On Inverses of Permutation Polynomials of Small Degree Over Finite Fields

Yanbin Zheng, Qiang Wang, and Wenhong Wei

***Abstract*— Permutation polynomials (PPs) and their inverses have applications in cryptography, coding theory and combinatorial design theory. In this paper, we make a brief summary of the inverses of PPs of finite fields, and give the inverses of all PPs of degree ≤ 6 over finite fields $\mathbb{F}_q$ for all q and the inverses of all PPs of degree 7 over $\mathbb{F}_{2^n}$. The explicit inverse of a class of fifth degree PPs is the main result, which is obtained by using Lucas' theorem, some congruences of binomial coefficients, and a known formula for the inverses of PPs of finite fields.**

***Index Terms*— Finite fields, permutation polynomials, inverses, binomial coefficients.**

I. Introduction

FOR a prime power q, let $\mathbb{F}_q$ denote the finite field with q elements, $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, and $\mathbb{F}_q[x]$ the ring of polynomials over $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if it induces a bijection from $\mathbb{F}_q$ to itself. Hence for any PP f of $\mathbb{F}_q$, there exists a polynomial $f^{-1} \in \mathbb{F}_q[x]$ such that $f^{-1}(f(c)) = c$ for each $c \in \mathbb{F}_q$ or equivalently $f^{-1}(f(x)) \equiv x \pmod{x^q - x}$, and f^{-1} is unique in the sense of reduction modulo $x^q - x$. Here f^{-1} is defined as the composition inverse of f on $\mathbb{F}_q$, and we simply call it the inverse of f.

PPs of finite fields have been extensively studied for their applications in coding theory, combinatorial design theory, cryptography, etc. For instance, some PPs of $\mathbb{F}_{2^m}$ were used in [14] to construct binary cyclic codes. The Dickson PPs of degree 5 of $\mathbb{F}_{3^m}$ were employed in [13] to construct new examples of skew Hadamard difference sets, which are inequivalent to the classical Paley difference sets. In block ciphers, a permutation is often used as an S-box to build the confusion layer during the encryption process and the inverse is needed while decrypting the cipher. PPs are useful in the construction of bent functions [11], [29], [30], which have optimal nonlinearity for offering resistance against the fast correlation attack on stream ciphers and the linear attack on block ciphers. PPs were employed in [16] to construct circular Costas arrays, which are useful in sonar and radar communications. PPs were also applied in the construction of check digit systems that detect the most frequent errors [37], [47].

The study of PPs of finite fields has a long history. In 1897, Dickson [12] listed all **normalized** PPs of degree ≤ 5 of $\mathbb{F}_q$ for all q, and classified all PPs of degree 6 of $\mathbb{F}_q$ for odd q. In 2010, the complete classification of PPs of degree 6 and 7 of $\mathbb{F}_{2^n}$ was settled in [22]. In recent years, a lot of progress has been made on the constructions of PPs of finite fields; see for example [18], [23], [27], [53], [54] for permutation binomials and trinomials of the form $x^r h(x^{q-1})$ of $\mathbb{F}_{q^2}$, see [42], [56] for PPs of the form $(x^q - x + c)^s + L(x)$ of $\mathbb{F}_{q^2}$, see [26], [60] for PPs of the form $(ax^q + bx + c)^r \phi((ax^q + bx + c)^s) + ux^q + vx$ of $\mathbb{F}_{q^2}$, see [3]–[6] for PPs of the form $x^s + \gamma h(f(x))$, see [24] for PPs with low boomerang uniformity. For a detailed introduction to the developments on PPs, we refer the reader to [19], [28], [32] and the references therein.

The problem of explicitly determining the inverses of these PPs is a more challenging problem. In theory one could directly use the Lagrange interpolation formula, but for large finite fields this becomes very inefficient. In fact, there are few known classes of PPs whose inverses have been obtained explicitly. It is also interesting to note that the explicit formulae of inverses of low degree PPs have been neglected in the literature. This motivates us to give a short review of the progress in this topic and find explicit expressions of inverses of all classes of PPs of degree ≤ 7 in [12], [22], [38].

The rest of the paper is organized as follows. Section II gives a brief summary of the results concerning the inverses of PPs of finite fields. In Section III, we obtain the inverses of all PPs of degree 6 of finite fields $\mathbb{F}_q$ for all q and the inverses of all PPs of degree 7 of $\mathbb{F}_{2^n}$. For simplicity, we only list

Manuscript received December 1, 2018; revised July 5, 2019; accepted August 9, 2019. Date of publication September 3, 2019; date of current version January 20, 2020. This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802000, in part by the National NSF of China under Grant 61602125, Grant 61702124, Grant 61862011, Grant 61862012, and Grant 61802221, in part by the China Postdoctoral Science Foundation under Grant 2018M633041, in part by the NSF of Guangxi under Grant 2016GXNSFBA380153 and Grant 2017GXNSFAA198192, in part by the Guangxi Science and Technology Plan Project under Grant AD18281065, in part by the Guangxi Key Laboratory of Cryptography and Information Security under Grant GCIS201817, in part by the research start-up grants of Dongguan University of Technology, in part by the Guangdong Provincial Science and Technology Plan Projects under Grant 2016A010101034 and Grant 2016A010101035, in part by the Key Research and Development Program for Guangdong Province under Grant 2019B010136001, and in part by the Peng Cheng Laboratory Project of Guangdong Province under Grant PCL2018KP005 and Grant PCL2018KP004. The work of Q. Wang was supported by the NSERC of Canada.

Y. Zheng is with the School of Computer Science and Technology, Dongguan University of Technology, Dongguan 523808, China, with the Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin 541004, China, with the School of Computer Science and Engineering, South China University of Technology, Guangzhou 510006, China, and also with the Peng Cheng Laboratory, Shenzhen 518055, China (e-mail: zhengyanbin@guet.edu.cn).

Q. Wang is with the School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada (e-mail: wang@math.carleton.ca).

W. Wei is with the School of Computer Science and Technology, Dongguan University of Technology, Dongguan 523808, China (e-mail: 2017164@dgut.edu.cn).

Communicated by V. Sidorenko, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2019.2939113

TABLE I

ALL NORMALIZED PPs OF DEGREE ≤ 5 AND THEIR INVERSES

Normalized PPs of $\mathbb{F}_q$	Inverses	q $(n \geq 1)$	Reference
x	x	any q	
x^2	$x^{q/2}$	$q = 2^n$	
x^3	$x^{(aq-a+1)/3}$ $(a \equiv 1 - q \pmod 3)$	$q \not\equiv 1 \pmod 3$	Thm 2
$x^3 - ax$ (a not a square)	$\sum_{i=0}^{n-1} a^{-\frac{3^{i+1}-1}{2}} x^{3^i}$	$q = 3^n$	[9,48]
x^4	$x^{q/4}$	$q = 2^n$	Thm 2
$x^4 \pm 3x$	$\mp(x^4 - 3x)$	$q = 7$	
$x^4 + ax$ (a not a cube)	$a^{\frac{q-1}{3}}(1 + a^{\frac{q-1}{3}})^{-1} \sum_{i=0}^{n-1} a^{-\frac{4^{i+1}-1}{3}} x^{4^i}$	$q = 2^{2n}$	[9,48]
$x^4 + bx^2 + ax$ $(ab \neq 0, S_n + aS_{n-2}^2 = 1)^*$	$\sum_{i=0}^{n-1} \big(S_{n-2-i}^{2^{i+1}} + a^{1-2^{i+1}} S_i\big) x^{2^i}$	$q = 2^n$	Cor 4
x^5	$x^{(aq-a+1)/5}$ $(a \equiv (1-q)^3 \pmod 5)$	$q \not\equiv 1 \pmod 5$	Thm 2
$x^5 + ax$ $(a^2 = 2)$	$x^5 + ax$	$q = 9$	
$x^5 - ax$ (a not a fourth power)	$a^{\frac{q-1}{4}}(1 - a^{\frac{q-1}{4}})^{-1} \sum_{i=0}^{n-1} a^{-\frac{5^{i+1}-1}{4}} x^{5^i}$	$q = 5^n$	[9,48]
$x^5 \pm 2x^2$	$x^5 \mp 2x^2$	$q = 7$	
$x^5 + ax^3 + 3a^2x$ (a not a square)	$-a^2x^9 - ax^7 + 4x^5 + 4a^5x^3 - 5a^4x$	$q = 13$	
$x^5 + ax^3 + 5^{-1}a^2x$ $(a \neq 0)^\dagger$	$\sum_{i=1}^{\lfloor m/2 \rfloor} \frac{m}{m-i}\binom{m-i}{i}(5^{-1}a)^{5i} x^{m-2i}$ $(m = \frac{3q^2-2}{5})$	$q \equiv \pm 2 \pmod 5$	[25, Lem 4.8]
$x^5 - 2ax^3 + a^2x$ (a not a square)	$\sum_{j=0}^{n-1} \sum_{i=0}^{j} a^{-\frac{q+5^{i+1}+5^{j+1}-3}{4}} b_{ij} x^{\frac{q+5^i+5^j-1}{2}}$	$q = 5^n$	Thm 8
$x^5 + ax^3 \pm x^2 + 3a^2x$ (a not a square)	$x^5 \pm (2ax^4 - 2x^2) + a^2x^3 + ax$	$q = 7$	

[*] In [28, Table 7.1], the PP $L(x) = x^4 + bx^2 + ax$ (if its only root in $\mathbb{F}_{2^n}$ is 0) was listed. Since $x^4 + bx^2$ is not a PP of $\mathbb{F}_{2^n}$ for any $b \in \mathbb{F}_{2^n}^*$, we divide $L(x)$ into x^4, $x^4 + ax$ (a not a cube), and $x^4 + bx^2 + ax$ ($ab \neq 0$, $S_n + aS_{n-2}^2 = 1$) in Table I. The motivation is to give the explicit inverses of x^4 and $x^4 + ax$. The sequence $\{S_i\}$ is defined as follows: $S_{-1} = 0$, $S_0 = 1$, $S_i = b^{2^{i-1}} S_{i-1} + a^{2^{i-1}} S_{i-2}$ for $1 \leq i \leq n$.

