Finite Fields and Their Applications **8,** 548–553 (2002)
doi:10.1006/ffta.2002.0363

Enumerating Permutation Polynomials over Finite Fields by Degree

Sergei Konyagin[1]

Department of Mechanics and Mathematics, Moscow State University, Vorobjovy Gory, 119899 Moscow, Russia
E-mail: kon@mech.math.msu.su,konyagin@ok.ru

and

Francesco Pappalardi

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

Communicated by Wan Daging

Received June 27, 2001; published online June 14, 2002

We prove an asymptotic formula for the number of permutations for which the associated permutation polynomial has degree smaller than $q-2$. © 2002 Elsevier Science (USA)

Let $\mathbb{F}_q$ be a finite field with $q = p^f > 2$ elements and let $\sigma \in S(\mathbb{F}_q)$ be a permutation of the elements of $\mathbb{F}_q$. The permutation polynomial f_σ of σ is

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

f_σ has the property that $f_\sigma(a) = \sigma(a)$ for every $a \in \mathbb{F}_q$ and this explains its name.

For an account of the basic properties of permutation polynomials we refer to the book of Lidl and Niederreiter [5].

[1]To whom correspondence should be addressed.

1071-5797/02 $35.00

From the definition, it follows that for every σ

$$\partial(f_\sigma) \le q-2.$$

A variety of problems and questions regarding permutation polynomials have been posed by Lidl and Mullen [3,4]. Among these there is problem of determining the number N_d of permutation polynomials of fixed degree d. In [6,9] Malvenuto and the second author address the problem of counting the permutations that move a fixed number of elements of $\mathbb{F}_q$ and whose permutation polynomials have "low" degree.

Here, we consider all permutations and we want to prove the following:

THEOREM 1. *Let*

$$N = \#\{\sigma \in S(\mathbb{F}_q) \mid \partial(f_\sigma) < q-2\}.$$

Then,

$$|N-(q-1)!| \le \sqrt{2e/\pi}\, q^{q/2}.$$

This confirms the common belief that *almost all permutation polynomials have degree* $q-2$.

The first few values of N are listed below:

q	2	3	4	5	7	8	9	11
N	0	0	12	20	630	5368	42 120	3 634 950
$(q-1)!$	1	2	6	24	720	5040	40 320	3 628 800

Proof. The proof uses exponential sums and a similar argument as the one in [2].

By extracting the coefficient of x^{q-2} in $f_\sigma(x)$, we obtain that the degree of $f_\sigma(x)$ is strictly smaller than $q-2$ if and only if

$$\sum_{c\in\mathbb{F}_q} c\sigma(c) = 0.$$

For a fixed subset S of $\mathbb{F}_q$, we introduce the auxiliary set of functions

$$N_S = \left\{ f \mid f : \mathbb{F}_q \to S, \text{ and } \sum_{c\in S} cf(c) = 0 \right\}$$

and set $n_S = \#N_S$. By inclusion exclusion, it is easy to check that

$$N = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S. \tag{1}$$

Now if $e_p(u) = e^{2\pi iu/p}$, consider the identity

$$n_S = \frac{1}{q}\sum_{a\in\mathbb{F}_q}\left(\sum_{f\,:\,\mathbb{F}_q\to S} e_p\left(\sum_{c\in\mathbb{F}_q}\mathrm{Tr}(acf(c))\right)\right),$$

which follows from the standard property

$$\frac{1}{q}\sum_{a\in\mathbb{F}_q} e_p(\mathrm{Tr}(ax)) = \begin{cases} 1 & \text{if } x=0,\\ 0 & \text{if } x\neq 0.\end{cases}$$

By exchanging the sum with the product, we obtain

$$n_S = \frac{1}{q}\sum_{a\in\mathbb{F}_q}\left(\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(act))\right).$$

By isolating the term with $a=0$ in the external sum and noticing that the internal product does not depend on a (for $a\neq 0$), we get

$$n_S = \frac{|S|^q}{q} + \frac{1}{q}\sum_{a\in\mathbb{F}_q^*}\left(\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(bt))\right).$$

Finally,

$$n_S = \frac{|S|^q}{q} + \frac{q-1}{q}\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(bt)). \tag{2}$$

Now let us insert Eq. (2) in Eq. (1) and obtain

$$N - \sum_{S\subseteq\mathbb{F}_q}\frac{(-1)^{q-|S|}}{q}|S|^q = \frac{q-1}{q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}\prod_{b\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(bt)).$$

Note that inclusion–exclusion gives

$$\sum_{S\subseteq\mathbb{F}_q}\frac{(-1)^{q-|S|}}{q}|S|^q = (q-1)!$$

Therefore,

$$N-(q-1)! = \frac{q-1}{q}\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}|S|\prod_{b\in\mathbb{F}_q^*}\sum_{t\in S} e_p(\mathrm{Tr}(bt)).$$

Using the fact that for $b\in\mathbb{F}_q^*$

$$\sum_{t\in S} e_p(\mathrm{Tr}(bt)) = -\sum_{t\notin S} e_p(\mathrm{Tr}(bt))$$

and grouping together the term relative to S and the term relative to $\mathbb{F}_q \setminus S$, we get

$$|N-(q-1)!| \leq \frac{q-1}{2q} \sum_{S \subseteq \mathbb{F}_q} |q-2|S|| \prod_{b \in \mathbb{F}_q^*} \left| \sum_{t \in S} e_p(\mathrm{Tr}(bt)) \right|. \tag{3}$$

