Chapter

Some Proposed Problems on Permutation Polynomials over Finite Fields

Mritunjay Kumar Singh and Rajesh P. Singh

Abstract

From the 19th century, the theory of permutation polynomial over finite fields, that are arose in the work of Hermite and Dickson, has drawn general attention. Permutation polynomials over finite fields are an active area of research due to their rising applications in mathematics and engineering. The last three decades has seen rapid progress on the research on permutation polynomials due to their diverse applications in cryptography, coding theory, finite geometry, combinatorics and many more areas of mathematics and engineering. For this reason, the study of permutation polynomials is important nowadays. In this chapter, we propose some new problems in connection to permutation polynomials over finite fields by the help of prime numbers.

Keywords: finite field, permutation polynomial

1. Introduction to permutation polynomials

In this section, we collect some basic facts about permutation polynomials over a finite field that will be frequently used throught the chapter. First it will be convenient to define permutation polynomial over a finite field.

Definition 1. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a permutation polynomial over $\mathbb{F}_q$ for which the associated polynomial function $c \mapsto f(c)$ ia a permutation of $\mathbb{F}_q$, that is, the mapping from $\mathbb{F}_q$ to $\mathbb{F}_q$ defined by f is one–one and onto.

Finite fields are polynomially complete, that is, every mapping from $\mathbb{F}_q$ into $\mathbb{F}_q$ can be represented by a unique polynomial over $\mathbb{F}_q$. Given any arbitrary function $\phi : \mathbb{F}_q \to \mathbb{F}_q$, the unique polynomial $g \in \mathbb{F}_q[x]$ with $\deg(g) < q$ representing ϕ can be found by the formula $g(x) = \sum_{c \in \mathbb{F}_q} \phi(c)\left(1 - (x-c)^{q-1}\right)$, see ([1], Chapter 7).

Two polynomials represent the same function if and only if they are the same by reduction modulo $x^q - x$, according to the following result.

Lemma 1. *[1] For $f, g \in \mathbb{F}_q[x]$ we have $f(\alpha) = g(\alpha)$ for all $\alpha \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x) \pmod{(x^q - x)}$.*

Due to the finiteness of the field, the followings are the equivalent conditions for a polynomial to be a permutation polynomial.

Definition 2. The polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following conditions holds:

i. the function $f : c \mapsto f(c)$ is onto;

ii. the function $f : c \mapsto f(c)$ is one-to-one;

iii. $f(x) = a$ has a solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$;

iv. $f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.

1.1 Criteria for permutation polynomials

Some well-known criteria for being permutation polynomials are the following.

1.1.1 First criterion for permutation polynomials

The first and in some way most useful, criterion was proved by Hermite for q prime and by Dickson for general q. This criterion has special name what is called Hermite's criterion.

Theorem 3 (Hermite's criterion). *[1] A polynomial $f(x) \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if following two conditions hold:*

i. *$f(x)$ has exactly one root in $\mathbb{F}_q$;*

ii. *for each integer t with $1 \le t \le q-2$ and t not divisible by p, the residue $f(x)^t \pmod{(x^q - x)}$ has degree $\le q-2$.*

For the detailed proof, one can see [1]. Above theorem is mainly used to show negative result. The following is a useful corollary for this purpose.

Corollary 4. *There is no permutation polynomial of degree d dividing $q-1$ over $\mathbb{F}_q$.*

Proof. We note that $\deg\left(f^{\frac{q-1}{d}}\right) = q-1$. The proof follows from the last condition of Hermite's criterion.

Remark 5. Hermite's criterion is interesting theoretically but difficult to use in practice.

1.1.2 Second criterion for permutation polynomials

Theorem 6. *[1] Let $f \in \mathbb{F}_q[x]$. Write*

$$D(f) = \left\{ \frac{f(b) - f(a)}{b - a} : a \neq b \in \mathbb{F}_q \right\}.$$

Then $f(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $0 \notin D(f)$.

1.1.3 Third criterion for permutation polynomials

Theorem 7. *[1] The polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = 0$$

for all nontrivial additive characters χ of $\mathbb{F}_q$.

