Polynomials over finite fields: an index approach

Qiang Wang

Abstract. The degree of a polynomial is an important parameter in the study of numerous problems on polynomials over finite fields. Recently, a new notion of the index of a polynomial over a finite field has been introduced to study the distribution of permutation polynomials over finite fields. This parameter also turns out to be very useful in studying bounds for the size of value sets, character sum bounds, among others. In this paper we survey this new index approach and report some recent results on polynomials over finite fields.

Keywords. polynomials, value sets, permutation polynomials, character sums, finite fields.

AMS classification. 11T06.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of q elements with characteristic p. Let γ be a fixed primitive element of $\mathbb{F}_q$ throughout the paper. The degree of a polynomial is an important parameter in the study of numerous problems on polynomials over finite fields, especially in the study of distribution of polynomials over finite fields.

It is well known that every polynomial g over $\mathbb{F}_q$ such that $g(0) = b$ has the form $ax^r f(x^s) + b$ for some positive integers r, s such that $s \mid (q-1)$. There are different ways to choose r, s in the form $ax^r f(x^s) + b$. However, in [2], based on [75], the concept of the index of a polynomial was first introduced. Any non-constant polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $\leq q-1$ can be written *uniquely* as $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$ such that the degree of f is less than the index ℓ which is defined below. Namely, write

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

where $a,\ a_{d-i_j} \neq 0$, $i_0 = 0 < i_1 < \cdots < i_k < d$, $j = 1, \ldots, k$. The case that $k = 0$ is trivial and we have $\ell = 1$. Thus we shall assume that $k \geq 1$. Write $d - i_k = r$, the vanishing order of x at 0 (i.e., the lowest degree of x in $g(x) - b$ is r). Then $g(x) = a\left(x^r f(x^{(q-1)/\ell})\right) + b$, where $f(x) = x^{e_0} + a_{d-i_1} x^{e_1} + \cdots + a_{d-i_{k-1}} x^{e_{k-1}} + a_r$, $s = gcd(d-r, d-r-i_1, \ldots, d-r-i_{k-1}, q-1)$, $d - r = e_0 s$, $d - r - i_j = e_j s$, $1 \leq j \leq k-1$, and $\ell := \frac{q-1}{s}$. Hence in this case $\gcd(e_0, e_1, \ldots, e_{k-1}, \ell) = 1$. The integer $\ell = \frac{q-1}{s}$ is called the *index* of $g(x)$. One can see that the greatest common

Research of Qiang Wang is partially supported by NSERC of Canada.

divisor condition in the defintion of s makes the index ℓ minimal among those possible choices.

We note that the index of a polynomial is closely related to the concept of the least index of a cyclotomic mapping polynomial [75]. Recall that γ is a fixed primitive element of $\mathbb{F}_q$. Let $\ell \mid (q-1)$ and the set of all nonzero ℓ-th powers be C_0. 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 $a_0, a_1, \ldots, a_{\ell-1} \in \mathbb{F}_q$ and a positive integer r, the *r-th order cyclotomic mapping $f^r_{a_0,a_1,\ldots,a_{\ell-1}}$ of index ℓ* from $\mathbb{F}_q$ to itself (see Niederreiter and Winterhof [75] for $r=1$ or Wang [87] for general r) is defined by

$$f^r_{a_0,a_1,\ldots,a_{\ell-1}}(x) = \begin{cases} 0, & \text{if } x = 0, \\ a_i x^r, & \text{if } x \in C_i,\ 0 \le i \le \ell-1. \end{cases} \tag{1.1}$$

It is shown that r-th order cyclotomic mappings of index ℓ produce the polynomials of the form $x^r f(x^s)$ where $s = \frac{q-1}{\ell}$. Indeed, the polynomial representation of (1.1) is given by

$$g(x) = \frac{1}{\ell} \sum_{j=0}^{\ell-1} \left(\sum_{i=0}^{\ell-1} a_i \zeta^{-ji} \right) x^{js+r}, \tag{1.2}$$

where $\zeta = \gamma^s$ is a fixed primitive ℓ-th root of unity. On the other hand, each polynomial $f(x)$ such that $f(0) = 0$ with index ℓ can be written as $x^r f(x^{(q-1)/\ell})$, which is an r-th order cyclotomic mapping with the least index ℓ defined as in (1.1) such that $a_i = f(\zeta^i)$ for $i = 0, \ldots, \ell-1$. An application of cyclotomic mapping permutations in check-digit systems can be found in [78] or [94].

The notion of the index of a polynomial over a finite field was introduced initially to study the distribution of permutation polynomials over finite fields. This parameter also turns out to be very useful in studying value set size bounds, character sum bounds, among others. In this paper we survey this new index approach in the study of polynomials over finite fields, and report some recent results on several specific problems. In Section 2 we briefly review an index bound for character sums of polynomials over finite fields [85]. This bound is very good when the polynomial has small index and large degree, a case when the classical Weil bound becomes trivial. The *value set* of a polynomial g over $\mathbb{F}_q$ is the set V_g of images when we view g as a mapping from $\mathbb{F}_q$ to itself. Clearly g is a *permutation polynomial (PP)* of $\mathbb{F}_q$ if and only if the cardinality $|V_g|$ of the value set V_g is q. There are also several results on explicit upper bounds for $|V_g|$ if g is not a PP over $\mathbb{F}_q$; see for example [41, 80, 82]. In Section 2, we review an index bound due to Mullen, Wan, and Wang [74] for the value set size of polynomials, which is an analogue of the well-known degree bound due to Wan [82]. The value set size of a polynomial with index ℓ is determined by the size of the corresponding cyclotomic mapping with the least index ℓ. The statistics of the value set size for a random r-th order cyclotomic mapping polynomial with index ℓ is studied by Gao and Wang [37]. Moreover, the distribution of missing values is asymptotically normal. These results are described in Section 3. Then we focus on permutation polynomials in Sections 4 and 5. We first describe Akbary, Ghioca, and Wang's result [2] on the enumeration of permutation polynomials with prescribed indices in Section 4, and then we classify many recent constructions of permutation polynomials in terms of indices in Section 5; see related work in [1]-[6], [10]-[17], [33]-[34], [43]-[46], [51]-[68], [81], [86]-[91], [95]-[106] and reference therein. Finally in Section 6 we comment on other recent results such as a bound on the Carlitz rank in terms of the index by Işik and Winterhof [48] and propose several more problems.

2 Index bound for character sums

Let $g(x)$ be a polynomial of degree $d > 0$ and $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character. If $g(x)$ is not of the form $c + f^p - f$ for some $f(x) \in \mathbb{F}_q[x]$ and constant $c \in \mathbb{F}_q$, then the Weil bound, see Page 233 in [63], is

$$\left| \sum_{x \in \mathbb{F}_q} \psi(g(x)) \right| \leq (d-1)\sqrt{q}. \tag{2.1}$$

This is the case if the degree d is not divisible by p. The Weil bound has a lot of applications in many different areas. However, the bound is trivial if the degree d of $g(x)$ is bigger than $\sqrt{q}$. In [85], Wan and Wang used the index of a polynomial to obtain the following index bound for character sums.

Theorem 2.1 (Wan-Wang 2016 [85]). *Let $g(x) = x^r f(x^{(q-1)/\ell}) + b$ be any polynomial with index ℓ. Let ζ be a primitive ℓ-th root of unity and $n_0 = \#\{0 \leq i \leq \ell - 1 \mid f(\zeta^i) = 0\}$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(g(x)) - \frac{q}{\ell} n_0 \right| \leq (\ell - n_0) \gcd(r, \frac{q-1}{\ell}) \sqrt{q}. \tag{2.2}$$

This implies that for many polynomials of large degree with small indices (for which the Weil bound becomes trivial), we have nontrivial bounds for the character sums in terms of indices. As a result, for any polynomial with index ℓ and vanishing order r at 0 such that $\gcd(r, p) = 1$, if both ℓ and $\gcd(r, \frac{q-1}{\ell})$ are small, we obtain a nontrivial bound for its character sum.

If $f(x)$ has no roots in μ_ℓ, then $n_0 = 0$ in Theorem 2.1. We note that all ℓ-th roots of unity belong to $\mathbb{F}_q$ because $\ell \mid q - 1$. Therefore, if $f(x)$ is an irreducible polynomial over $\mathbb{F}_q$ of degree ≥ 2, then $f(x)$ does not vanish at any ℓ-th root of unity and thus $n_0 = 0$.

Corollary 2.2. *Let $g(x) = x^r f(x^{(q-1)/\ell}) + a \in \mathbb{F}_q[x]$ where $f(x)$ is any irreducible polynomial over $\mathbb{F}_q$ of degree ≥ 2. Then*

$$\left|\sum_{x\in\mathbb{F}_q} \psi(g(x))\right| \leq \ell \gcd(r, \frac{q-1}{\ell})\sqrt{q}.$$

There are more examples such that $f(x)$ has no roots in μ_ℓ. For example, $f(x) = \prod_{a\in T}(x-a)$ where T is a multisubset of $\mathbb{F}_q^* \setminus \mu_\ell$ or

$$f(x) = \prod_{a\in T}(x-a) \prod_{\substack{f_i\ irred\\ deg f_i \geq 2}} f_i(x)^{e_i}.$$

On the other hand, n_0 can be very large and this gives large character sum. It is known by definition that all the roots of the ℓ-th order cyclotomic polynomial $\Phi_\ell(x)$ over $\mathbb{F}_q$ are primitive ℓ-th roots of unity. Therefore we obtain the following new nontrivial character sum estimate for a class of polynomials with large degree formed by cyclotomic polynomials.

Corollary 2.3. *Let q be a prime power, ℓ be a prime such that $\ell \mid q-1$, and $\gcd(r, \frac{q-1}{\ell}) = 1$. Let $g(x) = x^r\Phi_\ell(x^{(q-1)/\ell}) \in \mathbb{F}_q[x]$ where $\Phi_\ell(x)$ is the ℓ-th cyclotomic polynomial over $\mathbb{F}_q$. Then $\left|\sum_{x\in\mathbb{F}_q}\psi(g(x)) - \frac{\ell-1}{\ell}q\right| \leq \sqrt{q}$.*

There are many applications of character sums of binomials in the study of correlation spectrum of sequences, nonlinearity of monomials, among others. In the following we give estimates for the character sums of these binomials.

Corollary 2.4 (Wan-Wang 2016 [85]). *Let $g(x) = x^d + ax^r \in \mathbb{F}_q[x]$ with $a \in \mathbb{F}_q^*$ and $q-1 \geq d > r \geq 1$. Let $\ell = \frac{q-1}{\gcd(d-r, q-1)}$, $t = \gcd(d, r, q-1)$. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character. If $x^{d-r} + a$ has a solution in the subset of all ℓ-th roots of unity of $\mathbb{F}_q$, then*

$$\left|\sum_{x\in\mathbb{F}_q}\psi(x^d + ax^r) - \frac{qu}{\ell}\right| \leq (\ell-u)t\sqrt{q}, \tag{2.3}$$

otherwise,

$$\left|\sum_{x\in\mathbb{F}_q}\psi(x^d + ax^r)\right| \leq \ell t\sqrt{q}. \tag{2.4}$$

We remark that $x^{d-r} + a$ has a solution in the subset of all ℓ-th roots of unity of $\mathbb{F}_q$ if and only if $\frac{q-1}{\ell} \mid k$ where $k = \log_\gamma(-a)$ is the discrete logarithm of $-a$. So there are only ℓ possible a's such that the main term in the estimate (2.3) is $\frac{q}{\ell}$. Otherwise, we have the main term 0 and the index bound $\ell t\sqrt{q}$ for binomials $x^d + ax^r$. Because $t = \gcd(d, r, q-1)$ can easily achieve 1, our bound for many character sums evaluated in binomials is essentially $\ell\sqrt{q}$. We note that if $\ell < \sqrt{q} - 1$, then $\ell < \frac{q-1}{\ell} \leq d - 1$ and thus our bound $\ell\sqrt{q}$ is better than the Weil bound $(d-1)\sqrt{q}$.

