# On the enumeration of Permutation Polynomials (Extended abstract)

Claudia Malvenuto and Francesco Pappalardi

**Abstract**

Given a permutation $\sigma$ of the elements of a finite field $\mathbb{F}_q$, the permutation polynomial $f_\sigma \in \mathbb{F}_q[x]$ is the unique polynomial with degree less than $q-1$ that has the property that $f_\sigma(t) = \sigma(t)$ for every $t \in \mathbb{F}_q$. We consider the natural question of enumerating the permutations in a given conjugacy class for which the permutation polynomial has degree strictly less than $q-2$. We give formulas that extend existing ones. Furthermore for the case of $k$–cycles, we consider the harder problem of enumerating the permutations within a given conjugacy class for which the permutation polynomial has minimal degree. After giving an upper bound and a lower bound (for $q \equiv 1 \pmod{k}$) we consider various examples in which interesting Galois properties arise.

**Résumé**

Soit $\sigma$ une permutation des éléments d'un corps fini $\mathbb{F}_q$: le polynôme de permutation $f_\sigma \in \mathbb{F}_q[x]$ est le seul polynôme ayant degré inférieur à $q-1$ et tel que $f_\sigma(t) = \sigma(t)$ pour chaque $t \in \mathbb{F}_q$. Nous considérons la question naturelle d'énumérer les permutations dans une classe de conjugaison donnée dont le polynôme de permutation ait un degré strictement inférieur à $q-2$. Nous donnons des formules qui étendent celles dejà connues. De plus dans le cas de $k$–cycles, nous considérons le problème plus complexe d'énumérer les permutations dans une classe de conjugaison donnée dont le polynôme de permutation associé ait un degré minimal. Après avoir donné des bornes supérieure et inférieure (pour $q \equiv 1 \pmod{k}$) nous prenons en considération divers exemples qui possèdent des propriétés de Galois intéressantes.

## 1 Introduction

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

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

Such a polynomial has the property that

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

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

Permutation polynomials have increasingly attracted the attentions of various researchers in the past couple of decades. We suggest the inspiring survey papers by Rudolf Lidl and Gary Mullen[1] for an introduction. A key exchange protocol for public key cryptography based on permutation polynomials has been proposed by Joel V. Brawley[2]

Let us denote with $S_\sigma$ the set of elements of $\mathbb{F}_q$ that are moved by $\sigma$. Note that if $\sigma$ and $\sigma'$ are conjugated, then $|S_\sigma| = |S_{\sigma'}|$.

We have that $\partial(f_\sigma) \geq q - |S_\sigma|$. To see this it is enough to note that by the first property of the definition, the polynomial $f_\sigma(x) - x$ has as roots all the elements of $\mathbb{F}_q$ which are not in $S_\sigma$. 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 polynomials of degree $q-2$ while the degree of a 3–cycle can be $q-2$ or $q-3$.

Let $\mathcal{C}$ be a conjugation class of permutations of a finite field $\mathbb{F}_q$. We consider the function $N_{\mathcal{C}}(q)$ defined as the number of permutations in $\mathcal{C}$ for which the associated permutation polynomial has degree $< q-2$.

In 1969, C. Wells[3] proved the formula

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

where $[k]$ denotes the conjugation class of $k$–cycles.

## 2 Permutation Polynomials with non–maximal degree

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 $[2\ 2\ 2]$.

Namely, suppose $q$ is odd and let $\eta$ denote the quadratic character [4] of $\mathbb{F}_q$. Then

[1] *When does a polynomial over a finite field permute the elements of the field?* Amer. Math. Mon. **95** (1988), 243–246, Amer. Math. Mon. **100** (1993), 71–74 )

[2] *Some Cryptographic Applications of Permutation Polynomials*, Cryptologia **1**, Number 1, (1977) 76–92.

[3] *The degrees of permutation polynomials over finite fields*, J. Combinatorial Theory **7** (1969) 49–55

[4] i.e. $\eta(a) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_q \\ -1 & \text{if } a \text{ is not a square in } \mathbb{F}_q \\ 0 & \text{if } a=0 \end{cases}$

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

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

$$\begin{aligned} N_{[5]}(q) = & \tfrac{1}{5}q(q-1) \\ & (q^2-(9-\eta(5)-5\eta(-1)+5\eta(-9))\,q+26+5\eta(-7) \\ & +15\eta(-3)+15\eta(-1)) \end{aligned}$$

$$\begin{aligned} N_{[2\ 3]}(q) = & \tfrac{1}{12}q(q-1) \\ & (q^2-(9+\eta(-3)+3\eta(-1))q+(24+6\eta(-3)+18\eta(-1)+6\eta(-7))) \\ & +\eta(-1)(1-\eta(9))q(q-5) \end{aligned}$$

