CS 798 Lecture 2 1/7/2010 Stabilizer codes

Classical error-correcting code (ECC):

is a subset C of $\{0,1\}^n$

Its distance is d if the Hamming distance

$$d(x,y) = \#\{j : x_j \neq y_j\}$$

between any distinct codewords $x, y \in C$ is at least d.

Linear ECC:

is a linear subspace of $(\mathbb{Z}_2)^n$.

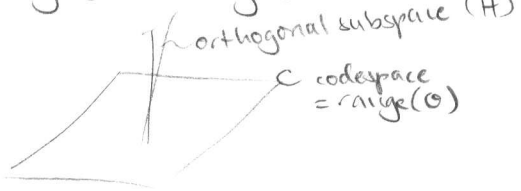
* If $\dim C = k$ then $|C| = 2^k$, i.e. C encodes k bits
* C can be equivalently specified by either a generating matrix

G, $n \times k$ 0-1 matrix with linearly independent columns

or a parity check matrix

H, $(n-k) \times n$ " " rows

where $C = \text{Range}(G) = \text{Range}(P^t)^\perp$



thus $HG = 0$

Example: * $C = \{000, 111\}$, $k=1$ repetition code

$$G = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \text{ (not unique)}$$

* Hamming code, $n = 2^m - 1$, $m \geq 3$, $k = n - m$

$$H = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ 0 & \cdots & 1 & 1 \end{pmatrix}^{\text{transpose!}}$$ cols all strings in $\{0,1\}^m \setminus \{0^m\}$

$$\text{numeric order} \left\{ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \right. \text{ if } m=3$$

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}^T \text{ if } m=3$$

* All codewords in a linear code are symmetrical, i.e. if $x, y \in C$, so is $x - y$

$\therefore$ the distance is the minimum weight of a nonzero codeword.

Equivalently, it is the min # of columns of P that are linearly dependent.

example, incl. error syndromes

Pauli operators: $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

and their tensor products, eg., $I \otimes X \otimes Y \otimes Z$

Properties:

* Hermitian, unitary $\Rightarrow P^2 = I$
* Form an orthogonal basis for $2^n \times 2^n$ matrices under the trace inner product
* $\Rightarrow$ each $P \neq I$ has half eigenvalues $+1$ and half -1
  (b/c $P^2 = I$ and $Tr(P) = Tr(IP) = 0 = \#_{+1} - \#_{-1}$ evs)
* Form a group, up to phases, under matrix multiplication

$XY = iZ = -YX$,

$YZ = iX = -ZY$ nonidentity Paulis anticommute

$ZX = iY = -XZ$

Pauli group $P_n = \{$n-qubit Paulis, with phases ± 1 or $\pm i\}$.

Def: A quantum stabilizer code (AKA "additive") is the simultaneous $+1$-eigenspace eigenspace of a set of Pauli operators. "stabilizers"

Example: Every linear code is a stabilizer code. $\{|\psi\rangle : |\psi\rangle = P|\psi\rangle \ \forall P \in S\}$

the rows of H are stabilizers, with $0 \to I$, $1 \to Z$

eg $H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \to \begin{matrix} Z \otimes Z \otimes I \\ I \otimes Z \otimes Z \end{matrix}$ diagonal matrices

$\langle x | Z \otimes Z \otimes I | x \rangle = (-1)^{x_1 + x_2} = (-1)^{(1,0)\cdot x}$

$= +1$ if parity is 0

Example: Shor's code

$|0\rangle = (|000\rangle + |111\rangle)^{\otimes 3}$ $\quad |1\rangle = (|000\rangle - |111\rangle)^{\otimes 3}$

$\begin{matrix} Z \otimes Z \otimes I \\ I \otimes Z \otimes Z \end{matrix}$

$X \otimes X \otimes X \otimes X \otimes X \otimes X$

$X \ X \quad X \ X \ X X$

We will determine 1. the dimension of a stabilizer code

2. the distance } generalizing linear codes

3. error syndrome = eigenvalues of the stabilizers

Note: If Paulis P and Q do not commute, then their simultaneous $+1$-eigenspace is 0-dimensional.

