ON PERMUTATION POLYNOMIALS OF PRESCRIBED SHAPE

AMIR AKBARY, DRAGOS GHIOCA, AND QIANG WANG

ABSTRACT. We count permutation polynomials of $\mathbb{F}_q$ which are sums of $m+1(\geq 2)$ monomials of prescribed degrees. This allows us to prove certain results about existence of permutation polynomials of prescribed shape.

1. INTRODUCTION

Let p be prime and let q be a nontrivial power of p. A polynomial is a permutation polynomial of $\mathbb{F}_q$ if it induces a bijective map from $\mathbb{F}_q$ onto itself. The study of permutation polynomials of a finite field goes back to 19-th century when Hermite and later Dickson pioneered this area of research. In recent years, interests in permutation polynomials have significantly increased because of their potential applications in cryptography, coding theory, and combinatorics (see for example [2], [8], [12]). For more background material on permutation polynomials we refer to Chapter 7 of [10]. In [9], Lidl and Mullen proposed nine open problems and conjectures involving permutation polynomials of finite fields. This is one of the open problems.

Problem 1.1 (Lidl-Mullen). *Let $N_d(q)$ denote the number of permutation polynomials 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 $1 \leq d < q-1$ such that d is either 1 or it is not a divisor of $(q-1)$. Find $N_d(q)$.*

Note that we may assume each polynomial defined over $\mathbb{F}_q$ has degree at most $(q-1)$ because $x^q = x$ for each $x \in \mathbb{F}_q$.

We review several recent results regarding this problem. In [3], Das proved that $N_{p-2}(p) \sim (\varphi(p)/p)p!$ as $p \to \infty$, where φ is the Euler function. More precisely he proves that

$$\left| N_{p-2}(p) - \frac{\varphi(p)}{p} p! \right| \leq \sqrt{\frac{p^{p+1}(p-2)+p^2}{p-1}}.$$

This result has been improved and generalized by Konyagin and Pappalardi [5] who proved that

$$\left| N_{q-2}(q) - \frac{\varphi(q)}{q} q! \right| \leq \sqrt{\frac{2e}{\pi}} q^{\frac{q}{2}}.$$

Furthermore, Konyagin and Pappalardi [6] count the permutation polynomials which have no monomials of prescribed degrees. More precisely, they prove the following result.

2000 *Mathematics Subject Classification.* 11T06, 05A16.

Key words and phrases. Permutation polynomials, Finite fields.

Research of the first and the third authors was partially supported by NSERC.

Theorem 1.2 (Konyagin-Pappalardi). *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 permutation polynomials h of $\mathbb{F}_q$ of degree less than $(q-1)$ such that the coefficient of x^{k_i} in h equals 0, for $i = 1, \dots, j$. Then*

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

Note that $N_{q-2}(q) = q! - N(q-2; q)$.

Theorem 1.2 leaves open the question that whether there are permutation polynomials with a prescribed set of nonzero monomials, as it only counts the permutation polynomials whose nonzero monomials are a *subset* of a given set of monomials. Moreover, Theorem 1.2 is vacuous when k_1 is quite small comparing to q, as in that case the right hand side of the above inequality is larger than $q!$.

In this paper we address both of the above issues. On one hand, we are able to count the permutation polynomials which have a prescribed set of nonzero monomials (see Theorem 1.3). More precisely, we provide a partition of the set of permutation polynomials of degree d and obtain upper and lower bounds for the number of permutation polynomials in each class. On the other hand, as a consequence of our main result (Theorem 1.3), we can prove the existence of many permutation polynomials which have a prescribed shape (see Corollary 1.5), or a prescribed degree (see Theorem 1.7).

In order to state our results we need the following terminology. For any nonconstant monic polynomial $g(x) \in \mathbb{F}_q[x]$ of degree $\leq q-1$ with $g(0) = 0$, let r be the vanishing order of $g(x)$ at zero and let $f_1(x) := g(x)/x^r$. Then let ℓ be the least divisor of $q-1$ with the property that there exists a polynomial $f(x)$ of degree $(\ell \cdot \deg(f_1))/(q-1)$ such that $f_1(x) = f(x^{(q-1)/\ell})$. So $g(x)$ can be written *uniquely* as $x^r f(x^{(q-1)/\ell})$. We call ℓ the *index* of g. More generally any nonconstant polynomial $h(x)$ can be written as $h(x) = ag(x) + b$ where $a \neq 0$ and $g(x)$ is monic with $g(0) = 0$. We define the *index* of $h(x)$ as the index of g. So any nonconstant polynomial $h(x) \in \mathbb{F}_q[x]$ of degree $\leq q-1$ and of index ℓ can be written *uniquely* as

$$a(x^r f(x^{(q-1)/\ell})) + b.$$

Clearly, h is a permutation polynomial of $\mathbb{F}_q$, if and only if $g(x) = x^r f(x^{(q-1)/\ell})$ is a permutation polynomial of $\mathbb{F}_q$.

If $\ell = 1$ then $f(x) = 1$ and so $g(x) = x^r$. In this case $g(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $(r, q-1) = 1$. So from now on we assume that $\ell > 1$.

