J. Algebra Comb. Discrete Appl.
10(2) • 115–118

Received: 22 February 2022
Accepted: 18 June 2022

Journal of Algebra Combinatorics Discrete Structures and Applications

A class of permutation polynomials over the group ring $\mathbb{F}_pC_{p^n}$

Research Article

Pooja Gahlyan, Reto Schnyder, Rajendra Sharma

Abstract: Let p be a prime number and $\mathbb{F}_pC_{p^n}$ denote the group ring of a cyclic group of order p^n over $\mathbb{F}_p$. We study the permutation property of the polynomial $a_0 + a_1x + a_px^p + \cdots + a_{p^n}x^{p^n}$ with coefficients $a_i \in \mathbb{F}_pC_{p^n}$ where $i = 0, 1, p, \ldots, p^n$. Necessary and sufficient conditions on the coefficients have been obtained so that it becomes a permutation polynomial.

2010 MSC: 11T06, 11T55

Keywords: Group ring, Permutation polynomial

1. Introduction

Let R be a finite ring of order m and G a group of order n, then the group ring RG has m^n elements. A polynomial $f(x) \in RG[x]$ is said to be a permutation polynomial over RG if the associated polynomial function $f : c \to f(c)$ from RG into RG is a permutation of RG, that is f, is bijective over RG. Therefore, to check whether a polynomial $f \in RG[x]$ is a permutation polynomial, it is sufficient to check whether the corresponding polynomial function is injective or surjective over RG.

Cryptographic systems are derived using units in group rings [9]. Group rings can also be used in designing codes. A strong connection of self dual codes with group rings can be found in [4]. The study of permutation polynomials over rings has several applications in many areas such as cryptography and coding theory [1, 10, 11, 15, 17, 18]. For one, permutation polynomials over finite rings are used as random number generators [19]. Permutations of elements of a finite ring will give sequences of random numbers. The group ring $\mathbb{F}_pC_{p^n}$ which we used in this paper is also a finite ring containing p^t elements where $t = p^n$ and hence can be used for generating sequences of random numbers. Random number generators play an important role in cryptography and coding theory. For example, In the $RC6$ block cipher there

Pooja Gahlyan (Corresponding Author); Indian Institute of Technology, Delhi (email: poojagahlyan1995@gmail.com).
Reto Schnyder; Institute of Mathematics, University of Zurich (email: reto.schnyder@math.uzh.ch).
Rajendra Sharma; Indian Institute of Technology, Delhi (email: rksharmaiitd@gmail.com).

is use of the permutation polynomial $x + 2x^2$ over the finite ring Z_{2^n}. Permutation polynomials are also used in designing of S-boxes. Permutation polynomials with few terms are important because of their applications. The study of permutation polynomials has been an interesting subject for many years. But characterizing permutation polynomials and finding new families of them remains a very interesting area of research.

Details related to the construction and applications of permutation polynomials can be found in [12]. Some classes related to the construction of permutation polynomials over finite fields can also be found in [6–8]. Rivest [14] characterized permutation polynomials over Z_{2^n}. Singh and Maity [16] studied permutation polynomials mod 3^n and 5^n and gave conditions alike to those given by Rivest for modulo 2^n. Some other characterization of permutation polynomials over finite rings can be found in [2, 5]. But characterization of permutation polynomials is not so easy when it comes to arbitrary commutative rings. In this paper, we study the permutation property of a class of polynomials over the group ring $\mathbb{F}_pC_{p^n}$.

The remaining paper is organized as follows. Section 2 consists of some notations and certain useful lemmas. In section 3, we prove our main results. In section 4, we state the conclusion.

2. Preliminaries

Let n be a positive integer and let $R = \mathbb{F}_pC_{p^n} = \{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{p^n-1}\alpha^{p^n-1} \mid c_i \in \mathbb{F}_p\}$, where $C_{p^n} = \langle \alpha \mid \alpha^{p^n} = 1\rangle$. Note that for any $a \in R$, $a^{p^n} \in \mathbb{F}_p$, and hence $a^{p^{n+k}} = a^{p^n}$ for $k \geq 0$. If R is a commutative ring with unity, then the set of units of R denoted by $U(R)$ forms a group under multiplication of R called the unit group of R. For a field F, the unit group is usually denoted by F^*.

Definition 2.1. *[13] The homomorphism $\varepsilon : RG \to R$ given by*

$$\varepsilon\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g$$

is called the augmentation mapping of RG and its kernel, denoted by $\Delta(G)$, is called the augmentation ideal of RG.

