The Structure of $Z_pZ_{p^2}-$ Cyclic Codes

Xuedong Dong[1, a]

[1]College of Information Engineering, Dalian University, Dalian 116622, P.R.China

[a]email: dongxuedong@sina.com

Keywords: Linear Code; Cyclic code; Finite ring

Abstract. A code C is a Z_2Z_4-cyclic code if and only if C is a $Z_4[x]$-submodule of the ring $Z_2[x]/(x^n-1)\times Z_4[x]/(x^m-1)$. Perfect Z_2Z_4-additive codes have been utilized in the subject of steganography. The algebraic structure of Z_2Z_4-cyclic codes was determined in 2014. In this paper we determine the algebraic structure of $Z_pZ_{p^2}-$cyclic codes ,where p is an odd prime. Any $Z_pZ_{p^2}-$cyclic code C can be generated by two elememts 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_2Z_4-additive codes [3],[4],[5],[6]. A Z_2Z_4-additive code C is defined to be a subgroup of the group $Z_2{}^r\times Z_4{}^s$. Perfect Z_2Z_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_2Z_4-cyclic codes has been given. It is interesting to determine the structure of $Z_pZ_{p^2}-$ cyclic codes,where $Z_pZ_{p^2}-$ codes should be definied as a subgroup of the group $Z_p{}^n\times Z_{p^2}{}^m$ and p is an odd prime. This short note gives a complete structure of $Z_pZ_{p^2}-$ cyclic codes.The results show that a $Z_pZ_{p^2}-$ 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 $Z_pZ_{p^2}-$ 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 $Z_p{}^n\times Z_{p^2}{}^m$ is called a $Z_pZ_{p^2}-$ code if C is a subgroup of $Z_p{}^n\times Z_{p^2}{}^m$.

Definition 2: A subset C of the group $Z_p{}^n\times Z_{p^2}{}^m$ is called a $Z_pZ_{p^2}-$cyclic code if

1) C is a $Z_pZ_{p^2}-$ code, and

2) For any codeword $\vec{u}=(a_0a_1\cdots a_{n-1},\ b_0b_1\cdots b_{m-1})\in C$, its cyclic shift

$T(\vec{u})=(a_{n-1}a_0\cdots a_{n-2},\ b_{m-1}b_0b_1\cdots\ b_{m-2})$ is also in C.

Definition 3: For any two elements $\vec{u}=(a_0a_1\cdots a_{n-1},\ b_0b_1\cdots\ b_{m-1})$ and $\vec{v}=(d_0d_1\cdots d_{n-1},\ e_0e_1\cdots\ e_{m-1})$, the inner product of $\vec{u}$ and $\vec{v}$ is defined as $\vec{u}\cdot\vec{v}=\vec{u}=p(a_0d_0+a_1d_1+\cdots+a_{n-1}d_{n-1})+b_0e_0+b_1e_1+\cdots+\ b_{m-1}e_{m-1} \bmod p^2$. If C is a $Z_pZ_{p^2}-$ code, then its dual is defined as $C^{\perp}=\left\{\vec{v}\,|\,\vec{u}\cdot\vec{v}=0,\forall\vec{u}\in C\right\}$.

Theorem 1: Let C be a $Z_pZ_{p^2}-$ cyclic code, then its dual $C^{\perp}$ is also a $Z_pZ_{p^2}-$ cyclic code.

Proof: Let C be a $Z_pZ_{p^2}-$cyclic code. Then it is clear that $C^{\perp}$ is a $Z_pZ_{p^2}-$ code. It is suffices to prove that any cyclic shift of an element in $C^{\perp}$. For any $\vec{v}=(d_0d_1\cdots d_{n-1},\ e_0e_1\cdots\ e_{m-1})\in C^{\perp}$ and any $\vec{u}=(a_0a_1\cdots a_{n-1},\ b_0b_1\cdots\ b_{m-1})\in C$, then $\vec{u}\cdot\vec{v}=0$. Let $l=[m,n]$. Then $T^l(\vec{u})=\vec{u}$. Assume that $T^{l-1}(\vec{u})=(a_1\cdots a_{n-1}a_0,\ b_1\cdots\ b_{m-1}b_0)$. Since C is a $Z_pZ_{p^2}-$ cyclic code, we have $T^{l-1}(\vec{u})=(a_1\cdots a_{n-1}a_0,\ b_1\cdots\ b_{m-1}b_0)\in C$. It follows that $T^{l-1}(\vec{u})\cdot\vec{v}=0$, that is,

