Finite Fields and Their Applications **8,** 531–547 (2002)
doi:10.1006/ffta.2002.0362

Enumerating Permutation Polynomials I: Permutations with Non-Maximal Degree

Claudia Malvenuto

*Dipartimento di Scienze dell'Informazione, Università degli studi "La Sapienza,"
Via Salaria, 113, Rome I-00198, Italy*
E-mail: claudia@dsi.uniroma1.it

and

Francesco Pappalardi

*Dipartimento di Matematica, Università degli studi Roma Tre, Largo S. L. Murialdo, 1,
Rome I-00146, Italy*
E-mail: pappa@mat.uniroma3.it

Communicated by Daqing Wan

Received June 4, 2001; revised February 21, 2002; published online June 25, 2002

Let $\mathscr{C}$ be a conjugation class of permutations of a finite field $\mathbb{F}_q$. We consider the function $N_{\mathscr{C}}(q)$ defined as the number of permutations in $\mathscr{C}$ for which the associated permutation polynomial has degree $<q-2$. In 1969, Wells proved a formula for $N_{[3]}(q)$ where $[k]$ denotes the conjugation class of k-cycles. We will prove formulas for $N_{[k]}(q)$ where $k=4,5,6$ and for the classes of permutations of type $[2\ 2], [3\ 2], [4\ 2]$, $[3\ 3]$ and $[2\ 2\ 2]$. Finally in the case $q=2^n$, we will prove a formula for the classes of permutations which are product of 2-cycles. © 2002 Elsevier Science (USA)

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 $\mathbb{F}_q[x]$

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

The following properties are easy to verify:

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

Notice that f_σ is the unique polynomial in $\mathbb{F}_q$ with these two properties. Such polynomials are called *permutation polynomials*.

Basic literature on permutation polynomials can be found in the book of Lidl and Niederreiter [5]. Various applications of permutation polynomials to cryptography have been described. See for example [1,2]. Lidl and Mullen in [3,4] (see also [6]) describe a number of open problems regarding permutations polynomials: among these, the problem of enumerating permutation polynomials by their degree.

We denote by

$$S_\sigma = \{x \in \mathbb{F}_q \; | \sigma(x) \neq x\}$$

the set of those elements of $\mathbb{F}_q$ which are moved by σ. Our first remark is that

$$\partial(f_\sigma) \geq q - |S_\sigma| \qquad \text{if } \sigma \neq \text{id}. \tag{2}$$

To see this it is enough to note that the polynomial $f_\sigma(x) - x$ has as roots all the elements of $\mathbb{F}_q$ fixed by σ, that is which are not in S_σ. Therefore, if not identically zero, it has to have degree at least $q - |S_\sigma|$. An immediate consequence is that all transpositions give rise to permutation polynomials of degree exactly $q-2$. This fact was noticed by Wells in [7], where he also proved the following:

Theorem 1.1 (Wells [7]). *If $q > 3$, the number of 3-cycles permutations σ of $\mathbb{F}_q$ such that $\partial(f_\sigma) \leq q-3$ (which in view of (2) implies $\partial(f_\sigma) = q-3$) is*

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

The goal of this note is to extend the previous result to the cases of k-cycles ($k = 4,5,6$) and to other classes of permutations.

Let $A_i(\sigma)$ denote the coefficient of x^{q-1-i} in the polynomial $f_\sigma(x)$ of (1), that is

$$f_\sigma(x) = A_1(\sigma)x^{q-2} + A_2(\sigma)x^{q-3} + \cdots + A_{q-2}(\sigma)x + A_{q-1}(\sigma).$$

From (1) it is very easy to derive the formula for the coefficient of the leading term

$$A_1(\sigma) = -\sum_{c\in\mathbb{F}_q} \sigma(c)c.$$

Since the squares of all the elements of $\mathbb{F}_q$ add up to zero when $q > 3$, the previous formula can be written as

$$A_1(\sigma) = \sum_{c\in\mathbb{F}_q} (c - \sigma(c))c = \sum_{c\in S_\sigma} (c - \sigma(c))c = \sum_{j=1}^{t} \sum_{k=1}^{l_j} (c_{j,k} - c_{j,k+1})c_{j,k}, \tag{3}$$

where we write σ as the product of disjoint cycles (of length larger than 1):

$$\sigma = (c_{1,1}, \dots, c_{1,l_1})(c_{2,1}, \dots, c_{2,l_2}) \dots (c_{k,1}, \dots, c_{t,l_t}).$$

Note that in (3) we set $c_{j,l_j+1} = c_{j,1}$.

It is well known that a conjugation class of permutations is determined by a cycle decomposition and we will denote by $[l_1\ l_2\ \cdots\ l_k]$ $(l_i > 1)$ a conjugation class. For example $[k]$ denotes the class of k-cycle permutations. If $\sigma \in [l_1\ l_2\ \cdots\ l_k]$, then $|S_\sigma| = l_1 + l_2 + \cdots + l_k$.

