Bull. Malays. Math. Sci. Soc. (2016) 39:689–697
DOI 10.1007/s40840-015-0134-0

BULLETIN of the MALAYSIAN MATHEMATICAL SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

A Note on the Weight Distribution of Minimal Constacyclic Codes

Pooja Grover[1] · **Ashwani K. Bhandari**[1]

Received: 23 January 2013 / Revised: 28 June 2013 / Published online: 7 May 2015

Abstract In this note, we determine weight distributions of minimal constacyclic codes of length p^n over the finite field F_l, where p is a prime which is coprime to l.

Keywords Cyclic codes · Constacyclic codes · Constabelian codes

Mathematics Subject Classification 20C05 · 94B05

1 Introduction

Let F_l be a finite field of order l. A linear code $\mathcal{C}$ of length n and dimension k is a linear subspace of vector space $(F_l)^n$. A linear code $\mathcal{C}$ is called a cyclic code if for every word $v = (v_0,\ v_1, \ldots, v_{n-1})$, the vector $(v_{n-1},\ v_0, \ldots, v_{n-2})$, obtain from v by the cyclic shift of co-ordinates $i \mapsto i+1$, taken modulo n, in also in $\mathcal{C}$. A group ring code is an ideal in the group ring RG, where G is a group and R is a suitable commutative ring. Cyclic codes of length n over F_l can be identified with ideals of the group algebra $F_l C_n$ of the cyclic group C_n of order n.

Communicated by Lee See Keong.

The research of the author is supported by CSIR, India and will form part of her Ph.D. thesis.

✉ Pooja Grover
poojagrover1285@gmail.com

Ashwani K. Bhandari
akb@pu.ac.in

1 Department of Mathematics, Centre of Advance Studies in Mathematics, Panjab University, Chandigarh, Chandigarh 160014, India

Using cocycles which arise from cohomology and the theory of projective representations of groups, this concept can be extended by taking ideals of a twisted group ring. In the simplest case of a cyclic group G, these ideals coincide with the constacyclic codes introduced by Berlekamp [1]. For abelian groups, the ideals in the twisted group rings are known as constabelian codes as defined by Lim [9]. Trivial cocycles (i.e., coboundaries) correspond to constacyclic codes that are scalar equivalent to cyclic codes. Throughout this note we take the ring R to be a finite field F_l of order l. In case the characteristic of the field does not divide the order of the group, the twisted group ring turns out to be semisimple (see [11]), so that every ideal (code) of the twisted group ring is a finite direct sum of minimal ideals (codes). The minimal ideals of twisted group ring of cyclic (respectively abelian) groups are defined as minimal constacyclic (respectively constabelian) codes. The weight of a codeword is the number of its elements that are non-zero, and the distance between two codewords (also known as Hamming distance) is the number of elements in which they differ. The distance d of a linear code is minimum weight of its non-zero codewords, or equivalently the minimum distance between distinct codewords. A linear code of length n, dimension k, and distance d will be called a $[n, k, d]_l$ code.

In this note, we take length of the code n to be coprime with the characteristic of the finite field F_l. We determine weight distribution of minimal constacyclic codes. We also compare the minimum distances of constacylic and constabelian codes and it turns out that constabelian codes may be better than cyclic or constacyclic codes in the sense that larger minimum distances can be found in these codes.

2 Some Preliminaries

We need a few definitions and results from cohomology (see, for example, [6]). Let G be a group. A function $\psi : G \times G \to F_l^*$ is called a cocycle if $\psi(1, 1) = 1$ and

$$\psi(xy, z)\psi(x, y) = \psi(x, yz)\psi(y, z) \quad \forall x, y, z \in G.$$

A consequence of the above equation is that $\psi(1, x) = \psi(x, 1) = 1 \; \forall x \in G$. We call a cocycle α on G to be a coboundary if for some $\tau : G \to F_l^*$

$$\alpha(x, y) = \tau(x)\tau(y)\big(\tau(xy)\big)^{-1} \quad \forall x, y \in G,$$

and write $\alpha = \partial\tau$. Two cocycles ψ and ψ' on G are said to be cohomologous if $\psi = \psi'\partial\tau$ for some $\tau : G \to F_l^*$. The set of cocycles from G to F_l forms a group under multiplication denoted by $Z^2(G, F_l)$. The set of coboundaries forms a normal subgroup of $Z^2(G, F_l)$ denoted by $B^2(G, F_l)$. The quotient group $Z^2(G, F_l)/B^2(G, F_l)$ is known as second cohomology group and is denoted by $H^2(G, F_l)$.

