Commutation Groups and State-Independent Contextuality

Samson Abramsky
Department of Computer Science, University College London, London, UK

Şerban-Ion Cercelescu
Department of Computer Science, University of Oxford, Oxford, UK

Carmen-Maria Constantin
Department of Computer Science, University College London, London, UK

Abstract

We introduce an algebraic structure for studying state-independent contextuality arguments, a key form of quantum non-classicality exemplified by the well-known Peres-Mermin magic square, and used as a source of quantum advantage. We introduce *commutation groups* presented by generators and relations, and analyse them in terms of a string rewriting system. There is also a linear algebraic construction, a directed version of the Heisenberg group. We introduce *contextual words* as a general form of contextuality witness. We characterise when contextual words can arise in commutation groups, and explicitly construct non-contextual value assignments in other cases. We give unitary representations of commutation groups as subgroups of generalized Pauli n-groups.

2012 ACM Subject Classification Theory of computation

Keywords and phrases Contextuality, state-independence, quantum mechanics, Pauli group, group presentations, unitary representations

Digital Object Identifier 10.4230/LIPIcs.FSCD.2024.28

Funding *Samson Abramsky*: EPSRC EP/V040944/1 Resources in Computation, UKRI 10050493 FoQaCiA
Carmen-Maria Constantin: UKRI 10050493 FoQaCiA

1 Introduction

Contextuality is a key form of non-classicality in quantum mechanics, and is the source of quantum advantage in a range of settings, including measurement-based quantum computation [17] and shallow circuits [8, 7]. In classical physics, observable quantities have well-defined values independently of which measurements are performed. This is contradicted by the predictions of quantum mechanics [13], as verified in numerous experiments [6, 10]. These say that values can only be assigned *locally*, in measurement contexts, *i.e.* with respect to sets of measurements which can be performed together, providing observational "windows" of classical information on the quantum system. These windows may overlap, and will agree on their overlaps (*local consistency*), but it is not possible, on pain of logical contradiction, to glue all these pieces of information together (*global inconsistency*).

The strongest form of this phenomenon is *state-independent contextuality*, where the structure of the observables dictates that contextuality arises for any state. The most famous example of this phenomenon is the Peres-Mermin magic square [14], which is constructed from the 2-qubit Pauli group[1]:

[1] We recall the definition of the Pauli group in the Appendix.

$$\begin{array}{ccccc} XI & - & IX & - & XX \\ | & & | & & | \\ IZ & - & ZI & - & ZZ \\ | & & | & & | \\ XZ & - & ZX & - & YY \end{array}$$

Here XI denotes the 2-qubit operator $\sigma_x \otimes I$, and similarly for the other entries. One can now calculate that the operators in each row and column pairwise commute, and hence form a valid measurement context. Moreover, the product of each of the rows, and of the first two columns, is II; while the product of the third column is $-II$.

We shall now see how to recognize contextuality in this example. The key point is that this can be done *a priori*, independently of any observational data. We ask if there is an assignment of outcomes $v : \mathfrak{X} \to \mathbb{Z}_2$, where $\mathfrak{X}$ is the set of operators in the table, subject to the conditions that

1. if p and q commute, then $v(pq) = v(p) + v(q)$.
2. $v(II) = 0$ and $v(-II) = 1$.

Such an assignment is called a *non-contextual value assignment*. If no such assignment exists, this yields an example of *contextuality*. We call this *state-independent*, since it arises purely at the level of the operators in the table, independently of any state.

Note that we only require the homomorphism condition (1) for *commuting* operators, which correspond to observables that can be performed together, in a common context. This is the key idea introduced by Kochen and Specker in their seminal work on contextuality [13].

Now assume for contradiction that such an assignment exists. We obtain the following set of equations over $\mathbb{Z}_2$ from the above table, one for each row and each column:

$$\begin{array}{rclcrcl} a+b+c & = & 0 & \qquad & a+d+g & = & 0 \\ d+e+f & = & 0 & & b+e+h & = & 0 \\ g+h+i & = & 0 & & c+f+i & = & 1 \end{array} \tag{1}$$

Here a is a variable corresponding to $v(XI)$, etc.

Since each variable appears twice in the left hand sides, summing over them yields 0, while summing over the right hand sides yields 1. This yields the required contradiction.

The justification for assuming the partial homomorphism condition comes from the quantum case, where if A and B are commuting observables and ψ is a common eigenvector of A and B, with eigenvalue v for A and w for B, then ψ is an eigenvector for AB with eigenvalue vw. Also, II has the unique eigenvalue $+1$, and $-II$ the unique eigenvalue -1.[2]

We now wish to abstract from the specifics of the Pauli group, and understand the general structure which makes such arguments possible. This leads us to introduce the notion of *commutation group*, to which we now turn.

2 Commutation groups

The idea behind commutation groups is that they are built freely from prescribed commutation relations on a set of generators. Commutation relations play a fundamental role in quantum mechanics, the canonical example being the commutation relation between position and momentum (see e.g. [11]): $[p, q] = i\hbar\mathbb{1}$. We can think of a commutation relation as saying that two elements commute *up to a prescribed scalar*. For this to make sense in a group theoretic

[2] Note that $\{+1, -1\}$ under multiplication is an isomorphic representation of $\mathbb{Z}_2$, with 0 corresponding to $+1$ and 1 to -1 under the mapping $i \mapsto (-1)^i$.

context, we need an action of a suitable (classical, hence abelian) group of scalars or "phases" on the group we are constructing. We are interested here in finite group constructions, so we shall work over the finite cyclic groups $\mathbb{Z}_d$, $d \geq 2$.

Given a finite set $\mathfrak{X}$ of generators, we define a *commutator matrix* to be a map $\mu : \mathfrak{X}^2 \to \mathbb{Z}_d$ which is skew-symmetric, meaning that $\mu(x, y) = -\mu(y, x)$ for all $x, y \in X$. We also assume that $\mu(x, x) = 0$ for all $x \in \mathfrak{X}$.[3]

We shall describe the construction of commutation groups from commutator matrices in two ways: by generators and relations, and by a linear algebraic construction. Both are useful, and convey different intuitions.

2.1 Commutation groups by generators and relations

We briefly review the standard notion of *presentation of a monoid by generators and relations* $\langle \mathfrak{X} \mid R \rangle$. We form the free monoid $\mathfrak{X}^*$, and quotient it by the congruence induced from the relations $R \subseteq \mathfrak{X}^* \times \mathfrak{X}^*$. Explicitly, we define a symmetric relation $\underset{R}{\longleftrightarrow} \subseteq \mathfrak{X}^* \times \mathfrak{X}^*$ by $s \underset{R}{\longleftrightarrow} t$ iff there is $(u, v) \in R \cup R^{-1}$ such that, for some $w_1, w_2 \in \mathfrak{X}^*$, $s = w_1 u w_2$, and $t = w_1 v w_2$. We then take the reflexive transitive closure $\overset{*}{\underset{R}{\longleftrightarrow}}$. This is a monoid congruence, and the quotient $M = \mathfrak{X}^* / \overset{*}{\underset{R}{\longleftrightarrow}}$ is the presented monoid.

Notation. We write relations as $u \doteq v$. We write the empty sequence, which forms the identity element of the free monoid, as 1.

Given a commutator matrix $\mu : \mathfrak{X}^2 \to \mathbb{Z}_d$, we define a set of relations R_{G} over the generators $\mathfrak{X} \sqcup \mathbb{Z}_d$ (using $\sqcup$ for disjoint union), where we write J_k for the generator corresponding to $k \in \mathbb{Z}_d$, and:

- We have relations $R_\mu := \{xy \doteq J_{\mu(x,y)} yx \mid x, y \in \mathfrak{X}\}$.
- We have $R_J := \{J_0 \doteq 1\} \cup \{J_k J_{k'} \doteq J_{k+k'} \mid k, k' \in \mathbb{Z}_d\} \cup \{J_k x \doteq x J_k \mid x \in \mathfrak{X}, k \in \mathbb{Z}_d\}$.
- We have $R_d := \{x^d \doteq 1 \mid x \in \mathfrak{X}\}$.
- Finally, $R_{\mathsf{G}} := R_\mu \cup R_J \cup R_d$.

The resulting monoid $\mathsf{G}(\mu) := \langle \mathfrak{X} \sqcup \mathbb{Z}_d \mid R_{\mathsf{G}} \rangle$ is in fact a group, since every generator has an inverse. We call it the *commutation group* generated by μ.

The J-relations ensure that there is an isomorphic copy of $\mathbb{Z}_d$ in the centre of the group. The key relations are the commutation relations $xy \doteq J_{\mu(x,y)} yx$. Note that these are *directional*, since by skew-symmetry of μ, if $\mu(x, y) = k$, then $yx \doteq J_{-k} xy$. Thus moving x right past y has the opposite "cost" to moving x left past y. This suggests that we can analyze $\mathsf{G}(\mu)$ by a directed *string rewriting system*.

To do this, we fix a linear ordering $x_1 < \cdots < x_n$ on $\mathfrak{X}$.[4] Relative to this ordering, elements of $\mathsf{G}(\mu)$ can be represented as ordered multisets over $\mathfrak{X}$ with multiplicities strictly less than d, together with a "global phase" from $\mathbb{Z}_d$. Explicitly, we define $\mathcal{N}$ to be the set of all expressions $J_k x_1^{k_1} \cdots x_n^{k_n}$, with $k \in \mathbb{Z}_d$, and $0 \leq k_i < d$, $1 \leq i \leq n$. There is an evident bijection $\mathcal{N} \cong \mathbb{Z}_d \times \mathbb{Z}_d^n$. Thus $\mathcal{N}$ has cardinality d^{n+1}.

