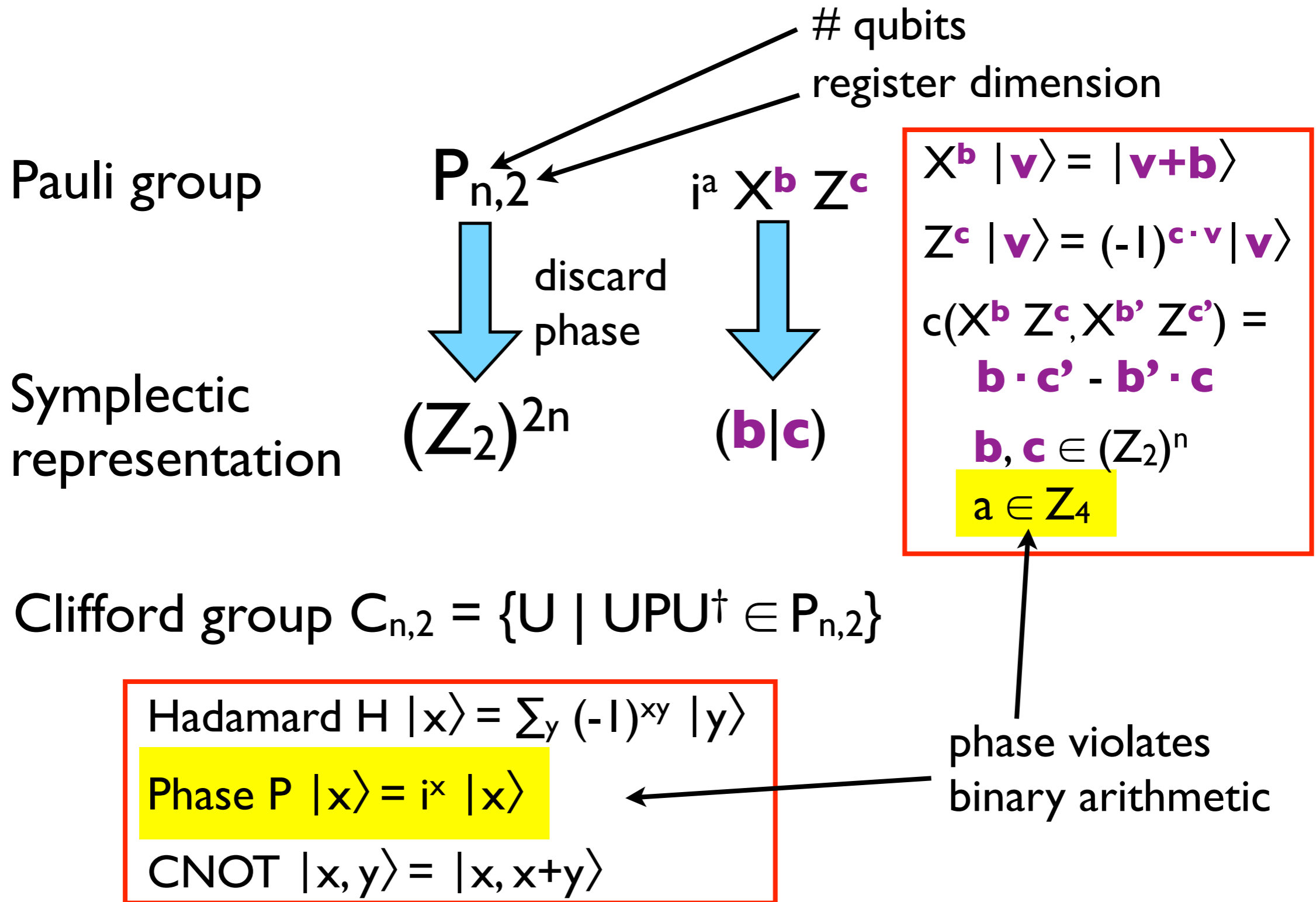


# Stabilizer Codes for Prime Power Qudits

Daniel Gottesman  
Perimeter Institute

# Qubit Pauli and Clifford Groups



# Qubit Stabilizer Codes

A qubit stabilizer  $S$  is an Abelian subgroup of  $P_{n,2}$  which does not contain  $-I$ . The code space corresponding to  $S$  is

$$\{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \quad \forall M \in S\}$$

