Hindawi
Mathematical Problems in Engineering
Volume 2018, Article ID 6962508, 9 pages
https://doi.org/10.1155/2018/6962508

Research Article

Primitive Idempotents of Irreducible Cyclic Codes of Length n

Yuqian Lin, Qin Yue, and Yansheng Wu

Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China

Correspondence should be addressed to Qin Yue; yueqin@nuaa.edu.cn

Received 2 March 2018; Accepted 18 April 2018; Published 3 June 2018

Academic Editor: Jean Jacques Loiseau

Let $\mathbb{F}_q$ be a finite field with q elements and n a positive integer. In this paper, we use matrix method to give all primitive idempotents of irreducible cyclic codes of length n, whose prime divisors divide $q-1$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^s$ and p is a prime. Let $\mathscr{C}$ be a $[n,k,d]$ linear code over $\mathbb{F}_q$, i.e., it is a k-dimensional subspace of $\mathbb{F}_q^n$ with minimum Hamming distance d. If for each codeword $(c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$, $(c_{n-1}, c_0, \ldots, c_{n-2})$ is also in $\mathscr{C}$, then we call $\mathscr{C}$ a cyclic code. In fact, each cyclic code of length n over $\mathbb{F}_q$ can be viewed as an ideal in the ring $R = \mathbb{F}_q[x]/\langle x^n - 1\rangle$ and each irreducible cyclic code of length n over $\mathbb{F}_q$ is an ideal of R generated by a primitive idempotent.

A lot of papers investigate primitive idempotents of R. We list some results about the length n.

(1) In [1, 2], $n = 2, 4, l^m$, and $2l^m$, where l is an odd prime and p is a primitive root modulo n.

(2) In [3, 4], $n = 2^m, m \geq 3$.

(3) In [5], $n = l_1^m l_2$, where l_1, l_2, p are distinct odd primes with $\gcd(\varphi(l_1^m)/2, \varphi(l_2)/2) = 1$ and p is a common primitive root modulo l_1^m and l_2.

(4) In [6], $n = l_1^{m_1} l_2^{m_2}$, where l_1, l_2, and p are three distinct odd primes, $\mathrm{ord}_{l_1^{m_1}}(p) = \varphi(l_1^{m_1})/2$, $\mathrm{ord}_{l_2^{m_2}}(p) = \varphi(l_2^{m_2})/2$, and $\gcd(\varphi(l_1^{m_1}), \varphi(l_2^{m_2})) = 2$.

(5) In [7, 8], $n = tl^m, t, m \geq 1$, where l is an odd prime different from the characteristic of $\mathbb{F}_q$, $t \mid (q-1)$, $\gcd(t,l) = 1$ and $\mathrm{ord}_{tl^m}(q) = \varphi(l^m)$; $n = l^m, m \geq 1$, where l is an odd prime and $l \mid (q-1)$.

(6) In [9, 10], $n = l_1^{m_1} l_2^{m_2}$, where l_1, l_2 are two distinct primes with $l_1 l_2 \mid (q-1)$; $n = 4l^m$ and $8l^m$, where l is an odd prime with $l \mid (q-1)$.

(7) In [11], $n = 2^m l_1^{m_1} l_2^{m_2}$, where l_1, l_2 are two distinct primes with $4 l_1 l_2 \mid (q-1)$.

(8) In [12], $n = l_1^{m_1} \cdots l_r^{m_r}$, where $l_1, \ldots, l_r$ are distinct odd primes with $l_1 \cdots l_r \mid (q-1)$.

In this paper, suppose that $\mathrm{rad}(n) \mid (q-1)$. We shall use matrix method to give all primitive idempotents of the ring R. The rest of paper is organized as follows: in Section 2, we give some basic results, in Section 3, we obtain all primitive idempotents in $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ under the condition: $\mathrm{rad}(n) \mid (q-1)$, and in Section 4, we conclude this paper.

2. Preliminaries

If a positive integer n has a prime factorization, $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$, where $p_1, p_2, \ldots, p_l$ are distinct primes and positive integers $\alpha_i \geq 1$ for $1 \leq i \leq l$, we denote $\mathrm{rad}(n) = p_1 p_2 \cdots p_l$ and $\nu_{p_i}(n) = \alpha_i$, $1 \leq i \leq l$, and $\mathrm{ord}(\alpha)$ is the order of $\alpha \in \mathbb{F}_q^*$. Through this paper, we always assume that $\gcd(n,q) = 1$.

Every cyclic code of length n over a finite field $\mathbb{F}_q$ is identified with exactly one ideal of the quotient algebra $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Some explicit factorizations of $x^n - 1$ can be found in [7–11, 13–16]. We need the following results about the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$.

Lemma 1 ([14, Corollary 1]). *Let $\mathbb{F}_q$ be a finite field and n a positive integer such that both $\mathrm{rad}(n) \mid (q-1)$ and either $q \not\equiv 3 \pmod 4$ or $8 \nmid n$. Let $m_1 = n/\gcd(n, q-1)$, $l_1 = (q-1)/\gcd(n, q-1)$, and θ be a generator of $\mathbb{F}_q^*$. Then one has the following:*

(1) The factorization of $x^n - 1$ into irreducible factors in $\mathbb{F}_q[x]$ is

$$\prod_{t|m_1}\prod_{\substack{1\le u\le \gcd(n,q-1)\\ \gcd(u,t)=1}}\left(x^t-\theta^{ul_1}\right). \tag{1}$$

(2) For each $t|m_1$, the number of irreducible factors of degree t is $\varphi(t)/t\cdot\gcd(n,q-1)$, where φ denotes the Euler Totient function, and the number of irreducible factors is

$$N_1=\gcd(n,q-1)\cdot\prod_{\substack{p|m_1\\ p\ \text{prime}}}\left(1+v_p(m_1)\cdot\frac{p-1}{p}\right). \tag{2}$$

Lemma 2 ([14, Corollary 2]). *Let $\mathbb{F}_q$ be a finite field and n a positive integer such that* $\mathrm{rad}(n)\mid(q-1)$, *$q\equiv 3\ (\mathrm{mod}\ 4)$, and $8\mid n$. Let $m_2=n/\gcd(n,q^2-1)$, $l_1=(q-1)/\gcd(n,q-1)$, $l_2=(q^2-1)/\gcd(n,q^2-1)$, $r=\min\{v_2(n/2),v_2(q+1)\}$, and α be a generator of $\mathbb{F}_{q^2}^*$ satisfying $\theta=\alpha^{q+1}$. Then one has the following:*

(1) The factorization of x^n-1 into irreducible factors in $\mathbb{F}_q[x]$ is

$$\begin{aligned}&\prod_{\substack{t|m_2\\ t\ \text{odd}}}\prod_{\substack{1\le w\le\gcd(n,q-1)\\ \gcd(w,t)=1}}\left(x^t-\theta^{wl_1}\right)\\ &\cdot\prod_{t|m_2}\prod_{u\in\mathscr{R}_t}\left(x^{2t}-\left(\alpha^{ul_2}+\alpha^{qul_2}\right)x^t+\theta^{ul_2}\right),\end{aligned} \tag{3}$$

where $\mathscr{R}_t$ is the set

$$\left\{u\in\mathbb{N}\ \middle|\ \begin{array}{l}1\le u\le\gcd\left(n,q^2-1\right),2^r\nmid u,\\ \gcd(u,t)=1,u<\{qu\}_{\gcd(n,q^2-1)}\end{array}\right\} \tag{4}$$

and $\{a\}_b$ denotes the remainder of the division of a by b.

