CO639 Scribe Notes

Prepared by Jamie Batuwantudawe
Edited by Daniel Gottesman
Guest Lecturer: Martin Rötteler

February 26, 2004

Higher Dimensional Stabilizers
The Pauli group $\mathcal{P}_{n,p}$ has order

$$|\mathcal{P}_{n,p}| = p^{2n+1}$$

Moreover, each element $E \in \mathcal{P}_{n,p}$ can be written uniquely as

$$E = \omega_p^\gamma \cdot X_{\vec{\alpha}} \cdot Z_{\vec{\beta}}$$

where $\gamma \in GF(p)$ and $\vec{\alpha}, \vec{\beta} \in GF(p)^n$.
Furthermore, we have that $\mathcal{P}_{n,p}/scalars \simeq GF(p)^n \times GF(p)^n$ and this space is equipped with a symplectic inner product

$$(\alpha|\beta) * (\alpha'|\beta') = \sum_{i=1}^{n} \alpha_i' \cdot \beta_i - \alpha_i \cdot \beta_i'$$

and two Pauli operators commute *iff* $(\alpha|\beta) * (\alpha'|\beta') = 0$.

Stabilizer matrix: Given an abelian subgroup $\mathcal{S} \subseteq \mathcal{P}_{n,p}$, pick a minimum generating set having trivial intersection with the centre.
$\omega_p^{r_i} \cdot X_{\vec{\alpha}_i} \cdot Z_{\vec{\beta}_i}$, where $i = 1, ...k$. Stabilizer matrix is,

$$\left(\begin{array}{c|c} \alpha_1 & \beta_1 \\ \vdots & \vdots \\ \alpha_n & \beta_n \end{array} \right) = (X|Z) \;\; \in \;\; GF(p)^{k \times 2n}$$

Corresponds to a $[[n, n-k, d]]_p$ stabilizer code.
Here, $d = \min\{wt(v),\ v \in \mathcal{S}^* \backslash \mathcal{S}\}^p$, where $\mathcal{S}^*$ is the dual of $\mathcal{S}$ with respect to $*$

$$\mathcal{S}^* = \{v : \ \ c * v = 0 \ \ \forall c \in \mathcal{S}\}$$

We have the following in $\mathcal{C}_{1,p}$: DFT_p, P, M_γ (operate like 2×2 matrices on $(\alpha|\beta)$).

$$DFT := \frac{1}{\sqrt{p}} \sum_{x,z=0}^{p-1} \omega_p^{xz} |z\rangle\langle x|$$

$$M_\gamma := \sum_{y=0}^{p-1} |\gamma y\rangle\langle y|, \quad \gamma \in GF(p)$$

$$P := \sum_{y=0}^{p-1} \omega_p^{y(y-1)/2} |y\rangle\langle y|$$

We have the following also in $\mathcal{C}_{2,p}$: $ADD^{(1,2)}$ (4×4 matrix).

$$ADD := \sum_{x,y=0}^{p-1} |x\rangle|x+y\rangle\langle y|\langle x|$$

The following is a standard fact:

$$\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \gamma^{-1} & 0 \\ 0 & \gamma \end{pmatrix} \right\rangle = SL(2, GF(p))$$

$SL(2, GF(p))$ can map an $(\alpha|\beta) \to (\alpha'|\beta')$, provided both are not $(0,0)$.

$ADD^{(1,2)}$ operates on pairs of qubits like in binary, sending $X \otimes I \to X \otimes X$.

Theorem: $\mathcal{C}_{n,p} = \langle DFT_p, P, M_\gamma, ADD^{(i,j)}, \text{scalars, and Paulis} \rangle$

Start with an abelian $\mathcal{S} \subseteq \mathcal{P}_{n,p}$. Map to $\mathcal{S}_0 = \langle Z_1^{(1)}, Z_1^{(2)}, ...Z_1^{(k)} \rangle$.

- bad for EC since weight is 1
- but, eigenstates can be read off directly
- $|00..0\rangle|\phi\rangle_{in}$ is eigenstate of $\mathcal{S}_0$. Now, map back to $\mathcal{S}$.

Reed-Solomon

- pick polynomial of degree $\leq d$
- evaluate at all possible points

For $GF(p)$,

$$\begin{array}{c c}
 & \begin{array}{ccccc} 0 & 1 & 2 & \dots & (p-1) \end{array} \\
\begin{array}{c} 1 \\ x \\ x^2 \\ \vdots \\ x^d \end{array} & \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 2 & \dots & (p-1) \\ 0 & 1 & 4 & \dots & (p-1)^2 \\ \vdots & & & & \\ 0 & 1 & 2^d & \dots & (p-1)^d \end{pmatrix} = \mathcal{G}^{d,p}
\end{array}$$

This is the generator matrix for a RS code $[p, d+1, p-d]_p$. We know the distance since there are at most d zeros for this polynomial.

Singleton bound for $[n, k, d]_p$ is always $n+1 \geq k+d$. If equality, get MDS codes (maximum distance separable). For classical codes, this means that codewords can be seperated into message symbols and check symbols.
By throwing away col 1 and row 1, get $[p-1, d-1, p-d]$. Again, this is an MDS code.

We can make a QECC by CSS,

$$C_1 = [n, k_1, d_1], \;\; C_2 = [n, k_2, d_2] \;\; \text{with}\, C_2^\perp \subseteq C_1$$

$$(X|Z) = \begin{pmatrix} C_1^\perp & 0 \\ 0 & C_2^\perp \end{pmatrix} \Rightarrow [[n, k_1 + k_2 - n, \geq \min(d_1, d_2)]]$$

For $1 \leq d \leq \lfloor \frac{p-1}{2} \rfloor$, we get $C^{d,p}$ (code with generator $\mathcal{G}^{d,p}$) is self-orthogonal with respect to $x - y = \sum x_i \cdot y_i$.

$$C^{d,p} \subseteq (C^{d,p})^\perp$$

Using CSS construction, QECC is $[[p, p-2d-2, d+2]]_p$. This is a QMDS code. It saturates the Quantum Singleton Bound, $n + 2 \geq k + 2d$. This bound holds for all alphabet sizes.

- can shorten, $[[p-1, p-2d-1, d+1]]_p$
- using classical $GF(p^2)$, get QECC $[[p^2, p^2 - 2d - 2, d+2]]_p$
  ie. $[[9, 5, 3]]$