoted by $\mathcal{S}(\mathcal{A}) \subseteq \mathcal{A}^*$, and is called the *state space* of $\mathcal{A}$.

A state φ on $\mathcal{A}$ is said to be *pure* if for every positive linear functional ρ on $\mathcal{A}$ such that $\rho \leq \varphi$, there exists a number $0 \leq t \leq 1$ such that $\rho = t\varphi$.

By Corollary 3.3.4 of [17], we note that a necessary and sufficient criterion for a linear functional φ of norm at most 1 to be a state is the property $\varphi(1) = 1$.

Importantly, it is possible to show (Proposition 2.9) that the state space of a unital C^*-algebra is compact. However, this statement does not yet make sense as we have no topology on the space of linear functionals of a C^*-algebra. Therefore, we now introduce the so-called weak-$*$ topology, which can be defined more generally for the dual space of any normed vector space:

Definition 2.7. Let X be a normed vector space with dual X^*. The *weak-$*$ topology* of X^* is the topology generated by the family of seminorms $\{p_x \mid x \in X\}$, where $p_x(x^*) = |x^*(x)|$.

That $p_x(x^*) = |x^*(x)|$ describes a seminorm on X^* for any $x \in X$ is clear by the familiar properties of $|\cdot|$. We also note that the weak-$*$ topology is the coarsest topology on X^* for which $x^* \mapsto x^*(x)$ is continuous for all $x \in X$. Indeed, $x^* \mapsto x^*(x)$ is continuous in the weak-$*$ topology by Theorem A.1 of [17]. So if $\mathcal{T}$ is a topology on X^* such that $x^* \mapsto x^*(x)$ is continuous for all x, then since $|\cdot|$ is a continuous map on the underlying scalar field, the maps $x^* \mapsto |x^*(x)| = p_x(x^*)$ are continuous for all x. So the weak-$*$ topology is coarser than $\mathcal{T}$.

Before stating and proving the compactness of $\mathcal{S}(\mathcal{A})$ for unital C^*-algebras, we first consider the following important result from functional analysis, the proof of which we here omit but can be found in [8], Chapter 4.3.

Theorem 2.8 (Banach-Alaoglu theorem)**.** *Let X be a normed vector space with dual X^*. The closed unit ball in X^* is weak-$*$ compact.*

Proposition 2.9. *Let $\mathcal{A}$ be a unital C^*-algebra. The state space $\mathcal{S}(\mathcal{A})$ is weak-$*$ compact.*

Proof. We note that any state $\varphi \in \mathcal{S}(\mathcal{A})$ has norm 1, so in particular, the state space is a subset of the closed unit ball of $\mathcal{A}^*$. Furthermore, since the condition $\varphi(1_{\mathcal{A}}) = 1$ characterizes states among the elements of this unit ball, we conclude by the Banach-Alaoglu theorem that $\mathcal{S}(\mathcal{A})$ is weak-$*$ closed as it is a closed subset of a compact space. ∎

We let the proof of this result conclude our section on basic results and definitions in the theory of C^*-algebras and move on to discuss the structure of finite-dimensional C^*-algebras, as promised.

§ 2.2. Structure of finite-dimensional C^*-algebras. This section aims to show the structure theorem of finite-dimensional C^*-algebras. Recalling that $M_n(\mathbb{C})$ is a C^*-algebra, we will show that for every every finite-dimensional C^*-algebra, there exists a decomposition into a direct sum of such matrix algebras. Before giving an overview of the steps included in this proof, we first need to state a few additional definitions:

Definition 2.10. An *ideal* I of a C^*-algebra $\mathcal{A}$ is a vector subspace of $\mathcal{A}$ such that if $a \in \mathcal{A}$ and $b \in I$ then $ab \in I$ and $ba \in I$. The ideal I is said to be *self-adjoint* in $\mathcal{A}$ if it is closed under the $*$-operation, i.e., $a^* \in I$ whenever $a \in I$. An ideal is said to be *closed* if it is closed in the topology induced by the norm on $\mathcal{A}$.

By Theorem 3.1.3 in [17], we note that a closed ideal is also self-adjoint. We say that a C^*-algebra is *simple* if it has no non-trivial closed ideals.

The first step towards proving the structure theorem is to show that there is a decomposition of a finite-dimensional C^*-algebra into simple C^*-algebras. Then, by showing that $M_n(\mathbb{C})$ is simple and that any finite-dimensional simple C^*-algebra is isomorphic to $M_n(\mathbb{C})$ the structure theorem will easily follow.

This promised decomposition of a finite-dimensional C^*-algebra is given by the *center* of the C^*-algebra in question, which we define next.

Definition 2.11. For a subset $A \subseteq \mathcal{A}$ of a C^*-algebra $\mathcal{A}$, the *commutant* A' of A is the set of elements of $\mathcal{A}$ which commute with all elements of A.

We note that the commutant depends on the larger space around $\mathcal{A}$, usually seen as a subspace of some $\mathcal{B}(\mathcal{H})$. However, in the following definition, we do not need to consider this fact.

Definition 2.12. The *center*, $Z(\mathcal{A})$, of a C^*-algebra $\mathcal{A}$ is defined as the set of elements of $\mathcal{A}$ which commute with all other elements in $\mathcal{A}$.

Note that $\mathcal{A}' \cap \mathcal{A} = Z(\mathcal{A})$.

Before we proceed to show how the center of a finite-dimensional C^*-algebra yields a decomposition into simple C^*-algebras, we first need to prove the following lemma:

Lemma 2.13. *Let $\mathcal{A}$ be a finite dimensional C^*-algebra, then $\mathcal{A}$ has a unit.*

Proof. Let $a \in \mathcal{A}$ be a non-zero, self-adjoint element. Then by the spectral theorem, there exist a projection $p \in \mathcal{A}$ such that $pa = a$ and p is a polynomial in a. If $pb = b$ for all $b \in \mathcal{A}$ we have found a unit since

$$bp = (b^*p^*)^* = ((pb)^*)^* = b.$$

So let $b \in \mathcal{A}$ be such that $pb \neq b$ and consider the non-zero, self-adjoint element given by $(pb - b)(pb - b)^*$. Again, there is a projection $q \in \mathcal{A}$ corresponding to this self-adjoint element, as p does to a above.

Since $p(pb - b) = 0$ it follows that $pq = 0$, so $p + q$ is a projection. Then, $(p+q)a = (p+q)pa = a$ and $(p+q)q = q$. Hence, the kernel of $a \mapsto (p+q)a - a$ is strictly larger than the kernel of $a \mapsto pa$. Since $\mathcal{A}$ is finite-dimensional, the result follows by induction. ∎

Proposition 2.14. *The center of a finite-dimensional C^*-algebra $\mathcal{A}$ results in a decomposition*

$$\mathcal{A} = \sum_{i=1}^{k} z_i \mathcal{A}$$

of $\mathcal{A}$ into simple C^*-algebras $z_i\mathcal{A}$.

Proof. Let I be a non-zero ideal of $\mathcal{A}$. Since $\mathcal{A}$ is finite-dimensional, so is I, and by Lemma 2.13 has a unit 1_I. Since unitary conjugation is an automorphism, for all unitary elements $u \in \mathcal{A}$, it holds that $u1_Iu^* = 1_I$. As $\mathcal{A}$ is spanned by unitary elements, it follows that 1_I is a non-zero central projection in $\mathcal{A}$, and $1_I \neq 1_\mathcal{A}$. Let $z_1 := 1_I$, so by induction on the dimension of $\mathcal{A}$ we obtain a sequence of central projections $z_1, \dots, z_k$ such that $\sum_{i=1}^k z_i = 1$.

For each $i \in \{1, \dots, k\}$ since the center of $z_i\mathcal{A}$ is trivial, i.e. $Z(z_i\mathcal{A}) = \mathbb{C}z_i$, it follows by the same reasoning as above that $z_i\mathcal{A}$ is simple, and the claim follows. ∎

We are now ready to revisit $M_n(\mathbb{C})$, and show that it is a simple C^*-algebra. In $M_n(\mathbb{C})$, we define the *matrix units* $(e_{ij})_{ij}$ to be the matrices such that e_{ij} is filled with zeroes, and has a single 1 in the ijth position. Then,

$$e_{ij}e_{kl} = \delta_{jk}e_{il}, \tag{2.2.1}$$

and

$$e_{ij}^* = e_{ji}, \tag{2.2.2}$$

for all i, j, k, l. The system of matrix units $(e_{ij})_{ij}$ can be seen to form a basis for $M_n(\mathbb{C})$. Note that multiplication of $a \in M_n(\mathbb{C})$ on the right by a matrix unit e_{ij} yields a matrix with the jth column corresponding to the ith column of a. Similarly, left multiplication of e_{ij} results in a matrix with the ith row corresponding to the jth row of a.

Proposition 2.15. *$M_n(\mathbb{C})$ is simple.*

Proof. Let I be a non-zero ideal of $M_n(\mathbb{C})$, and let $a \in I$ be an arbitrary element such that $a_{ij} \neq 0$ for some i, j. Then by our previous observations $e_{ii}ae_{jj} = a_{ij}e_{ij}$, by which it follows that $e_{ij} \in I$. Furthermore, for any $e_{kl} \in (e_{ij})_{ij}$ we have by (2.2.1) that $e_{kl} = e_{ki}e_{il} = e_{ki}e_{ij}e_{jl}$. Thus, $e_{kl} \in I$ and the ideal I must be all of $M_n(\mathbb{C})$. Thus, $M_n(\mathbb{C})$ is simple. ∎

One more lemma is necessary before we can show that simple finite-dimensional C^*-algebras have the desired structure, a result from which we can easily deduce the structure theorem by Proposition 2.14.

Lemma 2.16. *Let $\mathcal{A}$ be a finite-dimensional C^*-algebra. Then there is a finite family of minimal projections $p_1, \dots, p_k$ such that $\sum_{i=1}^k p_i = 1$.*

Proof. If $\mathcal{A}$ has dimension 1, then the statement follows immediately by considering the unit of $\mathcal{A}$.

Otherwise, there is an element $a \in \mathcal{A} \setminus \mathbb{C}1$, which is not a multiple of 1. By considering $a + a^*$ and $i(a - a^*)$, which are not both elements of $\mathbb{C}1$, we find a self-adjoint element $b \in \mathcal{A} \setminus \mathbb{C}1$. By the spectral theorem, we can write $b = \sum_{j=0}^{n} \lambda_j p_j$, for projections $p_j \in \mathcal{A}$ and scalars $\lambda_j \in \mathbb{R}$.

We claim that $p_0 \notin \{0, 1\}$. Indeed, $p_0 \neq 0$ by the definition of the spectral decomposition since $b \neq 0$. Also, $p_0 \neq 1$ as otherwise we would have that $n = 0$, since p_j is orthogonal to $p_{j'}$ for $j = j'$. Thus, p_0 is the projection we seek.

Now, either p_0 is minimal or $p_0 \mathcal{A} p_0 \neq \mathbb{C} p_0$, in which case induction on the dimension of $\mathcal{A}$ finishes the proof. We thus obtain the minimal projections $p_1, \ldots, p_k$ as desired. ∎

Proposition 2.17. *If $\mathcal{A}$ is a simple non-zero finite-dimensional C^*-algebra, it is $*$-isomorphic to a matrix algebra $M_n(\mathbb{C})$.*

Proof. Since $\mathcal{A}$ is finite-dimensional, Lemma 2.16 shows that there exist mutually commuting minimal (pairwise orthogonal) projections $p_1, \ldots, p_k \in \mathcal{A}$ such that $\sum_{i=1}^{k} p_i = 1$. Furthermore, for all i, j since p_i and p_j are non-zero, there exists $a \in \mathcal{A}$ such that $p_i a p_j \neq 0$. Otherwise, the set $A p_i A = I$, which is non-zero, would be a non-trivial ideal of $\mathcal{A}$, contradicting the simplicity of $\mathcal{A}$.

For $j \in \{1, \ldots, k\}$ let a_j be such that $p_1 a_j p_j \neq 0$ and define

$$v_{1j} = \frac{1}{\lambda_j} p_1 a_j p_j$$

where $\lambda_j = ||p_1 a_j p_j||$. Note that $0 < v_{1j} v_{1j}^* \leq p_1$. Since p_1 is minimal and

$$||v_{1j} v_{1j}^*|| = \frac{1}{\lambda_j^2} ||(p_1 a_j p_j)(p_1 a_j p_j)^*|| = \frac{1}{\lambda_j^2} ||p_1 a_j p_j||^2 = 1,$$

we find that $v_{1j} v_{1j}^* = p_1$. Similarly we find that $v_{1j}^* v_{1j} = p_j$, and we have a sequence $(v_{1j})_{j=1}^{k}$ of partial isometries.

Let $w_{ij} = v_{1i}^* v_{1j}$. We note that

$$w_{ij}^* = v_{1j}^* v_{1i} = w_{ji}. \tag{2.2.3}$$

Then, $\varphi : M_k(\mathbb{C}) \to \mathcal{A}$ defined on the matrix units like $e_{ij} \mapsto w_{ij}$ respects the $*$-property since by (2.2.3) it follows that $\varphi(e_{ij})^* = \varphi(e_{ij}^*)$. Furthermore, since

$$w_{ij} w_{kl} = v_{1i}^* v_{1j} v_{1k}^* v_{1l} = v_{1i} \delta_{jk} v_{1l}^* = \delta_{jk} w_{il}$$

and

$$\varphi(e_{ij}e_{kl}) = \varphi(\delta_{jk}e_{il}) = \delta_{jk}w_{il}$$

by (2.2.1), it follows that φ is multiplicative, and hence a $*$-isomorphism. ∎

Corollary 2.18. *If $\mathcal{A}$ is a non-zero finite-dimensional C^*-algebra, it is $*$-isomorphic to a direct sum of matrix algebras $\bigoplus_{i=1}^{k} M_{n_i}(\mathbb{C})$.*

Proof. The claim follows by Proposition 2.14 and Proposition 2.17. ∎

This result concludes the classification of finite-dimensional C^*-algebras. Before proceeding further to study concepts in the theory of C^*-algebras, we state the following result, which will be helpful for our future discussions in Section 3.3:

Proposition 2.19. *Let $A, B \subseteq M_n(\mathbb{C})$ be commuting C^*-subalgebras which generate $M_n(\mathbb{C})$. Then, there are isomorphisms $A \cong M_{n_A}(\mathbb{C}) \otimes \mathbb{1}_{M_{n_B}(\mathbb{C})}$ and $B \cong \mathbb{1}_{M_{n_A}(\mathbb{C})} \otimes M_{n_B}(\mathbb{C})$ such that $n_A \cdot n_B = n$ and*

$$M_{n_A}(\mathbb{C}) \otimes \mathbb{1}_{M_{n_B}(\mathbb{C})}, \mathbb{1}_{M_{n_A}(\mathbb{C})} \otimes M_{n_B}(\mathbb{C}) \subseteq M_{n_A}(\mathbb{C}) \otimes M_{n_B}(\mathbb{C}).$$

Proof. Recall by Proposition 2.15 that $M_n(\mathbb{C})$ is simple, and since A and B commute it follows that the center of A and B are both trivial. So by Proposition 2.14 both A and B are simple and by Proposition 2.17 there exist integers n_A and n_B such that $A \cong M_{n_A}(\mathbb{C})$ and $B \cong M_{n_B}(\mathbb{C})$.

Furthermore, we recall that a matrix algebra has a basis given by the set of matrix units, so let $(e_{ij})_{ij}$ be the matrix units in A given by the isomorphism, and similarly $(f_{kl})_{kl}$ the matrix units in B. Then, since A and B commute and generate $M_n(\mathbb{C})$, this yields a system of matrix units $(e_{ij}f_{kl})_{(ik),(jl)}$ in $M_n(\mathbb{C})$. We thus obtain the desired isomorphisms. ∎

§ 2.3. The GNS representation. We start by giving a summary of the *Gelfand-Neumark-Segal construction*, or GNS construction, which describes a correspondence between so-called cyclic representations of a C^*-algebra and its states. As we will see, given a state $\varphi \in \mathcal{S}(\mathcal{A})$, there exists a $*$-representation π of $\mathcal{A}$ on a Hilbert space $\mathcal{H}$ with cyclic vector ξ uniquely determined up to unitary conjugation by the relation $\varphi(a) = \langle \pi(a)\xi, \xi \rangle$. Arguably, the most useful property of this construction is to show that every C^*-algebra can be considered as a C^*-subalgebra of bounded operators on some Hilbert space.

We first state the necessary definitions:

Definition 2.20. Let $\mathcal{A}$ be a C^*-algebra. A $*$-*representation* of $\mathcal{A}$ is a pair $(\mathcal{H}, \varphi)$ where $\mathcal{H}$ is a Hilbert space and $\varphi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ is a $*$-homomorphism. If φ is injective, $(\mathcal{H}, \varphi)$ is said to be *faithful*.

Definition 2.21. If $(\mathcal{H}, \varphi)$ is a $*$-representation of a C^*-algebra $\mathcal{A}$, a vector $\xi \in \mathcal{H}$ is said to be *cyclic* for $(\mathcal{H}, \varphi)$ if $\varphi(\mathcal{A})\xi$ is dense in $\mathcal{H}$. If $(\mathcal{H}, \varphi)$ admits a cyclic vector, we say that it is a *cyclic representation*.

We will here omit the details of the proof of the GNS construction but only present its steps. The interested reader can consult [14,17] for proofs and further details.

Let $\mathcal{A}$ be a C^*-algebra, and φ a state on $\mathcal{A}$. Then, the set $N = \{a \in \mathcal{A} \mid \varphi(a^*a) = 0\}$ is a closed subspace of $\mathcal{A}$, so $\mathcal{A}/N$ is a vector space on which we can define an inner product

$$\langle a + N, b + N \rangle = \varphi(b^*a).$$

The completion of $\mathcal{A}/N$ is a Hilbert space, denoted by $\mathcal{H}_\varphi$. On $\mathcal{B}(\mathcal{H}_\varphi)$ we can define an operator $\pi_\varphi(a)$ by

$$\pi_\varphi(a)(b + N) = ab + N,$$

which extends to a cyclic $*$-representation of $\mathcal{A}$ on $\mathcal{H}_\varphi$, $a \mapsto \pi_\varphi(a)$ with cyclic vector ξ_φ satisfying

$$\left\langle \pi_\varphi(a)\xi_\varphi, \xi_\varphi \right\rangle = \varphi(a) \tag{2.3.1}$$

for all $a \in \mathcal{A}$.

Given a state φ, the three elements $\mathcal{H}_\varphi, \pi_\varphi$, and ξ_φ are used to denote the three components of the GNS construction, and we refer to them as the *GNS representation* of φ. Notably, the GNS representation is uniquely determined by the identity (2.3.1):

Proposition 2.22. *Let φ be a state of a C^*-algebra $\mathcal{A}$, π a $*$-representation of $\mathcal{A}$ on a Hilbert space $\mathcal{H}$ with a unit cyclic vector ξ satisfying (2.3.1) with φ, π, and ξ. Then if $\mathcal{H}_\varphi, \pi_\varphi, \xi_\varphi$ are given by the GNS construction, there is an isomorphism $u : \mathcal{H}_\varphi \to \mathcal{H}$ such that*

$$\pi(a) = u\pi_\varphi(a)u^*,$$

for all $a \in \mathcal{A}$, and $\xi = u\xi_\varphi$.

