NUMBER OF INFORMATION SYMBOLS OF BCH CODES OF LENGTH $2^m + 1$

Alberto Cáceres
Department of Mathematics, Humacao University College, Humacao Puerto Rico

Oscar Moreno
Department of Mathematics, University of Puerto Rico, Rio Piedras Puerto Rico

Proceedings TWENTY SECOND ANNUAL ALLERTON CONFERENCE ON
COMMUNICATION, CONTROL AND COMPUTING
University of Illinois at Urbana-Champaign
October 3-5 1984

Abstract

This paper offers a solution to the problem of finding the number of information symbols of a binary BCH code of length $2^m + 1$. In the general case we give a method to carry out the counting of the number of information symbols and in the particular case of designed distance $\delta = 2t + 1$ where $2t - 1 < 2^{[m/2]}$ we prove that the dimension is equal to $2^m + 1 - 2mt$. As a consequence we can also give the enumeration of information symbols of Goppa codes of length 2^m which, when extended, become cyclic.

I. Introduction

In the present paper we offer a solution to the problem of finding the number of information symbols of a binary BCH code of length $2^m + 1$.

In the general case we suggest an enumeration method by means of counting the cardinality of cyclotomic cosets modulo 2^m+1. This is done by the simple technique of cyclic shifting m-digit binary sequences. Unlike the primitive case $(2^m - 1)$, the shifting is not all the time cyclic. This is due to the fact that multiplication by 2 modulo $2^m + 1$, when the leading digit is 1, does not correspond exactly to cyclic shifting, as happens in the primitive case [1]. With the help of suitable altered shiftings, complete enumeration is achieved.

In the particular case of designed distance $\delta = 2t + 1$ where $2t - 1 < 2^{[m/2]}$ we obtain a closed formula, in a result similar to the primitive case given as Corollary 8, p 283 [2]. The above mentiomned shiftings are the key factor in proving the theorem.

The theorem also permits the enumeration of symbols of information of Goppa codes of length 2^m which when extended become cyclic. This is a cotribution to Problem 12.1 of Mac Williams and Sloane [2].

II. Cyclotomic Cosets modulo $2^m + 1$

Enumeration of information symbols of a BCH code of lenght n is carried on by measuring the

size of cyclotomic cosets modulo n. In the primitive case it is measured by counting the number of simple cyclic shiftings of the binary representation of coset representatives. When $n = 2^m + 1$ it is necessary to define some sort of corrected shiftings in order to carry out the enumeration.

A shifting modulo 2^m+1 or corrected shifting of the binary sequence $a_{m-1}\ a_{m-2}\ldots a_1\ a_0$ is achieved by simple cyclic shifting $a_{m-2}\ a_{m-3}\ldots a_1\ a_0\ a_{m-1}$ when the leading digit $a_{m-1} = 0$. When $a_{m-1} = 1$ this is done by a simple cyclic shifting followed by a formally bynary addition of the sequence $11\ldots10$. This addition corresponds, complementwise, to the substraction of 2 modulo $2^m + 1$.

Theorem 1. (Size of cyclotomic cosets modulo $2^m + 1$) Let C_i be the cyclotomic coset of i modulo $2^m + 1$ where i is its smallest representative. Then the cardinality of C_i is:

i) $|C_i| = 2m$. If $1 \leq k \leq$, $C_{2^k} = C_1$

ii) $|C_i|$ = number of different shiftings modulo 2^m+1 of the m-digit binary expression of i, provided $1 < i < 2m$ and $i \neq 2^k$.