$0=T^{l-1}(\vec{u})\cdot\vec{v}=p(a_1d_0+a_2d_1+\cdots+a_0d_{n-1})+b_1e_0+b_2e_1+\cdots+\ b_0e_{m-1} \bmod p^2$. On the other hand,

$\vec{u}\cdot T(\vec{v})=p(a_0d_{n-1}+a_1d_0+\cdots+a_{n-1}d_{n-2})+b_0e_{m-1}+b_1e_0+\cdots+\ b_{m-1}e_{m-2} \bmod p^2$. It is clear that

$\vec{u}\cdot T(\vec{v})=T^{l-1}(\vec{u})\cdot\vec{v}=0.$ This shows that $T(\vec{v})$ is also in $C^{\perp}$ and therefore $C^{\perp}$ is also a $Z_pZ_{p^2}-$ cyclic code. This completes the proof of the theorem.

As is common in the discussion of cyclic codes, an element $\vec{u}=(a_0a_1\cdots a_{n-1},\ b_0b_1\cdots\ b_{m-1})\in C$ can be identified with an element consisting of two polynomials

$$c(x)=(a(x),b(x))=(a_0+a_1x+\cdots+a_{n-1}x^{n-1},\ b_0+b_1x+\cdots+\ b_{m-1}x^{m-1})$$

in the finite ring $R_{n,m}=Z_p[x]/(x^n-1)\times Z_{p^2}[x]/(x^m-1)$. Code words of a cyclic code C are regard 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 $R_{n,m}=Z_p[x]/(x^n-1)\times Z_{p^2}[x]/(x^m-1)$ is a $Z_{p^2}[x]$-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 $f(x)\in Z_{p^2}[x],(a(x),b(x))\in R_{n,m}$ and $\overline{f(x)}$ is the reduction $\overline{f(x)}=f(x)(\bmod p)$. Moreover, A code C is a $Z_pZ_{p^2}-$ cyclic code if and only if C is a $Z_{p^2}[x]$ -submodule of $R_{n,m}=Z_p[x]/(x^n-1)\times Z_{p^2}[x]/(x^m-1)$.

The proof of the Theorem 2 is straightforward.

The Structure Of $Z_pZ_{p^2}-$Cyclic Codes

Theorem 3: Let C be a cyclic code in $R_{n,m}=Z_p[x]/(x^n-1)\times Z_{p^2}[x]/(x^m-1)$. Then C is one of following types:

1) $C=((f(x),0))$, where $f(x)\,|\,(x^n-1)$.

2) $C=((k(x),g(x)+ph(x)))$,where $x^n-1\,|\,(x^m-1/h(x))*k(x)$ and $h(x)\,|\,g(x)\,|\,(x^m-1)$ in $Z_{p^2}[x]$.

3) $C=((f(x),0),(k(x),g(x)+ph(x)))$, where $\deg k(x)<\deg f(x)$ or $k(x)=0$, $f(x)\,|\,(x^m-1/h(x))*k(x)$ and $h(x)\,|\,g(x)\,|\,(x^m-1)$ in $Z_{p^2}[x]$.

Proof: Let C be a cyclic code in $R_{n,m}$. Define the mapping $\varphi: C \to Z_{p^2}[x]/(x^m-1)$ as follows

$\varphi(f_1(x), f_2(x)) = f_2(x)$ .Then φ is a $Z_{p^2}[x]$ -module homomorphism and Im φ is a $Z_{p^2}[x]$-submodule of $Z_{p^2}[x]/(x^m-1)$. Therefore, $\mathrm{Im}\,\varphi$ is an ideal of the ring $Z_{p^2}[x]/(x^m-1)$. By Corollary 3.5 of [7] $\mathrm{Im}\,\varphi = (g(x), ph(x)) = (g(x)+ph(x))$,where $h(x) \mid g(x) \mid (x^m-1)$ in $Z_{p^2}[x]$. It is clear that $Ker\varphi = \left\{(f_1(x),0) \mid f_1(x) \in Z_p[x]/(x^n-1)\right\} \subseteq C$. Let $I = \{ f_1(x) \mid (f_1(x),0) \in Ker\varphi\}$ .Then I is an ideal of $Z_p[x]/(x^n-1)$. Therefore, by the well known results on generators of cyclic codes, we have $I = (f(x))$, where $f(x) \mid (x^n-1)$ .For any $(f_1(x),0) \in Ker\varphi$, we have $f_1(x) \in I = (f(x))$ and therefore

