

Cycle structures and parities of linearized permutation polynomials ^{*†}

Huajun Bian[‡], Shaoshi Chen[§] and Dabin Zheng[¶]

October 9, 2026

Abstract.

Linearized permutation polynomials over finite fields have important applications in coding theory, cryptography, and combinatorics. In this paper, we give an explicit description of the cycle structure of a general linearized permutation polynomial in terms of the Jordan blocks of its Dickson matrix, thereby providing a Dickson-matrix formulation of a question raised by Mullen and Vaughan in 1988. Building on the cycle structure, we establish a matrix-theoretic framework to characterize their parity. For finite fields of characteristic 2, we determine all odd linearized permutation polynomials explicitly. For fields of odd characteristic, we derive parity criteria in terms of the eigenvalue structure of the associated Dickson matrix. Based on the parity criteria, we then give an algorithm for deciding the parity of a given linearized permutation polynomial.

Keywords: cycle decomposition; Dickson matrices; linearized permutation polynomials; parity

1 Introduction

Permutation polynomials over finite fields have been extensively studied in the past decades [17, 19], due to their applications in coding theory [9, 15], cryptography [22], finite geometry [3], combinatorial design [8], and many other areas. A permutation polynomial $f(x)$ over a finite field $\mathbb{F}_{q^n}$ is called a *linearized permutation polynomial* if it is of the form

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}, \quad \text{where } a_i \in \mathbb{F}_{q^n}.$$

^{*}H. Bian and S. Chen were partially supported by the Strategic Priority Research Program of the Chinese Academy of Sciences (No. XDB0510201) and the NSFC grants (No. 12271511).

[†]D. Zheng was partially supported by the NSFC grants (No. 62272148).

[‡]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. Email: bianhuajun@amss.ac.cn.

[§]KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China. Email: schen@amss.ac.cn.

[¶]Hubei Province Key Laboratory of Applied Mathematics, Faculty of Mathematics and Statistics, Hubei University, Wuhan 430062, China. Email: dzheng@hubu.edu.cn.

It induces a $\mathbb{F}_q$ -linear map of $\mathbb{F}_{q^n}$, which is viewed as a linear space over $\mathbb{F}_q$. The study of linearized permutation polynomials has been motivated by their appearance as linear maps in the construction of MRD codes [5, 11] and as building blocks in the theory of planar functions [4, 6].

The cycle structure of a permutation polynomial $f(x)$, viewed as a permutation of $\mathbb{F}_{q^n}$, describes the decomposition of $\mathbb{F}_{q^n}$ into orbits under the action of $f(x)$. It determines, in particular, the compositional order and the parity of the induced permutation. Explicit cycle decompositions are known for only a few families. For the simplest case when $f(x)$ is a monomial x^k , the problem reduces to power maps on the cyclic group $\mathbb{F}_{q^n}^*$ as investigated by Ahmad [1]. Mullen and Vaughan determined the cycles of linearized permutation polynomials with coefficients in the base field $\mathbb{F}_q$ [20] in 1988, and inspired several subsequent studies. Lidl and Mullen treated Dickson permutation polynomials [16]. Subsequent studies considered broader families of permutation functions [21], Rédei permutations [2], and permutations whose cycle structures are invariant on suitable affine subspaces [12]. For instance, Zeng et al. in [25] determined the cycle structure of several classes of permutation polynomials over quadratic extensions of finite fields. They subsequently studied the permutation binomials

$$f(x) = \theta x^{2^m+2} + x^{2^{m+1}+1}$$

over $\mathbb{F}_{2^{2m}}$ and obtained their complete cycle structure by analyzing the periods of certain auxiliary sequences [24]. These results illustrate that the cycle decomposition of a sparse permutation polynomial may depend delicately on its parameters and on arithmetic properties of the extension degree.

Linear maps over finite fields have also been studied as finite dynamical systems. Elspas described the cycles of linear sequential networks over prime fields in terms of the elementary divisors of their transition matrices [10]. Hernández Toledo later placed these results in a general framework over arbitrary finite fields, and its periodic behavior can be recovered from the elementary divisors of the associated matrix [13]. For an invertible linear map, the functional graph consists entirely of cycles, so this theory provides a general method for determining its cycle structure.

A more specialized description is available when the coefficients of a linearized permutation polynomial lie in the base field $\mathbb{F}_q$. In this case, f is a polynomial in the Frobenius operator $T : x \mapsto x^q$. Mullen and Vaughan exploited the T -invariant decomposition of $\mathbb{F}_{q^n}$ to determine the cycle structure and to characterize cycle equivalence and strong cycle equivalence for such polynomials [20]. They also raised the question of extending this analysis beyond the base-field coefficient case. In the present paper, we give a formulation that applies to arbitrary linearized permutation polynomials: using the similarity between the induced $\mathbb{F}_q$ -linear transformation and its Dickson matrix, we express the number of cycles of each length explicitly in terms of the Jordan blocks of the Dickson matrix. This provides a Dickson-matrix treatment of the question considered by Mullen and Vaughan.

The parity of the induced permutation is another principal object of this paper. The sign of an algebraically defined permutation may encode nontrivial arithmetic information, as exemplified by Zolotarev's interpretation of the Legendre symbol [26]. Moreover, parity phenomena play an important role in the structural and enumerative theory of Latin squares [14], providing further motivation for studying the parity of permutations over finite fields. Starting from the cycle structure obtained through the Dickson matrix, we derive explicit parity criteria for linearized permutation polynomials. In characteristic two, we determine all odd linearized permutation polynomials. In odd characteristic, we characterize the parity in terms of the multiplicative orders of the eigenvalues of the Dickson matrix and their algebraic multiplicities. We then turn these criteria into algorithms

for deciding whether a given linearized permutation polynomial is even or odd; when all coefficients lie in $\mathbb{F}_q$, the algorithm can be carried out directly in $\mathbb{F}_q[x]/(x^n - 1)$, without explicitly constructing the Dickson matrix.

The structure of this paper is arranged as follows. In Section 2, we recall some basic terminologies and results on linearized permutation polynomials. In Section 3, we derive the cycle-counting formula in terms of the Jordan blocks of the Dickson matrix. In Section 4, we give criteria for determining the parity of a linearized permutation polynomial. In Section 5, we offer an algorithm for testing parity and an illustrative example.

2 Linearized polynomials and Dickson matrices

This section recalls basic terminology about linearized polynomials and Dickson matrices from [17]. Throughout this paper, let q be a power of some prime number p and $\mathbb{F}_q$ be the finite field with q elements. Any polynomial $f(x) \in \mathbb{F}_q[x]$ induces a map from $\mathbb{F}_q$ to $\mathbb{F}_q$ given by $c \mapsto f(c)$. Conversely, every map $\mathbb{F}_q \rightarrow \mathbb{F}_q$ can be represented by a unique polynomial with degree less than or equal to $q - 1$, and two polynomials induce the same map if and only if they are congruent modulo $x^q - x$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* if the induced map is a bijection.

Definition 2.1 (Linearized polynomials). *Let n be a positive integer. A polynomial $f \in \mathbb{F}_{q^n}[x]$ is q -linearized if it has the form*

$$\sum_{i=0}^{n-1} a_i x^{q^i}, \quad \text{where } a_i \in \mathbb{F}_{q^n}. \quad (2.1)$$

Every polynomial of the form (2.1) induces an $\mathbb{F}_q$ -linear map on $\mathbb{F}_{q^n}$; conversely, every such linear map has a unique representation of the form (2.1). Such a polynomial is also called a q -polynomial. If it induces a permutation of $\mathbb{F}_{q^n}$, we call it a q -linearized permutation polynomial.

Example 2.2. $f(x) = x^9 + x^3 - x \in \mathbb{F}_{27}[x]$ is a 3-linearized permutation polynomial of $\mathbb{F}_{27}$.

To each q -polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$, Dickson [7] introduced the associated Dickson matrix

$$D_f = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & a_1^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & a_3^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix}. \quad (2.2)$$

The basic properties of Dickson matrices are summarized in the following theorem.

