Chapter 9

Weight and Distance Enumeration

The weight and distance enumerators record the weight and distance information for the code. In turn they can be analyzed to reveal properties of the code. The most important result is MacWilliams' Theorem, which we prove several times. We also prove the related Delsarte Bound and Lloyd's Theorem.

9.1 Basics

The basic definitions are:

DEFINITION. Let code $C \subseteq F^n$ (F a field) contain c_i codewords of weight i, for $i = 1, \ldots n$. Then the *weight enumerator* is

weight enumerator

$$\mathrm{W}_C(z) = \sum_{\mathbf{c} \in C} z^{\mathrm{w_H}(\mathbf{c})} = \sum_{i=0}^{n} c_i z^i \in \mathbb{Z}[z] \,.$$

The *homogeneous weight enumerator* is

homogeneous weight enumerator

$$\mathrm{W}_C(x, y) = x^n \mathrm{W}_C(y/x) = \sum_{i=0}^{n} c_i x^{n-i} y^i \in \mathbb{Z}[x, y] \,.$$

Actually these definitions make sense whenever the alphabet admits addition, an example of interest being $F = \mathbb{Z}_s$.

DEFINITION. The *distance enumerator* of the code A is given by

distance enumerator

$$\mathrm{W}_A(z) = \; |A|^{-1} \sum_{\mathbf{c}, \mathbf{d} \in A} z^{\mathrm{d_H}(\mathbf{c}, \mathbf{d})} \in \mathbb{Q}[z] \,.$$

This can be defined for any alphabet. The notation does not greatly conflict with that above, since the distance enumerator of A equals the weight enumerator

of A when A is linear. (Indeed, for a code defined over an alphabet admitting addition, we can translate each codeword to the **0**-word and get an associated weight enumerator. The distance enumerator is then the average of these weight enumerators.) One could also define a homogeneous distance enumerator.

The basic results are that of MacWilliams:

(9.1.1) THEOREM. (MACWILLIAMS' THEOREM.) *Let C be a $[n,k]$ linear code over $\mathbb{F}_s$. Set*

$$\mathrm{W}_C(z) = \sum_{i=0}^{n} c_i\, z^i \text{ and } \mathrm{W}_{C^\perp}(z) = \sum_{i=0}^{n} c_i^\perp z^i\,.$$

Then

(1) $\mathrm{W}_C(z) = |C^\perp|^{-1} \sum_{i=0}^{n} c_i^\perp (1+(s-1)z)^{n-i}(1-z)^i$, *and*

(2) $\mathrm{W}_C(x,y) = |C^\perp|^{-1}\mathrm{W}_{C^\perp}(x+(s-1)y, x-y)\,.$

and its nonlinear relative due to Delsarte:

(9.1.2) THEOREM. (DELSARTE'S THEOREM.) *Let A be a code in F^n with distance enumerator $\mathrm{W}_A(z) = \sum_{i=0}^{n} a_i z^i$. Define the rational numbers b_m by*

$$|A|^{-1} \sum_{i=0}^{n} a_i (1+(s-1)z)^{n-i}(1-z)^i = \sum_{m=0}^{n} b_m z^m\,.$$

Then $b_m \geq 0$, for all m.

These two results are related to Lloyd's Theorem 9.4.9, which states that certain polynomials associated with perfect codes must have integral roots. Lloyd's Theorem is the most powerful tool available for proving nonexistence results for perfect codes.

9.2 MacWilliams' Theorem and performance

In this section we relate weight enumerators to code performance. This leads to a first proof of MacWilliams' Theorem. For easy of exposition, we shall restrict ourselves to the consideration of binary linear codes on the BSC(p) throughout this section. Let C be a binary $[n,k]$ linear code. (See Theorem 9.4.8 below for the general case of MacWilliams' Theorem 9.1.1.)

We begin with performance analysis for the binary linear code C on the BSC(p) under the basic error detection algorithm $\mathbf{SS}_0 = \mathcal{D}$:

Algorithm $\mathcal{D}$:
receive $\mathbf{r}$;
if $\mathbf{r} \in C$, then decode to $\mathbf{r}$;
otherwise decode to $\boldsymbol{\infty}$.

As before, we view the received vector $\mathbf{r}$ as being the sum of the transmitted codeword $\mathbf{c}$ and an error word $\mathbf{e}$, that is, $\mathbf{r} = \mathbf{c} + \mathbf{e}$. There are three things that can happen:

correct decoding (error vector $\mathbf{e} = \mathbf{0}$),
error detected (error vector $\mathbf{e} \notin C$),
and false decoding (error vector $\mathbf{e} \in C$, $\mathbf{e} \neq \mathbf{0}$).

The probability of correct decoding is q^n (where $q = 1 - p$). The probability of the other two events can be calculated using the weight enumerator of C. We calculate them in terms of the probability that decoding results in a guess at a codeword, whether or not that guess is correct.

(9.2.1) PROPOSITION. *Let P_D be the probability of detecting an error, P_E the probability of false decoding, and P_R the probability of getting a decoding result.*
(1) $P_R = q^n + P_E$.
(2) $P_R + P_D = 1$.
(3) $P_R = \sum_{i=0}^{n} c_i\, q^{n-i} p^i = \mathrm{W}_C(q, p)$.

PROOF. The first two parts are clear. For the third, observe that we have a decoding result precisely when the error word is a codeword. The chance of a given word of weight w occuring as an error word is $q^{n-w}p^w$. □

Next we use the dual code $C^\perp$ to calculate P_R in a different way. MacWilliams' Theorem results from equating the two probabilities. (This proof of MacWilliams' Theorem follows Chang and Wolf, 1980.)

Set $M = 2^{n-k}$, and let $C^\perp = \{\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_j, \ldots, \mathbf{h}_M\}$. For any $\mathbf{r} \in \mathbb{F}_2^n$, we let $s_j(\mathbf{r}) = \mathbf{h}_j \cdot \mathbf{r}$ and

$$S(\mathbf{r}) = (s_1(\mathbf{r}), s_2(\mathbf{r}), \ldots, s_j(\mathbf{r}), \ldots, s_M(\mathbf{r})) \in \mathbb{F}_2^M\,,$$

the "total syndrome" of $\mathbf{r}$. We have

$$\begin{array}{rccccc} \mathbf{r} \text{ gives a result} & \iff & \mathbf{r} \in C & \iff & \mathbf{e} \in C \\ & \iff & S(\mathbf{r}) = \mathbf{0} & \iff & S(\mathbf{e}) = \mathbf{0} \end{array}$$

and

$$\begin{array}{rccccc} \mathbf{r} \text{ gives a detected error} & \iff & \mathbf{r} \notin C & \iff & \mathbf{e} \notin C \\ & \iff & S(\mathbf{r}) \neq \mathbf{0} & \iff & S(\mathbf{e}) \neq \mathbf{0} \\ & \iff & s_j(\mathbf{r}) \neq 0, \text{ some } j & \iff & s_j(\mathbf{e}) \neq 0, \text{ some } j\,. \end{array}$$

Of course, for a fixed $\mathbf{e}$ and j, the probability that $S(\mathbf{e}) \neq \mathbf{0}$ or that $s_j(\mathbf{e}) \neq 0$ is either 0 or 1. Indeed

(9.2.2) LEMMA.

$$\begin{aligned} \mathrm{Prob}(S(\mathbf{e}) \neq 0 \,|\, \mathbf{e}) &= \mathrm{Prob}(s_j(\mathbf{e}) \neq 0,\ \textit{some } j \,|\, \mathbf{e}) \\ &= \frac{1}{2^{n-k-1}} \sum_{j=1}^{M} \mathrm{Prob}(s_j(\mathbf{e}) \neq 0 \,|\, \mathbf{e}, j)\,. \end{aligned}$$

PROOF. The sum is exactly the weight of $S(\mathbf{e})$. The number of entries 0 in $S(\mathbf{e})$ is the cardinality of $\mathbf{e}^\perp \cap C^\perp$, and so is $M = 2^{n-k}$ if $\mathbf{e} \in C$ and is $M/2 = 2^{n-k-1}$ if $\mathbf{e} \notin C$. Therefore $\mathrm{w_H}(S(\mathbf{e})) \neq 0$ if and only if $\mathrm{w_H}(S(\mathbf{e})) = 2^{n-k-1}$. □

From the lemma we get

$$\begin{aligned} P_D &= \mathrm{Prob}(S(\mathbf{e}) \neq 0) \\ &= \sum_{\mathbf{e}\in\mathbb{F}_2^n} \mathrm{Prob}(\mathbf{e})\mathrm{Prob}(S(\mathbf{e}) \neq 0 \,|\, \mathbf{e}) \\ &= \sum_{\mathbf{e}\in\mathbb{F}_2^n} \mathrm{Prob}(\mathbf{e}) \frac{1}{2^{n-k-1}} \sum_{j=1}^{M} \mathrm{Prob}(s_j(\mathbf{e}) \neq 0 \,|\, \mathbf{e}, j) \\ &= \frac{1}{2^{n-k-1}} \sum_{j=1}^{M} \sum_{\mathbf{e}\in\mathbb{F}_2^n} \mathrm{Prob}(\mathbf{e})\mathrm{Prob}(s_j(\mathbf{e}) \neq 0 \,|\, \mathbf{e}, j) \\ &= \frac{1}{2^{n-k-1}} \sum_{j=1}^{M} \mathrm{Prob}(s_j(\mathbf{e}) \neq 0 \,|\, j) \end{aligned}$$

Therefore of interest is

(9.2.3) LEMMA. *For* $\mathrm{w_H}(\mathbf{h}_j) = w_j$,

$$\begin{aligned} \mathrm{Prob}(s_j(\mathbf{e}) \neq 0 \,|\, j) &= \sum_{\substack{\mathrm{odd} \\ i=0}}^{w_j} \binom{w_j}{i} q^{w_j - i} p^i \\ &= (1 - (q-p)^{w_j})/2 \,. \end{aligned}$$

PROOF. Let $l_1, \ldots, l_{w_j}$ be the nonzero coordinate positions of $\mathbf{h}_j$. Then $s_j(\mathbf{e}) = \mathbf{h}_j \cdot \mathbf{e} \neq 0$ if and only if there are an odd number of 1's among the positions $\mathbf{e}_{l_i}$ for $i = 1, \ldots, w_j$. This gives the first equality. The rest follows from Lemma 9.2.4 below, as $q + p = 1$. □

(9.2.4) LEMMA. (1) $\sum_{i=0}^{w} \binom{w}{i} a^{w-i} b^i = (a+b)^w$.

