ENUMERATING PERMUTATION POLYNOMIALS OVER FINITE FIELDS BY DEGREE II

SERGEI KONYAGIN AND FRANCESCO PAPPALARDI

Abstract. This note is a continuation of a paper by the same authors that appeared in 2002 in the same journal. First we extend the method of the previous paper proving an asymptotic formula for the number of permutations for which the associated permutation polynomial has d coefficients in specified fixed positions equal to 0. This also applies to the function $N_{q,d}$ that counts the number of permutations for which the associated permutation polynomial has degree $< q-d-1$. Next we adopt a more precise approach to show that the asymptotic formula $N_{q,d} \sim q!/q^d$ holds for $d \le \alpha q$ and $\alpha = 0.03983$.

1. Introduction

Let $\mathbb{F}_q$ be a finite field with $q > 2$ elements. For any permutation σ of the elements of $\mathbb{F}_q$ the permutation polynomial

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

has the property that $f_\sigma(a) = \sigma(a)$ for every $a \in \mathbb{F}_q$. From the definition, it follows that for every σ, the degree $\partial(f_\sigma) \le q-2$.

In [2] the authors proved that if $\mathcal{S}(\mathbb{F}_q)$ denotes the group of permutations on $\mathbb{F}_q$, then

$$\left|\#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-2\right\} - (q-1)!\right| \le \sqrt{\frac{2e}{\pi}} q^q.$$

A similar result has also been proved by P. Das [1].

Here we consider a more general function. Fix d integers $k_1, k_2, \ldots, k_d$ with the property that $0 < k_1 < \cdots < k_d < q-1$ and define

$$N_q(k_1, \ldots, k_d) = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \forall i = 1, \ldots, d, \text{ the } k_i\text{–th coefficient of } f_\sigma \text{ is } 0\right\},$$

where by k-th coefficient of a polynomial f we mean its coefficient of x^k.

We will extend the method of [2] proving the following

Theorem 1.

$$\left|N_q(k_1, \ldots, k_d) - \frac{q!}{q^d}\right| < \left(1 + \sqrt{\frac{1}{e}}\right)^q ((q-k_1-1)q)^{q/2}.$$

The above result also applies to

$$N_{q,d} = \#\left\{\sigma \in \mathcal{S}(\mathbb{F}_q) \mid \partial(f_\sigma) < q-d-1\right\}$$

since

$$N_{q,d} = N_q(q-d-1, \ldots, q-3, q-2).$$

We also have

Corollary 1. *If* $d \le \frac{q}{\log q}\left(\frac{1}{2}\log\log q - \log\log\log q\right)$, *then* $N_{q,d} \sim q!/q^d$ $(q \to \infty)$.

In the case when d is larger with respect to q, the above statement for $N_{q,d}$ can be improved. In Section 3 we will prove:

Theorem 2. *Suppose* $\alpha = (e-2)/3e = 0.08808\cdots$, *and* $d < \alpha q$. *Then*

$$\left|N_{q,d} - \frac{q!}{q^d}\right| < 2^d d q^{2+q-d}\binom{q}{d}\left(\frac{2d}{q-d}\right)^{(q-d)/2}.$$

Therefore we have:

Corollary 2. *The asymptotic formula* $N_{q,d} \sim q!/q^d$ *holds for* $q \to \infty$, $d \le \alpha q$ *and* $\alpha = 0.03983$ *is a suitable constant.*

2. The method of [2] - Proof of Theorem 1

The coefficient of x^i in $f_\sigma(x)$ in (1) equals

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

for $i > 0$. Observe that $\binom{q-1}{i} = (-1)^i$ for $i = 1, \dots, q-1$ (the equality is considered in $\mathbb{F}_q$; see [3, Exercise 7.1]).

Hence the j–th coefficient of $f_\sigma(x)$ is 0 if and only if

$$\sum_{c\in\mathbb{F}_q} c^{q-j-1}\sigma(c) = 0.$$

We will follow the proof in [2] that uses exponential sums defining auxiliary functions for each $S \subseteq \mathbb{F}_q$:

$$n_S(k_1,\dots,k_d) = \#\left\{ f \;\middle|\; f : \mathbb{F}_q \longrightarrow S \text{ and } \sum_{c\in\mathbb{F}_q} c^{q-k_i-1} f(c) = 0, \text{ for } i = 1,\dots,d \right\}.$$