So finally, if we for a C^*-algebra have a cyclic representation π and a vector ξ satisfying (2.3.1), then π is equivalent to the GNS representation of φ.

Note that the GNS construction yields a way to describe a quantum state given by a state $\varphi \in \mathcal{S}(\mathcal{A})$ in the traditional way as a unit vector ξ in a Hilbert space H by finding ξ, H and π satisfying (2.3.1) for all $a \in \mathcal{A}$.

§ 2.4. Universal C^*-algebras. As we have seen when discussing matrix algebras and their matrix units, it is useful to describe a C^*-algebra in terms of a set of generators. The idea of constructing a C^*-algebra from a set of generators and relations between them by finding a suitable norm and completing it results in the theory of universal C^*-algebras, as we will see.

As an initial bit of notation, given a set of elements $S = \{x_i \mid i \in I\}$, we let $\mathbb{C}[S \cup S^*]$ denote the $*$-algebra freely generated by S and its formal adjoint $S^* = \{x_i^* \mid i \in I\}$. Note that any $p \in \mathbb{C}[S \cup S^*]$ can be represented as a polynomial in variables S and S^*, and if $p = 0$ it can be interpreted as an algebraic relation of elements in S and S^*.

Definition 2.23. Let $\mathcal{A}$ be a C^*-algebra. A seminorm $p : \mathcal{A} \to [0, \infty)$ is called a *C^*-seminorm* if it holds that

- $p(x^*x) = p(x)^2$ for all $x \in \mathcal{A}$, and
- $p(xy) \leq p(x)p(y)$ for all $x, y \in \mathcal{A}$.

Definition 2.24. Let S be a set of generators subject to relations $R \subseteq \mathbb{C}[S \cup S^*]$ such that for every $s \in S$ there is $c_s \geq 0$ such that for every $*$-representation $\pi : \mathbb{C}[S \cup S^*] \to \mathcal{B}(\mathcal{H})$ with $\pi(R) \subseteq \{0\}$, we have that $||\pi(s)|| \leq c_s$. Then, the *universal C^*-algebra* with generators S and relations R is denoted by $C^*(S \mid R)$ and is defined as the separation-completion of $\mathbb{C}[S \cup S^*]$ with respect to the C^*-seminorm

$$||x|| = \sup \{||\pi(x)|| \mid \pi : \mathbb{C}[S \cup S^*] \to \mathcal{B}(\mathcal{H}),\ \pi(R) \subseteq \{0\}\}.$$

Note that the kernel of this seminorm contains the ideal (R) generated by the relations R, by definition. In this way, the universal C^*-algebra is the completion of the quotient of $\mathbb{C}[S \cup S^*]$ by an ideal containing (R). The universal C^*-algebra satisfies the following universal property:

Proposition 2.25. *Let $\mathcal{A}$ be a C^*-algebra, and denote by $C^*(S \mid R)$ the universal C^*-algebra associated with generators S and relations R. Given a map $f : S \to \mathcal{A}$ such that the images of elements in S satisfy the relations R, there exists a unique $*$-homomorphism $\pi : C^*(S \mid R) \to \mathcal{A}$ sending every $s \in S$ to its image in $\mathcal{A}$ under f.*

Proof. Let $\pi_0 : \mathbb{C}[S \cup S^*] \to \mathcal{B}$ be the $*$-homomorphism sending each generator $s \in S$ to its image $f(s) \in \mathcal{B}$ under f. Indeed, such π_0 exists since by the property of $\mathbb{C}[S \cup S^*]$ being a polynomial ring, the evaluation polynomial is a homomorphism. Note that $(R) \subseteq \ker(\pi_0)$ since the relations in R are satisfied in $\mathcal{A}$ by assumption, so that $||\pi_0(x)|| \leq ||x||$ for all $x \in \mathbb{C}[S \cup S^*]$. Thus, the map is contractive and hence extends uniquely to a $*$-homomorphism $\pi : C^*(S \mid R) \to \mathcal{A}$ on the completion of the quotient. ∎

Example 2.26. We return for a moment to our initial motivation for the definition of the universal C^*-algebra, i.e. matrix algebras and their matrix units, and show that, as expected, the universal C^*-algebra generated by such matrix units, with the proper relations, is isomorphic to the matrix algebra.

Let e_{ij} denote the matrix units that we have seen in Section 2.2, and consider the C^*-algebra

$$C^*(x_{ij}, 1 \leq i, j \leq n \mid x_{ij}x_{kl} = \delta_{jk}x_{il}, x_{ij}^* = x_{ji}, 1 \leq i, j, k, l \leq n).$$

Since

$$(x_{ij}^* x_{ij})^2 = x_{ij}^* x_{ij} x_{jj} = x_{ij}^* x_{ij},$$

it follows that $x_{ij}^* x_{ij}$ is a projection, so $1 = ||x_{ij}^* x_{ij}|| = ||x_{ij}||$, or $||x_{ij}|| = 0$. Thus, this universal C^*-algebra exists. Then, by the universal property, there exists a $*$-homomorphism π from this C^*-algebra to $M_n(\mathbb{C})$, such that $\pi(x_{ij}) = e_{ij}$. By the relations on the x_{ij}, the $*$-algebra generated by these elements is at most n^2-dimensional since the $\{x_{ij} \mid 1 \leq i, j \leq n\}$ is a spanning set. Thus, the universal C^*-algebra also has dimension at most n^2, and since π maps it onto $M_n(\mathbb{C})$, it follows that π is an isomorphism. In particular, this also shows that the universal C^*-algebra is non-trivial. Since both spaces are n^2-dimensional, it follows that they are isomorphic.

§ 2.5. Group theoretical constructions. An instrumental group theoretic construction for our purposes is the so-called *Higman-Neumann-Neumann (HNN) extension*, which allows embedding a given group H into a larger group G such that two isomorphic subgroups of H end up being conjugate in G. The extension works as follows:

Definition 2.27. Let H be a finitely presented group $H = \langle S \mid R \rangle$ and $\alpha : K_0 \longrightarrow K_1$ an isomorphism between subgroups K_0 and K_1 of H. Then, the *HNN extension* of H is the group with presentation

$$G = \left\langle S \cup \{t\} \mid R \cup \{tkt^{-1} = \alpha(k), \text{ for all } k \in K_o\} \right\rangle,$$

where t is a symbol not in S.

It can be shown that H is embedded in G [16], Theorem 2.1.

For our discussions, the HNN extension of a specific group will be of interest: we define *Higman's group*

$$H = \left\langle a, b, c, d \mid aba^{-1} = b^2, bcb^{-1} = c^2, cdc^{-1} = d^2, dad^{-1} = a^2 \right\rangle. \qquad (2.5.1)$$

Two properties of this group stand out – its generators have infinite order, i.e., it has no non-trivial finite quotient and thus no non-trivial linear representations. Following [12] and [9] we now prove this.

Definition 2.28. A group G is said to be *residually finite* if for every non-identity element $g \in G$, there is a homomorphism $\phi : G \to H$ such that H is finite and $\phi(g) \neq 1$. Equivalently, the intersection of all its normal subgroups of finite index is trivial.

The property of a group being residually finite will be crucial in the proof of the main result of this text, given in Section 4.2. For this purpose, we note that a group without non-trivial finite quotients also does not have any non-trivial linear representations.

Lemma 2.29. *If n is an integer greater than 1, the least prime factor of n is smaller than the least prime factor of $2^n - 1$.*

Proof. Let p be a prime factor of $2^n - 1$, and r the least positive integer such that p divides $2^r - 1$ and has a prime factor q. In particular, 2 has order r in $(\mathbb{Z}/p\mathbb{Z})^*$, and since the order of any element necessarily must divide $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1$, it follows that r divides $p - 1$. Since $2^n \equiv 1 \pmod{p}$ the order r of 2 in $(\mathbb{Z}/p\mathbb{Z})^*$ divides n. Furthermore, since $q < p$ it follows that q is a prime factor of n. Thus, the statement follows. ∎

Proposition 2.30. *All elements $a, b, c,$ and d in a group satisfying the relations of Higman's group are either trivial or have infinite order.*

Proof. Suppose a, b, c, d are elements of a finite group that are not all equal to 1 and which satisfy the relations of Higman's group. Let n_a, n_b, n_c, n_d be the order of a, b, c, d, respectively. Then, $a^n b a^{-n} = b^{2^n}$ so that n_b divides $2^{n_a} - 1$, and similarly $n_c \mid 2^{n_b} - 1$, $n_d \mid 2^{n_c} - 1$, and $n_a \mid 2^{n_d} - 1$. Thus, either $n_a = n_b = n_c = n_d = 1$ or all orders are greater than 1. So we conclude that if the order of one of the generators is finite, then all have finite order.

By assumption, $n_a, n_b, n_c, n_d > 1$. By symmetry of the relations, assume without loss of generality that the smallest prime factor of $n_a n_b n_c n_d$ divides n_b. However, since n_b was shown to divide $2^{n_a} - 1$, by Lemma 2.29, there exists a smaller integer dividing n_a. This is a contradiction, so it follows that all generators have infinite order. ∎

Proposition 2.31. *Higman's group does not have any non-trivial linear representations. In other words, Higman's group is non-residually finite.*

Proof. By Proposition 2.30, Higman's group has no non-trivial finite quotients. By Mal'cev's theorem, any finitely generated linear group is residually finite; see for example [22]. In particular, any finitely generated linear group has a non-trivial finite quotient. Thus, the statement follows. ∎

3. Non-local games and quantum correlations

We present the fundamental definitions and theory of non-local games and the correlation sets arising from different strategies for such games. Notably, non-local games can be used as a theoretical tool to demonstrate the computational advantage of quantum entanglement as opposed to classical computational resources. In what follows, some familiarity with the basic notions of quantum information theory presented in Appendix A is needed.

§ 3.1. Non-local games. We will here consider only non-local games with two players understood as being physically separated at a great distance, thus making communication during the game unfeasible. In this section, we follow the notation in [18].

In what follows, let $[n]$ denote the set of integers from 1 to n, i.e. $[n] = \{1, \dots, n\}$.

Definition 3.1. A *two-player non-local game* $\mathcal{G}(V, \pi)$ with distinguished entities A and B consists of the following data:

- Question sets $[n_A]$ and $[n_B]$,
- Answer sets $[m_A]$ and $[m_B]$,
- A probability distribution π on $[n_A] \times [n_B]$,
- A function $V : [m_A] \times [m_B] \times [n_A] \times [n_B] \to \{0, 1\}$.

As a matter of convention, we write $V(a, b \mid x, y)$ in place of $V(a, b, x, y)$, where $(a, b) \in [m_A] \times [m_B]$ and $(x, y) \in [n_A] \times [n_B]$.

More intuitively, a non-local game takes place between two players, frequently referred to as Alice and Bob, and a referee. The referee chooses the function V, which determines the required conditions for Alice and Bob to win the game. Furthermore, the referee distributes a pair of questions $(x, y) \in [n_A] \times [n_B]$, chosen according to the probability distribution π, to the players, sending x to Alice and y to Bob.

At this point, the players cannot communicate and should return suitably chosen answers $a \in [m_A]$ and $b \in [m_B]$, respectively, to the referee. If, upon evaluation, the referee finds that $V(a, b \mid x, y) = 1$, the players win the game.

Presented with a non-local game, in order to optimize the probability of winning, Alice and Bob may decide to use a common strategy, which they can decide on beforehand. In particular, we will make a distinction between classical and quantum strategies.

The most straightforward classical strategy is for the players to each choose a function $f_A : [n_A] \to [m_A]$ and $f_B : [n_B] \to [m_B]$ which determines their respective output given any input pair. We refer to this as a *deterministic*

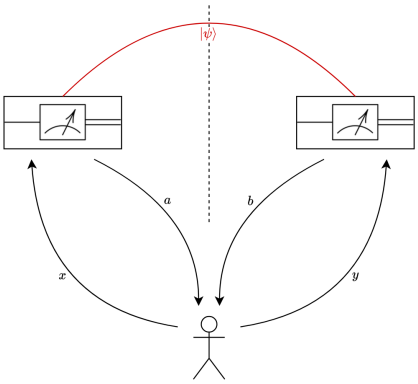

Figure 1: Model of a two-player non-local game with a shared quantum state.

strategy. Alternatively, the players could use randomization to select their answers, which can be understood as selecting a probability distribution over deterministic strategies. Such a strategy is called *probabilistic*.

Conversely, the players commit to using quantum entanglement as a shared computational resource in a quantum strategy. In particular, Alice and Bob now share an entangled quantum state. The output is given by applying projection-valued measures (PVMs) corresponding to the received question. Here, we will distinguish between two types of quantum strategies.

Definition 3.2. In the *tensor-product model* of a non-local game, separate Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ are associated with Alice and Bob, respectively. The shared quantum state $|\psi\rangle$ belongs to the space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. For each $x \in [n_A]$ is defined a PVM $(P_a^x)_{a=1}^{m_A}$ on $\mathcal{H}_A$, and for each $y \in [n_B]$ a PVM $(Q_b^y)_{b=1}^{m_B}$ on $\mathcal{H}_B$.

Then, a joint measurement is given by $(P_a^x \otimes Q_b^y)_{(a,b)\in[m_A]\times[m_B]}$, which can be seen to be a PVM on $\mathcal{H}$. The probability of observing (a, b) given the measurement corresponding to the input (x, y) is equal to $\langle\psi| P_a^x \otimes Q_b^y |\psi\rangle$, and we define the function

$$p(a, b \mid x, y) = \langle\psi| P_a^x \otimes Q_b^y |\psi\rangle\,, \tag{3.1.1}$$

for every $(a, b, x, y) \in [m_A] \times [m_B] \times [n_A] \times [n_B]$.

Definition 3.3. In the *commuting-operator model* of a non-local game, the shared quantum state $|\psi\rangle$ and PVMs $(P_a^x)_{a=1}^{m_A}$ and $(Q_b^y)_{b=1}^{m_B}$ given (x, y), all belong to a shared Hilbert space $\mathcal{H}$, on which the operators P_a^x and Q_b^y are taken to be commuting for all $(a, b) \in [n_A] \times [n_B]$. Then, a simple proof shows that the joint measurement $(P_a^x Q_b^y)_{(a,b)\in[m_A]\times[m_B]}$ is also a PVM, and, as before, the probability of observing the response (a, b) on input (x, y) is

given by the function

$$p(a, b \mid x, y) = \langle \psi | \, P_a^x Q_b^y \, | \psi \rangle \, . \tag{3.1.2}$$

Example 3.4 (The CHSH game)**.** One of the more famous examples of non-local games is the so-called *CHSH game*, named after physicists John Clauser, Michael Horne, Abner Shimony, and Richard Holt. The CHSH game provided a model to study quantum entanglement and was used to show that it is impossible to simulate this phenomenon using classical randomness. The interested reader may consult [4] for a further discussion of this significant result.

In this setting, $[n_A] = [n_B] = [m_A] = [m_B] = \{0, 1\}$ a set, π is the uniform probability distribution on $[n_A] \times [n_B]$, and

$$V(a, b \mid x, y) = \begin{cases} 1 \text{ if } a \oplus b = x \wedge y \\ 0 \text{ otherwise.} \end{cases}$$

As $x \wedge y = 1$ if and only if $x = y = 1$ and $a \oplus b = 1$ if and only if $a \neq b$, a simple deterministic strategy could be for Alice and Bob to both always return either 0 or 1. A strategy in which they instead return distinct answers only results in a win if $x = y = 1$. Since π is uniform, the former strategy leads to the players winning the CHSH game in $\frac{3}{4}$ of cases. By enumeration, it can be shown that no better deterministic strategy exists.

Now let $|\psi\rangle = \frac{1}{\sqrt{2}} |00\rangle + |11\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^2$ be the Bell pair discussed in Example A.7, and define projection-valued measures:

$$P_0^0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad P_1^0 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{if } x = 0, \text{ and}$$

$$P_0^1 = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad P_1^1 = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \quad \text{if } x = 1.$$

Likewise if $y = 0$ we define

$$Q_0^0 = \begin{bmatrix} \cos^2 \frac{\pi}{8} & \cos \frac{\pi}{8} \sin \frac{\pi}{8} \\ \cos \frac{\pi}{8} \sin \frac{\pi}{8} & \sin^2 \frac{\pi}{8} \end{bmatrix}, \quad Q_1^0 = \begin{bmatrix} \cos^2 \frac{5\pi}{8} & \cos \frac{5\pi}{8} \sin \frac{5\pi}{8} \\ \cos \frac{5\pi}{8} \sin \frac{5\pi}{8} & \sin^2 \frac{5\pi}{8} \end{bmatrix}$$

and if $y = 1$ the PVM

$$Q_0^1 = \begin{bmatrix} \cos^2 \frac{-\pi}{8} & \cos \frac{-\pi}{8} \sin \frac{-\pi}{8} \\ \cos \frac{-\pi}{8} \sin \frac{-\pi}{8} & \sin^2 \frac{-\pi}{8} \end{bmatrix}, \quad Q_1^1 = \begin{bmatrix} \cos^2 \frac{3\pi}{8} & \cos \frac{3\pi}{8} \sin \frac{3\pi}{8} \\ \cos \frac{3\pi}{8} \sin \frac{3\pi}{8} & \sin^2 \frac{3\pi}{8} \end{bmatrix}.$$

In this case, if for instance $x = y = 0$, the probability that Alice and Bob win the game is equal to $\langle \psi | \, P_0^0 \otimes Q_0^0 \, | \psi \rangle + \langle \psi | \, P_1^0 \otimes Q_1^0 \, | \psi \rangle = \cos^2 \frac{\pi}{8}$.

§ 3.2. Correlation sets. Given a non-local game, we want to compare different strategies and their winning probabilities. For this reason, we now consider in greater detail the functions (3.1.1) and (3.1.2), called *correlations*. We make the following definition:

Definition 3.5. A function $p \in \mathbb{R}^{[m_A]\times[m_B]\times[n_A]\times[n_B]}$ is called a *correlation* of a particular strategy if for every $(a,b,x,y) \in [m_A]\times[m_B]\times[n_A]\times[n_B]$, the number $p(a,b \mid x,y)$ is the probability that the referee of the corresponding non-local game sees output (a,b) on input (x,y). We call the collection $(p(a,b \mid x,y)) \subset \mathbb{R}^{[m_A]\times[m_B]\times[n_A]\times[n_B]}$ a *correlation matrix*.

In particular, based on what we have seen in (3.1.1) and (3.1.2) we define correlations corresponding to the different quantum strategies as follows:

Definition 3.6. A function $p \in \mathbb{R}^{[m_A]\times[m_B]\times[n_A]\times[n_B]}$ is called a *tensor-product correlation* if there exists Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a unit vector $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, and PVMs $(P_a^x)_{a=1}^{m_A}$ on $\mathcal{H}_A$ and $(Q_b^y)_{b=1}^{m_B}$ on $\mathcal{H}_B$ for every $x \in [n_A]$ and $y \in [n_B]$, respectively, such that

$$p(a,b \mid x,y) = \langle\psi| P_a^x \otimes Q_b^y |\psi\rangle$$

for all $(a,b,x,y) \in [m_A]\times[m_B]\times[n_A]\times[n_B]$.

