Some minimal cyclic codes over finite fields

Hongwei, Liu; Guanghui, Zhang; Bocong, Chen

2014

Chen, B., Liu, H., & Zhang, G. (2014). Some minimal cyclic codes over finite fields. Discrete Mathematics, 331, 142-150.

https://hdl.handle.net/10356/99891

https://doi.org/10.1016/j.disc.2014.05.007

Some Minimal Cyclic Codes over Finite Fields *

Bocong Chen[1], Hongwei Liu[2], Guanghui Zhang[3]

[1]Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore
[2]School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, 430079, China
[3]School of Mathematical Sciences, Luoyang Normal University, Luoyang, Henan, 471022, China

Abstract

In this paper, the explicit expressions for the generating idempotents, check polynomials and the parameters of all minimal cyclic codes of length tp^n over F_q are obtained, where p is an odd prime different from the characteristic of F_q, t and n are positive integers with $t \mid (q-1)$, $\gcd(t,p)=1$ and $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$. Our results generalize the main results in [M. Pruthi, S. K. Arora, Minimal codes of prime-power length, Finite Fields Appl., 3(1997), 99-113. [24]] and in [S. K. Arora, M. Pruthi, Minimal cyclic codes of length $2p^n$, Finite Fields Appl., 5(1999), 177-187. [1]], which considered the cases $t=1$ and $t=2$ respectively. We propose an approach different from those in [24, 1] to obtain the generating idempotents.

Keywords: Cyclic code, Hamming distance, irreducible character, primitive idempotent, check polynomial, minimal cyclic code.

2010 Mathematics Subject Classification: 94B15; 94B05.

1 Introduction

Cyclic codes were among the first codes practically used and they play a very significant role in coding theory. One is that they can be efficiently encoded using shift registers. There are also decoding schemes utilizing shift registers. Many important codes such as the Golay codes, Hamming codes and BCH codes can be represented as cyclic codes.

There is a lot of literature about cyclic codes (e.g. see [9]-[14], [23], [28]), which greatly enhances their practical applications. Dougherty and Ling in [14] classified cyclic codes of length 2^k over the Galois ring $GR(4,m)$. Jia *et al.* showed that self-dual cyclic codes of length n over F_q exist if and only if both n and q are even ([17], [18]). Dinh [11] obtained

*Email addresses: bocong_chen@yahoo.com (B. Chen), hwliu@mail.ccnu.edu.cn (H. Liu), zghui2012@126.com (G. Zhang).

the algebraic structures of cyclic codes of length p^s over $F_{p^m} + uF_{p^m}$, and determined the number of codewords in each of those cyclic codes. Dinh in [13] exhibited all repeated-root self-dual cyclic codes of length $3p^s$ over F_{p^m}. More recently, Chen *et al.* [9] determined the structures of all cyclic codes of length $2^m p^n$ over F_q, where F_q is of odd characteristic and p is an odd prime divisor of $q-1$.

Let F_q be a finite field of order q and n be a positive integer coprime to q. The *minimal cyclic codes* of length n over F_q are viewed as minimal ideals of the semisimple algebra $F_q[X]/\langle X^n-1\rangle \cong F_qC_n$, where F_qC_n denotes the group algebra of the cyclic group $C_n = \langle g\rangle$ of order n over F_q. Every cyclic code is a direct sum of some minimal cyclic codes. This is one of the principal reasons why minimal cyclic codes are so important. Also note that minimal cyclic codes include the important family of simplex codes, which are very useful in communications systems (see [22], Chapter 8).

It is well known that every minimal cyclic code is generated uniquely by one primitive idempotent, which is called the *generating idempotent* of the code (e.g. see [16, Theorem 4.3.8]). Theoretically, one can easily obtain all the primitive idempotents of F_qC_n. Suppose ζ is a primitive n-th root of unity in some extension field of F_q and $F_{q^s} = F_q(\zeta)$. Further assume that all the distinct q-cyclotomic cosets modulo n are given by $\Gamma_0, \Gamma_1, \cdots, \Gamma_{r-1}$. Then $F_{q^s}C_n$ has exactly n primitive idempotents given by $e_{\chi^i} = \frac{1}{n}\sum_{j=0}^{n-1} \zeta^{-ji} g^j$, $0 \le i \le n-1$. Moreover, F_qC_n has exactly r primitive idempotents given by $e_{\Gamma_t} = \sum_{j\in\Gamma_t} e_{\chi^j}$, $0 \le t \le r-1$. Determining the number of nonzero coefficients appearing in the primitive idempotent e_{Γ_t}, called the Hamming weight of the generating idempotent which is very important for the theory of error-correcting codes, appears to be still an intractable problem in general. It is a challenge to obtain the primitive idempotents in an explicit form such that the minimal Hamming distances of the codes generated by the primitive idempotents can be calculated precisely.

In recent years many papers have dealt with parameters and generating idempotents of minimal cyclic codes (e.g. see [1]-[5], [25]). Let p be an odd prime coprime to q. The minimal cyclic codes of length p^n and $2p^n$ over F_q were investigated in [4] and [5] sequentially where q has order $\frac{\phi(p^n)}{2}$ in the cyclic group $\mathbf{Z}_{p^n}^*$, i.e. $\mathrm{ord}_{p^n}(q) = \frac{\phi(p^n)}{2}$. The minimal cyclic codes of length p^n and $2p^n$ with $\mathrm{ord}_p(q) = f$ and $\gcd(\frac{q-1}{f}, q) = 1$ were considered in [26] and [27] respectively. We have studied minimal cyclic codes of length ℓ^m over F_q, where ℓ is a prime divisor of $q-1$ and m is an arbitrary positive integer [8]. Recently, van Zanten *et al.* in [29] introduced a new class of linear cyclic codes, which includes as special cases quadratic residue codes, generalized quadratic residue codes, e-residue codes and Q -codes. Expressions for idempotent generators are derived for these codes.

Berman listed the explicit expressions for the primitive idempotents of $F_qC_{p^n}$ in [6] without proof, where q is a primitive root modulo p^n. Pruthi and Arora in [24] presented a detailed calculation for the above result and obtained the parameters of these minimal cyclic codes. In the subsequent paper [1], minimal cyclic codes of length $2p^n$ over F_q with $\mathrm{ord}_{2p^n}(q) = \phi(p^n)$ were considered, where p is an odd prime different from the characteristic of F_q. The expressions for the primitive idempotents of $F_q[X]/\langle X^{2p^n}-1\rangle$ were given

explicitly.

Let t and n be positive integers with $t \mid (q-1)$, $\gcd(t,p)=1$ and $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$. In this paper, we study minimal cyclic codes of length tp^n over F_q. This extends the main results given in [24] and [1] which considered the cases $t=1$ and $t=2$ respectively. We propose a new approach to obtain the primitive idempotents of $F_q[x]/\langle X^{tp^n}-1\rangle$; that is, we obtain the primitive idempotents of $F_q[X]/\langle X^{tp^n}-1\rangle$ by computing irreducible characters of the cyclic group C_{tp^n} of order tp^n over F_q. Then we characterize explicitly the check polynomials and parameters of these minimal cyclic codes. It turns out that except for t cyclic code with parameters $[tp^n, 1, tp^n]$, all the others have parameters $[tp^n, \phi(p^i), 2tp^{n-i}]$, $1 \le i \le n$.