[†] The normalized PPs $x^5 + ax^3 + 5^{-1}a^2x$ (a arbitrary) of $\mathbb{F}_q$ with $q \equiv \pm 2 \pmod 5$ appeared in [28, Table 7.1]. Since the case $a = 0$ is a part of the normalized PP x^5 of $\mathbb{F}_q$ with $q \not\equiv 1 \pmod 5$, we impose a restriction $a \neq 0$.

[‡] In the expressions of the inverses, $\lfloor m/2 \rfloor$ denotes the largest integer $\leq m/2$, $b_{ij} = 1$ if $i < j$ and $b_{ij} = 3$ if $i = j$.

in Table I all **normalized** PPs of degree ≤ 5 and their inverses. In particular, the inverse of PP $F(x) = x^5 - 2ax^3 + a^2x$ of $\mathbb{F}_{5^n}$ is the main result of this paper; see Theorem 8. Section IV starts with a formula for the inverse of an arbitrary PP, which was first presented in [33]. This formula provides all the coefficients of the inverse of a PP $f(x)$ by computing the coefficients of x^{q-2} in $f(x)^k \pmod{x^q - x}$ for $1 \leq i \leq q-2$. Based on this method, we convert the problem of computing $F^{-1}(x)$ into the problem of finding the values of four classes of binomial coefficients. Section V gives the explicit values of these binomial coefficients by using Lucas' theorem and several congruences of binomial coefficients modulo 5.

II. PPs AND THEIR INVERSES

We now give a brief summary of the results concerning the inverses of PPs of finite fields, some of which will be used in the next section.

Linear PPs. For $a \neq 0$, $b \in \mathbb{F}_q$, $ax + b$ is a PP of $\mathbb{F}_q$ and its inverse is $a^{-1}(x - b)$.

Monomials. For positive integer n, x^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$. In this case, the inverse is x^m, where $mn \equiv 1 \pmod{q-1}$. In particular, the inverses of x^n on $\mathbb{F}_{2^t}$ for some APN exponents n were given explicitly in [21].

Dickson PPs. The Dickson polynomial $D_n(x, a)$ of the first kind of degree n with parameter $a \in \mathbb{F}_q$ is given as

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i},$$

where $\lfloor n/2 \rfloor$ denotes the largest integer $\leq n/2$. It is known that $D_n(x, a)$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q^2 - 1) = 1$. Its inverse was determined in [25] by the following lemma.

Lemma 1. [25, Lemma 4.8] *Let m, n be positive integers such that $mn \equiv 1 \pmod{q^2 - 1}$. Then the inverse of $D_n(x, a)$ on $\mathbb{F}_q$ is $D_m(x, a^n)$.*

PPs of the form $\mathbf{x^r h(x^s)}$. The first systematic study of PPs of $\mathbb{F}_q$ of the form $f(x) = x^r h(x^s)$ was made in [41], where $q - 1 = ds$, $1 \leq r < s$ and $h \in \mathbb{F}_q[x]$. A criterion for f to be a PP of $\mathbb{F}_q$ was given in [41]. Later on, several equivalent criteria were found in other papers; see for instance [35], [43], [61]. Essentially, it says that f is a PP of $\mathbb{F}_q$ if and only if $\gcd(r, s) = 1$ and $x^r h(x)^s$ permutes $U_d := \{1, \omega, \cdots, \omega^{d-1}\}$, where ω is a primitive d-th root of unity of $\mathbb{F}_q$. [33, Theorem 1] characterized all the coefficients of the inverse of $x^r g(x^s)^d$ on $\mathbb{F}_q$, where $\gcd(r, q-1) = 1$. This result was generalized in [44], and the inverse of f on $\mathbb{F}_q$ was given by

$$f^{-1}(x) = \frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1} \omega^{i(t-jr)}\big(x/h(\omega^i)\big)^{\widetilde{r}+js},$$

where $1 \leq \widetilde{r} < s$ and $r\widetilde{r} + st = 1$. This inverse was obtained later in [58] by a piecewise method. When $\gcd(r, q-1) = 1$, the inverses of f on $\mathbb{F}_q$ was given in [25] by

$$f^{-1}(x) = \big(x^{q-s} h(\ell(x^s))^{s-1}\big)^{r'} \ell(x^s),$$

where $rr' \equiv 1 \pmod{q-1}$ and $\ell(x)$ is the inverse of $x^r h(x)^s$ on U_d. The method employed in [25] is a multiplicative analogue of [39] and [51].

Linearized PPs. Suppose $L(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$. It is known that L is a PP of $\mathbb{F}_{q^n}$ if and only if the associate Dickson matrix

$$D_L := \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}$$

is nonsingular [28, Page 362]. In this case, the inverse was given in [52, Theorem 4.8] by

$$L^{-1}(x) = (\det(D_L))^{-1} \sum_{i=0}^{n-1} \bar{a}_i x^{q^i},$$

where $\bar{a}_i$ is the $(i,0)$-th cofactor of D_L, i.e., the determinant of D_L is $\det(D_L) = a_0\bar{a}_0 + \sum_{i=1}^{n-1} a_{n-i}^{q^i}\bar{a}_i$. The inverses of some special linearized PPs were also obtained; see [48] for the inverse of arbitrary linearized permutation binomial, see [49], [50] for the inverse of $x + x^2 + \mathrm{Tr}(x/a)$ on $\mathbb{F}_{2^n}$. Very recently, linearized PPs of the form $L(x) + K(x)$ of $\mathbb{F}_{q^n}$ and their inverses are presented in [36, Theorem 3.1], where L is a linearized PP of $\mathbb{F}_{q^n}$ and K is a nilpotent linearized polynomial such that $L \circ K = K \circ L$.

Bilinear PPs. The product of two linear functions is a bilinear function. Let q be even and n be odd. The inverse of bilinear PPs $x(\mathrm{Tr}_{q^n/q}(x) + ax)$ of $\mathbb{F}_{q^n}$ was obtained in [10], where $a \in \mathbb{F}_q \setminus \mathbb{F}_2$. The inverse of more general bilinear PPs

$$f(x) = x(L(\mathrm{Tr}_{q^n/q}(x)) + a\mathrm{Tr}_{q^n/q}(x) + ax)$$

of $\mathbb{F}_{q^n}$ was given in [51] in terms of the inverse of bilinear PP $xL(x)$ when restricted to $\mathbb{F}_q$, where $a \in \mathbb{F}_q^*$ and $L \in \mathbb{F}_q[x]$ is a 2-polynomial.

PPs of the form $\mathbf{x^s + \gamma h(f(x))}$. Let $\gamma \in \mathbb{F}_{q^n}^*$ be a b-linear translator with respect to $\mathbb{F}_q$ for the mapping $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$, i.e., $f(x + u\gamma) - f(x) = ub$ holds for all $x \in \mathbb{F}_{q^n}$, all $u \in \mathbb{F}_q$ and a fixed $b \in \mathbb{F}_q$. [20, Theorem 8] stated that $F_1(x) = x + \gamma f(x)$ is a PP of $\mathbb{F}_{q^n}$ if $b \neq -1$ (it is actually also a necessary condition). Its inverse was given in [20, Theorem 3] by $F_1^{-1}(x) = x - \frac{\gamma}{b+1} f(x)$. Let h be an arbitrary mapping from $\mathbb{F}_q$ to itself. [20, Theorem 6] stated that $F_2(x) = x + \gamma h(f(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $u + bh(u)$ permutes $\mathbb{F}_q$. When $b = 0$, the inverse was given in [3, Proposition 4] by $F_2^{-1}(x) = x + (p-1)\gamma h(f(x))$, where p is the characteristic of $\mathbb{F}_{q^n}$. PPs of the form $F_3(x) = x^s + \alpha\mathrm{Tr}(x^t)$ of $\mathbb{F}_{2^n}$ were studied in [4]–[6], where $1 \leq s, t \leq 2^n - 2$, $\alpha \in \mathbb{F}_{2^n}^*$, and Tr is the absolute trace function. A criterion for F_3 to be a PP of $\mathbb{F}_{2^n}$ was given in [5], [6]. If F_3 is a PP of $\mathbb{F}_{2^n}$ and $t = s(2^i + 1)$ for some $0 \leq i \leq n-1$ and $i \neq n/2$, then the inverse is given in [6, Theorem 4] by $F_3^{-1}(x) = (x + \alpha\mathrm{Tr}(x^{2^i+1}))^r$, where r is the inverse of s modulo $2^n - 1$.

Involutions. An involution is a permutation such that its inverse is itself. A systematic study of involutions over $\mathbb{F}_{2^n}$ was made in [8]. The authors characterized the involution property of monomials, Dickson polynomials [7] and linearized polynomials over $\mathbb{F}_{2^n}$, and proposed several methods of constructing new involutions from known ones. In particular, involutions of the form $G(x) + \gamma f(x)$ were studied in [8], where G is an involution, $\gamma \in \mathbb{F}_{2^n}^*$ and $f \in \mathbb{F}_{2^n}[x]$. Involutions of the form $x^r h(x^s)$ were studied in [55]. Moreover, the number of fixed points of involutions over $\mathbb{F}_{2^n}$ was also discussed in [8]. A class of involutions over $\mathbb{F}_{2^n}$ with no fixed points was given in [36]. Involutions satisfying special properties were presented in [11], [29], [30] to construct Bent functions.

