

A Note on the Weight Distributions of Binary Quadratic Residue Codes

Yaotsu Chang

Department of Applied Mathematics

I-Shou University

Kaohsiung, Taiwan, R.O.C

ytchang@isu.edu.tw

Coauthors:

T. K. Truong

Department of Information Engineering

I-Shou University

Kaohsiung, Taiwan, R.O.C

C. D. Lee

Department of Information Engineering

I-Shou University

Kaohsiung, Taiwan, R.O.C

Abstract

- In this talk, an algorithm to determine the weight distributions of binary cyclic codes is proposed.
- Moreover, some observations about the weight distributions of binary quadratic residue codes are provided.
- As a result, the weight distributions of $(73, 37, 13)$, $(89, 45, 17)$, $(97, 49, 15)$ quadratic residue codes are obtained.

C : a binary (n, k) cyclic code

$c = c_0c_1 \dots c_{n-1} \in C$: a codeword.

The number of nonzero terms in the bit-string c is called the **weight** of c , and is denoted by $\text{wt}(c)$.

For $i = 0, 1, \dots, n$, denote by A_i the number of codewords of weight i in C .

The sequence A_0, A_1, \dots, A_n is called the **weight distribution** of C .

Importance of the weight distribution

"One of the keys to obtaining an exact expression for the error detection and error correction performance of a block code is the weight distribution of the code."

$F = GF(2)$: the finite field of two elements.

A **binary cyclic code** $C = \langle g(x) \rangle$ of length n is an ideal of the ring $R = \frac{F[x]}{\langle x^n - 1 \rangle}$ and is generated by the polynomial $g(x)$.

That is, $C = \{v(x)g(x) \mid v(x) \in R\}$.

When viewed as a vector space, the ring $R = \frac{F[x]}{\langle x^n - 1 \rangle}$ is isomorphic to F^n and the ideal $C = \langle g(x) \rangle$ can be viewed as a subspace of R .

The dimension of the subspace C over F is called the **dimension** of the code C , and one has

$$\dim C = n - \deg(g(x)).$$

Usually the dimension of C is denoted by k .

The cyclic code $C = \langle g(x) \rangle$ can then be written as

$$C = \{v(x)g(x) \mid \deg(v(x)) < k\}.$$

Definition of binary quadratic residue codes

$$F = GF(2)$$

$n \equiv \pm 1 \pmod{8}$: prime number

m : the order of 2 modulo n , i.e., m is the smallest positive integer such that $2^m \equiv 1 \pmod{n}$.

$E = GF(2^m)$: the extension field of F of degree m .

α : a primitive element of E , i.e. a generator of the multiplicative group $E^* = GF(2^m) \setminus \{0\}$.

Then the element $\beta = \alpha^{(2^m-1)/n}$ is a primitive root of the unity, i.e., $\beta \neq 1$ and $\beta^n = 1$.

$Q := \{i^2 \mid i = 0, 1, \dots, n-1\}$ the set of quadratic residues modulo n

$$g(x) := \prod_{i \in Q} (x - \beta^i)$$

Then $g(x) \in F[x]$ and $g(x) \mid x^n - 1$.

The cyclic code $C = \langle g(x) \rangle$ generated by the polynomial $g(x)$ is called a **quadratic residue code** (QR code) of length n .

The dimension of the QR code C equals

$$k = n - \deg(g(x)) = n - |Q| = n - \frac{n-1}{2} = \frac{n+1}{2}.$$

In 1958, Prange introduced quadratic residue (QR) codes. These QR codes have code rates greater than or equal to $1/2$ and generally have large minimum distances, so that most of the known QR codes are the best-known codes. There are eleven binary QR codes with code length less than 100, say 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, and 97. Among those codes, (7, 4, 3) and (23, 12, 7) QR codes are the well-known Hamming code and Golay code.

Hard-to-obtain the weight distribution

V. Pless wrote, in the book “Introduction to the Theory of Error-Correcting Codes”, the following sentences:

“To give an idea of the difficulties involved, it is possible to compute, in a reasonable amount of time, the weight distribution of a specified (40, 20) binary code on a large computer, but larger codes usually require extra knowledge to obtain their weight distributions.”

Direct method to determine the weight distributions of binary cyclic codes

$C = \langle g(x) \rangle$: binary (n, k) cyclic code

Then $C = \{v(x)g(x) \mid \deg(v(x)) < k\}$.

