The Weight Distributions of Some Binary Quadratic Residue Codes

Trieu-Kien Truong, Yaotsu Chang, and Chong-Dao Lee

Abstract—The weight distributions of binary quadratic residue codes $C$ can be computed from the weight distribution of a subset of $C$ containing one-fourth (resp., one-eighth) of the codewords in $C$ when the length of the code is congruent to 1 (resp., $-1$) 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.

Index Terms—Binary cyclic codes, quadratic residue codes, weight distributions.

I. INTRODUCTION

Let $c = c_0 \cdots c_{n-1}$ be a codeword of an $(n,k)$ code $C$. The number of nonzero terms in $c$ is called the weight of $c$ and is denoted by $w(c)$. For $i \in \{0,1,\ldots,n\}$, let $C_i$ and $A_i$ denote the set of all codewords of weight $i$ in $C$ and the cardinality of $C_i$, respectively. The sequence $A_0,A_1,\ldots,A_n$ (or the set $\{A_0,A_1,\ldots,A_n\}$) is called the weight distribution of the code $C$.

It is important to know the probabilities of error detection and error correction performance when using a block code in a system of reliable communication, because the weight distributions of codes are necessary in computing those probabilities. However, it is a very difficult task to determine the weight distributions of commonly used cyclic codes, even codes of moderate lengths [1]. In this paper, a simplified and efficient algorithm is developed to accomplish this task, in particular for arbitrary cyclic codes over GF(2).

Recently, Chang et al. [2] proposed algebraic decoding schemes for quadratic residue (QR) codes of lengths 71, 79, and 97. Hence, all binary QR codes of lengths less than 100 have been decoded except for the case of length 89. In order to obtain the performances of these codes, it is necessary to know their weight distributions. Among many others, many excellent studies of finding weight distributions for various codes were presented in [3]–[7] and the weight distributions of binary QR codes with lengths 7, 17, 23, 31, 41, 47, 71, 79, and 103 have been derived in [8]–[15] separately. In this paper, we show that the weight distributions of QR codes $C$ can be calculated from a subset of $C$ whose cardinality is one-fourth (resp., one-eighth) of $C$’s when the code length of $C$ is congruent to 1 (resp., $-1$) modulo 8. Also, the weight distributions of $(73,37,13)$, $(89,45,17)$, and $(97,49,15)$ QR codes, which are not published before, are determined precisely and are listed in Table VI. Note that the minimum weights of these three codes were given in [5].

The structure of this paper is as follows. An algorithm is given in Section II to determine the weight distributions of binary cyclic codes. Its advantages lie in the fact that the time to calculate the weight distribution of an arbitrary binary QR code can be reduced. Programs written in C++ language have been executed to calculate the weight distributions of 11 binary QR codes with code lengths up to 97. Based on this algorithm, some propositions are derived to show that the computing time for the weight distribution of a binary QR code can be reduced by a factor of four (resp., eight) when the code length is congruent to 1 (resp., $-1$) modulo 8 in Sections III and IV, respectively. Moreover, the complete weight distributions of binary QR codes, with lengths up to 103, are listed in Tables V and VI.

II. PRELIMINARIES

Let $C$ be a binary $(n,k)$ cyclic code with a generator polynomial $g(x)$ of degree $n-k$ over GF(2). Then the codewords or code polynomials of $C$ are of the form $c(x) = v(x)g(x)$, where $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}$ is the information polynomial over GF(2). The code polynomials in $C$ are given in the following way:

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

The brute-force method to obtain the complete weight distribution $\{A_0,\ldots,A_n\}$ of a code $C$ is to calculate the weights of all the code polynomials in $C$. Since it is easier and faster to add vectors than to multiply polynomials, an alternative way to calculate the weight of codewords in $C$ is considered as follows.

Let $g(x) = g_0 + g_1x + \cdots + g_{n-k-1}x^{n-k}$ be a generator polynomial of $C$. Also, let $G_0 = g_0g_1\cdots g_{n-k}0\cdots 0$ be the $n$-bit string form of $g(x)$. Similarly, let

$$G_1 = 0g_0g_1\cdots g_{n-k}0\cdots 0, G_2 = 00g_0g_1\cdots g_{n-k}0\cdots 0,$$

$$\ldots, G_{k-1} = 0\cdots 0g_0g_1\cdots g_{n-k}$$

be the $n$-bit string forms of $x \cdot g(x), x^2 \cdot g(x), \ldots, x^{k-1} \cdot g(x)$, respectively. Given an information polynomial $v(x) = v_0 + v_1x + \cdots + v_{k-1}x^{k-1}$
its associated code polynomial \( c(x) = v(x)g(x) \) is given by
\[
(v_0 + v_1 x + \cdots + v_{k-1} x^{k-1})g(x) = v_0 g(x) + (x \cdot g(x)) + \cdots + v_{k-1} x^{k-1} \cdot g(x).
\] (1)

Obviously, the weight of \( c(x) \) is equal to the weight of the sum of binary \( n \)-bit strings \( v_0 G_0 + v_1 G_1 + \cdots + v_{k-1} G_{k-1} \), where the weight of a bit string is the number of nonzero bits in it. This can be illustrated in the following example.

