<table>
<thead>
<tr>
<th>Title</th>
<th>Some minimal cyclic codes over finite fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Bocong, Chen; Hongwei, Liu; Guanghui, Zhang</td>
</tr>
<tr>
<td>Date</td>
<td>2014</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/20361">http://hdl.handle.net/10220/20361</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2014 Elsevier. This is the author created version of a work that has been peer reviewed and accepted for publication by Discrete Mathematics, Elsevier. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<a href="http://dx.doi.org/10.1016/j.disc.2014.05.007">http://dx.doi.org/10.1016/j.disc.2014.05.007</a>].</td>
</tr>
</tbody>
</table>
Some Minimal Cyclic Codes over Finite Fields *

Bocong Chen¹, Hongwei Liu², Guanghui Zhang³

¹Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang
Technological University, Singapore 637616, Singapore
²School of Mathematics and Statistics, Central China Normal University,
Wuhan, Hubei, 430079, China
³School 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 $\text{ord}_{tp^n}(q) = \phi(p^n)$. 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 $F_{p^m} + u F_{p^m}$, 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 $F_q[X]/(X^n - 1) \cong F_q C_n$, where $F_q C_n$ 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 $F_q C_n$. Suppose $\zeta$ is a primitive $n$-th root of unity in some extension field of $F_q$ and $F_q(\zeta)$. Further assume that all the distinct $q$-cyclotomic cosets modulo $n$ are given by $\Gamma_0, \Gamma_1, \ldots, \Gamma_{r-1}$. Then $F_q C_n$ has exactly $n$ primitive idempotents given by $e_{\chi_i} = \frac{1}{n} \sum_{j=0}^{n-1} \zeta^{-ji} g^j$, $0 \leq i \leq n - 1$.

Moreover, $F_q C_n$ has exactly $r$ primitive idempotents given by $e_{\Gamma_{t1}} = \sum_{j \in \Gamma_{t1}} e_{\chi_j}$, $0 \leq t \leq r - 1$.

Determining the number of nonzero coefficients appearing in the primitive idempotent $e_{\Gamma_{t1}}$, 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 $p^s$ and $2p^s$ over $F_q$ were investigated in [4] and [5] sequentially where $q$ has order $\frac{\phi(p^s)}{2}$ in the cyclic group $\mathbb{Z}_{p^s}$, i.e. $\text{ord}_{p^s}(q) = \frac{\phi(p^s)}{2}$. The minimal cyclic codes of length $p^n$ and $2p^n$ with $\text{ord}_{p^n}(q) = f$ and $\gcd(\frac{f+1}{2}, q) = 1$ were considered in [26] and [27] respectively. We have studied minimal cyclic codes of length $\ell m$ over $F_q$, where $\ell$ 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 $F_q C_{p^m}$ 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 $\text{ord}_{2p^n}(q) = \phi(p^n)$ were considered, where $p$ is an odd prime different from the characteristic of $F_q$. The expressions for the primitive idempotents of $F_q[X]/(X^{2p^n} - 1)$ were given
Let $t$ and $n$ be positive integers with $t \mid (q - 1)$, $\gcd(t, p) = 1$ and $\text{ord}_{tp^n}(q) = \phi(p^n)$. 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 $F_q[X]/(X^{tp^n} - 1)$; that is, we obtain the primitive idempotents of $F_q[X]/(X^{tp^n} - 1)$ 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 $[tp^n, \phi(p^t), 2tp^n-1]$, $1 \leq i \leq n$.

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 $F_q[X]/(X^{tp^n} - 1)$ 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 $\beta$ in $F_q^*$, let $\text{ord}(\beta)$ be the order of $\beta$ in the group $F_q^*$, and $\beta$ is called a primitive $\text{ord}(\beta)$-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 $\xi$ is a primitive $(q - 1)$-th root of unity.

Let $\mathbb{Z}_n^*$ be the multiplicative group of all residue classes mod $n$ which are coprime to $n$ and let $\text{ord}_n(r)$ denote the order of the residue $\bar{r}$ in the group $\mathbb{Z}_n^*$. 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 $\Phi_n(X) = \prod_{\zeta \text{ a } n\text{-th root of unity}} (X - \zeta)$, where $\zeta$ 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 $\text{ord}_n(q) = \phi(n)$ (see [20, Theorem 2.45 and Theorem 2.47]).

