Chin. Ann. Math. Ser. B
40(4), 2019, 555–566
DOI: 10.1007/s11401-019-0151-7

Chinese Annals of Mathematics, Series B

On Constacyclic Codes over $Z_{p_1p_2\cdots p_t}$*

Derong XIE[1]   Qunying LIAO[1]

Abstract Let $t \geq 2$ be an integer, and let $p_1, \cdots, p_t$ be distinct primes. By using algebraic properties, the present paper gives a sufficient and necessary condition for the existence of non-trivial self-orthogonal cyclic codes over the ring $Z_{p_1p_2\cdots p_t}$ and the corresponding explicit enumerating formula. And it proves that there does not exist any self-dual cyclic code over $Z_{p_1p_2\cdots p_t}$.

Keywords Ideal, Isomorphism, Constacyclic code, Self-orthogonal code, Self-orthogonal cyclic code
2000 MR Subject Classification 94B15

1 Introduction

Let q be a power of the prime p and $\mathbb{F}_q$ be the finit field of q elements. In 1957, the concept of cyclic codes over $\mathbb{F}_q$ was proposed (cf. [14]). Cyclic codes over finite fields, as a class of good linear codes, have attracted extensive attentions due to their special algebraic properties, decoding algorithms, and easy realization etc. In 1967, the concept of negacyclic codes over $\mathbb{F}_q$ was given (cf. [1]). Later, scholars generalized cyclic codes over finite fields to be constacyclic codes over finite fields. Fixed $u \in \mathbb{F}_q^*$, the linear code $\mathcal{C}$ with length n over $\mathbb{F}_q$ is a u-constacyclic code if for any $\mathbf{c} = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, the u-constacyclic shift $(uc_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathcal{C}$. In particular, when $u = 1$, $\mathcal{C}$ is a cyclic code; when $u = -1$, $\mathcal{C}$ is a negacyclic code. It's well-known that self-orthogonal and self-dual cycle codes over finite fields are both useful in cryptography and coding theory due to their many good algebraic properties. In 2011, some sufficient and necessary conditions for the existence of self-dual cyclic codes over $\mathbb{F}_q$ were obtained (cf. [10]). In 2014, a sufficient and necessary condition for the existence of nontrivial self-orthogonal cyclic codes over $\mathbb{F}_q$ was obtained and then the corresponding explicit enumerating formula were determined (cf. [11]).

On the other hand, in recent years, codes over finite rings are also interesting since the binary image of a linear code over Z_4 is a binary code (not necessarily linear) (cf. [4–7, 12]).

Definition 1.1 (cf. [5]) *Let R be a finite ring, a code $\mathcal{C}$ with length n over R is a nonempty subset of R^n, and the ring R is referred to as the alphabet of the code. If this subset is, in addition, an R-submodule of R^n, then $\mathcal{C}$ is called linear. For a unit λ of R, the λ-constacyclic (λ-twisted) shift τ_λ on R^n is the shift*

$$\tau_\lambda(x_0, x_1, \cdots, x_{n-1}) = (\lambda x_{n-1}, x_0, \cdots, x_{n-2}),$$

Manuscript received April 8, 2016. Revised July 5, 2017.

[1] College of Mathematical Science, Sichuan Normal University, Chengdu 610066, China.
E-mail: qunyingliao@sicnu.edu.cn derongxie@yahoo.com

*This work was supported by the Project of Science and Technology Department of Sichuan Province (No. 2016JY0134).

and a linear code $\mathcal{C}$ is said to be λ-constacyclic if $\tau_\lambda(\mathcal{C}) = \mathcal{C}$. It means that $\mathcal{C}$ is closed under the λ-constacyclic shift τ_λ. In case $\lambda = 1$, those λ-constacyclic codes are called cyclic codes, and when $\lambda = -1$, such λ-constacyclic codes are called negacyclic codes.

Proposition 1.1 (cf. [5]) *Let R be a finite ring, a linear code $\mathcal{C}$ with length n is λ-constacyclic over R if and only if $\mathcal{C}$ is an ideal of the ring $R[x]/\langle x^n - \lambda\rangle$.*

Definition 1.2 (cf. [5, 8]) *Given two n-tuples $x = (x_0, x_1, \cdots, x_{n-1}), y = (y_0, y_1, \cdots, y_{n-1}) \in R^n$, their inner product or dot product is defined as usual*:

$$x \cdot y = x_0y_0 + x_1y_1 + x_2y_2 + \cdots + x_{n-1}y_{n-1}$$

evaluated in R. Two n-tuples x, y are called orthogonal if $x \cdot y = 0$. For a linear code $\mathcal{C}$ over R, its dual code $\mathcal{C}^\perp$ is the set of n-tuples over R which are orthogonal to all codewords of $\mathcal{C}$, i.e.,

$$\mathcal{C}^\perp = \{x \mid x \cdot y = 0, \forall y \in C\}.$$

A code $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subseteq \mathcal{C}^\perp$, and it is self-dual if $\mathcal{C} = \mathcal{C}^\perp$.

Definition 1.3 (cf. [13]) *Let $x \in \mathbb{R}$, $[x]$ denotes the largest integer less than x, the function $[x]$ is called the Gauss function.*

Proposition 1.2 (cf. [4]) *Suppose that R is a finite ring, λ is a unit of R and $\mathcal{C}$ is an λ-constacyclic code over the finite ring R with identity, then $\mathcal{C}^\perp$ is an λ^{-1}-constacyclic code over R.*

In 2003, Blackford [2] studied negative cyclic codes with even length over Z_4. In 2009, the structure of negative cyclic codes with even length and their dual codes over the finite chain ring Z_{2^a} was obtained, where a is a positive integer (cf. [15]). In 2013, a $(1 + \omega\gamma)$-constacyclic code of arbitrary length over the general finite chain ring were constructed (cf. [3]).

The present paper continues to the study, and discusses constacyclic codes over the finite non-chain ring $Z_{p_1p_2\cdots p_t}$, where $p_1, p_2, \cdots, p_t$ are distinct primes. A sufficient and necessary condition for the existence of both constacyclic codes and non-trivial self-orthogonal cyclic codes over $Z_{p_1p_2\cdots p_t}$ are obtained, and then the explicit enumerating formula for the numbers of these codes is given. In fact, the following main results are proved.

