

The Weight Distributions of Some Binary Quadratic Residue Codes

Yaotsu Chang

Department of Applied Mathematics

I-Shou University

Kaohsiung, Taiwan, R.O.C

ytchang@isu.edu.tw

2004.8.3

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

- The weight distributions of binary quadratic residue codes C can be obtained by calculating certain subsets with sizes one-fourth of C .
- This result can be further improved to one-eighth when the code lengths of C are congruent to 7 modulo 8.
- An algorithm to determine the weight distributions of binary cyclic codes is given.
- As a consequence, the weight distributions of $(73, 37, 13)$, $(89, 45, 17)$, and $(97, 49, 15)$ quadratic residue codes are determined precisely; they are new.

C : a binary (n, k) cyclic code

$c = c_0c_1 \cdots c_{n-1} \in C$: a codeword, where $c_0, c_1, \dots, c_{n-1} \in GF(2)$

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

For $i \in \{0, 1, \dots, n\}$, 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

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

Example 1.

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

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

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

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

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

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

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.

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 $\beta^n = 1$.

$Q := \{i^2 \mid i = 1, \dots, n-1\}$ 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

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

Example 2.

$$n = 23 = 3 \times 8 - 1$$

$$m = 11: \quad 2^{11} - 1 = 2047 = 23 \times 89 \equiv 0 \pmod{23}$$

$E = GF(2^{11})$: the extension field of $F = GF(2)$

$\alpha \in E$: generator of $E^* = GF(2^{11}) \setminus \{0\}$

$$u = \frac{(2^{11} - 1)}{23} = 89, \quad \beta = \alpha^u = \alpha^{89}$$

$$Q_{23} = \{i^2 \pmod{23} \mid i = 1, 2, \dots, 22\} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$$

$$g(x) = \prod_{i \in Q_{23}} (x - \beta^i) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

$C = \langle g(x) \rangle$: (23, 12, 7) QR code (Golay code)

Hard-to-obtain the weight distribution

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

“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

$g(x) = g_0 + g_1x + \cdots + g_{k-1}x^{k-1}$: 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

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

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

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

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

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

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

Example 3. 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 4. The weight distribution of (7, 4, 3) QR code is

$$\{1, 0, 0, 7, 7, 0, 0, 1\}.$$

The nonzero terms in that of (23, 12, 7) Golay code are as follows:

i	0	7	8	11	12	15	16	23
A_i	1	253	506	1288	1288	506	203	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 $i = 0, 1, \dots, n$.

Let C be a binary $(n, (n+1)/2)$ QR code and let

$$C^{11} = \{c(x) \in C \mid c_{n-1} = 0\}$$

and

$$C^{12} = \{c(x) \in C \mid c_{n-1} = 1\}.$$

Note that $C = C^{11} \cup C^{12}$. For each $i \in \{0, 1, \dots, n\}$, denote by A_i^{11} and A_i^{12} the numbers of code polynomials of weight i in C^{11} and C^{12} , respectively.

Example 5. In the (23, 12, 7) Golay code with the generator polynomial

$$g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1, \text{ one has}$$

TABLE I

WEIGHT DISTRIBUTIONS OF BOTH C^{11} AND C^{12} IN THE (23, 12, 7) GOLAY CODE

j	A_i^{1j}	$i=0$	$i=7$	$i=8$	$i=11$	$i=12$	$i=15$	$i=16$	$i=23$
1	A_i^{11}	1	176	330	672	616	176	77	0
2	A_i^{12}	0	77	176	616	672	330	176	1

Proposition 2. Let C be a binary quadratic residue code of length n .

Then, $A_i^{11} = A_{n-i}^{12}$ for $i \leq n$.

Theorem 1.

Let C be a quadratic residue code of length n .

Then, for $i = 0, 1, \dots, n$, one has the following formula:

$$A_i = A_i^{11} + A_{n-i}^{11}.$$

Now, the set C^{11} will be further partitioned into two subsets of equal size:

$$C^{21} = \{c(x) \in C \mid c_{n-1} = 0, c_{n-2} = 0\}$$

and

$$C^{22} = \{c(x) \in C \mid c_{n-1} = 0, c_{n-2} = 1\}.$$

Note that $C^{11} = C^{21} \cup C^{22}$.

For each $i \in \{0, 1, \dots, n\}$, denote by A_i^{21} and A_i^{22} the numbers of code polynomials of weight i in C^{21} and C^{22} , respectively.