(2) For each t odd with $t\mid m_2$, the number of irreducible polynomials of degree t is $\varphi(t)/t\cdot\gcd(n,q-1)$, and the number irreducible polynomials of degree $2t$ is

$$\begin{aligned}&\frac{\varphi(t)}{t}\cdot 2^{r-1}\cdot\gcd(n,q-1)\quad \text{if } t \text{ is even},\\ &\frac{\varphi(t)}{2t}\cdot\left(2^r-1\right)\cdot\gcd(n,q-1)\quad \text{if } t \text{ is odd}.\end{aligned} \tag{5}$$

The total number of irreducible factors is

$$\begin{aligned}N_2=&\gcd(n,q-1)\cdot\left(\frac{1}{2}+2^{r-2}\left(2+v_2(m)\right)\right)\\ &\cdot\prod_{\substack{p|m_2\\ p\ \text{odd prime}}}\left(1+v_p(m_2)\cdot\frac{p-1}{p}\right).\end{aligned} \tag{6}$$

Lemma 3 (see [17]). *Let $m_1,\dots,m_t$ be positive integers. For a set of integers $a_1,\dots,a_t$, the system of congruences $y\equiv a_i\ (\mathrm{mod}\ m_i)$, $i=1,\dots,t$, has solutions if and only if*

$$a_i\equiv a_j\quad\left(\mathrm{mod}\gcd\left(m_i,m_j\right)\right),\ i\ne j,\ 1\le i,\ j\le t. \tag{7}$$

If (7) is satisfied, the solution is unique modulo $\mathrm{lcm}(m_1,\dots,m_t)$.

3. Primitive Idempotents in R

In this section, we shall give all primitive idempotents in R if $\mathrm{rad}(n)\mid(q-1)$.

First, we consider the case $q\not\equiv 3\ (\mathrm{mod}\ 4)$ or $8\nmid n$.

In Lemma 1, let $t_1,\dots,t_d$ be all positive factors of $m_1=n/\gcd(n,q-1)$. For each t_i with $1\le i\le d$, there are $s_i=\varphi(t_i)/t_i\cdot\gcd(n,q-1)$ positive integers $u_{i1},u_{i2},\dots,u_{is_i}$ satisfying $1\le u_{ij}\le\gcd(n,q-1)$ and $\gcd(u_{ij},t_i)=1$, $j=1,\dots,s_i$. Since $l_1=(q-1)/\gcd(n,q-1)$ and $\langle\theta\rangle=\mathbb{F}_q^*$, $\delta=\theta^{l_1}$ is of order $\gcd(n,q-1)$. Then the irreducible factorization of x^n-1 over $\mathbb{F}_q$ can be rewritten as

$$\begin{aligned}x^n-1&=\prod_{\substack{1\le i\le d\\ 1\le j\le s_i}}\left(x^{t_i}-\delta^{u_{ij}}\right)\\ &=\prod_{1\le j\le s_1}\left(x^{t_1}-\delta^{u_{1j}}\right)\cdots\prod_{1\le j\le s_d}\left(x^{t_d}-\delta^{u_{dj}}\right).\end{aligned} \tag{8}$$

Note that the number of primitive idempotents in R coincides with the number of irreducible factors of x^n-1 over $\mathbb{F}_q$.

Theorem 4. *Let* $\mathrm{rad}(n)\mid(q-1)$ *and either $q\not\equiv 3\ (\mathrm{mod}\ 4)$ or $8\nmid n$. Then there are N_1 primitive idempotents in R as follows:*

$$\theta_{ij}(x)=\frac{t_i}{n}\sum_{k=0}^{n/t_i-1}\left(\delta^{-u_{ij}}\right)^k x^{kt_i}, \tag{9}$$

corresponding to the irreducible polynomials $x^{t_i}-\delta^{u_{ij}}$ over $\mathbb{F}_q$, $i=1,\dots,d$, $j=1,\dots,s_i$.

Proof. For each i, $1\le i\le d$, let $R_i=\prod_{1\le j\le s_i}\mathbb{F}_q[x]/\langle x^{t_i}-\delta^{u_{ij}}\rangle$ be a ring with s_i direct summands; for $0\le k\le n-1$, $k=t_iu+v$, $0\le u\le n/t_i-1$, and $0\le v\le t_i-1$. By (8) and Chinese Remainder Theorem, there is an $\mathbb{F}_q$-algebra isomorphism:

$$\psi=\left(\psi_1,\psi_2,\dots,\psi_d\right):R\longrightarrow R_1\times R_2\times\cdots\times R_d, \tag{10}$$

where each $\psi_i:R\to R_i$, $\sum_{k=0}^{n-1}a_kx^k\mapsto A_{i,0}+A_{i,1}x+\cdots+A_{i,t_i-1}x^{t_i-1}$ is an $\mathbb{F}_q$-algebraic epimorphism and each

$$\begin{aligned}A_{i,v}=&\left(\sum_{u=0}^{n/t_i-1}a_{t_iu+v}\delta^{uu_{i1}},\sum_{u=0}^{n/t_i-1}a_{t_iu+v}\delta^{uu_{i2}},\dots,\right.\\ &\left.\sum_{u=0}^{n/t_i-1}a_{t_iu+v}\delta^{uu_{is_i}}\right)\in\mathbb{F}_q^{s_i},\quad 0\le v\le t_i-1.\end{aligned} \tag{11}$$