**Example:** 5-qubit code  $[[5,1,3]]$

X	Z	Z	X	I
I	X	Z	Z	X
X	I	X	Z	Z
Z	X	I	X	Z

$n$  physical qubits

$r = n - k$  stabilizer generators  $M_1, \dots, M_r$

$k$  logical qubits

Other elements of  $S$  are products of generators.

E.g.:  $Z Z X I X = M_1 M_2 M_3 M_4$  for 5-qubit code

**Error syndrome:**

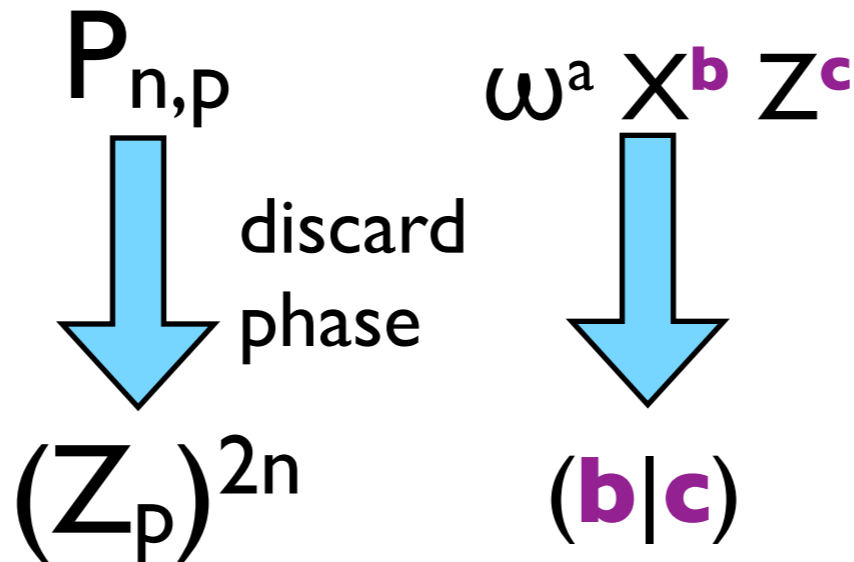
$$\mathbf{s}(P) = \{c(M_1, P), c(M_2, P), \dots, c(M_r, P)\} \in (\mathbb{Z}_2)^r$$

E.g., for 5-qubit code,  $\mathbf{s}(Y_3) = 1110$

# Prime Dimension Pauli and Clifford

Each register has prime dimension  $p$

Pauli group



Symplectic representation

$$X^b |v\rangle = |v+b\rangle$$

$$Z^c |v\rangle = \omega^{c \cdot v} |v\rangle$$

$$\omega = e^{2\pi i / p}$$

$$c(X^b Z^c, X^{b'} Z^{c'}) = b \cdot c' - b' \cdot c$$

$$b, c \in (\mathbb{Z}_p)^n$$

$$a \in \mathbb{Z}_p$$

Clifford group  $C_{n,p} = \{U \mid UPU^\dagger \in P_{n,p}\}$

$$\text{Fourier } F |x\rangle = \sum_y \omega^{xy} |y\rangle$$

$$\text{Phase } P |x\rangle = \omega^{x(x-1)} |x\rangle$$

$$\text{CNOT } |x, y\rangle = |x, x+y\rangle$$

phase uses mod  $p$  arithmetic, just like everything else

# Prime Dimensional Stabilizers

A qudit stabilizer  $S$  is an Abelian subgroup of  $P_{n,p}$  which does not contain  $\omega I$ . The code space corresponding to  $S$  is

