Title: Stabilizer codes for prime power qudits

Speakers: Daniel Gottesman

Collection: Symmetry, Phases of Matter, and Resources in Quantum Computing

Date: November 28, 2019 - 10:15 AM

URL: http://pirsa.org/19110138

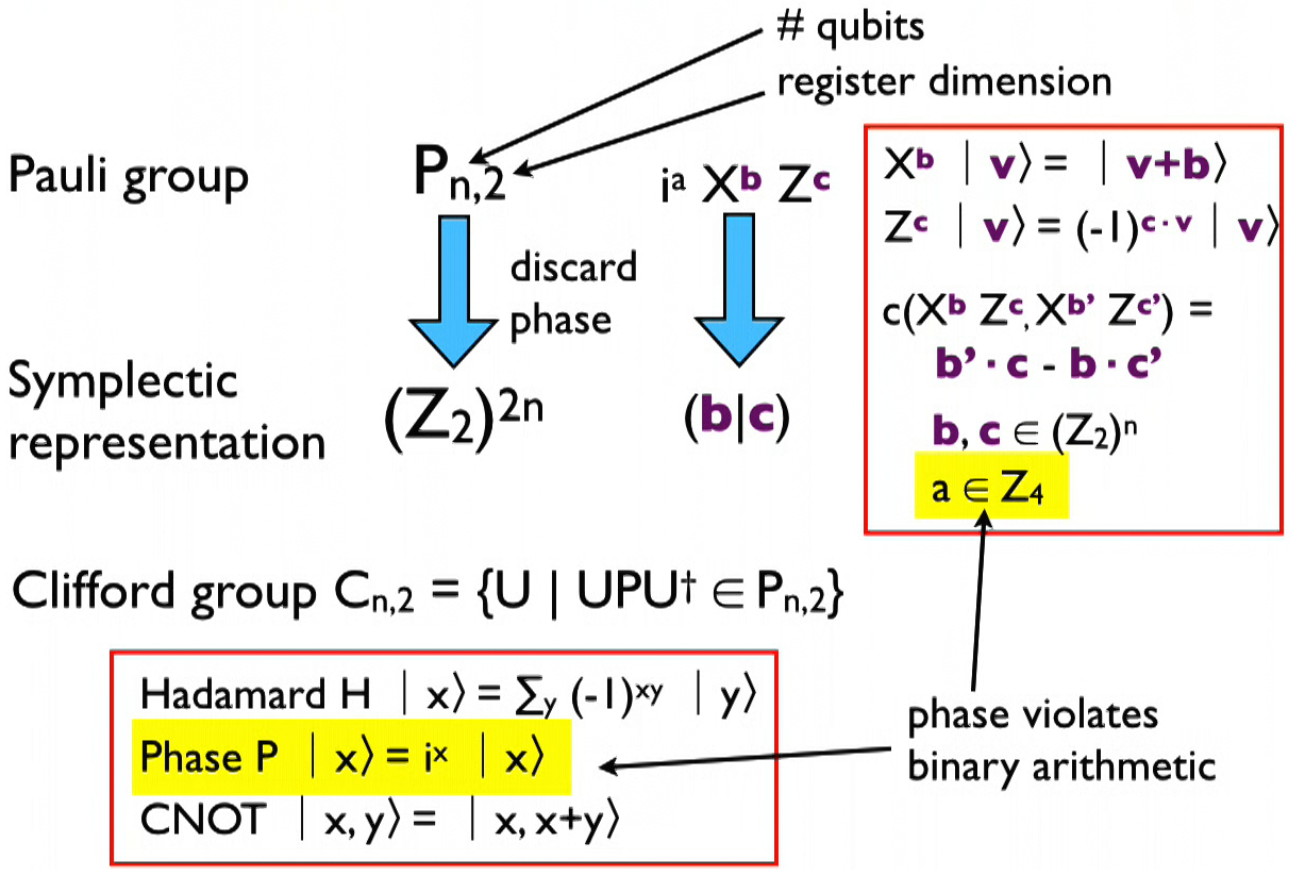
Abstract: There is a standard generalization of stabilizer codes to work with qudits which have prime dimension, and a slightly less standard generalization for qudits whose dimension is a prime power. However, for prime power dimensions, the usual generalization effectively treats the qudit as multiple prime-dimensional qudits instead of one larger object. There is a finite field GF(q) with size equal to any prime power, and it makes sense to label the qudit basis states with elements of the finite field, but the usual stabilizer codes do not make use of the structure of the finite field. I introduce the true GF(q) stabilizer codes, a subset of the usual prime power stabilizer codes which do make full use of the finite field structure. The true GF(q) stabilizer codes have nicer properties than the usual stabilizer codes over prime power qudits and work with a lifted Pauli group, which has some interesting mathematical aspects to it.