We set up the notation for our main result. Let q be a prime power, and $\ell \geq 2$ be a divisor of $q-1$. Let m, r be positive integers, and $\bar{e} = (e_1, \dots, e_m)$ be an m-tuple of integers that satisfy the following conditions:

$$0 < e_1 < e_2 \cdots < e_m \leq \ell - 1 \text{ and } (e_1, \dots, e_m, \ell) = 1 \text{ and } r + e_m s \leq q - 1, \tag{1.1}$$

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

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

Note that if r and $\bar{e}$ satisfy (1.1) then $g^{\overline{a}}_{r,\bar{e}}(x)$ has index ℓ.

We observe that if $g^{\overline{a}}_{r,\bar{e}}(x)$ is a permutation polynomial of $\mathbb{F}_q$ then

$$(r, s) = 1, \tag{1.2}$$

and so, $r + e_m s < q - 1$. This is true, since otherwise $(r, s) = c > 1$. Let ω be a primitive c-th root of unity in $\mathbb{F}_q$. Then $g^{\overline{a}}_{r,\overline{e}}(1) = g^{\overline{a}}_{r,\overline{e}}(\omega)$, and so $g^{\overline{a}}_{r,\overline{e}}(x)$ is not a permutation polynomial.

With the above notation define $N^m_{r,\overline{e}}(\ell, q)$ as the number of all tuples $\overline{a} \in \left(\mathbb{F}_q^*\right)^m$ such that $g^{\overline{a}}_{r,\overline{e}}(x)$ is a permutation polynomial of $\mathbb{F}_q$. In other words $N^m_{r,\overline{e}}(\ell, q)$ is the number of all monic permutation $(m+1)$-nomials $g^{\overline{a}}_{r,\overline{e}}(x) = x^r f(x^{(q-1)/\ell})$ of $\mathbb{F}_q$ with vanishing order at zero equal to r, set of exponents $\bar{e}$ for $f(x)$, and index ℓ.

In this paper we will find an asymptotic formula for $N^m_{r,\overline{e}}(\ell, q)$. Our main result is the following.

Theorem 1.3. *We have*

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

In fact in (2.16) and (2.17) we establish more precise upper and lower bounds for the quotient in Theorem 1.3. Our theorem together with (2.16) and (2.17) improve and generalize Theorem 4.5 of [7] which treats only the case that $m = 1$ and $e_1 = 1$. We also note that one may generalize the methods introduced in [11] to obtain similar bounds for $N^m_{r,\overline{e}}(\ell, q)$ as in our Theorem 1.3.

Next we employ Theorem 1.3 to study the existence of permutation polynomials of certain shapes. There are no permutation polynomials of $\mathbb{F}_q$ of degree $d \mid (q-1)$. Moreover Carlitz's conjecture (now a theorem due to Fried, Guralnick, and Saxl [4]) states that, for any positive even degree n, there is no permutation polynomial of degree n of $\mathbb{F}_q$ if q is sufficiently large compared to n. On the other hand one can prove the existence of permutation polynomials of varying degrees, as it is evident from the following result.

Theorem 1.4 (Carlitz-Wells). *(i) Let $\ell > 1$. Then for q sufficiently large, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$.*

(ii) Let $\ell > 1$, $(r, q-1) = 1$, and k be a positive integer. Then 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 permutation polynomial of $\mathbb{F}_q$.

See [1, Theorem 2 and Theorem 3] for a proof.

Recently several authors found quantitative versions of the Carlitz-Wells theorem in binomial case. In [7], Laigle-Chapuy proves the first assertion of Theorem 1.4 assuming $q > \ell^{2\ell+2}\left(1 + \frac{\ell+1}{\ell^{\ell+2}}\right)^2$. In [11], Masuda and Zieve obtain a stronger result for more general binomials of the form $x^r(x^{e_1(q-1)/\ell} + a)$. More precisely they show the truth of part (i) of Theorem 1.4 for $q > \ell^{2\ell+2}$.

Here by employing Theorem 1.3 we obtain the following quantitative generalization of the Carlitz-Wells theorem, which surpasses all the above results.

Corollary 1.5. *For any q, r, $\bar{e}$, m, ℓ that satisfy (1.1), (1.2), and $q > \ell^{2\ell+2}$, there exists an $\bar{a} \in (\mathbb{F}_q^*)^m$ such that the $(m+1)$-nomial $g^{\bar{a}}_{r,\bar{e}}(x)$ is a permutation polynomial of $\mathbb{F}_q$.*

Remark 1.6. For $q \geq 7$ we have $\ell^{2\ell+2} < q$ as long as $\ell < \frac{\log q}{2 \log\log q}$.

As an immediate corollary of Theorem 1.3 we can obtain the existence of permutation $(m+1)$-nomials which have coefficients equal to 0 for their x^k terms, where $2 \leq k \leq s$ (simply take $r = 1$ in a permutation polynomial of the form $x^r f(x^s)$ as in Corollary 1.5). This observation addresses one of the questions left open by Konyagin and Pappalardi (see the discussion after Theorem 1.2).