There are 2^k code polynomials in C and the code polynomials can be listed one by one in the following way:

$$0 \cdot g(x), 1 \cdot g(x), x \cdot g(x), \dots, (1 + x + \dots + x^{k-1}) \cdot g(x).$$

A straight way to obtain the complete weight distribution A_0, \dots, A_n is to calculate the weights of all the code polynomials in C .

That is to do $|C| = 2^k$ polynomial multiplications.

Alternative method to determine the weight distributions of binary cyclic codes

$g(x) = g_0 + g_1x + \dots + g_{k-1}x^{k-1}$: generator polynomial of C

let $G_0 = (g_0, g_1, \dots, g_{k-1}, 0, \dots, 0)$,

$G_1 = (0, g_0, g_1, \dots, g_{k-1}, 0, \dots, 0)$,

$G_2 = (0, 0, g_0, g_1, \dots, g_{k-1}, 0, \dots, 0)$

, and

$G_{k-1} = (0, \dots, 0, g_0, g_1, \dots, g_{k-1}, 0, \dots, 0)$

be the vector forms of $g(x), x \cdot g(x), \dots, x^{k-1}g(x)$, respectively.

$$\begin{aligned}
c(x) &= v(x)g(x) \\
&= (v_0 + v_1x + \dots + v_{k-1}x^{k-1}) \cdot g(x) \\
&= v_0g(x) + v_1(xg(x)) + \dots + v_{k-1}(x^{k-1}g(x)) \\
&\rightarrow v_0G_0 + v_1G_1 + \dots + v_{k-1}G_{k-1}
\end{aligned}$$

$$wt(c(x)) = wt(v_0G_0 + v_1G_1 + \dots + v_{k-1}G_{k-1})$$

To calculate the weight distribution of

$$C = \{v(x)g(x) \mid \deg v(x) \leq k-1\},$$

it is equivalent to determine the weight distribution of the following n -vectors set

$$\{v_0G_0 + v_1G_1 + \dots + v_{k-1}G_{k-1} \mid v_0, \dots, v_{k-1} \in GF(2)\}$$

Example 1. Let $g(x) = 1 + x + x^3$ be the generator polynomial of the $(7, 4)$ cyclic code C .

If $v(x) = 1 + x^2$ is the information polynomial, then the code polynomial is

$$c(x) = v(x)g(x) = (1 + x^2)(1 + x + x^3) = 1 + x + x^2 + x^5$$

and has weight 4.

Alternative method:

Since $g(x) = 1 + x + x^3$,

$$G_0 = (1,1,0,1,0,0,0),$$

$$G_1 = (0,1,1,0,1,0,0),$$

$$G_2 = (0,0,1,1,0,1,0),$$

$$G_3 = (0,0,0,1,1,0,1).$$

Since the information polynomial is $v(x) = 1 + 0x + 1x^2 + 0x^3$,

the weight of $v(x)g(x)$ equals the weight of the vector:

$$\begin{aligned} 1 \cdot G_0 + 0 \cdot G_1 + 1 \cdot G_2 + 0 \cdot G_3 &= 1 \cdot G_0 + 1 \cdot G_2 \\ &= (1,1,0,1,0,0,0) + (0,0,1,1,0,1,0) = (1,1,1,0,0,1,0) \end{aligned}$$

which has weight 4, too.

Example 2.

(a) The weight distribution of $(7, 4, 3)$ QR code is $\{1, 0, 0, 7, 7, 0, 0, 1\}$.

(b) The nonzero terms in that of $(17, 9, 5)$ QR code are as follows:

i	0	5	6	7	8	9	10	11	12	17
A_i	1	34	68	68	85	85	68	68	34	1

Proposition 1. Let C be a binary cyclic code whose generator polynomial $g(x)$ has an odd weight. Then the weight distribution of C is symmetric, i.e., $A_i = A_{n-i}$ for $i = 0, 1, \dots, n$.

Example 3. In the (17, 9, 5) QR code,

i	0	5	6	7	8	9	10	11	12	17
\overline{A}_i	1	24	44	40	45	40	28	24	10	0
\underline{A}_i	0	10	24	28	40	45	40	44	24	1

Proposition 2. Let C be a binary (n, k) QR code and let

$$\overline{C} = \{ v(x) \cdot g(x) \mid \deg v(x) < k - 1 \},$$

$$\underline{C} = \{ v(x) \cdot g(x) \mid \deg v(x) = k - 1 \}.$$

For each $i \in \{ 0, 1, \dots, n \}$, denote by \overline{A}_i and \underline{A}_i the numbers of code polynomials of weight i in \overline{C} and \underline{C} , respectively.