For a given conjugation class $\mathscr{C}$ here we will consider the following function:

$$N_{\mathscr{C}}(q) = |\{\sigma \in \mathscr{C} \mid \partial(f_\sigma) < q - 2\}|$$

that counts the number of permutations in $\mathscr{C}$ whose degree is non-maximal.

If we denote by η the quadratic character of $\mathbb{F}_q^*$ (q odd) and set $\eta(0) = 0$, for $q > 3$, Wells' result can be written as

$$N_{[3]}(q) = \begin{cases} \frac{1}{3}q(q-1)(1+\eta(-3)) & \text{if } q > 3 \text{ odd}, \\ \frac{1}{3}2^n(2^n-1)(1+(-1)^n) & \text{if } q = 2^n,\ q > 2, \\ 0 & \text{if } q \le 3. \end{cases}$$

Sometimes it is also useful to denote the class of those permutations that are the product of m_1 cycles of length 1, m_2 cycles of length $2, \dots, m_t$ cycles of length t, as $(m_1; m_2; \dots; m_t)$ where $m_1 + 2m_2 + \cdots + tm_t = q$. With this notation we have that if $\sigma \in \mathscr{C}$ then $|S_\sigma| = q - m_1$ and

$$|\mathscr{C}| = \frac{q!}{m_1!1^{m_1}m_2!2^{m_2}\cdots m_t!t^{m_t}}. \tag{4}$$

Now for $\mathscr{C} = [l_1 \ \cdots \ l_k]$ and $c = l_1 + \cdots + l_k$ consider the polynomial in c indeterminates (cf. (3))

$$A_{\mathscr{C}}(x_1, \dots, x_c) = \sum_{\substack{i=1 \\ i \notin \{l_1, l_1+l_2, \dots, c\}}}^{c} (x_i - x_{i+1})x_i + \sum_{i=1}^{k} (x_{l_1+\cdots+l_i} - x_{l_1+\cdots+l_{i-1}+1})x_{l_1+\cdots+l_i}. \qquad (5)$$

From the above discussion we deduce that

$$N_{\mathscr{C}}(q) = \frac{1}{m_2!2^{m_2} \cdots m_t!t^{m_t}} |\{\underline{x} \in \mathbb{F}_q^c\colon \underline{x} \text{ has coordinates all distinct and } A_{\mathscr{C}}(\underline{x}) = 0\}|. \qquad (6)$$

Indeed by (3) every permutation counted by $N_{\mathscr{C}}(q)$ gives rise to a root of (5); furthermore, by cyclically permuting the elements of every cycle and by permuting different cycles of the same length we get different roots of (5) that correspond to the same element of $N_{\mathscr{C}}(q)$.

2. 4-CYCLE POLYNOMIALS

Let us now consider the case of 4-cycles. We will show the following:

THEOREM 2.1. *Suppose $q > 3$ is odd. Then*

$$N_{[4]}(q) = \tfrac{1}{4}q(q-1)(q-5-2\eta(-1)-4\eta(-3)).$$

Suppose $q = 2^n$ with $n \geq 2$. Then

$$N_{[4]}(2^n) = \tfrac{1}{4}2^n(2^n-1)(2^n-4)(1+(-1)^n).$$

Proof. By (6), any $a, b, c, d \in \mathbb{F}_q$ (all distinct) such that the 4-cycle $(a\ b\ c\ d)$ is counted by $N_{[4]}(q)$, have to satisfy the equation:

$$(a-b)a + (b-c)b + (c-d)c + (d-a)d = 0. \qquad (7)$$

For every of the $q(q-1)$ fixed choices of a and b distinct in $\mathbb{F}_q$, substituting into (7) $c = x(b-a) + a$, $d = y(b-a) + a$, we obtain the equation

$$(1-x) + (x-y)x + y^2 = 0. \qquad (8)$$

Since the conditions that a, b, c and d are all distinct, are equivalent to the conditions that $x, y \notin \{0, 1\}$ and $x \neq y$, taking into account that every circular permutation of a solution of (7) gives rise to the same 4-cycle, we have

$$N_{[4]}(q) = \tfrac{1}{4}q(q-1)P_{[4]}(q),$$

where

$$P_{[4]}(q) = |\{(x,y)\,|\,x,y \in \mathbb{F}_q \backslash \{0,1\},\ x \neq y,\ (1-x)+(x-y)x+y^2=0\}|.$$

Assume q odd. The affine conic $(1-x)+(x-y)x+y^2=0$ has

$$q - \eta(-3) \tag{9}$$

rational points over $\mathbb{F}_q$. This can be seen by noticing that the associated projective conic has $q+1$ points and its points at infinity over $\bar{\mathbb{F}}_q$ are $[1,\omega,0]$, $[1,\omega^2,0]$ (where $\omega,\omega^2 \in \bar{\mathbb{F}}_q$ are the roots of T^2-T+1, i.e. $\omega = (-1+\sqrt{-3})/2$) which are rational if and only if $\eta(-3) \neq -1$.