The case of even characteristics has also been settled[5]. Suppose $q = 2^n$. Then

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

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

$$N_{[5]}(2^n) = \tfrac{1}{5}2^n(2^n-1)(2^n-3-(-1)^n)(2^n-6-3(-1)^n)$$

$$N_{[2\ 3]}(2^n) = \tfrac{1}{12}2^n(2^n-1)(2^n-3-(-1)^n)(2^n-6).$$

Similar formulas (which we report at the end of this section) have been computed for the four conjugation classes of permutations that move 6 elements.
As an example let us produce the proof that

**Proposition 1** *If $q$ is odd, then*

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

**Proof.** The first step consists in showing that if $a,\ b,\ c,\ d \in \mathbb{F}_q$ (all distinct) such that the 4–cycle $\sigma = (a\ b\ c\ d)$ is counted by $N_{[4]}(q)$, have to satisfy the equation:

$$(a-b)a+(b-c)b+(c-d)c+(d-a)d = 0. \tag{1}$$

Indeed, if $f_\sigma$ is the permutation polynomial of $\sigma$ and we write

$$f_\sigma(x) = A_1x^{q-2}+A_2x^{q-3}+\cdots+A_{q-2}x+A_{q-1},$$

then

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

Since the squares of all the elements of $\mathbb{F}_q$ add up to zero, the previous formula

[5]Part of the formulas for even characteristics are due to A. Conflitti

can be written as

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

In our case, $S_\sigma = \{a, b, c, d\}$. Therefore $A_1(\sigma)$ equals to the left hand side of (1). Since $N_{[4]}(q)$ counts the $\sigma$ for which $A_1(\sigma) = 0$, we conclude the first step of the proof.
Now for each of the $q(q-1)$ fixed choices of $a$ and $b$ distinct in $\mathbb{F}_q$,
substituting in (1), $c = x(b-a)+a$, $d = y(b-a)+a$, we obtain the equation

$$(1-x)+(x-y)x+y^2 = 0 \tag{2}$$

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

$$N_{[4]}(q) = \frac{1}{4}q(q-1)C_q$$

where

$$C_q = |\,\{(x,y)\ \big|\ x,y\in\mathbb{F}_q\setminus\{0,1\},\ x\neq y,\ (1-x)+(x-y)x+y^2=0\,\}\,|$$

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

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

rational points over $\mathbb{F}_q$.

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

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

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

$$(1,\omega),\quad (1,\overline{\omega}),\quad (\omega,0),\quad (\overline{\omega},0),\quad (\omega,\omega),\quad (\overline{\omega},\overline{\omega})$$

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 (3), we obtain the statement. □

In general if $q > k$ is odd, the

$$N_{[k]}(q) = \frac{1}{k} q(q-1) P_k(q)$$

where

$$P_k(x) = x^{k-3} + a_1 x^{k-4} + \cdots a_{k-3}$$

and the coefficients

$$a_i = \eta(\alpha_{i,1}) b_{i,1} + \cdots + \eta(\alpha_{i,s_i}) b_{i,s_i}$$

for appropriate integers $\alpha_{i,j}, \beta_{i,j}$. There are ways to compute upper bounds for $\alpha_{i,j}, \beta_{i,j}$ and $s_i$.

For example we can prove that for $k$ odd

$$\alpha_{i,j} \leq \binom{k}{i}^k.$$

This allows (in principle) to calculate formulas for $N_{[k]}(q)$, for any value of $k$ as long as one has calculated it for sufficiently many values of $q$.

For the general case, we can give some estimates. For example

$$P_k(q) = q^{k-3} + O(k^2 q^{k-4}).$$

Therefore

$$N_{[k]}(q) = \frac{1}{k} \left( q^{k-1} + O(k^2 q^{k-2}) \right).$$

We conclude this section with two tables containing the formulas announced. The first holds for $q$ odd[6].

