QIC 890 / CO781-486 / CS 867, W24

Lec 2: Stabilizer codes

- Classical binary linear codes (arithmetic mod 2)
  - linear: codewords form a linear space over $\mathbb{Z}_2$

eg 1: 3-bit repetition code

① Encode 0 as 000
1 111

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

Logical space: length-1 binary vector $[x]$ for $x = 0, 1$

Codewords are $G[x] = \begin{bmatrix} x \\ x \\ x \end{bmatrix}$. (linear code!).

② Without error, adjacent bits are identical

If at most 1 bit is flipped, checking parities of consecutive pairs of bit sufficient to locate the flip.

	b_1 b_2 b_3		$s_1 = b_1 \oplus b_2$	$s_2 = b_2 \oplus b_3$	
no error	0 0 0	or 1 1 1	0	0	identifies the error
1st bit flipped	1 0 0	0 1 1	1	0	
2nd – –	0 1 0	1 0 1	1	1	
3rd – –	0 0 1	1 1 0	0	1	

$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ is called the parity check matrix.

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$$

Parity check matrix · channel output · syndrome.

NB $HG = 0$

NB $e \in \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$ errors

$H(\underbrace{G[x] + e}_{\text{erroneous output}}) = He$ = ith column of H if ith bit is flipped

Q2: 7-bit Hamming code.

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

$H^T H = 0$ (H is self dual)

Each row has 4 1's (H is doubly even)

H is the parity check matrix of a 7-bit code (width 7) encoding 4 bits (3 rows → 3 checks).

Generator matrix $G = \begin{bmatrix} H^T \\ \vdots \end{bmatrix}$ (Ex: check $HG = 0$)

The 16 codewords are $G \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$.

For $e \in \left\{ \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \dots, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right\}$, $c \in$ code,

- e = no error
- e = bit flip on 1st bit
- e = bit flip on 7th bit

$H(c+e) = He = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \end{bmatrix}$ which is the bin rep of i if the ith bit is flipped, i.e. corrects 1 error.

- $H(c+e)$: erroneous output
- He: independent of c!!
- $\because HG = 0$

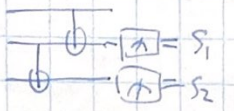
This is useful for Quantum!!

- Quantum generalization of binary linear codes

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

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

- The decoding circuit from lec 1:



where $s_1 \sim b_1 \oplus b_2$ If the state is $|b_1\rangle|b_2\rangle|b_3\rangle$
$s_2 \sim b_2 \oplus b_3$

- We now see that "parities" generalize to eigenvalues of Pauli o.p.s.

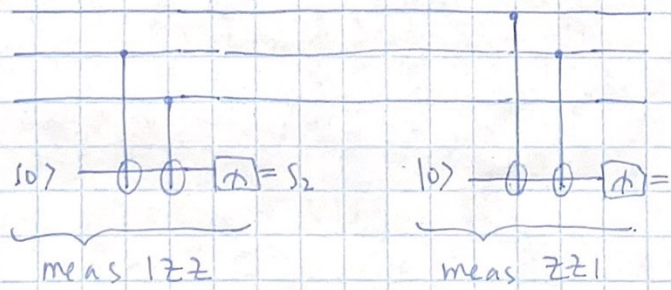
$$ZZ = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}, \quad \begin{matrix} +1 \text{ eigenspace is spanned by } \{|00\rangle, |11\rangle\} \\ -1 \qquad\qquad\qquad\qquad\quad \{|01\rangle, |10\rangle\} \end{matrix}$$

∴ measuring ZZ $\longleftrightarrow$ parity check in computational basis.

$$\begin{matrix} + & \longleftrightarrow & 0 \\ - & \longleftrightarrow & 1 \end{matrix}$$

commuting / compatible $\begin{cases} ZZI \longleftrightarrow s_1 \\ IZZ \longleftrightarrow s_2 \end{cases}$

- Can also meas ZZI, IZZ with non-demolition meas:



- Measurement preserves the superposition of the α, β terms because the <u>underlying</u> classical code is linear with $HG=0$, $H(c+e)=He$ indep of c

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

	no error	error $Z11$	error $1Z1$	error $11Z$
$\alpha\|0\rangle \longrightarrow$	$\alpha\|+++\rangle$	$\alpha\|-++\rangle$	$\alpha\|+-+\rangle$	$\alpha\|++-\rangle$
$+\beta\|1\rangle$	$+\beta\|---\rangle$	$+\beta\|+--\rangle$	$+\beta\|-+-\rangle$	$+\beta\|--+\rangle$
meas XXI	$+$	$-$	$-$	$+$
IXX	$+$	$+$	$-$	$-$

eg 3: 9-qubit Shor code

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

measure

$ZZ1 \otimes III \otimes III \leftrightarrow S_{11}$
$1ZZ \otimes III \otimes III \leftrightarrow S_{12}$

$111 \otimes ZZ1 \otimes 111 \leftrightarrow S_{21}$
$111 \otimes 1ZZ \otimes 111 \leftrightarrow S_{22}$

$111 \otimes 111 \otimes ZZ1 \leftrightarrow S_{31}$
$111 \otimes 111 \otimes 1ZZ \leftrightarrow S_{32}$

$XXX \otimes XXX \otimes 111 \leftrightarrow t_1$
$111 \otimes XXX \otimes XXX \leftrightarrow t_2$

↑ defined in circuit in lecture 1

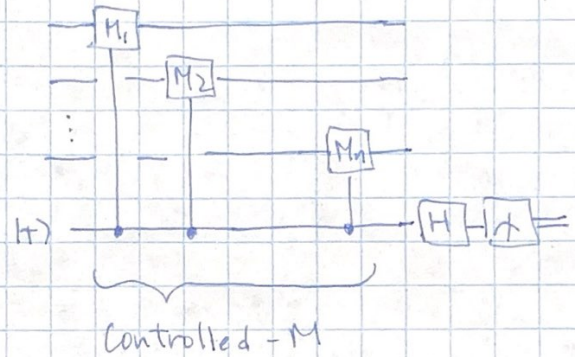
Pf = Ex

How to meas $M = M_1 \otimes M_2 \otimes \cdots \otimes M_n$ where $M_i \in \{I, X, Y, Z\}$?

