ELSEVIER

Discrete Mathematics 260 (2003) 223–230

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

Note

# On weights in duadic abelian codes[☆]

Qiaoliang Li[a,b]

[a] Department of Mathematics, Hunan Normal University, Changsha 410081, People's Republic of China

[b] Center for Combinatorics, The Key Laboratory of Pure Mathematics and Combinatorics of Ministry of Education, Nankai University, Tianjin 300071, People's Republic of China

Received 4 January 2000; received in revised form 24 May 2002; accepted 3 June 2002

**Abstract**

In this note, we prove that if $C$ is a duadic binary abelian code with splitting $\mu = \mu_{-1}$ and the minimum odd weight of $C$ satisfies $d^2 - d + 1 \neq n$, then $d(d-1) \geqslant n + 11$. We show by an example that this bound is sharp. A series of open problems on this subject are proposed.


*Keywords:* Duadic abelian codes; Primitive idempotent; Group algebra; Weight

## 1. Introduction

Duadic algebra codes were first introduced by Leon et al. [3] and Rushanan [7] as a generalization of quadratic residue codes. It is known [3,7,9] that the minimum odd weight of duadic algebra codes satisfy a square root bound. Tilborg [8,5] presented an useful method to evaluate the weight of binary quadratic residue codes. Since the core of this method is to decompose a kind of multiset, we name this method Tilborg's decomposition method. Using this method, Tilborg proved that if $C$ is a binary quadratic residue code of length $n \equiv -1 \pmod 8$ and the minimum odd weight $d$ of $C$ satisfies $d(d-1) > n-1$, then $d(d-1) \geqslant n+11$. Pless et al. [6] generalized the result to duadic binary cyclic codes with splitting $\mu = \mu_{-1}$.

The purpose of this note is to generalize the result of Tilborg [8,5] to duadic abelian codes. Tilborg's method is valid for the cyclic duadic codes. We first generalize

☆ This project is partially supported by the post-doctor grant of China.
*E-mail address:* liqiaoliang@eyou.com (Q. Li).

0012-365X/03/$ - see front matter 
PII: S0012-365X(02)00673-8

Tilborg's decomposition method to the abelian group case, and then prove the following:

**Theorem 1.1.** *Let $F = GF(2)$ and $G$ be an abelian group of order $n$. If $C$ is a duadic abelian code in $FG$ with splitting $\mu = \mu_{-1}$ and the minimum weight of $C$ satisfies $d^2 - d + 1 \neq n$, then $d(d-1) \geqslant n + 11$.*

The bound in the theorem is sharp. In [6, Table II], Pless et al. illustrate two duadic codes with length 31 and minimum weight 7.

## 2. Preliminaries

Throughout, $F = GF(q)$ is a finite field with $q$ elements and $G$ is a group of order $n$, where we assume that $\gcd(q, n) = 1$. All of our calculations take place in group algebra FG. Let $G = \{g_1, g_2, \ldots, g_n\}$, an element of $FG$ is the sums

$$\sum_{1 \leqslant i \leqslant n} a_i g_i, \quad a_i \in GF(q),\ g_i \in G,\ i = 1, 2, \ldots, n.$$

The multiplicative identity of $FG$ is denoted by 1. Any *automorphism* $\mu \in \mathrm{Aut}(G)$ defines an automorphism of $FG$ by

$$\mu\left(\sum_{1 \leqslant i \leqslant n} a_i g_i\right) = \sum_{1 \leqslant i \leqslant n} a_i \mu(g_i).$$

If $\gcd(n, t) = 1$, we define the automorphism $\mu_t(g) = tg$. Of special interest is the automorphism $\mu_{-1}$.

Because $\gcd(n, q) = 1$, $FG$ is semi-simple, which means that any ideal of $FG$ is the unique sum of minimal ideals (see [1,4]). Ideals in $FG$ are called *abelian group codes*. Each code is generated by a unique idempotent; minimal ideals are generated by *primitive idempotents.* If a code $C$ is generated by an idempotent $e$, then we denote $C = \langle e \rangle$. The idempotent $e_0 = (1/n)\sum_{1 \leqslant i \leqslant n} g_i$ is called *trivial idempotent*. All primitive idempotents not equal to $e_0$ are called *nontrivial*. If $C$ is a code in $FG$ and $\mu \in \mathrm{Aut}(G)$, then $\mu$ is an automorphism of $C$ if and only if $\mu$ fixes its idempotent.