Next note that for $1 \leq t \leq q-2$ the number of permutation polynomials of degree at least $(q-t-1)$ is $q! - N(q-t-1, q-t, \dots, q-2; q)$. In [6, Corollary 2] 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 will guarantee the existence of permutation polynomials of degree *at least* $(q-t-1)$ for $t \leq 0.03983\ q$ (as long as q is sufficiently large). Our next theorem gives generalization and refinement of this existence result for certain values of t.

Theorem 1.7. *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 $g^{\bar{a}}_{r,\bar{e}}(x)$ of degree $(q-t-1)$ which is a permutation polynomial of $\mathbb{F}_q$.*

Note that Theorem 1.7 establishes the existence of permutation polynomials with *exact* degree $(q-t-1)$.

Our arguments in the proof of our main result (Theorem 1.3) are of two flavors. Firstly, we use combinatorial arguments specific for permutation polynomials, which were inspired from Laigle-Chapuy's work [7]. Secondly, we use an upper bound on sums of multiplicative characters, which originally is a consequence of Weil's proof of the Riemann hypothesis for curves over finite fields. We further would like to point out that the proof of Theorem 1.3 for $m > 1$ differs significantly from the case $m = 1$. In fact the direct application of the method of [7] leads to difficulties in the case $m > 1$. In this paper we deal with the latter case by splitting all tuples in $(\mathbb{F}_q)^m$ in two categories: *good* and *bad* tuples (see Section 2 for the definition), and then applying the Weil bound only to the character sums associated to the good tuples.

In the next section we prove our main result (Theorem 1.3), and in Section 3 we prove Theorem 1.7.

2. Proof of the Main Theorem

In the proof of Theorem 1.3 we will use the following classical inequality for character sums which is proved by Weil in [14] using methods of algebraic geometry (see [10, Theorem 5.41] for an elementary proof; see also [10, Chapter 5] for a discussion of upper bounds for character sums).

Theorem 2.1 (Weil). *Let Ψ be a multiplicative character of $\mathbb{F}_q$ of order $\ell > 1$ and let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an ℓ-th power of a polynomial. Let d be the number of distinct roots of $f(x)$ in its splitting field over $\mathbb{F}_q$. Then for every $t \in \mathbb{F}_q$ we have*

$$\left| \sum_{a \in \mathbb{F}_q} \Psi(tf(a)) \right| \leq (d-1)\sqrt{q}.$$

We continue with the notation from Section 1; so, $\ell \geq 2$ is a divisor of $(q-1)$, and $s = (q-1)/\ell$. We denote by S_ℓ the set of all permutations of $\{1, \dots, \ell\}$, and by μ_ℓ the set of all ℓ-th roots of unity in $\mathbb{F}_q^*$.

We let α be a generator of the cyclic group $\mathbb{F}_q^*$. Let ψ be a multiplicative character of order ℓ of μ_ℓ. More precisely, let ω be a primitive ℓ-th root of unity in $\mathbb{C}$. Define $\psi(\alpha^s) = \omega$ and extend

it with $\psi(0) = 0$. Finally, we let a multiplicative character Ψ of $\mathbb{F}_q$ of order ℓ be defined by $\Psi(\alpha) = \psi(\alpha^s)$, and extended so that $\Psi(0) = 0$.

For any permutation $\sigma \in S_\ell$, and any $\beta_1, \ldots, \beta_\ell \in \mu_\ell$, we define

$$P_\sigma(\beta_1, \ldots, \beta_\ell) = \prod_{i=1}^{\ell} \left(\sum_{j=0}^{\ell-1} \left(\psi(\beta_i)\psi(\alpha^s)^{-\sigma(i)} \right)^j \right).$$

It is clear that

$$\{\beta_1, \ldots, \beta_\ell\} = \mu_\ell \iff \text{there exists } \sigma \text{ such that } P_\sigma(\beta_1, \ldots, \beta_\ell) = \ell^\ell. \tag{2.1}$$

Furthermore, there exists a unique permutation σ satisfying (2.1); it is given by solving the equations

$$\alpha^{s\cdot\sigma(i)} = \beta_i, \tag{2.2}$$

for each $i \in \{1, \ldots, \ell\}$. We summarize below our findings about P_σ.

Lemma 2.2. *Let $\beta_1, \ldots, \beta_\ell \in \mu_\ell$. Then*

$$\frac{1}{\ell^\ell} \sum_{\sigma \in S_\ell} P_\sigma(\beta_1, \ldots, \beta_\ell) = \begin{cases} 1 & \text{if } \{\beta_1, \ldots, \beta_\ell\} = \mu_\ell \\ 0 & \text{otherwise} \end{cases}.$$

We extend the definition of P_σ to $\beta_i \in \mu_\ell \cup \{0\}$. If there are exactly k numbers β_i (for some $k \in \{1, \ldots, \ell\}$), which are equal to 0, while the other β_j's are in μ_ℓ, then for every $\sigma \in S_\ell$ we have

$$\text{either } P_\sigma(\beta_1, \ldots, \beta_\ell) = 0, \text{ or } P_\sigma(\beta_1, \ldots, \beta_\ell) = \ell^{\ell-k}. \tag{2.3}$$

In (2.3) we used the convention that $0^0 = 1$.

We will use the following result in our proof of Theorem 1.3.