PPs from the AGW criterion. The Akbary–Ghioca–Wang (AGW) criterion [1] is an important method for constructing PPs. A necessary and sufficient condition for $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ to be a PP of $\mathbb{F}_{q^n}$ was given in [1] by using the additive analogue of AGW criterion, where $h, \psi, \varphi, g \in \mathbb{F}_{q^n}[x]$ satisfy some conditions. In [39], the inverse of f was written in terms of the inverses of two other polynomials bijecting two subspaces of $\mathbb{F}_{q^n}$. In some cases, these inverses can be explicitly obtained. Further extensions of [39] can be found in [40]. The general results in [39], [40] contain some concrete classes mentioned earlier such as bilinear PPs [51], linearized PPs of the form $L(x) + K(x)$ [36], and PPs of the form $x + \gamma f(x)$ with b-linear translator γ [20].

Generalized cyclotomic mapping PPs. Cyclotomic mapping PPs of finite fields were introduced in [34], [43], and were generalized in [45]. A simple class of generalized cyclotomic mapping PPs of $\mathbb{F}_q$ was defined in [45] as

$$f(x) = \frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1} a_i \omega^{-ij} x^{r_i + js}, \tag{1}$$

where $q - 1 = ds$, $a_i \in \mathbb{F}_q^*$, $1 \leq r_i < s$ and ω is a primitive d-th root of unity of $\mathbb{F}_q$. Several equivalent criteria for f permuting $\mathbb{F}_q$ were given in [45], which stated that f is a PP of $\mathbb{F}_q$ if and only if $\gcd(\prod_{i=0}^{d-1} r_i, s) = 1$ and $\{a_i^s \omega^{ir_i} : i = 0, 1, \ldots, d-1\} = U_d$. The inverses of f on $\mathbb{F}_q$ was given in [46], [58] by

$$f^{-1}(x) = \frac{1}{d}\sum_{i=0}^{d-1}\sum_{j=0}^{d-1} \omega^{i(t_i - jr_i)}(x/a_i)^{\widetilde{r_i} + js},$$

where $1 \leq \widetilde{r_i} < s$ and $r_i\widetilde{r_i} + st_i = 1$. In [46], all involutions of the form (1) were characterized, and a fast algorithm was provided to generate many classes of these PPs, their inverses, and involutions. The class of PPs of the form $x^r h(x^s)$ is in fact a special case of generalized cyclotomic mapping PPs.

More general piecewise PPs. The idea of more general piecewise constructions of permutations was summarized in [2], [15]. Piecewise constructions of inverses of piecewise PPs were studied in [58], [59]. As applications, the inverse of PP $f(x) = ax + x^{(q+1)/2}$ of $\mathbb{F}_q$ was given in [59] by

$$f^{-1}(x) = (a^2 - 1)^{-1}(ax - bx^{(q+1)/2}),$$

where $(a^2 - 1)^{(q-1)/2} = 1$, $b = (a+1)^{(q-1)/2} \in \{-1, 1\}$, and q is odd. The inverse of PP of $\mathbb{F}_{p^n}$ of the form

$$(ax^{p^k} - bx + c)^{\frac{p^n+1}{2}} \pm (ax^{p^k} + bx)$$

was obtained in [59], where p is odd and $a, b, c \in \mathbb{F}_{p^n}$. Three classes of involutions of finite fields were also given in [58], [59]. In addition, the PP f in (1) can be written as piecewise form, and its inverse was deduced by the piecewise method in [58].

III. The Inverses of PPs of Small Degree

Assume $g \in \mathbb{F}_q[x]$ and $b, c, d \in \mathbb{F}_q$ with $b \neq 0$. Then g is a PP of $\mathbb{F}_q$ if and only if $f(x) = bg(x+c) + d$ is. By choosing b, c, d suitably, we can obtain f in **normalized form**, that is, f is monic, $f(0) = 0$, and when the degree m of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{m-1} is 0. It suffices, therefore, to study normalized PPs. In 1897, Dickson [12] listed all normalized PPs of degree ≤ 5 of $\mathbb{F}_q$ for all q, and classified all PPs of degree 6 of $\mathbb{F}_q$ for odd q. In 2010, the complete classification of PPs of degree 6 and 7 of $\mathbb{F}_{2^n}$ was settled in [22]. For a verification of the classification of normalized PPs of degree 6 of $\mathbb{F}_q$ for all q, see [38].

According to the complete classifications of PPs in [12], [22], [38], all PPs of degree 6 of $\mathbb{F}_q$ for all q are over small fields $\mathbb{F}_q$ with $q \leq 32$, except for x^6 over $\mathbb{F}_{2^n}$. All PPs of degree 7 of $\mathbb{F}_{2^n}$ are over $\mathbb{F}_{2^n}$ with $n \leq 4$, except for x^7 and $x^7 + x^5 + x$. The inverses of PPs of $\mathbb{F}_q$ with $q \leq 32$ can be calculated by the Lagrange interpolation formula or Theorem 9 in the next section. The inverses of PPs x^6 and x^7 of $\mathbb{F}_{2^n}$ can be obtained by the following Theorem 2. The polynomial $x^7 + x^5 + x$ is actually the degree 7 Dickson polynomial $D_7(x, 1)$ over $\mathbb{F}_{2^n}$, and its inverse is $D_m(x, 1)$ (by Lemma 1), where m is the inverse of 7 modulo $2^{2n} - 1$. In other words, we obtain the inverses of all PPs of degree 6 of $\mathbb{F}_q$ for all q and the inverses of all PPs of degree 7 of $\mathbb{F}_{2^n}$.

In the rest of this section, we will give the inverses of all normalized PPs of degree ≤ 5 in [12], which are actually the same as that in [28, Table 7.1] or in the previous Table I. Since the inverses of normalized PPs of small fields $\mathbb{F}_q$ with $q \leq 13$ can be obtained by the Lagrange interpolation formula, we need only consider the normalized PPs of degree ≤ 5 of $\mathbb{F}_q$ for infinite many q.

A. Inverses of Monomials

The inverse of x is clearly itself, and the inverse of x^2 on $\mathbb{F}_{2^n}$ is $x^{2^{n-1}}$. The following theorem gives the explicit inverse of x^m on $\mathbb{F}_q$ for $m \geq 3$.

Theorem 2. *For $m \geq 3$, if x^m is a PP of $\mathbb{F}_q$, then its inverse on $\mathbb{F}_q$ is $x^{(aq-a+1)/m}$, where $a \equiv -(q-1)^{\phi(m)-1} \pmod{m}$ and ϕ is Euler's phi function.*

Proof: If x^m is a PP of $\mathbb{F}_q$, then $\gcd(m, q-1) = 1$ and so $aq - a + 1 = 1 + a(q-1) \equiv 1 - (q-1)^{\phi(m)} \equiv 0 \pmod{m}$. Also note that $m(aq - a + 1)/m - a(q-1) = 1$. Hence the inverse of m modulo $q - 1$ is $(aq - a + 1)/m$. ■

The proof above converts the problem of determining the inverse of m modulo $q - 1$ to that of computing the inverse of $q - 1$ modulo m, and the latter is easy for small m. For instance, if $m = 3$ and $\gcd(3, q-1) = 1$, then the inverse of $q-1$ modulo 3 is $(q-1)^{\phi(3)-1} = q-1$, and so the inverse of 3 modulo $q-1$ is $(aq-a+1)/3$, where $a \equiv 1 - q \pmod{3}$.

B. Inverses of Linearized Binomials and Trinomials

Assume $L_{st}(x) := bx^{q^s} + cx^{q^t}$ is an arbitrary linearized binomial of $\mathbb{F}_{q^n}$, where $b, c \in \mathbb{F}_{q^n}^*$ and $0 \leq t < s \leq n-1$. Then $L_{st}(x) = b(x^{q^{s-t}} + b^{-1}cx) \circ x^{q^t}$, and so L_{st} permutes $\mathbb{F}_{q^n}$ if and only if $L_r(x) := x^{q^r} - ax$ permutes $\mathbb{F}_{q^n}$, where $r = s - t$ and $a = -b^{-1}c$. The inverse of L_r on $\mathbb{F}_{q^n}$ was given in [9], [48] as follows.

Theorem 3 ([9], [48]). *Let $L_r(x) = x^{q^r} - ax$, where $a \in \mathbb{F}_{q^n}^*$ and $1 \leq r \leq n-1$. Then L_r is a PP of $\mathbb{F}_{q^n}$ if and only if the norm $\mathrm{N}_{q^n/q^d}(a) \neq 1$, where $d = \gcd(n, r)$. In this case, its inverse on $\mathbb{F}_{q^n}$ is*

$$L_r^{-1}(x) = \frac{\mathrm{N}_{q^n/q^d}(a)}{1 - \mathrm{N}_{q^n/q^d}(a)} \sum_{i=0}^{n/d-1} a^{-\frac{q^{(i+1)r}-1}{q^r-1}} x^{q^{ir}}.$$

The norm $\mathrm{N}_{q^n/q^d}(a) \neq 1$ if and only if a is not a $(q^d - 1)$th power. Hence, Theorem 3 gives the inverse of $x^{q^r} - ax$ for $q^r = 3, 4, 5$ in Table I.

