http://dx.doi.org/10.4314/bajopas.v13i2.11

Bayero Journal of Pure and Applied Sciences, 13(2): 84 - 86
Received: June, 2020
Accepted: September, 2020
ISSN 2006 – 6996

PERMUTATION POLYNOMIALS OVER GALOIS FIELDS OF CHARACTERISTIC 2

[1]Dahiru, Z.L. and [2]Lawan, A.M.
[1]Department of Sciences, School of continuing Education, Bayero university, kano.
[2]Department of Mathematical Sciences, Bayero University, Kano.
Correspondence author: amlawan.mth@buk.edu.ng

ABSTRACT
In this paper, a class of permutation polynomial known as o-polynomial over Galois fields of characteristic 2 was studied. A necessary and sufficients condition for a monomial x^{2^k} to be an o-polynomial over F_{2^t} is given and two results obtained by Gupta and Sharma (2016) were deduced.

1. INTRODUCTION

Let q be a power of a prime p, and F_q be the Galois field with q elements. A polynomial $f \in F_q[X]$ is called a permutation polynomial (PP) if the associated polynomial function $f: x \to f(x)$ is a bijection of F_q . Permutation polynomials have been a subject of study and have many applications in combinatorics, coding theory, cryptography, design theory and so on.For basic concepts in permutation polynomials, see for example (G. L. Mullen and D. Panario, 2013; R. Lidl and H. Niederreiter, 1997). In general, permutation polynomials of finite fields are easy to construct without much consideration (there are $q!$ permutation polynomials of F_q , all are given by the Lagranges interpolation), thus, the concern is on permutation polynomials with either simple or nice algebraic appearance or posses additional properties, such additional properties are require by applications of PPs in other areas of mathematics and engineering. In recent years, there have been significant progress in finding new classes of permutation polynomials. Let F_q be a Galois field of order 2^t where $t \geq 1$. A permutation polynomial $f(x)$ over F_{2^t} with $f(0) = 0$ and $f(1) = 1$, such that for each $v \in F_{2^t}$, the polynomial $fv(x) = \frac{f(x+v)+f(v)}{x}$ satisfying $f_v(0) = 0$ is called an o-polynomial. (Lidl and Gary,1993),discussed some open problems on permutation polynomials (problem [P16] asked to determine all o-polynomials up to degree 6)**,** **(**Gupta and Sharma, 2016) determined all o- polynomials up to degree 8 using the classification given by (L. E. Dickson, 1897).In this paper, using a technique known as multiplicative equivalent of permutation polynomils, we give necessary and sufficient condition for a monomial x^{2^k} to be an o-polynomial over F_{2^t} and two results obtained by (Gupta and Sharma, 2016) were deduced.

2. Preliminaries

In this section we give definition and some relevant results needed for the understanding of this paper.

***Definition 2.1*:** Two permutation polynomials $f(x)$ *and* $g(x)$ in $F_q[\mathrm{x}]$ are said to be multiplicative equivalent if there exist an integer $1 \leq d \leq q-1$ such that $\gcd(d, q-1) = 1$ and $f(x) = g(x)^d$. Moreover, $f(x)$ and $g(x)$ are equivalent if $f(x) = cg(ax+b) + d$ where $d, b \in F_q$ and $a, c \in {F_q}^*$.

A monomial is a polynomial consisting of only one term. Any polynomial of degree one is called linear polynomial.

***Lemma 2.2 (Lidl and Niederreiter, 1997; Lemma 7.1)*:** Let $f(x)$ be a polynomial over $F_q[X]$, then the following definitions are equivalent:

(i) $f(x)$ is a permutation polynomial on F_q.

(ii) The function $f: x \to f(x)$ is one to one for each$x \in F_q$.

(iii) The function $f: x \to f(x)$ is onto$x \in F_q$..

(iv) $f(x) = a$ has a solution in F_q for each $a \in F_q$.

(v) $f(x) = a$ has a unique solution in F_q for each $a \in F_q$.

Theorem 2.3 (J. Li. Chandler and Xiang, 2010; Theorem 3.4). There are no permutation polynomials of degree 6 over F_{2^t}, when $t > 4$ is even.

Theorem 2.4 (Lidl and Niederreiter, 1998;Theorem 7.8)

(i) Every linear polynomial over F_q is a permutation polynomial of F_q

(ii) The monomial x^i is a permutation polynomial if and only if $\gcd(i, q-1) = 1$**.**

3. Some results on o-polynomials

In this section, we present some important results on o-polynomials which are needed to achieve our objectives.

Theorem 3.1(Gupta and Sharma, 2016; Theorem 2.9). The coefficient of each term of odd power in an o-polynomials is zero.

As a consequence, we deduce the following corollary.

Corollary 3.2: There are no o-polynomials of odd degree.

Proof. Follows from the definition of o-polynomialand from the fact that if the coefficient of odd power is zero, then the whole term will be zero and the rest of the results follows directly from ***Theorem 3.1*.**

Table 1 below is the complete list of all o-polynomials of degree 2,4,6 and 8 obtained by (Gupta and Sharma, 2016).

Degree	Polynomial
2	$f(x) = x^2$
4	$f(x) = x^4$
6	$f(x) = x^6, a_1x^6 + a_2x^4 + a_1x^2, a_3 \neq 0, a_1 + a_2 + a_3 = 1, a_1a_3 = a_2$ for odd$t$
8	$f(x) = x^8,\ t \equiv 0$ mod 3

4. Main Results

In this section we present the necessary and sufficient condition for a monomial x^{2^k} to be an o-polynomial over F_{2^t} and two results obtained by (Gupta and Sharma, 2016) were deduced.

