Weight Distributions of Codes (Ketonen-Weldon, p. 64; )

Zehnder 11.397--

Let $A_i$ = number of codewords of weight $i$ in an $(N,K)$ block code. The weight enumerator for the code is

$$A(z) = \sum_{i=0}^{N} A_i z^i$$

The weight distribution can be used to calculate the undetected error probability. Any error pattern equal to a nonzero codeword causes an undetected error. For a code over $GF(2)$ used on a BSC with crossover probability $p$

$$P(\text{undetected error}) = \sum_{i=1}^{N} A_i p^i (1-p)^{N-i}$$

$$= (1-p)^N A_i [p/(1-p)] - (1-p)^N$$

The weight distribution $\{A_i\}$ has been found analytically for only a few codes, for example, the maximal length codes, Hamming codes, and Reed-Solomon codes. If $K$ is not too large, $A_i$ can be determined by examining all codewords using a computer. If $K$ is large, $N-K$ may be small. We will derive a formula relating the weight distributions of an $(N,K)$ code and its $(N,N-K)$ dual code in this section.
Definitions

Let $U$ and $V$ be subspaces of $W$. Let $U \cap V$ be the set of vectors in both $U$ and $V$. Then $U \cap V$ is also a subspace of $W$.

Let $U \oplus V$ be the set of vectors of the form $u + v$ with $u \in U$ and $v \in V$. $U \oplus V$ is a subspace of $W$.

Lemma 1

The sum of the dimensions of $U \cap V$ and $U \oplus V$ is the sum of the dimensions of $U$ and $V$.

Proof:

Let $k_1 = \dim U$, $k_2 = \dim V$, and $k_0 = \dim U \cap V$. There is a basis of $k_0$ vectors for $U \cap V$. It is possible to find a basis for $U$ consisting of these $k_0$ vectors and $k_1 - k_0$ others not in $U \cap V$, and a basis for $V$ consisting of these $k_0$ and $k_2 - k_0$ others not in $U \cap V$. Then the $k_0$ vectors in the basis for $U \cap V$ the $k_1 - k_0$ additional vectors in the basis for $U$, and the $k_2 - k_0$ additional vectors in the basis for $V$ taken together form a basis for $U \oplus V$. Thus $\dim U \oplus V = k_0 + (k_1 - k_0) + (k_2 - k_0) = k_1 + k_2 - k_0$.

G.E.O.

Lemma 2

Let $U^\perp$ be the null space of $U$ and $V^\perp$ be the null space of $V$. Then $(U \oplus V)^\perp = U^\perp \cap V^\perp$.

Proof:

Since $U \subseteq U \oplus V$, every vector in $(U \oplus V)^\perp$.
must be in \( U^+ \), i.e. \( (U \oplus V)^+ \subset U^+ \). Similarly, 
\( V \cap U \oplus V \), so \( (U \oplus V)^+ \subset V^+ \). Therefore 
\( (U \oplus V)^+ \subset U^+ \cap V^+ \). Every vector in \( U \oplus V \) 
has the form \( u + v \) with \( u \in U \) and \( v \in V \). If \( w \) 
is in \( U^+ \cap V^+ \), then \( u \cdot w = v \cdot w = 0 \) so 
\( (u + v) \cdot w = 0 \). Therefore \( U^+ \cap V^+ \subset (U \oplus V)^+ \). 
Q.E.D.