The normalized PP of the form $x^4 + bx^2 + ax$ of $\mathbb{F}_{2^n}$ is the only linearized trinomial in Table I. Its inverse has a close relation with the sequence

$$S_{-1} = 0, \ \ S_0 = 1, \ \ S_i = b^{2^{i-1}} S_{i-1} + a^{2^{i-1}} S_{i-2}, \qquad (2)$$

where $1 \leq i \leq n$ and $a, b \in \mathbb{F}_{2^n}^*$. An argument similar to that in [17, Lemma 2] leads to an equivalent definition of S_i:

$$S_i = bS_{i-1}^2 + a^2 S_{i-2}^4, \quad 1 \leq i \leq n. \qquad (3)$$

Denote $Z_n = S_n + aS_{n-2}^2$. Then

$$\begin{aligned} Z_n^2 &= S_n^2 + a^2 S_{n-2}^4 \overset{(2)}{=} bS_{n-1}^2 + aS_{n-2}^2 + a^2 S_{n-2}^4 \\ &\overset{(3)}{=} S_n + aS_{n-2}^2 = Z_n, \end{aligned}$$

and so $Z_n = 0$ or 1. A criterion for $f(x) = x^{q^2} + bx^q + ax$ to be a PP of $\mathbb{F}_{q^n}$ and the inverse of f on $\mathbb{F}_{q^n}$ were presented in [49, Theorem 3.2.29]. Taking $q = 2$ in this theorem and using the fact $Z_n = 0$ or 1, we obtain the following result.

Corollary 4. *Let $L(x) = x^4 + bx^2 + ax$, where $a, b \in \mathbb{F}_{2^n}^*$ and $n \geq 1$. Then L is a PP of $\mathbb{F}_{2^n}$ if and only if $S_n + aS_{n-2}^2 = 1$. In this case, the inverse of L on $\mathbb{F}_{2^n}$ is*

$$L^{-1}(x) = \sum_{i=0}^{n-1} \left(S_{n-2-i}^{2^{i+1}} + a^{1-2^{i+1}} S_i\right) x^{2^i}.$$

Note that Corollary 4 holds for $n = 1, 2$. Indeed, if $n = 1$ then $L(x) \equiv L^{-1}(x) \equiv x \pmod{x^2 + x}$. If $n = 2$ and L is a PP of $\mathbb{F}_4$, then $L(x) \equiv L^{-1}(x) \equiv bx^2 \pmod{x^4 + x}$.

The necessary and sufficient condition for L permuting $\mathbb{F}_{2^n}$ can also be obtained by [17, Proposition 2]. This proposition also shown that $M_0 = (2^n - (-1)^n)/3$, where M_0 is the number of $c \in \mathbb{F}_{2^n}^*$ such that $P_c(x) = x^3 + x + c$ has no root in $\mathbb{F}_{2^n}$. Since $L(b^{1/2}x) = b^2 x(x^3 + x + ab^{-3/2})$, L is a PP of $\mathbb{F}_{2^n}$ if and only if P_c has no root in $\mathbb{F}_{2^n}$, where $c = ab^{-3/2}$. Hence the number of $a, b \in \mathbb{F}_{2^n}^*$ such that L permutes $\mathbb{F}_{2^n}$ is equal to $(2^n - 1)(2^n - (-1)^n)/3$, which implies the probability of L permuting $\mathbb{F}_{2^n}$ is almost 1/3.

In Corollay 4, let $a = b = 1$. Then $S_i = S_{i-1} + S_{i-2}$ by (2), and so $(S_{-1}, S_0, S_1, S_2, S_3, S_4, \ldots) = (0, 1, 1, 0, 1, 1, \ldots)$. Thus we obtain the following result.

Corollary 5. *Let $L(x) = x^4 + x^2 + x$. Then L is a PP of $\mathbb{F}_{2^n}$ if and only if $n \equiv 1, 2 \pmod{3}$. In this case, the inverse of L on $\mathbb{F}_{2^n}$ is $L^{-1}(x) = \sum_{i=0}^{n-1} x^{2^i}$ with $i \not\equiv 2 - n \pmod{3}$.*

C. Inverses of Non-Linearized Trinomials

In Table I, there are only two infinite classes of non-linearized permutation trinomials. One is the polynomial $x^5 + ax^3 + 5^{-1}a^2x$, where $a \in \mathbb{F}_q$ and $q \equiv \pm 2 \pmod 5$. It is actually the Dickson PP $D_5(x, -5^{-1}a)$, and by Lemma 1 its inverse on $\mathbb{F}_q$ is $D_m(x, -(5^{-1}a)^5)$, where $m = (3q^2-2)/5$ (by the proof of Theorem 2). The other is as follows.

Lemma 6. [28, Table 7.1] *Let $f(x) = x^5 - 2ax^3 + a^2x$, where $a \in \mathbb{F}_{5^n}^*$ and $n \geq 1$. Then f is a PP of $\mathbb{F}_{5^n}$ if and only if $a^{(q-1)/2} = -1$.*

The inverse of f was given in [25] by solving equations over finite fields.

Theorem 7. [25, Lemma 4.9] *The inverse of f in Lemma 6 on $\mathbb{F}_{5^n}$ is*

$$f^{-1}(x) = x\left(\frac{(a/x^2)^{\frac{5^n-1}{4}}}{1-(a/x^2)^{\frac{5^n-1}{4}}}\sum_{i=0}^{n-1}(a/x^2)^{-\frac{5^{i+1}-1}{4}}(1/x^2)^{5^i}\right)^2,$$

where $x \in \mathbb{F}_{5^n}^*$ and $f^{-1}(0) = 0$.

By employing the method in the next section, we obtain the explicit polynomial form of f^{-1} as follows.

Theorem 8. *The inverse of f in Lemma 6 on $\mathbb{F}_{5^n}$ is*

$$f^{-1}(x) = \sum_{0\leq i\leq j\leq n-1} a^{-\frac{5^n+5^{i+1}+5^{j+1}-3}{4}} b_{ij}x^{\frac{5^n+5^i+5^j-1}{2}},$$

where $b_{ij} = 1$ if $i < j$ and $b_{ij} = 3$ if $i = j$.

Remark 1. *Theorem 8 can be obtained from Theorem 7 and*

$$\Big(\sum_{1\leq i\leq n} x_i\Big)^2 = \sum_{1\leq i\leq n} x_i^2 + \sum_{1\leq i<j\leq n} 2\,x_ix_j,$$

where $x_i = a^{-\frac{5^i-1}{4}}x^{\frac{5^{i-1}-1}{2}}$. However, we will demonstrate our method of deducing Theorem 8 in the next sections. The main reason is that our method can also be used to find the inverses of other PPs of small degree; see for example [57].

In summary, all inverses of normalized PPs of degree $\leq$ 5 are obtained. We list these PPs and their inverses in Table I.

IV. The Coefficients of Inverse of a PP

In this section, we will write the coefficients of inverse of the PP f in Lemma 6 in terms of binomial coefficients, by employing the following formula (4) presented first in [33].

Theorem 9 (See [33])**.** *Let $f \in \mathbb{F}_q[x]$ be a PP of $\mathbb{F}_q$ such that $f(0) = 0$, and let*

$$f(x)^{q-1-i} \equiv \sum_{0\leq k\leq q-1} b_{ik}x^k \pmod{x^q - x},$$

where $i = 1, 2, \ldots, q-2$. Then the inverse of f on $\mathbb{F}_q$ is

$$f^{-1}(x) = \sum_{1\leq i\leq q-2} b_{i,q-2}x^i. \tag{4}$$

Proof: Assume $f^{-1}(x) = \sum_{i=1}^{q-2} c_ix^i$. From the Lagrange interpolation formula, we have

$$\begin{aligned} f^{-1}(x) &= \sum_{a\in\mathbb{F}_q} a\big(1-(x-f(a))^{q-1}\big) \\ &= \sum_{a\in\mathbb{F}_q^*} a\Big(-\sum_{1\leq i\leq q-1}(-1)^i(-f(a))^{q-1-i}x^i\Big) \\ &= \sum_{1\leq i\leq q-1}\Big(-\sum_{a\in\mathbb{F}_q^*} af(a)^{q-1-i}\Big)x^i. \end{aligned}$$

Hence for $1 \leq i \leq q-2$, we have

$$\begin{aligned} c_i &= -\sum_{a\in\mathbb{F}_q^*} af(a)^{q-1-i} = -\sum_{a\in\mathbb{F}_q^*} a\sum_{0\leq k\leq q-1} b_{ik}a^k \\ &= -\sum_{0\leq k\leq q-1} b_{ik}\sum_{a\in\mathbb{F}_q^*} a^{k+1} = b_{i,q-2}, \end{aligned}$$

where the last identity follows from

$$\sum_{a\in\mathbb{F}_q} a^t = \begin{cases} -1 & \text{if } t = q-1, \\ 0 & \text{if } t = 0, 1, \ldots, q-2. \end{cases}$$

The proof is completed. ∎

Remark 2. *Theorem 9 is the same as the one in [33], [44]. All these results are essentially part of Theorem 2 in [31]. For the reason of completeness, we include a proof by using the Lagrange interpolation formula.*

Next we use Theorem 9 to calculate the coefficients of the inverse of f in Lemma 6. Recall that $f(x) = x^5 - 2ax^3 + a^2x$, where $a \in \mathbb{F}_{5^n}$ and $a^{(q-1)/2} = -1$. Let $q = 5^n$ and $r_i = q-1-i$, where $1 \leq i \leq q-2$. Then

$$\begin{aligned} f(x)^{r_i} &= x^{r_i}(x^2-a)^{2r_i} \\ &= \sum_{0\leq j\leq 2r_i}\binom{2r_i}{j}(-a)^{2r_i-j}x^{r_i+2j}. \end{aligned} \tag{5}$$

