arXiv:2209.14018v2 [quant-ph] 13 Dec 2024

No quantum solutions to linear constraint systems in odd dimension from Pauli group and diagonal Cliffords

Markus Frembs[1], Cihan Okay[2], and Ho Yiu Chung[2]

[1]Centre for Quantum Dynamics, Griffith University,
Yugambeh Country, Gold Coast, QLD 4222, Australia
[2]Department of Mathematics, Bilkent University, Ankara, Turkey

Linear constraint systems (LCS) have proven to be a surprisingly prolific tool in the study of non-classical correlations and various related issues in quantum foundations. Many results are known for the Boolean case, yet the generalisation to systems of odd dimension is largely open. In particular, it is not known whether there exist LCS in odd dimension, which admit finite-dimensional quantum, but no classical solutions. In recent work, [J. Phys. A, **53**, 385304 (2020)] have shown that unlike in the Boolean case, where the n-qubit Pauli group gives rise to quantum solutions of LCS such as the Mermin-Peres square, the n-qudit Pauli group never gives rise to quantum solutions of a LCS in odd dimension. Here, we generalise this result towards the Clifford hierarchy. More precisely, we consider tensor products of groups generated by (single-qudit) Pauli and diagonal Clifford operators.

Contents

1 Introduction **2**

2 Linear constraint systems and Mermin-Peres square **3**

3 On Paulis and Cliffords **4**
3.1 Pontryagin duality and Heisenberg-Weyl group 4
3.2 Diagonal Clifford hierarchy 5
3.3 Definition of $K_Q^{\otimes n}(d)$ 6

4 Properties **7**
4.1 Abelian subgroups of $K_Q^{\otimes n}(p)$ 8
4.2 Projecting p-torsion abelian subgroups into the Heisenberg-Weyl group 11

5 Solutions to LCS in $K_Q^{\otimes n}(p)$ are classical **15**

6 Discussion **16**

A Properties of $K_Q(p)$ **18**

B Even vs odd prime **21**

Markus Frembs: m.frembs@griffith.edu.au
Cihan Okay: cihan.okay@bilkent.edu.tr
Ho Yiu Chung: hoyiu.chung@bilkent.edu.tr

1 Introduction

Linear constraint systems (LCS) have sparked a lot of interest in recent years, see [2; 4; 5; 12; 26; 30] for instance. Every LCS can be cast into a two-player nonlocal game, which from a computational perspective are of interest as multi-prover interactive proof systems [5]. In this form, LCS have played a prominent role in the various stages and final solution of Tsirelson's problem [21; 29; 30; 32]. The surprisingly rich interplay between quantum foundations and computer science, as well as the structure theory of von Neumann algebras [11; 22; 23] shows that LCS have important applications in quantum theory.

Quantum solutions to LCS are known to exist only in even or infinite (Hilbert space) dimension;[1] it is an open question whether finite-dimensional quantum solutions to LCS also exist over $\mathbb{Z}_d$ for d odd. Notably, the qubit Pauli operators in the Mermin-Peres square (see Fig. 1 below) define a quantum solution to a LCS over $\mathbb{Z}_2$ (see Eq. (2)). This raises the question whether LCS with quantum but no classical solutions exist within the n-qudit Pauli group $\mathcal{P}_d^{\otimes n}$ for arbitrary finite dimension d; yet, [27] have shown that this is not the case.

Here, we generalise this result to a larger group, taking inspiration from (measurement-based) quantum computation, where the Pauli group appears at the first level of the so-called Clifford hierarchy (see Sec. 3.2 below) [7; 15; 16]. More precisely, we consider extensions of the (single-qudit) Pauli group by diagonal Clifford operators. Importantly, the resulting group contains a set of operators that has been shown to be universal for function computation in the restricted subtheory of deterministic, non-adaptive measurement-based quantum computation (MBQC) with linear side-processing (on a GHZ resource state) (see Ref. [9; 10; 28] for details). Within this subtheory, contextuality—roughly, the impossibility of assigning outcomes to all measurements independent of other simultaneously performed measurements—has been identified as a resource for computational advantage [9; 28]. Indeed, Pauli and diagonal Clifford measurement operators generally lead to contextual MBQC [10]. Since the nonexistence of classical solutions to a LCS is also a form of contextuality, this further motivates to seek quantum solutions to LCS for $\mathbb{Z}_d$ within this group.[2] Surprisingly, our main result (Thm. 2) shows that no such solutions exist. What is more, the techniques developed in this work constitute a first step towards the analysis of (the existence of quantum solutions to) LCS in groups generated from other gate sets used in quantum computation (beyond Pauli and diagonal Clifford gates).

The rest of this paper is organised as follows. In Sec. 2 we briefly review the Mermin-Peres square and the definition of linear constraint systems. In Sec. 3, we define the group of interest, generated from Pauli and diagonal Clifford gates. Sec. 4 studies its properties, and builds up to the proof of our key technical contribution (Thm. 1). The details are of independent interest, but may be skipped on first reading. Sec. 5 contains the main result of our work (Thm. 2), and Sec. 6 concludes.

[1] Here, the dimension refers to the (minimal) Hilbert space on which operators act. The existence of linear constraint systems over $\mathbb{Z}_d$ admitting possibly infinite-dimensional quantum but no classical solutions for arbitrary $d \in \mathbb{N}$ has been reported in [31].

[2] MBQC and LCS are related, in fact, every deterministic, non-adaptive MBQC acting on a GHZ state with operators from this enlarged group gives rise to an associated LCS. Note that measurement operators in MBQC commute on their common resource eigenstate. Consequently, the MBQC lifts to a quantum solution of its associated LCS if and only if measurement operators commute (independent of the resource state). Since it would distract from the results of the present paper, we will defer a more detailed analysis of the correspondence between MBQC and LCS to future work.

2 Linear constraint systems and Mermin-Peres square

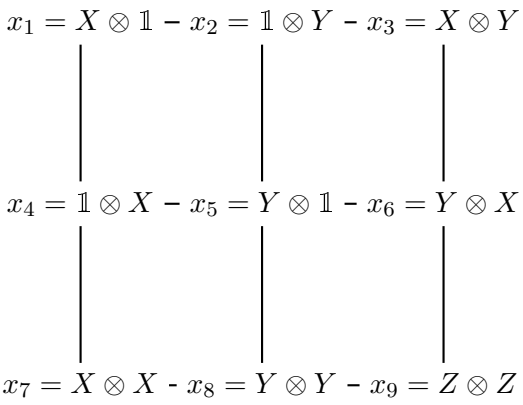

Figure 1: Two-qubit Pauli operators in the (contextuality proof of the) Mermin-Peres square [24; 25].

Let $\mathcal{P}_2^{\otimes n} = \langle X, Y, Z \rangle^{\otimes n}$ denote the n-qubit Pauli group.[3] The nine two-qubit Pauli operators $x_k \in \mathcal{P}_2^{\otimes 2}$, $k \in \{1, \cdots, 9\}$ in Fig. 1 satisfy the following constraints: (i) every operator is a square root of the identity, $x_k^2 = \mathbb{1} \otimes \mathbb{1}$ for all $k \in \{1, \cdots, 9\}$, (ii) the operators in every row and column commute, $[x_k, x_l] = 0$ for all $k, l \in \{1, \cdots, 9\}$, and (iii) the operators in every row and column obey the multiplicative constraints

$$\prod_{k=1}^{9} x_k^{A_{ik}} = (-1)^{b_i} \ , \quad \forall i \in \{1, \cdots, 6\} \ , \tag{1}$$

where $A \in M_{6,9}(\mathbb{Z}_2)$ and $b \in \mathbb{Z}_2^6$ are defined as follows

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad b = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \ . \tag{2}$$

Assume that there exists a (classical) solution $x_k = (-1)^{\tilde{x}_k}$ with $\tilde{x}_k \in \mathbb{Z}_2^9$. Then the constraints can be equivalently expressed in terms of the additive equation $A\tilde{x} = b \mod 2$,

$$\prod_{k=1}^{9} x_k^{A_{ik}} = (-1)^{\sum_{k=1}^{9} A_{ik}\tilde{x}_k} = (-1)^{b_i} \ . \tag{3}$$

However, as is easily seen by multiplying the constraints in Eq. (1), no such solution exists. The Mermin-Peres square thus constitutes a proof of *quantum contextuality*, that is, the impossibility of assigning spectral values to observables independent of other commuting, and thus simultaneously measurable observables. More generally, we will call a group $G \subset U(d)$ *noncontextual* if it admits a spectral value assignment, i.e., a map $v : G \to U(1)$ such that (i) $v(g) \in \mathrm{sp}(g)$ and (ii) $v(gg') =$

[3] The Pauli matrices are $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

$v(g)v(g')$ whenever $[g,g'] := gg'g^{-1}g'^{-1} = \mathbb{1}$.[4] Otherwise G is called *contextual*. Note that any classical solution to Eq. (2) would amount to a value assignment for $\mathcal{P}_2^{\otimes 2}$ in Fig. 1.

Generalising this example, one defines linear constraint systems (LCS) '$Ax = b \mod d$' for any $A \in M_{m,n}(\mathbb{Z}_d)$ and $b \in \mathbb{Z}_d^m$. A *classical solution* to a LCS is a vector $\tilde{x} \in \mathbb{Z}_d^n$ solving the system of linear equations $A\tilde{x} = b \mod d$, whereas a *quantum solution* is an assignment of unitary operators $x \in U^{\otimes n}(d)$ such that (i) $x_k^d = \mathbb{1}$ for all $k \in \{1, \cdots, n\}$ ('d-torsion'), (ii) $[x_k, x_{k'}] := x_k x_{k'} x_k^{-1} x_{k'}^{-1} = \mathbb{1}$ whenever (k, k') appear in the same row of A, i.e., $A_{lk} \neq 0 \neq A_{lk'}$ for some $l \in \{1, \cdots, m\}$ ('commutativity'), and (iii) $\prod_{k=1}^n x^{A_{lk}} = \omega^{b_l}$ for all $l \in \{1, \cdots, m\}$, and where $\omega = e^{\frac{2\pi i}{d}}$ 'constraint satisfaction').[5] For more details on linear constraint systems we refer to [4; 27; 30].

3 On Paulis and Cliffords

This section builds up to the definition of the groups $K_Q^{\otimes n}$ in Sec. 3.3, which encompasses Pauli and diagonal Clifford operators. We first review some basic facts about the Heisenberg-Weyl group in Sec. 3.1, before we extend it by additional operators, motivated by the diagonal Clifford hierarchy as shown in Sec. 3.2.