**Theorem (Mac Williams, 1963)**

Let \( V \) be an \((N, K)\) block code and \( V^+ \) be the \((N, N-K)\) dual code. Let \( A_i \) and \( B_i \) denote the number of vectors of weight \( i \) in \( V \) and 
\( V^+ \), respectively. Then, for codes over \( GF(q) \),

\[
\sum_{i=0}^{\infty} B_i z^i = \frac{q^{-K}}{Z} \sum_{i=0}^{N} A_i (1-z)^i \left[ 1 + (q-1)z \right]^{N-i}
\]

or

\[
B(z) = \frac{q^{-K}}{Z} \left[ 1 + (q-1)z \right]^{N} A \left[ (1-z)/(1+(q-1)z) \right]
\]

**Proof:**

Let \( S = (s_1, s_2, \ldots, s_m) \) be a set of \( m \) distinct integers from the set \( N = \{1, \ldots, N\} \) and let 
\( t = (t_1, \ldots, t_{N-m}) = S \). Let \( F_S \) be the subspace of 
all vectors whose components in positions \( s_1, \ldots, s_m \n\) may be nonzero but must be zero in \( t_1, \ldots, t_{N-m} \). 
Define \( F_+ \) similarly. Then \( F_+ = F_S^\perp \).

Now consider the subspace of all vectors in \( V \) 
which are zero in positions \( t_1, \ldots, t_{N-m} \). This subspace
\[ V \cap \mathcal{F}_S \quad \text{Similarly} \quad V^+ \cap \mathcal{F}_t \quad \text{the set of} \]
all vectors in \( V^+ \) with zero in positions \( s_1, \ldots, s_m \).

By Lemma 2, \( (V \cap \mathcal{F}_S)^+ = V^+ \cap \mathcal{F}_S \quad v^+ \cap \mathcal{F}_t \)
where \( d_s = \dim V \cap \mathcal{F}_S \) and \( d_t = \dim V^+ \cap \mathcal{F}_T \). Then
\[ \dim (V^+ \cap \mathcal{F}_t) = N - d_s \quad \text{because it is the null space of} \ V \cap \mathcal{F}_S. \]

Also, according to Lemma 1,
\[ \dim V^+ \cap \mathcal{F}_t = (N-k) + (N-m) - d_t. \]
Thus
\[ N - d_s = (N-k) + (N-m) - d_t, \]
or
\[ d_t = d_s + N-k - m. \]

Now consider pairs consisting of a set \( S \) of \( m \) integers and a vector \( v \in V \cap \mathcal{F}_S \). For each \( S \), there are \( q^{d_s} \) such pairs since \( \dim V \cap \mathcal{F}_S = d_s \). Considering all choices of \( S \), the total number of such pairs is
\[ \sum_{S} q^{d_s}. \]

On the other hand, each vector of weight \( j \) in \( V \)
has \( N-j \) zero components, and any set \( t \) which is
a subset of \( [N-m] \) of the indices of these
positions defines a set \( S \) which can be paired with
this vector. There are \( \binom{N-j}{N-m} \) choices with \( N-m \) integers
in \( t \), or \( m \) in \( S \). There are \( A_j \) vectors of weight \( j \)
in \( V \). Therefore, the number of pairs \((v, S)\) is also
\[ \sum_{S} q^{d_s} = \sum_{j=0}^{N} A_j \binom{N-j}{N-m}. \]

Similarly, considering \( V^+ \) and sets \( T \) of \( N-m \) integers yields
\[ \sum_{T} q^{d_T} = \sum_{r=0}^{N} B_r \binom{N-r}{m}. \]
Since \( d_x = d_s + N - k - m \) and each \( t \) determines a unique \( s \)

\[
\sum_t q^t = \sum_s q^{d_s + N - k - m} = \sum_s q^{d_s - N - k - m}
\]

\[
= q^{N - k - m} \sum_s q^s
\]

\[
\sum_{k=0}^N \sum_{m=0}^N B_k (N-k) y^m = q^{-k} \sum_{j=0}^N q^j \sum_{m=0}^N A_j (N-j) y^m
\]

\[
\sum_{k=0}^N \sum_{m=0}^N B_k (N-k) \frac{y^m}{m!} = q^{-k} \sum_{j=0}^N q^j \sum_{m=0}^N A_j (N-j) \frac{y^m}{m!}
\]

\[
\sum_{k=0}^N B_k (1 + y)^{N-k} = q^{-k} \sum_{j=0}^N A_j \frac{y^j}{j!}
\]