$$\{|\psi\rangle \mid M|\psi\rangle = |\psi\rangle \quad \forall M \in S\}$$

**Example:** 5-qudit code  $[[5,1,3]]_p$

$X$	$Z$	$Z^{-1}$	$X^{-1}$	$I$
$I$	$X$	$Z$	$Z^{-1}$	$X^{-1}$
$X^{-1}$	$I$	$X$	$Z$	$Z^{-1}$
$Z^{-1}$	$X^{-1}$	$I$	$X$	$Z$

$n$  physical qudits

$r = n - k$  stabilizer generators  $M_1, \dots, M_r$

$k$  logical qudits

Other elements of  $S$  are products of generators, including powers  $1, \dots, p-1$

$$\text{E.g.: } Z Z^{-1} X^{-1} I X = M_1^{-1} M_2^{-1} M_3^{-1} M_4^{-1}$$

**Error syndrome:**

$$\mathbf{s}(P) = \{c(M_1, P), c(M_2, P), \dots, c(M_r, P)\} \in (\mathbb{Z}_p)^r$$

$$\text{E.g., for 5-qubit code, } \mathbf{s}(X_3 Z_3) = (1, -1, 1, 0)$$

# Composite Dimension

For composite qudit dimension  $q$ , we can do this too, using the same Pauli group (often known as the Heisenberg-Weyl group).

This is workable, but the stabilizer codes derived this way lack some of the standard structure of stabilizer codes for prime-dimensional qudits.

$$X^{\mathbf{b}} |\mathbf{v}\rangle = |\mathbf{v}+\mathbf{b}\rangle$$

$$Z^{\mathbf{c}} |\mathbf{v}\rangle = \omega^{\mathbf{c}\cdot\mathbf{v}} |\mathbf{v}\rangle$$

$$\omega = e^{2\pi i / q}$$

$$c(X^{\mathbf{b}} Z^{\mathbf{c}}, X^{\mathbf{b}'} Z^{\mathbf{c}'}) =$$

$$\mathbf{b}\cdot\mathbf{c}' - \mathbf{b}'\cdot\mathbf{c}$$

$$\mathbf{b}, \mathbf{c} \in (\mathbb{Z}_q)^n$$

$$a \in \mathbb{Z}_q$$

For instance, not all elements of  $P_{n,q}$  are equivalent (some have different orders), and there is no simple relationship between the number of generators of  $S$  and the number of logical qudits. There also do not need to be an integral number of qudits.

When  $q=p^m$ , it is better to use an alternate Pauli group based on the finite field of size  $q$ .

# Finite Fields

A field has Abelian addition and multiplication rules, including 0, 1, additive and multiplicative inverses, and a distributive law.

Familiar examples of infinite fields are rationals, reals, & complex #s. The simplest finite fields are  $\mathbb{Z}_p$ , mod  $p$  arithmetic for prime  $p$ .

For any  $q = p^m$ , there exists a **unique finite field  $\text{GF}(q)$  of size  $q$** . Such a field can be constructed by taking  $\mathbb{Z}_p$  and adjoining the roots of irreducible polynomials.

$\text{GF}(q)$  has **characteristic  $p$** , meaning any element added  $p$  times gives 0.

Example:

$$\text{GF}(9) = \mathbb{Z}_3(\alpha),$$
$$\alpha^2 + \alpha + 2 = 0$$

Elements are 0, 1, 2,  $\alpha$ ,  $\alpha + 1$ ,  $\alpha + 2$ ,  $2\alpha$ ,  $2\alpha + 1$ ,  $2\alpha + 2$

$$\text{E.g., } \alpha(2\alpha + 1) = 2\alpha^2 + \alpha$$
$$= 2(-\alpha - 2) + \alpha = 2\alpha + 2$$

# $\mathbb{Z}_p$ Versus $\text{GF}(p^m)$

$\text{GF}(q)$ ,  $q=p^m$  can be viewed as a vector space over  $\mathbb{Z}_p$ : pick  $m$  independent adjoining elements  $\alpha_1, \dots, \alpha_m$ . Then the elements of  $\text{GF}(q)$  can all be written in the form  $\sum_i c_i \alpha_i$ , with  $c_i \in \mathbb{Z}_p$ .

