The Structure of \( Z_p^r Z_p^s \) – Cyclic Codes

Xuedong Dong\(^1\), a

\(^1\)College of Information Engineering, Dalian University, Dalian 116622, P.R.China

aemail: dongxuedong@sina.com

Keywords: Linear Code; Cyclic code; Finite ring

Abstract. A code \( C \) is a \( Z_2 Z_4 \) – cyclic code if and only if \( C \) is a \( Z_4[x] \)-submodule of the ring \( Z_2[x] / (x^n - 1) \times Z_4[x] / (x^n - 1) \). Perfect \( Z_2 Z_4 \) – additive codes have been utilized in the subject of steganography. The algebraic structure of \( Z_2 Z_4 \) – cyclic codes was determined in 2014. In this paper we determine the algebraic structure of \( Z_p^r Z_p^s \) – cyclic codes, where \( p \) is an odd prime. Any \( Z_p^r Z_p^s \) – cyclic code \( C \) can be generated by two elements and \( C \) is one of three types. The results obtained may have some promising applications.

Introduction

Cyclic codes have been considered to be one of the most important classes of error-correcting codes since 1950 [1]. Codes over finite rings have received much attention after it was proved that important families of binary non-linear codes are in fact images under a Gray map of linear codes over \( Z_4 \), where \( Z_4 = \{0,1,2,3\} \) is the ring of integers modulo 4, see [2] and the references cited there. Recently, a new class of error-correcting codes has emerged that generalizes binary linear codes and quaternary linear codes. This class of codes is called \( Z_p^r Z_p^s \) – additive codes [3],[4],[5],[6]. A \( Z_2 Z_4 \) – additive code \( C \) is defined to be a subgroup of the group \( Z_2^r \times Z_4^s \). Perfect \( Z_2 Z_4 \) – additive codes have been utilized in the subject of steganography [3]. Thus, this class of codes has some promising applications. In [6], the structure of \( Z_2 Z_4 \) – cyclic codes has been given. It is interesting to determine the structure of \( Z_p^r Z_p^s \) – cyclic codes, where \( Z_p^r Z_p^s \) – codes should be defined as a subgroup of the group \( Z_p^r \times Z_p^s \), and \( p \) is an odd prime. This short note gives a complete structure of \( Z_p^r Z_p^s \) – cyclic codes. The results show that a \( Z_p^r Z_p^s \) – cyclic code can be generated by at most two elements and these two elements satisfy some conditions. The rest of the paper is organized as follows. In Section 2, we give a brief preliminaries. In Section 3, the structure of \( Z_p^r Z_p^s \) – cyclic codes is obtained. Finally, summary is given in Section 4.

Preliminaries

Throughout this paper we assume that \( p \) is an odd prime, \( n,m \) are positive integers and \( (n,p) = (m,p) = 1 \).

Definition 1: A non-empty subset \( C \) of the group \( Z_p^r \times Z_p^s \) is called a \( Z_p^r Z_p^s \) – code if \( C \) is a subgroup of \( Z_p^r \times Z_p^s \).

Definition 2: A subset \( C \) of the group \( Z_p^r \times Z_p^s \) is called a \( Z_p^r Z_p^s \) – cyclic code if

1) \( C \) is a \( Z_p^r Z_p^s \) – code, and

2) For any codeword \( \tilde{u} = (a_0 a_1 \cdots a_{n-1}, b_0 b_1 \cdots b_{m-1}) \in C \), its cyclic shift
Definition 3: For any two elements \( \vec{u} = (a_0 a_1 \cdots a_{n-1}, b_0 b_1 \cdots b_{m-1}) \) and 
\( \vec{v} = (d_0 d_1 \cdots d_{n-1}, e_0 e_1 \cdots e_{m-1}) \), the inner product of \( \vec{u} \) and \( \vec{v} \) is defined as 
\[ \vec{u} \cdot \vec{v} = u = p(a_0 d_0 + a_1 d_1 + \cdots + a_{n-1} d_{n-1}) + b_0 e_0 + b_1 e_1 + \cdots + b_{m-1} e_{m-1} \mod p^2 \].

If \( C \) is a \( Z_p Z_p \)-code, then its dual is defined as 
\[ C^\perp = \{ \vec{v} | \vec{u} \cdot \vec{v} = 0, \forall \vec{u} \in C \} \).

**Theorem 1:** Let \( C \) be a \( Z_p Z_p \)-cyclic code, then its dual \( C^\perp \) is also a \( Z_p Z_p \)-cyclic code.