From (9) we have to subtract the number of rational points (x,y) verifying one of the conditions $x,y \in \{0,1\}$ or $x=y$. All these conditions give rise to the following (at most) 10 points over $\bar{\mathbb{F}}_q$:

$$(0,i), \qquad (0,-i), \qquad (1+i,1), \qquad (1-i,1),$$

$$(1,\omega), \qquad (1,\omega^2), \qquad (\omega,0), \qquad (\omega^2,0), \qquad (\omega,\omega), \qquad (\omega^2,\omega^2),$$

where i is a root of T^2+1. The number of the above points which are rational over $\mathbb{F}_q$ is

$$2[1+\eta(-1)] + 3[1+\eta(-3)].$$

Subtracting the above quantity from (9), we obtain the statement for q odd.

If $q=2^n$, then first note that the affine transformation $y=Y+1$, $x=X+Y$ maps the affine conic (8) to

$$X^2+Y^2+XY=0.$$

Therefore, the number of solutions of (8) is $2^{n+1}-1$ if n is even and 1 if n is odd. We can write this number with one formula by

$$(1+(-1)^n)2^n-(-1)^n.$$

Finally, the five conditions $x,y \neq 0,1$ and $x \neq y$ are equivalent to $Y \neq 0,1$, $X \neq Y, X \neq Y+1$ and $X \neq 1$. So the total number of rational points over $\mathbb{F}_{2^n}$ that have to be removed is $1+3(1+(-1)^n)$. This concludes the proof. ■

3. PRODUCT OF TWO DISJOINT TRANSPOSITION POLYNOMIALS

Let us now consider the case of permutations which are product of two disjoint transpositions, that is whose conjugation class is [2 2]. In his paper of 1969, Wells announces the following formula. For completeness we will prove it here.

Theorem 3.1. *Suppose $q > 3$ is odd. Then*

$$N_{[2\ 2]}(q) = \tfrac{1}{8}q(q-1)(q-4)\{1+\eta(-1)\} \tag{10}$$

and if $q = 2^n$, then

$$N_{[2\ 2]}(2^n) = \tfrac{1}{8}2^n(2^n-1)(2^n-2).$$

Proof. Following the same lines of previous section, if q is odd, by (3), a permutation $(a\ b)\ (c\ d)$ with degree $<q-2$ has to satisfy the equation:

$$(a-b)^2 + (c-d)^2 = 0. \tag{11}$$

It is clear that this equation has a (admissible) solution if and only if -1 is a square in $\mathbb{F}_q$. In this case, if q is odd, for any of the $q(q-1)$ fixed choices of the first two variables (a_0, b_0) we have the linear equations:

$$c = d \pm \sqrt{-1}(a_0 - b_0),$$

where d can assume all possible values except the ones in the set

$$\{a_0, b_0, a_0 \mp \sqrt{-1}(a_0-b_0), b_0 \mp \sqrt{-1}(a_0-b_0)\}.$$

This analysis yields $2q(q-1)(q-4)$ solutions. If $q = 2^n$ with $n \geq 2$, then (11) becomes

$$a^2+b^2+c^2+d^2 = (a+b+c+d)^2 = 0$$

and for any of the $q(q-1)(q-2)$ choices of a, b, c, the value $d = a+b+c$ is not equal to a or b or c.

Finally, regardless of the characteristic, since the 8 solutions

$$(a,b,c,d), \quad (b,a,c,d), \quad (a,b,d,c), \quad (b,a,d,c),$$

$$(c,d,a,b), \quad (d,c,a,b), \quad (c,d,b,a), \quad (d,c,b,a)$$

give rise to the same permutation, we deduce the formula for $N_{[2\ 2]}(q)$. ■

4. 5-CYCLE POLYNOMIALS

In this section we will see the limits of the approach under consideration.

THEOREM 4.1. *Let q be a power of a prime p. Then*

$$N_{[5]}(q) = \tfrac{1}{5}q(q-1)P_{[5]}(q),$$

where

$$\begin{cases} P_{[5]}(q) = q^2 - (9 - \eta(5))q + 26 + 5\eta(-7) + 15\eta(-3) + 15\eta(-1) & \textit{if } \; p > 3, \\ P_{[5]}(3^n) = 3^{2n} - (9 - 6(-1)^n)3^n + 26 + 35(-1)^n, & (12) \\ P_{[5]}(2^n) = (2^n - 3 - (-1)^n)(2^n - 6 - 3(-1)^n). \end{cases}$$

Proof. Using, as in the previous sections, identity (6) and a transformation that eliminates two of the variables, we deduce that

$$N_{[5]}(q) = \tfrac{1}{5}q(q-1)P_{[5]}(q),$$

where $P_{[5]}(q)$ is the number of solutions (x, y, z) of

$$1 - x + x^2 - xy + y^2 - yz + z^2 = 0 \tag{13}$$

with $x, y, z \notin \{0, 1\}$, $x \neq y$, $y \neq z$ and $z \neq x$.