Lemma 2.3. *If $\beta_i \in \mu_\ell \cup \{0\}$ for each $1 \le i \le \ell$, and at least one β_i is zero, then*

$$0 \le \frac{1}{\ell^\ell} \sum_{\sigma \in S_\ell} P_\sigma(\beta_1, \ldots, \beta_\ell) \le \frac{1}{\ell}.$$

Proof. If the nonzero β_i are not all distinct, then $P_\sigma(\beta_1, \ldots, \beta_\ell) = 0$ for every $\sigma \in S_\ell$ and the lemma is proved in this case. Hence we only need to consider that all nonzero β_i are distinct and k of the β_i's are equal to 0.

Now, assume without loss of generality, that $\beta_1 = \cdots = \beta_k = 0$ (for some $k \in \{1, \ldots, \ell\}$), while $\beta_{k+1}, \ldots, \beta_\ell$ are distinct elements of μ_ℓ. Then there are precisely $k!$ permutations $\sigma \in S_\ell$ such that $P_\sigma(\beta_1, \ldots, \beta_\ell) \neq 0$. Indeed, the value of $\sigma(i)$ for each $i \in \{k+1, \ldots, \ell\}$ is determined by (2.2), while the values $\sigma(i)$ for $i \in \{1, \ldots, k\}$ are arbitrary in the set $\{1, \ldots, \ell\} \setminus \{\sigma(k+1), \ldots, \sigma(\ell)\}$. Thus, using (2.3), we obtain

$$\frac{1}{\ell^\ell} \sum_{\sigma \in S_\ell} P_\sigma(\beta_1, \ldots, \beta_\ell) = \frac{k!}{\ell^k} \le \frac{1}{\ell},$$

as desired. □

We are ready to prove Theorem 1.3.

Proof of Theorem 1.3. Because $\overline{e}$ and r are fixed satisfying (1.1) and (1.2), for the sake of simplifying the notation, we drop the indices r and $\overline{e}$ and denote $g^{\overline{a}}_{r,\overline{e}}(x)$ by

$$g^{\overline{a}}(x) = x^r(x^{e_m s} + a_1 x^{e_{m-1}s} + \cdots + a_{m-1}x^{e_1 s} + a_m).$$

According to [13, Theorem 1.3], the polynomial $g^{\overline{a}}$ permutes $\mathbb{F}_q$ if and only if the following two conditions are satisfied:

(i) $\alpha^{ie_m s} + a_1\alpha^{ie_{m-1}s} + \cdots + a_{m-1}\alpha^{ie_1 s} + a_m \neq 0$, for each $i = 1, \ldots, \ell$;
(ii) $g^{\overline{a}}(\alpha^i)^s \neq g^{\overline{a}}(\alpha^j)^s$, for $1 \leq i < j \leq \ell$.

Using conditions (i) and (ii), and Lemma 2.2, we obtain

$$N^m_{r,\overline{e}}(\ell, q) = \frac{1}{\ell^\ell} \sum_{\substack{\overline{a}\in(\mathbb{F}_q^*)^m \\ \overline{a} \text{ satisfies (i)}}} \sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s\right). \tag{2.4}$$

We note that there are at least

$$\sum_{j=0}^{m-1} (-1)^j \binom{m}{j} q^{m-j-1},$$

and at most

$$\ell \cdot \sum_{j=0}^{m-1} (-1)^j \binom{m}{j} q^{m-j-1}$$

tuples $(a_1, \ldots, a_m) \in (\mathbb{F}_q{}^*)^m$ satisfying at least one of the equations

$$\alpha^{e_m is} + a_1\alpha^{e_{m-1}is} + \cdots + a_{m-1}\alpha^{e_1 is} + a_m = 0,$$

for some $1 \leq i \leq \ell$ (by using the inclusion-exclusion principle). An easy computation shows that

$$\sum_{j=0}^{m-1} (-1)^j \binom{m}{j} q^{m-j-1} = \frac{(q-1)^m - (-1)^m}{q}.$$

Using Lemma 2.3 in the formula (2.4) for each tuple $\overline{a}$ which fails condition (i), we obtain

$$\begin{aligned} & \frac{1}{\ell^\ell} \sum_{\overline{a}\in(\mathbb{F}_q^*)^m} \sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s\right) - \frac{(q-1)^m - (-1)^m}{q} \\ \leq\ & N^m_{r,\overline{e}}(\ell, q) \\ \leq\ & \frac{1}{\ell^\ell} \sum_{\overline{a}\in(\mathbb{F}_q^*)^m} \sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s\right). \end{aligned} \tag{2.5}$$

On the other hand, there are $(q^m - (q-1)^m)$ tuples $(a_1, \ldots, a_m) \in (\mathbb{F}_q)^m$ in which at least one $a_i = 0$. Thus, using Lemma 2.2 in (2.5) for each tuple $\overline{a}$ which has at least one entry equal

to 0, we obtain

$$\begin{aligned}(2.6)\qquad & \frac{1}{\ell^\ell}\sum_{\overline{a}\in\mathbb{F}_q^m}\sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\ldots,g^{\overline{a}}(\alpha^\ell)^s\right) - \frac{(q-1)^m-(-1)^m}{q} - (q^m-(q-1)^m)\\ =\ & \frac{1}{\ell^\ell}\sum_{\overline{a}\in\mathbb{F}_q^m}\sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\ldots,g^{\overline{a}}(\alpha^\ell)^s\right) - \frac{q^{m+1}-(q-1)^{m+1}-(-1)^m}{q}\\ \le\ & N^m_{r,\overline{e}}(\ell,q)\\ \le\ & \frac{1}{\ell^\ell}\sum_{\overline{a}\in\mathbb{F}_q^m}\sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\ldots,g^{\overline{a}}(\alpha^\ell)^s\right).\end{aligned}$$

Now we consider two cases.

