Available online at www.sciencedirect.com
SCIENCE DIRECT®
Finite Fields and Their Applications 10 (2004) 72–96
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Enumerating permutation polynomials II: k-cycles with minimal degree

Claudia Malvenuto[a] and Francesco Pappalardi[b,*]

[a] *Dipartimento di Informatica, Università degli studi "La Sapienza", Via Salaria, 113, I-00198 Roma, Italy*
[b] *Dipartimento di Matematica, Università degli studi Roma Tre, Largo S. L. Murialdo, 1, I-00146 Roma, Italy*

Received 26 November 2002; revised 22 June 2003; accepted 24 June 2003

Communicated by Daqing Wan

Abstract

We consider the function $m_{[k]}(q)$ that counts the number of cycle permutations of a finite field $\mathbb{F}_q$ of fixed length k such that their permutation polynomial has the smallest possible degree. We prove the upper-bound $m_{[k]}(q) \leqslant (k-1)!(q(q-1))/k$ for $\mathrm{char}(\mathbb{F}_q) > e^{(k-3)/e}$ and the lower-bound $m_{[k]}(q) \geqslant \varphi(k)(q(q-1))/k$ for $q \equiv 1 \pmod k$. This is done by establishing a connection with the $\mathbb{F}_q$-solutions of a system of equations $\mathscr{A}_k$ defined over $\mathbb{Z}$. As example, we give complete formulas for $m_{[k]}(q)$ when $k = 4, 5$ and partial formulas for $k = 6$. Finally, we analyze the Galois structure of the algebraic set $\mathscr{A}_k$.

1. Introduction

Let q be a power of a prime and denote with $\mathbb{F}_q$ the finite field with q elements. If σ is a permutation of the elements of $\mathbb{F}_q$, then one can associate to σ the polynomial in $\mathbb{F}_q[x]$

$$f_\sigma(x) = \sum_{c \in \mathbb{F}_q} \sigma(c)(1 - (x-c)^{q-1}). \tag{1}$$

*Corresponding author. Fax: 39-6548-88080.
E-mail addresses: claudia@dsi.uniroma1.it (C. Malvenuto), pappa@mat.uniroma3.it (F. Pappalardi).

1071-5797/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/S1071-5797(03)00044-3

Such a polynomial has the property that

1. $f_\sigma(b) = \sigma(b)$ for all $b \in \mathbb{F}_q$,
2. The degree $\partial(f_\sigma) \leqslant q-2$ (since the sum of all the elements of $\mathbb{F}_q$ is zero).

f_σ is the unique polynomial in $\mathbb{F}_q$ with these two properties and it is called the *permutation polynomial of* σ.

Permutation polynomials have increasingly attracted the attention of various researchers in the past couple of decades. We suggest the inspiring survey papers by Rudolf Lidl and Gary Mullen [11,5,6] for an introduction to the subject.

Various cryptographic applications, including a key exchange protocol for public key cryptography based on permutation polynomials have been proposed (see [4,7]).

In their paper of 1988, Rudolf Lidl and Gary Mullen [5] discuss a number of open problems regarding permutation polynomials. Among these, problem P6 asks to determine the number $N_d(q)$ of permutation polynomials of degree d where $1 \leqslant d \leqslant q-2$ and $d \nmid q-1$. This seems to be a difficult problem at the moment. Some partial results were given by Wells [12]. We will state his results later. See also the paper of Sergey Konyagin and the second author [3] and the results by Pinaki Das [1].

For a given permutation σ of $\mathbb{F}_q$, let us denote by S_σ the set of elements of $\mathbb{F}_q$ that are moved by σ. Note that if σ and σ' are conjugated, then $\#S_\sigma = \#S_{\sigma'}$.

If σ is not the identity we have that $\partial(f_\sigma) \geqslant q - \#S_\sigma$. To see this it is enough to note that the polynomial $f_\sigma(x) - x$ has as roots all the elements of $\mathbb{F}_q$ which are not in S_σ. Therefore, if not identically zero, f_σ has to have degree at least $q - \#S_\sigma$.

Let $\mathscr{C}$ be a conjugation class of permutations of a finite field $\mathbb{F}_q$ and $c(\mathscr{C})$ the number of elements of $\mathbb{F}_q$ moved by any permutation in $\mathscr{C}$ (that is: $c(\mathscr{C}) = \#S_\sigma$ for any $\sigma \in \mathscr{C}$). As we just noticed, for any $\sigma \in \mathscr{C}$,

$$q - 2 \geqslant \partial(f_\sigma) \geqslant q - c(\mathscr{C}). \tag{2}$$

An immediate consequence is that all transpositions have polynomials with degree $q-2$ while the degree of a 3-cycle can be $q-2$ or $q-3$.

In the first paper of this series [9] we dealt with the problem of determining $l_{\mathscr{C}}(\mathbb{F}_q)$, defined as the number of permutation polynomials associated to permutations in the class $\mathscr{C}$ whose degree is strictly less then $q-2$. There we obtained a number of formulas and estimates. For classes of permutations that move up to 6 elements we have computed closed formulas for $l_{\mathscr{C}}(\mathbb{F}_q)$. These results extend those of Wells.

In this paper we consider

$$M_{\mathscr{C}}(\mathbb{F}_q) = \{\sigma \in \mathscr{C} \mid \partial(f_\sigma) = q - \#S_\sigma\}$$

(i.e. the permutations in $\mathscr{C}$ for which the permutation polynomial has the minimum possible degree $q - c(\mathscr{C})$) and set $m_{\mathscr{C}}(q) = \#M_{\mathscr{C}}(\mathbb{F}_q)$.

Let us also denote by $[k]$ the class consisting of all the k-cycle permutations of $\mathbb{F}_q$.

Theorem 1.1. *Let φ be the Euler totient function. If $q \equiv 1 \pmod{k}$ then*

$$m_{[k]}(q) \geqslant \frac{\varphi(k)}{k} q(q-1).$$

Next, we will show the upper bound:

Theorem 1.2. *Suppose* $\mathrm{char}(\mathbb{F}_q) > e^{(k-3)/e}$. *Then*

$$m_{[k]}(q) \leqslant \frac{(k-1)!}{k} q(q-1).$$

The hypothesis $\mathrm{char}(\mathbb{F}_q) > e^{(k-3)/e}$ in Theorem 1.2 rules out the interesting case when k has approximately the same size as q. Our proof breaks down for these values of k. However, we are convinced that the upper bound for $m_{[k]}(q)$ holds for any value of $k < q$.

In general, if $\mathscr{C}$ is any conjugation class of permutations then an analogous upper bound as the one in Theorem 1.2 can be proved for $m_{\mathscr{C}}(q)$. In some cases the bounds are stronger. We have decided to restrict ourselves to the case of cycle permutations.

We will prove Theorem 1.2 in Section 3, Theorem 1.1 in Section 4. Section 5 is dedicated to examples. We will consider k-cycles ($k = 3, 4, 5, 6$) and give detailed description of $m_{[k]}(q)$ in these special cases.

2. Reduction to normalized permutations

A permutation σ of $\mathbb{F}_q$ is said to be *normalized*[1] if $\sigma(0) = 1$. We denote by $N_{\mathscr{C}}(\mathbb{F}_q)$ the set of normalized permutations of $\mathscr{C}$ that have (minimal) degree $q - c(\mathscr{C})$ and we set $n_{\mathscr{C}}(q) = \#N_{\mathscr{C}}(\mathbb{F}_q)$.

Proposition 2.1. *With the above notations we have*

$$m_{\mathscr{C}}(q) = \frac{1}{c(\mathscr{C})} q(q-1) n_{\mathscr{C}}(q).$$

Hence if $m_{\mathscr{C}}(q) \neq 0$, then

$$m_{\mathscr{C}}(q) \geqslant \frac{1}{c(\mathscr{C})} q(q-1).$$

[1] The definition of *normalized permutation* is different from the usual one where a permutation polynomial $f(x) \in \mathbb{F}_q[x]$ is said normalized if it is monic, if $f(0) = 0$ and if the coefficient of x^{n-1} is 0 when the degree n of f is not divisible by the characteristic p.

Proof. Let $\mathbb{A}^1(\mathbb{F}_q)$ be the group of affine transformations of $\mathbb{F}_q$, that is the group of applications

$$L_{a,b} : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto ax + b.$$

It is clear that $\#\mathbb{A}^1(\mathbb{F}_q) = q(q-1)$.