Proof. Part *i)* is well known since $2m$ is the multiplicative order of 2 modulo $2^m + 1$, so we will prove part *ii)*

If $i \neq 2^k$ and $i < 2^m$, let us take its m-digit binary representation

$$a_{m-1}\ a_{m-2}\ldots a_1\ a_0 \tag{1}$$

where at least two of the digits are 1. We can write

$$i = a_{m-1}2^{m-1} + a_{m-2}2^{m-2} + \ldots + a_1 2 + a_0 < 2^m$$

a) If $a_{m-1} = 0$ then $i < 2^{m-1}$ and $2i < 2^m < 2^m + 1$ and $i \not\equiv 2i \pmod{(2^m + 1)}$; also

$$2i = a_{m-2}2^{m-1} + a_{m-3}2^{m-2} + \ldots + a_1 2^2 + a_0 2^1 + a_{m-1}$$

which corresponds to the sequence $a_{m-2}\ a_{m-3}\ldots a_1\ a_0\ a_{m-1}$ and this is a simple shifting of (1)

b) If $a_{m-1} = 1$ then $2^{m-1} < i < 2^m$, hence $2^m < 2i < 2^{m+1}$. Moreover $2^m + 1 < 2i < 2^{m+1}$, $2i \equiv 2i - (2^m + 1) \pmod{(2^m + 1)}$ and $2i - (2^m + 1) < 2^m - 1$.

In order to obtain a cyclic shifting expression for $2i - (2^m + 1)$ we write

$$\begin{aligned} 2i - (2^m + 1) &= (a_{m-2}2^{m-1} + a_{m-3}2^{m-2} + \ldots a_0 2) + a_{m-1}2^m - (2^m + 1) \\ &= (a_{m-2}2^{m-1} + a_{m-3}2^{m-2} + \ldots a_0 2 + a_{m-1}) - a_{m-1} + a_{m-1}2^m - 2^m - 1 \\ &= (a_{m-2}2^{m-1} + a_{m-3}2^{m-2} + \ldots a_0 2 + a_{m-1}) - 2 \end{aligned}$$

since $a_{m-1} = 1$.

The expression in parenthesis corresponds to the regular cyclic shifting. Substraction of 2 accomplishes for a shifting modulo $2^m + 1$. ∎

Method to count the number of elements of a cyclotomic coset $C_i \pmod{(2^m+1)}$ for $1 < i < n$ and i odd

1. $|C_1| = |C_{2^m}| = 2m$
2. If $1 < i < 2^m$ then obtain the m-digit binary representation of i, say $a_{m-1}\ a_{m-2} \dots a_1\ a_0$, and perform a shifting modulo $2^m + 1$. It is always possible since at least two digits are 1.
3. The number of different shiftings modulo $2^m + 1$ is the number of elements of C_i.

Example. We calculate $|C_{13}| \pmod{2^6+1}$. The 6-digit binary representation of 13 is 001101

001101	
011010	cyclic shifting
110100	cyclic shifting
100111	corrected shifting
001101	corrected shifting

The last line is equal to the first one, hence $|C_{13}| = 4$.

III. Particular case

Let j be an odd integer such that $1 < j < 2^{[m/2]} + 1$ and let $w_0 = 00\dots01_\alpha X_{\alpha-1}\dots X_1 1_0$ be its m-digit binary representation where subscripts represent the original position of digits and will remain doing so. Since $w_0 < 2^{[m/2]} + 1$, we have $\alpha \leq [m/2] - 1$ and the number of leading zeroes in w_0 is $m - \alpha - 1$. Clearly $m - \alpha - 1 \geq m - \left\lceil \frac{m}{2} \right\rceil \geq \left\lceil \frac{m}{2} \right\rceil$.

Let us call w_k the k-th shifting modulo $2^m + 1$ of w_0. Now we shall prove the following lemmma

Lemma 1. Let j be an odd integer such that $1 < j < 2^{[m/2]} + 1$. Then

i) If $0 \leq k_1 < k_2 < m$ then $w_{k_1} \neq w_{k_2}$.

ii) For any positive $k < m$, $w_0 < w_k < w_m$, i.e., w_m is the largest of the first $m+1$ elements of the cyclotomic coset C_j..

