8

Permutation polynomials

8.1 One variable

Gary L. Mullen, *The Pennsylvania State University*
Qiang Wang, *Carleton University*

8.1.1 Introduction

8.1.1 Definition For q a prime power, let $\mathbb{F}_q$ denote the finite field containing q elements. A polynomial $f \in \mathbb{F}_q[x]$ is a *permutation polynomial (PP)* of $\mathbb{F}_q$ if the function $f : c \to f(c)$ from $\mathbb{F}_q$ into itself induces a permutation. Alternatively, f is a PP of $\mathbb{F}_q$ if the equation $f(x) = a$ has a unique solution for each $a \in \mathbb{F}_q$.

8.1.2 Remark The set of all PPs on $\mathbb{F}_q$ forms a group under composition modulo $x^q - x$, isomorphic to the symmetric group S_q of order $q!$. For $q > 2$, the group S_q is generated by x^{q-2} and all linear polynomials $ax + b$, and if c is a primitive element in $\mathbb{F}_q, S_q$ is generated by $cx, x + 1$, and x^{q-2}.

8.1.3 Remark Given a permutation g of $\mathbb{F}_q$, the unique permutation polynomial $P_g(x)$ of $\mathbb{F}_q$ of degree at most $q-1$ representing the function g can be found by the Lagrange Interpolation Formula (see Theorem 1.71 in [1937]). In particular $P_g(x) = \sum_{a \in \mathbb{F}_q} g(a)(1 - (x - a)^{q-1})$; see also Theorem 2.1.131.

8.1.4 Remark If f is a PP and $a \neq 0, b \neq 0, c \in \mathbb{F}_q$, then $f_1 = af(bx+c)$ is also a PP. By suitably choosing a, b, c we can arrange to have f_1 in *normalized form* so that f_1 is monic, $f_1(0) = 0$, and when the degree n of f_1 is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is 0.

8.1.5 Remark A few well known classes of PPs from [1937]:

Monomials: The monomial x^n is a PP of $\mathbb{F}_q$ if and only if $(n, q-1) = 1$.

Dickson: For $a \neq 0 \in \mathbb{F}_q$, the polynomial $D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}$ is a PP of $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$; see Section 9.6.

Linearized: The polynomial $L(x) = \sum_{s=0}^{n-1} a_s x^{q^s} \in \mathbb{F}_{q^n}[x]$ is a PP of $\mathbb{F}_{q^n}$ if and only if $\det(a_{i-j}^{q^j}) \neq 0$, $0 \leq i, j \leq n-1$. The set of linearized PPs forms the *Betti-Mathieu group* isomorphic to the group $GL(n, \mathbb{F}_q)$, the general linear group of all non-singular $n \times n$ matrices over $\mathbb{F}_q$ under matrix multiplication. Recently, there have been several papers devoted to explicit constructions of linearized PPs; see for example, [503, 3046, 3063].

For odd q, $f(x) = x^{(q+1)/2} + ax$ is a PP of $\mathbb{F}_q$ if and only if $a^2 - 1$ is a nonzero square in $\mathbb{F}_q$. Moreover, the polynomial $f(x) + cx$ is a PP of $\mathbb{F}_q$ for $(q-3)/2$ values of $c \in \mathbb{F}_q$ [1937].

The polynomial $x^r(f(x^d))^{(q-1)/d}$ is a PP of $\mathbb{F}_q$ if $(r, q-1) = 1$, $d \mid q-1$, and $f(x^d)$ has no nonzero root in $\mathbb{F}_q$.

8.1.6 Remark For more information, we refer to Chapter 7 of [1937], and survey papers [679, 1931, 1933, 2174, 2176].

8.1.2 Criteria

8.1.7 Theorem (Hermite) Let p be the characteristic of $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is a PP if and only if

1. the polynomial f has exactly one root in $\mathbb{F}_q$;
2. for each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $(f(x))^t$ $(\text{mod } x^q - x)$ has degree at most $q-2$.

8.1.8 Remark Hermite's criterion was used by Dickson to obtain all normalized PPs of degree at most 5 [1937] in the list below.

Normalized PPs of $\mathbb{F}_q$	q
x	any q
x^2	$q \equiv 0 \pmod 2$
x^3	$q \not\equiv 1 \pmod 3$
$x^3 - ax$ (a not a square)	$q \equiv 0 \pmod 3$
$x^4 \pm 3x$	$q = 7$
$x^4 + a_1x^2 + a_2x$ (if its only root in $\mathbb{F}_q$ is 0)	$q \equiv 0 \pmod 2$
x^5	$q \not\equiv 1 \pmod 5$
$x^5 - ax$ (a not a fourth power)	$q \equiv 0 \pmod 5$
$x^5 + ax$ ($a^2 = 2$)	$q = 9$
$x^5 \pm 2x^2$	$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$ (a not a square)	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$ (a arbitrary)	$q \equiv \pm 2 \pmod 5$
$x^5 + ax^3 + 3a^2x$ (a not a square)	$q = 13$
$x^5 - 2ax^3 + a^2x$ (a not a square)	$q \equiv 0 \pmod 5$

A list of PPs of degree 6 over finite fields with odd characteristic can be found in [838]. A list of PPs of degree 6 and 7 over finite fields with characteristic two can be found in [1914].

A recent preprint [2603] tabulates all monic PPs of degree 6 in the normalized form.

8.1.9 Theorem [1937] The polynomial f is a PP 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 $\mathbb{F}_q$.

8.1.10 Remark Another criterion for PPs conjectured by Mullen [2174] in terms of the size $|V_f|$ of the value set $V_f=\{f(a)\mid a\in\mathbb{F}_q\}$ of a polynomial f of degree n was proved by Wan [2910]. Namely, if $|V_f|>q-\frac{q-1}{n}$ then f is a PP of $\mathbb{F}_q$ [2910]. We refer to Section 8.3 for more information on value sets. A variation of Hermite's criterion in terms of combinatorial identities is given in [2014]. Hermite's criterion can be rewritten in terms of the invariant, $u_p(f)$, the smallest positive integer k such that $\sum_{x\in\mathbb{F}_q} f(x)^k\neq 0$. That is, f is a PP of $\mathbb{F}_q$ if and only if $u_p(f)=q-1$. In the case $q=p$, this criterion was improved in [1810] and only requires $k>\frac{p-1}{2}$. Using Teichmüller liftings, Wan et al. [2918] obtained an upper bound for $|V_f|$ and improved Hermite's criterion. Several other criteria were obtained by Turnwald [2825] in terms of invariants associated with elementary symmetric polynomials, without using Teichmüller liftings.

8.1.11 Theorem [2825] Let $f\in\mathbb{F}_q[x]$ be a polynomial of degree n with $1\leq n<q$. Let u be the smallest positive integer k with $s_k\neq 0$ if such k exists and otherwise set $u=\infty$, where s_k denotes the k-th elementary symmetric polynomial of the values $f(a)$. Let v be the size of the value set $V_f=\{f(a)\mid a\in\mathbb{F}_q\}$. Let w be the smallest positive integer k with $p_k=\sum_{a\in\mathbb{F}_q}f(a)^k\neq 0$ if such k exists and otherwise set $w=\infty$. The following are equivalent:

(1) f is a PP of $\mathbb{F}_q$; (2) $u=q-1$; (3) $u>q-\frac{q}{n}$;
(4) $u>q-v$; (5) $v>q-\frac{q-1}{n}$; (6) $w=q-1$;
(7) $\frac{2q}{3}-1<w<\infty$; (8) $q-\frac{q+1}{n}<w<\infty$; (9) $q-u\leq w<\infty$;
(10) $u>\frac{q-1}{2}$ and $w<\infty$.

8.1.12 Remark A criterion in terms of resultants was given by von zur Gathen [1220]. Using the Euclidean algorithm to compute the resultant, von zur Gathen provided a probabilistic test to determine whether a given polynomial is a PP or not. The number of operations in $\mathbb{F}_q$ has a softly linear running time $O(n\log q(\log(n\log q))^k)$ for some k. Furthermore, Ma and von zur Gathan showed that this decision problem has a zero-error probabilistic polynomial time in [1981] and provided a random polynomial time test for rational functions over finite fields, along with several related problems in [1982]. Earlier, Shparlinski had given a deterministic superpolynomial time algorithm for testing PP [2637]. In 2005 Kayal provided a deterministic polynomial-time algorithm for testing PP [1713].

8.1.3 Enumeration and distribution of PPs

8.1.13 Problem [1933] Let $N_n(q)$ denote the number of PPs of $\mathbb{F}_q$ which have degree n. We have the trivial boundary conditions: $N_1(q)=q(q-1)$, $N_n(q)=0$ if n is a divisor of $q-1$ larger than 1, and $\sum N_n(q)=q!$ where the sum is over all $1\leq n<q-1$ such that n is either 1 or is not a divisor of $q-1$. Find $N_n(q)$.

