Letter

Binary Constant Weight Codes Based on Cyclic Difference Sets*

Nian Li†, Student Member, Xiangyong ZENG†‡, Member, and Lei HU††b, Nonmember

SUMMARY Based on cyclic difference sets, sequences with two-valued autocorrelation can be constructed. Using these constructed sequences, two classes of binary constant weight codes are presented. Some codes proposed in this paper are proven to be optimal.

key words: cyclic difference set, sequence with two-valued autocorrelation, constant weight code, Hamming distance

1. Introduction

Binary constant weight codes play an important role in coding theory, and have important applications in communications. An \((n, M, d, w)\) code is the code with length \(n\), number of codewords \(M\), minimum Hamming distance \(d\) and constant weight \(w\). The central problem regarding constant weight codes is the following: what is the maximum number of codewords in a binary constant weight code with given parameters \(n\), \(d\), and \(w\)? This number is denoted by \(A(n, d, w)\). An \((n, M, d, w)\) code is said to be optimal if \(M = A(n, d, w)\). With a variety of methods from mathematics, many constant weight codes were constructed [2], [4], [8], [9], [11]. Recently, new binary \((2^n-1, 2^n-2, \cdots, 2, 0)\) and \((2^n-1, 2^n-1, \cdots, 2, 0, 0)\) constant weight codes were presented based on \(m\)-sequences. The codes can achieve optimum for some values of the parameter \(n\) [13].

A \(k\)-element subset \(D\) of an additive group \(G\) of order \(v\) is called a \((v, k, \lambda)\)-difference set in \(G\) provided that the multiset \(\{d_1 - d_2 | d_1, d_2 \in D, d_1 \neq d_2\}\) contains each non-identity element of \(G\) exactly \(\lambda\) times. In particular, \(D\) is called a cyclic difference set if \(G\) is taken to be the cyclic group \(Z_v = Z/\alpha Z\). From a \((v, k, \lambda)\)-cyclic difference set \(D\), a binary sequence \(a = (a_0, a_1, \cdots, a_{v-1})\) of period \(v\) can be defined as follows:

\[
a_{i \text{ (mod } v\text{)}} = \begin{cases} 
0, & \text{if } i \in D, \\
1, & \text{otherwise.}
\end{cases}
\]

With these sequences derived from cyclic difference sets, we extend the method of [13] to construct new binary constant weight codes. Some codes are proven to be optimal.

This paper is organized as follows: Sect.2 discusses the properties of the two-valued autocorrelation sequences derived from cyclic difference sets. Based on the sequences, two classes of binary constant weight codes are constructed in Sect.3, and the minimum Hamming distance is characterized. Section 4 shows some constructed codes are optimal.

2. The Properties of Sequences from Cyclic Difference Sets

In this section, some basic properties of cyclic difference set are listed, and we discuss the properties of the two-valued autocorrelation sequences that derived from cyclic difference sets.

As an immediate consequence of the definition of cyclic difference set, one has the following proposition [1].

**Proposition 1**:\( D = \{d_1, d_2, \cdots, d_k\} \) is a \((v, k, \lambda)\)-cyclic difference set, then

1. \((v-1)\lambda = k(k-1)\);
2. For any \(\tau \in Z_v \setminus [0]\), \(|D \cap (D + \tau)| = \lambda\), where \(D + \tau = \{d_1 + \tau | 1 \leq i \leq k\}\) and \(|X|\) denotes the number of elements in a finite set \(X\);
3. The complement of a \((v, k, \lambda)\)-cyclic difference set is a \((v, v-k, v-2k+\lambda)\)-cyclic difference set.

Since the parameters \(v\) and \(k\) satisfy one of the two inequalities \(v \geq 2k\) and \(v \geq 2(v - k)\), by Proposition 1(3), we will only consider the \((v, k, \lambda)\)-cyclic difference set with \(v \geq 2k\) in the rest of this paper.

Let \(a = (a_0, a_1, \cdots, a_{v-1})\) and \(b = (b_0, b_1, \cdots, b_{v-1})\) be two binary sequences with period \(v\). The following three operations on the sequences \(a\) and \(b\) follow that in [13].

1. \(\sum_{i=0}^{v-1} a_i\)
2. \(a \odot b = (a_0 b_0, a_1 b_1, \cdots, a_{v-1} b_{v-1})\),
3. \(a \oplus b = (a_0 \oplus b_0, a_1 \oplus b_1, \cdots, a_{v-1} \oplus b_{v-1})\)

where \(a_i \oplus b_i = a_i + b_i \text{ (mod } 2)\) for \(0 \leq i \leq v-1\).