The degree of $f(x)^{r_i}$ is $5r_i$, and $5 \leq 5r_i < 4(q-1)+q-2$. By (4), the coefficient $b_{i,q-2}$ of f^{-1} equals the sum of the coefficients of $x^{k(q-1)+(q-2)}$ ($k = 0, 1, 2, 3$) in (5). If i is even, then $r_i + 2j$ is even, and so the coefficients of odd powers of x in (5) are all 0. Also note $k(q-1)+(q-2)$ is odd. We have $b_{i,q-2} = 0$ for even i. If i is odd, then

$$b_{i,q-2} = \sum_{0\leq k\leq 3}\binom{2r_i}{(k(q-1)+i-1)/2}(-a)^{2r_i-\frac{k(q-1)+i-1}{2}}.$$

Let $i = 2m+1$. Then $0 \leq m \leq (q-3)/2$ and

$$\begin{aligned} b_{i,q-2} &= \sum_{0\leq k\leq 3}\binom{2q-4m-4}{k\frac{q-1}{2}+m}(-a)^{-k\frac{q-1}{2}-5m-2} \\ &= \sum_{0\leq k\leq 3}\binom{2q-4m-4}{k\frac{q-1}{2}+m}(-1)^{k+m}a^{-5m-2}, \end{aligned} \tag{6}$$

where the last identity follows from the fact $a^{(q-1)/2} = -1$ and $q = 5^n$. If $2q-4m-4 < k(q-1)/2+m$, i.e.,

$$m > ((4-k)q+k-8)/10,$$

then $\binom{2q-4m-4}{k\frac{q-1}{2}+m} = 0$. Thus a direct computation reduces (6) to

$$b_{i,q-2} = \begin{cases} 0 & \text{if } 4T+1 < m \le (q-3)/2, \\ e_{m0} & \text{if } 3T < m \le 4T+1, \\ e_{m0}+e_{m1} & \text{if } 2T < m \le 3T, \\ e_{m0}+e_{m1}+e_{m2} & \text{if } T < m \le 2T, \\ e_{m0}+e_{m1}+e_{m2}+e_{m3} & \text{if } 0 \le m \le T, \end{cases} \quad (7)$$

where $T = (q-5)/10 = (5^{n-1}-1)/2$ and

$$e_{mk} = \binom{2q-4m-4}{k\frac{q-1}{2}+m}(-1)^{k+m}a^{-5m-2}, k = 0, 1, 2, 3. \quad (8)$$

Now the key of deducing Theorem 8 is to find the values of binomial coefficients above.

V. Explicit Values of Binomial Coefficients

In this section, we first give the explicit values of binomial coefficients in (8), and then prove Theorem 8. In order to remove the multiples of q in these binomial coefficients, we need two lemmas.

Lemma 10 (Lucas' theorem)**.** *For non-negative integers n, k and a prime p, let $n = n_0 + n_1 p + \cdots + n_s p^s$ and $k = k_0+k_1 p+\cdots+k_s p^s$ be their p-adic expansions, where $0 \le n_i$, $k_i \le p-1$ for $i = 0, 1, \ldots, s$. Then*

$$\binom{n}{k} \equiv \prod_{i=0}^{s} \binom{n_i}{k_i} \pmod p$$

(with the convention $\binom{0}{0} = 1$ and $\binom{n}{k} = 0$ if $n < k$). In particular, $\binom{n}{k} \not\equiv 0 \pmod p$ if and only if $n_i \ge k_i$ for all i.

Lemma 11. *Let q be a power of a prime p, and let r, k be integers with $0 \le k \le q-1$. Then*

$$\binom{q+r}{k} \equiv \binom{r}{k} \pmod p.$$

where $\binom{n}{k} = n(n-1)\cdots(n-k+1)/k!$.

Proof: By the Chu-Vandermonde identity, we have

$$\binom{q+r}{k} = \sum_{i=0}^{k} \binom{q}{i}\binom{r}{k-i} \equiv \binom{r}{k} \pmod p,$$

where we use the fact $\binom{q}{i} \equiv 0 \pmod p$ for $1 \le i \le q-1$. ■

In (7) we defined $T = (q-5)/10$ with $q = 5^n$. Then for $0 \le m \le 4T+1$, applying Lemma 11 twice yields that

$$\binom{2q-4m-4}{m} \equiv \binom{-4m-4}{m} \equiv (-1)^m \binom{5m+3}{m} \pmod 5, \quad (9)$$

where we use the fact $\binom{-n}{m} = (-1)^m \binom{m+n-1}{m}$ for m, $n > 0$. Similarly, for $0 \le m \le 3T$,

$$\binom{2q-4m-4}{\frac{q-1}{2}+m} \equiv (-1)^m \binom{5m+3+\frac{q-1}{2}}{m+\frac{q-1}{2}} \pmod 5, \quad (10)$$

For $0 \le m \le 2T$, we have $q-4m-4 > 0$ and, by Lucas' theorem and Lemma 11,

$$\binom{2q-4m-4}{q+m-1} \equiv \binom{q-4m-4}{m-1} \equiv \binom{-4m-4}{m-1} \equiv (-1)^{m-1}\binom{5m+2}{m-1} \pmod 5. \quad (11)$$

Similarly, for $0 \le m \le T$,

$$\binom{2q-4m-4}{3\frac{q-1}{2}+m} \equiv (-1)^{m-1}\binom{5m+2+\frac{q-1}{2}}{m-1+\frac{q-1}{2}} \pmod 5. \quad (12)$$

Next we use Lucas' theorem to find the explicit value of the last binomial coefficients in (9)-(12).

Theorem 12. *Let $0 \le m \le 5^n - 1$ with $n \ge 1$. Write*

$$m = m_0 + m_1 5 + \cdots + m_{n-1}5^{n-1}, \quad 0 \le m_i \le 4.$$

Then the following three statements are equivalent:

(i) $\binom{5m+3}{m} \not\equiv 0 \pmod 5$*;*

(ii) $3 \ge m_0 \ge m_1 \ge \cdots \ge m_{n-1} \ge 0$*;*

(iii) $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4} + \frac{5^{k_3}-1}{4}$*, where $0 \le k_1 \le k_2 \le k_3 \le n$.*

Proof: It is easy to obtain the 5-adic expansions:

$$5m+3 = 3 + m_0 5 + \cdots + m_{n-2}5^{n-1} + m_{n-1}5^n,$$
$$m = m_0 + m_1 5 + \cdots + m_{n-1}5^{n-1}. \quad (13)$$

By Lucas' theorem, (i) is equivalent to (ii). To show (ii) is equivalent to (iii), it suffices to prove $M_1 = M_2$, where

$$M_1 = \{m : 3 \ge m_0 \ge m_1 \ge \cdots \ge m_{n-1} \ge 0\},$$
$$M_2 = \{\tfrac{5^{k_1}-1}{4} + \tfrac{5^{k_2}-1}{4} + \tfrac{5^{k_3}-1}{4} : 0 \le k_1 \le k_2 \le k_3 \le n\}.$$

Since $(5^k - 1)/4 = 1 + 1\cdot 5 + \cdots + 1 \cdot 5^{k-1}$ and $0 \le k_1 \le k_2 \le k_3 \le n$, we have $M_2 \subseteq M_1$. It remains to show that $M_1 \subseteq M_2$, i.e., $m \in M_2$ for any $m \in M_1$. The remainder of our proof is divided into two cases.

Case 1: assume $m \in M_1$ such that $m_0 = \cdots = m_{n-1} = a$, where $0 \le a \le 3$. If $a = 2$, then $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4} + \frac{5^{k_3}-1}{4}$, where $k_1 = 0$ and $k_2 = k_3 = n$. Hence $m \in M_2$. Similarly, $m \in M_2$ for $a = 0$, 1 or 3.

Case 2: assume $m \in M_1$ such that $m_0, m_1, \ldots, m_{n-1}$ are not all equal. Then the number N of the sign $>$ in the inequality $3 \ge m_0 \ge m_1 \ge \cdots \ge m_{n-1} \ge 0$ is 1, 2 or 3. If $N = 3$, then there exist a, b, c such that

$$0 \le a < b < c \le n-2,$$
$$m_0 = m_1 = \cdots = m_a = 3,$$
$$m_{a+1} = m_{a+2} = \cdots = m_b = 2,$$
$$m_{b+1} = m_{b+2} = \cdots = m_c = 1,$$
$$m_{c+1} = m_{c+2} = \cdots = m_{n-1} = 0.$$

Then $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4} + \frac{5^{k_3}-1}{4}$, where $k_1 = a+1$, $k_2 = b+1$ and $k_3 = c+1$. Hence $m \in M_2$. Similarly, $m \in M_2$ for $N = 1$ or 2. ■

Two criteria that $\binom{5m+3}{m} \not\equiv 0 \pmod 5$ are given in the theorem above. The following theorem finds the explicit values of this class of binomial coefficients.

Theorem 13. *Let* $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4} + \frac{5^{k_3}-1}{4}$ *with* $0 \le k_1 \le k_2 \le k_3 \le n$. *Then in* $\mathbb{F}_5$,

$$\binom{5m+3}{m} = \begin{cases} 1 & \text{if } k_1 = k_2 = k_3 \text{ or } k_1 < k_2 < k_3, \\ 3 & \text{if } k_1 = k_2 < k_3 \text{ or } k_1 < k_2 = k_3. \end{cases}$$

Proof: For ease of notations, we denote $A = \binom{5m+3}{m}$.