Any element of the quotient algebra $F_q[X]/(X^n - 1)$ 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 $a = (a_0, a_1, \cdots, a_{n-1})$ of length $n$ over $F_q$. Thus, we can define the corresponding Hamming weight and the Hamming distance on the quotient algebra $F_q[X]/(X^n - 1)$, namely we define $w_H(a(X)) = w_H(a)$ and $d_H(a(X), b(X)) = w_H(a - b)$, 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 $F_q[X]/(X^n - 1)$, 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 $F_q[X]/(X^n - 1)$.

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 $F_qG = \{\sum_{g \in G} a_g g \mid a_g \in F_q\}$ 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 $\chi_0$ defined by $\chi_0(g) = 1$ for all $g \in G$; the other characters of $G$ are called non-trivial. For a character $\chi$ afforded by an $F_qG$-module $V$, $\dim_{F_q} V$ is called the degree of $\chi$.

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 $g \mapsto [g]_B$ obtained by taking $B = \{g \mid g \in G\}$ to be the natural basis of $F_qG$ is called the regular representation of $G$ over $F_q$, where $[g]_B$ denotes the matrix of $g$ as an $F_qG$-linear transformation of $F_qG$ relative to the basis $B$. The regular character $\chi_{\text{reg}}$ 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 $\bigoplus_{i=1}^r (n_i L_i)$ as $F_qG$-module, where $n_i$ are positive integers; in the language of character theory, we see that $\chi_{\text{reg}} = \sum_{i=1}^r n_i \chi_i$, where the $\chi_i$ are the irreducible characters afforded by $L_i$, $1 \leq i \leq r$.

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 $W^G = F_qG \otimes_{F_qH} W$ is a left $F_qG$-module, called the module induced from $W$. Let $\chi$ be a character of $H$ afforded by $W$, and let $\text{Ind}_H^G(\chi)$ be the induced character of $\chi$ afforded by the left $F_qG$-module $W^G$. We then know (e.g. see [15, Lemma 9.2]) that $\text{Ind}_H^G(\chi)$ satisfies $\text{Ind}_H^G(\chi)(g) = 1/|H| \sum_{a \in G} \chi(ay^{-1}g)$, where $\chi(g) = \chi(g)$ if $g \in H$; otherwise, $\chi(g) = 0$. In particular, $\text{Ind}_H^G(\chi)(1) = |G|/|H| \chi(1)$.

It is true that if $\chi_{\text{reg}}$ is the regular character of $H$ over $F_q$, then $\text{Ind}_H^G(\chi_{\text{reg}})$ is the regular character of $G$ over $F_q$; if $\chi_1$ and $\chi_2$ are characters of $H$, then $\text{Ind}_H^G(\chi_1 + \chi_2) = \text{Ind}_H^G(\chi_1) + \text{Ind}_H^G(\chi_2)$ (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

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

### 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 $t \mid (q - 1)$.

As mentioned in Section 1, the primitive idempotents of the semisimple algebras $F_q[X]/(X^{p^n} - 1)$ and $F_q[X]/(X^{3p^n} - 1)$ were explicitly characterized in [24] and in [1] respectively, when $q$ has order $\phi(p^n)$ in the cyclic group $\mathbb{Z}_{p^n}$. In this section, we extend these results to a more general setting; that is, we obtain the primitive idempotents of $F_q[X]/(X^{tp^n} - 1)$ with $\ord_{tp^n}(q) = \phi(p^n)$.

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

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

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

$$\theta : \mathbb{Z}_{tp^n}^* \rightarrow \mathbb{Z}_t^* \times \mathbb{Z}_{p^n}^*, \quad m \mod tp^n \mapsto \left( m \mod t, m \mod p^n \right).$$

It follows that

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

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

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

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

$$(q \mod t, q \mod p^n) = (1 \mod t, q \mod p^n).$$

Then we obtain the desired result by the isomorphism $\theta$. $\square$

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

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

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

**Lemma 3.3.** ( [7, Corollary 3.5] ) Let $\alpha$ be an arbitrary element of $F_q^*$. If $\ell$ 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:

$$\varphi : F_q[X]/(X^\ell - 1) \rightarrow F_q[X]/(X^\ell - \alpha),$$

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

Combining Lemma 3.2 with Lemma 3.3, we have the following lemma.
Lemma 3.4. Let $\mu = \zeta^{q-1}$ be a primitive $t$-th root of unity. Assume that $\text{ord}_{p^n}(q) = \phi(p^n)$. Then for each $0 \leq j \leq t-1$, there exists a unique element $\lambda_j \in F_q^*$ such that $\lambda_j^n \mu^j = 1$. Furthermore, we have the following $F_q$-algebra isomorphism:
\[ \hat{\phi}_q : F_q[X]/(X^{p^n} - 1) \rightarrow F_q[X]/(X^{p^n} - \mu^j), \]
which maps any element $f(X) + \langle X^{p^n} - 1 \rangle$ of $F_q[X]/(X^{p^n} - 1)$ to the element $f(\lambda_j X) + \langle X^{p^n} - \mu^j \rangle$ of $F_q[X]/(X^{p^n} - \mu^j)$.

