The geometry of stabiliser codes

Simeon Ball

Let $\{|x\rangle \mid x \in \mathbb{F}_p\}$ be a basis for $\mathbb{C}^p$.

Let η be a primitive p-th root of unity in $\mathbb{C}$.

For $a, b \in \mathbb{F}_p$, define linear maps $X(a)$ and $Z(b)$ as

$$X(a)\,|x\rangle = |x + a\rangle$$

and

$$Z(b)\,|x\rangle = \eta^{bx}\,|x\rangle$$

The "commuting" relation is

$$X(a)Z(b)X(a')Z(b') = \eta^{a'b-b'a}X(a')Z(b')X(a)Z(b)$$

The n qupit Hilbert space of local dimension p is $(\mathbb{C}^p)^{\otimes n}$

the elements of which are

$$\sum_{x \in \mathbb{F}_p^n} c_x \left|x_1 x_2 \cdots x_n\right\rangle$$

The norm of c_x is the probability of finding the quantum state in $\left|x_1 x_2 \cdots x_n\right\rangle$.

Example
The Bell state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

The linear maps on $(\mathbb{C}^p)^{\otimes n}$

$$\sigma_1 \otimes \cdots \otimes \sigma_n,$$

where the Pauli operator $\sigma_i = X(a_i)Z(b_i)$, form a basis for the linear maps on this space.

Let $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$. The "commuting" relation is

$$X(a)Z(b)X(a')Z(b') = \eta^{a\cdot b' - b\cdot a'} X(a')Z(b')X(a)Z(b)$$

The (multiplicative) subgroup

$$S = \{X(a)Z(b) \mid (a,b) \in C\}$$

is commutative iff $C \subseteq \mathbb{F}_p^{2n}$ is a totally isotropic subspace w.r.t the symplectic form.

Let

$$Q(S) = \{|\phi\rangle \in (\mathbb{C}^p)^{\otimes n} \mid M|\phi\rangle = |\phi\rangle, \forall M \in S\}$$

Lemma

$$\dim Q(S) = p^k \text{ iff } |S| = p^{n-k} \text{ iff } \dim C = n-k.$$

Lemma

For E and E' Pauli operators and orthogonal $|\phi\rangle, |\phi'\rangle \in Q(S)$,

$$E|\phi\rangle \text{ and } E'|\phi'\rangle \text{ are orthogonal}$$

unless $E^{\dagger}E' \in \mathit{Centraliser}(S) \setminus S$.

Observe from the "commuting" relation

$$\mathit{Centraliser}(S) = \{X(a)Z(b) \mid (a,b) \in C^{\perp}\}.$$

Aim: Find C for which $C^{\perp} \setminus C$ has only large symplectic weight vectors. ($\mathrm{swt}((a,b)) = |\{i \mid (a_i, b_i) \neq (0,0)\}|$)

$Q(S)$ is a $[[n,k,d]]_p$ quantum stabiliser code, where d is the minimum symplectic weight of $C^{\perp} \setminus C$.

Suppose the $(n-k) \times 2n$ matrix

$$G = (A \mid B)$$

is the generator matrix of a symplectic self-orthogonal code C.

The i-th and the $(i+n)$-th coordinate correspond to the i-th Pauli operator.

Let ℓ_i be the line spanned by the i-th and $(i+n)$-th column of G.

The set

$$\mathcal{X} = \{\ell_i \mid i = 1, \ldots, n\}$$

of n lines in $PG(n-k-1, p)$ is called a quantum set of lines.

For $k = 0$ we can take A be a symmetric $n \times n$ matrix with entries from $\mathbb{F}_p$ and B to be the identity.

Replacing the i-th and $(i + n)$-th column of G with another basis for ℓ_i gives an equivalent stabiliser code.

Thus, equivalent $[[n, 0, d]]_p$ stabiliser codes are given by different graphs with $\mathbb{F}_p$ weighted edges.

(Glynn et al.) An $[[n, k, d]]_2$ stabiliser code is equivalent to a set $\mathcal{X}$ of n lines in $PG(n-k-1, 2)$ in which every co-dimension 2 subspace is skew to an even number of the lines of $\mathcal{X}$.

1. This is assuming that $C^\perp$ has no codewords of weight one.

2. The minimum distance is the minimum d for which $x_1 + \cdots + x_d = 0$ where x_i are on distinct lines of $\mathcal{X}$ (and the remaining lines are not all contained in a hyperplane).

3. (Bierbrauer, Marcugini, Pambianco 2009) used this to prove that there is no $[[13, 5, 4]]_2$ stabiliser code.

4. The line $\ell_i \in \mathcal{X}$ is the span of the i-th and $(i+n)$-th column of a generator matrix for C.

Given a $n \times n$ symmetric matrix (a_{ij}) over $\mathbb{F}_p$, we define the (graphical) set of lines in $PG(n-1, p)$ as the set of lines ℓ_i, where ℓ_i is the span of e_i and $\sum_j a_{ij} e_j$.

(Ball-Puig 2021)

An $[[n, k, d]]_p$ stabiliser code is equivalent to a graphical set $\mathcal{X}$ of n lines in $PG(n-1, p)$ and a $(k-1)$-dimensional subspace U.

1. If pure then the minimum distance is the minimum d for which $x_1 + \cdots + x_d \in U$, x_i are on distinct lines of $\mathcal{X}$.

2. An $[[n, k, d]]_p$ stabiliser code is a $((n, p^k, d))_p$ quantum error-correcting code.

(Ball-Puig 2021) We can replace U by a set of points and get a $((n,(p-1)|U|+1,d))_p$ quantum error-correcting code.

1.The minimum distance is the minimum d for which $x_1+\cdots+x_d\in\langle u_1,u_2\rangle$, x_i are on distinct lines of $\mathcal{X}$ and $u_i\in U$.

2. The Rains-Hardin-Shor-Sloane $((5,6,2))_2$ code from 1997 has $\ell_i=\langle e_i,e_{i-1}+e_{i+1}\rangle$ in $PG(4,2)$ with $e_i+e_{i+1}+e_{i+3}$ being the points of U.

3. The Yo-Chen-Lai-Oh $((9,12,3))_2$ code from 2007 has $\ell_i=\langle e_i,e_{i-1}+e_{i+1}\rangle$ in $PG(8,2)$ with U being a code of 5 linearly independent points with vertex $e_1+e_4+e_7$.

4. This may allow us to determine if there is a $((9,12,4))_3$ code which is the direct sum of stabiliser codes.

(Ball-Moreno 2022) An $[[n, k, d]]_{2^h}$ stabiliser code is equivalent to a set $\mathcal{X}$ of n sets of h lines in $PG(h(n-k)-1, 2)$ in which every co-dim 2 subspace is skew to an even number of the lines of $\mathcal{X}$.

1. This is assuming that $C^{\perp}$ has no codewords of weight one.
2. d is the minimum for which $x_1 + \cdots + x_d = 0$ where $x_i \in \pi_i$ and π_i is space spanned by i-th element of $\mathcal{X}$.
3. This should allow us to classify all $[[8, 0, 5]]_4$ stabiliser codes.