All Sciences Proceedings
http://as-proceeding.com/

2nd International Conference on Engineering, Natural and Social Sciences

April 4-6, 2023 : Konya, Turkey

© 2023 Published by All Sciences Proceedings

https://www.icensos.com/

Additive polycyclic codes over F_{p^2} for any prime p

Mustafa SARI*[1] and M. Emin KÖROĞLU [1]

[1]Department of Mathematics, Yildiz Technical University, Türkiye

*(musari@yildiz.edu.tr) Email of the corresponding author

Abstract – One of the most significant task in algebraic coding theory is to determine the structure of new class of linear or nonlinear codes and to find codes having good parameters. In this study, for any prime p, we define additive polycyclic codes over F_{p^2} as a generalization of additive polycyclic codes over F_4 studied in [5]. By making use of the polynomials over F_p instead of F_{p^2}, we determine the algebraic structure of additive polycyclic codes over F_{p^2} and present their generators completely. We also find the cardinality for these codes. Moreover, under certain conditions, we show that the Euclidean duals of additive polycyclic codes over F_{p^2} are also additive polycyclic codes over F_{p^2}. Finally, we illustrate what we discuss in this study by offering some examples of additive polycyclic codes over F_9 that contain codewords as three times the number of the codewords of the optimal linear codes with the same length and minimum distance.

Keywords – Linear Code, Additive Code, Optimal Code, Polycyclic Code, Generators

I. INTRODUCTION

Researchers have profoundly been carried out the studies on additive codes over different algebras [1-5]. In [1], the authors defined $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and determined the generators of these codes. They also obtained optimal linear codes over finite fields from these codes. In [2], the authors introduced a new class of additive codes defined as $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes. They also established standart generator matrices for these codes and obtain some optimal linear codes as the Gray images of these codes. In [3], Borges *et al.* considered $\mathbb{Z}_2\mathbb{Z}_4$-additive cyclic codes and gave generators of these codes and their duals by giving a special inner product on the polynomials. As a generalization of [4], Wu and Shi defined $\mathbb{Z}_2\mathbb{Z}_4$-additive polycyclic codes and determined their minimal spanning set. They also presented some almost optimal codes over F_2 as the Gray images $\mathbb{Z}_2\mathbb{Z}_4$-additive polycyclic codes. Recently, in [5], the authors considered additive polycyclic codes over F_4 induced by a binary vector and they obtained optimal binary linear codes and quantum codes from additive polycyclic codes over F_4 via the maps they defined.

In the light of above studies, as a generalization of [5], we consider additive polycyclic codes over F_{p^2} for any prime p in this study. We determine their generator polynomials and also study their duals. Finally, we give an example and conclude the study.

II. PRELIMINARIES

F_q is a finite field of q elements. We mean by an additive code over F_q of length n an additive subgroup of F_q^n. If an additive code over F_q of length n is closed under multiplication by scalars in

F_q, then it is called a linear code over F_q of length n. The Hamming distance $d(x,y)$ between two vectors x and y is $d(x,y)=|\{i:x_i\neq y_i\}|$. The minimum (Hamming) distance of a code is $\min\{d(x,y):x,y\in C,x\neq y\}$. We show a code over F_q of length n, minimum distance d and size q^k by $[n,k,d]_q$. The Euclidean dual $C^{\perp}$ of a code C over F_q of length n is the set of all vectors in F_q^n which are orthogonal to the codewords in C with respect to usual inner product.

III. ADDITIVE POLYCYCLIC CODES OVER F_{p^2}

Let $F_{p^2}=\{a+bw:a,b\in F_p\}$, where w is a root of a primitive polynomial of degree 2 over F_p.

Definition III.I**:** Let $b=(b_0,\ldots,b_{n-1})\in F_p^n$. For an additive code C over F_{p^2} of length n, if $(c_{n-1}b_0,c_0+c_{n-1}b_1,\ldots,c_{n-2}+c_{n-1}b_{n-1})\in C$ whenever $(c_0,c_1,\ldots,c_{n-1})\in C$, then we say that C is an additive b-polycyclic code over F_{p^2} of length n.