Case 1: $m>1$

Let $\beta:=\alpha^s$ be a fixed generator of μ_ℓ. We call a $(m-1)$-tuple $(a_1,\ldots,a_{m-1})\in(\mathbb{F}_q)^{m-1}$ *good* if there is no $1\le i_1<i_2\le\ell$ such that

$$(2.7)\qquad \beta^{i_1e_m}+a_1\beta^{i_1e_{m-1}}+\cdots+a_{m-1}\beta^{i_1e_1}=\beta^{i_2e_m}+a_1\beta^{i_2e_{m-1}}+\cdots+a_{m-1}\beta^{i_2e_1}.$$

We call a $(m-1)$-tuple *bad*, if it is not good. Observe that the number of bad tuples is at least q^{m-2} and at most $\binom{\ell}{2}q^{m-2}$. Indeed, this follows from the fact that for each pair (i_1,i_2) as above,

$$(2.8)\qquad \left(\beta^{i_1e_m},\beta^{i_1e_{m-1}},\ldots,\beta^{i_1e_1}\right)\neq\left(\beta^{i_2e_m},\beta^{i_2e_{m-1}},\ldots,\beta^{i_2e_1}\right),$$

which is true since $(e_1,\cdots,e_m,\ell)=1$. From (2.8) it follows that each equation (2.7) has at most q^{m-2} solutions in $(\mathbb{F}_q)^{m-1}$. There could be no solutions if $\beta^{i_1e_i}=\beta^{i_2e_i}$ for $1\le i\le m-1$, while $\beta^{i_1e_m}\neq\beta^{i_2e_m}$. However, if $i_2-i_1=1$, then (2.7) has precisely q^{m-2} solutions.

An additional application of Lemma 2.2 for each bad tuple $(a_1,\ldots,a_{m-1})$ in (2.6) yields that

$$\begin{aligned}(2.9)\qquad & \frac{1}{\ell^\ell}\sum_{\substack{a_m\in\mathbb{F}_q\\ (a_1,\ldots,a_{m-1})\text{ is good}}}\sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\ldots,g^{\overline{a}}(\alpha^\ell)^s\right) - \frac{q^{m+1}-(q-1)^{m+1}-(-1)^m}{q}\\ \le\ & N^m_{r,\overline{e}}(\ell,q)\\ \le\ & \binom{\ell}{2}q^{m-1}+\frac{1}{\ell^\ell}\sum_{\substack{a_m\in\mathbb{F}_q\\ (a_1,\ldots,a_{m-1})\text{ is good}}}\sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\ldots,g^{\overline{a}}(\alpha^\ell)^s\right).\end{aligned}$$

For a fixed permutation $\sigma\in S_\ell$, and a fixed good tuple $(a_1,\ldots,a_{m-1})$, and a fixed set of numbers $k_1,\ldots,k_\ell\in\{0,\ldots,\ell-1\}$ (not all equal to 0), and for every $a_m\in\mathbb{F}_q$, we let

$$M_{\overline{a},\sigma,\overline{k}}:=\prod_{i=1}^{\ell}\left(\psi(g^{\overline{a}}(\alpha^i)^s)\psi(\alpha^s)^{-\sigma(i)}\right)^{k_i},$$

where $\overline{a}=(a_1,\ldots,a_m)$ and $\overline{k}=(k_1,\ldots,k_\ell)$. We consider the sum $\sum_{a_m\in\mathbb{F}_q}M_{\overline{a},\sigma,\overline{k}}$, where the tuple $(a_1,\ldots,a_{m-1})$ is fixed in the above summation. Using the multiplicitivity of ψ, the sum $\sum_{a_m\in\mathbb{F}_q}M_{\overline{a},\sigma,\overline{k}}$ equals

$$\sum_{a_m\in\mathbb{F}_q}\psi\left(\beta^{\sum_{i=1}^{\ell}(rik_i-\sigma(i)k_i)}\cdot\prod_{i=1}^{\ell}\left(\beta^{e_mi}+a_1\beta^{e_{m-1}i}+\cdots+a_{m-1}\beta^{e_1i}+a_m\right)^{k_is}\right), \tag{2.10}$$

which can be written as a character sum

$$\sum_{a_m\in\mathbb{F}_q}\psi\left(t^s\prod_{i=1}^{\ell}\left(\beta^{e_mi}+a_1\beta^{e_{m-1}i}+\cdots+a_{m-1}\beta^{e_1i}+a_m\right)^{k_is}\right),$$

where $t:=\alpha^{\sum_{i=1}^{\ell}(rik_i-\sigma(i)k_i)}\in\mathbb{F}_q$. Furthermore, using the previously defined character Ψ of $\mathbb{F}_q$ of order ℓ, the sum in (2.10) can be written as

$$\sum_{a_m\in\mathbb{F}_q}\Psi\left(t\prod_{i=1}^{\ell}\left(\beta^{e_mi}+a_1\beta^{e_{m-1}i}+\cdots+a_{m-1}\beta^{e_1i}+a_m\right)^{k_i}\right).$$