Definition 3.7. A function $p \in \mathbb{R}^{[m_A]\times[m_B]\times[n_A]\times[n_B]}$ is called a *commuting operator correlation* if there exists a Hilbert space $\mathcal{H}$ with a unit vector $\psi \in \mathcal{H}$, and PVMs $(P_a^x)_{a=1}^{m_A}$ and $(Q_b^y)_{b=1}^{m_B}$ for every $x \in [n_A]$ and $y \in [n_B]$, respectively, such that $[P_a^x, Q_b^y] = 0$ and

$$p(a,b \mid x,y) = \langle\psi| P_a^x Q_b^y |\psi\rangle$$

for all $(a,b,x,y) \in [m_A]\times[m_B]\times[n_A]\times[n_B]$.

Given a non-local game, a natural question to ask is what the optimal probability of winning the game is, and which strategy Alice and Bob should use to obtain it. This motivates the following definition:

Definition 3.8. The *winning probability* of a correlation p for a non-local game $\mathcal{G}(V,\pi)$, is given by

$$\sum_{x=1}^{n_A}\sum_{y=1}^{n_B}\pi(x,y)\sum_{a=1}^{m_A}\sum_{b=1}^{m_B}V(a,b \mid x,y)p(a,b \mid x,y).$$

The *value* of $\mathcal{G}(V,\pi)$ with a given strategy, is defined as the supremum of the winning probability taken over all correlations. A strategy is said to be *perfect* if it has winning probability 1.

Example 3.9. We continue our discussion of the CHSH game, presented in Example 3.4. Note first that every deterministic strategy corresponds to choosing a pair of functions $f_A : [n_A] \to [m_A]$ and $f_B : [n_B] \to [m_B]$. Given input $x \in [n_A]$, the function f_A can take on four different values:

$$x \mapsto 0, \quad x \mapsto 1, \quad x \mapsto x, \quad \text{or } x \mapsto \neg x,$$

and similarly for f_B. This results in 16 different strategies with corresponding correlation matrices. For instance, if $f_A = f_B \equiv 0$ we have the correlation

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

for which we may compute the winning probability $3/4$, as expected. Simple case analysis now shows that the classical value of the CHSH game is $3/4$.

We now consider the tensor-product strategy described in Example 3.4. For this strategy, we have the following correlation matrix:

$$\frac{1}{2}\begin{bmatrix} \cos^2\frac{\pi}{8} & \cos^2\frac{\pi}{8} & \frac{1}{2}+\cos\frac{\pi}{8}\sin\frac{\pi}{8} & \frac{1}{2}-\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ \sin^2\frac{\pi}{8} & \sin^2\frac{\pi}{8} & \frac{1}{2}-\cos\frac{\pi}{8}\sin\frac{\pi}{8} & \frac{1}{2}+\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ \sin^2\frac{\pi}{8} & \sin^2\frac{\pi}{8} & \frac{1}{2}-\cos\frac{\pi}{8}\sin\frac{\pi}{8} & \frac{1}{2}+\cos\frac{\pi}{8}\sin\frac{\pi}{8} \\ \cos^2\frac{\pi}{8} & \cos^2\frac{\pi}{8} & \frac{1}{2}+\cos\frac{\pi}{8}\sin\frac{\pi}{8} & \frac{1}{2}-\cos\frac{\pi}{8}\sin\frac{\pi}{8} \end{bmatrix}.$$

Then, it follows that the tensor-product value of the CHSH game is at least

$$\frac{1}{2} + \frac{1}{2\sqrt{2}} = \cos^2\frac{\pi}{8} \approx 0.85,$$

so the winning probability of this quantum strategy is indeed higher than for any classical strategy in this case. That this value is indeed also the *quantum value* of the CHSH game is a result known as Tsirelson's bound, the proof of which is found in [3].

§ 3.3. Hierarchy of correlation sets – known results. We are particularly interested in comparing the correlation sets arising from tensor-product and commuting-operator strategies. Given (n_A, n_B, m_A, m_B), the set of tensor-product correlations on finite-dimensional Hilbert spaces is denoted by $C_q(n_A, n_B, m_A, m_B)$. If the Hilbert spaces are not necessarily finite-dimensional, this set is denoted by $C_{qs}(n_A, n_B, m_A, m_B)$. Furthermore, we denote the closure of C_{qs} by $C_{qa}(n_A, n_B, m_A, m_B)$. Lastly, the set of commuting-operator correlations is denoted by $C_{qc}(n_A, n_B, m_A, m_B)$. Often, when the tuple (n_A, n_B, m_A, m_B) is clear, we will drop it from the notation.

As we have seen in Example 3.9, a question of particular interest is whether or not we have equality between different correlation sets. In the same example, we saw that the set of classical correlations is not necessarily equal to the set of quantum tensor-product correlations. Boris Tsirelson first considered the extended question of comparing correlations of different quantum strategies in [3], in which Tsirelson claimed the equality of quantum correlation sets corresponding to different quantum strategies. Upon realizing that the claim needed a complete proof, Tsirelson posted the open question online [20].

Since the publication of the question, the following hierarchy of correlation sets have been the subject of intense study:

$$C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{qc}.$$

For any two correlation sets in the above hierarchy, we can ask whether or not there is equality – this is known as a *Tsirelson problem*.

Considering the particular finite-dimensional tensor-product strategy described in Example 3.4, we might ask if there exists a commuting-operator strategy which yields a greater value. It is clear that any tensor-product strategy with projections $(P_a^x)_{a=1}^{m_A}$ and $(Q_b^y)_{b=1}^{m_B}$ in finite-dimensional Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, can be extended to a commuting-operator strategy by considering $(P_a^x \otimes \mathbb{1})_{a=1}^{m_A}$ and $(\mathbb{1} \otimes Q_b^y)_{b=1}^{m_B}$, both easily seen to be PVMs in the finite-dimensional Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, such that $P_a^x \otimes \mathbb{1}$ and $\mathbb{1} \otimes Q_b^y$ commutes for all $(a, b) \in [n_A] \times [n_B]$. This shows that $C_q \subseteq C_{qc}$, so there at least exists a commuting-operator strategy with the same value as the strategy seen in Example 3.4.

The reverse inclusion does not hold in general: Slofstra showed in [18] that $C_{qs} \neq C_{qc}$ and hence also that $C_q \neq C_{qc}$. It is this Tsirelson problem we consider in this text. However, concerning ourselves only with finite-dimensional Hilbert spaces for a moment, Tsirelson sketched a proof in [21] that equality holds in this case. We here present a more detailed version of the proof, culminating in Corollary 3.13. In what follows, we use the word state in the context of C^*-algebras, as given in Section 2.1.

Lemma 3.10. *Let $\varphi : M_n(\mathbb{C}) \to \mathbb{C}$ be a state. Then there is a positive definite matrix $d \in M_n(\mathbb{C})$ such that $\varphi(a) = Tr(ad)$ for all $a \in M_n(\mathbb{C})$.*

Proof. Define d as the matrix with entries $d_{ij} := \varphi(e_{ji})$. For any $1 \leq k, l \leq n$,

we find that

$$\begin{aligned} Tr(e_{kl}d) &= \sum_{i,j} d_{ij} Tr(e_{kl}e_{ij}) \\ &= \sum_{j=1}^{n} d_{lj} Tr(e_{kj}) \\ &= d_{lk} = \varphi(e_{kl}), \end{aligned}$$

by (2.2.1). Furthermore, d is Hermitian since $\overline{d_{ij}} = \overline{\varphi(e_{ji})} = \varphi(e_{ji}^*) = \varphi(e_{ij}) = d_{ji}$. Let $x = (x_1, \ldots, x_n)^T \in \mathbb{C}^n$, then

$$\begin{aligned} x^* dx &= \sum_{i,j} x_i \overline{x_j} d_{ij} \\ &= \sum_{i,j} \varphi(x_i \overline{x_j} e_{ji}) \\ &= \varphi\left(\left(\sum_i^n x_i e_{1i}\right)^* \left(\sum_i^n x_i e_{1i}\right)\right) \geq 0, \end{aligned}$$

since φ is a state. Thus, d is positive definite. ∎

Lemma 3.11. *Every pure state on $M_n(\mathbb{C})$ is unitarily conjugate to the state $\tau(a) = Tr(ae_{11})$, whose GNS construction is the standard representation $M_n(\mathbb{C})$ on $\mathbb{C}^n$ with cyclic vector e_1.*

Proof. By the spectral theorem for positive operators and Lemma 3.10 it follows that for every pure state φ, there exist a unitary u such that $\varphi(u^*au) = Tr(ae_{11})$.

Under the standard representation of $M_n(\mathbb{C})$ on $\mathbb{C}^n$ we see that $\langle ae_1, e_1\rangle = a_{11}$ for all $a \in M_n(\mathbb{C})$ so the cyclic vector e_1 satisfies property (2.3.1). We deduce that the GNS construction of τ is indeed as claimed. ∎

The following proposition is the main result needed in the proof of the finite-dimensional Tsirelson problem:

Proposition 3.12. *Let $\mathcal{A}$ be a C^*-algebra generated by two mutually commuting C^*-subalgebras $A, B \subseteq \mathcal{A}$. Let $\varphi \in \mathcal{S}(\mathcal{A})$ be a pure state such that the associated GNS representation $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ is finite-dimensional. Then there exists a decomposition $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ such that $\pi_{|A} = \pi_A \otimes id_{\mathcal{H}_B}$ and $\pi_{|B} = id_{\mathcal{H}_A} \otimes \pi_B$, where $\pi_A : A \to \mathcal{B}(\mathcal{H}_A)$ and $\pi_B : B \to \mathcal{B}(\mathcal{H}_B)$.*

Proof. Since φ is pure, it follows by Theorem 5.1.6 of [17] that π is irreducible, and since it is finite-dimensional it is also surjective. Thus, without loss of

generality we may identify $\mathcal{A}$ with its image under π, i.e., $\pi(\mathcal{A}) = M_n(\mathbb{C})$ for some $n \in \mathbb{N}$.

Then, the images of A and B are also mutually commuting and generate $M_n(\mathbb{C})$, so by Proposition 2.19 there are $n_A, n_B \in \mathbb{N}$ such that we can make the identifications $\pi(A) = M_{n_A}(\mathbb{C}) \otimes \mathbb{1}_{M_{n_B}(\mathbb{C})}$ and $\pi(B) = \mathbb{1}_{M_{n_A}(\mathbb{C})} \otimes M_{n_B}(\mathbb{C})$ as subalgebras of $M_{n_A}(\mathbb{C}) \otimes M_{n_B}(\mathbb{C})$.

Thus, by Lemma 3.11 there exists a unitary $u : \mathcal{H} \to \mathbb{C}^n$ so that we obtain the desired decomposition of $\mathcal{H}$ with $\mathcal{H}_A = \mathbb{C}^{n_A}$ and $\mathcal{H}_B = \mathbb{C}^{n_B}$ and cyclic vector $e_1 \otimes e_1 \in \mathbb{C}^{n_A} \otimes \mathbb{C}^{n_B}$. ∎

Corollary 3.13. *Let $\langle\psi| P_a^x Q_b^y |\psi\rangle$ be a correlation in C_{qc} with finite-dimensional Hilbert space $\mathcal{H}$. Then there exists Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ and a tensor-product correlation $\langle\varphi| R_a^x \otimes S_b^y |\varphi\rangle$ with the same value, such that $(R_a^x)_a \in \mathcal{H}_A$, $(S_b^y)_b \in \mathcal{H}_B$ and $|\varphi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$.*

Proof. Let $\mathcal{A}$ denote the C^*-algebra generated by $(P_a^x)_a$ and $(Q_b^y)_b$. Then $\mathcal{A}'$ is a finite-dimensional C^*-algebra so by Lemma 2.16, there exists a family of minimal projections $p_1, \ldots, p_n$, such that $\sum_{i_1}^n p_i = \mathbb{1}$.

Let $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ be a finite-dimensional $*$-representation. Then, since $(\pi_{|p_i\mathcal{H}}(\mathcal{A}))' = p_i(\mathcal{A}')p_i = \mathbb{C}p_i$, we find that $\pi_{|p_i\mathcal{H}}$ is irreducible and we consider the decomposition $\mathcal{H} = \bigoplus_{i=1}^n p_i\mathcal{H}$.

Recall that we have decompositions of $\mathcal{A}$ and $\mathcal{A}'$ into direct sums of simple C^*-algebras $\mathcal{A} = \bigoplus_i \mathcal{A}_i$ and $\mathcal{A}' = \bigoplus_i \mathcal{A}_i'$, and by Proposition 3.12 for each i we can identify $\mathcal{A}_i$ and $\mathcal{A}_i'$ with $M_{k_i}(\mathbb{C}) \otimes \mathbb{1}_{M_{l_i}(\mathbb{C})}$ and $\mathbb{1}_{M_{k_i}(\mathbb{C})} \otimes M_{l_i}(\mathbb{C})$, respectively, acting on $p_i\mathcal{H} = \mathbb{C}^{k_i} \otimes \mathbb{C}^{l_i}$. We make the following simplifying notation: $\mathcal{H}_{A,i} = \mathbb{C}^{k_i}$ and $\mathcal{H}_{B,i} = \mathbb{C}^{l_i}$.

So we can embed

$$\mathcal{H} \subseteq \bigoplus_i \mathcal{H}_{A,i} \otimes \bigoplus_i \mathcal{H}_{B,i},$$

finding corresponding PVMs $(\pi_A(P_a^x))_a$ and $(\pi_B(Q_b^y))_b$ in $\bigoplus_i \mathcal{H}_{A,i}$ and $\bigoplus_i \mathcal{H}_{B,i}$, respectively.

Finally, for all i, consider $|\psi_i\rangle = p_i |\psi\rangle$ and assume without loss of generality that $|\psi_i\rangle \neq 0$ for all i. Then, $\sum_{i=1}^n |\psi_i\rangle \in \bigoplus_i \mathcal{H}_{A,i} \otimes \mathcal{H}_{B,i}$ is the sought-after quantum state. ∎

In particular, Corollary 3.13 shows that C_q is independent of the chosen quantum model and can be considered as the sets of correlations arising from any quantum strategy on finite-dimensional Hilbert spaces.

Today, we can consider each Tsirelson problem to have been resolved in the negative. After the initial results by William Slofstra in [18], where it was shown that $C_{qs} \neq C_{qc}$ and $C_q \neq C_{qc}$, Slofstra proceeded to show in [19] that C_{qs} is not a closed set, and therefore $C_{qs} \neq C_{qa}$. In [7], Coladangelo and Stark showed $C_q \neq C_{qs}$. Finally, a recent preprint by Ji, Natarajan, Vidick, Wright, and Yuen [13] resolved the last standing Tsirelson problem by showing that $C_{qa} \neq C_{qc}$.

We might ask ourselves whether there is also a Tsirelson problem asking if $C_{qc} = \overline{C_{qc}}$. However, it is possible to show that C_{qc} is closed. We here give a proof of this statement and additionally also show that C_{qc} is convex.

Proposition 3.14. *The set C_{qc} of commuting-operator correlations is closed.*

Proof. Let $(P_a^x)_a$ and $(Q_b^y)_b$ be the projective valued measures of Alice and Bob, on the Hilbert space $\mathcal{H}$, and such that $[P_a^x, Q_b^y] = 0$ for all a, b. Then there is a $*$-homomorphism from a universal C^*-algebra to a C^*-algebra $\mathcal{A}$ such that $(P_a^x)_a$ and $(Q_b^y)_b$ are images of elements in this universal C^*-algebra.

Now let (p_i) be a sequence of correlations in C_{qc} converging to some p, where $p_i = \langle\psi_i| P_a^x Q_b^y |\psi_i\rangle$ and unit vectors $\psi_i \in \mathcal{H}_i$ in Hilbert spaces $\mathcal{H}_i$. Universality of $\mathcal{A}$ implies existence of $*$-representations π_i on $\mathcal{H}_i$ for all i. For such π_i, consider the states

$$\begin{aligned} \varphi_i : \mathcal{A} &\to \mathbb{C} \\ T &\mapsto \langle \pi_i(T)\psi_i, \psi_i\rangle \,. \end{aligned}$$

Since the state space of a unital C^*-algebra is weak-$*$ compact by Proposition 2.9, there is some cluster point φ of the sequence (φ_i). The GNS construction now yields a $*$-representation π of $\mathcal{A}$ on a Hilbert space $\mathcal{H}$ and a vector $\psi \in \mathcal{H}$ such that $\varphi(T) = \langle \pi(T)\psi, \psi\rangle$ for all $T \in \mathcal{A}$. In particular, since π is unital and both $(P_a^x)_a$ and $(Q_b^y)_b$ are PVMs in $\mathcal{A}$, it follows that $(\pi(P_a^x))_a$ and $(\pi(Q_b^y))_b$ also are PVMs, and we find that $p = \langle\psi|\, \pi(P_a^x)\pi(Q_b^y)\, |\psi\rangle \in C_{qc}$. ∎

Proposition 3.15. *The set C_{qc} of correlations is convex.*

Proof. Let $p_1 = \langle\psi_1| P_a^x Q_b^y |\psi_1\rangle$ and $p_2 = \langle\psi_2| R_a^x S_b^y |\psi_2\rangle$ be correlations with commuting PVMs $P_a^x, Q_b^y \in \mathcal{B}(\mathcal{H})$ and $R_a^x, S_b^y \in \mathcal{B}(\mathcal{K})$, and unit vectors ψ_1 and ψ_2 in the respective Hilbert spaces. We want to show that for $0 \leq t \leq 1$ it holds that $tp_1 + (1-t)p_2 \in C_{qc}$. To this end, consider

$$P_a^x \oplus R_a^x \quad \text{and} \quad Q_b^y \oplus S_b^y,$$

both commuting PVMs in the Hilbert space $\mathcal{H} \oplus \mathcal{K}$. Take also the unit vector $\psi = \sqrt{t}\psi_1 \oplus \sqrt{1-t}\psi_2 \in \mathcal{H} \oplus \mathcal{K}$. This yields the desired correlation $tp_1 + (1-t)p_2$ in C_{qc}, and the result follows. ∎

In the remainder of this text, we will concern ourselves with the details of the proof that $C_{qs} \neq C_{qc}$, as presented originally in [18]. This is the Tsirelson problem which is the closest to the original problem as posed by Tsirelson.

4. Linear games

The focus of our endeavors will be to examine a specific class of non-local games, called linear system games. These games have been studied in [6] and [5]. Notably, these games are related to binary constraint systems, i.e., linear systems of binary variables in which the constraints are binary-valued functions on a subset of the variables. However, this text will not explore this connection to the theory further. Instead, we will associate linear system games with binary linear systems in the traditional sense, where this interpretation is helpful.

In this section, we will present the main result of the text – the embedding theorem, which ultimately yields a separation of C_{qs} and C_{qc}.

§ 4.1. Linear system games. We start by introducing the notion of a binary linear system:

Definition 4.1. A *binary linear system* is a tuple (A, b) where $A \in \mathbb{Z}_2^{m\times n}$ and $b \in \mathbb{Z}_2^m$.

Although we choose to define a binary linear system as a tuple, the reader easily recognizes that such a system corresponds to a usual system of linear equations in m binary variables with coefficients in $\mathbb{Z}_2$.

Binary linear systems give rise to a class of non-local games. For such a non-local game, the existence of a perfect quantum strategy is completely determined by structural properties of the corresponding solution group, as we will see in Theorem 4.5.