$$\begin{array}{c} \text{GF}(q) = (\mathbb{Z}_p)^m \\ \text{Tr} \downarrow \\ \mathbb{Z}_p \end{array}$$

The **trace** can be used to reduce elements of  $\text{GF}(q)$  to elements of  $\mathbb{Z}_p$ :

$$\text{tr } x = x + x^p + x^{p^2} + \dots + x^{p^{m-1}}$$

## Properties of trace:

1.  $\text{tr } \alpha \in \mathbb{Z}_p$
2.  $\text{tr } (\alpha + \beta) = \text{tr } \alpha + \text{tr } \beta$
3.  $\text{tr } (\alpha^p) = \text{tr } \alpha$
4.  $\text{tr } (a\beta) = a \text{tr } \beta$  (for  $a \in \mathbb{Z}_p$ )



# “Standard” Pauli Group for $q=p^m$

$$P_{n,q} = \{\omega^c X^\alpha Z^\beta\}$$

$$\alpha, \beta \in \text{GF}(q)^n, c \in \mathbb{Z}_p$$

$$X^\alpha |\gamma\rangle = |\gamma + \alpha\rangle$$

$$Z^\beta |\gamma\rangle = \omega^{\text{tr} \beta \cdot \gamma} |\gamma\rangle$$

For qudits of dimension  $q=p^m$ , the current preferred definition of the Pauli group takes advantage of the trace to allow the exponents of  $X$  and  $Z$  to be elements of  $\text{GF}(q)$ , but the phase is still drawn from  $\mathbb{Z}_p$ . Commutation can also be determined via  $\text{tr}$ :

$$c(X^\alpha Z^\beta, X^{\alpha'} Z^{\beta'}) = \text{tr} \alpha \cdot \beta' - \alpha' \cdot \beta$$

However, this definition of  $P_{n,q}$  is isomorphic to  $P_{mn,p}$ . That is, we actually have a  $p$ -dimensional Pauli group:

Given basis  $\{\alpha_1, \dots, \alpha_m\}$  for  $\text{GF}(q)$  over  $\mathbb{Z}_p$ , choose a **dual basis**  $\{\beta_1, \dots, \beta_m\}$  with the property  $\text{tr}(\alpha_i \beta_j) = \delta_{ij}$ .

Then let  $\alpha = \sum_i a_i \alpha_i$  and  $\beta = \sum_j b_j \beta_j$ , so we can interpret

$$\begin{array}{l} X^\alpha = X^{a_1} \otimes X^{a_2} \otimes \dots \otimes X^{a_m} \\ Z^\beta = Z^{b_1} \otimes Z^{b_2} \otimes \dots \otimes Z^{b_m} \end{array} \quad \longrightarrow \quad \begin{array}{l} q\text{-dim. qudit broken up} \\ \text{into } m \text{ } p\text{-dim qudits} \end{array}$$

# “Standard” Stabilizers for $q=p^m$

Consequently, if stabilizers are defined in the usual way from this Pauli group  $P_{n,q}$ , they are equivalent to  $mn$ -qudit stabilizers for  $p$ -dimensional qudits.

**Example:** 5-qudit code  $[[5,1,3]]_9$

$X$	$Z$	$Z^{-1}$	$X^{-1}$	$I$
$X^\alpha$	$Z^\alpha$	$Z^{-\alpha}$	$X^{-\alpha}$	$I$
$I$	$X$	$Z$	$Z^{-1}$	$X^{-1}$
$I$	$X^\alpha$	$Z^\alpha$	$Z^{-\alpha}$	$X^{-\alpha}$
$X^{-1}$	$I$	$X$	$Z$	$Z^{-1}$
$X^{-\alpha}$	$I$	$X^\alpha$	$Z^\alpha$	$Z^{-\alpha}$
$Z^{-1}$	$X^{-1}$	$I$	$X$	$Z$
$Z^{-\alpha}$	$X^{-\alpha}$	$I$	$X^\alpha$	$Z^\alpha$

$n$  physical qudits

$r$  stabilizer generators  $M_1, \dots, M_r$

$k = n-r/m$  logical qudits

Other elements of  $S$  are products of generators, including powers  $1, \dots, p-1$ . Powers of  $\alpha$  (for  $GF(9)$ ) require additional generators.