If q is odd, the affine transformation

$$(x, y, z) \mapsto (x - y + z - 2^{-1}, x - z - 2^{-1}, y - 2^{-1})$$

yields to the quadric

$$x^2 + y^2 + z^2 = 5/4$$

which has the same number of rational points of (13). Therefore, the number of rational points on (13), which can be calculated with the standard formulas that can be found in [5, Theorem 6.27], is

$$q^2 + q\eta(5). \tag{14}$$

If q is even then the quadric (13) is equivalent via the transformation $x = X + Y + Z,\ y = Y + 1,\ z = X + Y + 1$ to the quadric

$$X + YZ + Y^2 + Z^2 = 0$$

which has clearly q^2 points.

From (14) we have to subtract the number of points on the 9 quadratic curves obtained intersecting the previous surface with the following 9

TABLE I

			Number of points		
	Plane	Curve	$(6,q)=1$	$q=3^n$	$q=2^n$
1	$x=0$	$1+y^2-yz+z^2=0$	$q-\eta(-3)$	$3^n(1+(-1)^n)$	$2^n-(-1)^n$
2	$x=1$	$1-y+y^2-yz+z^2=0$	$q-\eta(-3)$	3^n	$2^n(1+(-1)^n)-(-1)^n$
3	$y=0$	$1-x+x^2+z^2=0$	$q-\eta(-1)$	$3^n(1+(-1)^n)-(-1)^n$	2^n
4	$y=1$	$2-2x+x^2-z+z^2=0$	$q-\eta(-1)$	$3^n(1+(-1)^n)-(-1)^n$	2^n
5	$z=0$	$1-x+x^2-xy+y^2=0$	$q-\eta(-3)$	3^n	$2^n(1+(-1)^n)-(-1)^n$
6	$z=1$	$2-x+x^2-xy+y^2-y=0$	$q-\eta(-3)$	$3^n(1+(-1)^n)$	$2^n-(-1)^n$
7	$x=y$	$1-x+x^2-xz+z^2=0$	$q-\eta(-3)$	3^n	$2^n(1+(-1)^n)-(-1)^n$
8	$x=z$	$1-z+2z^2-2yz+y^2=0$	$q-\eta(-1)$	$3^n(1+(-1)^n)-(-1)^n$	2^n
9	$y=z$	$1-x+x^2-xz+z^2=0$	$q-\eta(-3)$	3^n	$2^n(1+(-1)^n)-(-1)^n$

planes:

$$\begin{array}{lllll} x=0, & x=1, & y=0, & y=1, & z=0, \\ z=1, & x=y, & x=z, & y=z. & \end{array}$$

Note that all these quadrics are non-degenerate, except in characteristics 2 and 3: hence the cases $(6,q)=1$, $q=2^n$ and $q=3^n$ have to be considered separately. The equations of the 9 curves obtained in this way and the number of their points (calculated again with the formulas in [5, Theorems 6.26–6.32]) are listed in Table I.

Therefore, the total number of points to subtract from (14) is

$$\begin{cases} 9q-6\eta(-3)-3\eta(-1) & \text{if } (6,q)=1; \\ 9\cdot 3^n+5(-1)^n 3^n-3(-1)^n & \text{if } q=3^n; \\ 9\cdot 2^n+4(-1)^n 2^n-6(-1)^n & \text{if } q=2^n. \end{cases} \tag{15}$$

The final step is to add back the number of points that we have subtracted too many times, that is the points that lie in the intersection of two or more of the previous curves.

If the characteristic is odd, consider the following 19 pairs of points (see Table II) of the quadric (13) over $\overline{\mathbb{F}}_q$. Beside each pair of points we have written the number of quadrics of Table I to which the points belong.

The total number of points that has to be subtracted from (15) is therefore

$$26+5\eta(-7)+12\eta(-1)+9\eta(-3) \qquad \text{if } (6,q)=1 \tag{16}$$

and

$$26+17(-1)^n \qquad \text{if } q=3^n. \tag{17}$$

TABLE II

1	$(0,0,\pm i)$	3
2	$\left(0,1,\frac{1\pm\sqrt{-7}}{2}\right)$	2
3	$(0,\pm i,0)$	3
4	$\left(0,\frac{1\pm\sqrt{-7}}{2},1\right)$	2
6	$(1,1,\omega^{\pm 1})$	3
7	$(1,\omega^{\pm 1},0)$	2
8	$(1,1\pm i,1)$	3
9	$(\omega^{\pm 1},\omega^{\pm 1},\omega^{\pm 1})$	3
10	$(\omega^{\pm 1},\omega^{\pm 1},0)$	2
11	$(1\pm i,1\pm i,1)$	2
12	$(0,\pm i,\pm i)$	2
13	$(1,\omega^{\pm 1},\omega^{\pm 1})$	2
14	$\left(\frac{1\pm\sqrt{-7}}{4},0,\frac{1\pm\sqrt{-7}}{4}\right)$	2
15	$\left(\frac{3\pm\sqrt{-7}}{4},1,\frac{3\pm\sqrt{-7}}{4}\right)$	2
16	$(1\pm i,1,0)$	2
17	$\left(\frac{1\pm\sqrt{-7}}{2},0,1\right)$	2
18	$(\omega^{\pm 1},0,0)$	3
19	$(1\pm i,1,1)$	3