Stabilizer Codes for Prime Power Qudits

Daniel Gottesman
Perimeter Institute
Quantum Benchmark

Joint work with Greg Kuperberg

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

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

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 $M_1, ..., M_r$
k logical qubits

Other elements of S are products of generators.

E.g.: Z Z X I X = $M_1M_2M_3M_4$ for 5-qubit code

Error syndrome:

$\mathbf{s}(P) = \{c(M_1,P), c(M_2,P), ..., c(M_r,P)\} \in (Z_2)^r$

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

Prime Dimensional Stabilizers

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

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

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 $M_1, ..., M_r$
k logical qudits

Other elements of S are products of generators, including powers 1, ..., p-1

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

Error syndrome:

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

E.g., for 5-qubit code, $\mathbf{s}(X_3Z_3) = (-1,1,-1,0)$

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.

$$X^{\mathbf{b}} \,|\, \mathbf{v}\rangle = |\, \mathbf{v}+\mathbf{b}\rangle$$
$$Z^{\mathbf{c}} \,|\, \mathbf{v}\rangle = \omega^{\mathbf{c}\cdot\mathbf{v}} \,|\, \mathbf{v}\rangle$$
$$\omega = e^{2\pi i / q}$$
$$c(X^{\mathbf{b}} Z^{\mathbf{c}}, X^{\mathbf{b}'} Z^{\mathbf{c}'}) = \mathbf{b}'\cdot\mathbf{c} - \mathbf{b}\cdot\mathbf{c}'$$
$$\mathbf{b}, \mathbf{c} \in (Z_q)^n$$
$$a \in Z_q$$

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 Z_p, mod p arithmetic for prime p.

For any $q = p^m$, there exists a unique finite field GF(q) of size q. Such a field can be constructed by taking Z_p and adjoining the roots of irreducible polynomials.

GF(q) has characteristic p, meaning any element added p times gives 0.

Example:
$GF(9) = Z_3(\alpha)$,
$\alpha^2 + \alpha + 2 = 0$

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

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

Z_p Versus GF(p^m)

GF(q), $q=p^m$ can be viewed as a vector space over Z_p: pick m independent adjoined elements $\alpha_1, ..., \alpha_m$. Then the elements of GF(q) can all be written in the form $\sum_i c_i \alpha_i$, with $c_i \in Z_p$.

$$GF(q) = (Z_p)^m$$

Tr ↓

$$Z_p$$

The trace can be used to reduce elements of GF(q) to elements of Z_p:

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

Properties of trace:

1. $\text{tr } \alpha \in Z_p$
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 $a \in Z_p$)

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 Z_p, mod p arithmetic for prime p.

For any $q = p^m$, there exists a unique finite field GF(q) of size q. Such a field can be constructed by taking Z_p and adjoining the roots of irreducible polynomials.

GF(q) has characteristic p, meaning any element added p times gives 0.

Example:
$GF(9) = Z_3(\alpha)$,
$\alpha^2 + \alpha + 2 = 0$

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

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

Z_p Versus GF(p^m)

GF(q), $q=p^m$ can be viewed as a vector space over Z_p: pick m independent adjoined elements $\alpha_1, ..., \alpha_m$. Then the elements of GF(q) can all be written in the form $\sum_i c_i \alpha_i$, with $c_i \in Z_p$.

$$GF(q) = (Z_p)^m$$

Tr ↓

$$Z_p$$

The trace can be used to reduce elements of GF(q) to elements of Z_p:

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

Properties of trace:

1. $\text{tr } \alpha \in Z_p$
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 $a \in Z_p$)

"Standard" Pauli Group for $q=p^m$

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

$$\alpha, \beta \in GF(q)^n, \; c \in Z_p$$

$$X^\alpha \; | \gamma\rangle = \; | \gamma+\alpha\rangle$$
$$Z^\beta \; | \gamma\rangle = \omega^{tr\, \beta \cdot \gamma} \; | \gamma\rangle$$