The remaining sections of this paper are organized as follows. In Section 2, the necessary notations and known results are provided. In Section 3, explicit values for the irreducible characters of the cyclic group C_{tp^n} of order tp^n over F_q are obtained; the primitive idempotents of $F_q[X]/\langle X^{tp^n}-1\rangle$ are characterized in a very explicit form. In Section 4, the check polynomials, dimensions and minimum Hamming distances of the minimal cyclic codes generated by these primitive idempotents are explicitly given.

2 Preliminaries

Throughout this paper F_q denotes the finite field of order q and F_q^* denotes the multiplicative group of F_q. For β in F_q^*, let $\mathrm{ord}(\beta)$ be the order of β in the group F_q^*, and β is called a *primitive* $\mathrm{ord}(\beta)$*-th root of unity*. Note that F_q^* is a cyclic group of order $q-1$. We denote by $F_q^*=\langle\xi\rangle$, where ξ is a primitive $(q-1)$-th root of unity.

Let $\mathbf{Z}_n^*$ be the multiplicative group of all residue classes mod n which are coprime to n and let $\mathrm{ord}_n(r)$ denote the order of the residue $\bar{r}$ in the group $\mathbf{Z}_n^*$. As usual, the notation $\phi(n)$ denotes the Euler function.

Suppose n is a positive integer coprime to q. The *n-th cyclotomic polynomial* is defined by $\Phi_n(X)=\prod(X-\varsigma)$, where ς ranges over all the primitive n-th roots of unity in some extension field of F_q. It is well known that the coefficients of $\Phi_n(X)$ belong to the prime subfield of F_q and $\Phi_n(X)$ is irreducible over F_q if and only if $\mathrm{ord}_n(q)=\phi(n)$ (see [20, Theorem 2.45 and Theorem 2.47]).

Any element of the quotient algebra $F_q[X]/\langle X^n-1\rangle$ is uniquely represented by a polynomial $a(X)=a_0+a_1X+\cdots+a_{n-1}X^{n-1}$, hence it can be identified with a word $\mathbf{a}=(a_0,a_1,\cdots,a_{n-1})$ of length n over F_q. Thus, we can define the corresponding Hamming weight and the Hamming distance on the quotient algebra $F_q[X]/\langle X^n-1\rangle$, namely we define $w_H(a(X))=w_H(\mathbf{a})$ and $d_H(a(X),b(X))=w_H(\mathbf{a}-\mathbf{b})$, where $a(X)$ and $b(X)$ are polynomials over F_q with degrees being less than n.

In this way, any cyclic code C of length n over F_q is identified with exactly one ideal of the quotient algebra $F_q[X]/\langle X^n-1\rangle$, which is generated uniquely by a monic divisor $g(X)$ of X^n-1; in this case, $g(X)$ is called the *generator polynomial* of C. And, the polynomial $h(X)=\frac{X^n-1}{g(X)}$ is called the *check polynomial* of C. The *minimal cyclic codes* of length n over F_q are minimal ideals of the quotient algebra $F_q[X]/\langle X^n-1\rangle$.

In the rest of this section, we recall some basic concepts and results from character

theory of finite groups. The readers may refer to [15], [19] or [21] for more details. Let G be a finite group with $\gcd(q, |G|) = 1$ and $F_qG = \{\sum_{g\in G} a_g g \,|\, a_g \in F_q\}$ be the group algebra of G over F_q. We then see that F_qG is semisimple ([21, Theorem 1.5.6]), and that any F_qG-module V is the direct sum of of irreducible submodules. ([21, Corollary 1.5.3(b)]).

It is well known that if $\chi_1, \chi_2, \cdots, \chi_r$ are all the distinct irreducible characters of G over F_q, then any character of G over F_q can be expressed as a sum of some irreducible characters (see, [21, Lemma 1.5.2]). Among the characters of G we have the *trivial character* χ_0 defined by $\chi_0(g) = 1$ for all $g \in G$; the other characters of G are called *non-trivial*. For a character χ afforded by an F_qG-module V, $\dim_{F_q} V$ is called the *degree* of χ.

The F_q-vector space F_qG with the natural multiplication gv ($g \in G$, $v \in F_qG$) is called the *left regular F_qG-module*. The representation $g \mapsto [g]_{\mathcal{B}}$ obtained by taking $\mathcal{B} = \{g \,|\, g \in G\}$ to be the natural basis of F_qG is called the *regular representation* of G over F_q, where $[g]_{\mathcal{B}}$ denotes the matrix of g (as an F_q-linear transformation of F_qG) relative to the basis $\mathcal{B}$. The *regular character* χ_{reg} of G over F_q is the character afforded by the left regular F_qG-module F_qG. If $L_1, \cdots, L_r$ is a set of representatives of the isomorphism classes of irreducible F_qG-modules, it follows from Wedderburn's theorem ([21, Theorem 1.5.5]) that F_qG is isomorphic to $\bigoplus_{i=1}^{r}(n_iL_i)$ as F_qG-module, where n_i are positive integers; in the language of character theory, we see that $\chi_{reg} = \sum_{i=1}^{r} n_i\chi_i$, where the χ_i are the irreducible characters afforded by L_i, $1 \le i \le r$.

Let H be a subgroup of G and W a left F_qH-module. Since F_qG can be considered as an (F_qG, F_qH)-bimodule, the tensor product $W^G = F_qG \bigotimes_{F_qH} W$ is a left F_qG-module, called the module induced from W. Let χ be a character of H afforded by W, and let $Ind_H^G(\chi)$ be the *induced character* of χ afforded by the left F_qG-module W^G. We then know (e.g. see [15, Lemma 9.2]) that $Ind_H^G(\chi)$ satisfies $Ind_H^G(\chi)(g) = 1/|H| \sum_{u\in G} \dot{\chi}(y^{-1}gy)$, where $\dot{\chi}(g) = \chi(g)$ if $g \in H$; otherwise, $\dot{\chi}(g) = 0$. In particular, $Ind_H^G(\chi)(1) = |G|/|H|\chi(1)$.

It is true that if χ_{reg} is the regular character of H over F_q, then $Ind_H^G(\chi_{reg})$ is the regular character of G over F_q; if χ_1 and χ_2 are characters of H, then $Ind_H^G(\chi_1 + \chi_2) = Ind_H^G(\chi_1) + Ind_H^G(\chi_2)$ (see [21, Theorem 3.2.14]).

The following result shows that we can easily obtain the primitive idempotents of the group algebra F_qG once we have got the irreducible characters of G over F_q (see [21, Theorem 2.1.6]).