Because $(a_1,\dots,a_{m-1})$ is a good tuple, and because $k_i<\ell$ for each i, we obtain that the monic polynomial

$$R_{\overline{k}}^{(a_1,\dots,a_{m-1})}(x):=\prod_{i=1}^{\ell}\left(\beta^{e_mi}+a_1\beta^{e_{m-1}i}+\cdots+a_{m-1}\beta^{e_1i}+x\right)^{k_i}$$

is not an ℓ-th power of another polynomial.

Let $\mathrm{I}(\overline{k}):=\#\{i:\ k_i\neq 0\}$. Using that $(a_1,\dots,a_{m-1})$ is a good tuple, we conclude that $R_{\overline{k}}^{(a_1,\dots,a_{m-1})}$ has $\mathrm{I}(\overline{k})$ distinct roots. Because $R_{\overline{k}}^{(a_1,\dots,a_{m-1})}$ is not an ℓ-th power of another polynomial, we apply Theorem 2.1 and obtain that

$$\left|\sum_{a_m\in\mathbb{F}_q}\Psi\left(t\prod_{i=1}^{\ell}\left(\beta^{e_mi}+a_1\beta^{e_{m-1}i}+\cdots+a_{m-1}\beta^{e_1i}+a_m\right)^{k_i}\right)\right|\le(\mathrm{I}(\overline{k})-1)q^{1/2}. \tag{2.11}$$

For each $\sigma\in S_\ell$, we have

$$\begin{aligned}\sum_{\substack{(a_1,\dots,a_{m-1})\ \text{is good}\\ a_m\in\mathbb{F}_q}} & P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\dots,g^{\overline{a}}(\alpha^\ell)^s\right) \\ =\ & \sum_{(a_1,\dots,a_{m-1})\ \text{is good}}\left(\sum_{a_m\in\mathbb{F}_q}1\right) \\ & +\sum_{(a_1,\dots,a_{m-1})\ \text{is good}}\left(\sum_{\mathrm{I}(\overline{k})\ge 1}\left(\sum_{a_m\in\mathbb{F}_q}M_{\overline{a},\sigma,\overline{k}}\left(g^{\overline{a}}(\alpha^1)^s,\dots,g^{\overline{a}}(\alpha^\ell)^s\right)\right)\right).\end{aligned} \tag{2.12}$$

Using the bounds for the number of bad tuples, we obtain

$$q^m-\binom{\ell}{2}q^{m-1}\le\sum_{(a_1,\dots,a_{m-1})\ \text{is good}}\left(\sum_{a_m\in\mathbb{F}_q}1\right)\le q^m-q^{m-1}. \tag{2.13}$$

On the other hand,

$$\begin{aligned}(2.14)\qquad &\left|\sum_{(a_1,\dots,a_{m-1})\text{ is good}}\left(\sum_{\mathrm{I}(\overline{k})\geq 1}\left(\sum_{a_m\in\mathbb{F}_q} M_{\overline{a},\sigma,\overline{k}}\left(g^{\overline{a}}(\alpha^1)^s,\dots,g^{\overline{a}}(\alpha^\ell)^s\right)\right)\right)\right| \\ &\leq \sum_{(a_1,\dots,a_{m-1})\text{ is good}}\left(\sum_{i=1}^{\ell}\sum_{\mathrm{I}(\overline{k})=i}\left|\sum_{a_m\in\mathbb{F}_q} M_{\overline{a},\sigma,\overline{k}}\left(g^{\overline{a}}(\alpha^1)^s,\dots,g^{\overline{a}}(\alpha^\ell)^s\right)\right|\right),\end{aligned}$$

which by (2.11) is

$$\begin{aligned}&\leq \sum_{(a_1,\dots,a_{m-1})\text{ is good}}\left(\sum_{i=1}^{\ell}\sum_{\mathrm{I}(\overline{k})=i}(i-1)q^{1/2}\right)\\ &\leq \left(q^{m-1}-q^{m-2}\right)\left(\sum_{i=1}^{\ell}(\ell-1)^i\binom{\ell}{i}(i-1)q^{1/2}\right)\\ &\leq (q-1)q^{m-3/2}\left(\sum_{i=1}^{\ell}(\ell-1)^i\binom{\ell}{i}(i-1)\right)\\ &= \left(1+\ell^\ell(\ell-2)\right)(q-1)q^{m-3/2},\end{aligned}$$

where in the above we used the fact that there are $(\ell-1)^i\binom{\ell}{i}$ tuples $\overline{k}\in\{0,\dots,\ell-1\}^\ell$ such that $\mathrm{I}(\overline{k})=i$. Using (2.13) and (2.14) in (2.12) for each permutation $\sigma\in S_\ell$, we obtain

$$\begin{aligned}(2.15)\qquad &q^m-\binom{\ell}{2}q^{m-1}-\left(1+\ell^\ell(\ell-2)\right)(q-1)q^{m-3/2}\\ &\leq \sum_{\substack{(a_1,\dots,a_{m-1})\text{ is good}\\ a_m\in\mathbb{F}_q}} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s,\dots,g^{\overline{a}}(\alpha^\ell)^s\right)\\ &\leq q^m-q^{m-1}+\left(1+\ell^\ell(\ell-2)\right)(q-1)q^{m-3/2}.\end{aligned}$$