We can generalize the above results to polynomials of large indices that are defined by a small number of cyclotomic cosets. For more details we refer the readers to [88]. We expect that our technique also applies to other types of polynomials defined piece-wisely.

3 Value sets of polynomials

Let $|V_g|$ be the cardinality of the value set V_g of a polynomial $g \in \mathbb{F}_q[x]$. Asymptotic formulas such as $|V_g| = \lambda(g)q + O(q^{1/2})$, where $\lambda(g)$ is a constant depending only on certain Galois groups associated to g, can be found in Birch and Swinnerton-Dyer [18] and Cohen [22]. Later Williams [93] proved that almost all polynomials g of degree d satisfy $\lambda(g) = 1 - \frac{1}{2!} + \frac{1}{3!} + \cdots + (-1)^{d-1}\frac{1}{d!}$. Those polynomials are called general polynomials.

There are also several results on explicit upper bounds for $|V_g|$ if g is not a PP over $\mathbb{F}_q$; see for example [41, 80, 82]. Perhaps the most well-known result is due to Wan [82] who proved that if a polynomial g of degree d is not a PP then

$$|V_g| \leq q - \frac{q-1}{d}. \tag{3.1}$$

On the other hand, it is easy to see that $|V_g| \geq \lceil q/d \rceil$ for any polynomial g over $\mathbb{F}_q$ with degree d because $g(x) = 0$ has at most d solutions. The polynomials achieving this lower bound are called *minimal value set polynomials*. The classification of minimal value set polynomials over $\mathbb{F}_{p^k}$ with $k \leq 2$ can be found in [20, 69], and in [19] for all the minimal value set polynomials in $\mathbb{F}_q[x]$ whose value set is a subfield of $\mathbb{F}_q$. See [26, 84] for further results on lower bounds of $|V_g|$ and [40] for some classes of polynomials with small value sets. More recently, algorithms and complexity in computing $|V_g|$ have been studied in [21]. For a recent survey on value sets of polynomials over finite fields, we refer the readers to Section 8.3 in [71].

Clearly, the study of the value set of g over $\mathbb{F}_q$ is equivalent to studying the value set of $x^r f(x^{(q-1)/\ell})$ over $\mathbb{F}_q$ with index ℓ. Recently Mullen, Wan and Wang [74] used an index approach to study the upper bound of the value set for any polynomial which is not a PP. They proved that if g is not a PP then

$$|V_g| \leq q - \frac{q-1}{\ell}. \tag{3.2}$$

This result improves Wan's result when the index ℓ of a polynomial is strictly smaller than the degree d. We note that the index ℓ of a polynomial is always smaller than the degree d as long as $\ell \leq \sqrt{q} - 1$.

In [73], we obtained the following formula for the cardinality of the value set for an arbitrary polynomial according to its index and the vanishing order at zero.

Proposition 3.1 (Proposition 2.3 in [73]). *Let $g(x) = ax^r f(x^{(q-1)/\ell}) + b$ ($a \neq 0$) be any polynomial over $\mathbb{F}_q$ with index ℓ. Let $s = \frac{q-1}{\ell}$ and $\gcd(r,s) = t$. Let γ be a fixed primitive element of $\mathbb{F}_q$. Then*

$$|V_g| = c\frac{s}{t} + 1 \text{ or } |V_g| = (c-1)\frac{s}{t} + 1,$$

where $c = |\{(\gamma^{ir} f(\gamma^{si}))^{s/t} \mid i = 0, \ldots, \ell - 1\}|$.

The proof of Proposition 3.1 uses the properties of cyclotomic mapping polynomials. It is sufficient to assume that $a = 1$ and $b = 0$. That is, we can view $g(x)$ as an r-th order cyclotomic mapping polynomial with the least index ℓ. In this case, we have $g(x) = a_i x^r$ when $x \in C_i$, where $a_i = f(\gamma^{si})$ for $i = 0, \ldots, \ell - 1$. Recall that C_0 is the subgroup of $\mathbb{F}_q^*$ consisting of all the ℓ-th powers of $\mathbb{F}_q^*$ and we let T_0 be the subgroup of $\mathbb{F}_q^*$ consisting of all the $t\ell$-th powers. Hence the T_i's with $0 \leq i \leq t\ell - 1$ give all the cyclotomic cosets of index $t\ell$. We also note that x^r maps C_0 onto T_0 which contains $\frac{s}{t}$ distinct elements. So x^r maps each coset $C_i = \gamma^i C_0$ onto $\gamma^{ir} T_0$. Therefore g maps C_i onto $\gamma^{ir} f(\gamma^{si}) T_0$, which could be either the set $\{0\}$ (if $a_i = f(\gamma^{si}) = 0$) or one of the nonzero cyclotomic cosets of index $t\ell$. We observe that c is the number of distinct cyclotomic cosets of the form $\gamma^{ir} f(\gamma^{si}) T_0$, possibly along with the subset $\{0\}$ if one of a_i's is zero. Hence we have $|V_g| = c\frac{s}{t} + 1$ or $(c-1)\frac{s}{t} + 1$, the latter happens when some of a_i's in $g(x) = a_i x^r$ equal 0.

Therefore the value set problem for a random r-th order cyclotomic mapping polynomial (or random polynomial) g essentially requires us to study the number c in Proposition 3.1, the size of the union of some cyclotomic cosets and possibly the subset $\{0\}$ if a_i's take zero. More specifically, for $0 \leq i \leq \ell - 1$, each C_i is mapped to $A_{i+1} = g(C_i)$ which is one of $T_0, \ldots, T_{t\ell-1}$ or $\{0\}$. Then c is the number of distinct A_j's ($1 \leq j \leq \ell$) and the value set size is either $c\frac{s}{t} + 1$ or $(c-1)\frac{s}{t} + 1$.

Let $n = t\ell$ and let $D_0 = \{0\}$ and $D_j = T_{j-1}$ for $1 \leq j \leq t\ell$. For a random r-th order cyclotomic mapping polynomial with index ℓ where $(r,s) = t$, we let $Y_{t\ell}$ be the number of cosets $D_1, \ldots, D_{t\ell}$ which are not contained in $\cup_{j=1}^{\ell} A_j$. Then the random variable $X_{t\ell} = q - \frac{s}{t} Y_{t\ell}$ measures the size of the value set of a random r-th order cyclotomic mapping polynomial with index ℓ. We use $\mathbb{P}$, $\mathbb{E}$, $\mathbb{V}$ to denote the probability, expectation, and variance of a random variable, respectively.

Theorem 3.2 (Gao-Wang 2015 [37]). *Let $q - 1 = \ell s$ and r be a positive integer such that $(r,s) = t$. Let $f(x)$ be any random r-th order cyclotomic mapping polynomial $f^r_{a_0,\ldots,a_{\ell-1}}(x)$ with index ℓ over $\mathbb{F}_q$. Let $X_{t\ell} = q - \frac{s}{t} Y_{t\ell}$, where $Y_{t\ell}$ is the number of cosets $D_1, \ldots, D_{t\ell}$ which are not contained in $\cup_{j=1}^{\ell} A_j$ for a random r-th order* *cyclotomic mapping polynomial with index ℓ such that $(r,s)=t$. Then*

$$\begin{aligned}
\mathbb{E}(X_{t\ell}) &= q-(q-1)\left(1-\frac{s}{tq}\right)^{\ell},\\
\mathbb{V}(X_{t\ell}) &= (q-1)\left(q-1-\frac{s}{t}\right)+\frac{s(q-1)}{t}\left(1-\frac{s}{tq}\right)^{\ell}\\
&\quad -(q-1)^2\left(1-\frac{s}{tq}\right)^{2\ell},\\
\mathbb{P}(X_{t\ell}=1+ks/t) &= \binom{t\ell}{k}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\left(\frac{1}{q}+\frac{sj}{tq}\right)^{\ell}.
\end{aligned}$$

Theorem 3.3 (Gao-Wang 2015 [37]). *Define*

$$n=t\ell,\ \mu_n=e^{-1/t}n,\ \sigma_n^2=e^{-2/t}(e^{1/t}-1-1/t)n.$$

Suppose $t=o(n^{1/6})$ as $n\to\infty$. Then the distribution of $(Y_n-\mu_n)/\sigma_n$ tends to the standard normal distribution, as $n\to\infty$.

When $\ell=q-1$ (hence $s=t=1$), Theorem 3.2 becomes the known result for random mappings over $\mathbb{F}_q$; see for example, [8, 36]. More specifically, we note that the value set problem for any random polynomial g with degree at most $q-1$ is in fact the value set problem for a random r-th order cyclotomic mapping polynomial with index $\ell=q-1$. Without loss of generality, we can assume $g(0)=0$. Therefore, Theorem 3.2 implies that the size of the value set of any random polynomial with degree $q-1$ has expected value $q-(q-1)(1-\frac{1}{q})^{q-1}\sim q-\frac{q}{e}$. This verifies William's result [93] saying that almost all polynomials of degree $q-1$ are a general polynomials. Moreover, by applying Theorem 3.2 to the case $\ell=q-1$ (hence $s=t=1$), we obtain the exact probability distribution of the size of the value set for a random polynomial over the finite field $\mathbb{F}_q$.

Corollary 3.4 (Gao-Wang 2015 [37]). *Let $g(x)$ be a random polynomial of degree at most $q-1$ over $\mathbb{F}_q$ with $g(0)=0$. Then*

$$\mathbb{P}(|V_g|=k+1)=\binom{q-1}{k}\sum_{j=0}^{k}(-1)^{k-j}\binom{k}{j}\left(\frac{1+j}{q}\right)^{q-1}.$$

Consequently, for $k=o(q)$, we have

$$\mathbb{P}(|V_g|=k+1)\sim\frac{1}{k!}(q-1)^k\left(\frac{k+1}{q}\right)^{q-1}.$$

If $k>1$ is small compared to q, then the number of polynomials over $\mathbb{F}_q$, with degree at most $q-1$ and the value set size k, is exponential in q. Moreover we have

Corollary 3.5 (Gao-Wang [37]). *Let $g(x)$ be any random polynomial of degree at most $q-1$ over the finite field $\mathbb{F}_q$ with $g(0)=0$. Let $Y_q = q - |g(\mathbb{F}_q)|$ denote the number of missing nonzero values in the value set of g. Let $\mu_q = q/e$ and $\sigma_q^2 = (e^{-1} - 2e^{-2})q$. Then the distribution of $(Y_q - \mu_q)/\sigma_q$ tends to the standard normal distribution, as $q \to \infty$.*

4 Enumeration of permutation polynomials

We call $f(x) \in \mathbb{F}_q[x]$ a *permutation polynomial* (PP) of $\mathbb{F}_q$ if f induces a permutation of $\mathbb{F}_q$. The study of permutation polynomials over finite fields have attracted a lot of interest for many years due to their wide applications in coding theory, cryptography and combinatorial designs. For more background material on permutation polynomials we refer to Chap. 7 of [63]. For a detailed survey of open questions and recent results see [43], [61], [62], [70], [72] and references therein. The following problem is Problem 6 in [61].

