# On Sets of Commuting and Anticommuting Paulis

Rahul Sarkar [1,2] Ewout van den Berg [2]

[1]Institute for Computational Mathematics and Engineering, Stanford University

[2]IBM T.J. Watson Research Center

November 25, 2019

# Contents

# Contents

# Motivation

The Pauli group is important in the theory of quantum computing, quantum error correction etc. In many cases, people study sets of Paulis with a specific structure.

- For example, in the theory of stabilizers in quantum error correction, the set of stabilizers is a commuting set of Paulis. This topic is well studied.
- Comparatively we found that sets of anticommuting Paulis were less studied. But they are also important, for example in simulation of fermionic systems.
- Subsequently we have also learned that anticommuting sets can also be useful in aspects of quantum code designs.

We decided to look more into commuting and anticommting sets of Paulis, specifically *maximal sets*.

# Definitions: Pauli group

n-Pauli group: $\mathcal{P}_n = \{\gamma \left(\bigotimes_{j=1}^{n} T_j\right) : T_j \in \{\sigma_i, \sigma_x, \sigma_y, \sigma_z\}, \gamma \in \{\pm 1, \pm i\}\}$.

$\sigma_i, \sigma_x, \sigma_y, \sigma_z$ are the 1-qubit $I, X, Y, Z$ gates. $|\mathcal{P}_n| = 4^{n+1}$.

Abelian n-Pauli group: The quotient group $\mathcal{P}_n/K$, $K = \{I, -I, iI, -iI\}$.

$\mathcal{P}_n/K$ is an abelian group. $|\mathcal{P}_n/K| = 4^n$.

We say that two elements $P, Q \in \mathcal{P}_n/K$ *commute* (*anticommute*) whenever any chosen representative of $P$ commutes (anticommutes) with any chosen representative of $Q$. It is easily verified that this is a well defined notion, that is it does not depend on the choice of the representatives.

# Definitions: commuting/anticommuting sets

- **Commuting sets:** A subset $\mathcal{H} \subseteq \mathcal{P}_n/K$ is *commuting*, if no two distinct elements $P, Q \in \mathcal{H}$ anticommute.
- **Anticommuting sets:** A subset $\mathcal{H} \subseteq \mathcal{P}_n/K$ is *anticommuting*, if no two distinct elements $P, Q \in \mathcal{H}$ commute.
- **Maximally commuting sets:** A subset $\mathcal{H} \subseteq \mathcal{P}_n/K$ is *maximally commuting*, if $\mathcal{H} \cup \{P\}$ is not commuting for all $P \notin \mathcal{H}$.
- **Maximally anticommuting sets:** A subset $\mathcal{H} \subseteq \mathcal{P}_n/K$ is *maximally anticommuting*, if $\mathcal{H} \cup \{P\}$ is not anticommuting for all $P \notin \mathcal{H}$.

# Definitions: commutativity maps

Given $P, Q \in \mathcal{P}_n/K$ we define the commutativity function $\mathrm{comm}(P, Q)$ such that

$$\mathrm{comm}(P, Q) = \begin{cases} 1 & \text{if } P \text{ and } Q \text{ commute,} \\ -1 & \text{otherwise.} \end{cases}$$

- **Commutativity map:** For any set $\mathcal{H} \subseteq \mathcal{P}_n/K$ and element $P \in \mathcal{P}_n/K$, we define the *commutativity map* of $P$ with respect to $\mathcal{H}$ as $\Omega_{P,\mathcal{H}} : \mathcal{H} \to \{1, -1\}$, such that $\Omega_{P,\mathcal{H}}(Q) = \mathrm{comm}(P, Q)$ for all $Q \in \mathcal{H}$.

It is clear that if $|\mathcal{H}| = k$, then there are exactly $2^k$ distinct commutativity maps.

# Definitions: generating sets

Let $\mathcal{H}$ be a subset of $\mathcal{P}_n/K$.

- A set $\mathcal{G} \subseteq \mathcal{H}$ is a *generating set* of $\mathcal{H}$ whenever any element in $\mathcal{H}$ can be expressed as a product of the elements in $\mathcal{G}$.
- For any $\mathcal{G} \subseteq \mathcal{P}_n/K$, we denote by $\langle \mathcal{G} \rangle$ the *generated set* of $\mathcal{G}$; that is, all elements that can be generated by products of the elements in $\mathcal{G}$.
- The set $\mathcal{G}$ is called a *minimal generating set*, if no proper subset of $\mathcal{G}$ generates $\langle \mathcal{G} \rangle$.
- We say that the elements in minimal generating sets are *independent*.

# Two easy results

The first lemma shows that generated sets always form a subgroup of $\mathcal{P}_n/K$, and also deals with the sizes of minimal generating sets in relation to the sizes of the sets generated by them.

