Lecture #3
Peter Shor
02/14/2006

Today: CSS codes

Discussion — Φ is an operator on a state in a d-dimensional space. Then, $\Phi\left[\left(\frac{1}{\sqrt{d}}\sum_{i=1}^{d}|e_i\rangle|e_i\rangle\right)\left(\frac{1}{\sqrt{d}}\sum_{i=1}^{d}\langle e_i|\langle e_i|\right)\right]$ completely specifies the operator Φ.

7-qubit code

$$|0_L\rangle = \frac{1}{\sqrt{8}}\left[|0000000\rangle + |1110100\rangle + |0111010\rangle + \text{cyclic shifts}\right]$$

$$|1_L\rangle = \frac{1}{\sqrt{8}}\left[|1111111\rangle + |0001011\rangle + |1000101\rangle + \text{cyclic shifts}\right]$$

Claim: Corrects any 1-qubit error.

- Measure 1st qubit in "0-1" basis.
- Get '0'.
- $\alpha|0_L\rangle + \beta|1_L\rangle \longrightarrow \frac{\alpha}{2}\left[|0000000\rangle + |0111010\rangle + |0011101\rangle + |0100111\rangle\right] + \beta\left[\quad\cdots\quad\right]$

- Project onto spaces

$$\Pi_c = |0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|$$

$$\sigma_x^{(1)}\left(|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|\right)\sigma_x^{(1)}$$ X operated on 1st qubit

$\vdots \qquad \vdots \qquad \vdots$

$$\frac{1}{\sqrt{2}}\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) + \frac{1}{\sqrt{2}}\sigma_Z^{(1)}\left(\alpha|0_L\rangle + \beta|1_L\rangle\right)$$

(i) with prob $1/2$, gets projected into $|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|$

"no error"

(ii) with prob $1/2$, gets projected into $\sigma_Z^{(1)}\left[|0_L\rangle\langle 0_L| + |1_L\rangle\langle 1_L|\right]\sigma_Z^{(1)}$

"Z-error on 1st qubit" $\rightarrow$ correct it.

$\gamma|0\rangle + \delta|1\rangle$

$\rightarrow$ project it onto $(\gamma|0\rangle + \delta|1\rangle)(\gamma^*\langle 0| + \delta^*\langle 1|) = \begin{pmatrix} |\gamma|^2 & \gamma^*\delta \\ \delta^*\gamma & |\delta|^2 \end{pmatrix} = \frac{id}{2} + \left(\frac{|\gamma|^2 - |\delta|^2}{2}\right)\sigma_Z^{(1)}$

$+ Re(\gamma\delta^*)\sigma_X^{(1)} + Im(\gamma\delta^*)\sigma_Y^{(1)}$

Let Π_c be projection onto code subspace

$Tr\left(\Pi_c \sigma_X^{(i)} \Pi_c \sigma_X^{(i)}\right) = 0$ (claim) $\rightarrow$ will prove later

$$\Pi_c\left(\frac{id}{2} + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z\right)\Pi_c\left(\frac{id}{2} + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z\right)\Pi_c$$

Will project into one of 4 possibilities, and corr. recovery may then be applied.

$|0_L\rangle = \sum |0000000\rangle + \text{c.s.}\,|1110100\rangle$

$|1_L\rangle = \sum |1111111\rangle + \text{c.s.}\,|0001011\rangle$

Classical binary linear block codes.

Hamming code $[7,4,3]$ code
$$\uparrow n \quad \uparrow k \quad \uparrow d$$

16 codewords:

$$\begin{bmatrix} 0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1 \\ 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ & & & \vdots & & & \\ 0&0&0&1&0&1&1 \\ 1&0&0&0&1&0&1 \\ & & & \vdots & & & \end{bmatrix}$$

c.s.

Linear span of:-

$$G = \begin{bmatrix} 1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0 \\ 0&0&1&1&1&0&1 \\ 1&1&1&1&1&1&1 \end{bmatrix}$$

Any codeword of the $[7,4,3]$ code is a linear combination (mod 2) of rows of G. Any 2 codewords differ in at least 3 positions ($d=3$).

$$\{ wt_H(v-w) = wt_H(z) \geq 3 \}$$

~~$Tr\ \sigma_x^{(i)}$~~

$\sigma_x^{(i)} \Pi_c \sigma_x^{(i)}$ orthogonal to $\sigma_x^{(j)} \Pi_c \sigma_x^{(j)}$

So, we can correct any arbitrary bit-errors on the 7 qubits.