Problem 1 (Lidl-Mullen 1988 [61]). Let $N_d(q)$ denote the number of PPs of $\mathbb{F}_q$ which have degree d. We have the trivial boundary conditions: $N_1(q) = q(q-1)$, $N_d(q) = 0$ if d is a divisor of $q-1$ larger than 1, and $\sum N_d(q) = q!$ where the sum is over all $1 \le d < q-1$ such that d is either 1 or it is not a divisor of $q-1$. Find $N_d(q)$.

An estimation of $N_{q-2}(q)$ was first given by Das [25] in 2002 when q is prime, and then in general by Konyagin and Pappalardi [49]. Later in 2006, Konyagin and Pappalardi [50] also estimated the number of PPs with prescribed zero coefficients. Therefore the number of PPs with degree $q-2$ can be obtained from the number of PPs whose coefficient of x^{q-2} is zero.

Theorem 4.1 (Das 2002 [25]). *$N_{p-2}(p) \sim (\varphi(p)/p)p!$ as $p \to \infty$, where φ is the Euler function. More precisely, $\left|N_{p-2}(p) - \frac{\varphi(p)}{p}p!\right| \le \sqrt{\frac{p^{p+1}(p-2)+p^2}{p-1}}$.*

Theorem 4.2 (Konyagin-Pappalardi 2002 [49]). *Let q be a prime power. Then*

$$|N_{q-2}(q) - (q-1)!| \le \sqrt{\frac{2e}{\pi}} q^{\frac{q}{2}}.$$

Theorem 4.3 (Konyagin-Pappalardi 2006 [50]). *Fix j integers $k_1, \ldots, k_j$ with the property that $0 < k_1 < \cdots < k_j < q-1$ and define $N(k_1, \ldots, k_j; q)$ as the number of PPs h of $\mathbb{F}_q$ of degree less than $(q-1)$ such that the coefficient of x^{k_i} in h equals 0, for $i = 1, \ldots, j$. Then $\left|N(k_1, \ldots, k_j; q) - \frac{q!}{q^j}\right| < \left(1 + \sqrt{\frac{1}{e}}\right)^q ((q-k_1-1)q)^{q/2}$. In particular, $N_{q-2}(q) = q! - N(q-2; q)$.*

Motivated by Konyagin-Pappalardi's results, the index concept was first introduced by Akbary, Ghioca, and Wang [2] to study the distribution of permutation polynomials over finite fields. Obviously, every monic polynomial of index ℓ with vanishing order at zero r and degree less than or equal to $q-1$ can be written uniquely as

$$x^r f(x^s) = x^r \left(x^{e_m s} + b_{n_1} x^{e_{m-1} s} + \cdots + b_{n_{m-1}} x^{e_1 s} + b_{n_m}\right),$$

where

$$0 < e_1 < \cdots < e_m \leq \ell - 1, (e_1, \ldots, e_m, \ell) = 1, \text{ and } r + e_m s \leq q - 1. \tag{4.1}$$

Let m, r be positive integers, and $\bar{e} = (e_1, \ldots, e_m)$ be an m-tuple of integers that satisfy condition (4.1). We define by $N^m_{r,\bar{e}}(\ell, q)$ the number of all monic permutation polynomials of $\mathbb{F}_q$ with prescribed index ℓ and prescribed exponents $(r + e_m s, \ldots, r + e_1 s, r)$. We note that these polynomials with prescribed shape all have the fixed degree $r + e_m s$, the vanishing order at zero r, and $m+1$ nonzero terms in total.

Using Weil's bound on character sums, we obtained the following.

Theorem 4.4 (Akbary-Ghioca-Wang 2009 [2]).

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

We note that the proportion of PPs in the set of all these polynomials with prescribed index ℓ and exponents asymptotically goes to $\frac{\ell!}{\ell^\ell}$ as q goes to infinity. This shows that the density of PPs, in the set of polynomial with prescribed index and exponents, is higher when the index ℓ is smaller, although the absolute number of these PPs is smaller. To be more specific, we have

Theorem 4.5 (Akbary-Ghioca-Wang 2009 [2]). *For any q, r, $\bar{e}$, m, ℓ that satisfy conditions (4.1), $(r, s) = 1$, and $q > \ell^{2\ell+2}$, there exists $(b_{n_1}, b_{n_2}, \ldots, b_{n_m}) \in (\mathbb{F}_q^*)^m$ such that the $(m+1)$-nomial of the form $x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$.*

Remark 4.6. We note that for $1 \leq t \leq q-2$ the number of PPs of degree at least $(q-t-1)$ is $q! - N(q-t-1, q-t, \ldots, q-2; q)$. In [50] Konyagin and Pappalardi proved that $N(q-t-1, q-t, \ldots, q-2; q) \sim \frac{q!}{q^t}$ holds for $q \to \infty$ and $t \leq 0.03983\, q$. This result will guarantee 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 $q-t-1$.

Theorem 4.7 (Akbary-Ghioca-Wang 2009 [2]). *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 of degree $q-t-1$ which is a PP of $\mathbb{F}_q$.*

For $\ell = m + 1$, we obtain the following.

Corollary 4.8 (Akbary-Ghioca-Wang 2009 [2]). *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 $q-2$.*

The enumeration of PPs with prescribed index ℓ can be done through the enumeration of cyclotomic mapping permutation polynomials with the least index ℓ. For each fixed vanishing order r at zero, we can count the number of r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of index ℓ and then use the Möbius inversion formula to derive the number of those with the least index ℓ.

Corollary 4.9 (Wang 2007 [87]). *Let p be prime, $q = p^m$, and $\ell \mid q-1$ for some positive integer ℓ. For each positive integer r such that $(r, s) = 1$, there are $P_\ell = \ell!(\frac{q-1}{\ell})^\ell$ distinct r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of index ℓ. Moreover, the number Q_ℓ of r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of least index ℓ is*

$$Q_\ell = \sum_{\substack{t \mid \ell \\ (r,(q-1)/t)=1}} \mu\left(\frac{\ell}{t}\right)\left(\frac{q-1}{t}\right)^t t!.$$

We end this section with the following problem analogous to Problem 1 proposed by Akbary, Ghioca and Wang.

Problem 2. Let $N(\ell, q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have index ℓ. We have the trivial boundary conditions: $N(1, q) = q(q-1)\varphi(q-1)$, $N(\ell, q) = 0$ if ℓ is not a divisor of $q-1$, and $\sum N(\ell, q) = q!$ where the sum is over positive integers ℓ such that ℓ is a divisor of $q-1$. Find $N(\ell, q)$.

5 Classification of permutation polynomials by indices

Instead of classifying permutation polynomials according to their degrees, we can classify permutation polynomials in terms of indices. In particular, when the indices of polynomials are small or moderate, one could possibly obtain a nicer characterization according to the following multiplicative version of the AGW criterion (see [3] for more detail) with the commutative diagram:

$$\begin{tikzcd}
\mathbb{F}_q^* \arrow[r, "P"] \arrow[d, "x^s"] & \mathbb{F}_q^* \arrow[d, "x^s"] \\
\mu_\ell = \{1, \zeta, \ldots, \zeta^{\ell-1}\} \arrow[r, "\bar{P}"] & \mu_\ell = \{1, \zeta, \ldots, \zeta^{\ell-1}\}
\end{tikzcd}$$

Corollary 5.1 (Wan-Lidl 1991 [83], Park-Lee 2001 [76], Akbary-Wang 2007 [6], Wang 2007 [87], Zieve 2009 [104]). *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.*

Many classes of PPs are constructed via an application of this criterion. The criterion appeared in different forms in many references such as Wan-Lidl 1991 [83], Park-Lee 2001 [76], Akbary-Wang 2007 [6], Wang 2007 [87], and Zieve 2009 [104]. In this section, we use the index viewpoint to explain and classify many constructions of permutation polynomials. Due to the large number of references on constructions of permutation polynomials, we can only refer to some constructions that are closely related to our index viewpoint due to page limitation. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $\zeta=\gamma^{(q-1)/\ell}$ be a primitive ℓ-th root of unity. We have the following result.

Corollary 5.2 (Wan-Lidl 1991 [83], Wang 2007 [87], Wang 2017 [89]). *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 $\{ind_\gamma(f(\zeta^i))+ir \pmod{\ell} \mid i=0,\ldots,\ell-1\}=\mathbb{Z}_\ell$, where $ind_\gamma(f(\zeta^i))$ denotes the discrete logarithm of $f(\zeta^i)$ relative to the base γ.*

The benefit of this result is that we can use modular algorithms to generate all r-th order cyclotomic PPs with prescribed index ℓ by employing Equation (1.1). Then we can use the correspondence (1.2) to construct all permutation polynomials with prescribed index ℓ and vanishing order at zero equals to r. See more details in [89].

5.1 Small indices

As shown in [89], all PPs of the form $g(x)=x^r f(x^{(q-1)/\ell})$ with small indices ℓ can be generated algorithmically by Corollary 5.2 together with Equation (1.2). Theoretically, we can describe the coefficients of these PPs when ℓ is small as well. For example, for odd q, the polynomial $g(x)=x^r f(x^{(q-1)/2})$ is a PP of $\mathbb{F}_q$ if and only if $(r,(q-1)/2)=1$ and $\eta(f(-1)f(1))=(-1)^{r+1}$, where η is a quadratic character. Let us fix r such that $(r,(q-1)/2)=1$. Because we only need to consider polynomials with degree less than $q-1$, we have $f(x)=ax+b$ and thus $\eta(b^2-a^2)=(-1)^{r+1}$. On the other hand, by Corollary 5.2, the parity of $ind_\gamma(b+a)$ and $ind_\gamma(b-a)+r$ must be different. Hence $b=(\gamma^{2i}+\gamma^{2j+1+r})/2$ and $a=(\gamma^{2i}-\gamma^{2j+1+r})/2$, or $b=(\gamma^{2i+1}+\gamma^{2j+r})/2$ and $a=(\gamma^{2i+1}-\gamma^{2j+r})/2$ for some integers $0\le i,j\le q-2$.

When $\ell\ge 3$, the following list of PPs with small indices with special formats for $f(x)$ has been characterized earlier.

- $f(x)=x^e+1$ for $\ell=3,5,7$ (L. Wang 2002 [86], Akbary-Wang 2005 [4]).
- $f(x)=x^e+1$ for $p\equiv -1 \pmod{\ell}$ or $p\equiv 1 \pmod{\ell}$ and $\ell\mid m$. (Akbary-Wang 2006 [5])

- $h_k(x) = x^k + x^{k-1} + \cdots + x + 1$ and $f(x) = h_k(x)$; $p \equiv -1 \pmod{2\ell}$ where ℓ is either odd or $2\ell_1$ with odd ℓ_1. (Akbary-Wang 2007 [6])
- $h_k(x) := x^k + x^{k-1} + \cdots + x + 1$ for $\ell = 3, 5$ or odd prime $< 2p + 1$. (Akbary-Alaric-Wang 2008 [1]).
- $f(x) = h_k(x^e)^t$ for $\ell = 3, 5, 7, 11$. (Zieve 2008 [103])

Because of the restriction on the forms of the polynomials, the description of these PPs can be nice and clean. For example,

Theorem 5.3 (Akbary-Alaric-Wang 2008 [1]). *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 $(k+1)s \equiv 1 \pmod{p}$.*

Without restriction on the format of polynomials, it should be feasible to solve the following problem.