3.1 Pontryagin duality and Heisenberg-Weyl group

Given any finite abelian group G, we define its Pontryagin dual $\hat{G}$ as the set of group homomorphisms into the unitary group $U(1)$,

$$\hat{G} := \mathrm{Hom}(G, U(1)) = \{\chi : G \to U(1) \ \mid \chi(gh) = \chi(g)\chi(h) \ \forall g, h \in G\} \ . \tag{4}$$

$\hat{G}$ itself is a finite abelian group under pointwise multiplication. By Pontryagin duality, there is a canonical isomorphism $\mathrm{ev}_G : G \to \hat{\hat{G}}$ given by

$$\mathrm{ev}_G(x)(\chi) := \chi(x) \ .$$

The Heisenberg-Weyl group $\mathsf{H}(G)$ of G is now defined as follows. Let $\mathbb{C}^G$ be the Hilbert space of complex-valued functions on G and define the translation operators t_x, $x \in G$ and multiplication operators m_χ, $\chi \in \hat{G}$ by

$$(t_x f)(y) = f(x + y) \qquad (m_\chi f)(y) = \chi(y) f(y) \ , \tag{5}$$

for all $f \in \mathbb{C}^G$.[6] Clearly, the operators in Eq. (5) do not commute, instead they satisfy the canonical Weyl commutation relations,

$$t_x m_\chi = \overline{\chi(x)} m_\chi t_x \ , \quad \forall x \in G, \chi \in \hat{G} \ . \tag{6}$$

The Heisenberg-Weyl group is the subgroup of the unitary group on the Hilbert space $\mathbb{C}^G$ generated by these operators.

[4] Here, $\mathrm{sp}(g) = \{\lambda \in U(1) \mid \det(g - \lambda\mathbb{1}) = 0\}$ denotes the *spectrum of* g, that is, the set of eigenvalues of g.

[5] With [26], we call an *operator solution* an assignment $x \in U^{\otimes n}(d)$ satisfying (i) and (iii), but not (ii).

[6] The measure needed in the definition of $L^2(G)$ is the unique Haar measure on G.

Of particular interest for quantum computation is the discrete Heisenberg-Weyl group $\mathsf{H}(\mathbb{Z}_d)$ with $\hat{\mathbb{Z}}_d = \{\chi^a(q) = \omega^{aq} \mid \omega = e^{\frac{2\pi i}{d}}, a \in \mathbb{Z}_d\} \cong \mathbb{Z}_d$.[7] Note that the Heisenberg-Weyl group can also be seen as a subgroup of the normaliser $\mathsf{H}(\mathbb{Z}_d) \subset N(T)$ of a maximal torus of the special unitary group,

$$T = T(SU(d)) = \{S_\xi = \mathrm{diag}(\xi(0), \cdots, \xi(d-1)) \in SU(d) \mid \xi : \mathbb{Z}_d \to U(1), \prod_{q \in \mathbb{Z}_d} \xi(q) = 1\} \,. \tag{7}$$

See [18, Chapter 11] for details about maximal tori in Lie groups. There is a split extension

$$1 \to T \to N(T) \to W(T) \to 1 \,, \tag{8}$$

where $N(T)$ is the normalizer of T and $W(T) = N(T)/T$ is called the Weyl group. In the case of the special unitary group $SU(d)$, $W(T) \cong \mathrm{Sym}(d)$ is the symmetric group on d elements. It induces an action on T by

$$x \cdot t = xtx^{-1} \,, \tag{9}$$

where $x \in W(T) \cong \mathrm{Sym}(d)$ on $t \in T$. Let X be the generalised Pauli shift operator. The group $\langle X \rangle \cong \mathbb{Z}_d$ generated by X can be identified with a subgroup of $W(T) \cong \mathrm{Sym}(d)$. In particular, note that the Heisenberg-Weyl group arises from the split extension in Eq. (8), by restriction to the Pontryagin dual

$$1 \to \hat{\mathbb{Z}}_d \to \mathsf{H}(\mathbb{Z}_d) \to \langle X \rangle \to 1 \,. \tag{10}$$

Comparing Eq. (10) with Eq. (8) suggests to extend the Pontryagin dual $\hat{\mathbb{Z}}_d$ in the definition of the (discrete) Heisenberg-Weyl group to a maximal torus subgroup of the special unitary group.[8]

3.2 Diagonal Clifford hierarchy

Clifford hierarchy. Recall that the *Clifford hierarchy* is defined recursively from $\mathcal{C}_1(d) := \mathcal{P}_d$ and $\mathcal{C}_{k+1}(d) := \{C \in U(d) \mid \forall M \in \mathcal{P}_d : CMC^\dagger \subset \mathcal{C}_k(d)\}$, where we follow the notation in Ref. [7]. $\mathcal{C}_2(d)$ is also known as the *Clifford group*, it is the normaliser of the qudit Pauli group $\mathcal{P}_d$; note that $\mathcal{C}_k(d)$ is not a group for $k > 2$. We remark that the Clifford hierarchy is of fundamental importance in quantum computation with magic state injection [3; 16; 19; 20]. In particular, the Gottesman-Knill theorem proves that the so-called stabiliser subtheory [13; 14], which encompasses all unitary Clifford circuits on eigenstates of n-qubit Pauli group, and Pauli-measurements can be efficiently classically simulated [1; 7; 15]. While stabiliser subtheory is not universal for quantum computation, adding a single additional unitary gate, e.g. the T-gate ($\frac{\pi}{4}$-phase gate) to any set of generators of the Clifford group does yield a universal gate set.

Diagonal Clifford hierarchy. Similarly, the *diagonal Clifford hierarchy* for d odd is defined recursively from $\mathcal{D}_1(d) := \widehat{\mathbb{Z}}_d$ (see Sec. 3.1), and $\mathcal{D}_{k+1}(d) := \{S_\gamma = \mathrm{diag}(\gamma(0), \cdots, \gamma(d-1)) \in U(d) \mid \forall M \in \mathsf{H}(\mathbb{Z}_d) : \; S_\gamma M S_\gamma^\dagger \subset \mathcal{D}_k(d)\}$.[9] We will be particularly interested in the subgroups of the *special diagonal Clifford hierarchy* $\mathcal{SD}_k(d) := \mathcal{D}_k(d) \cap SU(d)$ for all $k \in \mathbb{N}$, since operators $S_\xi X^b$ with $S_\xi \in \mathcal{SD}_k(d)$ are d-torsion by Lm. 3 below.

---

[7] For d odd, $\mathcal{P}_d \cong \mathsf{H}(\mathbb{Z}_d)$, but for d even these groups differ by central elements [7]. In particular, note that the qubit Pauli group $\mathcal{P}_2 = \langle i, X, Z \rangle$, whereas $\mathsf{H}(\mathbb{Z}_2) = \langle X, Z \rangle$.

[8] The restriction to the special unitary group $SU(d)$ in Eq. (7) ensures that (local measurement) operators $M(\xi, b) = S_\xi X^b$, with $b \neq 0$ and $S_\xi \in T$ have order d (Lm. 3). We also remark that the extension of $\hat{\mathbb{Z}}_d$ to T is closely related to the diagonal Clifford hierarchy (cf. [6]), which embeds into the maximal torus of the unitary group $T(U(d))$ (see also Remark. 2).

[9] The definition of $(\mathcal{D}_k(d))_{k \in \mathbb{N}}$ notably depends on a choice of basis, viz. maximal torus $T(U(d)) \subset U(d)$ (cf. Eq. (7) below).

Lemma 1. *Let $\xi : \mathbb{Z}_d \to U(1)$ be a function with d odd. If $S_\xi \in \mathcal{SD}_k(d)$ then $S_\xi^{d^{k+1}} = \mathbb{1}$.*

Proof. The case $k = 1$ is immediate. The general case $k > 1$ follows by induction from the recursive definition of the (special) diagonal Clifford hierarchy. More precisely, for any diagonal element S_ξ with $\xi : \mathbb{Z}_d \to U(1)$ the canonical Weyl commutation relations in Eq. (6) generalise to

$$S_\xi X S_\xi^\dagger = S_{\Delta\xi} X \ , \tag{11}$$

where we define $\Delta\xi : \mathbb{Z}_d \to U(1)$ by $\Delta\xi(q) := \frac{\xi(q+1)}{\xi(q)} \in U(1)$. In particular,

$$\prod_{q=0}^{d-1} \Delta\xi(q) = \prod_{q=0}^{d-1} \frac{\xi(q+1)}{\xi(q)} = \frac{\prod_{q=0}^{d-1} \xi(q+1)}{\prod_{q=0}^{d-1} \xi(q)} = \frac{1}{1} = 1 \ .$$

By definition, $\mathcal{SD}_{k+1}(d)$ is the pre-image to $\mathcal{SD}_k(d)$ of the operator $\Delta : T \to T$ for T a maximal torus in $SU(d)$. Now, assume that the assertion holds for $k-1$ and let $S_{\xi'} \in \mathcal{SD}_{k-1}(d)$. From $\xi'(q) = \Delta\xi(q) = \frac{\xi(q+1)}{\xi(q)}$ we find that any pre-image $S_\xi \in \mathcal{SD}_k(d)$ of $S_{\xi'}$ under Δ satisfies $\xi(q+1) = \xi(q)\xi'(q)$. Let $\xi(0) = e^{ic}$ with $c \in \mathbb{R}$ arbitrary, then $\xi(q) = e^{ic} \prod_{k=0}^{q-1} \xi'(k)$. Moreover, since $S_\xi \in SU(d)$ by assumption we have $\xi^{-1}(0) = \prod_{q=1}^{d-1} \xi(q) = e^{i(d-1)c} \prod_{q=1}^{d-1} \prod_{k=0}^{q-1} \xi'(k)$, from which it follows that $e^{idc} = \prod_{q=1}^{d-1} \prod_{k=0}^{q-1} \xi'(k)$. Finally, since $\xi'(k)$ is a k-th root of unity by the inductive hypothesis, it follows that e^{ic} is a $k+1$-th root of unity. □

It follows that not every operator S_ξ with $\xi : \mathbb{Z}_d \to U(1)$ is an element of $\mathcal{D}_k(d)$ for some $k \in \mathbb{N}$. For instance, $\xi = (1, e^{i\sqrt{2}}, e^{-i\sqrt{2}}) \notin \mathcal{D}_k(3)$ for any $k \in \mathbb{N}$. Nevertheless, as a consequence of Thm. 3 in App. A, $S_\xi \in \mathcal{D}_k(d)$ if and only if $S_\xi^m = \mathbb{1}$ for some $m \in \mathbb{N}$.

Contextuality has been identified as a resource in measurement-based quantum computation (MBQC) [9; 28]. Motivated in part by the universality of Pauli and diagonal Clifford gates within the restricted subtheory of deterministic, non-adaptive MBQC with linear side-processing (on a GHZ resource state) [10], in the next section, we will define groups generated from tensor products of these operators.

3.3 Definition of $K_Q^{\otimes n}(d)$

In this section, we define a group generated from operators $S_\xi X^b$ that are d-torsion in the sense that $(S_\xi X^b)^d = \mathbb{1}$. For an integer $m \geq 1$, let $T_{(d^m)}$ denote the subgroup of the maximal torus of the special unitary group T consisting of elements of order d^m; that is $T_{(d^m)} = \{S_\xi \in T |\ S_\xi^{d^m} = \mathbb{1}\}$. In particular, when d is an odd prime, the subgroup $T_{(d)}$ consists of elements S_ξ where ξ is of the form $\xi(q) = a_0 + a_1 q + a_2 q^2 + \cdots + a_{d-1} q^{d-1}$ with $a_i \in \mathbb{Z}_d$ for all $0 \leq i \leq d-1$ (cf. Eq. (16)).