Definition 4.2. Given a binary linear system (A, v) with $A \in \mathbb{Z}_2^{m\times n}$, we can define a *linear system non-local game* with parameters

- $[n_A] = [m]$, $[n_B] = [n]$,
- $[m_A] = span\{e_1, \ldots, e_n\} = \mathbb{Z}_2^n$, $[m_B] = \mathbb{Z}_2$,
- π a uniform probability distribution on $[n_A] \times [n_B]$, and
- $V : [m_A] \times [m_B] \times [n_A] \times [n_B] \to \mathbb{Z}_2$ defined by

$$V(a, b \mid x, y) = \begin{cases} 1 \text{ if } A_{xi} = a_i \text{ for all } i, a_y = b, \text{ and } \sum_{i=1}^n a_i = v_x, \\ 0 \text{ otherwise.} \end{cases}$$

In other words, the game takes place as follows:

1. The referee uniformly at random selects the index of a row, x, and a column, y, of A. The row index is distributed to Alice, and the column index to Bob.
2. Alice returns an assignment of values to the variables in the row x.
3. Bob returns an assignment of the variable in column y.

The players win if the assignments are consistent and if Alice's assignment of variables satisfies the xth equation.

Definition 4.3. To a binary linear system (A, b) with $A \in \mathbb{Z}_2^{m\times n}$ we associate a *solution group* $\Gamma(A, b)$ with generators $\{x_1, \ldots, x_n, J\}$ satisfying the relations:

1. $x_i^2 = 1$ for all $1 \leq i \leq n$ and $J^2 = 1$,
2. $[x_i, J] = 1$ for all $1 \leq i \leq n$,
3. $[x_i, x_j] = 1$ for all pairs i, j such that $A_{ki} \cdot A_{kj} = 1$ for some $1 \leq k \leq m$,
4. $\prod_{i=1}^{n} x_i^{A_{ki}} = J^{b_k}$ for all $1 \leq k \leq m$.

In the context of viewing (A, b) as a linear system, $Ax = b$, we can identify the vector x with the generators $x_1, \ldots, x_n$ of Γ.

Note that the solution group is a finitely-presented group generated by involutions with a distinguished central element J of order two. Furthermore, a pair of generators are commuting if the corresponding variables occur in the same equation in the binary linear system.

Example 4.4. We now again return to the CHSH game seen in Example 3.4 and 3.9. We can realize the CHSH game as a linear system non-local game in the following way:

$$x_1 \oplus x_2 = 0 \qquad x_1 \oplus x_2 = 1.$$

Say Alice is assigned the ith equation and Bob the jth variable. This game is indeed equivalent to the CHSH game in the sense that it produces the same non-zero correlations: For the proposed linear system non-local game, the output set is $\{0, 1\}^2 \times \{0, 1\}$. However, we can reasonably assume that Alice always selects a satisfying assignment of variables in her equation so that her response is completely determined by her assignment of a single variable, otherwise the players can by definition of V not win the game. Thus, the output set is equal to the input set, which is $\{0, 1\}^2$, rendering the game equivalent to the CHSH game presented in the previous section.

The solution group is

$$\begin{aligned}\Gamma = \langle x_1, x_2, J \mid & x_1^2 = x_2^2 = J^2 = 1, \\ & [x_1, J] = [x_2, J] = [x_1, x_2] = 1, \\ & x_1 x_2 = 1, x_1 x_2 = J\rangle,\end{aligned}$$

which is seen to be $\mathbb{Z}_2$ since the two final relations yield that $J = 1$ and furthermore that $x_1 = x_2^{-1} = x_2$.

We now state the main result of this section, which gives a relation between the solution group of a linear system non-local game and the existence of perfect quantum strategies. The proof can be found in [6] and [5].

Theorem 4.5. *Let (A, b) be a binary linear system over $\mathbb{Z}_2$, let $\mathcal{G}$ be the associated linear system non-local game, and let Γ be its solution group. Then*

- *$\mathcal{G}$ has a perfect quantum commuting-operator strategy if and only if $J \neq 1$ in Γ.*
- *$\mathcal{G}$ has a perfect quantum tensor-product strategy if and only if $\mathcal{G}$ has a perfect finite-dimensional quantum strategy, and this happens if and only if Γ has a finite-dimensional representation π with $\pi(J) \neq \mathbb{1}$.*

By the theorem and the result of Example 4.4 we can conclude that the CHSH game indeed lacks a perfect quantum strategy since $J = 1$.

§ 4.2. The embedding theorem & main results. In light of Theorem 4.5 to show that $C_{qs} \neq C_{qc}$ it suffices to construct a linear system non-local game such that the distinguished central element of the associated solution group is non-trivial yet has a trivial image under every finite-dimensional representation of the group.

The *existence* of such a game will follow as a consequence of the so-called embedding theorem, which we now state.

Theorem 4.6 (Embedding Theorem [18])**.** *Let G be a finitely presented group with central element $J' \in G$ such that $(J')^2 = 1$. Furthermore, let $g_1, \ldots, g_n$ be a sequence of elements in G such that $g_i^2 = 1$ for all $1 \leq i \leq n$. Then there is a binary linear system (A, b) and a homomorphism $\phi : G \to \Gamma(A, b)$ such that ϕ is an embedding satisfying $\phi(J') = J$ and $\phi(g_i) = x_i$ for all $1 \leq i \leq n$.*

In other words, for a finitely presented group G of this kind, there is an embedding of G into a solution group, and given a sequence of involutions in G this embedding maps them to the generators. As we will see later, given G, it is possible to construct the binary linear system (A, b) and map ϕ embedding G into $\Gamma(A, b)$.

For now, we will postpone the proof of Theorem 4.6 until Section 4.3, where we will break it down into three major steps. We now present the two main consequences of this theorem, along with their proofs. The reader may consult Section 2.5 for the necessary group-theoretical results.

Corollary 4.7 ([18])**.** *There is a linear system non-local game which has a perfect commuting-operator strategy, but which does not have a perfect tensor-*

product strategy.

Proof. Suppose G is a finitely presented group with a non-trivial central element J' of order 2, such that $\pi(J') = \mathbb{1}$ for every finite-dimensional representation π of G. We will see shortly that examples of such groups exist. By the embedding theorem, there exists an embedding of G in a solution group Γ identifying J' with J.

It follows that $J \neq 1$ so by Theorem 4.5 the associated binary linear game has a perfect quantum commuting-operator strategy. Furthermore, if π is a finite-dimensional representation of Γ, then $\pi(J) = \pi_{|G}(J') = \mathbb{1}$ so the same game has no perfect quantum tensor-product strategy by Theorem 4.5.

We now show that such a group indeed exists. To this end, consider Higman's group H_0 as defined in (2.5.1). Let $H = H_0 \times \mathbb{Z}_2$ and let J be the generator of $\mathbb{Z}_2$ in the direct product. Recall by Proposition 2.30 that the generators of Higman's group have infinite order. Consider one such generator a of H_0 and let G be the HNN extension of H relative to the automorphism of $\langle a, J\rangle \cong \mathbb{Z} \times \mathbb{Z}_2$ where $J \mapsto J$ and $a \mapsto aJ$. Then, H is a subgroup of G, and J is non-trivial in G.

Finally, if π is a finite-dimensional representation of G, then $\pi_{|H_0}$ is trivial by Proposition 2.31, so $\pi(a) = \mathbb{1}$. Thus, $\pi(J) = \pi([x, a]) = \mathbb{1}$. ∎

From the proof of Corollary 4.7 we conclude that any finitely-generated group of infinite order with no non-trivial finite quotients can be used to give a separation of C_{qs} and C_{qc}.

The remainder of the text will now be concerned with the proof of the embedding theorem.

§ 4.3. Construction of the embedding. In order to prove the embedding theorem, we are seeking to understand better finitely presented groups that have a central element of order two and which further have a sequence of generators of order two. We will here study such groups and break down the proof of Theorem 4.6 in three steps, culminating in Proposition 4.19 which we will ultimately prove in Section 6.

Definition 4.8. A group G with distinguished central element J_G of order at most two is called a *group over* $\mathbb{Z}_2$. Given G_1 and G_2, two groups over $\mathbb{Z}_2$, a homomorphism $G_1 \to G_2$ such that $J_{G_1} \mapsto J_{G_2}$ is called a *morphism over* $\mathbb{Z}_2$. An injective morphism over $\mathbb{Z}_2$ is called an *embedding over* $\mathbb{Z}_2$.

Based on this definition, we recognize that solution groups are groups over $\mathbb{Z}_2$. In fact, they have slightly more structure, which we will see from the following definition:

Definition 4.9. Let S be a set and define $\mathcal{F}_2(S) = \langle S \mid s^2 = 1, s \in S \rangle$. A *presentation by involutions over* $\mathbb{Z}_2$ of a group G is a set of generators S and relations $R \subset \mathcal{F}_2(S) \times \mathbb{Z}_2$ such that $G \cong \mathcal{F}_2(S) \times \mathbb{Z}_2/(R)$, where (R) is the normal subgroup generated by R. Such presentations will be denoted by $\mathrm{Inv}\,\langle S \mid R \rangle$.

Note that a group G presented by involutions over $\mathbb{Z}_2$ can be regarded as a group over $\mathbb{Z}_2$ with distinguished central element J_G, the image of the generator of the $\mathbb{Z}_2$-factor in $\mathcal{F}_2(S) \times \mathbb{Z}_2$. We consider a few examples of such groups:

Example 4.10. We note that any group of the form $G \times \mathbb{Z}_2$ is a group over $\mathbb{Z}_2$. One simple example is $\mathbb{Z} \times \mathbb{Z}_2$. However, this group is not a group presented by involutions over $\mathbb{Z}_2$ since not all its generators are involutions.

Example 4.11. One class of groups that will easily lend itself to examples of groups presented by involutions is the class of Coxeter groups. These are groups of the form $G = \langle s_1, \ldots, s_n \mid (s_i s_j)^{m_{ij}} = 1 \rangle$, where $m_{ii} = 1$ and $m_{ij} \geq 2$ for $i \neq j$. If $m_{ij} = \infty$ it is taken to mean that there is no relation of the form $(s_i s_j)^{m_{ij}}$. Some familiar examples of Coxeter groups include symmetric groups and dihedral groups.

Consider the Coxeter group

$$G = \left\langle x_1, x_2, x_3, x_4 \mid x_i^2 = 1 \text{ for } 1 \leq i \leq 4, (x_1 x_2)^2 = (x_2 x_3)^2 = (x_3 x_4)^2 = 1 \right\rangle.$$

This is a group presented by involutions over $\mathbb{Z}_2$ with $J = 1$.

Given a set S, recall that $\mathcal{F}(S)$ consists of all words with symbols in $\{s, s^{-1} \mid s \in S\}$, in other words, an element $r \in \mathcal{F}(S)$ is of the form $s_1^{a_1} \ldots s_n^{a_n}$ where $a_i \in \{\pm 1\}$ for all $1 \leq i \leq n$. If it holds that $a_i = a_{i+1}$ whenever $s_i = s_{i+1}$, then the word is said to be *reduced*. Furthermore, a reduced word in which $a_n = a_1$ whenever $s_n \neq s_1$ is said to be *cyclically reduced*.

We analogously define *reduced* and *cyclically reduced* words in $\mathcal{F}_2(S)$. A set of relations R is said to be *cyclically reduced* if every $r \in R$ is cyclically reduced.

Now, to restate the embedding theorem in terms of this new terminology, we wish to prove that every finitely presented group over $\mathbb{Z}_2$ embeds in a solution group. As mentioned previously, the proof will be done in three steps; (1) every finitely presented group over $\mathbb{Z}_2$ embeds in a group presented by involutions over $\mathbb{Z}_2$, (2) every finitely presented group over $\mathbb{Z}_2$ generated by involutions naturally embeds in a presentation of involutions over $\mathbb{Z}_2$ of a specific kind (which we will define shortly), and finally (3) every group with a presentation of this kind embeds in a solution group.

Proposition 4.12 ([18])**.** *Let G be a group over $\mathbb{Z}_2$ with finite presentation $\langle S \mid R \rangle$, where $S = \{s_1, \ldots, s_n\}$, and with representative $W_G \in \mathcal{F}(S)$ of J_G.*

Further, let T be a set of indeterminates obtained by doubling all s_i, i.e., $T = \{z_{i1}, z_{i2} \mid 1 \le i \le n\}$, and choose integers $k_i \ge 1$ for all $1 \le i \le n$. Finally, let $\phi : \mathcal{F}(S) \to \mathcal{F}_2(S) \times \mathbb{Z}_2$ be the morphism defined by $s_i \mapsto (z_{i1}z_{i2})^{k_i}$. Then, the induced morphism

$$\phi : G \to K := Inv\langle T \mid R'\rangle \quad \text{where } R' = \{\phi(r) \mid r \in R\} \cup \{J_K\phi(W_G)\}$$

is an embedding over $\mathbb{Z}_2$. Furthermore, if $R \cup \{W_G\}$ is cyclically reduced, then so is R'.

Proof. Let $m_1, \ldots, m_n$ be the orders of $s_1, \ldots, s_n$ in G, respectively. For each $0 \le r \le n$ define the group

$$\begin{aligned} K_r = \langle S \cup \{z_{11}, z_{12}, \ldots, z_{r1}, z_{r2}, J_G\} \mid R \cup \{z_{ij}^2 = [z_{ij}, J_G] = 1 \mid 1 \le i \le r, j = 1, 2\} \\ \cup \{s_i = (z_{i1}z_{i2})^{k_i}\} \\ \cup \{J_G = W_G\}\rangle. \end{aligned}$$

We see that $K_n \cong K$ since there is an equivalence of the presentations, by making the identifications $s_i \mapsto \phi(s_i)$, $z_{ij} \mapsto z_{ij}$, and $J_G \mapsto J_K$.

We now argue by induction that there is an inclusion $G \to K_n \cong K$. First note that $G \cong K_0$. Suppose that the natural map $G \to K_{i-1}$ is an inclusion and let

$$D_i := \left\langle z_{i1}, z_{i2} \mid z_{i1}^2 = z_{i2}^2 = (z_{i1}z_{i2})^{k_i m_i} = 1 \right\rangle,$$

be the dihedral group of order $2k_im_i$, which might be infinite if m_i is infinite. If $J_G \notin \langle s_i\rangle$, then $\langle s_i, J_G\rangle \cong \mathbb{Z}_{m_i} \times \mathbb{Z}_2$, and we recognize K_i as the amalgamated product of K_{i-1} with $D_i \times \mathbb{Z}_2$ over $\langle s_i, J_G\rangle$, where $s_i \in G \subseteq K_{i-1}$ is identified with $(z_{i1}z_{i2})^{k_i}$ and J_G with the generator of $\mathbb{Z}_2$ in $D_i \times \mathbb{Z}_2$.

On the other hand, if $J_G \in \langle s_i\rangle$, then $J_G = s_i^a$ where $a = 0$ or $a = m_i/2$, since J_G is itself of order 2. In this case, s_i is again identified with $(z_{i1}z_{i2})^{k_i}$ and we also note that $J_G = s_i^a \mapsto (z_{i1}z_{i2})^{k_i a}$ is central in D_i both if $a = 0$ and if $a = m_i/2$. So we recognize K_i as the amalgamated product of K_{i-1} with D_i over $\langle s_i\rangle$. Thus, the natural map $G \to K_i$ is an inclusion, and it follows that $G \to K_n$ is indeed an inclusion.

Finally, since ϕ is a morphism, it follows that if $R \cup \{W_G\}$ is cyclically reduced, then so is R', as claimed. ∎

Example 4.13. In Example 4.10 we noticed that $G = \mathbb{Z} \times \mathbb{Z}_2 = \langle a, J \mid J^2 = 1, [a, J] = 1\rangle$ is not a group presented by involutions. By the preceding proposition, it is possible to embed G over $\mathbb{Z}_2$ into a group

presented by involutions, namely, it we have an embedding of G into the group

$$\mathrm{Inv}\left\langle z_{a1}, z_{a2}, z_{J1}, z_{J2} \mid (z_{J1}z_{J2})^4 = [(z_{a1}z_{a2})^2, (z_{J1}z_{J2})^2] = J_K(z_{J1}z_{J2})^2 = 1\right\rangle,$$

by taking $k_a = k_J = 2$ in the construction of Proposition 4.12. Since G contains J explicitly as a generator in the presentation of G, the resulting construction is slightly more complicated than necessary. Although it is possible to remediate this in the above proof, there is little use for this as we will exclusively focus on groups for which this is not the case.

Before continuing with the second step towards the proof of the embedding theorem, we introduce the notion of a collegial presentation by involutions.

Definition 4.14. Let $r \in \mathcal{F}_2(S) \times \mathbb{Z}_2$ be an element written as the reduced word $J^a s_1 \dots s_n$. The *multiplicity* of $s \in S$ in r is

$$\mathrm{mult}(s; r) = |\{1 \le i \le n \mid s_i = s\}|.$$

Two symbols $s \neq t \in S$ are said to be *adjacent* in r if $\{s, t\} = \{s_i, s_{i+1}\}$ or $\{s, t\} = \{s_1, s_n\}$.

Definition 4.15. A presentation $\mathrm{Inv}\langle S \mid R\rangle$ by involutions over $\mathbb{Z}_2$ is said to be *collegial* if

1. the presentation is finite and cyclically reduced,
2. $R \cap \{1, J\} = R \cap J \times S = \emptyset$, and
3. if $\mathrm{mult}(s; r_0)$ is odd for some $r_0 \in R$ and t is adjacent to s in some $r_1 \in R$, then $\mathrm{mult}(t; r')$ is even for all $r' \in R$.

Of the groups presented by involutions we have seen so far, we note that the Coxeter groups studied in Example 4.11 are collegial as the multiplicities of all generators in every relation are even.

Example 4.16. For any $n \in \mathbb{N}$, consider the dihedral group $D_{2n} = \left\langle s, t \mid s^2 = t^2 = (st)^{2n} = 1\right\rangle$, which is a group over $\mathbb{Z}_2$ with distinguished central element $(st)^n$. The group can thus be presented by involutions as $\mathrm{Inv}\left\langle s, t \mid (st)^{2n} = 1\right\rangle$. This presentation is collegial for all n, and we will return to this example in future sections.

Lemma 4.17. *In a collegial presentation of involutions over $\mathbb{Z}_2$, every relation has length at least four.*

Proof. Let $r = J^a s_1 \dots s_n$ be a relation of a collegial presentation of involutions over $\mathbb{Z}_2$. By property (2), the length of r must be at least two. Furthermore, by property (1), relations of the form $J^a s_1^2 s_2$ and $J^a s_1 s_2^2$ are excluded since they are not cyclically reduced. Lastly, relations of the form $J^a s_1 s_2$ and $J^a s_1 s_2 s_3$ are excluded by property (3). Thus, it must be that $n \ge 4$. ∎

This discussion leads us to the second step toward proving the embedding theorem, in which we show that finitely presented groups over $\mathbb{Z}_2$ with a sequence of involutions can be embedded into a collegial presentation by involutions as follows:

Proposition 4.18 ([18]). *Let G be a finitely presented group over $\mathbb{Z}_2$, with a sequence of elements $g_1, \dots, g_n \in G$ such that $g_i^2 = 1$ for all $1 \leq i \leq n$. Then there is a collegial presentation $Inv\langle S \mid R\rangle$ and an embedding $\phi : G \to Inv\langle S \mid R\rangle$ over $\mathbb{Z}_2$ such that $\phi(g_i) \in S \subset Inv\langle S \mid R\rangle$ for all $1 \leq i \leq n$.*

Proof. We construct a presentation $\langle S_0 \mid R_0\rangle$ of G such that Proposition 4.12 applies in the following way: Let J_G be a generator, $1 \notin R_0$ and for every i take a representative $g_i' \in \mathcal{F}(S_0) \setminus \{1\}$ of g_i, such g_i' can be constructed if necessary by adding a generator z and relation $z = 1$, a representative of the identity. Then, $\langle S_0 \mid R_0\rangle$ is a cyclically reduced presentation for G, where J_G is represented by a cyclically reduced non-identity element of $\mathcal{F}(S_0)$.