Problem 3. Classify all PPs of $\mathbb{F}_q$ of small indices explicitly in terms of their coefficients.

Let $g(x) = x^r f(x^{(q-1)/\ell})$ with $f(x) = b_{\ell-1}x^{\ell-1} + b_{\ell-2}x^{\ell-2} + \cdots + b_1 x + b_0$. First we use Corollary 5.2 to obtain conditions for $f(\zeta^i)$ for all $i = 0, \ldots, \ell - 1$. Essentially $f(\zeta^i) = \gamma^{c_i + \ell t_i - ir}$ for some positive integer t_i, where $0 \le i \le \ell - 1$ and $(c_0, c_1, \ldots, c_{\ell-1})$ is any permutation of $\mathbb{Z}_\ell$. This can be written as a system of linear equations $AX = C$ such that

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & \zeta^1 & \cdots & \zeta^{\ell-2} & \zeta^{\ell-1} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 1 & \zeta^{\ell-1} & \cdots & \zeta^{(\ell-1)(\ell-2)} & \zeta^{(\ell-1)(\ell-1)} \end{pmatrix},$$

$$X = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{\ell-1} \end{pmatrix}, C = \begin{pmatrix} \gamma^{c_0 + \ell t_0} \\ \gamma^{c_1 + \ell t_1 - r} \\ \vdots \\ \gamma^{c_{\ell-1} + \ell t_{\ell-1} - (\ell-1)r} \end{pmatrix}.$$

Then we can use the inverse of A (Inverse Discrete Fourier Transform) to solve for X and find all possible coefficients of PPs with prescribed index ℓ. This method works for PPs of any index, although it is more efficient for PPs of small indices.

5.2 Arbitrary indices

We can also obtain the following characterization of PPs of the form $x^r f(x^{(q-1)/\ell})$ with arbitrary index ℓ. In this case, further restrictions on either the polynomial $f(x)$ or the size of the finite field are required. For example, related to the work on small indices, Marcos [67] studied some permutation polynomials such that $f(x) = h_k(x) + bx^d$ for $\ell \geq 3$ and $0 \leq d \leq \ell - 1$, where $h_k(x) = x^k + x^{k-1} + \cdots + x + 1$. On the other hand, we have the following result when the format of the polynomial $f(x)$ is not explicit.

Theorem 5.4 (Akbary-Wang 2007 [6]). *Let $q - 1 = \ell s$. Assume that $(f(\zeta^i))^s = \zeta^{ik}$ for any $i = 0, \ldots, \ell - 1$ and a fixed k. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r, s) = 1$ and $(r + k, \ell) = 1$.*

In this case, $x^r f(x)^s$ behaves like a monomial x^{r+k} over μ_ℓ. The following corollaries are all important consequences of Theorem 5.4.

Corollary 5.5 (Akbary-Wang 2007 [6]). *Let $q - 1 = \ell s$. Assume that $(f(\zeta^i))^s = 1$ for any $i = 0, \ldots, \ell - 1$. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r, q - 1) = 1$.*

Corollary 5.6 (Rogers 1890, Dickson 1897, Wan and Lidl 1991, see Corollary 1.4 in [83]). *Let $\ell \mid q - 1$ and $f(x)$ be any polynomial over $\mathbb{F}_q$. Then $P(x) = x^r f(x^s)^\ell$ is a PP of $\mathbb{F}_q$ if and only if $(r, q - 1) = 1$ and $f(\zeta^i) \neq 0$ for all $0 \leq i \leq \ell - 1$.*

Corollary 5.7 (Laigle-Chapuy 2007 [64]). *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, take $q = p^m = p^{\ell v n}$ and $\ell s = q - 1$. Assume $f(x)$ 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 $f(\zeta^i) \neq 0$ for all $0 \leq i \leq \ell - 1$.*

In these corollaries $x^r f(x)^s$ behaves like the monomial x^r over μ_ℓ. The following is an extension of the previous results. In this case, $x^r f(x^e + a)^s$ behaves like the monomial x^{2r+tes} over μ_ℓ.

Theorem 5.8 (Zieve 2009 [104]). *Let $t > 0$ be an integer, and let $f(x) = x^t \hat{f}(x^\ell)$, where $\hat{f} \in \mathbb{F}_q[x]$. Let $a \in \mathbb{F}_q^*$ and $(e, \ell) = 1$. Assume that every $\eta \in \mu_{\ell \cdot (2,\ell)}$ satisfies $\eta + \frac{a}{\eta} \in \mu_{ts}$ and $x^t \hat{f}((\eta^{2e} + a)^\ell) \in \mu_s$. Then $P(x) = x^r f(x^{es} + a)$ is a PP of $\mathbb{F}_q$ iff $(2r + tes, \ell) = 1$ and $(r, s) = 1$.*

5.3 Intermediate indices

In recent years, there have been several studies on constructing permutation polynomials with indices ℓ close to the size of a subfield or the size of certain cosets (e.g., $q - 1$ or $q + 1$ over $\mathbb{F}_{q^2}$, $q - 1$ or $q^{n-1} + \cdots + q + 1$ over $\mathbb{F}_{q^n}$). We call them intermediate indices. Many of these permutation polynomials are often over finite fields with even extensions.

Index $\ell = q - 1$

Let us consider the finite field $\mathbb{F}_{q^n}$. When the index is $q-1$, then $s = \frac{q^n-1}{q-1}$. We can reduce a permutation of $\mathbb{F}_{q^n}$ to a permutation over a subfield $\mathbb{F}_q$ (because $x^r f(x)^s$ maps 0 to 0 and $\mu_\ell = \mathbb{F}_q^*$). Then we obtain a direct consequence of Corollary 5.1.

Theorem 5.9 (Zieve 2013 [105]). *Let q be a prime power, $\ell = q-1$ and $s = (q^n - 1)/(q-1) = q^{n-1} + \cdots + q + 1$. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_{q^n}$ if and only if $(r, s) = 1$ and $x^r f(x) f^{(q)}(x) \cdots f^{(q^{n-1})}(x)$ permutes $\mathbb{F}_q$, where $f^{(q^i)}(x)$ denotes the polynomial obtained from $f(x)$ by raising every coefficient to the q^i-th power.*

In particular, if $f(x) \in \mathbb{F}_q[x]$, i.e., all the coefficients of $f(x)$ are in $\mathbb{F}_q$, then we must have, over $\mathbb{F}_q$,

$$x^r f(x) f^{(q)}(x) \cdots f^{(q^{n-1})}(x) = x^r f(x)^n.$$

Namely, if $f(x) \in \mathbb{F}_q[x]$, then $P(x) = x^r f(x^{(q^n-1)/(q-1)})$ is a PP of $\mathbb{F}_{q^n}$ if and only if $(r, (q^n-1)/(q-1)) = 1$ and $x^r f(x)^n$ is a PP of $\mathbb{F}_q$.

When the coefficients of $f(x)$ are in $\mathbb{F}_{q^n} \setminus \mathbb{F}_q$, several recent papers study the cases when $f(x) = x^e + a$ and n is a small positive integer. This is related to the study of complete permutation polynomials. A complete permutation polynomial (CPP) is a polynomial $f(x)$ such that both $f(x)$ and $f(x) + x$ induce bijections of $\mathbb{F}_q$. The most studied class of CPPs are monomials $P(x) = a^{-1}x^d$. It is well known that $P(x) = a^{-1}x^d$ is a PP of $\mathbb{F}_{q^n}$ if and only if $\gcd(d, q^n - 1) = 1$. Hence the characterization of CPP monomials $P(x) = a^{-1}x^d$ is essentially reduced to the study of the permutation behavior of the binomial $x^d + ax$. If there exists a complete permutation monomial of degree d over $\mathbb{F}_q$, then d is called a CPP exponent over $\mathbb{F}_q$. Related work has been done recently in [12, 13, 15, 16, 66, 95].

Let $q = p^k$ and let $a^{-1}x^d$ be the CPP monomial over $\mathbb{F}_{p^{nk}}$ such that $d = \frac{p^{nk}-1}{p^k-1} + 1$. For any $a \in \mathbb{F}_{p^{nk}}$, let $a_i = a^{p^{ik}}$, where $0 \le i \le n-1$. Define

$$h_a(x) = x \prod_{i=0}^{n-1} (x + a_i).$$

Then Corollary 5.1 directly gives the following.

Corollary 5.10 (Wu-Li-Helleseth-Zhang 2015 [96]). *Let $d = \frac{p^{nk}-1}{p^k-1} + 1$. Then $x^d + ax \in \mathbb{F}_{p^{nk}}[x]$ is a PP of $\mathbb{F}_{p^{nk}}$ if and only if $h_a(x) \in \mathbb{F}_{p^k}[x]$ is a PP of $\mathbb{F}_{p^k}$.*

In this case $x(x+a)^{d-1}$ reduces to a polynomial $h_a(x)$ with a lower degree $n+1$ over μ_{p^k-1} or $\mathbb{F}_{p^k}$. When n is small, we essentially need to study permutation polynomials of low degree over a subfield $\mathbb{F}_{p^k}$.

Since the classification of low degree permutation polynomials over $\mathbb{F}_q$ is well known (see for example [63]), we can obtain the classification of CPP monomials $P(x) = a^{-1}x^{\frac{q^n-1}{q-1}}$ over $\mathbb{F}_{q^n}$ for small n's. Indeed, using cubic permutation polynomials, Zieve solved the case when $n = 2$.

Corollary 5.11 (Zieve 2013 [105]). *For $\alpha \in \mathbb{F}_{q^2}^*$ and $\beta \in \mathbb{F}_q$, the polynomial $P(x) = \alpha x^{q+2} + \beta x$ is a complete permutation polynomial over $\mathbb{F}_{q^2}$ if and only if*

- $q \equiv 5 \pmod 6$ *and α^{q-1} has order 6;*
- $q \equiv 2 \pmod 6$ *and α^{q-1} has order 3; or*
- $q \equiv 0 \pmod 3$ *and $\alpha^{q-1} = -1$.*

An extension of the above result for $f(x) = \alpha x^2 + \beta$ can be found in [105] using degree-4 permutation polynomials over $\mathbb{F}_q$. Similarly, the following result holds.

Corollary 5.12 (Zieve 2013 [105]). *For $\alpha \in \mathbb{F}_{q^3}^*$ and $\beta \in \mathbb{F}_q$, the polynomial $P(x) = \alpha x^{q^2+q+2} + \beta x$ is a complete permutation polynomial over $\mathbb{F}_{q^3}$ if and only if*

- $q \equiv 0 \pmod 2$ *and $\alpha^{q^2} + \alpha^{q^2-q+1} + \alpha = 0$;*
- $q = 7$ *and $2\alpha^{24} + 4\alpha^{12} + \alpha^6 + 1 = 0$ and $\beta \notin \{0, -1\}$;*
- $q = 3$ *and $\alpha^{12} + \alpha^8 + \alpha^2 + 1 = 0$ and $\beta = 1$;*
- $q = 2$ *and $\alpha \neq 1$.*

In [15, 16, 95, 96], PPs of the form $f_a(x) = x^d + ax$ over $\mathbb{F}_{q^n}$ were thoroughly investigated for $n = 2, 3, 4$. For any odd p, Wu et al [95] give a necessary and sufficient description for the case $n = 4$. For $n = 6$, sufficient conditions for $f_a(x)$ to be a PP of $\mathbb{F}_{q^6}$ were provided in [95, 96] for the special cases of characteristic $p \in \{2, 3, 5\}$, whereas in [12] all a's for which $ax^{\frac{q^6-1}{q-1}+1}$ is a CPP over $\mathbb{F}_{q^6}$ are explicitly listed. The case $n = p - 1$ was dealt with in [96, 66] as well. Using the classification of exceptional polynomials, Bartoli et al. [13] classified complete permutation monomials of degree $d = \frac{q^n-1}{q-1} + 1$ over the finite field with q^n elements in odd characteristic, where $n + 1$ is a prime and $(n + 1)^4 < q$. However, when $n + 1$ is large or not prime, the classification of CPP exponents is still open. For example, when $n + 1$ is a prime power such as 8 or 9, only a few new examples of CPPs are provided in [13]. Recently, we constructed several new classes of complete permutation monomials $a^{-1}x^d$ of $\mathbb{F}_q$ using the AGW criterion, when $h_a(x)$ is either a Dickson permutation polynomial or a degree p exceptional polynomial [33]. More interesting classes of PPs with intermediate indices are expected to be constructed and classified in this way. Hence we propose the following.