8.1.14 Remark In an invited address before the MAA in 1966, Carlitz conjectured that for each even integer n, there is a constant C_n so that for each finite field of odd order $q>C_n$, there does not exist a PP of degree n over $\mathbb{F}_q$. A polynomial f over $\mathbb{F}_q$ is *exceptional* if the only absolutely irreducible factors of $f(x)-f(y)$ in $\mathbb{F}_q[x,y]$ are scalar multiples of $x-y$. One can also characterize an exceptional polynomial as a polynomial which induces a permutation of infinitely many finite extension fields of $\mathbb{F}_q$. As first proved by Cohen in [665], any exceptional polynomial is a PP, and the converse holds if q is large compared to the degree of f. Cohen's equivalent statement of Carlitz's conjecture [675] says that there is no exceptional polynomial of even degree in odd characteristic. This was proved by Fried, Guralnick and Saxl in [1119]; in fact an even stronger result was obtained through the use of powerful group theoretic methods, including the classification of finite simple groups.

8.1.15 Remark For the next theorem we require the concept of an exceptional cover; see Section 9.7.

8.1.16 Theorem [1119] There is no exceptional cover of nonsingular absolutely irreducible curves over $\mathbb{F}_q$ of degree $2p$ where q is a power of p and p is prime.

8.1.17 Remark Several partial results on Carlitz's conjecture can be found in [675, 2907]. Moreover, Wan generalized Carlitz's conjecture in [2908] proving that if $q > n^4$ and $(n, q-1) = 1$ then there is no PP of degree n over $\mathbb{F}_q$. Later Cohen and Fried [686] gave an elementary proof of Wan's conjecture following an argument of Lenstra and this result was stated in terms of exceptional polynomials; see Section 8.4 for more information on exceptional polynomials.

8.1.18 Theorem [686, 2908] There is no exceptional polynomial of degree n over $\mathbb{F}_q$ if $(n, q-1) > 1$.

8.1.19 Theorem [550]

1. Let $\ell > 1$. For q sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a PP of $\mathbb{F}_q$.
2. Let $\ell > 1$, $(r, q-1) = 1$, and k be a positive integer. For q sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x^r(x^{(q-1)/\ell} + a)^k$ is a PP of $\mathbb{F}_q$.

8.1.20 Remark Any non-constant polynomial $h(x) \in \mathbb{F}_q[x]$ of degree $\leq q-1$ can be written *uniquely* as $ax^r f(x^{(q-1)/\ell}) + b$ with index ℓ [61]. Namely, write

$$h(x) = a(x^n + a_{n-i_1}x^{n-i_1} + \cdots + a_{n-i_k}x^{n-i_k}) + b,$$

where a, $a_{n-i_j} \neq 0$, $j = 1, \ldots, k$. Here we suppose that $j \geq 1$ and $n - i_k = r$. Then $h(x) = ax^r f(x^{(q-1)/\ell}) + b$, where $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} + \cdots + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$,

$$\ell = \frac{q-1}{(n-r, n-r-i_1, \ldots, n-r-i_{k-1}, q-1)},$$

and $(e_0, e_1, \ldots, e_{k-1}, \ell) = 1$. Clearly, h is a PP of $\mathbb{F}_q$ if and only if $g(x) = x^r f(x^{(q-1)/\ell})$ is a PP of $\mathbb{F}_q$. Then ℓ is the *index* of h.

8.1.21 Remark If $\ell = 1$ then $f(x) = 1$ so that $g(x) = x^r$. In this case $g(x)$ is a PP of $\mathbb{F}_q$ if and only if $(r, q-1) = 1$. We can assume $\ell > 1$.

8.1.22 Remark More existence and enumerative results for binomials can be found in [61, 64, 1830, 2014, 2017, 2018, 2824, 2904, 2912]. In [1830], Laigle-Chapuy proved the first assertion of Theorem 8.1.19 assuming $q > \ell^{2\ell+2}\left(1 + \frac{\ell+1}{\ell^{\ell+2}}\right)^2$. In [2018], Masuda and Zieve obtained a stronger result for more general binomials of the form $x^r(x^{e_1(q-1)/\ell} + a)$. More precisely they showed the truth of Part 1 of Theorem 8.1.19 for $q > \ell^{2\ell+2}$. Here we present a general result of Akbary-Ghioca-Wang (Theorem 8.1.25) which shows that there exist permutation polynomials of index ℓ for any prescribed exponents satisfying conditions (8.1.1). This result generalizes all the existence results from [550, 1830, 2018].

8.1.23 Definition [61] Let q be a prime power, and $\ell \geq 2$ be a divisor of $q-1$. Let m, r be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an m-tuple of integers that satisfy the following conditions:

$$0 < e_1 < e_2 < \cdots < e_m \leq \ell - 1, \ (e_1, \ldots, e_m, \ell) = 1 \text{ and } r + e_m s \leq q-1, \qquad (8.1.1)$$

where $s := (q-1)/\ell$. For a tuple $\bar{a} := (a_1, \dots, a_m) \in \left(\mathbb{F}_q^*\right)^m$, we let

$$g_{r,\bar{e}}^{\bar{a}}(x) := x^r \left(x^{e_m s} + a_1 x^{e_{m-1} s} + \cdots + a_{m-1} x^{e_1 s} + a_m\right).$$

We define $N_{r,\bar{e}}^m(\ell, q)$ as the number of all tuples $\bar{a} \in \left(\mathbb{F}_q^*\right)^m$ such that $g_{r,\bar{e}}^{\bar{a}}(x)$ is a PP of $\mathbb{F}_q$. In other words $N_{r,\bar{e}}^m(\ell, q)$ is the number of all monic permutation $(m+1)$-nomials $g_{r,\bar{e}}^{\bar{a}}(x) = x^r f(x^{(q-1)/\ell})$ over $\mathbb{F}_q$ with vanishing order at zero equal to r, set of exponents $\bar{e}$ for $f(x)$, and index ℓ. Note that if r and $\bar{e}$ satisfy (8.1.1) then $g_{r,\bar{e}}^{\bar{a}}(x)$ has index ℓ.

8.1.24 Theorem [61] With the above notation, we have

$$\left| N_{r,\bar{e}}^m(\ell, q) - \frac{\ell!}{\ell^\ell} q^m \right| < \ell! \ell q^{m-1/2}.$$

8.1.25 Theorem [61] For any q, r, $\bar{e}$, m, ℓ that satisfy (8.1.1), $(r, s) = 1$, and $q > \ell^{2\ell+2}$, there exists an $\bar{a} \in (\mathbb{F}_q^*)^m$ such that the $(m+1)$-nomial $g_{r,\bar{e}}^{\bar{a}}(x)$ is a permutation polynomial of $\mathbb{F}_q$.

8.1.26 Remark For $q \geq 7$ we have $\ell^{2\ell+2} < q$ if $\ell < \frac{\log q}{2 \log \log q}$.

8.1.27 Theorem [769] The value $N_{p-2}(p) \sim (\varphi(p)/p)p!$ as $p \to \infty$, where φ is the Euler function. More precisely, $\left| N_{p-2}(p) - \frac{\varphi(p)}{p} p! \right| \leq \sqrt{\frac{p^{p+1}(p-2)+p^2}{p-1}}$.

8.1.28 Theorem [1784] Let q be a prime power. Then $|N_{q-2}(q) - (q-1)!| \leq \sqrt{\frac{2e}{\pi}} q^{\frac{q}{2}}$.

8.1.29 Theorem [1785] Fix j integers $k_1, \dots, k_j$ with the property that $0 < k_1 < \cdots < k_j < q-1$ and define $N(k_1, \dots, k_j; q)$ as the number of PPs of $\mathbb{F}_q$ of degree less than $q-1$ such that the coefficient of x^{k_i} equals 0, for $i = 1, \dots, j$. Then

$$\left| N(k_1, \dots, k_j; q) - \frac{q!}{q^j} \right| < \left(1 + \sqrt{\frac{1}{e}}\right)^q ((q - k_1 - 1)q)^{q/2}.$$

In particular, $N_{q-2}(q) = q! - N(q-2; q)$.

8.1.30 Remark We note that for $1 \leq t \leq q-2$ the number of PPs of degree at least $q-t-1$ is $q! - N(q-t-1, q-t, \dots, q-2; q)$. In [1785] Konyagin and Pappalardi proved that $N(q-t-1, q-t, \dots, q-2; q) \sim \frac{q!}{q^t}$ holds for $q \to \infty$ and $t \leq 0.03983\, q$. This result guarantees the existence of PPs of degree at least $q-t-1$ for $t \leq 0.03983\, q$ (as long as q is sufficiently large). However, the following theorem establishes the existence of PPs with exact degree $q-t-1$.