Now applying Proposition 4.12 and taking all k_s to be equal to the same even number K, yields an embedding $\phi : G \to \mathrm{Inv}\langle T \mid R'\rangle$, where R' is cyclically reduced. Furthermore, since K is even, the multiplicity of every generator is even in every relation in $\mathcal{F}(S_0)$. Since every relation in R' has length at least four, all the degenerate cases discussed in Lemma 4.17 are excluded, and we conclude that $\mathrm{Inv}\langle T \mid R'\rangle$ is indeed collegial.

Now let $\overline{g_1}, \dots, \overline{g_n}$ be new indeterminates and define $S = T \cup \{\overline{g_1}, \dots, \overline{g_n}\}$ and $R = R' \cup \{\overline{g_i}\phi(g_i') \mid 1 \leq i \leq n\}$, where $\phi : \mathcal{F}(S_0) \to \mathcal{F}_2(T) \times \mathbb{Z}_2$ is the morphism defined in Proposition 4.12. Then, R is cyclically reduced since the $\overline{g_i}$ are new indeterminates and as such, do not appear in $\phi(g_i')$ for any i. Further, none of the $\overline{g_i}$ are adjacent, and $\mathrm{mult}(s; r)$ is even for all $s \in T$ and $r \in R$. By definition, no generators are trivial, so it follows that $\mathrm{Inv}\langle S \mid R\rangle$ is collegial. Since $\mathrm{Inv}\langle S \mid R\rangle$ is equivalent to $\mathrm{Inv}\langle T \mid R'\rangle$, the statement follows. ∎

By Proposition 4.18, the proof of the embedding theorem reduces to the following statement:

Proposition 4.19 ([18]). *Let G be a group with a collegial presentation $\mathcal{I} = Inv\langle S \mid R\rangle$. Then, there is a binary linear system $(A_\mathcal{I}, b_\mathcal{I})$ in variables $X_\mathcal{I}$ such that $S \subseteq X_\mathcal{I}$ and the map*

$$\begin{aligned} \mathcal{F}(S) \times \mathbb{Z}_2 &\to \Gamma(A_\mathcal{I}, b_\mathcal{I}) \\ s &\mapsto x_s \end{aligned}$$

descends to an embedding $G \hookrightarrow \Gamma(A_\mathcal{I}, b_\mathcal{I})$ over $\mathbb{Z}_2$.

With this, we are finally ready to prove the embedding theorem. In order to prove Proposition 4.19, a reformulation of the problem in terms of hypergraphs will be immensely helpful, and we will present the necessary theory in the upcoming sections before giving the final proof in Section 6.

Proof of Theorem 4.6. Let G be a group over $\mathbb{Z}_2$ with a sequence of elements $g_1, \dots g_n$ such that $g_i^2 = 1$ for all $1 \leq i \leq n$. By Proposition 4.18 there is a collegial presentation $\mathcal{I} = \mathrm{Inv}\langle S \mid R\rangle$ and an embedding $\phi_1 : G \to \mathcal{I}$ over $\mathbb{Z}_2$ such that $\phi_1(g_i) \in S$ for $1 \leq i \leq n$.

Furthermore, by Proposition 4.19, there is an embedding $\phi_2 : \mathcal{I} \to \Gamma(A_\mathcal{I}, b_\mathcal{I})$ over $\mathbb{Z}_2$ such that $\phi_2(s) = x_s$ for all $s \in S$. By the stated properties of ϕ_1 and ϕ_2, the homomorphism $\phi_2 \circ \phi_1$ satisfies the conditions of Theorem 4.6. ∎

5. Hypergraphs, pictures, and constellations

As mentioned in the previous section, proving Proposition 4.19 will require additional machinery – in this case, this includes several graphical concepts such as hypergraphs, pictures, and a particular construction called constellations. In this section, we present the necessary concepts to understand the proof, which is later given in Section 6.

We will begin this section by giving the fundamental definitions of hypergraphs before translating the main results we have seen so far in terms of binary linear system games in this new terminology.

§ 5.1. Definitions. Hypergraphs are generalizations of traditional graphs; in a hypergraph, an edge is allowed to connect more than two vertices. This section introduces the concept of hypergraphs needed to draw the connection to linear system games. We start by making the following definition:

Definition 5.1. A *hypergraph* is a tuple $H = (V, E)$, where V is a set of *vertices*, and E is a multiset of *edges* connecting vertices. A vertex v and an edge e are considered *incident* if $v \in e$. The *degree* of a vertex is the number of edges incident to it. Finally, the *order* of an edge $e \in E$ is given by $|e|$.

Notice that a hypergraph in which $|e| = 2$ for every $e \in E$ is a graph in the traditional sense. As usual, we say that a hypergraph is *simple* if it has no loops or repeated edges, i.e., no edges connecting only a single vertex or edges given by the same sets of vertices. Sometimes, our presentation will benefit from listing the edges separately, not as a multiset of elements from V, and then describe the incidences between vertices and edges. Note that it is possible to pass between these presentations as follows: Given a vertex set V and a multiset E of size n containing subsets of vertices, each edge is described by a unique element in E so we can enumerate the edges and

construct $\{e_1, \ldots, e_n\}$. Then, V and $\{e_1, \ldots, e_n\}$ correspond to the vertex- and edge set in the new formalism, with the incidence relation for each e_i given by its corresponding element in E

The notion of an incidence matrix will be helpful to describe compactly the structure of a hypergraph:

Definition 5.2. Let $H = (V, E)$ be a hypergraph with enumerations $V = \{v_1, \ldots, v_m\}$ and $E = \{e_1, \ldots, e_n\}$. The *incidence matrix* of H is the matrix $A \in \mathbb{Z}^{m \times n}$ in which a_{ij} is given by the degree of incidence between v_i and e_j.

Given the incidence matrix A of a hypergraph, the degree of a vertex v_i can be calculated as $|v_i| = \sum_{j=1}^{n} a_{ij}$. Likewise, we find that the order of an edge e_j can be calculated as $|e_j| = \sum_{i=1}^{m} a_{ij}$. We now define the correspondence between hypergraphs and binary linear systems by the definition of vertex labelings:

Definition 5.3. Let $H = (V, E)$ be a hypergraph. A function $b : V \to \mathbb{Z}_2$ is called a $\mathbb{Z}_2$-vertex labeling of H.

Thus, given a binary linear system (A, b), we get a $\mathbb{Z}_2$-vertex labeling of a hypergraph H with incidence matrix A, whose edges correspond to the variables of the binary linear system, and whose vertices correspond to the constraints.

Example 5.4. Naturally, our first example of a hypergraph and the correspondence to binary linear systems, and by extension also to linear system games, is to consider the CHSH game, which is familiar from previous sections.

Recall that the CHSH game is given as a linear system non-local game associated with

$$x_1 \oplus x_2 = 0 \quad x_1 \oplus x_2 = 1.$$

This yields a non-simple hypergraph $H = (V, E)$ with $V = \{v_1, v_2\}$, and $E = \{\{v_1, v_2\}, \{v_1, v_2\}\}$. Graphically, we may represent this as in Figure 2.

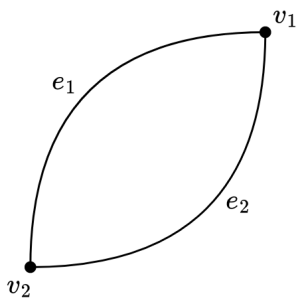

Figure 2: Hypergraph corresponding to the CHSH game.

Thus, the notion of a solution group, as seen in Definition 4.3, can also be defined for a hypergraph $H = (V, E)$ with a $\mathbb{Z}_2$-vertex labeling b, through the correspondence of hypergraphs and linear system non-local games. We then denote the solution group by $\Gamma(H, b)$.

In our figures of hypergraphs, we adopt the presentation of [18] and draw edges of order two as lines, similar to traditional graphs, while edges of order not equal to two are drawn as shaded regions.

Example 5.5. A more interesting hypergraph is given in Figure 3. The corresponding incidence matrix is given by

$$A = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Given a vertex labeling such that $b(v_1) = 1$ and $b(v_2) = 0$ we obtain the solution group

$$\begin{aligned} \Gamma(A, b) = \langle x_1, x_2, x_3, J \mid J^2 = x_i^2 = [x_i, J] = 1 \text{ for all } 1 \leq i \leq 3, \\ [x_1, x_2] = [x_2, x_3] = 1, \\ x_1^2 x_2 = J, x_2 x_3 = 1 \rangle. \end{aligned}$$

The relation $x_1^2 x_2 = J$ shows that $x_2 = J$, and since $x_2 x_3 = 1$ it follows that the group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

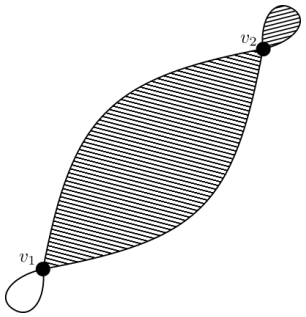

Figure 3: Hypergraph on two vertices from Example 5.5.

§ 5.2. Translation of results. We are now ready to restate the major results we have seen so far, this time in terms of hypergraphs, starting with the embedding theorem (Theorem 4.6).

Theorem 5.6 (Embedding Theorem)**.** *Let G be a finitely presented group with central element $J' \in G$ such that $(J')^2 = 1$. Furthermore, let $g_1, \ldots, g_n$ be a sequence of elements in G such that $g_i^2 = 1$ for all $1 \leq i \leq n$. Then there is a hypergraph $H = (V, E)$, a vertex labeling $b : V \to \mathbb{Z}_2$, a sequence of edges $e_1, \ldots, e_n \in E$, and a homomorphism $\phi : G \to \Gamma(H, b)$ such that ϕ is an embedding, $\phi(J') = J$, and $\phi(g_i) = x_i$ for all $1 \leq i \leq n$.*

Also the final step of the proof of the embedding theorem, Proposition 4.19 can be restated in terms of hypergraphs:

Proposition 5.7. *Let G be a group with collegial presentation $\mathcal{I} = Inv\langle S \mid R\rangle$. Then, there is a hypergraph $W := W(\mathcal{I})$ and a vertex labeling $b := b(\mathcal{I})$ such that $S \subset E(W)$, and the map*

$$\begin{aligned} \mathcal{F}(S) \times \mathbb{Z}_2 &\to \Gamma(W, b) \\ s &\mapsto x_s \end{aligned}$$

descends to an embedding $G \hookrightarrow \Gamma(W, b)$ over $\mathbb{Z}_2$.

From this, the proof of Theorem 5.6 follows analogously as the proof of Theorem 4.6.

The hypergraph W is the first construction toward the proof of Proposition 4.19, or its equivalent reformulation in Proposition 5.7, and is worth investigating in detail. To this end, we make the following definition:

Definition 5.8. Let $\mathcal{I} = \mathrm{Inv}\langle S \mid R\rangle$ be a presentation by involutions over $\mathbb{Z}_2$, where $R = \{r_1, \ldots, r_m\}$ and $r_i = J^{p_i} s_{i1} \ldots s_{in_i}$ has length n_i, and $p_i \in \mathbb{Z}_2$. The *wagon wheel hypergraph*, $W(\mathcal{I})$, is the simple hypergraph with vertex set

$$V = \{(i, j, k) \mid 1 \le i \le m, j \in \mathbb{Z}_{n_i}, 1 \le k \le 3\},$$

and edge set

$$E = S \cup \{a_{ij}, b_{ij}, c_{ij}, d_{ij} \mid 1 \le i \le m, j \in \mathbb{Z}_{n_i}\},$$

satisfying the following incidence relations:

- $s \in S$ is incident with $(i, j, 1)$ if and only if $s_{ij} = s$,
- a_{ij} is incident with $(i, j-1, 2)$ and $(i, j, 1)$,
- b_{ij} is incident with $(i, j, 1)$ and $(i, j, 2)$,
- c_{ij} is incident with $(i, j, 2)$ and $(i, j, 3)$, and
- d_{ij} is incident with $(i, j-1, 3)$ and $(i, j, 3)$.

Often, we omit $\mathcal{I}$ from the notation when the context is clear.

Note that for this hypergraph, W, we find that $|V| = 3M$ and $|E| = |S| + 4M$, where $M = \sum_{i=1}^{m} n_i$. For all $1 \le i \le m$ we also define the sets

$$V_i = \{(i, j, k) \mid j \in \mathbb{Z}_{n_i}, 1 \le k \le 3\} \quad \text{and} \quad E_i = \{a_{ij}, b_{ij}, c_{ij}, d_{ij} : j \in \mathbb{Z}_{n_i}\},$$

so that the sets V_i partition V, and the sets E_i together with S partition E.

The name of the graph reflects the shape given by its incidence relations. For each relation in $\mathcal{I}$, we get a "wheel" in the graphical representation of

$W(\mathcal{I})$. Edges corresponding to the generators contained in the relations connect the wheels together. Furthermore, an edge $s \in S$ is incident to exactly $\sum_{i=1}^{m} \text{mult}(s; r_i)$ vertices in W. The edges d_{ij} form the inner cycle of the wheel corresponding to r_i, while the a_{ij} and b_{ij} together form the outer cycle. The c_{ij}, on the other hand, form the "spokes" connecting the inner and outer cycle. We will now see our first example of such a graph.

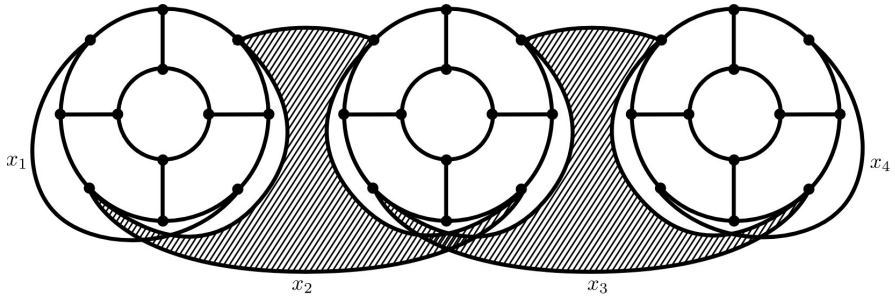

Figure 4: Wagon wheel hypergraph of Example 5.9

Example 5.9. Recall the Coxeter group from Example 4.11. Noting that $J = 1$ for this group, we can construct its wagon wheel hypergraph, which is pictured in Figure 4.

Interestingly, we find a more general relationship between the diagrams of right-angled Coxeter groups, such as G above, and their corresponding wagon wheel hypergraphs. Recall that to a given right-angled Coxeter group with generators S, there corresponds a graph with vertex set S and such that (x, y) is an edge if and only if $(xy)^2 = 1$ is a relation in the group. We can easily convert this graph into the corresponding wagon wheel hypergraph by making the following identifications:

Let G be a right-angled Coxeter group. Then

- edges in its graph correspond to wheels in $W(G)$, and
- vertices in its graph correspond to hyperedges in $W(G)$ connecting the wheels.

Since the commuting relations are all of length four, the wheel in $W(G)$ will have an inner cycle of four vertices. Furthermore, the order of an hyperedge $e \in W(G)$ corresponding to the vertex v in the graph representing G is equal to $2 \cdot \deg(v)$.

A few examples of this correspondence can be seen in Figure 5 for right-angled Coxeter groups with two and three generators.

The particular vertex labeling of Theorem 5.6 for W can be defined as follows:

Definition 5.10. Let $W(\mathcal{I})$ be a wagon wheel hypergraph. An *$\mathcal{I}$-labeling* of W is a $\mathbb{Z}_2$-vertex labeling $b : V \to \mathbb{Z}_2$ such that

$$|b^{-1}(1) \cap V_i| \equiv p_i \pmod 2$$

for all $1 \leq i \leq m$.

In fact, any $\mathcal{I}$-labeling can be chosen in the construction by Proposition 5.7:

Proposition 5.11. *Let b and b' be two $\mathcal{I}$-labelings of W. Then there is an isomorphism $\Gamma(W, b) \to \Gamma(W, b')$.*

Proof. Let $H = (V, E)$ be a hypergraph with incidence matrix A and vertex labeling b. Given $e \in E$, let b' be the vertex labeling $b'(v) = b(v) + A_{ve}$. Then there is an isomorphism

$$\begin{aligned} \Gamma(H, b) &\to \Gamma(H, b') \\ x_f &\mapsto \begin{cases} x_f \text{ if } f \neq e, \\ Jx_e \text{ otherwise.} \end{cases} \end{aligned}$$

Note that for a wagon wheel hypergraph W, between any two vertices of $W_i \subset W$ there exists a path of edges of order two. So, given two $\mathcal{I}$-labelings b and b' of W it is possible to transform $b|_{V_i}$ to $b'|_{V_i}$ through a sequence of steps, fixing an edge $e \in E(W_i)$ along this path, as shown above. Because $|b^{-1}(1) \cap V_i| \equiv |(b')^{-1}(1) \cap V_i| \mod 2$ there is no need to flip the labels along a path between distinct wheels W_i and W_j. ∎

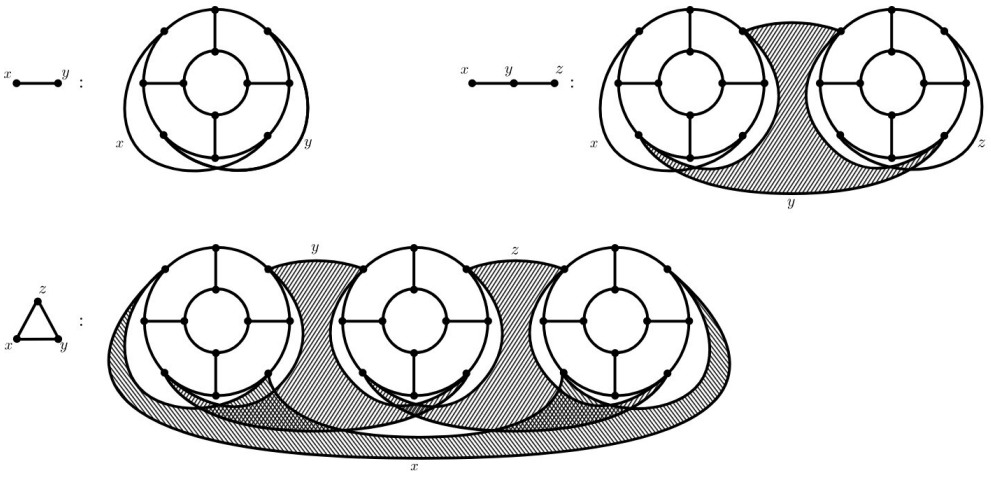

Figure 5: Diagrams and the corresponding wagon wheel hypergraphs for right angled Coxeter groups.

§ 5.3. Pictures. We now turn to consider another graphical concept – this time so-called pictures. As we will see, given a group presented by involutions, a corresponding picture can be created (Definition 5.16). Thus solution groups, and by extension, also hypergraphs can be represented in this way (Definition 5.19). This is the primary technical construct needed for the proof of Proposition 4.19. The main result of this section is the so-called Van Kampen lemma, which describes a necessary and sufficient criterion for when a word in a group presented by involutions is trivial based on the properties of a picture constructed from the group in question. This thus solves a special case of the word problem for groups.