1.1.4 Fourth criterion for permutation polynomials

Theorem 8. *[1] Let the trace map $Tr : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be defined as $Tr(x) = x + x^q + \cdots + x^{q^{n-1}}$. Then the polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if for every nonzero $\eta \in \mathbb{F}_q$,*

$$\sum_{x \in \mathbb{F}_q} \zeta^{\mathrm{Tr}(\eta f(x))} = 0,$$

where $\zeta = e^{\frac{2\pi i}{p}}$ is a primitive p-th root of unity.

In what follows, we will discuss some well known classes of permutation polynomials which are commonly used.

1.2 Some well-known classes of permutation polynomials

In this subsection, several basic results on permutation polynomials are presented. Many times, we see that one of these general classes are obtained by simplifying complicated classes of permutation polynomials for proving their permutation nature.

Theorem 9. *[1] Every linear polynomial, that is, polynomial of the form $ax + b, a \neq 0$ over finite field is a permutation polynomial.*

Theorem 10. *[1] The monomial x^n is a permutation polynomial over $\mathbb{F}_q$ if and only if* $\gcd(n, q-1) = 1$.

Theorem 11. *Let $g(x)$ and $h(x)$ be two polynomials over $\mathbb{F}_q$. Then $f(x) = g(h(x))$ is a permutation polynomial over $\mathbb{F}_q$ if and only if both $g(x)$ and $h(x)$ permute $\mathbb{F}_q$.*

1.3 Open problems on permutation polynomials

Very little is known concerning which polynomials are permutation polynomials, despite the attention of numerous authors. There are so many open problems and conjectures on permutation polynomials over finite fields but here we are listing few of them.

Open Problem 12. [2] Find new classes of permutation polynomials of $\mathbb{F}_q$.

Although several classes of permutation polynomials have been found in recent years, but, an explicit and unified characterization of permutation polynomials is not known and seems to be elusive today. Therefore, it is both interesting and important to find more explicit classes of permutation polynomials.

Open Problem 13. [2] Find inverse polynomial of known classes of permutation polynomials over $\mathbb{F}_q$.

The construction of permutation polynomials over finite fields is an old and difficult problem that continues to attract interest due to their applications in various area of mathematics. However, the problem of determining the compositional inverse of known classes of permutation polynomial seems to be an even more complicated problem. In fact, there are very few known permutation polynomials whose explicit compositional inverses have been obtained, and the resulting expressions are usually of a complicated nature except for the classes of the permutation linear polynomials, monomials, Dickson polynomials.

Open Problem 14. [2] Find N_d, where $N_d = N_d(q)$ denote the number of permutation polynomials of degree d over $\mathbb{F}_q$.

To date, there is no method for counting the exact number of permutation polynomials of given degree. However, Koyagin and Pappalardi [3, 4], found the

asymptotic formula for the number of permutations for which the associated permutation polynomial has degree smaller than $q-2$.

1.4 Applications of permutation polynomials

The study of permutation polynomials would not complete without mentioning their applications in other area of mathematics and engineering. It is a major subject in the theory and applications of finite fields. The study of permutation polynomials over the finite fields is essentially about relations between the algebraic and combinatoric structures of finite fields. Nontrivial permutation polynomials are usually the results of the intricate and sometimes mysterious interplay between the two structures. Here we mention some applications of permutation polynomials.

1.5 Coding theory

In coding theory, error correcting codes are fundamental to many digital communication and storage systems, to improve the error performance over noisy channels. First proposed in the seminal work of Claude Shannon [5], they are now ubiquitous and included even in consumer electronic systems such as compact disc players and many others. Permutation polynomials have been used to construct error correcting codes. Laigle-Chapuy [6] proposed a conjecture equivalent to a conjecture related to cross-correlation functions in coding theory. In [7], Chunlei and Helleseth derived several classes of p-ary quasi-perfect codes using permutation polynomials over finite fields. In 2005, Carlet, Ding and Yuan [8] obtained Linear codes using planar polynomials over finite fields.

