# Weights Modulo 8 in Binary Cyclic Codes

R. J. McEliece
Communications Systems Research Section

*A new technique is provided for computing the weights modulo 8 in binary cyclic codes. These codes have proved to be the most important for GCF error detection/correction, and the method described will frequently aid in the detailed analysis of such codes.*

## I. Introduction

In this article we will obtain an improved method of calculating the value of the weights modulo 8 in a binary cyclic code. Such codes are the most important class of block codes known. For example, the (32, 6) block code used in the high-rate telemetry system, the (1200, 1167) BCH error detection code used on the GCF/NASCOM lines, and the (23, 12) Golay code currently being studied for use on a concatenation scheme for MJS77 are all essentially binary cyclic codes. Weight information is a first step toward analyzing the error correction properties of a code.

If $C$ is an $(n, k)$ binary cyclic code, denote its weight enumerator by

$$A(Z) = \sum_{i=0}^{n} A_i Z^i$$

$A_i$ being the number of words of weight $i$ in $C$. Knowledge of $A(Z)$ is vital for evaluating the performance of the code $C$, but often $C$ contains so many codewords that a direct enumeration is not possible. Thus indirect methods must be adopted. In Section II we present a technique which can usually be used to evaluate $A(Z)$ modulo $Z^8 - 1$. This information can then be added to other known information about $A(Z)$ in the attempt to calculate $A(Z)$. An example of the technique is given in Section III.

## II. The New Technique

Let $c = (c_0, c_1, \cdots, c_{n-1})$ be a codeword from $C$. We assume $n$ is odd. Then the Mattson–Solomon polynomial of $c$,

$$s(x) = \sum_{i=0}^{n-1} s_i x^i$$

has the property that $c_j = s(\theta^j)$, where $\theta$ is a primitive $n$th root of unity in some extension of $GF(2)$. The $n$ coefficients $s_i$ also lie in an extension of $GF(2)$, and $s_i^2 = s_{2i}$

(subscripts mod $n$). Let us write the weight of $c$ in its binary expansion

$$w(c) = \Gamma_1(c) + 2\Gamma_2(c) + 4\Gamma_4(c) + \cdots$$

where $\Gamma_{2^r}(c) = 0$ or 1.

Let us first show that $\Gamma_1(c) \equiv s_0 \pmod 2$. $\Gamma_1(c) \equiv w(c) \equiv c_0 + c_1 + \cdots + c_{n-1} \pmod 2$. Thus

$$\Gamma_1(c) \equiv \sum_{j=0}^{n-1} \sum_{i=0}^{n-1} s_i \theta^{ji} \equiv \sum_{i=0}^{n-1} s_i \sum_{j=0}^{n-1} \theta^{ij} \pmod 2. \tag{1}$$

Now since for $i = 1, 2, \cdots, n-1$ $\theta^i$ is a zero of

$$\frac{x^n - 1}{x - 1} = \sum_{j=0}^{n-1} x^j$$

the inner sum in (1) is zero unless $i = 0$. Thus $\Gamma_1(c) \equiv n s_0 \equiv s_0 \pmod 2$.

The simple argument above was extended by Solomon and McEliece (Ref. 1) to $\Gamma_2$ and to $\Gamma_4$. They assumed that $\Gamma_1(c) = 0$. This assumption involves no essential loss of generality, since in a binary $(n, k)$ cyclic code with $n$ odd, either all words have even weight, or else exactly half have odd weight, the words of odd weight being the mod-2 complements of the words of even weight. Under this assumption, Solomon and McEliece proved

$$\Gamma_2(c) \equiv \sum \{s_i s_j : i < j, i + j \equiv 0 \pmod n\} \pmod 2 \tag{2}$$

To give their expression for $\Gamma_4$, we must first introduce some notation. Let $P_r$ represent the set of unordered selections, with repetitions permitted, of $r$ elements from the set $\{0, 1, 2, \cdots, n-1\}$. Let $P_r^0$ be the subset of $P_r$ of those selections whose entries sum to 0 (mod $n$). Thus if $n = 3$, $P_4$ contains 15 selections but $P_4^0$ contains only 0000, 0012, 0111, 0222, and 1122. If $\alpha = (\alpha_1\alpha_2\alpha_3\alpha_4) \varepsilon P_4$, define $s_\alpha = s_{\alpha_1} s_{\alpha_2} s_{\alpha_3} s_{\alpha_4}$. Then Solomon and McEliece proved that