**Example 1:** Let \( C \) be the \((7, 4)\) cyclic code generated by \( g(x) = 1 + x + x^3 \). Then, \( G_0 = 1101000, G_1 = 0011010, G_2 = 0011010, G_3 = 0001101 \). If \( v(x) = 1 + x^2 \), then the weight of \( v(x)g(x) = (1 + x^2) \cdot (1 + x + x^3) = 1 + x + x^2 + x^5 \) equals 4. By (1), \( c(x) = 1 \cdot g(x) + x^2 \cdot g(x) \) and the weight of \( 1 \cdot G_0 + 1 \cdot G_2 = 1101000 + 0011010 = 1110100 \) is 4 as well.

The determination of the weight distribution of the code \( C = \{v(x)g(x) \mid \deg v(x) \leq k-1 \} \) is therefore equivalent to the determination of the weight distribution of the set of \( n \)-bit strings
\[
\{v_0 G_0 + v_1 G_1 + \cdots + v_{k-1} G_{k-1} \mid v_0, \ldots, v_{k-1} \in GF(2)\}.
\]

Consequently, the weight distribution \( \{A_0, \ldots, A_n\} \) of the binary \((n, k)\) code can be obtained by the following algorithm:
1. Set \( A_0 = 0, A_1 = 0, \ldots, A_n = 0, \) and \( i = 1 \).
2. Express \( i = v_0 + v_2 2^1 + \cdots + v_{k-1} 2^{k-1} \) in its binary expansion form.
3. Make the codeword \( c = v_0 G_0 + v_1 G_1 + \cdots + v_{k-1} G_{k-1} \).
4. Count the weight of the codeword \( r = \text{wt}(v_0 G_0 + v_1 G_1 + \cdots + v_{k-1} G_{k-1}) \).
5. Set \( A_r + 1 \) into \( A_r \).
6. Set \( i+1 \) into \( i \); if \( i > 2^{k-1} - 1 \), stop; Otherwise, go to step 2.

In this algorithm, only the additions of bit strings are used, hence, the weight distributions of binary cyclic codes can be calculated efficiently. The truth of this algorithm has been checked by obtaining all the known results of QR codes of length less than 100.

Next, a brief review about the binary QR code is given. A binary QR code \( C \) of length \( n \) is defined as follows: For a prime number \( n \) of the form \( n \equiv \pm 1 \pmod{8} \), let \( Q \) be the collection of all nonzero quadratic residues modulo \( n \); that is,
\[
Q = \{ i^2 \pmod{n} \mid i = 1, 2, \ldots, n-1 \}.
\]

Also, let \( E = GF(2^m) \) be the finite field of order \( 2^m \), where \( m \) is the smallest positive integer such that \( 2^m - 1 \) is divisible by \( n \). Then the set of nonzero elements in \( E \) forms a cyclic group under the multiplication. If \( \alpha \in E \setminus \{0\} \) is a generator of that cyclic group, then the element \( \beta = \alpha^{(2^m-1)/n} \) is a primitive \( n \)-th root of unity in \( E \). Note, \( g(x) \) be the polynomial defined as \( g(x) = \prod_{i=0}^{n-1} (x - \beta^i) \). Then \( g(x) \) is a factor of \( x^n - 1 \) with degree \( \deg g(x) = (n - 1)/2 \). Since \( n \) has the form \( n \equiv \pm 1 \pmod{8}, 2 \in Q \). Hence, the square of any root of \( g(x) \) is also a root of \( g(x) \) and the minimal polynomial of \( \beta \) divides \( g \). Therefore, \( g(x) \) is a product of irreducible polynomials over \( GF(2) \), which implies \( g(x) \in GF(2)[x] \). The cyclic code \( C \) generated by \( g(x) \) is called a binary quadratic residue code of length \( n \), with dimension \( k = (n + 1)/2 \).

The notation of \( t \)-designs is used to derive the main results of this paper. To see this, let \( X \) be a set of \( v \) elements, called points. For \( k < v \), let \( B \) be a collection of distinct \( k \)-subsets of \( X \), called blocks. The pair \((X, B)\) is called a \( t \)-\((v, k, \lambda)\) design if every \( t \)-subset of \( X \) is contained in exactly \( \lambda \) blocks in \( B \). For two disjoint subsets \( I \) and \( J \) of \( X \) with \( |I| = i \) and \( |J| = j \), let \( \lambda_{ij} \) be the number of blocks in \( B \) which contain \( I \) but disjoint from \( J \).

**Theorem 1:** [16, p. 100, Theorems 11.3, 4]. Let \((X, B)\) be a \( t \)-\((v, k, \lambda) \) design. Then
i) for \( 0 \leq i \leq t \), the pair \((X, B)\) is an \( i \)-\((v, k, \lambda_i) \) design with
\[
\lambda_i = \lambda \left( \binom{v-i}{t-i} / \binom{k-i}{t-i} \right);
\]
ii) the number \( \lambda_{ij} \) is independent of the choice of \( I \) and \( J \) if \( i + j \leq t \).