Consider the map

$$\Pi : \mathbb{A}^1(\mathbb{F}_q) \times N_{\mathscr{C}}(\mathbb{F}_q) \to M_{\mathscr{C}}(\mathbb{F}_q),$$

$$(L_{a,b}, \sigma) \mapsto (L_{a,b}^{-1} \sigma L_{a,b}).$$

Clearly Π is well defined since

$$\partial((L_{a,b}^{-1} f_\sigma L_{a,b}(x)) = \partial(a^{-1}(f(ax+b) - b)) = \partial(f_\sigma).$$

Furthermore Π is surjective. This follows from the fact that, given $\tau \in M_{\mathscr{C}}(\mathbb{F}_q)$, chosen $b \in S_\tau$ and set $a = \tau(b) - b$, we have that $L_{a,b}^{-1} \tau L_{a,b}$ is normalized and therefore

$$\tau = \Pi(L_{a,b}^{-1}, L_{a,b}^{-1} \tau L_{a,b}).$$

To complete the proof we need to show that for every $\tau \in M_{\mathscr{C}}(\mathbb{F}_q)$, the fibre $\Pi^{-1}(\tau)$ has exactly $c(\mathscr{C})$ elements. Indeed, consider the map

$$\Sigma : S_\tau \to \Pi^{-1}(\tau),$$

$$b \mapsto (L_{a,b}^{-1}, L_{a,b}^{-1} \tau L_{a,b}),$$

where $a = \tau(b) - b$. It is clear that Σ is well defined and injective. Furthermore, Σ is also surjective since if $(L_{c,d}, \sigma) \in \Pi^{-1}(\tau)$, then

$$\tau(-d/c) = L_{c,d}^{-1} \sigma L_{c,d}(-d/c) = L_{c,d}^{-1} \sigma(0) = (1-d)/c.$$

Therefore $-d/c \in S_\tau$, $1/c = \tau(-d/c) - (-d/c)$ and

$$\Sigma(-d/c) = (L_{c,d}, \sigma).$$

Finally $\#\Pi^{-1}(\tau) = \#S_\tau = c(\mathscr{C})$ and this concludes the proof. □

Remark. The previous proposition allows us to reduce the problem of computing $m_{\mathscr{C}}(\mathbb{F}_q)$ to the easier one of computing $n_{\mathscr{C}}(\mathbb{F}_q)$. Indeed since $c([k]) = k$, Theorem 1.2 is equivalent to $n_{[k]}(\mathbb{F}_q) \leqslant (k-1)!$ and Theorem 1.1 is equivalent to $n_{[k]}(\mathbb{F}_q) \geqslant \varphi(k)$ for $q \equiv 1 \pmod{k}$.

3. From normalized permutation polynomials to affine algebraic sets. Proof of Theorem 1.2

Let us write

$$f_\sigma(x) = A_{q-1} + A_{q-2}x + \cdots + A_1 x^{q-2}.$$

From definition (1) it follows that for every $i = 1, \ldots, q-2$,

$$A_i = A_i(\sigma) = (-1)^{i+1}\binom{q-1}{i}\sum_{c\in\mathbb{F}_q}\sigma(c)c^i.$$

It is well known (see for example [8, Exercise 7.1]) that for $0 \leqslant i \leqslant q-1$, $(-1)^{i+1}\binom{q-1}{i} = -1$ in $\mathbb{F}_q$. Furthermore using the identity (see for example [8, Lemma 6.3]),

$$\sum_{c\in\mathbb{F}_q} c^{i+1} = 0$$

for $i < q-2$, we deduce that

$$A_i(\sigma) = \sum_{c\in\mathbb{F}_q} c^i(c-\sigma(c)) = \sum_{c\in S_\sigma} c^i(c-\sigma(c)).$$

From these observations it follows that

$$m_{\mathscr{C}}(q) = \#\left\{\sigma\in\mathscr{C} \text{ such that } \sum_{c\in S_\sigma} c^i(c-\sigma(c)) = 0 \text{ for } i = 1, \ldots, c(\mathscr{C})-2\right\}.$$

Let us now specialize to the case when σ is a normalized k-cycle:

$$\sigma = (0, 1, a_1, a_2, \ldots, a_{k-2}).$$

In this case

$$A_i(\sigma) = (1-a_1) + a_1^i(a_1-a_2) + \cdots + a_{k-3}^i(a_{k-3}-a_{k-2}) + a_{k-2}^{i+1}.$$

For $i = 1, \ldots, k-2$, define the polynomial with integer coefficients:

$$G_i(x_1, \ldots, x_{k-2}) = 1 - x_1 + \sum_{j=1}^{k-3} x_j^i(x_j - x_{j+1}) + x_{k-2}^{i+1} \in \mathbb{Z}[x_1, \ldots, x_{k-2}]. \tag{3}$$

The degree $\partial(f_\sigma) = q - \#S_\sigma$ if and only if

$$A_1(\sigma) = \cdots = A_{k-2}(\sigma) = 0.$$

Therefore

$$n_{[k]}(q) = \#\left\{ \underline{x} \in (\mathbb{F}_q \backslash \{0,1\})^{k-2} \quad \begin{array}{l} \text{such that } G_1(\underline{x}) = \cdots = G_{k-2}(\underline{x}) = 0 \\ \text{and all the components of } \underline{x} \text{ are distinct} \end{array} \right\}.$$

We are naturally lead to consider the affine algebraic set $\mathscr{A}_k$ in $\mathbb{A}^{k-2}$ defined by the equations:

$$\mathscr{A}_k: \begin{cases} (1-x_1) + x_1(x_1 - x_2) + \cdots + x_{k-3}(x_{k-3} - x_{k-2}) + x_{k-2}^2 &= 0, \\ (1-x_1) + x_1^2(x_1 - x_2) + \cdots + x_{k-3}^2(x_{k-3} - x_{k-2}) + x_{k-2}^3 &= 0, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots & \\ (1-x_1) + x_1^{k-2}(x_1 - x_2) + \cdots + x_{k-3}^{k-2}(x_{k-3} - x_{k-2}) + x_{k-2}^{k-1} &= 0. \end{cases} \tag{4}$$

Clearly $\mathscr{A}_k$ is defined over $\mathbb{Z}$ and therefore over any field.

We can also write that

$$n_{[k]}(q) = \#\{\underline{x} \in \mathscr{A}_k(\mathbb{F}_q) \text{ with components not in } \{0,1\} \text{ and all distinct}\}. \tag{5}$$

Theorem 3.1. *Let* $\mathbf{K}$ *be any algebraic closed field and* $k \in \mathbb{N}$ *be an integer such that either* $\mathrm{char}(\mathbf{K}) = 0$ *or* $\mathrm{char}(\mathbf{K}) > e^{(k-3)/e}$. *Then we have that the algebraic variety dimension*

$$\dim_{\mathbf{K}}(\mathscr{A}_k) = 0.$$

Remark. Note that the hypothesis $\mathrm{char}(\mathbf{K}) > e^{(k-3)/e}$ is not redundant. In fact it can be seen that, if $p = \mathrm{char}(\mathbf{K})$ is fixed, then

$$\lim_{k \to \infty} \dim_{\mathbf{K}}(\mathscr{A}_k) = +\infty.$$

Corollary 3.1. *Let* $\mathbf{K}$ *be any algebraic closed field and* $k \in \mathbb{N}$ *be an integer such that either* $\mathrm{char}(\mathbf{K}) = 0$ *or* $\mathrm{char}(\mathbf{K}) > e^{(k-3)/e}$. *Then*

$$\#\mathscr{A}_k(\mathbf{K}) = (k-1)!$$

where the points are counted with multiplicity.

Proof. We apply the Theorem of Bézout (see for example the book of Harris [2]) which states that if $k-2$ hypersurfaces in $\mathbb{P}^{k-2}(\bar{\mathbf{K}})$ do intersect in a zero-dimensional subvariety of $\mathbb{P}^{k-2}(\bar{\mathbf{K}})$, then the number of points that they have in common is given by the product of the degrees of the equations. In our case the product of the degrees is $2 \cdot 3 \cdots (k-1)$ and since none of the points is "at infinity" we have the claim. □

In order to prove Theorem 3.1, we will need the following three auxiliary lemmas:

Lemma 3.1. *Let* $\mathbf{K}$ *be any field and let* $X_1, \ldots, X_n \in \mathbf{K}^*$. *The linear system*

$$\begin{cases} X_1U_1 + \cdots + X_nU_n &= 0, \\ X_1^2U_1 + \cdots + X_n^2U_n &= 0, \\ & \vdots \\ X_1^nU_1 + \cdots + X_n^nU_n &= 0, \\ U_1 + \cdots + U_n &= X_1 \end{cases}$$

has no solutions $(U_1, \ldots, U_n)$ *in* $\mathbf{K}^n$.

Proof. The proof is done by induction on n. If $n = 1$, then the conditions $X_1U_1 = 0$ and $U_1 = X_1$ imply that $X_1 = 0$. Therefore no solution exists. Assume $n \geqslant 2$.