For a cocycle ψ on G, the twisted group algebra $F_l^\psi G$ over F_l is defined as an algebra which has the same module structure as that of the group algebra $F_l G$ but the multiplication is defined by linearly extending the multiplication

$$\bar{g}\bar{h} = \psi(g, h)\overline{gh} \quad \forall g, \; h \in G.$$

Let $a \in F_l^* = F_l \setminus \{0\}$. A linear code $\mathcal{C}$ of length n over F_l is said to be a-constacyclic if for $(c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$, the constacyclically shifted vector $(ac_{n-1}, c_0, \ldots, c_{n-2}) \in \mathcal{C}$. In the special case when $a = -1$, such codes are called negacyclic. Constacyclic codes can be viewed as ideals in the ring $\frac{F_l[X]}{\langle X^n - a \rangle}$.

Let $C_n = \langle x \rangle$ be the cyclic group of order n. For $a \in F_l^*$, let $\psi : C_n \times C_n \rightarrow F_l^*$ be a cocycle of C_n given by

$$\psi(x^i, x^j) = \begin{cases} 1, & \text{if } i + j < n \\ a, & \text{if } i + j \geq n. \end{cases}$$

In fact, every cocycle of C_n is of above type (Theorem 3.1 in [6]). Let $F_l^{\psi} C_n$ be the twisted group algebra of C_n over F_l corresponding to the cocycle ψ. It follows that $\frac{F_l[X]}{\langle X^n - a \rangle}$ is isomorphic to the twisted group algebra $F_l^{\psi} C_n$ resulting in a one to one correspondence between the a-constacyclic codes of length n over F_l and the ideals of the twisted group algebra $F_l^{\psi} C_n$.

By the Fundamental Theorem of finite abelian groups $G = C_{n_1} \times \cdots \times C_{n_t}$, where $n_1 | n_2 \ldots | n_t$ and $C_{n_i} = \langle x_i \rangle$. Let $\psi : G \times G \rightarrow F_l^*$ be a cocycle of G, which is the product of cocycles of $C_{n_1}, \ldots, C_{n_t}$ given by

$$\psi_i\left(x_i^{k_1}, x_i^{k_2}\right) = \begin{cases} 1, & \text{if } k_1 + k_2 < n_i \\ a_i, & \text{if } k_1 + k_2 \geq n_i, \end{cases}$$

where, for $1 \leq i \leq t$, $a_i \in F_l^*$. In [9], a code $\mathcal{C}$ is called a constabelian code associated with abelian group G if there exist $a_1, \ldots, a_t \in F_l^*$ such that $\mathcal{C}$ is an ideal of the ring $\mathcal{A} = \frac{F_l[X_1, \ldots, X_t]}{\langle X_1^{n_1} - a_1, \ldots, X_t^{n_t} - a_t \rangle}$. It follows easily that $\mathcal{A} \cong F_l^{\psi} G$, where ψ is the product cocycle defined above and as stated earlier, minimal (irreducible) ideals of the twisted group algebra $F_l^{\psi} G$ for abelian group G are known as minimal (irreducible) constabelian codes. In [4], minimal constabelian (and constacyclic) codes have been explicitly determined for several families of abelian and cyclic groups.

3 Weight Distribution of Constacyclic Codes of Length p^n

Let $A_i^{(n)}$ denote the number of codewords of weight i in a code $\mathcal{C}$ of length n. The list $A_0^{(n)}, A_1^{(n)}, \ldots, A_n^{(n)}$ is called the weight distribution (or weight spectrum) of the code $\mathcal{C}$, and the corresponding homogeneous polynomial

$$W_{\mathcal{C}}(x, y) = \sum_{i=0}^{n} A_i^{(n)} x^{n-i} y^i$$

is called the Hamming weight enumerator of $\mathcal{C}$. The knowledge of the weight distribution of a code enables one to calculate the probability of undetected errors when the code is used purely for error detection. The least positive value of i for which A_i is non-zero is the minimum Hamming weight of the code which gives a measure that how good a code is at error correcting. The problem of the determination of weight distribution of a code is of considerable interest.

It is known that if $\mathcal{C}$ and $\mathcal{D}$ are two codes of length n, then the weight enumerator of the direct sum $\mathcal{C} \bigoplus \mathcal{D}$ is $W_{\mathcal{C} \bigoplus \mathcal{D}}(x, y) = W_{\mathcal{C}}(x, y) W_{\mathcal{D}}(x, y)$ (for example, see [5]). As every constacyclic code is a direct sum of irreducible constacyclic codes, it is enough to compute weight distributions of irreducible constacyclic codes.