Theorem 1.1 *Let $p_1, p_2, \cdots, p_t$ be distinct primes, λ be a unit of $Z_{p_1p_2\cdots p_t}$. Suppose that $\mathcal{C}$ is a code with length n over $Z_{p_1p_2\cdots p_t}$, then*

(1) *$\mathcal{C}$ is an λ-constacyclic code if and only if there exist some λ_i-constacyclic codes $\mathcal{C}_i$ with length n over Z_{p_i} such that $\mathcal{C} \cong \bigoplus_{i=1}^{t} \mathcal{C}_i$, where $\lambda_i \equiv \lambda (\mathrm{mod}\ p_i)$ $(1 \le i \le t)$;*

(2) *$\mathcal{C}$ is a cyclic code if and only if for any $i = 1, \cdots, t$, $\mathcal{C}_i$ is a cyclic code over Z_{p_i};*

(3) *$\mathcal{C}$ is a self-orthogonal* (*self-dual*) *cyclic code if and only if for any $i = 1, \cdots, t$, $\mathcal{C}_i$ is a self-orthogonal* (*self-dual*) *cyclic code over Z_{p_i}.*

Without loss of generality, if $\mathcal{C} = \{0\}$, then a code $\mathcal{C}$ over $Z_{p_1p_2\cdots p_t}$ is trivial. Otherwise, $\mathcal{C}$ is non-trivial. The following Theorem 1.2 gives a sufficient and necessary condition for the existence of non-trivial self-orthogonal cyclic codes over $Z_{p_1p_2\cdots p_t}$.

Theorem 1.2 *There exists a non-trivial self-orthogonal cyclic code with length n over $Z_{p_1p_2\cdots p_t}$ if and only if there is at least one p_i, such that one of the following conditions is satisfied.*

(1) $\gcd(n, p_i) \neq 1$.

(2) *If* $\gcd(n,p_i)=1$, *then* $2\nmid \mathrm{ord}_n(p_i)$.
(3) *If* $\gcd(n,p_i)=1$ *and* $2\mid \mathrm{ord}_n(p_i)$, *then* $n\nmid (q^{\frac{\mathrm{ord}_n(p_i)}{2}}+1)$.

It is well-known that, for a polynomial

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_{m+1}x^{m+1}+a_mx^m(n>m,a_n,a_m\neq 0)\in\mathbb{F}_q[x],$$

the reverse polynomial is

$$f^*(x)=a_nx^m+a_{n-1}x^{m+1}+\cdots+a_{m+1}x^{n-1}+a_mx^n.$$

Especially, there exists some $\alpha\in\mathbb{F}_q^*$ such that $f(x)=\alpha g^*(x)$, then $f(x)$ and $g(x)$ are a pair reciprocal polynomials. Furthermore, if $f(x)=\alpha f^*(x)$, then $f(x)$ is an introspect polynomial. On the other hand, for any positive integer n with $\gcd(n,q)=1$, x^n-1 has the unique irreducible factorizations over $\mathbb{F}_q$ as follows:

$$x^n-1=f_1(x)\cdots f_k(x)h_1(x)h_1^*(x)\cdots h_l(x)h_l^*(x),\tag{$*$}$$

where $f_i(x)$ $(1\le i\le k)$ is irreducible introspect and $h_j(x)$ $(1\le j\le l)$ is irreducible over $\mathbb{F}_q$ (cf. [8, 11]). Based on this, the explicit enumerating formula for the number of non-trivial self-orthogonal cyclic codes over the ring $Z_{p_1p_2\cdots p_t}$ is obtained. And then there is no self-dual cyclic code with any length over $Z_{p_1p_2\cdots p_t}$ when $t\ge 2$.

Theorem 1.3 *Let $t\ge 2$ be an integer, $p_1,p_2,\cdots,p_t$ be distinct primes. Suppose that $n=p_i^{r_i}n_i$ with $\gcd(n_i,p_i)=1$ $(1\le i\le t)$ and $x^{n_i}-1$ has the unique irreducible factorizations over $\mathbb{F}_{p_i}$ as follows*:

$$x^{n_i}-1=f_{1_i}(x)\cdots f_{k_i}(x)h_{1_i}(x)h_{1_i}^*(x)\cdots h_{l_i}(x)h_{l_i}^*(x).$$

Set

$$S_i=\{d_i:d_i\mid n,d_i>2,2\mid \mathrm{ord}_{d_i}(p_i),d_i\mid (p_i^{\frac{\mathrm{ord}_{d_i}(p_i)}{2}}+1)\},$$

then

$$k_i=\frac{3+(-1)^n}{2}+\sum_{d_i\in S_i}\frac{\varphi(d_i)}{\mathrm{ord}_{d_i}(p_i)},\quad l_i=\frac{1}{2}\sum_{d_i\mid n}\frac{\varphi(d_i)}{\mathrm{ord}_{d_i}(p_i)}-\frac{k_i}{2},\quad i=1,2,\cdots,t,$$

and the number of non-trivial self-orthogonal cyclic codes with length n over $Z_{p_1p_2\cdots p_t}$ is

$$N(n,p_1p_2\cdots p_t)=\prod_{i=1}^{t}\Big(\Big[\frac{p_i^{r_i}}{2}+1\Big]\Big)^{k_i}\Big(\frac{(p_i^{r_i}+1)(p_i^{r_i}+2)}{2}\Big)^{l_i}-1,$$

where $[\cdot]$ is the Gauss function.

Theorem 1.4 *Let $t\ge 2$ be an integer, $p_1,p_2,\cdots,p_t$ be distinct primes. Then there is no self-dual cyclic code with any length over $Z_{p_1p_2\cdots p_t}$.*

2 Preliminaries

Some preliminaries are needed before proving our main results. Let q be a power of the prime p, n be a positive integer, and $\mathrm{ord}_n(q)$ be the order of q modulo n. Without loss of generality, set $\mathrm{ord}_1(q)=1$. For convenience, all rings in this paper have identities.

Definition 2.1 (cf. [9]) *Let $R_1, R_2, \cdots, R_t$ be rings and*

$$R = \bigoplus_{i=1}^{t} R_i = \{(a_1, a_2, \cdots, a_t) \mid a_i \in R_i, i = 1, 2, \cdots, t\}.$$

For $(a_1, a_2, \cdots, a_t), (b_1, b_2, \cdots, b_t) \in R$, define two operations "$+$" and "$*$" over R as follows:

$$\begin{aligned}(a_1, a_2, \cdots, a_t) + (b_1, b_2, \cdots, b_t) &= (a_1 + b_1, a_2 + b_2, \cdots, a_t + b_t),\\ (a_1, a_2, \cdots, a_t) * (b_1, b_2, \cdots, b_t) &= (a_1 b_1, a_2 b_2, \cdots, a_t b_t),\end{aligned}$$

easily to see that $(R, +, *)$ is a ring and called to be the direct sum of R_i $(i = 1, 2, \cdots, t)$.