Note that $\sum_{i=1}^d s_it_i=n$. Hence there is a $\mathbb{F}_q$-linear space isomorphism:

$$\begin{aligned}\phi=\left(\phi_1,\phi_2,\dots,\phi_d\right):R_1\times R_2\times\cdots\times R_d\longrightarrow\prod_{i=1}^d\mathbb{F}_q^{s_it_i}\\ =\mathbb{F}_q^n,\end{aligned} \tag{12}$$

where each $\phi_i:R_i\to\mathbb{F}_q^{s_it_i}$, $A_{i,0}+A_{i,1}x+\cdots+A_{i,t_i-1}x^{t_i-1}\mapsto(A_{i,0},A_{i,1},\dots,A_{i,t_i-1})$ is a $\mathbb{F}_q$-linear space epimorphism. Hence there is a $\mathbb{F}_q$-linear space isomorphism:

$$\begin{aligned}\chi = \phi\psi : R &\longrightarrow \mathbb{F}_q^n,\\ \sum_{k=0}^{n-1} a_k x^k &\longmapsto \left(A_{1,0},\ldots,A_{1,t_1-1},\ldots,A_{d,0},\ldots,A_{d,t_d-1}\right),\end{aligned} \tag{13}$$

$$\begin{aligned}&\left(A_{1,0},\ldots,A_{1,t_1-1},\ldots,A_{d,0},\ldots,A_{d,t_d-1}\right)\\ &\quad = \left(a_0,a_1,\ldots a_{n-1}\right)B,\end{aligned} \tag{14}$$

where B is a $n \times n$ invertible matrix over $\mathbb{F}_q$. Now we shall determine B and B^{-1}.

In (14), let $B := (B_1(\delta),\ldots,B_d(\delta))$ be a $n\times n$ matrix, where each $B_i(\delta) = (B_i^{(1)}(\delta),\ldots,B_i^{(t_i)}(\delta))$ is a $n\times s_i t_i$ matrix and each $B_i^{(v)}(\delta)$, $1 \le v \le t_i$, is a $n \times s_i$ matrix:

$$B_i^{(v)}(\delta) = \begin{array}{c}\left(\begin{array}{cccc}\vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & 0\\ (\delta^{u_{i1}})^0 & (\delta^{u_{i2}})^0 & \cdots & (\delta^{u_{is_i}})^0\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & 0\\ (\delta^{u_{i1}})^1 & (\delta^{u_{i2}})^1 & \cdots & (\delta^{u_{is_i}})^1\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & 0\\ (\delta^{u_{i1}})^{n/t_i-1} & (\delta^{u_{i2}})^{n/t_i-1} & \cdots & (\delta^{u_{is_i}})^{n/t_i-1}\\ 0 & 0 & \cdots & 0\\ \vdots & \vdots & & \vdots\end{array}\right)\end{array} \begin{array}{c}\\ \\ (v)\\ \\ \\ \\ (t_i+v)\\ \\ \\ \\ \left(\left(\dfrac{n}{t_i}-1\right)t_i+v\right)\\ \\ \\ \end{array} \qquad 1 \le v \le t_i. \tag{15}$$

In fact, each $B^{(v)}(\delta)$ is determined by these k rows, where $k = t_i u + v$, $0 \le u \le n/t_i - 1$.

We know that $\operatorname{ord}(\delta) = \gcd(n, q-1)$, $x^{t_i} - \delta^{u_{ij}}$, $1 \le u_{ij} \le \gcd(n,q-1)$, and $\gcd(t_i,u_{ij}) = 1$ are an irreducible polynomial of $x^n - 1$, so $(\delta^{u_{ij}})^{n/t_i} = 1$. Fix i and t_i, $1 \le i \le d$. If $1 \le u_{ij} \ne u_{ij'} \le \gcd(n,q-1)$, $\gcd(u_{ij},t_i) = 1$, $\gcd(u_{ij'},t_i) = 1$. Then $\delta^{u_{ij}-u_{ij'}} \ne 1$ and $(\delta^{u_{ij}-u_{ij'}})^{n/t_i} = 1$. Let

$$\left(B_i^{(v)}\left(\delta^{-1}\right)\right)^T = \begin{array}{c}\left(\begin{array}{cccccccccccc}\cdots & 0 & (\delta^{-u_{i1}})^0 & 0 & \cdots & (\delta^{-u_{i1}})^1 & 0 & \cdots & (\delta^{-u_{i1}})^{n/t_i-1} & 0 & \cdots\\ \cdots & 0 & (\delta^{-u_{i2}})^0 & 0 & \cdots & (\delta^{-u_{i2}})^1 & 0 & \cdots & (\delta^{-u_{i2}})^{n/t_i-1} & 0 & \cdots\\ & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & \\ \cdots & 0 & (\delta^{-u_{is_i}})^0 & 0 & \cdots & (\delta^{-u_{is_i}})^1 & 0 & \cdots & (\delta^{-u_{is_i}})^{n/t_i-1} & 0 & \cdots\end{array}\right)\\ \begin{array}{ccc}(v) & \qquad (t_i+v) & \qquad \left(\left(\dfrac{n}{t_i}-1\right)t_i+v\right)\end{array}\end{array} \tag{16}$$

be a $s_i \times n$ matrix over $\mathbb{F}_q$. Then,

$$\begin{aligned}&\left(B_i^{(v)}\left(\delta^{-1}\right)\right)^T B_i^{(v)}(\delta) = \frac{n}{t_i}E_{s_i},\\ &\left(B_i^{(v)}\left(\delta^{-1}\right)\right)^T B_i^{(v')}(\delta) = 0 \quad \text{if } 1 \le v \ne v' \le t_i,\end{aligned} \tag{17}$$

i.e.,

$$\begin{aligned}&\left(B_i\left(\delta^{-1}\right)\right)^T \cdot B_i(\delta)\\ &\quad = \begin{pmatrix}\left(B_i^{(1)}\left(\delta^{-1}\right)\right)^T\\ \vdots\\ \left(B_i^{(t_i)}\left(\delta^{-1}\right)\right)^T\end{pmatrix}\left(B_1^{(1)}(\delta),\ldots,B_i^{(t_i)}(\delta)\right)\\ &\quad = \frac{n}{t_i}E_{s_i t_i},\end{aligned} \tag{18}$$

where E_{s_i} and $E_{s_it_i}$ are the identity matrices of order $s_i\times s_i$ and $s_it_i\times s_it_i$, respectively.