Let $G = \langle C_{p^n} \rangle = \langle x \rangle$ be a cyclic group of order p^n, where p is an odd prime. Let F_l be a finite field such that l is coprime to p. Let $a \in F_l^*$ and let, as usual, ψ be the cocycle given by

$$\psi\left(x^i, x^j\right) = \begin{cases} 1, & \text{if } i + j < p^n \\ a, & \text{if } i + j \geq p^n. \end{cases}$$

The following well-known result characterizes 2-cocycles of cyclic groups (See, for example [6], p. 52).

Proposition 3.1 *Let $G = C_n$ be a cyclic group of order n and let K be a field. Then the second cohomology group $H^2(G, K^*)$ is isomorphic to $\frac{K^*}{(K^*)^n}$.*

Corollary 3.2 *Let C_n be the cyclic group of order n and let K be a finite field such that n is coprime to $o(K^*)$, the order of the multiplicative group of K. Then $H^2(C_n, K^*)$ is trivial.*

Proof As n is coprime to $o(K^*)$, $(K^*)^n = K^*$. □

From the above corollary, it follows that proper constacyclic codes of length n over F_l exist if and only if $\gcd(n, o(K^*)) > 1$; otherwise, they are equivalent to cyclic codes, as the corresponding twisted group algebras are isomorphic to group algebras in these cases, (see [[6], Page 17]). Let K be the splitting field of $x^{p^n} - a$ over F_l. For $1 \leq i \leq n$, let ε_{p^i} be the primitive p^ith root of unity. Depending on the divisibility of $l - 1$ by p, the following cases arise:

Suppose that $p \nmid l - 1$. Then $\gcd(p^n, l - 1) = 1$ implies that there exist integers x' and y' such that $p^n x' + (l - 1)y' = 1$, so that $a = a^{p^n x' + (l-1)y'} = a^{p^n x'} a^{(l-1)y'} = a^{p^n x'}$ and hence $a \in (F_l)^{p^n}$. So, $F_l^{\psi} C_{p^n} \cong F_l C_{p^n}$ ([6], p. 53), yielding that constacyclic codes in this case are equivalent to cyclic codes. Weight distributions of cyclic codes have been studied by many authors, for instance in [2,3,10,12–14].

Suppose that p divides $l - 1$. Again, there are two possibilities; either $p \nmid o(a)$ or $p | o(a)$. In the first case, as $\gcd(p^n, o(a)) = 1$, it follows that $a \in (F_l)^{p^n}$, yielding $F_l^{\psi} C_{p^n} \cong F_l C_{p^n}$.

Thus, it only remains to consider the case when p divides both $l - 1$ and $o(a)$. Proper constacyclic codes, i.e., constacyclic codes which are not equivalent to cyclic codes exist in this case only. We shall determine the weight distributions of such constacyclic codes of length p^n.

The main result about the weight distribution of the irreducible constacyclic codes of length p^n over the finite field F_l is given in the following:

Theorem 3.3 *Let F_l be a finite field with l elements. Let p be an odd prime such that $p \mid l-1$. Let $a \in F_l^* = F_l \setminus \{0\}$ such that $p \mid o(a)$. The weight distribution of each a-constacyclic code of length p^n over F_l is given by*

$$A_i^{(p^n)} = \begin{cases} 0, & \text{if } p^s \nmid i \\ \binom{p^{n-s}}{w'}(l-1)^{w'}, & \text{if } i = p^s w'. \end{cases}$$

where s is the largest integer such that $a \in (F_l)^{p^s}$.

Proof Let s be the largest integer such that $a \in (F_l)^{p^s}$, i.e., there exists an element $b \in F_l \setminus (F_l)^p$ such that $a = b^{p^s}$ and let α be an element in some extension field of F_l such that $\alpha^{p^n} = a$. As $\alpha^{p^{n-s}} = b$,

$$\begin{aligned} x^{p^n} - a &= x^{p^n} - b^{p^s} \\ &= \left(x^{p^{n-s}} - b\right)\left(x^{p^{n-s}\left(p^s-1\right)} + b\, x^{p^{n-s}\left(p^s-2\right)} + \cdots + b^{p^s-1}\right) \\ &= \left(x^{p^{n-s}} - b\right) b^{p^s-1} \prod_{i=1}^{s} \Phi_{p^i}\left(\left(\alpha^{-1}x\right)^{p^{n-s}}\right), \end{aligned}$$