If the characteristic is even and ξ is a root of T^2+T+1 in $\bar{\mathbb{F}}_{2^n}$, then the corresponding points lying on more than one of the quadrics 1–9 are:

$$(0,0,1),\qquad (0,1,0),\qquad (0,1,1),\qquad (1,0,1)$$

each lying on 4 quadrics,

$$(\xi,\xi,\xi),\qquad (\xi,0,0),\qquad (1,1,\xi)$$

each lying on 3 quadrics and

$$(1,\xi,0),\qquad (\xi,\xi,0),\qquad (1,\xi,\xi)$$

each lying on 2 quadrics. The total number of points to be subtracted when $q=2^n$ is

$$12+9(1+(-1)^n), \tag{18}$$

because $\xi \in \mathbb{F}_{2^n}$ if and only if n is even.

Collecting together the various quantities, we obtain the formulas. ■

The same argument applied to permutations that are the product of a 3-cycle and a 2-cycle lead to the following result whose proof we omit.

THEOREM 4.2. *Let q be a power of a prime p. Then*

$$N_{[2\ 3]}(q) = \tfrac{1}{12}q(q-1)P_{[2\ 3]}(q)$$

where

$$P_{[2\ 3]}(q) = \begin{cases} (q^2 - (9 + \eta(-3) + 3\eta(-1))q & \text{if } p > 3; \\ \quad + (24 + 6\eta(-3) + 18\eta(-1) + 6\eta(-7))) & \\ (1 + (-1)^n)(3^{2n} - 9 \cdot 3^n + 24) & \text{if } q = 3^n; \\ (2^n - 3 - (-1)^n)(2^n - 6) & \text{if } q = 2^n. \end{cases}$$

5. GENERAL CONJUGATION CLASSES OF PERMUTATIONS

It is not difficult in principle to generalize the inclusion–exclusion argument of the previous sections to any conjugation class of permutation.

For example, if we want to compute $N_{[k]}(q)$, the number of k-cycles permutations σ of $\mathbb{F}_q$ such that $\partial f_\sigma < q-2$, then (see (5)), we want to count the number of $\sigma = (a_1, a_2, \ldots, a_k)$ for which

$$(a_1 - a_2)^2 + (a_2 - a_3)^2 + \cdots + (a_{k-1} - a_k)^2 + (a_k - a_1)^2 = 0.$$

We perform the transformation $a_{i+2} = x_i(a_1 - a_2) + a_1$, $i = 1, \ldots, k-2$ and simplify $(a_1 - a_2)^2$. Taking into account that there are q possibilities for a_1 and $q-1$ for a_2 and that circular permutations of the a_i's give rise to the same σ, we have that $N_{[k]}(q) = q(q-1)/k$ times the number of rational points of the quadric hypersurface

$$1 + (x_1 - 1)^2 + (x_2 - x_1)^2 + \cdots + (x_{k-3} - x_{k-2})^2 + x_{k-2}^2 = 0 \tag{19}$$

with the $(k+1)(k-2)/2$ conditions that $x_i \neq 0, 1$, $x_i \neq x_j$, for $i, j = 1, \ldots, k-2$ and $i \neq j$.

Let us assume for simplicity that q is odd. Then we can associate to the quadratic hypersurface in (19) the $(k-1) \times (k-1)$

matrix:

$$M_k = \begin{pmatrix} 2 & -1 & 0 & 0 & \cdots & 0 \\ -1 & 2 & -1 & 0 & & 0 \\ 0 & -1 & 2 & -1 & & 0 \\ \vdots & & -1 & \ddots & -1 & \\ 0 & & & -1 & 2 & -1 \\ 0 & & & & -1 & 2 \end{pmatrix}. \tag{20}$$

It is easy to see that the determinant of M_k is k. If $(q, k-1) = 1$, then the transformation of variables:

$$(x_1, x_2, \ldots, x_{k-2}) \mapsto \left(x_1 - \frac{k-2}{k-1}, x_2 - \frac{k-3}{k-1}, \ldots, x_{k-2} - \frac{1}{k-1} \right)$$

brings (19) to

$$x_1^2 + (x_2 - x_1)^2 + \cdots + (x_{k-3} - x_{k-2}) + x_{k-2}^2 + \frac{k}{k-1} = 0$$

which has matrix

$$\begin{pmatrix} k/(k-1) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & M_{k-1} & \\ 0 & & & \end{pmatrix}.$$

From [5, Theorems 6.26 and 6.27] we find that if $(q, (k-1)) = 1$, the number of rational points of (19) equals

$$a_k(q) = \begin{cases} q^{k-3} + q^{(k-3)/2}\eta((-1)^{(k-1)/2}k) & \text{if } k \text{ is odd}, \\ q^{k-3} + v(k)q^{(k-4)/2}\eta((-1)^{(k-2)/2}(k-1)) & \text{if } k \text{ is even}, \end{cases} \tag{21}$$

where $v(k) = -1$ if $(q, k) = 1$ and $v(0) = q - 1$.