Let

$$\left(B_i\left(\delta^{-1}\right)\right)^T=\begin{pmatrix}\left(B_i^{(1)}\left(\delta^{-1}\right)\right)^T\\ \vdots\\ \left(B_i^{(t_i)}\left(\delta^{-1}\right)\right)^T\end{pmatrix} \tag{19}$$

be a $s_it_i\times n$ matrix. Next, we shall prove that $(B_i(\delta^{-1}))^T\cdot B_{i'}(\delta)=0, 1\le i\ne i'\le d$. In fact,

$$\begin{aligned}&\left(B_i\left(\delta^{-1}\right)\right)^T\cdot B_{i'}(\delta)\\ &=\begin{pmatrix}\left(B_i^{(1)}\left(\delta^{-1}\right)\right)^T\\ \vdots\\ \left(B_i^{(t_i)}\left(\delta^{-1}\right)\right)^T\end{pmatrix}\left(B_{i'}^{(1)}(\delta)\ ,\ldots,\ B_{i'}^{(t_{i'})}(\delta)\right)\\ &=\begin{pmatrix}\left(B_i^{(1)}\left(\delta^{-1}\right)\right)^T B_{i'}^{(1)}(\delta) & \cdots & \left(B_i^{(1)}\left(\delta^{-1}\right)\right)^T B_{i'}^{(t_{i'})}(\delta)\\ \vdots & & \vdots\\ \left(B_i^{(t_i)}\left(\delta^{-1}\right)\right)^T B_{i'}^{(1)}(\delta) & \cdots & \left(B_i^{(t_i)}\left(\delta^{-1}\right)\right)^T B_{i'}^{(t_{i'})}(\delta)\end{pmatrix}.\end{aligned} \tag{20}$$

Hence we only need to show that

$$\left(B_i^{(v)}\left(\delta^{-1}\right)\right)^T B_{i'}^{(v')}(\delta)=0,\quad 1\le v\le t_i,\ 1\le v'\le t_{i'}. \tag{21}$$

We consider the following congruence equations:

$$\begin{aligned}x&\equiv v \pmod{t_i}\\ x&\equiv v' \pmod{t_{i'}}.\end{aligned} \tag{22}$$

Suppose that $\gcd(t_i,t_{i'})\nmid(v-v')$. Then it has no solution in (22) by Lemma 3, so it holds in (21).

Suppose that $\gcd(t_i,t_{i'})\mid(v-v')$. Then this is unique solution $x=a_0$ in (22) with $1\le x\le \operatorname{lcm}(t_i,t_{i'})$. Let $\operatorname{lcm}(t_i,t_{i'})=c=t_i\alpha=t_{i'}\beta$. Then $x=a_0+cl, l=0,1,\ldots,n/c-1$ are all solutions in (22) with $1\le x\le n$. Let $(M_i^{(v)}(\delta^{-1}))^T M_{i'}^{(v')}(\delta)=(c_{jj'})$ be a $s_i\times s_{i'}$ matrix over $\mathbb{F}_q$. Then for $1\le j\le s_i, 1\le j'\le s_{i'}$, the (j,j') entry is

$$c_{jj'}=\sum_{l=0}^{n/c-1}\left(\delta^{-u_{ij}}\right)^{\alpha l}\left(\delta^{u_{i'j'}}\right)^{\beta l}=\sum_{l=0}^{n/c-1}\left(\delta^{-u_{ij}\alpha+u_{i'j'}\beta}\right)^l, \tag{23}$$

where $1\le u_{ij},u_{i'j'}\le\gcd(n,q-1)$, $\gcd(u_{ij},t_i)=1$, and $\gcd(u_{i'j'},t_{i'})=1$. Since $x^{t_i}-\delta^{u_{ij}}$ is an irreducible divisor of x^n-1 over $\mathbb{F}_q$, $(\delta^{u_{ij}})^{n/t_i}=1$; similarly, $(\delta^{u_{i'j'}})^{n/t_{i'}}=1$. Hence

$$\left(\delta^{-u_{ij}\alpha+u_{i'j'}\beta}\right)^{n/c}=\left(\delta^{-u_{ij}}\right)^{n/t_i}\left(\delta^{u_{i'j'}}\right)^{n/t_{i'}}=1. \tag{24}$$

On the other hand, by $t_i\ne t_{i'}$ we assume that there is a prime p such that $v_p(t_i)>v_p(t_{i'})$. Then $p\mid\beta$ and $p\nmid\alpha$ by $\operatorname{lcm}(t_i,t_{i'})=c=t_i\alpha=t_{i'}\beta$, so $p\nmid(-u_{ij}\alpha+u_{i'j'}\beta)$ and $p\mid\gcd(n,q-1)$. Hence $\delta^{-u_{ij}\alpha+u_{i'j'}\beta}\ne1$. Therefore, $c_{jj'}=\sum_{l=0}^{n/c-1}(\delta^{-u_{ij}\alpha+u_{i'j'}\beta})^l=0$, and it holds in (21).

In conclusion, $(B_i(\delta^{-1}))^T B_i(\delta)=(n/t_i)E_{s_it_i}$, $(B_i(\delta^{-1}))^T B_{i'}(\delta)=0,\ 1\le i\ne i'\le d$, and

$$B^{-1}=\frac{1}{n}\begin{pmatrix}t_1\left(B_1\left(\delta^{-1}\right)\right)^T\\ t_2\left(B_2\left(\delta^{-1}\right)\right)^T\\ \vdots\\ t_d\left(B_d\left(\delta^{-1}\right)\right)^T\end{pmatrix}. \tag{25}$$

In the following, we present all primitive idempotents in R by lifting some primitive idempotents in $\mathbb{F}_q^n$ through the isomorphism χ.

By Lemma 1, the number of irreducible factors of x^n-1, which coincides with the number of primitive idempotents in R, is N_1. Let $\{e_1,\ldots,e_n\}$ denote the standard basis of $\mathbb{F}_q^n$. Hence the vectors of $\mathbb{F}_q^n$, $e_1,e_2,\ldots,e_{s_1},e_{t_1s_1+1}$, $e_{t_1s_1+2},\ldots,e_{t_1s_1+s_2},\ldots,e_{\sum_{h=1}^{d-1}t_hs_h+1},e_{\sum_{h=1}^{d-1}t_hs_h+2},\ldots,e_{\sum_{h=1}^{d-1}t_hs_h+s_d}$, correspond to all primitive idempotents in R. Hence for i, j, $1\le i\le d, 1\le j\le s_i$, let $\theta_{ij}(x)=\sum_{k=0}^{n-1}a_kx^k$ be a primitive idempotent in R, which is corresponding to $e_{\sum_{h=1}^{i-1}t_hs_h+j}$. By (14),

$$\begin{aligned}\chi\left(\theta_{ij}(x)\right)&=(a_0,a_1,\ldots,a_{n-1})B\\ &=\left(0,\ldots,0,\overset{\sum_{h=1}^{i-1}t_hs_h+j}{1},0,\ldots,0\right)\\ &=e_{\sum_{h=1}^{i-1}t_hs_h+j},\end{aligned} \tag{26}$$

and $(a_0,a_1,\ldots,a_{n-1})=e_{\sum_{h=1}^{i-1}t_hs_h+j}B^{-1}$. So we have proved the theorem. □

Remark 5. In special cases in Theorem 4, we can give those results in [8–11].