8.1.31 Theorem [61] Let $m \geq 1$. Let q be a prime power such that $q-1$ has a divisor ℓ with $m < \ell$ and $\ell^{2\ell+2} < q$. Then for every $1 \leq t < \frac{(\ell-m)}{\ell}(q-1)$ coprime with $(q-1)/\ell$ there exists an $(m+1)$-nomial $g_{r,\bar{e}}^{\bar{a}}(x)$ of degree $q-t-1$ which is a PP of $\mathbb{F}_q$.

8.1.32 Corollary [61] Let $m \geq 1$ be an integer, and let q be a prime power such that $(m+1) \mid (q-1)$. Then for all $n \geq 2m+4$, there exists a permutation $(m+1)$-nomial of $\mathbb{F}_{q^n}$ of degree $q-2$.

8.1.33 Definition Let $m_{[k]}(q)$ be the number of permutations of $\mathbb{F}_q$ which are k-cycles and are represented by polynomials of degree $q-k$.

8.1.34 Theorem [2966] Every transposition of $\mathbb{F}_q$ is represented by a unique polynomial of degree $q-2$. Moreover,

$$m_{[3]}(q) = \begin{cases} \frac{2}{3}q(q-1) & \text{if } q \equiv 1 \pmod{3}, \\ 0 & \text{if } q \equiv 2 \pmod{3}, \\ \frac{1}{3}q(q-1) & \text{if } q \equiv 0 \pmod{3}. \end{cases}$$

8.1.35 Theorem [1994]

1. If $q \equiv 1 \pmod{k}$, then $m_{[k]}(q) \geq \frac{\varphi(k)}{k} q(q-1)$.
2. If $\mathrm{char}(\mathbb{F}_q) > e^{(k-3)/e}$, then $m_{[k]}(q) \leq \frac{(k-1)!}{k} q(q-1)$.

8.1.36 Remark It is conjectured in [1994] that the above upper bound for $m_{[k]}(q)$ holds for any $k < q$. Small k-cycles such as $k = 4, 5$ are also studied in [1993, 1994, 1995].

8.1.37 Theorem [2966] Let r and s be fixed positive integers, and $k_2, \ldots, k_s$ be non-negative integers such that $\sum_{i=2}^{s} ik_i = r$. Let $P(k_2, \ldots, k_s)$ be the set of permutations of $\mathbb{F}_q$ which are the disjoint products of k_2 transpositions, k_3 3-cycles, etc. Then the number of permutations in $P(k_2, \ldots, k_s)$ represented by a polynomial of degree $q-2$ is asymptotic to the number of all permutations in $P(k_2, \ldots, k_s)$ as q goes to ∞.

8.1.4 Constructions of PPs

8.1.38 Remark For the purpose of introducing the construction of PPs in the next few sections, we present the following recent result by Akbary-Ghioca-Wang (AGW).

8.1.39 Theorem (AGW's criterion, [62]) Let A, S and $\bar{S}$ be finite sets with $\#S = \#\bar{S}$, and let $f : A \to A$, $\bar{f} : S \to \bar{S}$, $\lambda : A \to S$, and $\bar{\lambda} : A \to \bar{S}$ be maps such that $\bar{\lambda} \circ f = \bar{f} \circ \lambda$. If both λ and $\bar{\lambda}$ are surjective, then the following statements are equivalent:

1. f is a bijection (a permutation of A);
2. $\bar{f}$ is a bijection from S to $\bar{S}$ and f is injective on $\lambda^{-1}(s)$ for each $s \in S$.

8.1.40 Remark We note that this criterion does not require any restriction on the structures of the sets S and $\bar{S}$ in finding new classes of PPs of a set A. In particular, if we take A as a group and S and $\bar{S}$ as homomorphic images of A, then we obtain the following general result for finding permutations of a group.

8.1.41 Theorem [62] Let $(G, +)$ be a finite group, and let $\varphi, \psi, \bar{\psi} \in \mathrm{End}(G)$ be group endomorphisms such that $\bar{\psi} \circ \varphi = \varphi \circ \psi$ and $\#\mathrm{im}(\psi) = \#\mathrm{im}(\bar{\psi})$. Let $g : G \longrightarrow G$ be any mapping, and let $f : G \longrightarrow G$ be defined by $f(x) = \varphi(x) + g(\psi(x))$. Then,

1. f permutes G if and only if the following two conditions hold:
   a. $\ker(\varphi) \cap \ker(\psi) = \{0\}$ (or equivalently, φ induces a bijection between $\ker(\psi)$ and $\ker(\bar{\psi})$); and
   b. the function $\bar{f}(x) := \varphi(x) + \bar{\psi}(g(x))$ restricts to a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$.
2. For any fixed endomorphisms φ, ψ and $\bar{\psi}$ satisfying Part 1.a, there are $(\#\mathrm{im}(\psi))! \cdot \left(\#\ker(\bar{\psi})\right)^{\#\mathrm{im}(\psi)}$ such permutation functions f (when g varies).
3. Let $g : G \longrightarrow G$ be such that $\left(\bar{\psi} \circ g\right)|_{\mathrm{im}(\psi)} = 0$. Then $f = \varphi + g \circ \psi$ permutes G if and only if φ is a permutation of G.
4. Assume $\varphi \circ \psi = 0$ and $g : G \longrightarrow G$ is a mapping such that $g(x)$ restricted to $\mathrm{im}(\psi)$ is a permutation of $\mathrm{im}(\psi)$. Then $f(x) = \varphi(x) + g(\psi(x))$ permutes G if and only if φ and ψ satisfy Part 1.a, and $\bar{\psi}$ restricted to $\mathrm{im}(\psi)$ is a bijection from $\mathrm{im}(\psi)$ to $\mathrm{im}(\bar{\psi})$.

8.1.42 Remark One can apply this result to a multiplicative group of a finite field, an additive group of a finite field, or the group of rational points of an elliptic curve over finite fields [62]. This reduces a problem of determining whether a given polynomial over a finite field

$\mathbb{F}_q$ is a permutation polynomial to a problem of determining whether another polynomial permutes a smaller set.

8.1.43 Corollary [2357, 2939, 3074] Let $q-1=\ell s$ for some positive integers ℓ and s. Then $P(x)=x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r,s)=1$ and $x^r f(x)^s$ permutes the set μ_ℓ of all distinct ℓ-th roots of unity.

8.1.44 Remark The above corollary is a consequence of Theorem 8.1.41 when taking multiplicative group endomorphisms x^r and x^s. There are several other equivalent descriptions of PPs of the form $x^r f(x^s)$; see for example, [65, 2357, 2915, 2939, 3074]. All of the classes of PPs in Subsection 8.1.5 are of this type. There are also many recent results on new classes of PPs when taking additive group endomorphisms in Theorem 8.1.41, see [62, 2001, 3045, 3075]. We give some classes of PPs in Subsection 8.1.6. We note that AGW's criterion does not require any restriction on the structures of subsets S and $\bar{S}$, which has even broader applications in finding new classes of PPs. Many classes of PPs in Subsection 8.1.7 can be obtained through this general construction method.

8.1.5 PPs from permutations of multiplicative groups

8.1.45 Definition [2276, 2939] Let γ be a primitive element of $\mathbb{F}_q$, $q-1=\ell s$ for some positive integers ℓ and s, and the set of all nonzero ℓ-th powers of $\mathbb{F}_q$ be $C_0=\{\gamma^{\ell j} : j=0,1,\ldots,s-1\}$. Then C_0 is a subgroup of $\mathbb{F}_q^*$ of index ℓ. The elements of the factor group $\mathbb{F}_q^*/C_0$ are the *cyclotomic cosets*

$$C_i := \gamma^i C_0, \quad i=0,1,\ldots,\ell-1.$$

For any integer $r>0$ and any $A_0, A_1, \ldots, A_{\ell-1} \in \mathbb{F}_q$, we define an *$r$-th order cyclotomic mapping $f^r_{A_0,A_1,\ldots,A_{\ell-1}}$ of index ℓ* from $\mathbb{F}_q$ to itself by $f^r_{A_0,A_1,\ldots,A_{\ell-1}}(0)=0$ and

$$f^r_{A_0,A_1,\ldots,A_{\ell-1}}(x) = A_i x^r \quad \text{if } x \in C_i, \quad i=0,1,\ldots,\ell-1.$$

Moreover, $f^r_{A_0,A_1,\ldots,A_{\ell-1}}$ is an *r-th order cyclotomic mapping of the least index ℓ* if the mapping can not be written as a cyclotomic mapping of any smaller index.

