Weight enumerators of codes and dual codes.

Yangrong Zhao Math 846

Weight enumerators of codes:

Def: Hamming distance $\partial(x,y) = |\{j \mid 1 \le j \le n, x_j \ne y_j\}|$
# of distinct entries between x and y.

Def: Weight $w(x) = |\{i \mid x_i \ne 0 \ (1 \le i \le n)\}| = \partial(x, 0)$
# of nonzero entries

E.g. $C = \{\overset{x_1}{000}, \overset{x_2}{111}\}$ Receive $x = 010$ $\partial(x_1, x) = 1$, $\partial(x_2, x) = 2$
We believe that the possibility of flipping in each entry is almost equivalent $\Rightarrow$ The $x_1 \in C$ that has smaller Hamming distance with x, so it has higher possibility to be the original ~~message~~ codeword $\Rightarrow$ We error-correct it into x_1

Thm: If C is a linear code, then $d(C) = \min\{\partial(x,y) : x, y \in C, x \ne y\}$
$= \min\{w(x-y) : x, y \in C, x \ne y\} = \min\{w(c) : c \in C, c \ne 0\}$

Def: Weight enumerator: $W_C(x,y) = \sum_{c \in C} x^{n-w(c)} y^{w(c)} = \sum_{i=0}^{n} A_i x^{n-i} y^i$,
and A_i is the # of elements of C with weight i.

E.g. Hamming $[7, \overset{\text{dimension}}{4}, \overset{\text{distance}}{3}]$-code with generator matrix G:

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

Encoding rule: m message
G generator matrix
c codeword
$c = mG$ $\quad F_2^4 \to C \subseteq F_2^7$

$F_2^4 = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$

$C = \{0000000, 1111111, 1010101, 0101010, 0110011, 1001100, 1100110, 0011001, 0001111, 1110000, 1011010, 0100101, 0111100, 1000011, 1101001, 0010110\}$

Weight enumerator is $x^7 + 7x^4 y^{\boxed{3}} + 7x^{\boxed{3}} y^4 + y^7$ distance

Dual codes

Def: Inner product: $x=(x_1, x_2, \ldots, x_n)$, $y=(y_1, y_2, \ldots, y_n)$, $x, y \in F_2^n$, $x \cdot y = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \in F_2$

Def: Dual codes: $C^{\perp} = \{x \in F_2^n \mid x \cdot y = 0, \forall y \in C\}$
In particular, if $C^{\perp} = C$ holds, we call C the self-dual code.

Thm: If C is an $[n,k]$-code, then $C^{\perp}$ is an $[n, n-k]$ code.
Pf: Let G be a generator matrix for C, and let the rows of G be $v_1, v_2, \ldots, v_k$.
For $\forall x \in C^{\perp}$, $x \cdot v_1 = x \cdot v_2 = \ldots = x \cdot v_k = 0$ since $v_i \in C$.
For $\forall y \in C$, $y = mG = m_1 v_1 + m_2 v_2 + \ldots + m_k v_k$,
$x \cdot y = x \cdot (m_1 v_1 + m_2 v_2 + \ldots + m_k v_k) = m_1 x \cdot v_1 + m_2 x \cdot v_2 + \ldots + m_k x \cdot v_k = 0$
$\therefore C^{\perp} = \{x \in F_2^n \mid G x^T = 0\}$ = null space of G.
Since G has rank k, so $C^{\perp}$ is with dimension $n-k$.

If G and H are the generator matrix and the parity check matrix of a linear code C, then H and G are the generator matrix and the parity check matrix of a linear code C.
Parity check matrix: $Hx^T = 0 \ \forall x \in C$

Note: If C is a self-dual code, if G is a generator matrix, then G is a parity check matrix.

Motivation: We cannot directly find the minimum distance of the dual code $C^{\perp}$ with the minimum distance of a code C is given.

Thm: MacWilliams identity: For a linear code over $\mathbb{F}_q$, we have
$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+(q-1)y, x-y)$.
Particularly, $W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$ if the field is $\mathbb{F}_2$.
We now know the minimum distance by checking the smallest d of nonzero $x^{n-d}y^d$ term of $W_{C^\perp}(x,y)$.

Pf: Similar idea to what we see in Lecture 29.