For $\xi = \sum_{1 \leqslant i \leqslant n} a_i g_i \in FG$ if $\xi e_0 = 0$, that is, $\sum_{1 \leqslant i \leqslant n} a_i = 0$, then the element $\xi$ is called *even-like*. Otherwise it is called *odd-like*.

**Definition 2.1.** Let $e_1$ and $e_2$ be two idempotents of $FG$ and $\mu \in \mathrm{Aut}(G)$ satisfying the following two properties:

1. $e_1 + e_2 = \mathbf{1} + e_0$,
2. $\mu(e_1) = e_2$ and $\mu(e_2) = e_1$.

Then $\langle e_1 \rangle$, $\langle e_2 \rangle$, $\langle \mathbf{1} - e_1 \rangle$ and $\langle \mathbf{1} - e_2 \rangle$ are called duadic abelian codes determined by $e_1$ and $e_2$. The automorphism $\mu$ is said to give the splitting for the duadic codes.

The following proposition gave the necessary and sufficient condition for the existence of duadic abelian codes.

**Proposition 2.2** (Zhang [10] and Ward and Zhu [9]). *FG contains duadic abelian codes with splitting $\mu_{-1}$ if and only if q has odd order modulo n.*

## 3. Generalization of Tilborg's decomposition method

In this section, we will introduce a generalization of Tilborg's decomposition method. Let $\xi = \sum_{g\in G} a_g g \in FG$, the set $\{g\in G: a_g \neq 0\}$ is said to be the *support* of $\xi$ and is denoted by $\mathrm{Supt}(\xi)$. Let $\mathscr{D}(\xi)$ be the multiset defined by $\{g_i g_j : g_i \in \mathrm{Supt}(\xi),\ g_j \in \mathrm{Supt}(\mu_{-1}(\xi)), i\neq j\}$. The number of elements in $\mathscr{D}(\xi)$ which appear exactly $s$ times is denote by $n_s$. Let $g\in\mathscr{D}(\xi)$, we say that an element $g_i\in\mathrm{Supt}(\xi)$ *is related to* $g$ if there exists some element $g_j\in\mathrm{Supt}(\xi)$ such that $g=g_i g_j^{-1}$ or $g=g_j g_i^{-1}$. Denote the set of elements in $\mathscr{D}(\xi)$ which are related to $g$ by $\mathscr{R}_{\mathscr{D}(\xi)}(g)$.

**Lemma 3.1.** *Let $g$ be an element of $G$ that appears exactly $s$ times in $\mathscr{D}(\xi)$. Then $\mathscr{R}_{\mathscr{D}(\xi)}(g)$ can be uniquely divided into the following blocks*

$$[g_{i_1}, g_{i_1}g, \ldots, g_{i_1}g^{c_1}], [g_{i_2}, g_{i_2}g, \ldots, g_{i_2}g^{c_2}], \ldots, [g_{i_r}, g_{i_r}g, \ldots, g_{i_r}g^{c_r}], \tag{1}$$

*where $g_{i_l}\in\mathscr{R}_{\mathscr{D}(\xi)}(g)$, $1\leqslant l\leqslant r$, and (1) satisfies the following properties*:

1. *each element in $\mathscr{R}_{\mathscr{D}(\xi)}(g)$ appears in exactly one block,*
2. *if $g_i, g_j$ are two elements in different blocks in (1), then $g_i g_j^{-1}\neq g$,*
3. *$1\leqslant c_1\leqslant c_2\leqslant\cdots\leqslant c_r < o(g)$ and $c_1+c_2+\cdots+c_r=s$.*

*Where $\mathrm{o}(g)$ denotes the order of $g$ and $r, c_i, 1\leqslant i\leqslant r$, are uniquely determined by $g$.*

We say that $(c_1, c_2, \ldots c_r)$ is the *structure* of $g$.

We now give two examples to illustrate the notations and the lemma.