8.1.46 Remark Cyclotomic mapping permutations were introduced in [2276] when $r=1$ and in [2939] for any positive r. Let $\zeta=\gamma^s$ be a primitive ℓ-th root of unity in $\mathbb{F}_q$ and $P(x)=x^r f(x^s)$ be a polynomial of index ℓ over $\mathbb{F}_q$ with positive integer r. Then $P(x)=x^r f(x^s)=f^r_{A_0,A_1,\ldots,A_{\ell-1}}(x)$ where $A_i=f(\zeta^i)$ for $0\le i\le \ell-1$. We note that the least index of a cyclotomic mapping is equal to the index of the corresponding polynomial. If P is a PP of $\mathbb{F}_q$ then $(r,s)=1$ and $A_i=f(\zeta^i)\ne 0$ for $0\le i\le \ell-1$. Under these two necessary conditions, $P(x)=x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $f^r_{A_0,A_1,\ldots,A_{\ell-1}}$ is a PP of $\mathbb{F}_q$ [2939]. The concept of cyclotomic mapping permutations have recently been generalized in [2942] allowing each branch to take a different r_i value so that $P(x)$ has the form $\sum_{i=0}^n x^{r_i} f_i(x^s)$. More results can be found in [2942] and related piecewise constructions in [1060, 3056].

8.1.47 Remark There are several other equivalent descriptions of PPs of the form $x^r f(x^s)$, see [65, 2357, 2915, 2939, 3074] for example. In particular, in [65], it is shown that $P(x)=x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r,s)=1$, $A_i=f(\zeta^i)\ne 0$ for $0\le i\le \ell-1$, and $\displaystyle\sum_{i=0}^{\ell-1} \zeta^{cri} A_i^{cs}=0$ for all $c=1,\ldots,\ell-1$. This criterion is equivalent to Hermite's criterion when the index ℓ equals $q-1$. However, if $\ell<q-1$, this criterion in fact improves Hermite's

criterion because we only need to verify that the coefficient of x^{q-1} is 0 for $\ell - 1$ different powers of P instead of all of the $q-2$ powers of P. We note that $\ell = 2$ implies that q must be odd.

8.1.48 Remark [65] For odd q, the polynomial $P(x) = x^r f(x^{(q-1)/2})$ is a PP of $\mathbb{F}_q$ if and only if $(r, (q-1)/2) = 1$ and $\eta(f(-1)f(1)) = (-1)^{r+1}$. Here η is the quadratic character of $\mathbb{F}_q$ with the standard convention $\eta(0) = 0$.

8.1.49 Remark Let $P(x) = x^k + ax^r$ be a binomial of index ℓ and $s = \frac{q-1}{\ell}$. Then $P(x) = x^r(x^{es} + a)$ for some e such that $(e, \ell) = 1$. If $a = b^s$ for some $b \in \mathbb{F}_q$, then $x^r(x^{es} + a)$ is a PP of $\mathbb{F}_q$ if and only if $x^r(x^{es} + 1)$ is a PP of $\mathbb{F}_q$.

8.1.50 Remark Necessary conditions for $P(x) = x^r(x^{es} + 1)$ of index ℓ to be a PP are as follows:

$$(r, s) = 1, (2e, \ell) = 1, (2r + es, \ell) = 1, \text{ and } 2^s = 1. \tag{8.1.2}$$

8.1.51 Remark For $\ell = 3$, the conditions in (8.1.2) are sufficient to determine whether P is a PP of $\mathbb{F}_q$ [2926]. However, for $\ell > 3$, it turns out not to be the case (for example, see [63, 64, 2926]). For general ℓ, a characterization of PPs of the form $x^r(x^{es}+1)$ in terms of generalized Lucas sequences of order $k := \frac{\ell-1}{2}$ is given in [2939, 2941].

8.1.52 Definition [64] For any integer $k \geq 1$ and η a fixed primitive $(4k+2)$-th root of unity, the *generalized Lucas sequence* (or *unsigned generalized Lucas sequence*) of order k is defined as $\{a_n\}_{n=0}^{\infty}$ such that

$$a_n = \sum_{\substack{t=1 \\ t \text{ odd}}}^{2k} (\eta^t + \eta^{-t})^n = \sum_{t=1}^{k} ((-1)^{t+1}(\eta^t + \eta^{-t}))^n.$$

The *characteristic polynomial* of the generalized Lucas sequence is defined by $g_0(x) = 1$, $g_1(x) = x - 1$, $g_k(x) = xg_{k-1}(x) - g_{k-2}(x)$ for $k \geq 2$.

8.1.53 Theorem [2939, 2941] Let $q = p^m$ be an odd prime power and $q - 1 = \ell s$ with odd $\ell \geq 3$ and $(e, \ell) = 1$. Let $k = \frac{\ell-1}{2}$. Then $P(x) = x^r(x^{es} + 1)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(2r + es, \ell) = 1$, $2^s = 1$, and

$$R_{j_c,k}(L)(a_{cs}) = -1, \text{ for all } c = 1, \ldots, \ell - 1, \tag{8.1.3}$$

where a_{cs} is the (cs)-th term of the generalized Lucas sequence $\{a_i\}_{i=0}^{\infty}$ of order k over $\mathbb{F}_p$, $j_c = c(2e^{\phi(\ell)-1}r + s) \pmod{2\ell}$, $R_{j_c,k}(x)$ is the remainder of the Dickson polynomial $D_{j_c}(x)$ of the first kind of degree j_c divided by the characteristic polynomial $g_k(x)$, and L is a left shift operator on sequences. In particular, all j_c are distinct even numbers between 2 and $2\ell - 2$.

8.1.54 Remark We note that the degree of any remainder $R_{n,k}$ is at most $k-1$ and $R_{n,k}$ is either a Dickson polynomial of degree $\leq k-1$ or the degree $k-1$ characteristic polynomial $g_{k-1}(x)$ of the generalized Lucas sequence of order k, or a negation of the above polynomials [2941]. We can extend the definition of $\{a_n\}$ to negative subscripts n using the same recurrence relations. We also remark that, for $\ell \leq 7$, the sequences used in the descriptions of permutation binomials have simple structures and are fully described [63, 2926]. We note that signed generalized Lucas sequences are defined in [2941] and they are used to compute the coefficients of the compositional inverse of permutation binomials $x^r(x^{es} + 1)$. Finally we note that Equation (8.1.3) always holds if the sequence $\{a_n\}$ is *s-periodic* over $\mathbb{F}_p$, which means that $a_n \equiv a_{n+ks} \pmod{p}$ for integers k and n. We remark that these sequences are defined over prime fields and checking the s-periodicity of these sequences is a much simpler task than checking whether the polynomial is a PP over the extension field directly.

8.1.55 Theorem [64] Assume the conditions (8.1.2) on ℓ, r, e and s hold. If $\{a_n\}$ is s-periodic over $\mathbb{F}_p$, then the binomial $P(x) = x^r(x^{es} + 1)$ is a permutation binomial of $\mathbb{F}_q$.

8.1.56 Theorem [65] Let p be an odd prime and $q = p^m$ and let ℓ, r, s be positive integers satisfying that $q - 1 = \ell s$, $(r, s) = 1$, $(e, \ell) = 1$, and ℓ odd. Let $p \equiv -1 \pmod{\ell}$ or $p \equiv 1 \pmod{\ell}$ and $\ell \mid m$. Then the binomial $P(x) = x^r(x^{es} + 1)$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(2r + es, \ell) = 1$. In particular, if $p \equiv 1 \pmod{\ell}$ and $\ell \mid m$, then the conditions $(r, s) = 1$, $(e, \ell) = 1$, and ℓ odd imply that $(2r + es, \ell) = 1$ [60].

8.1.57 Remark For $a = 1$ (equivalent to $a = b^s$ for some b), under the assumptions on q, s, ℓ, r, e, it is shown in [3074] that the s-periodicity of the generalized Lucas sequence implies that $(\eta + \eta^{-1})^s = 1$ for every (2ℓ)-th root of unity η. However, we note that these two conditions are in fact equivalent for $a = 1$. The following result extends Theorem 8.1.55 as it also deals with even characteristic.

8.1.58 Theorem [3074] For q, s, ℓ, e, r, a satisfying $q - 1 = \ell s$, $(r, s) = 1$, $(e, \ell) = 1$, $r, e > 0$ and $a \in \mathbb{F}_q^*$, suppose $(-a)^\ell \neq 1$ and $(z + a/z)^s = 1$ for every (2ℓ)-th root of unity z. Then $P(x) = x^r(x^{es} + a)$ is a permutation binomial of $\mathbb{F}_q$ if and only if $(2r + es, 2\ell) \leq 2$.