## Lemma

*The abelian Pauli group $\mathcal{P}_n/K$ satisfies the following properties.*

a. *If $\mathcal{G} \subseteq \mathcal{P}_n/K$ is non-empty, then $\langle \mathcal{G} \rangle$ is a subgroup of $\mathcal{P}_n/K$.*
b. *If $\mathcal{S}$ is a subgroup of $\mathcal{P}_n/K$, then $|\mathcal{S}| = 2^\ell$, for some $0 \leq \ell \leq 2n$. $\mathcal{G}$ is a generating set of $\mathcal{S}$ iff $\langle \mathcal{G} \rangle = \mathcal{S}$. For minimal generating sets $\mathcal{G}$ it holds that $I \in \mathcal{G}$ iff $\mathcal{S} = \{I\}$. In addition, if $\mathcal{S} \neq \{I\}$ then a minimal generating set $\mathcal{G}$ of $\mathcal{S}$ always exists, and satisfies $|\mathcal{G}| = \ell$, and $\prod \mathcal{H} \neq I$ for all $\mathcal{H} \subseteq \mathcal{G}$.*
c. *If $\mathcal{G} \subseteq \mathcal{P}_n/K$ is a minimal generating set, then $|\mathcal{G}| \leq 2n$. Moreover if $|\mathcal{G}| \geq 2$, and $\mathcal{G}' \subset \mathcal{G}$, then $P \in (\mathcal{G} \setminus \mathcal{G}')$ implies $P \notin \langle \mathcal{G}' \rangle$.*

# Two easy results

The next lemma characterizes what happens when we take the product of all the elements of a generated set.

## Lemma

*Let $\mathcal{G} \subseteq \mathcal{P}_n/K$ be a generating set. Then*

$$\prod \langle \mathcal{G} \rangle = \begin{cases} Q & \text{if } \mathcal{G} = \{Q\}, \\ I & \text{otherwise.} \end{cases} \tag{1}$$

*Thus if $\mathcal{S}$ is a subgroup of $\mathcal{P}_n/K$, and $|\mathcal{S}| \neq 2$, then $\prod \mathcal{S} = I$.*

## Proof.

Observe that this is true if you have a minimal generating set of 2 elements. Then use induction. □

# An important lemma

There are many ways of proving the following result.

## Lemma

*Let $\mathcal{G} \subseteq \mathcal{P}_n/K$ be a minimal generating set with $\mathcal{G} \neq \{I\}$ and $|\mathcal{G}| = k$. Then each of the $2^k$ commutativity maps with respect to $\mathcal{G}$ is generated by $4^n/2^k$ distinct elements $P \in \mathcal{P}_n/K$.*

## Proof.

The result is easy to prove if you can prove the special case $k = 2n$. This is turn is equivalent to showing that if $k = 2n$, then $I$ is the only element that commutes with the generating set. □

We think this result should be commonly known, however we were not able to find a reference. Definitely this is known in the case $\mathcal{G}$ is a commuting set.

# Contents

# An easy consequence

**Lemma**

*If $\mathcal{S} \subseteq \mathcal{P}_n/K$ is maximally commuting, then $\mathcal{S}$ is a subgroup of $\mathcal{P}_n/K$.*

**Proof.**

Since $I$ commutes with all elements in $\mathcal{P}_n/K$, it follows that $I \in \mathcal{S}$ by maximality. If $P, Q \in \mathcal{C}$ are distinct elements, then $PQ$ commutes with all elements in $\mathcal{S}$, and therefore by maximality $PQ \in \mathcal{C}$. Hence $\mathcal{S}$ is a subgroup of $\mathcal{P}_n/K$. □

This lemma establishes the fact that for a maximally commuting set, the product of all the elements in the set is equal to $I$.

# A decomposition

We can decompose any set $\mathcal{S} \subseteq \mathcal{P}_n/K$, with $n \geq 2$, as

$$\mathcal{S} = (\sigma_i \otimes \mathcal{C}_i) \cup (\sigma_x \otimes \mathcal{C}_x) \cup (\sigma_y \otimes \mathcal{C}_y) \cup (\sigma_z \otimes \mathcal{C}_z), \tag{2}$$

with possibly empty sets $\mathcal{C}_\ell \subseteq \mathcal{P}_{n-1}/K$ for $\ell \in \{i, x, y, z\}$. In the above we use the convention that $\sigma_\ell \otimes \mathcal{C} = \{\sigma_\ell \otimes P : P \in \mathcal{C}\}$, where we define $\sigma_\ell \otimes P$ to be the equivalence class $[\sigma_\ell \otimes A] \in \mathcal{P}_n/K$ for any chosen representative $A \in P$, the notion being well defined and independent of the choice of the representative $A$. In many cases we are not concerned with the exact labels of the sets and instead work with the decomposition

$$\mathcal{S} = (\sigma_i \otimes \mathcal{C}_i) \cup (\sigma_u \otimes \mathcal{C}_u) \cup (\sigma_v \otimes \mathcal{C}_v) \cup (\sigma_w \otimes \mathcal{C}_w), \tag{3}$$

where $(u, v, w)$ is an arbitrary permutation of $(x, y, z)$ that satisfies the condition that $\mathcal{C}_u = \emptyset$ implies $\mathcal{C}_v = \emptyset$, and $\mathcal{C}_v = \emptyset$ implies $\mathcal{C}_w = \emptyset$.