We now define a string rewriting system on $\mathfrak{X} \sqcup \mathbb{Z}_d$, obtained by orienting a subset of the relations R_{G}, determined by the chosen linear order on $\mathfrak{X}$:

- $\to_\mu := \{xy \to J_{\mu(x,y)} yx \mid x > y\}$.
- $\to_J := \{J_0 \to 1\} \cup \{J_k J_{k'} \to J_{k+k'} \mid k, k' \in \mathbb{Z}_d\} \cup \{x J_k \to J_k x \mid x \in \mathfrak{X}, k \in \mathbb{Z}_d\}$.
- $\to_d := \{x^d \to 1\}$.
- $\to_{\mathsf{G}} := \to_\mu \cup \to_d \cup \to_J$.

[3] Note that if d is even, this does not follow automatically from skew-symmetry.
[4] As we shall see, the choice of ordering is immaterial, leading to isomorphic results.

This induces a relation on $(\mathfrak{X} \sqcup \mathbb{Z}_d)^*$ by $s \to t$ iff for some $u \to_{\mathsf{G}} v$, for some $w_1, w_2 \in (\mathfrak{X} \sqcup \mathbb{Z}_d)^*$, $s = w_1 u w_2$, and $t = w_1 v w_2$.

▶ **Theorem 1.** *The rewrite system $\to_{\mathsf{G}}$ is confluent and normalizing. The set of normal forms is $\mathcal{N}$ (up to identification of J_0 and 1).*

Proof. Given a word $s \in (\mathfrak{X} \sqcup \mathbb{Z}_d)^*$, we define:

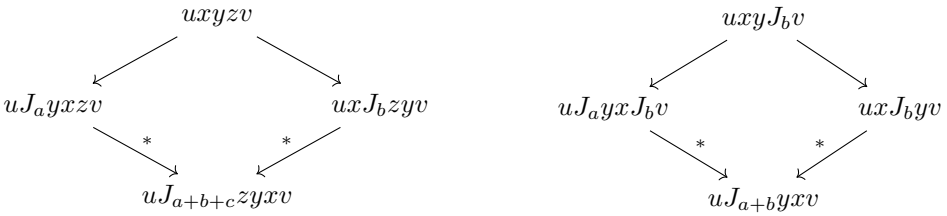
- An $\mathfrak{X}$-inversion in s is (u, v, w, x, y) such that $s = uxvyw$, and $x > y$.
- A J-inversion in s is (u, v, w, x, k) such that $s = uxvJ_k w$.

We define a function $\varphi : (\mathfrak{X} \sqcup A)^* \to \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ by $\varphi(s) = (n, m, l)$, where n is the number of $\mathfrak{X}$-inversions in s, m is the number of J-inversions, and l is the length of s.

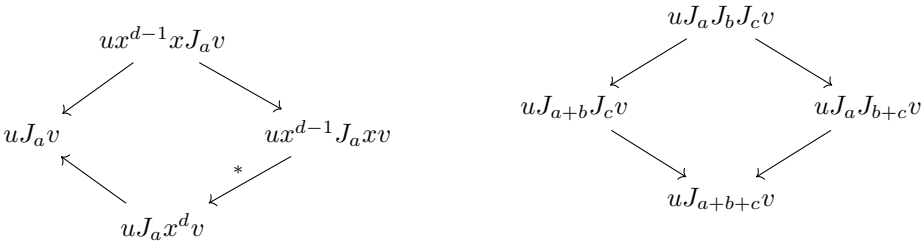
We now observe that for each rewrite $s \to t$ in the above system $\to_{\mathsf{G}}$, $\varphi(s) \succ \varphi(t)$ in the lexicographic ordering on $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$. Indeed, the μ relations decrease the number of $\mathfrak{X}$-inversions, the J-commutation rule decreases the number of J-inversions while not increasing the number of $\mathfrak{X}$-inversions, and the remaining rules decrease length while not increasing the number of inversions. Since this ordering is well-founded, it follows that $\to_{\mathsf{G}}$ is normalizing.

By Newman's Lemma, it now suffices to show that $\to_{\mathsf{G}}$ is weakly confluent. This is verified straightforwardly by examining the critical pairs.

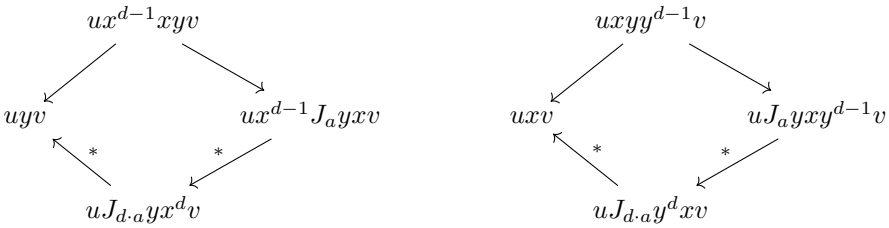
Firstly, consider $x > y > z$, $\mu(x, y) = a$, $\mu(y, z) = b$, $\mu(x, z) = c$:



Next, two cases involving J-generators:



Finally:



Note that $d \cdot a = 0 \mod d$, justifying the final legs. ◀

By virtue of this theorem, we can define a function $\theta : (\mathfrak{X} \sqcup \mathbb{Z}_d)^* \to \mathcal{N}$, which returns the normal form of a word. Note that, if $w \to^* w'$, then by confluence, $\theta(w) = \theta(w')$.

We can use this function to define an equivalence on $(\mathfrak{X} \sqcup \mathbb{Z}_d)^*$ by $s \simeq t$ iff $\theta(s) = \theta(t)$. This equivalence is in fact a congruence, since if $\theta(u) = s = \theta(u')$ and $\theta(v) = t = \theta(v')$, then, using confluence, $\theta(uv) = \theta(st) = \theta(u'v')$.

▶ **Proposition 2.** *For all $s, t \in (\mathfrak{X} \sqcup \mathbb{Z}_d)^*$, $s \simeq t$ iff $s \doteq t$.*

Proof. The left-to-right implication follows immediately since $\to_{\mathsf{G}} \subset R_{\mathsf{G}}$. For the converse, it suffices to show that $s \simeq t$ for all relations $s \doteq t$ in R_{G}, since $\doteq$ is the least congruence containing these relations.

Consider firstly $xy \doteq J_k yx$, where $k = \mu(x, y)$. There are two cases:

1. If $x < y$, then $xy \in \mathcal{N}$, and $J_k yx \to J_k J_{-k} xy \to^* xy$.
2. If $x > y$, then $J_k yx \in \mathcal{N}$, and $xy \to J_k yx$.

The other relations are verified similarly. ◀

We now define a monoid with carrier $\mathcal{N}$. Note that 1 and J_k, $k \in \mathbb{Z}_d$, are in $\mathcal{N}$. We define the multiplication by $u \cdot v := \theta(uv)$.

▶ **Proposition 3.** *$(\mathcal{N}, \cdot, 1)$ is a monoid.*

Proof. We need to verify associativity. This follows from

$$\theta(\theta(uv)w) = \theta(uvw) = \theta(u\theta(vw)) \tag{2}$$

which in turn follows from confluence. ◀

We now define a map $h : \mathsf{G}(\mu) \to \mathcal{N}$ by $h([w]) = \theta(w)$.

▶ **Theorem 4.** *The map h is well-defined, and is a monoid isomorphism $h : \mathsf{G}(\mu) \cong \mathcal{N}$.*

Proof. If $u \doteq v$, then by Proposition 2, $\theta(u) = \theta(v)$. Thus h is well-defined. The fact that it preserves multiplication follows from $\theta(uv) = \theta(\theta(u)\theta(v))$, which follows from confluence. If $w \in \mathcal{N}$, then $h([w]) = \theta(w) = w$. Thus h is surjective. Finally, if $h([u]) = h([v])$, then $u \simeq v$, so by Proposition 2, $[u] = [v]$. ◀

We now come to a key property for applications to contextuality.

▶ **Theorem 5.** *The internal $\mathbb{Z}_d$-action given by the J-generators is faithful: if $J_k \doteq J_{k'}$ in $\mathsf{G}(\mu)$, then $k = k'$.*

Proof. This is immediate from the isomorphic representation given by $\mathcal{N}$, since if $k \neq k'$, J_k and $J_{k'}$ are distinct normal forms. ◀

The parameter d plays a double role in the commutation groups, defining the order of the generators by the relations $x^d = 1$, and also the abelian "phase group" $\mathbb{Z}_d$ acting on the commutation group. We used this double role of d in proving confluence for the rewriting system. This assumption is in fact necessary to obtain a confluent system with a faithful action, as the following example shows.

▶ **Example 6.** We assume the relations $x^d \doteq 1$ for the generators. Consider the word $w \equiv yxy^{d-1}x^{d-1}$, and let $a = \mu(x, y)$. Then $w \doteq J_{(d-1)\cdot a} y^d x^d \doteq J_{(d-1)\cdot a}$, and also $w \doteq J_{-a} xy^d x^{d-1} \doteq J_{-a} x^d \doteq J_{-a}$. Thus to maintain confluence and faithfulness of the action, we require $(d-1) \cdot a = -a$, and hence $d \cdot a = 0$.

Comparison with solution groups

In [9] another way of abstracting from the Peres-Mermin square and similar constructions is pursued, leading to the introduction of *solution groups*. These groups are specified by sets of equations of similar form to (1). The generators appearing together in an equation, and only these, are specified to commute. These groups are shown in [9] to control the question of whether there is a quantum realization for these equations. Importantly, this is shown to be equivalent to the existence of quantum perfect strategies for Alice-Bob non-local games.

