Quantum Error Correction

Lecture 3

•

Daniel Gottesman, Perimeter Institute

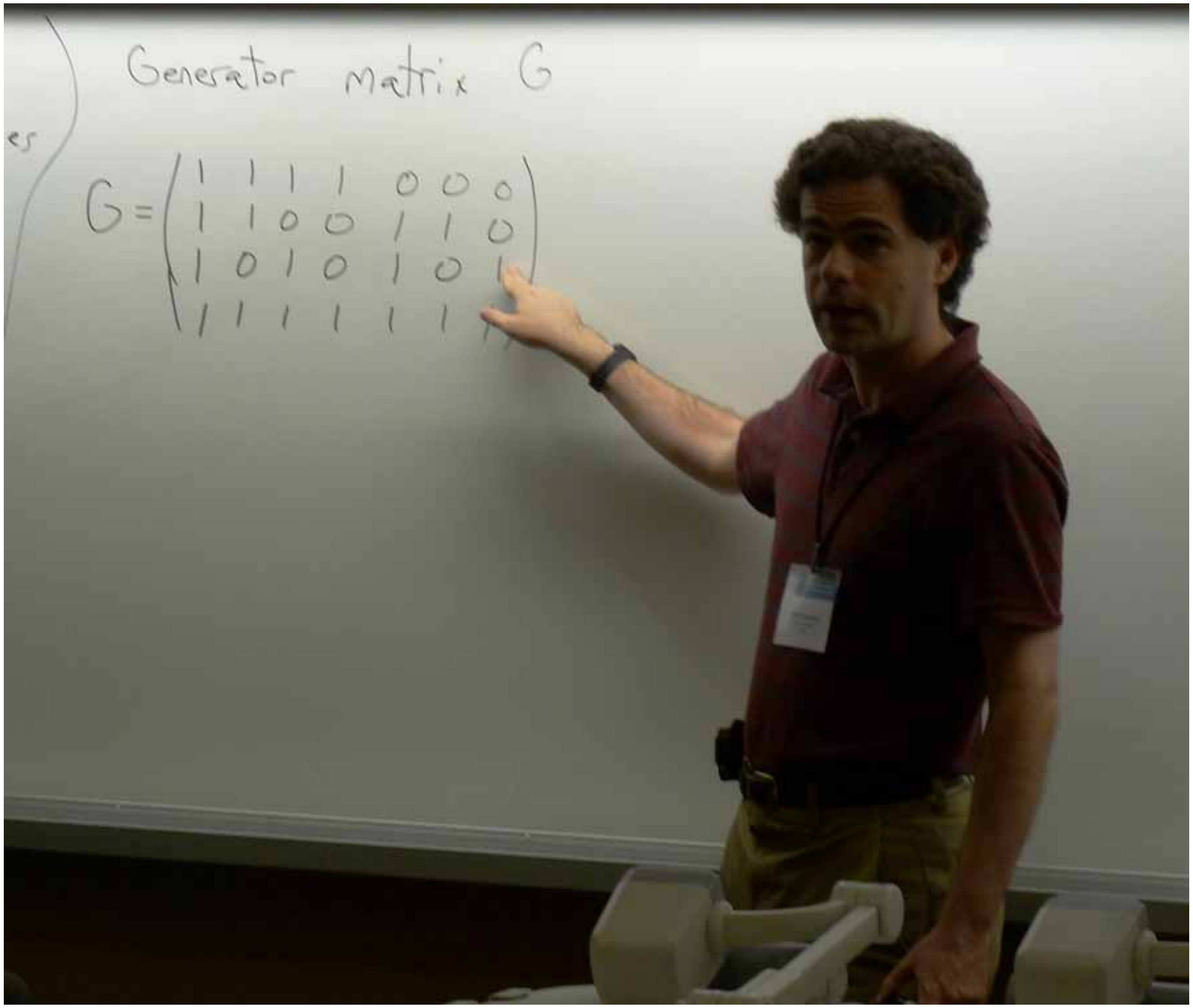
University of British Columbia, July 18, 2010

Linear error-correcting codes

Classical code C is a set of bit strings.

Linear code: $x, y \in C \Rightarrow x \oplus y \in C$

Repetition code: $\{000, 111\}$


Generator matrix G
G =
1 1 1 1 0 0 0
1 1 0 0 1 1 0
1 0 1 0 1 0 1
1 1 1 1 1 1 1

odes

Generator matrix G

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

Encode message $v = \begin{pmatrix} v_0 \\ v_1 \\ v_2 \\ v_3 \end{pmatrix}$

Corresponding codeword $G^T v$

$v, v' \Rightarrow v \oplus v'$ has encoding

$$G^T(v \oplus v') = G^T v \oplus G^T v'$$

Parity check matrix P

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

$\in C$

x a codeword $\Leftrightarrow$ $Px = 0$

Corresponds to stabilizer

$1 \to Z$, $0 \to I$

$Z \otimes Z \otimes Z \otimes Z$

$Z \otimes Z \otimes \qquad Z \otimes Z$

$Z \otimes \quad Z \otimes \quad Z \otimes \quad Z$

Given P, we can define

$$C = \{ x \mid Px = 0 \}$$

$$P(x+y) = Px + Py = 0 + 0 = 0$$

$$PG^T = 0$$

For any linear C, define $C^\perp$ (dual code to C) to be the code with generator matrix P & parity check matrix G.