(2) $\sum_{i=0}^{w} \binom{w}{i} (-1)^i a^{w-i} b^i = (a-b)^w$.

(3) $\sum_{\mathrm{odd}\ i=0}^{w} \binom{w}{i} a^{w-i} b^i = ((a+b)^w - (a-b)^w)/2$. □

Lemma 9.2.3 and the previous calculation now give

$$\begin{aligned}
P_R &= 1 - P_D \\
&= 1 - \left(\frac{1}{2^{n-k-1}} \sum_{j=1}^{M} \mathrm{Prob}(s_j(\mathbf{e}) \neq 0 \,|\, j) \right) \\
&= 1 - \left(\frac{1}{2^{n-k-1}} \sum_{j=1}^{M} (1 - (q-p)^{w_j})/2 \right) \\
&= 1 - \left(\frac{1}{2^{n-k}} \sum_{j=1}^{M} (1 - (q-p)^{w_j}) \right) \\
&= 1 - \frac{1}{2^{n-k}} \sum_{j=1}^{M} 1 + \frac{1}{2^{n-k}} \sum_{j=1}^{M} (q-p)^{w_j} \\
&= \frac{1}{2^{n-k}} \sum_{j=1}^{M} (q-p)^{w_j} \\
&= \frac{1}{2^{n-k}} \sum_{i=0}^{n} c_i^{\perp} (q-p)^i \,,
\end{aligned}$$

where $\sum_{i=0}^{n} c_i^{\perp} z^i = \mathrm{W}_{C^{\perp}}(z)$.

Comparing this with Proposition 9.2.1, we obtain

(9.2.5) PROPOSITION. $\sum_{i=0}^{n} c_i \, q^{n-i} p^i = P_R = \frac{1}{2^{n-k}} \sum_{i=0}^{n} c_i^{\perp} (q-p)^i$. □

PROOF OF MACWILLIAMS' THEOREM 9.1.1 (BINARY CASE):
In the equation of the proposition, replace p by $\frac{z}{1+z}$ and $q = 1 - p$ by $\frac{1}{1+z}$ to get

$$\sum_{i=0}^{n} c_i \left(\frac{1}{1+z} \right)^{n-i} \left(\frac{z}{1+z} \right)^{i} = \frac{1}{(1+z)^n} \sum_{i=0}^{n} c_i \, z^i \frac{1}{2^{n-k}} \sum_{i=0}^{n} c_i^{\perp} \left(\frac{1-z}{1+z} \right)^{i} ,$$

hence

$$\sum_{i=0}^{n} c_i \, z^i = \frac{1}{2^{n-k}} \sum_{i=0}^{n} c_i^{\perp} (1+z)^{n-i} (1-z)^i \,.$$

These two polynomial functions are equal when evaluated at any $0 \leq p < 1$, hence for all $z \geq 0$. We conclude that the equality is still valid in the polynomial ring $\mathbb{Q}[z]$. This gives a first proof of MacWilliams' Theorem 9.1.1 in the binary case. □

REMARK. The full version of MacWilliams' Theorem 9.1.1 for linear codes over $\mathbb{F}_s$ can be proven with exactly the same approach, evaluating in two ways

the performance of error detection on the $s\mathrm{SC}(p)$. A proof of MacWilliams' Theorem in full generality is given below in Theorem 9.4.8(2).

Next we consider performance at the other end of the decoding spectrum—maximum likelihood decoding for error correction. The weight enumerator of a linear code can still be used to help us bound the probability of decoding falsehood $P_E = P_C(\mathbf{MLD})$.

(9.2.6) THEOREM. *When decoding the binary linear code C on the* $\mathrm{BSC}(p)$ *(with $p \le \frac{1}{2}$) under* **MLD**, *we have*

$$P_C(\mathbf{MLD}) \le \sum_{w=1}^{n} c_w \, E_w \,,$$

where

$$E_w = \sum_{i=\lceil w/2 \rceil}^{w} \binom{w}{i} p^i (1-p)^{w-i} \,.$$

In particular

$$P_C(\mathbf{MLD}) \le \mathrm{W}_C\Big(2\sqrt{p(1-p)}\Big) - 1 \,.$$

PROOF. For a given nonzero codeword $\mathbf{x}$ of weight w, E_w is the probability that the error vector $\mathbf{e}$ is at least as close to $\mathbf{x}$ as it is to $\mathbf{0}$. This must be the case if, when decoding $\mathbf{r} = \mathbf{c} + \mathbf{e}$, **MLD** incorrectly prefers $\mathbf{c} + \mathbf{x}$ to $\mathbf{c} + \mathbf{0} = \mathbf{c}$. This gives the first bound on $P_C(\mathbf{MLD})$. (It is very unlikely to be tight, since a given $\mathbf{e}$ might be closer to several codewords than it is to $\mathbf{0}$.)

As $p \le \frac{1}{2}$, we have

$$\begin{aligned} E_w = \sum_{i=\lceil w/2 \rceil}^{w} \binom{w}{i} p^i (1-p)^{w-i} &\le p^{w/2}(1-p)^{w/2} \sum_{i=\lceil w/2 \rceil}^{w} \binom{w}{i} \\ &\le p^{w/2}(1-p)^{w/2} \sum_{i=1}^{w} \binom{w}{i} \\ &= p^{w/2}(1-p)^{w/2} 2^w \\ &= \Big(2\sqrt{p(1-p)}\Big)^w \,. \end{aligned}$$

Therefore

$$P_C(\mathbf{MLD}) \le \sum_{w=1}^{n} c_w \, E_w \le \sum_{w=1}^{n} c_w \, \Big(2\sqrt{p(1-p)}\Big)^w = \mathrm{W}_C\Big(2\sqrt{p(1-p)}\Big) - 1,$$

as desired. □

This theorem is an example of the Union Bound, and our treatment follows McEliece and Van Tilborg.

9.3 Delsarte's Theorem and bounds

We use a version of the Plotkin Bound to prove a "nonlinear MacWilliams' Theorem," due originally to Delsarte. Delsarte's Theorem (9.1.2, 9.3.5, 9.4.8(1)) then leads to other important bounds.

For integers m, n, s with $0 \le m \le n$ and $s \ge 2$, define the s-ary *Krawtchouk polynomial* Krawtchouk polynomial

$$\mathrm{K}_m(x; n, s) = \sum_{j=0}^{m} (-1)^j \binom{x}{j} \binom{n-x}{m-j} (s-1)^{m-j} ,$$

where, by definition,

$$\binom{x}{j} = \frac{x(x-1)\cdots(x-j+1)}{j!} ,$$

for $x \in \mathbb{R}$. For fixed m, n, s, the Krawtchouk polynomial $\mathrm{K}_m(x; n, s)$ has degree (at most) m in x. In particular, it is uniquely determined (using, say, Lagrange interpolation) by its values at the integers $i \in \{0, 1, \ldots, n\}$. Indeed its degree in x is exactly m, since the coefficient of x^m is

$$\sum_{j=0}^{m} (-1)^j \frac{1^j}{j!} \frac{(-1)^{m-j}}{(m-j)!} (s-1)^{m-j} = \frac{(-1)^m}{m!} \sum_{j=0}^{m} \binom{m}{j} (s-1)^{m-j} = \frac{(-s)^m}{m!} .$$

For us, the point of introduction to these interesting polynomials is

(9.3.1) PROPOSITION. *The Krawtchouk polynomial $\mathrm{K}_m(x; n, s)$ has degree m in x. For $i \in \{0, 1, \ldots, n\}$, $\mathrm{K}_m(i; n, s)$ is the coefficient of z^m in*

$$(1 + (s-1)z)^{n-i}(1-z)^i .$$

PROOF. The first remark was proven above. Calculating the convolution, we see that the coefficient of z^m in this product is

$$\sum_{j=0}^{m} \left(\binom{n-i}{m-j} (s-1)^{m-j} z^{m-j} \right) \left(\binom{i}{j} (-1)^j z^j \right) . \qquad \square$$

(9.3.2) COROLLARY. (1) $\mathrm{K}_0(i; n, s) = 1$.
(2) $\mathrm{K}_1(i; n, s) = (n-i)(s-1) - i = (s-1)n - si$.
(3) $\mathrm{K}_m(0; n, s) = (s-1)^n \binom{n}{m}$. $\square$

These could also be calculated directly.

(9.3.3) COROLLARY. *For $1 \le m \le n$ and $1 \le i \le n$, we have the recursion*

$$\mathrm{K}_m(i; n, s) = \mathrm{K}_m(i-1; n, s) - \mathrm{K}_{m-1}(i-1; n, s) - (s-1)\mathrm{K}_{m-1}(i; n, s) .$$

PROOF. If we evaluate the coefficient of z^m on both sides of

$$((1+(s-1)z)^{n-i}(1-z)^i)(1+(s-1)z) = ((1+(s-1)z)^{n-(i-1)}(1-z)^{i-1})(1-z)\,,$$

then we find

$$\mathrm{K}_m(i;n,s) + (s-1)\mathrm{K}_{m-1}(i;n,s) = \mathrm{K}_m(i-1;n,s) - \mathrm{K}_{m-1}(i-1;n,s)\,. \qquad \square$$

Corollary 9.3.3 gives an easy recursive method for calculating the Krawtchouk coefficients, with Corollary 9.3.2(1) and (3) providing initialization.

