

CORRIGENDUM TO
“ENUMERATING PERMUTATION POLYNOMIALS I:
PERMUTATIONS WITH NON-MAXIMAL DEGREE”

CLAUDIA MALVENUTO AND FRANCESCO PAPPALARDI

ABSTRACT. This note corrects a statement that appeared in *Finite Fields Appl.* **8** (2002) no. 4, 531–547. It also provides a self contained proof.

Let \mathbb{F}_q be a finite field with q elements and suppose \mathcal{C} is a conjugation class of permutations of the elements of \mathbb{F}_q . We denote by $\mathcal{C} = (c_1; c_2; \dots; c_t)$ the conjugation class of permutations that admit a cycle decomposition with c_i i -cycles ($i = 1, \dots, t$). Further we set $c = 2c_2 + \dots + tc_t = q - c_1$ to be the number of elements of \mathbb{F}_q moved by any permutation in \mathcal{C} .

If $\sigma \in \mathcal{C}$ then the permutation polynomial associated to σ is defined as

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

Therefore for $q > 3$ the function

$$N_{\mathcal{C}}(q) = \# \left\{ \sigma \in \mathcal{C} \mid \sum_{x \in \mathbb{F}_q} x(\sigma(x) - x) = 0 \right\}$$

enumerates the permutations in \mathcal{C} whose permutation polynomials have degree strictly less than $q - 2$.

The reviews of [2] that appeared in Math Reviews (MR1933624 (2003j:11146)) and in Zentralblatt Math (Zbl 1029.11068) point out that the case of transpositions provides a counterexample to the statement of Proposition 5.1. The statement is also obviously wrong in the cases of three-cycles and the case of the conjugation class of the product of two transpositions (see [2, Theorems 1.1 and 3.1]). For brevity, we will indicate these three classes of permutations respectively by [2], [3] and [2 2]. Other counterexamples to Proposition 5.1 occur if the characteristic of \mathbb{F}_q is “small”. The correct statement should read:

Proposition 5.1. *Suppose $\mathcal{C} = (c_1; c_2; \dots; c_t)$ is a fixed conjugation class of permutations which does not coincide with the classes [2], [3] and [2 2]. Then, if $\text{char}(\mathbb{F}_q) > 2$ and does not divide $2^{c_2} \dots t^{c_t}$, we have*

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

Therefore, since $|\mathcal{C}| = \frac{q^c}{c_2! 2^{c_2} \dots c_t! t^{c_t}} \left(1 + O\left(\frac{1}{q}\right) \right)$, as $\text{char}(\mathbb{F}_q) \rightarrow \infty$, the probability that an element of $\sigma \in \mathcal{C}$ is such that the degree $\partial f_\sigma < q - 2$ is $\frac{1}{q} + O\left(\frac{1}{q^2}\right)$.

Date: July 5, 2005.

Proof. We associate to \mathcal{C} the quadratic form in c variables

$$Q_{\mathcal{C}}(\underline{X}) = \sum_{i=2}^t \sum_{j=1}^{c_i} (X_{ij1}(X_{ij1} - X_{ij2}) + X_{ij2}(X_{ij2} - X_{ij3}) + \cdots + X_{ij i}(X_{ij i} - X_{ij1})).$$

Let $\hat{N}(Q_{\mathcal{C}})$ be the number of solutions of $Q_{\mathcal{C}}(\underline{X}) = 0$ over \mathbb{F}_q with all distinct coordinates. We have that

$$(1) \quad N_{\mathcal{C}}(q) = \frac{\hat{N}(Q_{\mathcal{C}})}{c_2! 2^{c_2} \cdots c_t! t^{c_t}}$$

since the denominator above counts the number of distinct representations of any permutation in \mathcal{C} as product of disjoint cycles.

Next we consider the inequalities:

$$N(Q_{\mathcal{C}}) - \sum_I N(Q_{\mathcal{C}}^I) \leq \hat{N}(Q_{\mathcal{C}}) \leq N(Q_{\mathcal{C}})$$

where the sum ranges over 2-element sets of variables $I = \{X_{i_1 j_1 k_1}, X_{i_2 j_2 k_2}\}$ of the quadratic form $Q_{\mathcal{C}}$, where $Q_{\mathcal{C}}^I$ denotes the quadratic form in $c-1$ variables obtained by $Q_{\mathcal{C}}$ substituting $X_{i_1 j_1 k_1} = X_{i_2 j_2 k_2}$ and for any quadratic form Q , $N(Q)$ denotes the number of solutions over \mathbb{F}_q of $Q = 0$.