Definition 1. *For a subgroup $T_{(d)} \subset Q \subset T_{(d^m)}$ invariant under the action of $\langle X \rangle$ we define the following subgroup of the special unitary group:*

$$K_Q(d) = \langle S_\xi X^b \mid b \in \mathbb{Z}_d, S_\xi \in Q \rangle \subset SU(d) \ ,$$

where $X|q\rangle = |q+1\rangle$ is the generalised Pauli shift operator and $S_\xi|q\rangle = \xi(q)|q\rangle$ is a generalised phase gate. [10]

[10] Note that not all (diagonal) elements in $K_Q(d)$ have order d. Such operators do not arise as local measurement operators in (deterministic, non-adaptive) *ld*-MBQC, they are merely a byproduct of Def. 1.

We denote the n-fold Kronecker tensor product of $K_Q(d)$ by

$$K_Q^{\otimes n}(d) = \overbrace{K_Q(d) \otimes \cdots \otimes K_Q(d)}^{n \text{ copies}}.$$

Similarly $H^{\otimes n}(\mathbb{Z}_d)$ denotes the n-fold Kronecker tensor product of $H(\mathbb{Z}_d)$.

Note that $K_Q(d) = \mathsf{H}(\mathbb{Z}_d)$ reduces to the discrete Heisenberg-Weyl group[11] for $Q = T_{(d)}$ where d is an odd prime. In this paper we will consider the other extreme that is when $Q = T_{(d^m)}$.

Note also that $K_Q(d) = Q \rtimes \langle X \rangle \cong Q \rtimes \mathbb{Z}_d$ is a split extension, (as a restriction of Eq. (8))

$$1 \to Q \to K_Q(d) \to \langle X \rangle \to 1 \,. \tag{12}$$

We will therefore often write $S_\xi X^b \in K_Q(d)$ as (ξ, b), where $b \in \mathbb{Z}_d$ and $S_\xi \in Q$. By Eq. (9), the group action of $\mathbb{Z}_d$ on Q is given by

$$S_{b\cdot\xi}|q\rangle := X^b \cdot S_\xi|q\rangle = X^b S_\xi X^{-b}|q\rangle = X^b S_\xi|q-b\rangle = X^b \xi(q-b)|q-b\rangle = \xi(q-b)|q\rangle \,,$$

that is $b \cdot \xi(q) = \xi(q-b)$ for all $q \in \mathbb{Z}_p$. The group operation of $K_Q(d)$ is given by

$$(\xi, b)(\xi', b') = (\xi b \cdot \xi', b + b') \,,$$

and the inverse is given by

$$(\xi, b)^{-1} = ((-b) \cdot \xi^{-1}, -b) \,,$$

where $(\xi, b), (\xi', b') \in K_Q(d)$.

Lemma 2. *Let $(\xi, b), (\chi, 0) \in K_Q(d)$. Let n be a positive integer, we have*

(1) $(\xi, b)^n = \Big(\prod_{i=0}^{n-1}(ib) \cdot \xi \,,\, nb\Big)$.

(2) $(\xi, b)^n(\chi, 0) = ((nb) \cdot \chi, 0)(\xi, b)^n$. *Thus we also have* $(\chi, 0)(\xi, b)^n = (\xi, b)^n((-nb) \cdot \chi, 0)$.

(3) $\big((\xi, b)(\chi, 0)\big)^n = \big(\prod_{i=1}^{n}(ib) \cdot \chi, 0\big)(\xi, b)^n$.

Proof. The proofs of all three statements are straightforward; see App. A for details. □

4 Properties

We are interested in quantum solutions to LCS in $K_Q^{\otimes n}(p)$, the group generated by Pauli and diagonal Clifford operators; to this end, we first analyse its abelian subgroups in the next section, before defining a map from $K_Q^{\otimes n}(p)$ to the Heisenberg-Weyl group $H^{\otimes n}(\mathbb{Z}_p)$ that preserves p-torsion abelian subgroups in Sec. 4.2. This map will allow us to prove our main result, Thm. 2 in Sec. 5. This section is of a technical nature and may be skipped on first reading.

[11] For d odd, $\mathcal{P}_d \cong \mathsf{H}(\mathbb{Z}_d)$, but for d even these groups differ by central elements [7]. In particular, note that the qubit Pauli group $\mathcal{P}_2 = \langle i, X, Z \rangle$, whereas $\mathsf{H}(\mathbb{Z}_2) = \langle X, Z \rangle$.

4.1 Abelian subgroups of $K_Q^{\otimes n}(p)$

From now on, we fix p to be an odd prime. In this section we will describe (p-torsion) abelian subgroups of $K_Q^{\otimes n}(p)$ where $Q = T_{(p^m)}$. For simplicity, we will use the following notation:

$$K = K_Q(p) \quad \text{and} \quad K^{\otimes n} = K_Q^{\otimes n}(p) \,.$$

We begin with a description of p-torsion elements in K.

Lemma 3. *An element $M \in K$ is p-torsion, i.e. $M^p = \mathbb{1}$, if either*

- *$M = S_\xi$ for some $S_\xi \in T_{(p)}$, or*
- *$M = S_\xi X^b$ with $b \neq 0$.*

Proof. Follows from Lm. 2(1), and our assumption $S_\xi \in T$, which implies $\det(S_\xi) = \prod_{k=0}^{p-1} k \cdot \xi = 1$. □

Next, we describe commuting pairs of elements in K up to a phase.

Lemma 4. *Let $M = S_\xi X^b$ and $M' = S_{\xi'} X^{b'}$ be elements in K such that $[M, M'] = \omega^c \mathbb{1}$ for some $c \in \mathbb{Z}_p$. Then one of the following cases hold:*

1. *$b = b' = 0$ and $M, M' \in Q$. In particular, $c = 0$.*
2. *$b \neq 0$ and $b' = 0$ and $M' \in \hat{\mathbb{Z}}_p$. In addition, if $c = 0$, then $M' \in Z(K)$.*
3. *$b, b' \neq 0$ and there exits $a, y \in \mathbb{Z}_p$ and $S_\chi \in \hat{\mathbb{Z}}_p$ such that $\omega^a M' = (MS_\chi)^y$. Here $\chi(q) = \omega^{c'q}$ where $b'c' = -c$ and $yb = b'$. In addition, if $c = 0$, then $\omega^a M' = M^y$.*

Proof. We will use the alternative notation $(\xi, b) = S_\xi X^b$. First, we calculate the commutator:

$$\begin{aligned}
[M, M'] &= (\xi, b)(\xi', b')(\xi, b)^{-1}(\xi', b')^{-1} \\
&= (\xi b \cdot \xi', b + b') \ \Big((-b) \cdot \xi^{-1}, -b\Big) \Big((-b') \cdot \xi'^{-1}, -b'\Big) \\
&= (\xi b \cdot \xi', b + b') \Big((-b) \cdot \xi^{-1}(-b - b') \cdot \xi'^{-1}, -b - b'\Big) \\
&= \Big(\xi b \cdot \xi'(b + b' - b) \cdot \xi^{-1}(b + b' - b - b') \cdot \xi'^{-1}, b + b' - b - b'\Big) \\
&= \Big(\xi b \cdot \xi' b' \cdot \xi^{-1}\xi'^{-1}, 0\Big) \ .
\end{aligned} \tag{13}$$

Thus we have $[M, M'] = (\hat{\xi}, 0)$, where $\hat{\xi}(q) = \xi(q)\xi'(q - b)\xi^{-1}(q - b')\xi'^{-1}(q)$ for all $q \in \mathbb{Z}_p$.

Case 1: We assume $b = b' = 0$. In this case, we have $M, M' \in Q$. This group is abelian, thus $c = 0$.

Case 2: We assume $b \neq 0$ and $b' = 0$. In this case, we have

$$\begin{aligned}
[M, M'] = \omega^c \mathbb{1} &\iff \xi(q)\xi'(q - b)\xi^{-1}(q)\xi'^{-1}(q) = \omega^c \\
&\iff \xi'(q - b) = \xi'(q)\omega^c \\
&\iff \xi'(q) = \xi'(q + b)\omega^c \,.
\end{aligned}$$

Let $m \in \mathbb{Z}_p$ such that $mb = -1$. Thus we have $q + mqb = 0$. By the equation above, we have

$$\xi'(q) = \xi'(q + b)\omega^c = \xi'(q + 2b)\omega^{2c} = \cdots = \xi'(q + mqb)\omega^{mqc} = \xi'(0)\omega^{mqc} \,.$$

By definition (cf. Eq. (7)), we have $\prod_{q=0}^{p-1}\xi'(q)=1$. Thus we obtain

$$1=\prod_{q=0}^{p-1}\xi'(q)=\prod_{q=0}^{p-1}\xi'(0)\omega^{mqc}=(\xi'(0))^p\omega^{mc\sum_{q=0}^{p-1}q}=(\xi'(0))^p\ ,$$

where we used that $\sum_{q=0}^{p-1}q=\frac{p(p-1)}{2}$ is divisible by 2, hence, $\sum_{q=0}^{p-1}q$ is a multiple of p and thus $\omega^{mc\sum_{q=0}^{p-1}q}=1$. Finally, we set $\xi'(0)=\omega^a$ for some $a\in\mathbb{Z}_p$ and obtain

$$\xi'(q)=\xi'(0)\omega^{mqc}=\omega^a\omega^{mqc}=\omega^{mcq+a}\ ,$$

therefore $M'=(\xi',b')\in\hat{\mathbb{Z}}_p$. In particular, if $c=0$ we have $\xi'(q)=\omega^a$, and as a result $M'\in Z(K)$.