where $\Phi_{p^i}(x)$ is cyclotomic polynomial of order p^i. Now $p|o(a)$ and $p|l-1$. Let m be the largest integer such that $p^m|l-1$. Supposing $F_l^* = C_{p^m} \times C_{q_1^{k_1}} \times \cdots \times C_{q_t^{k_t}}$, where q_i's are distinct primes, we get $(F_l^*)^{p^m} \cong C_{q_1^{k_1}} \times \cdots \times C_{q_t^{k_t}}$ so that $a \notin (F_l^*)^{p^m}$. It follows that $s < m$ and for $1 \le i \le s$, $\text{ord}_{p^i}(l) = 1$, where $\text{ord}_{p^i}(l)$ denotes the multiplicative order of l modulo p^i. Consequently, by Theorem 2.47 of [8], $\Phi_{p^i}(x)$ factors into linear polynomials over F_l so that $\Phi_{p^i}\left((\alpha^{-1}x)^{p^{n-s}}\right)$ factors into polynomials of degree p^{n-s} over F_l.

Let ϕ denote the Euler phi function. For a prime p, $\phi(p^i) = p^i - p^{i-1}$. Thus,

$$\begin{aligned} &\Phi_{p^i}\left(\left(\alpha^{-1}x\right)^{n-s}\right) \\ &= \left(\left(\alpha^{-1}x\right)^{p^{n-s}} - \varepsilon_{p^i}\right)\left(\left(\alpha^{-1}x\right)^{p^{n-s}} - \varepsilon_{p^i}^2\right)\cdots\left(\left(\alpha^{-1}x\right)^{p^{n-s}} - \varepsilon_{p^i}^{\phi\left(p^i\right)}\right) \\ &= \frac{1}{b^{\phi(p^i)}}\left[\left(x^{p^{n-s}} - b\varepsilon_{p^i}\right)\left(x^{p^{n-s}} - b\varepsilon_{p^i}^2\right)\cdots\left(x^{p^{n-s}} - b\varepsilon_{p^i}^{\phi\left(p^i\right)}\right)\right] \\ &= \frac{1}{b^{p^i-p^{i-1}}}\left[\left(x^{p^{n-s}} - b\varepsilon_{p^i}\right)\left(x^{p^{n-s}} - b\varepsilon_{p^i}^2\right)\cdots\left(x^{p^{n-s}} - b\varepsilon_{p^i}^{p^i-p^{i-1}}\right)\right]. \end{aligned}$$

Since $b \notin (F_l)^p$, therefore, $b\varepsilon_{p^i} \notin (F_l)^p$, so that by ([7], Lemma 16.5) each of the polynomial $x^{p^{n-s}} - b\varepsilon_{p^i}^j$ is irreducible over F_l and

$$x^{p^n} - a = \left(x^{p^{n-s}} - b\right) \prod_{i=1}^{s} \prod_{j=1}^{p^i - p^{i-1}} \left(x^{p^{n-s}} - b\varepsilon_{p^i}^{j}\right).$$

We observe that $\varepsilon_{p^i}^{h^j}$, $1 \le i \le s, 0 \le j \le p^i - p^{i-1} - 1$, are contained in F_l. Thus, replacing b by $b\varepsilon_{p^i}^{h^j}$ will yield the same factorization of $x^{p^n} - a$, as $a = b^{p^s} = (b\varepsilon_{p^i}^{h^j})^{p^s}$.

The ring $\frac{F_l[x]}{\langle x^{p^n} - a\rangle}$ is a principal ideal ring and any ideal in it is generated by (the image of) a divisor of $x^{p^n} - a$. Consider the ideal I generated by the polynomial

$$g(x) = x^{p^{n-s}\left(p^s-1\right)} + bx^{p^{n-s}\left(p^s-2\right)} + \cdots + b^{p^s-1},$$

so that, $I = \frac{F_l[x]}{\langle x^{p^{n-s}} - b\rangle}$ is an irreducible constacyclic code. Dimension of the ideal I over F_l is p^{n-s}. Note that $g(x),\ x^{p^s} g(x),\ x^{2p^s} g(x), \ldots, x^{(p^{n-s}-1)p^s} g(x)$ form a basis of the ideal I over F_l, as this is a linearly independent set and the number of elements in this set is equal to the dimension of I.