**Table 1: Permutation that move 6 elements in odd characteristics**

| | |
|---|---|
| $N_{[6]}(q) = \frac{1}{6} q(q-1)$ | $q^3 - 14q^2 + (68 - 6\eta(5) - 6\eta(50))q$ $-(154 + 66\eta(-3) + 93\eta(-1) + 12\eta(-2) + 54\eta(-7)) +$ $(-2\eta(-1)q^2 + (3 + 51\eta(-1))q + 4)(1 + \eta(9))$ |
| $35?N_{[4\ 2]}(q) = \frac{1}{8} q(q-1)$ | $q^3 - (14 - \eta(2))q^2 + (71 + 12\eta(-1) + \eta(-2) + 4\eta(-3) - 8\eta(2))q$ $-(148 + 100\eta(-1) + 24\eta(-2) + 44\eta(-3) + 40\eta(-7))$ |
| $3?N_{[3\ 3]}(q) = \frac{1}{18} q(q-1)$ | $q^3 - 13q^2 + (62 + 9\eta(-1) + 4\eta(-3))q$ $-(150 + 99\eta(-1) + 42\eta(-3) + 72\eta(-7))$ |
| $N_{[2\ 2\ 2]}(q) = \frac{1}{48} q(q-1)$ | $q^3 - (14 + 3\eta(-1))q^2 + (70 + 36\eta(-1) + 6\eta(-2))q$ $-(136 + 120\eta(-1) + 48\eta(-2) + 8\eta(-3) + 16(1 - \eta(9)))$. |

**Table 2: Permutation that move 6 elements in even characteristics**

$$N_{[6]}(2^n) = \tfrac{1}{6} 2^n (2^n - 1)(2^n - 3 - (-1)^n)(2^{2n} - (11 - (-1)^n)2^n + (41 + 7(-1)^n))$$

$$N_{[4\ 2]}(2^n) = \tfrac{1}{8} 2^n (2^n - 1)(2^n - 3 - (-1)^n)(2^{2n} - 11 \cdot 2^n + 37 + (-1)^n)$$

$$N_{[3\ 3]}(2^n) = \tfrac{1}{18} 2^n (2^n - 1)(2^n - 3 - (-1)^n)(2^{2n} - (10 - (-1)^n)2^n + 45 - 3(-1)^n))$$

$$N_{[2\ 2\ 2]}(2^n) = \tfrac{1}{48} 2^n (2^n - 1)(2^n - 2)(2^n - 4)(2^n - 8).$$

[6]The symbols 35? (resp. 3?) means that for characteristic 3 and 5 (resp 3), the formula needs adjustment.

## 3 $k$-cycle Permutation Polynomials with minimal degree

As we noticed above, if a permutation $\sigma$ moves $c$ elements of $\mathbb{F}_q$ then

$\partial(f_\sigma) \geq q - c$. For example the permutation polynomial of any $k$–cycle has degree at least $q - k$. For practical applications it is very important to produce permutation polynomials with "small" degree.

This justifies the definition. For a given conjugation class $\mathcal{C}$, let $c = c(\mathcal{C})$ be the number of elements moved by any element of $\mathcal{C}$. Then

$$m_{\mathcal{C}}(q) = \{\sigma \in \mathcal{C} \mid \partial(f_\sigma) = q - c\}$$

(i.e. the permutations in $\mathcal{C}$ such that their permutation polynomial has minimal degree)

The first elementary lower bound is:

**Proposition 2** *With the above notations, assume that $q > 4$. If $m_{\mathcal{C}}(q) \neq 0$, then*

$$m_{\mathcal{C}}(q) \geq \frac{1}{c^2} q(q-1).$$

**Proof.** Let $\sigma_0$ be a permutation in $m_{\mathcal{C}}(q)$, $a, b \in \mathbb{F}_q$, $a \neq 0$ and $L_{a,b}$ is the linear transformation[7] of $\mathbb{F}_q$, then $L_{a,b}^{-1}\sigma_0 L_{a,b} \in m_{\mathcal{C}}(q)$.

It is easy to see that the number of distinct elements in $m_{\mathcal{C}}(q)$ produced in this way equals to the index of the centralizer $C_{\sigma_0}$. of $\sigma_0$ in $\mathbb{A}^1(\mathbb{F}_q)$.

We claim that $|C_{\sigma_0}| \leq c^2$. Indeed assume first that $\sigma_0(0) \neq 0$ and $\sigma_0(1) \neq 1$. Then if $a, b \in \mathbb{F}_q$, $a \neq 0$ and

$$\sigma_0 L_{a,b} = L_{a,b}\sigma_0,$$

for all $x \in \mathbb{F}_q$, $\sigma_0(ax + b) = a\sigma_0(x) + b$.

If we substitute $x = 0$, we obtain $\sigma_0(b) - b = a\sigma_0(0) \neq 0$. So $b \in S_{\sigma_0}$. If we substitute $x = 1$, we obtain $\sigma_0(a + b) - (a + b) = a(\sigma_0(0) - 1) \neq 0$. So $a + b \in S_{\sigma_0}$.

Finally $b \in S_{\sigma_0}$ can be chosen in at most $c$ distinct ways and for each fixed $b$, $a \in S_{\sigma_0} - b$ can also be chosen in at most $c$ distinct ways.