Theorem 2.3. *Let $f(x)$ be a q -linearized polynomial over $\mathbb{F}_{q^n}$ with its associated Dickson matrix D_f . Then*

- (i) $f(x)$ is a permutation polynomial if and only if D_f is invertible.
- (ii) D_f is $\mathbb{F}_{q^n}$ -similar to the matrix of the $\mathbb{F}_q$ -linear map $f : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_{q^n}$ with respect to any basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Proof. The first assertion was proved by Dickson in his thesis [7] (one can also see [17, page 362]). The second assertion is Lemma 4.1 in [23]. $\square$

Let $A \in GL_n(\mathbb{F}_q)$ be an invertible matrix, since the characteristic polynomial of A splits over a finite extension of $\mathbb{F}_q$, all eigenvalues of A belong to $\mathbb{F}_{q^m}$ for some positive integer m . In particular, the multiplicative order of each eigenvalue is well defined. We define the order set of A by $S(A) := \{\text{ord}(\lambda) : \lambda \text{ is an eigenvalue of } A\}$, where $\text{ord}(\lambda)$ denotes the multiplicative order of λ . We further define the totalized order set of A by $T(A) := \{\text{lcm}(E) : E \subseteq S(A)\}$, where the least common multiple of a finite set of positive integers is defined to be the least common multiple of all elements of it, with the convention that $\text{lcm}(\emptyset) = 1$.

Lemma 2.4. *Every element of $S(A)$ is relatively prime to p . Moreover, $T(A)$ is closed under the least common multiple operation.*

Proof. Let λ be an eigenvalue of A . Since $\lambda \in \mathbb{F}_{q^m}$ for some m , it belongs to the finite cyclic group $\mathbb{F}_{q^m}^\times$, whose order is $q^m - 1$. Hence $\text{ord}(\lambda) \mid (q^m - 1)$. Because $q^m - 1$ is relatively prime to p , every element of $S(A)$ is relatively prime to p .

To prove the second assertion, let $r_1, r_2 \in T(A)$. By definition, there exist subsets $E_1, E_2 \subseteq S(A)$ such that $r_1 = \text{lcm}(E_1)$ and $r_2 = \text{lcm}(E_2)$. Therefore,

$$\text{lcm}(r_1, r_2) = \text{lcm}(\text{lcm}(E_1), \text{lcm}(E_2)) = \text{lcm}(E_1 \cup E_2).$$

Since $E_1 \cup E_2 \subseteq S(A)$, it follows that $\text{lcm}(r_1, r_2) \in T(A)$. Thus $T(A)$ is closed under the least common multiple operation. $\square$

Throughout the paper, we use the notation

$$S := S(D_f) = \{\theta_1, \dots, \theta_s\}$$

and write

$$T := T(D_f)$$

for short. For each $i \in \{1, \dots, s\}$, define

$$u_i := \sum_{\substack{\lambda \text{ is an eigenvalue of } D_f \\ \text{ord}(\lambda) = \theta_i}} \text{mult}_{D_f}(\lambda),$$

where $\text{mult}_{D_f}(\lambda)$ denotes the algebraic multiplicity of λ as an eigenvalue of D_f . We call u_i the order weight of θ_i .

Example 2.5. Let $f(x) = x^9 + x^3 - x \in \mathbb{F}_{27}[x]$. The associated Dickson matrix is

$$D_f = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

The characteristic polynomial is

$$\begin{aligned} \det(\lambda E_3 - D_f) &= \det \begin{pmatrix} 1 + \lambda & -1 & -1 \\ -1 & 1 + \lambda & -1 \\ -1 & -1 & 1 + \lambda \end{pmatrix} \\ &= (\lambda - 1)^3. \end{aligned}$$

Hence D_f has a unique eigenvalue $\lambda = 1$ with algebraic multiplicity 3. The set of distinct orders of eigenvalues of D_f is $\{\theta_1\} = \{1\}$ and the corresponding total algebraic multiplicity is $u_1 = 3$.

3 Cycles of linearized permutation polynomials

In this section, we investigate the cycle structure of a linearized permutation polynomial $f(x)$ over $\mathbb{F}_{q^n}$. By Theorem 2.3, the linear map induced by $f(x)$ is $\mathbb{F}_{q^n}$ -similar to its Dickson matrix D_f . This allows us to translate the cycle-counting problem into a question about the Jordan normal form of D_f over the algebraic closure of $\mathbb{F}_q$.

Let $f(x)$ be a linearized permutation polynomial. For each $a \in \mathbb{F}_{q^n}$, define m_a to be the minimal positive integer such that $f^{(m_a)}(a) = a$, where $f^{(k)}$ denotes the k -th composition of the map induced by $f(x)$. For a positive integer i , we define

$$K_i := \{a \in \mathbb{F}_{q^n} : m_a = i\} \quad \text{and} \quad C_i := \frac{|K_i|}{i},$$

where $|K_i|$ denotes the cardinality of the set K_i . Then C_i counts the number of cycles with length i in the decomposition of f . Since $a \in \mathbb{F}_{q^n}$ is fixed by $f^{(k)}$ if and only if $m_a \mid k$, we have

$$|\{a \in \mathbb{F}_{q^n} : f^{(k)}(a) = a\}| = \sum_{i \mid k} |K_i|. \quad (3.1)$$

On the other hand, since f induces a linear transformation, the map $f^{(k)} - \text{id}$ is also $\mathbb{F}_q$ -linear, and the fixed points set of $f^{(k)}$ is precisely $\ker(f^{(k)} - \text{id})$, which is an $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^n}$ with cardinality $q^{\dim(\ker(f^{(k)} - \text{id}))}$. By Theorem 2.3, the matrix of f is similar to the Dickson matrix D_f , hence the matrix of $f^{(k)} - \text{id}$ is similar to $D_f^k - E_n$, where E_n is the $n \times n$ identity matrix. Combining these observations yields

$$\sum_{i \mid k} |K_i| = q^{\dim(\ker(D_f^k - E_n))}. \quad (3.2)$$

To evaluate the right hand side of (3.2), we analyze the Jordan normal form of $D_f^k - E_n$ over the algebraic closure of $\mathbb{F}_q$. Any square matrix is similar to a block diagonal matrix with each block is of the form $J_t(\lambda) = \lambda E_t + N_t$, where λ is an eigenvalue of D_f and

$$N_t = \begin{pmatrix} 0 & 1 & & \\ & 0 & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}_{t \times t}.$$

Since $\ker(D_f^k - E_n)$ is the direct sum of the kernels of all corresponding Jordan blocks, it suffices to compute the kernel dimension for each block.

Lemma 3.1. *Let $J_t(\lambda) = \lambda E_t + N_t$ be a Jordan block of order t with eigenvalue λ , and p be the characteristic of $\mathbb{F}_q$. For any positive integer k ,*

$$\dim_{\overline{\mathbb{F}_q}}(\ker(J_t(\lambda)^k - E_t)) = \begin{cases} \min(t, p^{v_p(k)}) & \text{if } \lambda^k = 1, \\ 0 & \text{if } \lambda^k \neq 1, \end{cases}$$

where $v_p(k)$ is the p -adic valuation of k , i.e., the largest integer m such that p^m divides k .

Proof. We first consider the case when $\lambda^k \neq 1$. Since the only eigenvalue of $J_t(\lambda)$ is λ , $J_t(\lambda)^k - E_t$ has a unique eigenvalue $\lambda^k - 1 \neq 0$. Thus $J_t(\lambda)^k - E_t$ is invertible and its kernel is trivial.

We next consider the case when $\lambda^k = 1$. Since $N_t^t = 0$ and λE_t commutes with N_t , we have

$$J_t(\lambda)^k - E_t = (\lambda E_t + N_t)^k - E_t = \lambda^k E_t + \sum_{j=1}^{t-1} \binom{k}{j} \lambda^{k-j} N_t^j - E_t = \sum_{j=1}^{t-1} \binom{k}{j} \lambda^{k-j} N_t^j.$$

Thus $J_t(\lambda)^k - E_t$ is strictly upper triangular, with the j -th superdiagonal entries all equal to $\binom{k}{j} \lambda^{k-j}$:

$$J_t(\lambda)^k - E_t = \begin{pmatrix} 0 & \binom{k}{1} \lambda^{k-1} & \binom{k}{2} \lambda^{k-2} & \dots & \binom{k}{t-1} \lambda^{k-t+1} \\ 0 & 0 & \binom{k}{1} \lambda^{k-1} & \dots & \binom{k}{t-2} \lambda^{k-t+2} \\ 0 & 0 & 0 & \ddots & \vdots \\ \vdots & & & \ddots & \binom{k}{1} \lambda^{k-1} \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