Case 3: Assume that $b,b'\neq 0$. We pick $c'\in\mathbb{Z}_p$ and $y\in\mathbb{Z}_p$ such that $b'c'=-c$ and $yb=b'$, and we define $\chi(q)=\omega^{c'q}$. By Lm. 2(1), we have

$$(MS_\chi)^y=((\xi,b)(\chi,0))^y=(\xi b\cdot\chi,b)^y=(\bar{\xi},yb)=(\bar{\xi},b')\ , \tag{14}$$

where $\bar{\xi}=\left(\prod_{i=0}^{y-1}(ib)\cdot\xi\right)\left(\prod_{i=0}^{y-1}(ib+b)\cdot\chi\right)$. Since $[M,M']=\omega^c\mathbb{1}$, by Eq. (13), we have

$$\xi(q)\xi'(q-b)\xi^{-1}(q-b')\xi'^{-1}(q)=\omega^c\iff\frac{\xi(q)}{\xi(q-b')}=\frac{\xi'(q)}{\xi'(q-b)}\omega^c\ . \tag{15}$$

Then we calculate

$$\begin{aligned}
\frac{\bar{\xi}(q)}{\bar{\xi}(q-b)}=\frac{\bar{\xi}}{b\cdot\bar{\xi}}(q)&=\frac{\left(\prod_{i=0}^{y-1}(ib)\cdot\xi\right)\left(\prod_{i=0}^{y-1}(ib+b)\cdot\chi\right)}{\left(\prod_{i=0}^{y-1}(ib+b)\cdot\xi\right)\left(\prod_{i=0}^{y-1}(ib+b+b)\cdot\chi\right)}(q)\\
&=\frac{\xi\left(\prod_{i=1}^{y-1}(ib)\cdot\xi\right)b\cdot\chi\left(\prod_{i=1}^{y-1}(ib+b)\cdot\chi\right)}{\left(\prod_{i=1}^{y}(ib)\cdot\xi\right)\left(\prod_{i=1}^{y}(ib+b)\cdot\chi\right)}(q)\\
&=\left(\frac{\xi}{(yb)\cdot\xi}\right)\frac{b\cdot\chi}{(yb+b)\cdot\chi}(q)\\
&=\left(\frac{\xi(q)}{\xi(q-b')}\right)\frac{\omega^{(q-b)c'}}{\omega^{(q-b'-b)c'}}\quad\text{(by defintion of }\chi\text{ and }yb=b')\\
&=\frac{\xi'(q)}{\xi'(q-b)}\omega^c\omega^{b'c'}\quad\text{(by Eq. (15))}\\
&=\frac{\xi'(q)}{\xi'(q-b)}\ .
\end{aligned}$$

By rearranging this equation, we get

$$\frac{\bar{\xi}(q)}{\xi'(q)}=\frac{\bar{\xi}(q-b)}{\xi'(q-b)}\ ,$$

for all $q\in\mathbb{Z}_p$. Thus we conclude that there is a constant x such that for all $q\in\mathbb{Z}_p$, we have $\bar{\xi}(q)=x\xi'(q)$. By definition, we have $\prod_{q=0}^{p-1}\bar{\xi}(q)=\prod_{q=0}^{p-1}\xi'(q)=1$. It follows that

$$1=\prod_{q=0}^{p-1}\bar{\xi}(q)=\prod_{q=0}^{p-1}x\xi'(q)=x^p\prod_{q=0}^{p-1}\xi'(q)=x^p\ .$$

Thus $x = \omega^a$ for some $a \in \mathbb{Z}_p$ and we have $\bar{\xi}(q) = \omega^a \xi'(q)$ for some $a \in \mathbb{Z}_p$. Combining $\bar{\xi}(q) = \omega^a \xi'(q)$ with Eq. (14), we obtain

$$(MS_\chi)^y = (\bar{\xi}, b') = (\omega^a \xi', b') = (\omega^a, 0)(\xi', b') = \omega^a M' \, .$$

In particular, if $c = 0$, then $\chi(q) = 1$ and $\omega^a M' = M^y$. □

These two results combined gives us the description of p-torsion abelian subgroups of K.

Corollary 1. *Maximal p-torsion abelian subgroups of K fall into two classes:*

- *the subgroup $T_{(p)}$, and*
- *$\langle \omega \mathbb{1}, S_\xi X \rangle$ where $S_\xi \in Q = T_{(p^m)}$.*

Any two distinct maximal p-torsion abelian subgroup intersect at the center $Z(K) = \langle \omega \mathbb{1} \rangle$.

Proof. This follows immediately from Lm. 4 with $c = 0$ and Lm. 3. □

We reformulate Lm. 4 in a way that will be useful for computing the commutator in terms of a symplectic form.

Corollary 2. *Let $M = S_\xi X^b$ and $M' = S_{\xi'} X^{b'}$ be elements in K such that $[M, M'] = \omega^c \mathbb{1}$ for some $c \in \mathbb{Z}_p$. Then one of the following cases hold:*

(1) $b = b' = 0$, in which case $c = 0$.

(2) $b \neq 0$, in which case $M' = S_{\chi'} M^{b'/b}$ where $\chi'(q) = \omega^{\alpha'_0 + \alpha'_1 q}$ for some $\alpha'_0, \alpha'_1 \in \mathbb{Z}_p$ and $c = -b\alpha'_1$.

(3) $b' \neq 0$, in which case $M = S_\chi M^{b/b'}$ where $\chi(q) = \omega^{\alpha_0 + \alpha_1 q}$ for some $\alpha_0, \alpha_1 \in \mathbb{Z}_p$ and $c = b'\alpha_1$.

Proof. We will explain the case where at least one of b or b' is nonzero. Then we are either in case (2) or (3) of Lm. 4. Assume we are in case (3). We can write $M' = S_{\chi'} M^{b'/b}$ for some $S_{\chi'} \in \hat{\mathbb{Z}}_p$ using part (2) and (3) of Lm. 4. Using Eq. (13) we compute $c = -b\alpha'_1$. Note that taking $b' = 0$ we see that Lm. 4 part (2) is also covered by this case. Case (3) can be dealt with in a similar way. □

Next we move on to analyzing $K^{\otimes n}$. Using Thm. 3 in the Appendix we can express ξ as follows:

$$\xi(q) = \exp\left(\sum_{j=1}^{m} \frac{2\pi i}{p^j} f_j(q) \right) \, , \tag{16}$$

where each f_j is a polynomial of the form

$$f_j(q) = \sum_{a=0}^{p-1} \vartheta_{j,a} q^a, \quad \vartheta_{j,a} \in \mathbb{Z}_p \, . \tag{17}$$

We need a generalized version of Lm. 3 to describe p-torsion elements in $K^{\otimes n}$.

Lemma 5. *An element $M = M_1 \otimes M_2 \otimes \cdots \otimes M_n$ in $K^{\otimes n}$ is p-torsion if there exists a subset $I \subset \{1, 2, \cdots, n\}$ such that the following holds:*

- *$M_i \notin Q$, that is, $M_i = S_{\xi_i} X^{b_i}$ with $b_i \neq 0$ for all $i \notin I$.*

- *For all $i \in I$ we have $M_i \in Q$ such that $\vartheta^{(i)}_{j,a} = 0$ for all $j \geq 2, a \neq 0$ and $\sum_{i\in I} \vartheta^{(i)}_{2,0} = 0 \mod p$.*

Proof. It suffices to show that $M_i \in Q$ satisfies $M_i^p = \omega^{c_i}\mathbb{1}$ for some $c_i \in \mathbb{Z}_p$ whenever $\vartheta^{(i)}_{j,a} = 0$ for all $j \geq 2, a \neq 0$. This follows from Eq. (16). □

To track the commutator in the case of $K^{\otimes n}$ we will need the symplectic form borrowed from the Heisenberg-Weyl group $H^{\otimes n}(p)$. For $v = (v_Z, v_X)$ and $v' = (v'_Z, v'_X)$ in $\mathbb{Z}_p^n \times \mathbb{Z}_p^n$ the symplectic form is defined by

$$[v, v'] = v_Z \cdot v'_X - v'_Z \cdot v_X \mod p \,,$$

where $\cdot$ denotes the inner product on vectors in $\mathbb{Z}_p^n$. Using this symplectic form we can describe the commutator of two elements that commute up to a phase.

Corollary 3. *Let $M = M_1 \otimes M_2 \otimes \cdots \otimes M_n$ and $M' = M'_1 \otimes M'_2 \otimes \cdots \otimes M'_n$ be elements in $K^{\otimes n}$ such that $[M, M'] = \omega^c\mathbb{1}$. For every $1 \leq i \leq n$, write $M_i = (\xi_i, b_i)$, let $\bar{b} = (b_1, b_2, \cdots, b_n)$ and let $\bar{f} = (\vartheta^{(1)}_{1,1}, \vartheta^{(2)}_{1,1}, \cdots, \vartheta^{(n)}_{1,1})$, where $\vartheta^{(i)}_{1,1}$ is the coefficient in Eq. (17) that appears in the expansion of ξ_i in Eq. (16); similarly for $\bar{f}'$ and $\bar{b}'$. Then we have*

$$[M, M'] = \omega^{[v,v']}\mathbb{1} \,,$$

where $v = (\bar{f}, \bar{b})$ and $v' = (\bar{f}', \bar{b}')$.

Proof. Since $[M, M'] = \omega^c\mathbb{1}$ we have $[M_i, M'_i] = \omega^{c_i}\mathbb{1}$ such that $\sum_{i=1}^n c_i = c \mod p$. Cor. 2 implies that c_i is either zero or given by the formula in parts (2) and (3) of this result. Suppose we are in case (2). Then $M'_i = S_{\chi'} M_i^{b'/b}$ where $\chi' = \alpha'_0 + \alpha'_1 q$. Using Lm. 2 (1) we can compute the coefficient $\vartheta'^{(i)}_{1,1}$ in ξ'. It turns out that $\vartheta'^{(i)}_{1,1} = \alpha'_1 + \frac{b'}{b}\vartheta^{(i)}_{1,1}$, which gives

$$[M_i, M'_i] = \omega^{-b\alpha'_1}\mathbb{1} = \omega^{-b(\vartheta'^{(i)}_{1,1} - \frac{b'}{b}\vartheta^{(i)}_{1,1})}\mathbb{1} = \omega^{\vartheta^{(i)}_{1,1}b' - \vartheta'^{(i)}_{1,1}b}\mathbb{1} \,.$$

Case (3) can be dealt with similarly. Combining ω^{c_i}'s we obtain the formula for the symplectic form. □

For each $M = M_1 \otimes \cdots \otimes M_n$ we will associate the vector $v = (\bar{f}, \bar{b})$ defined in Cor. 3. A subspace W in $\mathbb{Z}_d^n \times \mathbb{Z}_d^n$ is called isotropic if $[w, w'] = 0$ for all $w, w' \in W$. Using this definition we observe that a subgroup $\langle M^{(1)}, M^{(2)}, \cdots, M^{(n)}\rangle$ of $K^{\otimes n}$ is abelian if and only if the subspace $\langle v^{(1)}, v^{(2)}, \cdots, v^{(n)}\rangle$ of $\mathbb{Z}_d^{2n}$, where $v^{(i)} = (\bar{f}^{(i)}, b^{(i)})$, is isotropic.

4.2 Projecting p-torsion abelian subgroups into the Heisenberg-Weyl group

Let $K^{\otimes n}_{(p)}$ denote the subset of p-torsion elements in $K^{\otimes n}$. In this section, we will construct a map

$$\phi : K^{\otimes n}_{(p)} \to H^{\otimes n}(\mathbb{Z}_p) \,,$$

that restricts to a group homomorphism on every p-torsion abelian subgroup. Cor. 3 hints at a "linearization map" that could potentially serve for this purpose. The map we need is closely related to linearization, yet needs to be slightly adjusted when acting on p-torsion elements. We will revisit this point in Remark. 1 below, after the definition of the map.