8.1.59 Theorem [2018] Suppose $x^r(x^{es} + a)$ permutes $\mathbb{F}_p$, where $a \in \mathbb{F}_p^*$ and $r, e, s > 0$ such that $p - 1 = \ell s$ and $(\ell, e) = 1$. Then $s \geq \sqrt{p - 3/4} - 1/2 > \sqrt{p} - 1$.

8.1.60 Remark For earlier results on permutation binomials, we refer to [568, 2014, 2018, 2125, 2679, 2680, 2824, 2904, 2912].

8.1.61 Theorem [65] Let $q - 1 = \ell s$. Assume that $f(\zeta^t)^s = 1$ for any $t = 0, \ldots, \ell - 1$. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r, q - 1) = 1$.

8.1.62 Corollary Let $q - 1 = \ell s$ and g be any polynomial over $\mathbb{F}_q$. Then $P(x) = x^r g(x^s)^\ell$ is a PP of $\mathbb{F}_q$ if and only if $(r, q - 1) = 1$ and $g(\zeta^t) \neq 0$ for all $0 \leq t \leq \ell - 1$.

8.1.63 Corollary [65, 1830] Let p be a prime, ℓ be a positive integer and v be the order of p in $\mathbb{Z}/\ell\mathbb{Z}$. For any positive integer n, let $q = p^m = p^{\ell v n}$ and $\ell s = q - 1$. Assume f is a polynomial in $\mathbb{F}_{p^{vn}}[x]$. Then the polynomial $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r, q - 1) = 1$ and $f(\zeta^t) \neq 0$ for all $0 \leq t \leq \ell - 1$.

8.1.64 Remark Corollary 8.1.63 is reformulated as Theorem 2.3 in [3074]. Namely, let $\ell, r > 0$ satisfy $\ell s = q - 1$. Suppose $q = q_0^m$ where $q_0 \equiv 1 \pmod{\ell}$ and $\ell \mid m$, and $f \in \mathbb{F}_{q_0}[x]$. Then $P(x) = x^r f(x^s)$ permutes $\mathbb{F}_q$ if and only if $(r, s) = 1$ and f has no roots in the μ_ℓ, the set of ℓ-th roots of unity.

8.1.65 Theorem [65] Let $q - 1 = \ell s$, and suppose that $\overline{\mathbb{F}}_q$ (the algebraic closure of $\mathbb{F}_q$) contains a primitive $(j\ell)$-th root of unity η. Assume that $\left(\eta^{-ut} f(\eta^{jt})\right)^s = 1$ for any $t = 0, \ldots, \ell - 1$ and a fixed u. Moreover assume that $j \mid us$. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$ and $(r + \frac{us}{j}, \ell) = 1$.

8.1.66 Remark Some concrete classes of PPs satisfying the above assumptions can be found in [60, 65, 2031, 3073, 3074]. For example, let $h_k(x) := x^k + \cdots + x + 1$. Then the permutation behavior of the polynomials $x^r h_k(x^s) = x^r(x^{ks} + \cdots + x^s + 1)$ and $x^r h_k(x^{es})^t$ has been studied in detail. Moreover, for certain choices of indices ℓ and finite fields $\mathbb{F}_q$ (for example, $p \equiv -1 \pmod{2\ell}$ where $\ell > 1$ is either odd or $2\ell_1$ with ℓ_1 odd), several concrete classes of PPs can be obtained [65, 3073, 3074].

8.1.67 Remark When $\ell \leq 5$, much simpler descriptions involving congruences and gcd conditions can be found in [60, 2031]. A reformulation of these results in terms of roots of unity can be found in [3073] which also covers the case of $\ell = 7$. For larger index ℓ, one can also construct PPs of this form when ℓ is an odd prime such that $\ell < 2p + 1$.

8.1.68 Theorem [60] Let ℓ be an odd prime such that $\ell < 2p+1$, then $P(x) = x^r(x^{ks} + \cdots + x^s + 1)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$, $(\ell, k + 1) = 1$, $(2r + ks, \ell) = 1$, and $(k + 1)^s \equiv 1 \pmod{p}$.

8.1.6 PPs from permutations of additive groups

8.1.69 Remark There are several results on new classes of PPs when using additive group endomorphisms ψ, $\bar{\psi}$, and φ in Theorem 8.1.39 [62, 2001, 3045, 3075].

8.1.70 Theorem [62] Consider any polynomial $g \in \mathbb{F}_{q^n}[x]$, any additive polynomials $\varphi, \psi \in \mathbb{F}_{q^n}[x]$, any $\mathbb{F}_q$-linear polynomial $\bar{\psi} \in \mathbb{F}_{q^n}[x]$ satisfying $\varphi \circ \psi = \bar{\psi} \circ \varphi$ and $\#\psi(\mathbb{F}_{q^n}) = \#\bar{\psi}(\mathbb{F}_{q^n})$, and any polynomial $h \in \mathbb{F}_{q^n}[x]$ such that $h(\psi(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q \setminus \{0\}$. Then

1. $f(x) := h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_{q^n}$ if and only if
   a. $\ker(\varphi) \cap \ker(\psi) = \{0\}$; and
   b. $\bar{f}(x) := h(x)\varphi(x) + \bar{\psi}(g(x))$ is a bijection between $\psi(\mathbb{F}_{q^n})$ and $\bar{\psi}(\mathbb{F}_{q^n})$.
2. For any fixed h, φ, ψ and $\bar{\psi}$ satisfying the above hypothesis and Part 1.a, there are $(\#\mathrm{im}(\psi))! \cdot \big(\#\ker(\bar{\psi})\big)^{\#\mathrm{im}(\psi)}$ such permutation functions f (when g varies) (where ψ and $\bar{\psi}$ are viewed as endomorphisms of $(\mathbb{F}_{q^n}, +)$).
3. Assume in addition that $\big(\bar{\psi} \circ g\big)\mid_{\mathrm{im}(\psi)} = 0$. Then $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$ and $h(x)\varphi(x)$ induces a bijection from $\psi(\mathbb{F}_{q^n})$ to $\bar{\psi}(\mathbb{F}_{q^n})$.
4. Assume in addition that $\varphi \circ \psi = 0$, and that $g(x)$ restricted to $\mathrm{im}(\psi)$ is a permutation of $\mathrm{im}(\psi)$. Then $f(x) = h(\psi(x))\varphi(x) + g(\psi(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $\ker(\varphi) \cap \ker(\psi) = \{0\}$ and $\bar{\psi}$ restricted to $\mathrm{im}(\psi)$ is a bijection between $\mathrm{im}(\psi)$ and $\mathrm{im}(\bar{\psi})$.

8.1.71 Theorem [62, 3045] Let $q = p^e$ for some positive integer e.

1. If k is an even integer or k is odd and q is even, then $f_{a,b,k}(x) = ax^q + bx + (x^q - x)^k$, $a, b \in \mathbb{F}_{q^2}$, permutes $\mathbb{F}_{q^2}$ if and only if $b - a^q \in \mathbb{F}_q^*$ and $a + b \neq 0$.

2. If k and q are odd positive integers, then $f_{a,k}(x) = ax^q + a^q x + (x^q - x)^k$, $a \in \mathbb{F}_{q^2}^*$ and $a + a^q \neq 0$, permutes $\mathbb{F}_{q^2}$ if and only if $(k, q - 1) = 1$.

8.1.72 Remark The classes $f_{a,b,k}$ with $a, b \in \mathbb{F}_q$ and k even and $f_{a,k}$ for $a \in \mathbb{F}_q$ and p and k odd were first constructed in [62]. The remaining classes were obtained in [3045]. For other concrete classes of PPs of additive groups, we refer to [62, 324, 728, 1829, 2001, 3045, 3075].

8.1.7 Other types of PPs from the AGW criterion

8.1.73 Remark In this subsection, we give several other constructions of PPs that can be obtained by using arbitrary surjective maps λ and $\bar{\lambda}$ in Theorem 8.1.39, instead of using multiplicative or additive group homomorphism.

8.1.74 Theorem [62] Let q be a prime power, let n be a positive integer, and let L_1, L_2, L_3 be $\mathbb{F}_q$-linear polynomials over $\mathbb{F}_q$ seen as endomorphisms of $(\mathbb{F}_{q^n}, +)$. Let $g \in \mathbb{F}_{q^n}[x]$ be such that $g(L_3(\mathbb{F}_{q^n})) \subseteq \mathbb{F}_q$. Then $f(x) = L_1(x) + L_2(x)g(L_3(x))$ is a PP of $\mathbb{F}_{q^n}$ if and only if

1. $\ker(F_y) \cap \ker(L_3) = \{0\}$, for any $y \in \operatorname{im}(L_3)$, where $F_y(x) := L_1(x) + L_2(x)g(y)$; and
2. $\bar{f}(x) := L_1(x) + L_2(x)g(x)$ permutes $L_3(\mathbb{F}_{q^n})$.