How do we correct phase errors.

$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ turns $\sigma_x \Leftrightarrow \sigma_z$: $H\sigma_x H = \sigma_z$.

$$Tr\ \sigma_z^{(i)} \Pi_c \sigma_z^{(i)} \sigma_z^{(j)} \Pi_c \sigma_z^{(j)}$$

$$= Tr\left[\cancel{H^{\otimes 7}} \sigma_x^{(i)} H^{\otimes 7} \Pi_c H^{\otimes 7} \sigma_x^{(i)} \sigma_x^{(j)} H^{\otimes 7} \Pi_c H^{\otimes 7} \sigma_x^{(j)} \cancel{H^{\otimes 7}} \right]$$

this cancels with the 1^{st} $H^{\otimes 7}$ due to cyclic prop. of Tr

(on non-(i) qubits $HH = I$, so doesn't matter)

$$H^{\otimes 7}\Pi_C H^{\otimes 7} = \Pi_C$$

A general CSS-code

$$0 \subseteq C_1 \subseteq C_2 \subseteq \mathbb{Z}_2^n \quad --- \circledast$$

C_1, C_2 are linear subspaces over $\mathbb{Z}_2^n$

$\#$ of codewords $= \dfrac{|C_2|}{|C_1|}$,

and the codewords corresponding to $\underbrace{\text{cosets } C_2/C_1}_{\begin{array}{c}|||\\ \{v + C_1 \mid v \in C_2\}\end{array}}$.

quantum codewords

$$|v + C_1\rangle = \cancel{\frac{1}{\sqrt{|C_2|/|C_1|}}} \ \frac{1}{\sqrt{|C_1|}} \sum_{c \in C_1} |v + c\rangle$$

$$C_1 = \left\{\begin{matrix} 0000000 \\ 1110100 \\ 0111010 \\ 0011101 \end{matrix}\right\} \ ; \quad C_2 = C_1 \cup \{1111111 + C_1\}$$

C_2 good error-correcting code
$\Rightarrow$ quantum code is good against bit errors.

How does it correct phase errors?

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \sum_{s,t \in 0,1} |s\rangle\langle t| (-1)^{st}$$

$$H^{\otimes n} = \frac{1}{2^{n/2}}\left(\sum_{s,t \in \mathbb{Z}_2^n} |s\rangle\langle t| (-1)^{s \cdot t} \right)$$

$$H^{\otimes 2} = \begin{array}{cc} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \end{array}$$

$$H^{\otimes n} |v + C_1\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{\substack{s,t \in \mathbb{Z}_2^n \\ c_1 \in C_1}} \frac{1}{\sqrt{|C_1|}} \; |s\rangle\langle t| \; |v + c_1\rangle$$

$$= \frac{1}{2^{n/2}} \cdot \frac{1}{\sqrt{|C_1|}} \sum_{\substack{s \in \mathbb{Z}_2^n \\ c_1 \in C_1}} |s\rangle \cancel{} (-1)^{s\cdot(v+c_1)}$$

$$= \sum_{s \in \mathbb{Z}_2^n} (-1)^{s\cdot v} \left[\sum_{c_1 \in C_1} (-1)^{c_1 \cdot s} \; |s\rangle \right] \left(\frac{1}{2^{n/2}\sqrt{|C_1|}} \right)$$ normalization.

$$\boxed{C_1^{\perp} = \cancel{} \; \{ v \mid v \cdot c_1 \text{ is even } = 0 \ (\text{mod } 2) \ \forall c_1 \in C_1 \}}$$

Self orthogonality: $|1110100\rangle$ is $\perp^r$ to itself

C_1 (for Hamming code)

1110100
0111010
0011101

Weakly self-dual code. (code whose dual contains the code itself)

If C is subspace of $\mathbb{Z}_2^n$

$v.c = 0, \ \forall c \in C$

$v.c = 0$ half of $c \in C$.

Proof:

Suppose it is NOT true.

Either $v.c = 0 \ \forall c \in C$,

or $\exists\, x \in C$, $v.x = 1$

In the case (second),

c, $c+x$ have inner product of 1 and 0 (in pairs).