1.6 Cryptography

The advent of public key cryptography in the 1970's has generated innumerable security protocols which find widespread application in securing digital communications, electronic funds transfer, email, internet transactions and the like. In recent years, permutation polynomials over finite fields has been used to design public key cryptosystem. Singh, Saikia and Sarma [9–15] designed efficient multivariate public key cryptosystem using permutation polynomials over finite fields. The same authors used a group of linearized permutation polynomials to design an efficient multivariate public key cryptosystem [16].

Permutation polynomials with low differential uniformity are important candidate functions to design substitution boxes (S-boxes) of block ciphers. S-boxes can be constructed from permutation polynomials over even characteristics [17] with desired cryptographic properties such as low differential uniformity and play important role in iterated block ciphers.

1.7 Finite geometry

Permutation polynomial $f(x) \in \mathbb{F}_q[x]$ is called a complete permutation polynomial if $f(x)+x$ is also a permutation polynomial and an orthomorphism polynomial if $f(x)-x$ is also a permutation polynomial. Orthomorphism polynomials can be used in check digit systems to detect single errors and adjacent transpositions whereas complete permutation polynomials to detect single and twin errors. For more details on complete mappings and orthomorphisms over finite fields, we refer to the reader [3–19]. In addition, complete permutation polynomials are very useful in the study of orthogonal latin squares and orthomorphism polynomials are useful

in close connection to hyperovals in finite projective plane. In 1968, planar functions were introduced by Dembowski and Ostrom [20] in context of finite geometry to describe projective planes with specific properties. Since 1991, planar functions have attracted interest also from cryptography as functions with optimal resistance to differential cryptanalysis.

2. Some proposed problems

Let $\mathbb{F}_q$ denotes finite fields with $q = 2^m$ elements. Nowaday permutation polynomials are an interesting subject for study not for only research purposes but also for their various applications in many areas of mathematics and engineering. We refer [21] to the reader for recent advances and contributions to the area.

The rising applications of permutation polynomials in mathematics and engineering from last decade propels us to do new research. Recently, permutation polynomials with few terms over finite fields paying more attention due to their simple algebraic form and some extraordinary properties. We refer to the reader [22–25] for some recent developments. This motivates us to propose some new problems. In this chapter, by the help of prime numbers, we constructed several new polynomials that have no root in μ_{2^m+1} and two of them are generalizations of known ones. The constructed polynomials here may lay a good foundation for finding new classes of permutation polynomials.

Throughout the chapter, for a positive integer d, the set of d-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ is denoted by μ_d. That is,

$$\mu_d = \left\{x \in \overline{\mathbb{F}}_q : x^d = 1\right\}.$$

For every element $x \in \mathbb{F}_q$, we denote x^{2^m} by $\overline{x}$ in analogous to the usual complex conjugation. Clearly, $x\overline{x}, x + \overline{x} \in \mathbb{F}_q$. Define the unit circle of $\mathbb{F}_q$ as

$$\mu_{2^m+1} = \left\{x \in \mathbb{F}_q : x^{2^m+1} = x\overline{x} = 1\right\}.$$

The permutation polynomial of the form $x^r h\left(x^{\frac{q-1}{d}}\right)$ are interesting and have been paid attention, where $h(x) \in \mathbb{F}_q[x]$ with d dividing $q-1$ and $1 \le r \le \frac{q-1}{d}$. The permutation behavior of this type of polynomials are investigated by Park and Lee [26] and Zieve [27].

Lemma 2 ([26, 27]). *Let $r, d > 0$ with d dividing $q-1$ and $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h\left(x^{\frac{q-1}{d}}\right)$ permutes $\mathbb{F}_q$ if and only if*

i. $\gcd\left(r, \frac{q-1}{d}\right) = 1$ *and*

ii. $x^r h(x)^{\frac{q-1}{d}}$ *permutes* μ_d.

In view of Lemma 2, the permutation property of $x^r h\left(x^{\frac{q-1}{d}}\right)$ is decided by whether $x^r h(x)^{\frac{q-1}{d}}$ permutes μ_d. In the process to prove that $x^r h(x)^{\frac{q-1}{d}}$ permutes μ_d, first we need to prove that $h(x)$ has no root in μ_d [22]. Thus the polynomials which have no roots in μ_d are interesting and can be used to construct new classes of permutation polynomials. Therefore, it is is both interesting and important to find more polynomials that have no roots in μ_d which play key role in showing the

permutation property of $x^r h(x)^{\frac{q-1}{d}}$. For more recent progresses about this type of constructions, we refer [23, 25]. In next section, we also need the following definition.