Let A be the matrix of the coefficients of the first n equations. Expanding the Vandermonde determinant we obtain

$$\det(A) = X_1 \cdots X_n \prod_{i>j} (X_i - X_j).$$

If the system of equations admits a solution $(u_1, \ldots, u_n)$, then not all the u_i's can be equal to 0 otherwise the last equation cannot be satisfied. Therefore, the homogeneous system given by the first n equations has to have a non-trivial solution. This implies that $\det(A) = 0$ and therefore $X_i = X_j$ for some $i \neq j$. Let us assume, without loss of generality, that $X_n = X_{n-1}$. Now $(u_1, \ldots, (u_{n-1} + u_n))$ is a solution of the system

$$\begin{cases} X_1U_1 + \cdots + X_{n-1}U_{n-1} &= 0, \\ X_1^2U_1 + \cdots + X_{n-1}^2U_{n-1} &= 0, \\ & \vdots \\ X_1^{n-1}U_1 + \cdots + X_{n-1}^{n-1}U_{n-1} &= 0, \\ U_1 + \cdots + U_{n-1} &= X_1 \end{cases}$$

which is a contradiction to the inductive hypothesis. □

Lemma 3.2. *Let* $A = (a_{ij})$ *be a* $t \times t$ *matrix with integer entries such that the following properties hold*:

1. *For all* $i, j = 1, \ldots, t,\ i \neq j,\ a_{ii} > 0,\ a_{ij} \leqslant 0$ (*i.e. the elements in the diagonal of* A *are strictly positive and those outside are negative*).
2. *For every* $i = 1, \ldots, t$ *there exists* $j \neq i$ *such that* $a_{ij} \neq 0$ (*i.e. every row has at least a non-zero entry outside the diagonal*).
3. *For every* $j = 1, \ldots, t,\ \sum_{i=1}^{t} a_{ij} \geqslant 0$ *and there exists* j *with* $\sum_{i=1}^{t} a_{ij} > 0$ (*i.e. the sum of the elements in every column is positive and for at least one column is strictly positive*).

Then

$$0 < \det(A) \leqslant a_{11} \cdots a_{tt}.$$

Proof. We proceed by induction on t.

If $t = 2$, then $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $\det(A) = a_{11}a_{22} - a_{21}a_{12}$. By the third hypothesis we have that $a_{11} \geqslant -a_{21}$, $a_{22} \geqslant -a_{12}$ and one of the two inequalities is a strict one. Therefore, since by property 1, $-a_{21} \geqslant 0$ and $-a_{12} \geqslant 0$, we have

$$a_{11}a_{22} > a_{21}a_{12}.$$

Finally $\det(A) > 0$. The inequality $\det(A) \leqslant a_{11}a_{22}$ follows from the first hypothesis.

Assume now that $t \geqslant 3$ and also assume, without loss of generality, that $\sum_{i=1}^{t} a_{i1} \geqslant 1$. If $A_1, A_2, \ldots, A_t$ are the rows of A, then consider that matrix:

$$\begin{pmatrix} A_1 \\ a_{11}A_2 - a_{21}A_1 \\ \vdots \\ a_{11}A_t - a_{t1}A_1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix},$$

where $B = (b_{ij})$, $i, j = 2, \ldots, t$ and

$$b_{ij} = a_{11}a_{ij} - a_{i1}a_{1j}.$$

It is clear that $a_{11}^{t-1} \det(A) = a_{11} \det(B)$. We claim that B verifies the hypothesis of the Lemma and therefore, as $a_{j1}a_{1j} \geqslant 0$ for $j = 2, \ldots, t$, by induction

$$0 < \det(B) \leqslant (a_{11}a_{22} - a_{21}a_{12}) \cdots (a_{11}a_{tt} - a_{t1}a_{1t}) \leqslant a_{11}^{t-1} a_{22} \cdots a_{tt}$$

and this implies the claim.

Let us check that B verifies the hypothesis of the lemma:

1. Since $\sum_{i=1}^{t} a_{i1} \geqslant 1$, for every $i = 2, \ldots, t$, $a_{11} > -a_{i1}$. Furthermore $a_{ii} \geqslant -a_{1i}$, therefore

$$b_{ii} = a_{11}a_{ii} - a_{i1}a_{1i} > 0.$$

   Also $b_{ij} = a_{11}a_{ij} - a_{i1}a_{1j} \leqslant 0$ (if $i \neq j$) since it is the sum of two negative numbers.
2. For every $i = 2, \ldots, t$, let $j \neq i$ be such that $a_{ij} \neq 0$. Then $b_{ij} \leqslant a_{11}a_{ij} < 0$ is also non-zero.
3. Consider

$$\sum_{i=2}^{t} b_{ij} = a_{11} \sum_{i=2}^{t} a_{ij} - a_{1j} \sum_{i=2}^{t} a_{i1} \geqslant -a_{11}a_{1j} - a_{1j}(1 - a_{11}) = -a_{1j}.$$

Therefore $\sum_{i=2}^{t} b_{ij} \geqslant 0$ for all $j = 2, \ldots, t$ and if j is such that $a_{1j} \neq 0$, then $\sum_{i=2}^{t} b_{ij} > 0$.

This concludes the proof. □

The following lemma is a standard application of calculus.

Lemma 3.3. *If $T \in \mathbb{N}$ is given, then*

$$\max\{x_1 \cdots x_s \mid x_1, \ldots, x_s \in \mathbb{N}_{\geqslant 2}, x_1 + \cdots + x_s \leqslant T\} \leqslant e^{T/e},$$

where e is the Napier constant.

Proof. Since the arithmetic mean always bounds the geometric mean, we have

$$x_1 \cdots x_s \leqslant \left(\frac{x_1 + \cdots + x_s}{s}\right)^s \leqslant \left(\frac{T}{s}\right)^s.$$

The real variable function on the right-hand side above has a maximum for $s = T/e$. The result follows from the fact that for $T \geqslant 3$,

$$\max\left\{\left(\frac{T}{[T/e]}\right)^{[T/e]}, \left(\frac{T}{[T/e]+1}\right)^{[T/e]+1}\right\} \leqslant e^{T/e}. \qquad \square$$

Proof of Theorem 3.1. The proof will proceed as follows: we denote by $\mathscr{V}_k$ the projective variety in $\mathbb{P}^{k-2}$ corresponding to $\mathscr{A}_k$:

$$\mathscr{V}_k: \begin{cases} X_0(X_0 - X_1) + X_1(X_1 - X_2) + \cdots + X_{k-3}(X_{k-3} - X_{k-2}) + X_{k-2}^2 = 0, \\ X_0^2(X_0 - X_1) + X_1^2(X_1 - X_2) + \cdots + X_{k-3}^2(X_{k-3} - X_{k-2}) + X_{k-2}^3 = 0, \\ \qquad\qquad \vdots \\ X_0^{k-2}(X_0 - X_1) + X_1^{k-2}(X_1 - X_2) + \cdots + X_{k-3}^{k-2}(X_{k-3} - X_{k-2}) + X_{k-2}^{k-1} = 0. \end{cases} \tag{6}$$

To prove that $\mathscr{V}_k(\bar{\mathbf{K}})$ is zero-dimensional, we will show that it has no points of intersection with the projective hyperplane "at infinity" $X_0 = 0$. Indeed, note that if $\mathscr{V}_k(\bar{\mathbf{K}})$ contains a positive dimensional subvariety, then it has to have non-empty intersection with any plane. In particular, if we substitute $X_0 = 0$ in (6) we should obtain some non-trivial solutions. We will see that this is impossible and that the only solution is $(X_1, \ldots, X_{k-2}) = (0, \ldots, 0)$.

Assume that $k > 3$, otherwise the statement can be verified directly and also follows from the work of Wells [11] (see (9) below) and let $n = k - 2$. If $n = 2$, then we have

the equation

$$\begin{cases} X_1^2 - X_1X_2 + X_2^2 = 0, \\ X_1^3 - X_1^2X_2 + X_2^3 = 0 \end{cases}$$

which is quickly seen to have as solutions only $(X_1, X_2) = (0, 0)$ over any field.

Assume $n \geqslant 3$ and let $(X_1, \ldots, X_n) \neq (0, \ldots, 0)$ be a non-trivial solution. We can assume that $X_1 \neq 0$ otherwise we would have a non-trivial solution $(X_2, \ldots, X_n)$ that we rule out by induction. For the same reason we can assume that $X_n \neq 0$ and that $X_i \neq X_{i+1}$ for $i = 1, \ldots, n-1$.

Let us rewrite the equations in the following way:

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & & \cdots & \vdots \\ X_1^n & X_2^n & \cdots & X_n^n \end{pmatrix} \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 \\ 0 & 1 & -1 & \cdots & 0 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Note that the first matrix has determinant

$$X_1 \cdots X_n \cdot \prod_{i>j} (X_i - X_j)$$

while the second has determinant 1.