Recall that an infinitely differentiable function $f : A \to \mathbb{R}$ is said to be *real analytic* if for every $x \in A$ there is a Taylor series converging to f in a neighborhood of x. Let $a < b$ and consider the interval $[a, b]$. We will refer to the image of a real analytic function γ on $[a, b]$ to either the plane or the sphere as a *curve*. If $\gamma(s) \neq \gamma(t)$ for all $a \leq s < t \leq b$, except possibly when $s = a$ and $t = b$, we say that γ is *simple*. If $\gamma(a) = \gamma(b)$, then γ is said to be *closed*.

Definition 5.12. A *picture* is a collection $\mathcal{P} = (V, E, \mathcal{D})$, where

- $\mathcal{D}$ is a closed simple region, i.e., a connected region in the plane whose boundary is a simple closed curve,
  - V is a finite collection of points, called *vertices* in $\mathcal{D}$,
  - E is a finite collection of simple curves, called *edges*, in $\mathcal{D}$, and
- for all edges $e \in E$ and points p of e,
  - if e is not closed and p is an endpoint of e, then either $p \in V$, or p belongs to the boundary of $\mathcal{D}$ and is not the endpoint of any other edge,
  - if e is closed and p is an endpoint of e, then p does not belong to the boundary of $\mathcal{D}$,
  - if p is not an endpoint of e, then $p \notin V$, and p does not belong to any other edge or the boundary of $\mathcal{D}$.

If the edge e contains the vertex v, we say that e and v are *incident*. If e contains a point of the boundary of $\mathcal{D}$, then e is said to be *incident with the boundary*. A picture is said to be *closed* if no edges are incident with the boundary of $\mathcal{D}$.

The region $\mathcal{D}$ can be pictured as a disk or square into which E and V are embedded. Alternatively, the boundary of $\mathcal{D}$ can be drawn as a vertex at infinity if we imagine the picture as drawn on a sphere, see Figure 6. Furthermore, for a closed picture we can leave out drawing $\mathcal{D}$ entirely and instead imagine the picture as embedded in the sphere.

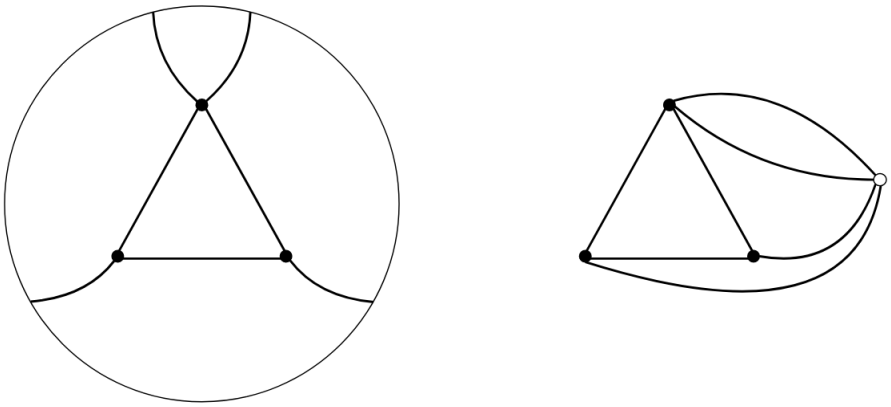

Figure 6: The same open picture presented drawn embedded in a disk and with the boundary as a point at infinity.

We also note that under isotopy, we are allowed to move the boundary of $\mathcal{D}$ and the endpoints of the edges incident with the boundary. We consider two pictures to be equal if they differ up to isotopy.

Definition 5.13. Let $\mathcal{P}$ be a picture. A *simple cycle* in $\mathcal{P}$ is a collection of edges whose union is a simple closed curve.

Definition 5.14. Let $\mathcal{P}$ be a picture in $\mathcal{D}$. An open, connected region $\mathcal{D}'$ of $\mathcal{D}$ not containing any points of $\mathcal{P}$ and such that the boundary of $\mathcal{D}'$ is a union of points of $\mathcal{P}$ and points in the boundary of $\mathcal{D}$ is called a *face* of $\mathcal{P}$. A simple cycle is said to be *facial* if it is the boundary of a face.

Example 5.15. In the right picture seen in Figure 6, the simple cycle consisting of the three edges forming the inner triangle is facial, while neither one of the outer regions is facial cycles, as they all contain points of the boundary of the disk.

After having seen the general definition of pictures and their faces, we are ready to put them to use as a tool to graphically encode group relations, as we will see in Proposition 5.18. In particular, we will define the notion of pictures for groups generated by involutions, and thus by extension, also for hypergraphs.

Consider the group $\mathrm{Inv}\,\langle S \mid R\rangle$. We denote by R^{sym} the set of relations

$$R^{\mathrm{sym}} = \{J^a s_i s_{i+1} \dots s_n s_1 \dots s_{i-1},\, J^a s_i s_{i-1} \dots s_1 s_n \dots s_{i+1} \mid \\ 1 \le i \le n \text{ for } J^a s_1 \dots s_n \in R\},$$

the set of cyclic permutations of the $s_1, \dots, s_n$ and their inverses in every relation $r = J^a s_1 \dots s_n$ in R. Note that for the element corresponding to

$i = 1$, we have that $\{r\}^{\text{sym}} = \{r, J^a s_n \dots s_1\}$. Likewise, for $i = n$, we obtain $\{r\}^{\text{sym}} = \{r, J^a s_n \dots s_1\}$.

Further, a relation $r = J^a s_1 \dots s_n$ is said to be *odd* or *even*, depending on whether a is odd or even, respectively. We denote by r^+ the so-called *even part* of r, i.e. $r^+ = s_1 \dots s_n$. We can consider the *even presentation* of $\text{Inv}\langle S \mid R\rangle$ over $\mathbb{Z}_2$ as $\text{Inv}\langle S \mid R^+\rangle$, where $R^+ = \{r^+ \mid r \in R\}$.

This new terminology will simplify our notation going forward, starting with the following definition:

Definition 5.16. Let $G = \text{Inv}\langle S \mid R\rangle$. A *$G$-picture* is a picture, $\mathcal{P}$, in which each vertex v is labeled by a relation $r(v) \in R$, and every edge e is labeled by a generator $s(e) \in S$, such that if $e_1, \dots, e_n$ is the sequence of edges incident to v, read in counterclockwise order with multiplicity from some starting point, then $s(e_1)s(e_2)\dots s(e_n) \in \{r(v)^+\}^{\text{sym}}$.

The *boundary* of $\mathcal{P}$ is the cyclic word $\text{bd}(\mathcal{P}) = s(e_1)\dots s(e_n)$ over S, where $e_1, \dots, e_n$ is the list of edges incident with the boundary, read in counterclockwise order around the boundary of the disk with multiplicity. If $\mathcal{P}$ is closed we say that $\text{bd}(\mathcal{P}) = 1$, the empty word.

The *sign* of $\mathcal{P}$ is given by

$$\text{sign}(\mathcal{P}) = |\{v \in V(\mathcal{P}) \mid r(v) \text{ is odd}\}| \pmod 2.$$

Example 5.17. We consider again the familiar class of right-angled Coxeter groups, see Figure 7. We see that these pictures have boundary $xyxy$, $xyxzyz$, and $xzyxzy$, respectively.

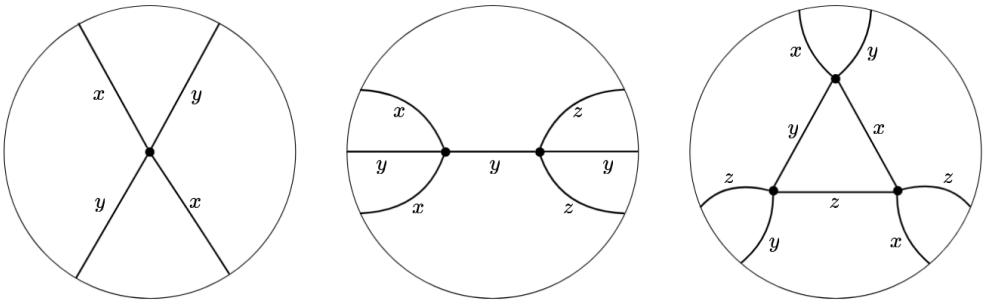

Figure 7: G-pictures corresponding to the right-angled Coxeter groups of Example 5.9.

We are now ready to state the Van Kampen lemma. The lemma originates from [15], where it is given in a slightly different form. Here, we consider a modified version that applies to groups presented by involutions, which then also applies to solution groups.

Proposition 5.18 (Van Kampen lemma)**.** *Let $G = Inv\langle S \mid R\rangle$, $r \in R$, and $a \in \mathbb{Z}_2$. Then, $r = J^a$ in G if and only if there is a G-picture $\mathcal{P}$ with $bd(\mathcal{P}) = r$ and $sign(\mathcal{P}) = a$.*

Proof. First assume that $r = J^a$. We construct a G-picture with boundary and sign as stated above. In what follows, if $w = s_1 \dots s_n$ is a word over S, we let $\overline{w} = s_n \dots s_1$ denote the reverse word over S.

It is true that $r = J^a$ in G if and only if there is a sequence $r_0, \dots, r_n$, with $r_0 = r$ and $r_n = 1$, of words over S in which r_i is constructed from r_{i-1} by either replacing a subword w_0 with w_1, where $w_0\overline{w_1} = w^+$ for some $w \in R^{\text{sym}}$, or by inserting or deleting s^2 for some $s \in S$. In this construction, a is the parity of the number of replacements of a subword w_0 with w_1 as described above in which the corresponding $w \in R^{\text{sym}}$ is odd. This is because each such replacement introduces a J into the word.

From such a sequence of words, we can construct a G-picture $\mathcal{P}$ embedded in a rectangle with boundary equal to r and sign equal to a by constructing a sequence of G-pictures $\mathcal{P}_1, \dots, \mathcal{P}_n$ such that $\text{bd}(\mathcal{P}_i) = r_{i-1}\overline{r_i}$, and the edges labeled by r_{i-1} adjacent to the boundary are connected to the top of the rectangle, and the edges labeled by $\overline{r_i}$ adjacent to the boundary are connected to the bottom of the rectangle. This process can be summarized as follows:

- If r_i was obtained from r_{i-1} by making a replacement of a word w_0 with w_1, as described above, so that $r_{i-1} = xw_0y$ and $r_i = xw_1y$ where x and y are words over S, then $\mathcal{P}_i$ consists of a single vertex labeled by w, incident to edges labeled from left to right by w_0 connected to the top of the rectangle and to edges labeled by w_1 connected to the bottom of the rectangle. To the left of the vertex, there are edges labeled by x, and to the right are edges labeled by y, all connecting the top and the bottom of the rectangle.
- If r_i was obtained from r_{i-1} by inserting s^2 for some $s \in S$, so that $r_{i-1} = xy$ and $r_i = xs^2y$ where x and y are words over S, then $\mathcal{P}_i$ consists of edges labeled by x and y connecting the top and the bottom of the rectangle, and an edge labeled by s with both endpoints connected to the bottom of the rectangle, in between the x and y edges.
- If r_i was obtained from r_{i-1} by deleting s^2 for some $s \in S$, so that $r_{i-1} = xs^2y$ and $r_i = xy$ where x and y are words over S, then $\mathcal{P}_i$ consists of edges labeled by x and y connecting the top and the bottom of the rectangle, and an edge labeled by s with both endpoints connected to the top of the rectangle, in between the x and y edges.

Since $r_0 = r$ and $r_n = 1$, we note that $\mathcal{P}_n$ has no edges incident to the bottom of the rectangle, while $\mathcal{P}_1$ has edges incident to the top labeled by r. Thus, by

stacking the pictures $\mathcal{P}_1, \ldots, \mathcal{P}_n$ on top of each other we obtain a G-picture in which we have effectively "tied together" the loose ends coming from r at the top so that $\mathrm{bd}(\mathcal{P}) = r$ and $\mathrm{sign}(\mathcal{P}) = a$ as desired.

Conversely, let $\mathcal{P}$ be a G-picture with $\mathrm{bd}(\mathcal{P}) = r$ and $\mathrm{sign}(\mathcal{P}) = a$. After isotopy, we assume without loss of generality that $\mathcal{P}$ is embedded into a rectangle in which every horizontal line intersects every edge in a finite number of points and every edge intersects finitely many horizontal lines non-transversely. A point in the interior of the picture is said to be a *critical point* if it is a vertex of $\mathcal{P}$ or a point on an edge that intersects a horizontal line non-transversely. Moving the critical points up or down, can modify the picture so that each horizontal line hits at most one critical point. Thus, $\mathcal{P}$ can be cut horizontally into a sequence of pictures $\mathcal{P}_1, \ldots, \mathcal{P}_n$, each of which contains a single critical point. This sequence corresponds to a sequence of words $r_0, \ldots, r_n$ in G, as above. ∎

A graphical overview of this step-by-step construction for the group $G = \mathrm{Inv}\left\langle x, y, z \mid (xy)^2 = (yz)^2 = 1 \right\rangle$ is shown in Figure 8.

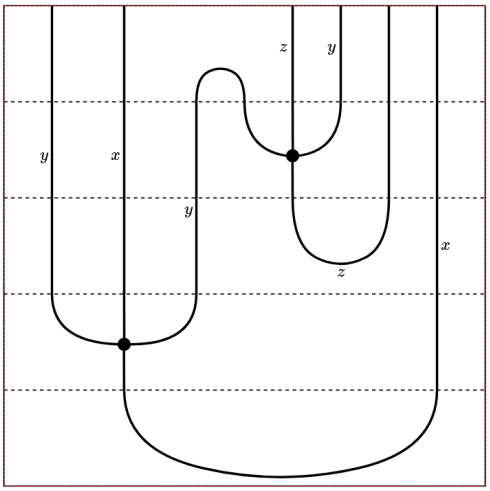

Figure 8: Construction of a G-picture corresponding to the sequence $yxzyzx = yxy^2zyzx = yxyz^2x = yxyx = x^2 = 1$.

Finally, we consider pictures corresponding to hypergraphs. Recall that given a hypergraph H and vertex labeling b, we can construct its corresponding solution group $\Gamma(H, b)$, which is a group presented by involutions over $\mathbb{Z}_2$. Thus, by picking a presentation of $\Gamma(H, b)$ we should be able to state the Van Kampen lemma for hypergraphs as well, as we will see in Proposition 5.22.

Definition 5.19. Let H be a hypergraph with incidence matrix A. An *H-picture* is a triple $(\mathcal{P}, h_V, h_E)$, where $\mathcal{P}$ is a picture, and h_V and h_E are *labeling*

functions $V(\mathcal{P}) \to V(H)$ and $E(\mathcal{P}) \to E(H)$, respectively, such that for all $v \in V(\mathcal{P})$ and $e' \in E(H)$, if we list the edges $e_1, \ldots, e_n$ of $\mathcal{P}$ incident to v with multiplicity, then $A_{h_V(v)e'} = |\{1 \leq i \leq n \mid h_E(e_i) = e'\}|$.

The *boundary* of $\mathcal{P}$ is the cyclic word $\mathrm{bd}(\mathcal{P}) = h(e_1) \ldots h(e_n)$ over $E(H)$, where $e_1, \ldots, e_n$ is the list of edges incident with the boundary, read in counterclockwise order around the boundary with multiplicity. The *character* of $\mathcal{P}$ is the vector $\mathrm{ch}(\mathcal{P}) \in \mathbb{Z}_2^{V(H)}$ with $\mathrm{ch}(\mathcal{P})_v = |h_V^{-1}(v)| \pmod 2$.

Often, we simply write $\mathcal{P}$ in place of $(\mathcal{P}, h_V, h_E)$, and h in place of h_V and h_E.

Example 5.20. Consider the dihedral group $D_4 = \mathrm{Inv}\left\langle s, t \mid (st)^4 = 1 \right\rangle$ that we saw in Example 4.16 to be a group presented by involutions for general n. Its wagon wheel hypergraph together with a corresponding H-picture, $\mathcal{P}$, is shown in Figure 9. We note that $\mathrm{bd}(\mathcal{P}) = (st)^4$.

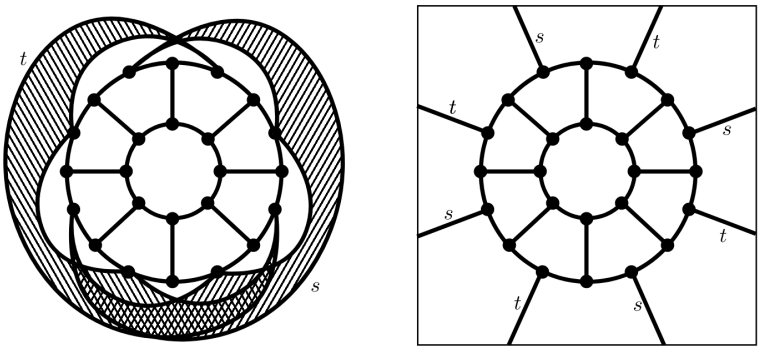

Figure 9: Wagon wheel hypergraph for $D_4 = \mathrm{Inv}\left\langle s, t \mid (st)^4 = 1 \right\rangle$ (left) and the corresponding H-picture (right).

Definition 5.21. Let $H = (V, E)$ be a hypergraph with vertex labeling function $b : V \to \mathbb{Z}_2$. Two H-pictures $\mathcal{P}_1$ and $\mathcal{P}_2$ are said to be *b- equivalent* if $\mathrm{bd}(\mathcal{P}_1) = \mathrm{bd}(\mathcal{P}_2)$ and $\mathrm{ch}(\mathcal{P}_1) \cdot b = \mathrm{ch}(\mathcal{P}_1) \cdot b$.

Finally, we now state the Van Kampen lemma as it stands for H-pictures. The proof is the same as for Proposition 5.18.

Proposition 5.22 (Van Kampen lemma)**.** *Let $\Gamma(H, b)$ be a solution group. Then $J^a = x_{e_1} \ldots x_{e_n}$ in $\Gamma(H, b)$ if and only if there is an H-picture $\mathcal{P}$ with $bd(\mathcal{P}) = e_1 \ldots e_n$ and $ch(\mathcal{P}) \cdot b = a$.*

§ 5.4. Constellations. Last in our section of definitions leading up to the proof of Proposition 4.19, and by extension also the embedding theorem, is the concept of stellar cycles and constellations. Essentially, constellations are collections of cycles in a hypergraph. It is a technical construction used for the proof of Proposition 4.19, and its equivalent statement Proposition 5.7.

At the moment, it is not clear how to formulate a conceptual justification for this particular construction.

Recall that the structure of the wagon wheel hypergraph is consisting of several "wheels" on vertices denoted by V_i and edges E_i. Throughout this section, we let W_i denote the closed subhypergraph on vertices V_i and edges E_i.

Before introducing constellations, we need to state a few more definitions (with examples where appropriate), in particular those of subhypergraphs and cycles.

Definition 5.23. Let $H = (V, E)$ be a hypergraph with incidence matrix A. A *subhypergraph* of H is a hypergraph $H' = (V', E')$ with $V' \subset V$, $E' \subset E$, and incidence matrix A' such that $A'_{ve} = A_{ve}$ for all $v \in V'$ and $e \in E'$. We write $H' \subset H$.