There exists a relation between additive polycyclic codes over F_{p^2} and submodules of a special F_p-module. Let the polynomial correspondence of a vector $b=(b_0,\ldots,b_{n-1})\in F_p^n$ be $b(x)=b_0+b_1x+\cdots+b_{n-1}x^{n-1}\in F_p[x]$. Then, the quotient ring $R_n=\dfrac{F_{p^2}[x]}{\langle x^n-b(x)\rangle}$ becomes an $F_p[x]$-module under usual polynomial addition and multiplication ,and we have the following.

Lemma III.II: There exists a one-to-one correspondence between additive $b-$polycyclic codes over F_{p^2} of length n and submodules of $F_p[x]$-module. R_n.

Proof: Let C be an additive b-polycyclic code over F_{p^2} of length n and $c=(c_0,\ldots,c_{n-1})\in C$. Consider the set C' of all polynomial correspondences of the codewords in C. Then, $(c_{n-1}b_0,c_0+c_{n-1}b_1,\ldots,c_{n-2}+c_{n-1}b_{n-1})\in C$ and see that $c_{n-1}b_0+(c_0+c_{n-1}b_1)x+\cdots+(c_{n-2}+c_{n-1}b_1)x^{n-1}=xc(x)$ in $F_p[x]$-module. R_n, which implies that C' is closed under multiplication by x and so any polynomial in $F_p[x]$. Hence, C' is a submodule of $F_p[x]$-module. R_n.

Conversely, let C' be a submodule of $F_p[x]$-module R_n and consider the set of all vectorial correspondences of the elements in C'. Let $c(x)\in C'$. Then, $xc(x)$ in R_n is equal to $c_{n-1}b_0+(c_0+c_{n-1}b_1)x+\cdots+(c_{n-2}+c_{n-1}b_1)x^{n-1}=xc(x)$ and its vectorial correspondence is $(c_{n-1}b_0,c_0+c_{n-1}b_1,\ldots,c_{n-2}+c_{n-1}b_{n-1})\in C$, which implies that C is an additive b-polycyclic code over F_{p^2} of length n.

By Lemma III.II, we view an additive b-polycyclic code over F_{p^2} of length n as a submodule of $F_p[x]$-module R_n. In this case, it is needed to give generators of a submodule of $F_p[x]$-module R_n to determine algebraic structure of an additive b-polycyclic code over F_{p^2} of length n.

Let C be a submodule of $F_p[x]$-module R_n. For the polynomials $wg_1(x)+g_2(x)$ and $u(x)$, it is desired to satisfy the following conditions:

Condition 1: $u(x)=0$ when there is no nonzero polynomial over F_p in C. If C has nonzero polynomials over F_p, then $u(x)$ is a nonzero polynomial in $F_p[x]$ such that it has minimal degree.

Condition 2: $wg_1(x)+g_2(x)=0$ when there exist only polynomials over F_p in C. If there exist nonzero polynomials in C which are over F_{p^2} not F_p, then $g_1(x),g_2(x)\in F_p[x]$ and $g_1(x)$ has minimal degree.

Theorem III.III: If C is an additive b-polycyclic code over F_{p^2} of length n, then for some polynomials $g_1(x),g_2(x),u(x)\in F_p[x]$ satisfying the conditions 1 and 2, C is generated by the polynomials $wg_1(x)+g_2(x)$ and $u(x)$, that is,

$$C=\langle wg_1(x)+g_2(x),u(x)\rangle,$$

where we may assume that $\deg g_2(x)<\deg u(x)$.

Proof: Let $c(x)\in C$ be over F_p. Then, for some $q(x),r(x)\in F_p[x]$, $r(x)=c(x)-q(x)u(x)\in C$ where $\deg r(x)<\deg u(x)$ or $r(x)=0$. The condition 1 forces that $r(x)=0$ and $c(x)=q(x)u(x)$.