The proposition allows us to reformulate MacWilliams' Theorem as

(9.3.4) THEOREM. (MACWILLIAMS' THEOREM IN KRAWTCHOUK FORM.) *Let A and B be $\mathbb{F}_s$-linear codes of length n with $B = A^\perp$. Set $\mathrm{W}_A(z) = \sum_{i=0}^n a_i\, z^i$ and $\mathrm{W}_B(z) = \sum_{i=0}^n b_i\, z^i$. Then*

$$|A|^{-1} \sum_{i=0}^{n} \mathrm{K}_m(i;n,s) a_i = b_m\,.$$

PROOF. Set $A = C^\perp$ and $B = C$ in MacWilliams' Theorem 9.1.1. Then b_m is the coefficient of z^m in

$$\mathrm{W}_B(z) = |A|^{-1} \sum_{i=0}^{n} a_i (1+(s-1)z)^{n-i}(1-z)^i\,,$$

and the result follows from Proposition 9.3.1. $\square$

We will prove Delsarte's Theorem 9.1.2 in its Krawtchouk form:

(9.3.5) THEOREM. (DELSARTE'S THEOREM IN KRAWTCHOUK FORM.) *Let A be a code of length n over an alphabet of size s, and set $\mathrm{W}_A(z) = \sum_{i=0}^n a_i\, z^i$. Then, for $0 \le m \le n$,*

$$\sum_{i=0}^{n} \mathrm{K}_m(i;n,s)\, a_i \ge 0\,.$$

In view of Theorem 9.3.4, Delsarte's Theorem can be thought of as a "nonlinear" version of MacWilliams' Theorem. Our proof here of Delsarte's Theorem follows Simonis and DeVroedt (1991). For linear codes A we also recover MacWilliams' Theorem (in its Krawtchouk form, Theorem 9.3.4) in the process, giving us a second proof of that result.

Let A be a code of length n with size $|A| = M$, and let $\mathrm{W}_A(z) = \sum_{i=0}^n a_i\, z^i$ be its distance enumerator. In the next lemma s is arbitrary, but after that we will restrict our attention again to the binary case $s = 2$. As before, this restriction is only for the sake of clarity. The arguments readily extend to larger alphabets. (See Theorem 9.4.8(1) below for the general case.)

(9.3.6) LEMMA. (1) $\sum_{i=0}^n a_i = M$.

(2) $M \sum_{i=0}^n i\, a_i = \sum_{\mathbf{c},\mathbf{d}\in A} \mathrm{d_H}(\mathbf{c},\mathbf{d})\,.$

PROOF. We have

$$\mathrm{W}_A(z) = M^{-1} \sum_{\mathbf{c},\mathbf{d}\in A} z^{\mathrm{d_H}(\mathbf{c},\mathbf{d})} = \sum_{i=0}^{n} a_i\, z^i\,;$$

so

$$\mathrm{W}_A(1) = M^{-1} \sum_{\mathbf{c},\mathbf{d}\in A} 1^{\mathrm{d_H}(\mathbf{c},\mathbf{d})} = \sum_{i=0}^{n} a_i\,,$$

giving (1). Similarly

$$\mathrm{W}_A(1)' = M^{-1} \sum_{\mathbf{c},\mathbf{d}\in A} \mathrm{d_H}(\mathbf{c},\mathbf{d})\, 1^{\mathrm{d_H}(\mathbf{c},\mathbf{d})-1} = \sum_{i=0}^{n} i\, a_i\,,$$

giving (2). □

Again direct arguments are available. The given proof of the lemma illustrates how standard generating function methods can be used with weight and distance enumerators.

Lemma 9.3.6(1) is a strong form of the 0'th Delsarte inequality:

$$\sum_{i=0}^{n} \mathrm{K}_0(i;n,s)\, a_i = \sum_{i=0}^{n} 1 \cdot a_i = M \geq 0\,.$$

For linear A, this could be phrased as $\sum_{i=0}^{n} \mathrm{K}_0(i;n,s)\, a_i = Mb_0$, where $b_0 = 1$ is the number of words of weight 0 in $A^\perp$.

At this point, we assume additionally that A is a binary code.

(9.3.7) LEMMA. (FIRST BINARY DELSARTE INEQUALITY.) *We have*

$$\sum_{i=0}^{n} \mathrm{K}_1(i;n,2)\, a_i = \sum_{i=0}^{n} (n-2i) a_i \geq 0\,.$$

Indeed, if A is binary and linear, then this sum is Mb_1, where b_1 is the number of words of weight 1 in $A^\perp$.

PROOF. Let G be an $M \times n$ matrix whose rows are the codewords of A, and let w_j be the weight of the j'th column of G. In Lemma 9.3.6

$$M \sum_{i=0}^{n} i\, a_i = \sum_{\mathbf{c},\mathbf{d}\in A} \mathrm{d_H}(\mathbf{c},\mathbf{d})$$

effectively counts pairwise distances in A by examining G row-by-row. To count instead by columns, observe that in column j a 0 of row $\mathbf{x}$ and 1 of row $\mathbf{y}$ contribute twice to the sum, once for each of $\mathrm{d_H}(\mathbf{x},\mathbf{y})$ and $\mathrm{d_H}(\mathbf{y},\mathbf{x})$. Thus

$$\sum_{\mathbf{c},\mathbf{d}\in A} \mathrm{d_H}(\mathbf{c},\mathbf{d}) = 2 \sum_{j=1}^{n} w_j (M - w_j)\,.$$

Therefore

$$\begin{aligned}\sum_{i=0}^{n} i\,a_i &= 2M^{-1}\sum_{j=1}^{n} w_j(M-w_j)\\ &\le 2M^{-1}\sum_{j=1}^{n}\frac{M^2}{4}\\ &= \frac{n}{2}M\\ &= \frac{n}{2}\sum_{i=0}^{n} a_i\,,\end{aligned}$$

and so

$$\begin{aligned}0 &\le 2\left(\frac{n}{2}\sum_{i=0}^{n} a_i - \sum_{i=0}^{n} i\,a_i\right)\\ &= \sum_{i=0}^{n}(n-2i)a_i\,.\end{aligned}$$

This proves the first Delsarte inequality.

If A is linear, then the various w_j are either 0 or $M/2$. Indeed w_j is 0 only when there is in $A^\perp$ a word of weight 1 whose nonzero entry is at position j, the number of such positions being b_1. Therefore

$$\begin{aligned}\sum_{i=0}^{n} i\,a_i &= 2M^{-1}\sum_{j=1}^{n} w_j(M-w_j)\\ &= (n-b_1)M/2\end{aligned}$$

and

$$\sum_{i=0}^{n}(n-2i)a_i = nM-(n-b_1)M = b_1M\,. \qquad \square$$

(9.3.8) Corollary. (Binary Plotkin bound.) *If A is a binary code with minimum distance d and length $n < 2d$, then*

$$|A| \le \frac{2d}{2d-n}\,.$$

PROOF. The first Delsarte inequality yields

$$\begin{aligned} 0 &\leq \sum_{i=0}^{n}(n-2i)a_i \\ &= n+\sum_{i=d}^{n}(n-2i)a_i \\ &\leq n+(n-2d)\sum_{i=d}^{n}a_i \\ &= n+(n-2d)(|A|-1) \\ &= n-(n-2d)+(n-2d)|A| \\ &= 2d+(n-2d)|A|\,. \end{aligned}$$

This implies $(2d-n)|A| \leq 2d$ and so proves the Plotkin bound. □

In Lemmas 9.3.6(1) and 9.3.7 we have the Delsarte inequalities for $m = 0, 1$ (and the corresponding linear interpretation). We next attack the m'th Delsarte inequality.

For a fixed m, consider a new code $A^{[m]} = \{\, \mathbf{c}^{[m]} \mid \mathbf{c} \in C \,\}$ of length $N = \binom{n}{m}$. Starting with a codeword $\mathbf{c} \in A$, we construct the codeword $\mathbf{c}^{[m]} \in A^{[m]}$, whose entries $c_J^{[m]}$ are indexed by the m-subsets of $\{1, \ldots, n\}$, and are given by

$$c_J^{[m]} = \sum_{j \in J} c_j\,,$$

for each m-subset J.

(9.3.9) LEMMA.
(1) *If* $\mathbf{x}+\mathbf{y}=\mathbf{z}$, *then* $\mathbf{x}^{[m]}+\mathbf{y}^{[m]}=\mathbf{z}^{[m]}$.
(2) *If* $\mathrm{w_H}(\mathbf{x})=i$, *then* $\mathrm{w_H}(\mathbf{x}^{[m]}) = \sum_{j\,\mathrm{odd}} \binom{i}{j}\binom{n-i}{m-j}$.

PROOF. The first part is immediate. For the second part, let I be the subset of $\{1, \ldots, n\}$ whose positions hold the 1's of $\mathbf{x}$. Then the entry $x_J^{[m]}$ is 0 or 1 as $|I \cap J| = j$ is even or odd. For a fixed j, there are $\binom{i}{j}$ choices for $I \cap J$ and $\binom{n-i}{m-j}$ ways of completing this choice to an appropriate m-subset of $\{1, \ldots, n\}$. □

A particular consequence of Lemma 9.3.9 is that $A^{[m]}$ has the same number of codewords as A. The weight in (2) depends only on the original weight i, so we can define

$$w^{[m]}(i) = \sum_{\substack{j=0 \\ \mathrm{odd}}}^{m} \binom{i}{j}\binom{n-i}{m-j}\,.$$

If $\mathrm{d_H}(\mathbf{x},\mathbf{y}) = i$, then $\mathrm{d_H}(\mathbf{x}^{[m]},\mathbf{y}^{[m]}) = w^{[m]}(i)$. Therefore, for $\mathrm{W}_{A^{[m]}}(z) = \sum_r a_r^{[m]} z^r$, we have

$$a_r^{[m]} = \sum_{w^{[m]}(i)=r} a_i \,.$$

The definition of $w^{[m]}(i)$ is to be compared with the well-known binomial identity

$$\binom{n}{m} = \sum_{j=0}^{m} \binom{i}{j}\binom{n-i}{m-j},$$

proved by counting m-subsets of a two-colored n set according to how many elements of each color have been selected.