A remarkable result of Slofstra [19] shows that solution groups, even over $\mathbb{Z}_2$, are extremely expressive (*i.e.* "wild"). Every finitely presentable group can be embedded in a solution group. It follows immediately that the word problem for solution groups, and hence the quantum realization questions, are undecidable.

By contrast, commutation groups are highly tractable. By Theorem 4, they are always finite. From the proof of termination in Theorem 1, we see that reduction to normal form, and hence the decision procedure for the word problem, is at most quadratic in the length of the word. As we shall see later, every commutation group admits a faithful unitary representation.

2.2 Linear algebraic construction of commutation groups

The characterization of commutation groups in Theorem 4 suggests another description. We shall now use the fact that $\mathbb{Z}_d$ is not just an abelian group, but a commutative ring with unit. We can write a commutator matrix, with a chosen order on the set of generators, as an $n \times n$ matrix with entries in $\mathbb{Z}_d$. We write $\mathfrak{so}(n, \mathbb{Z}_d)$ for the set of all $n \times n$ commutator matrices (skew-symmetric and zero on the diagonal) over $\mathbb{Z}_d$. Given a commutator matrix μ, we write $\check{\mu}$ for its lower triangular part, so that $\mu = \check{\mu} - \check{\mu}^{\mathsf{T}}$.

An $n \times n$ matrix M over $\mathbb{Z}_d$ defines a bilinear form on the free $\mathbb{Z}_d$-module $\mathbb{Z}_d^n$, by $M(\vec{k}, \vec{l}) := \vec{k}^{\top} M \vec{l}$. Now given $\mu \in \mathfrak{so}(\mathbb{Z}_d, n)$, we define a group $H(\mu)$ with carrier $\mathbb{Z}_d \times \mathbb{Z}_d^n$. The group product is defined by

$$(k, \vec{k}) \cdot (l, \vec{l}) \;=\; (k + l + \check{\mu}(\vec{k}, \vec{l}),\, \vec{k} + \vec{l}).$$

Thus it is precisely the phase factor $\check{\mu}(\vec{k}, \vec{l})$ which makes the group non-commutative.

The associativity of the product follows from bilinearity. The unit is $(0, 0)$. The inverse of $(k, \vec{k})$ is $(-k - \check{\mu}(\vec{k}, -\vec{k}), -\vec{k})$.

▶ **Proposition 7.** *For any $\mu \in \mathfrak{so}(n, \mathbb{Z}_d)$, $H(\mu) \cong \mathsf{G}(\mu)$.*

Proof. By Theorem 4, the carriers are in evident bijection: $J_k x_1^{k_1} \cdots x_n^{k_n} \leftrightarrow (k, (k_1, \ldots, k_n))$. We just have to check that the group product is preserved. The only non-imediate part of this is to check that the phase factors agree.

Suppose in $\mathcal{N}$ we have normal forms with vector parts $u = x_1^{k_1} \cdots x_n^{k_n}$ and $v = x_1^{l_1} \cdots x_n^{l_n}$. To combine them into $\theta(uv)$, with vector part $x_1^{k_1+l_1} \cdots x_n^{k_n+l_n}$, we must move l_1 copies of x_1 over k_n copies of x_n, each with a cost of $\mu(x_n, x_1)$; and similarly for the occurrences of $x_{n-1}, \ldots, x_2$ in u, with total cost $\sum_{i>1} k_i \mu(x_i, x_1) l_1$. A similar analysis applies to the occurrences of $x_2, \ldots, x_{n-1}$ in v, leading to a total cost of $\sum_{i>j} k_i \mu(x_i, x_j) l_j$. This is exactly $\vec{k}^{\top} \check{\mu} \vec{l} = \check{\mu}(\vec{k}, \vec{l})$. ◀

Note that we would get the same result if we moved the vector part of u rightwards over the vector part of v. The choice of left/right orientation is just a convention. On the other hand, the use of $\check{\mu}$ rather than μ is significant. As we will see in the next section, using μ would render the structure useless for our purpose of analyzing contextuality.

However, we do retrieve μ as the group-theoretic commutator in $H(\mu)$.

▶ **Proposition 8.** *Given $g = (k, \vec{k}), h = (l, \vec{l}) \in H(\mu)$, their group theoretic commutator is given by $[g, h] := ghg^{-1}h^{-1} = (\check{\mu}(\vec{k}, \vec{l}) - \check{\mu}(\vec{l}, \vec{k}), 0) = (\mu(\vec{k}, \vec{l}), 0)$. In terms of $\mathsf{G}(\mu)$, for $u, v \in X^*$, $[u, v] \doteq J_{k-l}$, where $\theta(uv) \doteq J_k w$, $\theta(vu) \doteq J_l w$.*

As Proposition 7 makes clear, commutation groups are very close to the (discrete version of) the Heisenberg or Heisenberg-Weyl groups [18], and their close relatives the Pauli groups. The novelty lies mainly in our combinatorial mode of presentation of commutation groups, which we will make use of in our analysis of contextuality arguments. It should be noted, though, that the direct equivalent of the usual Heisenberg group construction in our setting would be to use the full commutator matrix μ.[5] As we have mentioned, using μ would yield a non-isomorphic construction, which would not be useful for analyzing contextuality. This perhaps suggests that we can think of commutation groups as a *directed* version of Heisenberg groups.

3 Contextuality arguments in commutation groups

The commutation group has an evident short exact sequence

$$\mathbf{0} \longrightarrow \mathbb{Z}_d \xrightarrow{\ i\ } H(\mu) \xrightarrow{\ \pi_2\ } \mathbb{Z}_d^n \longrightarrow \mathbf{0} \tag{3}$$

where $i(k) = (k, 0)$. This says that it is a non-abelian group extension of $\mathbb{Z}_d^n$ by $\mathbb{Z}_d$. The image of $\mathbb{Z}_d$ lies in the centre of $H(\mu)$, so the extension is central. Because of the non-commutativity of $H(\mu)$, it is easy to see that there is no left-splitting of this extension, *i.e.* a homomorphism $l : H(\mu) \to \mathbb{Z}_d$ such that $l \circ i = \mathsf{id}_{\mathbb{Z}_d}$. One could say that this simple observation is essentially a form of von Neumann's much criticised No-Go theorem for hidden variables [15]. The point of the criticism is that it is not reasonable to ask for a splitting which preserves non-commuting products.

Following Kochen-Specker [13] and the huge literature on ensuing developments, we want to consider only assignments to *observationally accessible contexts*, *i.e.* those constructed from commuting products. A general setting for capturing this idea is provided by *compatible monoids*, introduced in [1] with different terminology. A compatible monoid is a structure $(M, \odot, \cdot, 1)$, where $\odot$ is a reflexive, symmetric relation on M, of "compatibility" or "comeasurability", and $\cdot : \odot \to M$ is a partial binary operation with domain $\odot \subseteq M^2$, such that:

- $x \odot y \ \Rightarrow\ x \cdot y = y \cdot x$,
- $x \odot 1$ for all $x \in M$, and $x \cdot 1 = x$,
- if $x \odot y$, $x \odot z$, and $y \odot z$, then $x \odot (y \cdot z)$ and $(x \cdot y) \odot z$, and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

Homomorphisms of compatible monoids are maps which preserve the compatibility relation, and the monoid operations when defined.

Any monoid M defines a compatible monoid with the same carrier, with $x \odot y$ iff $xy = yx$ in M. We will be interested in the compatible submonoid of M generated by a set $S \subseteq M$. This is the least set T containing $S \cup \{1\}$, and such that, whenever $u, v \in T$ and $u \odot v$, then $u \cdot v \in T$. In particular, we will apply this to $\mathsf{G}(\mu)$ with respect to the generators $\mathfrak{X} \sqcup \mathbb{Z}_d$. We will write $\mathsf{C}(\mu)$ for this compatible submonoid of $\mathsf{G}(\mu)$.

[5] There is a notion of polarized Heisenberg group, but this is isomorphic to the usual presentation.

In terms of $H(\mu)$, we can identify the generators as follows: $k \in \mathbb{Z}_d$ can be identified with the scalar $(k, 0)$, while the generators $\mathfrak{X}$ can be identified with the standard basis E of the free module $\mathbb{Z}_d^n$, $x_i \leftrightarrow e_i := [\underbrace{0, \ldots, 0}_{i-1}, 1, \underbrace{0, \ldots, 0}_{n-i}]^\top$.

We obtain a short exact sequence for $\mathsf{C}(\mu)$:

$$\mathbf{0} \longrightarrow \mathbb{Z}_d \xrightarrow{\ i\ } \mathsf{C}(\mu) \xrightarrow{\ p\ } P \longrightarrow \mathbf{0} \tag{4}$$

Here p is the restriction of the second projection to $\mathsf{C}(\mu)$, and P is its image.

A non-contextual value assignment for the commutation group $\mathsf{G}(\mu)$ is exactly a left splitting of this short exact sequence: *i.e.* a homomorphism $l : \mathsf{C}(\mu) \to \mathbb{Z}_d$ such that $l \circ i = \mathsf{id}_{\mathbb{Z}_d}$. If no such left splitting exists, then we say that $\mathsf{G}(\mu)$ exhibits *state-independent contextuality*.

3.1 Contextual words

We can distill the essential features of "parity proofs" such as the one given for the Peres-Mermin square into a notion of *contextual word*, which provides a witness for state-independent contextuality. This notion was introduced, somewhat informally, in the concrete context of Pauli groups over qubits in [12], but can be formulated generally for any commutation group $\mathsf{G}(\mu)$. A contextual word for $\mathsf{G}(\mu)$ is given by a triple (w, β, k) such that:

- $w \in \mathfrak{X}^+$.
- The number of occurrences of each generator $x \in \mathfrak{X}$ in w is a multiple of d.
- β is a bracketing of w, witnessing that it is in $\mathsf{C}(\mu)$.
- $w \doteq J_k$, where $k \neq 0$.