Suppose $C_m = \langle a \rangle$ is a cyclic group of order $m$. Assume further that $\text{gcd}(m, q) = 1$. It is well known that $F_q C_m$ can be identified with the quotient algebra $F_q[X]/(X^m - 1)$ 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, $F_q C_m$ is isomorphic to $F_q[X]/(f_1(X)) \times \cdots \times F_q[X]/(f_r(X))$ as $F_q$-algebras. Note that $V_i = F_q[X]/(f_i(X))$ are finite fields, $1 \leq j \leq r$. In fact, it is easy to see that $V_i$ are irreducible $F_q C_m$-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 $V_1, \ldots, V_r$ is a set of representatives of the isomorphism classes of irreducible $F_q C_m$-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 $\text{ord}_{p^n}(q) = \phi(p^n)$, then $F_q C_{p^n}$ has exactly $n$ non-trivial irreducible characters $\chi_i^{(n)}$ for $1 \leq i \leq n$, which are given by
\[
\chi_i^{(n)}(g) = \begin{cases} 
-p^{i-1}, & g \in \langle z^{p^{i-1}} \rangle \setminus \langle z^{p^i} \rangle; \\
p^i - p^{i-1}, & g \in \langle z^p \rangle; \\
0, & g \in \langle z \rangle \setminus \langle z^{p^{i-1}} \rangle.
\end{cases}
\]

Proof. We claim that $F_q C_{p^n}$ has exactly $n$ non-trivial irreducible characters and they are of degree $\phi(p^i)$ for $1 \leq i \leq n$. Since $\text{ord}_{p^i}(q) = \phi(p^i)$, we get $\text{ord}_{p^i}(q) = \phi(p^i)$, 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 $F_q[X]/(\Phi_{p^i}(X))$. In the following, we first determine the irreducible character $\chi_1^{(n)}$.

Let $V = F_q[X]/(\Phi_{p}(X))$ with an ordered basis $v_1 = 1, v_2 = X, \ldots, v_{p-1} = X^{p-2}$, and let $GL(V)$ denote the group of all nonsingular $F_q$-linear transformations $V \rightarrow V$. The irreducible $F_q C_{p^n}$-module $V$ corresponds an irreducible representation of $C_{p^n}$ over $F_q$ as follows:
\[ \mathcal{X} : C_{p^n} \rightarrow GL(V) \\
z \mapsto \sigma \]

6
where $\sigma(v_1) = v_2, \sigma(v_2) = v_3, \ldots, \sigma(v_{p-2}) = v_{p-1}$ and $\sigma(v_{p-1}) = \sum_{\ell=1}^{p-1} (-v_\ell)$. It is easy to check that for any $1 \leq b \leq p - 2$,

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

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

and

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

Hence

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

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 $F_q C_{p^n} = \bigoplus_{i=0}^n F_q[X]/\langle \Phi_{p^i}(X) \rangle$ is a direct sum of irreducible $F_q C_{p^n}$-modules. Then we have

$$\chi_{reg}^{(n+1)} = \text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_{reg}^{(n)}) = \text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_0^{(n)}) + \text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_1^{(n)}) + \cdots + \text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_n^{(n)}). \quad (3.1)$$

On the other hand, we have

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

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 $\phi(p^j), 0 \leq j \leq n + 1$. On the other hand, $F_q C_{p^{n+1}} \bigotimes_{F_q C_{p^n}} F_q$ affords the character $\text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_0^{(n)})$ which is of degree $p$; further, $F_q C_{p^{n+1}} \bigotimes_{F_q C_{p^n}} F_q$ is a direct sum of some irreducible $F_q C_{p^{n+1}}$-modules. This forces that $F_q C_{p^{n+1}} \bigotimes_{F_q C_{p^n}} F_q = F_q \bigoplus F_q / \langle \Phi_{p}(X) \rangle$ is the only possible solution. Therefore, $\text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_0^{(n)}) = \chi_0^{(n+1)}$. Similar reasoning then shows that $\text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_i^{(n)}) = \chi_i^{(n+1)}, 1 \leq i \leq n$. In particular, $\chi_0^{(n+1)}$ and $\text{Ind}_{\langle z^p \rangle}^{\langle z \rangle} (\chi_i^{(n)})$ consist all the non-trivial irreducible characters of $C_{p^{n+1}}$ over $F_q$ for all $1 \leq i \leq n$. 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

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

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 \( 0 \leq s \leq t-1 \). In the following lemma, we obtain all the irreducible characters of \( C_{tp^n} \) over \( \mathbb{F}_q \).