Consider bit flip errors as a vector e. (1 in locations of errors & 0 in bits which don't have an error.)

Codeword x with error e: $x+e$

Can identify error by

$$P(x+e) = Px + Pe = Pe$$

(Error syndrome)

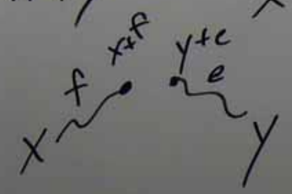
$$\text{Error on ith bit} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow Pe = \text{ith column of } P$$

Def.: Distance of a linear code is smallest weight of any non-zero vector in C.

Codewords x, y

Bits to flip to get from x to y:

$e = x + y$ $\quad x + e = y \quad y + e = x$

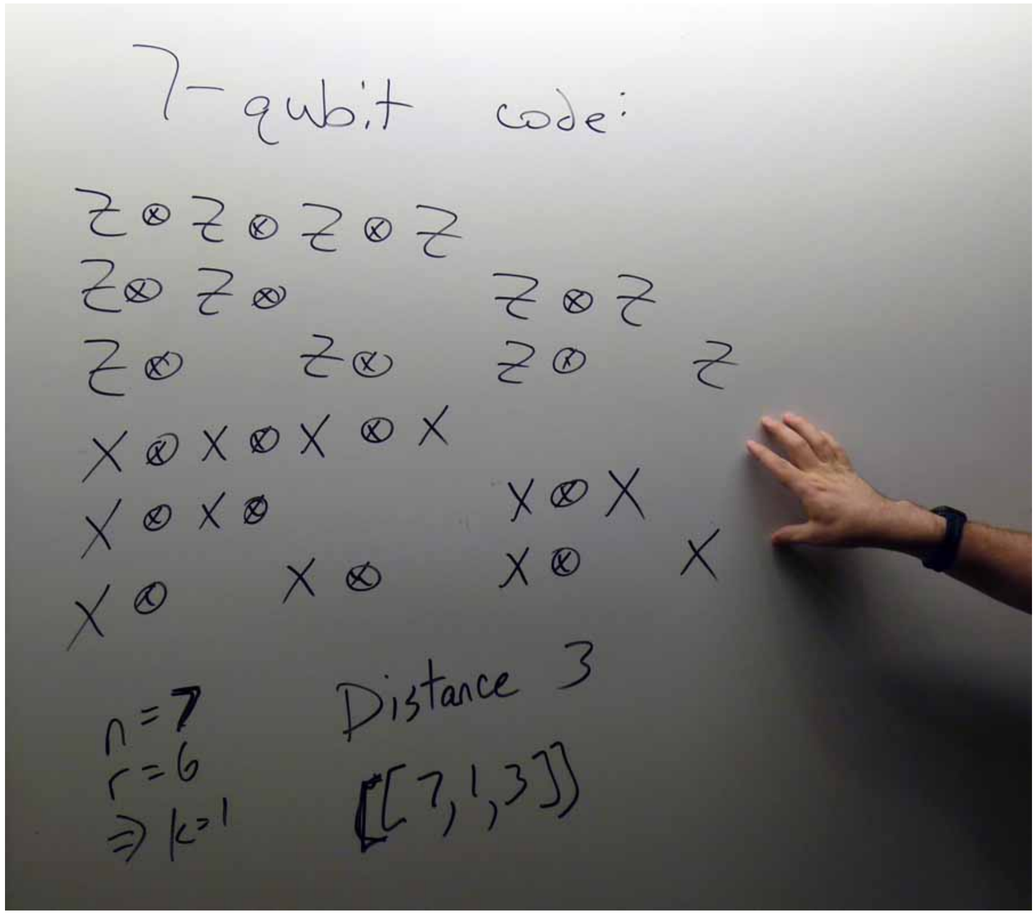


$f + e \neq C$

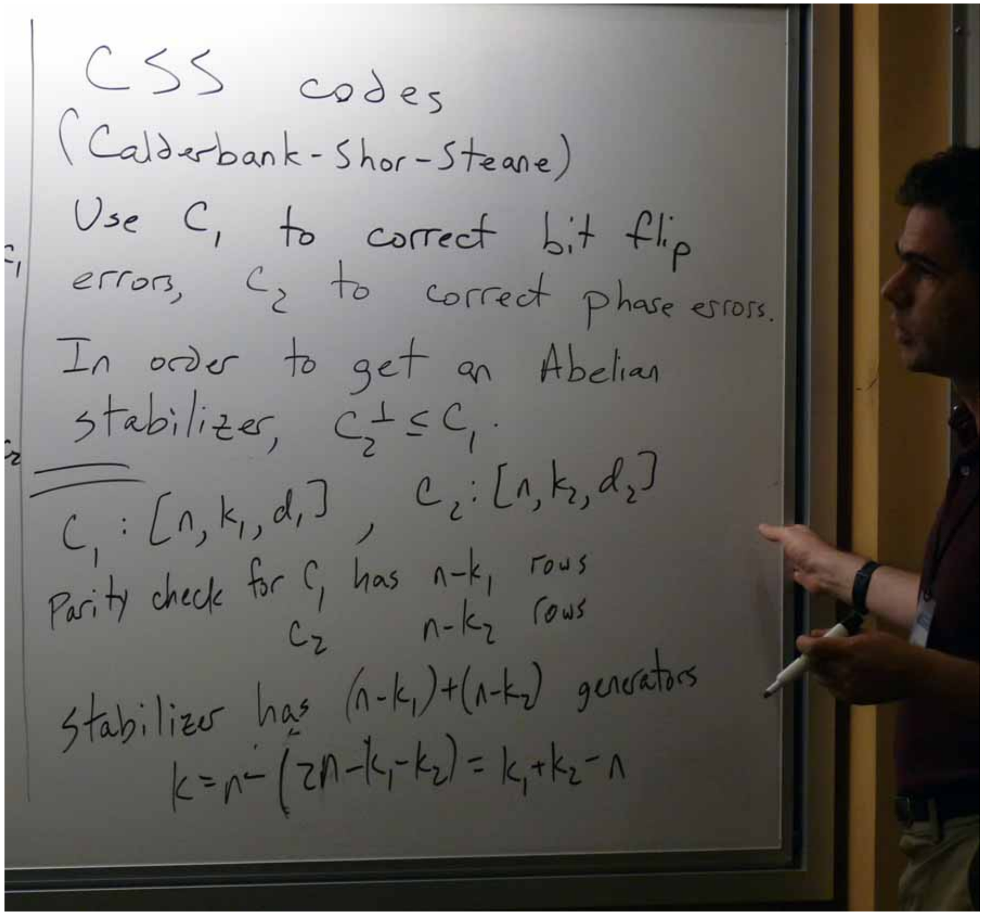
$wt(f+e) <$ distance

To correct t errors, need distance $2t+1$

$[n, k, d]$ $\quad$ n physical bits
k logical bits
d distance



7-qubit code:
Z⊗Z⊗Z⊗Z
Z⊗Z⊗ Z⊗Z
Z⊗ Z⊗ Z⊗ Z
X⊗X⊗X⊗X
X⊗X⊗ X⊗X
X⊗ X⊗ X⊗ X
n=7
r=6
⇒ k=1
Distance 3
[[7,1,3]]


CSS codes
(Calderbank-Shor-Steane)
Use C_1 to correct bit flip errors, C_2 to correct phase errors.
In order to get an Abelian stabilizer, $C_2^{\perp} \leq C_1$.
$C_1 : [n, k_1, d_1]$, $C_2 : [n, k_2, d_2]$
Parity check for C_1 has $n-k_1$ rows
C_2 $n-k_2$ rows
stabilizer has $(n-k_1)+(n-k_2)$ generators