Lemma 2.1. *Let $C_m = \langle g \rangle$ be a cyclic group of order m. Suppose that F_qC_m is semisimple and has exactly r irreducible characters, say $\chi_1, \chi_2, \cdots, \chi_r$. Then F_qC_m has precisely r primitive idempotents given by*

$$e_i = \frac{1}{m} \sum_{j=0}^{m-1} \chi_i(g^{-j}) g^j, \ 1 \le i \le r.$$

3 Primitive idempotents in $F_q[X]/\langle X^{tp^n} - 1\rangle$

Let F_q be the finite field of order q and $F_q^* = \langle \xi \rangle$ as before. Throughout this paper, p denotes an odd prime different from the characteristic of F_q; t denotes a positive integer

with $\gcd(t,p)=1$ and $t\,|\,(q-1)$.

As mentioned in Section 1, the primitive idempotents of the semisimple algebras $F_q[X]/\langle X^{p^n}-1\rangle$ and $F_q[X]/\langle X^{2p^n}-1\rangle$ were explicitly characterized in [24] and in [1] respectively, when q has order $\phi(p^n)$ in the cyclic group $\mathbf{Z}_{p^n}^*$. In this section, we extend these results to a more general setting; that is, we obtain the primitive idempotents of $F_q[X]/\langle X^{tp^n}-1\rangle$ with $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$.

We begin with the following lemma which shows that $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$ implies $\mathrm{ord}_{p^n}(q)=\phi(p^n)$ and conversely.

Lemma 3.1. *Let t,p,n,q be set as our conventions. Then $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$ if and only if $\mathrm{ord}_{p^n}(q)=\phi(p^n)$.*

Proof. Since $\gcd(p,t)=1$, it follows from the Chinese Remainder Theorem that $\theta(z)=\big(z\ (\mathrm{mod}\ t),\ z\ (\mathrm{mod}\ p^n)\big)$ defines a ring isomorphism θ from $\mathbf{Z}_{tp^n}$ onto $\mathbf{Z}_t\times\ \mathbf{Z}_{p^n}$. We then have the following isomorphism of groups (also denoted by θ for simplicity):

$$\theta:\quad \mathbf{Z}_{tp^n}^*\longrightarrow\ \mathbf{Z}_t^*\times\ \mathbf{Z}_{p^n}^*,\ \ m\ (\mathrm{mod}\ tp^n)\mapsto\Big(m\ (\mathrm{mod}\ t),\ m\ (\mathrm{mod}\ p^n)\Big).$$

It follows that

$$\theta\big(q\ (\mathrm{mod}\ tp^n)\big)=\big(q\ (\mathrm{mod}\ t),\ q\ (\mathrm{mod}\ p^n)\big)=\big(1\ (\mathrm{mod}\ t),\ q\ (\mathrm{mod}\ p^n)\big).$$

The second equality holds since $t\,|\,(q-1)$.

If $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$, i.e. q has order $\phi(p^n)$ in the group $\mathbf{Z}_{tp^n}^*$. Then $\big(1\ (\mathrm{mod}\ t),\ q\ (\mathrm{mod}\ p^n)\big)$ has order $\phi(p^n)$ in $\mathbf{Z}_t^*\times\ \mathbf{Z}_{p^n}^*$. We deduce that $q\ (\mathrm{mod}\ p^n)$ has order $\phi(p^n)$ in $\mathbf{Z}_{p^n}^*$, i.e. $\mathrm{ord}_{p^n}(q)=\phi(p^n)$.

Conversely, by $t\,|\,(q-1)$ we have

$$\big(q\ (\mathrm{mod}\ t),\ q\ (\mathrm{mod}\ p^n)\big)=\big(1\ (\mathrm{mod}\ t),\ q\ (\mathrm{mod}\ p^n)\big).$$

Then we obtain the desired result by the isomorphism θ. □

Lemma 3.2. *If $\mathrm{ord}_{tp^n}(q)=\phi(p^n)$, then p is coprime to $q-1$.*

Proof. By Lemma 3.1, we get that $\mathrm{ord}_{p^n}(q)=\phi(p^n)$, which implies $\mathrm{ord}_p(q)=\phi(p)$. Now, suppose otherwise that $p\,|\,(q-1)$, i.e. $\mathrm{ord}_p(q)=1$. Combining with $\mathrm{ord}_p(q)=\phi(p)$, we have $\phi(p)=1$. This is a contradiction, since p is an odd prime. Therefore, $\gcd(p,q-1)=1$. □

It was shown that if ℓ is a positive integer coprime to $q-1$, then there is an F_q-algebra isomorphism between $F_q[X]/\langle X^\ell-1\rangle$ and $F_q[X]/\langle X^\ell-\alpha\rangle$, where α is an arbitrary element of F_q^* (see [7, Corollary 3.5]).

Lemma 3.3. *([7, Corollary 3.5]) Let α be an arbitrary element of F_q^*. If ℓ is a positive integer coprime to $q-1$, then there exists a unique element $\lambda\in F_q^*$ such that $\lambda^\ell\alpha=1$. Furthermore, we have the following F_q-algebra isomorphism:*

$$\varphi:\quad F_q[X]/\langle X^\ell-1\rangle\ \longrightarrow\ F_q[X]/\langle X^\ell-\alpha\rangle,$$

which maps any element $f(X)+\langle X^\ell-1\rangle$ of $F_q[X]/\langle X^\ell-1\rangle$ to the element $f(\lambda X)+\langle X^\ell-\alpha\rangle$ of $F_q[X]/\langle X^\ell-\alpha\rangle$.

Combining Lemma 3.2 with Lemma 3.3, we have the following lemma.

Lemma 3.4. *Let $\mu = \xi^{\frac{q-1}{t}}$ be a primitive t-th root of unity. Assume that $\mathrm{ord}_{tp^n}(q) = \phi(p^n)$. Then for each $0 \leq j \leq t-1$, there exists a unique element $\lambda_j \in F_q^*$ such that $\lambda_j^{p^n}\mu^j = 1$. Furthermore, we have the following F_q-algebra isomorphism:*

$$\hat{\rho}_j : \quad F_q[X]/\langle X^{p^n}-1\rangle \longrightarrow F_q[X]/\langle X^{p^n}-\mu^j\rangle,$$

which maps any element $f(X)+\langle X^{p^n}-1\rangle$ of $F_q[X]/\langle X^{p^n}-1\rangle$ to the element $f(\lambda_j X)+\langle X^{p^n}-\mu^j\rangle$ of $F_q[X]/\langle X^{p^n}-\mu^j\rangle$.