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

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

and

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

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

**Proof.** We prove that \( F_q C_{tp^n} \) 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 \( \mu = \xi^{\frac{tp^n-1}{q-1}} \), then \( \mu \) 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 \( 0 \leq j \leq t-1 \). By Lemma 3.4, we recall the following \( F_q \)-algebra isomorphism:

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

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 $\theta_j$ of $\langle x^{p^n} \rangle$ are given by

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

We get our desired result by Lemma 3.5.

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

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

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

where $\lambda_j$ was stated in Lemma 3.4,

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

and

$$e_1(x) = \frac{1}{p^{n-i}} \sum_{j=0}^{p^{n-i-1}} X^{p^j} - \frac{1}{p^{n-i+1}} \sum_{j=0}^{p^{n-i+1}-1} X^{p^j}, \quad \text{for } 1 \leq i \leq n.$$

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

$$\psi_j^{(i)}(x^{-rj}) = \psi_j^{(i)}(x^{-rj} \cdot x^{-sp^n}) = -p^{i-1} \mu^{-mj} = -p^{i-1} \lambda_j^{sp^n}.$$

By Lemma 2.1 and Lemma 3.6, we deduce that

$$E_j^{(i)}(x) = \frac{1}{tp^n} \sum_{g \in \langle x^{p^{i-1}} \rangle} \psi_j^{(i)}(g^{-1}g)$$

$$= \frac{1}{tp^n} \sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \left( -p^{i-1}(1 + (\lambda_j x)^{p^{i-1}} + \cdots + (\lambda_j x)^{(p^{n-i+1})^{p^{i-1}}}) + p^i(1 + (\lambda_j x)^{p^i} + \cdots + (\lambda_j x)^{(p^{n-i+1})^{p^i}}) \right)$$

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

$$E_j^{(0)}(x) = \frac{1}{t} c_0(\lambda_j x) \sum_{s=0}^{t-1} \mu^{-js} x^{sp^n},$$

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

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

**Corollary 3.8.** If $\text{ord}_{p^n}(q) = \phi(p^n)$, then the quotient algebra $F_q[X]/(X^{p^n} - 1)$ has $n+1$ primitive idempotents given by $e_i(X)$, where $0 \leq i \leq n$ 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 $\text{ord}_{2p^n}(q) = \phi(p^n)$, then the quotient algebra $F_q[X]/(X^{2p^n} - 1)$ 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 $0 \leq i \leq n$ and $e_i(X)$ was stated in Theorem 3.7.

**Proof.** We just note that $\mu$ 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 $\text{ord}_{p^n}(q) = \phi(p^n)$. It was showed that, except for one minimal cyclic code with parameters $[p^n,1,p^n]$, the others have parameters $[p^n,\phi(p^i),2p^{n-i}]$, $1 \leq i \leq n$. In [1], the authors considered minimal cyclic codes of length $2p^n$ over $F_q$ with $\text{ord}_{2p^n}(q) = \phi(p^n)$. It turns out that except for two minimal cyclic code with parameters $[2p^n,1,2p^n]$, the others have parameters $[2p^n,\phi(p^i),4p^{n-i}]$, $1 \leq i \leq n$.

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 $\text{ord}_{tp^n}(q) = \phi(p^n)$. We have the following theorem.

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

(i) $E_j^{(0)}(X)$ has parameters $[tp^n,1,tp^n]$, and its check polynomial is $\lambda_jX - 1$, for each $0 \leq j \leq t - 1$;

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

**Proof.** (i) We first show that the check polynomial of $E_j^{(0)}(X)$ is $\lambda_jX - 1$ for $0 \leq j \leq t - 1$. It suffices to prove that the root of $\lambda_jX - 1$ does not satisfy $E_j^{(0)}(X)$. Obviously, $\lambda_j^{-1}$ 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 \(\lambda_j^p = 1\), 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

\[
X^{tp^n} - 1 = (\mu^{-j} X^{p^n} - 1) \left( \sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \right)
\]

\[
= (\lambda_j^p X^{p^n} - 1) \left( \sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \right)
\]

\[
= (\lambda_j^{p^i-1} X^{p^i-1} - 1) \left( \sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}} \right) \left( \sum_{\ell=0}^{p^{n-i}-1} (\lambda_j X)^{\ell} \right) \left( \sum_{s=0}^{t-1} \mu^{-js} X^{sp^n} \right).
\]