Error syndrome still a  $Z_p$  vector

**Error syndrome:**

$$\mathbf{s}(P) = \{c(M_1, P), c(M_2, P), \dots, c(M_r, P)\} \in (Z_p)^r$$

# True GF(q) Stabilizer Codes

Note the example 5-qudit code has an extra symmetry as do most other interesting GF(q) stabilizer codes. In the symplectic representation, it is GF(q)-linear, not just  $\mathbb{Z}_p$ -linear:

$$\begin{array}{cccc|cccccc}
 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 0 & 0 \\
 \alpha & 0 & 0 & -\alpha & 0 & 0 & \alpha & -\alpha & 0 & 0 \\
 0 & 1 & 0 & 0 & -1 & 0 & 0 & 1 & -1 & 0 \\
 0 & \alpha & 0 & 0 & -\alpha & 0 & 0 & \alpha & -\alpha & 0 \\
 -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\
 -\alpha & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & \alpha & -\alpha \\
 0 & -1 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 1 \\
 0 & -\alpha & 0 & \alpha & 0 & -\alpha & 0 & 0 & 0 & \alpha
 \end{array}$$

However, since each generator can have an independent phase, so there is no clear meaning of the “multiplication by  $\alpha$ ” symmetry in the Pauli group  $P_{n,q}$ . It should mean “exponentiation by  $\alpha$ ” but that is not a well-defined operation.

# Lifted Pauli Group (Odd q)

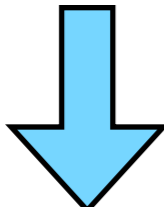
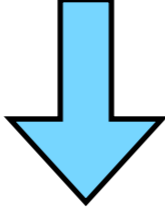
We want to lift the Pauli group to a larger group where exponentiation by elements of  $GF(q)$  is well-defined. We expand the set of possible phases to be all elements of  $GF(q)$ :

$$\dot{P}_{n,q} = \{\omega^\mu X^\alpha Z^\beta \mid \alpha, \beta \in GF(q)^n, \mu \in GF(q)\}$$

$$(\omega^\mu X^\alpha Z^\beta)(\omega^{\mu'} X^{\alpha'} Z^{\beta'}) = \omega^{\mu+\mu'-\alpha' \cdot \beta} X^{\alpha+\alpha'} Z^{\beta+\beta'}$$

$$c(X^\alpha Z^\beta, X^{\alpha'} Z^{\beta'}) = \alpha \cdot \beta' - \alpha' \cdot \beta \in GF(q)$$

We can project an element of the lifted Pauli group back to the regular Pauli group by using  $\text{tr}$  on the phase:

$\dot{P}_{n,q}$		$\omega^\mu X^\alpha Z^\beta$		$\Pi(PQ) = (\Pi P)(\Pi Q)$
	$\Pi$		$\Pi$	$c(\Pi P, \Pi Q) = \text{tr } c(P, Q)$
$P_{n,q}$		$\omega^{\text{tr } \mu} X^\alpha Z^\beta$		

# Exponentiation (Odd q)

phase and existing exponents  
get multiplied by  $\gamma$

$$(\omega^\mu X^\alpha Z^\beta)^\gamma = \omega^{\gamma\mu - [\gamma(\gamma-1)/2] \alpha \cdot \beta} X^{\gamma\alpha} Z^{\gamma\beta}$$

new phase term giving phase  
accumulation from  
“reorganizing” X and Z powers

Note that this formula reduces to the correct one for  $\gamma \in \mathbb{Z}_p$ .  
Exponentiation satisfies other standard properties:

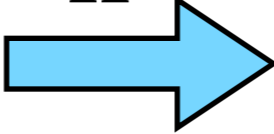
1.  $P^\gamma P^\delta = P^{\gamma+\delta}$
2.  $(P^\gamma)^\delta = P^{\gamma\delta}$
3.  $P^\gamma Q^\gamma = (PQ)^\gamma$  when  $c(P,Q)=0$

Because of the 1/2 that appears in the definition of exponentiation, this only works for odd q.