By Lucas' theorem on binomial coefficients [18], when $v_p(j) < v_p(k)$, writing

$$k = \sum_{i \geq v_p(k)} k_i p^i, \quad j = \sum_{i \geq v_p(j)} j_i p^i,$$

we obtain

$$\binom{k}{j} \equiv \prod_i \binom{k_i}{j_i} \equiv \binom{0}{j_{v_p(j)}} \prod_{i > v_p(j)} \binom{k_i}{j_i} \equiv 0 \pmod{p},$$

since the digit of k at position $v_p(j)$ is 0, while the digit of j at that position is $j_{v_p(j)} > 0$, forcing $\binom{k_{v_p(j)}}{j_{v_p(j)}} = \binom{0}{j_{v_p(j)}} = 0$. In particular, when $1 \leq j < p^{v_p(k)}$, we have $v_p(j) < v_p(k)$, so

$$\binom{k}{j} \equiv 0 \pmod{p}.$$

For $j = p^{v_p(k)}$, Lucas' theorem gives

$$\binom{k}{j} \equiv \binom{k_{v_p(k)}}{1} \not\equiv 0 \pmod{p}.$$

Thus $j = p^{v_p(k)}$ is the smallest positive integer j for which $\binom{k}{j} \not\equiv 0 \pmod{p}$. If $p^{v_p(k)} < t$, then the leading nonzero superdiagonal is $p^{v_p(k)}$ -th. So the kernel has dimension $p^{v_p(k)}$. If $p^{v_p(k)} \geq t$, then all coefficients $\binom{k}{j}$ are 0 in $\mathbb{F}_q$ for $1 \leq j \leq t-1$, whence $J_t(\lambda)^k - E_t = 0$, and the kernel has dimension t . Combining both cases gives that $\dim \ker(J_t(\lambda)^k - E_t)$ is equal to $\min(t, p^{v_p(k)})$ when $\lambda^k = 1$. $\square$

We are now ready to describe the cycle structure of $f(x)$ as a permutation of $\mathbb{F}_{q^n}$. Recall that each element in T is either 1 or the least common multiple of the orders of some eigenvalues

Theorem 3.2 (Cycle structure). *Let f be a linearized permutation polynomial over $\mathbb{F}_{q^n}$ with Dickson matrix D_f . Let $\mathcal{J}(D_f)$ be the multiset of Jordan blocks of D_f . Then for each positive integer ℓ , the number of cycles of length ℓ in the permutation induced by f on $\mathbb{F}_{q^n}$ is*

$$C_\ell = \frac{1}{\ell} \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) q^{\beta(d)},$$

where μ is the classical Möbius function, and

$$\beta(d) = \sum_{\substack{J_{t_\lambda}(\lambda) \in \mathcal{J}(D_f) \\ \text{ord}(\lambda) | d}} \min(t_\lambda, p^{v_p(d)}),$$

In particular, we have $C_\ell = 0$ unless $\frac{\ell}{p^{v_p(\ell)}} \in T$.

Proof. Lemma 3.1 together with (3.1) gives $\sum_{i|k} |K_i| = q^{\beta(k)}$ for all $k \geq 1$. Setting $F(k) = \sum_{i|k} |K_i|$, the classical Möbius inversion formula yields

$$|K_\ell| = \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) F(d) = \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) q^{\beta(d)},$$

and dividing by ℓ gives $C_\ell = |K_\ell|/\ell$.

When $\frac{\ell}{p^{v_p(\ell)}} \notin T$, Take $\tilde{\ell} = \text{lcm}\{t \in T | t \mid \ell\}$. Since T is the set of least common multiples of subsets of S and $\text{lcm}(\text{lcm}(A), \text{lcm}(B)) = \text{lcm}(A \cup B)$ it follows that $\tilde{\ell} \in T$. In particular this forces $\frac{\ell}{p^{v_p(\ell)}} \neq \tilde{\ell}$. So there exists a prime $p' \neq p$ dividing $\frac{\ell}{\tilde{\ell}}$. Write $e_1 := v_{p'}(\ell)$.

We claim that for every $d \mid \ell$ with $v_{p'}(d) = e_1 - 1$,

$$\beta(d) = \beta(dp'), \quad \mu\left(\frac{\ell}{d}\right) = -\mu\left(\frac{\ell}{dp'}\right).$$

Since $v_{p'}(d) = e_1 - 1$ and $v_{p'}(\ell) = e_1$, we have $v_{p'}(\frac{\ell}{d}) = 1$, so $\frac{\ell}{d} = p' \cdot \frac{\ell}{dp'}$ with $p' \nmid \frac{\ell}{dp'}$. By the multiplicativity of the Möbius function on squarefree arguments,

$$\mu\left(\frac{\ell}{d}\right) = \mu(p') \mu\left(\frac{\ell}{dp'}\right) = -\mu\left(\frac{\ell}{dp'}\right).$$

Since $d \mid dp'$, $\text{ord}(\lambda) \mid d$ implies $\text{ord}(\lambda) \mid dp'$. Conversely, suppose $\text{ord}(\lambda) \mid dp' \mid \ell$. Since $\text{ord}(\lambda) \in T$, we have $\text{ord}(\lambda) \mid \tilde{\ell}$, thus $v_{p'}(\text{ord}(\lambda)) \leq v_{p'}(\tilde{\ell}) < e_1$. So $\text{ord}(\lambda) \mid d$. On the other hand, since $\gcd(p, p') = 1$, $v_p(d) = v_p(dp')$. Hence $\beta(d) = \beta(dp')$. Thus

$$\begin{aligned} |K_\ell| &= \sum_{d|\ell} \mu\left(\frac{\ell}{d}\right) q^{\beta(d)} \\ &= \sum_{\substack{d|\ell \\ v_{p'}(d)=e_1-1}} \mu\left(\frac{\ell}{d}\right) q^{\beta(d)} + \sum_{\substack{d|\ell \\ v_{p'}(d)=e_1}} \mu\left(\frac{\ell}{d}\right) q^{\beta(d)} \\ &= \sum_{\substack{d|\ell \\ v_{p'}(d)=e_1-1}} \left(\mu\left(\frac{\ell}{d}\right) q^{\beta(d)} + \mu\left(\frac{\ell}{dp'}\right) q^{\beta(dp')} \right) \\ &= \sum_{\substack{d|\ell \\ v_{p'}(d)=e_1-1}} \left(\mu\left(\frac{\ell}{d}\right) q^{\beta(d)} - \mu\left(\frac{\ell}{d}\right) q^{\beta(d)} \right) \\ &= 0 \end{aligned}$$

□

Thus Theorem 3.2 may be viewed as the Dickson-matrix form of the general cycle-counting formula for invertible linear finite dynamical systems.

Remark 3.3. Assume that the coefficients of f lie in $\mathbb{F}_q$. Let $T: x \mapsto x^q$ be the Frobenius operator on $\mathbb{F}_{q^n}$. Then there exists a polynomial $\tilde{f} \in \mathbb{F}_q[X]$ such that $f(x) = \tilde{f}(T)(x)$. With respect to a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, the Dickson matrix D_f is the matrix of $\tilde{f}(T)$.

Let g be an irreducible factor of $X^n - 1$, and, for $a \geq 1$, put $W^{(a)} = \ker(g(T)^a)$. The chain $W^{(1)} \subseteq W^{(2)} \subseteq \dots$ stabilizes, define W to be the stable space. The restriction of D_f to the W has eigenvalues $\tilde{f}(\omega)$, where ω runs through the roots of g . These eigenvalues are Galois conjugate and therefore have the same multiplicative order j .

Moreover, [20] gives the fixed-point spaces of f^{jp^a} restricted to W is $\ker(g(T)^{p^a s}) \cap W$, where $g(x)^s \parallel \tilde{f}(x)^j - 1$, its cardinality is $q^{\beta(d)}$, in agreement with Theorem 3.2.