Proposition 2.1 (cf. [9])

(1) *Let Z be the integer ring and $m \in N^+$, then $Z/\langle m\rangle \cong Z_m$.*

(2) *Let $\theta : R \to T$ be a ring homomorphism, then θ is a monomorphism if and only if $\ker(\theta) = 0$, where $\ker(\theta) = \{a \in R \mid \theta(a) = 0\}$.*

(3) *Let R be a commutative ring, and I_i $(i = 1, 2, \cdots, t)$ be pairwise coprime ideals of R. If $I = \bigcap\limits_{i=1}^{t} I_i$, then there is a ring isomorphism $R/I \cong \prod\limits_{i=1}^{n} R/I_i$.*

Proposition 2.2 (cf. [11]) *Let $n \in Z^+$ and q be a power of the prime p.*

(1) *If $\gcd(n, q) \neq 1$, then there exists a non-trivial self-orthogonal cyclic code with length n.*

(2) *If $\gcd(n, q) = 1$, then there exists a non-trivial self-orthogonal cyclic code with length n if and only if $n > 2$, there exists a positive divisor $d \geq 3$ of n and one of the following is true:*

(1°) $2 \nmid \mathrm{ord}_d(q)$;

(2°) *if $2 \mid \mathrm{ord}_d(q)$, then $d \nmid (q^{\frac{\mathrm{ord}_d(q)}{2}} + 1)$.*

Proposition 2.3 (cf. [11]) *Let $n \in Z^+$, q be a power of the prime p with $\gcd(n, p) = 1$. Then there exists a non-trivial self-orthogonal cyclic code with length n over $\mathbb{F}_q$ if and only if $n > 2$ and one of the following is true:*

(1) $2 \nmid \mathrm{ord}_n(q)$;

(2) *if $2 \mid \mathrm{ord}_n(q)$, then $n \nmid (q^{\frac{\mathrm{ord}_n(q)}{2}} + 1)$.*

Proposition 2.4 (cf. [11]) *Let $n \in Z^+, q$ be a power of the prime p with $\gcd(n, p) = 1$, and $\varphi(n)$ be the Euler function of n. If $x^n - 1 \in \mathbb{F}_q[x]$ has the factorizations as $(*)$, and*

$$S = \{d : d \mid n, d > 2, 2 \mid \mathrm{ord}_d(q), d \mid (q^{\frac{\mathrm{ord}_d(q)}{2}} + 1)\},$$

then

$$k = \frac{3 + (-1)^n}{2} + \sum_{d \in S} \frac{\varphi(d)}{\mathrm{ord}_d(q)}, \quad l = \frac{P(n, q) - k}{2},$$

and the number of irreducible factors for $x^n - 1$ over $\mathbb{F}_q$ is

$$P(n, q) = k + 2l = \sum_{d \mid n} \frac{\varphi(d)}{\mathrm{ord}_d(q)}.$$

Proposition 2.5 (cf. [8]) *Let $n \in Z^+$, q be a power of the prime p, and $x^n - 1 = g(x)h(x)$ with $g(x), h(x) \in \mathbb{F}_q[x]$. Then the cyclic code $\mathcal{C} = (g(x))$ with length n over $\mathbb{F}_q$ is self-orthogonal if and only if $h^*(x) \mid g(x)$, i.e., $g(x) = m(x)h^*(x), x^n - 1 = m(x)h(x)h^*(x)$, where $h^*(x)$ is the reverse polynomial of $h(x)$.*

Proposition 2.6 (cf. [11]) *Let p be a prime and $n = p^r n_0$ with $\gcd(n_0, p) = 1$. Suppose q is a power of the prime p, and $x^{n_0} - 1 \in \mathbb{F}_q[x]$ has the unique irreducible factorizations over $\mathbb{F}_q$ as follows*:

$$x^{n_0} - 1 = f_1(x)\cdots f_k(x)h_1(x)h_1^*(x)\cdots h_l(x)h_l^*(x).$$

Then the number of non-trivial self-orthogonal cyclic codes with length n over $\mathbb{F}_q$ is

$$N(n,q) = \Big(\Big[\frac{p^r}{2}+1\Big]\Big)^k\Big(\frac{(p^r+1)(p^r+2)}{2}\Big)^l - 1.$$

Proposition 2.7 (cf. [11]) *Let q be a power of the prime p. Suppose that there exists a self-dual cyclic code $\mathcal{C}$ with length n over $\mathbb{F}_q$, then $2 \mid \gcd(n,q)$.*

The following two lemmas are important to prove our main results.

Lemma 2.1 *Let t be a positive integer, $R, R_1, \cdots, R_t$ be commutative rings with identities. If there is a ring isomorphism between R and $\bigoplus\limits_{i=1}^{t} R_i$, then there is a polynomial ring isomorphism $R[x] \cong \bigoplus\limits_{i=1}^{t} R_i[x]$.*

Proof Let $\varphi : R \to \bigoplus\limits_{i=1}^{t} R_i$ be a ring isomorphism with $\varphi(a_j) = (a_{1j}, a_{2j}, \cdots, a_{tj})$, where $a_j \in R, a_{ij} \in R_i$ $(i = 1, 2, \cdots, t)$. Define the map φ' :

$$R[x] \to R_1[x] \oplus R_2[x] \oplus \cdots \oplus R_t[x],$$
$$\sum_j a_jx^j \mapsto \Big(\sum_j a_{1j}x^j, \sum_j a_{2j}x^j, \cdots, \sum_j a_{tj}x^j\Big),$$

i.e., $\varphi'\big(\sum\limits_j a_jx^j\big) = \sum\limits_j \varphi(a_j)x^j$, it's easy to show that φ' is bijective. Since φ is a ring isomorphism, thus for any $\sum\limits_j a_jx^j, \sum\limits_j b_jx^j \in R[x]$, we have