There is a connection between binary QR codes and \( t \)-designs; some designs can be constructed from binary QR codes. First, let \( C \) be a binary QR code of length \( n \) and let \( C^* \) be the extended code of \( C \) whose codewords are obtained by adjoining a parity-check bit to every codeword \( c \) of \( C \). Actually, the extended code can be obtained by adding a parity-check bit to any fixed position of \( c \). For convenience, we add the parity-check bit to the first position of \( c \). Next, let \( X = \{0, 1, \ldots, n\} \) and for every codeword \( c = c_0 c_1 c_2 \cdots c_0 \) of \( C^* \), let \( B_c \) be the collection of indices \( i \)'s so that \( c_i \) is not zero, i.e.,
\[
B_c = \{ i \mid c_i = 1, \text{ for } i = 0, 1, \ldots, n \}.
\]

If the weight of \( c \) is \( k \), then \( B_c \) is a subset of \( X \) of cardinality \( k \). Finally, let \( B \) be the collection of all \( k \)-subsets of \( X \) associated to all the codewords of \( C^* \) of weight \( k \). Assmus and Mattson [17] proved that the pair \((X, B)\) forms a \( t \)-design for some \( t \geq 2 \).

**Theorem 2:** [17, p. 137, Theorem 4.1]. The pair \((X, B)\) constructed above forms a \( 2 \)-\((n + 1, 2j, \lambda^0) \) design for all \( n \) and \( 3 - (n + 1, 2j, \lambda^0) \) design when \( n \equiv -1 \pmod{8} \), from every class of codewords of weights \( 2j \).

Having detoured briefly through the topic of combinatorial design, we return to our main concern, weight distribution.

**Lemma 1:** If the generator polynomial \( g(x) \) of a binary cyclic code is of odd weight, then the all-one polynomial \( 1 + x + \cdots + x^{n-1} \) is a code polynomial.

**Proof:** If the weight of \( g(x) \) is odd, then \( g(1) \neq 0 \), i.e., \( x + 1 \) is not a factor of \( g(x) \). Hence, \( g(x) \) divides \( 1 + x + \cdots + x^{n-1} \) because \( g(x)|1 + x^n \).

Throughout the rest of this paper, we assume the generator polynomial \( g(x) \) has odd weight and let
\[
h(x) = (1 + x + \cdots + x^{n-1})/g(x).
\]
Some basic properties of the numbers \( A_i \)'s are considered in Proposition 1 and Theorem 3 as follows.
**Proposition 1:** Let $C$ be a binary cyclic code with an odd weight generator polynomial $g(x)$. Then the weight distribution of $C$ is symmetric, i.e., $A_i = A_{n-i}$ for $i = 0, 1, \ldots, n$.

**Proof:** Since $\text{wt}(g(x))$ is odd, $1 + x + \cdots + x^{n-1} \in C$ by Lemma 1. For any $c(x) \in C$ with $\text{wt}(c(x)) = i$, we have

$$\text{wt}(c(x) + (1 + x + \cdots + x^{n-1})) = n - \text{wt}(c(x)) = n - i.$$ Given $i \leq n$, the mapping defined by assigning $c(x)$ to $c(x) + (1 + x + \cdots + x^{n-1})$ is a one-to-one correspondence from $C_i$ to $C_{n-i}$; it follows that $A_i = A_{n-i}$.

A relation between $A_{2j-1}$ and $A_{2j}$, for $j = 1, 2, \ldots, (n - 1)/2$, can be derived from a result in Pless’s book [1, p. 124, (vi) of Theorem 83] as follows.

**Theorem 3:** If $C$ is a binary QR code with an odd weight generator polynomial, then $2^j A_{2j} = (n - (2^j - 1)) A_{2j-1}$ for $j \leq (n - 1)/2$.

Some notations used in proving the main results in Sections III and IV are given below. First, let $V$ be the set of all possible binary information polynomials of degree less than $k$, i.e., $V = \{v(x) | \deg v(x) < k\}$. The set $V$ is divided evenly into two subsets $V^{11}$ and $V^{12}$, where

$$V^{11} = \{v(x) \in V | \deg v(x) < k - 1\}$$

and

$$V^{12} = \{v(x) \in V | \deg v(x) = k - 1\}.$$ Clearly, $|V^{11}| = |V^{12}| = 2^{k-1}$. The following example illustrated these notations.