Example 3.4. Let $f(x) = x^9 + x^3 - x \in \mathbb{F}_{27}[x]$. The associated Dickson matrix is

$$D_f = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

The Jordan normal form of D_f is

$$J_{D_f} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Consequently, $\beta(d)$ in Theorem 3.2 is given by

$$\beta(d) = \begin{cases} 2, & \text{if } v_3(d) = 0, \\ 3, & \text{if } v_3(d) \geq 1. \end{cases}$$

By Theorem 3.2, $C_l = 0$ whenever l is not a power of 3. It remains to consider the case $l = 3^i$. For $i = 0$, we have

$$C_1 = 1 \sum_{d|1} \mu\left(\frac{1}{d}\right) 3^{\beta(d)} = 1 \mu(1) 3^{\beta(1)} = 9.$$

For $i \geq 1$, we have

$$C_{3^i} = \frac{1}{3^i} \sum_{d|3^i} \mu\left(\frac{3^i}{d}\right) q^{\beta_d}.$$

Since the only divisors of 3^i contributing nonzero Möbius values are 3^{i-1} and 3^i , we have

$$C_{3^i} = \frac{1}{3^i} \left[\mu(3) q^{\beta_{3^{i-1}}} + \mu(1) q^{\beta_{3^i}} \right] = \frac{1}{3^i} \left(-q^{\beta_{3^{i-1}}} + q^{\beta_{3^i}} \right).$$

Therefore,

$$C_{3^i} = \begin{cases} 6, & \text{if } i = 1, \\ 0, & \text{if } i \geq 2. \end{cases}$$

In summary, the cycle structure of f consists of 6 cycles of length 3 and 9 cycles of length 1.

4 Parity criteria for linearized permutation polynomials

We now apply the argument about cycle structures to determine the parity of the permutations induced by linearized permutation polynomials over $\mathbb{F}_{q^n}$.

We define the parity of a permutation polynomial to be the parity of the permutation it induces on $\mathbb{F}_{q^n}$. Recall that every cycle of length i in the disjoint cycle decomposition of a permutation can be written as a product of $i - 1$ transpositions, for example,

$$(a_1 a_2 \cdots a_i) = (a_1 a_i)(a_1 a_{i-1}) \cdots (a_1 a_2).$$

Hence the permutation induced by a linearized permutation polynomial f decomposes into

$$\sum_{i=1}^{q^n} C_i(i-1) = \sum_{i=1}^{q^n} \frac{|K_i|}{i}(i-1) = q^n - \sum_{i=1}^{q^n} \frac{|K_i|}{i}$$

transpositions. Since $q^n \equiv q \pmod{2}$, the right hand side has the same parity as

$$Par(f) := q + \sum_{i=1}^{q^n} \frac{|K_i|}{i}, \quad (4.1)$$

so it suffices to determine the parity of $Par(f)$.

Theorem 4.1. *Let $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ be a q -linearized permutation polynomial over $\mathbb{F}_{q^n}$, and let D_f denote its associated Dickson matrix, whose distinct eigenvalue orders are $\theta_1, \dots, \theta_s$ with corresponding sums of algebraic multiplicities $u_1, \dots, u_s$, respectively.*

- (i) *If $\text{char}(\mathbb{F}_q) = 2$, then f is an odd permutation if and only if $n = q = 2$ and $f(x) = bx^2$ for some $b \neq 0$.*
- (ii) *If $\text{char}(\mathbb{F}_q) \neq 2$, then the parity of f coincides with the parity of the integer*

$$\sum_{j=1}^s \frac{q^{u_j} - 1}{2^{v_2(\theta_j)}},$$

where $v_2(\theta_j)$ denotes the 2-adic valuation of θ_j .

The proof naturally splits into two cases according to the characteristic of $\mathbb{F}_{q^n}$.

4.1 The case when $\text{char}(\mathbb{F}_{q^n}) = 2$

In this case, q is a power of 2, hence even. Thus the parity of $Par(f)$ is determined by the parity of

$$Par(f) = q + \sum_{i=1}^{q^n} \frac{|K_i|}{i} \equiv \sum_{i=1}^{q^n} \frac{|K_i|}{i} \pmod{2}.$$

By Lemma 2.4, every element of T is odd. Theorem 3.2 gives $K_i = \emptyset$ unless $i = 2^t j$ for some $t \geq 0$ and $j \in T$. Consequently,

$$\sum_{i=1}^{q^n} \frac{|K_i|}{i} \equiv \sum_{t \geq 0} \sum_{j \in T} \frac{|K_{2^t j}|}{2^t j} \equiv \sum_{t \geq 0} \sum_{j \in T} \frac{|K_{2^t j}|}{2^t} \pmod{2}, \quad (4.2)$$

where the second congruence holds since j is odd.

Let m_k denote the number of Jordan blocks of D_f of size at least k , so that $\{m_k\}$ is a non-increasing sequence. Let r be the maximal size of the Jordan blocks of D_f , then $m_1 \geq m_2 \geq \dots \geq m_r > m_{r+1} = 0$. We consider two cases.

Case (i): $r = 1$ (i.e., D_f is diagonalizable).

Here $m_2 = 0$, thus for every even integer i and Jordan block J , $J^i - E$ and $J^{i/2} - E$ has the same rank, thus by (3.1), $K_i = \emptyset$ for all even i . Hence

$$\sum_{i=1}^{q^n} \frac{|K_i|}{i} \equiv \sum_{i \in T} \frac{|K_i|}{i} \equiv \sum_{i \in T} |K_i| \equiv q^n \pmod{2}.$$

and f is an even permutation.

Case (ii): $r > 1$ (i.e., D_f is not diagonalizable).

Let t be the largest integer such that $m_{2^t} > 0$. Expanding (4.2) and we have

$$\begin{aligned} \sum_{t \geq 0} \sum_{i \in T} \frac{|K_{2^t, i}|}{2^t} &= \sum_{i \in T} |K_i| + \sum_{t \geq 1} \sum_{i \in T} \frac{|K_{2^t, i}|}{2^t} \\ &= q^{m_1} + \sum_{j=0}^t \frac{1}{2^{j+1}} (q^{m_1 + \dots + m_{2^{j+1}}} - q^{m_1 + \dots + m_{2^j}}) \\ &\equiv \sum_{j=0}^t \frac{q^{m_1 + \dots + m_{2^j}}}{2^{j+1}} (q^{m_{2^j+1} + m_{2^j+2} + \dots + m_{2^{j+1}}} - 1) \\ &\equiv \sum_{j=0}^{t-1} \frac{q^{m_1 + \dots + m_{2^j}}}{2^{j+1}} + \frac{q^{m_1 + \dots + m_{2^t}}}{2^{t+1}} (q^{m_{2^t+1} + m_{2^t+2} + \dots + m_r} - 1) \pmod{2}. \end{aligned} \quad (4.3)$$

where the last step uses $q \equiv 0 \pmod{2}$, so $q^k - 1 \equiv 1 \pmod{2}$ for all $k \geq 1$.

We claim that for $2 \leq j \leq t-1$, the term $\frac{q^{m_1 + \dots + m_{2^j}}}{2^{j+1}}$ is even. Indeed, since $\{m_i\}$ is non-increasing and $m_{2^t} \geq 1$,

$$m_1 + m_2 + \dots + m_{2^j} \geq 2^j > j+1,$$

and therefore

$$v_2(q^{m_1 + \dots + m_{2^j}}) \geq v_2(2^{m_1 + \dots + m_{2^j}}) = m_1 + \dots + m_{2^j} \geq j+1,$$

so $\frac{q^{m_1 + \dots + m_{2^j}}}{2^{j+1}} \in 2\mathbb{Z}$. Hence (4.3) reduces to

$$\sum_{i=1}^{q^n} \frac{|K_i|}{i} \equiv \frac{q^{m_1}}{2} + \frac{q^{m_1 + m_2}}{4} (1 - \delta_{m_3, 0}) \pmod{2}. \quad (4.4)$$

We further distinguish the following subcases.

- (a) If $q = 2^m$ for some $m > 1$, or if $m_1 > 1$, then $\frac{q^{m_1}}{2}$ is even. Moreover, when $m_3 > 0$, $\frac{q^{m_1 + m_2}}{4}$ is also even. Hence the right-hand side of (4.4) is even and f is an even permutation.

(b) If $q = 2$ and $m_1 = 1$, then since $r > 1$ we have $m_2 = 1$.

- If $m_3 > 0$: the right-hand side of (4.4) equals $\frac{2}{2} + \frac{2^2}{4} = 1 + 1 = 2 \equiv 0 \pmod{2}$, so f is even.
- If $m_3 = 0$: the right-hand side equals $\frac{2}{2} = 1 \equiv 1 \pmod{2}$, so f is odd.

In subcase (b) with $m_3 = 0$, we have $n = q = 2$ and the minimal polynomial of D_f is $(x - a)^2 = x^2 - a^2$ for some $a \neq 0$. Since this is also the minimal polynomial of the induced linear map on $\mathbb{F}_{q^n}$, we have $a^2 \in \mathbb{F}_2$, forcing $a = 1$. Writing

$$D_f = \begin{pmatrix} a_0 & b_0 \\ b_0^2 & a_0^2 \end{pmatrix},$$

its characteristic polynomial is $\chi_{D_f}(x) = x^2 + (a_0 + a_0^2)x + (a_0^3 + b_0^3)$. For $\chi_{D_f}(x) = x^2 + 1$, we need $a_0 + a_0^2 = 0$, i.e. $a_0 \in \mathbb{F}_2$.