Second, we consider the case $q\equiv3\pmod 4$ and $8\mid n$.

In Lemma 2, let $t_1,t_2,\ldots,t_d$ be all odd factors of $m_2=n/\gcd(n,q^2-1)$ and let $t_{d+1},t_{d+2},\ldots,t_{d+d'}$ be all even factors of m_2. For each t_i with $1\le i\le d$, there are $s_i=\varphi(t_i)/t_i\cdot\gcd(n,q-1)$ positive integers $w_{i1},w_{i2},\ldots,w_{is_i}$ satisfying $1\le w_{ij}\le\gcd(n,q-1)$ and $\gcd(w_{ij},t_i)=1$, $j=1,2,\ldots,s_i$. For each t_i with $1\le i\le d+d'$, there are g_i positive integers $u_{i1},u_{i2},\ldots,u_{ig_i}$ satisfying $1\le u_{ij}\le 2^r\gcd(n,q-1)$, $\gcd(t_i,u_{ij})=1, 2^r\nmid u_{ij}$, $j=1,\ldots,g_i$. In fact, $n=\sum_{i=1}^d s_it_i+\sum_{i=1}^{d+d'}2t_ig_i$.

Since $l_1=(q-1)/\gcd(n,q-1)$, $l_2=(q^2-1)/\gcd(n,q^2-1)$, $\langle\theta\rangle=\mathbb{F}_q^*$, and $\langle\alpha\rangle=\mathbb{F}_{q^2}^*$, there exist $\delta\in\mathbb{F}_q^*$ and $\sigma\in\mathbb{F}_{q^2}^*$ such that $\theta^{l_1} = \delta$ and $\alpha^{l_2} = \sigma$. Then the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$ can be rewritten as

$$\begin{aligned} x^n - 1 &= \prod_{\substack{1\le i\le d\\ 1\le j\le s_i}} \left(x^{t_i} - \delta^{w_{ij}}\right) \\ &\cdot \prod_{\substack{1\le i\le d+d'\\ 1\le j\le g_i}} \left(x^{2t_i} - \left(\sigma^{u_{ij}} + \sigma^{qu_{ij}}\right) x^{t_i} + \sigma^{(q+1)u_{ij}}\right). \end{aligned} \tag{27}$$

Theorem 6. *Suppose that* $\mathrm{rad}(n) \mid (q-1)$, $q \equiv 3 \pmod 4$, *and* $8 \mid n$. *Then there are* N_2 *primitive idempotents in* R *as follows:*

(1)

$$\theta_{ij} = \frac{t_i}{n} \sum_{k=0}^{n/t_i - 1} \left(\delta^{-w_{ij}}\right)^k x^{kt_i} \tag{28}$$

correspond to the irreducible polynomials $x^{t_i} - \delta^{w_{ij}}$ *over* $\mathbb{F}_q$, $i = 1, \ldots, d$, $j = 1, \ldots, s_i$.

(2)

$$\eta_{ij} = \frac{t_i}{n} \sum_{k=0}^{n/t_i - 1} \mathrm{Tr}\left(\left(\sigma^{-u_{ij}}\right)^k\right) x^{kt_i} \tag{29}$$

correspond to the irreducible polynomials $x^{2t_i} - (\sigma^{u_{ij}} + \sigma^{qu_{ij}}) x^{t_i} + \sigma^{(q+1)u_{ij}}$ *over* $\mathbb{F}_q$, $i = 1, \ldots, d+d'$, $j = 1, \ldots, g_i$, *where* Tr *is the trace map from* $\mathbb{F}_{q^2}$ *into* $\mathbb{F}_q$.

Proof. The factorization of $x^n - 1$ into irreducible factors in $\mathbb{F}_{q^2}[x]$ is

$$\begin{aligned} x^n - 1 &= \prod_{\substack{1\le i\le d\\ 1\le j\le s_i}} \left(x^{t_i} - \delta^{w_{ij}}\right) \\ &\cdot \prod_{\substack{1\le i\le d+d'\\ 1\le j\le g_i}} \left(x^{t_i} - \sigma^{u_{ij}}\right)\left(x^{t_i} - \sigma^{qu_{ij}}\right). \end{aligned} \tag{30}$$

Similarly to proving Theorem 4, there is a $\mathbb{F}_{q^2}$-linear space isomorphism:

$$\begin{aligned} &\chi = \left(\chi_1, \ldots, \chi_d, \lambda_1, \ldots, \lambda_{d+d'}, \lambda_1^{(q)}, \ldots, \lambda_{d+d'}^{(q)}\right) : \\ &\frac{\mathbb{F}_{q^2}[x]}{\langle x^n - 1\rangle} \longrightarrow \mathbb{F}_{q^2}^n, \end{aligned} \tag{31}$$

$$\begin{aligned} \sum_{k=0}^{n-1} a_k x^k &\longmapsto \left(A_{1,0}, \ldots, A_{d,t_d-1}, D_{1,0}, \ldots, D_{d+d',t_{d+d'}-1},\right. \\ &\left. D_{1,0}^{(q)}, \ldots, D_{d+d',t_{d+d'}-1}^{(q)}\right), \end{aligned} \tag{32}$$

where there are $\mathbb{F}_{q^2}$-epimorphisms: for $1 \le i \le d$,

$$\chi_i : \frac{\mathbb{F}_{q^2}[x]}{(x^n - 1)} \longrightarrow \prod_{1\le j\le s_i} \frac{\mathbb{F}_{q^2}[x]}{\langle x^{t_i} - \delta^{w_{ij}}\rangle} \longrightarrow \mathbb{F}_{q^2}^{s_i t_i} \tag{33}$$

$$\sum_{k=0}^{n-1} a_k x^k \longmapsto \left(A_{i,0}, \ldots, A_{i,t_i-1}\right), \tag{34}$$

for $1 \le i \le d + d'$,

$$\lambda_i : \frac{\mathbb{F}_{q^2}[x]}{(x^n - 1)} \longrightarrow \prod_{1\le j\le g_i} \frac{\mathbb{F}_{q^2}[x]}{\langle x^{t_i} - \sigma^{u_{ij}}\rangle} \longrightarrow \mathbb{F}_{q^2}^{g_i t_i} \tag{35}$$

$$\sum_{k=0}^{n-1} a_k x^k \longmapsto \left(D_{i,0}, \ldots, D_{i,t_i-1}\right), \tag{36}$$

and for $1 \le i \le d + d'$,

$$\lambda_i^{(q)} : \frac{\mathbb{F}_{q^2}[x]}{(x^n - 1)} \longrightarrow \prod_{1\le j\le g_i} \frac{\mathbb{F}_{q^2}[x]}{\langle x^{t_i} - \sigma^{qu_{ij}}\rangle} \longrightarrow \mathbb{F}_{q^2}^{g_i t_i} \tag{37}$$

$$\sum_{k=0}^{n-1} a_k x^k \longmapsto \left(D_{i,0}^{(q)}, \ldots, D_{i,t_i-1}^{(q)}\right). \tag{38}$$