By inclusion-exclusion, it is easy to check that

$$N_q(k_1,\dots,k_d) = \sum_{S\subseteq\mathbb{F}_q} (-1)^{q-|S|} n_S(k_1,\dots,k_d). \tag{2}$$

Now we need to evaluate $n_S(k_1,\dots,k_d)$. If $e_p(u) = e^{\frac{2\pi i u}{p}}$ and $\mathrm{Tr}(\alpha) \in \mathbb{F}_p$ denotes the trace of $\alpha \in \mathbb{F}_q$, then

$$\begin{aligned} n_S(k_1,\dots,k_d) &= \frac{1}{q^d}\sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d}\sum_{f:\mathbb{F}_q\longrightarrow S} e_p\left(\sum_{c\in\mathbb{F}_q}\mathrm{Tr}(f(c)\sum_{i=1}^d a_i c^{q-k_i-1})\right) \\ &= \frac{1}{q^d}\sum_{(a_1,\dots,a_d)\in\mathbb{F}_q^d}\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^d a_i c^{q-k_i-1})) \qquad (3) \\ &= \frac{|S|^q}{q^d} + R_S \end{aligned}$$

where

$$|R_S| \le \frac{q^d-1}{q^d}\max_{(a_1,\dots,a_d)\in\mathbb{F}_q^d\setminus\{0\}}\prod_{c\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(t\sum_{i=1}^d a_i c^{q-k_i-1}))\right|.$$

Furthermore, since the geometric mean is always bounded by the arithmetic mean,

$$\prod_{c\in\mathbb{F}_q}\left|\sum_{t\in S}e_p(\mathrm{Tr}(t\sum_{i=1}^{d}a_ic^{q-k_i-1}))\right| \leq$$
$$\left(\frac{1}{q}\sum_{c\in\mathbb{F}_q}\left|\sum_{t\in S}e_p(\mathrm{Tr}(t\sum_{i=1}^{d}a_ic^{q-k_i-1}))\right|^2\right)^{q/2} \leq$$
$$\left(\frac{1}{q}\sum_{u\in\mathbb{F}_q}(q-k_1-1)\left|\sum_{t\in S}e_p(\mathrm{Tr}(tu))\right|^2\right)^{q/2}.$$

By the identity

$$\sum_{u\in\mathbb{F}_q}\left|\sum_{t\in S}e_p(\mathrm{Tr}(tu))\right|^2 = q|S| \tag{4}$$

we get

$$\prod_{c\in\mathbb{F}_q}\left|\sum_{t\in S}e_p(\mathrm{Tr}(t\sum_{i=1}^{d}a_ic^{q-k_i-1}))\right| \leq ((q-k_1-1)|S|)^{q/2}.$$

Using inclusion-exclusion for counting the mappings $\mathbb{F}_q \to \mathbb{F}_q$ we see that

$$\sum_{S\subseteq\mathbb{F}_q}(-1)^{q-|S|}|S|^q = q!. \tag{5}$$

Now let us plug the estimate for $|R_S|$ in equation (3) and then in equation (2). By (5) we obtain

$$\begin{aligned}\left|N_q(k_1,\ldots,k_d)-\frac{q!}{q^d}\right| &= \left|N_q(k_1,\ldots,k_d)-\sum_{S\subseteq\mathbb{F}_q}\frac{(-1)^{q-|S|}}{q^d}|S|^q\right| \\ &\leq \frac{q^d-1}{q^d}\sum_{S\subseteq\mathbb{F}_q}((q-k_1-1)|S|)^{q/2}.\end{aligned}$$

Next, using the inequality

$$1+x\leq e^x \tag{6}$$

we get

$$\left|N_q(k_1,\ldots,k_d)-\frac{q!}{q^d}\right| < (q-k_1-1)^{q/2}\sum_{u=0}^{q}u^{q/2}\binom{q}{u} \leq$$
$$(q-k_1-1)^{q/2}\sum_{u=0}^{q}\binom{q}{u}\left(q\exp\left(-\frac{q-u}{q}\right)\right)^{q/2} =$$
$$((q-k_1-1)q)^{q/2}\sum_{u=0}^{q}\binom{q}{u}\left(\sqrt{\frac{1}{e}}\right)^{q-u} =$$
$$((q-k_1-1)q)^{q/2}\left(1+\sqrt{\frac{1}{e}}\right)^q.$$