Proof. By shifting w_0 for the first time we obtain

$$w_1 = 0\dots01_\alpha X_{\alpha-1}\dots X_1 1_0 0$$

which is a simple shifting since the leading didgit is zero. Simple shiftings will occur until we get

$$w_{m-\alpha-1} = 1_\alpha X_{\alpha-1}\dots X_1\ 1_0\ \underbrace{00\dots0}_{m-\alpha-1}$$

Clearly all these shiftings are different. By the position of 1_α we get $w_0 < w_k$ for $0 < k < m-\alpha-1$. Next we have a corrected shifting, i.e., move the leading 1_α to the right end and obtain

$$X_{\alpha-1} \dots X_1 \ 1_0 \ 0 \dots 0 \ 1_\alpha$$

and substract 10 to obtain

$$w_{m-\alpha} = X_{\alpha-1} \dots X_1 \ 0_0 \ \underbrace{11 \dots 1}_{m-\alpha-1} 1_\alpha$$

which is also different than the previous shiftings and $w_0 < w_{m-\alpha}$. Now

$$w_{m-\alpha+1} = \begin{cases} X_{\alpha-2} \dots X_1 \ 0_0 \ 1_{m-1} \dots 0 \ 1_{\alpha+1}, \ 1_\alpha \ 0_{\alpha-1} & \text{if } X_{\alpha-1} = 0 \\ X_{\alpha-2} \dots X_1 \ 0_0 \ \underbrace{1_{m-1} \dots 0 \ 1_{\alpha+1}}_{m-\alpha-1}, \ 0_\alpha \ 1_{\alpha-1} & \text{if } X_{\alpha-1} = 1 \end{cases}$$

Next shiftings will move the remaining $X's$ one by one to the right end and, be it 0 or 1, the block of $m-\alpha-1$ $1's$ will not change until 1_{m-1} reaches leading position and we obtain

$$w_m = 1_{m-1} \ 1 \dots 1_{\alpha+1} \ Y_\alpha \ Y_{\alpha-1} \dots Y_1 \ 0_0$$

which is also the negative of $w_0 \pmod{2^m+1}$, since $w_m = w_0 2^m \pmod{2^m+1}$. At this point all shiftings have created $m+1$ different elements all of them larger than w_0. Moreover, since w_m has the largest leading block of 1's it is the largest of all shiftings, and this completes the proof of i) and ii). ∎

Theorem 2. For $n = 2^m + 1$ the cyclotomic cosets $C_1, C_3, C_5, \dots, C_i$ are distinct and each contains $2m$ elements, provided $i < 2^{[m/2]} + 1$.

Proof. We prove first that each of these cyclotomic cosets contais $2m$ elements. This is a direct consequence of the first part of the Lemma, since the shifting generates $m+1$ elements in C_j and $|C_j|$ is a divisor of $2m$.

In order to prove that the cyclotomic cosets are different, let us observe that for any $0 \le k < m$, $w_k 2^m + w_k = w_k(2^m+1) \pmod{2^m+1}$, hence $-w_k = w_k(2^m+1) \pmod{2^m+1}$, since w_{m+k} is obtained from w_k after m shiftings. Hence $w_k + w_{m+k} = 2^m + 1$. Now, for any $0 < k < m$, the second part of the lemma tells $w_0 < w_k < w_m < 2^m + 1$ which substracted from $2^m + 1$ gives

$$(2^m+1) - w_m < (2^m+1) - w_k < (2^m+1) - w_0,$$

i.e., $w_0 < w_{m+k} < w_m$ as long as $j < 2^{[m/2]} + 1$. No room is left for any $i < j$ in C_j, hence $C_i \neq C_j$. ∎

Note. If m is even and $j = 2^{m/2} + 1$, C_j contains an element $i = 2^{m/2} - 1 < j$. In fact,

$$j \cdot 2^{m/2} = (2^{m/2}+1)2^{m/2} = (2^{m/2}-1) + (2^m+1) \equiv i \pmod{2^m+1}.$$

Corollary. If C is a binary BCH code of length $n = 2^m + 1$ and *designed distance* $\delta = 2t + 1$ where $2t - 1 < 2^{[m/2]} + 1$, then $dimC = 2^m + 1 - 2mt$ ∎

References

[1] Berlekamp E.R., *Algebraic Coding Theory*, McGraw Hill, 1968

[2] Mac Williams F. J. and Sloane N.J.A., *The Theory of Error Correcting Codes*, North Holland Pub. Co. Third Printing, 1981.

Acknowledgment

This work was jointly supported by the NSF-Resource Center for Science and Engeneering, UPR and by the Humacao University College, UPR.