$$\Gamma_4(c) \equiv \sum_{\alpha \varepsilon P_4^0} A_\alpha s_\alpha \pmod 2 \tag{3a}$$

where the coefficients $A_\alpha$ are all zero, except that $A_\alpha = 1$ in the four mutually exclusive cases

$$\alpha = (i, i, j, k) \qquad i, j, k \text{ distinct} \tag{3b}$$

$$\alpha = (i, i, i, j) \qquad i, j \text{ distinct} \tag{3c}$$

$$\alpha = (i, j, n-i, n-j) \quad i, j \text{ distinct} \tag{3d}$$

$$\alpha = (i, i, n-i, n-i) \text{ and } n \equiv 1 \pmod 4. \tag{3e}$$

Our object here is to show that (3a) can be greatly simplified. First, the sum in (3a) over the terms (3e) is, when $n \equiv 1 \pmod 4$,

$$\sum s_i^2 s_{n-1}^2 \equiv \sum s_i s_{n-1} \equiv \Gamma_2(c) \pmod 2$$

from (2). Next the sum over the terms (3d) is

$$\sum_{i<j} s_i s_{n-1} s_j s_{n-j}.$$

But this is just the second elementary symmetric function of the terms $s_\alpha$, $\alpha \varepsilon P_2^0$.

We now come to the terms (3b) and (3c). If $\alpha$ is a term in (3b), $s_\alpha = s_i^2 s_j s_k = s_{2i} s_j s_k$, since as mentioned above $s_i^2 = s_{2i}$. Similarly in case (3c) $s_\alpha = s_i^3 s_j = s_{2i} s_i s_j$. Of course these terms could "collapse" further if, for example, $2i \equiv j \pmod n$. Thus every term $s_\alpha$ from (3b) and (3c) "collapses" to a term of one of the forms $s_a s_b s_c$ with $a < b < c$ and $a + b + c \equiv 0 \pmod n$ or $s_a s_b$ with $a < b$ and $a + b \equiv 0 \pmod n$.

Thus we are led to define $Q_r$ as the set of unordered selections, *without* repetition, of $r$ objects from $\{0, 1, \cdots, n-1\}$, and $Q_r^0$ as the subset of $Q_r$ of those selections whose entries sum to 0 (mod $n$). We have seen that every term $\alpha \varepsilon P_4^0$ from (3b) or (3c) collapses to a term in either $Q_3^0$ or $Q_2^0$. Let us now see how many elements in $P_4^0$ can collapse to a particular element in $Q_3^0$ or $Q_2^0$.

First consider $Q_2^0$. A typical term is $(i, j)$ with $i < j$ and $i + j \equiv 0 \pmod n$. We easily see that the only terms in $P_4^0$ which collapse to $(i, j)$ are:

$$\left(\frac{i}{4}, \frac{i}{4}, \frac{i}{2}, j\right) = \alpha_1$$

$$\left(\frac{j}{4}, \frac{j}{4}, \frac{j}{2}, i\right) = \alpha_2$$

$$\left(\frac{i}{2}, \frac{i}{2}, \frac{j}{2}, \frac{j}{2}\right) = \alpha_3$$

The last of these terms is not of form (3b) or (3c) and so does enter into the sum (3). The other two terms are distinct elements of $P_4^0$, either of class (3b) or (3c), and since $s_{\alpha_1} + s_{\alpha_2} \equiv 0 \pmod 2$, we see that the terms of $P_4^0$ which collapse to terms in $Q_2^0$ do not contribute to the sum (3).

Finally we consider those terms (3b) and (3c) of $P_4^0$ which collapse to a term in $Q_3^0$. A typical term in $Q_3^0$ is

$(i, j, k)$ with $i < j < k$ and $i + j + k \equiv 0 \pmod{n}$. The terms in $P_4^0$ which collapse to $(i, j, k)$ are then

$$\left(\frac{i}{2}, \quad \frac{i}{2}, \quad j, k\right) = \alpha_1$$

$$\left(i, \quad \frac{j}{2}, \quad \frac{j}{2}, \quad k\right) = \alpha_2$$

$$\left(i, \quad j, \quad \frac{k}{2}, \quad \frac{k}{2}\right) = \alpha_3$$

Now $\alpha_1$, $\alpha_2$ and $\alpha_3$ are all distinct elements of $P_4^0$ belonging to either (3b) or (3c). And since $s_{\alpha_1} + s_{\alpha_2} + s_{\alpha_3} = s_i s_j s_k$, we see that the sum in (3) over the $\alpha$'s in classes (3b) and (3c) is $\sum \{s_\alpha : \alpha \varepsilon Q_3^0\}$.