Hence there is a $n \times n$ invertible matrix B over $\mathbb{F}_{q^2}$ such that

$$\begin{aligned} &(a_0, a_1, \ldots, a_{n-1}) B = \left(A_{1,0}, \ldots, A_{d,t_d-1}, D_{1,0}, \ldots,\right. \\ &\quad \left. D_{d+d',t_{d+d'}-1}, D_{1,0}^{(q)}, \ldots, D_{d+d',t_{d+d'}-1}^{(q)}\right). \end{aligned} \tag{39}$$

Now we shall construct the matrix B. Let

$$\begin{aligned} B = &\left(B_1(\delta), \ldots, B_d(\delta), B_1(\sigma), \ldots, B_{d+d'}(\sigma), B_1(\sigma^q), \ldots,\right. \\ &\left. B_{d+d'}(\sigma^q)\right), \end{aligned} \tag{40}$$

where $B_i(\delta)$ are $n \times s_i t_i$ matrices over $\mathbb{F}_{q^2}$, $1 \le i \le d$, and $B_i(\sigma)$, $B_i(\sigma^q)$ are $n \times g_i t_i$ matrices over $\mathbb{F}_{q^2}$, $1 \le i \le d + d'$.

(a) For each i with $1 \le i \le d$, by (33) we have

$$(a_0, a_1, \ldots, a_{n-1}) B_i(\delta) = \left(A_{i,0}, A_{i,1}, \ldots, A_{i,t_i-1}\right), \tag{41}$$

where $A_{i,0}, A_{i,1}, \ldots, A_{i,t_i-1} \in \mathbb{F}_q^{s_i}$. Let $B_i(\delta) = (B_i^{(1)}(\delta), \ldots, B_i^{(t_i)}(\delta))$ be a $n \times s_i t_i$ matrix, and each $B_i^{(v)}(\delta)$, $1 \le v \le t_i$ be a $n \times s_i$ matrix as shown in Theorem 4.

(b) For each i with $1 \le i \le d + d'$, by (35) we have that $(a_0, a_1, \ldots, a_{n-1}) B_i(\sigma) = (D_{i,0}, D_{i,1}, \ldots, D_{i,t_i-1})$, where $D_{i,0}, D_{i,1}, \ldots, D_{i,t_i-1} \in \mathbb{F}_q^{g_i}$. Let $B_i(\sigma) = (B_i^{(1)}(\sigma), \ldots, B_i^{(t_i)}(\sigma))$ be a $n \times g_i t_i$ matrix and each $B_i^{(v)}(\sigma)$, $1 \le v \le t_i$, a $n \times g_i$ matrix:

$$B_i^{(v)}(\sigma) = \begin{array}{cc} \left(\begin{array}{cccc} \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ (\sigma^{u_{i1}})^0 & (\sigma^{u_{i2}})^0 & \cdots & (\sigma^{u_{is_i}})^0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ (\sigma^{u_{i1}})^1 & (\sigma^{u_{i2}})^1 & \cdots & (\sigma^{u_{is_i}})^1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ (\sigma^{u_{i1}})^{n/t_i-1} & (\sigma^{u_{i2}})^{n/t_i-1} & \cdots & (\sigma^{u_{is_i}})^{n/t_i-1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \end{array}\right) & \begin{array}{c} \\ \\ (v) \\ \\ \\ \\ (t_i + v) \\ \\ \\ \\ \left(\left(\frac{n}{t_i} - 1\right) t_i + v\right) \\ \\ \\ \end{array} \end{array} \qquad 1 \le v \le t_i. \tag{42}$$

(c) For each i with $1 \le i \le d + d'$, by (37) we have that $(a_0, a_1, \ldots, a_{n-1}) B_i(\sigma^q) = (D_{i,0}^{(q)}, D_{i,1}^{(q)}, \ldots, D_{i,t_i-1}^{(q)})$, where $D_{i,0}^{(q)}, D_{i,1}^{(q)}, \ldots, D_{i,t_i-1}^{(q)} \in \mathbb{F}_q^{g_i}$. Let $B_i(\sigma^q) = (B_i^{(1)}(\sigma^q), \ldots, B_i^{(t_i)}(\sigma^q))$ be a $n \times g_i t_i$ matrix, and each $B_i^{(v)}(\sigma^q)$, $1 \le v \le t_i$, a $n \times g_i$ matrix:

$$B_i^{(v)}(\sigma^q) = \begin{array}{cc} \left(\begin{array}{cccc} \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ (\sigma^{qu_{i1}})^0 & (\sigma^{qu_{i2}})^0 & \cdots & (\sigma^{qu_{is_i}})^0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ (\sigma^{qu_{i1}})^1 & (\sigma^{qu_{i2}})^1 & \cdots & (\sigma^{qu_{is_i}})^1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \\ (\sigma^{qu_{i1}})^{n/t_i-1} & (\sigma^{qu_{i2}})^{n/t_i-1} & \cdots & (\sigma^{qu_{is_i}})^{n/t_i-1} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \end{array}\right) & \begin{array}{c} \\ \\ (v) \\ \\ \\ \\ (t_i + v) \\ \\ \\ \\ \left(\left(\frac{n}{t_i} - 1\right) t_i + v\right) \\ \\ \\ \end{array} \end{array} \qquad 1 \le v \le t_i. \tag{43}$$

Similarly to proving Theorem 4, we obtain that

$$B^{-1}=\frac{1}{n}\begin{pmatrix} t_1\left(B_1\left(\delta^{-1}\right)\right)^T \\ \vdots \\ t_d\left(B_d\left(\delta^{-1}\right)\right)^T \\ t_1\left(B_1\left(\sigma^{-1}\right)\right)^T \\ \vdots \\ t_{d+d'}\left(B_{d+d'}\left(\sigma^{-1}\right)\right)^T \\ t_1\left(B_1\left(\sigma^{-q}\right)\right)^T \\ \vdots \\ t_{d+d'}\left(B_{d+d'}\left(\sigma^{-q}\right)\right)^T \end{pmatrix}, \tag{44}$$

where

(a) for each i with $1 \le i \le d$, $(B_i(\delta^{-1}))^T = \begin{pmatrix} (B_i^{(1)}(\delta^{-1}))^T \\ \vdots \\ (B_i^{(t_i)}(\delta^{-1}))^T \end{pmatrix}$, and for each ν with $1 \le \nu \le t_i$, $(B_i^{(\nu)}(\delta^{-1}))^T$ is a $s_i \times n$ matrix as shown in Theorem 4.