Definition 15. Two polynomials are said to be conjugate to each other if one is obtained by raising 2^m-th power and multiplying them by the highest degree term of the other.

Next, we propose some new problems by reviewing various recent contributions. The polynomials that have no roots in μ_{2^m+1} play important role in theory of finite fields because these polynomials may give rise to a new class of permutation polynomials.

Let $p \in \{1, 2, \ldots, 2^m - 1\}$, and let the binary representation of p be

$$p = \sum_{k=0}^{m-1} p_k \, 2^k$$

with $p_k \in \{0, 1\}$. Define the weight of p by

$$w(p) = \sum_{k=0}^{m-1} p_k.$$

We define a polynomial function over $\mathbb{F}_{2^m}$ as

$$L_p(x) = \sum_{k=0}^{m-1} p_k \cdot x^{2^k}.$$

For example,

$$L_{11}(x) = 1 + x + x^3$$

$$L_{13}(x) = 1 + x^2 + x^3$$

$$L_{19}(x) = 1 + x + x^4.$$

We observe that there is a good connection between prime numbers and polynomials that have no roots in μ_{2^m+1} in the sense that most of these polynomials can be derived from prime numbers. In this way, for the prime numbers 11, 13 and 19 we get the polynomials $L_{11}(x), L_{13}(x)$ and $L_{19}(x)$ respectively that have no roots in μ_{2^m+1}. This result is obtained by Gupta and Sharma in [22]. More precisely,

Lemma 3 ([22]). *Let $m > 0$ be integer. Then each of the polynomials $1 + x + x^3, 1 + x^2 + x^3$ and $1 + x + x^4$ have no roots in μ_{2^m+1}.*

Similarly, for the primes 59 and 109, we obtain the same polynomials as in [25] of Xu Guangkui et al.

Lemma 4 ([25]). *Let $m > 0$ be integer. Then each of the polynomials $1 + x + x^3 + x^4 + x^5$ and $1 + x^2 + x^3 + x^5 + x^6$ have no roots in μ_{2^m+1}.*

It is not necessary that all polynomials are obtained from prime numbers. For example, the polynomials $1 + x^3 + x^4$ by Gupta and Sharma in [22] and $1 + x + x^2 + x^4 + x^5$ by Xu Guangkui et al. [25] are obtained corresponding to the number 25 and 55 respectively. In this respect, we propose the following problem.

Problem 16. *Which prime numbers will give polynomials that have no roots in μ_{2^m+1}?.*

The generalization of Lemma 2.2 of [22] corresponding to the polynomials $1 + x + x^3$ and $1 + x^2 + x^3$ are given by the following lemma.

Lemma 5. *For sufficiently large positive integers m and n, each of the polynomials* $1+x^n+x^{2n-1}$ *and* $1+x^n+x^{2n+1}$ *have no roots in* μ_{2^m+1}.

Proof. Suppose $\alpha \in \mu_{2^m+1}$ satisfies the equation

$$1+\alpha^n+\alpha^{2n-1}=0. \tag{1}$$

Raising both sides of (1) to the 2^m-th power and multiplying by α^{2n-1}, we get

$$1+\alpha^{n-1}+\alpha^{2n-1}=0. \tag{2}$$

Adding (1) and (2), we get

$$\alpha^{n-1}+\alpha^n=0$$

Since $\alpha \neq 0$, which gives $\alpha=1$. But $\alpha=1$ does not satisfy (1), a contradiction. Hence $1+x^n+x^{2n-1}$ has no roots in μ_{2^m+1}. Similarly, we can show that the polynomial $1+x^n+x^{2n+1}$ has no roots in μ_{2^m+1}.

In particular, we get the following lemma by Gupta and Sharma [22].

Lemma 6 ([22]). *Let* $m>0$ *be integer. Then each of the polynomials* $1+x+x^3$ *and* $1+x^2+x^3$ *have no roots in* μ_{2^m+1}.