This immediately implies that the first matrix has to have determinant equal to 0 otherwise we would obtain the contradiction that $(X_1, \ldots, X_n) = (0, \ldots, 0)$.

By setting $U_i = X_i - X_{i+1}$, if $i < n$ and $U_n = X_n$, and applying Lemma 3.1, we obtain that at least one of the $X_i = 0$.

Now let us relabel the set $\{X_1, X_2, \ldots, X_n\} \subseteq \mathbf{K}$ as $\{y_1, y_2, \ldots, y_t, 0\}$ in such a way that

1. $y_1, \ldots, y_t$ are all distinct;
2. $y_1, \ldots, y_t$ are all not zero;
3. for every $s \in \{1, \ldots, n\}$ there exists $i \in \{1, \ldots, t\}$ such that $X_s = y_i$.

Let us also assume that $y_1 = X_1$ and note that $t \leqslant n-1$. Now consider the first t equations of (6) and replace $(X_1, \ldots, X_n)$ with $(y_1, \ldots, y_t)$, so that

$$\begin{cases} y_1L_1(y_1, \ldots, y_t) + \cdots + y_tL_t(y_1, \ldots, y_t) &= 0, \\ & \vdots \\ y_1^tL_1(y_1, \ldots, y_t) + \cdots + y_t^tL_t(y_1, \ldots, y_t) &= 0, \end{cases} \tag{7}$$

where for $i = 1, \ldots, t$,

$$L_i(y_1, \ldots, y_t) = \sum_{j=1}^{t} a_{ij}y_j$$

and

$$a_{ij} = \begin{cases} \#\{s \in \{1, \ldots, n\} \mid X_s = y_i\} & \text{if } i = j, \\ -\#\{s \in \{1, \ldots, n-1\} \mid X_s = y_i, X_{s+1} = y_j\} & \text{if } i \neq j. \end{cases} \tag{8}$$

Let $A = (a_{ij})$ be the $t \times t$ matrix with integer entries defined by (8) and $\hat{A}$ be the matrix obtained by A reducing the entries in $\mathbf{K}$, where we assume that either $\mathrm{char}(\mathbf{K}) = 0$ or $\mathrm{char}(\mathbf{K}) > e^{(k-3)/e}$.

Note that $a_{ii} \geqslant 2$ otherwise one row of A would contain only one 1 and possibly one -1 and this would imply the contradiction that either two y_i's are equal or one y_i is zero.

Relations (7) can be written as

$$\begin{pmatrix} y_1 & \cdots & y_t \\ y_1^2 & \cdots & y_t^2 \\ \vdots & \cdots & \vdots \\ y_1^t & \cdots & y_t^t \end{pmatrix} \hat{A} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since the first matrix has determinant

$$y_1 \cdots y_t \prod_{i>j} (y_i - y_j) \neq 0,$$

we deduce that

$$\hat{A} \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_t \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We want to obtain a contradiction by showing that $\det(\hat{A}) \neq 0$. We will do this by applying Lemma 3.2 to A which will give

$$0 < \det A \leqslant a_{11} \cdots a_{tt}$$

and since

$$\sum_{i=1}^{t} a_{ii} = \#\{s \in \{1, \ldots, n\} \mid X_s \neq 0\} \leqslant n - 1 = k - 3,$$

we have by Lemma 3.3 that

$$0 < \det A \leqslant e^{(k-3)/e} < \mathrm{char}(\mathbf{K}).$$

Therefore $\det(\hat{A}) \neq 0$ which implies the claim.

The only thing left to show is that A satisfies the hypothesis of Lemma 3.2: the first hypothesis is immediately verified by the definition of the matrix A in (8). Similarly the second hypothesis follows from the fact that if all the elements outside the diagonal were 0 this would imply that $a_{ii}y_i = 0 \in \mathbf{K}$ and since $a_{ii} < n < \mathrm{char}(\mathbf{K})$, $a_{ii} \neq 0$ would give a contradiction.

Let us check that the third hypothesis holds. Indeed by (8),

$$\sum_{i=1}^{t} a_{ij} = \#\{s \in [2, \ldots, n] \mid X_s = y_j, X_{s-1} = 0\} + \varepsilon_j \geqslant 0,$$

where $\varepsilon_j = 1$ if $j = 1$ and 0 otherwise. It follows that the sum of the elements in the first column is strictly positive. This concludes the proof of the theorem. □

Proof of Theorem 1.2. Apply the corollary to Theorem 3.1 with $\mathbf{K} = \bar{\mathbb{F}}_q$. For $\mathrm{char}(\mathbb{F}_q) > e^{(k-3)/e}$, we have the bound

$$\#\mathscr{A}_k(\mathbb{F}_q) \leqslant \#\mathscr{A}_k(\bar{\mathbb{F}}_q) = (k-1)!$$

Finally, from (5) and from Proposition 2.1 we obtain

$$m_{[k]}(q) = \frac{q(q-1)}{k} n_{[k]}(q) \leqslant \frac{q(q-1)}{k} \#\mathscr{A}_k(\mathbb{F}_q) \leqslant \frac{(k-1)!}{k} q(q-1).$$

and this concludes the proof of Theorem 1.2. □

4. Cyclotomic permutation polynomials. Proof of Theorem 1.1

We want to prove Theorem 1.1 by producing, in the case $q \equiv 1 \pmod{k}$, $\varphi(k)$ distinct normalized k-cycles in $N_{[k]}(\mathbb{F}_q)$.

Let us start noticing that the condition $q \equiv 1 \pmod{k}$ implies that $\mathbb{F}_q$ contains all the kth roots of unity and that they are all distinct. Denote by ζ a primitive kth root of unity in $\mathbb{F}_q$. Consider the normalized k-cycle:

$$\sigma_\zeta = (0, 1, (1+\zeta), \ldots, (1+\zeta+\cdots+\zeta^{k-2})).$$

Clearly as ζ varies among the $\varphi(k)$ primitive kth roots of unity, we obtain distinct normalized k-cycles. We want to check that $\partial(f_{\sigma_\zeta}) = q - k$ (i.e. $\sigma_\zeta \in N_{[k]}(\mathbb{F}_q)$).

Let us compute, for $i = 1, \ldots, k-2$,

$$\begin{aligned}
A_i(\sigma_\zeta) &= G_i((1+\zeta), \ldots, (1+\zeta+\cdots+\zeta^{k-2})) \\
&= -\left(\sum_{j=0}^{k-3} \zeta^{j+1}(1+\zeta+\cdots+\zeta^j)^i\right) + (1+\zeta+\cdots+\zeta^{k-2})^{i+1} \\
&= \frac{-1}{(\zeta-1)^i}\left(\sum_{j=0}^{k-3} \zeta^{j+1}(\zeta^{j+1}-1)^i - \frac{(\zeta^{k-1}-1)^{i+1}}{\zeta-1}\right) \\
&= \frac{-1}{(\zeta-1)^i}\left(\sum_{j=0}^{k-3} \zeta^{j+1} \sum_{t=0}^{i} \binom{i}{t}(-1)^{i-t}\zeta^{(j+1)t} - \frac{(\zeta^{k-1}-1)^{i+1}}{\zeta-1}\right).
\end{aligned}$$

Interchange the two sums of the last equation and observe that, since $t+1 \leqslant i+1 \leqslant k-1$ and ζ is primitive, we have

$$\sum_{j=0}^{k-3} (\zeta^{t+1})^j = \frac{\zeta^{(k-2)(t+1)}-1}{\zeta^{t+1}-1}.$$

Therefore

$$A_i(\sigma_\zeta) = \frac{-1}{(\zeta-1)^i}\left(\sum_{t=0}^{i} \binom{i}{t}(-1)^{i-t}\zeta^{t+1}\frac{\zeta^{(k-2)(t+1)}-1}{\zeta^{t+1}-1} - \frac{(\zeta^{k-1}-1)^{i+1}}{\zeta-1}\right).$$

Now use the fact that $\zeta^{k-1} = \zeta^{-1}$. The above becomes

$$\begin{aligned}
A_i(\sigma_\zeta) &= \frac{-1}{(\zeta-1)^i}\left(\sum_{t=0}^{i} \binom{i}{t}(-1)^{i-t}\zeta^{1+t}\frac{\zeta^{-2(t+1)}-1}{\zeta^{t+1}-1} - \frac{(\zeta^{-1}-1)^{i+1}}{\zeta-1}\right) \\
&= \frac{-1}{(\zeta-1)^i}\left(-\left(\sum_{t=0}^{i} \binom{i}{t}(-1)^{i-t}\zeta^{-t}\right)\zeta^{-1} + \zeta^{-1}(\zeta^{-1}-1)^i\right) \\
&= \frac{1}{\zeta(\zeta-1)^i}\left(\sum_{t=0}^{i} \binom{i}{t}(-1)^{i-t}\zeta^{-t} - (\zeta^{-1}-1)^i\right) \\
&= 0.
\end{aligned}$$