Lemma 2.2. *[3] Let R be a finite commutative ring with unity, then every non zero element of R is either a zero divisor or a unit.*

Lemma 2.3. *If u is a unit and y a non unit in $\mathbb{F}_pC_{p^n}$, then u^{p^n} is a unit of $\mathbb{F}_p$ and $y^{p^n} = 0$.*

Proof. Let $z = c_0 + c_1\alpha + c_2\alpha^2 + ... + c_{p^n-1}\alpha^{p^n-1} \in \mathbb{F}_pC_{p^n}$, then

$$\begin{aligned} z^{p^n} &= (c_0 + c_1\alpha + c_2\alpha^2 + ... + c_{p^n-1}\alpha^{p^n-1})^{p^n} \\ &= c_0 + c_1(\alpha)^{p^n} + c_2(\alpha^2)^{p^n} + ... + c_{p^n-1}(\alpha^{p^n-1})^{p^n} \\ &= c_0 + c_1 + ... + c_{p^n-1} = \varepsilon(z) \quad \text{as } \alpha^{p^n} = 1 \end{aligned} \tag{1}$$

where $\varepsilon : \mathbb{F}_pC_{p^n} \to \mathbb{F}_p$ is the augmentation mapping defined in definition **??**. Obviously $z^{p^n} \in \mathbb{F}_p$

Now, u is a unit and $u^{p^n} = \varepsilon(u)$. Since $\varepsilon : \mathbb{F}_pC_{p^n} \to \mathbb{F}_p$ is a ring homomorphism, it follows that $\varepsilon(u) \in \mathbb{F}_p^*$ for all $u \in U(\mathbb{F}_pC_{p^n})$ where $U(\mathbb{F}_pC_{p^n})$ denotes the set of units of $\mathbb{F}_pC_{p^n}$.

If y is a non-zero non-unit in $\mathbb{F}_pC_{p^n}$ then $y^{p^n} = \varepsilon(y) \in \mathbb{F}_p$. Again, if $\varepsilon(y) \neq 0$ then y^{p^n} is a unit, which implies that y is also a unit. A contradiction. Hence $y^{p^n} = 0$. □

3. A class of permutation polynomials over the group ring $\mathbb{F}_p C_{p^n}$

In this section we consider the permutation property of $f(x) = a_0 + a_1x + a_px^p + \cdots + a_{p^n}x^{p^n}$ over $R = \mathbb{F}_pC_{p^n}$. We will repeatedly use lemma 2.2 and lemma 2.3 throughout the proof.

Theorem 3.1. *Let $f(x) = a_0 + a_1x + a_px^p + \cdots + a_{p^n}x^{p^n} \in R[x]$ with $a_i \in R$ for $i = 0, 1, p, \ldots, p^n$. Then f is a permutation polynomial if and only if both a_1 and $a_1 + a_p + \cdots + a_{p^n}$ are units.*

Proof. Since the constant term has no bearing on whether f is a permutation polynomial, we will assume $a_0 = 0$. In this case, $f\colon R \to R$ is an $\mathbb{F}_p-$ linear map.

We consider the following cases:

Case 1: a_1 is a non-unit

If a_1 is zero, let $s \in R \setminus \{0\}$ satisfy $s^p = 0$ (for example, $s = 1 - \alpha^{p^{n-1}}$). Then,

$$f(s) = a_1s + a_ps^p + \cdots + a_{p^n}s^{p^n} = 0.$$

Hence f is not injective.

If a_1 is not zero and a zero divisor, let $s \in R \setminus \{0\}$ be a zero divisor such that $a_1s = 0$. Since $s^{p^0} \neq 0$ and $s^{p^n} = 0$, there is a maximal $k \geq 0$ such that $s^{p^k} \neq 0$. Hence,

$$f(s^{p^k}) = a_1ss^{p^k-1} + a_ps^{p^{k+1}} + \cdots + a_{p^n}s^{p^{k+n}} = 0,$$

Again, f is not injective.

Case 2: $a_1 + \cdots + a_{p^n}$ is a non-unit

It follows that $(a_1 + \cdots + a_{p^n})^{p^n} = 0$. For an arbitrary $s \in R$, we get

$$f(s)^{p^n} = a_1^{p^n}s^{p^n} + a_p^{p^n}s^{p^n} + \cdots + a_{p^n}^{p^n}s^{p^n} = (a_1 + a_p + \cdots + a_{p^n})^{p^n}s^{p^n} = 0.$$

Hence, the image of f consists only of zero divisors, and f can not be surjective.

Case 3: a_1 and $a_1 + \cdots + a_{p^n}$ both are units

It follows that also $a_1^{p^k}$ and $(a_1 + \cdots + a_{p^n})^{p^k}$ are units for all $k \geq 0$. We show that f is injective.