# Main results: commuting structure lemma

## Lemma

*Let $\mathcal{S} \subseteq \mathcal{P}_n/K$ be maximally commuting with $n \geq 2$ and decomposition of the form (3). Then $I \in \mathcal{C}_i$, and the following are true:*

a. *For $\ell \in \{i, x, y, z\}$ the elements within $\mathcal{C}_\ell$ commute with each other, as well as with all elements in $\mathcal{C}_i$. The elements between any pair of sets $\mathcal{C}_x$, $\mathcal{C}_y$, and $\mathcal{C}_z$ anticommute.*

b. *If $\mathcal{C}_v = \mathcal{C}_w = \emptyset$, then $\mathcal{C}_i = \mathcal{C}_u$, and $\mathcal{C}_i$ is a maximally commuting set.*

# Main results: commuting structure lemma

## Lemma

*Let $\mathcal{S} \subseteq \mathcal{P}_n/K$ be maximally commuting with $n \geq 2$ and decomposition of the form (3). Then $I \in \mathcal{C}_i$, and the following are true:*

- *Otherwise the sets $\mathcal{C}_i$, $\mathcal{C}_u$, $\mathcal{C}_v$, and $\mathcal{C}_w$ satisfy the following properties:*

  1. *for any $P \in \mathcal{C}_i$ we have $P * \mathcal{C}_i = \mathcal{C}_i * \mathcal{C}_i = \mathcal{C}_i$,*
  2. *for any $P \in \mathcal{C}_u$ we have $P * \mathcal{C}_u = \mathcal{C}_u * \mathcal{C}_u = \mathcal{C}_i$,*
  3. *for any $P \in \mathcal{C}_i$ and any $Q \in \mathcal{C}_u$ we have $P * \mathcal{C}_u = Q * \mathcal{C}_i = \mathcal{C}_i * \mathcal{C}_u = \mathcal{C}_u$,*
  4. *for any $P \in \mathcal{C}_u$ and any $Q \in \mathcal{C}_v$ we have $P * \mathcal{C}_v = Q * \mathcal{C}_u = \mathcal{C}_u * \mathcal{C}_v = \mathcal{C}_w$,*
  5. *$|\mathcal{C}_i| = |\mathcal{C}_u| = |\mathcal{C}_v| = |\mathcal{C}_w|$, and the sets are non-empty and disjoint*
  6. *sets $\mathcal{C}_i$, $(\mathcal{C}_i \cup \mathcal{C}_u)$, $(\mathcal{C}_i \cup \mathcal{C}_v)$, and $(\mathcal{C}_i \cup \mathcal{C}_w)$ are subgroups of $\mathcal{P}_{n-1}/K$.*

# Main results: All maximally commuting sets are of maximum size (no local "maximums")

**Theorem**

*Let $\mathcal{S} \subseteq \mathcal{P}_n/K$ be a maximally commuting set, then $|\mathcal{S}| = 2^n$.*

**Proof.**

Let $\mathcal{G}$ be a minimal generator set for $\mathcal{S}$. Suppose by contradiction that $k := |\mathcal{G}| > n$, then it follows that each commutativity map with $\mathcal{G}$ is generated by $4^n/2^k < 2^n$ elements. For all $Q \in \langle \mathcal{G} \rangle$, the commutativity map with respect to $\mathcal{G}$ is the all-commuting map, but this gives a contradiction, since $|\langle \mathcal{G} \rangle| = 2^k > 2^n$. Similarly, suppose that $|\mathcal{G}| < n$. In this case it follows that there must exist a $P \in (\mathcal{P}_n/K) \setminus \langle \mathcal{G} \rangle$ that commutes with all elements in $\mathcal{G}$, and therefore with all elements in $\langle \mathcal{G} \rangle$. It follows that $P$ could be added to $\mathcal{S}$, thus contradicting maximality. □

# Consequences

Strengthening of the commuting structure lemma.