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 GF(q), but the phase is still drawn from Z_p. Commutation can also be determined via tr:

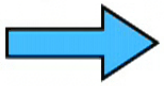
$$c(X^\alpha Z^\beta, X^{\alpha'} Z^{\beta'}) = tr\; \alpha' \cdot \beta - \alpha \cdot \beta'$$

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 $\{\alpha_1, \ldots, \alpha_m\}$ for GF(q) over Z_p, choose a dual basis $\{\beta_1, \ldots, \beta_m\}$ with the property $tr\,(\alpha_i\beta_j) = \delta_{ij}$.

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

$$X^\alpha = X^{a_1} \otimes X^{a_2} \otimes \ldots \otimes X^{a_m}$$
$$Z^\beta = Z^{b_1} \otimes Z^{b_2} \otimes \ldots \otimes Z^{b_m}$$



q-dim. qudit broken up into m p-dim qudits

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

n physical qudits
r stabilizer generators $M_1, \ldots, M_r$
$k = n - r/m$ logical qudits

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

Error syndrome still a Z_p vector

Error syndrome:

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

True GF(q) Stabilizer Codes

Note the example 5-qudit code has an extra symmetry. It is a true GF(q) stabilizer code. In the symplectic representation, it is GF(q)-linear, not just Z_p-linear:

1	0	0	-1	0	0	1	-1	0	0
α	0	0	-α	0	0	α	-α	0	0
0	1	0	0	-1	0	0	1	-1	0
0	α	0	0	-α	0	0	α	-α	0
-1	0	1	0	0	0	0	0	1	-1
-α	0	α	0	0	0	0	0	α	-α
0	-1	0	1	0	-1	0	0	0	1
0	-α	0	α	0	-α	0	0	0	α

However, since each generator can have an independent phase, so there is no clear meaning of the "multiplication by α" symmetry in the Pauli group $P_{n,q}$. It should mean "exponentiation by α" 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):

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

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

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

We can project an element of the lifted Pauli group back to the regular Pauli group by using tr on the phase:

$$\begin{array}{ccc} \dot{P}_{n,q} & & \omega^{\mu} X^{\alpha} Z^{\beta} \\ \downarrow \Pi & & \downarrow \Pi \\ P_{n,q} & & \omega^{tr\,\mu} X^{\alpha} Z^{\beta} \end{array}$$

$$\Pi(PQ) = (\Pi P)(\Pi Q)$$

$$c(\Pi P, \Pi Q) = tr\, c(P,Q)$$

Exponentiation (Odd q)

phase and existing exponents get multiplied by γ

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

new phase term giving phase accumulation from "reorganizing" X and Z powers

Note that this formula reduces to the correct one for $\gamma \in Z_p$. 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.

This formula can be derived by representing the lifted Pauli group as a matrix group over GF(q) and using $P^{\gamma} = \exp(\gamma \ln P)$.

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: $\dot{P}_{1,9}$

$P = \omega^0 X^1 Z^1$

$P^2 = \omega^1 X^2 Z^2$

$P^\alpha = \omega^{2+2\alpha} X^\alpha Z^\alpha$

$\vdots$

Π

$P_{1,9}$

$\omega^0 X^1 Z^1$

$\omega^2 X^2 Z^2$

$\omega^2 X^\alpha Z^\alpha$

$\vdots$

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

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

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.

$$S \Leftrightarrow \Pi S$$

Exponential eigenvalues: $|\psi\rangle$ is an exponential 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 ω^{a_i} for P^{γ_i}, then the exponential eigenvalue is ω^μ s.t. $tr(\gamma_i \mu) = a_i$ for all i.

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

Phases for Even q

For the qubit Pauli group, the phase is a power of i, a 4th root of unity, rather than of a pth 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 $\mathrm{tr}\ \alpha = \sum_{r=0}^{m-1} F^r(\alpha)$.
Then $\mathrm{tr}\ \alpha \in W_2(2) = Z_4$.

$W_2(q)$ is a Galois ring or a ring of truncated Witt vectors.

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:

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

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

Commutation of X and Z gives i^2

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

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

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

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 $\{\Pi P^{\gamma}\}$, but a set $\{\Pi P^{\gamma}\}$ corresponds to some lifted Pauli for any α_2, β_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)