Note that if $\mathcal{C} \neq [2]$, then $Q_{\mathcal{C}}^I \neq 0$ (indeed if X_{rst} is a variable not in I , then the coefficient of X_{rst}^2 in Q^I is 1). From this we deduce that $N(Q_{\mathcal{C}}^I) \leq 2q^{c-2}$. Hence we obtain that

$$(2) \quad \hat{N}(Q_{\mathcal{C}}) = N(Q_{\mathcal{C}}) + O(q^{c-2}).$$

Furthermore note that $Q_{\mathcal{C}}$ is equivalent to the form in $\tilde{c} = c - (c_2 + \cdots + c_t)$ variables $\tilde{Q}_{\mathcal{C}}(\underline{Y})$

$$= \sum_{\substack{2 < i \leq t \\ j \leq c_i}} \left(Y_{ij1}(Y_{ij1} - Y_{ij2}) + \cdots + Y_{ij(i-2)}(Y_{ij(i-2)} - Y_{ij(i-1)}) + Y_{ij(i-1)}^2 \right) + \sum_{j \leq c_2} Y_{2j1}^2,$$

where the equivalence is obtained with the linear transformation

$$\begin{cases} X_{ijk} = Y_{ijk} + Y_{iji} & i = 2, \dots, t; \ j = 1, \dots, c_i; \ k = 1, \dots, i-1; \\ X_{iji} = Y_{iji} & i = 2, \dots, t; \ j = 1, \dots, c_i. \end{cases}$$

If q is odd and $i > 2$, the $(i-1) \times (i-1)$ matrix

$$\mathcal{M}_i = \begin{pmatrix} 1 & -\frac{1}{2} & 0 & 0 & \cdots & 0 \\ -\frac{1}{2} & 1 & -\frac{1}{2} & 0 & \cdots & 0 \\ 0 & -\frac{1}{2} & 1 & -\frac{1}{2} & \cdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & -\frac{1}{2} & 1 & -\frac{1}{2} \\ 0 & 0 & \cdots & 0 & -\frac{1}{2} & 1 \end{pmatrix}$$

associated to the quadratic form

$$Y_{ij1}(Y_{ij1} - Y_{ij2}) + Y_{ij2}(Y_{ij2} - Y_{ij3}) + \cdots + Y_{ij(i-2)}(Y_{ij(i-2)} - Y_{ij(i-1)}) + Y_{ij(i-1)}^2$$

has determinant equal to $i/2^{i-1}$.

To see this it is enough to notice that $\det \mathcal{M}_3 = 3/4$, $\det \mathcal{M}_4 = 1/2$ and if, for $i > 4$, we expand the determinant with respect to the first column, we obtain the recursive formula:

$$\det \mathcal{M}_i = \det \mathcal{M}_{i-1} - \frac{1}{4} \det \mathcal{M}_{i-2}$$

which allows us to deduce the claim by induction.

Hence $\tilde{Q}_{\mathcal{C}}$ has discriminant $\Delta_{\mathcal{C}} = 2^{c_2} \cdots t^{c_t} / 2^{\tilde{c}}$. This implies that if the characteristic of \mathbb{F}_q is larger than 2 and does not divide $2^{c_2} \cdots t^{c_t}$, then $\tilde{Q}_{\mathcal{C}}$ is non-singular.

Therefore for odd characteristics coprime to $\Delta_{\mathcal{C}}$, we can use the formulas of [1, Theorems 6.26 and 6.27] to enumerate $N(Q_{\mathcal{C}}) = q^{c_2 + \cdots + c_t} N(\tilde{Q}_{\mathcal{C}})$, obtaining:

$$N(\tilde{Q}_{\mathcal{C}}) = \begin{cases} q^{\tilde{c}-1} + \eta((-1)^{\tilde{c}/2} \Delta_{\mathcal{C}})(q-1)q^{(\tilde{c}-2)/2} & \text{if } \tilde{c} \text{ is even;} \\ q^{\tilde{c}-1} & \text{if } \tilde{c} \text{ is odd,} \end{cases}$$

where η is the quadratic character of \mathbb{F}_q^* . Observe that the power of q in the first term above is larger than the one in the second term except when $\tilde{c} = c_2 + 2c_3 + \cdots + (t-1)c_t = 2$ which is satisfied only in the cases: $c = 3, c_3 = 1$ or $c = 4, c_2 = 2$.

Hence, if $\mathcal{C} \notin \{[2], [3], [2 \ 2]\}$ and $\text{char}(\mathbb{F}_q)$ is even and does not divide $\Delta_{\mathcal{C}}$, then $N(Q_{\mathcal{C}}) = q^{c-1} + O(q^{c-2})$. Substituting this in (2) and then in (1), we conclude the proof. \square

REFERENCES

- [1] LIDL R. & NIEDERREITER, H., *Finite Fields*, Encyclo. Math. and Appls. V. 20, Addison-Wesley, Reading, MA 1983.
- [2] MALVENUTO C. & PAPPALARDI F., *Enumerating Permutation Polynomials I: Permutations with Non-Maximal Degree*. Finite Fields Appl. **8** (2002) no. 4, 531–547.

(Malvenuto) DIPARTIMENTO DI INFORMATICA, UNIVERSITÀ DEGLI STUDI “LA SAPIENZA”, VIA SALARIA, 113, I-00198, ROMA – ITALY.

E-mail address: `claudia@di.uniroma1.it`

(Pappalardi) DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DEGLI STUDI ROMA TRE, LARGO S. L. MURIALDO, 1, I-00146, ROMA – ITALY.

E-mail address: `pappa@mat.uniroma3.it`