proof: $PQ = \bigotimes_i (P_i Q_i)$ but $P_i Q_i = \pm Q_i P_i$

$QP = \bigotimes_i (Q_i P_i)$

Thus either $PQ = QP$ (they commute)

or $PQ = -QP$ (they anticommute)

In the latter case, if $P|\psi\rangle = |\psi\rangle = Q|\psi\rangle$, then

$|\psi\rangle = PQ|\psi\rangle = -QP|\psi\rangle = -|\psi\rangle \Rightarrow |\psi\rangle = 0$! □

$\Rightarrow$ The stabilizers must pairwise commute for code to be nontrivial.

Note: If $P|\psi\rangle = |\psi\rangle$ and $Q|\psi\rangle = |\psi\rangle$ then $PQ|\psi\rangle = |\psi\rangle$.

Thus given a set of (commuting) stabilizers $P_1, \dots, P_m$, adding in $\{P_1^{a_1} P_2^{a_2} \cdots P_m^{a_m} : a \in \{0,1\}^m\}$ all products does not change the code.

$\Rightarrow$ We may assume the stabilizers form an abelian subgroup of P_n.

If there are m independent stabilizers, the subgroup's size is 2^m.

Of course, tensor products of I's and Z's always commute.

In that case, this says the sum of two parity checks is a parity check.

- dim
- distance
- sgrd-one
- special case of stab states

Example: Do these stabilizers commute?

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

No

What about after doubling them?

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

Yes (Thus if we have a quantum side-channel, we can choose arbitrary stabilizers on the left half. The dim of the side channel can be reduced.)

Remark: Any n-qubit pauli P can be represented by a $2n$-bit string (P_x, P_z) with $(P_x)_i = 1$ if $P_i \in \{X, Y\}$ and $(P_z)_i = 1$ if $P_i \in \{Y, Z\}$.

Then if $R = PQ$, up to a phase $R_x = P_x + Q_x \bmod 2$,

$R_z = P_z + Q_z \bmod 2$

Def: Symplectic inner product $P \cdot Q = P_x Q_z + P_z Q_x \bmod 2$.

$P \cdot Q = 0 \iff [P, Q] = 0$ (since holds for $n=1$)

Theorem The dimension of the space stabilized by m independent n-qubit Pauli operators is 2^{n-m}. ($k=n-m$ encoded qubits)

Proof:

First a sanity check. Consider

$$\underbrace{ZII\cdots I}_{Z_1},\ \underbrace{IZI\cdots I}_{Z_2},\ \underbrace{IIZ\cdots I}_{Z_3},\ \ldots,\ Z_m$$

As these operators act on different qubits, they commute & are independent of each other. They are also diagonal in comp'l basis.

Z_j stabilizes the space spanned by $\{|x\rangle \mid x\in\{0,1\}^n, x_j=+1\}$.

Their jointly stabilized space is thus $\{|x\rangle : x_1=x_2=\cdots=x_m=1\}$, indeed 2^{n-m}-dimensional. ✓

Def The Clifford group $\mathcal{C}_n$ on n-qubits is

$$\mathcal{C}_n=\{n\text{-qubit unitaries } U \mid UPU^\dagger\in\mathcal{P}_n \text{ for all Paulis } P\}.$$

Examples:

* $U=e^{i\theta}I$
* U = permutation of the qubits
* $U=Q$ a Pauli: $QPQ=(-1)^{P\cdot Q}PQQ=(-1)^{P\cdot Q}P$
* Hadamard $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}=|+\rangle\langle 0|+|-\rangle\langle 1|$

  $X\to Z,\ Z\to X,\ Y\to -Y$
* $T=\frac{1}{\sqrt{2}}\begin{pmatrix}1&-i\\1&i\end{pmatrix}$: $X\to Y,\ Y\to Z,\ Z\to X$
* CNOT = controlled NOT $=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes X$
  $=I\otimes|+\rangle\langle+|+Z\otimes|-\rangle\langle-|$

$$X\otimes I\to X\otimes X,\quad Z\otimes I\to Z\otimes I,$$
$$I\otimes X\to I\otimes X,\quad I\otimes Z\to Z\otimes Z$$

$XI\to XI$, $XY\to YZ$, $XZ\to -YY$, $YX\to YI$, $YY\to -XZ$, $YZ\to XY$, $ZX\to ZX$, $ZY\to IY$, $ZZ\to IZ$

Fact: These generate the Clifford group. (Pf is easy but not needed.)