Bracketings are defined inductively by

$$\beta \in \mathsf{BE} \ ::= \ x \mid (\beta_1, \beta_2).$$

We define $\partial : \mathsf{BE} \to \mathfrak{X}^+$ by $\partial(x) = x$, $\partial(\beta_1, \beta_2) = \partial(\beta_1)\partial(\beta_2)$. If $\partial(\beta) = w$, then w is the word bracketed by β. A bracketing β provides a witness for $w = \partial(\beta) \in \mathsf{C}(\mu)$ if, for every (β_1', β_2') occurring in β, with $u = \partial(\beta_1')$ and $v = \partial(\beta_2')$, $uv \doteq vu$ in $\mathsf{G}(\mu)$.

▶ **Proposition 9.** *If there is a contextual word for $\mathsf{G}(\mu)$, then it is state-independently contextual.*

Proof. If (w, β, k) is a contextual word over S, assume for a contradiction that $l : \mathsf{C}(\mu) \to \mathbb{Z}_d$ is a non-contextual value assignment, *i.e.* a left splitting of (4). The bracketing β witnesses that $w \in \mathsf{C}(\mu)$. By the homomorphism property, $l(w) = \sum_i l(x_i)$, where $w = x_1 \cdots x_n$. Since each $x \in \mathfrak{X}$ occurs with multiplicity kd in w for some $k \geq 0$, $l(w) = 0 \pmod d$. However, we also have $w \doteq J_k$, so we must have $l(w) = l(J_k) = k \neq 0$, yielding the required contradiction. ◀

▶ **Example 10.** Consider the following commutator matrices over $\mathbb{Z}_2$

$$\mu_1 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \qquad \mu_2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \qquad \mu_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

with generators $a < b < c < d$. Then $(w_i, \beta_i, 1)$ is a contextual word for $\mathsf{G}(\mu_i)$, with

$$\begin{array}{lcllcl} w_1 & = & abdccabd & \beta_1 & = & ((ab)(dc))((ca)(bd)) \\ w_2 & = & bdccaabd & \beta_2 & = & (b(dc))((ca)((ab)d)) \\ w_3 & = & dcabbadc & \beta_3 & = & (d(ca))(b(((ba)d)c)) \end{array}$$

▶ **Example 11.** We show that the Peres-Mermin square arises in commutation groups.

Firstly, we show that the tensor product construction underlying the extension of the Pauli group to $\mathbf{Pauli}_n$ has a simple form in terms of group presentations. Given a commutator matrix $\mu : \mathfrak{X}^2 \to \mathbb{Z}_d$, we define $\mu_2 : (\mathfrak{X} + \mathfrak{X})^2 \to \mathbb{Z}_d$ by $\mu_2(x_i, y_i) = \mu(x, y)$, $\mu_2(x_i, y_j) = 0$, $i \neq j$. Thus elements in different copies of $\mathfrak{X}$ commute with each other.

We now consider the commutator matrix with $\mu(x, y) = 1$ for generators x, y. We can define the following Peres-Mermin square over $\mathsf{G}(\mu_2)$:

$$\begin{array}{ccccc} x_1 & — & x_2 & — & x_1x_2 \\ | & & | & & | \\ y_2 & — & y_1 & — & y_1y_2 \\ | & & | & & | \\ x_1y_2 & — & y_1x_2 & — & J_1(x_1y_1)(x_2y_2) \end{array}$$

We can verify that exactly the same algebraic properties hold for this square as in the concrete example: each row and column pairwise commutes, the product of each row and the first two columns is 1, the product of the third column is -1 (or more pedantically, J_1 in additive notation).

We can extract a contextual word from this construction: $((x_1y_2)(y_1x_2))((x_1x_2)(y_1y_2))$. Up to dropping the J_1 factor, and interchanging the commuting pair x_2y_1, this can be read off from product of the bottom row of the square.

This provides a more succinct contextuality witness than the usual parity proof, which amounts to taking the product of all the rows and columns.

A similar treatment can be given of the Mermin star [14].

3.2 Comparison with other Heisenberg groups

We can now see why taking the more standard Heisenberg group construction, defined exactly as for $H(\mu)$, but using μ rather than $\check{\mu}$, would not be suitable for our purposes. Let us denote the construction using μ rather than $\check{\mu}$ by $H^+(\mu)$. By Proposition 8, the commutator in $H(\mu)$ is μ, which means that we can have commuting products $gh = hg$ with non-zero but equal phase factors, which is clearly essential for contextual words to exist. By contrast, the commutator in $H^+(\mu)$ is easily seen to be 2μ, which means in Z_2 that *all products commute*, while in odd orders, no products commute.

4 No state-independent contextuality in odd characteristics

We shall now show that contextual words can only exist over $\mathbb{Z}_d$ if d is even. Moreover, we shall explicitly describe the non-contextual value assignments which exist when d is odd.

In order to prove these results, we will analyze the structure of inversions in bracketed words.

Notation. In this section, we will deal exclusively with non-empty words over the generators, $w \in \mathfrak{X}^+$. We will also write formal sums in variables $v_{x,y}$ to stand in for values of the commutator matrix $\mu(x, y)$. We will use the following notation. If $S = \{\lambda_i\}_{i \in I}$ is a family of inversions, then $\sum S := \sum_{i \in I} v_{x_i, y_i}$, where λ_i is an inversion between x_i and y_i, $x_i > y_i$.

Given a word s, we write $\mathcal{I}(s)$ for the set of inversions in s. Given words s, t, $\mathcal{I}(s, t)$ is the set of inversions between s and t, *i.e.* the set of all (w_1, x, w_2, y) such that w_1x is a prefix of s, w_2y is a prefix of t, and $x > y$.

The following is immediate.

▶ **Lemma 12.** *For all words s, t,*

$$\sum \mathcal{I}(st) \;=\; \sum \mathcal{I}(s) + \sum \mathcal{I}(t) + \sum \mathcal{I}(s,t).$$

In this notation, the equation forcing the global phase factor for a word s to be k is

$$\sum \mathcal{I}(s) \;=\; k.$$

Also, given words s, t, we define the "formal commutator" of s and t to be

$$[\![s,t]\!] \;:=\; \sum \mathcal{I}(s,t) - \sum \mathcal{I}(t,s).$$

The equation forcing s and t to commute is $\sum \mathcal{I}(st) - \sum \mathcal{I}(ts) = 0$. By the previous lemma, this is equivalently written as $[\![s,t]\!] = 0$.

▶ **Lemma 13.** *Let $s^\dagger$ be the reverse of a word s. Then $\sum \mathcal{I}(s,t) \;=\; \sum \mathcal{I}(s^\dagger, t^\dagger)$.*

Proof. Note that $s^\dagger$ defines the same multiset of occurrences of generators as s, so there will be a bijection between the inversions in $\mathcal{I}(s,t)$ and those in $\mathcal{I}(s^\dagger,t^\dagger)$, inducing the same multiset of variables $v_{x,y}$. ◀

We now consider bracketings of words. Given a bracketing β, we define the multiset $\Phi(\beta)$ by

$$\Phi(x) = \varnothing, \qquad \Phi(\beta_1,\beta_2) = \{\!\{(\partial(\beta_1),\partial(\beta_2))\}\!\} \uplus \Phi(\beta_1) \uplus \Phi(\beta_2).$$

Given a word s with bracketing β, we can write $\Phi(\beta)$ as a family $\{(s_i,t_i)\}_{i\in I}$ of adjacent subwords of s corresponding to subexpressions of the full bracketing.

▶ **Lemma 14.** *With notation as above, let $s^\dagger$ be the reverse of s. Then*

$$\sum_{i\in I} [\![s_i,t_i]\!] \;=\; \sum \mathcal{I}(s) \;-\; \sum \mathcal{I}(s^\dagger). \tag{5}$$

Proof. By induction on the length of s. If $s = x$, then the sums on both sides of (5) are empty, and we have the equation $0 = 0$.

In the inductive case, suppose the top-level bracketing of s is $s = uv$. We can write the bracketings of u and v as families $\{(u_j,u'_j)\}_{j\in J}$, $\{(v_k,v'_k)\}_{k\in K}$. Then, applying the induction hypothesis:

$$\begin{aligned}\textstyle\sum_{i\in I}[\![s_i,t_i]\!] &= [\![u,v]\!] \;+\; \textstyle\sum_j [\![u_j,u'_j]\!] \;+\; \sum_k [\![v_k,v'_k]\!] \\ &= \left(\textstyle\sum \mathcal{I}(u,v) - \sum \mathcal{I}(v,u)\right) \;+\; \left(\sum \mathcal{I}(u) - \sum \mathcal{I}(u^\dagger)\right) \;+\; \left(\sum \mathcal{I}(v) - \sum \mathcal{I}(v^\dagger)\right).\end{aligned}$$

By Lemma 12, $\sum \mathcal{I}(s) \;=\; \sum \mathcal{I}(uv) \;=\; \sum \mathcal{I}(u,v) + \sum \mathcal{I}(u) + \sum \mathcal{I}(v)$. Since $s^\dagger = v^\dagger u^\dagger$, applying Lemma 12 again yields $\sum \mathcal{I}(s^\dagger) \;=\; \sum \mathcal{I}(v^\dagger,u^\dagger) + \sum \mathcal{I}(v^\dagger) + \sum \mathcal{I}(u^\dagger)$. Applying Lemma (13) and rearranging terms yields (5). ◀

▶ **Lemma 15.** *Let w be a word in which each generator x occurs n_x times, modulo d. Then*

$$\sum \mathcal{I}(w) + \sum \mathcal{I}(w^\dagger) = \sum_{x<y} n_y n_x v_{yx}$$

In particular, when each generator occurs a multiple of d times, we have $\sum \mathcal{I}(w) \;=\; -\sum \mathcal{I}(w^\dagger)$.

