QIC 890 / CO 781 / CS 867, W22

Lec 3-4: Stabilizer codes

- Classical linear codes

eg 1: 3 bit repetition code (adjacent bits are identical)

	after error on	1st bit	2nd bit	3rd bit
Encode 0 as 0 0 0		1 0 0	0 1 0	0 0 1
1 as 1 1 1		0 1 1	1 0 1	1 1 0
Parity of bits 1&2: $b_1 \oplus b_2$	0	1	1	0
------ 2&3: $b_2 \oplus b_3$	0	0	1	1

If at most 1 error occurs, the 2 parity bits uniquely identify the error which can be reverted.

More succinctly: $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$ ($\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}$: the output of the channel)

H: parity check matrix for 3-bit code.

$\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$: 2-bit syndrome, $s_1 = b_1 \oplus b_2$, $s_2 = b_2 \oplus b_3$

NB: $G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ is called the generater matrix for the code.

Codewords are $G[x]$ for all possible $[x]$ ($[0]$ or $[1]$).
$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

($G[x]$: length-1 binary vector, since only encode 1 bit x)

NB: $HG = 0$.

NB: Let $e \in \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ be the error vectors corresponding to the 4 correctable errors.

$$H(G[x] + e) = He = \begin{bmatrix} s_1(e) \\ s_2(e) \end{bmatrix}.$$

eg 2: 7 bit Hamming code

Let $H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$ (i-th column = binary rep of i)

Ex: check that $G = \left[\begin{array}{c|c} H^T & \begin{matrix} 1 \\ 1 \\ 1 \\ 1 \end{matrix} \end{array}\right]$. Codewords are $G \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$. (encodes 4 bits into 7)

Let c be a codeword, $e \in \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\}$.

error on 0 bit = no error, error on 1st bit, ... error on 7th bit.

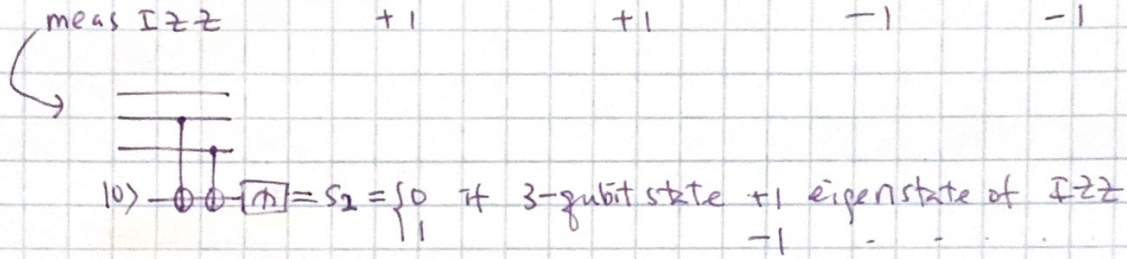
$H(c+e) = He = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix}$ (binary rep of i if e = error on ith bit).

so this code corrects up to 1 bit flip error.

- Quantum generalization:

eg 1: 3-qubit rep code for X-error:

	no error	error XII	error IXI	error IIX
$\alpha\|0\rangle + \beta\|1\rangle \longrightarrow$	$\alpha\|000\rangle + \beta\|111\rangle$	$\alpha\|100\rangle + \beta\|011\rangle$	$\alpha\|010\rangle + \beta\|101\rangle$	$\alpha\|001\rangle + \beta\|110\rangle$
meas ZZI	+1	−1	−1	+1
meas IZZ	+1	+1	−1	−1



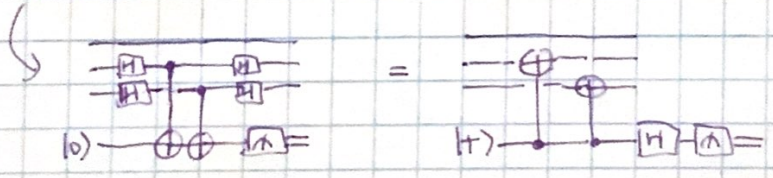
$ZZ = \begin{bmatrix} 1 & 0 & & \\ 0 & -1 & & \\ & & -1 & \\ & & 0 & 1 \end{bmatrix}$, $+1$ eigenspace spanned by $\{|00\rangle, |11\rangle\}$ $\{|01\rangle, |10\rangle\}$, -1

The meas of ZZI, IZZ are <u>compatible</u> and preserve the superposition.