Case 1: $k_1 = k_2 = k_3 = k$ with $0 \le k \le n$. If $k = 0$ then $m = 0$ and $A = \binom{3}{0} = 1$. If $1 \le k \le n$, then $m = 3(5^k - 1)/4$, i.e., $m_0 = \cdots = m_{k-1} = 3$ and $m_k = \cdots = m_{n-1} = 0$. By Lucas' theorem and (13), $A \equiv \binom{3}{3}\binom{3}{0} = 1 \pmod 5$.

Case 2: $k_1 = k_2 < k_3$. If $k_1 = k_2 = 0$, then

$$m_0 = \cdots = m_{k_3-1} = 1, \quad m_{k_3} = \cdots = m_{n-1} = 0.$$

Thus $A \equiv \binom{3}{1}\binom{1}{0} = 3 \pmod 5$. If $k_1 = k_2 = k \ge 1$, then $m_0 = \cdots = m_{k-1} = 3$, $m_k = \cdots = m_{k_3-1} = 1$, $m_{k_3} = \cdots = m_{n-1} = 0$. Hence $A \equiv \binom{3}{3}\binom{3}{1}\binom{1}{0} = 3 \pmod 5$.

Case 3: $k_1 < k_2 = k_3$. The proof is similar to that of Case 2 and so is omitted.

Case 4: $k_1 < k_2 < k_3$. If $k_1 = 0$ then $m_0 = \cdots = m_{k_2-1} = 2$, $m_{k_2} = \cdots = m_{k_3-1} = 1$, $m_{k_3} = \cdots = m_{n-1} = 0$. Hence $A \equiv \binom{3}{2}\binom{2}{1}\binom{1}{0} \equiv 1 \pmod 5$. If $0 < k_1 < k_2 < k_3$, then

$$m_0 = \cdots = m_{k_1-1} = 3, \quad m_{k_1} = \cdots = m_{k_2-1} = 2,$$
$$m_{k_2} = \cdots = m_{k_3-1} = 1, \quad m_{k_3} = \cdots = m_{n-1} = 0.$$

Hence $A \equiv \binom{3}{3}\binom{3}{2}\binom{2}{1}\binom{1}{0} \equiv 1 \pmod 5$. ■

Corollary 14. *Let* $T = (5^{n-1} - 1)/2$, $n \ge 1$ *and* $2T < m \le 4T + 1$. *Then in* $\mathbb{F}_5$,

$$\binom{5m+3}{m} = \begin{cases} 3^{\binom{k_1}{k_2}} & \text{if } m = (5^n + 5^{k_1} + 5^{k_2} - 3)/4, \\ 0 & \text{otherwise,} \end{cases}$$

where $0 \le k_1 \le k_2 \le n - 1$.

Proof: Let $A = \binom{5m+3}{m}$. According to Theorem 12, if $0 \le m \le 5^n - 1$ then $A \not\equiv 0 \pmod 5$ if and only if

$$m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4} + \frac{5^{k_3}-1}{4},$$

where $0 \le k_1 \le k_2 \le k_3 \le n$. Since $2T + 1 = 5^{n-1}$ and

$$4T + 1 = 4 + 4 \cdot 5 + \cdots + 4 \cdot 5^{n-2} + 1 \cdot 5^{n-1},$$

we have, for $2T < m \le 4T + 1$, $A \not\equiv 0 \pmod 5$ if and only if $m = (5^{k_1} + 5^{k_2} + 5^n - 3)/4$, where $0 \le k_1 \le k_2 < n$. In this case, $A \equiv 3^{\binom{k_1}{k_2}} \pmod 5$ by Theorem 13. ■

The following corollary presents a congruence relation for the binomial coefficients in (9) and (11).

Corollary 15. *Let* $T = (5^{n-1}-1)/2$, $n \ge 2$ *and* $T < m \le 2T$. *Then*

$$\binom{5m+3}{m} \equiv \binom{5m+2}{m-1} \pmod 5.$$

Proof: Denote by A and B the above binomial coefficients, respectively. Then $mA = (5m+3)B$, and so $2mA \equiv B \pmod 5$. If $A \equiv 0 \pmod 5$, then $B \equiv 0 \pmod 5$, and thus $A \equiv B \pmod 5$. We next show $A \equiv B \pmod 5$ for $A \not\equiv 0 \pmod 5$. By Theorem 12, for $0 \le m \le 5^n - 1$, $A \not\equiv 0 \pmod 5$ if and only if $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4} + \frac{5^{k_3}-1}{4}$, where $0 \le k_1 \le k_2 \le k_3 \le n$. Since

$$T = 2 + 2 \cdot 5 + \cdots + 2 \cdot 5^{n-2},$$
$$2T = 4 + 4 \cdot 5 + \cdots + 4 \cdot 5^{n-2},$$

we obtain, for $T < m \le 2T$, $A \not\equiv 0 \pmod 5$ if and only if $m = \frac{5^{k_1}-1}{4} + T$, where $1 \le k_1 \le n - 1$. Hence $m \equiv 3 \pmod 5$, and so $A \equiv 2mA \equiv B \pmod 5$. ■

Next we study the last binomial coefficient in (10).

Theorem 16. *Let* $0 \le m \le 5^n - 1$ *with* $n \ge 1$. *Write*

$$m = m_0 + m_1 5 + \cdots + m_{n-1} 5^{n-1}, \quad 0 \le m_i \le 4.$$

Then the following three statements are equivalent:

(i) $\binom{5m+3+\frac{5^n-1}{2}}{m+\frac{5^n-1}{2}} \not\equiv 0 \pmod 5$*;*
(ii) $3 = m_0 \ge m_1 \ge \cdots \ge m_{n-1} \ge 2$*;*
(iii) $m = \frac{5^n-1}{2} + \frac{5^k-1}{4}$, *where* $1 \le k \le n$.

Proof: Denote $\alpha = 5m + 3 + \frac{5^n-1}{2}$ and $\beta = m + \frac{5^n-1}{2}$. Then their 5-adic expansions are as follows:

$$\begin{aligned} \alpha &= 0 + (m_0+3)5 + (m_1+2)5^2 + (m_2+2)5^3 + \cdots \\ &\quad + (m_{n-2}+2)5^{n-1} + m_{n-1}5^n, \end{aligned} \tag{14}$$

$$\begin{aligned} \beta &= (m_0+2) + (m_1+2)5 + (m_2+2)5^2 + \cdots \\ &\quad + (m_{n-1}+2)5^{n-1} + 0 \cdot 5^n. \end{aligned} \tag{15}$$

If $\binom{\alpha}{\beta} \not\equiv 0 \pmod 5$, then by Lucas' theorem, $0 \succeq m_0 + 2$, i.e., $m_0 = 3$, where $a_i \succeq b_i$ denotes $a_i \ge b_i$ in $\mathbb{F}_5$. The condition $m_0 = 3$ leads to a carry 1 in (14) and (15), respectively. Then

$$\alpha = 0 + 1 \cdot 5 + (m_1+3)5^2 + (m_2+2)5^3 + \cdots,$$
$$\beta = 0 + (m_1+3)5 + (m_2+2)5^2 + (m_3+2)5^3 + \cdots.$$

If $\binom{\alpha}{\beta} \not\equiv 0 \pmod 5$, then $1 \succeq m_1 + 3$, i.e., $m_1 = 2, 3$, which also yields a carry 1 in the expansions above. Now

$$\alpha = 0 + 1 \cdot 5 + (m_1-2)5^2 + (m_2+3)5^3 + \cdots,$$
$$\beta = 0 + (m_1-2)5 + (m_2+3)5^2 + (m_3+2)5^3 + \cdots.$$

If $\binom{\alpha}{\beta} \not\equiv 0 \pmod 5$, then $1 \succeq m_1 - 2 \succeq m_2 + 3$, and so $1 \succeq m_2 + 3$, i.e., $m_2 = 2, 3$, which also yields a carry 1. And so on, we obtain $\binom{\alpha}{\beta} \not\equiv 0 \pmod 5$ if and only if

$$m_0 = 3, \ 1 \succeq m_1 - 2 \succeq \cdots \succeq m_{n-1} - 2, \ m_{n-1} + 1 \succeq 1. \tag{16}$$

So $m_k = 2, 3$ for $1 \le k \le n - 1$. There are exactly two cases:

- $m_1 = \cdots = m_{n-1} = 3$, i.e., $m = \frac{5^n-1}{2} + \frac{5^n-1}{4}$;
- $m_1 = \cdots = m_{k-1} = 3$ and $m_k = \cdots = m_{n-1} = 2$ for some $1 \le k \le n - 1$. That is, $m = \frac{5^n-1}{2} + \frac{5^k-1}{4}$, where $1 \le k \le n - 1$.

Therefore, (16) is equivalent to (ii) or (iii). ■

Corollary 17. *Let* $0 \le m \le (5^n - 1)/2$ *with* $n \ge 1$. *Then*

$$\binom{5m+3+\frac{5^n-1}{2}}{m+\frac{5^n-1}{2}} \equiv 0 \pmod 5.$$

Now we consider the last binomial coefficient in (12).

