

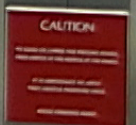
Title: IQC - Quantum Error Correction - Lecture 2

Date: Jan 11, 2018 02:00 PM

URL: <http://pirsa.org/18010048>

Abstract:

TA: John Schanck <jschanck@uwaterloo.ca>



$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Def.: The Pauli group $\mathcal{P}_n$ is the group consisting of tensor products of I, X, Y , and Z on n qubits, with overall phase $\pm 1, \pm i$.

Properties:

$$1) |\mathcal{P}_n| = 4^{n+1}$$

2) $P \in \mathcal{P}_n \Rightarrow P$ has eigenvalues ± 1 or $\pm i$.

3) $P, Q \in \mathcal{P}_n \Rightarrow$ either $PQ = QP$ or $PQ = -QP$
 $[P, Q] = 0$ or $\{P, Q\} = 0$

$$4) P \in \mathcal{P}_n \Rightarrow P^2 = \pm I$$

$$|0\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

$$|0\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

$z \otimes z$

$z \otimes z$

$z \otimes z$

$z \otimes z$

$z \otimes z$

$z \otimes z$

$$|0\rangle = (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle = (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

$$z \otimes z$$

$$z \otimes z$$

$$z \otimes z$$

$$z \otimes z$$

$$z \otimes z$$

$$z \otimes z$$

$$x \otimes x \otimes x \otimes x \otimes x$$

$$x \otimes x \otimes x \otimes x \otimes x$$

Def. Given code Q , let the stabilizer of Q be

$$S(Q) = \{P \in P_n \mid P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in Q\}$$

Properties of stabilizers:

1) $-I \in S(Q)$

2) $S(Q)$ is a group

3) $S(Q)$ is Abelian

$$M, N \in S(Q)$$

$$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \Rightarrow MN \in S(Q)$$

$$\rightarrow M, N \in S(Q)$$

$$(MN - NM)|\psi\rangle = 0$$

Def. Given code Q , let the stabilizer of Q be

$$S(Q) = \{P \in P_n \mid P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in Q\}$$

Properties of stabilizers:

1) $I \in S(Q)$

2) $S(Q)$ is a group

3) $S(Q)$ is Abelian

$$M, N \in S(Q)$$

$$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \Rightarrow MN \in S(Q)$$

$$\rightarrow M, N \in S(Q)$$

$$(MN - NM)|\psi\rangle = 0$$

$$M, N \in P_n \Rightarrow (M, N) = 0 \text{ or } \{M, N\} = 0$$

$$\Downarrow \\ (M, N) = 0$$

$$\downarrow \\ \cancel{MN - NM = 2MN}$$

Def: Given code Q , let the stabilizer of Q be

$$S(Q) = \{P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \quad \forall |\psi\rangle \in Q\}$$

Properties of stabilizers:

1) $-I \in S(Q)$

2) $S(Q)$ is a group

3) $S(Q)$ is Abelian

$$M, N \in S(Q)$$

$$MN|\psi\rangle = M|\psi\rangle = |\psi\rangle \Rightarrow MN \in S(Q)$$

$$\rightarrow M, N \in S(Q)$$

$$(MN - NM)|\psi\rangle = 0$$

$$M, N \in \mathcal{P}_n \Rightarrow (M, N) = 0 \text{ or } \{M, N\} = 0$$

$$\Downarrow$$

$$(M, N) = 0$$

$$\cancel{MN - NM = 2MN}$$

r generators $M_1, \dots, M_r; M_i^2 = I$

$$M_1^{a_1} M_2^{a_2} \dots M_r^{a_r}$$

$$a_i, a_r \in \{0, 1\}$$

$$|S(Q)| = 2^r$$

Let S be an Abelian group, $S \subseteq P_n$, with $-I \notin S$.