$(v.c = 0 \Leftrightarrow v.(c+x) = 1)$

So, going back,

$$\frac{1}{2^{n/2}\sqrt{|C_1|}} \sum_{s \in \mathbb{Z}_2^n} (-1)^{s.v} \sum_{c_1 \in C_1} (-1)^{c_1.s} |s\rangle$$

$$= \frac{|C_1|^{1/2}}{2^{n/2}} \sum_{s \in C_1^\perp} (-1)^{s.v} |s\rangle$$

$\left\{ \mathbb{Z}_2^n \supseteq C_1^\perp \supseteq C_2^\perp \supseteq \{0^n\} \ \ldots \text{(from } \circledast \text{ on page 4)} \right\}$

$$= \frac{|C_1|^{1/2}}{2^{n/2}} \sum_{s \in C_1^\perp/C_2^\perp} \sum_{t \in C_2^\perp} (-1)^{(s+t).v} |s+t\rangle$$

$(v \in C_2$, so $t.v = 0$ (as $t \in C_2^\perp))$

$$= \frac{|C_1|^{1/2}}{2^{n/2}} \sum_{s \in C_1^\perp/C_2^\perp} (-1)^{s.v} \sum_{t \in C_2^\perp} |s+t\rangle$$

$$= \frac{1}{\sqrt{|C_1^\perp/C_2^\perp|}} \sum_{s \in C_1^\perp/C_2^\perp} (-1)^{s.v} \underbrace{|s + C_2^\perp\rangle}$$

Codeword in CSS code corresponding to $\{0\} \subseteq C_2^\perp \subseteq C_1^\perp \subseteq \mathbb{Z}_2^n$

corrects bit errors if $C_1^\perp$ is a good error-corr. code.

How does the CSS code correct qubit-errors?

- Generator matrix of the $[7,4,3]$ H.C. :

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

parity check matrix $\quad GH^T = 0.$

$v \in \mathcal{C}$. Claim : vH^T tells you where the most likely error is.

Codeword : v

$\downarrow$ error

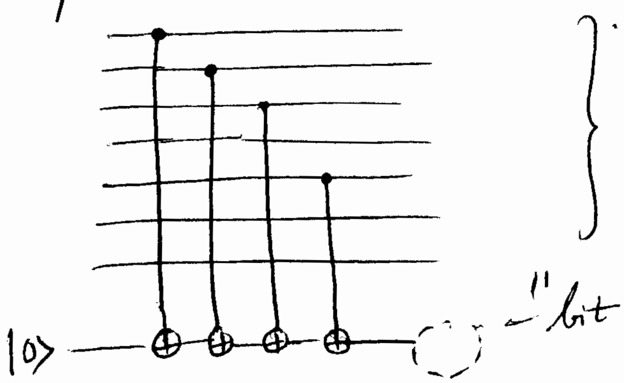
$v + e$

$$(v+e)H^T = vH^T + eH^t = eH^T$$

$eH^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ ...suppose $\Rightarrow$ this 3-bit syndrome uniquely tells the most likely error (As no two columns of H are identical.

Finding error from syndrome : No general good algothism known.

- 7-qubit CSS code :



correction of bit-error.

"bit one of syndrome".

<u>exercise</u> :— correction of phase-errors.

Gilbert-Varshamov Bound

$\exists$ QECC $[[n,k,d]]$ (CSS code), $\frac{k}{n} = R$ ~~$\geq 1 - 2H\left(2\frac{d}{n}\right)$~~

$\sim 1 - 2H\left(\frac{d}{n}\right)$

$\left(H = -x \log_2 x - (1-x)\log_2(1-x) \right)$

Classical GV Bound:

$R \geq 1 - H\left(\frac{d}{n}\right)$

Look at all codes of dim k. # of codes codeword appears in, is the same for all codewords.

Compute # of codes,

# of codes that contain short codewords

$$W \sum_{j=0}^{d-1} \binom{n}{j} \leq W \left(\frac{2^n - 1}{2^k - 1} \right)$$

Taking $\log_2$, we get:

$$H\left(\frac{d}{n}\right) \leq 1 - \underbrace{\frac{k}{n}}_{R} \qquad \square$$

Quantum GV ~~bound~~:

just look at weakly self-dual codes ...