Theorem 18. *Let* $T = (5^{n-1}-1)/2$, $n \geq 1$ *and* $0 \leq m \leq 2T$. *Write* $m = m_0 + m_1 5 + \cdots + m_{n-2}5^{n-2}$, *where* $0 \leq m_i \leq 4$. *Then the following three statements are equivalent*:

(i) $\binom{5m+2+\frac{5^n-1}{2}}{m-1+\frac{5^n-1}{2}} \not\equiv 0 \pmod 5$;

(ii) $2 \geq m_0 \geq m_1 \geq \cdots \geq m_{n-2} \geq 0$;

(iii) $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4}$, *where* $0 \leq k_1 \leq k_2 \leq n-1$.

Proof: Denote $\alpha = 5m+2+\frac{5^n-1}{2}$ and $\beta = m-1+\frac{5^n-1}{2}$. Then their 5-adic expansions are as follows:

$$\alpha = 4 + (m_0+2)5 + \cdots + (m_{n-2}+2)5^{n-1},$$
$$\beta = (m_0+1) + (m_1+2)5 + \cdots + 2 \cdot 5^{n-1}.$$

The proof that (i) is equivalent to (ii) is divided in two cases.

Case 1: $0 \leq m_i \leq 2$ for all i. Then by Lucas' Theorem, $\binom{\alpha}{\beta} \not\equiv 0 \pmod 5$ if and only if

$$4 \geq m_0 + 1,\ m_0 + 2 \geq \cdots \geq m_{n-2} + 2 \geq 2, \quad \text{i.e.,}$$
$$2 \geq m_0 \geq \cdots \geq m_{n-2} \geq 0.$$

Case 2: $m_i = 3$ or 4 for some i $(0 \leq i \leq n-2)$. We first show $\binom{\alpha}{\beta} \equiv 0 \pmod 5$ if $m_0 = 3$. An argument similar to the one used in Theorem 16 shows that $\binom{\alpha}{\beta} \not\equiv 0 \pmod 5$ if and only if $m_1 = 3$ and $1 \geq m_2 - 2 \geq \cdots \geq m_{n-2} - 2 \geq 3$. This is contrary to $3 > 1$. Similarly, we have $\binom{\alpha}{\beta} \equiv 0 \pmod 5$ when $m_0 = 4$, $m_i = 3$ or 4 for $1 \leq i \leq n-2$.

An argument similar to the one used in Theorem 12 can show that (ii) is equivalent to (iii). ■

The following corollaries give the linear congruence relations between the binomial coefficients in (9), (11) and (12).

Corollary 19. *Let* $T = (5^{n-1}-1)/2$, $n \geq 1$ *and* $0 \leq m \leq 2T$. *Then*

$$\binom{5m+2+\frac{5^n-1}{2}}{m-1+\frac{5^n-1}{2}} \equiv -\binom{5m+2}{m} \pmod 5.$$

Proof: Denote by C and D the above binomial coefficients, respectively. Then by Lucas' theorem, $D \not\equiv 0 \pmod 5$ if and only if $2 \geq m_0 \geq m_1 \geq \cdots \geq m_{n-2} \geq 0$. That is, $D \not\equiv 0 \pmod 5$ if and only if $C \not\equiv 0 \pmod 5$. Hence $C \equiv -D \pmod 5$ when $C \equiv 0 \pmod 5$. On the other hand, if $C \not\equiv 0 \pmod 5$, then, by Theorem 18, $m = \frac{5^{k_1}-1}{4} + \frac{5^{k_2}-1}{4}$, where $0 \leq k_1 \leq k_2 \leq n-1$. An argument similar to that in Theorem 13 shows $C \equiv 3 + \binom{k_1}{k_2} \equiv -D \pmod 5$. Hence $C \equiv -D \pmod 5$ for $C \not\equiv 0 \pmod 5$. ■

Corollary 20. *Let* $T = (5^{n-1}-1)/2$, $n \geq 2$ *and* $0 \leq m \leq T$. *Then*

$$\binom{5m+3}{m} + \binom{5m+2+\frac{5^n-1}{2}}{m-1+\frac{5^n-1}{2}} \equiv \binom{5m+2}{m-1} \pmod 5.$$

Proof: Denote by A, C, B the above binomial coefficients, respectively. By $mA = (5m+3)B$, we get $2mA \equiv B \pmod 5$. Let $D = \binom{5m+2}{m}$. Then $(4m+3)A = (5m+3)D$, and so $D \equiv (3m+1)A \pmod 5$. By Corollary 19, $C \equiv -D \equiv (2m-1)A \pmod 5$. Hence $A + C \equiv B \pmod 5$. ■

With the help of the preceding results, we now prove Theorem 8. According to (7), the coefficients $b_{i,q-2}$ of f^{-1} are linear combinations of e_{m0}, e_{m1}, e_{m2}, e_{m3} defined by (8). Corollary 17 and the congruence (10) imply that

$$e_{m1} \equiv 0 \pmod 5 \quad 0 \leq m \leq 3T,$$

where $T = (5^{n-1}-1)/2$. By (9), (11) and Corollary 15,

$$e_{m0} + e_{m2} \equiv 0 \pmod 5 \quad \text{for } T < m \leq 2T.$$

From (9), (11), (12) and Corollary 20, we obtain

$$e_{m0} + e_{m2} + e_{m3} \equiv 0 \pmod 5 \quad \text{for } 0 \leq m \leq T.$$

By (9) and Corollary 14, for $2T < m \leq 4T+1$ we get, in $\mathbb{F}_5$,

$$e_{m0} = \begin{cases} 3\binom{k_1}{k_2} a^{-5m-2} & \text{if } m = (5^n + 5^{k_1} + 5^{k_2} - 3)/4, \\ 0 & \text{otherwise,} \end{cases}$$

where $0 \leq k_1 \leq k_2 \leq n-1$. Then Theorem 8 follows from (7) and Theorem 9 when $n \geq 2$ (since $n \geq 2$ is a necessary condition of Corollaries 15 and 20). In addition, it is easy to verify that Theorem 8 also holds for $n = 1$.

Acknowledgment

They are grateful to the referees and the editor for many useful comments and suggestions. They would like to thank Junwei Guo, Fu Wang, Baofeng Wu for their helpful suggestions.

References

[1] A. Akbary, D. Ghioca, and Q. Wang, "On constructing permutations of finite fields," *Finite Fields Appl.*, vol. 17, pp. 51–67, 2011.

[2] X. Cao, L. Hu, and Z. Zha, "Constructing permutation polynomials from piecewise permutations," *Finite Fields Appl.*, vol. 26, pp. 162–174, Mar. 2014.

[3] N. Cepak, P. Charpin, and E. Pasalic, "Permutations via linear translators," *Finite Fields Appl.*, vol. 45, pp. 19–42, May 2017.

[4] P. Charpin and G. Kyureghyan, "When does $G(x)+\gamma Tr(H(x))$ permute $\mathbb{F}_{p^n}$?" *Finite Fields Appl.*, vol. 15, no. 5, pp. 615–632, Oct. 2009.

[5] P. Charpin and G. M. Kyureghyan, "Monomial functions with linear structure and permutation polynomials," in *Finite Fields: Theory and Applications* (Contemporary Mathematics), vol. 518, Providence, RI, USA: AMS, 2010, pp. 99–111.

[6] P. Charpin, G. M. Kyureghyan, and V. Suder, "Sparse permutations with low differential uniformity," *Finite Fields Appl.*, vol. 28, pp. 214–243, Mar. 2014.

[7] P. Charpin, S. Mesnager, and S. Sarkar, "Dickson polynomials that are involutions," in *Contemporary Developments in Finite Fields and Applications*. Singapore: World Scientific, 2016, pp. 22–47.

[8] P. Charpin, S. Mesnager, and S. Sarkar, "Involutions over the Galois field $\mathbb{F}_{2^n}$," *IEEE Trans. Inf. Theory*, vol. 62, no. 4, pp. 2266–2276, Apr. 2016.

[9] R. Coulter and M. Henderson, "A note on the roots of trinomials over a finite field," *Bull. Austral. Math. Soc.*, vol. 69, no. 3, pp. 429–432, 2004.

[10] R. S. Coulter and M. Henderson, "The compositional inverse of a class of permutation polynomials over a finite field," *Bull. Austral. Math. Soc.*, vol. 65, no. 3, pp. 521–526, 2002.

[11] R. S. Coulter and S. Mesnager, "Bent functions from involutions over $\mathbb{F}_{2^n}$," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2979–2986, Apr. 2018.

[12] L. E. Dickson, "The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Part I," *Ann. Math.*, vol. 11, no. 1, pp. 65–120, 1897.

[13] C. Ding and J. Yuan, "A family of skew Hadamard difference sets," *J. Combinat. Theory Ser. A*, vol. 113, no. 1, pp. 1526–1535, 2006.

[14] C. Ding and Z. Zhou, "Binary cyclic codes from explicit polynomials over GF(2^m)," *Discrete Math.*, vol. 321, pp. 76–89, Apr. 2014.

[15] N. Fernando and X.-D. Hou, "A piecewise construction of permutation polynomials over finite fields," *Finite Fields Appl.*, vol. 18, no. 6, pp. 1184–1194, 2012.

[16] S. W. Golomb and O. Moreno, "On periodicity properties of Costas arrays and a conjecture on permutation polynomials," *IEEE Trans. Inf. Theory*, vol. 42, no. 6, pp. 2252–2253, Nov. 1996.

[17] T. Helleseth and A. Kholosha, "$x^{2^l+1}+x+a$ and related affine polynomials over GF(2^k)," *Cryptogr. Commun.*, vol. 2, no. 1, pp. 85–109, 2010.

[18] X.-D. Hou, "Determination of a type of permutation trinomials over finite fields, II," *Finite Fields Appl.*, vol. 35, pp. 16–35, Sep. 2015.