Proof of Delsarte's Theorem 9.3.5 (Binary Case):
By the first Delsarte inequality for $A^{[m]}$, we have

$$\begin{aligned}
0 &\le \sum_{r=0}^{N}(N-2r)a_r^{[m]} \\
&= \sum_{r=0}^{N}(N-2r)\sum_{w^{[m]}(i)=r} a_i \\
&= \sum_{r=0}^{N}\sum_{w^{[m]}(i)=r}(N-2w^{[m]}(i))a_i \\
&= \sum_{i=0}^{n}\left(\binom{n}{m} - 2w^{[m]}(i)\right)a_i \\
&= \sum_{i=0}^{n}\left(\left(\sum_{j=0}^{m}\binom{i}{j}\binom{n-i}{m-j}\right) - 2\left(\sum_{\substack{\text{odd}\\ j=0}}^{m}\binom{i}{j}\binom{n-i}{m-j}\right)\right)a_i \\
&= \sum_{i=0}^{n}\left(\sum_{j=0}^{m}(-1)^j\binom{i}{j}\binom{n-i}{m-j}\right)a_i \\
&= \sum_{i=0}^{n}\mathrm{K}_m(i;n,2)\,a_i \,. \qquad \square
\end{aligned}$$

In the case that A is linear, $A^{[m]}$ is also linear by Lemma 9.3.9(1). The sum counts $|A^{[m]}| = |A|$ times the number of weight 1 words in ${A^{[m]}}^{\perp}$. Let $\mathbf{x}$ be a word of weight 1 in $\mathbb{F}_2^N$, and suppose its unique nonzero entry is in position J, where J is an m-subset of $\{1,\ldots,n\}$. Then $\mathbf{x}$ will be in ${A^{[m]}}^{\perp}$ when all codewords of $A^{[m]}$ have J-entry 0. This happens when every codeword $\mathbf{c}$ of A has an even number of 1's in the positions of J. That is, when the word of $\mathbb{F}_2^n$ with 1's in the positions of J belongs to $A^{\perp}$. Therefore words of weight 1 in

$A^{[m]^\perp}$ correspond exactly to words of weight m in $A^\perp$, and we have recovered MacWilliams' Theorem in its Krawtchouk form 9.3.4.

(9.3.10) THEOREM. (LINEAR PROGRAMMING BOUND.) *Let A be a code of length n over an alphabet of size s with $\mathrm{d}_{\min}(A) \geq d$. Then*

$$|A| \leq \max\left\{ \sum_{i=0}^{n} A_i \;\middle|\; A_0 = 1,\ A_i = 0,\ 1 \leq i \leq d,\ A_m \geq 0\,,\ \sum_{i=0}^{n} A_i \mathrm{K}_m(i;n,s) \geq 0,\ 1 \leq m \leq n \right\}.$$

If $s = 2$ and d is even, then we can also assume that $A_i = 0$, for all odd i.

PROOF. For $\mathrm{W}_A(z) = \sum_{i=0}^{n} a_i\, z^i$, the choice $A_i = a_i$ solves all the inequalities by Delsarte's Theorem 9.3.5. It has $\sum_{i=0}^{n} A_i = |A|$, by Lemma 9.3.6(1).

If $s = 2$ and d is even, then when we first puncture and then extend A, the resulting code A^* (even in the nonlinear case) has $|A^*| = |A|$ and $\mathrm{d}_{\min}(A^*) \geq d$. Furthermore, the coefficients a_i^* of $\mathrm{W}_{A^*}(z)$ satisfy the same inequalities as the a_i and additionally have $a_i^* = 0$, for odd i. □

As our proof of the Plotkin bound in Corollary 9.3.8 suggests, these methods can be used to find general bounds; but new bounds of this type are very difficult to prove. On the other hand, the linear programming bound is remarkably effective in specific cases, as the following example suggests.

EXAMPLE. Let C be a binary linear code of length 8 with $\mathrm{d}_{\min}(C) \geq 4$. We prove that $|C| \leq 16$ (the extended Hamming code providing an example that has exactly 16 codewords).

We have $A_0 = 1$, $A_2 = A_3 = A_5 = A_7 = 0$, and also $A_4 \geq 0$, $A_6 \geq 0$, and $A_8 \geq 0$. The Delsarte inequalities for m and $8 - m$ are equal under these circumstances, so only $m = 1, 2, 3, 4$ can be of help. In fact, those for $m = 1$ and $m = 2$ are all we need. We have (using Corollaries 9.3.2 and 9.3.3)

$$0 \leq \sum_{i=0}^{8} A_i \mathrm{K}_1(i;n,s) = 8 + 0A_4 - 4A_6 - 8A_8\,;$$

$$0 \leq \sum_{i=0}^{8} A_i \mathrm{K}_2(i;n,s) = 28 - 4A_4 + 4A_6 + 28A_8\,.$$

The first inequality gives

$$A_6 \leq 2 - 2A_8,$$

so that in particular $A_8 \leq 1$. Adding the two inequalities produces

$$A_4 \leq 9 + 5A_8\,.$$

Therefore

$$\begin{aligned} |C| &\leq \sum_{i=0}^{8} A_8 \\ &= A_0 + A_4 + A_6 + A_8 \\ &\leq 1 + (9 + 5A_8) + (2 - 2A_8) + A_8 \\ &= 12 + 4A_8 \\ &\leq 16\,, \end{aligned}$$

as claimed. Indeed, in order for the sum to be 16 we must have $A_8 = 1$, in which case $0 \leq A_6 \leq 2 - 2A_8$ yields $A_6 = 0$. Also $A_4 \leq 9 + 5A_8 = 14$. As

$$\begin{aligned} \sum_{i=0}^{8} A_8 &= A_0 + A_4 + A_6 + A_8 \\ &\leq 1 + 14 + 0 + 1 \\ &\leq 16\,, \end{aligned}$$

there is a unique solution to the linear programming problem, namely

$$A_0 = 1,\ A_1 = A_2 = A_3 = A_5 = A_6 = A_7 = 0,\ A_4 = 14,\ A_8 = 1\,.$$

This corresponds to the weight enumerator $1 + 14z^4 + z^8$ for the extended binary Hamming code of length 8.

Of course this toy example could also be handled by more combinatorial methods, but the linear programming approach has better scaling properties. For instance, codes with lengths in the teens can still be handled very easily, while combinatorial approaches can already at that point require extensive case-by-case analysis.

9.4 Lloyd's theorem and perfect codes

We present MacWilliams' theorem a third time, Delsarte's theorem a second time, and Lloyd's theorem a first time.

In this section, we will be concerned with codes defined over a finite alphabet F that has the structure of a commutative ring with a multiplicative identity 1. Our main examples are fields $\mathbb{F}_s$ and rings of modular integers $\mathbb{Z}_s = \mathbb{Z} \pmod{s}$. It is important to realize that any code over a finite alphabet of s letters can be viewed as a code over $\mathbb{Z}_s$ (merely by assigning each letter a unique value from $\mathbb{Z}_s$). In particular, our proof here of Delsarte's Theorem in Theorem 9.4.8(1) does not suffer any loss of generality by restricting attention to codes over $\mathbb{Z}_s$.

In this situation we have an additive structure on F^n with identity element $\mathbf{0}$, and we have natural scalar multiplication given by

$$r(a_1, \ldots, a_j, \ldots, a_n) = (ra_1, \ldots, ra_j, \ldots, ra_n)\,,$$

for arbitrary $r \in F$. Therefore we can still talk about $r\mathbf{a} + t\mathbf{b}$, $\mathbf{c} \cdot \mathbf{d}$, $\mathrm{w_H}(\mathbf{e})$, and so forth.

F-linear code

An *F-linear code* of length n will be, as before, any nonempty subset C of F^n that is closed under addition and scalar multiplication. The code $C^\perp$ dual to C is also defined as before:

$$C^\perp = \{\, \mathbf{v} \in F^n \mid \mathbf{v} \cdot \mathbf{c} = 0, \text{ for all } \mathbf{c} \in C \,\},$$

and is F-linear even if C is not.

linear character

A *linear character* χ of $(F, +)$ is a map $\chi\colon F \longrightarrow \mathbb{C}^*$ with

$$\chi(a+b) = \chi(a)\chi(b) \quad \text{for all} \quad a, b \in F\,.$$

For finite F the image of χ will be in the roots of unity, and we must have

$$\chi(0) = 1 \text{ and } \chi(-a) = \chi(a)^{-1} = \overline{\chi(a)}\,.$$

A basic example is the trivial character $1_F(a) = 1$, for all $a \in F$. Later we will make a specific choice for χ, but for the moment χ can be any linear character of $(F, +)$.

We next define, for $\mathbf{u}, \mathbf{v} \in V = F^n$, the related notation

$$\chi(\mathbf{u}|\mathbf{v}) = \chi(\mathbf{u} \cdot \mathbf{v}) = \chi\left(\sum_{i=1}^{n} u_i v_i\right) = \prod_{i=1}^{n} \chi(u_i v_i)\,.$$

For $n = 1$, $\chi(u|v) = \chi(uv)$; and the first two parts of the next lemma are consequences of the commutativity of F, while the third part is just a restatement of the defining property for a character. The general case follows directly.

(9.4.1) LEMMA. (1) $\chi(\mathbf{u}|\mathbf{v}) = \chi(\mathbf{v}|\mathbf{u})$;
(2) *for $a \in F$,* $\chi(\mathbf{u}|a\mathbf{v}) = \chi(a\mathbf{u}|\mathbf{v}) = \chi(a|\mathbf{u} \cdot \mathbf{v})$;
(3) $\chi(\mathbf{a}+\mathbf{b}|\mathbf{v}) = \chi(\mathbf{a}|\mathbf{v})\chi(\mathbf{b}|\mathbf{v})$. □

We thus see that $\chi(\cdot|\cdot)$ is symmetric and biadditive on F^n.