Now let us also observe that

$$\sum_{b \in \mathbb{F}_q} \left| \sum_{t \in S} e_p(\mathrm{Tr}(bt)) \right|^2 = q|S|,$$

so that

$$\sum_{b \in \mathbb{F}_q^*} \left| \sum_{t \in S} e_p(\mathrm{Tr}(bt)) \right|^2 = (q-|S|)|S|.$$

From the fact that the geometric mean is always bounded by the arithmetic mean (i.e. $(\prod_{i=1}^k |a_i|^2)^{1/k} \leq \frac{1}{k} \sum_{i=1}^k |a_i|^2$), we have that

$$\begin{aligned} \prod_{b \in \mathbb{F}_q^*} \left| \sum_{t \in S} e_p(\mathrm{Tr}(bt)) \right| &\leq \left(\frac{1}{q-1} \sum_{b \in \mathbb{F}_q^*} \left| \sum_{t \in S} e_p(\mathrm{Tr}(bt)) \right|^2 \right)^{(q-1)/2} \\ &= \left(\frac{(q-|S|)|S|}{q-1} \right)^{(q-1)/2}. \end{aligned} \tag{4}$$

Furthermore, using (3) and (4) we obtain

$$|N-(q-1)!| \leq \frac{q-1}{2q(q-1)^{(q-1)/2}} \sum_{S \subseteq \mathbb{F}_q} |q-2|S||((q-|S|)|S|)^{(q-1)/2}. \tag{5}$$

We want to estimate the above sum. Consider the inequality

$$((q-|S|)|S|)^{(q-1)/2} \leq \left(\frac{q}{2}\right)^{q-1}, \tag{6}$$

and the identity

$$\sum_{S \subseteq \mathbb{F}_q} |q-2|S|| = 2q \binom{q-1}{[q/2]}, \tag{7}$$

which holds since

$$2\sum_{\substack{S\subseteq\mathbb{F}_q,\\ |S|\le q/2}}(q-2|S|) = 2\left[\sum_{j=0}^{[q/2]}\binom{q}{j}(q-j)-\sum_{j=1}^{[q/2]}\binom{q}{j}(j)\right]$$

$$= 2q\left[\sum_{j=0}^{[q/2]}\binom{q-1}{j}-\sum_{j=1}^{[q/2]}\binom{q-1}{j-1}\right] = 2q\binom{q-1}{[q/2]}.$$

From the standard inequality

$$\binom{2n}{n} \le \sqrt{\frac{2}{\pi}}\frac{2^{2n}}{\sqrt{2n+1/2}},$$

which can be found for example in [1], we deduce

$$\binom{q-1}{[q/2]} \le \sqrt{\frac{2}{\pi}}\frac{2^{q-1}}{\sqrt{q-1/2}}. \tag{8}$$

Therefore, (5), (6), (7) and (8) imply

$$|N-(q-1)!| \le \left(\frac{q-1}{\sqrt{q-1/2}\sqrt{q}}\right)\sqrt{\frac{2}{\pi}}\left(\frac{q}{q-1}\right)^{(q-1)/2} q^{q/2}$$

and in view of the inequalities

$$\frac{q-1}{\sqrt{q-1/2}\sqrt{q}}<1, \qquad \left(\frac{q}{q-1}\right)^{(q-1)/2}<\sqrt{e},$$

we finally obtain

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

and this completes the proof. ∎

CONCLUSION

Computations suggest that a more careful estimate of the sum in (5) would yield to a constant $\sqrt{e/2\pi}$ instead of $\sqrt{2e/\pi}$ as coefficient in $q^{q/2}$ in the statement of Theorem 1. However, we feel that such a minor improvement does not justify the extra work.

The ideas in the proof of Theorem 1 can be used to deal with the analogous problem of enumerating the permutation polynomials that have the ith coefficient equal to 0 and also to the problem of enumerating the permutation polynomials with degree less than $q - k$ (for fixed k). However, the exponential sums that need to be considered are significantly more complicated.

ACKNOWLEDGMENTS

The first author was supported by Grants 02-01-00248 and 00-15-96109 from the Russian Foundation for Basic Research. The second author was partially supported by G.N.S.A.G.A. from Istituto Nazionale di Alta Matematica.

The authors thank Igor Shparlinski for suggesting a substantial improvement with respect to the original result.

Note added in proof. Recently the asymptotic estimate in Theorem 1 for a prime q (with slightly weaker remainder term) has been proved in the paper "The number of permutation polynomials of a given degree" by Pinaki Das (to appear in this journal). The author uses algebraic arguments rather than exponential sums.

REFERENCES

1. E. Grosswald, Algebraic Inequalities for π, Solution to a problem proposed by R. E. Shafer, *Amer. Math. Monthly* **84** (1977), 63.
2. S. Konyagin, A note on the least prime in an arithmetic progression, *East J. Approx.* **1** (1995), 403–418.
3. R. Lidl and G. L. Mullin, 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. Mullin, 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, Reading, MA, 1983.
6. C. Malvenuto and F. Pappalardi, Enumerating permutation polynomials I: Permutations with non-maximal degree, submitted.
7. C. Malvenuto and F. Pappalardi, Enumerating permutation polynomials II: k-cycles with minimal degree, in preparation.