**Example 3.2.** Let $G=\langle a,b\rangle$ be a group with $a^7=b^7=1$ (identity of $G$) and $ab=ba$. $G$ is an abelian group of order 49. Then $e=1+(b+b^2+b^4)\sum_{i=0}^{6}a^i+a+a^2+a^4$ is an idempotent of $FG$. Let $C=\langle e\rangle$ be a code in $FG$ then $C$ has minimum odd weight 9. Let $\xi=(ab^3+ab^4+ab^6)e$ be a codeword of $C$ with weight 9. By definition, $\mathrm{Supt}(\xi)=\{b^3,\ b^4,\ b^6,\ a^4b^3,\ a^4b^4,\ a^4b^6,\ a^6b^3,\ a^6b^4,\ a^6b^6\}$ and $\mathscr{R}_{\mathscr{D}(\xi)}(a)=\{b^3,\ b^4,\ b^6,\ a^6b^3,\ a^6b^4,\ a^6b^6\}$. $\mathscr{R}_{\mathscr{D}(\xi)}(a)$ can be decomposed into the following blocks which satisfies the conditions given by Lemma 3.1

$$[a^6b^3, a^6b^3a=b^3], [a^6b^4, a^6b^4a=b^4], [a^6b^6, a^6b^6a=b^6].$$

**Example 3.3.** Let $G=\langle g\rangle$ with $g^{47}=1$ and $GF(47)$ be a field, $Q$ is the set of quadratic residues of $GF(47)$. Let $e=\sum_{i\in Q}x^i$. Then $\langle e\rangle$ is a code with minimum weight 11 and $\xi=x^9+x^{17}++x^{20}+x^{22}+x^{25}+x^{30}+x^{31}+x^{32}+x^{34}+x^{43}+x^{44}$ is a codeword with minimum odd weight. $\mathrm{Sup}(\xi)=\{x^9, x^{17}, x^{20}, x^{22}, x^{25}, x^{30}, x^{31}, x^{32}, x^{34}, x^{43}, x^{44}\}$ and $x^{12}=x^9x^{-44}=x^{32}x^{-20}=x^{34}x^{-22}=x^{43}x^{-31}=x^{44}x^{-32}$. Consider the set $\mathscr{R}_{\mathscr{D}(\xi)}(x^{12})$. At the first step, we can get the following blocks:

$$[x^{44},x^9],[x^{20},x^{32}],[x^{22},x^{34}],[x^{31},x^{43}],[x^{32},x^{44}]$$

can concatenate the second, fifth and the first block into a block. By arranging the blocks, we get

$$[x^{22},x^{22}x^{12}],[x^{31},x^{43}],[x^{20},x^{20}x^{12},x^{20}(x^{12})^2,x^{20}(x^{12})^3].$$

It is easily seen that the above blocks are the needed blocks.

We now prove Lemma 3.1.

**Proof.** Let $\mathscr{R}_{\mathscr{D}(\xi)}(g)=\{g_{i_1},g_{i_2},\dots,g_{i_s},g_{j_1}=g_{i_1}g,\ g_{j_2}=g_{i_2}g,\dots,g_{j_s}=g_{i_s}g\}$ be the multiset of the elements in $\mathscr{D}(\xi)$ which are related to $g$. We first construct the following blocks:

$$[g_{i_1},g_{i_1}g],[g_{i_2},g_{i_2}g],\dots,[g_{i_s},g_{i_s}g]. \tag{2}$$

If there does exists some $k\neq l, 1\leqslant k,l\leqslant s$, such that $i_k=j_l$, we are done. Otherwise, we can concatenate the blocks into one block. Without loss of generality, we assume that $i_2=j_1$. Then $g_{j_2}=gg_{j_1}$, it follows that the elements $g_{i_1},\ g_{j_1}=g_{i_1}g,\ g_{j_2}=g_{i_1}g^2$ are in the same block. Thus, we get the following blocks:

$$[g_{i_1},gg_{i_1}=g_{j_1},g_{i_1}g^2=g_{j_2}],[g_{i_2},g_{i_2}g],\dots,[g_{i_k},g_{i_k}g].$$

Assume that we have gotten the following blocks:

$$[g_{i_1},g_{i_1}g,\dots,g_{i_1}g^{a_1}],[g_{i_2},g_{i_2}g,\dots,g_{i_2}g^{a_2}],\dots,[g_{i_t},g_{i_t}g,\dots,g_{i_t}g^{a_t}]. \tag{3}$$