If $(q, (k-1)) > 1$, then $k = 1$ in $\mathbb{F}_q$. In this case we can count the number of points on (19) as follows:

$$a_k(q) = \frac{1}{(q-1)}(a' - a''),$$

where a' is the number of solutions of the non-degenerate quadric

$$x_0^2 + (x_1 - x_0)^2 + (x_2 - x_1)^2 + \cdots + (x_{k-3} - x_{k-2})^2 + x_{k-2}^2 = 0$$

and a'' is the number of solutions of the degenerate quadric

$$x_1^2 + (x_2 - x_1)^2 + \cdots + (x_{k-3} - x_{k-2})^2 + x_{k-2}^2 = 0$$

which is equivalent to the quadric (non-degenerate in $k-3$ variables)

$$x_2^2 + (x_3 - x_2)^2 + \cdots + (x_{k-3} - x_{k-2})^2 + x_{k-2}^2 = 0$$

via the transformation

$$(x_1, x_2, \ldots, x_{k-2}) \mapsto (x_1, x_2 - 2x_1, x_3 - 3x_1 \ldots, x_{k-2} - (k-2)x_1).$$

Note that a' is the number of projective solutions of the projective quadric associated to (19) and a'' is the number of its solutions at infinity (i.e. on the hyperplane $x_0 = 0$).

From [5, Theorems 6.26 and 6.27] we have that

$$a' = \begin{cases} q^{k-2} + (q-1)q^{(k-3)/2}\eta((-1)^{(k-1)/2}) & \text{if } k \text{ is odd,} \\ q^{k-2} & \text{if } k \text{ is even} \end{cases}$$

and

$$a'' = \begin{cases} q^{k-3} + (q-1)q^{(k-3)/2}\eta((-1)^{(k-1)/2})) & \text{if } k \text{ is odd,} \\ q^{k-3} & \text{if } k \text{ is even.} \end{cases}$$

Therefore, we obtain that $a_k(q) = q^{k-3}$ when $(q, k-1) > 1$.

In all cases, if q is odd, we have the upper bound

$$N_{[k]}(q) \leq \frac{q(q-1)}{k} a_k(q).$$

To compute $N_{[k]}(q)$, we have to subtract from $a_k(q)$ the number of points in the $(k+1)(k-2)/2$ quadratic varieties obtained intersecting (19) with the hyperplanes $x_i = 0$, $x_i = 1$, $x_i = x_j$, for $i, j = 1, \ldots, k-2$, $i \neq j$ and so on. In each step we have to compute the number of solutions of some quadric equations over $\mathbb{F}_q$. However, we are not able to control how the discriminant of the quadrics behaves in the generic step.

In the case when $\mathscr{C} = [l_1 \ \cdots \ l_s]$ is a general conjugation class (after a transformation which reduces the number of variables to $c - s$, being $c = l_1 + \cdots + l_s$ the number of elements moved by any permutation in $\mathscr{C}$), one will have to consider a quadric hypersurface whose matrix will be

$$\begin{pmatrix} M_{l_1} & & & 0 \\ & M_{l_2} & & \\ & & \ddots & \\ 0 & & & M_{l_s} \end{pmatrix} \tag{22}$$

with determinant $l_1 \cdots l_s$. This can be used to deduce an upper bound for $N_{\mathscr{C}}(q)$.

If we use the other notation introduced in Section 1 for a conjugation class $\mathscr{C} = (m_1; m_2; \ldots; m_t)$, then we have that

$$N_{\mathscr{C}}(q) = \frac{q(q-1)}{m_2!2^{m_2} \cdots m_t!t^{m_t}} P_{\mathscr{C}}(q) \qquad \text{and} \qquad P_{\mathscr{C}}(q) = a_0 + a_1 q + \cdots + a_{c-3} q^{c-3},$$

where, when q is odd, each a_i is an expression of the form

$$a_i = a_{i1}\eta(\alpha_{i1}) + \cdots + a_{ij_i}\eta(\alpha_{ij_i})$$

with $a_{ij}, \alpha_{ij} \in \mathbb{Z}$. Furthermore, $a_{c-3} = 1$ for q large enough with respect to c.