# Pauli Group Vs. Lifted Pauli Group

Exponentiation in  $\dot{P}_{n,q}$  lets us group together operators in  $P_{n,q}$  whose symplectic representations are related by  $GF(q)$  multiplication:

**Example:**  $\dot{P}_{1,9}$   $P_{1,9}$

$P = \omega^0 X^1 Z^1$ $P^2 = \omega^2 X^2 Z^2$ $P^\alpha = \omega^{1+\alpha} X^\alpha Z^\alpha$ $\vdots$	$\Pi$ 	$\omega^0 X^1 Z^1$ $\omega^1 X^2 Z^2$ $\omega^2 X^\alpha Z^\alpha$ $\vdots$
--	--	--

This single element is enough to generate all of the others, which correspond to  $m$  independent elements of  $P_{n,q}$ . The single phase  $\omega^\mu$  ( $\mu \in GF(q)$ ) gives the  $m$  independent phases  $\omega^a$  ( $a \in \mathbb{Z}_p$ ).

There is a **unique** correspondence  $P \in \dot{P}_{n,q}$  to  $\{\Pi P^Y\} \subset P_{n,q}$ .

# Lifted Stabilizers

$S$  is a **lifted stabilizer** if  $S$  is an Abelian subgroup of  $\dot{P}_{n,q}$  closed under exponentiation (i.e.,  $P \in S \Rightarrow P^\gamma \in S \forall \gamma \in GF(q)$ ), with  $\omega^\mu \notin S$ .

**Thm.:** The lifted stabilizers are in one-to-one correspondence with the true  $GF(q)$  stabilizers.

$$S \longleftrightarrow \Pi S$$

**Generalized eigenvalues:**  $|\psi\rangle$  is a generalized eigenvector of  $P \in \dot{P}_{n,q}$  if it is an eigenvector of  $P^\gamma \forall \gamma \in GF(q)$ . If it has eigenvalue  $\omega^{a_i}$  for  $P^{\gamma_i}$ , then the generalized eigenvalue is  $\omega^\mu$  s.t.  $\text{tr}(\gamma_i \mu) = a_i$  for all  $i$ .

The codewords are the generalized  $\omega^0$  eigenvectors of the elements of the lifted stabilizer, and an error  $E$  alters the generalized eigenvalues, so the error syndrome is the  $GF(q)$  vector of generalized eigenvalues after  $E$ , given by  $c(E, M_i)$  for generators  $M_i$  of the lifted stabilizer.

# True GF(q) Clifford Group

Consider  $\dot{C}_{n,q}$ , the group of automorphisms of  $\dot{P}_{n,q}$  that fix pure phases (i.e.  $U(\omega^\mu) = \omega^\mu$ ).

Elements of  $\dot{C}_{n,q}$  preserve exponentiation:  $U(P^\gamma) = [U(P)]^\gamma$  as well as preserving commutation relations like the regular Clifford group.

$$\begin{array}{ccc}
 U \in \dot{C}_{n,q} & & \Pi U(P) = U' (\Pi P) \text{ for } U' \text{ s.t.} \\
 \updownarrow \Pi & & U'(\gamma \mathbf{x} | \gamma \mathbf{z}) = \gamma U' (\mathbf{x} | \mathbf{z}) \text{ in the} \\
 U' \in C_{n,q} & & \text{symplectic representation}
 \end{array}$$

$\dot{P}_{n,q}$  can be interpreted as a subgroup of  $\dot{C}_{n,q}$  (inner automorphisms), and  $\dot{C}_{n,q} / \dot{P}_{n,q} = Sp(2n, GF(q))$



# Phases for Even $q$

With help from Greg Kuperberg

For the qubit Pauli group, the phase is a power of  $i$ , a 4th root of unity, rather than of a  $p$ th root of unity. To lift the phase properly, we need a way to lift  $Z_4$  to include elements of  $GF(2^m)$ .