Then for $i = 0, 1, \dots, n$, one has

$$\overline{A}_i = \underline{A}_{n-i}.$$

Corollary. Let C be a binary quadratic residue code of length n . Then for $i = 0, 1, \dots, n$, one has the following formula:

$$A_i = \overline{A}_i + \underline{A}_{n-i}.$$

Notations.

$$C^1 = \{ v(x) \cdot g(x) \mid \deg v(x) < k - 2 \},$$

$$C^2 = \{ (x^{k-2} + v(x)) \cdot g(x) \mid \deg v(x) < k - 2 \}.$$

$$\bar{C} = C^1 \cup C^2$$

For each $i \in \{ 0, 1, \dots, n \}$, denote by A_i^1 and A_i^2 the numbers of code polynomials of weight i in C^1 and C^2 , respectively.

Proposition 3. Let C be a binary quadratic residue code of length n . Then one has the following result:

$$A_i^2 = A_{n-i}^2.$$

Theorem. (E. F. Assmus, Jr. and H. F. Mattson, Jr., 1969)

The finite extended quadratic-residue codes of length $n+1$ yields 2-designs for all n and 3-designs when $n \equiv -1 \pmod{8}$, from every weight class of code-vectors.

Proposition 4.. When C is a binary quadratic residue code of length $n \equiv -1 \pmod{8}$, then one has the following:

$$A_{2i-1}^1 = A_{2i}^2$$

Theorem. If C is a binary quadratic residue code of length $n \equiv -1 \pmod{8}$, then one has the following results:

$$1. \quad \overline{A}_i = A_i^1 + A_i^2 = \begin{cases} A_i^1 + A_{n-i-1}^1 & i : \text{odd} \\ A_i^1 + A_{i-1}^1 & i : \text{even} \end{cases}$$

$$2. \quad A_i = \overline{A}_i + \overline{A_{n-i}} = \begin{cases} A_i^1 + 2A_{n-i-1}^1 + A_{n-i}^1 & i : \text{odd} \\ A_i^1 + 2A_{i-1}^1 + A_{n-i}^1 & i : \text{even} \end{cases}$$

Example.

$$n = 7, \quad g(x) = 1 + x^2 + x^3$$

$$R = \frac{F[x]}{\langle x^7 - 1 \rangle} = \{0, 1, x, 1 + x, \dots, 1 + x + x^2 + x^3 + x^4 + x^5 + x^6\}$$

$$C = \langle 1 + x^2 + x^3 \rangle$$

$$= \{0, 1 \cdot (1 + x^2 + x^3), x \cdot (1 + x^2 + x^3), \dots, \\ (1 + x + x^2 + x^3 + x^4 + x^5 + x^6)(1 + x^2 + x^3)\}$$

$$k = n - \deg(g(x)) = 7 - 3 = 4$$

$$= \{0, 1 \cdot (1 + x^2 + x^3), x \cdot (1 + x^2 + x^3), \dots, (1 + x + x^2 + x^3)(1 + x^2 + x^3)\}$$

$v(x)$	$c(x) = v(x)g(x)$	$\text{wt}(c(x))$
0	0	0
1	$1 + x^2 + x^3$	3
x	$x + x^3 + x^4$	3
$1 + x$	$1 + x + x^2 + x^4$	4
x^2	$x^2 + x^4 + x^5$	3
$1 + x^2$	$1 + x^3 + x^4 + x^5$	4
$x + x^2$	$x + x^2 + x^3 + x^5$	4
$1 + x + x^2$	$1 + x + x^5$	3
x^3	$x^3 + x^5 + x^6$	3
$1 + x^3$	$1 + x^2 + x^5 + x^6$	4
$x + x^3$	$1 + x^4 + x^5 + x^6$	4
$1 + x + x^3$	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$	7
$x^2 + x^3$	$x^2 + x^3 + x^4 + x^6$	4
$1 + x^2 + x^3$	$1 + x^4 + x^6$	3
$x + x^2 + x^3$	$x + x^2 + x^6$	3
$1 + x + x^2 + x^3$	$1 + x + x^3 + x^6$	4