This completes the proof. □

Proof of Corollary 1. From Theorem 1 since $N_{q,d} = N_q(q-d-1, q-d, \ldots, q-2)$, we have

$$\left| N_{q,d} - \frac{q!}{q^d} \right| < 2^q (dq)^{q/2}.$$

By the Stirling formula $q! \geq \left(\frac{q}{e}\right)^q \sqrt{q}$, we obtain that the error term is dominated by the main term if

$$(dq)^{q/2}\, 2^q = o\left(\frac{1}{q^d} \left(\frac{q}{e}\right)^q \sqrt{q} \right) \quad (q \to \infty).$$

The above is satisfied if

$$\frac{d}{q} = o\left(\frac{1}{q^{2d/q}} \right) \quad (q \to \infty). \tag{7}$$

Replace $d = u \cdot q \frac{\log\log q}{\log q}$ and obtain that (7) holds for

$$u \leq \frac{1}{2} - \frac{\log\log\log q}{\log\log q}$$

and q large enough. □

3. Proof of Theorem 2

The key ingredient is to use the special properties of $N_{q,d}$ to estimate (3) more accurately.

Assume that d is a positive integer and $d < q$. Let $\mathbb{F}_q(d)$ denote the vector space of polynomials with degree up to d with constant term equal to 0.

If $P(x) \in \mathbb{F}_q(d)$, then define

$$\mu(P) = \min_{T \subset \mathbb{F}_q, |T| = d} |P(T)|.$$

In view of the identity (5) and from (2) and (3) we can write:

$$\begin{aligned} N_{q,d} - \frac{q!}{q^d} &= N_{q,d} - \sum_{S \subseteq \mathbb{F}_q} \frac{(-1)^{q-|S|}|S|^q}{q^d} \\ &= \frac{1}{q^d} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} \sum_{P \in \mathbb{F}_q(d)\setminus\{0\}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \\ &= \frac{1}{q^d} \sum_{S \subseteq \mathbb{F}_q} (-1)^{q-|S|} \sum_{\mu \leq d} \sum_{\substack{P \in \mathbb{F}_q(d)\setminus\{0\} \\ \mu(P)=\mu}} \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))). \end{aligned} \tag{8}$$

In order to estimate the above we will need some lemmas.

Lemma 1. *Given an integer $\mu \in \mathbb{N}$, Let H_μ be the set of polynomials $P \in \mathbb{F}_q(d)$ such that $\mu(P) = \mu$. Then*

$$|H_\mu| \leq \mu^d \binom{q}{\mu} \binom{q}{d}.$$

Proof of Lemma 1. Let us fix one of the $\binom{q}{d}$ subsets of $\mathbb{F}_q$ with d elements and denote it with T. It is sufficient to show that the number of polynomials $P \in \mathbb{F}_q(d)$ with $|P(T)| = \mu$ is at most $\mu^d \binom{q}{\mu}$.

There are $\binom{q}{\mu}$ choices for the set $U = P(T)$. Take an arbitrary $a \in \mathbb{F}_q \setminus T$ and observe that the polynomials of degree $\le d$ correspond to functions $T \cup \{a\} \to \mathbb{F}_q$. Therefore, the number of polynomials P of degree $\le d$ such that $P(T) \subset U$ is equal to $q\mu^d$ and the number of polynomials P of degree $\le d$ such that $|P(T)| = \mu$ is at most $q\mu^d \binom{q}{\mu}$.

Finally, observe that $|P(T)|$ does not change if we add a constant to any polynomial P. Thus the number of polynomials $P \in \mathbb{F}_q(d)$ such that $|P(T)| = \mu$ is at most $\mu^d \binom{q}{\mu}$ as required. □

Lemma 2. *Assume that $d \le q/3$ and $S \subseteq \mathbb{F}_q$. If $P \in \mathbb{F}_q(d)$ is such that $\mu(P) \ge \mu \ge 2$, then*

$$\left| \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \right| \le \left(\frac{q}{2}\right)^{(q+d)/2} \left(\frac{d}{\mu - 1} \frac{q}{q-d} \right)^{(q-d)/2}$$

while if $\mu(P) = 1$, $P \neq 0$, then

$$\left| \prod_{c \in \mathbb{F}_q} \sum_{t \in S} e_p(\mathrm{Tr}(tP(c))) \right| \le \left(\frac{q}{2}\right)^{(q+d)/2} \left(\frac{dq}{q-d} \right)^{(q-d)/2}$$

Proof. Assume $\mu(P) \ge \mu$ and write

$$P(\mathbb{F}_q) = \{u_1, u_2, \ldots\}$$

where the order is chosen in such a way that

$$\#P^{-1}(u_1) \ge \#P^{-1}(u_2) \ge \cdots .$$

Note that since $\mu(P) \ge \mu$,

$$\#P^{-1}(u_1) + \cdots + \#P^{-1}(u_{\mu-1}) < d. \tag{9}$$

Therefore for $j = \mu - 1, \mu, \ldots$ we have

$$\#P^{-1}(u_j) < \frac{d}{\mu - 1}$$

provided that $\mu \ge 2$.