Problem 4. Classify complete permutation monomials $a^{-1}x^{\frac{q^n-1}{q-1}+1}$ of $\mathbb{F}_{q^n}$ for more general n.

For $q = 2^t$ and $n = 2^s t$, Bhattacharya and Sarkar [17] solved the problem for $a \in \mathbb{F}_{q^2}$. However, it is not known if $a \in \mathbb{F}_{2^n}$. They also extended their study to trinomials. Our next proposed problem is the following.

Problem 5. Classify sparse permutation polynomials of $\mathbb{F}_{q^n}$ with index $q-1$, i.e., sparse permutation polynomials of the form $P(x) = x^r f(x^{\frac{q^n-1}{q-1}})$ of $\mathbb{F}_{q^n}$.

Index $\ell = q + 1$

In this subsection we consider PPs over $\mathbb{F}_{q^2}$, $\ell = q+1$ and $s = q-1$. Then we must have $x^q = x^{-1}$ where $x \in \mu_\ell$. Because

$$x^r f(x)^{q-1} = x^r \frac{f(x)^q}{f(x)},$$

we can simplify $f(x)^q$ using $x^q = x^{-1}$ over μ_ℓ and study the permutation behavior of $x^r f(x)^s$ over μ_ℓ as a rational function. Sometimes this approach is called the fractional method [55]. Under certain assumptions, $x^r f(x)^s$ can behave very nicely over μ_{q+1}.

Theorem 5.13 (Zieve 2013 [105]). *Let q be a prime power, $\ell = q+1$ and $s = q-1$. Let β be an ℓ-th root of unity in $\mathbb{F}_q$. Let $f(x) \in \mathbb{F}_{q^2}[x]$ be a polynomial of degree d such that $f(0) \neq 0$ and $x^d f(1/x)^q = \beta f(x^q)$. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(r, s) = 1$, $(r-d, \ell) = 1$, and $f(x)$ has no roots in μ_ℓ.*

Corollary 5.14 (Zieve 2013 [105]). *Let $\ell = q+1$ and $\beta^\ell = 1$. Then $f(x) = x^r(x^{d(q-1)} + \beta^{-1})$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(r, q-1) = 1$, $(r-d, \ell) = 1$, and $(-\beta)^{(q+1)/gcd(q+1,d)} \neq 1$.*

In the previous result, $x^r f(x)^s$ behaves like βx^{r-d} over μ_{q+1}. For these permutation binomials of index $q+1$, it was conjectured that there are only finitely many (q, β) for which $f(x) = x^r(x^{d(q-1)} + \beta^{-1})$ is a PP of $\mathbb{F}_{q^2}$ under the assumption that $r > 2$ be a prime and $\beta^{q+1} \neq 1$. See Hou and Lappano [43, 46, 52] and references therein for this conjecture and partial results along this direction. We remark that they used different techniques such as Hermite's criterion, power sums, and combinatorial identities.

In a series of works on permutation binomials and trinomials using power sums, Hou characterized the class of permutation trinomials of the form $P(x) = x(a + bx^{q-1} + cx^{2(q-1)})$ over $\mathbb{F}_{q^2}$ (see [46] and references therein). Here we can view $P(x) = xf(x^{q-1})$ where $f(x) = a + bx + cx^2$.

Theorem 5.15 (Hou 2013-2014 [46]). *Let q be an odd prime power, let $f(x) = ax + bx^q + cx^{2q-1} \in \mathbb{F}_{q^2}[x]$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following is satisfied:*

- $a = b = 0$, $q \equiv 1, 3 \pmod 6$.
- $(-a)^{(q+1)/2} = -1$ *or* 3, $b = 0$.
- $ab \neq 0$, $a = b^{1-q}$, $1 - \frac{4a}{b^2}$ *is a square of* $\mathbb{F}_q^*$.
- $ab(a - b^{1-q}) \neq 0$, $1 - \frac{4a}{b^2}$ *is a square of* $\mathbb{F}_q^*$, $b^2 - a^2 b^{q-1} - 3a = 0$.

Theorem 5.16 (Hou 2013-2014 [46]). *Let q be an even prime power, let $P(x) = ax + bx^q + cx^{2q-1} \in \mathbb{F}_{q^2}[x]$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following is satisfied:*

- $a = b = 0$, $q = 2^{2k}$.
- $ab \neq 0$, $a = b^{1-q}$, $Tr_{q/2}(b^{-1-q}) = 0$.
- $ab(a - b^{1-q}) \neq 0$, $\frac{a}{b^2} \in \mathbb{F}_q$, $Tr_{q/2}(\frac{a}{b^2}) = 0$, $b^2 + a^2 b^{q-1} + a = 0$.

Recently, in Li-Helleseth [58], Li-Qu-Li-Fu [55], Gupta-Sharma [38], Zha-Hu-Fan [100], various researchers constructed permutation trinomials in the form of $x^r h\left(x^{q-1}\right)$, where $h(x) = 1 + x^s + x^t$ has low degree over $\mathbb{F}_{q^2}$ and q is even. In general,

$$\begin{aligned} x^r h(x)^{q-1} &= x^r \frac{h(x)^q}{h(x)} \\ &= x^r \frac{(1 + x^s + x^t)^q}{1 + x^s + x^t} \\ &= x^r \frac{1 + x^{-s} + x^{-t}}{1 + x^s + x^t} \\ &= \frac{x^r + x^{r-s} + x^{r-t}}{1 + x^s + x^t} \end{aligned}$$

The idea of the fractional method is to show that $\frac{x^r + x^{r-s} + x^{r-t}}{1 + x^s + x^t} \neq \frac{y^r + y^{r-s} + y^{r-t}}{1 + y^s + y^t}$ if $x \neq y \in \mu_{q+1}$. This is equivalent to solving multivariate equations (see [29, 27, 53, 91] for q even) or ensuring that an algebraic curves $C(x, y) = 0$ has no rational points (x, y) over μ_ℓ^2 with $x \neq y$ ([11, 14]). There are several results dealing with higher degree polynomials $h(x) = 1 + x^s + x^t$ of special type. For example,

Theorem 5.17 (Li-Qu-Chen 2017 [53]). *Let $q = 2^h$ and h be a positive integer. Then $P(x) = x + x^{q-1} + x^{(q-1)q/2}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $h \not\equiv 0 \pmod 3$.*

Theorem 5.18 (Li-Qu-Chen-Li 2017 [54]). *Let $q = 2^h$, where h is odd, and $f(x) = x + x^{\frac{q^2-3q+5}{3}} + x^{\frac{2q^2-3q+4}{3}}$. Then $f(x)$ is a permutation trinomial over $\mathbb{F}_{q^2}$.*

Theorem 5.19 (Li-Qu-Chen-Li 2017 [54]). *Let $q = 2^h$, $h \geq 1, i$ be integers and $f(x) = x^{iq+i+3} + x^{(i+6)q+i-3} + x^{(i-2)q+i+5}$. Then $f(x)$ is a permutation trinomial over $\mathbb{F}_{q^2}$ if $\gcd(3 + 2i, q - 1) = 1$ and $k \not\equiv 0 \pmod 4$.*

Li, Qu, and Wang [56] have developed another systematic way to characterize permutation polynomials of the form $f(x) = x^r h\left(x^{q-1}\right) \in \mathbb{F}_{q^2}[x]$ over $\mathbb{F}_{q^2}$ where $h(x) \in \mathbb{F}_q[x]$ is an arbitrary polynomial. The main tools consist of the reduction of the degree of the q-th power of $h(x)$ by using the structure of μ_{q+1}, and the application of the AGW criterion twice so that we can reduce the permutation of $\mathbb{F}_{q^2}$ to a subset of the subfield $\mathbb{F}_q$.

Theorem 5.20 (Li-Qu-Wang 2018 [56]). *Let $f(x) = x^r h\left(x^{q-1}\right) \in \mathbb{F}_{q^2}[x]$ be such that all coefficients of $h(x)$ belong to $\mathbb{F}_q$ and S be the set defined as follows:*

$$S := \begin{cases} \{a \in \mathbb{F}_q^* : Tr\left(\frac{1}{a}\right) = 1\} & \text{if } q \text{ is even,} \\ \{a \in \mathbb{F}_q : \eta\left(a^2 - 4\right) = -1\} & \text{if } q \text{ is odd.} \end{cases}$$

Let $a = x + x^{-1}$ and $h(x) = h_1(a)x + h_2(a)$. Assume that

$$R(a) = \frac{h_1^2(a)D_{r-2}(a) + h_2^2(a)D_r(a) + 2h_1(a)h_2(a)D_{r-1}(a)}{h_1^2(a) + h_1(a)h_2(a)a + h_2^2(a)},$$

where $D_r(a)$ is the Dickson polynomial of the first kind. Then $f(x)$ permutes $\mathbb{F}_{q^2}$ if and only if the following conditions hold simultaneously:

- $\gcd(r, q-1) = 1$;
- *for the corresponding fractional polynomial $g(x) = x^r h(x)^{q-1}$, $g(x) = 1$ has a unique solution $x = 1$ in μ_{q+1} and $g(x) = -1$ has a unique solution $x = -1$ in μ_{q+1};*
- *$h(x) \neq 0$ for any $x \in \mu_{q+1}$;*
- *$R(a)$ permutes $\{2, -2\} \cup S$.*

Many explicit classes of PPs of the form $x^r h\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$ can be explained by using this result. We refer the reader to [56] and references therein. When the coefficients of $h(x)$ are in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the characterization is even more complicated, so we need to restrict our polynomial $h(x)$ to some special polynomials. We propose the following problem.

Problem 6. Classify sparse permutation polynomials of $\mathbb{F}_{q^2}$ of index $q+1$. Namely, PPs of the form $x^r f(x^{q-1})$ when f is sparse.

For example, there are many recent works on characterization of PPs of trinomials when the coefficients are in $\mathbb{F}_{q^2}$. In [53], Li, Qu and Chen proved

Theorem 5.21 (Li-Qu-Chen 2017 [53]). *Let $q = 2^k$ and k be a positive integer. Let $P(x) = x(1 + ax^{2(q-1)} + a^{q/2}x^{q(q-1)})$ be such that $a \in \mathbb{F}_{q^2}$ and the order of a is $q+1$. Then $P(x)$ is a PP of $\mathbb{F}_{q^2}$.*

Tu, Zeng, Li and Helleseth in [81] proved the sufficiency of the conditions in the following theorem and conjectured their necessity. Then Bartoli [10] proved the necessity using low degree algebraic curves and computational packages such as MAGMA. Hou [47] found a way to prove both directions at the same time.