More generally, for subsets A, B of V, we define

$$\chi(A|B) = \sum_{\mathbf{a}\in A, \mathbf{b}\in B} \chi(\mathbf{a}|\mathbf{b})\,.$$

We have before encountered the notation

$$A + B = \{\, \mathbf{a} + \mathbf{b} \mid \mathbf{a} \in A\,, \mathbf{b} \in B \,\},$$

and we further write $A \oplus B$ for $A + B$ if every element of $A + B$ has a unique expression as $\mathbf{a} + \mathbf{b}$, for $\mathbf{a} \in A$ and $\mathbf{b} \in B$.

The defining property of a character χ and biadditivity then extend to

(9.4.2) LEMMA. $\chi(A \oplus B|\mathbf{v}) = \chi(A|\mathbf{v})\chi(B|\mathbf{v})$

PROOF.

$$\begin{aligned}\chi(A \oplus B|\mathbf{v}) &= \sum_{\mathbf{a}\in A,\mathbf{b}\in B} \chi(\mathbf{a}+\mathbf{b}|\mathbf{v}) \\ &= \sum_{\mathbf{a}\in A,\mathbf{b}\in B} \chi(\mathbf{a}|\mathbf{v})\chi(\mathbf{b}|\mathbf{v}) \\ &= \sum_{\mathbf{a}\in A} \chi(\mathbf{a}|\mathbf{v}) \sum_{\mathbf{b}\in B} \chi(\mathbf{b}|\mathbf{v}) \\ &= \chi(A|\mathbf{v})\chi(B|\mathbf{v}) \qquad \square\end{aligned}$$

REMARK. The lemma and proof remain valid for all A and B if we view $A+B$ as a multiset, keeping track of the number of different ways each element can be written as $\mathbf{a}+\mathbf{b}$. This is the "group algebra" approach, which can be very effective.

The next two lemmas are elementary but fundamental for what we are doing in this section.

(9.4.3) LEMMA. *Consider the property:*

> (**ND**) *F is a commutative ring with identity, and $(F,+)$ possesses a linear character χ such that, for each $0 \neq v \in F$, there is an $a_v \in F$ with $\chi(a_v v) \neq 1$.*

Then $\mathbb{F}_s$ and $\mathbb{Z}_s$ both have the property (**ND**).

PROOF. For $F = \mathbb{Z}_s$, let ζ be a primitive s'th root of 1 in $\mathbb{C}$. (That is, $\zeta^s = 1$ but $\zeta^i \neq 1$, for $0 < i < s$.) Then $\chi(i) = \zeta^i$ has the desired properties with respect to $a_v = 1$, for all $v \neq 0$.

Let $F = \mathbb{F}_s$ with $s = p^d$, a power of the prime p. In fact, every nontrivial linear character χ has the desired property. We give a concrete construction. Let ζ be a primitive p'th root of 1. Realize F as $\mathbb{F}_p[x] \pmod{m(x)}$ for an irreducible polynomial $m(x)$ of degree d in $\mathbb{F}_p[x]$. Each element of F is represented by a unique polynomial $f(x) \in \mathbb{F}_p[x]$ of degree less than d. Then $\chi(f(x)) = \zeta^{f(0)}$ has the desired properties. (Each $f(0)$ is in $\mathbb{F}_p = \mathbb{Z}_p$ and can be thought of as an integer.) For each $v \neq 0$, we can choose $a_v = v^{-1}$. $\square$

If we view $\chi(\cdot|\cdot)$ as a symmetric, biadditive form on F^n, then Property (**ND**) of the lemma says that, at least for F^1, the form is nondegenerate:

$$0 = \{\, v \in F^1 \mid \chi(a|v) = 1, \text{ for all } a \in F^1 \,\}.$$

The next lemma continues this line of thought.

From now on we will assume that the alphabet F has a character χ of $(F,+)$ satisfying Property (**ND**) of Lemma 9.4.3. We choose and fix such a character χ. Our main examples remain $\mathbb{Z}_s$ and $\mathbb{F}_s$.

(9.4.4) LEMMA. *Let* $\mathbf{v} \in V$.

(1) *Always*

$$\begin{aligned} \chi(V|\mathbf{v}) &= |V| \text{ if } \mathbf{v} = 0 \\ &= 0 \text{ otherwise.} \end{aligned}$$

(2) *If* W *is an* F*-linear code in* V*, then*

$$\begin{aligned} \chi(W|\mathbf{v}) &= |W| \text{ if } \mathbf{v} \in W^{\perp} \\ &= 0 \text{ otherwise.} \end{aligned}$$

PROOF. If $\mathbf{0} \neq \mathbf{v} \in V$, then by Property (**ND**) of Lemma 9.4.3 there is a word $\mathbf{a} \in V$ with weight 1 and $\mathbf{a} \cdot \mathbf{v} \neq 0$. Therefore $V^{\perp} = \{\mathbf{0}\}$, and (1) is a special case of (2).

For (2), if $\mathbf{v} \in W^{\perp}$, then

$$\chi(W|\mathbf{v}) = \sum_{\mathbf{w} \in W} 1 = |W| \,.$$

Therefore to complete (2) and the lemma we may assume that there is a $\mathbf{w} \in W$ with $v = \mathbf{w} \cdot \mathbf{v} \neq 0$.

By Property (**ND**) of Lemma 9.4.3, there is an $a = a_v \in F$ with $\chi(av) \neq 1$. Therefore, for $\mathbf{a} = a\mathbf{w}$,

$$\chi(\mathbf{a}|\mathbf{v}) = \chi(a|\mathbf{w} \cdot \mathbf{v}) = \chi(a|v) \neq 1 \,,$$

by Lemma 9.4.1(2).

Now we have

$$\begin{aligned} \chi(W|\mathbf{v}) &= \chi(W \oplus \mathbf{a}|\mathbf{v}) \\ &= \chi(W|\mathbf{v})\chi(\mathbf{a}|\mathbf{v}) \end{aligned}$$

by Lemma 9.4.2. Therefore

$$0 = \chi(W|\mathbf{v})(\chi(\mathbf{a}|\mathbf{v}) - 1) \,,$$

and $\chi(W|\mathbf{v}) = 0$, as required. □

(9.4.5) COROLLARY. *Suppose that, for some set of constants* $\alpha_{\mathbf{u}}$*,*

$$\sum_{\mathbf{u} \in V} \alpha_{\mathbf{u}} \, \chi(\mathbf{u}|\mathbf{v}) = 0 \,,$$

for all $\mathbf{0} \neq \mathbf{v} \in V$*. Then* $\alpha_{\mathbf{u}} = \alpha$ *is constant, for all* $\mathbf{u} \in V$*.*

PROOF. By Lemma 9.4.4(1), a constant choice $\alpha_{\mathbf{u}} = \alpha$ does have the stated property. In particular, after subtracting an appropriate constant α from each coefficient, we could assume that $\sum_{\mathbf{u} \in V} \alpha_{\mathbf{u}} \, \chi(\mathbf{u}|\mathbf{v}) = 0$ holds for all $\mathbf{v}$, including $\mathbf{0}$. We do so, and then aim to prove that each $\alpha_{\mathbf{u}}$ equals 0.

For fixed but arbitrary $\mathbf{z} \in V$, we have

$$\begin{aligned} 0 &= \sum_{\mathbf{v}\in V} 0 \cdot \overline{\chi(\mathbf{z}|\mathbf{v})} \\ &= \sum_{\mathbf{v}\in V} \left(\sum_{\mathbf{u}\in V} \alpha_{\mathbf{u}}\, \chi(\mathbf{u}|\mathbf{v}) \right) \overline{\chi(\mathbf{z}|\mathbf{v})} \\ &= \sum_{\mathbf{u}\in V} \alpha_{\mathbf{u}} \left(\sum_{\mathbf{v}\in V} \chi(\mathbf{u}|\mathbf{v}) \overline{\chi(\mathbf{z}|\mathbf{v})} \right) \\ &= \sum_{\mathbf{u}\in V} \alpha_{\mathbf{u}} \sum_{\mathbf{v}\in V} \chi(\mathbf{u}-\mathbf{z}|\mathbf{v}) \\ &= \alpha_{\mathbf{z}} |V| \end{aligned}$$

by Lemma 9.4.4(1). □

(9.4.6) PROPOSITION. *For all* $\mathbf{v} \in V$ *with* $\mathrm{w_H}(\mathbf{v}) = i$,

$$\sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})} \chi(\mathbf{u}|\mathbf{v}) = (1+(s-1)z)^{n-i}(1-z)^i \,.$$

PROOF. For all $(v_1, \ldots, v_n) = \mathbf{v} \in V$, we have

$$\begin{aligned} \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})} \chi(\mathbf{u}|\mathbf{v}) &= \sum_{\mathbf{u}\in V} \prod_{j=1}^{n} z^{\mathrm{w_H}(u_j)} \chi(u_j|v_j) \\ &= \prod_{j=1}^{n} \sum_{u\in F} z^{\mathrm{w_H}(u)} \chi(u|v_j) \end{aligned}$$

by distributivity. Here

$$\sum_{u\in F} z^{\mathrm{w_H}(u)} \chi(u|v_j) = 1 + z\, \chi(F \setminus \{0\}\,|v_j)$$

which, by the case $n = 1$ of Lemma 9.4.4(1), is $1 + (s-1)z$ when $v_j = 0$ and is $1 - z$ when $v_j \neq 0$. Therefore

$$\begin{aligned} \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})} \chi(\mathbf{u}|\mathbf{v}) &= \prod_{j=1}^{n} \sum_{u\in F} z^{\mathrm{w_H}(u)} \chi(u|v_j) \\ &= (1+(s-1)z)^{n-\mathrm{w_H}(\mathbf{v})} (1-z)^{\mathrm{w_H}(\mathbf{v})} \,, \end{aligned}$$

as claimed. □

Let $Y_m = \{\, \mathbf{x} \in V \mid \mathrm{w_H}(\mathbf{x}) = m \,\}$, so that the sphere of radius e centered at $\mathbf{0}$, $S_e = \mathrm{S}_e(\mathbf{0})$, is the disjoint union of the Y_m, for $m = 1, \ldots, e$.

(9.4.7) COROLLARY. *Let* $\mathrm{w_H}(\mathbf{v}) = i$.