**Example 2:** Let $C$ be the $(7, 4, 3)$ Hamming code generated by $g(x) = x^3 + x + 1$. Then

$$V^{11} = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\} \text{ and } V^{12} = \{x^3, x^3 + 1, x^3 + x, x^3 + x + 1, x^3 + x^2, x^3 + x^2 + 1, x^3 + x^2 + x, x^3 + x^2 + x + 1\}.$$ If $v(x) = v_{k-1}x^{k-1} + \cdots + v_1x + v_0 \in V$, then the set $V^{11}$ can be expressed as $V^{11} = \{v(x) \in V | v_{k-1} = 0\}$. In Section III, the set $V^{11}$ will be further partitioned into two subsets of equal size:

$$V^{21} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 0\}$$

and

$$V^{22} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 1\}.$$ In Section IV, we consider another further partition of $V^{11}$ into four subsets of the same size:

$$V^{31} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 0, v_{k-3} = 0\}$$

$$V^{32} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 0, v_{k-3} = 1\}$$

$$V^{33} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 1, v_{k-3} = 0\}$$

$$V^{34} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 1, v_{k-3} = 1\}.$$ and

$$V^{34} = \{v(x) \in V | v_{k-1} = 0, v_{k-2} = 1, v_{k-3} = 1\}.$$ Next, for suitable indices $i$ and $j$, let

$$C^{ij} = \{v(x) \cdot g(x) | v(x) \in V^{ij}\}.$$ Then $|C^{ij}| = |V^{ij}| = 2^{k-i}$. For $u \in \{0, 1, \ldots, n\}$, let

$$C^{ij}_u = \{c(x) \in C^{ij} | \text{wt}(c(x)) = u\}$$

and let

$$V^{ij}_u = \{v(x) \in V^{ij} | \text{wt}(v(x) \cdot g(x)) = u\}.$$ Denote by $A^{ij}_u$ the cardinality of $C^{ij}_u$. Then

$$A^{ij}_u = |V^{ij}_u|.$$ **Example 2. (Continued):**

$$C^{11} = \{v(x) \cdot g(x) | v(x) \in V^{11}\} = \{0, x^3 + x + 1, x^4 + x^2 + x, x^4 + x^2 + x + 1, x^5 + x^4 + x^3 + x, x^5 + 1\}.$$ $C^{12} = \{v(x) \cdot g(x) | v(x) \in V^{12}\} = \{x^6 + x^4 + x^3, x^6 + x^4 + 1, x^6 + x^4 + x + 1, x^6 + x^3 + x^2, x^6 + x^3 + x = 1, x^6 + x^3 + x + 1, x^6 + x^5 + x^4 + x^3 + x^2 + 1, x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\}.$$ By counting the weights of code polynomials in both $C^{11}$ and $C^{12}$, the result is as shown in Table I.

**Example 3:** Based on the above algorithm, the weight distributions of code polynomials of both $C^{21}$ and $C^{22}$ (resp., $C^{31}$, $C^{32}$, $C^{33}$, and $C^{34}$) in the $(23, 12, 7)$ Golay code with generator polynomial $g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$ are listed in Table II (resp., Table III).

In both Sections III and IV, if the generator polynomial $g(x)$ of a binary QR code $C$ is given by

$$g(x) = x^{k-1} + g_{k-2}x^{k-2} + \cdots + g_1x + 1$$

then the code polynomial of $C$ is of the form

$$c(x) = v(x)g(x) = c_{n-1}x^{n-1} + \cdots + c_0$$

where $c_{n-1} = v_{k-1}$ and $c_{n-2} = v_{k-2} + v_{k-1} \cdot g_{k-2}$. This implies that

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

and

$$C^{22} = \{c(x) \in C | c_{n-1} = 0, c_{n-2} = 1\}.$$
Finally, for each information polynomial \( v(x) \), the notation \([v(x)]\), used in the proofs of Propositions 4 and 7, is defined to be \([v(x)] = v(x)/x^k\) if \( v_0 = 1 \) and \( v_{-k} = \cdots = v_0 = 0 \). From this definition, one has the following properties: i) \( \deg([v(x)]) \leq \deg(v(x)) \), ii) \( \text{wt}([v(x)]) = \text{wt}(v(x)) \), and iii) the constant term of \([v(x)]\) is one.

### III. SOME PROPERTIES OF THE WEIGHT DISTRIBUTIONS OF BINARY QR CODES

Consider a binary \((n, k)\) QR code \( C \) with generator polynomial \( g(x) \). In this section, we will show that the weight distribution \( A_i \)'s of \( C \) can be expressed as function in terms of \( A_{2i} \)'s, the weight distribution of \( C^{2l} \).

From the construction of \( g(x) \), \( 1 \) is not a root of \( g(x) \). Hence, \( g(x) \) divides \( 1 + x + \cdots + x^{n-1} \), and the quotient polynomial \( h(x) = (1 + x + \cdots + x^{n-1})/g(x) \) is of degree \( k - 1 \) as well.

Furthermore, one observes from Example 2 that the distribution is “antisymmetric,” i.e., \( A_{11} = A_{12} \). Indeed, this observation is true for all binary QR codes.

**Proposition 2:** \( A_{11} = A_{12} \) for \( i \leq n \).

**Proof:** Due to \( A_{ij} = |V_i^2| \), it suffices to build a one-to-one correspondence between the two sets \( V_{i1} \) and \( V_{i2} \). For each \( v(x) \in V_i^{11} \), \( \deg(v(x)) < k-1 \) and \( \text{wt}(v(x) \cdot g(x)) = i \), which implies that

\[
\deg(v(x) + h(x)) = k - 1
\]

and

\[
\text{wt}((v(x) + h(x)) \cdot g(x)) = n - i.
\]

Hence, \( v(x) + h(x) \in V_{n-i}^{12} \), and the mapping from \( v_i^{11} \) to \( V_{n-i}^{12} \), defined by assigning \( v(x) \) into \( v(x) + h(x) \) is well defined and one-to-one. Therefore,

\[
A_{11} = |C_i^{11}| = |V_i^{11}| = |V_i^{12}| = |C_{n-i}^{12}| = A_{2i}^{12} \]

as required.