Definition 2. *For ξ given as in Eq. (16) we introduce two maps:*

$$R(\xi) = \omega^{\vartheta_{1,0}+\vartheta_{2,0}+\vartheta_{1,1}q} \quad \textit{and} \quad P(\xi) = \omega^{\vartheta_{1,0}+\vartheta_{1,1}q} \ .$$

Using this notation we define a map

$$\phi : K_{(p)}^{\otimes n} \to H^{\otimes n}(\mathbb{Z}_p)$$

as follows:

$$\phi(M_1 \otimes M_2 \otimes \cdots \otimes M_n) = \phi_1(M_1) \otimes \phi_1(M_2) \otimes \cdots \otimes \phi_1(M_n) \ ,$$

where $\phi_1(M)$ for $M = (\xi, b) \in K$ is defined by

$$\phi_1(M) = \begin{cases} (R(\xi), 0) & \textit{if } b = 0 \\ (P(\xi), 1) & \textit{if } b = 1 \end{cases} \ .$$

and $\phi_1(M) = \phi_1(M^{b_i^{-1}})^{b_i}$ if $1 < b < p-1$.

Remark 1. *Note the additional factor $\omega^{\vartheta_{2,0}}$ in the definition of $\phi_1(M)$ for $M \in Q$. Recall that for $M^p = \mathbb{1}$,*

$$M = (\omega^{\sum_{a=0}^{p-1} \vartheta_{1,a} q^a} \sqrt[p]{\omega}^{\vartheta_{2,0}}, 0) \ ,$$

by Lm. 5. It is easy to see that defining ϕ_1 as a linear projection in both cases, that is for $b = 0, 1$, would not restrict to a group homomorphism as desired.

To see this, let $p = 3$ and consider $S_{\xi_1} \otimes S_{\xi_2}$ where $\xi_1(q) = \sqrt[3]{\omega}$ and $\xi_2(q) = \sqrt[3]{\omega}^2$:

$$\begin{aligned} \phi(M_1 \otimes M_2)\phi(M_1 \otimes M_2) &= (\phi_1(M_1) \otimes \phi_1(M_2))(\phi_1(M_1) \otimes \phi_1(M_2)) \\ &= \mathbb{1} \otimes \mathbb{1} \ , \end{aligned}$$

which is not the same as

$$\begin{aligned} \phi((M_1 \otimes M_2)(M_1 \otimes M_2)) &= \phi(M_1^2 \otimes M_2^2) \\ &= \phi(\sqrt[3]{\omega}^2 \mathbb{1} \otimes \omega \sqrt[3]{\omega} \mathbb{1}) \\ &= \phi_1(\sqrt[3]{\omega}^2 \mathbb{1}) \otimes \phi_1(\omega \sqrt[3]{\omega} \mathbb{1}) \\ &= \omega(\mathbb{1} \otimes \mathbb{1}) \ . \end{aligned}$$

Lemma 6. *Let $S_\xi, S_{\xi'} \in Q$ be such that $S_\xi^p, S_{\xi'}^p \in Z(K)$. Then we have*

$$\phi(S_\xi S_{\xi'}) = \phi(S_\xi)\phi(S_{\xi'}) \ .$$

Proof. The condition $S_\xi^p, S_{\xi'}^p \in Z(K)$ implies that $\vartheta_{j,a} = 0$ for $j \geq 2, a \neq 0$; similarly for $\vartheta'_{j,a}$ (according to the proof of Lm. 5). In other words, we have

$$\begin{aligned} \xi(q) &= \omega^{\sum_{a=0}^{p-1} \vartheta_{1,a} q^a} \sqrt[p]{\omega}^{\vartheta_{2,0}} \\ \xi'(q) &= \omega^{\sum_{a=0}^{p-1} \vartheta'_{1,a} q^a} \sqrt[p]{\omega}^{\vartheta'_{2,0}} \\ \xi(q)\xi'(q) &= \omega^{\sum_{a=0}^{p-1} (\vartheta_{1,a}+\vartheta_{1,a}) q^a} \sqrt[p]{\omega}^{\vartheta_{2,0}+\vartheta'_{2,0}} . \end{aligned}$$

By definition of ϕ, we have

$$\phi(S_\xi S_{\xi'})(q) = \omega^{\vartheta_{1,0}+\vartheta'_{1,0}+(\vartheta_{1,1}+\vartheta'_{1,1})q} \sqrt[p]{\omega}^{\vartheta_{2,0}+\vartheta'_{2,0}} \ ,$$

which is the same as

$$\phi(S_\xi)(q)\phi(S_{\xi'})(q) = \omega^{\vartheta_{1,0}+\vartheta_{1,1}q}\sqrt[p]{\omega}^{\vartheta_{2,0}}\omega^{\vartheta'_{1,0}+\vartheta'_{1,1}q}\sqrt[p]{\omega}^{\vartheta'_{2,0}} = \omega^{\vartheta_{1,0}+\vartheta'_{1,0}+(\vartheta_{1,1}+\vartheta'_{1,1})q}\sqrt[p]{\omega}^{\vartheta_{2,0}+\vartheta'_{2,0}} .$$

Thus $\phi(S_\xi S_{\xi'}) = \phi(S_\xi)\phi(S_{\xi'})$. □

Lemma 7. *Let $M \in K$ such that $M \notin Q$ and $S_\chi \in \hat{\mathbb{Z}}_p$. Then we have*

$$\phi(S_\chi M) = \phi(S_\chi)\phi(M) = S_\chi \phi(M) .$$

Proof. We denote $M = (\xi, b)$ and $S_\chi = (\chi, 0)$. Define $\bar{\chi} = \prod_{i=0}^{y-1}(ib)\cdot\chi$ and $\bar{\xi} = \prod_{i=0}^{y-1}(ib)\cdot\xi$, where $y \in \mathbb{Z}_p$ such that $yb = 1$. Consider the element (χ, b). By Lm. 2, we have

$$(\chi, b) = ((\chi, b)^y)^b = \left(\prod_{i=0}^{y-1}(ib)\cdot\chi, 1\right)^b = \left(\prod_{j=0}^{b-1} j\cdot\bar{\chi}, b\right) \implies \chi = \prod_{j=0}^{b-1} j\cdot\bar{\chi} .$$

Next, consider the element (ξ, b), we have

$$(\xi, b) = ((\xi, b)^y)^b = \left(\prod_{i=0}^{y-1}(ib)\cdot\xi, 1\right)^b = (\bar{\xi}, 1)^b$$
$$\implies \phi(\xi, b) = (P(\bar{\xi}), 1)^b = \left(\prod_{j=0}^{b-1} j\cdot P(\bar{\xi}), b\right) .$$

For the element $S_\chi M$, we have

$$(\chi, 0)(\xi, b) = ((\chi\xi, b)^y)^b = \left(\left(\prod_{i=0}^{y-1}(ib)\cdot\chi\right)\left(\prod_{i=0}^{y-1}(ib)\cdot\xi\right), 1\right)^b = (\bar{\chi}\bar{\xi}, 1)^b.$$

Notice that since $S_{\bar{\chi}} \in \hat{\mathbb{Z}}_p$, we have $P(\bar{\chi}\bar{\xi}) = \bar{\chi}P(\bar{\xi})$. Therefore

$$\phi((\chi, 0)(\xi, b)) = (P(\bar{\chi}\bar{\xi}), 1)^b = (\bar{\chi}P(\bar{\xi}), 1)^b$$
$$= \left(\left(\prod_{j=0}^{b-1} j\cdot\bar{\chi}\right)\left(\prod_{j=0}^{b-1} j\cdot P(\bar{\xi})\right), b\right) = (\chi, 0)\phi(\xi, b) = \phi(\chi, 0)\phi(\xi, b) . \square$$

Lemma 8. *Let $M = (\xi, b)$ and $M' = (\xi', b')$ be elements of K such that $[M, M'] = \omega^c \mathbb{1}$ for some $c \in \mathbb{Z}_p$ and $b, b' \neq 0$. Then we have*

$$\phi(MM') = \phi(M)\phi(M') .$$

Proof. We have $M' = (\xi', b') = (\xi'_0, 1)^{b'}$ where $\xi'_0 = \prod_{i=0}^{z-1}(ib')\cdot\xi'$ and $z \in \mathbb{Z}_p$ such that $zb' = 1$. Thus we have

$$\phi(M') = (P(\xi'_0), 1)^{b'}.$$

By Lm. 4(3), there exists $a \in \mathbb{Z}_p$ and $y \in \mathbb{Z}_p$ where $yb' = b$ and $S_\chi = (\chi, 0) \in \hat{\mathbb{Z}}_p$ such that $M = S_{\omega^a}(M'S_\chi)^y$. Thus we have

$$\begin{aligned} M = \omega^a((\xi', b')(\chi, 0))^y &= \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (\xi', b')^y \quad \text{(apply Lm. 2(3))} \\ &= \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) ((\xi'_0, 1)^{b'})^y \\ &= \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (\xi'_0, 1)^b \, . \end{aligned}$$

By Lm. 7, we have

$$\phi(M) = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) \phi((\xi'_0, 1)^b) = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (P(\xi'_0), 1)^b \, .$$

Next, consider the product of M and M'. We have

$$MM' = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (\xi'_0, 1)^b (\xi'_0, 1)^{b'} = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (\xi'_0, 1)^{b+b'}.$$

We consider two cases. First, we assume $b + b'$ is a multiple of p. In this case, we have $(\xi'_0, 1)^{b+b'} = (P(\xi'_0), 1)^{b+b'} = 1$. Thus $MM' \in T_{(p)}$. Hence

$$\phi(MM') = \phi \left(\omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) \right) = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) \, .$$

Therefore we have

$$\phi(M)\phi(M') = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (P(\xi'_0), 1)^{b+b'} = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) = \phi(MM') \, .$$

Second, we assume that $b + b'$ is not a multiple of p. By Lm. 7, we then have

$$\begin{aligned} \phi(MM') = \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) \phi((\xi'_0, 1)^{b+b'}) &= \omega^a \left(\prod_{j=1}^{y} (jb') \cdot \chi, 0 \right) (P(\xi'_0), 1)^b (P(\xi'_0), 1)^{b'} \\ &= \phi(M)\phi(M') \, . \end{aligned}$$

□

Theorem 1. *The map $\phi : K_{(p)}^{\otimes n} \to H^{\otimes n}(\mathbb{Z}_p)$ restricts to a group homomorphism on p-torsion abelian subgroups. That is,*

$$\phi(MM') = \phi(M)\phi(M') \, ,$$

for all $M, M' \in K_{(p)}^{\otimes n}$ such that $[M, M'] = \mathbb{1}$.