Theorem 5.22 ([81], [10], [47]). *Let $q = 2^h$, $h \geq 3$. Let $P(x) = x + \beta x^{2(q-1)+1} + \alpha x^{q(q-1)+1} \in \mathbb{F}_{q^2}[x]$ be such that $\alpha, \beta \in \mathbb{F}_{q^2}^*$. Then $P(x)$ is a PP of $\mathbb{F}_{q^2}$ if and only if*

- $\beta = \alpha^{q-1}$ *and* $Tr_{q/2}(1 + \frac{1}{\alpha^{q+1}}) = 0$*; or*
- $\beta(1 + \alpha^{q+1} + \beta^{q+1}) + \alpha^{2q} = 0$, $\beta^{q+1} \neq 1$, *and* $Tr_{q/2}(\frac{\beta^{q+1}}{\alpha^{q+1}}) = 0$.

Exponents of many of these permutation polynomials are so called Niho exponents. See Li and Zeng [60] for an extensive survey of permutation polynomials from Niho exponents. Many open problems are proposed in [60] as well. Sometimes $P(x)$ may not be explicitly expressed as $P(x) = x^r f(x^{q-1})$. Indeed, Kyureghyan and Zieve [51] studied polynomials of the form $x + \gamma \mathrm{Tr}(x^k)$ and proved the following result.

Theorem 5.23 (Kyureghyan-Zieve 2016 [51]). *Let $q \equiv 1 \pmod 4$ and let $\gamma \in \mathbb{F}_{q^2}$ satisfy $(2\gamma)^{(q+1)/2} = 1$. Then $P(x) = x + \gamma Tr_{q^2/q}(x^{(q+1)^2/4})$ permutes $\mathbb{F}_{q^2}$.*

Let $N = \frac{q+3}{4}$. Then $P(x) = x + \gamma \mathrm{Tr}_{q^2/q}(x^{(q+1)^2/4}) = x(1 + \gamma x^{N(q-1)} + \gamma x^{(qN+1)(q-1)})$ is a PP of $\mathbb{F}_{q^2}$ if and only if $g(x) = x(1 + \gamma x^N + \gamma x^{qN+1})^{q-1}$ is a bijection on μ_{q+1}. In fact, $g(x)$ behaves as $c_1^2 x$ on the non-squares in μ_{q+1} and $c_2^2 x^N$ on the squares, for certain elements $c_1, c_2 \in \mu_{q+1}$.

Theorem 5.24 (Li-Qu-Chen-Li 2017 [54]). *Let $q = 2^h$. Then $f(x) = cx + \mathrm{Tr}_{q^2/q}\left(x^k\right)$ is a PP over $\mathbb{F}_{q^2}$ for each of the following cases:*

- $k = 2q - 1$, $c = 1$ *if h is even or $c^3 = 1$ if h is odd.*
- $k = \frac{(3q-2)\left(q^2+q+1\right)}{3}$, *$h$ is even and $c^3 = 1$.*
- $k = \frac{(3q^2-2)(q+4)}{5}$, *$h$ is odd and $c^3 = 1$.*
- $k = 2^{2h-2} + 3 \cdot 2^{h-2}$, $c \in \mathbb{F}_q$ *and $x^3 + x + c = 0$ has no solution in $\mathbb{F}_q$.*
- $k = \frac{2^{2h-1}+3\cdot 2^{h-1}+1}{3}$, *$h$ is odd and $c^{\frac{q+1}{3}} = 1$.*
- $k = \frac{q^2-2q+4}{3}$, *h is even and $c = 1$.*
- $c = 1$ *and* $k = \begin{cases} \frac{(2q^2-1)(q+6)}{7}, & h \equiv 1 \pmod 3; \\ -\frac{(q^2-2)(q+6)}{7}, & h \equiv 2 \pmod 3). \end{cases}$

The fractional polynomial $x^r f(x)^s$ can behave like a rational function. For example, in the following result, the polynomial $x^r f(x)^s$ behaves like $g^{-1} \circ x^n \circ g$ where $g(x) = \frac{x-\beta\gamma^q}{\gamma x-\beta}$ is injective from μ_ℓ to μ_ℓ.

Theorem 5.25 (Zieve 2013 [105]). *Let q be a prime power, $\ell = q+1$ and $s = q-1$. Let $n > 0$ and $k \geq 0$ be integers, and let $\beta, \gamma \in \mathbb{F}_{q^2}$ be such that $\beta^\ell = 1$ and $\gamma^\ell \neq 1$. Then $P(x) = x^{n+k\ell}((\gamma x^s - \beta)^n - \gamma(x^s - \gamma^q \beta)^n)$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(n+2k, s) = 1$ and $(n, \ell) = 1$.*

Similarly, we have

Theorem 5.26 (Zieve 2013 [105]). *Let q be a prime power, $\ell = q+1$ and $s = q-1$. Let $n > 0$ and $k \geq 0$ be integers, and let $\beta, \delta \in \mathbb{F}_{q^2}$ be such that $\beta^\ell = 1$ and $\delta \notin \mathbb{F}_q$. Then $P(x) = x^{n+k\ell}((\delta x^s - \beta\delta^q)^n - \delta(x^s - \beta)^n)$ is a PP of $\mathbb{F}_{q^2}$ if and only if $(n(n+2k), s) = 1$.*

Here $x^r f(x)^s$ behaves like $g^{-1} \circ x^n \circ g$ where $g(x) = \frac{\delta x - \beta\delta^q}{x - \beta}$ is injective from μ_ℓ to $\mathbb{F}_q \cup \{\infty\}$. There are also several work on rational functions of low degree, see for example, Bartoli and Giulietti [11, 14]. A generalization of Theorems 5.25, 5.26 can be found in [14]. Also in [51], Kyureghyan and Zieve constructed a few classes of PPs of the form $x + \mathrm{Tr}_{q^2/q}(x^k)$ using rational bijections over μ_ℓ when $n = 2, 3$.

Now we describe a construction through rational functions of arbitrary high degree. Let n be a positive integer and $\alpha \in \mathbb{F}_{q^2} \setminus \{0\}$. Then we define the following polynomials over $\mathbb{F}_{q^2}$.

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

$$H_n(x, \alpha) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i+1} \alpha^i x^{n-2i-1}.$$

The *Rédei function* is a rational function over $\mathbb{F}_{q^2}$ defined as $R_n(x, \alpha) = \frac{G_n(x,\alpha)}{H_n(x,\alpha)}$. It is easy to check that

$$(x + \sqrt{\alpha})^n = G_n(x, \alpha) + H_n(x, \alpha)\sqrt{\alpha}. \tag{5.1}$$

In the following result, the fractional polynomial $x^r f(x)^s$ behaves like a Rédei function that is a rational function of arbitrary degree.

Theorem 5.27 (Fu-Feng-Lin-Wang 2018 [34]). *Suppose $n > 0$ and m are two integers. Let $\alpha \in \mathbb{F}_{q^2}$ satisfy $\alpha^{q+1} = 1$, and μ_{q+1} be the set of all distinct $(q+1)$-th roots of unity. Then the polynomial*

$$P(x) = x^{n+m(q+1)} H_n(x^{q-1}, \alpha)$$

permutes $\mathbb{F}_{q^2}$ if and only if any one of the following conditions holds:

(i) $\sqrt{\alpha} \in \mu_{q+1}$ *and* $\gcd(n(n+2m), q-1) = 1$.

(ii) $\sqrt{\alpha} \notin \mu_{q+1}$, $\gcd(n+2m, q-1) = 1$ *and* $\gcd(n, q+1) = 1$.

Similarly, the statement works for $P(x) = x^{n+m(q+1)}G_n(x^{q-1}, \alpha)$.

This class of PPs of the form $x^r f(x^{q-1})$ has a nice property such that the degree of f can be arbitrarily high and can be generated recursively.

Large intermediate indices

For a finite field of size q^n, we can study permutation polynomials of index $\ell = q^{n-1} + \cdots + q + 1$. However, $P(x)$ may not be explicitly expressed as $P(x) = x^r f(x^{q-1})$. Indeed, in the study of polynomials of the form $x + \gamma \mathrm{Tr}(x^k)$, Kyureghyan and Zieve considered $n = 3$ and $\ell = q^2 + q + 1$ and they proved the following

Theorem 5.28 (Kyureghyan-Zieve 2016 [51]). *If q is odd, then $P(x) = x + Tr_{q^3/q}(x^{\frac{q^2+1}{2}})$ permutes $\mathbb{F}_{q^3}$.*

The index approach requires us to prove that $g(x) = x(1 + x^{(q+1)/2} + x^{(q^2+q+2)/2} + x^{(q^2+2)(q+1)/2)})^{q-1}$ permutes the set μ_{q^2+q+1}.

Theorem 5.29 (Li-Qu-Chen-Li 2017 [54]). *Let $q = 2^h$ and $f(x) = cx + \mathrm{Tr}_{q^4/q^2}\left(x^k\right) \in \mathbb{F}_{q^4}[x]$. Then $f(x)$ is a permutation polynomial over $\mathbb{F}_{q^4}$ if one of the following conditions occurs:*

- $k = 2^{4h-1} - 2^{3h-1} + 2^{2h-1} + 2^{h-1}$ *and* $c \in \mathbb{F}_q^*$.
- $k = q^3 - q + 1$ *and* $c = 1$.
- $k = q^4 - q^3 + q$ *and* $c = 1$.

We note that $\ell = q^3 + q^2 + q + 1$ in the above theorem. Also in the paper, two other permutation trinomials with index $\ell = q^2 + q + 1$ over $\mathbb{F}_{q^3}$ are constructed by multivariate method. Similar results were given by Wang, Zhang and Zha [91] for $\ell = q^2 + q + 1$ over $\mathbb{F}_{q^3}$.

Theorem 5.30 (Wang-Zhang-Zha 2018 [91]). *Let $q = 2^h$ and $h \not\equiv 1 \pmod 3$. If $f(x) = 1 + x^{q+1} + x^{-q}$ or $f(x) = 1 + x^{q+2} + x^{-q}$, then $P(x) = xf(x^{q-1})$ is a permutation polynomial over $\mathbb{F}_{q^3}$.*

The following result follows directly from Corollary 5.1.

Theorem 5.31 (Bartoli-Masuda-Quoos 2018 [14]). *Let $n \geq 2$, $s \geq 0$ be integers, $\beta \in \mu_{q^{n-1}+\cdots+q+1}$, and $L \in \mathbb{F}_{q^n}[x]$ be such that $L^q = \beta x^{-t} L$ for some fixed integer t. Then $x^{s+k(q^{n-1}+q^{n-2}+\cdots+q+1)}L(x^{q-1})$ permutes $\mathbb{F}_{q^n}$ if and only if $(s-t, q^{n-1}+\cdots+q+1) = 1$, $(s+k(q+1), q-1) = 1$, and L has no roots in $\mu_{q^{n-1}+\cdots+q+1}$.*

A concrete class of permutation polynomials over $\mathbb{F}_{q^3}$ using Theorem 5.31 and MAGMA is also provided in [14]. Earlier, for $\ell = q^2 + q + 1$, Ding et al. [28] and Yuan [97] gave several explict classes permutation polynomials over $\mathbb{F}_{q^3}$ where $q = 3^k$ and $q \equiv 3 (\mathrm{mod}\ 4)$ respectively. Wang et al. [92] presented six classes of permutation trinomials over $\mathbb{F}_{q^3}$ with $q = 3^k$. Bartoli [9] characterized four classes of permutation trinomials over $\mathbb{F}_{q^3}$ in terms of their coefficients in $\mathbb{F}_q$, $q = p^k$ and $p > 3$. Finally we propose the following problem.