## Corollary

*Let $\mathcal{S} \subseteq \mathcal{P}_n/K$ be a maximally commuting set with $n \geq 2$ and decomposition (3) with $\mathcal{C}_w \neq \emptyset$. Then $|\mathcal{C}_i| = |\mathcal{C}_u| = |\mathcal{C}_v| = |\mathcal{C}_w| = 2^{n-2}$. In addition, $(\mathcal{C}_i \cup \mathcal{C}_u)$, $(\mathcal{C}_i \cup \mathcal{C}_v)$, and $(\mathcal{C}_i \cup \mathcal{C}_w)$ are maximally commuting subgroups of $\mathcal{P}_{n-1}/K$.*

## Proof.

By Theorem 7, $|\mathcal{S}| = 2^n$. Since each of the four sets $\mathcal{C}$ have equal size by Lemma 5(c), it follows that each must have size $2^n/4 = 2^{n-2}$. The set $\mathcal{H} := \mathcal{C}_i \cup \mathcal{C}_\ell$ is commuting for any $\ell \in \{u, v, w\}$. From property 5 of Lemma 5(c) we know that $\mathcal{C}_i \cap \mathcal{C}_\ell = \emptyset$, and it therefore follows that $|\mathcal{H}| = 2^{2n-2}$, which is maximal by Theorem 7. □

# Two converses of the commuting structure lemma

## Lemma

*Let $\mathcal{S} \subseteq \mathcal{P}_{n-1}/K$ be maximally commuting. Then the set $\mathcal{S}' = (\sigma_i \otimes \mathcal{S}) \cup (\sigma_\ell \otimes \mathcal{S})$ is a maximally commuting subgroup of $\mathcal{P}_n/K$, for all $\ell \in \{x, y, z\}$.*

## Lemma

*Suppose we have four subsets $\mathcal{C}_i$, $\mathcal{C}_x$, $\mathcal{C}_y$, and $\mathcal{C}_z$ of $\mathcal{P}_{n-1}/K$, that satisfy the property in Lemma 5 (a), and also satisfy $|\mathcal{C}_i| = |\mathcal{C}_x| = |\mathcal{C}_y| = |\mathcal{C}_z| = 2^{n-2}$. Then the subset $\mathcal{S} = (\sigma_i \otimes \mathcal{C}_i) \cup (\sigma_u \otimes \mathcal{C}_x) \cup (\sigma_v \otimes \mathcal{C}_y) \cup (\sigma_w \otimes \mathcal{C}_z)$ is a maximally commuting subgroup of $\mathcal{P}_n/K$, for all permutations $(u, v, w)$ of $(x, y, z)$. In particular this implies that $\mathcal{C}_i$, $\mathcal{C}_x$, $\mathcal{C}_y$, and $\mathcal{C}_z$ also satisfy properties 1–6 of Lemma 5 (c).*

# Contents

# Basic properties of anticommuting sets

## Theorem

*Let $\mathcal{G} = \{P_1, \ldots, P_k\}$ be a set of anticommuting Paulis, then*

a. *if $k$ is even, then $Q = \prod \mathcal{G}$ anticommutes with $\mathcal{G}$, and $\mathcal{G} \cup \{Q\}$ is maximally anticommuting,*
b. *$\mathcal{G}$ is maximal implies that $k$ is odd,*
c. *$\prod \mathcal{G} = I$ implies that $\mathcal{G}$ is maximal and $k$ is odd,*
d. *for any proper subset $\mathcal{H} \subset \mathcal{G}$ it holds that $\prod \mathcal{H} \neq I$,*
e. *$\prod \mathcal{G} \neq I$ implies that $\mathcal{G}$ is a minimal generating set for a subgroup of order $2^k$,*
f. *$\prod \mathcal{G} = I$ implies that $\mathcal{G}$ is a generating set for a subgroup of order $2^{k-1}$.*

# Anticommuting structure theorem

**Theorem 4.2.** *(Anticommuting structure theorem) Let $\mathcal{G} \subseteq \mathcal{P}_n/K$ be maximally anticommuting with decomposition (3). Then the following statements are true.*

*(i) The elements within each of the sets anticommute, and elements in $\mathcal{C}_i$ anticommute with $\mathcal{C}_\ell$ for $\ell \in \{u, v, w\}$. Elements between $\mathcal{C}_u$, $\mathcal{C}_v$, and $\mathcal{C}_w$ commute.*