Suppose $C_m = \langle a\rangle$ is a cyclic group of order m. Assume further that $\gcd(m,q) = 1$. It is well known that F_qC_m can be identified with the quotient algebra $F_q[X]/\langle X^m-1\rangle$ via the F_q-algebra isomorphism given by $a \mapsto X$. We know that the number of the irreducible characters of C_m over F_q and the number of the irreducible factors of X^m-1 in $F_q[X]$ coincide. Moreover, every degree of the irreducible character of C_m over F_q is exactly one degree of the irreducible factor of X^m-1 in $F_q[X]$. Indeed, let $X^m-1 = \prod_{i=1}^r f_i(X)$ be the monic irreducible factorization over F_q ($f_i(X)$ are pairwise distinct monic irreducible polynomials, $1 \leq i \leq r$). By the ring-theoretic version of the Chinese Remainder Theorem, F_qC_m is isomorphic to $F_q[X]/\langle f_1(X)\rangle \times \cdots \times F_q[X]/\langle f_r(X)\rangle$ as F_q-algebras. Note that $V_j = F_q[X]/\langle f_j(X)\rangle$ are finite fields, $1 \leq j \leq r$. In fact, it is easy to see that V_j are irreducible F_qC_m-modules by using [21, Lemma 1.3.2(b)]. This gives that the degree of the irreducible character afforded by V_j is equal to $\dim_{F_q} V_j = \deg f_j(X)$. From Wedderburn's theorem (see [21, Theorem 1.5.5]), we know that $V_1, \cdots, V_r$ is a set of representatives of the isomorphism classes of irreducible F_qC_m-modules; in particular, the number of the irreducible characters of C_m over F_q is equal to r.

Next we give all the irreducible characters of C_{p^n} over F_q.

Lemma 3.5. *Let $C_{p^n} = \langle z\rangle$ be the cyclic group of order p^n. If $\mathrm{ord}_{p^n}(q) = \phi(p^n)$, then $F_qC_{p^n}$ has exactly n non-trivial irreducible characters $\chi_i^{(n)}$ for $1 \leq i \leq n$, which are given by*

$$\chi_i^{(n)}(g) = \begin{cases} -p^{i-1}, & g \in \langle z^{p^{i-1}}\rangle \setminus \langle z^{p^i}\rangle; \\ p^i - p^{i-1}, & g \in \langle z^{p^i}\rangle; \\ 0, & g \in \langle z\rangle \setminus \langle z^{p^{i-1}}\rangle. \end{cases}$$

Proof. We claim that $F_qC_{p^n}$ has exactly n non-trivial irreducible characters and they are of degree $\phi(p^i)$ for $1 \leq i \leq n$. Since $\mathrm{ord}_{p^n}(q) = \phi(p^n)$, we get $\mathrm{ord}_{p^i}(q) = \phi(p^i)$, for any $1 \leq i \leq n$. It follows that every p^i-th cyclotomic polynomial $\Phi_{p^i}(X)$ is irreducible over F_q (see [20, Theorem 2.45 and Theorem 2.47]). Thus

$$X^{p^n}-1 = \prod_{i=0}^{n} \Phi_{p^i}(X),$$

is the monic irreducible factorization of $X^{p^n}-1$ in $F_q[X]$. It is easy to see that $X^{p^n}-1$ has exactly n non-linear irreducible factors in $F_q[X]$, and they are of degree $\phi(p^i)$. Let $\chi_i^{(n)}$ be the irreducible character of C_{p^n} over F_q which is afforded by the irreducible module $F_q[X]/\langle\Phi_{p^i}(X)\rangle$. In the following, we first determine the irreducible character $\chi_1^{(n)}$.

Let $V = F_q[X]/\langle\Phi_p(X)\rangle$ with an ordered basis $v_1 = 1, v_2 = X, \cdots, v_{p-1} = X^{p-2}$, and let $GL(V)$ denote the group of all nonsingular F_q-linear transformations $V \to V$. The irreducible $F_qC_{p^n}$-module V corresponds an irreducible representation of C_{p^n} over F_q as follows:

$$\begin{array}{rccc} \mathfrak{X} : C_{p^n} & \longrightarrow & GL(V) \\ z & \mapsto & \sigma \end{array}$$

where $\sigma(v_1) = v_2, \sigma(v_2) = v_3, \cdots, \sigma(v_{p-2}) = v_{p-1}$ and $\sigma(v_{p-1}) = \sum_{\ell=1}^{p-1}(-v_\ell)$. It is easy to check that for any $1 \le b \le p-2$,

$$\sigma^b(v_1) = v_{b+1}, \cdots, \sigma^b(v_{p-b-1}) = v_{p-1},\ \sigma^b(v_{p-b}) = \sum_{\ell=1}^{p-1}(-v_\ell),\ \sigma^b(v_{p-b+j}) = v_j\,(1 \le j \le b-1),$$

$$\sigma^{p-1}(v_1) = \sum_{\ell=1}^{p-1}(-v_\ell), \quad \sigma^{p-1}(v_s) = v_{s-1}, \quad \text{for any } 2 \le s \le p-1,$$

and

$$\sigma^p(v) = v, \quad \text{for any } v \in V.$$

Hence

$$\chi_1^{(n)}(g) = \begin{cases} -1, & g \in C_{p^n} \setminus \langle z^p \rangle; \\ p-1, & g \in \langle z^p \rangle. \end{cases}$$

Now we prove the lemma by induction on n. The first step $n = 1$ is true, since C_p over F_q has only one non-trivial irreducible character, namely $\chi_1^{(1)}$. For the inductive step, let $C_{p^{n+1}} = \langle z \rangle$ denote the cyclic group of order p^{n+1} and $\chi_{reg}^{(n+1)}$ the regular character of $C_{p^{n+1}}$ over F_q. Then $C_{p^n} = \langle z^p \rangle$ is a cyclic subgroup of $C_{p^{n+1}}$ with order p^n. We see that

$$\chi_{reg}^{(n)} = \chi_0^{(n)} + \chi_1^{(n)} + \cdots + \chi_n^{(n)},$$

where $\chi_0^{(n)}$ is the trivial character of C_{p^n} over F_q; this is because $F_qC_{p^n} = \bigoplus_{i=0}^{n} F_q[X]/\langle \Phi_{p^i}(X) \rangle$ is a direct sum of irreducible $F_qC_{p^n}$-modules. Then we have

$$\chi_{reg}^{(n+1)} = Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_{reg}^{(n)}) = Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_0^{(n)}) + Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_1^{(n)}) + \cdots + Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_n^{(n)}). \tag{3.1}$$

On the other hand, we have

$$\chi_{reg}^{(n+1)} = \chi_0^{(n+1)} + \chi_1^{(n+1)} + \cdots + \chi_{n+1}^{(n+1)}, \tag{3.2}$$

where $\chi_0^{(n+1)}$ is the trivial character of $C_{p^{n+1}}$ over F_q. Note that the degree of $\chi_j^{(n+1)}$ is equal to $\phi(p^j)$, $0 \le j \le n+1$. On the other hand, $F_qC_{p^{n+1}} \bigotimes_{F_qC_{p^n}} F_q$ affords the character $Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_0^{(n)})$ which is of degree p; further, $F_qC_{p^{n+1}} \bigotimes_{F_qC_{p^n}} F_q$ is a direct sum of some irreducible $F_qC_{p^{n+1}}$-modules. This forces that $F_qC_{p^{n+1}} \bigotimes_{F_qC_{p^n}} F_q = F_q \bigoplus F_q/\langle \Phi_p(X) \rangle$ is the only possible solution. Therefore, $Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_0^{(n)}) = \chi_0^{(n+1)} + \chi_1^{(n+1)}$. Similar reasoning then shows that $Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_i^{(n)}) = \chi_{i+1}^{(n+1)}$, $1 \le i \le n$. In particular, $\chi_1^{(n+1)}$ and $Ind_{\langle z^p \rangle}^{\langle z \rangle}(\chi_i^{(n)})$ consist all the non-trivial irreducible characters of $C_{p^{n+1}}$ over F_q for all $1 \le i \le n$. Since $C_{p^n} = \langle z^p \rangle$ is a cyclic subgroup of $C_{p^{n+1}}$ with order p^n, by the inductive hypothesis we get that

$$\chi_i^{(n)}(g) = \begin{cases} -p^{i-1}, & g \in \langle z^{p^i} \rangle \setminus \langle z^{p^{i+1}} \rangle; \\ p^i - p^{i-1}, & g \in \langle z^{p^{i+1}} \rangle; \\ 0, & g \in C_{p^n} \setminus \langle z^{p^i} \rangle. \end{cases}$$