The autocorrelation function of the sequence \(a\) has the following property.

**Lemma 1**: [1] The binary sequence \(a\) defined by Eq. (1) has an autocorrelation function

\[
C_a(\tau) = \sum_{i=0}^{v-1} (-1)^{i + a_i a_{\tau+i}}.
\]


†The authors are with the Faculty of Mathematics and Computer Science, Huazhong University, Wuhan, 430062, China. X. Zeng is the corresponding author.

‡The author is with the State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), 19A Yuyuan Road, Beijing 100049, P.R. China.

††The work of N. Li and X. Zeng was supported in part by the National Science Foundation of China (NSFC) under Grant 60603012 and L. Hu’s work was supported in part by the NSFC under Grant 60573053.

a) E-mail: xzeng@hubu.edu.cn
b) E-mail: hu@is.ac.cn

DOI: 10.1093/ietfec/e91-a.5.1288

Copyright © 2008 The Institute of Electronics, Information and Communication Engineers
which is two-valued.

**Lemma 2:** Let \( a \) be a binary sequence of period \( v \) and its autocorrelation function is two-valued. Then, for any \( 0 \leq i \neq j \leq v - 1 \), \( \text{sum}(a^t a') \) is a constant where \( a^t = (a_i, a_{i+1}, \cdots, a_{i+1}, a_0, \cdots, a_{i-1}) \). In particular, if \( a \) is defined by Eq. (1) based on a \((v, k, \lambda)\)-cyclic difference set \( D \), then \( \text{sum}(a^t a') = v - 2k + \lambda \).

**Proof:** Since the autocorrelation function of \( a \) is two-valued, one has

\[
C_a(t) = \begin{cases} 
  v, & \text{if } t \equiv 0 \pmod{v}, \\
  c, & \text{otherwise},
\end{cases}
\]

where \( c \) is a constant. For any \( 0 \leq i \neq j \leq v - 1 \),

\[
C_a(j - i \bmod{v}) = v - 2\text{sum}(a^t a')
\]

which is a constant.

When \( a \) is defined by Eq. (1), \( \text{sum}(a) = v - k \) and \( (v - c)/4 = [v - (v - 4k + 4\lambda)]/4 = k - \lambda \) by Lemma 1. Thus,

\[
\text{sum}(a^t a') = v - 2k + \lambda.
\]

This finishes the proof.

**Lemma 3:** Let \( a \) be defined by Eq. (1). Then, for any three distinct integers \( i, j, \) and \( t \), \( 0 \leq i, j, t \leq v - 1 \), one has

\[
v - 3k + 2\lambda \leq v - 3k + 3\lambda.
\]

**Proof:** For \( 0 \leq l \leq v - 1 \), let the \((l + 1)\)-th-components of \( a^t \), \( a^t \) and \( a^t \) be \( a_{i+l} \), \( a_{i+l} \) and \( a_{i+l} \), respectively. Suppose that the pair \( (a_{i+l} a_{i+l}) \) takes values \((1, 1), (0, 1), (0, 0)\) exactly \( x_1, x_2, x_3, x_4 \) times, respectively. Then, by Eq. (1), one has

\[
x_1 + x_2 = x_1 + x_3 = v - k.
\]

By Lemma 1, one has

\[
x_1 + x_4 - (x_2 + x_3) = v - 4k + 4\lambda.
\]

Equations (4), (5) together with \( x_1 + x_2 + x_3 + x_4 = v \) determine values of \( x_i \), for \( 1 \leq i \leq 4 \) as

\[
x_1 = v - 2k + \lambda, \quad x_2 = k - \lambda, \quad x_3 = k - \lambda, \quad x_4 = \lambda.
\]

For \( 0 \leq l \leq v - 1 \), let \( (a_{i+l} a_{i+l}, a_{i+l} a_{i+l}) \) take values \((1, 1), (1, 0), (0, 1), (0, 0)\) exactly \( y_1, y_2, y_3, y_4 \) times, respectively. Thus, the pair \( (a_{i+l} a_{i+l}) \) takes value \((0, 1)\) exactly \( (y_2 + y_4) \) times. By Eq. (6), one has

\[
y_2 + y_4 = k - \lambda.
\]

By Lemma 2,

\[
\text{sum}(a^t a') = \text{sum}(a^t a')
\]

This finishes the proof.