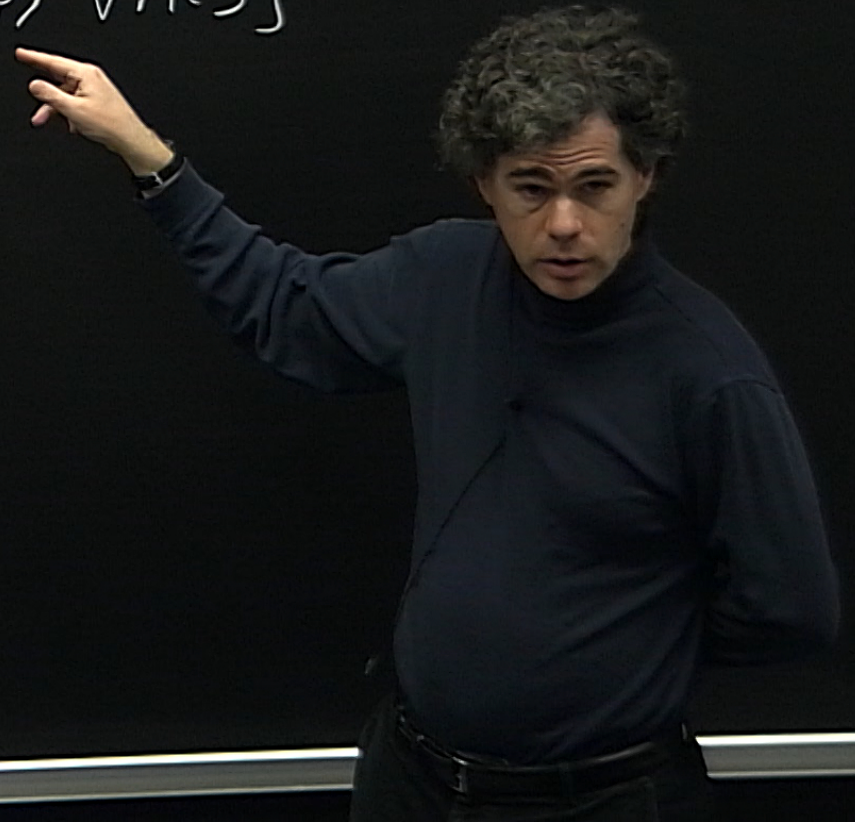
Then

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

$T(S)$ is codespace of S .

$$S = S(T(S))$$

$$T(S(Q))$$



Let S be an Abelian group, $S \subseteq P_n$, with $-I \notin S$.

Then

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

$T(S)$ is codespace of S .

$$S = S(T(S))$$

If $Q = T(S(Q))$, then Q is a stabilizer code.

Let S be an Abelian group, $S \subseteq P_n$, with $-I \notin S$.

Then

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

$T(S)$ is codespace of S .

$$S = S(T(S))$$

If $Q = T(S(Q))$, then Q is a stabilizer code.

E.g. non-stabilizer code $|\bar{0}\rangle = |00\rangle$
 $|\bar{1}\rangle = |01\rangle + |10\rangle$

Thm.: The dimension of $T(s)$ is 2^k , where $k=n-r$, r generators for S

Proof: Projector onto codespace

$$(|S|=2^r) \quad \Pi_S = \frac{1}{2^r} \sum_{M \in S} M$$

$$|\psi\rangle \in T(s) \Rightarrow \Pi_S |\psi\rangle = \frac{1}{2^r} \sum_{M \in S} M |\psi\rangle = |\psi\rangle \quad \checkmark$$

$$\sum_{N \in S} N(\Pi_S |\psi\rangle) = \frac{1}{2^r} \sum_{M \in S} \sum_{N \in S} NM |\psi\rangle = \frac{1}{2} \sum_{\tilde{M} \in S} \tilde{M} |\psi\rangle = \Pi_S |\psi\rangle \Rightarrow \Pi_S |\psi\rangle \in T(s)$$

$$\dim T(s) = \text{tr } \Pi_S = \frac{1}{2^r} \sum_{M \in S} \text{tr } M = \frac{\text{tr } I}{2^r} = \frac{2^n}{2^r} = 2^{n-r}$$