Hence,

$$\chi_{i+1}^{(n+1)}(g) = Ind_{\langle z^{p^i}\rangle}^{\langle z\rangle}(\chi_i^{(n)})(g) = \begin{cases} -p^i, & g \in \langle z^{p^i}\rangle \setminus \langle z^{p^{i+1}}\rangle; \\ p^{i+1} - p^i, & g \in \langle z^{p^{i+1}}\rangle; \\ 0, & g \in C_{p^{n+1}} \setminus \langle z^{p^i}\rangle. \end{cases}$$

□

Let $C_{tp^n} = \langle x\rangle$ be a cyclic group of order tp^n. Since $\gcd(t,p) = 1$, we have $C_{tp^n} = \langle x\rangle = \langle x^t\rangle \times \langle x^{p^n}\rangle$. Here $\langle x^t\rangle$ is a cyclic subgroup of order p^n and $\langle x^{p^n}\rangle$ is a cyclic subgroup of order t. We know that every element in C_{tp^n} has a unique expression as gx^{sp^n}, where $g \in \langle x^t\rangle$ and $0 \le s \le t-1$. In the following lemma, we obtain all the irreducible characters of C_{tp^n} over F_q.

Lemma 3.6. *Let $C_{tp^n} = \langle x\rangle$ be the cyclic group of order tp^n. If $\mathrm{ord}_{tp^n}(q) = \phi(p^n)$, then $F_qC_{tp^n}$ has $t(n+1)$ irreducible characters given by*

$$\psi_j^{(i)}(gx^{sp^n}) = \begin{cases} -\mu^{sj}p^{i-1}, & g \in \langle x^{tp^{i-1}}\rangle \setminus \langle x^{tp^i}\rangle; \\ \mu^{sj}(p^i - p^{i-1}), & g \in \langle x^{tp^i}\rangle; \\ 0, & g \in \langle x^t\rangle \setminus \langle x^{tp^{i-1}}\rangle, \end{cases}$$

and

$$\psi_j^{(0)}(gx^{sp^n}) = \mu^{sj}, \text{ for all } g \in \langle x^t\rangle,$$

where $\mu = \xi^{\frac{q-1}{t}}$ is a primitive t-th root of unity, $1 \le i \le n$ and $0 \le j, s \le t-1$.

Proof. We prove that $F_qC_{tp^n}$ has $t(n+1)$ primitive idempotents by showing that $X^{tp^n} - 1$ has $t(n+1)$ irreducible factors in $F_q[X]$. We take $\mu = \xi^{\frac{q-1}{t}}$, then μ is a primitive t-th root of unity in F_q. Hence,

$$X^t - 1 = (X-1)(X-\mu)\cdots(X-\mu^{t-1}),$$

and

$$X^{tp^n} - 1 = (X^{p^n} - 1)(X^{p^n} - \mu)\cdots(X^{p^n} - \mu^{t-1}).$$

We claim that each factor $X^{p^n} - \mu^j$ has $n+1$ irreducible factors in $F_q[X]$ for $0 \le j \le t-1$. By Lemma 3.4, we recall the following F_q-algebra isomorphism:

$$\hat{\rho}_j : \quad F_q[X]/\langle X^{p^n} - 1\rangle \longrightarrow F_q[X]/\langle X^{p^n} - \mu^j\rangle,$$

which maps any element $f(X) + \langle X^{p^n} - 1\rangle$ of $F_q[X]/\langle X^{p^n} - 1\rangle$ to the element $f(\lambda_j X) + \langle X^{p^n} - \mu^j\rangle$ of $F_q[X]/\langle X^{p^n} - \mu^j\rangle$. Since

$$X^{p^n} - 1 = \prod_{i=0}^{n} \Phi_{p^i}(X),$$

is the irreducible factorization of $X^{p^n} - 1$ in $F_q[X]$, then

$$X^{p^n} - \mu^j = \mu^j \prod_{i=0}^{n} \Phi_{p^i}(\lambda_j X),$$

is the irreducible factorization of $X^{p^n} - \mu^j$ in $F_q[X]$. It follows that $X^{tp^n} - 1$ has $t(n+1)$ irreducible factors in $F_q[X]$.

On the other hand, all the irreducible representations of $\langle x^{p^n}\rangle$ over F_q are of degree one. Thus $\langle x^{p^n}\rangle$ has t irreducible characters over F_q, and the irreducible characters θ_j of $\langle x^{p^n}\rangle$ are given by

$$\theta_j(x^{sp^n}) = \mu^{sj},\ 0 \le s, j \le t-1.$$

We get our desired result by Lemma 3.5. □

Now we are ready to compute the primitive idempotents of $F_q[X]/\langle X^{tp^n}-1\rangle$.

Theorem 3.7. *Let $C_{tp^n} = \langle x\rangle$ be the cyclic group of order tp^n. If $\mathrm{ord}_{tp^n}(q) = \phi(p^n)$, then the group algebra $F_qC_{tp^n}$ has $t(n+1)$ primitive idempotents given as follows:*

$$E_j^{(i)}(x) = \frac{1}{t}e_i(\lambda_j x)\sum_{s=0}^{t-1}\mu^{-js}x^{sp^n}, \qquad 0 \le i \le n,\ 0 \le j \le t-1, \tag{3.3}$$

where λ_j was stated in Lemma 3.4,

$$e_0(x) = \frac{1}{p^n}\sum_{i=0}^{p^n-1} x^i$$

and

$$e_i(x) = \frac{1}{p^{n-i}}\sum_{j=0}^{p^{n-i}-1} X^{p^i j} - \frac{1}{p^{n-i+1}}\sum_{j=0}^{p^{n-i+1}-1} X^{p^{i-1}j}, \quad \textit{for } 1 \le i \le n.$$