If $\sigma_0(0) = 0$ or $\sigma_0(1) = 1$, then one can chose $a_0, b_0 \in \mathbb{F}_q$ such that

$$\sigma(b_0) \neq b_0 \quad \sigma(a_0 + b_0) \neq a_0 + b_0.$$

and replace $\sigma_0$ by $\sigma_1 = L_{a_0,b_0}^{-1}\sigma L_{a_0,b_0}$.

Therefore if not $m_{\mathcal{C}}(q)$ is not empty, we have that

$$|m_{\mathcal{C}}(q)| \geq \frac{1}{c^2} q(q-1)$$

and this concludes the proof. □

We can improve the previous result for some $k$–cycles.

**Theorem 1** *If $q \equiv 1 (\mathrm{mod} k)$ then*

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

[7] The group $\mathbb{A}^1(\mathbb{F}_q)$ of linear transformations of $\mathbb{F}_q$ consists on those maps $L_{a,b} : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto ax + b$. This group has order $q(q-1)$.

Furthermore, using algebraic geometry, we prove the upper bound

**Theorem 2** *If $q \geq k$, then*

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

In principle one should be able to prove similar estimates for other conjugation classes of permutations. However, technical problems arise. For permutations that move less then 5 elements we study the problem in detail. For example

$$|m_{[4]}(q)| = \frac{1}{4} q(q-1) K_q$$

where

$$K_q = 1 + \eta(-1) + \begin{cases} 4 & \text{if } q \equiv 1 \pmod 5 \\ 0 & \text{otherwise} \end{cases}$$

The formulas for 5–cycles are more complicated.

Next we restrict our attention to prime fields.

We deal with the problem of studying how sharp is the previous estimate. We provide evidence of the fact that the estimate is essentially the best possible. This will be a consequence of the Chebotarev Density Theorem. More precisely, let $a$ be an integer with $1 \leq a \leq (k-1)!$ and consider the function:

$$F_{a,k}(x) = \{p \leq x \mid p \text{ prime}, p \geq k, N_{[k]}(p) = \frac{a}{k}(p(p-1))\}.$$

If $\pi(x)$ is the number of primes up to $x$, $F_{a,k}(x)/\pi(x)$ measures the probability that a $\mathbb{F}_p$ has exactly $\frac{a}{k}(p(p-1))$ $k$–cycle permutation polynomial with minimal degree $p-k$. It is natural to expect that this probability tends to a finite limit as $x$ tends to $\infty$. That is to say that one expects.

$$F_{a,k}(x) \sim c_{a,k}\pi(x),$$

Where the condition $c_{a,k} = 0$ should be interpreted as to say that $F_{a,k}(x) = 0$. We conjecture that $c_{(k-1)!,k} \neq 0$. In general $c_{(k-1)!,k} \leq 1/(k-1)!!$. However it is difficult to compute. We can show that $c_{3!,4} = 1/8$ and $c_{5!,6} \leq 1/(288 \cdot 108!)$. Furthermore $c_{4!,5} = 1/60000$. Here is a list of the first few primes that enjoy the property $N_{[5]}(p) = 24(p(p-1))/5$.

| | | | | | |
|---|---|---|---|---|---|
| 471301 | 1695341 | 2134241 | 3676831 | 4845761 | 4938181 |
| 5892011 | 8276131 | 8748281 | 9589201 | 10922651 | 10996471 |
| 11208671 | 11622601 | 11683751 | 11794661 | 13910161 | 13950281 |
| 14679361 | 15379361. | | | | |

Although $1/30000 = 0.000016\%$ seems a small a small proportion of primes. It is surprisingly high respect to the bound $c_{4!,5} \leq 1/24! \sim 1.6 \cdot 10^{-24}$.

The bulk of our technique is based on the reduction of the problem of determining the solutions over $\mathbb{F}_q$
of a family of homogeneous equations defined over $\mathbb{Z}$.
We bound this number by the number of solutions over $\overline{\mathbb{Q}}$ which
after proving finiteness is estimated with the Bezout Theorem. The algebraic structure of the minimal field which contains all the solutions and its Galois group over $\mathbb{Q}$ will be used to attack the conjecture.
The results described in this note will appear in two papers:


1. C. Malvenuto & F. Pappalardi, *Enumerating Permutation Polynomials I: permutations with non maximal degree*, Preprint
2. C. Malvenuto & F. Pappalardi, *Enumerating Permutation Polynomials II: k–cycles with minimal degree*, Preprint



Claudia Malvenuto
Dipartimento di Scienze dell'Informazione
Università degli studi "La Sapienza"
Via Salaria, 113
I–00198, Roma – ITALY
claudia@dsi.uniroma1.it

Francesco Pappalardi
Dipartimento di Matematica
Università Roma Tre
Largo S. L. Murialdo, 1
I–00146, Roma – ITALY
pappa@mat.uniroma3.it