8.1.75 Remark The above result extends some constructions in [324, 728].

8.1.76 Theorem [62] Let q be any power of the prime number p, let n be any positive integer, and let S be any subset of $\mathbb{F}_{q^n}$ containing 0. Let $h, k \in \mathbb{F}_{q^n}[x]$ be polynomials such that $h(0) \neq 0$ and $k(0) = 0$, and let $B \in \mathbb{F}_{q^n}[x]$ be any polynomial satisfying $h(B(\mathbb{F}_{q^n})) \subseteq S$ and $B(a\alpha) = k(a)B(\alpha)$ for all $a \in S$ and all $\alpha \in \mathbb{F}_{q^n}$. Then the polynomial $f(x) = xh(B(x))$ is a PP of $\mathbb{F}_{q^n}$ if and only if $\bar{f}(x) = xk(h(x))$ induces a permutation of the value set $B(\mathbb{F}_{q^n})$.

8.1.77 Remark The case that $S = \mathbb{F}_q$ and $k(x) = x^2$ was considered in [2001]. Some examples of B are given in [62]. It is remarked in [62] that Theorem 8.1.76 can be generalized for $f(x) = A(x)h(B(x))$ and $\bar{f}(x) = C(x)k(h(x))$ where $A, C \in \mathbb{F}_{q^n}[x]$ are polynomials such that $B(A(x)) = C(B(x))$ with $C(0) = 0$ and A is injective on $B^{-1}(s)$ for each $s \in B(\mathbb{F}_{q^n})$, under the similar assumptions $h(B(\mathbb{F}_{q^n})) \subseteq S \setminus \{0\}$ and $B(a\alpha) = k(a)B(\alpha)$ for all $a \in S$ and all $\alpha \in \mathbb{F}_{q^n}$.

8.1.78 Definition [62] Let $S \subseteq \mathbb{F}_q$ and let $\gamma, b \in \mathbb{F}_q$. Then γ is a *b-linear translator* with respect to S for the mapping $F : \mathbb{F}_q \longrightarrow \mathbb{F}_q$, if

$$F(x + u\gamma) = F(x) + ub$$

for all $x \in \mathbb{F}_{q^n}$ and for all $u \in S$.

8.1.79 Remark The above definition is a generalization of the concept of b-linear translator studied in [592, 594, 1814], which deals with the case $q = p^{mn}$, and $S = \mathbb{F}_{p^m}$. The relaxation on the condition for S to be any subset of $\mathbb{F}_q$ provides a much richer class of functions (see examples in [62]). Using the original definition of linear translators, several classes of PPs of the form $G(x) + \gamma Tr(H(x))$ are constructed in [592, 594, 1814]. In the case that G is also a PP, it is equivalent to constructing polynomials of the form $x + \gamma Tr(H'(x))$.

8.1.80 Theorem [62] Let $S \subseteq \mathbb{F}_q$ and $F : \mathbb{F}_q \longrightarrow S$ be a surjective map. Let $\gamma \in \mathbb{F}_q$ be a b-linear translator with respect to S for the map F. Then for any $G \in \mathbb{F}_q[x]$ which maps S into S, we have that $x + \gamma G(F(x))$ is a PP of $\mathbb{F}_q$ if and only if $x + bG(x)$ permutes S.

8.1.81 Definition A *complete mapping* f of $\mathbb{F}_q$ is a permutation polynomial $f(x)$ of $\mathbb{F}_q$ such that $f(x) + x$ is also a permutation polynomial of $\mathbb{F}_q$.

8.1.82 Corollary [62, 592] Under the conditions of Theorem 8.1.80, we have

1. If $G(x) = x$ then $x + \gamma F(x)$ is a PP of $\mathbb{F}_q$ if and only if $b \neq -1$.
2. If q is odd and $2S = S$, then $x + \gamma F(x)$ is a complete mapping of $\mathbb{F}_q$ if and only if $b \notin \{-1, -2\}$.

8.1.83 Theorem [1814] Let $L : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$ be an $\mathbb{F}_q$-linear mapping of $\mathbb{F}_{q^n}$ with kernel $\alpha\mathbb{F}_q$, $\alpha \neq 0$. Suppose α is a b-linear translator with respect to $\mathbb{F}_q$ for the mapping $f : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_q$ and $h : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Then the mapping $G(x) = L(x) + \gamma h(f(x))$ permutes $\mathbb{F}_{q^n}$ if and only if $b \neq 0$ and γ does not belong to the image set of L.

8.1.84 Corollary [1814] Let t be a positive integer with $(t, q-1) = 1$, $H \in \mathbb{F}_{q^n}[x]$ and $\gamma, \beta \in \mathbb{F}_{q^n}$. Then the mapping $G(x) = x^q - x + \gamma\left(Tr(H(x^q - x)) + \beta x\right)^t$ is a PP of $\mathbb{F}_{q^n}$ if and only if $Tr(\gamma) \neq 0$ and $Tr(\beta) \neq 0$.

8.1.85 Theorem [3045] Let A be a finite field, S and $\bar{S}$ be finite sets with $\#S = \#\bar{S}$ such that the maps $\psi : A \to S$ and $\bar{\psi} : A \to \bar{S}$ are surjective and ψ is additive, i.e., $\bar{\psi}(x+y) = \bar{\psi}(x)+\bar{\psi}(y)$, for all $x, y \in A$. Let $g : S \to A$ and $f : A \to A$ be maps such that $\bar{\psi}(f + g \circ \psi) = f \circ \psi$ and $\bar{\psi}(g(\psi(x))) = 0$ for every $x \in A$. Then the map $f(x) + g(\psi(x))$ permutes A if and only if f permutes A.

8.1.86 Corollary [3045] Let n and k be positive integers such that $(n, k) = d > 1$, and let s be any positive integer with $s(q^k-1) \equiv 0 \pmod{q^n-1}$. Let $L_1(x) = a_0x+a_1x^{q^d}+\cdots+a_{n/d-1}x^{q^{n-d}}$ be a polynomial with $L_1(1) = 0$ and let $L_2 \in \mathbb{F}_q[x]$ be a linearized polynomial and $g \in \mathbb{F}_{q^n}[x]$. Then $f(x) = (g(L_1(x)))^s + L_2(x)$ permutes $\mathbb{F}_{q^n}$ if and only if L_2 permutes $\mathbb{F}_{q^n}$.

8.1.87 Corollary [3045] Let n and k be positive integers such that $(n, k) = d > 1$, let s be any positive integer with $s(q^k - 1) \equiv 0 \pmod{q^n - 1}$. Then $h(x) = (x^{q^k} - x + \delta)^s + x$ permutes $\mathbb{F}_{q^n}$ for any $\delta \in \mathbb{F}_{q^n}$.

8.1.88 Remark More classes of PPs of the form $(x^{q^k} - x + \delta)^s + L(x)$ and their generalization can be found in [1060, 3056]. See [1479, 3042, 3043, 3055] for more classes of PPs of the form $(x^{p^k}+x+\delta)^s+L(x)$. One can also find several classes of PPs of the form $x^d+L(x)$ over $\mathbb{F}_{2^n}$ in [1927, 2361, 2360]. It is proven in [1927] that, under the assumption $\gcd(d, 2^n - 1) > 1$, if $x^d + L(x)$ is a PP of $\mathbb{F}_{2^n}$ then L must be a PP of $\mathbb{F}_{2^n}$. Hence some of these classes of PPs of the form $x^d + L(x)$ are compositional inverses of PPs of the form $L_1(x)^d + x$.

8.1.89 Remark See [870, 3044] for some explicit classes of PPs over $\mathbb{F}_{3^m}$.

8.1.8 Dickson and Reversed Dickson PPs

8.1.90 Remark The permutational behavior of Dickson polynomials of the first kind is simple and classical; see Remark 8.1.5. For more information on Dickson polynomials, see Section 9.6.