$k = n - (2n - k_1 - k_2) = k_1 + k_2 - n$

Distance of CSS code:

$$\min(d_1, d_2)$$

$$\left.\begin{array}{l} Z\otimes Z \\ \quad Z\otimes Z \\ \qquad Z\otimes Z \\ \qquad\quad Z\otimes Z \\ \qquad\qquad Z\otimes Z \\ \qquad\qquad\quad Z\otimes Z \end{array}\right\} \text{distance } 3$$

$$\left.\begin{array}{l} X\otimes X\otimes X\otimes X\otimes X\otimes X \\ \qquad\qquad X\otimes X\otimes X\otimes X\otimes X\otimes X \end{array}\right\} - \begin{pmatrix} 111 & 111 & 000 \\ 000 & 111 & 111 \end{pmatrix}$$

Distance 2

Stabilizer code:

Distance = min wt $N(S) \setminus S$.

Classical linear code:

Distance = min wt. nonzero vector

=

Degenerate quantum code

has some non-identity operator in S with weight less than distance.

i.e. $\min \text{wt} \, (N(S) \setminus S)$

$\neq \min \text{wt} \, (N(S) \setminus \{I\})$

Codewords of CSS code:

Let $x \in C_1$

$\displaystyle\sum_{u \in C_2^\perp} |x+u\rangle$

Correspond to cosets $C_1/C_2^\perp$

$(x+u \in C_1)$

Consider $y \in C_1$

with $y = x+v$, $v \in C_2^\perp$

$$\Rightarrow \sum_{u \in C_2^\perp} |x+u\rangle = \sum_{u' \in C_2^\perp} |x+\underbrace{v+u'}_{C_2^\perp}\rangle$$

$$= \sum_{u''=u'+v \in C_2^\perp} |x+u''\rangle$$