Theorem 4.1:A monomial x^{2^k} is an o-polynomial over F_{2^t} if and only if $\gcd(k,t) = 1$, for $k \in \mathbb{N}$.

Proof: Suppose x^{2^k} is an o-polynomial over F_{2^t}, then gcd(`2^k,2^t −1) =1. Notice that, since x^{2^k} is a permutation over F_{2^t} satisfying$f(0) = 0$, $f(1) = 1$, and for each $v \in F_{2^t}$ we have $\frac{x^{2^k} + v^{2^k} + v^{2^k}}{x} = \frac{x^{2^k}}{x}$ $= x^{2^k}.x^{-1} = x^{2^k - 1}$ which is also a permutation polynomial. This implies that $\gcd(2^k - 1, 2^t - 1) = 1$, thus$\gcd(k,t) = 1$.

Conversely, suppose $\gcd(k,t) = 1$, this implies$\gcd(2^k - 1, 2^t - 1) = 1$. We may without loss of generality, consider $f(x) = x^{2^k - 1}$.By (theorem 2.4(ii)),x^{2^k-1} is a permutation polynomial over $F_{2^t}$and by direct computation we have$f(x) = x^{2^k}$ as a monomialo-polynomials over F_{2^t}.

Next, we support theorem 4.1 with the following example.

Example 4.2: Let k = 4 and consider the polynomial $f(x) = x^{2^4} = x^{16}$. To prove the existence of this o-polynomial, we proceed as follows. Since $\gcd(2^4, 2^t - 1) = 1$ for all $t \in \mathbb{N}$, then $f(x) = x^{2^4}$ is a permutation polynomial. Notice that $\gcd(4,t) = 1$ whenever t is odd and by *(theorem 4.1)*, $f(x) = x^{2^4} = x^{16}$ is an o-polynomial.

As a consequence of the above theorem we deduced two results obtained by (Gupta and Sharma, 2016) as follows

Corollary 4.3:The polynomial $f(x) = x^2$ is a monomial o-polynomial of degree 2.

Proof: There are 4polynomials of degree 2 over F_{2^t}, these are$f_1(x) = x^2$, $f_2(x) = x^2 + x$, $f_3(x) = x^2 + x + 1$ *and* $f_4(x) = x^2 + 1$. Clearly for the polynomials$f_2(x), f_3(x)$ *and* $f_4(x)$, the polynomial function $f(x) = a$ has no unique solution for each $a \in F_2$, hence it is not a permutation polynomials by (*lemma 2.2(iv))*. For $f_1(x)$,$\gcd(2, 2^t - 1) = 1$ for all $t \in \mathbb{N}$, then by *(lemma 2.4)* $f_1(x)$ is a permutation polynomial. Moreover, since the $gcd(1,t) = 1$ for all positive number t and by *(theorem 4.1),*$f_1(x)$ is an o-polynomial of degree 2 . Hence $f_1(x) = x^2$ is a monomial o-polynomial of degree 2.

Corollary 4. 4: The polynomial $f(x) = x^4$ is a monomial o-polynomial of degree 4.

Proof. Here the only possible choices are polynomial of the form $(x) = a_1x^4 + a_2x^2$, where $a_1, a_2 \in F_{2^t}$. Let $f(x) = g(x^2)$with$g(x) = a_1x^2 + a_2x$, then $f(x)$ *and* $g(x)$ are multiplicative equivalent since there exists a positive integer $1 \leq 2 \leq 2^t - 1$ with $\gcd(2, 2^t - 1) = 1$. Since by definition $f(x)$ is a permutation polynomial if and only if $g(x)$ is a permutation polynomial. From (corollary 4.3), $g(x)$

is a permutation polynomial if $a_2 = 0$, $a_1 = 1$, and $g(x) = x^2$. Hence,$f(x) = x^4$ is a permutation polynomial. Notice that the $\gcd(4, t) = 1$ whenever t is a positive odd number and by *(theorem 4.1)*, the polynomial x^4 is a monomial o-polynomial.

5. CONCLUSION

Permutation polynomials over Galois fields are both interesting and important in theory and in many applications. We have studied some properties of monomialso-polynomials over Galois fields of characteristic 2and gave a necessary and sufficient condition foron monomials polynomials to be an o-polynomials, some existing results were deduced from our results.

REFERENCES

Dickson, L.E, (1897). The Analytic Representation of Substitutions on a Power of a Prime Number of Letters with a Discussion of the Linear Group, part I. Annals of Mathematics*.* 11:65–120.

Gupta,R., and Sharma, R.K.(2016).On Permutation Polynomials over Finite Fields of Characteristic Two. Journal of Algebra and its Applications.

Laigle-chapuy, Y. (2007). Permutation polynomials and Applications to Coding Theory. Journal of Finite Fields and its Applications

Li.J., Chandler, D.B. and Xiang. Q.(2010).Permutation polynomials of degree 6 or 7 over Finite fields of characteristic 2.Journal of Finite Fields and its Applications.

Lidl, R. and Gary, L.M. (1993). When Does a Polynomial over a Finite Field Permute the Elements of the Field?. Monthly Magazine of American Math.

Lidl, R.and Niederreiter, H. (1997).*Finite Fields, 2nd edition.* Cambridge University, Press. Cambridge, United Kingdom.

Xiang-dong, Hou. (2015). Permutation Polynomials over Finite Fields A survey of recent advances. Finite fields and Applications.

X. Hou., (2011). Two classes of Permutation Polynomials over Finite Fields. J. Comb. Theory, series

A.T. Hellesth and V. Zinoviev, (2003). New Kloosterman sums identities over $F_{2^m}$for all m. Finite fields and Applications.