*(ii) Decomposition (3) has exactly one of the following forms:*

| *Non-empty sets* | *Properties* |
|---|---|
| *(a)* $\mathcal{C}_i$ | $\mathcal{C}_i$ *is maximally anticommutative and* $\lvert\mathcal{G}\rvert < 2n$. |
| *(b)* $\mathcal{C}_i$, $\mathcal{C}_u$ | $\lvert\mathcal{C}_i\rvert$ *is odd and* $\lvert\mathcal{C}_u\rvert$ *is even,* $\mathcal{C}_i \cup \mathcal{C}_u$ *is maximally anticommutative,* $\lvert\mathcal{G}\rvert < 2n$. |
| *(c)* $\mathcal{C}_i$, $\mathcal{C}_u$, $\mathcal{C}_v$ | $\lvert\mathcal{C}_i\rvert$ *is odd and* $\lvert\mathcal{C}_u\rvert$ *and* $\lvert\mathcal{C}_v\rvert$ *are even.* |
| *(d)* $\mathcal{C}_u$, $\mathcal{C}_v$, $\mathcal{C}_w$ | $\lvert\mathcal{C}_\ell\rvert$ *is odd for all* $\ell \in \{u, v, w\}$. |
| *(e) all* | $\lvert\mathcal{C}_u\rvert$, $\lvert\mathcal{C}_v\rvert$, *and* $\lvert\mathcal{C}_w\rvert$ *are either all odd or all even.* |

*(iii) The sets $\mathcal{C}_i$, $\mathcal{C}_\ell$ are disjoint for all $\ell \in \{u, v, w\}$. The sets $\mathcal{C}_a$, $\mathcal{C}_b$ are disjoint whenever $\lvert\mathcal{C}_a\rvert > 1$ or $\lvert\mathcal{C}_b\rvert > 1$, for every distinct $a, b \in \{u, v, w\}$.*

# The important result

## Corollary

*An anticommuting subset $\mathcal{G} \subseteq \mathcal{P}_n/K$ is maximally anticommuting iff $\prod \mathcal{G} = I$.*

## Proof.

The "if" part was already proved in Theorem 11 (c). For the other direction, assume that $\mathcal{G} \subseteq \mathcal{P}_n/K$ is maximally anticommuting. Without loss of generality, choose any term index of the underlying Pauli operators and permute the term order such that the selected index is the first one. It suffices to show that the product of all the elements in $\mathcal{G}$ can be written as $\sigma_i \otimes p$, since the result then holds for all terms due to the fact that the selected index was arbitrary. To complete the proof, consider the decomposition in (3). Anticommuting structure theorem guarantees that only one of the cases (a)–(e) can occur, and in each case the product of the first term is $\sigma_i$, as desired. □

# Sizes of anticommuting sets

For 1-Paulis we find that $\{I\}$ and $\{\sigma_x, \sigma_y, \sigma_z\}$ are maximally anticommuting sets. We can hierarchically generate set of higher-dimensional anticommuting sets from existing sets. For example, given sets $\mathcal{G}_n$ of maximally anticommuting $n$-Paulis, we can generate

1. $\mathcal{G}_{n+1} = (\sigma_x \otimes \mathcal{G}_n) \cup (\sigma_y \otimes I) \cup (\sigma_z \otimes I)$.
2. $\mathcal{G}_{2n+1} = (\sigma_x \otimes I \otimes \mathcal{G}_n) \cup (\sigma_y \otimes \mathcal{G}_n \otimes I) \cup (\sigma_z \otimes I \otimes I)$.

which are also maximally anticommuting subsets of $\mathcal{P}_{n+1}/K$ and $\mathcal{P}_{2n+1}/K$ respectively.

# Sizes of anticommuting sets

The next lemma is well known.

## Lemma

*If $\mathcal{G} \subseteq \mathcal{P}_n/K$ is anticommuting, then $|\mathcal{G}| \leq 2n+1$.*

No maximally anticommuting sets of even size.

## Corollary

*For every odd integer $\ell$ up to and including $2n+1$, there exists a maximally anticommuting subset of $\mathcal{P}_n/K$ of cardinality $\ell$.*

## Proof.

We know from the example at the beginning of this section that maximally anticommuting subsets of size $2n+1$ exist in $\mathcal{P}_n/K$, so take any such set $\mathcal{G}$. The result then follows by taking a subset of even size and then adding the product of all the elements to the subset. □

# Anticommuting sets of maximum size

In the next theorem, we clarify the structure of maximally anticommuting subsets of $\mathcal{P}_n/K$ that attain the maximum size.

## Theorem

*Given an anticommuting set $\mathcal{G} \subseteq \mathcal{P}_n/K$ with $2n+1$ with and decomposition (2). Then*

a. $\prod(\mathcal{C}_i \cup \mathcal{C}_\ell) = I$ *for* $\ell \in \{x, y, z\}$.

b. $\mathcal{C}_i \cup \mathcal{C}_\ell$ *is a maximally anticommuting set for* $\ell \in \{x, y, z\}$.

c. *Sets* $\mathcal{C}_x$, $\mathcal{C}_y$, *and* $\mathcal{C}_z$ *are non-empty.*

d. $\prod \mathcal{C}_i = \prod \mathcal{C}_x = \prod \mathcal{C}_y = \prod \mathcal{C}_z$. *Additionally* $\mathcal{C}_i = \emptyset$, *if and only if* $\prod \mathcal{C}_x = \prod \mathcal{C}_y = \prod \mathcal{C}_z = I$.