Proof. Let $M = M_1 \otimes \cdots \otimes M_n$ and $M' = M'_1 \otimes \cdots \otimes M'_n$ be elements of $K_{(p)}^{\otimes n}$. Since $M^p = (M')^p = \mathbb{1}$ and $[M, M'] = \mathbb{1}$ both Lm. 5 and Cor. 3 apply. In particular, we can reduce to the case $n = 1$ according to Def. 2. Consequently, there are four cases to consider:

- Case 1: $M_i, M_i' \in Q$. Follows from Lm. 6.
- Case 2: $M_i \in T_{(p)}$ and $M_i \notin Q$. Follows from Lm. 7.
- Case 3: $M_i \notin Q$ and $M_i' \in T_{(p)}$. Follows from

$$\begin{aligned}\phi(MM') &= \phi(\omega^\alpha M'M) \\ &= \omega^\alpha \phi(M')\phi(M) \\ &= \omega^\alpha \omega^{-\alpha}\phi(M)\phi(M') \\ &= \phi(M)\phi(M') \ ,\end{aligned}$$

  where in the first line $\omega^\alpha = [M, M']$, in the second line we used Lm. 7 and in the third line we used $[M, M'] = [\phi(M), \phi(M')]$ which is a consequence of Cor. 3.
- Case 4: M_i and M_i' are not in Q. Follows from Lm. 8. □

5 Solutions to LCS in $K_Q^{\otimes n}(p)$ are classical

For convenience, we recall the definition of a solution group associated to a LCS from Def. 1 in [27]:

Definition 3. *For a LCS 'Ax = b mod d' with $A \in M_{m,n}(\mathbb{Z}_d)$ and $b \in \mathbb{Z}_d^m$, the solution group $\Gamma(A, b)$ is the finitely presented group generated by the symbols $J, g_1, \cdots, g_n$ and the relations*

(a) $g_i^d = e$, $J^d = e$ *('d-torsion'),*

(b) $Jg_iJ^{-1}g_i^{-1} = e$ *for all* $i \in \{1, \cdots, n\}$ *and* $g_jg_kg_j^{-1}g_k^{-1} = e$ *whenever there exists a row* i *such that* $L_{ij} \neq 0$ *and* $L_{ik} \neq 0$*, ('commutativity')*

(c) $\prod_{j=1}^N g_j^{A_{ij}} = J^{b_i}$ *for all* i $\{1, \cdots, m\}$ *('constraint satisfaction').*

We are interested in solutions to LCS in $K_Q^{\otimes n}(p)$ for p odd prime, the group generated by Pauli and diagonal Clifford operators (see Def. 1). Surprisingly, we find that LCS admitting a solution $\Gamma \to K_Q^{\otimes n}(p)$ are classical. To prove this, we will reduce a solution $\Gamma \to K_Q^{\otimes n}(p)$ to a solution $\Gamma \to \mathsf{H}^{\otimes n}(\mathbb{Z}_p)$ using the map ϕ from the previous section.

Theorem 2. *Let Γ be the solution group of a LCS over $\mathbb{Z}_p$ where p is an odd prime. Then the LCS admits a quantum solution $\eta : \Gamma \to K_Q^{\otimes n}(p)$ with $T_{(p)} \subset Q \subset T_{(p^m)}$ if and only if it admits a classical solution $\eta : \Gamma \to \mathbb{Z}_p$.*

Proof. A classical solution $x \in \mathbb{Z}_p^n$ becomes a quantum solution under the identification $M_k = \omega^{x_k}\mathbb{1} \in Z(K_Q^{\otimes n}(p))$ for all $k \in \{1, \cdots, n\}$. For the converse, assume that $\eta : \Gamma \to K_Q^{\otimes n}(p)$ is a quantum solution of the LCS. We show that $\phi \circ \eta : \Gamma \to \mathsf{H}^{\otimes n}(\mathbb{Z}_p)$ defines a solution of the LCS, i.e., that the map $\phi : K_Q^{\otimes n}(p)_{(p)} \to \mathsf{H}^{\otimes n}(\mathbb{Z}_p)$ preserves the constraints in Γ. This follows directly form Thm. 1 more precisely,

(i) d-torsion: clearly, every (n-qudit Pauli) operator $P \in \mathsf{H}^{\otimes n}(\mathbb{Z}_p)$ has order p (for p odd prime). In fact, ϕ preserves d-torsion by Thm. 1: $\phi(M)^p = \phi(M^p) = \phi(\mathbb{1}) = \mathbb{1}$ for all $M \in K_Q^{\otimes n}(p)_{(p)}$.

(ii) commutativity: ϕ preserves commutativity by Thm. 1.

(iii) constraint satisfaction: let $\{M_j\}_{j\in J}$, $M_j \in K_Q^{\otimes n}(p)$ be a set of pairwise commuting operators such that $M_j^p = \mathbb{1}$ for all $j \in J$ and $\omega^{b_J}\mathbb{1} = \prod_{j\in J} M_j$. It follows that $\{M_j\}_{j\in J}$ generates an abelian subgroup of order p, hence, ϕ preserves constraints by Thm. 1:

$$\omega^{b_J}\mathbb{1} = \phi(\omega^{b_j}\mathbb{1}) = \phi(\prod_{j\in J} M_j) = \prod_{j\in J}\phi(M_j)\ .$$

Consequently, $\phi\circ\eta : \Gamma \to \mathsf{H}^{\otimes n}(\mathbb{Z}_p)$ also defines a solution of the LCS.

Finally, the existence of a classical solution of the LCS follows from Thm. 2 in [27], which defines a map $v : \mathsf{H}(\mathbb{Z}_p) \to \mathbb{Z}_p$—a homomorphism in abelian subgroups. Similar to above, it follows that $v\circ\phi\circ\eta : \Gamma \to \mathbb{Z}_p$ yields a classical solution of the LCS described by Γ. □

More generally, the argument applies to any map $\phi : G \to H$ that restricts to a group homomorphism on p-torsion abelian subgroups.

Corollary 4. *Let Γ be the solution group of a LCS over $\mathbb{Z}_p$ for p odd prime, let $\eta : \Gamma \to G$ be a solution and $\phi : G \to H$ be a map that restricts to a group homomorphism on p-torsion abelian subgroups of G. Then $\phi\circ\eta : \Gamma \to H$ is a solution to the LCS.*

Proof. Constraints of LCS hold in abelian subgroups of Γ, hence, are preserved by ϕ (Thm. 2). □

Remark 2. *Thm. 2 is a generalisation of Thm. 2 in [27]. The latter proves that any solution in the Heisenberg-Weyl group $\mathcal{P}^{\otimes n} \cong \mathsf{H}^{\otimes n}(\mathbb{Z}_p) \cong K_{\hat{\mathbb{Z}}_p}^{\otimes n}(p) = (\hat{\mathbb{Z}}_p \rtimes \langle X\rangle)^{\otimes n}$ for p odd prime is classical. Diagonal elements $S = \mathrm{diag}(\xi(0),\cdots,\xi(d-1)) \in \mathsf{H}(\mathbb{Z}_p)$ are restricted to the Pontryagin dual $\hat{\mathbb{Z}}_p \subset T_{(p)}$; equivalently they lie in the first level of the special diagonal Clifford hierarchy $\mathcal{SD}_1(d)$ (cf. [6]). Thm. 2 generalises these to higher levels in the special diagonal Clifford hierarchy $\mathcal{SD}_k(d)$. In particular, we note that Thm. 3 (see App. A) closely resembles the classification of the diagonal Clifford hierarchy of Thm. 2 in [6], as well as the resource analysis of contextuality in ld-MBQC of Thm. 5 in [10]. Finally, we will discuss the even prime case in App. B.*

6 Discussion

The Mermin-Peres square in Fig. 1 defines a linear constraint system (LCS) over the Boolean ring $\mathbb{Z}_2$, which admits a quantum solution in terms of two-qubit Pauli operators. To date, no generalisation of the Mermin-Peres square to qudit systems, more generally no finite-dimensional quantum solution to a LCS over $\mathbb{Z}_d$ for d odd, has been found.[12] It has been shown that no such examples can be constructed within the Heisenberg-Weyl group, equivalently the qudit Pauli group [27]. Our main theorem, Thm. 2, generalises this result beyond Pauli operators to the diagonal Clifford hierarchy, lending support to the conjecture that no quantum solutions exist in all of $SU(d)$.

The connection with the Clifford hierarchy further suggests an avenue either towards generalisations of our result or towards examples of contextual LCS in odd prime dimension. Recall that $K_Q(p)$ contains the diagonal Clifford hierarchy (up to phase). However, $K_Q(p)$ does not contain general Clifford operators. Still, for $p = 3$ every single-qutrit Clifford operator M is semi-Clifford, i.e., $M = C_1DC_2$ with $C_1, C_2 \in \mathcal{C}_2(3)$ and D diagonal [17; 33]. Moreover, this result is conjectured to be true for all prime dimensions [8]. This hints at a generalisation of our construction to tensor products of groups generated from (semi-)Clifford operators, and, to analyse the existence of quantum solutions to LCS in groups generated from gate sets in quantum computation more generally.

[12] Note that possibly infinite-dimensionsal solutions to LCS over $\mathbb{Z}_d$ for arbitrary d exist by [31].

Acknowledgements. This work was conducted during a visit of the first author at Bilkent University, Ankara. MF was supported through grant number FQXi-RFP-1807 from the Foundational Questions Institute and Fetzer Franklin Fund, a donor advised fund of Silicon Valley Community Foundation, and ARC Future Fellowship FT180100317. CO and HC are supported by the Air Force Office of Scientific Research under award number FA9550-21-1-0002.

References

[1] Scott Aaronson and Daniel Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A, 70:052328*, (Nov 2004).

[2] Alex Arkhipov. Extending and characterizing quantum magic games. *arXiv.1209.3819* (2012).

[3] Ingemar Bengtsson, Kate Blanchfield, Earl Campbell, and Mark Howard. Order 3 symmetry in the clifford hierarchy. *J. Phys. A, 47(45):455302*, (2014).

[4] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *J. Math. Phys. 58(1):012202*, (2017).

[5] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. *In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, Automata, Languages, and Programming, pages 320–331, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg*

[6] S. X. Cui, D. Gottesman, and A. Krishna. Diagonal gates in the Clifford hierarchy. *Phys. Rev. Lett., 95(1):012329*, (2017).

[7] Niel de Beaudrap. A linearized stabilizer formalism for systems of finite dimension. *Quantum Info. Comput., 13(1-2):73–115*, (Jan 2013).

[8] Nadish de Silva. Efficient quantum gate teleportation in higher dimensions. *Proc. Math. Phys. Eng. Sci., 477(2251):20200865*, (2021).

[9] Markus Frembs, Sam Roberts, and Stephen D. Bartlett. Contextuality as a resource for measurement-based quantum computation beyond qubits. *New J. Phys., 20(10):103011*, (Oct 2018).

[10] Markus Frembs, Sam Roberts, Earl T Campbell, and Stephen D Bartlett. Hierarchies of resources for measurement-based quantum computation. *New J. Phys., 25(1):013002*, (Jan 2023).

[11] Tobias Fritz. Tsirelson's problem and Kirchberg's conjecture. *Rev. Math. Phys., 24(05):1250012*, (2012).

[12] Tobias Fritz. Quantum logic is undecidable. *Arch. Math. Logic 60, 329-341*, (2021).