[19] X.-D. Hou, "Permutation polynomials over finite fields—A survey of recent advances," *Finite Fields Appl.*, vol. 32, pp. 82–119, Mar. 2015.

[20] G. M. Kyureghyan, "Constructing permutations of finite fields via linear translators," *J. Combinat. Theory, A*, vol. 118, no. 3, pp. 1052–1061, Apr. 2011.

[21] G. M. Kyureghyan and V. Suder, "On inversion in $\mathbb{Z}_{2^n-1}$," *Finite Fields Appl.*, vol. 25, pp. 234–254, Jan. 2014.

[22] J. Li, D. B. Chandler, and Q. Xiang, "Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2," *Finite Fields Appl.*, vol. 16, no. 6, pp. 406–419, 2010.

[23] K. Li, L. Qu, and X. Chen, "New classes of permutation binomials and permutation trinomials over finite fields," *Finite Fields Appl.*, vol. 43, pp. 69–85, Jan. 2017.

[24] K. Li, L. Qu, B. Sun, and C. Li, "New results about the boomerang uniformity of permutation polynomials," *IEEE Trans. Inf. Theory*, to be published. doi: 10.1109/TIT.2019.2918531.

[25] K. Li, L. Qu, and Q. Wang, "Compositional inverses of permutation polynomials of the form $x^rh(x^s)$ over finite fields," *Cryptogr. Commun.*, vol. 11, pp. 279–298, Mar. 2019.

[26] L. Li, S. Wang, C. Li, and X. Zeng, "Permutation polynomials $(x^{p^m}-x+\delta)^{s_1}+(x^{p^m}-x+\delta)^{s_2}+x$ over $\mathbb{F}_{p^n}$," *Finite Fields Appl.*, vol. 51, pp. 31–61, May 2018.

[27] N. Li, "On two conjectures about permutation trinomials over $\mathbb{F}_{3^{2k}}$," *Finite Fields Appl.*, vol. 47, pp. 1–10, Sep. 2017.

[28] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1997.

[29] S. Mesnager, "Further constructions of infinite families of bent functions from new permutations and their duals," *Cryptogr. Commun.*, vol. 8, no. 2, pp. 229–246, 2016.

[30] S. Mesnager, "On constructions of bent functions from involutions," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 110–114.

[31] G. L. Mullen, A. Muratović-Ribić, and Q. Wang, "On coefficients of powers of polynomials and their compositions over finite fields," in *Contemporary Developments in Finite Fields and Applications*. Singapore: World Scientific, 2016, pp. 270–281.

[32] G. L. Mullen and D. Panario, *Handbook of Finite Fields*. Boca Raton, FL, USA: CRC Press, 2013.

[33] A. Muratović-Ribić, "A note on the coefficients of inverse polynomials," *Finite Fields Appl.*, vol. 13, no. 4, pp. 977–980, 2007.

[34] H. Niederreiter and A. Winterhof, "Cyclotomic $\mathscr{R}$-orthomorphisms of finite fields," *Discrete Math.*, vol. 295, nos. 1–3, pp. 161–171, 2005.

[35] Y. H. Park and J. B. Lee, "Permutation polynomials and group permutation polynomials," *Bull. Austral. Math. Soc.*, vol. 63, no. 1, pp. 67–74, 2001.

[36] L. Reis, "Nilpotent linearized polynomials over finite fields and applications," *Finite Fields Appl.*, vol. 50, pp. 279–292, Mar. 2018.

[37] R. Shaheen and A. Winterhof, "Permutations of finite fields for check digit systems," *Des., Codes Cryptogr.*, vol. 57, pp. 361–371, Dec. 2010.

[38] C. J. Shallue and I. M. Wanless, "Permutation polynomials and orthomorphism polynomials of degree six," *Finite Fields Appl.*, vol. 20, pp. 84–92, Mar. 2013.

[39] A. Tuxanidy and Q. Wang, "On the inverses of some classes of permutations of finite fields," *Finite Fields Appl.*, vol. 28, pp. 244–281, Jul. 2014.

[40] A. Tuxanidy and Q. Wang, "Compositional inverses and complete mappings over finite fields," *Discrete Appl. Math.*, vol. 217, pp. 318–329, Jan. 2017.

[41] D. Wan and R. Lidl, "Permutation polynomials of the form $x^rf(x^{(q-1)/d})$ and their group structure," *Monatshefte Math.*, vol. 112, no. 2, pp. 149–163, 1991.

[42] L. Wang and B. Wu, "General constructions of permutation polynomials of the form $(x^{2^m}+x+\delta)^{i(2^m-1)+1}+x$ over $\mathbb{F}_{2^{2m}}$," *Finite Fields Appl.*, vol. 52, pp. 137–155, Jul. 2018.

[43] Q. Wang, "Cyclotomic mapping permutation polynomials over finite fields," in *Sequences, Subsequences, and Consequences* (Lecture Notes in Computer Science), vol. 4893. Berlin, Germany: Springer, 2007, pp. 119–128.

[44] Q. Wang, "On inverse permutation polynomials," *Finite Fields Appl.*, vol. 15, no. 2, pp. 207–213, 2009.

[45] Q. Wang, "Cyclotomy and permutation polynomials of large indices," *Finite Fields Appl.*, vol. 22, pp. 57–69, Jul. 2013.

[46] Q. Wang, "A note on inverses of cyclotomic mapping permutation polynomials over finite fields," *Finite Fields Appl.*, vol. 45, pp. 422–427, May 2017.

[47] A. Winterhof, "Generalizations of complete mappings of finite fields and some applications," *J. Symbolic Comput.*, vol. 64, pp. 42–52, Aug. 2014.

[48] B. Wu, "The compositional inverses of linearized permutation binomials over finite fields," 2013, *arXiv:1311.2154*. [Online]. Available: https://arxiv.org/abs/1311.2154

[49] B. Wu, "Linearized and linearized derived permutation polynomials over finite fields and their compositional inverses," (in Chinese), Ph.D. dissertation, Acad. Math. Syst. Sci., Chin. Acad. Sci., Beijing, China, May 2013.

[50] B. Wu, "The compositional inverse of a class of linearized permutation polynomials over $\mathbb{F}_{2^n}$, n odd," *Finite Fields Appl.*, vol. 29, pp. 34–48, Sep. 2014.

[51] B. Wu and Z. Liu, "The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2," *Finite Fields Appl.*, vol. 24, pp. 136–147, Nov. 2013.

[52] B. Wu and Z. Liu, "Linearized polynomials over finite fields revisited," *Finite Fields Appl.*, vol. 22, pp. 79–100, Jul. 2013.

[53] D. Wu, P. Yuan, C. Ding, and Y. Ma, "Permutation trinomials over $\mathbb{F}_{2^m}$," *Finite Fields Appl.*, vol. 46, pp. 38–56, Jul. 2017.

[54] Z. Zha, L. Hu, and S. Fan, "Further results on permutation trinomials over finite fields with even characteristic," *Finite Fields Appl.*, vol. 45, pp. 43–52, May 2017.

[55] D. Zheng, M. Yuan, N. Li, L. Hu, and X. Zeng, "Constructions of involutions over finite fields," *IEEE Trans. Inf. Theory*, to be published. doi: 10.1109/TIT.2019.2919511.

[56] D. Zheng, M. Yuan, and L. Yu, "Two types of permutation polynomials with special forms," *Finite Fields Appl.*, vol. 56, pp. 1–16, Mar. 2019.

[57] Y. Zheng, F. Wang, L. Wang, and W. Wei, "On inverses of some permutation polynomials over finite fields of characteristic three," 2019, *arXiv:1904.03029*. [Online]. Available: https://arxiv.org/abs/1904.03029

[58] Y. Zheng, Y. Yu, Y. Zhang, and D. Pei, "Piecewise constructions of inverses of cyclotomic mapping permutation polynomials," *Finite Fields Appl.*, vol. 40, pp. 1–9, Jul. 2016.

[59] Y. Zheng, P. Yuan, and D. Pei, "Piecewise constructions of inverses of some permutation polynomials," *Finite Fields Appl.*, vol. 36, pp. 151–169, Nov. 2015.

[60] Y. Zheng, P. Yuan, and D. Pei, "Large classes of permutation polynomials over $\mathbb{F}_{q^2}$," *Des., Codes Cryptogr.*, vol. 81, no. 3, pp. 505–521, 2016.

[61] M. E. Zieve, "On some permutation polynomials over $\mathbb{F}_q$ of the form $x^rh(x^{(q-1)/d})$," *Proc. Amer. Math. Soc.*, vol. 137, no. 7, pp. 2209–2216, 2009.

Yanbin Zheng received the Ph.D. degree in Mathematics from Guangzhou University, China, in 2015. He then joined the School of Computer Science and Engineering, Guilin University of Electronic Technology, China. He is currently a joint postdoctoral research fellow between the School of Computer Science and Engineering, South China University of Technology, and the School of Computer Science and Technology, Dongguan University of Technology. His research interests include finite fields and cryptography.

Qiang Wang was born in China where he received B. Sc., M.Sc. degrees in Mathematics from ShaanXi Normal University (China). He received a M. Sc. degree in information and System Science from Carleton University (Canada) and a Ph.D. in Mathematics from the Memorial University of Newfoundland (Canada). He is currently a Professor at Carleton University in Ottawa (Canada). His main research interests are in finite fields and applications in coding theory, combinatorics, and cryptography.

Wenhong Wei received the Ph.D. degree in Computer Science from South China University of Technology, China, in 2009. He is currently a full professor in the School of Computer Science and Technology, Dongguan University of Technology, China. His research interests include discrete mathematics and computer network.