# Contents

# Can any anticommuting set be extended to the maximum size of $2n+1$?

By definition this cannot be done if $\mathcal{S}$ is maximally anticommuting, or when $|\mathcal{S}| = 2n+1$, in which case there is nothing to do. So the interesting case is when $\prod \mathcal{S} \neq I$.

## Lemma

*Let $\mathcal{S} \subseteq \mathcal{P}_n/K$ be an anticommuting set that is not maximally anticommuting. Then $\mathcal{S}$ can be extended to a maximally anticommuting set of cardinality $2n+1$.*

## Proof.

Basic idea is to extend the set by 1 element making sure that it is still anticommuting and independent. This can be done. Do this repeatedly till you reach size $2n$, then add the product of all elements to the set. □

# Is there an efficient algorithm to do the extension?

Previous lemma raises some interesting questions:

1. *Given an anticommuting set $\mathcal{S} \subseteq \mathcal{P}_n/K$ which is not maximally anticommuting, in how many distinct ways can we extend it to a bigger size?*

2. *Is there an efficient algorithm to perform the extension?*

# A technical device

## Lemma

*Let $\mathcal{S}$ be a set with $|\mathcal{S}| = m \geq 1$, and let $v : \mathcal{S} \to \{1, -1\}$ be any arbitrary map. Define a map $F_v : 2^{\mathcal{S}} \times \mathcal{S} \to \{1, -1\}$ by*

$$F_v(\mathcal{T}, x) = \begin{cases} v(x)(-1)^{|\mathcal{T}|-1} & \text{if } x \in \mathcal{T}, \\ v(x)(-1)^{|\mathcal{T}|} & \text{if } x \notin \mathcal{T}, \end{cases} \tag{4}$$

*and also define*

$$f(v) := \left( \sum_{x \in \mathcal{S}} (1 + v(x))/2 \right) = \sum_{x \in \mathcal{S}} \mathbb{1}_{\{v(x)=1\}}. \tag{5}$$

*If $m$ is even, then for every map $q : \mathcal{S} \to \{1, -1\}$, there exists a unique $\mathcal{U} \in 2^{\mathcal{S}}$ (possibly empty), such that $F_v(\mathcal{U}, \cdot) = q$.*

# A technical device (Cont.)

## Lemma

*If $m$ is odd, then we have the following cases:*

a. *If $q : \mathcal{S} \to \{1, -1\}$ is a map such that $f(q) \equiv f(v) \mod 2$, then there exist exactly two subsets $\mathcal{V}$, $\mathcal{S} \setminus \mathcal{V} \in 2^{\mathcal{S}}$ (at most one possibly empty), such that $F_v(\mathcal{V}, \cdot) = F_v(\mathcal{S} \setminus \mathcal{V}, \cdot) = q$.*

b. *If $q : \mathcal{S} \to \{1, -1\}$ is a map such that $f(q) \not\equiv f(v) \mod 2$, then there does not exist any subset $\mathcal{V}$ of $\mathcal{S}$ such that $F_v(\mathcal{V}, \cdot) = q$.*

## Proof.

Skipped but not too complicated. □

# Pattern of commutativity maps on cosets

## Theorem

*Let $\mathcal{G}$ be an anticommuting minimal generating set with $|\mathcal{G}| = m$. If $\mathcal{G} = \{I\}$, all elements of $\mathcal{P}_n/K$ commute with $I$. Otherwise the commutativity maps with respect to $\mathcal{G}$ of the elements in the cosets of $\langle\mathcal{G}\rangle$, have the following structure:*

1. *If $m$ is even, then in every coset of $\langle\mathcal{G}\rangle$, for every commutativity map $q : \mathcal{G} \to \{1, -1\}$ there exists exactly one element $P$, such that $\Omega_{P,\mathcal{G}} = q$.*

# Pattern of commutativity maps on cosets (Cont.)

## Theorem

2. *If $m$ is odd and $\mathcal{T}$ is a coset of $\langle \mathcal{G} \rangle$, then for all $Q \in \mathcal{T}$, $f(\Omega_{Q,\mathcal{G}}) \mod 2$ is a constant, using the notation in (5). Moreover if $P \in \mathcal{T}$, then for every commutativity map $q : \mathcal{S} \to \{1, -1\}$ such that $f(q) \equiv f(\Omega_{P,\mathcal{G}}) \mod 2$, there exist exactly two elements $Q, Q(\prod \mathcal{G}) \in \mathcal{T}$, such that $\Omega_{Q,\mathcal{G}} = \Omega_{Q(\prod \mathcal{S}),\mathcal{G}} = q$; while for every commutativity map $q : \mathcal{G} \to \{1, -1\}$ such that $f(q) \not\equiv f(\Omega_{P,\mathcal{G}}) \mod 2$, $\Omega_{Q,\mathcal{G}} \neq q$ for all $Q \in \mathcal{T}$.*
2. *If $m$ is odd, the cosets of $\langle \mathcal{G} \rangle$ can be grouped into two disjoint sets $\mathcal{F}_0$ and $\mathcal{F}_1$, with $|\mathcal{F}_0| = |\mathcal{F}_1| = 2^{2n-m-1}$, such that for all $\mathcal{T}_0 \in \mathcal{F}_0$ and all $P_0 \in \mathcal{T}_0$ it holds that $f(\Omega_{P_0,\mathcal{G}}) \equiv 0 \mod 2$, while for all $\mathcal{T}_1 \in \mathcal{F}_1$ and all $P_1 \in \mathcal{T}_1$ it holds that $f(\Omega_{P_1,\mathcal{G}}) \equiv 1 \mod 2$.*