(b) for each i with $1 \le i \le d+d'$, $(B_i(\sigma^{-1}))^T = \begin{pmatrix} (B_i^{(1)}(\sigma^{-1}))^T \\ \vdots \\ (B_i^{(t_i)}(\sigma^{-1}))^T \end{pmatrix}$, and for each ν with $1 \le \nu \le t_i$, $(B_i^{(\nu)}(\sigma^{-1}))^T$ is a $g_i \times n$ matrix:

$$\left(B_i^{(\nu)}\left(\sigma^{-1}\right)\right)^T = \begin{array}{c}\begin{pmatrix} \cdots & 0 & \left(\sigma^{-u_{i1}}\right)^0 & 0 & \cdots & 0 & \left(\sigma^{-u_{i1}}\right)^1 & 0 & \cdots & \left(\sigma^{-u_{i1}}\right)^{n/t_i-1} & 0 & \cdots \\ \cdots & 0 & \left(\sigma^{-u_{i2}}\right)^0 & 0 & \cdots & 0 & \left(\sigma^{-u_{i2}}\right)^1 & 0 & \cdots & \left(\sigma^{-u_{i2}}\right)^{n/t_i-1} & 0 & \cdots \\ & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \\ \cdots & 0 & \left(\sigma^{-u_{is_i}}\right)^0 & 0 & \cdots & 0 & \left(\sigma^{-u_{is_i}}\right)^1 & 0 & \cdots & \left(\sigma^{-u_{is_i}}\right)^{n/t_i-1} & 0 & \cdots \end{pmatrix} \\ \begin{array}{ccc} (\nu) & \qquad\qquad (t_i+\nu) & \qquad\qquad \left(\left(\dfrac{n}{t_i}-1\right)t_i+\nu\right) \end{array}\end{array}; \tag{45}$$

(c) for each i with $1 \le i \le d+d'$, $(B_i(\sigma^{-q}))^T = \begin{pmatrix} (B_i^{(1)}(\sigma^{-q}))^T \\ \vdots \\ (B_i^{(t_i)}(\sigma^{-q}))^T \end{pmatrix}$, and for each ν with $1 \le \nu \le t_i$, $(B_i^{(\nu)}(\sigma^{-q}))^T$ is a $g_i \times n$ matrix:

$$\left(B_i^{(\nu)}\left(\sigma^{-q}\right)\right)^T = \begin{array}{c}\begin{pmatrix} \cdots & 0 & \left(\sigma^{-qu_{i1}}\right)^0 & 0 & \cdots & 0 & \left(\sigma^{-qu_{i1}}\right)^1 & 0 & \cdots & \left(\sigma^{-qu_{i1}}\right)^{n/t_i-1} & 0 & \cdots \\ \cdots & 0 & \left(\sigma^{-qu_{i2}}\right)^0 & 0 & \cdots & 0 & \left(\sigma^{-qu_{i2}}\right)^1 & 0 & \cdots & \left(\sigma^{-qu_{i2}}\right)^{n/t_i-1} & 0 & \cdots \\ & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \\ \cdots & 0 & \left(\sigma^{-qu_{is_i}}\right)^0 & 0 & \cdots & 0 & \left(\sigma^{-qu_{is_i}}\right)^1 & 0 & \cdots & \left(\sigma^{-qu_{is_i}}\right)^{n/t_i-1} & 0 & \cdots \end{pmatrix} \\ \begin{array}{ccc} (\nu) & \qquad\qquad (t_i+\nu) & \qquad\qquad \left(\left(\dfrac{n}{t_i}-1\right)t_i+\nu\right) \end{array}\end{array}. \tag{46}$$

In the following, we give all primitive idempotents in $\mathbb{F}_q[x]/\langle x^n-1\rangle$.

(1) For fixed i and j with $1 \le i \le d$ and $1 \le j \le s_i$, $\delta^{w_{ij}} \in \mathbb{F}_q$. Hence the primitive idempotents in $\mathbb{F}_{q^2}[x]/\langle x^{t_i}-\delta^{w_{ij}}\rangle$ are the same as $\mathbb{F}_q[x]/\langle x^{t_i}-\delta^{w_{ij}}\rangle$. We have the result.

(2) For fixed i and j with $1 \le i \le d+d'$ and $1 \le j \le g_i$, the polynomial $x^{2t_i}-(\sigma^{u_{ij}}+\sigma^{qu_{ij}})x^{t_i}+\sigma^{(q+1)u_{ij}}$ is irreducible over $\mathbb{F}_q$. In fact, the primitive idempotents in $\mathbb{F}_{q^2}[x]/\langle x^{2t_i}-(\sigma^{u_{ij}}+\sigma^{qu_{ij}})x^{t_i}+\sigma^{(q+1)u_{ij}}\rangle$ are the same as $\mathbb{F}_q[x]/\langle x^{2t_i}-(\sigma^{u_{ij}}+\sigma^{qu_{ij}})x^{t_i}+\sigma^{(q+1)u_{ij}}\rangle$.

Note that there are $\mathbb{F}_{q^2}$-algebra isomorphisms:

$$\tau_i : \frac{\mathbb{F}_{q^2}[x]}{\left\langle x^{2t_i} - (\sigma^{u_{ij}} + \sigma^{qu_{ij}}) x^{t_i} + \sigma^{(q+1)u_{ij}} \right\rangle} \longrightarrow \frac{\mathbb{F}_{q^2}[x]}{\langle x^{t_i} - \sigma^{u_{ij}} \rangle} \times \frac{\mathbb{F}_{q^2}[x]}{\langle x^{t_i} - \sigma^{qu_{ij}} \rangle}, \quad (47)$$

$$c(x) = \sum_{k=0}^{2t_i-1} a_k x^k = y + z x^{t_i} \longmapsto (y, z) N = (y', z'),$$

where $y = \sum_{k=0}^{t_i-1} a_i x^i$, $z = \sum_{k=0}^{t_i-1} a_{t_i+k} x^k \in \mathbb{F}_{q^2}[x]$, and N is a 2×2 matrix over $\mathbb{F}_{q^2}$:

$$N = \begin{pmatrix} 1 & 1 \\ \sigma^{u_{ij}} & \sigma^{qu_{ij}} \end{pmatrix}. \quad (48)$$