Problem 7. Construct and classify permutation polynomials of $\mathbb{F}_{q^n}$ with intermediate indices such as $\ell = q^{n-1} + \cdots + q + 1$, $c(q^{n-1} + \cdots + q + 1)$, or $\frac{q^{n-1}+\cdots+q+1}{d}$, where c is a positive factor of $q - 1$ and d is a positive factor of $q^{n-1} + \cdots + q + 1$. For even n, construct and classify permutation polynomials of $\mathbb{F}_{q^n}$ with index $\ell = q^{n-1} - q^{n-2} + q^{n-3} + \cdots + q - 1$ or a constant scale of ℓ.

5.4 The maximum index

Obviously, most PPs over the finite field $\mathbb{F}_{q^n}$ have index $q^n - 1$, the largest possible index. In particular, Corollary 5.1 or Corollary 5.2 is trivial when the index is the largest possible. Therefore the index viewpoint is not so useful when the index of a polynomial is the largest index. Nevertheless, we could still construct polynomials piece-wisely and use cyclotomy of the small index ℓ to generate PPs with maximum index. Here is an example of such constructions where we use simple monomials for branch functions that are used to define polynomials piece-wisely.

Theorem 5.32 (Wang 2013 [88]). *Let $q - 1 = \ell s$ and $A_0, \ldots, A_{\ell-1} \in \mathbb{F}_q^*$. Then*

$$P(x) = \begin{cases} 0, & \text{if } x = 0; \\ A_i x^{r_i}, & \text{if } x \in C_i,\ 0 \le i \le \ell - 1. \end{cases} \tag{5.2}$$

is a PP of $\mathbb{F}_q$ if and only if $(r_i, s) = 1$ for any $i = 0, 1, \ldots, \ell - 1$ and $\{ind_\gamma(A_i) + r_i i \mid i = 0, \ldots, \ell - 1\}$ is a complete set of residues modulo ℓ.

In particular, these PPs have the following form with at most ℓ^2 terms.

$$P(x) = \frac{1}{\ell} \sum_{j=0}^{\ell-1} \sum_{i=0}^{\ell-1} A_i \zeta^{-ji} x^{r_i + js}$$

Their inverses can be easily obtained as well, see [89]. For more results on other types of piecewise construction, we refer the readers to [35, 24].

Problem 8. Classify more classes of permutation polynomials using other types of branch functions.

There is vast literature on constructing permutation polynomials of special forms over finite fields; many of these also have maximum indices. For more information on permutation polynomials prior to the year 2015, we refer the interested readers to [44, 72] and reference therein. Recently there is a focused study on sparse permutation polynomials such as binomials, trinomials, few-nomials. Most of them have special exponents and are defined over finite fields of even characteristic. One main technique to prove these results is to generate the polynomial equation into a system of equations by raising powers of the equation, and then covert the system into a lower-degree multivariate systems of equations. See [29, 27, 53, 91] and the references therein.

There is also an extensive study of permutation polynomials of the form $\sum(x^{p^m} - x + \delta_i)^{s_i} + L(x)$; we refer the readers to recent papers [39, 65, 101] and references therein. Other than solving special equations over finite fields using the multivariate method, many of these results were obtained via an application of the general AGW criterion; see [98, 99, 102, 56]. Because our purpose in this paper is to demonstrate the index approach, we therefore decide not to list all the articles dealing with maximum indices.

6 Conclusion: other results and problems

As mentioned above, the notion of the index of a polynomial over finite fields is quite useful in the study of permutation polynomials, value set bounds, as well as character sums of polynomials over finite fields. We can also study the inverses of permutation polynomials by index approach [89, 57]. We would like to explore this index approach further to some related problems. For example, it would be interesting to explicitly evaluate character sums of polynomials using their indices. For the value sets of polynomials, we would like to characterize polynomials with small value sets in terms of their indices. Furthermore, it seems very interesting to classify PPs of small indices up to intermediate indices in terms of their coefficients. Another interesting problem is the distribution of PPs in terms of their indices. In [68], Masuda and Zieve showed that permutation binomials over prime field $\mathbb{F}_p$ must have their indices less than $\sqrt{p} + 1$. We would like to know whether this kind of behavior works for permutation trinomials or few-nomials.

Problem 9. Study the distribution of indices for “sparse" permutation polynomials over finite prime field.

It is also interesting to extend the index approach to other new types of problems. Recently, Işik and Winterhof [48] studied the relationship between Carlitz rank and the index of permutation polynomials. The Carlitz rank was introduced in [7] for permutation polynomials to measure the smallest number of inversions used to represent this permutation as a composition of linear polynomials and inversions in alternating order. We refer to [79] for a survey of results on Carlitz rank. Işik and

Winterhof [48] proved that, if the permutation polynomial g is neither close to a polynomial of the form ax nor a rational function of the form ax^{-1}, then the Carlitz rank $Crk(g) > q - \max\{3Ind(g), (3q)^{1/2}\}$, where $Ind(g)$ denotes the index of g. Moreover, they showed that the permutation polynomial which represents the discrete logarithm guarantees both a large index and a large Carlitz rank. This results has cryptographic applications.

Problem 10. Find more applications of indices of polynomials over finite fields.

Another interesting new problem is to study the distribution or characterization of irreducible polynomials $g(x) = x^r f(x^{(q-1)/\ell}) + b$ ($b \neq 0$) according to their indices. For example, the characterization of irreducible polynomials of the form $x^r + b$ (corresponding to $\ell = 1$) was done earlier. It would be natural to characterize/enumerate those irreducible polynomials with prescribed indices. Similarly, it would be interesting to study primitive polynomials, primitive normal polynomials with prescribed indices. See related work in [31, 32, 42, 77, 71] and references therein.

We remark that the index for multivariate polynomials and polynomial vector maps is also introduced in [74]. Results for value set bounds in terms of indices for such polynomials are also obtained similarly. It would be interesting to extend our study for other problems involving multivariate polynomials and polynomial vector maps as well.

Acknowledgments. We would like to thank Amir Akbary, Daniele Bartoli, Xiang-Dong Hou, Kangquan Li, Ariane M. Masuda, Longjiang Qu, Aleksandr Tuxanidy, Yanping Wang, Arne Winterhof, Yanbin Zheng for their helpful suggestions.

Bibliography

[1] A. Akbary, S. Alaric, and Q. Wang, On some classes of permutation polynomials, *Int. J. Number Theory* 4 (2008), no. 1, 121-133.

[2] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* 15 (2009), 195-206.

[3] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.* 17 (2011), no. 1, 51-67.

[4] A. Akbary and Q. Wang, On some permutation polynomials, *Int. J. Math. Math. Sci.* 16 (2005), 2631–2640.

[5] A. Akbary and Q. Wang, A generalized Lucas sequence and permutation binomials, *Proc. Amer. Math. Soc.* 134 (2006), no 1, 15-22.

[6] A. Akbary and Q. Wang, On polynomials of the form $x^r f(x^{(q-1)/l})$, *Int. J. Math. Math. Sci.*, Volume 2007, Article ID 23408, 7 pages.

[7] E. Aksoy, A. Çesmelioğlu, W. Meidl, A. Topuzoğlu, On the Carlitz rank of permutation polynomials, *Finite Fields Appl.* 15 (2009), no. 4, 428-440.

[8] J. Arney and E A. Bender, Random mappings with constraints on coalescence and number of origins, *Pacific J. Math.* 103 (1982), no. 2, 269-294.

[9] D. Bartoli, Permutation trinomials over $\mathbb{F}_{q^3}$,*arXiv.1804.01305vl*, 2018.

[10] D. Bartoli, On a conjecture about a class of permutation trinomials, *Finite Fields Appl.* 52 (2018), 30-50.

[11] D. Bartoli and M. Giulietti, Permutation polynomials, fractional polynomials, and algebraic curves, *Finite Fields Appl.* 51 (2018), 1-16.

[12] D. Bartoli, M. Giulietti, G. Zini, On monomial complete permutation polynomials, *Finite Fields Appl.* 41 (3) (2016), 132-158.

[13] D. Bartoli, M. Giulietti, L. Quoos, G. Zini, Complete permutation polynomials from exceptional polynomials, *J. Number Theory* 176 (2017), 46-66.

[14] D. Bartoli, A. M. Masuda, L. Quoos, Permutation polynomials over $\mathbb{F}_{q^2}$ from rational functions, *arXiv:1802.05260*, 2018.

[15] L.A. Bassalygo, V.A. Zinoviev, On one class of permutation polynomials over finite fields of characteristic two, *Mosc. Math. J.* 15 (4) (2015), 703-713.

[16] L.A. Bassalygo, V.A. Zinoviev, Permutation and complete permutation polynomials, *Finite Fields Appl.* 33 (2015), 198-211.

[17] S. Bhattacharya and S. Sarkar, On some permutation binomials and trinomials over $\mathbb{F}_{2^n}$, *Des. Codes Cryptogr.* 82 (2017), no. 1-2, 149-160.

[18] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, Acta Arith. 5 (1959), 417-423.

[19] H. Borges and R. Conceicao, On the characterization of minimal value set polynomials, *J. Number Theory* 133 (2013), 2021-2035.

[20] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, *Mathematika* 8 (1961), 121-130.

[21] Q. Cheng, J. Hill and D. Wan, Counting value sets: algorithms and complexity, Tenth Algorithmic Number Theory Symposium ANTS-X, 2012, University of California at San Deigo.

[22] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* 17 (1970), 255-271.

[23] S. D. Cohen, Primitive polynomials with a prescribed coefficient, *Finite Fields Appl.* 12 (2006), no. 3, 425-491.

[24] R. Coulter, M. Henderson, R. Matthews, A note on constructing permutation polynomials, *Finite Fields Appl.* 15 (2009), no. 5, 553-557.

[25] P. Das, The number of permutation polynomials of a given degree over a finite field, *Finite Fields Appl.* 8 (2002), 478–490.

[26] P. Das and G. L. Mullen, Value sets of polynomials over finite fields, in *Finite Fields with Applications in Coding Theory, Cryptography and Related Areas*, G.L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, Eds., Springer, 2002, 80-85.

[27] C. Ding, L. Qu, Q. Wang, J. Yuan and P. Yuan, Permutation trinomials over finite fields with even characteristic, *SIAM J. Discrete Math.*29 (2015), 79-92.

[28] C. Ding, Q. Xiang, J. Yuan, P. Yuan, Explicit classes of permutation polynomials of $\mathbb{GF}(3^{3m})$, *Sci. China Series A* 53 (2009), 639-647.

[29] H. Dobbertin, almost perfect nonlinear power functions on $\mathbf{GF}(2^n)$: the Welch case, *IEEE Trans. Inform. Theory.*, 45 (1999), 1271-1275.

[30] A. B. Evans, Orthomorphism Graphs of Groups, Lecture Notes in Mathematics, Vol. 1535, Springer, Berlin, 1992.

[31] S.Q. Fan and W.B. Han, *p-Adic formal series and primitive polynomials over finite fields*, Proc. Amer. Math. Soc. 132 (2004), 15–31.

[32] S. Fan, W. Han, K. Feng, Primitive normal polynomials with multiple coefficients prescribed: An asymptotic result, *Finite Fields Appl.* 13 (2007): 1029-1044.

[33] X. Feng, D. Lin, L. Wang, Q. Wang, Further results on complete permutation monomials over finite fields, https://arxiv.org/abs/1708.06955.