**Proof:** Let \( C \) be a \( Z_p Z_p \)-cyclic code. Then it is clear that \( C^\perp \) is a \( Z_p Z_p \)-code. It is sufficient to prove that any cyclic shift of an element in \( C^\perp \). For any 
\[ \vec{u} = (a_0 a_1 \cdots a_{n-1}, b_0 b_1 \cdots b_{m-1}) \in C \], then \( \vec{u} \cdot \vec{v} = 0 \). Let \( l = [m, n] \). Then \( T^l(\vec{u}) = \vec{u} \). Assume that 
\[ T^{-l}(\vec{u}) = (a_0 a_1 \cdots a_{n-1}, b_0 b_1 \cdots b_{m-1}) \in C \). It follows that \( T^{-l}(\vec{u}) \cdot \vec{v} = 0 \), that is, 
\[ 0 = T^{-l}(\vec{u}) \cdot \vec{v} = p(a_0 d_0 + a_1 d_1 + \cdots + a_{n-1} d_{n-1}) + b_0 e_0 + b_1 e_1 + \cdots + b_{m-1} e_{m-1} \mod p^2 \]. On the other hand, 
\[ \vec{u} \cdot T(\vec{v}) = p(a_0 d_0 + a_1 d_1 + \cdots + a_{n-1} d_{n-1}) + b_0 e_0 + b_1 e_1 + \cdots + b_{m-1} e_{m-1} \mod p^2 \]. It is clear that 
\[ \vec{u} \cdot T(\vec{v}) = T^{-l}(\vec{u}) \cdot \vec{v} = 0 \]. This shows that \( T(\vec{v}) \) is also in \( C^\perp \) and therefore \( C^\perp \) is also a \( Z_p Z_p \)-cyclic code. This completes the proof of the theorem.

As is common in the discussion of cyclic codes, an element \( \vec{u} = (a_0 a_1 \cdots a_{n-1}, b_0 b_1 \cdots b_{m-1}) \in C \) can be identified with an element consisting of two polynomials 
\[ c(x) = (a_0, a_1 x + \cdots + a_{n-1} x^{n-1}, b_0 + b_1 x + \cdots + b_{m-1} x^{m-1}) \]

in the finite ring \( R_{n,m} = Z_p[x]/(x^n - 1) \times Z_p[x]/(x^m - 1) \). Code words of a cyclic code \( C \) are regarded as vectors or as polynomials interchangeably. In either case, we use the same notation \( C \) to denote the set of all code words. We follow this convention in the rest of the paper.

**Theorem 2:** The finite ring \( R_{n,m} = Z_p[x]/(x^n - 1) \times Z_p[x]/(x^m - 1) \) is a \( Z_p[x] \)-module with respect to the following multiplication: 
\[ f(x) * c(x) = f(x) * (a(x), b(x)) = (\overline{f(x)} a(x), f(x) b(x)) \]

Where \( f(x) \in Z_p[x], (a(x), b(x)) \in R_{n,m} \) and \( \overline{f(x)} \) is the reduction \( f(x) = f(x)(\mod p) \). Moreover, A code \( C \) is a \( Z_p Z_p \)-cyclic code if and only if \( C \) is a \( Z_p[x] \)-submodule of \( R_{n,m} = Z_p[x]/(x^n - 1) \times Z_p[x]/(x^m - 1) \).

The proof of the Theorem 2 is straightforward.

The Structure Of \( Z_p Z_p \)-Cyclic Codes

**Theorem 3:** Let \( C \) be a cyclic code in \( R_{n,m} = Z_p[x]/(x^n - 1) \times Z_p[x]/(x^m - 1) \). Then \( C \) is one of the following types:

1. \( C = ((f(x), 0)) \), where \( f(x) \) divides \( x^n - 1 \).
2. \( C = ((k(x), g(x) + ph(x))) \), where \( x^n - 1 \) divides \( (x^n - 1/h(x)) \) and \( h(x) \) divides \( g(x) \) in \( Z_p[x] \).
3. \( C = ((f(x), 0), (k(x), g(x) + ph(x))) \), where \( \deg k(x) < \deg f(x) \) or \( k(x) = 0 \), \( f(x) \) divides \( (x^n - 1/h(x)) \) and \( h(x) \) divides \( g(x) \) in \( Z_p[x] \).
Proof: Let \( C \) be a cyclic code in \( R_{m,n} \). Define the mapping \( \varphi : C \rightarrow Z_p[x]/(x^m-1) \) as follows
\[
\varphi(f_1(x), f_2(x)) = f_2(x) \text{.}
\]
Then \( \varphi \) is a \( Z_p[x] \)-module homomorphism and \( \text{Im} \varphi \) is a \( Z_p[x] \)-submodule of \( Z_p[x]/(x^m-1) \). Therefore, \( \text{Im} \varphi \) is an ideal of the ring \( Z_p[x]/(x^m-1) \). By Corollary 3.5 of [7] \( \text{Im} \varphi = \{ (f_1(x), 0) \mid f_1(x) \in Z_p[x]/(x^m-1) \} \subseteq C \). Let \( I = \{ f_1(x) \mid (f_1(x), 0) \in \text{Ker} \varphi \} \). Then \( I \) is an ideal of \( Z_p[x]/(x^m-1) \). Therefore, by the well known results on generators of cyclic codes, we have \( I = (f(x)) \), where \( f(x) | (x^m-1) \). For any \( (f_1(x), 0) \in \text{Ker} \varphi \), we have \( f_1(x) \in I = (f(x)) \) and therefore
\[
f_1(x) = k(x)f(x) \text{ for some } k(x) \in Z_p[x] \text{.}
\]
This shows that \( \text{Ker} \varphi \) is generated by one element \( (f(x), 0) \). From the isomorphism theorem of ring it follows that \( C / \ker \varphi \cong \text{Im} \varphi \). Let \( \varphi(k(x), g(x) + ph(x)) = (g(x) + ph(x)) \). For any \( (f_1(x), f_2(x)) \in C \), \( \varphi(f_1(x), f_2(x)) = f_2(x) \in \text{Im} \varphi \). Since \( \text{Im} \varphi = (g(x), ph(x)) = (g(x) + ph(x)) \), there is a \( s(x) \in Z_p[x] \) such that \( \varphi(f_1(x), f_2(x)) = f_2(x) = \varphi(s(x)k(x), s(x)(g(x) + ph(x))) \) by Theorem 2. Thus, we have \( (f_1(x), f_2(x)) - (s(x)k(x), s(x)(g(x) + ph(x))) \in \text{Ker} \varphi = (f(x)) \) which implies that \( f_1(x) - s(x)k(x) = t(x)f(x) \) and \( f_2(x) = s(x)(g(x) + ph(x)) \) for some \( t(x) \in Z_p[x] \). It follows that \( (f_1(x), f_2(x)) = t(x)(f(x), 0) + s(x)(k(x), g(x) + ph(x)) \). This shows that \( C \) can be generated by two elements \( (f(x), 0) \) and \( (k(x), g(x) + ph(x)) \). Let \( k(x) = f(x)q(x) + r(x) \), where \( q(x), r(x) \in Z_p[x] \) and \( \deg r(x) < \deg f(x) \) or \( r(x) = 0 \). Then \( (r(x), g(x) + ph(x)) = (k(x), g(x) + ph(x)) - q(x)(f(x), 0) \in C \). Thus we can assume that \( (f(x), 0) \) and \( (k(x), g(x) + ph(x)) \) are generators of \( C \) with \( \deg k(x) < \deg f(x) \) if \( f(x) \neq 0 \) and \( k(x) \neq 0 \). If \( C \) has a generator, then \( C = ((f(x), 0)) \), where \( f(x) | (x^m-1) \) or \( f(x) = x^n-1 \) and \( C = (k(x), g(x) + ph(x)) \). In this case, note that
\[
\varphi\left(\frac{x^m-1}{h(x)}(k(x), g(x) + ph(x))\right) = \varphi\left(\frac{x^m-1}{h(x)}k(x), (x^m-1)(\frac{g(x)}{h(x)} + p)\right) = 0 \text{,}
\]
we have \( \frac{x^m-1}{h(x)}k(x), 0) \in \text{Ker} \varphi \subseteq C \) and therefore \( f(x) = x^n-1 | (x^m-1/h(x))k(x) \). If \( C \) has two generators \( (f(x), 0) \) and \( (k(x), g(x) + ph(x)) \), then we have \( \deg k(x) < \deg f(x) \) or \( k(x) = 0 \), \( f(x) | (x^m-1/h(x))k(x) \) and \( h(x) | g(x) | (x^m-1) \) in \( Z_p[x] \). This completes the proof of the Theorem.

Summary
Using coding theory, we have determined the algebraic structure of \( Z_pZ_p' \)-cyclic codes, where \( p \) is an odd prime. Any \( Z_pZ_p' \)-cyclic code \( C \) can be generated by two elements and \( C \) is one of three types. The results obtained are similar to that of \( Z_pZ_4 \)-cyclic codes. Since perfect \( Z_pZ_4 \)-additive codes have been utilized in the subject of steganography [3], we believe that these codes may have some promising applications besides elegant theory.

Acknowledgements
This research was financially supported by the Research Project of Liaoning Education Bureau under Project Code L2014490.
References