Proof. In order to count the number of occurrences of the variable v_{yx}, consider each occurrence of y within w. For the i^{th} occurrence we can write $w = u_i y v_i$ and for each x such that $x < y$, the m_i occurrences of x in v_i will yield m_i inversions in w, while the occurrences of x in u_i will yield n_i inversions in $w^\dagger$. Thus, the total multiplicity of $v_{x,y}$ in $\sum \mathcal{I}(w)$ will be $\sum_i m_i$, where i ranges over occurrences of y in w. Similarly, the total multiplicity of $v_{x,y}$ in $\sum \mathcal{I}(w^\dagger)$ will be $\sum_i n_i$. Since for each i, $m_i + n_i = n_x$ we will have the overall multiplicity

$$n_{yx} = \sum_{i=1}^{n_y} m_i + \sum_{i=1}^{n_y} n_i = \sum_{i=1}^{n_y} n_x = n_y n_x.$$

When each n_x is a multiple of d we therefore have $\sum \mathcal{I}(w) + \sum \mathcal{I}(w^\dagger) = 0 \pmod d$. ◀

▶ **Theorem 16.** *If (w, β, k) is a contextual word over $\mathbb{Z}_d$, then d is even.*

Proof. Since (w, β, k) is contextual, we have $[\![s, t]\!] = 0$ for all bracketed subexpressions (s, t) in β. Hence summing over all such subexpressions yields $\sum_i [\![s_i, t_i]\!] = 0$. By Lemma 14, this implies that $\sum \mathcal{I}(w) - \sum \mathcal{I}(w^\dagger) = 0$. Applying Lemma 15 yields $2\sum \mathcal{I}(w) = 0$. The contextuality of (w, β, k) forces $\sum \mathcal{I}(w) = k$, where $k \neq 0$. We can only have a non-zero solution of $2k = 0 \pmod d$ if d is even. ◀

▶ **Theorem 17.** *If w_1 and w_2 are words in $\mathfrak{X}^+$ formed out of commuting products and which have the same multiset of generators, modulo d, then if d is odd their overall commutation factors are equal.*

Proof. Since w_1 and w_2 are formed out of commuting products, each of the formal commutators corresponding to the sub-expressions of w_1 and w_2 is equal to zero, hence $\sum \mathcal{I}(w_i) = \sum \mathcal{I}(w_i^\dagger)$. From Lemma 15 it follows that

$$2\sum \mathcal{I}(w_i) = \sum_{x<y} n_y^i n_x^i \cdot v_{yx}$$

The right hand side of this equation is the same for w_1 and w_2, since the number n_x^i of occurrences of each generator is equal modulo d in the two words. Since d is odd, the equation $2x = k \pmod d$ has a unique solution for any $k \in \mathbb{Z}_d$, and $\sum \mathcal{I}(w_1) = \sum \mathcal{I}(w_2)$. ◀

▶ **Theorem 18.** *Let μ be a commutator matrix over $\mathbb{Z}_d$. If d is odd, there is a non-contextual value assignment $\upsilon : \mathsf{C}(\mu) \to \mathbb{Z}_d$.*

Proof. We use the vector representation of $\mathsf{C}(\mu) \subseteq \mathsf{G}(\mu)$. Define $S := \{\vec{k} \in \mathbb{Z}_d^n \mid \exists k.\, (k, \vec{k}) \in \mathsf{C}(\mu)\}$. By Lemma 17, there is a unique $\varphi(\vec{k}) \in \mathbb{Z}_d$ such that every word $w \in \mathfrak{X}^+$ which can be formed by commuting products and evaluates to a normal form $\theta(w)$ with corresponding vector part $\vec{k} \in S$ has global phase factor $\varphi(\vec{k})$. Thus if w is such a word, $\varphi(\vec{k}) = \sum \mathcal{I}(w)$. By Theorem 16, $\varphi(\mathbf{0}) = 0$. Given $(k, \vec{k}) \in \mathsf{C}(\mu)$, we define $\upsilon : (k, \vec{k}) \mapsto k - \varphi(\vec{k})$. Clearly this is left-inverse to the inclusion $\iota : \mathbb{Z}_d \to \mathsf{C}(\mu)$. We must verify the homomorphism condition. Given a commuting product $(k, \vec{k}) \cdot (l, \vec{l}) = (k + l + \breve{\mu}(\vec{k}, \vec{l}), \vec{k} + \vec{l})$ in $\mathsf{C}(\mu)$, we must show that

$$(k - \varphi(\vec{k})) + (l - \varphi(\vec{l})) \;=\; (k + l + \breve{\mu}(\vec{k}, \vec{l})) - \varphi(\vec{k} + \vec{l}),$$

i.e. that $\varphi(\vec{k} + \vec{l}) = [\varphi(\vec{k}) + \varphi(\vec{l}) + \breve{\mu}(\vec{k}, \vec{l})]$. Taking words s, t evaluating to $\vec{k}$, $\vec{l}$, this is $\sum \mathcal{I}(st) = \sum \mathcal{I}(s) + \sum \mathcal{I}(t) + \sum \mathcal{I}(s, t)$, *i.e.* Lemma 12. ◀

5 Contextuality in even characteristics

We now show that contextual words exist in abundance in even characteristics. Firstly, we characterize the circumstances under which non-contextual value assignments *do* arise.

Given $S \subseteq \mathsf{C}(\mu)$, we define $\mathcal{Z}(S) := \{a \in S \mid \forall b \in S.\, a \odot b\}$. A *graph* will always mean a reflexive undirected graph, *i.e.* a set of vertices with a reflexive, symmetric relation.

A *cluster graph* is a coproduct (disjoint union) of complete graphs. Equivalently, it is a graph in which the adjacency relation is transitive, so that the maximal cliques are the equivalence classes, and hence disjoint, with no adjacencies between them.

We will show that, if $(\mathsf{C}(\mu) \setminus \mathcal{Z}(\mathsf{C}(\mu)), \odot)$ is a cluster graph, every empirical model over $\mathsf{C}(\mu)$ has global sections, which are exactly non-contextual value assignments.

We briefly review what we need of empirical models; for further details, see [4, 3]. A maximal clique over the graph $(\mathsf{C}(\mu), \odot)$ is a (total) commutative sub-monoid of $\mathsf{C}(\mu)$: closure under products is implied by maximality. Moreover, it contains $\mathcal{Z}(\mathsf{C}(\mu))$. Let $\mathscr{M}$ be the set of maximal cliques. Note that the union of this family is $\mathsf{C}(\mu)$.

A (possibilistic) empirical model over $\mathsf{C}(\mu)$ assigns to each $C \in \mathscr{M}$ a non-empty set of homomorphisms $s : C \to \mathbb{Z}_d$ which split the inclusion $\mathbb{Z}_d \hookrightarrow C$. We write $\{e_C\}_{C \in \mathscr{M}}$ for this family of sets of homomorphisms. The family is moreover required to satisfy the following *local consistency* property: for all $C, C' \in \mathscr{M}$, $e_C|_{C \cap C'} = e_{C'}|_{C \cap C'}$, where e.g

$$e_C|_{C \cap C'} := \{s|_{C \cap C'} \mid s \in e_C\}.$$

We say that such an empirical model is non-contextual (in the sense of not strongly contextual [4]) if there exists a *global section*: a homomorphism $s : \mathsf{C}(\mu) \to \mathbb{Z}_d$ such that $s|_C \in e_C$ for all $C \in \mathscr{M}$. Such a global section is necessarily a left splitting, and hence a non-contextual value assignment for $\mathsf{C}(\mu)$.

▶ **Theorem 19.** *If $(\mathsf{C}(\mu) \setminus \mathcal{Z}(\mathsf{C}(\mu)), \odot)$ is a cluster graph, then every empirical model over $\mathsf{C}(\mu)$ is non-contextual.*

Proof. Let $N := \mathsf{C}(\mu) \setminus \mathcal{Z}(\mathsf{C}(\mu)), Z := \mathcal{Z}(\mathsf{C}(\mu))$. Each maximal clique of $(\mathsf{C}(\mu), \odot)$ is of the form $C \sqcup Z$, where C is a maximal clique of $(N, \odot)$. Let e be an empirical model, and consider $s \in e_{C \sqcup Z}$ for $C \sqcup Z \in \mathscr{M}$. We can write $s = [s_C, s_Z] : C \sqcup Z \to \mathbb{Z}_d$. By the local consistency property for e, for any $C' \neq C$ maximal in $(N, \odot)$, there is $s_{C'} : C' \to \mathbb{Z}_d$ such that $s' = [s_{C'}, s_Z] : C' \sqcup Z \to \mathbb{Z}_d \in e_{C' \sqcup Z}$. Morever, as C', C'' range over maximal cliques of $(N, \odot)$, since $C' \cap C'' = \varnothing$, $s' = [s_{C'}, s_Z]$ is compatible with $s'' = [s_{C''}, s_Z]$, *i.e.* $s'|_Z = s_Z = s''|_Z$. Thus we obtain a pairwise compatible family of sections $\{[s_C, s_Z]\}_{C \sqcup Z \in \mathscr{M}}$.