Let \( s \) denote the weight of the \((v - k, v - 1, d, v - 2k + \lambda)\) code with weight \( d \leq 2(k - \lambda) \).

**Theorem 1:** Let \( g \) be defined by Eq. (1) and \( X \) denote a \((v - 1) \times v\) matrix whose \( i \)-th row is \( g a_i \) for \( 0 \leq i \leq v - 1 \). After deleting all zero columns in \( X \), all rows of \( X \) form a \((v - k, v - 1, d, v - 2k + \lambda)\) code with weight \( d \leq 2(k - \lambda) \).

**Proof:** By Eq. (1), the number of zeros in \( a \) is \( k \). We need to show that the number of zero columns in \( X \) is \( k \).

For \( 0 \leq i \leq v - 1 \), let the \((l + 1)\)-th-component of \( a^t \) be \( a_{i+l} \), \( 0 \leq i \leq v - 1 \). Suppose that \( a_{i+l} \) is a nonzero component of \( a \) and \( a_{i+l} = 0 \) for all \( 1 \leq i \leq v - 1 \). Then, one has

\[
a_{i+l} = \sum_{j \equiv (l+1) \bmod{v}} a_{i+l} = 0
\]

for \( 1 \leq i \leq v - 1 \), which contradicts with Eq. (1). Thus, if \( a_{i+l} \) is a nonzero component of \( a \), then there is an integer \( i \in [Z \setminus 0] \) such that \( a_{i+l} \neq 0 \). That is to say, the length of the codeword is \( n = v - k \). By Lemma 2, the weight of the constructed code is \( w = v - 2k + \lambda \), and by Lemma 3, the minimum Hamming distance satisfies

\[
2(k - 2\lambda) = 2[[v - 2k + \lambda] - (v - 3k + 3\lambda)] \leq d
\]

To complete the proof, it is sufficient to show that the number of codewords is \( M = v - 1 \).

If there are two integers \( i \) and \( j \), \( 1 \leq i < j \leq v - 1 \), such that \( a a_i = a a_j \), then

\[
\text{sum}(a a_i a a_j) = \text{sum}(a a_i a a_j) = \text{sum}(a a_i) = v - 2k + \lambda.
\]
This together with Lemma 3 imply \( v-2k+\lambda \leq v-3k+3\lambda, \) i.e., \( k \leq 2\lambda. \) Then, by Proposition 1(1), one has \( v \leq 2k-1, \) which contradicts to the assumption \( v \geq 2k. \) Thus, the constructed code has \( v-1 \) different codewords and the proof is finished. \( \Box \)

The following theorem can be similarly proven and the proof is omitted.

**Theorem 2:** Let \( Y \) denote a matrix whose rows are listed from top to bottom as
\[
\overrightarrow{a^1}, \overrightarrow{a^2}, \cdots, \overrightarrow{a^{v-1}}, \overrightarrow{a^v}, \cdots, \overrightarrow{a^{v-2}}, \overrightarrow{a^{v-1}}.
\]
Then, all rows of \( Y \) form a \((v, v(v-1)/2, d, v-2k+\lambda)\) code with \( d \geq 2(k-2\lambda). \)

In Theorems 1 and 2 of [13], \( m \)-sequences of period \( 2^n-1 \) were used to construct binary constant weight codes. By a fact that \( m \)-sequences of period \( 2^n-1 \) are equivalent to cyclic difference sets with parameters \((2^n-1, 2^{n-1}-1, 2^{n-2}-1)\) [1], this paper uses general sequences with two-valued autocorrelation to extend Zeng's work as above, that is, two classes of constant weight codes from cyclic difference sets are obtained.

Applying trinomial property of \( m \)-sequences [3], [6], the minimum Hamming distance of constructed codes was determined [13]. For a general case, the minimum Hamming distances for these codes can be discussed as follows.

Let \( D = \{d_1, d_2, \cdots, d_k\} \) be a \((v, k, \lambda)\)-cyclic difference set and
\[
D_i = \{d_j - i \mod(v) \mid j = 1, 2, \cdots, k\}
\]
for integer \( i. \) Since \( D_i = D_j \) if and only if \( v| (i - j) \), the set \( D_i \) will be considered only for \( i \in Z_v \) in the sequel. It is easy to observe that the elements of \( D_i \) can be interpreted as the positions of zeros in \( \overrightarrow{a^i}. \)

The condition that \( d = 2(k-2\lambda) \) holds in Theorems 1 and 2 can be characterized with the sets \( D_i \) \((0 \leq i \leq v-1)\) as in the following theorem.