Suppose error E st. $\{E, M\} = 0$ for some $M \in S$.

$$|\psi\rangle \in T(S) \Rightarrow M(E|\psi\rangle) = -EM|\psi\rangle = -(E|\psi\rangle) \quad E|\psi\rangle \text{ is a } -1 \text{ eigenvector of } M.$$

If $[E, M] = 0$

$$M(E|\psi\rangle) = EM|\psi\rangle = E|\psi\rangle \Rightarrow E|\psi\rangle \text{ is a } +1 \text{ eigenvector}$$

M detects errors that anticommute with it.

$$\text{Let } N(S) = \{N \in \mathcal{P}_n \mid [M, N] = 0 \ \forall M \in S\}$$

Set of undetectable errors: $N(S) \setminus S$

Note that $S \subseteq N(S)$

$$\text{Let } N(S) = \{N \in \mathcal{P}_n \mid [M, N] = 0 \ \forall M \in S\}$$

Set of undetectable errors: $N(S) \setminus S$

Note that $S \subseteq N(S)$

Correct errors

E & F have ~~different~~^{same} error syndromes $\Rightarrow E$ & F commute w/ same elements of S

$$\Rightarrow [E^+ F, M] = 0 \ \forall M \in S$$

$$\Rightarrow E^+ F \in N(S)$$

Thm: S can correct a set CSP_n iff $E^+ F \notin N(S) \setminus S \quad \forall E, F \in C$

Cor: The distance of S is minimum weight of $N(S) \setminus S$. The code is degenerate if this is 0 .

Thm: S can correct a set $C \subseteq \mathcal{P}_n$ iff $E^\dagger F \notin N(S) \setminus S \quad \forall E, F \in C$.

Cor: The distance of S is minimum weight of $N(S) \setminus S$. The code is degenerate if S contains an element of lower weight.

Def: For a stabilizer code, if we have n physical qubits, k logical qubits and distance d , it is a $[[n, k, d]]$ code.

Example: 5-qubit code

X Z Z X I

I X Z Z X

X I X Z Z

Z X I X Z

$[[5, 1, 3]]$

Example: 5-qubit code

X Z Z X I

I X Z Z X

X I X Z Z

Z X I X Z

$[[5, 1, 3]]$

$5 \times 3 + 1 = 16$ possible errors

Example: 5-qubit code

$X \ Z \ Z \ X \ I$

$I \ X \ Z \ Z \ X$

$X \ I \ X \ Z \ Z$

$Z \ X \ I \ X \ Z$

$[[5, 1, 3]]$

$5 \times 3 + 1 = 16$ possible errors

$$N, N' \in N(S)$$

$$N' = NM, \quad M \in S$$

$$N'|\psi\rangle = NM|\psi\rangle = N|\psi\rangle \quad \text{if } |\psi\rangle \in T(S)$$

Look at $N(S)/S$

$$N(S)/S \cong \mathcal{P}_k$$

Example: 5-qubit code

$$X \otimes Z \otimes Z \otimes X \otimes I$$

$$I \otimes X \otimes Z \otimes Z \otimes X$$

$$X \otimes I \otimes X \otimes Z \otimes Z$$

$$Z \otimes X \otimes I \otimes X \otimes Z$$

$$[[5, 1, 3]]$$

$5 \times 3 + 1 = 16$ possible errors

$$\bar{X} = X \otimes X \otimes X \otimes X \otimes X$$

$$\bar{Z} = Z \otimes Z \otimes Z \otimes Z \otimes Z$$

$$N, N' \in N(S)$$

$$N' = NM, m \in S$$

$$N'|\psi\rangle = NM|\psi\rangle = N|\psi\rangle \quad \text{if } |\psi\rangle \in T(S)$$

Look at $N(S)/S$

$$|N(S)/S| \cong P_k \quad \text{logical Pauli group}$$

Linear codes

Def: A classical code C is a set of bit strings. C is a linear code if $x, y \in C \Rightarrow x + y \in C$.