Since $\mathscr{M}$ covers $\mathsf{C}(\mu)$, this family determines a unique function $s : \mathsf{C}(\mu) \to \mathbb{Z}_d$. We must check the homomorphism condition. This holds because whenever $g \odot h$, $\{g, h\} \subseteq C$ for some $C \in \mathscr{M}$, hence $s(gh) = s_C(gh) = s_C(g) + s_C(h) = s(g) + s(h)$. ◀

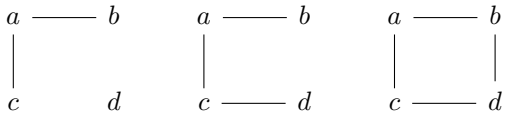
Note that in the last part of the argument, we were verifying the sheaf property for the cover $\mathscr{M}$ over the presheaf of left splittings on cliques in $(\mathsf{C}(\mu), \odot)$.

One remaining question is whether empirical models over $\mathsf{C}(\mu)$ actually exist.[6] We shall discuss unitary representations of commutation groups in the next section. Given a quantum realization of the associated measurements, we can always obtain an empirical model by applying any quantum state.

[6] The issue is whether we can have a non-empty model satisfying the local consistency conditions.

5.1 Positive results

We now assume that $(\mathsf{C}(\mu) \setminus \mathcal{Z}(\mathsf{C}(\mu)), \odot)$ is *not* a cluster graph, which means that there are elements a, b, c such that $a \odot b$, $a \odot c$, but not $b \odot c$. Since a is not in $\mathcal{Z}(\mathsf{C}(\mu))$, there must be some d such that not $a \odot d$. Allowing for the various possibilities for commutativity of d with b and c, up to relabelling this gives us the following three compatibility graphs [12]:



(6)

5.1.1 The $\mathbb{Z}_2$ case

In the case where μ is a commutator matrix over $\mathbb{Z}_2$, we can give a definitive characterisation of contextuality in $\mathsf{C}(\mu)$. This follows similar lines to [12], in the general setting of commutation groups.

▶ **Theorem 20.** *If μ is a commutator matrix over $\mathbb{Z}_2$, then the following are equivalent:*

1. *$\mathsf{C}(\mu)$ is contextual.*
2. *There are contextual words over $\mathsf{C}(\mu)$.*
3. *The graph $(\mathsf{C}(\mu), \odot)$ contains one of the graphs in (6) as an induced sub-graph.*

Proof. The implication (2) ⇒ (1) is Proposition 9. By contraposition, (1) ⇒ (3) follows from Theorem 19. Now assume (3). If a, b, c, d are generators, the matrices μ_i given in Example 10 correspond to the graphs in (6), and the corresponding contextual words given in the Example show that (2) holds. Otherwise, these elements arise as commuting products, each of which can be described by a suitably bracketed word. If any of these words has global phase factor 1, they are already contextual words. Otherwise, we can substitute them into the words given in Example 10 to obtain contextual words. ◀

5.1.2 Beyond $\mathbb{Z}_2$: padding, splitting and variable changes

We can transfer contextual words from $\mathbb{Z}_2$ to $\mathbb{Z}_{2k}$, using the embedding $\mathbb{Z}_2 \rightarrowtail \mathbb{Z}_{2k}$ which sends 1 to k, which can be applied to a commutator matrix over $\mathbb{Z}_2$ to produce one over $\mathbb{Z}_{2k}$. If we take any of the contextual words w from Example 10, we can then perform a simple padding construction. We append $a^{2k-2}b^{2k-2}c^{2k-2}d^{2k-2}$ to w, and this produces a contextual word over $\mathbb{Z}_{2k}$.

Can we construct contextual words over $\mathbb{Z}_{2k}$ using matrix values other than 0 and k? By Theorem 16, the global phase factor for a contextual word over $\mathbb{Z}_{2k}$ must be k, but we may use other values from $\mathbb{Z}_{2k}$ in constructing the word. We can use a splitting construction to achieve this. We illustrate the idea with a simple example over $\mathbb{Z}_4$. Given the contextual word $((ab)(dc))((ca)(bd))$ from Example 10, we split the generator a into a_1 and a_2. We can use the commutator matrix

$$\mu = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 3 & 3 & 1 \\ 3 & 1 & 0 & 2 & 0 \\ 3 & 1 & 2 & 0 & 0 \\ 3 & 3 & 0 & 0 & 0 \end{bmatrix}$$

and obtain the contextual word $[((a_1a_2)b)(cd)][((a_1a_2)c)(bd)][a_1^2a_2^2b^2c^2d^2]$, using also the padding construction described previously.

5.1.3 Classification of contextuality for matrices in Darboux normal form

Our overall aim is to give a complete classification of which commutation groups $\mathsf{G}(\mu)$ admit contextual words. We shall achieve this for matrices μ in *Darboux normal form*, *i.e.* whose only non-zero entries occur in block 2×2 matrices on the main diagonal of the form

$$\begin{matrix} 0 & \lambda_i \\ -\lambda_i & 0 \end{matrix}$$

Given a matrix μ over $\mathbb{Z}_{2n}$, which is in Darboux normal form, it is possible to decide whether it supports contextual words by considering the parity, relative to n, of the non-zero entries of μ. By relative parity, we mean whether the power with which 2 appears in the prime factor decomposition of n is lower than the power with which it appears in the prime factor decomposition of each of the non-zero entries. Thus, if $n = n' \times 2^y$ and $\lambda = l \times 2^x$, where n' and l' are both odd integers, we say that λ is even relative to n if $x > y$ and that λ is odd relative to n if $x \leq y$.

Firstly, a preliminary lemma. We use the notation $m \vdots n$ to mean that m is divisible by n.

▶ **Lemma 21.** *If a word s is formed out of commuting products, and s_a and s_b denote the multiplicities with which a and b appear within s, then $s_a s_b \vdots 2^{k+1}$.*

Proof. We prove this by induction on the length of s. If s is length 1 then either s_a or s_b, or both, are zero, and the statement holds trivially. Assume that the statement holds for words of length less than or equal to L and let s be a word of length $L+1$. Then $s = uv$ for some u and v of length at most L and let u_a, u_b, v_a, v_b denote the respective multiplicities of a and b within u and v. Since u and v commute, we must have

$$(u_a v_b - u_b v_a) \vdots 2^{k+1}$$

By the inductive hypothesis $u_a u_b \vdots 2^{k+1}$ and $v_a v_b \vdots 2^{k+1}$ and therefore $u_a u_b v_a v_b \vdots 2^{2k+2}$. If $u_a v_b \not\vdots 2^{k+1}$ then $u_b v_a$ must be divisible by 2^{k+1} and this would contradict the commutativity condition. Hence both $u_a v_b$ and $u_b v_a$ are divisible by 2^{k+1}. This allows us to complete the inductive proof, as $s_a = u_a + v_a$ and $s_b = u_b + v_b$ and so the product $s_a s_b$ expands as a sum of terms which are each divisible by 2^{k+1}:

$$s_a s_b = u_a u_b + u_a v_b + u_b v_a + v_a v_b. \qquad \blacktriangleleft$$

▶ **Theorem 22.** *If μ is in Darboux normal form, then there is a contextual word over $\mathsf{G}(\mu)$ if and only if there are two non-zero entries above the main diagonal, $\lambda_i = l_i \times 2^{x_i}$ and $\lambda_j = l_j \times 2^{x_j}$ which are both odd relative to n.*

Proof. If we can find two non-zero entries above the main diagonal, $\lambda_i = l_i \times 2^{x_i}$ and $\lambda_j = l_j \times 2^{x_j}$ which are both odd relative to n and we denote their corresponding variables by a, b, c, d, then we can form the contextual word

$$((\underbrace{a \ldots a}_{k}\ \underbrace{c \ldots c}_{k})(bd))((\underbrace{a \ldots a}_{k} d)(b \underbrace{c \ldots c}_{k}))(\underbrace{a \ldots a}_{m})(\underbrace{b \ldots b}_{2n-2})(\underbrace{c \ldots c}_{m})(\underbrace{d \ldots d}_{2n-2})$$

where $k = n' \times 2^{y-x_j}$, $m = n' \times 2^{y-x_i}(2^{x_i+1} - 2)$ and $k + m = 2n$. It is straightforward to check that all the brackets commute and that the overall commutation factor is equal to

$$n' \times 2^{y-x_i} \times l_i \times 2^{x_i} = n \times l_i$$

which is equal to n modulo $2n$, since l_i is odd.

On the other hand, if all the non-zero entries of μ are even relative to n then we will not be able to get any word w with a non-zero commutation factor since, as we have shown in Section 4, the commutation factor of w must satisfy the equation

$$2\sum \mathcal{I}(w) = 0$$

In $\mathbb{Z}_{2n}$ the only non-zero solution to this equation is $\sum \mathcal{I}(w) = n = n' \times 2^y$ and since all the commutation variables in the matrix μ have a factor of 2 greater than y, any linear combination of them will also have a factor of 2 greater than y, and so will not yield a commutation factor equal to n modulo $2n$.