By (9), there is a set $T \subset \mathbb{F}_q$ such that $|T| = d$ and

$$T \supset \{t : \ P(t) \in \{u_1, \ldots, u_{\mu-1}\}\}.$$

Hence, for each $c \notin T$ we have that $P(c) \in \{u_\mu, u_{\mu+1}, \ldots\}$. Therefore there are at most $d/(\mu - 1)$ elements c' of $\mathbb{F}_q$ with $P(c') = P(c)$. If $\mu = 1$ then we use the observation that there are at most d elements c' with this property. Denoting $\mu' = \max(\mu, 2)$, we see that there are at most $d/(\mu' - 1)$ elements c' of $\mathbb{F}_q$ with $P(c') = P(c)$.

Now, bounding from the above the geometric mean with the arithmetic mean, we deduce

$$\begin{aligned}\left|\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(tP(c)))\right| &= \left|\prod_{c\in T}\sum_{t\in S} e_p(\mathrm{Tr}(tP(c)))\right| \times \left|\prod_{c\in\mathbb{F}_q\setminus T}\sum_{t\in S} e_p(\mathrm{Tr}(tP(c)))\right| \\ &\le |S|^d\left(\frac{1}{q-d}\sum_{c\in\mathbb{F}_q\setminus T}\left|\sum_{t\in S} e_p(\mathrm{Tr}(tP(c)))\right|^2\right)^{(q-d)/2} \\ &\le |S|^d\left(\frac{1}{q-d}\frac{d}{\mu'-1}\sum_{u\in\mathbb{F}_q}\left|\sum_{t\in S} e_p(\mathrm{Tr}(tu))\right|^2\right)^{(q-d)/2} \\ &= |S|^d\left(\frac{1}{q-d}\frac{d}{\mu'-1}q|S|\right)^{(q-d)/2}\end{aligned}$$

where we used once again (4). This concludes the proof of the Lemma in the case $|S| \le q/2$.

If $|S| > q/2$ then, by the identity

$$\sum_{t\in\mathbb{F}_q} e_p(\mathrm{Tr}(tP(c)) = 0$$

for $P(c) \neq 0$, we can reduce the product for S to the product for $\mathbb{F}_q \setminus S$. Also, the identity combined with the supposition $d < q$ shows that the product is zero for $|S| = q$. Thus, we can consider $q/2 < |S| < q$. If ν is the number of the zeros of the polynomial P in $\mathbb{F}_q$ then we have

$$\left|\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(tP(c)))\right| = \left(\frac{|S|}{q-|S|}\right)^{\nu}\left|\prod_{c\in\mathbb{F}_q}\sum_{t\in\mathbb{F}_q\setminus S} e_p(\mathrm{Tr}(tP(c)))\right|.$$

Therefore,

$$\begin{aligned}\left|\prod_{c\in\mathbb{F}_q}\sum_{t\in S} e_p(\mathrm{Tr}(tP(c)))\right| &\le \left(\frac{|S|}{q-|S|}\right)^d (q-|S|)^d\left(\frac{1}{q-d}\frac{d}{\mu'-1}q(q-|S|)\right)^{(q-d)/2} \\ &= (|S|(q-|S|))^d(q-|S|)^{(q-3d)/2}\left(\frac{1}{q-d}\frac{d}{\mu'-1}q\right)^{(q-d)/2} \\ &\le \left(\frac{q^2}{4}\right)^d\left(\frac{q}{2}\right)^{(q-3d)/2}\left(\frac{1}{q-d}\frac{d}{\mu'-1}q\right)^{(q-d)/2},\end{aligned}$$

as required. We have taken into account that $(q-3d)/2 \ge 0$ by our supposition. The proof of the lemma is complete. □

Lemma 3. *If $d < \frac{e-2}{3e}q$ then we have the following estimate:*

$$\sum_{\mu=2}^{d}\left(\frac{1}{\mu-1}\right)^{(q-d)/2}\cdot\binom{q}{\mu}\mu^d \le 2^{d-1}(d-1)q^2.$$