Define via generator matrix, $k \times n$ ^{# logical bits} ^{# physical bits} binary matrix. Each row is a basis codeword.

General codeword - given logical v , encoded as $G^T v$.

E.g. Hamming code

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Def: The Hamming distance between two bit strings is the # of places where they differ. The distance of linear code C is the minimum Hamming distance between any pair of codewords. Linear code $[n, k, d]$

Def: The Hamming distance between two bit strings is the # of places where they differ. The distance of ~~linear~~ code C is the minimum Hamming distance between any pair of codewords. Linear code $[n, k, d]$
General code (n, K, d)

$$\text{Hamming distance} = \text{wt}(x, y)$$

$\Rightarrow$ Linear code: distance = lowest wt nontrivial codeword.

Thm: S can correct a set $C \subseteq \mathcal{P}_n$ iff $E^T F \notin N(S) \forall E, F \in C$

Def: For a linear code, the parity check matrix H is a matrix of maximal rank st. $HG^T = 0$

$$H(G^T v) = 0$$

maximal rank st. $HG^T = 0$

$$H(G^T v) = 0$$

Error e , codeword $x \mapsto x + e$

$$H(x + e) = Hx + He = He \quad \text{error syndrome}$$

Hamming code $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

single-bit errors have syndromes which are i th column of H

Def: For a linear code, the parity check matrix H is a matrix of maximal rank st. $HG^T = 0$

$$H(G^T v) = 0$$

Error e , codeword $x \mapsto x+e$

$$H(x+e) = Hx + He = He \quad \text{error syndrome}$$

Hamming code $H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$

$$\rightarrow \begin{matrix} z & z & z & z & I & I & I \\ z & z & I & I & z & z & I \\ z & I & z & I & z & I & z \end{matrix}$$

single-bit errors have syndromes which are i th column of H

$[7, 4, 3]$ code

CSS code (Calderbank-Shor-Stearns)

Two Classical linear codes C_1 & C_2

C_1 has parity check $H_1 \rightarrow$ convert $1 \rightarrow Z$
 C_2 " " " $H_2 \rightarrow$ convert $1 \rightarrow X$

E.g. $C_1 = C_2$ Hamming code

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



CSS code (Calderbank-Shor-Stearns)

Two Classical linear codes C_1 & C_2

C_1 has parity check $H_1 \rightarrow$ convert $1 \rightarrow Z$
 C_2 " " " $H_2 \rightarrow$ convert $1 \rightarrow X$

Eg: $C_1 = C_2$ Hamming code

$[[7, 1, 3]]$

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

$$\begin{matrix} X & X & X & I & X & X & I \\ X & X & I & I & X & X & I \\ X & I & X & I & X & I & X \end{matrix}$$

Row v of H_1 , row w of H_2 $\Rightarrow v \cdot w$ is parity of places where both are 1.

Corresponding $P_v, P_w \in \mathcal{P}_n$ commute $\Leftrightarrow v \cdot w = 0$

Def: C linear code. $C^\perp$ is the dual code defined as $\{x \mid x \cdot z = 0 \forall z \in C\}$

Parity check matrix of C is generator matrix for $C^\perp$, $(C^\perp)^\perp = C$

C_1 & C_2 compatible if:

$$x \in C_1^\perp, z \in C_2^\perp \Rightarrow x \cdot z = 0$$

$$x \in (C_2^\perp)^\perp = C_2 \Rightarrow C_1^\perp \subseteq C_2$$

$$C_2^\perp \subseteq C_1$$

$$\begin{matrix} I & I & I \\ z & z & I \\ z & I & z \end{matrix}$$

CAUTION

Row v of H_1 , row w of H_2 , $v \cdot w$ is parity of places where both are 1.