If there does not exist any $i_k,i_l\in\{i_1,i_2,\dots i_t\}$ and $0\leqslant h\leqslant a_k,\ 0\leqslant m\leqslant a_l$, such that $g_{i_k}g^h(g_{i_l}g^m)^{-1}=g$, then we are done. Otherwise, if $h\geqslant m-1$, then $g_{i_l}=g_{i_k}g^{(h-m-1)}$; if $h<m-1$, then $g_{i_k}=g_{i_l}g^{(m+1-h)}$. In either case, we can concatenate the $l$th block and the $k$th block into a block. Continue in this way and arrange the blocks such that the blocks satisfies the property 3, we get the required blocks. $\square$

Let $c_1+c_2+\cdots+c_r+r=N$. Obviously $N\leqslant d$. We have the following:

**Lemma 3.4.** *Let $g$ be an element of $G$ that appears $s$ times in $\mathscr{D}(\xi)$ and $g$ has structure $(c_1,c_2,\dots,c_r)$. Then $N(N-1)-2\varepsilon-2r(r-1)\leqslant\sum_{s\geqslant 2}sn_s$, where $N=c_1+c_2+\cdots+c_r+r=r+s$ and $\varepsilon=1$ if $c_r>c_{r-1}$ or $r=1$; $\varepsilon=0$ if $c_r=c_{r-1}$.*

**Proof.** Let $\mathscr{R}^*_{\mathscr{D}(\xi)}(g)$ denote the multi-set $\{g_{i_j}g^h(g_{i_k}g^m)^{-1} : 1\leqslant j,k\leqslant r, 1\leqslant h\leqslant c_j, 1\leqslant m\leqslant c_k, (i_j,h)\neq(i_k,m)\}$ generated by the elements in the blocks of (1). Obviously, $|\mathscr{R}^*_{\mathscr{D}(\xi)}(g)|=N(N-1)$. Consider the total number of elements in $\mathscr{R}^*_{\mathscr{D}(\xi)}(g)$ that appear at least twice. Realize that an element in $\mathscr{R}^*_{\mathscr{D}(\xi)}(g)$ appears exactly once only if $h=c_j$ and $m=0$ or $h=0$ and $m=c_k$ or $c_r>c_{r-1}$.

Thus, the number of elements in $\mathscr{R}^*_{\mathscr{D}(\xi)}(g)$ that appears at least twice is equal to $N(N-1)-2-2r(r-1)$, if $c_r > c_{r-1}$ or $N(N-1)-2r(r-1)$, if $c_r = c_{r-1}$.

On the other hand, the number of elements in $\mathscr{D}(\xi)$ that appears at least twice is equal to $\sum_{s\geqslant 2} sn_s$. Lemma 3.4 now follows from the observation that $\mathscr{R}^*_{\mathscr{D}(\xi)}(g) \subseteq \mathscr{D}(\xi)$. $\square$

The following lemma tells us the information about $n_s$.

**Lemma 3.5.** *Let $F = GF(2)$, then*

(1) $\sum_s n_s = n-1$,
(2) $n_{2s} = 0$ *for all* $s$,
(3) $n_s$ *is even for all* $s$,
(4) $n_s = 0$ *for all* $s > d$,
(5) $\sum_s sn_s = d(d-1)$.

**Proof.** By Definition 1, we have

$$e + \mu_{-1}(e) = \mathbf{1} + e_0 \tag{4}$$

and there is an element $\eta = \sum_{g\in G} b_g g \in FG$ such that $\xi = \eta e$. Since $\xi$ is odd-like, $\eta$ is odd-like too, that is $\sum_{g\in G} b_g \neq 0$. It follows that:

$$\eta\mu_{-1}(\eta)e_0 = \left(\sum_{g\in G} b_g\right)^2 e_0 \tag{5}$$

and that the weight of $\eta\mu_{-1}(\eta)e_0$ is $n$. Since $e$ is an odd-like idempotent, by the definition, we have

$$e\mu_{-1}(e) = e(\mathbf{1} + e_0 - e) = e_0. \tag{6}$$

Since $\xi\mu_{-1}(\xi) = \eta\mu_{-1}(\eta)e\mu_{-1}(e) = \eta\mu_{-1}(\eta)e_0$, then the weight of $\xi\mu_{-1}(\xi)$ is $n$, thus each non-identity element of $G$ appears in $\mathscr{D}(\xi)$. (1) is now proved

Since $F = GF(2)$ and $\xi\mu_{-1}(\xi)$ has weight $n$, there does not exist any element $g \in G$ such that $g$ appears even times in the multi-set $\mathscr{D}(\xi)$. So $n_{2s} = 0$ for all $s$.