Suppose there exists $s \in R$ such that $f(s) = 0$. We prove by induction that $s^{p^k} = 0$ for $k = n, \ldots, 0$. For the case $k = n$, we see that

$$0 = f(s)^{p^n} = a_1^{p^n}s^{p^n} + a_p^{p^n}s^{p^n} + \cdots + a_{p^n}^{p^n}s^{p^n} = (a_1 + a_p + \cdots + a_{p^n})^{p^n}s^{p^n}.$$

Since $a_1 + \cdots + a_{p^n}$ is a unit, $(a_1 + \cdots + a_{p^n})^{p^n}$ is also a unit, and it follows that $s^{p^n} = 0$.

Now, assume that $s^{p^\ell} = 0$ for all $\ell > k$. Hence

$$0 = f(s)^{p^k} = a_1^{p^k}s^{p^k} + a_p^{p^k}s^{p^{k+1}} + \cdots + a_{p^{n-k}}^{p^k}s^{p^n} + \cdots + a_{p^n}^{p^k}s^{p^n} = a_1^{p^k}s^{p^k}.$$

Again $a_1^{p^k}$ is a unit, hence $s^{p^k} = 0$.

From the case $k = 0$, we conclude that $s = 0$, and hence that f is injective. □

4. Conclusion

In this paper, we obtained necessary and sufficient conditions on the coefficients $a_i \in \mathbb{F}_p C_{p^n}$ such that $a_0 + a_1 x + a_p x^p + \cdots + a_{p^n} x^{p^n}$ is a permutation polynomial over the group ring $\mathbb{F}_p C_{p^n}$.

Acknowledgment: The first author is supported by University Grants Commission(UGC), India under the grant number 1089/(CSIR-UGC NET DEC. 2016). The second author was supported by the Swiss National Science Foundation grant 188430. The last auothor is ConsenSys Block Chain Professor. The authors thank for their previleges.

References

[1] C. Ding, T. Helleseth, Optimal ternary cyclic codes from monomials, IEEE Trans. Inf. Theory 59 (2013) 5898–5904.
[2] S. Frisch, Polynomial functions on finite commutative rings, Advances in Commutative Ring Theory, Proc. of Fez 1997 Conf. 205 (1999) 323–336.
[3] J. A. Gallian, Contemporary Abstract Algebra, Narosa Publishing House, 4th edition (2008).
[4] J. Gildea, A. Kaya, R. Taylor, Bahattin Yildiz, Constructions for self-dual codes induced from group rings, Finite Fields and Their Applications 51(1), 2018 71–92.
[5] D. Görcsös, G. Horváth, A. Mészáros, Permutation polynomials over finite rings, Finite Fields and Their Applications 49 (2018) 198–211.
[6] R. Gupta, R. K . Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, Finite Fields and Their Applications 41 (2016) 89–96.
[7] R. Gupta, R. K. Sharma, Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$, Finite Fields and Their Applications 50 (2018) 196–208.
[8] R. Gupta, R. K . Sharma, On permutation polynomials over finite fields of charcteristic 2, Journal of Algebra and Its Applications 15(7), (2016) 1650133(7 pages).
[9] B. Hurley, T. Hurley, Group ring cryptography, International Journal of Pure and Applied Mathematics 69(1) (2011).
[10] Y. Laigle-Chapuy, Pemutations polynomials and applications to coding theory, Finite fields and Their Applications 13 (2007) 58–70.
[11] R. Lidl and W. B. Mullen, Permutation polynomials in RSA-Cryptosystems, Advances in Cryptology (1984) 293–301.
[12] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics 20, Cambridge University Press (1984).
[13] C. P. Milies, S K. Sehgal, An Introduction to Group Rings, Kulwer Academic Publishers, London (2002).
[14] R. L. Rivest, Permutation Polynomials Modulo 2^w, Finite Fields and Their Applications 7 (2001), 287–292.
[15] R. L. Rivest, M. J. B Robshaw, R. Sidney, Y. L. Yin, RC6^{TM} block cipher (1998).
[16] R. P. Singh, S. Maity, Permutation Polynomials modulo p^n, Cryptology ePrint Archive Report 2009/393.
[17] R. P. Singh, Permutation polynomials and their applications in cryptography, Ph.D. thesis, Indian Institute of Technology, Guwahati, India, Jan. 2010.
[18] J. Schwenk, K. Huber, Public key encryption and digital signatures based on permutation polynomials, Electron. Lett. 34 (1998) 759–760.
[19] G. R. Vadiraja Bhatta, B.R. Shankar, Vishnu Narayan Mishra, Prasanna Poojary, Sequence of numbers via permutation polynomials over some finite rings, Proyecciones 39(5) (2020) 1295–1313.