$$\begin{aligned}\varphi'\Big(\sum_j a_jx^j + \sum_j b_jx^j\Big) &= \varphi'\Big(\sum_j (a_j+b_j)x^j\Big) = \sum_j \varphi(a_j+b_j)x^j \\ &= \sum_j(\varphi(a_j)+\varphi(b_j))x^j = \sum_j \varphi(a_j)x^j + \sum_j \varphi(b_j)x^j \\ &= \varphi'\Big(\sum_j a_jx^j\Big) + \varphi'\Big(\sum_j b_jx^j\Big)\end{aligned}$$

and

$$\begin{aligned}\varphi'\Big(\sum_j a_jx^j \sum_j b_jx^j\Big) &= \varphi'\Big(\sum_l \Big(\sum_{j+k=l} a_jb_k\Big)x^l\Big) = \sum_l \varphi\Big(\sum_{j+k=l} a_jb_k\Big)x^l \\ &= \sum_j \varphi(a_j)x^j * \sum_j \varphi(b_j)x^j = \varphi'\Big(\sum_j a_jx^j\Big) * \varphi'\Big(\sum_j b_jx^j\Big),\end{aligned}$$

this means that φ' is a ring homomorphism.

Thus we complete the proof of Lemma 2.1.

Lemma 2.2 *Let $R, R_1, \cdots, R_t$ be commutative rings, and ϕ be a ring isomorphism between R and $\bigoplus\limits_{i=1}^{t} R_i$. If I is an ideal of R, i.e., $I \lhd R$, and $J = \phi(I)$, then we have*

(1) $J \lhd \bigoplus_{i=1}^{t} R_i$ *and* $J = \bigoplus_{i=1}^{t} I_i$, *where*

$$I_i = \{r_i \in R_i \mid (0, \cdots, r_i, \cdots, 0) \in J\} \lhd R_i \ (i = 1, 2, \cdots, t);$$

(2) $R/I \cong \bigoplus_{i=1}^{t} R_i/I_i$.

Proof (1) Since ϕ is a ring isomorphism between R and $\bigoplus_{i=1}^{t} R_i$ and $I \lhd R$, thus $J = \phi(I) \lhd \bigoplus_{i=1}^{t} R_i$. Furthermore, for $(r_1, r_2, \cdots, r_t) \in J$, we have

$$(0, 0, \cdots, r_i, 0, \cdots, 0) = (0, 0, \cdots, 1, 0, \cdots, 0) * (r_1, r_2, \cdots, r_t) \in J,$$

namely, $r_i \in I_i$ $(i = 1, 2, \cdots, t)$, and then $(r_1, r_2, \cdots, r_t) \in \bigoplus_{i=1}^{t} I_i$, i.e., $J \subseteq \bigoplus_{i=1}^{t} I_i$. On the other hand, for $(r_1, r_2, \cdots, r_t) \in \bigoplus_{i=1}^{t} I_i$, we can get $\bigoplus_{i=1}^{t} I_i \subseteq J$ by

$$(r_1, r_2, \cdots, r_t) = \sum_{i=1}^{t} (0, 0, \cdots, r_i, 0, \cdots, 0) \in J.$$

Hence $J = \bigoplus_{i=1}^{t} I_i$.

Note that for any $i = 1, 2, \cdots, t$, from $0 \in I_i$ we know that I_i is not empty. Now for $a, b \in I_i$, from the definition of I_i, we have

$$(0, 0, \cdots, a, \cdots, 0), (0, 0, \cdots, b, \cdots, 0) \in J.$$

Since J is an ideal of $\bigoplus_{i=1}^{t} R_i$, thus

$$(0, 0, \cdots, a, \cdots, 0) + (0, 0, \cdots, -b, \cdots, 0) = (0, 0, \cdots, a - b, \cdots, 0) \in J,$$

which means that $a - b \in I_i$. Secondly, for any $r_i \in R_i$ $(i = 1, 2, \cdots, t)$, we know that

$$(0, 0, \cdots, r_i, \cdots, 0) \in R_1 \oplus R_2 \oplus \cdots \oplus R_t.$$

Now from $J \lhd \bigoplus_{i=1}^{t} R_i$ we can get

$$(0, 0, \cdots, a, \cdots, 0) * (0, 0, \cdots, r_i, \cdots, 0) = (0, 0, \cdots, r_i a, \cdots, 0) \in J$$

and

$$(0, 0, \cdots, r_i, \cdots, 0) * (0, 0, \cdots, a, \cdots, 0) = (0, 0, \cdots, a r_i, \cdots, 0) \in J,$$

i.e., $ar_i, r_i a \in I_i$ $(1 \le i \le t)$. Hence $I_i \lhd R_i$ $(i = 1, 2, \cdots, t)$. Thus we complete the proof of (1).

(2) For any $r \in R$, denote $\phi(r) = (r_1, r_2, \cdots, r_t)$, where $r_i \in R_i$ $(1 \le i \le t)$. Now define a map ϕ' :

$$R/I \to \bigoplus_{i=1}^{t} R_i/I_i,$$

$$r+I \mapsto (r_1+I_1, r_2+I_2, \cdots, r_t+I_t).$$

Note that if $\phi'(r+I) = (0,0,\cdots,0)$, i.e.,

$$(r_1+I_1, r_2+I_2, \cdots, r_t+I_t) = (0,0,\cdots,0),$$

equivalently, $r_i \in I_i$ $(i=1,2,\cdots,t)$, then

$$\phi(r) = (r_1, r_2, \cdots, r_t) \in \bigoplus_{i=1}^{t} I_i = J = \phi(I),$$

which means that $r \in I$, i.e., $r+I=0$, thus from (2) of Proposition 2.1, ϕ' is injective.

Now for any $(r_1+I_1, r_2+I_2, \cdots, r_t+I_t) \in \bigoplus\limits_{i=1}^{t} R_i/I_i$, there exists some $r \in R$ such that $\phi(r) = (r_1, r_2, \cdots, r_t)$ since ϕ is an epimorphism, hence we can get

$$\phi'(r+I) = (r_1+I_1, r_2+I_2, \cdots, r_t+I_t) \in \bigoplus_{i=1}^{t} R_i/I_i,$$

i.e., ϕ' is an epimorphism.