Finally, recalling that $\partial(f_\sigma) \geqslant q - c(\mathscr{C})$, we have $\sigma_\zeta \in N_{[k]}(\mathbb{F}_q)$ for all primitive ζ. Therefore $n_{[k]}(q) \geqslant \varphi(k)$ and by Proposition 2.1, this concludes the proof of Theorem 1.1. □

Remark. We will call the permutations σ_ζ *cyclotomic permutations*. In the case $k = 3$, Theorem 1.2 gives that $N_{[3]}(\mathbb{F}_q) \leqslant \frac{2}{3}q(q-1)$ while Theorem 1.1 gives that if $q \equiv 1 \pmod 3$, then $N_{[3]}(\mathbb{F}_q) \geqslant \frac{2}{3}q(q-1)$. Therefore all normalized 3-cycles are cyclotomic permutations if $q \equiv 1 \pmod 3$. On the other hand in 1969, Wells [12] proved the

formula

$$N_{[3]}(\mathbb{F}_q) = \begin{cases} \frac{2}{3}q(q-1) & \text{if } q \equiv 1 \pmod 3, \\ 0 & \text{if } q \equiv 2 \pmod 3, \\ \frac{1}{3}q(q-1) & \text{if } q \equiv 0 \pmod 3. \end{cases} \tag{9}$$

Our results can be seen as generalizations of the above. Note that in [12, p. 50] there is a misprint in the case $q \equiv 0 \pmod 3$ where the claim that $N_{[3]}(3^n) = 3^n(3^n-1)$ should be corrected into $N_{[3]}(3^n) = 3^{n-1}(3^n-1)$ as all possible 3-cycles permutations are

$$(a, a+b, a-b)$$

which for all choices of $a, b \in \mathbb{F}_{3^n}$ give rise to the above amount of permutations.

5. Numerical examples: the number of k-cycles with minimal degree for $k \leqslant 6$

In this section we consider the specific examples of 4-, 5- and 6-cycles. The case of 3-cycles has been analyzed with by Wells [12] (see the remark in the previous section).

5.1. Computation of $m_{[4]}(q)$

We will prove the following:

Theorem 5.1. *Let $m_{[4]}(\mathbb{F}_q)$ be the number of 4-cycle permutations of $\mathbb{F}_q$ such that their permutation polynomial has minimal degree $q-4$. Then, if $(q, 10) = 1$,*

$$m_{[4]}(\mathbb{F}_q) = \tfrac{1}{4}q(q-1)K_q,$$

where

$$K_q = \begin{cases} 6 & \text{if } q \equiv 1 \pmod{20}, \\ 4 & \text{if } q \equiv 11 \pmod{20}, \\ 2 & \text{if } q \equiv 9, 13, 17 \pmod{20}, \\ 0 & \text{if } q \equiv 3, 7, 19 \pmod{20} \end{cases}$$

while

$$m_{[4]}(\mathbb{F}_{5^n}) = \tfrac{1}{2}5^n(5^n-1)$$

and

$$m_{[4]}(\mathbb{F}_{2^n}) = \begin{cases} 2^n(2^n-1) & \text{if } 4|n, \\ 0 & \text{otherwise.} \end{cases}$$

Remark. From (2) it follows that the degree of a 4-cycle permutation polynomial can either be $q-2$, $q-3$ or $q-4$. In [9] we proved that the number of 4-cycle permutation polynomials over $\mathbb{F}_q$ with degree strictly less then $q-3$ is

$$\frac{1}{4}q(q-1)t_q \quad \text{where } t_q = \begin{cases} q-11 & \text{if } q \equiv 1 \pmod{12}, \\ q-3 & \text{if } q \equiv 5 \pmod{12}, \\ q-7 & \text{if } q \equiv 7 \pmod{12}, \\ q+11 & \text{if } q \equiv 11 \pmod{12}, \\ (q-4)(1+(-1)^n) & \text{if } q = 2^n, \\ q-5-2(-1)^n & \text{if } q = 3^n. \end{cases}$$

This result together with Theorem 5.1 provides complete information of the number of 4-cycles of each given degree.

Proof of Theorem 5.1. From Proposition 2.1, we have that

$$m_{[4]}(\mathbb{F}_q) = \frac{q(q-1)}{4} n_{[4]}(\mathbb{F}_q)$$

and from (5) it follows that

$$n_{[4]}(\mathbb{F}_q) \# \{(x,y) \in (\mathbb{F}_q \backslash \{0,1\})^2 \mid x \neq y, (x,y) \in \mathscr{A}_4(\mathbb{F}_q)\},$$

where

$$\mathscr{A}_4 \colon \begin{cases} (1-x) + x(x-y) + y^2 = 0, \\ (1-x) + x^2(x-y) + y^3 = 0. \end{cases}$$

The resultant R with respect to the variable y of the two equations defining $\mathscr{A}_4$ is

$$\begin{aligned} R &= 10x^4 - 4x^5 + x^6 + 15x^2 - 15x^3 - 8x + 2 \\ &= (x^2 - 2x + 2)(x^4 - 2x^3 + 4x^2 - 3x + 1). \end{aligned}$$

Now denote by $h_1(x)$ the first factor and by $h_2(x)$ the second. The resultant of h_1 and h_2 is equal to 5. Therefore, if $(q,5) = 1$, h_1 and h_2 will never have common roots.

The number of roots of $h_1(x)$ is

$$\begin{cases} 0 & \text{if } q \equiv 3 \pmod 4, \\ 2 & \text{if } q \equiv 1 \pmod 4, \\ 1 & \text{if } q \text{ is even.} \end{cases} \tag{10}$$

Furthermore, if $q \equiv 1 \pmod 4$ and $\imath = \sqrt{-1}$ is a primitive fourth root of unity in $\mathbb{F}_q^*$, from the roots of h_1 we can construct the two points of $\mathscr{A}_4(\mathbb{F}_q)$

$$(x_1, y_1) = (1 + \imath, 1 + \imath + \imath^2), \quad (x_2, y_2) = (1 - \imath, 1 - \imath + \imath^2). \tag{11}$$

These points give rise to the two distinct (normalized) cyclotomic permutations:

$$(0, 1, (1 + \imath), (1 + \imath + \imath^2)); (0, 1, (1 - \imath), (1 - \imath + \imath^2)).$$

If q is even, then the root $x = 0$ of h_1 gives the point $(0, 1) \in \mathbb{F}_{2^n}$ that leads to no permutation polynomials.

Let us now deal with h_2. We claim that the number of roots of h_2 is

$$\begin{cases} 4 & \text{if } q \equiv 1 \pmod 5, \\ 1 & \text{if } q \equiv 0 \pmod 5, \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

Indeed a calculation shows that if ζ is a primitive fifth root of unity in $\mathbb{F}_q$, then

$$h_2(x) = \prod_{i=1}^{4} (x - 1 - \zeta^i - \zeta^{2i})$$

while

$$h_2(x) \equiv (x + 2)^4 \pmod 5.$$

Hence (12) follows.

If $q \equiv 1 \pmod 5$ and x_i is a root of h_2 then a computation shows that $y_i = 1 - 2x_i + x_i^2 - x_i^3$ is the only value for which $(x_i, y_i) \in \mathscr{A}_4(\mathbb{F}_q)$.

The conditions $x_i = 0$ or $x_i = 1$ are never satisfied since $h_2(0) = 1$ and $h_2(1) = 1$ and the other conditions

$$x_i = y_i, \quad y_i = 0, \quad y_i = 1$$

are also never satisfied. This is easily checked by some computation. For example the condition $y_i = 0$ can be checked by calculating the resultant between $h_2(x)$ and $1 - 2x + x^2 - x^3$. This resultant is equal to 1.

Putting together (10) and (12), and working out the various congruence relations modulo 20, we obtain the claim for characteristic different from 2 and 5.

Let us now deal with the case when $q = 5^n$. The two roots of $h_1(y)$ will provide the two points of $\mathscr{A}_4(\mathbb{F}_{5^n})$ $(3,2)$ and $(4,3)$, while

$$h_2(x) = (x+2)^4$$

has only one root $x_1 = 3$ which gives $y_1 = 2$, but the point $(2,3) \in \mathscr{A}_4(\mathbb{F}_{5^n})$ has already been counted. Therefore $\#\mathscr{A}_4(\mathbb{F}_{5^n}) = 2$.

Finally let us deal with the case when $q = 2^n$. The root $x = 0$ of $h_1(x)$ has to be excluded and $h_2(x)$ provides 4 distinct points if $2^n \equiv 1 \pmod 5$ (i.e. $n|4$).