Now we assume that some element $g = g_i g_j^{-1}$ appears $s$ times in $\mathscr{D}(\xi)$, then $g^{-1} = g_i^{-1} g_j$ appears $s$ times in $\mathscr{D}(\xi)$ too. Statement (2) now follows from the observation that $g \neq g^{-1}$ for any $g \in \mathscr{D}(\xi)$. Indeed, if $g = g^{-1}$, then $g^2 = 1$. By Lagrange Theorem, $2|n$. This contradicts the assumption that $\gcd(2, n) = 1$.

Suppose that there is some $s > d$ such that $n_s > 0$, then there exists some $g \in G$ such that $g$ appears $s$ times in $\mathscr{D}(\xi)$. Without loss of generality, assume that $g = g_{i_k} g_{j_k}^{-1}$, $k = 1, 2, \ldots, s$. Since there exactly $d$ distinct terms in $\xi$, there exist $k$ and $l$, such that $g_{i_k} = g_{i_l}$. Since $g_{i_k} g_{j_k}^{-1} = g_{i_l} g_{j_l}^{-1}$, it follows that $g_{j_k} = g_{j_l}$. This means that $(i_k, j_k) = (i_l, j_l)$, a contradiction. Thus for each $g \in G$, $g$ appears at most $d$ times in $\mathscr{D}(\xi)$. (3) is now proved.

Since there are $d(d-1)$ terms in $\mathscr{D}(\xi)$ and $\xi\mu_{-1}(\xi)$ has weight $n$, then

$$\sum_s sn_s = d(d-1). \tag{7}$$

Lemma 3.5 is now proved. □

## 4. Proof of Theorem 1.1

In order to prove our main results, the following lemmas are needed:

**Lemma 4.1** ([2]). *For any odd integer $m$,* $\gcd(2^m-1,3)=1$.

**Lemma 4.2** ([2]). *For any odd integer $m$,* $\gcd(2^m-1,5)=1$.

**Proof of Theorem 1.1.** Since $d(d-1)>n-1$, then $d(d-1)-(n-1)=n_2+2n_3+3n_4+4n_5+5n_6+6n_7+\cdots>0$. By Lemma 3.5, $n_{2s}=0$ for all $s$, so $d(d-1)-n=-1+n_2+2n_3+3n_4+4n_5+5n_6+6n_7+\cdots=-1+2n_3+4n_5+6n_7+\cdots$.

Assume to the contrary, that $d(d-1)<n+11$. By Lemma 3.5 $n_s$ is even. Since $2n_3+4n_5+6n_7+\cdots<12$, then there are three cases

*Case* 1: $n_3=2$ and $n_s=0$ for all $s>3$. Let $g$ be an element of $G$ that appears 3 times and $g$ has structure $(c_1,c_2,\ldots,c_r)$. If $r=3$, then $(c_1,c_2,c_3)=(1,1,1)$ and $N(N-1)-2\varepsilon-2r(r-1)=18$; if $r=2$, then $(c_1,c_2)=(1,2)$ and $N(N-1)-2\varepsilon-2r(r-1)=14$; if $r=1$, then $(c_1)=(3)$ and $N(N-1)-2\varepsilon-2r(r-1)=10$. Because $\sum_{s\geqslant 3} sn_s=3\times 2=6$, we see that all possibilities contradict Lemma 3.4.

*Case* 2: $n_5=2$ and $n_s=0$ for all $s\geqslant 3$ and $s\neq 5$. Then there is some element $g$ that appears 5 times. Let the structure of $g$ be $(c_1,c_2,\ldots,c_r)$. Of course, $r\leqslant 5$. Since $g$ appears 5 times in $\mathscr{D}(\xi)$ then $N=c_1+c_2+\cdots+c_r+r=r+5$. Thus $N(N-1)-2\varepsilon-2r(r-1)\geqslant(r+5)(r+4)-2-2r(r-1)$. By Lemma 3.4, we have

$$(r+5)(r+4)-2-2r(r-1)\leqslant N(N-1)-2\varepsilon-2r(r-1)\leqslant\sum_s in_s=10.$$

But the above inequalities does not hold for $1\leqslant r\leqslant 5$.