As an immediate consequence of Proposition 2, one has the following result.

**Theorem 4:** Let \( C \) be a binary QR code having length \( n \). The weight distribution \( A_i \) of \( C \) can be determined completely by

\[
A_i = A_{11} + A_{12} \]

for \( i = 0, 1, \ldots, n \).

Some formulas regarding the numbers \( A_{2i} \)'s are listed in Proposition 3. Parts of them will be used to prove Theorem 6 in the next section.

**Proposition 3:** For \( i \leq n \) and \( j \leq (n - 1)/2 \), the following equalities hold:

i) \( A_i = (n/i)A_{12} \),
ii) \( iA_{11} = (n - i)A_{12} \),
iii) \( 2jA_{2j} = (n - 2j)A_{2j-1} \),
iv) \( (2j - 1)A_{2j} = (n - 2j + 1)A_{2j-1} \).

**Proof:** For each \( i \leq n \), let \( M_i \) be the matrix whose rows are all the codewords of weight \( i \) in \( C \). Then the number of nonzero entries in the matrix \( M_i \) equals \( iA_i \) since \( M_i \) has \( A_i \) rows of weight \( i \). Next, since \( C \) is a cyclic code, each column vector of \( M_i \) has the same weight that equals the number \( r \) of codewords \( c \) in \( C_r \) with \( c_{n-r} = 1 \). They are exactly the codewords in \( C_r \). Thus, \( r = A_{2r} \). By counting the number of \( i \)'s in the matrix \( M_i \) in two different ways, one has \( nr = iA_i \), i.e., \( nA_{12} = iA_i \) and the proof of i) is completed.

Equality ii) can be obtained easily from i).

Combining i) and ii), we obtain \( A_{11} = ((n - i)/n)A_i \). Replacing \( i \) by \( 2j \) gives \( A_{2j} = ((n - 2j)/n)A_{2j} \). Since \( A_{2j} = ((n - 2j + 1)/2j)A_{2j-1} \) by Theorem 3, we have

\[
A_{2j} = ((n - 2j)/n) \cdot ((n - 2j + 1)/2j)A_{2j-1} \]

Next, substituting \( i = 2j - 1 \) into \( A_{11} = ((n - i)/n)A_i \), it becomes \( 2jA_{2j} = (n - 2j + 1)A_{2j-1} \).

To prove iv), multiplying \( A_{2j} = (n-i)A_{2j} \) by \( n-i \) and then replacing \( i \) by \( 2j - 1 \), we have

\[
(n - 2j + 1)A_{2j-1} = (n - 2j + 1) \cdot \left( \frac{n}{2j - 1} \right) A_{2j-1} \]

Next, in i) replacing \( i \) by \( 2j \) and then applying \( A_{2j-1} = (2j/(n - 2j + 1))A_{2j} \) from Theorem 3, (4) becomes

\[
A_{2j} = ((n - 2j + 1)/(2j - 1))A_{2j-1} \]

which implies \( (2j - 1)A_{2j} = (n - 2j + 1)A_{2j-1} \).
For each $v(x) \in V_i^{2^2}$, $\deg(v(x)) = k - 2$ and $\text{wt}(v(x) \cdot g(x)) = i$. Since the polynomial $[v(x)]$, defined in Section II, has constant term one, $[v(x)] + h(x)$ is divided by $x$. Moreover, the quotient $([v(x)] + h(x))/x$ has degree $k - 2$ and its related code polynomial $([v(x)] + h(x))/x \cdot g(x)$ has weight $n - i$. Thus, $([v(x)] + h(x))/x \in V_{n-i}^{2^2}$. Next, define a mapping $\varphi$ from $V_i^{2^2}$ to $V_{n-i}^{2^2}$ by $\varphi(v(x)) = ([v(x)] + h(x))/x$. It is clear that $\varphi$ is well defined. Moreover, $\varphi$ is also one-to-one. If $u(x), v(x) \in V_i^{2^2}$ such that $\varphi(u(x)) = \varphi(v(x))$, then
$$
([u(x)] + h(x))/x = ([v(x)] + h(x))/x
$$
$$
[u(x)] + h(x) = [v(x)] + h(x)
$$
and
$$
[u(x)] = [v(x)].
$$
Since $u(x), v(x) \in V_i^{2^2}$, $\deg(u(x)) = \deg(v(x)) = k - 2$. Therefore, $u(x) = v(x)$ and this implies that $\varphi$ is one-to-one. Hence,
$$
A_{i}^2 = |V_i^{2^2}| \leq |V_{n-i}^{2^2}| = A_{n-i}^2
$$
for each $i \in \{0, 1, \ldots, n\}$ and then
$$
A_{2^2} = A_{0}^2 + \ldots + A_{n}^2 \leq A_{n}^2 + \ldots + A_{0}^2 = A_{2^2}^2.
$$
The only possibility for all these to be true is $A_{i}^2 = A_{n-i}^2$ for each $i$, as required.