- $a_0 = 1$: $f(x) = x$, which is the identity, hence even.
- $a_0 = 0$: $f(x) = b_0x^2$, which induces a single transposition on $\mathbb{F}_4$, hence odd.

Combining all cases, we conclude:

Corollary 4.2. *Let q be a power of 2. A q -linearized permutation polynomial f over $\mathbb{F}_{q^n}$ is an odd permutation if and only if $n = q = 2$ and $f(x) = bx^2$ for some $b \in \mathbb{F}_4^*$.*

4.2 The case when $\text{char}(\mathbb{F}_{q^n}) \neq 2$

In this case, q is odd. Thus, the parity of f is equivalent to the parity of $\text{Par}(f) \equiv 1 + \sum_{i=1}^{q^n} \frac{|K_i|}{i} \pmod{2}$. By Lemma 2.4, every element in T is coprime with p . Moreover, by Theorem 3.2, we have

$$\text{Par}(f) \equiv 1 + \sum_{i \geq 1} \frac{|K_i|}{i} \equiv 1 + \sum_{i \in T} \sum_{j \geq 0} \frac{|K_{p^j \cdot i}|}{p^j \cdot i} \equiv \sum_{i \in T} \frac{\sum_{j \geq 0} |K_{p^j \cdot i} \setminus \{0\}|}{i} \pmod{2}. \quad (4.5)$$

The last identity is because 0 can only appear in K_1 , thus $K_i \setminus \{0\} = K_i$ when $i > 1$ and $|K_1 \setminus \{0\}| = |K_1| - 1$.

Set

$$\Phi: \mathbb{Z} \rightarrow 2^S, \quad i \mapsto \{\theta_j \in S : \theta_j \mid i\}.$$

The key observation is the following.

Lemma 4.3. *For a positive integer i coprime with p , the sum $\sum_{j \geq 0} |K_{p^j \cdot i} \setminus \{0\}|$ depends only on the sequence $\{u_j\}_{1 \leq j \leq s}$ and not on the entries of the Jordan form of D_f off the diagonal.*

Proof. By Theorem 3.2, if $i \notin T$, then $K_{p^j \cdot i}$ is empty for all nonnegative j , so the sum is 0.

Now suppose $i \in T$. Write $\Phi(i) = \{\theta_{k_1}, \dots, \theta_{k_r}\}$. We proceed by induction on the size of $\phi(i)$.

Base case. If $r = 0$, then $i = 1$ and the sum is 0. When $r = 1$, since $i = \theta_1$ is not divisible by other elements in T and K_j is empty when $j > q^n$, we have

$$\sum_{j \geq 0} |K_{p^j \cdot i} \setminus \{0\}| = \left| \bigcup_{j \geq 0} K_{p^j \cdot i} \setminus \{0\} \right| = \left| \bigcup_{j | q^n i} K_j \setminus \{0\} \right| = |\ker(D_f^{q^n \cdot i} - E) \setminus \{0\}| = q^{u_{k_1}} - 1,$$

which depends only on u_{k_1} .

Inductive step. Assume the lemma holds for all positive integers whose index set has cardinality at most $r - 1$ ($r \geq 2$). Since $\gcd(i, p) = 1$, every divisor of $q^n i$ can be written uniquely in the form $p^j t$, where $j \geq 0$ and $t \mid i$. The divisors with $t = i$ are precisely $p^j i$, while the remaining ones correspond to proper divisors $t \mid i$, $t \neq i$. We therefore have

$$\sum_{j \geq 0} |K_{p^j \cdot i} \setminus \{0\}| = \sum_{j | q^n \cdot i} |K_j| - \sum_{t \mid i, t \neq i} \sum_{j \geq 0} |K_{p^j \cdot t}| = q^{u_{k_1} + \dots + u_{k_r}} - \sum_{t \mid i, t \neq i} \sum_{j \geq 0} |K_{p^j \cdot t}|. \quad (4.6)$$

For each $t \mid i$ with $t \neq i$: if $t \notin T$ the inner sum vanishes; if $t \in T$, then $\Phi(t)$ has at most $r - 1$ elements, so the induction hypothesis applies and the inner sum depends only on the $\{u_j\}_{1 \leq j \leq s}$. Hence the entire expression (4.6) depends only on $\{u_j\}$, completing the induction. $\square$

Let D_f^Δ denote a matrix in $M_n(\mathbb{F}_q)$ similar to the diagonal of the Jordan form of D_f , then D_f^Δ induces a permutation of $\mathbb{F}_q^n$. For each $a \in \mathbb{F}_q^n$, define m_a^Δ to be the minimal positive integer such that $D_f^{\Delta m_a}(a) = a$, $K_i^\Delta := \{a \in \mathbb{F}_q^n : m_a^\Delta = i\}$ and $C_i^\Delta = |\frac{K_i^\Delta}{i}|$ be the number cycles with length i . Then $\text{Par}(f) \equiv 1 + \sum_{i \geq 1} \frac{|K_i|}{i} \pmod{2}$. Lemma 3.1 gives $|K_i^\Delta| = 0$ whenever $i \notin T$.

Now we consider the case $i \in T \setminus S$, let $\{\theta_{k_1}, \dots, \theta_{k_r}\}$ denotes $\Phi(i)$. If $\Phi(i) = \emptyset$, $K_i^\Delta = \{0\}$ and $\frac{|K_i \setminus \{0\}|}{i} = 0$ is even. If $\Phi(i)$ is nonempty, since $i = \text{lcm}(\theta_{k_1}, \dots, \theta_{k_r}) \notin S$, we have $r \geq 2$.

Lemma 4.4. *For $i \in T \setminus S$ with $\Phi(i) = \{\theta_{k_1}, \dots, \theta_{k_r}\}$ ($r \geq 2$), write $i = 2^l \cdot t$ with t odd. Then:*

1. $\frac{|K_i^\Delta \setminus \{0\}|}{i} \equiv 0 \pmod{2}$;
2. for each $j \in \{1, 2, \dots, r\}$ with $v_2(\theta_{k_j}) = l$, we have $2^l \mid q^{u_{k_j}} - 1$, moreover

$$\frac{1}{2^l} |K_{\theta_{k_j}}^\Delta \setminus \{0\}| \equiv \frac{1}{2^l} (q^{u_{k_j}} - 1) \pmod{2}.$$

Proof. Since $i \in T$, we have i is the least common multiple of elements in $\Phi(i)$. Among $\theta_{k_1}, \dots, \theta_{k_r}$, at least one achieves the maximum 2-adic valuation $v_2(i)$. Without loss of generality, suppose

$$v_2(\theta_{k_1}) = \dots = v_2(\theta_{k_{r'}}) = v_2(i) \quad \text{and} \quad v_2(\theta_{k_{r'+j}}) < v_2(i) \text{ for } 1 \leq j \leq r - r',$$

where $r' \geq 1$.

We prove (1) and (2) simultaneously by induction on r .