(1) $\chi(Y_m|\mathbf{v}) = \mathrm{K}_m(i; n, s)$,

(2) $\chi(S_e|\mathbf{v}) = \sum_{m=0}^{e} \mathrm{K}_m(i; n, s)$.

PROOF. By the proposition, $\chi(Y_m|\mathbf{v})$ is the coefficient of z^m in

$$(1 + (s-1)z)^{n-i}(1-z)^i\,.$$

By Proposition 9.3.1 this coefficient is also $\mathrm{K}_m(i; n, s)$. This gives (1), and (2) follows directly. □

(9.4.8) THEOREM. *Let A be a code in F^n with distance enumerator $\mathrm{W}_A(z) = \sum_{i=0}^{n} a_i z^i$. Define the rational numbers b_m by*

$$|A|^{-1} \sum_{i=0}^{n} a_i (1 + (s-1)z)^{n-i}(1-z)^i = \sum_{m=0}^{n} b_m z^m\,.$$

Then

(1) (DELSARTE'S THEOREM 9.1.2.) *$b_m \geq 0$, for all m. (Indeed we have $b_m = |A|^{-2} \sum_{\mathrm{w_H}(\mathbf{u})=m} |\chi(\mathbf{u}|A)|^2$.)*

(2) (MACWILLIAMS' THEOREM 9.1.1.) *If A is an F-linear code, then $\mathrm{W}_{A^\perp}(z) = \sum_{m=0}^{n} b_m z^m$.*

PROOF. We calculate

$$\sum_{\mathbf{c},\mathbf{d}\in A} \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})} \chi(\mathbf{u}|\mathbf{c}-\mathbf{d})$$

in two different ways.

By Proposition 9.4.6,

$$\begin{aligned} \sum_{\mathbf{c},\mathbf{d}\in A} \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})} \chi(\mathbf{u}|\mathbf{c}-\mathbf{d}) &= \sum_{\mathbf{c},\mathbf{d}\in A} (1 + (s-1)z)^{n-\mathrm{w_H}(\mathbf{c}-\mathbf{d})} (1+z)^{\mathrm{w_H}(\mathbf{c}-\mathbf{d})} \\ &= |A| \sum_{i=0}^{n} a_i (1 + (s-1)z)^{n-i}(1+z)^i\,, \end{aligned}$$

which is $|A|^2$ times the lefthand side of the definition.

On the other hand

$$\begin{aligned}
\sum_{\mathbf{c},\mathbf{d}\in A}\sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})}\chi(\mathbf{u}|\mathbf{c}-\mathbf{d}) &= \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})}\sum_{\mathbf{c},\mathbf{d}\in A}\chi(\mathbf{u}|\mathbf{c}-\mathbf{d}) \\
&= \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})}\sum_{\mathbf{c},\mathbf{d}\in A}\chi(\mathbf{u}|\mathbf{c})\chi(\mathbf{u}|-\mathbf{d}) \\
&= \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})}\chi(\mathbf{u}|A)\chi(\mathbf{u}|-A) \\
&= \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})}\chi(\mathbf{u}|A)\overline{\chi(\mathbf{u}|A)} \\
&= \sum_{\mathbf{u}\in V} z^{\mathrm{w_H}(\mathbf{u})}|\chi(\mathbf{u}|A)|^2 \\
&= \sum_{m=0}^{n}\left(\sum_{\mathrm{w_H}(\mathbf{u})=m}|\chi(\mathbf{u}|A)|^2\right)z^m\,.
\end{aligned}$$

We conclude that

$$|A|\sum_{i=0}^{n} a_i(1+(s-1)z)^{n-i}(1+z)^i = \sum_{m=0}^{n}\left(\sum_{\mathrm{w_H}(\mathbf{u})=m}|\chi(\mathbf{u}|A)|^2\right)z^m\,.$$

Therefore

$$b_m = |A|^{-2}\sum_{\mathrm{w_H}(\mathbf{u})=m}|\chi(\mathbf{u}|A)|^2 \geq 0\,,$$

proving Delsarte's Theorem.

Furthermore, if A is linear, then by Lemma 9.4.4(2)

$$\begin{aligned}
\chi(\mathbf{u}|A) &= |A| \text{ if } \mathbf{u}\in A^\perp \\
&= 0 \text{ otherwise.}
\end{aligned}$$

Therefore

$$\begin{aligned}
b_m &= |A|^{-2}\sum_{\mathrm{w_H}(\mathbf{u})=m}|\chi(\mathbf{u}|A)|^2 \\
&= |A|^{-2}\sum_{\substack{\mathrm{w_H}(u)=m\\ \mathbf{u}\in A^\perp}}|A|^2 \\
&= |\{\,\mathbf{u}\mid \mathrm{w_H}(\mathbf{u})=m, \mathbf{u}\in A^\perp\,\}|\,,
\end{aligned}$$

proving MacWilliams' Theorem. □

This proof of MacWilliams' Theorem is essentially one of the two given in the original paper (and thesis) of MacWilliams for linear codes over fields. Its modification to prove Delsarte's Theorem as well is due to Welch, McEliece, and Rumsey (1974).

Here we have proved MacWilliams' Theorem for a more general class of codes than the linear codes of Theorem 9.1.1, namely for those codes that are F-linear, where F has Property (**ND**) of Lemma 9.4.3. Many properties of linear codes over fields go over to these codes. For instance, substituting 1 into the equations of Theorem 9.4.8, we learn that, for the F-linear code A,

$$|A|^{-1}\, s^n = |A|^{-1} \sum_{i=0}^{n} a_i (1 + (s-1)1)^{n-i} (1-1)^i = \sum_{m=0}^{n} b_m 1^m = |A^\perp|\,.$$

That is, $|A||A^\perp| = |V|$, whence $A^{\perp\perp} = A$ (things that could also be proved directly).

(9.4.9) THEOREM. (LLOYD'S THEOREM.) *Let $C \subseteq F^n$ be a perfect e-error-correcting code. Then the polynomial*

$$\Psi_e(x) = \sum_{i=0}^{e} \mathrm{K}_i(x; n, s)$$

of degree e has e distinct integral roots in $\{1, \ldots, n\}$.

PROOF. The basic observation is that, since C is a perfect e-error-correcting code,

$$S_e \oplus C = V\,.$$

Therefore, by Lemma 9.4.2

$$\chi(S_e|\mathbf{v})\, \chi(C|\mathbf{v}) = \chi(V|\mathbf{v})\,,$$

for all $\mathbf{v} \in V$. As $V = S_n$, we have by Corollary 9.4.7

$$\Psi_e(x)\, \chi(C|\mathbf{v}) = \Psi_n(x)\,,$$

where $x = \mathrm{w_H}(\mathbf{v})$ and $\Psi_j(x) = \sum_{i=0}^{j} \mathrm{K}_i(x; n, s)$.

By Proposition 9.3.1, $\mathrm{K}_i(x; n, s)$ is a polynomial of degree i in x, so $\Psi_j(x)$ has degree j in x. In particular, $\Psi_n(x) = \chi(V|\mathbf{v})$ has degree n. But by Lemma 9.4.4(1) it has roots $x = 1, \ldots, n$. Therefore

$$\Psi_n(x) = c(x-1)(x-2)\cdots(x-n)\,,$$

for an appropriate constant c (which can be calculated using Corollary 9.3.2). We conclude that

$$\Psi_e(x)\, \chi(C|\mathbf{v}) = c(x-1)(x-2)\cdots(x-n)\,,$$

for $x = \mathrm{w_H}(\mathbf{v})$.

As the polynomial $\Psi_e(x)$ has degree e in x, the theorem will be proven once we can show that, for at least e values of $m \neq 0$, there are words $\mathbf{v} \in Y_m$ with $\chi(C|\mathbf{v}) \neq 0$. By Theorem 9.4.8(1), this is equivalent to proving that $|\{\, m \neq 0 \mid b_m \neq 0 \,\}| \geq e$. But this is immediate from Proposition 9.4.10 below. □

(9.4.10) PROPOSITION. *For the e-error-correcting code A with the b_m defined as in Theorem 9.4.8, we have*

$$|\{\, m \neq 0 \mid b_m \neq 0 \,\}| \geq e\,.$$

PROOF. Let $N(A) = \{\, m \neq 0 \mid b_m \neq 0 \,\}$ and $g = |N(A)|$, and assume that $g \leq e$. Define the polynomial $a(x) = \prod_{m \in N(A)}(x - m)$, of degree g (an empty product being taken as 1). Therefore $a(m) = 0$ when $m \in N(A)$, whereas $\chi(A|\mathbf{v}) = 0$ whenever $0 \neq m = \mathrm{w_H}(\mathbf{v}) \notin N(A)$, by Theorem 9.4.8(1).

As each $\mathrm{K}_i(x; n, s)$ has degree i in x (by Proposition 9.3.1), there are constants α_i (not all 0) with

$$a(x) = \sum_{i=0}^{g} \alpha_i \,\mathrm{K}_i(x; n, s)\,.$$

Using Corollary 9.4.7(1), we get, for all $\mathbf{v} \neq \mathbf{0}$,

$$\begin{aligned} 0 &= a(\mathrm{w_H}(\mathbf{v}))\chi(A|\mathbf{v}) \\ &= \left(\sum_{i=0}^{g} \alpha_i\, \chi(Y_i|\mathbf{v})\right) \chi(A|\mathbf{v}) \\ &= \sum_{i=0}^{g} \alpha_i\, \chi(Y_i \oplus A|\mathbf{v}) \\ &= \sum_{i=0}^{g} \sum_{\mathbf{y} \in Y_i, \mathbf{a} \in A} \alpha_i\, \chi(\mathbf{y} + \mathbf{a}|\mathbf{v})\,. \end{aligned}$$

From Corollary 9.4.5 we learn $\alpha_i = \alpha$ is a nonzero constant function of i and that every element $\mathbf{u} \in V$ is equal to some $\mathbf{y} + \mathbf{a}$. In particular, it must be possible to write the word $\mathbf{e}$ at distance e from a codeword $\mathbf{c}$ in the form $\mathbf{y} + \mathbf{a}$. As A is an e-error-correcting code, the only possibility is $\mathbf{e} = (\mathbf{e} - \mathbf{c}) + \mathbf{c}$, with $\mathbf{e} - \mathbf{c} \in Y_e$, hence $g \geq e$, as claimed. □

REMARKS. 1. The proposition is also due to MacWilliams and Delsarte. In MacWilliams' version for linear codes, $|\{\, m \neq 0 \mid b_m \neq 0 \,\}|$ is the number of nonzero weights in the dual code (as is evident from our proof of Theorem 9.4.8(2)).