*Case* 3: $n_3=4$ and $n_s=0$ for all $s>3$. In this case, $\sum_{s\geqslant 3} sn_s=12$. Let $g$ be the element appears 3 times and $g$ has structure $(c_1,c_2,\ldots,c_r)$. If $r=3$, then $(c_1,c_2,c_3)=(1,1,1)$ and $N(N-1)-2\varepsilon-2r(r-1)=30$. If $r=2$, then $(c_1,c_2)=(1,2)$ and $N(N-1)-2\varepsilon-2r(r-1)=14$. We see that all the above possibilities contradict Lemma 3.4. Thus $r=1$ and each $g\in G$ that appears three times has structure (3). Let $g$ be such an element, then there exists $g_{i_1},g_{i_2},g_{i_3},g_{i_4}$ such that $g=g_{i_1}g_{i_2}^{-1}=g_{i_2}g_{i_3}^{-1}=g_{i_3}g_{i_4}^{-1}$. Realize that $g^2=g_{i_1}g_{i_2}^{-1}g_{i_2}g_{i_3}^{-1}=g_{i_1}g_{i_3}^{-1}$ and also $g^2=g_{i_2}g_{i_4}^{-1}$, one know that $g^2$ appears 3 times, then there exists $g_{i_5},g_{i_6}\in\{g_1,g_2,\ldots,g_d\}$ such that $g^2=g_{i_5}g_{i_6}^{-1}$. Since $g^2$ has structure (3) and $g^2=g_{i_1}g_{i_3}^{-1}=g_{i_2}g_{i_4}^{-1}$, then $i_5=i_3$ and $i_6=i_2$ or $i_5=i_4$ and $i_6=i_1$.

(1) If $i_5=i_3$ and $i_6=i_2$, then $g^2=g_{i_5}g_{i_6}^{-1}=g_{i_3}g_{i_2}^{-1}=g^{-1}$, it follows that $g^3=1$. Thus $3|n$. But by Proposition 2.2, 2 has odd order modulo $n$. This implies that there exists

some odd positive integer $m$, such that $n|2^m-1$, thus $3|2^m-1$. This contradicts Lemma 4.1.

(2) If $i_5=i_4$ and $i_6=i_1$, then $g^2=g_{i_5}g_{i_6}^{-1}=g_{i_4}g_{i_2}^{-1}=(g_{i_1}g_{i_2}^{-1}g_{i_2}g_{i_3}^{-1}g_{i_3}g_{i_4}^{-1})^{-1}=g^{-3}$, it follows that $g^5=1$. Thus $5|n$. It follows that $5|2^m-1$ for some odd positive integer $m$. This contradicts Lemma 4.2.

Thus $d(d-1)-(n-1)\geqslant 12$. The Theorem is now proved. □

## 5. Further remarks

Firstly, it is worth mentioning that although the bound given in Theorem 1.1 is sharp we could not find more duadic codes such that the minimum odd weight $d$ satisfies $d^2-d=n+11$. We would like to propose the following:

**Problem 5.1.** *Is there infinitely family of other duadic code such that the minimum weight $d$ satisfies $d^2-d=n+11$?*

Secondly, it is well known that if $C$ is an odd-like duadic code in $FG$ with splitting $\mu=\mu_{-1}$ and $C$ contains an odd-like vector $\xi$ with weight $d$ satisfying $d^2-d+1=n$, then the support of all vectors with weight $d$ in $C$ forms a projective plane of order $d-1$ [7,11]. An interesting question has been proposed by the referee: Is there something to be said for the case $d(d-1)=n+11$?