Note that the identity of $\mathbb{F}_{q^2}[x]/\langle x^{2t_i} - (\sigma^{u_{ij}} + \sigma^{qu_{ij}}) x^{t_i} + \sigma^{(q+1)u_{ij}} \rangle$ is equal to the identity of $\mathbb{F}_q[x]/\langle x^{2t_i} - (\sigma^{u_{ij}} + \sigma^{qu_{ij}}) x^{t_i} + \sigma^{(q+1)u_{ij}} \rangle$. Now, take $c(x) = 1$, then

$$\tau_i(c(x)) = \tau_i(1) = (1, 0) N = (1, 1). \quad (49)$$

Let $\eta_{ij}(x) = \sum_{k=0}^{n-1} a_k x^k$ be a primitive idempotent in R corresponding to the irreducible polynomials $x^{2t_i} - (\sigma^{u_{ij}} + \sigma^{qu_{ij}}) x^{t_i} + \sigma^{(q+1)u_{ij}}$. By (31)

$$\begin{aligned} \chi(\eta_{ij}(x)) &= (a_0, a_1, \ldots, a_{n-1}) B = (b_0, b_1, \ldots, b_{n-1}) \\ &= \left(A_{1,0}, \ldots, A_{d,t_d-1}, D_{1,0}, \ldots, D_{d+d', t_{d+d'}-1}, D^{(q)}_{1,0}, \ldots, D^{(q)}_{d+d', t_{d+d'}-1}\right) \\ &= \left(0, \ldots, 0, D_{i,0}, 0, \ldots, 0, D^{(q)}_{i,0}, 0, \ldots, 0\right), \end{aligned} \quad (50)$$

where $D_{i,0} = (0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0)$, $D^{(q)}_{i,0} = (0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0)$. Hence

$$\begin{aligned} (a_0, a_1, \ldots, a_{n-1}) &= (b_0, b_1, \ldots, b_{n-1}) B^{-1} \\ &= \frac{t_i}{n}\left(\mathrm{Tr}\left((\sigma^{-u_{ij}})^0\right), 0, \ldots, 0, \mathrm{Tr}\left((\sigma^{-u_{ij}})^1\right), 0, \ldots, 0, \mathrm{Tr}\left((\sigma^{-u_{ij}})^{n/t_i-1}\right), 0, \ldots, 0\right). \end{aligned} \quad (51)$$

Hence we complete the proof. □

4. Concluding Remarks

In this paper, suppose that $\mathrm{rad}(n) \mid (q-1)$, we use matrix method to give all primitive idempotents in the ring $\mathbb{F}_q[x]/\langle x^n - 1 \rangle$. Suppose that the order of q modulo $\mathrm{rad}(n)$ is w, where w is a positive integer. We can also obtain all primitive idempotents of irreducible cyclic codes by the similar method in Theorems 4 and 6. Hence, all primitive idempotents of simple root irreducible cyclic codes can be presented by the method in Theorems 4 and 6.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The paper is supported by National Natural Science Foundation of China (nos. 61772015, 11601475, and 11661014), the Guangxi Science Research and Technology Development Project (1599005-2-13), and Foundation of Science and Technology on Information Assurance Laboratory (no. KJ-17-010).

References

[1] S. K. Arora and M. Pruthi, "Minimal cyclic codes of length $2p^n$," *Finite Fields and Their Applications*, vol. 5, no. 2, pp. 177–187, 1999.

[2] M. Pruthi and S. K. Arora, "Minimal codes of prime-power length," *Finite Fields and Their Applications*, vol. 3, no. 2, pp. 99–113, 1997.

[3] M. Pruthi, "Cyclic codes of length 2^m," *The Proceedings of the Indian Academy of Sciences – Mathematical Sciences*, vol. 111, no. 4, pp. 371–379, 2001.

[4] A. Sharma, G. K. Bakshi, V. C. Dumir, and M. Raka, "Irreducible cyclic codes of length 2^n," *Ars Combinatoria*, vol. 86, pp. 133–146, 2008.

[5] G. K. Bakshi and M. Raka, "Minimal cyclic codes of length $p^n q$," *Finite Fields and Their Applications*, vol. 9, no. 4, pp. 432–448, 2003.

[6] R. Singh and M. Pruthi, "Primitive idempotents of irreducible quadratic residue cyclic codes of length pnqm," *International Journal of Algebra*, vol. 5, no. 5-8, pp. 285–294, 2011.

[7] B. Chen, H. Liu, and G. Zhang, "Some minimal cyclic codes over finite fields," *Discrete Mathematics*, vol. 331, pp. 142–150, 2014.

[8] B. Chen, H. Liu, and G. Zhang, "A class of minimal cyclic codes over finite fields," *Designs, Codes and Cryptography. An International Journal*, vol. 74, no. 2, pp. 285–300, 2015.

[9] F. Li, Q. Yue, and C. Li, "The minimum Hamming distances of irreducible cyclic codes," *Finite Fields and Their Applications*, vol. 29, pp. 225–242, 2014.

[10] F. Li, Q. Yue, and C. Li, "Irreducible cyclic codes of length $4p^n$ and $8p^n$," *Finite Fields and Their Applications*, vol. 34, pp. 208–234, 2015.

[11] F. Li and X. Cao, "A class of minimal cyclic codes over finite fields," *Discrete Mathematics*, vol. 340, no. 1, pp. 3197–3206, 2017.

[12] M. Pruthi, "The minimum Hamming distances of the irreducible cyclic codes of length $l_1^{m_1}, l_2^{m_2} \ldots l_r^{m_r}$," *Journal of Discrete Mathematical Sciences and Cryptography*, pp. 965–995, 2016.

[13] B. Chen, L. Li, and R. Tuerhong, "Explicit factorization of $x^{2mpn} - 1$ over a finite field," *Finite Fields and Their Applications*, vol. 24, pp. 95–104, 2013.

[14] F. Martnez, C. Vergara, and L. Oliveira, "Explicit factorization of $x^n - 1 \in \mathbb{F}_q[x]$," *Designs, Codes and Cryptography. An International Journal*, vol. 77, no. 1, pp. 277–286, 2015.

[15] S. Yang and Z.-A. Yao, "Complete weight enumerators of a class of linear codes," *Discrete Mathematics*, vol. 340, no. 4, pp. 729–739, 2017.

[16] S. Yang, X. Kong, and C. Tang, "A construction of linear codes and their complete weight enumerators," *Finite Fields and Their Applications*, vol. 48, pp. 196–226, 2017.

[17] C. Ding, D. Pei, and A. Salomaa, *Chinses Remainder Theorem: Applications in Computing, Coding, Cryptography, Section 2.4*, World Scientific Publishing Co., Inc., Singapore, 1996.