Let $e_i,\ 1 \le i \le p^n$, be the standard basis of $(F_l)^{p^n}$ as a vector space over F_l. Identifying the polynomial $g(x)$ with the tuple $\sum_{j=1}^{p^s} b^{j-1} e_{p^n - jp^{n-s}}$, any codeword c in I can be written as

$$c = \sum_{i=0}^{p^{n-s}-1} \sum_{j=1}^{p^s} \alpha_i b^{j-1} e_{p^s\left(p^{n-s}+i\right) - jp^{n-s}},$$

where $\alpha_i \in F_l$ [as $x^{ip^s} g(x)$ is the touple $\sum_{j=1}^{p^s} b^{j-1} e_{p^n - jp^{n-s} + ip^s}$ for $0 \le i \le p^{n-s} - 1$]. Clearly, $\text{wt}(c) = p^s w'$, where $\text{wt}(c)$ denotes the weight of the codeword c and w' is the number of non-zeros α_i's. Therefore,

$$A_w^{p^n} = 0, \quad \text{when } p^s \nmid w,$$

and a codeword in I has weight $w = p^s w'$ if and only if it is a linear combination of any w' basis vectors over F_l out of total p^{n-s} basis vectors of I. Therefore, there are $\binom{p^{n-s}}{w'}(l-1)^{w'}$ codewords of weight $w = p^s w'$ in I.

If we take another ideal of the ring $\frac{F_l[x]}{\langle x^{p^n} - a\rangle}$, for instance $I' = \frac{F_l[x]}{\langle x^{p^{n-s}} - b\varepsilon_{p^i}^{h^j}\rangle}$, for some $1 \le i \le s$ and $1 \le j \le \phi(p^i)$, on replacing b by $b\varepsilon_{p^i}^{h^j}$, we get the same result as $a = b^{p^s} = \left(b\varepsilon_{p^i}^{h^j}\right)^{p^s}$ and it follows that the weight enumerator of every irreducible constacyclic code of length p^n is the same, which is given by

$$A_i^{(p^n)} = \begin{cases} 0, & \text{if } p^s \nmid i \\ \binom{p^{n-s}}{w'}(l-1)^{w'}, & \text{if } i = p^s w' \end{cases}$$

where s is the largest integer such that $a \in (F_l)^{p^s}$. □

Corollary 3.4 *It follows that the minimum distance of an irreducible constacyclic codes of length* p^n *and dimension* p^{n-s} *over* F_l *is* p^s*, as* $A_i^{(p^n)} = 0$ *for* $p^s \nmid i$*, so that the least value of i for which* $A_i^{(p^n)}$ *is non-zero is* p^s*.*

Example 3.5 Let $C_{27} = \langle x \rangle$ be cyclic group of order 27. Let $l = 19$ and let the cocycle $\psi : C_{27} \times C_{27} \to F_{19}^*$ be given by

$$\psi\left(x^i, x^j\right) = \begin{cases} 1, & \text{if } i + j < 27 \\ 7, & \text{if } i + j \geq 27, \end{cases}$$

for $0 \leq i, j \leq 27$. The order of 7 in F_{19} is 3. In the above notations, $s = 1,\ m = 2$, and $x^{27} - 7 = (x^9 - 4)(x^9 - 6)(x^9 - 9)$ is the irreducible factorization of $x^{27} - 7$ over F_{19}. Consider the ideal $I = \frac{F_{19}[x]}{\langle x^9 - 4 \rangle} = \langle g(x) \rangle$, where $g(x) = (x^9 - 6)(x^9 - 9) = x^{18} - 15x^9 + 16$. We note that $g(x),\ x^3 g(x),\ x^6 g(x), \ldots, x^{24} g(x)$ form a basis of I and the weight enumerators are given by

$$A_i^{(27)} = \begin{cases} 0, & \text{if } 3 \nmid i \\ \binom{9}{w'} (18)^{w'}, & \text{if } i = 3w'. \end{cases}$$

It would be of considerable interest to determine weight distribution of other minimal constacyclic and in general, of constabelian codes, which at present seems to be difficult.

We now compare the minimum distances of constacyclic codes with the minimum distances of constabelian codes.