8.1.91 Definition For any positive integer n, let $E_n(x, a)$ be the *Dickson polynomial of the second kind* (DPSK) defined by

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

8.1.92 Remark Matthews observed in his Ph.D. thesis [2032] that if q is a power of an odd prime p and n satisfies the system of congruences

$$\begin{aligned} n+1 &\equiv \pm 2 \pmod{p}, \\ n+1 &\equiv \pm 2 \pmod{\tfrac{1}{2}(q-1)}, \\ n+1 &\equiv \pm 2 \pmod{\tfrac{1}{2}(q+1)}, \end{aligned} \tag{8.1.4}$$

then E_n is a PP of $\mathbb{F}_q$. However, the above is not a necessary condition in general. When $p = 3$ or 5 and q is composite there are examples of DPSK E_n known which are PP for which (8.1.4) does not hold, see [1589, 2173]. Moreover, there are several papers concentrating on the permutational behavior of DPSK over finite fields with small characteristics including characteristic two and general a which is not necessarily ± 1 [731, 1480, 1481, 1482]. On the other hand, when $q = p$ or p^2 and $a = 1$, Cipu and Cohen proved that the condition (8.1.4) is also necessary [650, 651, 677, 678].

8.1.93 Definition [1544] For any positive integer n, the *reversed Dickson polynomial*, $D_n(a,x)$, is defined by

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

8.1.94 Remark It is easy to check that $D_n(0,x)=0$ if n is odd and $D_n(0,x)=2(-x)^k$ if $n=2k$. Hence $D_n(0,x)$ is a PP of $\mathbb{F}_q$ if and only if q is odd, $n=2k$, and $(k,q-1)=1$. For $a \neq 0$, we can also check that $D_n(a,x) = a^n D_n(1, x/a^2)$. Hence $D_n(a,x)$ is a PP of $\mathbb{F}_q$ where $a \neq 0$ if and only if $D_n(1,x)$ is a PP of $\mathbb{F}_q$. If $D_n(1,x)$ is a PP of $\mathbb{F}_q$, then (q,n) is a *desirable pair*.

8.1.95 Definition A mapping f from $\mathbb{F}_q$ to $\mathbb{F}_q$ is *almost perfect nonlinear* (APN) if the difference equation $f(x+a)-f(x)=b$ has at most two solutions for any fixed $a \neq 0, b \in \mathbb{F}_q$.

8.1.96 Remark We refer to Section 9.2 for more information on APN functions and their applications.

8.1.97 Theorem [1544] Let $q=p^e$ with p a prime and $e>0$. If $p=2$ or $p>3$ and n is odd, then x^n is an APN on $\mathbb{F}_{q^2}$ implies that $D_n(1,x)$ is a PP of $\mathbb{F}_q$, which also implies that x^n is an APN over $\mathbb{F}_q$.

8.1.98 Theorem [1542] The pair (p^e, n) is a desirable pair in each of the following cases:

p	e	n	
2		2^k+1, $(k,2e)=1$	[1293, 1544]
2		$2^{2k}-2^k+1$, $(k,2e)=1$	[1544, 1689]
2	even	2^e+2^k+1, $k>0$, $(k-1,e)=1$	[1544]
2	$5k$	$2^{8k}+x^{6k}+2^{4k}+2^{2k}-1$	[904, 1544]
3		$(3^k+1)/2$, $(k,2e)=1$	[1544]
3	even	3^e+5	[1539]
5		$(5^k+1)/2$, $(k,2e)=1$	[1477]
≥ 3		p^k+1, $k \geq 0$, $p^k \equiv 1 \pmod 4$, $v_2(e) \leq v_2(k)$	[1544]
≥ 3		p^e+2, $k \geq 0$, $p^e \equiv 1 \pmod 3$	[1477, 1544]
≥ 5		3	

8.1.99 Remark Two pairs (q,n_1) and (q,n_2), where n_1 and n_2 are positive integers, are equivalent if n_1 and n_2 are in the same p-cyclotomic coset modulo q^2-1, i.e., $D_{n_1}(1,x) \equiv D_{n_2}(1,x) \pmod{x^q - x}$. No desirable pairs outside the ten families (up to equivalence) given in Theorem 8.1.98 are known. There are several papers on necessary conditions for a reverse Dickson polynomial to be a PP [1541, 1542]. In particular, it is proved in [1542] that (p^e,n) is a desirable pair if and only if $f_n(x) = \sum_{j \geq 0}\binom{n}{2j}x^j$ is a PP of $\mathbb{F}_{p^e}$. However, it is not known whether the above classes are the only non-equivalent desirable pairs. Several new classes of reversed Dickson polynomials can be found in [1539, 1541].

8.1.100 Remark Dickson polynomials are used to prove the following class of PPs.

8.1.101 Theorem [1524] Let $m \geq 1$ and $1 \leq k, r \leq m-1$ be positive integers satisfying that $kr \equiv 1 \pmod m$. Let $q = 2^m$, $\sigma = 2^k$, and $Tr(x) := x + x^2 + \cdots + x^{2^{m-1}}$. For α, γ in $\{0,1\}$, we define

$$H_{\alpha,\gamma}(x) := \gamma Tr(x) + \frac{(\alpha Tr(x) + \sum_{i=0}^{r-1} x^{\sigma^i})^{\sigma+1}}{x^2}.$$

Then $H_{\alpha,\gamma}(x)$ is a PP of $\mathbb{F}_{2^m}$ if and only if $r + (\alpha+\gamma)m \equiv 1 \pmod 2$.

8.1.9 Miscellaneous PPs

8.1.102 Remark Cyclic and Dickson PPs play a vital role in the Schur Conjecture from 1922 which postulated that if f is a polynomial with integer coefficients which is a PP of $\mathbb{F}_p$ (when considered modulo p) for infinitely many primes p, then f must be a composition of binomials $ax^n + b$ and Dickson polynomials. This has been shown to be true; see [1108], the notes to Chapter 7 of [1937] and [2190]. A proof without the use of complex analysis can be found in [2826]. More generally, a matrix analogue of the Schur conjecture was studied in [2176]. Let $\mathbb{F}_q^{m\times m}$ denote the ring of $m \times m$ matrices over the finite field $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is a *permutation polynomial* (PP) on $\mathbb{F}_q^{m\times m}$ if it gives rise to a permutation of $\mathbb{F}_q^{m\times m}$. Using a characterization of PPs of the matrix ring over finite fields $\mathbb{F}_q$ in [395], it is shown by Mullen in [2176] that any polynomial f with integral coefficients which permutes the matrices of fixed size over a field of p elements for infinitely many p is a composition of linear polynomials and Dickson polynomials $D_n(x, a)$ with $n \neq 3$ an odd prime and $a \neq 0$ an integer. Several related questions are also addressed in [2176]; see Section 9.7 for more information on Schur's conjecture.

8.1.103 Remark Let f be an integral polynomial of degree $n \geq 2$. Cohen [674] proved one of the Chowla and Zassenhaus conjectures [630] (concerning irreducible polynomials), which postulated that if f is a PP over $\mathbb{F}_p$ of degree n modulo p for any $p > (n^2 - 3n + 4)^2$, then $f(x) + cx$ is not a PP of $\mathbb{F}_p$ unless $c = 0$. This shows that if both f and g are integral PPs of degree $n \geq 2$ over a large prime field, then their difference $h = f - q$ can not be a linear polynomial cx where $c \neq 0$. Suppose that $t \geq 1$ denotes the degree of h. More generally, it is proved in [697] that $t \geq 3n/5$. Moreover, if $n \geq 5$ and $t \leq n - 3$ then $(t, n) > 1$. Roughly speaking, two PPs over a large prime field $\mathbb{F}_p$ can not differ by a polynomial with degree less than $3n/5$.

8.1.104 Remark Evans [997] considers *orthomorphisms*, mappings θ with $\theta(0) = 0$ so that θ and $\theta(x) - x$ are both PPs of $\mathbb{F}_q$. He studies connections between orthomorphisms, latin squares, and affine planes. A map θ is an orthomorphism if and only if $\theta(x) - x$ is a complete mapping. Complete mappings of small degrees and existence of complete mappings (in particular, binomials) are studied in [2266]. Enumeration results for certain types of cyclotomic orthomorphisms are provided in [2276]. It is proved in [2266] for odd q and in [2903] for even q that the degree of a complete mapping is at most $q - 3$. It is known that families of permutation polynomials of the form $f(x) + cx$ can be used in the construction of maximal sets of mutually orthogonal Latin squares [996, 2917]. Let $C(f)$ be the number of c in $\mathbb{F}_q$ such that $f(x) + cx$ is a permutation polynomial over $\mathbb{F}_q$. Cohen's theorem [674] on the Chowla-Zassenhaus conjecture shows that $C(f) \leq 1$ if the degree n of f is not divisible by p and q is sufficiently large compared to n. Chou showed that $C(f) \leq q - 1 - n$ in his thesis [622]. Then Evans, Greene and Niederreiter proved $C(f) \leq q - \frac{q-1}{n-1}$ in [1015], which also proves a conjecture of Stothers [2728] when q is prime. In the case that q is an odd prime, it gives the best possible result $C(f) \leq (q - 3)/2$ for polynomials of the form $x^{(q+1)/2} + cx$. A general bound for $C(f)$ which implies Chou's bound was obtained by Wan, Mullen and Shiue in [2917], as well as a significant bound $C(f) \leq r$ where r is the least nonnegative residue of $q - 1$ modulo n under certain mild conditions. It is conjectured in [1015] that $f(x) - f(0)$ is a linearized p-polynomial over $\mathbb{F}_q$ if $C(f) \geq \lfloor q/2 \rfloor$; this was proved to be true for $q = p$ or any monomial $f(x) = x^e$ in [1015]. Wan observed that this conjecture holds also for $q = p^2$ from the results in [622, 1015]. Several other related results on the function $C(f)$ can be found in [996, 2825, 2911].