**Proposition 5:** $A_{j+1}^{2^2} = A_{2^2}^{2^2}$ for $j \leq (n - 1)/2$.

**Proof:** Recall that $C^*$ is the extended code of $C$ defined in Section II. That is, every codeword in $C^*$ has the form $c^* = c_n c_{n-1} \ldots c_0$, where $c = c_{n-1} \ldots c_0$ is a codeword of $C$ and $c_n \equiv (c_{n-1} + \ldots + c_0) \pmod 2$. Denote the set of codewords of weight $2j$ in $C^*$ by $C_{2j}^{2^2}$. Now, let $X = \{0, 1, \ldots, n\}$ and let $\mathcal{B}$ be the collection of blocks related to all the codewords in $C_{2j}^{2^2}$.

Then, by Theorem 2, the pair $(X, \mathcal{B})$ forms a $2 - (n, 1, 2j, \lambda)$ design. By (ii) of Theorem 1
$$
\lambda_0^2 = |\{c^* \in C_{2^2}^*|c_{n-1} = 0, c_{n-2} = 0\}| = |\{c^* \in C_{2^2}^*|c_n = 0, c_{n-1} = 0\}|.
$$
Since all the codewords of the first set are precisely those obtained by adjoining $c_{n} = 1$ to every codeword of $C_{2j-1}^*$ and those obtained by adjoining $c_{n} = 0$ to every codeword of $C_{2j}^*$, one has $\lambda_0^2 = |C_{2j-1}^*| + |C_{2j-2}^*| = A_{2j-1}^2 + A_{2j-2}^2$. Similarly, one has $\lambda_0^2 = |C_{2j+1}^*| + |C_{2j}^*| = A_{2j+1}^2 + A_{2j}^2$ by analyzing codewords of the second set. Therefore, $A_{j+1}^{2^2} = A_{2^2}^{2^2}$ for $j \leq (n - 1)/2$.

Now we are ready to prove the first of the main results of this paper.

**Theorem 5:** The weight distribution $\{A_0, \ldots, A_n\}$ of a binary QR code $C$ with length $n$ can be completely determined by the weight distribution $\{A_{2^1}, \ldots, A_{2^1}^n\}$ of $C_{2^1}$ as follows:
$$
A_i = \begin{cases} A_{i+1}^2 + 2A_{i-1}^2 + A_{i-2}^2, & \text{for odd } i \\ A_{i+1}^2 + 2A_{i-1}^2 + A_{i-2}^2, & \text{for even } i \end{cases}
$$
(5)

**Proof:** Since $A_{i}^2 = |C_{i}^2|$, one has $A_{1}^2 = A_{2}^2 + A_{1}^2$ and $A_{n}^2 = A_{n-1}^2 + A_{n-2}^2$. From the formula $A_i = A_{i+1}^2 + A_{i-1}^2$ given in (2), one has $A_i = A_{i+1}^2 + A_{i-1}^2 + A_{i-2}^2$. Therefore,
$$
A_i = A_{i+2}^2 + 2A_{i-1}^2 + A_{i-2}^2
$$
(6.1)
$$
= A_{i+2}^2 + 2A_{i-1}^2 + A_{i-2}^2
$$
(6.2)
by Proposition 4. If $i$ is even (resp., $i$ is odd or $n - i$ is even), then $A_{i+1}^2 = A_{i+1}^2$ (resp., $A_{n-i}^2 = A_{n-i}^2$) by Proposition 5. Substituting these into (6.1) and (6.2) yields (5).

Theorem 5 shows that the weight distribution of a binary QR code $C$ can be obtained by calculating that of a certain subset having size one-fourth of $C$. 

---

**TABLE V**

<table>
<thead>
<tr>
<th>Weights</th>
<th>QR(7,4,3)</th>
<th>QR(23,12,7)</th>
<th>QR(31,16,7)</th>
<th>QR(47,24,11)</th>
<th>QR(71,36,11)</th>
<th>QR(79,40,15)</th>
<th>QR(103,52,19)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>506</td>
<td>465</td>
<td>433</td>
<td>497</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1288</td>
<td>5208</td>
<td>12972</td>
<td>2485</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>18259</td>
<td>178365</td>
<td>47570</td>
<td>19513</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>356730</td>
<td>166495</td>
<td>78052</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1664740</td>
<td>5084310</td>
<td>3220672</td>
<td>218875</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2330636</td>
<td>13219206</td>
<td>9662016</td>
<td>919275</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>3840840</td>
<td>4103051184</td>
<td>158640600</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1710651635</td>
<td>3705860928</td>
<td>428330248</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2688166855</td>
<td>6882311352</td>
<td>11626317816</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>7377935180</td>
<td>31183071220</td>
<td>174684872920</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>9222418975</td>
<td>47824606380</td>
<td>39304964070</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>12879738244</td>
<td>118486862496</td>
<td>343279473780</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>144817051384</td>
<td>648830563940</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>195535169504</td>
<td>33992695303425</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>5437244485480</td>
<td>174966874539720</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>23858927931780</td>
<td>478328764312680</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>558050225031460</td>
<td>70302265147378</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE VI
WEIGHT DISTRIBUTIONS OF BINARY QR CODES WITH LENGTHS 17, 41, 73, 89, AND 97