Example 6. The detailed distributions of code polynomials of both C^{21} and C^{22} in the $(23, 12, 7)$ Golay code with generator polynomial shown in Example 3 are listed in Table II.

TABLE II

WEIGHT DISTRIBUTIONS OF BOTH C^{21} AND C^{22} IN THE $(23, 12, 7)$ GOLAY CODE

j	A_i^{2j}	$i=0$	$i=7$	$i=8$	$i=11$	$i=12$	$i=15$	$i=16$
1	A_i^{21}	1	120	210	336	280	56	21
2	A_i^{22}		56	120	336	336	120	56

Proposition 3. Let C be a binary quadratic residue code of length

$n \equiv \pm 1 \pmod{8}$. Then $A_i^{22} = A_{n-i}^{22}$ for $0 \leq i \leq n$.

Theorem 2. (E. F. Assmus, Jr. and H. F. Mattson, Jr., 1969)

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

Proposition 4.

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

$$A_{2j-1}^{21} = A_{2j}^{22},$$

where $1 \leq j \leq (n - 1)/2$.

Theorem 3. The weight distribution $\{A_0, \dots, A_n\}$ of a binary QR code C with length n can be completely determined by the weight distribution $\{A_0^{21}, \dots, A_n^{21}\}$ of C^{21} as follows:

$$A_i = \begin{cases} A_i^{21} + 2A_{n-i-1}^{21} + A_{n-i}^{21} & \text{for odd } i \\ A_i^{21} + 2A_{i-1}^{21} + A_{n-i}^{21} & \text{for even } i \end{cases}$$

In the remainder of this talk, we consider another further partition of C^{11} into four subsets of equal size:

$$C^{31} = \{c(x) \in C \mid c_{n-1} = 0, c_{n-2} = 0, c_{n-3} = 0\},$$

$$C^{32} = \{c(x) \in C \mid c_{n-1} = 0, c_{n-2} = 0, c_{n-3} = 1\},$$

$$C^{33} = \{c(x) \in C \mid c_{n-1} = 0, c_{n-2} = 1, c_{n-3} = 0\},$$

$$C^{34} = \{c(x) \in C \mid c_{n-1} = 0, c_{n-2} = 1, c_{n-3} = 1\}.$$

That is, $C^{11} = C^{31} \cup C^{32} \cup C^{33} \cup C^{34}$.

For each $i \in \{0, 1, \dots, n\}$ and $j \in \{1, 2, 3, 4\}$, denote by A_i^{3j} the numbers of code polynomials of weight i in C^{3j} .

Example 7. The detailed distributions of code polynomials between C^{31} and C^{34} in the (23, 12, 7) Golay code are listed in Table III.

TABLE III

WEIGHT DISTRIBUTIONS BETWEEN C^{31} AND C^{34} IN THE (23, 12, 7) GOLAY CODE

j	A_i^{3j}	$i=0$	$i=7$	$i=8$	$i=11$	$i=12$	$i=15$	$i=16$
1	A_i^{31}	1	80	130	160	120	16	5
2	A_i^{32}		40	80	176	160	40	16
3	A_i^{33}		40	80	176	160	40	16
4	A_i^{34}		16	40	160	176	80	40

Proposition 5. Let C be a binary quadratic residue code of length $n \equiv -1 \pmod{8}$. Then, for $j \leq (n-1)/2$,

$$A_{2j-1}^{31} = A_{2j}^{32}.$$

Proposition 6. Let C be a binary quadratic residue code having length $n \equiv -1 \pmod{8}$. For each $i \leq n$, the following equalities are valid:

$$A_i^{32} = A_i^{33} = A_{n-i}^{34}.$$

Theorem 4. The weight distribution $\{A_0, \dots, A_n\}$ of a binary QR code C with length $n \equiv -1 \pmod{8}$ and with an odd-weighted generator polynomial can be determined completely by the weight distribution $\{A_0^{31}, \dots, A_n^{31}\}$ of C^{31} . More precisely,

$$A_i = \begin{cases} \frac{n}{n-3i} (A_i^{31} - 2A_{n-i}^{31} - 3A_{n-i-1}^{31}) & \text{for odd } i \\ \frac{n}{2n-3i} (3A_{i-1}^{31} + 2A_i^{31} - A_{n-i}^{31}) & \text{for even } i \end{cases}$$

where $i \leq n$.