Applying (2.15) in (2.9) yields

$$\begin{aligned}(2.16)\qquad &\frac{\ell!}{\ell^\ell}q^m-\frac{\ell!}{\ell^\ell}\left(1+\ell^\ell(\ell-2)\right)(q-1)q^{m-3/2}-\frac{\binom{\ell}{2}\cdot\ell!}{\ell^\ell}q^{m-1}\\ &\quad-\frac{q^{m+1}-(q-1)^{m+1}-(-1)^m}{q}\\ &\leq N^m_{r,\overline{e}}(\ell,q)\\ &\leq \frac{\ell!}{\ell^\ell}q^m+\frac{\ell!}{\ell^\ell}\left(1+\ell^\ell(\ell-2)\right)(q-1)q^{m-3/2}+\left(\binom{\ell}{2}-\frac{\ell!}{\ell^\ell}\right)q^{m-1}.\end{aligned}$$

Case 2: $m=1$

The computation in this case is similar to $m>1$, the only difference is that the bad tuples will not appear in this case. The final result is the following.

$$\frac{\ell!}{\ell^\ell}q - \frac{\ell!}{\ell^\ell}\left(1+\ell^\ell(\ell-2)\right)q^{1/2} - 2 \le N^1_{r,e_1}(\ell,q) \le \frac{\ell!}{\ell^\ell}q + \frac{\ell!}{\ell^\ell}\left(1+\ell^\ell(\ell-2)\right)q^{1/2}. \tag{2.17}$$

Now let

$$C^m_{r,\bar{e}}(\ell,q) := \frac{\frac{\ell^\ell}{\ell!}N^m_{r,\bar{e}}(\ell,q) - q^m}{\ell^{\ell+1}q^{m-1/2}}.$$

Observe that $N^m_{r,\bar{e}}(\ell,2)$ is not well defined, $N^m_{r,\bar{e}}(2,3)=0$, and $N^m_{r,\bar{e}}(3,4)=0$. So $|C^m_{r,\bar{e}}(\ell,q)|<1$ if $q=3$ or 4. So from now on we assume that $q>4$.

From (2.16) and (2.17) we have that for $m>1$,

$$\begin{aligned} & -\left(1-2\ell^{-1}+\ell^{-\ell-1}\right)(q-1)q^{-1} - \frac{\ell-1}{2\ell^\ell}q^{-1/2} - \frac{1}{\ell\cdot\ell!}\frac{q^{m+1}-(q-1)^{m+1}-(-1)^m}{q^{m+1/2}} \\ \le\ & C^m_{r,\bar{e}}(\ell,q) \\ \le\ & \left(1-2\ell^{-1}+\ell^{-\ell-1}\right)(q-1)q^{-1} + \left(\frac{\ell-1}{2\ell!}-\ell^{-\ell-1}\right)q^{-1/2}, \end{aligned}$$

and for $m=1$,

$$-\left(1-2\ell^{-1}+\ell^{-\ell-1}\right) - \frac{2}{\ell\cdot\ell!\cdot q^{1/2}} \le C^1_{r,e_1}(\ell,q) \le 1-2\ell^{-1}+\ell^{-\ell-1}.$$

For $m=1$, it is clear that $\left|C^m_{r,\bar{e}}(\ell,q)\right|<1$ (note that $q>4$).

Now we assume $m>1$. For the upper bound of $C^m_{r,\bar{e}}(\ell,q)$ we obtain

$$\begin{aligned} & \left(1-2\ell^{-1}+\ell^{-\ell-1}\right)\cdot\frac{q-1}{q} + \left(\frac{\ell-1}{2\ell!}-\ell^{-\ell-1}\right)\cdot\frac{1}{q^{1/2}} \\ <\ & 1-\frac{1}{\ell}\cdot\frac{q-1}{q}+\frac{1}{2\ell}\cdot\frac{1}{q^{1/2}} \\ <\ & 1, \end{aligned}$$

as desired (note that $q>4$).