2. We could combine Lloyd's Theorem and the proposition, with the rephrased proposition saying that equality holds if and only if A is perfect, in which case the appropriate polynomial has the appropriate roots. This might shorten the proof somewhat but also make it more mysterious.

3. Recall that the covering radius $g = \mathrm{cr}(A)$ of the code $A \subseteq F^n$ is the smallest g such that $F^n = \bigcup_{\mathbf{a} \in A} \mathrm{S}_g(\mathbf{a})$. That is, it is the smallest g with $V = S_g + A$. A more careful proof of the proposition gives

$$|\{\, m \neq 0 \mid b_m \neq 0 \,\}| \geq \mathrm{cr}(A)\,.$$

Lloyd's Theorem and the Sphere Packing Condition are the main tools used in proving nonexistence results for perfect codes and other related codes. The Sphere Packing Condition has a natural derivation in the present language:

$$|S_e|\,|C| = \chi(S_e|\mathbf{0})\chi(C|\mathbf{0}) = \chi(S_e \oplus C|\mathbf{0}) = \chi(V|\mathbf{0}) = |V|\,,$$

for the perfect e-error-correcting code C in V.

The following simple example of a nonexistence result for perfect codes is a good model for more general results of this type.

(9.4.11) THEOREM. *If C is a binary perfect 2-error-correcting code of length $n \geq 2$, then either $n = 2$ and $C = \mathbb{F}_2^2$ or $n = 5$ and $C = \{\,\mathbf{x}, \mathbf{y} \mid \mathbf{x} + \mathbf{y} = \mathbf{1}\,\}$.*

PROOF. We do this in three steps:

Step 1. *Sphere Packing Condition:* There is a positive integer r with $2 + n + n^2 = 2^{r+1}$. If $n \leq 6$, then we have one of the examples of the theorem. Therefore we can assume that $n \geq 7$, and in particular $8n < 2^{r+1}$.

By the Sphere Packing Condition we have

$$1 + n + \binom{n}{2} = 2^r\,,$$

where r is the redundancy of the code. This simplifies to $2 + n + n^2 = 2^{r+1}$. We record the first few values:

n	2	3	4	5	6
$2 + n + n^2$	8	14	22	32	44

Only $n = 2, 5$ can occur, and in these cases we easily find the examples described. Therefore we may assume from now on that $n \geq 7$, in which case

$$2 + n(7 + 1) \leq 2 + n(n + 1) = 2^{r+1}\,.$$

Step 2. *Lloyd's Theorem:* $n \equiv 3 \pmod 4$.

$$\begin{aligned}
\Psi_2(x) &= \mathrm{K}_1(x; n, 2) + \mathrm{K}_1(x; n, 2) + \mathrm{K}_2(x; n, 2) \\
&= 1 + (n - 2x) + \\
&\qquad + \left((-1)^0\binom{x}{0}\binom{n-x}{2} + (-1)^1\binom{x}{1}\binom{n-x}{1} + (-1)^2\binom{x}{2}\binom{n-x}{0}\right) \\
&= \frac{1}{2}(4x^2 - 4(n+1)x + (2 + n + n^2))
\end{aligned}$$

By *Step 1.* $2+n+n^2 = 2^{r+1}$; so if we substitute y for $2x$, then Lloyd's Theorem 9.4.9 says that the quadratic polynomial

$$y^2 - 2(n+1)y + 2^{r+1}$$

has two even integer roots in the range 2 through $2n$. Indeed

$$y^2 - 2(n+1)y + 2^{r+1} = (y - 2^a)(y - 2^b)\,,$$

for positive integers a, b with $a + b = r + 1$ and $2^a + 2^b = 2(n + 1)$.

We next claim that 2^a and 2^b are not 2 or 4. If $y = 2$ is a root, then

$$4 - 2(n+1)2 + 2^{r+1} = 0 \text{ hence } 2^{r+1} = 4n < 8n\,.$$

Similarly if $y = 4$ is a root, then

$$16 - 2(n+1)4 + 2^{r+1} = 0 \text{ hence } 2^{r+1} = 8n - 8 < 8n\,;$$

and in both cases we contradict *Step 1.*

Therefore $a, b \geq 3$, and

$$n + 1 = 2^{a-1} + 2^{b-1} \equiv 0 \pmod 4\,,$$

as desired.

Step 3. *Conclusion.*

Let $n = 4m + 3$ and substitute into the Sphere Packing Condition:

$$\begin{aligned} 2^{r+1} &= 2 + (4m+3) + (4m+3)^2 \\ &= 2 + 4m + 3 + 16m^2 + 24m + 9 \\ &= 14 + 28m + 16m^2 \end{aligned}$$

The lefthand side is congruent to 0 modulo 4, while the righthand side is congruent to 2 modulo 4. This contradiction completes the proof. □

REMARK. For $n = 2$, we find

$$y^2 - 2(n+1)y + 2^{r+1} = y^2 - 6y + 8 = (y-2)(y-4)\,;$$

and, for $n = 5$, we find

$$y^2 - 2(n+1)y + 2^{r+1} = y^2 - 12y + 32 = (y-4)(y-8)\,.$$

9.5 Generalizations of MacWilliams' Theorem

In Sections 9.2 and 9.3, for ease of exposition we only presented proofs of MacWilliams' Theorem 9.1.1 in the case of binary linear codes. On the other hand, in Section 9.4, once we had introduced the appropriate machinery, we were easily able to prove MacWilliams' Theorem for a class of codes larger than that of all linear codes over finite fields. It seems to have been Gleason (1971) who first fully appreciated the strength and generality of MacWilliams' proof using characters.

Initially in this section F is a ring that satisfies Property (**ND**) of Lemma 9.4.3, but we mainly concentrate on the case $F = \mathbb{Z}_4$ as it is of independent interest. We only give examples of two of the many generalizations that MacWilliams' Theorem admits.

Let $V = F^n$, and let $f\colon V \longrightarrow R$ be a map to any vector space over $\mathbb{C}$. Then the (discrete) *Fourier transform* (or Hadamard transform) of f is $\hat{f}\colon V \longrightarrow R$ given by

Fourier transform

$$\hat{f}(\mathbf{v}) = \sum_{\mathbf{u}\in V} f(\mathbf{u})\chi(\mathbf{u}|\mathbf{v})\,.$$

(9.5.1) Proposition. (Poisson summation formula.)
If A is an F-linear code then

$$\sum_{\mathbf{u}\in A^\perp} f(\mathbf{u}) = |A|^{-1} \sum_{\mathbf{v}\in A} \hat{f}(\mathbf{v})\,.$$

Proof. We use Lemma 9.4.4(2) to calculate

$$\begin{aligned}
|A|^{-1} \sum_{\mathbf{v}\in A} \hat{f}(\mathbf{v}) &= |A|^{-1} \sum_{\mathbf{v}\in A} \left(\sum_{\mathbf{u}\in V} f(\mathbf{u})\chi(\mathbf{u}|\mathbf{v}) \right) \\
&= |A|^{-1} \sum_{\mathbf{u}\in V} f(\mathbf{u}) \left(\sum_{\mathbf{v}\in A} \chi(\mathbf{u}|\mathbf{v}) \right) \\
&= |A|^{-1} \sum_{\mathbf{u}\in A^\perp} f(\mathbf{u})\,|A| \\
&= \sum_{\mathbf{u}\in A^\perp} f(\mathbf{u})\,,
\end{aligned}$$

as desired. □

This calculation was embedded in our proof of Theorem 9.4.8 for the particular choice of map $f(\mathbf{u}) = z^{\mathrm{wH}(\mathbf{u})} \in \mathbb{C}[z]$. Using the proposition and Proposition

9.4.6 in that case, we find

$$\begin{aligned}
\mathrm{W}_{A^\perp}(z) &= \sum_{\mathbf{u}\in A^\perp} f(\mathbf{u}) \;=\; |A|^{-1} \sum_{\mathbf{v}\in A} \hat{f}(\mathbf{v}) \\
&= |A|^{-1} \sum_{\mathbf{v}\in A} \left(\sum_{\mathbf{u}\in V} f(\mathbf{u}) \chi(\mathbf{u}|\mathbf{v}) \right) \\
&= |A|^{-1} \sum_{\mathbf{v}\in A} (1+(s-1)z)^{n-\mathrm{w_H}(\mathbf{v})} (1-z)^{\mathrm{w_H}(\mathbf{v})} \\
&= |A|^{-1} \sum_{i=0}^{n} a_i (1+(s-1)z)^{n-i} (1-z)^i \,.
\end{aligned}$$

This is MacWilliams' Theorem. (This can not really be described as a fourth proof but rather a rewording of the third proof.)