We recall that given a picture $\mathcal{P}$, a collection of edges whose union form a simple closed curve is called a *simple cycle*.

Definition 5.24. Let H be a hypergraph. A simple connected 2-regular subhypergraph C of H is called a *cycle* if for all $v \in V(H)$, it holds that $v \in V(C)$ whenever v is incident to $e \in E(C)$, i.e., it is *closed*. A C*-cycle* in an H-picture is a simple cycle C such that every edge of C is labeled by an edge of C.

Definition 5.25. A C-cycle C is called a *copy* of C if the labeling function $h : C \to C$ is a graph isomorphism, or equivalently if $|h^{-1}(v)| = 1$ for all $v \in V(C)$.

Example 5.26. We can easily recognize cycles in the hypergraphs we have seen so far. Consider, for example, the (hyper)graph in Figure 2 representing the CHSH game, in which the edges e_1 and e_2 form a cycle.

Also, considering a wagon wheel hypergraph with incidence relations as stated in Definition 5.8, we find that the edges $B_i = \{d_{ij} \mid j \in \mathbb{Z}_{n_i}\}$ and $C_{ij} = \{a_{ij}, b_{ij}, c_{ij}, d_{ij}, c_{i,j-1}\}$ for all $j \in \mathbb{Z}_{n_i}$, form cycles for all $1 \leq i \leq m$. Furthermore, for W we can easily construct a corresponding W-picture, as the one seen in Figure 9, in which the cycles B_i and C_{ij} have corresponding B_i-cycles and C_{ij}-cycles. We also note that these cycles are copies of the corresponding cycles in W.

Before we are ready to define constellations and b-stellar cycles, we describe and define the notion of retracts of hypergraphs through generalized morphism. These yield a systematic procedure of "collapsing" an existing hypergraph by removing or identifying edges and removing some vertices.

Definition 5.27. Let $H' \subset H$. The *neighborhood* $N(H')$ of H' is the subhypergraph with vertex set $V(N(H')) = V(H')$ and edge set

$$E(N(H')) = E(H') \cup \{e \in E(H) \mid \text{ there exists } v \in V(H') \text{ such that } v \in e\},$$

i.e., edges outside of H' are only included in the neighborhood if they are incident to any vertex in H'.

As we have seen, a subhypergraph $H' \subset H$ is said to be *closed* if for all $v \in V(H)$ it holds that if v is incident to an edge $e \in E(H')$ then v is also part of the subhypergraph, i.e., $v \in V(H')$. Furthermore, H' is said to be *open* if $H' = N(H')$.

Example 5.28. Consider the hypergraph H pictured in Figure 10 with incidence matrix

$$A(H) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

and let H' be the closed subhypergraph highlighted in this figure. The neighborhood of H' also includes the edge e_2 so H' is not open. Note that in general, a subhypergraph or neighborhood need not contain the all vertices of the included edges, thus potentially resulting in self-loops.

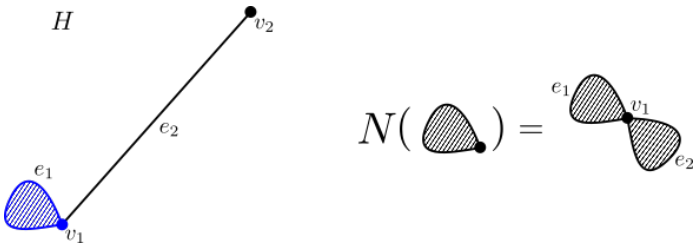

Figure 10: A subhypergraph and its neighborhood.

Definition 5.29. Let $H_1 = (V_1, E_1)$ and $H_2 = (V_2, E_2)$ be hypergraphs. A *generalized morphism* $\phi : H_1 \to H_2$ consists of a pair of functions

$$\phi_V : V_1 \to V_2 \cup \{\varepsilon\} \quad \text{and} \quad \phi_E : E_1 \to E_2 \cup \{\varepsilon\},$$

where $\varepsilon \notin V_i \cup E_i$ for $i = 1, 2$, such that for all $v \in V_1$,

1. if $\phi_V(v) \neq \varepsilon$, then

$$\sum_{e \in \phi_E^{-1}(e')} A(H_1)_{ve} = A(H_2)_{\phi_V(v)e'}$$

for all $e' \in E_2$, and

2. if $\phi_V(v) = \varepsilon$, then

$$\sum_{e \in E_1 \setminus \phi_E^{-1}(\varepsilon)} A(H_1)_{ve} \equiv 0 \pmod 2,$$

and $\phi_E(e_1) = \phi_E(e_2)$ for all edges $e_1, e_2 \in E_1 \setminus \phi_E^{-1}(\varepsilon)$ incident to v.

Intuitively, from these rules, we can deduce that we are allowed to make the following modifications:

- freely remove and identify edges, preserving the incidences according to condition (1)
- remove isolated vertices,
- remove vertices incident to an even number of edges, collapsing the incident edges, and more generally
- remove any vertex v, and identify a number of edges incident to v so that condition (2) above is satisfied.

Given a hypergraph containing repeated structure in the form of a subhypergraph, a nice useful example of generalized morphisms is that of successively removing edges until only several copies of said subhypergraph remains, and then identify those copies. Figures 12 and 13 show such a process.

Example 5.30. Consider the hypergraph H, pictured to the left in Figure 11. It is given by the incidence matrix

$$A(H) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

A generalized morphism removing the vertex v_1 must, in order to preserve identity (2) of the definition also identify e_1 and e_2, thus resulting in the incidence matrix

$$A(H') = \begin{bmatrix} 2 & 0 \\ 2 & 0 \\ 2 & 1 \end{bmatrix}.$$

Figure 11 shows this generalized morphism. If we instead let $e_1 \mapsto \varepsilon$ and $e_2 \mapsto e_2'$, where $e_2' = \{v_2', v_3', v_4'\}$, obtaining the hypergraph H', then

$$A(H)_{v_2 e_2} + A(H)_{v_2 e_3} = 1 + 0 \not\equiv 0 \pmod 2$$

and $A(H_1)_{v_3 e_2} = 0 \neq A(H')_{v_3' e_2'}$, so both property (1) and (2) would be violated.

In our later constructions, we will not directly use the concept of generalized morphism, but rather focus on so-called retracts:

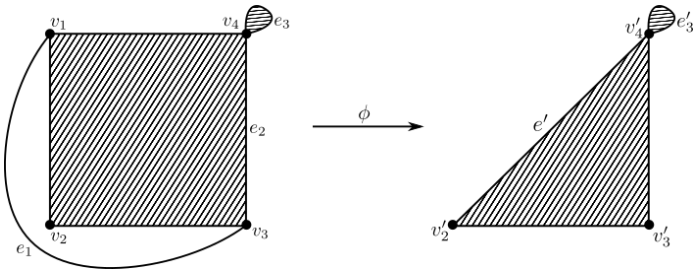

Figure 11: Generalized morphism between two hypergraphs, removing the vertex v_1 and making the identifications $e_1, e_2 \mapsto e'$.

Definition 5.31. Let $H' \subset H$. If there is a generalized morphism $r : H \longrightarrow H'$ such that $r_{|H'}$ is the identity then H' is said to be a *retract* of H.

In particular, we note that every closed subhypergraph is a retract.

Based on our understanding of generalized morphisms above, we find that a subhypergraph $H' \subset H$ is a retract if it can be obtained from H through any sequence of the following modifications:

- removal and identification of edges outside of H', and
- removal of vertices outside of $V(H')$ that are not incident to any edges in $E(H')$, along with the necessary identifications to satisfy property (2) in Definition 5.29.

Example 5.32. Consider the cube hypergraph pictured in Figure 12, and consider the generalized morphism removing the highlighted edges, and then identifying the vertices of the top square with the bottom square. Then, we see that the subhypergraph given by the vertices $\{1, 2, 3, 4\}$ and edges $\{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}\}$, i.e. the bottom square, is a retract.

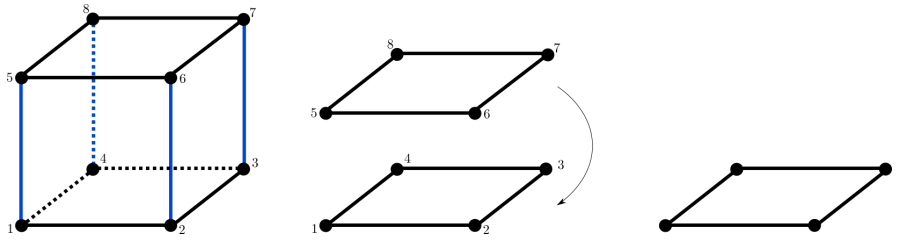

Figure 12: The square is a retract of the cube hypergraph.

Example 5.33. Let W be a wagon wheel hypergraph with "wheels" $W_1, \ldots, W_m$. Recall the cycles C_{ij} and B_i seen in Example 5.26.

To see that there is a retract of $N(W_i)$ onto $N(B_i)$, we can simply remove all vertices $(i, j, 1)$ for $j \in \mathbb{Z}_{n_i}$, along with their incident edges. The resulting graph then consists of an outer cycle with the same number of vertices as the

inner cycle B_i, as well as the neighborhood $N(B_i)$. Much like the squares in the previous example, the outer cycle can then be identified with the inner cycle, and we obtain the suggested retract, see Figure 13.

It is possible to show that there is a retract of $N(W_i)$ onto $N(C_{ij})$ if $\mathrm{mult}(s_{ij}; r_{i'})$ is even for all $1 \leq i' \leq m$. The description of this retract is a bit more involved than that of $N(B_i)$, so we refer the interested reader to [18], Lemma 12.3.

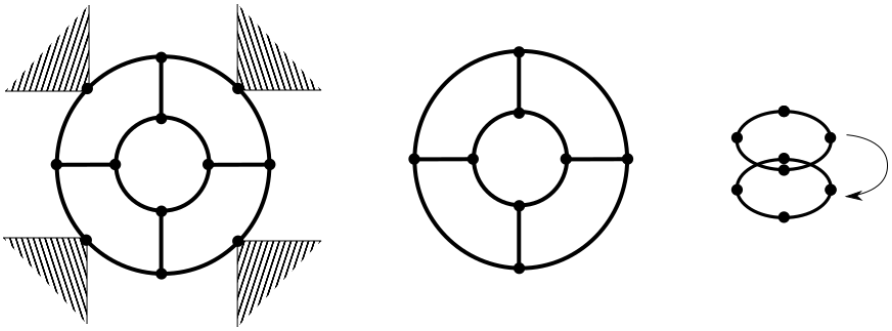

Figure 13: Retract of $N(W_i)$ to the cycle $N(B_i)$ for $n_i = 4$.

Finally, we consider another family of hypergraphs that will be helpful for our later constructions:

Definition 5.34. The *sun of size n* is the hypergraph with vertex set $V = \{1, \ldots, n\}$, edge set $E = \{e_i, f_i \mid 1 \leq i \leq n\}$, such that the vertex i is incident with f_j if $i = j$, and e_j if $i \equiv j \pmod{n}$ or $i \equiv j + 1 \pmod{n}$.

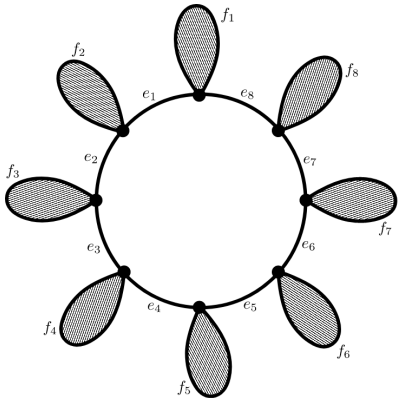

Figure 14: The sun of size 8.

Example 5.35. In fact, we have already seen several examples of suns without realizing. In particular, the neighborhoods of the cycles C_{ij} and B_i for $1 \leq i \leq m$ and $j \in \mathbb{Z}_{n_i}$ can easily be seen to be suns. The inner cycle $N(B_i)$ is a sun of size n_i, while the cycles $N(C_{ij})$ are suns of size 5.

We are now ready to state our final definitions for this section, before pursuing the proof of the embedding theorem.

Definition 5.36. Let H be a hypergraph with vertex labeling function $b : V(H) \to \mathbb{Z}_2$. A cycle C in H is *b-stellar* if

1. $N(C)$ is isomorphic to a sun,
2. $N(C)$ is a retract of H, and
3. $b(v) = 0$ for all $v \in V(C)$.

Definition 5.37. Let H be a hypergraph with vertex labeling $b : V(H) \to \mathbb{Z}_2$. A collection Φ of cycles of H is called a *b-constellation* if it satisfies to following properties:

1. If $C \in \Phi$, then the neighborhood $N(C)$ is isomorphic to a sun and is either b-stellar or a sequence of edges $e_1 e_2 \dots e_n$, $n \geq 3$, such that e_k belongs to a b-stellar cycle $C' \in \Phi$ for all $3 \leq k \leq n$.
2. For every $C \in \Phi$, either:
   - there is an edge $e \in E(C)$ which does not belong to any cycle in $\Phi \setminus \{C\}$, or
   - there is another cycle $C' \in \Phi$ such that $E(C) \cap E(C') \neq \emptyset$, and C' contains an edge e which does not belong to any cycle in $\Phi \setminus \{C'\}$.
3. For distinct cycles $C_0, C_1 \in \Phi$, it holds that $|E(C_0) \cap E(C_1)| \leq 1$, and if neither C_0 nor C_1 is b-stellar, then $E(C_0) \cap E(C_1) = \emptyset$.

Example 5.38. Consider the hypergraph pictured in Figure 15 and take b to be the 0-labeling, and let Φ contain the cycles $C_1 = \{v_1, v_3, v_4\}$, $C_2 = \{v_2, v_3, v_4\}$, and $C_3 = \{v_1, v_2, v_4\}$. It is clear that each cycle of Φ is b-stellar. Furthermore, for the cycle C_1, the edge $\{v_1, v_3\}$ is not included in any other cycle in Φ, similarly, the edges $\{v_2, v_3\}$ and $\{v_1, v_2\}$ in C_2 and C_3, respectively are not included in any other cycles of Φ. Lastly, each pair of cycles in Φ meet in only a single edge. Thus, Φ is a b-constellation.

Note that under this labeling, we cannot include the cycle $\{v_1, v_2, v_3\}$ in Φ since, despite it being b-stellar, neither cycle would then contain an edge not included in any other cycle of Φ, thus violating property (2) of the definition.

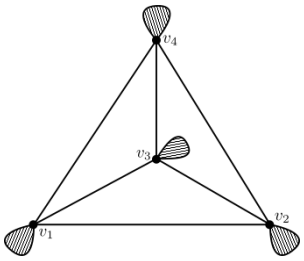

Figure 15: The hypergraph described in Example 5.38.

6. Proof of Proposition 4.19

This section finally gives the conclusion to our endeavors of proving the embedding theorem, and in particular, the last remaining step to show – Proposition 4.19.

First, we will work out the proof through an example using the now familiar presentation of the dihedral group before giving the general proof of the proposition as stated in [18].

To simplify our notation, we first make the following definition:

Definition 6.1. Let $W(\mathcal{I})$ be the wagon wheel hypergraph corresponding to $\mathcal{I} = \operatorname{Inv}\langle S \mid R\rangle$. Denote by B_i the cycle containing the edges d_{ij} for all $1 \leq i \leq m$ and $j \in \mathbb{Z}_{n_i}$, and by C_{ij} the cycle of edges $a_{ij}, b_{ij}, c_{ij}, d_{ij}$ and $c_{i,j-1}$ for all $1 \leq i \leq m$ and $j \in \mathbb{Z}_{n_i}$. Finally, let $\Phi_{\mathcal{I}}$ denote the collection of all cycles B_i and C_{ij}.

§ 6.1. Illustration of the proof. We present a general overview of the proof of Proposition 4.19 by working through an example based on the presentation of the dihedral group D_{2n}, as given in Example 4.16. Recall that we have the presentation $D_{2n} = \left\langle s, t \mid s^2 = t^2 = (st)^{2n} = 1\right\rangle$ so that D_{2n} is a group presented by involutions over $\mathbb{Z}_2$ with $J = (st)^n$, i.e. $D_{2n} = \operatorname{Inv}\left\langle s, t \mid (st)^{2n} = 1\right\rangle$.

We aim to show that there is an embedding over $\mathbb{Z}_2$ of D_{2n} into a solution group $\Gamma(A, b)$ corresponding to a binary linear system in variables X such that $\{s, t\} \subset X$.

We have seen several examples of the wagon wheel hypergraph corresponding to this group. In the top-left of Figure 5 is the wagon wheel corresponding to D_2, and in Figure 9, we find the wheel of the group D_8. For any n, we see that the 0-labeling is a D_{2n}-labeling of W. Let $\Phi_{D_{2n}}$ be as in Definition 6.1, and for simplicity we write $C_j := C_{1j}$ for $0 \leq j \leq 3$, and $B := B_1$. We find that $\Phi_{D_{2n}}$ is a 0-constellation:

As mentioned in Example 5.35, $N(B)$ is a sun of size 4, and by Example 5.33 it is also a retract of W. Thus, it follows that B is 0-stellar. Likewise, for $0 \leq j \leq 3$, the cycle C_j can also be seen to be 0-stellar. Thus, condition (1) of Definition 5.37 is satisfied.

Since C_j is the only cycle in Φ containing the edges a_{1j} and b_{1j}, and $E(B) \cap E(C_j) = \{d_j\}$ we also find that condition (2) is satisfied. Lastly, for all $C_0, C_1 \in \Phi$ we have that $|E(C_0) \cap E(C_1)| = 1$, so we conclude that $\Phi_{D_{2n}}$ is a 0-constellation indeed.

We now consider the morphism $\phi : D_{2n} \to \Gamma(W, 0)$ such that $s \mapsto x_s$ and $t \mapsto x_t$. Note that the word $w = (st)^{2n}$ is mapped to the identity by ϕ. Thus,

by Proposition 5.22 there is a W-picture $\mathcal{P}$ such that $\mathrm{bd}(\mathcal{P}) = (st)^{2n}$. An example of such a picture is seen to the right in Figure 9, and this example can easily be extended to a W-picture for any n.

For our later discussions, it is now helpful to note that for such a picture, all $\Phi_{D_{2n}}$-cycles in $\mathcal{P}$ are facial copies. Now, by collapsing the $\Phi_{D_{2n}}$-cycles of $\mathcal{P}$ to a single vertex, we obtain a D_{2n}-picture $\mathcal{P}'$, resembling a star graph embedded in a square, in which the single vertex is labeled by $(st)^{2n}$, see Figure 16. In particular, $\mathrm{bd}(\mathcal{P}) = \mathrm{bd}(\mathcal{P}')$.

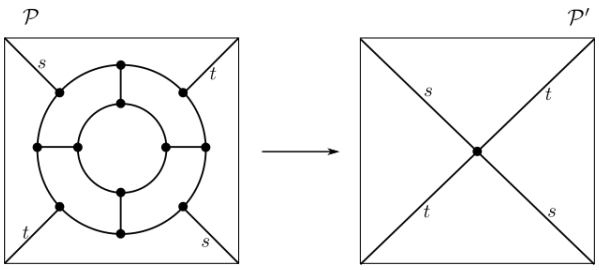

Figure 16: By collapsing the Φ_{D_2}-cycles of the picture $\mathcal{P}$ to a single vertex, we obtain the picture $\mathcal{P}'$.