Corresponding $P_v, P_w \in \mathcal{P}_n$ commute $\Leftrightarrow v \cdot w = 0$

Def: C linear code. $C^\perp$ is the dual code defined as $\{x \mid x \cdot z = 0 \forall z \in C\}$
 Parity check matrix of C is generator matrix for $C^\perp$, $(C^\perp)^\perp = C$

C_1 & C_2 compatible if:

$$x \in C_1^\perp, z \in C_2^\perp \Rightarrow x \cdot z = 0$$

$$x \in (C_2^\perp)^\perp = C_2 \Rightarrow C_1^\perp \subseteq C_2$$

$$C_2^\perp \subseteq C_1$$

TA: John Schanck <jschanck@uwaterloo.ca>

Thm: Let $C_1^\perp \subseteq C_2$, C_1, C_2 linear codes. C_1 is $[n, k_1, d_1]$, C_2 is $[n, k_2, d_2]$.
Then $\exists$ quantum code (CSS code) which is $[[n, k_1 + k_2 - n, d]]$, with
 $d \geq \min(d_1, d_2)$

TA: John Schanck <jschanck@uwaterloo.ca>

Thm: Let $C_1^\perp \subseteq C_2$, C_1, C_2 linear codes C_1 is $[n, k_1, d_1]$, C_2 is $[n, k_2, d_2]$.
Then $\exists$ quantum code (CSS code) which is $[[n, \underbrace{k_1 + k_2 - n}_k, d]]$, with
 $d \geq \min(d_1, d_2)$

$$k = n - \# \text{generators}$$

$$= n - (n - k_1) - (n - k_2) = k_1 + k_2 - n$$

$$\Pi_S = \sum_{M \in S} M = \left(\sum_{M \in S_x} M \right) \left(\sum_{N \in S_z} N \right)$$

add vectors in $C_2^\perp$

→ use only codewords of C_1

$$\Rightarrow |\bar{z}\rangle = \sum_{x \in C_2^\perp} |z+x\rangle, \quad z \in C_1$$

labelled by an element of $C_1/C_2^\perp$ sum over coset of $C_2^\perp$ in C_1

Ignore phase of generators of S

$$\begin{array}{l} \text{I} \\ \text{X} \\ \text{Y} \\ \text{Z} \end{array} \begin{array}{l} (0|0) \\ (1|0) \\ (1|1) \\ (0|1) \end{array} \quad \text{XZ ZX I} \rightarrow (10010 | 01100)$$

Commutation:

$$P \leftrightarrow (a|b), \quad Q \leftrightarrow (c|d)$$

$$(P, Q) = 0 \Leftrightarrow a \cdot d + b \cdot c = 0$$

symplectic inner product

Ignore phase of generators of S

$$\begin{array}{l} \text{I} \\ \text{X} \\ \text{Y} \\ \text{Z} \end{array} \begin{array}{l} (0|0) \\ (1|0) \\ (1|1) \\ (0|1) \end{array} \quad X Z Z X I \rightarrow (10010 | 01100)$$

Commutation:

$$P \leftrightarrow (a|b), \quad Q \leftrightarrow (c|d)$$

$$(P, Q) = 0 \Leftrightarrow a \cdot d + b \cdot c = 0$$

symplectic inner product

$$\text{CSS code: } \left(\begin{array}{c} | \end{array} \right)$$

Ignore phase of generators of S

$$\begin{array}{l} \text{I} \\ \text{X} \\ \text{Y} \\ \text{Z} \end{array} \begin{array}{l} (0|0) \\ (1|0) \\ (1|1) \\ (0|1) \end{array} \quad \text{XZ ZX I} \rightarrow (10010 | 01100)$$