Proof. We first note that $\langle x^{tp^{i-1}}\rangle \times \langle x^{p^n}\rangle = \langle x^{p^{i-1}}\rangle$ for each $1 \le i \le n$. From Lemma 3.6, the irreducible character $\psi_j^{(i)}$ vanishs on $\langle x\rangle \setminus \langle x^{p^{i-1}}\rangle$ for every $1 \le i \le n$ and $0 \le j \le t-1$. Let $E_j^{(i)}(x)$ be the primitive idempotent of $F_qC_{tp^n}$, which corresponds to the irreducible character $\psi_j^{(i)}$. Since $\gcd(t,p) = 1$, then there are two integers ℓ, m such that $t\ell + mp^{n-i+1} = 1$. Hence, $\lambda_j^{p^{i-1}} = \lambda_j^{p^{i-1}t\ell}\cdot\lambda_j^{mp^n} = \mu^{-mj}$, where λ_j was stated in Lemma 3.4 satisfying $\lambda_j^{p^n}\mu^j = 1$. On the other hand, each element in $\langle x^{p^{i-1}}\rangle$ can be written uniquely as $x^{rp^{i-1}}\cdot x^{sp^n}$, where $0 \le r \le p^{n-i+1}-1$ and $0 \le s \le t-1$. We have

$$\psi_j^{(i)}(x^{-rp^{i-1}}) = \psi_j^{(i)}(x^{-tp^{i-1}r\ell}\cdot x^{-p^n rm}) = -p^{i-1}\mu^{-rmj} = -p^{i-1}\lambda_j^{rp^{i-1}}.$$

By Lemma 2.1 and Lemma 3.6, we deduce that

$$\begin{aligned}
E_j^{(i)}(x) &= \frac{1}{tp^n}\sum_{g\in\langle x^{p^{i-1}}\rangle}\psi_j^{(i)}(g^{-1})g \\
&= \frac{1}{tp^n}\sum_{s=0}^{t-1}\mu^{-js}X^{sp^n}\Big(-p^{i-1}\big(1+(\lambda_j x)^{p^{i-1}}+\cdots+(\lambda_j x)^{(p^{n-i+1}-1)p^{i-1}}\big) \\
&\qquad + p^i\big(1+(\lambda_j x)^{p^i}+\cdots+(\lambda_j x)^{(p^{n-i}-1)p^i}\big)\Big) \\
&= \frac{1}{t}e_i(\lambda_j x)\sum_{s=0}^{t-1}\mu^{-js}x^{sp^n}.
\end{aligned}$$

Finally, let $E_j^{(0)}(x)$ be the primitive idempotent of $F_qC_{tp^n}$ corresponding to $\psi_j^{(0)}$, for $0 \le j \le t-1$. We note that each element in $\langle x \rangle$ can be written uniquely as $x^r \cdot x^{sp^n}$, $0 \le r \le p^n - 1$ and $0 \le s \le t-1$. Then, taking arguments similar to the previous paragraph, we get that

$$E_j^{(0)}(x) = \frac{1}{t} e_0(\lambda_j x) \sum_{s=0}^{t-1} \mu^{-js} x^{sp^n},$$

where $0 \le j \le t-1$.

□

Taking $t = 1$ in Theorem 3.7, we can get the main result in [24, Theorem 3.5] directly.

Corollary 3.8. *If* $\mathrm{ord}_{p^n}(q) = \phi(p^n)$*, then the quotient algebra* $F_q[X]/\langle X^{p^n} - 1\rangle$ *has* $n+1$ *primitive idempotents given by* $e_i(X)$*, where* $0 \le i \le n$ *and* $e_i(X)$ *was stated in Theorem 3.7.*

Taking $t = 2$ in Theorem 3.7, we can easily obtain the main result in [1, Theorem 2.6], as stated below in our notation.

Corollary 3.9. *If* $\gcd(q, 2p) = 1$ *and* $\mathrm{ord}_{2p^n}(q) = \phi(p^n)$*, then the quotient algebra* $F_q[X]/\langle X^{2p^n} - 1\rangle$ *has* $2(n+1)$ *primitive idempotents given by* $\frac{1}{2}(1 + X^{p^n})e_i(X)$ *and* $\frac{1}{2}(1 - X^{p^n})e_i(-X)$*, where* $0 \le i \le n$ *and* $e_i(X)$ *was stated in Theorem 3.7.*

Proof. We just note that μ is a primitive 2nd root of unity in F_q, i.e. $\mu = -1$, $\lambda_1 = 1$ and $\lambda_2 = -1$ as in Theorem 3.7. □

4 Minimal cyclic codes of length tp^n

Arora and Pruthi [24] determined the parameters of all the minimal cyclic codes of length p^n over F_q with $\mathrm{ord}_{p^n}(q) = \phi(p^n)$. It was showed that, except for one minimal cyclic code with parameters $[p^n, 1, p^n]$, the others have parameters $[p^n, \phi(p^i), 2p^{n-i}]$, $1 \le i \le n$. In [1], the authors considered minimal cyclic codes of length $2p^n$ over F_q with $\mathrm{ord}_{2p^n}(q) = \phi(p^n)$. It turns out that except for two minimal cyclic code with parameters $[2p^n, 1, 2p^n]$, the others have parameters $[2p^n, \phi(p^i), 4p^{n-i}]$, $1 \le i \le n$.

In this section, we extend these results to minimal cyclic codes of length tp^n, where $t \mid (q-1)$, $\gcd(p, t) = 1$ and $\mathrm{ord}_{tp^n}(q) = \phi(p^n)$. We have the following theorem.

Theorem 4.1. *Let* $\bar{E}_j^{(i)}(X)$ *be the minimal cyclic codes generated by the primitive idempotents* $E_j^{(i)}(X)$*, which is given in Theorem 3.7 for* $0 \le i \le n$ *and* $0 \le j \le t-1$*. Then*

(i) $\bar{E}_j^{(0)}(X)$ *has parameters* $[tp^n, 1, tp^n]$*, and its check polynomial is* $\lambda_j X - 1$*, for each* $0 \le j \le t-1$;

(ii) $\bar{E}_j^{(i)}(X)$ *has parameters* $[tp^n, \phi(p^i), 2tp^{n-i}]$*, and its check polynomial is* $\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}}$ *for each* $0 \le j \le t-1$ *and* $1 \le i \le n$.

Proof. (i) We first show that the check polynomial of $\bar{E}_j^{(0)}(X)$ is $\lambda_j X - 1$ for $0 \le j \le t-1$. It suffices to prove that the root of $\lambda_j X - 1$ does not satisfy $E_j^{(0)}(X)$. Obviously, λ_j^{-1} is the only

root of $\lambda_j X - 1$. Since $e_0(X) = \frac{1}{p^n} \sum_{i=0}^{p^n-1} X^i$ and $\lambda_j^{p^n} \mu^j = 1$, then

$$E_j^{(0)}(\lambda_j^{-1}) = \frac{1}{t} e_0(1) \sum_{s=0}^{t-1} \mu^{-js} \lambda_j^{-sp^n} = e_0(1) = 1 \neq 0.$$

Now we determine the minimum Hamming distance of $\bar{E}_j^{(0)}(X)$. Recall that

$$E_j^{(0)}(X) = \frac{1}{t} e_0(\lambda_j X) \sum_{s=0}^{t-1} \mu^{-js} X^{sp^n},$$

and the degree of $e_0(\lambda_j X)$ is less than p^n. Clearly, the Hamming distance of $\bar{E}_j^{(0)}(X)$ is tp^n. This completes the proof of (i).