This concludes the proof of the theorem. □

Remark. We want to summarize the process that we used to construct all the points in $\mathbb{A}_4(\mathbb{F}_q)$ since we will adopt the same approach in the following examples:

1. We have decomposed

$$\mathscr{A}_4(\overline{\mathbb{F}_q}) = \mathscr{A}_4(\mathbb{F}_q(\sqrt{-1})) \cup \mathscr{A}_4(\mathbb{F}_q(\zeta_5)),$$

   where the union is disjoint except in the case $5|q$.
2. We have checked that the coordinates of each point of $\mathscr{A}_4(\overline{\mathbb{F}_q})$ were distinct and different from 0 or 1. This has always been the case except when $2|q$.
3. If $(q,10) = 1$, then the number $m_{[4]}(q)$ is $q(q-1)/4$ times $n_1 + n_2$ where n_1 is the number of points in $\mathscr{A}_4(\mathbb{F}_q(\sqrt{-1}))$ and n_2 is the number of points in $\mathscr{A}_4(\mathbb{F}_q(\zeta_5))$.

Note that for every prime $p \neq 2, 5$, n_1 is the number of prime ideals of $\mathbb{Q}(\sqrt{-1})$ over p and n_2 is the number of prime ideals of $\mathbb{Q}(\zeta_5)$ over p. This property suggests to first look at $\mathscr{A}_4(\bar{\mathbb{Q}})$ and then consider the reduction in the various finite fields. We will follow this approach in the sequel.

5.2. *Computation of* $m_{[5]}(q)$

We will prove the following:

Theorem 5.2. *Let q be a power of a prime p which is not in the set*

$$\{2, 13, 61, 3719, 3100067\}.$$

Then

$$m_{[5]}(\mathbb{F}_q) = \frac{q(q-1)}{5} s_q,$$

where

$$s_q = r_q + t_q + u_q, \quad t_q = \begin{cases} 4 & \text{if } q \equiv 1 \pmod 5, \\ 1 & \text{if } q \equiv 0 \pmod 5, \\ 0 & \text{otherwise}, \end{cases} \quad u_q = \begin{cases} -1 & \text{if } p = 11, 41, \\ 0 & \text{otherwise} \end{cases}$$

and r_q is the number of roots in $\mathbb{F}_q$ of the polynomial

$$\begin{aligned} g_2(x) = {} & 2x^{20} - 29x^{19} + 229x^{18} - 1249x^{17} + 5187x^{16} \\ & - 17222x^{15} + 47040x^{14} - 107505x^{13} + 207622x^{12} \\ & - 340496x^{11} + 474638x^{10} - 560999x^9 + 559052x^8 \\ & - 465487x^7 + 319628x^6 - 177653x^5 + 77807x^4 - 25797x^3 \\ & + 6074x^2 - 904x + 64. \end{aligned}$$

Proof. Again we start from the formula:

$$m_{[5]}(\mathbb{F}_q) = \frac{q(q-1)}{5} \#\{(x, y, z) \in \mathscr{A}_5(\mathbb{F}_q), x, y, z \notin \{0, 1\}, x \neq y \neq z \neq x\},$$

where

$$\mathscr{A}_5: \begin{cases} H_1 = (1-x) + x(x-y) + y(y-z) + z^2 = 0, \\ H_2 = (1-x) + x^2(x-y) + y^2(y-z) + z^3 = 0, \\ H_3 = (1-x) + x^3(x-y) + y^3(y-z) + z^4 = 0. \end{cases}$$

Let us first compute $\mathscr{A}_5(\bar{\mathbb{Q}})$.

From Theorem 3.1 we know that $\#\mathscr{A}_5(\bar{\mathbb{Q}}) = 24$. Furthermore 4 points of $\mathscr{A}_5(\bar{\mathbb{Q}})$ are the cyclotomic ones

$$(1 + \zeta^j, 1 + \zeta^j + \zeta^{2j}, 1 + \zeta^j + \zeta^{2j} + \zeta^{3j}), \quad \zeta = e^{2\pi i/5}, \quad j = 1, 2, 3, 4. \tag{13}$$

We solve the system of equations defining $\mathscr{A}_5$ in the following way. Consider $H_2 - (z + y)H_1 = 0$ and note that we can solve it for z obtaining

$$z = \frac{x^3 - 2x^2y + xy^2 + xy - x - y + 1}{x^2 - xy + y^2 - x + 1}. \tag{14}$$

Similarly, consider $H_3 - zH_2 - y^2H_1 = 0$. Also here we can solve it for z obtaining:

$$z = \frac{x^4 - x^3y - x^2y^2 + xy^3 + xy^2 - y^2 - x + 1}{x^3 - x^2y + y^3 - x + 1}. \tag{15}$$

Now, subtracting $H_3 - z^2 H_1 - yH_2 = 0$, we can solve it for z^2 obtaining:

$$z^2 = \frac{x^4 - 2x^3y + x^2y^2 + xy - x - y + 1}{x^2 - xy + y^2 - x + 1}. \tag{16}$$

Replacing z^2 in H_1 with the right-hand side of (16) and z with the right-hand side of (14) we obtain (after simplification):

$$(x^4 - 2x^3y + x^2y^2 + xy - x - y + 1) - y(x^3 - 2x^2y + xy^2 + xy - x - y + 1)(1 - x + x(x - y) + y^2)^2 = 0. \tag{17}$$

Finally, consider the equation obtained replacing z in (14) by the right-hand side of (15)

$$(x^4 - x^3y - x^2y^2 + xy^3 + xy^2 - y^2 - x + 1)(x^2 - xy + y^2 - x + 1) - (x^3 - x^2y + y^3 - x + 1)(x^3 - 2x^2y + xy^2 + xy - x - y + 1) = 0. \tag{18}$$

In this way we have eliminated the variable z. We might have introduced new solutions but we will see later that this is not the case.

We have used Maple V [10] to compute the resultant R of (17) and (18) with respect to y and we obtained:

$$R = g_1(x) \cdot g_2(x),$$

where

$$g_1(x) = x^4 - 3x^3 + 4x^2 - 2x + 1 \tag{19}$$

and

$$\begin{aligned} g_2(x) = {} & 2x^{20} - 29x^{19} + 229x^{18} - 1249x^{17} + 5187x^{16} - 17222x^{15} \\ & + 47040x^{14} - 107505x^{13} + 207622x^{12} - 340496x^{11} \\ & + 474638x^{10} - 560999x^9 + 559052x^8 - 465487x^7 \\ & + 319628x^6 - 177653x^5 + 77807x^4 - 25797x^3 \\ & + 6074x^2 - 904x + 64 \end{aligned} \tag{20}$$

Now the splitting field of $g_1(x)$ is $\mathbb{Q}(e^{2\pi i/5})$. Furthermore, the roots of g_1 are

$$x_j = (1 + \zeta^i), \quad j = 1, 2, 3, 4.$$

We can also easily compute x and y for each of the above. Hence $\mathscr{A}_5(\mathbb{Q}(\zeta_5))$ is exactly the set described in (13).

Let $\mathbf{M}_5$ be the splitting field of g_2. For each root α of $g_2(x)$, one can compute $(\alpha, y(\alpha), z(\alpha)) \in A_5(\mathbf{M}_5)$ where:

$$\begin{aligned} y(x) = &\frac{1}{2^3 \cdot 13 \cdot 61 \cdot 3719 \cdot 3100067}(6245340990732510 - 74275247020348477x \\ &+ 425897367479627411x^2 - 1556772755104088477x^3 \\ &+ 406812235642376552 0x^4 - 8092377944341897339x^5 \\ &+ 127391557470725031 54x^6 - 16281608694400072277x^7 \\ &+ 171914678928898784 76x^8 - 15176855331347725064x^9 \\ &+ 112892101116159201 88x^{10} - 7103742513094855073x^{11} \\ &+ 37820814073014444 60x^{12} - 1696979431552752820x^{13} \\ &+ 635807089991226023x^{14} - 195705738631474759x^{15} \\ &+ 48121368022605621x^{16} - 9009616966592957x^{17} \\ &+ 1165803130533438x^{18} - 82558295396232x^{19}) \end{aligned}$$

and from (14) and some computation

$$\begin{aligned} z(x) = &\frac{x^3 - 2x^2y(x) + xy(x)^2 + xy(x) - x - y(x) + 1}{(x)^2 - xy(x) + y(x)^2 - x + 1} \\ = &\frac{1}{2^3 \cdot 13 \cdot 61 \cdot 3719 \cdot 3100067}(-292290150269490x^{19} + 3950333490943181x^{18} \\ &- 294846644286178 01x^{17} + 152268243151302965x^{16} \\ &- 599002775464475543x^{15} + 188043834591716 7218x^{14} \\ &- 484113598946175 1552x^{13} + 1037837455146985 6881x^{12} \\ &- 186798784031511151 30x^{11} + 283039428732860208 48x^{10} \\ &- 360411512674745877 82x^9 + 383367021769330858 23x^8 \\ &- 337119580961745933 04x^7 + 241294665125392783 43x^6 \\ &- 137423594160007561 36x^5 + 602024561116746133x^4 \\ &- 192567750149432428 3x^3 + (413273185040891961x^2 \\ &- 51203861193252214x + 2593061963570136). \end{aligned}$$

Finally

$$\mathscr{A}_5(\bar{\mathbb{Q}}) = \mathscr{A}_5(\mathbb{Q}(e^{2\pi i/5})) \cup \mathscr{A}_5(\mathbf{M}_5),$$

where the union is disjoint.