# Pattern of commutativity maps on cosets (Cont.)

## Proof.

*(1), (2)* If $\mathcal{T}$ is a coset of $\langle\mathcal{G}\rangle$, then choosing any element $P \in \mathcal{T}$, we have $\mathcal{T} = P * \langle\mathcal{G}\rangle$. Because $\mathcal{G}$ is a minimal generating set, this induces a bijection $h : 2^{\mathcal{G}} \to \mathcal{T}$, defined by $h(\mathcal{U}) = P(\prod \mathcal{U})$. Given any element $Q \in \mathcal{T}$, we have $Q = P(\prod \mathcal{U})$ for some $\mathcal{U} \subseteq \mathcal{G}$. Moreover, the commutativity map $\Omega_{Q,\mathcal{G}}$, can be expressed in terms of the commutativity map $\Omega_{P,\mathcal{G}}$ as

$$\Omega_{Q,\mathcal{G}}(x) = \begin{cases} \Omega_{P,\mathcal{G}}(x)(-1)^{|\mathcal{U}|-1} & \text{if } x \in \mathcal{U}, \\ \Omega_{P,\mathcal{G}}(x)(-1)^{|\mathcal{U}|} & \text{if } x \notin \mathcal{U}, \end{cases} \tag{6}$$

for all $x \in \mathcal{G}$. The results then follow by applying Lemma 17, with $v(x) = \Omega_{P,\mathcal{G}}(x)$. For all commutativity maps $q$ that satisfy $f(q) \equiv f(\Omega_{P,\mathcal{G}}) \mod 2$, we can find the corresponding sets using the constructions in Lemma 17, and additionally for the odd case, by noting that for any $\mathcal{R} \subseteq \mathcal{G}$, $P(\prod \mathcal{R})(\prod \mathcal{G}) = P(\prod(\mathcal{G} \setminus \mathcal{R}))$. □

# Extend an anticommuting minimal generating set

**Algorithm 1** Extend anticommuting minimal generating set to cardinality $2n$

**procedure** EXTEND_GENERATING_SET($\mathcal{G}$) ▷ $\mathcal{G}$ is an anticommuting minimal generating set
  Set $\mathcal{T} \leftarrow \mathcal{G}$, $P \leftarrow \prod \mathcal{G}$, and $k \leftarrow |\mathcal{G}|$
  **while** $k < 2n$ **do**
    $U \leftarrow$ Sample uniformly from $\mathcal{P}_n/K$
    $V \leftarrow$ ANTICOMMUTING_ELEMENT_COSET($\mathcal{T}, U$) ▷ Find anticommuting element in coset
    **if** (($k$ even and $V \neq P$) or ($k$ odd and $V \neq 0$)) **then** ▷ Acceptance criteria
      $\mathcal{T} \leftarrow \mathcal{T} \cup \{V\}$, $P \leftarrow PV$
      $k \leftarrow k + 1$
  **return** $\mathcal{T}$

**Algorithm 2** Find anticommuting Pauli in coset given Pauli, and anticommuting minimal generating set

**procedure** ANTICOMMUTING_ELEMENT_COSET($\mathcal{T}, P$)
  Set $\mathcal{C} \leftarrow \{x \in \mathcal{T} : \Omega_{P,\mathcal{T}}(x) = 1\}$ ▷ Find elements in $\mathcal{T}$ that commute with $P$
  **if** $|\mathcal{T}|$ odd and $|\mathcal{C}|$ odd **then**
    $U \leftarrow 0$ ▷ Anticommuting element does not exist in coset
  **else if** ($|\mathcal{T}|$ even and $|\mathcal{C}|$ even) or ($|\mathcal{T}|$ odd and $|\mathcal{C}| \leq \lfloor |\mathcal{T}|/2 \rfloor$) **then**
    $U \leftarrow P(\prod \mathcal{C})$
  **else**
    $U \leftarrow P(\prod(\mathcal{T} \setminus \mathcal{C}))$
  **return** $U$

# Contents

# Counting commuting sets

Given a commuting minimal generating set, in how many ways can we extend it to a minimal commuting generating set of size $n$?