The inverse of a Clifford is Clifford, as is the product of two Cliffords.

Back to proving the theorem:

Given $P_1, P_2, \ldots, P_m$ independent, commuting Paulis

Proof idea: Show that they are symmetric to $Z_1, Z_2, \ldots, Z_m$.

ie. find a unitary U such that $UP_jU^\dagger=Z_j$, $j=1,\ldots,m$.

Now $P|\psi\rangle=|\psi\rangle \iff (UPU^\dagger)(U|\psi\rangle)=U|\psi\rangle$

Thus the stabilized space is just multiplied by U, its dimension unchanged.

How to construct U: Gaussian elimination

eg $x_1 + x_2 + x_3 + x_4 = 1$
$x_2 + x_4 = 1$ (mod 2)
$x_3 = 1$

$\rightsquigarrow x_1 = 1$

Same idea works for Paulis, e.g.

$P_1 = X\ X\ Y\ Z\ I$
$P_2 = X\ Y\ Z\ I\ I$
$P_3 = Z\ Y\ X\ Y\ X$

$\xrightarrow{T_3^2 T_4}$

$X\ X\ X\ X\ I$
$X\ Y\ Y\ I\ I$
$Z\ Y\ Z\ Z\ X$

① Starting w/ P_1, change all nontrivial positions to X, using T (there must be some)

② Permute the qubits so P_1 starts with an X

③ Use CNOTs to kill off the other entries of P_1:

CNOT 1,2
CNOT 1,3
CNOT 1,4

$X\ I\ I\ I\ I$
$X\ Z\ Z\ X\ I$
$I\ Y\ Z\ Z\ X$

$\sim -I\ Z\ Z\ X\ I$

④ Eliminate the first coordinate from the other Paulis

⑤ Repeat on remaining Paulis

$-I\ Z\ Z\ X\ I$
$I\ Y\ Z\ Z\ X$

$\xrightarrow{T_2 T_3}$

$-I\ X\ X\ X\ I$
$I\ Z\ X\ Z\ X$

$\xrightarrow[CX_{2,4}]{CX_{2,3}}$

$-I\ X\ I\ I\ I$
$I\ I\ X\ Z\ X$

$\xrightarrow[CX_{3,5}]{CX_{3,4}}$

$X\ I\ I\ I\ I$
$-\ I\ X\ I\ I$
$I\ I\ X\ I\ I$

$\xrightarrow{Z_2}$ to switch the sign

$\xrightarrow{H_1 \cdots H_5}$ Z_1 Z_2 Z_3 ✓

□

Remark: * If $m = n$, then the stabilized space is $2^{n-n} = 1$ dimensional.
→ Called a "stabilizer state" $|\psi\rangle$ (well-defined up to a phase)

This procedure lets us prepare it!
Start with $|0^n\rangle$, stabilized by $Z_1, \ldots, Z_n$.
Apply (the inverses of) the above unitaries (in reverse order), i.e. $U^\dagger$.
$U|0^n\rangle$ is stabilized by $\{UZ_jU^\dagger\} = \{P_j\}$ ✓

* Since $P^2 = I$, $\frac{1}{2}(I+P)$ is a projection onto P's $+1$ eigenspace.

$$\prod_{j=1}^{m} \frac{1}{2}(I+P_j) = \frac{1}{2^m} \sum_{x \in \{0,1\}^m} \bigotimes P_j^{x_j} = \frac{1}{2^m} \sum_{\text{all stabilizers } S} S$$

is the projection onto the stabilized subspace.