Base case. When $r = 2$, first we prove statement (1). Since $i \notin S$, neither $\theta_{k_1} \mid \theta_{k_2}$ nor $\theta_{k_2} \mid \theta_{k_1}$. The assumption $\theta_j \nmid i$ for $j \notin \{k_1, k_2\}$ ensures $\theta_j \nmid \theta_{k_t}$ for $j \neq k_t$ ($t = 1, 2$), so that

$$|K_{\theta_{k_t}}^\Delta \setminus \{0\}| = \sum_{j \mid \theta_{k_t}} |K_j^\Delta| - 1 = q^{u_{k_t}} - 1, \quad t = 1, 2. \quad (4.7)$$

By the principle of inclusion-exclusion,

$$\begin{aligned}
|K_i^\Delta \setminus \{0\}| &= \sum_{j|i} |K_j^\Delta| - |K_{\theta_{k_1}}^\Delta \setminus \{0\}| - |K_{\theta_{k_2}}^\Delta \setminus \{0\}| - 1 \\
&= q^{u_{k_1} + u_{k_2}} - (q^{u_{k_1}} - 1) - (q^{u_{k_2}} - 1) - 1 \\
&= (q^{u_{k_1}} - 1)(q^{u_{k_2}} - 1).
\end{aligned} \tag{4.8}$$

Since $v_2(\theta_{k_1}) = v_2(i)$,

$$\frac{|K_i^\Delta \setminus \{0\}|}{i} \equiv \frac{(q^{u_{k_1}} - 1)(q^{u_{k_2}} - 1)}{2^{v_2(i)}} = \frac{|K_{\theta_{k_1}}^\Delta|}{2^{v_2(\theta_{k_1})}} \cdot (q^{u_{k_2}} - 1).$$

Since $\frac{|K_{\theta_{k_1}}^\Delta|}{\theta_{k_1}} = C_{\theta_{k_1}}^\Delta \in \mathbb{Z}$, we have $\theta_{k_1} \mid |K_{\theta_{k_1}}^\Delta|$ and in particular $2^{v_2(\theta_{k_1})} \mid |K_{\theta_{k_1}}^\Delta|$. Also q is odd, and $q^{u_{k_2}} - 1$ is even. Hence

$$2 \mid \frac{|K_{\theta_{k_1}}^\Delta|}{2^{v_2(\theta_{k_1})}} \cdot (q^{u_{k_2}} - 1),$$

so $\frac{|K_i^\Delta \setminus \{0\}|}{i}$ is even.

Now we prove statement (2). For $j \in \{1, 2\}$ with $v_2(\theta_{k_j}) = l$, (4.7) gives $|K_{\theta_{k_j}}^\Delta \setminus \{0\}| = q^{u_{k_j}} - 1$. Since $2^l \mid \theta_{k_j} \mid q^{u_{k_j}} - 1$, we have $2^l \mid q^{u_{k_j}} - 1$ and

$$\frac{1}{2^l} |K_{\theta_{k_j}}^\Delta \setminus \{0\}| = \frac{1}{2^l} (q^{u_{k_j}} - 1),$$

so both sides have the same parity. This establishes (2) for $r = 2$.

Inductive step. Suppose both (1) and (2) hold for all integers in $T \setminus S$ with the image of Φ has size less than r . We first prove (2), then use it to prove (1).

To prove (2), it suffices to consider $j = 1$, if $v_2(\theta_{k_j}) < v_2(i)$, then θ_{k_j} divides m for some positive integer m satisfying $|\Phi(m)| < |\Phi(i)|$. Hence, the conclusion follows from the inductive hypothesis. Suppose $\Phi(\theta_{k_1}) = \{\theta_{k_{i_1}}, \theta_{k_{i_2}}, \dots, \theta_{k_{i_a}}\}$ with $1 = i_1 < i_2 < \dots < i_{a'} \leq r' < i_{a'+1} < \dots < i_a$. We induct on a (noting $a < r$).

When $a = 1$, the same argument as the base case gives $|K_{\theta_{k_1}}^\Delta \setminus \{0\}| = q^{u_{k_1}} - 1$, so $2^l \mid \theta_{k_1} \mid q^{u_{k_1}} - 1$ and $\frac{1}{2^l} |K_{\theta_{k_1}}^\Delta \setminus \{0\}| = \frac{1}{2^l} (q^{u_{k_1}} - 1)$, which have the same parity.

Suppose (2) holds for $a - 1$ ($a \geq 2$). By dividing the divisors of θ_1 into three classes, we have

$$\begin{aligned}
\frac{1}{2^l} |K_{\theta_{k_1}}^\Delta \setminus \{0\}| &= \frac{1}{2^l} \left(\sum_{j|\theta_{k_1}} |K_j^\Delta \setminus \{0\}| - \sum_{j|\theta_{k_1}/2} |K_j^\Delta \setminus \{0\}| - \sum_{2^l | j | \theta_{k_1} \ j \neq \theta_{k_1}} |K_j^\Delta \setminus \{0\}| \right) \\
&\equiv \frac{1}{2^l} \left(q^{u_{k_{i_1}} + \dots + u_{k_{i_a}}} - q^{u_{k_{i_{a'+1}}} + \dots + u_{k_{i_a}}} - \sum_{j=2}^{a'} |K_{\theta_{k_{i_j}}}^\Delta \setminus \{0\}| \right) \pmod{2},
\end{aligned}$$

where the last congruence uses the induction hypothesis of (1) (since $|\Phi(\theta_{k_{i_j}})| \leq a < r$ for $j \geq 2$). By the induction hypothesis on a , $\frac{1}{2^l}(q^{u_{k_{i_j}}} - 1)$ is an integer and $\frac{1}{2^l}|K_{\theta_{k_{i_j}}}^\Delta \setminus \{0\}| \equiv \frac{1}{2^l}(q^{u_{k_{i_j}}} - 1) \pmod{2}$ for $j = 2, \dots, a'$. Therefore,

$$\begin{aligned}
\frac{1}{2^l}|K_{\theta_{k_1}}^\Delta \setminus \{0\}| &\equiv \frac{1}{2^l}(q^{u_{k_{i_1}} + \dots + u_{k_{i_{a'}}}} - 1) - \sum_{j=2}^{a'} \frac{1}{2^l}(q^{u_{k_{i_j}}} - 1) \\
&\equiv \frac{1}{2^l} \left((q^{u_{k_{i_1}} + \dots + u_{k_{i_{a'-1}}} - 1) + q^{u_{k_{i_{a'}}}} - 1 \right) - \sum_{j=2}^{a'} \frac{1}{2^l}(q^{u_{k_{i_j}}} - 1) \\
&\equiv \dots \\
&\equiv \sum_{j=1}^{a'} \frac{1}{2^l}(q^{u_{k_{i_j}}} - 1) - \sum_{j=2}^{a'} \frac{1}{2^l}(q^{u_{k_{i_j}}} - 1) \\
&\equiv \frac{1}{2^l}(q^{u_{k_1}} - 1) \pmod{2}.
\end{aligned}$$

Hence by induction on a , $2^l \mid |K_{\theta_{k_1}}^\Delta \setminus \{0\}|$ and $\frac{1}{2^l}|K_{\theta_{k_j}}^\Delta \setminus \{0\}| \equiv \frac{1}{2^l}(q^{u_{k_j}} - 1) \pmod{2}$ for all $j \in [r']$.

Now we look back to (1). By dividing the divisors of i into three classes,

$$\begin{aligned}
\frac{|K_i^\Delta \setminus \{0\}|}{i} &= \frac{1}{i} \left(\sum_{j|i} |K_j \setminus \{0\}| - \sum_{j|2^{l-1}i} |K_j \setminus \{0\}| - \sum_{j=2^l m, m|i, m \neq i} |K_j \setminus \{0\}| \right) \\
&= \frac{1}{i} \left(q^{u_{k_1} + \dots + u_{k_r}} - q^{u_{k_{r'+1}} + \dots + u_{k_r}} - \sum_{j=2^l m, m|i, m \neq i} |K_j \setminus \{0\}| \right),
\end{aligned}$$

where when $l = 1$ the sum over $j \mid 2^{l-1}i$ is defined to be 0. For $j = 2^l m$ with $m \mid i$, $m \neq i$: if $j \notin T$ then $K_j = \emptyset$; if $j \in T$ then $\Phi(j) \subsetneq \Phi(i)$, so $|\Phi(j)| < r$, and by the induction hypothesis on r , $\frac{|K_j \setminus \{0\}|}{j}$ is even. Hence

$$\begin{aligned}
\frac{|K_i \setminus \{0\}|}{i} &\equiv \frac{1}{i} \left(q^{u_{k_{r'+1}} + \dots + u_{k_r}} (q^{u_{k_1} + \dots + u_{k_{r'}}} - 1) - \sum_{j=1}^{r'} |K_{\theta_{k_j}} \setminus \{0\}| \right) \\
&\equiv \frac{1}{2^l} \left(q^{u_{k_{r'+1}} + \dots + u_{k_r}} (q^{u_{k_1} + \dots + u_{k_{r'}}} - 1) - \sum_{j=1}^{r'} |K_{\theta_{k_j}} \setminus \{0\}| \right) \pmod{2}.
\end{aligned}$$