Furthermore, for $s \in R$, set $\phi(s) = (s_1, s_2, \cdots, s_t)$ and $\phi(rs) = ((rs)_1, (rs)_2, \cdots, (rs)_t)$. Since ϕ is a ring isomorphism from R to $\bigoplus\limits_{i=1}^{t} R_i$, we have

$$\begin{aligned}((rs)_1, (rs)_2, \cdots, (rs)_t) &= \phi(rs) = \phi(r) * \phi(s)\\ &= (r_1, r_2, \cdots, r_t) * (s_1, s_2, \cdots, s_t)\\ &= (r_1s_1, r_2s_2, \cdots, r_ts_t). \qquad (3.1)\end{aligned}$$

Now for any $r+I, s+I \in R/I$, we have

$$\begin{aligned}\phi'((r+I)+(s+I)) &= \phi'(r+s+I) = (r_1+s_1+I_1, r_2+s_2+I_2, \cdots, r_t+s_t+I_t)\\ &= (r_1+I_1, r_2+I_2, \cdots, r_t+I_t) + (s_1+I_1, s_2+I_2, \cdots, s_t+I_t)\\ &= \phi'(r+I) + \phi'(s+I) \qquad (3.2)\end{aligned}$$

and

$$\begin{aligned}\phi'((r+I)(s+I)) &= \phi'(rs+I)\\ &= ((rs)_1+I_1, (rs)_2+I_2, \cdots, (rs)_t+I_t). \qquad (3.3)\end{aligned}$$

From (3.1) and (3.3), we know that

$$\begin{aligned}\phi'((r+I)(s+I)) &= (r_1+I_1, r_2+I_2, \cdots, r_t+I_t) * (s_1+I_1, s_2+I_2, \cdots, s_t+I_t)\\ &= \phi'(r+I) * \phi'(s+I).\end{aligned}$$

This means that ϕ' is a ring homomorphism.

From the above, ϕ' is a ring isomorphism from R/I to $\bigoplus\limits_{i=1}^{t} R_i/I_i$. This completes the proof of (2).

3 The Proofs of Our Main Results

In this section, we give the proofs of the main results.

Proof of Theorem 1.1 (1) Since $p_1, p_2, \cdots, p_t$ are distinct primes, $\langle p_i \rangle$ $(i = 1, 2, \cdots, t)$ are pairwise coprime ideals of Z. From (1) and (3) of Proposition 2.1 and Lemma 2.1, we can get the following two ring isomorphisms:

$$\begin{aligned}&\varphi : Z_{p_1p_2\cdots p_t} \cong Z_{p_1} \oplus Z_{p_2} \oplus \cdots \oplus Z_{p_t},\\ &a_j \mapsto (a_{1j}, a_{2j}, \cdots, a_{tj}), \text{where } a_j \equiv a_{ij} (\text{mod } p_i)\end{aligned}$$

and

$$\begin{aligned}&\varphi' : Z_{p_1p_2\cdots p_t}[x] \cong Z_{p_1}[x] \oplus Z_{p_2}[x] \oplus \cdots \oplus Z_{p_t}[x],\\ &\sum_j a_jx^j \mapsto \Big(\sum_j a_{1j}x^j, \sum_j a_{2j}x^j, \cdots, \sum_j a_{tj}x^j\Big),\end{aligned}$$

hence $\varphi'\big(\sum\limits_j a_jx^j\big) = \sum\limits_j \varphi(a_j)x^j$.

For any ideal $I = \langle x^n - \lambda \rangle \lhd Z_{p_1p_2\cdots p_t}[x]$, from $\lambda_i \equiv \lambda (\text{mod } p_i)$ and the definitions of both φ and φ', we know that

$$\begin{aligned}\varphi'(I) &= \varphi'(\langle x^n - \lambda \rangle) = \langle \varphi'(x^n - \lambda) \rangle\\ &= \langle (x^n - \lambda_1), (x^n - \lambda_2), \cdots, (x^n - \lambda_t) \rangle\\ &= \bigoplus_{i=1}^{t} \langle x^n - \lambda_i \rangle.\end{aligned}$$

Thus by Lemma 2.2 we have

$$Z_{p_1p_2\cdots p_t}[x]/\langle x^n - \lambda \rangle \cong \bigoplus_{i=1}^{t} Z_{p_i}[x]/\langle x^n - \lambda_i \rangle,$$

which means that $I' \lhd Z_{p_1p_2\cdots p_t}[x]/\langle x^n - \lambda \rangle$ if and only if $I'_i \lhd Z_{p_i}[x]/\langle x^n - \lambda_i \rangle$ $(i = 1, 2, \cdots, t)$ and $I' \cong \bigoplus\limits_{i=1}^{t} I'_i$. Now by Proposition 1.1, we immediately have (1).

(2) By taking $\lambda = 1$ in (1), we can get (2).

(3) By Proposition 1.1, there exists a ring isomorphism

$$\tau :\ Z_{p_1p_2\cdots p_t}[x]/\langle x^n - 1 \rangle \cong \bigoplus_{i=1}^{t} Z_{p_i}[x]/\langle x^n - 1 \rangle$$

such that for any $\mathcal{C} \lhd Z_{p_1p_2\cdots p_t}[x]/\langle x^n - 1 \rangle$, there exists $\mathcal{C}_i \lhd Z_{p_i}[x]/\langle x^n - 1 \rangle$ $(i = 1, 2, \cdots, t)$ (i.e., $\mathcal{C}_i \subseteq Z_{p_i}^n$ is a cyclic code) such that $\tau(\mathcal{C}) = (\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_t)$. Note that $\mathcal{C}$ is an ideal and then $\mathcal{C}$ is a cyclic code over $Z_{p_1p_2\cdots p_t}$. Thus by Proposition 1.2, the dual code $\mathcal{C}^\perp$ is also a cyclic code over $Z_{p_1p_2\cdots p_t}$. Hence, from (1)–(2) of Theorem 1.1 there exist some cyclic codes $\mathcal{D}_i$ over Z_{p_i} $(i = 1, 2, \cdots, t)$ such that

$$\tau(\mathcal{C}^\perp) = (\mathcal{D}_1, \mathcal{D}_2, \cdots, \mathcal{D}_t).$$

Now, for any $c_i \in \mathcal{C}_i$ and $d_i \in \mathcal{D}_i$ $(i = 1, 2, \cdots, t)$, we have

$$c = (c_1, c_2, \cdots, c_t) \in (\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_t) = \tau(\mathcal{C}),$$

$$d=(d_1,d_2,\cdots,d_t)\in(\mathcal{D}_1,\mathcal{D}_2,\cdots,\mathcal{D}_t)=\tau(\mathcal{C}^{\perp}).$$

Note that τ is an isomorphism and so τ^{-1} is also an isomorphism. Thus $\tau^{-1}(c)\in\mathcal{C}$ and $\tau^{-1}(d)\in\mathcal{C}^{\perp}$, namely, $\tau^{-1}(c)\tau^{-1}(d)=0$. While τ^{-1} is an isomorphism, hence

$$\begin{aligned}0&=\tau^{-1}(c)\tau^{-1}(d)=\tau^{-1}(c*d)\\&=\tau^{-1}((c_1,c_2,\cdots,c_t)*(d_1,d_2,\cdots,d_t))\\&=\tau^{-1}(c_1d_1,c_2d_2,\cdots,c_td_t),\end{aligned}$$

i.e., $c_id_i=0$ $(1\le i\le t)$, this means that $\mathcal{D}_i\subseteq\mathcal{C}_i^{\perp}$ $(i=1,2,\cdots,t)$.