Finally let us define $\sigma_j^{(r)}(c)$ as the $j$th elementary symmetric function of the terms $s_\alpha$, $\alpha \varepsilon Q_r^0$. We have then proved that the formula of Solomon–McEliece (3a) can be rewritten as:

$$\Gamma_4(c) \equiv \sigma_1^{(3)}(c) + \sigma_2^{(2)}(c) + (1 + n_1)\,\sigma_1^{(2)}(c) \pmod 2 \tag{4}$$

where $n = n_m \cdots n_2 n_1 1$ is the binary expansion of $n$. This is our main result. In Section III we give an example of the use of (4).

## III. An Example

We will illustrate our result on the (17, 8) cyclic code whose check polynomial $x^8 + x^5 + x^4 + x^3 + 1$ is irreducible mod 2. It follows from the Mattson–Solomon results that every codeword $c \varepsilon C$ has $s_j = 0$ except possibly for $j \varepsilon \{1, 2, 4, 8, 16, 15, 13, 9\} = K$; i.e., $j \equiv 2^m \pmod{17}$ for $m = 0, 1, \cdots, 7$. Furthermore for each such codeword there will exist a unique $x \varepsilon GF(2^8)$ such that $s_{2^m} = x^{2^m}$.

Now we are ready to apply our formula for $\Gamma_4$. The first term, $\sigma_1^{(3)}(c)$, will involve only those selections $(i, j, k)$ from $Q_4^0$, all of whose elements lie in the set $K$. But it is easily verified that no such tuples $(i, j, k)$ exist. Thus $\sigma_1^{(3)}(c) = 0$ for all $c \varepsilon C$. The next two terms are the first two elementary symmetric functions of the nonzero terms $\{s_\alpha : \alpha \varepsilon Q_2^0\}$; i.e., $\{s_1 s_{16}, s_2 s_{15}, s_4 s_{13}, s_8 s_9\}$ but since $s_{2^m} = x^{2^m}$ for some $x \varepsilon GF(2^8)$ this set is $\{x^{17}, x^{17 \cdot 2}, x^{17 \cdot 4}, x^{17 \cdot 8}\}$. If $x \neq 0$, $x^{2^8 - 1} = x^{17 \cdot 15} = 1$ in $GF(2^8)$, and so $x^{17}$ in fact lies in the smaller field $GF(2^4)$. In fact for every $y \varepsilon GF(2^4) - \{0\}$, there are exactly 17 values of $x \varepsilon GF(2^8) - \{0\}$ such that $x^{17} = y$. For every codeword $c$ corresponding to such an $x$, then

$$\Gamma_4(c) = \sigma_2(y) + \sigma_1(y),$$

where $Z^4 + \sigma_1(y) Z^3 + \sigma_2(y) Z^2 + \sigma_3(y) Z + \sigma_4(y) = (Z - y)(Z - y^2)(Z - y^4)(Z - y^8)$ is the field polynomial for $y$.

Similarly, but more easily,

$$\Gamma_2(c) = \sigma_1(y).$$

Finally all that is needed is a list of the field polynomials of the 15 nonzero elements of $GF(2^4)$:

| Polynomial | Number of distinct roots | $\Gamma_4$ | $\Gamma_2$ |
|---|---|---|---|
| $Z^4 + Z + 1$ | 4 | 0 | 0 |
| $Z^4 + Z^3 + 1$ | 4 | 1 | 1 |
| $Z^4 + Z^3 + Z^2 + Z + 1$ | 4 | 0 | 1 |
| $Z^4 + Z^2 + 1$ | 2 | 1 | 0 |
| $Z^4 + 1$ | 1 | 0 | 0 |

Thus we see that in the code $C$ there are, apart from the all-zero word,

$85 = 17 \cdot 5$ words with weight $\equiv 0 \pmod 8$

$68 = 17 \cdot 4$ words with weight $\equiv 2 \pmod 8$

$34 = 17 \cdot 2$ words with weight $\equiv 4 \pmod 8$

$68 = 17 \cdot 4$ words with weight $\equiv 6 \pmod 8$

Since the BCH bound assures us that there are no words of weight less than 5 or greater than 12, the complete weight enumerator for $C$ is

$$A(Z) = 1 + 68Z^6 + 85Z^8 + 68Z^{10} + 34Z^{14}$$

## Reference


1. Solomon, G., and McEliece, R., "Weights of Cyclic Codes," *J. Comb. Th.* Vol 1, pp. 459–475, 1966.