**Theorem 3:** The constructed codes in Theorems 1 and 2 have the minimum Hamming distance \( d = (2k-2\lambda) \) if and only if there exist integers \( i, j, t, 0 \leq i, j, t \leq v-1, \) such that \( D_i \cap D_j \cap D_t = \emptyset. \)

**Proof:** When \( d = 2(k-2\lambda) \) if and only if there are two codewords \( \overrightarrow{a^i} \) and \( \overrightarrow{a^j} \) such that their Hamming distance is
\[
2((v-2k+\lambda) - \sum(\overrightarrow{a^i} \cdot \overrightarrow{a^j} \cdot \overrightarrow{a^t})) = 2(k-2\lambda).
\]
Thus, \( \sum(\overrightarrow{a^i} \cdot \overrightarrow{a^j} \cdot \overrightarrow{a^t}) = v-3k+3\lambda. \)
In Theorems 1 and 2, \( \overrightarrow{a^i}, \overrightarrow{a^j} \) and \( \overrightarrow{a^t} \) denoting two different codewords imply that there are at least three different integers among \( i, j, t, s. \) Without loss of generality, we assume these three integers are \( i, j, t. \) By Lemma 3, one has \( \sum(\overrightarrow{a^i} \cdot \overrightarrow{a^j} \cdot \overrightarrow{a^t}) = v-3k+3\lambda. \) By Eq. (10), \( \sum(\overrightarrow{a^i} \cdot \overrightarrow{a^j} \cdot \overrightarrow{a^t}) = v-3k+3\lambda \) holds if and only if \( \{a^i_l, a^j_l, a^t_l\} \) take value \((0,0,0)\) \( \lambda \) times, \( \{a^i_l, a^j_l, a^t_l\} \) take value \((0,0,1)\) \( \lambda \) times, \( \{a^i_l, a^j_l, a^t_l\} \) never takes value \((0,0,1)\) \( 0 \leq l \leq v-1. \) By Eq. (6), the pair \( \{a^i_l, a^j_l\} \) take value \((0,0)\) \( \lambda \) times, then \( \{a^i_l, a^j_l, a^t_l\} \) never takes value \((0,0,1)\) \( 0 \leq l \leq v-1. \)}
Since \( c_{ij} = c_{ji} \), we only consider \( c_{ij} \) of \( L \) with \( i < j \). Let  
\[ L^* = \{(i, j) \mid c_{ij} \in L, i < j \} \]
and for a fixed integer \( t, 1 \leq t \leq v/3 \),  
\[ L_t = \{(i, j) \in L^* \mid i = t, 2t \leq j \leq v - t, \]
or \( j = v - t, t \leq i \leq v - 2t, \]
or \( j - i = t, t \leq i \leq v - 2t \}. \quad (16) \]

The relation between \( L^* \) and \( L_t(1 \leq t \leq v/3) \) is given in the following lemma.

**Lemma 4:** Let \( L^* \) and \( L_t(1 \leq t \leq v/3) \) be defined as above, then \( L^* = \bigcup_{t=1}^{\lfloor v/3 \rfloor} L_t \), where \( \lfloor v/3 \rfloor \) denotes the largest integer not exceeding \( v/3 \).

**Proof:** For different integers \( r \) and \( s \), \( 1 \leq r, s \leq v/3 \), by Eq. (16), one has  
\[ L_r \cap L_s = \emptyset. \quad (17) \]
Furthermore, if \( 2t \neq v - t \), i.e., \( t \neq v/3 \), then  
\[ |L_t| = 3(v - t - 2t + 1) - 3 = 3(v - 3t). \quad (18) \]
Then, for \( v \equiv 0 \) (mod 3), by the fact \( |L^*| = (v - 2)(v - 1)/2 \), Eqs. (17) and (18), one has  
\[ L^* = \bigcup_{t=1}^{\lfloor v/3 \rfloor} L_t \text{ since } \bigcup_{t=1}^{\lfloor v/3 \rfloor} L_t \subseteq L^*. \]
For \( v \equiv 0 \) (mod 3), by Eq. (16),  
\[ L_{v/3} = \{(v/3, 2v/3)\}. \]
With a similar analysis, one has  
\[ L^* = \bigcup_{i=1}^{v/3-1} L_i \text{ since } \bigcup_{i=1}^{v/3-1} L_i \subseteq L^*. \]