$f_1(x) = k(x)f(x)$ for some $k(x) \in Z_p[x]$ .This shows that $Ker\varphi$ is generated by one element $(f(x),0)$ .From the isomorphism theorem of ring it follows that $C/\ker\varphi \cong \mathrm{Im}\,\varphi$ .Let $\varphi(k(x), g(x)+ph(x)) = g(x)+ph(x)$ .For any $(f_1(x), f_2(x)) \in C$, $\varphi(f_1(x), f_2(x)) = f_2(x) \in \mathrm{Im}\,\varphi$. Since Im φ = $(g(x), ph(x)) = (g(x)+ph(x))$, there is a $s(x) \in Z_{p^2}[x]$ such that $\varphi(f_1(x), f_2(x)) = f_2(x) \quad = \varphi(s(x)k(x), s(x)(g(x)+ph(x)))$ by *Theorem 2*.Thus, we have $(f_1(x), f_2(x)) -$ $(s(x)k(x), s(x)(g(x)+ph(x))) \in Ker\varphi = (f(x))$ 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 elememts $(f(x),0)$ 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 $f(x) \mid (x^n-1)$ or $f(x) = x^n-1$ and $C = ((k(x), g(x)+ph(x)))$. In this case, note that $\varphi(\frac{x^m-1}{h(x)}(k(x), g(x)+ph(x))) = \varphi(\frac{x^m-1}{h(x)} * k(x), (x^m-1)(\frac{g(x)}{h(x)}+p) = 0$, we have $(\frac{x^m-1}{h(x)} * k(x), 0) \in Ker\varphi \subseteq C$ and therefore $f(x) = x^n - 1 \mid (x^m - 1/h(x)) * k(x)$ .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 $k(x)=0$, $f(x) \mid (x^m-1/h(x)) * k(x)$ and $h(x) \mid g(x) \mid (x^m-1)$ in $Z_{p^2}[x]$ .This completes the proof of the Theorem.

Summary

Using coding theory, we have determined the algebraic structure of $Z_pZ_{p^2}-$cyclic codes ,where p is an odd prime. Any $Z_pZ_{p^2}-$cyclic code C can be generated by two elememts and C is one of three types.The results obtained are similar to that of Z_2Z_4-cyclic codes. Since perfect Z_2Z_4-additive codes have been utilized in the subject of steganography [3],we belive 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

[1] V. Pless, Introduction to the Theory of Error-Correcting Codes, 3rd ed.New York, NY, USA: Wiley, 1998.

[2]A. R., Jr.Hammons, P. V., Kumar, A. R.Calderbank, N. J. A. Sloane, P.Sol´e, The Z4 linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory, 40 (1994), 301–319.

[3]H. Rifà-Pous, J. Rifà, and L. Ronquillo, Z_2Z_4-additive perfect codes in steganography, Adv. Math. Communications, 5(2011), 425–433.

[4] M. Bilal, J. Borges, S. T. Dougherty, and C. Fernandez-Cordoba,Maximum distance separable codes over Z_4 and $Z_2 \times Z_4$, Des. Codes Cryptogrph., 61 (2011), 31–40.

[5] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà, and M. Villanueva, Z_2Z_4-linear codes: Generator matrices and duality, Des. Codes Cryptogrph., 54(2009), 167–179.

[6] Taher Abualrub, Irfan Siap, and Nuh Aydin, Z_2Z_4-Additive cyclic codes, IEEE Trans. Inform. Theory, 60(2014),1508-1514.

[7] Pramod Kanwar and Sergio R. Lo´ pez-Permouth, Cyclic codes over the integers modulo Z_{p^m}, Finite Fields and Their Applications, 3(1997),334–352.