Applying (2), we substitute $|K_{\theta_{k_j}} \setminus \{0\}| \equiv q^{u_{k_j}} - 1 \pmod{2^{l+1}}$ for $j = 1, \dots, r'$, giving

$$\begin{aligned}
\frac{|K_i \setminus \{0\}|}{i} &\equiv \frac{1}{2^l} \left(q^{u_{k_{r'+1}} + \dots + u_{k_r}} (q^{u_{k_1} + \dots + u_{k_{r'}}} - 1) - \sum_{j=1}^{r'} (q^{u_{k_j}} - 1) \right) \pmod{2} \\
&\equiv \frac{1}{2^l} \left(\prod_{j=1}^{r'} (q^{u_{k_j}} - 1 + 1) - 1 - \sum_{j=1}^{r'} (q^{u_{k_j}} - 1) \right) \pmod{2}.
\end{aligned}$$

Setting $x_j = q^{u_{k_j}} - 1$, then each x_j is even with $2^l \mid x_j$.

$$\prod_{j=1}^{r'} (x_j + 1) - 1 - \sum_{j=1}^{r'} x_j = \sum_{\substack{A \subseteq [r'] \\ |A| \geq 2}} \prod_{j \in A} x_j,$$

and each term in the sum is even and divisible by 2^{2l} , so the whole expression is divisible by 2^{l+1} . Therefore

$$\frac{1}{2^l} \left(\prod_{j=1}^{r'} (q^{u_{k_j}} - 1 + 1) - 1 - \sum_{j=1}^{r'} (q^{u_{k_j}} - 1) \right) \equiv 0 \pmod{2},$$

and $\frac{|K_i \setminus \{0\}|}{i}$ is even. This completes the induction and the proof of both (1) and (2). $\square$

Combining Lemma 4.3 and Lemma 4.4, the parity of f equals the parity of

$$1 + \left(\sum_{i=1}^s \frac{q^{u_i} - 1}{2^{v_2(\theta_i)}} - 1 \right) \equiv \sum_{i=1}^s \frac{q^{u_i} - 1}{2^{v_2(\theta_i)}} \pmod{2},$$

which completes the proof of Theorem 4.1.

5 An algorithm for parity testing

Theorem 4.1 provides a practical algorithm to compute the parity of linearized permutation polynomials. In this section we outline algorithms for parity testing without considering larger fields avoids explicitly passing to larger fields.

To evaluate the sum $\sum_{i=1}^s \frac{q^{u_i} - 1}{2^{v_2(\theta_i)}}$ appearing in Theorem 4.1, we choose an odd integer l and integer t satisfies $2^t \cdot l$ divisible by all θ_i and exploit the identity.

Lemma 5.1. *Assume that q is odd. Let $t \geq 0$ and let l be a positive odd integer such that $\chi_{D_f}(X) \mid X^{2^t l} - 1$, where χ_{D_f} denotes the characteristic polynomial of D_f . Define*

$$d_k := \deg \left(\gcd \left(\chi_{D_f}, x^{2^{k_l}} - 1 \right) \right), \quad k = 0, 1, \dots, t.$$

Then

$$\sum_{i=1}^s \frac{q^{u_i} - 1}{2^{v_2(\theta_i)}} \equiv \sum_{k=1}^t \frac{q^{d_k - d_{k-1}} - 1}{2^k} \pmod{2}. \quad (5.1)$$

Proof. Grouping the terms in the sum by the 2-adic valuation of θ_i :

$$\begin{aligned} \sum_{i=1}^s \frac{q^{u_i} - 1}{2^{v_2(\theta_i)}} &= \sum_{j \geq 0} \sum_{v_2(\theta_i)=j} \frac{q^{u_i} - 1}{2^j} \\ &\equiv \sum_{j \geq 0} \frac{q^{\sum_{v_2(\theta_i)=j} u_i} - 1}{2^j} \\ &= q^{d_0} - 1 + \sum_{k=1}^t \frac{q^{d_k - d_{k-1}} - 1}{2^k} \\ &\equiv \sum_{k=1}^t \frac{q^{d_k - d_{k-1}} - 1}{2^k} \pmod{2}. \end{aligned} \quad (5.2)$$

where the second congruence uses $\frac{q^a-1}{2^j} + \frac{q^b-1}{2^j} \equiv \frac{q^{a+b}-1}{2^j} \pmod{2}$ for odd q , and the last step uses q^{d_0} is odd. $\square$

We present the algorithm in full below.

Algorithm 5.2. *Input:* $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_{q^n}[x]$.

Output: f is not a PP, or f is a PP together with its parity.

1. Using the coefficients $a_0, a_1, \dots, a_{n-1}$, construct the Dickson matrix D_f as defined in (2.2).
2. Determine if D_f is invertible. If $\det(D_f) = 0$, return that f is **not** a PP, and the algorithm terminates.
3. Decide whether q is even.
 - If q is even and $q = n = 2$, $f(x) = bx^2$ for some $b \in \mathbb{F}_4^*$, return that f is an odd PP.
 - If q is even and $q \neq 2$ or $n \neq 2$ or $f(x)$ is not of the form bx^2 for any $b \in \mathbb{F}_4^*$, return that f is an even PP.
4. Compute the characteristic polynomial $\chi_{D_f} = \det(xE_n - D_f)$.
5. Compute the order m of χ_{D_f} , i.e., the minimal positive integer m such that $\chi_{D_f}(x) \mid x^m - 1$. Factor $m = 2^t \cdot l$, where l is odd.
6. Compute the degrees

$$d_k := \deg\left(\gcd\left(\chi_{D_f}, x^{2^{k l}} - 1\right)\right), \quad k = 0, \dots, t.$$

7. Compute the sum

$$S = \sum_{k=1}^t \frac{q^{d_k - d_{k-1}} - 1}{2^k}.$$

If S is odd, return that f is an odd PP; otherwise return that f is an even PP.

Now we present an example to illustrate Algorithm 5.2.

Example 5.3. Let $q = n = 5$, and $f(x) = 2x^{625} + x^{125} + 4x^{25} + x^5 + 4x$. The associated Dickson matrix is

$$D_f = \begin{pmatrix} 4^{5^0} & 1^{5^0} & 4^{5^0} & 1^{5^0} & 2^{5^0} \\ 2^5 & 4^5 & 1^5 & 4^5 & 1^5 \\ 4^{5^2} & 2^{5^2} & 4^{5^2} & 1^{5^2} & 4^{5^2} \\ 1^{5^3} & 4^{5^3} & 2^{5^3} & 4^{5^3} & 1^{5^3} \\ 4^{5^4} & 1^{5^4} & 4^{5^4} & 2^{5^4} & 4^{5^4} \end{pmatrix} = \begin{pmatrix} 4 & 1 & 4 & 1 & 2 \\ 2 & 4 & 1 & 4 & 1 \\ 1 & 2 & 4 & 1 & 4 \\ 4 & 1 & 2 & 4 & 1 \\ 1 & 4 & 1 & 2 & 4 \end{pmatrix},$$

This matrix is invertible, so f is a permutation polynomial of $\mathbb{F}_{5^5}$. Since $q = 5$ is odd, we determine the parity using Algorithm 5.2. The characteristic polynomial is $\chi_{D_f}(x) = x^5 + 3$, with order $m = 20 = 2^2 \cdot 5$; thus $t = 2$ and $l = 5$. The degrees $d_1 = \deg \gcd(\chi_{D_f}, x^5 - 1) = 0$ and $d_2 = \deg \gcd(\chi_{D_f}, x^{20} - 1) = 5$ give

$$S = \frac{q^{d_1 - d_0} - 1}{2} + \frac{q^{d_2 - d_1} - 1}{4} = \frac{5^{0-0} - 1}{2} + \frac{5^{5-0} - 1}{4} = 781,$$

which is odd. Hence f is an odd permutation polynomial of $\mathbb{F}_{5^5}$.

When the linearized polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i}$ has all coefficients in the base field $\mathbb{F}_q$, the Dickson matrix D_f is a polynomial in the companion matrix

$$J := \begin{pmatrix} 0 & E_{n-1} \\ 1 & 0 \end{pmatrix}$$

with coefficients $a_0, \dots, a_{n-1}$. Since the eigenvalues of J are the n -th roots of unity $\omega_1, \dots, \omega_n$ in $\overline{\mathbb{F}_q}$, the eigenvalues of D_f are $g(\omega_i)$ for $i = 1, \dots, n$, where $g(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q[x]$ is the associated polynomial of f . Consequently, the characteristic polynomial χ_{D_f} and all subsequent GCD computations reduce to polynomial arithmetic in $\mathbb{F}_q[x]/(x^n - 1)$, yielding the following simplified algorithm.

Algorithm 5.4. *Input:* $f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \in \mathbb{F}_q[x]$, a linearized polynomial over $\mathbb{F}_{q^n}$.

