Quantum Error Correction Course (Notes)

Prepared by Jean-Christian Boileau
Edited by Daniel Gottesman

January 22^{nd} 2004 (Lecture # 5)

1 Distance 2 Codes:

- Generators of the stabilizer for 4 qubits: XXXX, ZZZZ
  $[[4, 2, 2]]$
- Generators of the stabilizer for 2n qubits: XXX..X, ZZZ..Z
  $[[2n, 2n-2, 2]]$
- Generators of the stabilizer for 2n+1 qubits: XXX..XXI, ZZZ...ZZZ, III...IXX
  $[[2n+1, n-3, 2]]$ (Three generators are required since the stabilizer needs to be abelian.)

2 Classical Linear Codes:

Codewords $\mathbf{v} \in C$ are binary vectors. Linear code: $\mathbf{v} + \mathbf{w} \in C$ when $\mathbf{v}, \mathbf{w} \in C$ (for a code over a finite field F, also if $\alpha \in F, \mathbf{v} \in C \Rightarrow \alpha\mathbf{v} \in C$)

2.1 Generator matrix

Codewords are linear combinations of rows of a generator matrix. (Example for $[7, 4, 3]$ classical code) :

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

2.2 Parity Check Matrix:

$GH^T = 0$ so that if G is a $k \times n$ matrix, then H is $n-k \times n$. In the previous case, we can show that one possible parity matrix is

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

H annihilates valid codewords v: $Hv = 0$. $H(v+e)$ in general gives us the error syndrome of the vector e.

Let $\mathbf{h_i}$ be the i^{th} row of H. Since $\mathbf{h_i}v = 0, \mathbf{h_j}v = 0 \Rightarrow (\mathbf{h_i} + \mathbf{h_j})v = 0$ then H generates the "dual code" $C^{\perp}$.

2.3 Distance (classical case):

- **Definition of Hamming distance:** The Hamming distance between **v** and **w** is the # of bits on which **v** and **w** differ.
- **Definition of Distance:** The distance of an error-correcting code C is the minimum Hamming distance between any two vectors in C.
- Distance d code can correct $\lfloor (d-1)/2 \rfloor$ errors.
- Distance of C = minimum weight of any $\mathbf{v} \in C$ = minimum # of columns of H that are linearly dependent.

2.4 Hamming Codes (example):

Hamming codes have r rows in their parity check matrix H, and the columns are all possible nonzero r-bit vectors (there are $2^r - 1$ of them). Thus, any two columns of H are distinct, but there are sets of three that are linearly dependent. Thus, Hamming codes have distance 3. A Hamming code has parameters $[2^r - 1, n - r, 3]$.

Consider $r = 2$ and look at the matrix

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

(G gives the repetition code.)
If $\mathbf{v} \in C$ and $\mathbf{e} \in C^{\perp}$ then $\mathbf{v} + \mathbf{e}$ has the same error syndrome as $\mathbf{e}$ ($H\mathbf{v} = 0$). In the previous parity check matrix, replace 1 by Z and 0 by I to obtain ZZI and ZIZ. The stabilizer generated by these operator will correct the same number of bit flip errors as the classical code should have corrected.
If we replace 1 by X instead of Z then we obtain XXI and XIX. The stabilizer generated by these operators will correct the same number of phase flip errors as the classical code should have corrected.

3 CSS (Calderbank-Shor-Steane) Codes:

- Consider 2 classical linear codes: $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$
  In the parity check matrix for C_1 replace 1 by Z and 0 by I. In the parity check matrix for C_2 replace 1 by X and 0 by I. If the new operators commute, we get a quantum CSS code $[[n, k_1 + k_2 - n, d]]$ where d= min(d_1, d_2) (if the code is non-degenerate).

- Example: **7-qubit code.** From $C_1 = C_2 = [7, 4, 3]$ we can get $[[7, 1, 3]]$ with a stabilizer generated by ZZZZIII, ZZIIZZI, ZIZIZIZ, XXXXIII, XXIIXXI and XIXIXIX.
  However, the stabilizer is an abelian group if and only if $H_1 H_2^T = 0$ where H_i is the parity check matrix of C_i, which generates the code $C_i^\perp$. This imply that $C_2^\perp \subseteq C_1$ (which is equivalent to $C_1^\perp \subseteq C_2$).

- We get a family of Hamming codes $C_1 = C_2 = [2^r - 1, 2^r - 1 - r, 3]$ that give CSS codes $[[2^r - 1, 2^r - 1 - 2r, 3]]$

4 Question for next class:

Why does the 9-qubit code have distance 3, but the classical code given by the stabilizer generated by XXXXXXIII and IIIXXXXXX as only distance 2?
Short answer: Since the 9-qubit code is degenerate. Since ZZIIIIIII is in the stabilizer, it implies that the errors ZIIIIIIII and IZIIIIIII (which have the same syndrome) can be corrected by the same operation. Many other errors are also degenerate and that make the distance of the code more than 2.

Moral: The distance of a CSS code could be greater than min(d_1, d_2).