$[ZZI, IZZ] = 0$

eg 2: 3-qubit rep code for Z-error

	no error	error ZII	error IZI	error IIZ
$\alpha\|0\rangle + \beta\|1\rangle \longrightarrow$	$\alpha\|+++\rangle + \beta\|---\rangle$	$\alpha\|-++\rangle + \beta\|+--\rangle$	$\alpha\|+-+\rangle + \beta\|-+-\rangle$	$\alpha\|++-\rangle + \beta\|--+\rangle$
meas XXI	+	−	−	+
meas IXX	+	+	−	−



eg 3: 9-qubit Shor code:

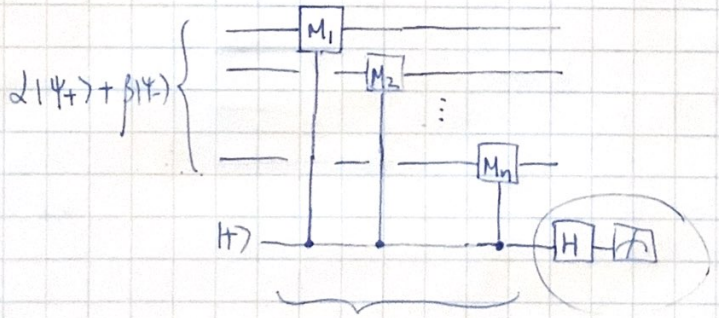
$$\begin{matrix}\alpha|0\rangle \\ +\beta|1\rangle\end{matrix} \longrightarrow \begin{matrix}\alpha\,(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)\otimes(|000\rangle+|111\rangle)/\sqrt{8} \\ +\beta\,(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)\otimes(|000\rangle-|111\rangle)/\sqrt{8}\end{matrix}$$

Meas:

ZZI	⊗	III	⊗	III	corrto	S_{11}
IZZ	⊗	III	⊗	III	,	S_{12}
III	⊗	ZZI	⊗	III	;	S_{21}
III	⊗	IZZ	⊗	III	,	S_{22}
III	⊗	III	⊗	ZZI	,	S_{31}
III	⊗	III	⊗	IZZ		S_{32}
XXX	⊗	XXX	⊗	III		t_1
III	⊗	XXX	⊗	XXX	.	t_2
					+	0
					−	1

NB: Measuring eigenvalues of Pauli operators is a quantum analogue of parity check

General circuit for measuring $M_1 \otimes M_2 \otimes \cdots \otimes M_n$
where $M_i \in \{I, X, Y, Z\}$



$$(\alpha|\psi_+\rangle+\beta|\psi_-\rangle)|+\rangle \longrightarrow \alpha|\psi_+\rangle|+\rangle + \beta\left[|\psi_-\rangle\frac{|0\rangle}{\sqrt{2}} - |\psi_-\rangle\frac{|1\rangle}{\sqrt{2}}\right]$$

$$= \alpha|\psi_+\rangle|+\rangle + \beta|\psi_-\rangle|-\rangle$$

$H\,H\,(\cdot) =$ picks out one of these. wip $|\alpha|^2$, $|\beta|^2$ resp.

The Pauli group

Recall $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

Def: The Pauli group on n-qubits $\mathcal{P}_n$ is the group generated multiplicatively by X & Z on each qubit.

Fact: $\mathcal{P}_n$ contains tensor products of I, X, Y, Z on n qubits with overall phase $\pm 1, \pm i$

Def: $\hat{\mathcal{P}}_n = \mathcal{P}_n / \{I, iI, -I, -iI\}$

Facts:

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

② If $P \in \hat{\mathcal{P}}_n$, then $P^2 = I$ (so eigenvalues of $P = \pm 1$).
If $P \neq I$, then $\mathrm{Tr} P = 0$ (so exactly half of the eigenvalues are -1)

eg. $ZZ = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

③ $P, Q \in \mathcal{P}_n$, P, Q either commute or anticommute
$[P, Q] = 0$ $\{P, Q\} = 0$.

To see this; note that any two of I, X, Y, Z either commute or anticommute.

Let $P = M_1 \otimes M_2 \otimes \cdots \otimes M_n$, $M_i \in \{I, X, Y, Z\}$
$Q = N_1 \otimes N_2 \otimes \cdots \otimes N_n$, $N_i \in \{I, X, Y, Z\}$

Then P, Q commute if an even number of M_i, N_i anticommute
... anticom ... odd ... anticom.

eg. XX, ZZ commute, XY, ZZ commute, XY, XZ anticom.