The proof is finished. \( \square \)

**Lemma 5:** Let \( D \) be a \((v, k, \lambda)\)-cyclic difference set and \( L = (c_{ij}) \) be defined as above. Then, for \( v \equiv 0 \) (mod 3),  
\[ |c_{ij}| 1 \leq i < j \leq v - 1 \]  
\[ = \bigcup_{i=1}^{v-3} |c_{ij}| 2t \leq s \leq v - t - 1 \cup \{c_{v/3,2v/3}\}. \]
Otherwise,  
\[ |c_{ij}| 1 \leq i < j \leq v - 1 \]  
\[ = \bigcup_{i=1}^{v/3} |c_{ij}| 2t \leq s \leq v - t - 1. \]

**Proof:** By a fact that \( D_{i+j} + i = D_j \) and \( D + i = D_{v-i} \), one has  
\[ |D \cap D_{i+j} + i| = |D_{v-i} \cap D \cap D_{i+j}| \]
\[ = \left| (D_{v-i} \cap D) \cap D_{i+j} \right| + j \]
\[ = \left| D_{v-i} \cap D_{i+j} \cap D \right|, \]
i.e.,  
\[ |D \cap D_{i+j} + i| = |D \cap D_j \cap D_{v-i}|. \]
that is to say,  
\[ c_{i+j} = c_{v-i} = c_{v-i-j}, \]
which implies for a fixed integer \( t, 1 \leq t \leq v/3, \)  
\[ c_{t,2t} = c_{t,v-t} = c_{v-2t}, \]
\[ c_{t,2t+1} = c_{t,v-t-1} = c_{v-2t-1}, \]
\[ \cdots \]
\[ c_{t,v-t-1} = c_{v-2t-1,v-t} = c_{v+1,2t+1}. \quad (19) \]
By Eqs. (16) and (19), one has  
\[ |c_{ij}| (i, j) \in L_1 = |c_{ij}| 2t \leq j \leq v - t - 1 \]
for \( t \neq v/3, 1 \leq t \leq [1/3] \) and  
\[ |c_{ij}| (i, j) \in L_{v/3} = (c_{v/3,2v/3}). \]

This and Lemma 4 finish the proof. \( \square \)

Combining above analysis and Lemma 5, the minimum Hamming distance in Theorems 1 and 2 can be characterized as follows.

**Theorem 4:** By the construction methods of Theorems 1 and 2, a \((v - k, v - 1, 2(k - 2\lambda + \mu), v - 2k + \lambda)\) code and a \((v, (v - (v - 1)/2, 2(k - 2\lambda + \mu), v - 2k + \lambda)\) code can be obtained from every \((v, k, \lambda)\)-cyclic difference set respectively, where  
\[ \mu = \min \left\{ \min_{1 \leq i < j < v} c_{ij}, c_{v/3,2v/3} \right\} \]
for \( v \equiv 0 \) (mod 3) and for other cases  
\[ \mu = \min \left\{ \min_{1 \leq i < j < v} c_{ij}, c_{i,v} \right\} \]

**Proof:** By Theorems 1 and 2, to complete this proof, it is sufficient to show that the minimum Hamming distance is \( 2(k - 2\lambda + \mu) \), where \( \mu \) is defined as above. By Lemma 5 and Eq. (15), one has  
\[ \min_{0 < i < j < v} |D \cap D_i \cap D_j| = \min_{0 < i < j < v} c_{ij} = \mu, \]
and \( z = \lambda - \mu \),
and then by Eq. (14), one has  
\[ d = 2[(v - 2k + \lambda) - (v - 3k + 2\lambda + \lambda - \mu)] \]
\[ = 2(k - 2\lambda + \mu). \]
This finishes the proof. \( \square \)

Applying Lemma 5 and Theorem 4, the value of \( \mu \) can be determined with the help of computer. Using the known cyclic difference sets \( [5] \) and a \((v - k, v - 1, 2(k - 2\lambda + \mu), v - 2k + \lambda)\) code and a \((v, (v - (v - 1)/2, 2(k - 2\lambda + \mu), v - 2k + \lambda)\) code can be obtained from each of them.