[13] Keisuke Fujii. Stabilizer Formalism and Its Applications, pages 24–55. *Springer Singapore, Singapore*, (Dec 2015).

[14] Daniel Gottesman. Stabilizer codes and quantum error correction. *arXiv:quant-ph/9705052* (1997).

[15] Daniel Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A, 57:127–137*, (Jan 1998).

[16] Daniel Gottesman and Isaac L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature, 402(6760):390–393*, (Nov 1999).

[17] David Gross and Maarten Nest. The LU-LC conjecture, diagonal local operations and quadratic forms over $GF(2)$. *Quantum Information & Computation, 8:263–281*, (Mar 2008).

[18] Brian C. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction. Springer.*

[19] Mark Howard. Maximum nonlocality and minimum uncertainty using magic states. *Phys. Rev. A, 91:042103*, (Apr 2015).
[20] Mark Howard and Jiri Vala. Qudit versions of the qubit $\pi/8$ gate. *Phys. Rev. A, 86:022316*, (Aug 2012).
[21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* = RE. *Communications of the ACM, Volume 64, Issue 11 (2021), p131-138*.
[22] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner. Connes' embedding problem and Tsirelson's problem. *J. Math. Phys., 52(1)*, (Jan 2011).
[23] Eberhard Kirchberg. On non-semisplit extensions, tensor products and exactness of group C^*-algebras. *Inventiones mathematicae, 112:449–489*, (1993).
[24] N. David Mermin. Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett., 65:3373–3376*, (Dec 1990).
[25] N. David Mermin. Hidden variables and the two theorems of John Bell. *Rev. Mod. Phys., 65:803–815*, (Jul 1993).
[26] Cihan Okay and Robert Raussendorf. Homotopical approach to quantum contextuality. *Quantum, 4:217*, (Jan 2020).
[27] Hammam Qassim and Joel J Wallman. Classical vs quantum satisfiability in linear constraint systems modulo an integer. *J. Phys. A, 53(38):385304*, (Aug 2020).
[28] Robert Raussendorf. Contextuality in measurement-based quantum computation. *Phys. Rev. A, 88(2):022322*, (Aug 2013).
[29] William Slofstra. The set of quantum correlations is not closed. *Forum of Mathematics, Pi, 7:41*, (Jan 2019).
[30] William Slofstra. Tsirelson's problem and an embedding theorem for groups arising from non-local games. *J. Am. Math. Soc., 33(1):1–56*, (Sep 2019).
[31] William Slofstra and Luming Zhang. *private communication.*
[32] Boris S. Tsirelson. Bell inequalities and operator algebras. *This was posted by Boris Tsirelson as problem, 33.*, (2006)
[33] Bei Zeng, Xie Chen, and Isaac L Chuang. Semi-Clifford operations, structure of $C(k)$ hierarchy, and gate complexity for fault-tolerant quantum computation. *Phys. Rev. A, 77(4):042313*, (Apr 2008).

A Properties of $K_Q(p)$

Proof of Lm. 2. (1) We do induction on n. The statement is trivial for $n = 1$. Assume the statement is true when $n = k$ and consider the case $n = k + 1$. We have

$$(\xi, b)^{k+1} = (\xi, b)^k(\xi, b) = \left(\prod_{i=0}^{k-1}(ib)\cdot\xi, kb\right)(\xi, b) = \left((\prod_{i=0}^{k-1}(ib)\cdot\xi)(kb)\cdot\xi\,,\,(k+1)b\right)$$
$$= \left(\prod_{i=0}^{k}(ib)\cdot\xi\,,\,(k+1)b\right)\,.$$

(2) We first prove the statement for $n = 1$. In this case, we have

$$(\xi, b)(\chi, 0) = (\xi b\cdot\chi, b) = (b\cdot\chi, 0)(\xi, b)\,. \tag{18}$$

Now, we consider the general case. By part (i), we have

$$(\xi,b)^n(\chi,0)=\left(\prod_{i=0}^{n-1}(ib)\cdot\xi\,,\,nb\right)(\chi,0)\overset{\text{Eq. (18)}}{=}((nb)\cdot\chi,0)\left(\prod_{i=0}^{n-1}(ib)\cdot\xi\,,\,nb\right)=((nb)\cdot\chi,0)(\xi,b)^n\,.$$

(3) We proceed by induction on n. By part (ii), the statement holds for $n=1$. Consider $n=k+1$. We have

$$\begin{aligned}\left((\xi,b)(\chi,0)\right)^{k+1}=\left((\xi,b)(\chi,0)\right)^k(\xi,b)(\chi,0)&=\left(\prod_{i=1}^{k}(ib)\cdot\chi,0\right)(\xi,b)^k(\xi,b)(\chi,0)\\&=\left(\prod_{i=1}^{k}(ib)\cdot\chi,0\right)(\xi,b)^{k+1}(\chi,0)\\&=\left(\prod_{i=1}^{k}(ib)\cdot\chi,0\right)((k+1)b\cdot\chi,0)(\xi,b)^{k+1}\quad\text{(by part }(ii))\\&=\left(\prod_{i=1}^{k+1}(ib)\cdot\chi,0\right)(\xi,b)^{k+1}\,.\end{aligned}$$

□

Next, we are going to prove that for every $S_\xi\in T_{(p^m)}$, the function ξ can be expressed uniquely as

$$\xi(q)=\prod_{k=1}^{m}exp\left[\frac{2\pi i}{p^k}\left(\sum_{a=0}^{p-1}\vartheta_{k,a}q^a\right)\right]\,,$$

where $\vartheta_{i,j}\in\mathbb{Z}_p$. We define the following sets:

$$Q_m^{(p)}=\left\{\begin{pmatrix}x_0&&\\&\ddots&\\&&x_{p-1}\end{pmatrix}\;\middle|\;\forall i\in 0,\cdots,p-1,\,x_i=exp\left(\frac{2\pi i}{p^m}y_i\right)\text{ where }y_i\in\mathbb{Z}_{p^m}\right\}\,,$$

$$G_m^{(p)}=\left\{S_\xi=\begin{pmatrix}\xi(0)&&\\&\ddots&\\&&\xi(p-1)\end{pmatrix}\;\middle|\;\xi(q)=\prod_{k=1}^{m}exp\left[\frac{2\pi i}{p^k}\left(\sum_{a=0}^{p-1}\vartheta_{k,a}q^a\right)\right]\text{ where }\vartheta_{k,a}\in\mathbb{Z}_p\right\}\,.$$

Remark 3. *We have the following remarks related to the above definitions:*

(i) Both $Q_m^{(p)}$ and $G_m^{(p)}$ are groups with respect to matrix multiplication.

(ii) For $i\in\{1,\cdots,p\}$, define a matrix M_i to be as follows

$$(M_i)_{jk}=\begin{cases}exp\left(\frac{2\pi i}{p^m}\right)&\text{if } j=k=i\\1&\text{if } j=k\text{ and }j,k\neq i\\0&\text{otherwise}\end{cases}\,.$$

Then $\{M_1,\cdots,M_p\}$ is a generating set of $Q_m^{(p)}$.

(iii) $T_{(p^m)}$ is a subgroup of $Q_m^{(p)}$. Explicitly, we have $T_{(p^m)}=\{M\in Q_m^{(p)}\mid det(M)=1\}$.

Remark 4 (Fermat's little theorem)**.** *Let p be a prime. If $a \in \mathbb{Z}$ and a is not divisible by p, then we have*

$$a^{p-1} \equiv 1 \mod p \, .$$

Corollary 5. *Let p be a prime and $q \in \{1, \cdots, p-1\}$. Then there exists $0 \neq c \in \mathbb{N}$ such that $1 + (p-1)q^{p-1} = cp$.*

Proof. Since p is a prime and q is not divisible by p, we have

$$\begin{aligned} & q^{p-1} \equiv 1 \mod p \\ \implies & (p-1)q^{p-1} \equiv p-1 \mod p \\ \implies & 1 + (p-1)q^{p-1} \equiv p \equiv 0 \mod p \, . \end{aligned}$$

Thus there exists $c \in \mathbb{N}$ such that $1 + (p-1)q^{p-1} = cp$. □

Theorem 3. *Let p be a prime. For any $m \in \mathbb{N}$, we have $Q_m^{(p)} = G_m^{(p)}$. In particular, for every element $S_\xi \in T_{(p^m)}$, we can express ξ uniquely as*

$$\xi(q) = \prod_{k=1}^{m} exp\left[\frac{2\pi i}{p^k}\left(\sum_{a=0}^{p-1} \vartheta_{k,a} q^a\right)\right] \, , \tag{19}$$

where $\vartheta_{k,a} \in \mathbb{Z}_p$ (and $\prod_{q=0}^{p} \xi(q) = 1$).

Proof. This result can be obtained from Thm. 2 in [6]. Here, we provide an independent proof. It is clear that $G_m^{(p)} \subseteq Q_m^{(p)}$. We are left to show that $Q_m^{(p)} \subseteq G_m^{(p)}$. We claim that there exists $S_{\xi_0} \in G_m^{(p)}$ such that $S_{\xi_0} = diag\left(exp(\frac{2\pi i}{p^m}), 1, \cdots, 1\right)$. Then for $b \in \{1, \cdots, p-1\}$, we define $S_{\xi_b} \in G_m^{(p)}$ by $\xi_b(q) = \xi_0(q-b)$. Thus we have $S_{\xi_b} = diag(1, \cdots, 1, exp(\frac{2\pi i}{p^m}), 1, \cdots, 1)$ where $exp(\frac{2\pi i}{p^m})$ appear in the $b+1^{th}$ position. Observe that any $M \in Q_m^{(p)}$ can be expressed as

$$M = S_{\xi_0}^{k_0} S_{\xi_1}^{k_1} \cdots S_{\xi_{m-1}}^{k_{m-1}} \, ,$$

where $k_0, \cdots, k_{m-1} \in \mathbb{Z}_{p^m}$. Therefore we can define $S_{\bar{\xi}} \in G_m^{(p)}$ where $\bar{\xi} = \prod_{b=0}^{m-1} \xi_b^{k_b}$ such that $S_{\bar{\xi}} = M$. Thus we can conclude that for any $M \in Q_m^{(p)}$, there exists $S_\xi \in G_m^{(p)}$ such that $S_\xi = M$, hence, $Q_m^{(p)} \subseteq G_m^{(p)}$.