On the other hand, for any $c_i'\in\mathcal{C}_i^{\perp}$ $(i=1,2,\cdots,t)$, i.e., $c_ic_i'=0$. By (1)–(2) of Theorem 1.1, there exist some $c_i\in\mathcal{C}_i$ $(i=1,2,\cdots,t)$ and $c'\in\tau^{-1}(\mathcal{C}_1^{\perp},\mathcal{C}_2^{\perp},\cdots,\mathcal{C}_t^{\perp})$ such that

$$\tau(c)=(c_1,c_2,\cdots,c_t)\in(\mathcal{C}_1,\mathcal{C}_2,\cdots,\mathcal{C}_t),\quad \tau(c')=(c_1',c_2',\cdots,c_t')\in(\mathcal{C}_1^{\perp},\mathcal{C}_2^{\perp},\cdots,\mathcal{C}_t^{\perp}).$$

Thus

$$\tau(c)*\tau(c')=(c_1,c_2,\cdots,c_t)*(c_1',c_2',\cdots,c_t')=(0,0,\cdots,0).$$

Hence from $c_ic_i'=0$ $(1\le i\le t)$ and τ^{-1} is an isomorphism, we have

$$\begin{aligned}cc'&=\tau^{-1}(c_1,c_2,\cdots,c_t)\tau^{-1}(c_1',c_2',\cdots,c_t')=\tau^{-1}((c_1,c_2,\cdots,c_t)*(c_1',c_2',\cdots,c_t'))\\&=\tau^{-1}(c_1c_1',c_2c_2',\cdots,c_tc_t')=\tau^{-1}(0,0,\cdots,0)=0,\end{aligned}$$

i.e., $c'\in\mathcal{C}^{\perp}$. Now from $\tau(\mathcal{C}^{\perp})=(\mathcal{D}_1,\mathcal{D}_2,\cdots,\mathcal{D}_t)$, we know that

$$\tau(c')=(c_1',c_2',\cdots,c_t')\in(\mathcal{D}_1,\mathcal{D}_2,\cdots,\mathcal{D}_t),$$

i.e., $c_i'\in\mathcal{D}_i$ $(i=1,2,\cdots,t)$, thus $\mathcal{C}_i^{\perp}\subseteq\mathcal{D}_i$ $(i=1,2,\cdots,t)$.

Therefore $\mathcal{C}_i^{\perp}=\mathcal{D}_i$ $(i=1,2,\cdots,t)$, i.e.,

$$\tau(\mathcal{C}^{\perp})=(\mathcal{C}_1^{\perp},\mathcal{C}_2^{\perp},\cdots,\mathcal{C}_t^{\perp}).\tag{3.4}$$

Thus from τ is an isomorphism and (3.4), we can obtain:

$$\begin{aligned}\mathcal{C}\text{ is a self-orthogonal cyclic code}&\Leftrightarrow\mathcal{C}\subseteq\mathcal{C}^{\perp}\Leftrightarrow\tau(\mathcal{C})\subseteq\tau(\mathcal{C}^{\perp})\\&\Leftrightarrow(\mathcal{C}_1,\mathcal{C}_2,\cdots,\mathcal{C}_t)\subseteq(\mathcal{C}_1^{\perp},\mathcal{C}_2^{\perp},\cdots,\mathcal{C}_t^{\perp})\\&\Leftrightarrow\mathcal{C}_i\subseteq\mathcal{C}_i^{\perp}\ (i=1,2,\cdots,t)\\&\Leftrightarrow\forall i=1,2,\cdots,t,\ \mathcal{C}_i\text{ is a self-orthogonal cyclic code.}\end{aligned}$$

In particular, $\mathcal{C}$ is self-dual, i.e., $\mathcal{C}=\mathcal{C}^{\perp}$ if and only if for any $i=1,2,\cdots,t,\ \mathcal{C}_i=\mathcal{C}_i^{\perp}$, i.e., $\mathcal{C}_i$ is self-dual.

This completes the proof of (3).

Proof of Theorem 1.2 By Theorem 1.1 we know that $\mathcal{C}$ is a self-orthogonal cyclic code over $Z_{p_1p_2\cdots p_t}$ if and only if there exist self-orthogonal cyclic codes $\mathcal{C}_i$ over Z_{p_i} $(i=1,2,\cdots,t)$ such that $\mathcal{C}\cong\bigoplus_{i=1}^{t}\mathcal{C}_i$. Note that, $\mathcal{C}=\{0\}$ if and only if $\mathcal{C}_i=\{0\}$ $(i=1,2,\cdots,t)$. Now by Theorem 1.1, $\mathcal{C}$ is non-trivial self-orthogonal if and only if there exist some $\mathcal{C}_i\subseteq Z_{p_i}^n$ $(i=1,2,\cdots,t)$ such that $\mathcal{C}_i$ is a non-trivial self-orthogonal cyclic code. By Propositions 2.2–2.3, this is equivalent to that there exist some p_i $(i=1,2,\cdots,t)$ such that one of the following conditions is true.

(1) $\gcd(n,p_i)\neq1$;

(2) If $\gcd(n, p_i) = 1$, then $2 \nmid \mathrm{ord}_n(p_i)$;
(3) If $\gcd(n, p_i) = 1$ and $2 \mid \mathrm{ord}_n(p_i)$, then $n \nmid (q^{\frac{\mathrm{ord}_n(p_i)}{2}} + 1)$.
This completes the proof of Theorem 1.2.