So indeed $w = 1$ in D_{2n} and since $\phi(J^a w) = 1$ for $a \in \mathbb{Z}_2$ if and only if $a = 0$ and $\phi(w) = 1$ it follows that ϕ is injective. Thus, D_{2n} can be embedded into the solution group $\Gamma(W, 0)$ in the desired way, for all n.

§ 6.2. Presenting the proof. After the hopefully illuminating example of the previous section, we now proceed to give the general steps of the proof, referencing the relevant results from [18] where needed. For the purpose of this text, we will not delve further into the details of this proof beyond this overview and instead urge the reader to pursue a deeper understanding of the matter by consulting [18].

The primary results from this article, which are here taken as facts, are the following statements:

Fact 1 ([18], Lemma 12.4)**.** Let $\mathcal{I} = \mathrm{Inv}\langle S \mid R\rangle$ be a collegial representation by involutions over $\mathbb{Z}_2$, and let $W = W(\mathcal{I})$ be its wagon wheel hypergraph. Let b be an $\mathcal{I}$- labeling b of $W(\mathcal{I})$ such that

- $|b^{-1}(1) \cap V(W_i)| \leq 1$ for all $1 \leq i \leq m$,
- $b((i, j, 2)) = b((i, j, 3)) = 0$ for all $1 \leq i \leq m$ and $j \in \mathbb{Z}_{n_i}$, and
- if $b((i, j, 1)) = 1$, then either $\mathrm{mult}(s_{ij}, r_{i'})$ is odd for some $1 \leq i' \leq m$, or $\mathrm{mult}(s_{ij'}, r_{i'})$ is even for all $j \in \mathbb{Z}_{n_i}$ and $1 \leq i' \leq m$.

Then, $\Phi_{\mathcal{I}}$ is a b-constellation.

Fact 2 ([18], Theorem 11.4)**.** Let H be a hypergraph with vertex labeling b, and let Φ be a b-constellation. Let $\mathcal{P}$ be an H-picture such that

1. $\mathrm{bd}(\mathcal{P})$ does not contain any edges from any cycle $C \in \Phi$, and
2. either $b = 0$ or $\mathcal{P}$ is closed.

Then $\mathcal{P}$ is b-equivalent to a picture $\mathcal{P}'$ such that all Φ-cycles in $\mathcal{P}'$ are facial copies.

Fact 3 ([18], Lemma 12.5)**.** Let $\mathcal{I} = \mathrm{Inv}\langle S \mid R\rangle$ with $\mathcal{I}$- labeling b, and let $\mathcal{P}$ be a $W(\mathcal{I})$-picture in which all $\Phi_{\mathcal{I}}$-cycles are facial copies, and such that all edges in $\mathrm{bd}(\mathcal{P})$ belong to S. Then there is a G-picture $\mathcal{P}'$ with $\mathrm{bd}(\mathcal{P}') = \mathrm{bd}(\mathcal{P})$ and $\mathrm{sign}(\mathcal{P}') = \mathrm{ch}(\mathcal{P}) \cdot b$.

Recall that $\mathrm{Inv}\langle S \mid R^+\rangle$ denotes the even presentation of $\mathrm{Inv}\langle S \mid R\rangle$. Likewise, for any group G over $\mathbb{Z}_2$ we define the *even quotient* $G^+ = G/\langle J_G\rangle \times \mathbb{Z}_2$, a group over $\mathbb{Z}_2$ with J_{G^+} as the generator of the $\mathbb{Z}_2$-factor. In particular, if $G = \mathrm{Inv}\langle S \mid R\rangle$, then $G^+ = \mathrm{Inv}\langle S \mid R^+\rangle$.

We now present the final proof of the embedding theorem, following the presentation in [18].

Proof of Proposition 4.19. Let G be a group with a presentation by involutions over $\mathbb{Z}_2$, $\mathcal{I} = \mathrm{Inv}\langle S \mid R\rangle$, and suppose that this presentation is collegial. By Fact 1 there is an $\mathcal{I}$-labeling b of $W := W(\mathcal{I})$ such that $\Phi_{\mathcal{I}}$ is a b-constellation. Since every b-stellar cycle is also 0-stellar by (3) of Definition 5.36, it follows that $\Phi_{\mathcal{I}}$ is also a 0-constellation.

Note that there is an $N(W_i)$-picture $\mathcal{P}$ such that $\mathrm{bd}(\mathcal{P}) = s_{i1}, \ldots, s_{in_i}$ and $\mathrm{ch}(\mathcal{P}) \cdot b = \sum_{v \in V_i} b_v = p_i$. Thus, by Proposition 5.22 the relation r_i holds also in $\Gamma(W, b)$. Hence, there is a well-defined morphism $\phi : G \to \Gamma(W, b)$ over $\mathbb{Z}_2$ such that $s \mapsto x_s$ for all $s \in S$. Likewise, there is a morphism $\phi^+ : G^+ \to \Gamma(W, 0)$, also sending $s \mapsto x_s$ for all $s \in S$.

We first show that ϕ^+ is injective. We again rely on the Van Kampen lemma (Proposition 5.22) to say that if $\phi^+(w) = 1$ for some word $w \in \mathcal{F}_2(S)$, then there is a W-picture $\mathcal{P}$ with $\mathrm{bd}(\mathcal{P}) = w$. Now by Fact 2 we can choose $\mathcal{P}$ so that all Φ-cycles in $\mathcal{P}$ are facial copies. Then, by Fact 3, there is a G^+-picture $\mathcal{P}'$ such that $\mathrm{bd}(\mathcal{P}') = \mathrm{bd}(\mathcal{P})$, so it follows that $\phi^+(w) = 1$ in G^+. Since $\phi^+(J^a w) = 1$ for $a \in \mathbb{Z}_2$ and $w \in \mathcal{F}_2(S)$ if and only if $a = 0$ and $\phi^2(w) = 1$, it follows that ϕ^+ is injective.

Consider the quotient maps $q_1 : G \to G^+$ and $q_2 : \Gamma(W, b) \to \Gamma(W, 0)$ by J_G

and $J_{\Gamma(W,b)}$, respectively, and the commutative diagram:

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \Gamma(W,b) \\ \downarrow{\scriptstyle q_1} & & \downarrow{\scriptstyle q_2} \\ G^+ & \xrightarrow[\phi^+]{} & \Gamma(W,0) \end{array}$$

Now, since J_G is central of order at most 2, either $\ker(q_1) = 1$ or $\ker(q_1) = J_G$. Since ϕ^+ is injective, if $\phi(w) = 1$ then $q_1(w) = 1$, so $w \in \{1, J_G\}$. We show that $\phi(J_G) = 1$ if and only if $J_G = 1$ in G.

By definition, $\phi(J_G) = J_\Gamma$, and if $J_\Gamma = 1$, then by Proposition 5.22 there is a closed W-picture $\mathcal{P}$ with $\mathrm{ch}(\mathcal{P}) \cdot b = 1$. Since $\mathcal{P}$ is closed, we can choose $\mathcal{P}$ so that all Φ-cycles in $\mathcal{P}$ are facial copies, by Fact 2. Finally, Fact 3 implies that there is a closed G-picture $\mathcal{P}'$ such that $\mathrm{sign}(\mathcal{P}') = 1$, and it follows that $J_G = 1$ in G. Thus, ϕ is injective. ∎

§ 6.3. Concluding remarks. The proof in the preceding section concludes our proof of the embedding theorem. By showing in Propositions 4.12 and 4.18 it is possible to embed any finitely presented group over $\mathbb{Z}_2$ into a group presented by involutions, and more specifically that every finitely presented group over $\mathbb{Z}_2$ with a sequence of distinguished involutions can be embedded into a collegial presentation by involutions, we paved the way to Proposition 4.19 stating that any group with a collegial presentation by involutions can be embedded into the solution group corresponding to some binary linear system and hence to some linear system non-local game.

By these three steps, we conclude with the embedding theorem (Theorem 4.6) that any finitely presented group generated by involutions and with a distinguished central element of order two can be embedded into a solution group corresponding to a linear system non-local game. Through purely group theoretic results and using Theorem 4.5 we thus find that there are non-local games with perfect commuting-operator strategies, but lacking perfect tensor-product strategies.

Although this construction yields quite unwieldy games that are difficult to describe in a truly meaningful way, this result nonetheless resolves a long-standing Tsirelson problem of whether $C_{qs} = C_{qc}$, the answer to which we can now conclude to be negative.

For example, corresponding to the tiny group D_2, we get a wagon wheel with 12 vertices and 18 edges, which correspond to a solution group for a linear system non-local game with $A \in \mathbb{Z}_2^{12\times 19}$. Even worse, working through the

construction with a group over $\mathbb{Z}_2$ in which $J_G \neq 1$ yet such that $\pi(J_G) = 1$ for all finite-dimensional representations of G, such as the one used in the proof of Corollary 4.7, we obtain a system with several hundred variables and relations, as seen in [18].

However, we might see improvements in this regard with future simplification of this construction.Furthermore, it is of interest to determine the smallest linear system non-local game which results in a separation of C_{qs} and C_{qc}. The author hopes that this overview of the main result and its underlying constructions can be helpful in this regard.

Appendices

A. Quantum computing

Here, we introduce the basic notions of quantum computing, including qubits and their states and how operations are performed through gates and measurements. Finally, we introduce the reader to what can be considered the hidden power of quantum computing – the concept of entanglement.

§ A.1. Qubits and their states. As we are familiar with from the classical theory of computation, the simplest and primary unit of information is that of a *bit*. Analogously, in the theory of quantum computation, we deal with quantum bits, or *qubits*:

Definition A.1. A *qubit* is a unit vector in $\mathbb{C}^2$, denoted by $|\psi\rangle$, and we distinguish the so-called *basic states*

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

More generally, a *quantum state* is a unit vector in a Hilbert space and a multi-qubit state, or a *register*, of n qubits is a unit vector in the Hilbert space $(\mathbb{C}^2)^{\otimes n}$

This notation of vectors is called *Dirac* or *ket notation* and is a common notation for quantum state vectors, i.e, $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$. We also let $\langle\psi|$ denote the conjugate transpose of $|\psi\rangle$ in the conjugate Hilbert space. This conveniently lets us write the inner product of $|\psi_1\rangle$ and $|\psi_2\rangle$ as $\langle\psi_1|\psi_2\rangle$.

The notion of basic states extends more generally to states on n qubits as we can simply consider the basic states $|0\rangle^{\otimes n}$ and $|1\rangle^{\otimes n}$.

A quantum state like $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ in which $\alpha_0, \alpha_1 \neq 0$ is said to be in *superposition* of the two basic states. Interestingly, this distinguishes quantum states from classical states in that they can simultaneously hold more information that, theoretically, could be retrieved through a procedure called a *measurement*.

In particular, in contrast to states of bits in the usual sense, the value of a quantum state cannot be directly observed but is instead measured, which leads to some interesting consequences, as we will see in Section A.3.

§ A.2. Operations on qubits. In further analogy with the theory of classical computation, we consider operations of qubits called *gates*.

Definition A.2. A unitary transformation on $(\mathbb{C}^2)^{\otimes n}$ is called a *gate*.

This definition is motivated by the fact that unitary transformations preserve the property of being a unit vector, so a gate indeed transforms one quantum state into another. Some notable examples of quantum gates include the following transformations on qubits:

Example A.3. Two of the most simple gates are the following:

$$\text{Identity: } \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\text{NOT-gate: } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

which are both analogous to the identity and NOT gate of classical computation in that the identity leaves a qubit unchanged, while a NOT-gate "flips" a $|0\rangle$ to a $|1\rangle$ and vice versa.

Another useful gate is the CNOT-gate, or *controlled-not* gate, which, when applied to a two-qubit register, flips the second qubit if and only if the first qubit – called the *control bit* – is 1. It is given by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

It is a simple matter to check that each of these transformations is indeed unitary.

Finally, we define the perhaps most crucial gate in quantum computing:

Definition A.4. On a single-qubit system, the transformation defined by

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

is called the *Hadamard transform*.

Notably, the Hadamard transform transforms a state in the basis $\{|0\rangle, |1\rangle\}$ to the orthogonal basis $\left\{ \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right\}$, and vice versa.

§ A.3. Measurements on qubits. As suggested previously, the concept of measurements is highly central in quantum computing as it is the process through which the value of a quantum state can be obtained.

According to the *Born rule*, a fundamental postulate of quantum mechanics, a measurement of the state $|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ will result in an observation of either $|0\rangle$ or $|1\rangle$ with probability $|\alpha_0|^2$ or $|\alpha_1|^2$, respectively. This can be generalized to multi-qubit states.

Notably, this means that after measurement, the state effectively collapses to either of the states $|0\rangle$ or $|1\rangle$ according to some probability distribution. Furthermore, the measurement here is made with respect to the standard basis $\{|0\rangle, |1\rangle\}$, but could just as easily have been made according to some other orthonormal basis, such as the Hadamard basis of the previous section after a change of basis.

We make the following formal definition:

Definition A.5. Let $\mathcal{H}$ be a Hilbert space and $[n] = \{1, \ldots, n\}$ a set of outcomes. A *projective valued measurement (PVM)* is a collection of self-adjoint projections $\{P_i\}_{i\in[n]}$ such that $\sum_{i=1}^{n} P_i = \mathbb{1}$. Given a state $|\psi\rangle$, the probability of observing the outcome i is given by

$$||P_i |\psi\rangle||^2 = \langle\psi| P_i^* P_i |\psi\rangle = \langle\psi| P_i |\psi\rangle,$$

and after measurement, the state collapses to

$$\frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}}.$$

Example A.6. Given a Hilbert space $\mathcal{H}$ with orthonormal basis $B = \{|v_1\rangle, \ldots, |v_n\rangle\}$, the collection of self-adjoint projections

$$P_i = |v_i\rangle \langle v_i|$$

yields a PVM with outcome set corresponding to the basis B.

§ A.4. Entanglement. Finally, we introduce the concept of entanglement – the primary property of quantum mechanics, which distinguishes it from classical mechanics when we consider physically separated systems.

Given two qubits $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$, we can consider them as forming a multi-qubit system in $\mathcal{H}_1 \otimes \mathcal{H}_2$, according to our definition of quantum registers. However, not all states in this space can be written as a product of states coming from $\mathcal{H}_1$ and $\mathcal{H}_2$. Such inseparable states are said to be *entangled*.

Example A.7. Consider the qubits $|0\rangle$ and $|0\rangle$ forming the two-qubit register $|00\rangle$. To this state, we apply first the Hadamard transform to the first qubit and then the CNOT gate, thus obtaining the state

$$(CNOT)(H \otimes \mathbb{1}) \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = CNOT \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}},$$

which is entangled. This state is called a *Bell-pair*.

What makes entanglement an interesting phenomenon to study is the behavior of such states when measured. Consider, for instance, the Bell-pair in the preceding example: if we were to measure the first qubit using the PVM discussed in Example A.6, and observe $|0\rangle$ with probability $\frac{1}{2}$, then the state in its entirety would collapse to $|00\rangle$. Thus, the second qubit can immediately be determined to be $|0\rangle$! In fact, no matter the outcome, entanglement ensures that the resulting observations are not independent anymore.

This property is sometimes described as the *non-locality* of quantum mechanics in that the entangled qubits themselves do not a priori need to be physically close to each other at the time of measurement so that the collapse of the system seems to imply that a distant action immediately results in an altered physical property in a local system.

References

[1] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nature Communications. 9 (2018) 459. https://doi.org/10.1038/s41467-017-02307-4.

[2] J.S. Bell, On the Einstein Podolsky Rosen paradox, Physics Physique Fizika. 1 (1964) 195–200. https://doi.org/10.1103/PhysicsPhysiqueFizika.1.195.

[3] B.S. Cirel'son, Quantum generalizations of Bell's inequality, Letters in Mathematical Physics. 4 (1980) 93–100. https://doi.org/10.1007/BF00417500.

[4] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Physical Review Letters. 23 (1969) 880–884. https://doi.org/10.1103/PhysRevLett.23.880.

[5] R. Cleve, L. Liu, W. Slofstra, Perfect commuting-operator strategies for linear system games, Journal of Mathematical Physics. 58 (2017) 012202, 7. https://doi.org/10.1063/1.4973422.

[6] R. Cleve, R. Mittal, Characterization of binary constraint system games, in: Automata, Languages, and Programming. Part I, Springer, Heidelberg, 2014: pp. 320–331. https://doi.org/10.1007/978-3-662-43948-7_27.

[7] A. Coladangelo, J. Stark, Unconditional separation of finite and infinite-dimensional quantum correlations, (2018). https://doi.org/10.48550/arXiv.1804.05116.

[8] J.B. Conway, A Course in Functional Analysis, Springer New York, New York, NY, 2007. https://doi.org/10.1007/978-1-4757-4383-8.

[9] A.J. Derrick, Groups with no nontrivial linear representations, Bulletin of the Australian Mathematical Society. 50 (1994) 1–11. https://doi.org/10.1017/S0004972700009503.

[10] A. Einstein, B. Podolsky, N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, Physical Review. 47 (1935) 777–780. https://doi.org/10.1103/PhysRev.47.777.

[11] A.K. Ekert, Quantum cryptography based on Bell's theorem, Physical Review Letters. 67 (1991) 661–663. https://doi.org/10.1103/PhysRevLett.67.661.

[12] G. Higman, A Finitely Generated Infinite Simple Group, Journal of the London Mathematical Society. s1-26 (1951) 61–64. https://doi.org/10.1112/jlms/s1-26.1.61.

[13] Z. Ji, A. Natarajan, T. Vidick, J. Wright, H. Yuen, MIP*=RE, (2020). http://arxiv.org/abs/2001.04383 (accessed June 17, 2022).

[14] R. Kadison, J. Ringrose, Fundamentals of the Theory of Operator Algebras. Volume I, American Mathematical Society, Providence, Rhode Island, 1997. https://doi.org/10.1090/gsm/015.

[15] E.R.V. Kampen, On Some Lemmas in the Theory of Groups, American Journal of Mathematics. 55 (1933) 268. https://doi.org/10.2307/2371129.

[16] R.C. Lyndon, P.E. Schupp, Combinatorial Group Theory, Springer, Berlin, Heidelberg, 2001. https://doi.org/10.1007/978-3-642-61896-3.

[17] G.J. Murphy, C *-algebras and operator theory, Repr., Academic Press, Boston, 2004.

[18] W. Slofstra, Tsirelson's problem and an embedding theorem for groups arising from non-local games, Journal of the American Mathematical Society. 33 (2020) 1–56. https://doi.org/10.1090/jams/929.

[19] W. Slofstra, The set of quantum correlations is not closed, Forum of Mathematics, Pi. 7 (2019) e1. https://doi.org/10.1017/fmp.2018.3.

[20] B. Tsirelson, Bell inequalities and operator algebras, (2006). https://web.archive.org/web/20090414083019/http://www.imaph.tu-bs.de/qi/problems/33.html (accessed January 31, 2023).

[21] B. Tsirelson, Some results and problems on quantum Bell-type inequalities, Hadronic Journal Supplement. 8 (1993) 329–345.

[22] B.A.F. Wehrfritz, Infinite Linear Groups, Springer, Berlin, Heidelberg, 1973. https://doi.org/10.1007/978-3-642-87081-1.

[23] C. Wood, Pioneering Quantum Physicists Win Nobel Prize in Physics, Quanta Magazine. (2022). https://www.quantamagazine.org/pioneering-quantum-physicists-win-nobel-prize-in-physics-20221004/ (accessed May 11, 2023).