(ii) For $1 \leq i \leq n$, observe that

$$\begin{aligned} X^{tp^n} - 1 &= (\mu^{-j} X^{p^n} - 1)\Big(\sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \Big) \\ &= (\lambda_j^{p^n} X^{p^n} - 1)\Big(\sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \Big) \\ &= (\lambda_j^{p^{i-1}} X^{p^{i-1}} - 1)\Big(\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}} \Big)\Big(\sum_{\ell=0}^{p^{n-i}-1} (\lambda_j X)^{\ell p^i} \Big)\Big(\sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \Big). \end{aligned}$$

By Theorem 3.7, we have

$$E_j^{(i)}(X) = \frac{1}{t} e_i(\lambda_j x) \sum_{s=0}^{t-1} \mu^{-js} x^{sp^n} \quad \text{for each } 1 \leq i \leq n \text{ and } 0 \leq j \leq t-1,$$

where

$$e_i(x) = \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i}-1} X^{p^i j} - \frac{1}{p^{n-i+1}} \sum_{j=0}^{p^{n-i+1}-1} X^{p^{i-1} j}, \quad \text{for } 1 \leq i \leq n.$$

We claim that the check polynomial of $\bar{E}_j^{(i)}(X)$ is $\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}}$. Since $\mathrm{ord}_{p^i}(q) = \phi(p^i)$, then $\sum_{\ell=0}^{p-1} X^{\ell p^{i-1}}$ is irreducible over F_q. Using the algebra isomorphism $\hat{\rho}_j$ presented in Lemma 3.4, we get that $\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}}$ is an irreducible divisor of $X^{tp^n} - 1$. It remains to prove that the roots of $\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}}$ do not satisfy $E_j^{(i)}(X)$. Obviously the roots of $\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}}$ are $\lambda_j^{-1}\delta$, where δ ranges over the primitive p^i-th roots of unity in some extension field of F_q.

$$E_j^{(i)}(\lambda_j^{-1}\delta) = \frac{1}{t} e_i(\delta) \sum_{s=0}^{t-1} \mu^{-js} (\lambda_j^{-1}\delta)^{sp^n} = e_i(\delta) = 1 - 0 = 1 \neq 0.$$

Hence, the check polynomial of $\bar{E}_j^{(i)}(X)$ is $\sum_{\ell=0}^{p-1}(\lambda_j X)^{\ell p^{i-1}}$ and the generating polynomial is

$$g_j^{(i)}(X) = (\lambda_j^{p^{i-1}} X^{p^{i-1}} - 1)\Big(\sum_{\ell=0}^{p^{n-i}-1}(\lambda_j X)^{\ell p^i}\Big)\Big(\sum_{s=0}^{t-1}\mu^{-js}X^{sp^n}\Big).$$

We are left to compute the minimum Hamming distance of $\bar{E}_j^{(i)}(X)$. Obviously, $w_H(g_j^{(i)}(X)) \le 2tp^{n-i}$, which implies $d_H(\bar{E}_j^{(i)}(X)) \le 2tp^{n-i}$. For the inverse inequality, let $\bar{c}(X)$ be an arbitrary nonzero element in $\bar{E}_j^{(i)}(X)$ and we assume that $\bar{c}(X) = c(X)\cdot g_j^{(i)}(X) + \langle X^{tp^n}-1\rangle$. We have $c(X) = q(X)\sum_{\ell=0}^{p-1}(\lambda_j X)^{\ell p^{i-1}} + r(X)$, where $q(X)$ and $r(X)$ are polynomials in $F_q[X]$ with $\deg r(X) < \phi(p^i)$. Since $\sum_{\ell=0}^{p-1}(\lambda_j X)^{\ell p^{i-1}}\cdot g_j^{(i)}(X) = 0$ in $F_q[X]/\langle X^{tp^n}-1\rangle$, we get

$$\bar{c}(X) = c(X)\cdot g_j^{(i)}(X) = \big((q(X)\sum_{\ell=0}^{p-1}(\lambda_j X)^{\ell p^{i-1}} + r(X)\big)\cdot g_j^{(i)}(X) = r(X)\cdot g_j^{(i)}(X).$$

To prove $d_H(\bar{E}_j^{(i)}(X)) \ge 2tp^{n-i}$, it suffices to show that $d_H(r(X)\cdot g_j^{(i)}(X)) \ge 2tp^{n-i}$ for any nonzero polynomial $r(X)\in F_q[X]$ with $\deg r(X) < \phi(p^i)$. Observe that $\deg(r(X)g_j^{(i)}(X)) < tp^n$, which implies that $d_H(r(X)\cdot g_j^{(i)}(X))$ is equal to the number of nonzero coefficients occurring in the expansion of $r(X)\cdot g_j^{(i)}(X)$. If $w_H(r(X)) = 1$, then $w_H(r(X)(\lambda_j^{p^{i-1}}X^{p^{i-1}}-1)) = 2$. If $w_H(r(X)) \ge 2$, it is easy to see that $w_H(r(X)(\lambda_j^{p^{i-1}}X^{p^{i-1}}-1)) \ge 2$. Suppose $r(X)(\lambda_j^{p^{i-1}}X^{p^{i-1}} - 1) = a_uX^u + a_{u+1}X^{u+1} + \cdots + a_{u+v}X^{u+v}$ ($u\ge 0, v>0$ and $u+v<p^i$) with a_u, a_{u+v} being nonzero elements of F_q. After expanding $r(X)(\lambda_j^{p^{i-1}}X^{p^{i-1}}-1)(\sum_{\ell=0}^{p^{n-i}-1}(\lambda_j X)^{\ell p^i})$, it is easy to see that

$$w_H(r(X)(\lambda_j^{p^{i-1}}X^{p^{i-1}}-1)(\sum_{\ell=0}^{p^{n-i}-1}(\lambda_j X)^{\ell p^i})) = w_H\big(r(X)(\lambda_j^{p^{i-1}}X^{p^{i-1}}-1)\big)w_H(\sum_{\ell=0}^{p^{n-i}-1}(\lambda_j X)^{\ell p^i}) \ge 2p^{n-i}.$$

With a similar argument, we obtain $w_H(r(X)g_j^{(i)}(X)) \ge 2tp^{n-i}$, which gives the desired result. □

We now give an illustrative example.