Finally, note that α_{ij} is, up to a sign, the discriminant of a quadratic form which is the intersection of (19) with a number of hyperplanes among $x_i = 0, 1$, $x_i = x_j$, $i, j = 1, \ldots, k-2$. This implies that there are finitely many possibilities for α_{ij}. Hence, the expressions $P_{\mathscr{C}}(q)$ can be calculated by computing $N_{\mathscr{C}}(q)$ for sufficiently many values of q and by solving linear equations. For example using Pari [8] we calculated, if $q = p^n$ and $p > 3$:

$$\begin{aligned} P_{[6]}(q) &= q^3 - 14q^2 + [68 - 6\eta(5) - 6\eta(50)]q - [154 + 66\,\eta(-3) \\ &\qquad +93\eta(-1) + 12\eta(-2) + 54\eta(-7)], \\ P_{[4\ 2]}(q) &= q^3 - [14 - \eta(2)]q^2 + [71 + 12\eta(-1) + \eta(-2) + 4\eta(-3) - 8\eta(50)]q \\ &\qquad -[148 + 100\eta(-1) + 24\,\eta(-2) + 44\eta(-3) + 40\,\eta(-7)], \\ P_{[3\ 3]}(q) &= q^3 - 13q^2 + [62 + 9\eta(-1) + 4\,\eta(-3)]q \\ &\qquad -[150 + 99\eta(-1) + 42\eta(-3) + 72\eta(-7)], \\ P_{[2\ 2\ 2]}(q) &= q^3 - [14 + 3\eta(-1)]q^2 + [70 + 36\eta(-1) + 6\eta(-2)]q \\ &\qquad -[136 + 120\eta(-1) + 48\eta(-2) + 8\,\eta(-3)], \end{aligned}$$

$$\begin{aligned}
P_{[6]}(3^n) &= 3^{3n} - [14+2(-1)^n]3^{2n} + [71+39(-1)^n]3^n - [162+147(-1)^n],\\
P_{[4\ 2]}(3^n) &= 3^{3n} - [14+3(-1)^n]3^{2n} + [72+40(-1)^n]3^n - [164+140(-1)^n],\\
P_{[3\ 3]}(3^n) &= (1+(-1)^n)3^{3n} - [14+15(-1)^n]3^{2n} + [71+81(-1)^n]3^n\\
&\quad -[150+171(-1)^n],\\
P_{[2\ 2\ 2]}(3^n) &= 3^{3n} - [14+3(-1)^n]3^{2n} + [76+36(-1)^n]3^n - [168+120(-1)^n]
\end{aligned}$$

and

$$\begin{aligned}
P_{[6]}(2^n) &= (2^n-3-(-1)^n)(2^{2n}-(11-(-1)^n)2^n+(41+7(-1)^n)),\\
P_{[4\ 2]}(2^n) &= (2^n-3-(-1)^n)(2^{2n}-11\cdot 2^n+37+(-1)^n),\\
P_{[3\ 3]}(2^n) &= (2^n-3-(-1)^n)(2^{2n}-(10-(-1)^n)2^n+45-3(-1)^n)),\\
P_{[2\ 2\ 2]}(2^n) &= (2^n-2)(2^n-4)(2^n-8).
\end{aligned}$$

As a last consequence of the above discussion we have that

PROPOSITION 5.1. *Suppose $\mathscr{C}$ is a fixed conjugation class of permutations. Then*

$$N_{\mathscr{C}}(q) = \frac{q^{c-1}}{c_2!2^{c_2}\cdots c_t!t^{c_t}}\left(1+O\left(\frac{1}{q}\right)\right).$$

Therefore, since by (4)

$$|\mathscr{C}| = \frac{q^{c}}{c_2!2^{c_2}\cdots c_t!t^{c_t}}\left(1+O\left(\frac{1}{q}\right)\right),$$

the probability that an element of $\sigma \in \mathscr{C}$ is such that $\partial f_\sigma < q-2$ is

$$\frac{1}{q}+O\left(\frac{1}{q^2}\right).$$

6. PERMUTATIONS OF $\mathbb{F}_{2^n}$ THAT ARE PRODUCT OF 2-CYCLES

A permutation has order 2 if and only if its cycle decomposition consists only of cycles of length 2. Let $\mathscr{T}_r = [2\ 2\ \ldots\ 2]$ be the conjugation class of those permutations of $\mathbb{F}_q$ which have a cycle decomposition consisting of r cycles of length 2.

THEOREM 6.1. *Let $q=2^n$. Then $N_{[2]}(2^n)=0$ and the following recursive relation holds*:

$$N_{\mathscr{T}_r}(q) = \frac{q!}{r!2^r(q-2r+1)!} - \frac{(q-2(r-1))(2r-1)}{2r}N_{\mathscr{T}_{r-1}}(q).$$

Therefore (*in accordance with the formulas already proven*):

$$\begin{aligned} N_{[2\ 2]}(2^n) &= \tfrac{1}{8}2^n(2^n-1)(2^n-2),\\ N_{[2\ 2\ 2]}(2^n) &= \tfrac{1}{48}2^n(2^n-1)(2^n-2)(2^n-4)(2^n-8),\\ N_{[2\ 2\ 2\ 2]}(2^n) &= \tfrac{1}{384}2^n(2^n-1)(2^n-2)(2^n-4)(2^n-6)(2^{2n}-15\cdot 2^n+71). \end{aligned}$$