We are now ready to investigate $\mathscr{A}_5(\mathbb{F}_q)$.

The roots of $g_1(x)$ in $\mathscr{A}_5(\mathbb{F}_q)$ are 4 if $q \equiv 1 \pmod 5$ and in this case the 4 points give the cyclotomic permutation polynomials. If $q = 5^n$, then $g_1(x) = (x+3)^4$ and the root $x_0 = 2$ leads to the point $(2,3,4) \in \mathscr{A}_5(\mathbb{F}_{5^n})$ and therefore to the normalized 5-cycle $(0,1,2,3,4)$.

Let us deal with the roots of $g_2(x)$. The characteristics

$$\{2, 13, 61, 3719, 3100067\} \tag{21}$$

appearing in the denominators of $y(x)$ and $z(x)$ will have to be treated separately and we have not done it here.

For all other primes, note that $g_2(0) = 2^6$, $g_2(1) = 2$ and we have the following resultants:

$$R(y(x), g_2(x)) = 2^{24}, \quad R(y(x)-1, g_2(x)) = 2^{24}, \quad R(y(x)-x, g_2(x)) = 2^{19},$$

$$R(z(x), g_2(x)) = 2^{19}, \quad R(z(x)-1, g_2(x)) = 2^{24}, \quad R(z(x)-x, g_2(x)) = 2^{24},$$

$$R(y(x)-z(x), g_2(x)) = 2^{19},$$

where $R(a,b)$ is the resultant of the univariate polynomials a and b. Therefore, for any finite field $\mathbb{F}_q$ (of characteristic distinct from those in (21)), if $g_2(x_0) = 0$, then $(x_0, y(x_0), z(x_0)) \in \mathscr{A}(\mathbb{F}_q)$ and $\sigma = (0, 1, x_0, y(x_0), z(x_0))$ is a well-defined normalized permutation in $n_{[5]}(\mathbb{F}_q)$.

The characteristics $\{11, 41, 160591\}$ are those for which $g_1(x)$ and $g_2(x)$ have roots in common. These can be determined by computing the resultant $R(g_1, g_2)$.

For $p = 11$, the only common root is $x = 6$ and the only point in $\mathscr{A}_5(\mathbb{F}_{11^n})$ that has such a value as first coordinate is $(6,9,2)$; for $p = 41$, the only common root is $x = 38$ and the only point in $\mathscr{A}_5(\mathbb{F}_{41^n})$ that has such an x is $(38,13,31)$. Therefore in these two cases the number of normalized permutations should be one less. Finally for $p = 160591$ the only common root is $x = 93$ but there are two points in $\mathscr{A}_5(\mathbb{F}_{160591^n})$ with $x = 93$ which are $(93, 8557, 144881)$ and $(93, 36072, 14312)$.

This concludes the proof. □

5.3. Partial computation of $m_{[6]}(q)$

Let us consider the affine algebraic set $\mathscr{A}_6$:

$$\mathscr{A}_6\colon \begin{cases} H_1 = (1-x) + x(x-y) + y(y-z) + z(z-t) + t^2 = 0, \\ H_2 = (1-x) + x^2(x-y) + y^2(y-z) + z^2(z-t) + t^3 = 0, \\ H_3 = (1-x) + x^3(x-y) + y^3(y-z) + z^3(z-t) + t^4 = 0, \\ H_4 = (1-x) + x^4(x-y) + y^4(y-z) + z^4(z-t) + t^5 = 0. \end{cases}$$

We know from Theorem 3.1 that $\#\mathscr{A}_6(\bar{\mathbb{Q}}) = 120$. The problem can be solved along the same lines as in the last subsection. Here is the Maple V program that we used:

```
restart:
H[1]:=1-x+x*(x-y)+y*(y-z)+z*(z-t)+t^2:
H[2]:=1-x+x^2*(x-y)+y^2*(y-z)+z^2*(z-t)+t^3:
H[3]:=1-x+x^3*(x-y)+y^3*(y-z)+z^3*(z-t)+t^4:
H[4]:=1-x+x^4*(x-y)+y^4*(y-z)+z^4*(z-t)+t^5:
F[1]:=solve(H[2]-(t+z)*H[1],t):
F[2]:=solve(H[3]-t*H[2]-z^2*H[1],t):
F[3]:=solve(H[4]-t*H[3]-z^3*H[1],t):
F[4]:=solve(H[3]-z*H[2]-t^2*H[1],t)[1]^2:
G[1]:=numer(F[1]-F[2]):
G[2]:=numer(F[3]-F[1]):
G[3]:=numer(F[4]-z*F[1]+1-x+x*(x-y)+y*(y-z)+z^2):
A[1]:=resultant(G[1],G[2],z):
A[2]:=resultant(G[1],G[3],z):
A[3]:=resultant(G[2],G[3],z):
B[1]:=resultant(A[1],A[2],y):
B[2]:=resultant(A[1],A[3],y):
B[3]:=resultant(A[2],A[3],y):
factor(gcd(B[1],gcd(B[2],B[3])));
```

It produces as output:

$$f_1(x)\cdot f_2(x)\cdot f_3(x)\cdot f_4(x)\cdot g_2(x)^2\cdot g_1(x)^2,$$

where g_1 and g_2 are the same polynomials of the previous subsection and do not yield any point in $\mathscr{A}_6(\bar{\mathbb{Q}})$,

$$f_1(x) = x^2 - 3x + 3, \quad f_2(x) = x^4 - 3x^3 + 9x^2 - 9x + 3,$$

$$f_3(x) = x^6 - 4x^5 + 12x^4 - 22x^3 + 25x^2 - 14x + 3$$

and $f_4(x)$ is a degree 108 polynomial, shown below. Very little can be done about it (e.g. we cannot factor its discriminant). However, we know that given one of its 108 roots x, there exist rational functions $y(x), z(x), t(x)$ such that $(x, y(x), z(x), t(x)) \in \mathscr{A}_6(\bar{\mathbb{Q}})$.