Based on the Lemma 5, we propose the following problem.

Problem 17. *Let* $h_1(x)=1+x^n+x^{2n-1}$ *and* $h_2(x)=1+x^n+x^{2n+1}$. *Characterize n and r such that the polynomials* $x^r h_1(x)^{2^m-1}$ *and* $x^r h_2(x)^{2^m-1}$ *permutes* μ_{2^m+1}.

By the help of prime numbers below 1000, we obtain the following polynomials that have no roots in μ_{2^m+1}. Most of these polynomials are directly or indirectly associated with prime numbers in the sense that corresponding to either each polynomial or their conjugate polynomial, a prime number can be obtained. The proof of the following lemmas can be done in similar fashion as in [22].

Lemma 7. *For a positive integer m, each of the polynomials* $1+x+x^2+x^7+x^8$, $1+x+x^6+x^7+x^8$, $1+x+x^3+x^7+x^8$, $1+x+x^5+x^7+x^8$, $1+x+x^4+x^8+x^9$, $1+x+x^5+x^8+x^9$, $1+x^2+x^3+x^5+x^8$, $1+x^3+x^5+x^6+x^8$, $1+x+x^3+x^4+x^8$, $1+x^4+x^5+x^7+x^8$, $1+x^2+x^3+x^6+x^8$, $1+x^2+x^5+x^6+x^8$, $1+x^3+x^4+x^7+x^8$, $1+x+x^4+x^5+x^8$, $1+x^3+x^4+x^6+x^9$, $1+x^3+x^5+x^6+x^9$, $1+x+x^2+x^7+x^9$, $1+x^2+x^7+x^8+x^9$, $1+x^2+x^4+x^7+x^9$, $1+x^2+x^5+x^7+x^9$ *have no roots in* μ_{2^m+1}.

Lemma 8. *For a positive integer m, each of the polynomials* $1+x+x^3+x^5+x^6+x^7+x^8$, $1+x+x^2+x^3+x^5+x^7+x^8$, $1+x+x^2+x^3+x^6+x^7+x^8$, $1+x+x^2+x^5+x^6+x^7+x^8$, $1+x+x^4+x^5+x^6+x^7+x^8$, $1+x+x^2+x^3+x^4+x^7+x^8$, $1+x+x^3+x^5+x^6+x^8+x^9$, $1+x+x^3+x^4+x^6+x^8+x^9$, $1+x+x^3+x^4+x^5+x^8+x^9$, $1+x+x^4+x^5+x^6+x^8+x^9$, $1+x+x^2+x^3+x^7+x^8+x^9$, $1+x+x^2+x^6+x^7+x^8+x^9$, $1+x+x^2+x^4+x^7+x^8+x^9$, $1+x+x^2+x^5+x^7+x^8+x^9$, $1+x^2+x^3+x^4+x^6+x^7+x^9$, $1+x^2+x^3+x^5+x^6+x^7+x^9$, $1+x^2+x^3+x^4+x^5+x^7+x^9$, $1+x^2+x^4+x^5+x^6+x^7+x^9$, *have no roots in* μ_{2^m+1}.

Lemma 9. *For a positive integer m, each of the polynomials* $1+x+x^2+x^3+x^4+x^6+x^7+x^8+x^9$, $1+x+x^2+x^3+x^5+x^6+x^7+x^8+x^9$ *have no roots in* μ_{2^m+1}.

The above list of polynomials are not complete. However, computational experiments shows that there should be more polynomials. A complete determination of all polynomials with few terms over finite fields seems to be out of reach for the time bing.

Now, we are in condition to propose the following problem in connection to above three lemmas.

Problem 18. *Find new classes of permutation polynomials corresponding to polynomials obtained in Lemmas 7, 8 and 9.*

Classification

AMS 2020 MSC: 11T06.

Author details

Mritunjay Kumar Singh[1*] and Rajesh P. Singh[2]

1 Government Polytechnic, Gaya, Bihar, India

2 Department of Mathematics, Central University of South Bihar, Gaya, Bihar, India

*Address all correspondence to: mmathbhu2012@gmail.com

References

[1] R. Lidl, H. Niederreiter, Finite fields, Vol. 20, Cambridge University Press, 1997.