<table>
<thead>
<tr>
<th>weights</th>
<th>QR(17,9,5)</th>
<th>QR(41,21,9)</th>
<th>QR(73,37,13)</th>
<th>QR(89,45,17)</th>
<th>QR(97,49,15)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>68</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>85</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>410</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1312</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>3034</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>7585</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>16605</td>
<td>1533</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>33210</td>
<td>6570</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>60024</td>
<td>19272</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>97539</td>
<td>69861</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>146370</td>
<td>266008</td>
<td>54824</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>195160</td>
<td>827820</td>
<td>219296</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>232060</td>
<td>2292200</td>
<td>626560</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>255266</td>
<td>6188940</td>
<td>2192960</td>
<td>741468</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>15841584</td>
<td>7462917</td>
<td>3375978</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>37443744</td>
<td>23067198</td>
<td>1162504</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>82642716</td>
<td>66429244</td>
<td>40893648</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>172127325</td>
<td>182680421</td>
<td>126088748</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>337713987</td>
<td>476804328</td>
<td>360406410</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>623471976</td>
<td>1173672192</td>
<td>998048250</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>1086405418</td>
<td>2739870518</td>
<td>2614461952</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>1784808901</td>
<td>6066856147</td>
<td>6536154880</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>2766489030</td>
<td>12753805999</td>
<td>15589859400</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>4057517244</td>
<td>25507611998</td>
<td>35337014640</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>5630905444</td>
<td>48541216592</td>
<td>76345991760</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>7389493389</td>
<td>8798095073</td>
<td>157463608005</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>9183695358</td>
<td>15199978216</td>
<td>31018632386</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>10804347480</td>
<td>250352582396</td>
<td>583880136256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>12034542312</td>
<td>393412044806</td>
<td>1050952990464</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>12703127996</td>
<td>590118067209</td>
<td>1809974594688</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>845206560770</td>
<td>2983811977229</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>1156598451580</td>
<td>4711282061520</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>1512562040968</td>
<td>7127686860200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>1890702551120</td>
<td>10335148586290</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>2259707219462</td>
<td>14368570181112</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>2582522563528</td>
<td>19156093574816</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>28225905551580</td>
<td>24503812839176</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>2950890125870</td>
<td>30072861211716</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>35419208941404</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>40039105759848</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>43447332367896</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>45257637883225</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IV. WEIGHT DISTRIBUTIONS FOR THE BINARY QR CODES OF LENGTH CONGRUENT TO \(-1\) MODULO 8

We assume that the binary QR code \(C\) has length \(n \equiv -1 \pmod{8}\) in this section. The aim in this section is to show that the complete weight distribution \(\{A_i\}\) can be determined from the weight distribution \(\{A_{3i}\}\). Some phenomena found in Table III of Example 3 in Section II provide motivations for Proposition 6 and 7 given below. Also, the argument used in the proof of Proposition 5 can be modified to prove Proposition 6.

Proposition 6: \(A_{3j-1}^{31} = A_{3j}^{32}\) for \(j \leq (n - 1)/2\).

Proof: Let \(C^9, X,\) and \(\mathcal{B}\) be those defined in Proposition 5; then the pair \((X, \mathcal{B})\) forms a 3-design according to Theorem 2. By ii) of Theorem 1

\[
\lambda_0^3 = \left\{ e^* \in C_{3j}^9 | e_{n-1} = e_{n-2} = e_{n-3} = 0 \right\}
\]

This leads to

\[
\lambda_0^3 = |C_{3j-1}^{31}| + |C_{3j}^{32}| = |C_{3j}^{31}| + |C_{3j}^{32}|
\]

i.e.,

\[
\lambda_0^3 = A_{3j-1}^{31} + A_{3j}^{32} = A_{3j}^{32} + A_{3j}^{32}
\]

consequently, \(A_{3j-1}^{31} = A_{3j}^{32}\), as required.

Recall that

\[
g(x) = x^{k-1} + g_{k-2}x^{k-2} + \cdots + g_1x + 1
\]

and

\[
h(x) = (1 + x + \cdots + x^{n-1})/g(x).
\]

Assume \(h(x) = x^{k-1} + h_{k-2}x^{k-2} + \cdots + h_1x + 1\). We have \(g_{k-2} + h_{k-2} = 1\) because \(g(x)h(x) = 1 + x + \cdots + x^{n-1}\).
Proposition 7: For each \( i \leq n \), the following equalities are valid:

i) \( A_{32}^i = A_{33}^i = A_{34}^i \) when \( g_{k-2} = 0 \);

ii) \( A_{42}^i = A_{33}^{n-i} = A_{34}^{n-i} \) when \( g_{k-2} = 1 \).