Define a ring  $W_2(q)$  as follows, for  $q=2^m$ :

- Elements have the form  $\alpha = \alpha_1 + 2\alpha_2$ , with  $\alpha_1, \alpha_2 \in GF(q)$
- $\alpha + \beta = (\alpha_1 + \beta_1) + 2(\alpha_2 + \beta_2 + \sqrt{\alpha_1\beta_1})$
- $\alpha\beta = (\alpha_1\beta_1) + 2(\alpha_1\beta_2 + \alpha_2\beta_1)$

Square root is uniquely defined in a field of characteristic 2.

Let  $F(\alpha) = (\alpha_1)^2 + 2(\alpha_2)^2$  and let  $\text{tr } \alpha = \sum_{r=0}^{m-1} F^r(\alpha)$ .

Then  $\text{tr } \alpha \in W_2(2) = Z_4$ .

$W_2(q)$  is the ring of truncated Witt vectors, although with non-universal addition and multiplication rules.

# Lifted Pauli Group (Even q)

For even q, we let the phase and the exponents of X and Z be from  $W_2(q)$  to define the lifted Pauli group:

$$\dot{P}_{n,q} = \{i^\mu X^\alpha Z^\beta \mid \alpha, \beta \in W_2(q)^n, \mu \in W_2(q)\}$$

$$(i^\mu X^\alpha Z^\beta)(i^{\mu'} X^{\alpha'} Z^{\beta'}) = i^{\mu+\mu'-2\alpha' \cdot \beta} X^{\alpha+\alpha'} Z^{\beta+\beta'}$$

$$c(X^\alpha Z^\beta, X^{\alpha'} Z^{\beta'}) = \alpha \cdot \beta' - \alpha' \cdot \beta$$

but P and Q commute if  $2c(P,Q) = 0$

Commutation of X and Z gives  $i^2$

Projection  $\Pi (i^\mu X^\alpha Z^\beta) = i^{\text{tr } \mu} X^{\alpha_1} Z^{\beta_1}$

**Exponentiation:** for  $\gamma \in W_2(q)$ ,

$$(i^\mu X^\alpha Z^\beta)^\gamma = i^{\gamma\mu - \gamma(\gamma-1)\alpha \cdot \beta} X^{\gamma\alpha} Z^{\gamma\beta}$$

Notice that the 1/2 in the phase has been absorbed by the i.

$i^\mu X^\alpha Z^\beta$  is Hermitian if  $2\mu = 2\alpha \cdot \beta$

# Lifted Stabilizers, Cliffords (Even $q$ )

The rest of the construction is similar, with one exception:

Lifts are no longer unique

Thus:

- One lifted Pauli  $P$  corresponds to  $\{\Pi P^Y\}$ , but a set  $\{\Pi P^Y\}$  corresponds to some Pauli for any  $\alpha_2, \beta_2$ .
- A lifted stabilizer  $S$  corresponds to a true  $GF(q)$  stabilizer  $S' = \Pi S$ , but more than one  $S$  corresponds to the same  $S'$ .
- Automorphisms of  $\dot{P}_{n,q}$  correspond to Clifford group elements that are  $GF(q)$ -linear in the symplectic representation, but non-uniquely.

(Fine print: these constructions generally require Hermitian elements of  $\dot{P}_{n,q}$ .)

# Summary and Future Outlook

The lifted Pauli groups provide a way to define stabilizer codes for prime power qudits that:

- Have the natural  $GF(q)$  symmetry that one expects when dealing with codes on  $GF(q)$  registers
- Encode  $n-r$  logical qudits with  $r$  generators
- Correctly organize error syndrome information into vectors over  $GF(q)$

The mathematical context:

- The construction provides an unusual context in which one can define exponentiation
- $W_2(q)$  and related ideas may be helpful understanding other puzzles relating to stabilizers and the Clifford group (e.g., magic states)