Def: $c: \mathcal{P}_n \otimes \mathcal{P}_n \to \mathbb{Z}_2$

$$c(P, Q) = \begin{cases} 0 & \text{if } [P, Q] = 0 \\ 1 & \text{if } \{P, Q\} = 0 \end{cases}$$

Binary symplectic representation of $\hat{P}_n$:

We can represent each qubit-Pauli by 2 bits:

I	$\leftrightarrow$	0 0
X	$\leftrightarrow$	1 0
Y	$\leftrightarrow$	1 1
Z	$\leftrightarrow$	0 1
↑		↑ ↖
Pauli		x-bit z-bit

We can represent each $P \in \hat{P}_n$ by $2n$ bits: $v_P = (x_P | z_P)$
where the ith bit of x_P = x-bit of i-th tensor component of P
z_P = z-bit - - .

eg. $ZZ \leftrightarrow (00|11)$
$XY \leftrightarrow (11|01)$

$XIYZ \leftrightarrow (\underbrace{1010}_{\text{x-part}} | \underbrace{0011}_{\text{z-part}})$ of $XIYZ$

Def: symplectic inner product between $v_P = (x_P | z_P)$ and $v_Q = (x_Q | z_Q)$ is defined as $v_P \odot v_Q = x_P \cdot z_Q + z_P \cdot x_Q \mod 2$

↑ inner product on n-bit string mod 2.

Facts:
- $v_{PQ} = v_P + v_Q \mod 2$ (multiplicative of Paulis $\leftrightarrow$ addition of vector)
- $c(P,Q) = v_P \odot v_Q$
- $Q_1, Q_2, \ldots, Q_t$ multiplicatively independent $\Leftrightarrow$ $v_{Q_1}, v_{Q_2}, \ldots, v_{Q_t}$ lin. indep. (over $\mathbb{Z}_2$)
- Subgroup of Paulis in $\hat{P}_n$ $\Leftrightarrow$ subspace of vector in $(\mathbb{Z}_2)^{\otimes 2n}$

Generator of subgroup $\Leftrightarrow$ basis of the subspace

↑ Multiplicative

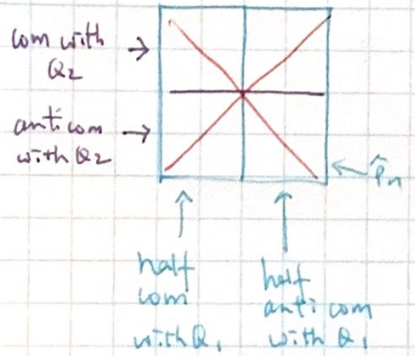
Linear algebra Lemma:

eg How many 2 qubit Paulis in $\hat{P}_2$ commute with XX?
II, IX, XI, ZZ, YY, YZ, ZY, XX

How many 2 qubit Paulis in $\hat{P}_2$ commute with XX and anticom with ZI?
XI, YY, YZ, XX

Take a Pauli indep of XX & ZI. say YY.
How many of the above also com or anticom with YY?
com: YY, XX
anticom: YZ, XI

- Consider $\hat{P}_n$. ① Pick $Q_1 \in \hat{P}_n$, $Q_1 \neq I$.



② Pick $Q_2 \in \hat{P}_n$, Q_1, Q_2 indep.
Half of the set com with Q_1 also com with Q_2
anticom with Q_2
anticom com ....
com anticom ....

③ $Q_3 \in \hat{P}_n$, Q_1, Q_2, Q_3 independent ....

⋮

Lemma= Let $\{Q_1, Q_2, \ldots, Q_m\} \subseteq \hat{P}_n$ be independent
Let $s_1, s_2, \ldots, s_m$ be m arbitrary bits.

Then there are 2^{2n-m} Paulis $P \in \hat{P}_n$ s.t. $\forall i$, $c(P, Q_i) = s_i$.

Pf: Let v_{Q_i} be symplectic rep of Q_i.

We want 2n-bit string w s.t. $\forall i$: $w \odot v_{Q_i} = s_i$ [linear eq on w over $\mathbb{F}_2$]

∵ v_{Q_i}'s linearly indep, solution space 2n−m dim (↑ binary)

∴ 2^{2n-m} such w's.

Abelian subgroups of $\hat{P}_n$:

eg $\{II, IZ, ZI, ZZ\}$ generated multiplicatively by ZI, IZ

eg. $\{II, XX, ZZ, YY\}$ generated by XX, ZZ.

Cor of Lin alg Lemma: Abelian subgroups of $\hat{P}_n$ have at most 2^n elements.

Pf: Let such a subgroup S be generated by an independent set $\{Q_1 \ldots Q_m\}$

The # of Pauli's commuting with all elmts in $S = 2^{2n-m}$

But all elements of S qualify, $|S| = 2^m$.

$\therefore \quad 2^m \leq 2^{2n-m} \quad \Rightarrow \quad m \leq n.$

Def: abelian subgroups of $\hat{P}_n$ with 2^n elmts are called "maximal".