Proof of Theorem 1.3 Note that for any $i = 1, 2, \cdots, t$, Z_{p_i} is a finite field since p_i $(1 \leq i \leq t)$ is a prime. Thus by Proposition 2.6, the number of non-trivial self-orthogonal cyclic codes with length n over Z_{p_i} is

$$N(n, p_i) = \Big(\Big[\frac{p_i^{r_i}}{2} + 1\Big]\Big)^{k_i} \Big(\frac{(p_i^{r_i} + 1)(p_i^{r_i} + 2)}{2}\Big)^{l_i} - 1, \quad i = 1, 2, \cdots, t.$$

Now from (3) of Lemma 2.1, the number of self-orthogonal cyclic codes with length n over $Z_{p_1 p_2 \cdots p_t}$ is

$$\prod_{i=1}^{t} \Big(\Big[\frac{p_i^{r_i}}{2} + 1\Big]\Big)^{k_i} \Big(\frac{(p_i^{r_i} + 1)(p_i^{r_i} + 2)}{2}\Big)^{l_i}.$$

Note that $\mathcal{C} = \{0\}$ if and only if $\mathcal{C}_i = \{0\}$ $(i = 1, 2, \cdots, t)$, thus from Theorem 1.2 and Proposition 2.6, we immediately have Theorem 1.3.

Proof of Theorem 1.4 From (3) of Theorem 1.1, there exists a self-dual cyclic code with length n over $Z_{p_1 p_2 \cdots p_t}$ if and only if for any $i = 1, 2, \cdots, t$, there exists a self-dual cyclic code with length n over Z_{p_i}. Note that $t \geq 2$ is an integer and $p_1, p_2, \cdots, p_t$ are distinct primes, hence there is no self-dual cyclic code over $Z_{p_1 p_2 \cdots p_t}$ by Proposition 2.7.

4 Examples

In this section, by using elementary methods and techniques, one can get the number of non-trivial self-orthogonal cyclic codes over $Z_{p_1 p_2 \cdots p_t}$ basing on Theorem 1.3.

Example 4.1 For $n = 10 = 2 \times 5$, we have $\gcd(10, 3) = 1$. Then by Theorem 1.1, we know that there exists a self-orthogonal cyclic code $\mathcal{C}$ over Z_6 if and only if there exists a self-orthogonal cyclic code $\mathcal{C}_1$ over Z_2 and a self-orthogonal cyclic code $\mathcal{C}_2$ over Z_3, such that $\mathcal{C} \cong \mathcal{C}_1 \oplus \mathcal{C}_2$.

Note that $\mathrm{ord}_5(2) = 4, \mathrm{ord}_2(3) = 1, \mathrm{ord}_5(3) = 4$ and $\mathrm{ord}_{10}(3) = 4$, then by Theorem 1.3, we have $k_1 = 2, k_2 = 4, l_1 = 0$ and $l_2 = 0$. Thus the number of non-trivial self-orthogonal cyclic codes over Z_6 is

$$\begin{aligned} N(10, 6) &= \Big(\Big[\frac{2^{r_1}}{2} + 1\Big]\Big)^{k_1} \Big(\frac{(2^{r_1} + 1)(2^{r_1} + 2)}{2}\Big)^{l_1} \Big(\Big[\frac{3^{r_2}}{2} + 1\Big]\Big)^{k_2} \Big(\frac{(3^{r_2} + 1)(3^{r_2} + 2)}{2}\Big)^{l_2} - 1 \\ &= \Big(\Big[\frac{2^1}{2} + 1\Big]\Big)^{2} \Big(\frac{(2^1 + 1)(2^1 + 2)}{2}\Big)^{0} \Big(\Big[\frac{3^0}{2} + 1\Big]\Big)^{4} \Big(\frac{(3^0 + 1)(3^0 + 2)}{2}\Big)^{0} - 1 \\ &= 4 - 1 = 3. \end{aligned}$$

Furthermore, by Theorem 1.4, there doesn't exist any self-dual cyclic code over Z_6.

On the other hand, the canonical decomposition of $x^{10} - 1$ over Z_2 is

$$x^{10} - 1 = (x + 1)^2 (x^4 + x^3 + x^2 + x + 1)^2.$$

And the canonical decomposition of $x^{10} - 1$ over Z_3 is

$$x^{10} - 1 = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x - 1).$$

Now set

$$\begin{aligned} g_{11} &= (x+1)(x^4+x^3+x^2+x+1) = x^5+1, \\ g_{12} &= (x+1)^2(x^4+x^3+x^2+x+1) = x^6+x^5+x+1, \end{aligned}$$

and

$$g_{13} = (x+1)(x^4+x^3+x^2+x+1)^2 = x^9+x^8+x^7+x^6+x^5+x^4+x^3+x^2+x+1.$$

Then by Proposition 2.5, $\mathcal{C}_{11} = \langle g_{11}\rangle, \mathcal{C}_{12} = \langle g_{12}\rangle$ and $\mathcal{C}_{13} = \langle g_{13}\rangle$ are non-trivial self-orthogonal cyclic codes over Z_2 and there doesn't exist any non-trivial self-orthogonal cyclic code over Z_3. Thus by Theorem 1.1, there are three non-trivial self-orthogonal cyclic codes over Z_6 as follows:

$$\begin{aligned} &\mathcal{C}^1 = \langle 4x^{10}+3x^5-1\rangle \cong \mathcal{C}_{11} \oplus \{0\}, \\ &\mathcal{C}^2 = \langle 4x^{10}+3x^6+3x^5+3x-1\rangle \cong \mathcal{C}_{12} \oplus \{0\}, \\ &\mathcal{C}^3 = \langle 4x^{10}+3x^9+3x^8+3x^7+3x^6+3x^5+3x^4+3x^3+3x^2+3x-1\rangle \cong \mathcal{C}_{13} \oplus \{0\}, \end{aligned}$$

which are not self-dual cyclic.

Example 4.2 For $n = 9 = 3^2$, we have $\gcd(9,5) = 1$. Now by Theorem 1.1, we know that there exists a self-orthogonal cyclic code $\mathcal{C}$ over Z_{15} if and only if there exists a self-orthogonal cyclic code $\mathcal{C}_1$ over Z_3 and a self-orthogonal cyclic code $\mathcal{C}_2$ over Z_5, such that $\mathcal{C} \cong \mathcal{C}_1 \oplus \mathcal{C}_2$.