8.1.105 Remark Results on the cycle structure of monomials and of Dickson polynomials can be found in [44] and [1932], respectively. Cycle decomposition, in particular, decomposition of them into cycles of the same length (which are motivated by Turbo codes [2741, 2768]), are studied in [44, 2150, 2294, 2493, 2494, 2517]. Moreover, we refer readers to [68, 574, 623] for cycle structure of permutation polynomials with small Carlitz rank [574] or with full cycles.

8.1.106 Remark Finding the compositional inverse of a PP is a hard problem except for the trivial well known classes such as the inverses of linear polynomial, monomials, and Dickson polynomials. There are several papers on the explicit format of the inverses of some special classes of permutation polynomials, for example, [725, 1814, 2203, 2204, 2941]. Because the problem is equivalent to finding the inverses of PPs of the form $x^r f(x^s)$, the most general result can be found in [2940].

8.1.107 Remark PPs are related to special functions. For example, Dobbertin constructed several classes of PPs [901, 902] over finite fields of even characteristic and used them to prove several conjectures on APN monomials. The existence of APN permutations on $\mathbb{F}_{2^{2n}}$ is a long-term open problem in the study of vectorial Boolean functions. Hou [1538] proved that there are no APN permutations over $\mathbb{F}_{2^4}$ and there are no APN permutations on $\mathbb{F}_{2^{2n}}$ with coefficients in $\mathbb{F}_{2^n}$. Only recently the authors in [423] found the first APN permutation over $\mathbb{F}_{2^6}$. However, the existence of APN permutations on $\mathbb{F}_{2^{2n}}$ for $n \geq 4$ remains open. Over finite fields of odd characteristics, a function f is a *planar function* if $f(x+a) - f(x)$ is a PP for each nonzero a; see Sections 9.2 and 9.5. In [872], Ding and Yuan constructed a new family of planar functions over $\mathbb{F}_{3^m}$, where m is odd, and then obtained the first examples of skew Hadamard difference sets, which are inequivalent to classical Paley difference sets. Permutation polynomials of $\mathbb{F}_{3^{2h+1}}$ obtained from the Ree-Tits slice symplectic spreads in $\mathrm{PG}(3, 3^{2h+1})$ were studied in [191]. Later on, they were used in [869] to construct a family of skew Hadamard difference sets in the additive group of this field. For more information on these special functions and their applications, we refer the readers to Sections 9.2, 9.5 and 14.6.

8.1.108 Remark Golomb and Moreno [1303] show that PPs are useful in the construction of circular Costas arrays, which are useful in sonar and radar communications. They gave an equivalent conjecture for circular Costas arrays in terms of permutation polynomials and provided some partial results. The connection between Costas arrays and APN permutations of integer rings $\mathbb{Z}_n$ was studied in [915]. Composed with discrete logarithms, permutation polynomials of finite fields are used to produce permutations of integer rings $\mathbb{Z}_n$ with optimum ambiguity and deficiency [2351, 2353], which generate APN permutations in many cases. Earlier results on PPs of $\mathbb{Z}_n$ can be found in Section 5.6 of [868] and [2169, 2458, 3060].

See Also

§8.2	For discussion of PPs in several variables.
§8.3	For value sets of polynomials.
§8.4	For exceptional polynomials over finite fields.
§9.2	For discussion of PN and APN functions.
§9.5	For studies of planar functions.
§9.6	For Dickson polynomials over finite fields.
§9.7	For connections to Schur's Conjecture.
[900]	For connections with monomial graphs.
[2601]	For connections with check digit systems.

References Cited: [44, 60, 61, 62, 63, 64, 65, 68, 191, 324, 395, 423, 503, 550, 568, 574, 592, 594, 622, 623, 630, 650, 651, 665, 674, 675, 677, 678, 679, 686, 697, 725, 728, 731, 769, 838, 868, 869, 870, 872, 900, 901, 902, 904, 915, 996, 997, 1015, 1060, 1108, 1119, 1220, 1293, 1303, 1477, 1479, 1480, 1481, 1482, 1524, 1538, 1539, 1541, 1542, 1544, 1589, 1689, 1713, 1784, 1785, 1810, 1814, 1829, 1830, 1914, 1927, 1931, 1932, 1933, 1934, 1937, 1981, 1982, 1993, 1994, 1995, 2001, 2014, 2017, 2018, 2031, 2032, 2125, 2150, 2169, 2173, 2174, 2176, 2190, 2203, 2204, 2266, 2276, 2294, 2351, 2353, 2357, 2360, 2361, 2458, 2493, 2494, 2517, 2601, 2603, 2637, 2679, 2680, 2728, 2741, 2768, 2824, 2825, 2826, 2903, 2904, 2907, 2908, 2910, 2911, 2912, 2915, 2917, 2918, 2926, 2939, 2940, 2941, 2942, 2966, 3042, 3043, 3044, 3045, 3046, 3055, 3056, 3060, 3063, 3073, 3074, 3075]

8.2 Several variables

Rudolf Lidl, *University of Tasmania*
Gary L. Mullen, *The Pennsylvania State University*

8.2.1 Definition A polynomial $f \in \mathbb{F}_q[x_1, \dots, x_n]$ is a *permutation polynomial in* n *variables over* $\mathbb{F}_q$ if the equation $f(x_1, \dots, x_n) = \alpha$ has exactly q^{n-1} solutions in $\mathbb{F}_q^n$ for each $\alpha \in \mathbb{F}_q$.

8.2.2 Remark A permutation polynomial $f(x_1, \dots, x_n)$ induces a mapping from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ but does not induce a $1-1$ mapping unless $n = 1$.

8.2.3 Remark [2170] A combinatorial computation shows that there are $(q^n)!/((q^{n-1})!)^q$ permutation polynomials in n variables over $\mathbb{F}_q$.

8.2.4 Definition A set of polynomials $f_i(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n], 1 \le i \le r$, forms an *orthogonal system in* n *variables over* $\mathbb{F}_q$ if the system of equations $f_i(x_1, \dots, x_n) = \alpha_i, 1 \le i \le r$, has exactly q^{n-r} solutions in $\mathbb{F}_q^n$ for each $(\alpha_1, \dots, \alpha_r) \in \mathbb{F}_q^r$.

8.2.5 Theorem [2226] For every orthogonal system $f_1, \dots, f_m \in \mathbb{F}_q[x_1, \dots, x_n], 1 \le m < n$, over $\mathbb{F}_q$ and every $r, 1 \le r \le n - m$, there exist $f_{m+1}, \dots, f_{m+r} \in \mathbb{F}_q[x_1, \dots, x_n]$ so that $f_1, \dots, f_{m+r}$ forms an orthogonal system over $\mathbb{F}_q$.

8.2.6 Theorem [541] The system $f_1, \dots, f_m, 1 \le m \le n$, is orthogonal over $\mathbb{F}_q$ if and only if

$$\sum_{(c_1,\dots,c_n)\in\mathbb{F}_q^n} \chi_{b_1}(f_1(c_1, \dots, c_n)) \cdots \chi_{b_m}(f_m(c_1, \dots, c_n)) = 0$$

for all additive characters $\chi_{b_1}, \dots, \chi_{b_m}$ of $\mathbb{F}_q$ with $(b_1, \dots, b_m) \ne (0, \dots, 0)$.

8.2.7 Corollary [541] A polynomial $f \in \mathbb{F}_q[x_1, \dots, x_n]$ is a permutation polynomial over $\mathbb{F}_q$ if and only if

$$\sum_{(c_1,\dots,c_n)\in\mathbb{F}_q^n} \chi(f(c_1, \dots, c_n)) = 0$$

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

8.2.8 Theorem [2226] A set of polynomials $f_1, \dots, f_r$ in n variables over $\mathbb{F}_q$ forms an orthogonal system over $\mathbb{F}_q$ if and only if the polynomial $b_1 f_1 + \cdots + b_r f_r$ is a permutation polynomial for each $(b_1, \dots, b_r) \ne (0, \dots, 0) \in \mathbb{F}_q^r$.