For the lower bound for $C^m_{r,\bar{e}}(\ell,q)$, using that $\ell > e_m \ge m \ge 2$, we first obtain that

$$\begin{aligned} & \frac{1}{\ell\cdot\ell!}\cdot\frac{q^{m+1}-(q-1)^{m+1}-(-1)^m}{q^{m+1/2}} \\ =\ & \frac{1}{\ell\cdot\ell!}\cdot\frac{q^m+q^{m-1}(q-1)+\ldots+(q-1)^m-(-1)^m}{q^{m+1/2}} \\ <\ & \frac{1}{\ell\cdot\ell!}\cdot\frac{m+1}{q^{1/2}} \\ \le\ & \frac{\ell}{\ell\cdot\ell!\cdot q^{1/2}} \\ \le\ & \frac{1}{2\ell\cdot q^{1/2}}. \end{aligned}$$

Similarly, using that $\ell \geq 3$, we get

$$\frac{\ell-1}{2\ell^{\ell}} \cdot q^{-1/2} < \frac{1}{2\ell \cdot q^{1/2}}.$$

Hence

$$\begin{aligned} & -\left(1-2\ell^{-1}+\ell^{-\ell-1}\right)(q-1)q^{-1} - \frac{\ell-1}{2\ell^{\ell}}q^{-1/2} - \frac{1}{\ell\cdot\ell!}\frac{q^{m+1}-(q-1)^{m+1}-(-1)^m}{q^{m+1/2}} \\ > \; & -1+\frac{1}{\ell}\cdot\frac{q-1}{q} - \frac{1}{2\ell\cdot q^{1/2}} - \frac{1}{2\ell\cdot q^{1/2}} \\ = \; & -1+\frac{1}{\ell}\cdot\left(\frac{q-1}{q}-\frac{1}{q^{1/2}}\right) \\ > \; & -1, \end{aligned}$$

as desired (since $q > 4$). □

3. Existence of Permutation Polynomials

Proof of Corollary 1.5. In Theorem 1.3 if $N^m_{r,\bar{e}}(\ell, q) = 0$ then $q < \ell^{2\ell+2}$. □

Using Theorem 1.3 we can easily prove Theorem 1.7.

Proof of Theorem 1.7. We look for a permutation polynomial of the form $g(x) = x^r f(x^s)$ of degree $(q-1-t)$ where

$$f(x) = x^{e_m} + a_1 x^{e_{m-1}} + \cdots + a_{m-1}x^{e_1} + a_m,$$

and $s = (q-1)/\ell$. This means that the degree e_m of f satisfies the equation $r + e_m s = q-1-t$. Note that $s > 1$ because $\ell^{2\ell+2} < q$. Moreover since $t < (\ell - m)s$ and t is coprime with s, we can write t as

$$t = u \cdot s + v,$$

where $0 \leq u < \ell - m$, and $v \in \{1, \ldots, s-1\}$ is coprime with s.

If $m = 1$ we let $r := (\ell - u - 1)s - v$ and $e_m := 1$. Note that $r > 0$ since $r = (\ell-1)s - t$ and $t < (\ell-1)s$. It is clear that these choices for r and e_m satisfy (1.1), (1.2) and $r + e_m s = q-1-t$. Now since $\ell^{2\ell+2} < q$, Corollary 1.5 implies the result in the case $m = 1$.

If $m \geq 2$ we let $r := s - v$ and $e_m := \ell - u - 1$ and choose $(m-1)$-tuple $(e_1, \ldots, e_{m-1})$ such that

$$0 < e_1 < e_2 \cdots < e_{m-1} < e_m$$

and

$$(e_1, \ldots, e_{m-1}, e_m, \ell) = 1. \tag{3.1}$$

Note that $e_m \geq m$ and condition (3.1) is satisfied by various choices for $(e_1, \ldots, e_{m-1})$ such as $e_{m-1} = e_m - 1$, or $e_1 = 1$. It is easy to check that these values for r and $\bar{e} = (e_1, \ldots, e_m)$ satisfy (1.1), (1.2) and $r + e_m s = q - 1 - t$. Since $\ell^{2\ell+2} < q$, Corollary 1.5 establishes the result for $m \geq 2$. □

The following result is an immediate consequence of Theorem 1.7 for $\ell = m+1$ and $t = 1$.

Corollary 3.1. *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 $(q-2)$.*

References

[1] L. Carlitz and C. Wells, *the number of solutions of a special system of equations in a finite field*, Acta Arithmetica **XII** (1966), 77–84.

[2] W. Chu and S. W. Golomb, *Circular Tuscan-k arrays from permutation binomials*, J. Combin. Theory Ser. A **97** (2002), no. 1, 195–202.

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

[4] M. D. Fried, R. Guralnick, J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. Math. **82** (1993), no. 1–3, 157–225.

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

[6] S. Konyagin and F. Pappalardi, *Enumerating permutation polynomials over finite fields by degree. II*, Finite Fields Appl. **12** (2006), no. 1, 27–36.

[7] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. **13** (2007), no. 1, 58–70.

[8] R. Lidl and W. B. Müller, *Permutation polynomials in RSA-cryptosystems*, Advances in Cryptology, Plenum, New York, 1984, 293-301.

[9] 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.

[10] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[11] A. Masuda and M. E. Zieve, *Permutation binomials over finite fields*, Trans. Amer. Math. Soc., to appear.

[12] J. Sun and O. Y. Takeshita, *Interleavers for Turbo codes using permutation polynomials over integer rings*, IEEE Trans. Inform. Theory **51** (2005), no. 1, 101-119.

[13] 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.

[14] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U. S. A. **27** (1941), 345–347.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada

E-mail address: amir.akbary@uleth.ca

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada

E-mail address: dragos.ghioca@uleth.ca

School of Mathematics and Statistics, Carleton University, Ottawa, ON K1S 5B6, Canada

E-mail address: wang@math.carleton.ca