[34] S. Fu, X. Feng, D. Lin, Q. Wang, A Recursive Construction of Permutation Polynomials over $\mathbb{F}_{q^2}$ with Odd Characteristic from Rédei Functions, Des. Codes Cryptogr. (2018). https://doi.org/10.1007/s10623-018-0548-4.

[35] N. Fernando and X. Hou, A piecewise construction of permutation polynomial over finite fields, *Finite Fields Appl.* 18 (2012), 1184-1194.

[36] P. Flajolet and A. M. Odlyzko, Random mapping statistics, Advances in Cryptology-EUROCRYPT'89, Lecture Notes in Computer Science 434, 329-354, 1990.

[37] Z. Gao and Q. Wang, A probabilistic approach to value sets of polynomials over finite fields. *Finite Fields Appl.* 33 (2015), 160-174.

[38] R. Gupta, R.K. Sharma, Some new classes of permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.* 41(2016), 89-96.

[39] R. Gupta, R. K. Sharma, Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x$ over $\mathbb{F}_{p^{2m}}$, *Finite Fields Appl.* 50 (2018), 196-208.

[40] J. Gomez-Calderon and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* 28 (1988), no. 2, 167-188.

[41] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* 101 (1997), 255-287.

[42] J. Ha, Irreducible polynomials with several prescribed coefficients, *Finite Fields Appl.* 40 (2016), 10-25.

[43] X. Hou, Permutation polynomials over finite fields - a survey of recent advances, *Finite Fields Appl.* 32 (2015), 82-119.

[44] X. Hou, A survey of permutation binomials and trinomials over finite fields. Topics in finite fields, 177-191, Contemp. Math., 632, Amer. Math. Soc., Providence, RI, 2015.

[45] X. Hou, Determination of a type of permutation trinomials over finite fields, II. *Finite Fields Appl.* 35 (2015), 16-35.

[46] X. Hou, Permutation polynomials of $\mathbb{F}_{q^2}$ of the form $aX + X^{r(q-1)+1}$. Contemporary developments in finite fields and applications, 74-101, World Sci. Publ., Hackensack, NJ, 2016.

[47] X. Hou, On a Class of Permutation Trinomials in Characteristic 2, *arXiv:1803.04071*, 2018.

[48] L. Işik and A. Winterhof, Carlitz rank and index of permutation polynomials, *Finite Fields Appl.* 49 (2018), 156-165.

[49] S. Konyagin and F. Pappalardi, Enumerating permutation polynomials over finite fields by degree, *Finite Fields Appl.* 8 (2002), no. 4, 548–553.

[50] S. Konyagin and F. Pappalardi, Enumerating permutation polynomials over finite fields by degree. II, *Finite Fields Appl.* 12 (2006), no. 1, 26–37.

[51] G. Kyureghyan and M. E. Zieve, Permutation polynomials of the form $X + \gamma\text{Tr}(X^k)$. Contemporary developments in finite fields and applications, 178-194, World Sci. Publ., Hackensack, NJ, 2016.

[52] S. D. Lappano, A note regarding permutation binomials over $\mathbb{F}_{q^2}$, *Finite Fields Appl.* 34 (2015), 153-160.

[53] K. Li, L. Qu, X. Chen, New classes of permutation binomials and permutation trinomials over finite fields, *Finite Fields Appl.* 43 (2017), 69-85.

[54] K. Li, L. Qu, X. Chen and C. Li, Permutation polynomials of the form $cx + \text{Tr}_{q^l/q}(x^a)$ and permutation trinomials over finite fields with even characteristic, *Cryptogr. Commun.*, https://doi.org/10.1007/s12095-017-0236-7, 2017.

[55] K. Li, L. Qu, C. Li and S. Fu, New permutation trinomials constructed from fractional polynomials, *arXiv: 1605.06216v1*, 2016.

[56] K. Li, L. Qu and Q. Wang, New Constructions of Permutation Polynomials of the Form $x^r h\left(x^{q-1}\right)$ over $\mathbb{F}_{q^2}$, *Des. Codes Crypto.* https://doi.org/10.1007/s10623-017-0452-3, 2018.

[57] K. Li, L. Qu and Q. Wang, Compositional inverses of permutation polynomials of the form $x^r h(x^s)$ over finite fields, Cryptogr. Commun., https://doi.org/10.1007/s12095-018-0292-7, 2018.

[58] N. Li and T. Helleseth, Several classes of permutation trinomials from Niho exponents, *Cryptogr. Commun.* 9 (2017), no. 6, 693-705.

[59] N. Li and T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *arXiv: 1606.03768v1*, 2016.

[60] N. Li and X. Zeng, A survey on the applications of Niho exponents, *Cryptogr. Commun.*, https://doi.org/10.1007/s12095-018-0305-6, 2018.

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

[62] R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, *Amer. Math. Monthly* 100 (1993), 71-74.

[63] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1997.

[64] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields Appl.* 13 (2007), 58–70.

[65] L. Li, S. Wang, C. Li, 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.* 51 (2018), 31-61.

[66] J. Ma, T. Zhang, T. Feng, G. Ge, New results on permutation polynomials over finite fields, *Des. Codes Cryptogr.* 83 (2017), no. 2, 425-443.

[67] J. E. Marcos, Specific permutation polynomials over finite fields, *Finite Fields Appl.* 17 (2011), no. 2, 105-112

[68] A. M. Masuda and M. E. Zieve, Permutation binomials over finite fields, *Trans. Amer. Math. Soc.* 361 (2009), no. 8, 4169-4180.

[69] W. H. Mills, Polynomials with minimal value sets, *Pacific J. Math* 14 (1964), 225-241.

[70] G. L. Mullen, Permutation polynomials over finite fields, *Finite Fields, Coding Theory, and Advances in Communications and Computing*, 131-151, Marcel Dekker, New York, 1993.

[71] G. L. Mullen and D. Panario, Handbook of Finite Fields, CRC Press, 2014.

[72] G. L. Mullen and Q. Wang, Permutation polynomials of one variable, Section 8.1 in Handbook of Finite Fields, CRC, 2014.

[73] G. L. Mullen, D. Wan, and Q. Wang, Value sets of polynomial maps over finite fields, *Quart. J. Math.* 64 (2013), no. 4, 1191-1196.

[74] G. L. Mullen, D. Wan, and Q. Wang, An index bound on value sets of polynomial maps over finite fields, *Proceedings of Workshop on the Occasion of Harald Niederreiter's 70th Birthday: Applications of Algebra and Number Theory*, June 23-27, 2014.

[75] H. Niederreiter and A. Winterhof, Cyclotomic $\mathcal{R}$-orthomorphisms of finite fields, *Discrete Math.* 295 (2005), 161-171.

[76] Y. H. Park and J. B. Lee, Permutation polynomials and group permutation polynomials, *Bull. Austral. Math. Soc.* 63 (2001), 67–74.

[77] P. Pollack, Irreducible polynomials with several prescribed coefficients, Finite Fields Appl. 22 (2013), 70–78.

[78] R. Shaheen and A. Winterhof, Permutations of finite fields for check digit systems, *Des. Codes Cryptogr.* 57 (2010), no. 3, 361-371.

[79] A. Topuzoğlu, Carltiz ranks of permutations of finite fields: a survey, *J. Symbolic Comput.* 64 (2014), 53-66.

[80] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* 1 (1995), 64-82.

[81] Z. Tu, X. Zeng, C. Li, T. Helleseth, A class of new permutation trinomials, *Finite Fields Appl.* 50 (2018), 178-195.

[82] D. Wan, A p-adic lifting lemma and its applications to permutation polynomials, Lecture Notes in Pure and Appl. Math., Marcel Dekker, New York, Vol. 141, 1992, 209-216.

[83] D. Wan and R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* 112 (1991), 149–163.

[84] D. Wan, P. J. S. Shiue and C. S. Chen, Value sets of polynomials over finite fields, *Proc. Amer. Math. Soc.* 119 (1993), 711-717.

[85] D. Wan, Q. Wang, Index bounds for character sums of polynomials over finite fields, *Des. Codes Cryptogr.* 81 (2016), no. 3, 459-468.

[86] L. Wang, On permutation polynomials, *Finite Fields Appl.* 8 (2002), no. 3, 311-322.

[87] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, Sequences, Subsequences, and Consequences (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), 119-128, Lecture Notes in Comput. Sci. Vol. 4893, Springer, Berlin, 2007.

[88] Q. Wang, Cyclotomy and permutation polynomials of large indices, *Finite Fields Appl.* 22 (2013), 57-69.

[89] Q. Wang, A note on inverses of cyclotomic mapping permutation polynomials over finite fields. *Finite Fields Appl.* 45 (2017), 422-427.

[90] L. Wang, B. Wu, Z. Liu, Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x^{p^m} + x$ over $\mathbb{F}_{p^{2m}}$, *Finite Fields Appl.* 44 (2017), 92-112.

[91] Y. Wang, W. Zhang, Z. Zha, More new classes of permutation trinomials over $\mathbb{F}_{2^n}$, *SIAM J. Discrete Math.* 32(2018), 1946âĂŞ1961.

[92] Y. Wang, Z. Zha, W. Zhang, Six new classes of permutation trinomials over $\mathbb{F}_{3^{3k}}$, *Appl. Algebra Eng. Commun. Comput.* https://doi.org/10.1007/s00200-018-0353-3, 2018, 1-21.

[93] K. S. Williams, On general polynomials, *Canad. Math. Bull.* 10 (1967), no. 4, 579-583.

[94] A. Winterhof, Generalizations of complete mappings of finite fields and some applications, *J. Symbolic Comput.* 64 (2014), 42-52.

[95] G. Wu, N. Li, T. Helleseth, Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields Appl.* 28 (2014) 148-165.

[96] G. Wu, N. Li, T. Helleseth, Y. Zhang, Some classes of complete permutation polynomials over $\mathbb{F}_q$, *Sci. China Math.* 58 (10) (2015) 2081-2094.

[97] P. Yuan, More explicit classes of permutation polynomials of $\mathbb{GF}(3^{3m})$, *Finite Fields Appl.* 53 (2010), 88-95.

[98] P. Yuan and C. Ding, Permutation polynomials over finite fields from a powerful lemma, *Finite Fields Appl.* 17 (2011), no. 6, 560-574.

[99] P. Yuan and C. Ding, Further results on permutation polynomials over finite fields, *Finite Fields Appl.* 27 (2014), 88-103.

[100] Z. Zha, L. Hu, S. Fan, Further results on permutation trinomials over finite fields with even characteristic, *Finite Fields Appl.* 45 (2017), 43-52.

[101] Z. Zha, L. Hu, Z. Zhang, New results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + x^{p^m} + x$ over $\mathbb{F}_{p^{2m}}$, *Cryptogr. Commun.* 10 (2018), no. 3, 567-578.

[102] Y. Zheng, P. Yuan and D. Pei, Large classes of permutation polynomials over $\mathbb{F}_{q^2}$, *Des. Codes Cryptogr.* 81 (2016), 505-521.

[103] M. E. Zieve, Some families of permutation polynomials over finite fields, *Int. J. Number Theory* 4 (2008), 851–857.

[104] M. E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h\left(x^{(q-1)/d}\right)$, *Proc. Am. Math. Soc.* 137 (2009), 2209-2216.

[105] M. E. Zieve, Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares, *arXiv:1312.1325*, 2013.

[106] M. E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$, *arXiv:1310.0776*, 2013.

Author information

Qiang Wang, School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada.
E-mail: wang@math.carleton.ca