Example 3.6 Let $C_{729} = \langle z | z^{729} = 1 \rangle$ be the cyclic group of order 729. Let $l = 19$ and let the cocycle ψ be given by

$$\psi\left(z^i, z^j\right) = \begin{cases} 1, & \text{if } i + j < 729 \\ 7, & \text{if } i + j \geq 729. \end{cases}$$

The order of 7 in F_{19} is 3. In the notations described earlier, $m = 2$ (as $3^2 \mid 19 - 1$, but $3^3 \nmid 19 - 1$), $s = 1$ [as $7 \in F_{19}$, but $7 \notin (F_{19})^2$] and over F_{19}, $x^{729} - 7 = (x^{243} - 4)(x^{243} - 6)(x^{243} - 9)$. By Corollary 3.4, we get that the minimum distance of the minimal constacyclic code of length 729 is $3^s = 3^1 = 3$. Thus, we get a $[729, 243, 3]_{19}$ constacyclic code.

Let $G = C_9 \times C_{81} = \langle x, y | x^9 = 1 = y^{81} \rangle$ be an abelian group of order 729. Let $\psi = \psi_1 \psi_2$ be given by

$$\psi_1\left(x^i, x^j\right) = \begin{cases} 1, & \text{if } i + j < 9 \\ 7, & \text{if } i + j \geq 9 \end{cases}$$

Table 1 Comparison of constacyclic and constablelian codes

Codes	Length (n)	Dimension (k)	Minimum distance (d)
Constacyclic	729	243	3
Constabelian	729	3	243

and

$$\psi_2(y^{i'}, y^{j'}) = \begin{cases} 1, & \text{if } i' + j' < 81 \\ 7^9 = 1 \pmod{19}, & \text{if } i' + j' \geq 81. \end{cases}$$

Note that $F_{19}^{\psi_2} C_{81} \cong F_{19} C_{81}$. As $\mathrm{ord}(7) = 3$ and $\mathrm{ord}(7^9) = 1$, $3 | \mathrm{ord}(7)$ but $3 \nmid \mathrm{ord}(7^9)$.

One checks that constabelian code generated by the idempotent $e = \frac{1}{243}(1 + 4x^3 + 16x^6)\left(\sum_{v=0}^{80} y^v\right) \in F_{19}^{\psi}(C_9 \times C_{81})$ has minimum distance $3 \times 81 = 243$, as any element in this ideal will be of the type $\alpha = \sum_{u,v} \alpha_{u,v} x^u y^v.e = \sum_{u,v} \alpha_{u,v} x^u.e$. Since the length of the element $\sum_{v=0}^{80} y^v$ is 81, the minimum distance of this ideal will be 81 times the minimum distance of the constacyclic code of length 9 and dimension 3, which is 3 and we get a $[729, 3, 243]_{19}$ constabelian code. Thus, minimum distance of the constabelian code of length 729 is 81 times more than the constacyclic code of length 729.

We have Table1.

It turns out that constabelian codes may have larger minimum distances than constacyclic codes of same length.

References

1. Berlekamp, E.R.: Algebraic Coding Theory. McGraw-Hill, New York (1968)
2. Baumert, L.D., McEliece, R.J.: Weights of irreducible cyclic codes. Inf. Control **20**, 158–175 (1972)
3. Cunsheng, D.: The weight distribution of some irreducible cyclic codes. IEEE Trans. Inf. Theory **55**(3), 255–260 (2009)
4. Grover, P., Bhandari, A.K.: Explicit determination of certain constabelian codes. Finite Fields Appl. **18**(6), 1037–1060 (2012)
5. Huffman, W.C., Pless, V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003)
6. Karpilovsky, G.: Projective Representations of Finite Groups. Marcel Dekker, New York (1985)
7. Karpilovsky, G.: Field Theory, Classical Foundations and Multiplicative Groups. Marcel Dekker, New York (1988)
8. Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia Mathematics and its Applications. Addison Wesley Publishing Company, London (1983)
9. Lim, C.J.: Consta abelian polyadic codes. IEEE Trans. Info. Theory **51**(6), 2198–2206 (2005)
10. MacWilliams, F., Seery, J.: The weight distributions of some minimal cyclic codes. IEEE Trans. Info. Theory **27**(6), 796–806 (1981)
11. Passman, D.S.: On the semisimplicity of twisted group algebras. Proc. Am. Math. Soc. **25**(1), 161–166 (1970)
12. Segal, R.B., Ward, R.L.: Weight distributions of some irreducible cyclic codes. Math. Comput. **46**(173), 341–354 (1986)

13. Sharma, A., Bakshi, G.K.: The weight distribution of some irreducible cyclic codes. Finite Fields Appl. **18**, 144–159 (2012)
14. Sharma, A., Bakshi, G.K., Raka, M.: The weight distribution of irreducible cyclic codes of length 2^m. Finite Fields Appl. **13**(4), 1086–1095 (2007)