Output: f is not a PP, or f is a PP together with its parity.

1. Construct the associate polynomial $g(x) = a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \in \mathbb{F}_q[x]$.
2. Determine if $g(x)$ and $x^n - 1$ are coprime. If $\gcd(g(x), x^n - 1) \neq 1$, return 0 and the algorithm terminates (i.e., f is not a PP).
3. Decide whether q is even.
 - If q is even and $q = n = 2$, $f(x) = bx^2$ for some $b \in \mathbb{F}_4^*$, return that f is an odd PP.
 - If q is even and $q \neq 2$, $n \neq 2$ or $f(x)$ is not of the form bx^2 for any $b \in \mathbb{F}_4^*$, return that f is an even PP.
4. Compute the minimal positive integer m such that $x^n - 1 \mid g(x)^m - 1$. Factor $m = 2^t \cdot l$, where l is odd.
5. Compute the degrees

$$d_k := \deg\left(\gcd\left(x^n - 1, g(x)^{2^{kl}} - 1\right)\right), \quad k = 0, \dots, t.$$

6. Compute the sum

$$S = \sum_{k=1}^t \frac{q^{d_k - d_{k-1}} - 1}{2^k}.$$

If S is odd, return that f is an odd PP; otherwise return that f is an even PP.

Now we test the parity of $f(x)$ in Example 5.3 again for illustrating Algorithm 5.4

Example 5.5. Let $q = 5$ and $f(x) = 4x + x^5 + 4x^{25} + x^{125} + 2x^{625} \in \mathbb{F}_5[x]$. We test the parity of f using Algorithm 5.4. The associated polynomial is $g(x) = 4 + x + 4x^2 + x^3 + 2x^4 \in \mathbb{F}_5[x]$, and $\gcd(g(x), x^5 - 1) = 1$, so f is a permutation polynomial of $\mathbb{F}_{5^5}$. Since $q = 5$ is odd, we proceed. The minimal positive integer m satisfying $x^5 - 1 \mid g(x)^m - 1$ in $\mathbb{F}_5[x]/(x^5 - 1)$ is $m = 20 = 2^2 \cdot 5$, so $t = 2$ and $l = 5$. Computing $d_1 = \deg \gcd(x^5 - 1, g(x)^{10} - 1) = 0$ and $d_2 = \deg \gcd(x^5 - 1, g(x)^{20} - 1) = 5$, we obtain

$$S = \frac{5^{d_1 - d_0} - 1}{2} + \frac{5^{d_2 - d_1} - 1}{4} = \frac{5^0 - 1}{2} + \frac{5^5 - 1}{4} = 0 + 781 = 781,$$

which is odd. Hence f is an odd permutation polynomial of $\mathbb{F}_{5^5}$, consistent with the result obtained in Example 5.3

Remark 5.6. When the coefficients of f are restricted to $\mathbb{F}_q$, Algorithm 5.4 can be recovered relatively easily from the cycle structure analysis of linearized permutation polynomials over $\mathbb{F}_{q^n}$ established by Mullen and Vaughan [20] and may thus be viewed as a direct application of their results.

6 Conclusion

In this paper, we present results on the cycle structure and parity of linearized permutation polynomials over finite fields using Dickson matrices. Building on the cycle structure, Theorem 4.1 gives a complete parity criterion for a linearized permutation polynomial. In characteristic two, a q -linearized permutation polynomial over $\mathbb{F}_{q^n}$ is odd precisely when $q = n = 2$ and $f(x) = bx^2$ with $b \in \mathbb{F}_4^*$. In odd characteristic, its parity is determined by the multiplicative orders of the eigenvalues of the Dickson matrix and their total algebraic multiplicities. This criterion also leads to an algorithm for the parity testing. It would be interesting to extend the method in this work to other class of permutation polynomials, as the work on Dickson polynomials [16].

7 Declaration on the Use of AI

The results of this paper, including all mathematical derivations and proofs, were conceived, developed, and verified by the authors. During the preparation of this manuscript, AI-assisted tools were used to help draft the Introduction and to improve the clarity and readability of the language throughout the paper. No mathematical reasoning, proof steps, or conclusions were generated by these tools. All changes suggested with AI assistance were reviewed by the authors, who take full responsibility for the content of this work.

References

- [1] Shair Ahmad. Cycle structure of automorphisms of finite cyclic groups. *J. Combinatorial Theory*, 6:370–374, 1969.
- [2] Juliane Capaverde, Ariane M. Masuda, and Virgínia M. Rodrigues. Rédei permutations with the same cycle structure. *Finite Fields Appl.*, 81:Paper No. 102046, 24, 2022.
- [3] Yunwen Chi, Kangquan Li, and Longjiang Qu. Constructing rotatable permutations of $\mathbb{F}_{2^m}^3$ with 3-homogeneous functions. *Adv. Math. Commun.*, 19(3):872–890, 2025.
- [4] Robert S. Coulter and Rex W. Matthews. Planar functions and planes of Lenz-Barlotti class II. *Des. Codes Cryptogr.*, 10(2):167–184, 1997.
- [5] Ph. Delsarte. Bilinear forms over a finite field, with applications to coding theory. *J. Combin. Theory Ser. A*, 25(3):226–241, 1978.
- [6] Peter Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2 . *Math. Z.*, 103:239–258, 1968.

- [7] Leonard Eugene Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Annals of Mathematics*, 11(1/6):65–120, 1896.
- [8] Cunsheng Ding and Jin Yuan. A family of skew Hadamard difference sets. *J. Combin. Theory Ser. A*, 113(7):1526–1535, 2006.
- [9] Cunsheng Ding and Zhengchun Zhou. Binary cyclic codes from explicit polynomials over $\text{GF}(2^m)$. *Discrete Math.*, 321:76–89, 2014.
- [10] Bernard Elspas. The theory of autonomous linear sequential networks. *IRE Transactions on Circuit Theory*, 6(1):45–60, 1959.
- [11] È.Ì. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.
- [12] Daniel Gèrike and Gohar M. Kyureghyan. Permutations on finite fields with invariant cycle structure on lines. *Des. Codes Cryptogr.*, 88(9):1723–1740, 2020.
- [13] René A. Hernández Toledo. Linear finite dynamical systems. *Communications in Algebra*, 33(9):2977–2989, 2005.
- [14] Jeannette C. M. Janssen. On even and odd Latin squares. *J. Combin. Theory Ser. A*, 69(1):173–181, 1995.
- [15] Yann Laigle-Chapuy. Permutation polynomials and applications to coding theory. *Finite Fields Appl.*, 13(1):58–70, 2007.
- [16] Rudolf Lidl and Gary L. Mullen. Cycle structure of Dickson permutation polynomials. *Math. J. Okayama Univ.*, 33:1–11, 1991.
- [17] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
- [18] E. Lucas. Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques suivant un module premier. *Bulletin de la Société Mathématique de France*, 6:49–54, 1878.
- [19] Gary L. Mullen and Carl Mummert. *Finite fields and applications*, volume 41 of *Student Mathematical Library*. American Mathematical Society, Providence, RI; Mathematics Advanced Study Semesters, University Park, PA, 2007.
- [20] Gary L. Mullen and Theresa P. Vaughan. Cycles of linear permutations over a finite field. *Linear Algebra Appl.*, 108:63–82, 1988.
- [21] Amin Sakzad, Mohammad-Reza Sadeghi, and Daniel Panario. Cycle structure of permutation functions over finite fields and their applications. *Adv. Math. Commun.*, 6(3):347–361, 2012.
- [22] Rajesh P. Singh, Bhaba K. Sarma, and Anupam Saikia. A public key cryptosystem using a group of permutation polynomials. *Tatra Mt. Math. Publ.*, 77:139–162, 2020.

- [23] Baofeng Wu and Zhuojun Liu. Linearized polynomials over finite fields revisited. *Finite Fields Appl.*, 22:79–100, 2013.
- [24] Dan Zeng, Yunge Xu, Lisha Li, Xianping Liu, and Xiangyong Zeng. The cycle structure of a class of permutation binomials. *Discrete Math.*, 349(2):Paper No. 114740, 20, 2026.
- [25] Dan Zeng, Xiangyong Zeng, Lisha Li, and Yunge Xu. The cycle structure of a class of permutation polynomials. *Des. Codes Cryptogr.*, 91(4):1373–1400, 2023.
- [26] Zolotareff. Nouvelle démonstration de la loi de réciprocité de legendre. *Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale*, 11:354–362, 1872.