$$
\begin{aligned}
f_4(x) = {} & \\
& 2048\,x^{108} - 165888\,x^{107} + 6799872\,x^{106} - 187752960\,x^{105} + 3922763776\,x^{104} - 66068319680\,x^{103} \\
& +933320077408\,x^{102} - 11363232453904\,x^{101} + 121609445410488\,x^{100} - 1161198732496436\,x^{99} \\
& +10008850476882864\,x^{98} - 78606667549447068\,x^{97} + 566828548445747784\,x^{96} - 3776776878293093668\,x^{95} \\
& +23377338985281206132\,x^{94} - 135038479362980318078\,x^{93} + 730833294640515925896\,x^{92} \\
& -3718457594383449440377\,x^{91} + 17839854280234088048504\,x^{90} - 80918773915266921688911\,x^{89} \\
& +347817829980603691940144\,x^{88} - 1419720414224675767707558\,x^{87} + 5513288219047478965908265\,x^{86} \\
& -20403343418466290909559217\,x^{85} + 72065722093337704619789754\,x^{84} - 243267380374046351368535386\,x^{83} \\
& +785782176891688617129372777\,x^{82} - 2431475137872624992934580357\,x^{81} + 7214881866132247318290915548\,x^{80} \\
& -20548659512217571859089105859\,x^{79} + 56221257258312886794846517663\,x^{78} \\
& -147882404554712812657831273826\,x^{77} + 374230043847540583315597499959\,x^{76} \\
& -911691931385646228439986925230\,x^{75} + 2139449841280212409103799322605\,x^{74} \\
& -4838781255382865924142092881113\,x^{73} + 10552734185292011384044411424566\,x^{72} \\
& -22201680743797784367677070019329\,x^{71} + 45079400421222501688611989232857\,x^{70} \\
& -88370131835128893374420804013985\,x^{69} + 167308044867058677528870842347726\,x^{68} \\
& -306018091440642946312309370096773\,x^{67} + 540901707766162203714093161026402\,x^{66} \\
& -924145503563203698506557364196092\,x^{65} + 1526550997692643704549449565023087\,x^{64} \\
& -2438475861371766718260022687359403\,x^{63} + 3767372156555906676771592362227252\,x^{62} \\
& -5630386387795750914878787596953278\,x^{61} + 8140939139357659835287965640730513\,x^{60} \\
& -11389249472014526491272002805160961\,x^{59} + 15418372730959804119154464592501925\,x^{58} \\
& -20199212963332568595992849480574793\,x^{57} + 25609653568875523492121650783680523\,x^{56} \\
& -31423786674815287982856648211485665\,x^{55} + 37316636201275774332720329351064002\,x^{54} \\
& -42887487674528678056202555216506600\,x^{53} + 47701189936940459634356766395673379\,x^{52} \\
& -51342370723861934089578323730701241\,x^{51} + 53473605808047948459645336373877904\,x^{50} \\
& -53886451035411447622870618958843743\,x^{49} + 52534755181805885450898834956212846\,x^{48} \\
& -49542943308323803416607202273116258\,x^{47} + 45187255671028388860208926229245651\,x^{46} \\
& -39853834776380146454538798283342894\,x^{45} + 33982440027129229551505906960627180\,x^{44} \\
& -28007124276968506959166892217933313\,x^{43} + 22304864978517515995360691909021985\,x^{42} \\
& -17160233130232486543207338901006740\,x^{41} + 12749752732446670751318525720373287\,x^{40} \\
& -9145009691119593703082103400176233\,x^{39} + 6330015056336126215839775082630388\,x^{38} \\
& -4226514548260823401239096740258288\,x^{37} + 2720942861141654856875643560186175\,x^{36} \\
& -1688109362923362914905627143729438\,x^{35} + 1008768415625546502227835131362059\,x^{34} \\
& -580279479672452851412256035043958\,x^{33} + 321115048795909727104320629068345\,x^{32} \\
& -170828586279878576733366714859762\,x^{31} + 87299009196449969872102046466464\,x^{30} \\
& -42820393799631399542004753630026\,x^{29} + 20141728505903344673399260414668\,x^{28} \\
& -9076637830955551006671020183951\,x^{27} + 3914484242526498208181639312379\,x^{26} \\
& -1613770892718885947479095327793\,x^{25} + 635149654477638378211058318534\,x^{24} \\
& -238326908840088875601414025833\,x^{23} + 85127356062476807845436220758\,x^{22} \\
& -28895680606614726658303804088\,x^{21} + 9303712106309033749916140254\,x^{20} \\
& -2835587512930135705228988470\,x^{19} + 816198705952614985217016076\,x^{18} - 221309370680671620177529840\,x^{17} \\
& +56364041482436139001235584\,x^{16} - 13439641318120378785990472\,x^{15} + 2989147250976033209662704\,x^{14} \\
& -617501175174317760066496\,x^{13} + 117904318811134669800960\,x^{12} - 20688959726700010283264\,x^{11} \\
& +3313845039406468383232\,x^{10} - 480619489043461936640\,x^{9} + 62499665119858375680\,x^{8} \\
& -7198855775276720128\,x^{7} + 723131989749039104\,x^{6} - 62070327274504192\,x^{5} + 4427182693416960\,x^{4} \\
& -251951884271616\,x^{3} + 10728106885120\,x^{2} - 303868936192\,x + 4294967296.
\end{aligned}
$$

We have named the above polynomial: "*Devil's Hat*". For every root ζ of the polynomial f_1, we have the cyclotomic points

$$(\zeta, 2\zeta - 2, 2\zeta - 3, \zeta - 2) \in \mathscr{A}_6(\bar{\mathbb{Q}}).$$

For every root τ of the polynomial f_2, we have the points in $\mathscr{A}_6(\bar{\mathbb{Q}})$

$$(\tau, \tfrac{1}{5}(11 - 19\tau + 7\tau^2 - 3\tau^3), \tfrac{1}{5}(9 - 11\tau + 3\tau^2 - 2\tau^3), \tfrac{1}{5}(-7 + 13\tau - 4\tau^2 + \tau^3)).$$

Furthermore, for every root γ of f_3, we have the points of $\mathscr{A}_6(\mathbb{Q})$ $(\gamma, y_\gamma, z_\gamma, t_\gamma)$ where

$$y_\gamma = 7 - \tfrac{61}{3}\gamma + 22\gamma^2 - \frac{41}{3}\gamma^3 + \frac{14}{3}\gamma^4 - \tfrac{4}{3}\gamma^5,$$

$$z_\gamma = 6 - \tfrac{61}{3}\gamma + 22\gamma^2 - \frac{41}{3}\gamma^3 + \frac{14}{3}\gamma^4 - \frac{4}{3}\gamma^5,$$

$$t_\gamma = 7 - \tfrac{64}{3}\gamma + 22\gamma^2 - \tfrac{41}{3}\gamma^3 + \frac{14}{3}\gamma^4 - \frac{4}{3}\gamma^5.$$

Finally

$$\mathscr{A}_6(\bar{\mathbb{Q}}) = \mathscr{A}_6(\mathbf{K}_1) \cup \mathscr{A}_6(\mathbf{K}_2) \cup \mathscr{A}_6(\mathbf{K}_3) \cup \mathscr{A}_6(\mathbf{K}_4),$$

where $\mathbf{K}_i$ is the splitting field of f_i. Note however that the union is not disjoint this time. Indeed $\mathbf{K}_1 = \mathbb{Q}(\sqrt{-3}) \subset \mathbf{K}_2 = \mathbb{Q}(\sqrt{-18 + 2\sqrt{-3}})$.

Furthermore,

$$\#\mathscr{A}_6(\mathbf{K}_i) = \begin{cases} 2 & \text{if } i = 1, \\ 4 & \text{if } i = 2, \\ 6 & \text{if } i = 3, \\ 108 & \text{if } i = 4. \end{cases}$$

Numerically if can be verified that all the coordinates of each point of $\mathscr{A}_6(\bar{\mathbb{Q}})$ are distinct and never in $\{0, 1\}$. This allows us to conclude

Theorem 5.3. *For all but finitely many characteristics*

$$m_{[6]}(\mathbb{F}_q) = \frac{q(q-1)}{4}(s_1 + s_2 + s_3 + s_4),$$

where s_i is the number of roots of f_i in $\mathbb{F}_q$.

6. Conclusion

The complete computations of $\mathscr{A}_7$ is out of our reach at the present.

It is natural to ask whether the construction of the present paper can be extended to more general classes of permutations. The answer is yes. Indeed if $\mathscr{C}$ is any partition with parts larger then 1, then one can define an algebraic set $\mathscr{A}_{\mathscr{C}}$ analogue to $\mathscr{A}_k$. The connection with normalized permutation polynomials with minimal degree can be established also in this more general setting. However the extensions of Theorems 1.2 and 1.1 are not straightforward. We expect in some cases stronger estimates to hold. For example it can be shown that

$$m_{[2\ 3]}(\mathbb{F}_q) \leqslant 2q(q-1).$$

Numerical examples indicate interesting arithmetical properties. For these reasons we have decided to dedicate a future paper to general classes of permutation.

Acknowledgments

We thank Lucia Caporaso for suggesting the idea that led us to prove Theorem 3.1. Furthermore we thank Igor Shparlinski for offering shelter at Macquarie University where this manuscript was finally written and revised.

References

[1] P. Das, The number of permutation polynomials of a given degree over a finite field, Finite Fields Appl. 8 (4) (2002) 478–490.
[2] J. Harris, Algebraic Geometry, A First Course, Graduate Texts in Mathematics, Vol. 133, Springer, Berlin, 1992.
[3] S. Konyagin, F. Pappalardi, Enumerating permutation polynomials over finite fields by degree, Finite Fields Appl. 8 (4) (2002) 548–553.
[4] J. Levine, J.V. Brawley, Some cryptographic applications of permutation polynomials, Cryptologia 1 (1) (1977) 76–92.
[5] R. Lidl, G.L. Mullen, When does a polynomial over a finite field permute the elements of the field?, Amer. Math. Monthly 95 (1988) 243–246.
[6] R. Lidl, 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.
[7] R. Lidl, W.B. Müller, A note on polynomials and functions in cryptography, Ars Combin. 17A (1984) 223–229.
[8] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics Applications, Vol. 20, Addison-Wesley, Reading, MA, 1983.
[9] C. Malvenuto, F. Pappalardi, Enumerating permutation polynomials I: permutations with non-maximal degree, Finite Fields Appl. 8 (4) (2002) 531–547.
[10] Maple V Release 5.1 (1999), Waterloo Maple Inc.
[11] G.L. Mullen, Permutation polynomials over finite fields, Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, NV, 1991, Lecture Notes in Pure and Applied Mathematics, Vol. 141, Dekker, New York, 1993, pp. 131–151.
[12] C. Wells, The degrees of permutation polynomials over finite fields, J. Combin. Theory 7 (1969) 49–55.