## Lemma

*Let $\mathcal{G} \subseteq \mathcal{P}_n/K$ be a commuting minimal generating set, possibly empty, and $|\mathcal{G}| = m$. If $\mathcal{G} = \{I\}$, then it cannot be extended to a larger commuting minimal generating set. Otherwise there are $\left(\prod_{k=m}^{m'-1}(4^n/2^k - 2^k)\right)/(m'-m)!$ distinct ways to extend $\mathcal{G}$ to a larger commuting minimal generating set $\mathcal{G}' \subseteq \mathcal{P}_n/K$, such that $\mathcal{G} \subseteq \mathcal{G}'$, $|\mathcal{G}'| = m' > 1$, and $m < m' \leq n$. For the case $m' = 1$, $m = 0$, there are $4^n$ distinct ways to perform the extension.*

# Counting commuting sets

## Lemma

*Let $\mathcal{S} \subseteq \mathcal{P}_n/K$, be a subgroup such that all elements commute. By Lemma 1 (b) and Theorem 7, $|\mathcal{S}| = 2^m$, for $0 \leq m \leq n$. Then the number $N_m$ of distinct commuting minimal generating sets $\mathcal{G}$ such that $\langle \mathcal{G} \rangle = \mathcal{S}$ is given by*

$$N_m = \frac{1}{m!} \prod_{k=0}^{m-1} (2^m - 2^k). \tag{7}$$

## Lemma

*The number $N_m$ of distinct commuting subgroups of $\mathcal{P}_n/K$ of order $2^m$, for $0 \leq m \leq n$, is*

$$N_m = \prod_{k=0}^{m-1} \frac{(4^n/2^k - 2^k)}{(2^m - 2^k)}. \tag{8}$$

# Counting anticommuting sets

Given an anticommuting minimal generating set, in how many ways can we extend it to a minimal anticommuting generating set of size $2n$?

## Theorem

*Let $\mathcal{G} \subseteq \mathcal{P}_n/K$ be an anticommuting minimal generating set, possibly empty, and $|\mathcal{G}| = m$. If $\mathcal{G} = \{I\}$, then it cannot be extended. Otherwise there are $\left(\prod_{k=m}^{m'-1} s(k)\right)/(m'-m)!$ distinct ways to extend $\mathcal{G}$ to a larger anticommuting minimal generating set $\mathcal{G}' \subseteq \mathcal{P}_n/K$, such that $\mathcal{G} \subseteq \mathcal{G}'$, $|\mathcal{G}'| = m' > 1$, and $m < m' \leq 2n$, where*

$$s(k) = \begin{cases} 4^n/2^k & \text{if } k \text{ is odd,} \\ 4^n/2^k - 1 & \text{if } k \text{ is even.} \end{cases} \tag{9}$$

*For the case $m' = 1$, $m = 0$, there are $4^n$ distinct ways to perform the extension.*

# Counting maximally anticommuting sets

How many maximally anticommuting sets are there of a fixed size?

## Corollary

*If $N_m$ is the number of maximally anticommuting subsets of $\mathcal{P}_n/K$ of cardinality $m$, then using $s(k)$ as defined in (9)*

$$N_m = \begin{cases} \frac{1}{m!} \prod_{k=0}^{m-2} s(k) & \text{if } m \text{ odd, and } m \leq 2n+1, \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

# Discussions

Some applications (work in progress) that we have learned to be important, by speaking to people, are:

- Can we find anticommuting sets of Paulis that have low Hamming weight? Best known result constructs $2n$ anticommuting Paulis with $\log_2 n$ Hamming weight. This is important in fermionic simulation. Lower bounds not known (?) [Sergey Bravyi]

- Anticommuting sets of Paulis are related to cyclically anticommuting sets of Paulis. These sets have use in quantum code design. [Ted Yoder]

# Discussions

Some applications (nothing immediate, needs more work) that we have learned to be important, by speaking to people, are:

- Can we find anticommuting sets of Paulis that have low Hamming weight? Best known result constructs $2n$ anticommuting Paulis with $\log_2 n$ Hamming weight. This is important in fermionic simulation. Lower bounds not known (?) [Sergey Bravyi]

- Anticommuting sets of Paulis are related to cyclically anticommuting sets of Paulis. These sets have use in quantum code design. [Ted Yoder]

# Acknowledgments


- We would like to thank Kristan Temme, Sergey Bravyi, and Ted Yoder for valuable discussions.

- R.S. would like to thank Arthur, Kanav, Jason, Katherine.

- R.S. would like to thank IBM for the internship opportunity, and Marco for giving me the freedom to work on this project.

Questions?