Commutation:

$$P \leftrightarrow (a|b), \quad Q \leftrightarrow (c|d)$$

$$(P, Q) = 0 \Leftrightarrow a \cdot d + b \cdot c = 0$$

symplectic inner product

$$\text{CSS code: } \left(\begin{array}{c|c} 0 & H_1 \\ \hline H_2 & 0 \end{array} \right)$$

Ignore phase of generators of S

$$\begin{array}{l} \text{I} \\ \text{X} \\ \text{Y} \\ \text{Z} \end{array} \begin{array}{l} (0|0) \\ (1|0) \\ (1|1) \\ (0|1) \end{array} \quad X Z Z X I \rightarrow (10010 | 01100)$$

Commutation:

$$P \leftrightarrow (a|b), \quad Q \leftrightarrow (c|d)$$

$$(P, Q) = 0 \Leftrightarrow a \cdot d + b \cdot c = 0$$

symplectic inner product

$$\text{CSS code: } \left(\begin{array}{c|c} 0 & H_1 \\ H_2 & 0 \end{array} \right)$$

$$\begin{array}{c|c} P & Q \\ \hline \{ & \{ \\ v & + \\ w \end{array}$$

Codes over $GF(4)$

Field has addition & multiplication

$0, 1, \omega, \omega^2$

Characteristic 2 $x+x=0$

$1+\omega=\omega^2, \omega^3=1$

$$0 \leftrightarrow I$$

$$1 \leftrightarrow X$$

$$\omega^2 \leftrightarrow Y$$

$$\omega \leftrightarrow Z$$

$$X Z Z X I \leftrightarrow (1 \omega \omega 1 0)$$

Codes over $GF(4)$

Field has addition & multiplication

$0, 1, \omega, \omega^2$

Characteristic? $x+x=0$

$$1 + \omega = \omega^2, \quad \omega^3 = 1$$

$$0 \leftrightarrow I$$

$$1 \leftrightarrow X$$

$$\omega^2 \leftrightarrow Y$$

$$\omega \leftrightarrow Z$$

$$X Z Z X I \leftrightarrow (1 \omega \omega 1 0)$$

$$P.Q \leftrightarrow v+u$$

Codes over $GF(4)$

Field has addition & multiplication

$0, 1, \omega, \omega^2$

Characteristic 2 $x+x=0$

$$1 + \omega = \omega^2, \omega^3 = 1$$

$\overline{0} = 0$	$\text{tr } 0 = 0$
$\overline{1} = 1$	$\text{tr } 1 = 0$
$\overline{\omega} = \omega^2$	$\text{tr } \omega = 1$
$\overline{\omega^2} = \omega$	$\text{tr } \omega^2 = 1$

$$0 \leftrightarrow I$$

$$1 \leftrightarrow X$$

$$\omega^2 \leftrightarrow Y$$

$$\omega \leftrightarrow Z$$

$$X Z Z X I \leftrightarrow (1 \omega \omega 1 0)$$

$$P \cdot Q \leftrightarrow v + w$$

$$(P, Q) = 0 \Leftrightarrow \text{tr}(\overline{v} \cdot w) = 0$$

Linear code over $\text{GF}(4)$

$$x, y \in C, \alpha \in \text{GF}(4)$$

$$\Rightarrow x + \alpha y \in C$$

Additive $\text{GF}(4)$ code

$$x, y \in C \Rightarrow x + y \in C$$

Linear code over $GF(4)$

$$x, y \in C, \alpha \in GF(4)$$

$$\Rightarrow x + \alpha y \in C$$

Additive $GF(4)$ code

$$x, y \in C \Rightarrow x + y \in C$$

5-qubit code

Linear $GF(4)$ code

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & \omega & \omega^2 & \omega^2 \end{pmatrix} \quad (\text{parity check})$$



I	X	X	X	X
I	Z	Z	Z	Z
X	I	X	Z	Y
Z	I	Z	Y	X