Proof: If \( v(x) \in V_{32} \), then

\[
\deg[v(x)] = \deg v(x) = k - 3.
\]

Since \( \deg h(x) = k - 1 \)

\[
\deg((v(x) + h(x))/x) = \deg h(x) - 1 = k - 2
\]

and the second leading coefficient of \( (v(x) + h(x))/x \) equals \( h_{k-2} \). Therefore, \( (v(x) + h(x))/x \) is in either \( V_{33} \) or \( V_{34} \) depending on whether \( h_{k-2} \) is 0 or 1, or equivalently, depending on whether \( g_{k-2} \) is 0 or 1. If \( g_{k-2} = 0 \), then \( h_{k-2} = 1 \) and \( (v(x) + h(x))/x \) is in \( V_{34} \). Then by a proof similar to that of Proposition 4, we have \( A_{32}^i = A_{34}^i \) for \( i \leq n \).

When \( g_{k-2} = 0 \), the proof of \( A_{32}^i = A_{33}^i \) is analogous to the proof of Proposition 6 by calculating the numbers \( \lambda_2^i \) and \( \lambda_3^i \).

Equality in ii) can be proved similarly.

Another main result of this paper is included in the following Theorem.

Theorem 6: The weight distribution \( \{A_0, \ldots, A_n\} \) of a binary QR code \( C \) with length \( n \equiv -1 \pmod{8} \) and with an odd weight generator polynomial can be determined completely by the weight distribution \( \{A_{31}^0, \ldots, A_{n}^0\} \) of \( C_{31} \). More precisely

\[
A_i = \begin{cases} 
\frac{n}{2} \cdot (A_{31}^{i} - 2A_{33}^{n-i} - 4A_{34}^{n-i}), & \text{for odd } i \\
2 \cdot (A_{31}^{i} + 2A_{31}^{n-i} - 4A_{33}^{n-i}), & \text{for even } i
\end{cases}
\]

where \( i \leq n \).

Proof: Without loss of generality, assume that the second leading coefficient of the generator polynomial \( g(x) \) is zero, i.e., \( g_{k-2} = 0 \). One may assume by Propositions 6 and 7 that the weight distributions of \( C_{31} \), \( C_{32} \), \( C_{33} \), and \( C_{34} \) are as shown in Table V. It follows from Proposition 5 that \( A_{32}^{n-1} = A_{32}^{n-2} \) which implies \( A_{32}^{n-1} + A_{32}^{n-2} = A_{32}^{n-3} + A_{34}^{n-2} \). That is, \( a + x = a + y \) and \( x = y \).

If the index \( i \) of \( A_i \) is odd, say \( i = 2u - 1 \), then

\[
A_i = A_{2u-1} = A_{32}^{n-1} + 2A_{32}^{n-2} + 3A_{32}^{n-2u+1} = a + 3x + d + 3x
\]

by Theorem 5. Next, by taking

\[
2j = n - (2u - 1) \quad \text{or} \quad 2j - 1 = n - 2u
\]

one has \( (n-(2u-1)) \cdot A_{31}^{(n-(2u-1))} = (n-(2u-1)) \cdot A_{31}^{2u-1} - (n-(2u-1)) \cdot A_{n} \)
by iii) of Proposition 3. Hence,

\[
(n-2u+1) \cdot (d + c + c + x) = (2u-1) \cdot (c + y + y + a).
\]

This implies that

\[
x = \frac{1}{n-3} (2u-1) \cdot (2u-1) \cdot (a + (3) \cdot (2u-1) - 2n) \cdot c
- (n-2u-1) \cdot d
\]

\[
= \frac{1}{n-3} (i \cdot a + (3i - 2n) \cdot c - (n-i) \cdot d).
\]

Substituting \( x \) into the formula for \( A_i \) one has

\[
A_i = n \cdot (A_{31}^{i} - 2A_{33}^{n-i} - 3A_{34}^{n-i-1})/(n-3i)
\]

when \( i \) is odd. On the other hand, if the index \( i \) of \( A_i \) is even, say \( i = 2u \), then by a similar argument, one has the formula

\[
A_i = n \cdot (3A_{31}^{i} - 2A_{31}^{n-i} - 2A_{34}^{n-i-1})/(2n-3i)
\]

when \( i \) is even.

V. CONCLUSION

Indeed, the formula in Theorem 6 holds for all known cases, not just for the case \( n \equiv -1 \pmod{8} \). The authors believe that the same formula may hold in general.

The known weight distributions of binary QR codes are listed in two tables. Table V contains the weight distributions of binary QR codes whose lengths are of the form \( n \equiv -1 \pmod{8} \), namely, 7, 23, 31, 47, 71, 79, and 103 whereas Table VI contains those of binary QR codes of length \( n \equiv 1 \pmod{8} \), namely, 17, 41, 73, 89, and 97. All the binary QR codes of lengths up to 103 are included in these two tables. Among them, the weight distributions of QR codes of lengths 73, 89, and 97 which are not yet discovered are new results given in this paper.

ACKNOWLEDGMENT

The authors would like to express their appreciation to the Associate Editor, Dr. McEliece, for handling this paper and to the reviewers for their constructive and helpful comments and suggestions.

REFERENCES