### 4. Binary Optimal Constant Weight Codes

Based on the properties of \( m \)-sequences, binary optimum constant weight codes with parameters \((2^{n-1}, 2^n -\)

2, 2^{n-2}, 2^{n-2}) (n \geq 3) and (2^n-1, (2^{n-1}-1)(2^n-1), 2^{n-2}, 2^{n-2}) (n = 3 or n = 4) were constructed in [13]. These binary constant weight codes from (2^{n-1}, 2^{n-1}-1, 2^{n-2}-1)-cyclic difference sets by Theorems 1 and 2, can be proven to be optimal by applying the trinomial property of m-sequences. Besides these codes, other binary constant weight codes based on cyclic difference sets can also be obtained. Some codes can achieve Johnson Bound II and be proven to be optimal according to the following analysis.

Lemma 6: [8] A(n, 2\delta, w) = A(n, 2\delta, n - w).

Lemma 7: [7] Johnson Bound II:

$$A(n, 2\delta, w) \leq \left\lfloor \frac{n}{w} \left( \frac{n-1}{w-1} \cdots \frac{n-w+\delta}{\delta} \right) \right\rfloor.$$  

A difference set with \( \lambda = 1 \) is called a planar difference set. It is well known that there exists a \((q^2 + q + 1, q + 1, 1)\)-planar difference set where \( q(q \neq 1) \) is a prime. Thus, by Theorem 1 and Corollary 2, a binary \((q^2, q^2 + q, 2(q - 1), q^2 - q)\) constant weight code can be obtained from \((q^2 + q + 1, q + 1, 1)\)-planar difference set for each \( q = p^r \), where \( p \) is a prime and \( n \geq 1 \). These codes are proven to be optimal as follows.

Proposition 2: The binary \((q^2, q^2 + q, 2(q - 1), q^2 - q)\) constant weight code obtained from planar difference set is optimal for each \( q = p^r \), where \( p \) is a prime and \( n \geq 1 \).

Proof: To complete this proof, it is sufficient to show that \( A(q^2, 2(q - 1), q^2 - q) = q^2 + q \). By above analysis, a binary \((q^2, q^2 + q, 2(q - 1), q^2 - q)\) constant weight code can be obtained for each \( q = p^r \), where \( p \) is a prime and \( n \geq 1 \). This implies

$$A(q^2, 2(q - 1), q^2 - q) \geq q^2 + q.$$  

By Lemmas 6 and 7, one has

$$A(q^2, 2(q - 1), q^2 - q) = A(q^2, 2(q - 1), q) \leq \left\lfloor \frac{q^2}{q} \left( \frac{q^2 - 1}{q - 1} \right) \right\rfloor = q^2 + q.$$  

Therefore,

$$A(q^2, 2(q - 1), q^2 - q) = q^2 + q.$$  

That is, for each \( q = p^r \), where \( p \) is a prime and \( n \geq 1 \), we can obtain a binary optimum \((q^2, q^2 + q, 2(q - 1), q^2 - q)\) constant weight code, which achieves the Johnson Bound II.

Example 1: For \((q^2 + q + 1, q + 1, 1)\)-planar difference set, let \( q = 2, 3, 4, 5, 7 \), by Theorem 1 and Corollary 2, one can get \((4, 6, 2, 2), (9, 12, 4, 6), (16, 20, 6, 12), (25, 30, 8, 20)\) and \((49, 56, 12, 42)\) codes respectively. The \((4, 6, 2, 2)\) code was also obtained in [13] and it is optimal. By Lemma 6 and the tables I-III of constant weight codes in [12], the \((9, 12, 4, 6), (16, 20, 6, 12)\) and \((25, 30, 8, 20)\) codes are optimal. The \((49, 56, 12, 42)\) code is optimal since the \((49, 56, 12, 7)\) code is optimal by [10].

Example 2: \( D = \{0, 1, 3, 5, 9, 15, 22, 25, 26, 27, 34, 35, 38\} \) is a \((40, 13, 4)\)-cyclic difference set [5], applying Lemma 5 and Theorem 4 with the help of computer, one can get \( \mu = 1 \). By Theorem 1 and Corollary 2, a \((27, 39, 12, 18)\) code is obtained and it is optimal by Lemma 6 and the table V of constant weight codes in [12].

5. Conclusion

In this paper, based on cyclic difference sets, the method of [13] is extended to construct more binary constant weight codes and a new class of binary optimum constant weight codes is obtained. Remaining works in future along this line are to find new constructions of constant weight codes based on cyclic difference sets.

Acknowledgement

The authors wish to thank the referee for helpful suggestions.

References