Proof. We have observed in the Introduction that all transpositions have permutation polynomial with degree exactly $q-2$ so

$$N_{[2]}(2^n) = 0.$$

The polynomial $A_{\mathscr{C}}$ of (5) is in this case:

$$\begin{aligned} A_{T_r}(\underline{x}) &= \sum_{\substack{i=1\\ i\ \text{odd}}}^{2r} x_i(x_i - x_{i+1}) + \sum_{i=1}^{r} x_{2i}(x_{2i} - (x_{2i-1}))\\ &= \sum_{i=1}^{2r} x_i^2 + 2\sum_{i=1}^{r} x_{2i}x_{2i-1}\\ &= \sum_{i=1}^{2r} x_i^2\\ &= \left(\sum_{i=1}^{2r} x_i\right)^2. \end{aligned}$$

From this, applying (6), we have that

$$N_{\mathscr{T}_r}(q) = \frac{1}{r!2^r}\left|\left\{\underline{x}\in\mathbb{F}_q^{2r}:\quad \underline{x}\text{ has coordinates all distinct and }\sum_{i=1}^{2r} x_i = 0\right\}\right|.$$

For simplicity, call $\mathscr{N}_r$ the last set above. Let start selecting arbitrarily $2r-1$ distinct values $(x_1,\dots,x_{2r-1})$ for the first $2r-1$ coordinates of $\underline{x}\in\mathbb{F}_q^{2r}$: this can be done in $q(q-1)\cdots(q-(2r-2))$ ways. For each such choice, the value of the last coordinate is uniquely determined by $x_{2r} = \sum_{j<2r} x_j$ if we want to have $\underline{x}\in\mathscr{N}_r$. However, a value for x_{2r} is not admissible if it coincides with one of the previous coordinates. There are $2r-1$ possible indices j_0 where this can happen and if $\sum_{j<2r} x_j = x_{2r} = x_{j_0}$, then

$$\sum_{\substack{j=1\\ j\neq j_0}}^{2r-1} x_j = 2x_{j_0} + \sum_{\substack{j=1\\ j\neq j_0}}^{2r-1} x_j = \sum_{j=1}^{2r} x_j = 0,$$

that is $(x_1, \dots, x_{j_0-1}, x_{j_0+1}, \dots, x_{2r-1}) \in \mathcal{N}_{r-1}$. So for each choice of index j_0, the number of possible values for $\{x_1, \dots, x_{2r-1}\} \setminus \{x_{j_0}\}$ above is $|\mathcal{N}_{r-1}|$. Taking into account that for any choice of an element in $\mathcal{N}_{r-1}$, there are $q - 2r + 2$ choices for x_{j_0}, we deduce that

$$|\mathcal{N}_r| = \frac{q!}{(q-2r+1)!} - (q - 2(r-1))(2r-1)|\mathcal{N}_{r-1}|,$$

which, in view of the fact that

$$N_{\mathcal{T}_r}(q) = \frac{|\mathcal{N}_r|}{r! 2^r},$$

is equivalent to the statement. This concludes the proof. ■

7. CONCLUSION

In a forthcoming paper we will deal with the problem of counting permutation polynomials with minimal possible degree in a fixed conjugation class. Note also that S. Konyagin and the second author have recently proved that if

$$\mathcal{N} = |\{\sigma \text{ permutation of } \mathbb{F}_q \text{ such that } \partial f_\sigma < q-2\}|,$$

then

$$|\mathcal{N} - (q-1)!| \leq \sqrt{\frac{2e}{\pi}}\, q^{q/2}$$

which confirms the common belief that almost all permutation polynomials have degree $q - 2$. A similar result has been proven independently by Pinaki Das.

ACKNOWLEDGMENT

We would like to thank the referee for some useful comments and corrections.

REFERENCES

1. J. Levine and J. V. Brawley, Some cryptographic applications of permutation polynomials, *Cryptologia* **1**, No. 1 (1977), 76–92.

2. R. Lidl and W. B. Müller, A note on polynomials and functions in cryptography, *Ars Combin.* **17**-A (1984), 223–229.

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

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

5. R. Lidl and H. Niederreiter, Finite fields, "Encyclopedia of Mathematics and its Applications," Vol. 20, Addison-Wesley Publishing Company, Reading, MA, 1983.

6. G. L. Mullen, Permutation polynomials over finite fields, *in:* "Finite fields, coding theory, and advances in communications and computing," Las Vegas, NV, 1991, pp. 131–151, Lecture Notes in Pure and Applied Mathematics, Vol. 141, Dekker, New York, 1993.

7. C. Wells, The degrees of permutation polynomials over finite fields, *J. Combin. Theory* **7** (1969), 49–55.

8. C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier, GP/PARI Calculator Version 2.0.14 1989–1999.