Now, let $c(x)=wc_1(x)+c_2(x)\in C$ be over F_{p^2} not F_p. Then, for some polynomials $q_1(x),r_1(x)\in F_p[x]$, $c_1(x)=q_1(x)g_1(x)+r_1(x)$ where $\deg r_1(x)<\deg g_1(x)$ and we also have $wc_1(x)=q_1(x)\left[wg_1(x)+g_2(x)\right]+(p-1)q_1(x)g_2(x)+wr_1(x)$. Furthermore, for some polynomials $q_1(x),r_1(x)\in F_p[x]$, $c_2(x)=q_2(x)u(x)+r_2(x)$ where $\deg r_2(x)<\deg b(x)$ and we also have

$$\begin{aligned}wc_1(x)+c_2(x)=q_1(x)\left[wg_1(x)+g_2(x)\right]+q_2(x)u(x)\\+wr_1(x)+(p-1)q_1(x)g_2(x)+r_2(x).\end{aligned}$$

Since $wg_1(x)+g_2(x),u(x)\in C$, we get $wr_1(x)+(p-1)q_1(x)g_2(x)+r_2(x)\in C$. Then, the condition 2 forces that $r_1(x)=0$ and so $(p-1)q_1(x)g_2(x)+r_2(x)=q_3(x)u(x)$ for some $q_3(x)\in F_p[x]$. Then, it follows that

$$wc_1(x)+c_2(x)=q_1\left[wg_1(x)+g_2(x)\right]+\left[q_2(x)+q_3(x)\right]u(x),$$

which completes proof of the first part.

For proof of the second part, if $\deg g_2(x)\geq\deg u(x)$, then for some polynomials $q(x),r(x)\in F_p[x]$ with $\deg r(x)<\deg u(x)$, we have $g_2(x)=q(x)b(x)+r(x)$. In this case, it follows from additive b-polycyclic code C'' over F_{p^2} of length n defined by $\langle wg_1(x)+r(x),u(x)\rangle$ that $C=C''$, which completes the proof.

Since the proof of the following is similar to the proof of Lemma 3.2 in [1], we give it without proof.

Lemma III.IV: If $C=\langle wg_1(x)+g_2(x),u(x)\rangle$ is an additive b-polycyclic code over F_{p^2} where $g_1(x),g_2(x),u(x)\in F_p[x]$ satisfy the conditions 1 and 2, then the polynomials $g_1(x),g_2(x)$ and $u(x)$ are unique.

Let $C=\langle wg_1(x)+g_2(x),u(x)\rangle$ be an additive b-polycyclic code over F_{p^2} of length n where the polynomials $g_1(x),g_2(x),u(x)\in F_p[x]$ satisfying the conditions 1 and 2. If $x^n-b(x)=q_1(x)u(x)+r_1(x)$ for some polynomials $q_1(x),r_1(x)\in F_p[x]$ where $\deg r_1(x)<\deg u(x)$ or $r_1(x)=0$., then we get $r_1(x)=x^n-b(x)-q_1(x)u(x)\in C$, which is only possible when $r_1(x)=0$. Similarly, if $x^n-b(x)=q_2(x)g_1(x)+r_2(x)$ for some polynomials $q_2(x),r_2(x)\in F_p[x]$ where $\deg r_2(x)<\deg g_1(x)$ or $r_2(x)=0$, then we get $wr_2(x)=w\left[x^n-b(x)\right]-wq_2(x)g_1(x)\in C$, which is only possible when $r_2(x)=0$. Because $\left[wg_1(x)+g_2(x)\right]\frac{x^n-b(x)}{g_1(x)}=\frac{x^n-b(x)}{g_1(x)}g_2(x)\in F_p[x]$, by condition 1, we get that $u(x)$ divides $\frac{x^n-b(x)}{g_1(x)}g_2(x)$. Then, we sum up exact characterization of an additive b-polycyclic code over F_{p^2} of length n as the following:

Theorem III.V: For the polynomials $g_1(x),g_2(x),u(x)\in F_p[x]$ satisfying the conditions 1 and 2, if $C=\langle wg_1(x)+g_2(x),u(x)\rangle$ is an additive b-polycyclic code over F_{p^2} of length n, then $\deg g_2(x)<\deg u(x)$, $g_1(x),u(x)\mid x^n-b(x)$ and $u(x)\mid\frac{x^n-b(x)}{g_1(x)}g_2(x)$. Moreover, the cardinality of C is $q^{2n-\deg(g_1(x))-\deg(u(x))}$.

Proof: The cardinality of C follows from proof of Theorem 3.4 in [1].