Finally, we can show that if only one non-zero entry is odd relative to n, while all the others are relatively even, then contextual words cannot exist. For simplicity of notation, we will show this for 4 generators but the proof, which is essentially a parity argument, works equally well for any number of generators. Let $n = n' \times 2^y$, as before, and let a and b denote the two variables whose corresponding entry in the commutation matrix is $m \times 2^{y-k}$ for some odd m and $k \geq 0$. By assumption, all other entries are of the form $m' \times 2^{y+1+t}$ for some odd m' and $t \geq 0$. Then any bracketed subexpression of the form

$$w = (a^{l_a} b^{l_b} c^{l_c} d^{l_d})(a^{r_a} b^{r_b} c^{r_c} d^{r_d})$$

commutes only if

$$2^{y-k} \times m(l_a r_b - l_b r_a) + 2^{y+1+t} \times m'(l_c r_d - l_d r_c) = N \times 2^{y+1} \times n'$$

Since the right hand side is a multiple of 2^{y+1} and the terms on the left hand side coming from the relatively even entries are also multiples of 2^{y+1} and m is odd, it follows that

$$(l_a r_b - l_b r_a) \vdots 2^{k+1}$$

By Lemma 21, $l_b r_a$ is divisible by 2^{k+1} and so the contribution to the overall commutation factor, which is

$$2^{y-k} \times m l_b r_a + 2^{y+1+t} \times m' l_d r_c$$

will also be a multiple of 2^{y+1}. Recall that the only possible non-zero value for the overall commutation factor is n modulo $2n$ which implies

$$\sum \mathcal{I}(w) = (2N+1)n = (2N+1)n' \times 2^y$$

and therefore a sum of terms which are divisible by 2^{y+1} cannot yield a non-zero overall commutation factor, which completes the proof. ◀

5.1.4 Reduction to Darboux normal form

Every commutator matrix can be reduced to one in Darboux normal form. This is standard over a field, but less obvious over $\mathbb{Z}_d$ for arbitrary d, so we include a proof.

Note that since μ plays the role of a bilinear form, if we wish to perform a change of basis preserving this form, we must perform the corresponding row and column operations on the matrix μ. These operations are encoded by an invertible base change matrix U; the resulting matrix $U^T \mu U$ is said to be *cogredient* to μ.

▶ **Lemma 23.** *Every commutation matrix μ is cogredient to a skew-symmetric matrix μ_d whose only non-zero entries occur directly above and below the main diagonal. We call this the standard form of the commutation matrix.*

Proof. We start by noting that the "swapping" matrix $U_{i,j}$ which is obtained by swapping the i^{th} and j^{th} columns of the identity matrix is self-inverse over $\mathbb{Z}_{2n}$ and

$$U_{i,j}^T \mu U_{i,j}$$

is the commutation matrix obtained from μ by first swapping the i^{th} and j^{th} rows of μ and then the i^{th} and j^{th} columns.

Similarly, the "adding" matrix $V_{i,j}^{\alpha}$ which is obtained by adding to the i^{th} column of the identity matrix α times the j^{th} column is invertible, its inverse being $V_{i,j}^{-\alpha}$. Hence the matrix

$$V_{i,j}^{\alpha T} \mu V_{i,j}^{\alpha}$$

is cogredient with μ and has the corresponding effect of adding α times the j^{th} row/column of μ to its i^{th} row/column.

Using these two types of cogredient operations it is possible, using Euclid's algorithm to change μ into a cogredient matrix μ_d with the desired property.

The first step is to consider the n^{th} row of the matrix μ:

$$\begin{array}{ccccc} \ddots & \vdots & \vdots & \vdots & \vdots \\ \dots & 0 & * & * & -c \\ \dots & * & 0 & * & -b \\ \dots & * & * & 0 & -a \\ \dots & c & b & a & 0 \end{array}$$

If it has k non-zero entries, we can use suitable swapping $U_{i,j}$ matrices to bring those entries to the right of all zero entries, ordered ascendingly. Then if $a = \mu(n, n-1) > \mu(n, n-2) = b$ we can use $V_{n-1,(n-2)}^{\alpha}$ and $U_{n-1,n-2}$ matrices to perform Euclid's algorithm on the bottom entries of these penultimate two columns, resulting in a cogredient matrix μ_1 with $\mu_1(n, n-2) = 0$ and $\mu_1(n, n-1) = gcd(a, b)$. For example, if the first step of the algorithm gives the decomposition $a = bq_1 + r_1$ then the matrix

$$\mu' = U_{n-1,n-2}^T V_{n-1,n-2}^{-q_1 T} \mu V_{n-1,n-2}^{-q_1} U_{n-1,n-2}$$

will have $\mu'(n, n-2) = r_1$ and $\mu'(n, n-1) = b$. If r_1 is non-zero, we can continue iterating the next steps of the algorithm, until eventually we reach μ_1.

The next step is to consider $c = \mu_1(n, n-3)$ and use suitable $U_{n-3,n-1}$ and $V_{n-1,n-3}^{\alpha}$ matrices to again perform Euclid's algorithm, resulting in a matrix μ_2 for which $\mu_2(n, n-2) = \mu_2(n, n-3) = 0$ and $\mu_2(n, n-1) = gcd(a, b, c)$. And we proceed to eliminate all the k next non-zero entries of the last row, thus leaving

$$\mu_{k-1}(n, n-1) = gcd(\mu(n, n-1), \mu(n, n-2), \dots, \mu(n, n-k))$$

as the only non-zero entry on the n^{th} row. And since cogredient operations result in skew-symmetric matrices, the only non-zero entry on the n^{th} column will also be the one above the main diagonal.

We can repeat these steps to clear out the t non-zero entries on row $n-1$, which are to the left of the $(n-1, n-2)$ position. This results in some matrix μ_{t-1} whose only nonzero entries on row $n-1$ are $\mu_{t-1}(n-1, n) = \mu_{k-1}(n-1, n)$ and

$$\mu_{t-1}(n-1, n-2) = gcd(\mu_{k-1}(n-1, n-2), \mu_{k-1}(n-1, n-3), \dots, \mu_{k-1}(n-1, n-t)).$$

We proceed similarly with the remaining rows, eventually resulting in a matrix μ_d in standard form. ◀

▶ **Theorem 24.** *Every commutation matrix μ is cogredient to a matrix μ_D in Darboux normal form, whose only non-zero entries occur in block 2×2 matrices on the main diagonal of the type*

$$\begin{matrix} 0 & \lambda_i \\ -\lambda_i & 0 \end{matrix}$$

Proof. From Lemma 23, we know that μ is cogredient to a matrix μ_d in standard form. We describe an algorithm which, given a 4×4 diagonal block of μ_d of the type

$$\begin{matrix} 0 & a & 0 & 0 \\ -a & 0 & b & 0 \\ 0 & -b & 0 & c \\ 0 & 0 & -c & 0 \end{matrix}$$

performs cogredient operations on μ_d to produce a block in Darboux normal form of the type

$$\begin{matrix} 0 & \lambda_1 & 0 & 0 \\ -\lambda_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda_2 \\ 0 & 0 & -\lambda_2 & 0 \end{matrix}$$

Assume without loss of generality that the 4×4 block is in the top left-hand corner of μ_d. If $b = 0$ the block already has the desired format. If c is equal to zero, we can use "swapping" $U_{1,3}$ and suitable "adding" $V^{\alpha}_{1,3}$ matrices to perform Euclid's algorithm on the non-zero entries in the first and third columns, resulting in a block of the desired format, with $\lambda_1 = gcd(a, b)$ and $\lambda_2 = 0$, and the same type of procedure can be used when $a = 0$.

In the remaining case, when all entries are non-zero, we have to distinguish two scenarios: first, if $aq = b$ then $V^{qT}_{3,1} \mu_d V^{q}_{3,1}$ has the top left-hand block in Darboux normal form with $\lambda_1 = a$ and $\lambda_2 = c$.

Otherwise, performing Euclid's algorithm as above will initially result in a block with non-zero entries away from the main diagonal:

$$\begin{matrix} 0 & gcd(a,b) & 0 & y \\ -gcd(a,b) & 0 & 0 & 0 \\ 0 & 0 & 0 & x \\ -y & 0 & -x & 0 \end{matrix}$$

We now make a slight modification to the procedure in Lemma 23 in order to bring this block matrix back to standard form: instead of applying Euclid's algorithm to reduce the entries on the last row and column, we use it to reduce the entries on the first row and column. The resulting matrix will be of the form

$$\begin{matrix} 0 & gcd(a,b,y) & 0 & 0 \\ -gcd(a,b,y) & 0 & y' & 0 \\ 0 & -y' & 0 & x' \\ 0 & 0 & -x' & 0 \end{matrix}$$

At this point we can repeat the steps outlined so far until we eventually bring the block to Darboux normal form. Since we started with the assumption that a is not a factor of b, the greatest common divisor of a, b and y must be strictly less than a in the divisibility order, so eventually the process will terminate. ◀

Discussion. There is an important caveat to this result. We have defined contextuality for $\mathsf{G}(\mu)$ in terms of $\mathsf{C}(\mu)$, which is defined relative to the set of generators $\mathfrak{X}$. When transforming μ to μ' in Darboux normal form, we will have $\mathsf{G}(\mu) \cong H(\mu) \cong H(\mu') \cong \mathsf{G}(\mu')$, but this transformation will not preserve the generators. In particular, the new generators corresponding to the transformed basis for μ' may correspond to words in the old generators which cannot be formed from commuting products. This means that a contextual word over $\mathsf{G}(\mu')$ may not correspond to one over $\mathsf{G}(\mu)$.

6 Unitary representation

Since $\mathsf{G}(\mu)$ is a finite group, it has unitary representations. Indeed, every linear representation is equivalent to a unitary one. We wish to have unitary representations which faithfully preserve the internal $\mathbb{Z}_d$-action.

We use the qudit Hilbert space $\mathscr{H}_d := \mathbb{C}^d$, with basis vectors $|k\rangle$ labelled by elements of $\mathbb{Z}_d$. The tensor product of n copies of this space, $\mathscr{H}_{n,d}$, has basis vectors $|\vec{k}\rangle$ labelled by $\vec{k} \in \mathbb{Z}_d^n$. We write $\mathsf{U}(\mathscr{H}_{n,d})$ for the unitary group on $\mathscr{H}_{n,d}$. The centre of this group is isomorphic to the circle group, $\mathsf{U}(1) := \{z \in \mathbb{C} \mid |z| = 1\}$. For each $d \geq 2$, this contains the cyclic subgroup of the d'th complex roots of unity. We write $\omega := e^{\frac{2\pi i}{d}}$ for the primitive d'th root of unity. The map $k \mapsto \omega^k$ is an isomorphism from $\mathbb{Z}_d$ to the multiplicative group of d'th complex roots of unity.