[2] R. Lidl, G. L. Mullen, When does a polynomial over a finite field permute the elements of the field?, Amer. Math. Monthly 95 (3) (1988) 243–246.

[3] S. Konyagin, F. Pappalardi, Enumerating permutation polynomials over finite fields by degree, Finite Fields Appl. 8 (4) (2002) 548–553.

[4] S. Konyagin, F. Pappalardi, Enumerating permutation polynomials over finite fields by degree ii, Finite Fields Appl. 12 (1) (2006) 26–37.

[5] C. E. Shannon, A mathematical theory of communication, The Bell system technical journal 27 (3) (1948) 379–423.

[6] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields and Their Applications 13 (1) (2007) 58–70.

[7] C. Li, T. Helleseth, Quasi-perfect linear codes from planar and apn functions, Cryptography and Communications 8 (2) (2016) 215–227.

[8] C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Trans. Inform. Theory 51 (6) (2005) 2089–2102.

[9] W.-S. Chou, Set complete mappings of finite fields, finite fields, coding theory and advances in communications and computing (1991).

[10] W.-S. Chou, H. Niederreiter, Monomials and binomials over finite fields as r-orthomorphisms (2002).

[11] G. L. Mullen, H. Niederreiter, Dickson polynomials over finite fields and complete mappings, Canadian Mathematical Bulletin 30 (1) (1987) 19–27.

[12] H. Niederreiter, K. H. Robinson, Complete mappings of finite fields, Journal of the Australian Mathematical Society 33 (2) (1982) 197–212.

[13] H. Niederreiter, A. Winterhof, Cyclotomic r-orthomorphisms of finite fields, Discrete mathematics 295 (1–3) (2005) 161–171.

[14] Q. Sun, Q. Zhang, A simple proof of a conjecture about complete mapping over finite fields, Journal-Sichuan University Natural Science Edition 35 (1998) 842–847.

[15] Y. Yuan, Y. Tong, H. Zhang, Complete mapping polynomials over finite field $\mathbb{F}_{16}$, in: International Workshop on the Arithmetic of Finite Fields, Springer, 2007, pp. 147–158.

[16] R. P. Singh, B. K. Sarma, A. Saikia, Public key cryptosystem using a group of permutation polynomials, Tatra Mt. Math. Publ. 77 (2020) 1–24.

[17] K. Nyberg, Differentially uniform mappings for cryptography, in: Workshop on the Theory and Application of of Cryptographic Techniques, Springer, 1993, pp. 55–64.

[18] R. P. Singh, A. Saikia, B. Sarma, Little dragon two: An efficient multivariate public key cryptosystem, Int. J. Netw. Secur. Appl. 2 (2) (2010) 1–10.

[19] R. P. Singh, A. Saikia, B. K. Sarma, Poly-dragon: An efficient multivariate public key cryptosystem, J. Math. Cryptol. 4 (4) (2011) 349–364.

[20] P. Dembowski, T. G. Ostrom, Planes of ordern with collineation groups of order n^2, Math. Z. 103 (3) (1968) 239–258.

[21] X. Hou, Permutation polynomials over finite fields—A survey of recent advances, Finite Fields and Their Applications 32 (2015) 82–119.

[22] R. Gupta, R. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, Finite Fields and Their Applications 41 (2016) 89–96.

[23] Z. Zha, L. Hu, S. Fan, Further results on permutation trinomials over finite fields with even characteristic, Finite Fields and Their Applications 45 (2017) 43–52.

[24] K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, Finite Fields and Their Applications 43 (2017) 69–85.

[25] G. Xu, X. Cao, J. Ping, Some permutation pentanomials over finite fields with even characteristic, Finite Fields and Their Applications 49 (2018) 212–226.

[26] Y. H. Park, J. B. Lee, Permutation polynomials and group permutation polynomials, Bulletin of the Australian Mathematical Society 63 (1) (2001) 67–74.

[27] M. E. Zieve, On some permutation polynomials over $_q$ of the form $x^r f\left(x^{(q-1)/d}\right)$, Proceedings of the American Mathematical Society 137 (7) (2009) 2209–2216.