Note that $\mathrm{ord}_3(5) = 2$ and $\mathrm{ord}_9(5) = 6$, then by Theorem 1.3, we have

$$k_1 = 1, \quad k_2 = 3, \quad l_1 = 0, \quad l_2 = 0, \quad r_1 = 2, \quad r_2 = 0.$$

Thus the number of non-trivial self-orthogonal cyclic codes over Z_{15} is

$$\begin{aligned} N(9,15) &= \Big(\Big[\frac{3^{r_1}}{2}+1\Big]\Big)^{k_1}\Big(\frac{(3^{r_1}+1)(3^{r_1}+2)}{2}\Big)^{l_1}\Big(\Big[\frac{5^{r_2}}{2}+1\Big]\Big)^{k_2}\Big(\frac{(5^{r_2}+1)(5^{r_2}+2)}{2}\Big)^{l_2} - 1 \\ &= \Big(\Big[\frac{3^1}{1}+1\Big]\Big)^1\Big(\frac{(3^1+1)(3^1+2)}{2}\Big)^0\Big(\Big[\frac{5^0}{2}+1\Big]\Big)^3\Big(\frac{(5^0+1)(5^0+2)}{2}\Big)^1 - 1 \\ &= 5-1 = 4. \end{aligned}$$

Furthermore, by Theorem 1.4, there doesn't exist any self-dual cyclic code over Z_{15}.

On the other hand, the canonical decomposition of x^9-1 over Z_5 is

$$x^9-1 = (x+1)(x^2+x+1)(x^6+x^3+1).$$

Now set

$$\begin{aligned} g_{11} &= (x+2)^5 = x^5+x^4+x^3+2x^2+2x+2, \\ g_{12} &= (x+2)^6 = x^6+x^3+1, \\ g_{13} &= (x+2)^7 = x^7+2x^6+x^{4+2x^3+x+2}, \\ g_{14} &= (x+2)^8 = x^7+x^6+x^5+x^4+x^3+x^2+x+1. \end{aligned}$$

Then by Proposition 2.5, $\mathcal{C}_{11} = \langle g_{11}\rangle, \mathcal{C}_{12} = \langle g_{12}\rangle, \mathcal{C}_{13} = \langle g_{13}\rangle$ and $\mathcal{C}_{14} = \langle g_{14}\rangle$ are non-trivial self-orthogonal cyclic codes over Z_3 and there doesn't exist any non-trivial self-orthogonal cyclic code over Z_5. Thus by Theorem 1.1, there are eight non-trivial self-orthogonal cyclic codes over Z_{15} as follows:

$$\mathcal{C}^1 = \langle 6x^9+10x^5+10x^4+10x^3+5x^2+5x-1\rangle \cong \mathcal{C}_{11} \oplus \{0\},$$

$$\mathcal{C}^2 = \langle 6x^9 + 10x^6 + 10x^3 + 4\rangle \cong \mathcal{C}_{12} \oplus \{0\},$$
$$\mathcal{C}^3 = \langle 6x^9 + 10x^7 + 5x^6 + 10x^4 + 5x^3 + 10x - 1\rangle \cong \mathcal{C}_{13} \oplus \{0\},$$
$$\mathcal{C}^4 = \left\langle 6x^9 + 10\sum_{i=1}^{8} x^i + 4\right\rangle \cong \mathcal{C}_{14} \oplus \{0\},$$

which are not self-dual cyclic.

5 Conclusion

It's well-known that the polynomial ring $Z_{p_1p_2\cdots p_t}[x]$ is not a unique factorization domain. Hence to study constacyclic codes over $R = Z_{p_1p_2\cdots p_t}$ is difficult basing on polynomial factorizations. By constructing an isomorphic between R and Z_{p_i} $(i = 1, 2, \cdots, t)$, to study constacyclic codes over R is reduced to study the corresponding constacyclic codes over finite fields Z_{p_i}, which is much easier. Based on this, the present paper studies constacyclic codes over $Z_{p_1p_2\cdots p_t}$ and obtains some good results.

References

[1] Berlekamp, E. R., Negacyclic Codes for the Lee Metric, Combinatorial Mathematics and Its Applications Proc. Conference, North Carolina Press, Chapel Hill, N.C., 1967.

[2] Blackford, T., Negacyclic codes over Z_4 of even length, *IEEE Trans. Inform. Theory,* 2003, **49**(6), 1417–1424.

[3] Cao, Y. L., On constacyclic codes over finite chain rings, *Finite Fields and Their Applications,* 2013, **24**, 124–135.

[4] Dinh, H. Q., Constacyclic codes of length p^s over $F_{p^m} + uF_{p^m}$, *Journal of Algebra,* 2010, **324**(5), 940–950.

[5] Dinh, H. Q., Wang, L. Q. and Zhu, S. X., Negacyclic codes of length $2p^s$ over $F_{p^m} + uF_{p^m}$, *Finite Fields and Their Applications,* 2015, **31**, 178–201.

[6] Garrett, P., The Mathematics of Coding Theory, China Machine Press, Beijing, 2005.

[7] Hammons, R., Kumar, P. V., Calderbank, A. R., et al., The Z_4-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory,* 1994, **40**(2), 301–319.

[8] Huffman, W. C. and Pless, V., Fundamentals of Error-Correcting Codes, Cambridge University Press, New York, 2003.

[9] Jacobson, N., Basic Algebra I, W. H. Freeman and Company, New York, 1985.

[10] Jia, Y., Ling, S. and Xing, C. P., On self-dual cyclic codes over finite fields, *IEEE Trans. Inform. Theory,* 2011, **57**(4), 2243–2251.

[11] Liao, Q. Y., Li, Y. B. and Liao, H., The existence for self-orthogonal cyclic codes over finite fields, *Acta Mathematica Sinica,* 2014, **57**(1), 117–124.

[12] Nechaev, A. A., Kerdock code in a cyclic form, *Discrete Mathematics and Applications,* 1991, **1**(4), 365–384.

[13] Pan, C. D. and Pan, C. B., Elementary Number Theory, Peking University Press, Beijing, 1992.

[14] Prange, E., Cyclic Error-Correcting Codes in Two Symbols, Air Force Cambridge Research Center, Cambridge, 1957.

[15] Zhu, S. X. and Kai, X. S., Dual and self-dual negacyclic codes of even length over Z_{2^a}, *Discrete Mathematics,* 2009, **309**(8), 2382–2391.