Example 4.2. *Take $q=13, p=5, n=2$ and $t=3$. Let ξ be a primitive 12th root of unity in F_{13}. It is easy to check that* $\mathrm{ord}_{75}(13) = 20 = \phi(5^2)$. *It follow from Lemma 3.4 that $\mu = \xi^4$, and so $\lambda_0 = 1$, $\lambda_1 = \xi^8$ and $\lambda_2 = \xi^4$. By Theorem 3.7, the semisimple algebra $F_{13}[X]/\langle X^{75}-1\rangle$ has exactly 9 primitive idempotents, and $e_1(X) = \frac{1}{5}\sum_{h=0}^{4}X^{5h} - \frac{1}{25}\sum_{h=0}^{24}X^h$, $e_2(X) = 1 - \frac{1}{5}\sum_{h=0}^{4}X^{5h}$. The minimal cyclic codes are given in Table 1.*

Table 1

Code	checking polynomial	primitive idempotent	parameters
$\bar{E}_0^{(0)}(X)$	$X-1$	$\frac{1}{3}e_0(X)\sum_{s=0}^{2}X^{25s}$	$[75,1,75]$
$\bar{E}_1^{(0)}(X)$	$\lambda_1 X-1$	$\frac{1}{3}e_0(\lambda_1 X)\sum_{s=0}^{2}\mu^{-s}X^{25s}$	$[75,1,75]$
$\bar{E}_2^{(0)}(X)$	$\lambda_2 X-1$	$\frac{1}{3}e_0(\lambda_2 X)\sum_{s=0}^{2}\mu^{-2s}X^{25s}$	$[75,1,75]$
$\bar{E}_0^{(1)}(X)$	$\sum_{j=0}^{4}X^j$	$\frac{1}{3}e_1(X)\sum_{s=0}^{2}X^{25s}$	$[75,4,30]$
$\bar{E}_1^{(1)}(X)$	$\sum_{j=0}^{4}(\lambda_1 X)^j$	$\frac{1}{3}e_1(\lambda_1 X)\sum_{s=0}^{2}\mu^{-s}X^{25s}$	$[75,4,30]$
$\bar{E}_2^{(1)}(X)$	$\sum_{j=0}^{4}(\lambda_2 X)^j$	$\frac{1}{3}e_1(\lambda_2 X)\sum_{s=0}^{2}\mu^{-2s}X^{25s}$	$[75,4,30]$
$\bar{E}_0^{(2)}(X)$	$\sum_{j=0}^{4}X^{5j}$	$\frac{1}{3}e_2(X)\sum_{s=0}^{2}X^{25s}$	$[75,20,6]$
$\bar{E}_1^{(2)}(X)$	$\sum_{j=0}^{4}(\lambda_1 X)^{5j}$	$\frac{1}{3}e_2(X)\sum_{s=0}^{2}\mu^{-s}X^{25s}$	$[75,20,6]$
$\bar{E}_2^{(2)}(X)$	$\sum_{j=0}^{4}(\lambda_2 X)^{5j}$	$\frac{1}{3}e_2(\lambda_1 X)\sum_{s=0}^{2}\mu^{-2s}X^{25s}$	$[75,20,6]$

Acknowledgements

The authors would like to thank the anonymous referees for their many helpful comments. The authors are supported by NSFC, Grant No. 11171370. The third author is also supported by the Youth Backbone Teacher Foundation of Henan's Universities (Grant No. 2013GGJS-152) and Science and Technology Development Program of Henan Province in 2014 (144300510051).

References

[1] S. K. Arora, M. Pruthi, Minimal cyclic codes of length $2p^n$, Finite Fields Appl., **5**(1999), 177-187.

[2] S. K. Arora, S. Batra, S. D. Cohen, M. Pruthi, The primitive idempotents of a cyclic group algebra, Southeast Asian Bull. Math., **26**(2002), 197-208.

[3] G. K. Bakshi, M. Raka, Minimal Cyclic Codes of length $p^n q$, Finite Fields Appl., **9**(2003), 432-438.

[4] S. Batra, S. K. Arora, Minimal quadratic residue cyclic codes of length p^n (p odd). J. Appl.Math. Comput., (Old: KJCAM), **3**(2001), 531-547.

[5] S. Batra, S. K. Arora, Some cyclic codes of length $2p^n$, Designs Codes Cryptogr., **61**(2011), 41-69.

[6] S. D. Berman, Semisimple cyclic and abelian code, II, Cybernatics **3**(1967), 17-23.

[7] B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic codes over finite fields, Finite Fields Appl., **18**(2012), 1217-1231.

[8] B. Chen, H. Liu, G. Zhang, A class of minimal cyclic codes over finite fields, Designs Codes Cryptogr., (2013), DOI: 10.1007/s10623-013-9857-9.

[9] B. Chen, L. Li, R. Tuerhong, Explicit factorization of $X^{2^m p^n}-1$ over a finite field, Finite Fields Appl., **24**(2013), 95-104.

[10] H. Q. Dinh, S. R. López-Permouth, Cyclic and negacyclic codes over finite chain rings, IEEE Trans. Inform. Theory **50**(2004), 1728-1744.

[11] H. Q. Dinh, Constacyclic codes of length p^s over $F_{p^m}+uF_{p^m}$, J. Algebra, **324**(2010), 940-950.

[12] H. Q. Dinh, Repeated-root constacyclic codes of length $2p^s$, Finite Fields Appl. **18**(2012) 133-143.

[13] H. Q. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, Discrete Math., **313**(2013), 983-991.

[14] S. T. Dougherty, S. Ling, Cyclic codes over Z_4 of even length, Des. Codes Cryptogr., **39**(2006), 127-153.

[15] L. Dornhoff, Group representation theory part A, Dekker, New York, 1971.

[16] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.

[17] Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, IEEE Trans. Inform. Theory **57**(2011), 2243-2251.

[18] X. Kai, S. Zhu, On cyclic self-dual codes, Appl. Algebra Engrg. Comm. Comput., **19**(2008), 509-525.

[19] G. Karpilovsky, Group Representations Volume 1, Part B: Introduction to Group Representations and Characters, North-Holland-Amsterdam, New York, 1992.

[20] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 2008.

[21] K. Lux, H. Pahlings, Representations of Groups: A Computational Approach, Cambridge University Press, Cambridge, 2010.

[22] F. J. MacWilliams, N. J. A. Sloane, The theory of error correcting codes. NorthHolland, Amsterdam (1977).

[23] V. Pless, Z. Qian, Cyclic codes and quadratic residue codes over Z_4, IEEE Trans. Inform. Theory, **42**(1996), 1594-1600.

[24] M. Pruthi, S. K. Arora, Minimal codes of prime-power length, Finite Fields Appl., **3**(1997), 99-113.

[25] A. Sahni, P. T. Sehgal, Minimal cyclic codes of length p^nq, Finite Fields Appl., **18**(2012), 1017-1036.

[26] A. Sharma, G. K. Bakshi, V. C. Dumir, M. Raka, Cyclotomic numbers and primitive idempotents in the ring $GF(q)[X]/\langle X^{p^n}-1\rangle$, Finite Fields Appl., **10**(2004), 653-673.

[27] A. Sharma, G. K. Bakshi, M. Raka, Irreducible cyclic codes of length $2p^n$, Ars Combin., **83**(2007), 267-278.

[28] J. H. Van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory, **37**(1991), 343-345.

[29] A. J. van Zanten, A. Bojilov, S. M. Dodunekov, Generalized residue and t-residue codes and their idempotent generators, Designs Codes Cryptogr., (2014), DOI: 10.1007/s10623-013-9905-5.