Next we prove our claim. We proceed by induction on m. Consider the case $m = 1$, and define

$$\xi(q) = exp\left(\frac{2\pi i}{p}(1 + (p-1)q^{p-1})\right) \, .$$

Then for $q = 0$, we have $\xi(0) = exp(\frac{2\pi i}{p})$. For $q \in \{1, \cdots, p-1\}$, by Cor. 5, there exists $c_q \in \mathbb{N}$ such that

$$1 + (p-1)q^{p-1} = c_q p \, . \tag{20}$$

Thus for $q \neq 0$, we have

$$\xi(q) = exp\left(\frac{2\pi i}{p}(1 + (p-1)q^{p-1})\right) = exp(2\pi i c_q) = 1 \, .$$

Assume the statement is true for $m = n$, and consider the case $m = n + 1$. We want to find $S_\xi \in G_{n+1}^{(p)}$ such that $S_\xi = diag\left(exp(\frac{2\pi i}{p^{n+1}}), 1, \cdots, 1\right)$. Let $M \in Q_n^{(p)}$ be given as

$$M = diag\left(1, exp\left(-\frac{2\pi i}{p^n}(c_1)\right), exp\left(-\frac{2\pi i}{p^n}(c_2)\right), \cdots, exp\left(-\frac{2\pi i}{p^n}(c_{p-1})\right)\right) .$$

By induction hypothesis, there exists $S_\theta \in G_n^{(p)}$ where

$$\theta(q) = \prod_{k=1}^{n} exp\left[\frac{2\pi i}{p^k}\left(\sum_{a=0}^{p-1} c_{k,a} q^a\right)\right] ,$$

such that

$$S_\theta = diag\left(1, exp\left(-\frac{2\pi i}{p^n}(c_1)\right), exp\left(-\frac{2\pi i}{p^n}(c_2)\right), \cdots, exp\left(-\frac{2\pi i}{p^n}(c_{p-1})\right)\right) .$$

Next, we define $S_\xi \in G_{n+1}^{(p)}$ where

$$\xi(q) = \theta(q) exp\left(\frac{2\pi i}{p^{n+1}}(1 + (p-1)q^{p-1})\right) .$$

For $q = 0$, we have $\xi(0) = \theta(0) exp(\frac{2\pi i}{p^{n+1}}) = exp(\frac{2\pi i}{p^{n+1}})$. For $q \in \{1, \cdots, p-1\}$, we have

$$\xi(q) = \theta(q) exp\left(\frac{2\pi i}{p^{n+1}}(1 + (p-1)q^{p-1})\right) = exp\left(-\frac{2\pi i}{p^n} c_q\right) exp\left(\frac{2\pi i}{p^{n+1}}(c_q p)\right) = 1 ,$$

where we used Eq. (20). Consequently, there exists $S_\xi \in G_{n+1}^{(p)}$ such that $S_\xi = diag(exp(\frac{2\pi i}{p^{n+1}}), 1, \cdots, 1)$. □

B Even vs odd prime

In this section, we will discuss the group structure of $K_Q^{\otimes n}(2)$ where $Q = T_{(2^m)}$ for some $m \geq 1$. We will show that Thm. 2 does not work for $p = 2$.

Lemma 9. *Let $Q = T_{(2^m)}$. Then $K_Q(2)$ is isomorphic to the dihedral group $D_{2^{m+1}}$ of order 2^{m+1}.*

Proof. Observe that $T_{(2^m)}$ can be expressed as

$$T_{(2^m)} = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \middle| \, a \in \mathbb{C},\ a^{2^m} = 1 \right\} ,$$

which is a cyclic group generated by the matrix $M = \begin{pmatrix} e^{2\pi i/2^m} & 0 \\ 0 & e^{-2\pi i/2^m} \end{pmatrix}$. Therefore

$$K_{T_{(2^m)}}(2) = \langle M, X \rangle . \tag{21}$$

Notice that M has order 2^m and X has order 2. By simple calculation, we also have $XMX = M^{-1}$. By identifying X with reflection and M with rotation in the dihedral group, we have

$$K_{T_{(2^m)}}(2) = \langle M, X \rangle \cong \langle r, s \mid r^{2^m} = s^2 = 1, srs = r^{-1} \rangle \cong D_{2^{m+1}} . \qquad \square$$

Remark 5. *Observe that* $K_{T_{(4)}}(2) \cong D_8 \cong H(\mathbb{Z}_2) = \langle X, Z\rangle$[13] *and* $K_{T_{(2)}}(2) \cong \mathbb{Z}_2^2$.

Lemma 10. *Assume that* $Q = T_{(2^m)}$ *where* $m \geq 2$. *Let* $M = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} X^b$ *and* $M' = \begin{pmatrix} a' & 0 \\ 0 & a'^{-1} \end{pmatrix} X^{b'}$ *be elements of* $K_Q(2)$ *such that* $[M, M'] = \pm\mathbb{1} \in Z(K_Q(2))$. *Then one of the following cases hold:*

(1) $b = b' = 0$ *and* $M, M' \in Q$. *In particular,* $[M, M'] = \mathbb{1}$.

(2) $b = 1$, $b' = 0$ *and* $M' \in T_{(4)}$. *In addition, if* $[M, M'] = \mathbb{1}$, *then* $M' \in Z(K_Q(p))$.

(3) $b = 0$, $b' = 1$ *and* $M \in T_{(4)}$. *In addition, if* $[M, M'] = \mathbb{1}$, *then* $M \in Z(K_Q(p))$.

(4) $b = b' = 1$ *and* $M = S_\chi M'$ *where* $S_\chi \in T_{(4)}$. *In addition, if* $[M, M'] = \mathbb{1}$, *then* $M = \pm M'$.

Proof. First, we consider the case where $b = b' = 0$. In this case, we have $M, M' \in Q$. Thus $[M, M'] = \mathbb{1}$. Next, by Lm. 9, we can identity $K_Q(2)$ with the dihedral group. In other words, we have $M = r^k s^b$ and $M' = r^{k'} s^{b'}$ for some $k, k' \in \mathbb{N}$, where r and s are the rotation and reflection generator of the dihedral group; respectively. Then our assumption $[M, M'] = \pm\mathbb{1}$ can be rewritten as $[r^k s^b, r^{k'} s^{b'}] = r^n$ where $r^{2n} = 1$.

First, we consider $b = 1$ and $b' = 0$. In this case, we have $M = r^k s$ and $M' = r^{k'}$. By calculation, we get

$$r^{-n} = r^n = [M, M'] = (r^k s)(r^{k'})(sr^{-k})(r^{-k'}) = r^k r^{-k'} r^{-k} r^{-k'} = r^{-2k'} \Rightarrow (r^{k'})^4 = 1 \, .$$

Thus we can conclude that $M'^4 = \mathbb{1}$ and therefore $M' \in T_{(4)}$. In addition, if $[M, M'] = \mathbb{1}$, we have $1 = r^{2k'}$, then $M'^2 = \mathbb{1}$. It follows that $M' = \pm\mathbb{1} \in Z(K_Q(2))$. The case $b = 0$ and $b' = 1$ is similar.

Next, consider $b = b' = 1$. In this case, we have $M = r^k s$ and $M' = r^{k'} s$. By calculation, we get

$$r^n = [M, M'] = (r^k s)(r^{k'} s)(sr^{-k})(sr^{-k'}) = r^k r^{-k'} r^k r^{-k'} = r^{2(k-k')} \, .$$

We can now conclude that $(r^{k-k'})^4 = 1$ and $r^{k'} = r^{-n} r^{k-k'} r^k$. Observe that $(r^{-n} r^{k-k'})^4 = 1$. Thus $M = S_\chi M'$ for some $S_\chi \in T_{(4)}$. In addition, if $[M, M'] = \mathbb{1}$, we have $(r^{k-k'})^2 = 1$ and therefore $M = \pm M'$. □

Corollary 6. *Maximal* 2*-torsion abelian subgroups of* $K_Q(2)$ *fall into two classes:*

- *the subgroup* $T_{(2)}$, *and*
- $\langle -\mathbb{1}, S_\xi X\rangle$ *where* $S_\xi \in Q = T_{(2^m)}$.

Any two distinct maximal 2*-torsion abelian subgroups intersect at the center* $Z(K_Q(2)) = \{\pm\mathbb{1}\}$.

Proof. This follows immediately from Lm. 10 with $[M, M'] = \mathbb{1}$. □

Example 1. *Define* $M = S_{\xi_1} X$ *and* $N = S_{\xi_2} X$ *where*

$$\xi_1(q) = (-1)^{1+q} i \, ,$$
$$\xi_2(q) = (-1)^q i \, .$$

[13]The isomorphism is given by mapping $X \in K_{T_{(4)}}(2)$ to $X \in H(\mathbb{Z}_2)$ and mapping $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \in K_{T_{(4)}}(2)$ to $XZ \in H(\mathbb{Z}_2)$.

In other words, we have $M = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ *and* $N = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$. *Notice that* $M^2 = N^2 = \mathbb{1}$ *and* $[M, N] = \mathbb{1}$. *Suppose that we define* ϕ *for* $p = 2$ *analogous to the odd case, more precisely using the* P *map in Def. 2, we have*

$$\phi(M) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} ,$$
$$\phi(N) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

Thus we have $\phi(M)\phi(N) = \mathbb{1}$. *On the other hand, we have* $MN = -\mathbb{1}$ *and therefore*

$$\phi(MN) = -\mathbb{1} \neq \phi(M)\phi(N) .$$

Notice that both $\phi(M)$ *and* $\phi(N)$ *are elements of* $H(\mathbb{Z}_2)$ *rather than* $K_{T_{(2)}}(2)$.

Remark 6. *Thm. 2 does not work for* $p = 2$. *Note first that unlike the odd prime case (cf. Rmk. 2), for* $p = 2$ *we have* $\mathcal{P}_2 \ncong H(\mathbb{Z}_2) \ncong K_{T_{(2)}}(2) = T_{(2)} \rtimes \langle X \rangle = \langle -\mathbb{1}, X \rangle$. *Now, as defined in Def. 2,* ϕ *maps into* $H^{\otimes n}(\mathbb{Z}_2)$ *rather than* $\langle -\mathbb{1}, X \rangle^{\otimes n}$, *yet it is easy to see that* $\phi : K_{T_{(2)}}^{\otimes n} \to H^{\otimes n}(\mathbb{Z}_2)$ *is not a homomorphism when restricted to 2-torsion abelian subgroups (see Ex. 1 above).*

Moreover, there is no way to adapt Def. 2 in such a way that ϕ *maps* $K_Q^{\otimes n}(2)$ *into* $\langle -\mathbb{1}, X \rangle^{\otimes n}$ *for* $n > 1$. *If that were the case, analogous arguments to those in Thm. 2 would imply that* $K_Q^{\otimes n}$ *is noncontextual, yet* $K_Q^{\otimes n}$ *is contextual. To see this, we remark that the quantum solution corresponding to the LCS given by Mermin-Peres square already arises for* $H(\mathbb{Z}_2)^{\otimes 2}$.[14] *Consequently,* $H(\mathbb{Z}_2)^{\otimes n}$ *is contextual for all* $n > 1$. *Finally, using the isomorphism* $K_{(4)} \cong H(\mathbb{Z}_2)$ *(cf. Rmk. 5) it also follows that* $K_{(2^m)}^{\otimes n}$ *is contextual for all* $n > 1, m > 2$. *As a final remark note that Corollary 6 implies that* $K_Q(2)$ *is noncontextual.*

[14] In fact, it is sufficient to note that $Y \otimes Y = -ZX \otimes ZX$ in Fig. 1 (a).