Remember that the homogeneous weight enumerator of A is

$$\mathrm{W}_A(x,y) = \sum_{\mathbf{a}\in A} x^{n-\mathrm{w_H}(\mathbf{a})} y^{\mathrm{w_H}(\mathbf{a})} \,.$$

Thus, for a given $\mathbf{a} = (a_1, \ldots, a_j, \ldots, a_n)$, we have in $x^{n-\mathrm{w_H}(\mathbf{a})} y^{\mathrm{w_H}(\mathbf{a})}$ factors x, one for each $a_j = 0$, and factors y, one for each $a_j \neq 0$. Different nonzero coefficients make the same contribution. If instead we wish to note the contribution of each member of F, we look at the (homogeneous) *complete weight enumerator* $\mathrm{C}_A(x_1, \ldots, x_s)$ for A, a polynomial in $s = |F|$ commuting variables, one to count occurrences of each member of the alphabet. (For the binary alphabet, the complete weight enumerator is just the usual homogeneous weight enumerator.)

complete weight enumerator

At this point we specialize to $F = \mathbb{Z}_4$. For the word $\mathbf{v} = (v_1, \ldots, v_j, \ldots, v_n)$ of V, we write $\mathrm{w}_0(\mathbf{v})$ for the number of 0's among the v_j, $\mathrm{w}_1(\mathbf{v})$ for the number of 1's, $\mathrm{w}_2(\mathbf{v})$ for the number of 2's, and $\mathrm{w}_3(\mathbf{v})$ for the number of 3's among the v_j. Thus $\mathrm{w}_0(\mathbf{v}) + \mathrm{w}_1(\mathbf{v}) + \mathrm{w}_2(\mathbf{v}) + \mathrm{w}_3(\mathbf{v}) = n$. The complete weight enumerator for A is then

$$\mathrm{C}_A(x,y,z,w) = \sum_{\mathbf{v}\in A} x^{\mathrm{w}_0(\mathbf{v})}\, y^{\mathrm{w}_1(\mathbf{v})}\, z^{\mathrm{w}_2(\mathbf{v})}\, w^{\mathrm{w}_3(\mathbf{v})} \,.$$

If we want a version of MacWilliams' Theorem for complete weight enumerators, we do not have to retrace our steps in the previous sections. We just apply Poisson summation and the Fourier transform to a different base function f.

For $F = \mathbb{Z}_4$, we set $f(\mathbf{u}) = x^{\mathrm{w}_0(\mathbf{u})}\, y^{\mathrm{w}_1(\mathbf{u})}\, z^{\mathrm{w}_2(\mathbf{u})}\, w^{\mathrm{w}_3(\mathbf{u})}$. Then, as before, we have

$$\mathrm{C}_{A^\perp}(x,y,z,w) = \sum_{\mathbf{u}\in A^\perp} f(\mathbf{u}) \;=\; |A|^{-1} \sum_{\mathbf{v}\in A} \hat{f}(\mathbf{v}) \,.$$

To compute the Fourier transform, we follow Proposition 9.4.6:

$$\begin{aligned}
\hat{f}(\mathbf{v}) &= \sum_{\mathbf{u}\in V} f(\mathbf{u})\chi(\mathbf{u}|\mathbf{v}) \\
&= \sum_{\mathbf{u}\in V} x^{\mathrm{w}_0(\mathbf{u})}\, y^{\mathrm{w}_1(\mathbf{u})}\, z^{\mathrm{w}_2(\mathbf{u})}\, w^{\mathrm{w}_3(\mathbf{u})}\chi(\mathbf{u}|\mathbf{v}) \\
&= \sum_{\mathbf{u}\in V} \left(\prod_{j=1}^{n} x^{\mathrm{w}_0(u_j)}\, y^{\mathrm{w}_1(u_j)}\, z^{\mathrm{w}_2(u_j)}\, w^{\mathrm{w}_3(u_j)}\chi(u_j|v_j) \right) \\
&= \prod_{j=1}^{n} \left(\sum_{u\in F} x^{\mathrm{w}_0(u)}\, y^{\mathrm{w}_1(u)}\, z^{\mathrm{w}_2(u)}\, w^{\mathrm{w}_3(u)}\chi(u|v_j) \right) \\
&= \prod_{j=1}^{n} (x\,\chi(0|v_j) + y\,\chi(1|v_j) + z\,\chi(2|v_j) + w\,\chi(3|v_j)) \,.
\end{aligned}$$

The value of each factor will depend upon that of v_j:

v_j	$x\,\chi(0\|v_j) + y\,\chi(1\|v_j) + z\,\chi(2\|v_j) + w\,\chi(3\|v_j)$
0	$x + y + z + w$
1	$x + iy - z - iw$
2	$x - y + z - w$
3	$x - iy - z + iw$

Hence finally

$$\begin{aligned}
\hat{f}(\mathbf{v}) &= (x+y+z+w)^{\mathrm{w}_0(\mathbf{v})}\,(x+iy-z-iw)^{\mathrm{w}_1(\mathbf{v})} \\
&\qquad (x-y+z-w)^{\mathrm{w}_2(\mathbf{v})}\,(x-iy-z+iw)^{\mathrm{w}_3(\mathbf{v})} \,.
\end{aligned}$$

When inserted into the summation formula, this gives MacWilliams' Theorem for complete weight enumerators over $\mathbb{Z}_4$:

(9.5.2) THEOREM. *If A is a $\mathbb{Z}_4$-linear code, then*

$$\begin{aligned}
\mathrm{C}_{A^\perp}(x,y,z,w) &= |A|^{-1}\, \mathrm{C}_A(x+y+z+w, x+iy-z-iw, \\
&\qquad x-y+z-w, x-iy-z+iw) \,. \qquad \square
\end{aligned}$$

Although this is quite complicated, it is also relatively powerful. For instance we regain the usual homogeneous $\mathbb{Z}_4$-version of MacWilliams' Theorem by specializing to $y = z = w$.

$$\begin{aligned}
\mathrm{W}_{A^\perp}(x,y) &= \mathrm{C}_{A^\perp}(x,y,y,y) \\
&= |A|^{-1}\, \mathrm{C}_A(x+y+y+y, x+iy-y-iy, \\
&\qquad x-y+y-y, x-iy-y+iy) \\
&= |A|^{-1}\, \mathrm{C}_A(x+3y, x-y, x-y, x-y) \\
&= |A|^{-1}\, \mathrm{W}_A(x+3y, x-y) \,.
\end{aligned}$$

In certain situations there are metrics on F^n that are more appropriate than the Hamming metric. For instance, when reading time from a clock with hands but no numbers, it will be easier to mistake 3 o'clock for 2 or 4 than for 8 o'clock. The *Lee metric* on $\mathbb{Z}_s$ sets the Lee distance

Lee metric

$$\mathrm{d_L}(i,j) = \min(|i-j|, s-|i-j|)\,,$$

for $i, j \in \mathbb{Z}_s$, and the Lee weight

$$\mathrm{w_L}(i) = \mathrm{d_L}(i,0)\,.$$

Thus, on $\mathbb{Z}_4$, we have

$$\mathrm{w_L}(0) = 0,\ \mathrm{w_L}(1) = \mathrm{w_L}(3) = 1,\ \text{and } \mathrm{w_L}(2) = 2\,.$$

This is the first new case, since the Lee metric on $\mathbb{Z}_2$ and $\mathbb{Z}_3$ is the same as the Hamming metric.

As before, two words $\mathbf{v} = (v_1, \ldots, v_n)$ and $\mathbf{w} = (w_1, \ldots, w_n)$ from $\mathbb{Z}_s^n$ have Lee distance given by

$$\mathrm{d_L}(\mathbf{v}, \mathbf{w}) = \sum_{j=1}^{n} \mathrm{d_L}(v_j, w_j)$$

and Lee weight $\mathrm{w_L}(\mathbf{v}) = \mathrm{d_L}(\mathbf{v}, \mathbf{0})$.

The *Lee weight enumerator* of $A \subseteq \mathbb{Z}_s^n$ is then

Lee weight enumerator

$$\mathrm{L}_A(z) = \sum_{\mathbf{v}\in A} z^{\mathrm{w_L}(\mathbf{v})}\,.$$

As the largest weight of a word in $\mathbb{Z}_s^n$ is $t\,n$, where $t = \lfloor s/2 \rfloor$, the *homogeneous Lee weight enumerator* is

homogeneous Lee weight enumerator

$$\mathrm{L}_A(x,y) = \sum_{\mathbf{v}\in A} x^{tn-\mathrm{w_L}(\mathbf{v})} y^{\mathrm{w_L}(\mathbf{v})}\,.$$

When $F = \mathbb{Z}_4$, the homogeneous Lee weight enumerator is

$$\mathrm{L}_A(x,y) = \sum_{\mathbf{v}\in A} x^{2n-\mathrm{w_L}(\mathbf{v})} y^{\mathrm{w_L}(\mathbf{v})}\,.$$

For a particular word $\mathbf{v} \in \mathbb{Z}_4^n$ we see that

$$x^{2n-\mathrm{w_L}(\mathbf{v})} y^{\mathrm{w_L}(\mathbf{v})} = (x^2)^{\mathrm{w}_0(\mathbf{v})} (xy)^{\mathrm{w}_1(\mathbf{v})} (y^2)^{\mathrm{w}_2(\mathbf{v})} (xy)^{\mathrm{w}_3(\mathbf{v})}\,,$$

and therefore

$$\mathrm{L}_A(x,y) = \mathrm{C}_A\big(x^2, xy, y^2, xy\big)\,.$$

(9.5.3) THEOREM. *If A is a $\mathbb{Z}_4$-linear code, then*

$$\mathrm{L}_{A^\perp}(x,y) = |A|^{-1} \mathrm{L}_A(x+y, x-y)\,.$$

PROOF. We use Theorem 9.5.2.

$$\begin{aligned}
\mathrm{L}_{A^\perp}(x,y) &= \mathrm{C}_{A^\perp}\big(x^2, xy, y^2, xy\big) \\
&= |A|^{-1}\ \mathrm{C}_A\big(x^2+xy+y^2+xy, x^2+ixy-y^2-ixy, \\
&\qquad\qquad x^2-xy+y^2-xy, x^2-ixy-y^2+ixy\big) \\
&= |A|^{-1}\ \mathrm{C}_A\big((x+y)^2, x^2-y^2, (x-y)^2, x^2-y^2\big) \\
&= |A|^{-1}\ \mathrm{L}_A(x+y, x-y)\ . \qquad \square
\end{aligned}$$

It is notable (and significant) that the transformation

$$x \longrightarrow x+y \qquad y \longrightarrow x-y\,,$$

which takes the homogeneous Lee weight enumerator of the $\mathbb{Z}_4$-linear code A to $|A|$ times that of its dual, is the same transformation that takes the homogeneous weight enumerator of the binary linear code A to $|A|$ times that of its dual. (See Theorem 9.1.1(2).)