Given a commutator matrix $\mu \in \mathfrak{so}(n, \mathbb{Z}_d)$, we shall define a representation $\rho : H(\mu) \to \mathsf{U}(\mathscr{H}_{n,d})$: $\rho(k, \vec{k}) |\vec{l}\rangle \;=\; \omega^{k+\check{\mu}(\vec{k},\vec{l})} |\vec{l} + \vec{k}\rangle$.

▶ **Proposition 25.** *For each $(k, \vec{k}) \in H(\mu)$, $\rho(k, \vec{k})$ is a well-defined unitary operation. Moreover, ρ is an injective group homomorphism which preserves scalars, i.e. $\rho(k, 0) = \omega^k \mathbb{1}$.*

Proof. The verification that ρ is a homomorphism amounts to showing that

$$\rho(k, \vec{k}) \circ \rho(k', \vec{k}') |\vec{l}\rangle \;=\; \rho(k + k' + \check{\mu}(\vec{k}, \vec{k}'), \vec{k} + \vec{k}') |\vec{l}\rangle$$

which reduces to

$$\check{\mu}(\vec{k}, \vec{k}') + \check{\mu}(\vec{k} + \vec{k}', \vec{l}) \;=\; \check{\mu}(\vec{k}', \vec{l}) + \check{\mu}(\vec{k}, \vec{k}' + \vec{l})$$

which follows from bilinearity. ◀

Representation in Pauli groups

The generalized Pauli groups $\mathbb{P}_{n,d}$ are the subgroups of $\mathsf{U}(\mathscr{H}_{n,d})$ generated by the X and Z operations. These operations are defined on $\mathscr{H}_d$ by $X |k\rangle = |k+1\rangle$, and $Z |k\rangle = \omega^k |k\rangle$. These are the Sylvester "shift" and "clock" matrices [20], and can be seen as discrete versions of position and momentum operators. Note that they satisfy the basic commutation relation $ZX = \omega XZ$. They are then extended to $\mathscr{H}_{n,d}$ as $X_i := \underbrace{I \otimes \cdots \otimes I}_{i-1} \otimes X \otimes \underbrace{I \otimes \cdots \otimes I}_{n-i}$, and similarly for Z_i, $i = 1, \ldots, n$. Note that the commutator matrix for the generators X_i, Z_i is in Darboux normal form: the only non-zero entries are $\mu(Z_i, X_i) = 1$, $\mu(X_i, Z_i) = -1 \pmod d$.

▶ **Proposition 26.** *The image of $H(\mu)$ under ρ is a subgroup of $\mathbb{P}_{n,d}$.*

Proof. Given an element e_i of the standard basis of $\mathbb{Z}_d^n$, we have $\rho(e_i) = X_i \prod_{j=1}^n Z_j^{\check{\mu}_{i,j}}$, which can be verified by a simple computation:

$$\begin{aligned} X_i \prod_{j=1}^n Z_j^{\check{\mu}_{i,j}} |k_1\rangle \otimes \cdots \otimes |k_n\rangle &= X_i(\omega^{\check{\mu}_{i,1}k_1}|k_1\rangle \otimes \cdots \otimes \omega^{\check{\mu}_{i,n}k_n}|k_n\rangle) \\ &= X_i(\prod_j \omega^{\mu_{i,j}k_j})\,|\vec{k}\rangle \\ &= \omega^{\sum_j \check{\mu}_{i,j}k_j} X_i\,|\vec{k}\rangle \\ &= \omega^{\check{\mu}(e_i,\vec{k})}\,|\vec{k}+e_i\rangle \\ &= \rho(e_i)\,|\vec{k}\rangle. \end{aligned}$$

Since $H(\mu)$ is generated by the e_i and the scalar $(1,0)$, this yields the result. ◀

This result shows the universality of the Pauli operations for expressing discrete commutation relations. At the same time, the structural tools made available by the presentations of commutation groups allow for a fine-grained analysis of the "algebra of contextuality".

7 Outlook

Non-commutativity is a fundamental mathematical feature of quantum mechanics, distinguishing it from classical physics. But in many key cases, we do not simply have the failure of commutativity, but rather that commutativity holds *up to* a specified scalar. This is the phenomenon of *commutation relations*, which play a central role in quantum physics. There are many familiar examples.

In this paper, we have given an answer, in the discrete case working over $\mathbb{Z}_d$, to the question: what *is* a commutation relation in general? This opens up the possibility of classifying the possible contextual behaviours arising from commutation relations. By virtue of the existence of unitary representations, these arise within quantum mechanics.

We mention a few topics of current and future work:

- Studying the cohomology of commutation groups, and relating this to the cohomological criteria for contextuality studied e.g. in [5, 3, 16, 1].
- Studying commutation groups in relation to state-dependent contextuality and empirical models [4].
- Relating commutation groups to the logical analysis of contextuality in terms of partial Boolean algebras [13, 2].
- Generalizing commutation groups to more general abelian groups of scalars.
- A Stone-von Neumann type theorem for commutation groups.

References

1 Sivert Aasnæss. Comparing two cohomological obstructions for contextuality, and a generalised construction of quantum advantage with shallow circuits. *arXiv preprint*, 2022. arXiv:2212.09382.

2 Samson Abramsky and Rui Soares Barbosa. The logic of contextuality. In Christel Baier and Jean Goubault-Larrecq, editors, *29th EACSL Annual Conference on Computer Science Logic, CSL 2021, January 25-28, 2021, Ljubljana, Slovenia (Virtual Conference)*, volume 183 of *LIPIcs*, pages 5:1–5:18. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPICS.CSL.2021.5.

3 Samson Abramsky, Rui Soares Barbosa, Kohei Kishida, Raymond Lal, and Shane Mansfield. Contextuality, cohomology and paradox. In Stephan Kreutzer, editor, *24th EACSL Annual Conference on Computer Science Logic, CSL 2015, September 7-10, 2015, Berlin, Germany*, volume 41 of *LIPIcs*, pages 211–228. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2015. doi:10.4230/LIPIcs.CSL.2015.211.

4 Samson Abramsky and Adam Brandenburger. The sheaf-theoretic structure of non-locality and contextuality. *New Journal of Physics*, 13(11):113036, 2011.

5 Samson Abramsky, Shane Mansfield, and Rui Soares Barbosa. The cohomology of non-locality and contextuality. In Bart Jacobs, Peter Selinger, and Bas Spitters, editors, *Proceedings 8th International Workshop on Quantum Physics and Logic, QPL 2011, Nijmegen, Netherlands, October 27-29, 2011*, volume 95 of *EPTCS*, pages 1–14, 2011. doi:10.4204/EPTCS.95.1.

6 Hannes Bartosik, Jürgen Klepp, Claus Schmitzer, Stephan Sponar, Adán Cabello, Helmut Rauch, and Yuji Hasegawa. Experimental test of quantum contextuality in neutron interferometry. *Physical review letters*, 103(4):040403, 2009.

7 Sergey Bravyi, David Gosset, Robert Koenig, and Marco Tomamichel. Quantum advantage with noisy shallow circuits. *Nature Physics*, 16(10):1040–1045, 2020.

8 Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018.

9 Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1), 2017.

10 Yuji Hasegawa, Rudolf Loidl, Gerald Badurek, Matthias Baron, and Helmut Rauch. Quantum contextuality in a single-neutron optical experiment. *Physical Review Letters*, 97(23):230401, 2006.

11 Thomas F Jordan. *Quantum mechanics in simple matrix form*. Wiley, 1986.

12 William M Kirby and Peter J Love. Variational quantum eigensolvers for sparse Hamiltonians. *Physical Review Letters*, 127(11):110503, 2021.

13 Simon Kochen and Ernst P. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17(1):59–87, 1967.

14 N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical review letters*, 65(27):3373, 1990.

15 N David Mermin and Rüdiger Schack. Homer nodded: von Neumann's surprising oversight. *Foundations of Physics*, 48:1007–1020, 2018.

16 Cihan Okay, Sam Roberts, Stephen D Bartlett, and Robert Raussendorf. Topological proofs of contextuality in quantum mechanics. *arXiv preprint*, 2017. arXiv:1701.01888.

17 Robert Raussendorf. Contextuality in measurement-based quantum computation. *Physical Review A*, 88(2):022322, 2013.

18 Stephen Semmes. An introduction to Heisenberg groups in analysis and geometry. *Notices of the AMS*, 50(6):640–646, 2003.

19 William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *Journal of the American Mathematical Society*, 33(1):1–56, 2020.

20 James Joseph Sylvester. *On quaternions, nonions, sedenions, etc.* Johns Hopkins, 1883.

A The Pauli group on qubits

We recall the definition of the **Pauli operators**, dichotomic (*i.e.* two-valued) observables corresponding to measuring spin in the x, y, and z axes, with eigenvalues ± 1

$$X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y \coloneqq \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

These matrices are self-adjoint, have eigenvalues ± 1, and together with the identity matrix I satisfy the following relations:

$$\begin{aligned} &X^2 = Y^2 = Z^2 = I \\ &XY = iZ, \quad YZ = iX, \quad ZX = iY, \\ &YX = -iZ, \quad ZY = -iX, \quad XZ = -iY. \end{aligned} \tag{7}$$