Define \( f(n, k) = 0 \) for \( k > n \). Multiplying (2) by \( y^m \) and summing yields

Now let \( z = (1+y)^{-1} \), then \( y = (1-z)/z \)

\[
\sum_{k=0}^N B_k z^{-k} = \frac{z}{1} \sum_{j=0}^N A_j \frac{z^j}{j!} \left( \frac{1}{z} \right)^{N-j}
\]

\[
= q^{-k} \sum_{j=0}^N A_j (1-z)^j \left( 1 + (q-1)z \right)^{N-j}
\]
\[ B(z) = q^{-N} \sum_{i=0}^{N} R_i \left( \sum_{j=0}^{i} \binom{i}{j} (-1)^j z^j \right) \left( \sum_{s=0}^{i} \binom{i}{s} z^s (q-1)^i t^s \right) \]

An explicit formula for \( B_i \) can be determined from (3) as follows:

\[
\sum_{i=0}^{N} B_i z^i = q^{-N} \sum_{i=0}^{N} R_i \left( \sum_{j=0}^{i} \binom{i}{j} (-1)^j z^j \right) \left( \sum_{s=0}^{i} \binom{i}{s} z^s (q-1)^i t^s \right)
\]

Letting \( s + t = i \), and eliminating \( t \) gives

\[
B(z) = q^{-N} \sum_{j=0}^{N} R_j \left( \sum_{s=0}^{j} \binom{j}{s} (-1)^s (q-1)^s z^i \right)
\]

\[
= q^{-N} \sum_{j=0}^{N} R_j \left( \sum_{s=0}^{j} \binom{j}{s} (-1)^s (q-1)^s \right) z^i
\]

Equating coefficients of \( z^i \) yields

\[
B_i = q^{-N} \sum_{j=0}^{N} R_j \left( \sum_{s=0}^{j} \binom{j}{s} (-1)^s (q-1)^s \right) z^i
\]

(4)

The sum of the \( k \) th powers of the weights can be found by using the identity

\[
(z \frac{d}{dz}) \sum_{i=0}^{N} B_i z^i = \sum_{i=0}^{N} i A_i B_i z^i
\]

and letting \( z = 1 \). Due to the factor \((1-z)\) on the right of (1), it follows that all the terms involving \( A_i \) for \( i > k \) disappear. The results for \( k = 0, 1, 2 \) are...
\[ \sum_{i=1}^{N} B_{i} = q^{N-K} \]
\[ \sum_{i=1}^{N} i B_{i} = q^{N-K-1} [N(q-1) - A_{1}] \]
\[ \sum_{i=1}^{N} i^2 B_{i} = q^{N-K-2} \{ q(q-1)(q^{N-1} - A_{1}) \} + 2A_{2} \]

**Example**

Consider the Hamming code with \( N = 2^m - 1 \) and \( N - K = m \). Its dual is the \((2^m - 1, m)\) maximal length code over \( GF(2) \). The weight distribution for the maximal length code is

\[ A_{0} = 1, \ A_{2^m-1} = 2^{m-1}, \ A_{x} = 0 \quad \text{otherwise}. \]

Thus

\[ A(z) = 1 + (2^{m-1})z^{2^m-1} \]

and

\[ B(z) = 2^{m-2} \left( 1 + \frac{z}{1+z} \right)^{2^m-1} \left[ 1 + (2^{m-1}) \left( \frac{1-z}{1+z} \right)^{2^m-1} \right] \]

Suppose \( m = 3 \) to give the \((7,4)\) Hamming code. Then

\[ B(z) = 2^{-3} (1+z)^{7} \left[ 1 + 7 \left( \frac{1-z}{1+z} \right)^{4} \right] \]

\[ = 2^{-3} \left[ (1+z)^{7} + 7 (1+z)^{3} (1-z)^{4} \right] \]

\[ = 1 + 0z + 0z^2 + 7z^3 + 7z^4 + 0z^5 + 0z^6 + z^7 \]