IV. EUCLIDEAN DUALS OF ADDITIVE POLYCYCLIC CODES OVER F_{p^2}

Let the polynomial $b(x)$ be a nonzero constant in F_p and say $b(x)=b$. Let $o(b)$ be the multiplicative order of b in $F_p-\{0\}$. For nonzero $b\in F_p$, we call an additive b-polycyclic code as an additive b-constacyclic code. The following determines the Euclidean duals of additive b-constacyclic codes over F_{p^2}.

Theorem IV.I: The Euclidean dual of an additive b -constacyclic code over F_{p^2} of length n is an additive b^{-1}-constacyclic code over F_{p^2} of length n.

Proof: Let ${}_b\delta(c)=(bc_{n-1},c_0,\dots,c_{n-2})$ for a vector $c=(c_0,\dots,c_{n-1})\in C$ and ${}_b\delta^j(c)={}_b\delta^{j-1}({}_b\delta(c))$. Observe that ${}_b\delta^{o(b).n}(c)=c$ and ${}_b\delta^{o(b)n-1}(c)=(c_1,\dots,c_{n-1},b^{-1}c_0)\in C$. Now, let $d=(d_0,\dots,d_{n-1})\in C^{\perp}$. It follows from

$$0={}_b\delta^{o(b).n-1}(c)\cdot d=c_0b^{-1}d_{l-1}+c_1d_0+\cdots+c_{l-1}d_{l-2}$$
$$=c\cdot{}_{b^{-1}}\delta(d)$$

that ${}_{b^{-1}}\delta(d)\in C^{\perp}$, which completes the proof.

V. EXAMPLE

Example V.I: Let $p=3$ and $n=13$. For the vector $b=(2,0,1,1,1,2,0,1,0,0,0,0,2)\in F_3^{13}$, take the generators $u(x)=x^4+x^3+x^2+1$, $g_1(x)=x+2$ and $g_2(x)=x^3+x+1$. Let C be an additive b-polycyclic code over F_9 of length 13 where $C=\langle wg_1(x)+g_2(x),u(x)\rangle$. Then, by computer software MAGMA, we say that C is a $[13,21/2,3]_9$ additive code and this code contains codewords as three times the number of the codewords of the optimal linear code $[13,10,3]_9$.

VI. CONCLUSION

In this study, we give the definition for additive polycyclic codes over F_{p^2} for any prime p and study their algebraic structures. We characterize the generator polynomials for additive polycyclic codes over F_{p^2} with respect to polynomials over F_p. We give the cardinality of these codes. Furthermore, for special case of additive polycyclic codes over F_{p^2} we show that the Euclidean duals of these codes are also additive polycyclic codes. over F_{p^2}. Finally, by giving example of an additive polycyclic code over F_9 of length 13 containing codewords as three times the number of the codewords of the optimal linear code with the same length and minimum distance, we complete the study.

ACKNOWLEDGMENT

This study is supported by Yildiz Technical University Scientific Research Projects Coordination Department with Project Number FBA-2023-5424.

REFERENCES

[1] T. Abualrub, I. Siap and N. Aydın, “$\mathbb{Z}_2\mathbb{Z}_4$-Additive cyclic codes”, *IEEE Trans. Inform. Theory,* vol. 60, no. 3, pp. 1508-1513, 2014.

[2] I. Aydoğdu, T. Abualrub and I. Siap, “On $\mathbb{Z}_2\mathbb{Z}_2[u]$-additive codes”, *Int. J. Comput. Math,* vol.92, no. 9, pp. 1806-1814, 2015.

[3] J. Borges, C. Fernandez-Córdoba and R. Ten-Valls,” On $\mathbb{Z}_{p^r}\mathbb{Z}_{p^s}$ -additive cyclic codes”, *Adv. Math. Commun.*, vol. 12, no.1, pp. 169-179, 2018.

[4] R. Wu and M. Shi,” On $\mathbb{Z}_2\mathbb{Z}_4$-additive polycyclic codes and their Gray images,” *Des. Codes Cryptogr.*, vol. 90, pp: 2251-2562, 2022.

[5] A. S. Karbaski, T. Abualrub, N. Aydın and P. Liu, “Additive polycyclic codes over F_4 induced by binary vectors and some optimal codes,” *Adv. Math. Commun.*, 2022, doi:10.3934/amc.2022004.