With the aid of computer, we have found all the minimum weight vectors of the two $(31,16,7)$ codes. Let $C_1$ be the $(31,16,7)$ cyclic duadic code generated by $x+x^2+x^4+x^5+x^7+x^8+x^9+x^{10}+x^{14}+x^{16}+x^{18}+x^{19}+x^{20}+x^{25}+x^{28}$. Then the minimum weight vectors of $C_1$ are $x^i(x^1+x^2+x^7+x^{10}+x^{26}+x^{27}+x^{28})$, $x^i(x^4+x^7+x^{11}+x^{19}+x^{20}+x^{22}+x^{25})$, $x^i(x^2+x^6+x^7++x^9+x^{13}+x^{17}+x^{26})$, $x^i(x^3+x^6+x^{11}+x^{19}+x^{20}+x^{28}+x^{30})$, $x^i(x^9+x^{15}+x^{16}+x^{18}+x^{20}+x^{28}+x^{30})$, $i=0,1,2,\ldots,30$. Using difference family theory, we know that they constitute a $(31,7,7)$-BIBD.

Let $C_2$ be the $(31,16,7)$ cyclic duadic code generated by $x+x^2+x^3+x^4+x^5+x^6+x^8+x^9+x^{10}+x^{12}+x^{16}+x^{17}+x^{18}+x^{20}+x^{24}$. Then the minimum weight vectors of $C_2$ are $x^i(x^2+x^4+x^7+x^9+x^{11}+x^{27}+x^{28})$, $x^i(x^7+x^{10}+x^{11}+x^{23}+x^{28}+x^{29}+x^{30})$, $x^i(1+x^4+x^6+x^{12}+x^{15}+x^{21}+x^{30})$, $x^i(x^2+x^5+x^{10}+x^{12}+x^{13}+x^{16}+x^{25})$, $x^i(1+x^4+x^8+x^9+x^{11}+x^{21}+x^{25})$, $i=0,1,2,\ldots,30$. They also constitute a $(31,7,7)$-BIBD.

If the answer to our Problem 5.1 is affirmative, we would like to propose the following:

**Problem 5.2.** *Suppose $C$ is an abelian duadic code with minimum weight $d$ satisfying $d^2-d=n+11$. Whether the support of all vectors with minimum odd weight $d$ form a BIBD?*

Next, we have checked by computer that the support of the minimum odd weight codewords of $(23,12,7)$-code, $(41,21,9)$-code, $(47,24,7)$-code constitute a $(23,7,21)$-BIBD, $(41,9,18)$-BIBD and $(47,11,220)$-BIBD, respectively, while the support of the minimum odd weight codewords of a $(17, 8, 5)$ code does not constitute a BIBD. The following problem seems challenging.

**Problem 5.3.** *Characterize those duadic codes whose support of all vectors with minimum odd weight $d$ form a BIBD.*

## Acknowledgements

The author wishes to thank Prof. Qingde Kang for providing him with Ref. [8]. The author are grateful to the referees for many helpful comments on an early version of this paper.

## References

[1] C. Curtis, I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Interscience Publishers, New York, 1962.
[2] N. Koblitz, A Course in Number Theory and Cryptography, Springer, Berlin, 1987.
[3] J.S. Leon, J.M. Masley, V. Pless, Duadic codes, IEEE Trans. Inform. Theory IT-30 (1984) 709–714.
[4] F.J. MacWilliams, Codes and ideals in group algebras, in: R.C. Bose, T.A. Dowling (Eds.), Combinatorial Mathematics and its Applications, University of North Carolina Press, Chapel Hill, 1969 (Chapter 18).
[5] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, Amsterdam, 1978.
[6] V. Pless, J.M. Masley, J.S. Leon, On weights in duadic codes, J. Combin. Theory Ser. A 44 (1987) 6–21.
[7] J.J. Rushanan, Duadic codes and difference sets, J. Combin. Theory Ser. A 57 (1991) 254–261.
[8] H.C.A. van Tilborg, On weights in codes, Rep. 71-WSK-03, Department of Math. Tech., University of Eindhoven, Netherlands, December 1971.
[9] H.N. Ward, L. Zhu, Existence of abelian group codes partitions, J. Combin. Theory Ser. A 67 (1994) 276–281.
[10] S. Zhang, Extremal Self-dual codes and Duadic Group Algebra Codes, Ph.D. Thesis, Suzhou University, 1997.
[11] L. Zhu, Duadic group algebra codes, J. Statist. Plann. Inference 51 (1996) 395–401.