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

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

We claim that the check polynomial of \(E_j^{(i)}(X)\) is \(\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell p^{i-1}}\). Since \(\text{ord}_p(q) = \phi(p^i)\), 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 \(\delta\) 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 $E_j^{(i)}(X)$ is $\sum_{\ell=0}^{p-1} (\lambda_j X)^{\ell \cdot \ell - 1}$ and the generating polynomial is

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

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

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

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

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

With a similar argument, we obtain $w_H(r(X)g_j^{(i)}(X)) \geq 2tp^{n-1}$, which gives the desired result. $\square$

We now give an illustrative example.

**Example 4.2.** Take $q = 13, p = 5, n = 2$ and $t = 3$. Let $\xi$ be a primitive 12th root of unity in $F_{13}$. It is easy to check that $\text{ord}_{13}(13) = 20 = \phi(5^2)$. It follows 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 $F_{13}[X]/(X^{75} - 1)$ has exactly 9 primitive idempotents, and $e_1(X) = \frac{1}{2} \sum_{h=0}^{4} X^{5h} - \frac{1}{25} \sum_{h=0}^{24} X^h$, $e_2(X) = 1 - \frac{1}{2} \sum_{h=0}^{4} X^{5h}$. The minimal cyclic codes are given in Table 1.
Table 1

<table>
<thead>
<tr>
<th>Code</th>
<th>checking polynomial</th>
<th>primitive idempotent</th>
<th>parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\bar{E}_0^{(0)}(X)$</td>
<td>$X - 1$</td>
<td>$\frac{1}{3}c_0(X) \sum_{s=0}^2 X^{25s}$</td>
<td>[75, 1, 75]</td>
</tr>
<tr>
<td>$\bar{E}_1^{(0)}(X)$</td>
<td>$\lambda_1 X - 1$</td>
<td>$\frac{1}{3}c_0(\lambda_1 X) \sum_{s=0}^2 \mu^{-s} X^{25s}$</td>
<td>[75, 1, 75]</td>
</tr>
<tr>
<td>$\bar{E}_2^{(0)}(X)$</td>
<td>$\lambda_2 X - 1$</td>
<td>$\frac{1}{3}c_0(\lambda_2 X) \sum_{s=0}^2 \mu^{-2s} X^{25s}$</td>
<td>[75, 1, 75]</td>
</tr>
<tr>
<td>$\bar{E}_0^{(1)}(X)$</td>
<td>$\sum_{j=0}^4 X^j$</td>
<td>$\frac{1}{3}c_1(X) \sum_{s=0}^2 X^{25s}$</td>
<td>[75, 4, 30]</td>
</tr>
<tr>
<td>$\bar{E}_1^{(1)}(X)$</td>
<td>$\sum_{j=0}^4 (\lambda_1 X)^j$</td>
<td>$\frac{1}{3}c_1(\lambda_1 X) \sum_{s=0}^2 \mu^{-s} X^{25s}$</td>
<td>[75, 4, 30]</td>
</tr>
<tr>
<td>$\bar{E}_2^{(1)}(X)$</td>
<td>$\sum_{j=0}^4 (\lambda_2 X)^j$</td>
<td>$\frac{1}{3}c_1(\lambda_2 X) \sum_{s=0}^2 \mu^{-2s} X^{25s}$</td>
<td>[75, 4, 30]</td>
</tr>
<tr>
<td>$\bar{E}_0^{(2)}(X)$</td>
<td>$\sum_{j=0}^4 X^{5j}$</td>
<td>$\frac{1}{3}c_2(X) \sum_{s=0}^2 X^{25s}$</td>
<td>[75, 20, 6]</td>
</tr>
<tr>
<td>$\bar{E}_1^{(2)}(X)$</td>
<td>$\sum_{j=0}^4 (\lambda_1 X)^{5j}$</td>
<td>$\frac{1}{3}c_2(\lambda_1 X) \sum_{s=0}^2 \mu^{-s} X^{25s}$</td>
<td>[75, 20, 6]</td>
</tr>
<tr>
<td>$\bar{E}_2^{(2)}(X)$</td>
<td>$\sum_{j=0}^4 (\lambda_2 X)^{5j}$</td>
<td>$\frac{1}{3}c_2(\lambda_1 X) \sum_{s=0}^2 \mu^{-2s} X^{25s}$</td>
<td>[75, 20, 6]</td>
</tr>
</tbody>
</table>

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