Note that M has eigenvalues $+1, -1$.

For any $|\psi\rangle$, $|\psi\rangle = a|\psi_+\rangle + b|\psi_-\rangle$ where $M|\psi_+\rangle = |\psi_+\rangle$
$M|\psi_-\rangle = -|\psi_-\rangle$.

Consider the circuit:



$$\therefore \left(a|\psi_+\rangle + b|\psi_-\rangle\right)|+\rangle \xrightarrow{c\text{-}M} a|\psi_+\rangle|+\rangle + b\left(|\psi_-\rangle\frac{|0\rangle}{\sqrt{2}} - |\psi_-\rangle\frac{|1\rangle}{\sqrt{2}}\right)$$

$$= a|\psi_+\rangle|+\rangle + b|\psi_-\rangle|-\rangle.$$

$$\xrightarrow{H} a|\psi_+\rangle|0\rangle + b|\psi_-\rangle|1\rangle.$$

So final meas corr to meas M ("0" if $|\psi\rangle = |\psi_+\rangle$, "1" if $|\psi\rangle = |\psi_-\rangle$) and for a superposition of $|\psi_+\rangle, |\psi_-\rangle$, post-meas state is collapsed correctly.

Ex: draw the circuit to meas $\begin{matrix} ZZI & III & III \\ IZZ & III & III \end{matrix}$ for the 9-qubit code.

$$\vdots$$

$$\begin{matrix} XXX & XXX & III \\ III & XXX & XXX \end{matrix}$$

Will now study these Q parity checks in detail!!

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

A set S is generated multiplicatively by $\{g_1, g_2, \ldots\}$ if each element of S is a product of the g_i's.

Facts:

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

② If $P \in \hat{\mathcal{P}}_n$, then $P^2 = I \in \hat{\mathcal{P}}_n$

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

If $P \in \mathcal{P}_n$, either $P \propto I$

or else $\mathrm{tr}\, P = 0$, spectrum of $P = \{1, -1\}$ or $\{i, -i\}$ (multiplicity 2^{n-1})

③ $P, Q \in \mathcal{P}_n$, P, Q either commute or anticommute

$[P, Q] = 0$ $\quad \{P, Q\} = 0$.

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: $C: \mathcal{P}_n \otimes \mathcal{P}_n \to \mathbb{Z}_2$ (Similarly for $\hat{\mathcal{P}}_n \otimes \hat{\mathcal{P}}_n$)

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

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

We can represent each qubit-Pauli by 2 bits:

$$\begin{array}{lll} I \leftrightarrow & 0 & 0 \\ X \leftrightarrow & 1 & 0 \\ Y \leftrightarrow & 1 & 1 \\ Z \leftrightarrow & 0 & 1 \end{array}$$

Pauli | x-bit | z-bit

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

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

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

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

($\cdot$: inner product on n-bit string mod 2.)

Facts:

- $v_{PQ} = v_P + v_Q \mod 2$ (multiplicative of Paulis $\leftrightarrow$ addition of vector)
- $C(P,Q) = v_P \odot v_Q$
- $Q_1, Q_2, \ldots, Q_t$ multip indep $\Leftrightarrow$ $v_{Q_1}, v_{Q_2}, \ldots, v_{Q_t}$ lin indep (over $\mathbb{Z}_2$)
  (ie no Q_i = product of subset of the rest) (ie no v_{Q_i} = lin comb of the rest)
- Subgroup of Pauli's in $\hat{P}_n$ $\Leftrightarrow$ subspace of vector in $(\mathbb{Z}_2)^{\otimes 2n}$

Generator of sub group $\Leftrightarrow$ basis of the subspace

(Generator: multiplicative)

Motivation: can prove useful results on Pauli & Clifford groups in symplectic rep using lin alg

$\hat{P}_2$: II IX IY IZ
XI XX XY XZ
YI YX YY YZ
ZI ZX ZY ZZ

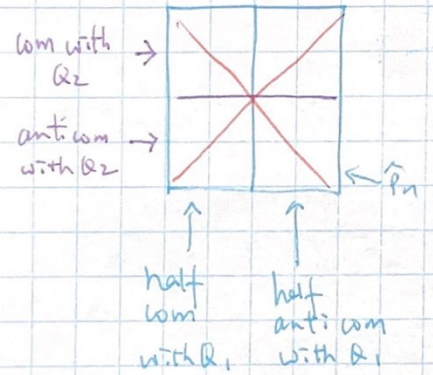
Linear algebra Lemma:

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 anti com with ZI?
XI, YY, YZ, XX

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

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 count 2n-bit strings 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 $S = 2^{2n-m}$

These include all elmts of S $\therefore$ $|S| \leq 2^{2n-m}$

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

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