Proof. Lemma is trivial for $d = 1$. Consider $d > 1$ and define the function

$$f(\mu) = \left(\frac{1}{\mu - 1}\right)^{(q-d)/2} \cdot \binom{q}{\mu} \mu^d.$$

Let $d = uq$, $u < \frac{e-2}{3e}$. Taking into account (6), we have

$$\begin{aligned} f(\mu+1)/f(\mu) &= \left(\frac{\mu-1}{\mu}\right)^{(q-d)/2} \left(\frac{\mu+1}{\mu}\right)^{d} \binom{q}{\mu+1} \binom{q}{\mu}^{-1} \\ &< \left(\frac{\mu-1}{\mu}\right)^{(1-3u)q/2} \frac{q}{\mu+1} \\ &< \exp\left(-\frac{(1-3u)q}{2\mu}\right) \frac{q}{\mu}. \end{aligned}$$

By our supposition, $(1 - 3u)/2 > 1/e$. Denoting $v = q/\mu$ we have

$$f(\mu + 1)/f(\mu) < ve^{-v/e}.$$

But, by (6), $ve^{-v/e} \leq 1$ for any v. Therefore, $f(\mu+1)/f(\mu) < 1$. Thus, the function $f(\mu)$ is decreasing for $2 \leq \mu \leq d$. Hence,

$$\sum_{\mu=2}^{d} \left(\frac{1}{\mu - 1}\right)^{(q-d)/2} \cdot \binom{q}{\mu} \mu^d = \sum_{\mu=2}^{d} f(\mu) \leq (d - 1)f(2).$$

This implies the statement of Lemma 3. □

We are in the condition to prove Theorem 2.

Proof of Theorem 2. In view of Lemma 2 (recall that $d < \frac{e-2}{3e}q$) and Lemma 1, the absolute value of the right hand side of (8) is

$$\leq \sum_{S \subseteq \mathbb{F}_q} \frac{1}{q^d} \binom{q}{d} \left(\frac{q}{2}\right)^{(q+d)/2} \left(\frac{dq}{q-d}\right)^{(q-d)/2} \left(q + \sum_{\mu=2}^{d} \left(\frac{1}{\mu-1}\right)^{(q-d)/2} \cdot \binom{q}{\mu} \mu^d\right).$$

by Lemma 3, we obtain that the above is

$$\begin{aligned} &< \frac{2^q}{q^d} \binom{q}{d} \left(\frac{q}{2}\right)^{(q+d)/2} \left(\frac{dq}{q-d}\right)^{(q-d)/2} 2^d dq^2. \\ &= 2^d dq^{2+q-d} \binom{q}{d} \left(\frac{2d}{q-d}\right)^{(q-d)/2}. \end{aligned} \tag{10}$$

This concludes the proof by using (8). □

4. Range of uniformity (Proof of Corollary 2)

In this last section we want to establish how large d can be in order for the asymptotic formula $N_{q,d} \sim q!/q^d$ to hold.

Substitute $d = \beta q$ in (10) and note that in order to have an asymptotic formula it is enough to verify that

$$2^{\beta q} q^{3+q} \binom{q}{\beta q} \left(\frac{2\beta}{1-\beta}\right)^{q(1-\beta)/2} = o(q!) \quad (q \to \infty). \tag{11}$$

From the Stirling formula,

$$\binom{q}{\beta q} \ll \left(\frac{1}{\beta^\beta (1-\beta)^{1-\beta}}\right)^q,$$

we obtain that (11) is satisfied uniformly over $\beta \le \beta_0$ if we have

$$\forall \beta \in (0, \beta_0] \quad -1 > \log\left(2^\beta\right) - \log\left(\beta^\beta (1-\beta)^{1-\beta}\right) + \log\left(\left(\frac{2\beta}{1-\beta}\right)^{\frac{1-\beta}{2}}\right).$$

The last inequality holds for $\beta_0 = 0.03983$. This completes the proof of the corollary. □

In a future paper we are planning to adopt the method of Theorem 2 to prove an asymptotic formula for $N_q(k_1, \dots, k_d)$ with arbitrary $k_1, \dots, k_d$ where d is fixed or grows slowly as $q \to \infty$.

It would be of interest to enumerate permutation polynomials with degree approximately $\sqrt{q}$. Unfortunately our approach cannot reach this range since we know that for q odd there are no permutation polynomials of degree $(q-1)/2$ (see [3, Corollary 7.5]).

Acknowledgements. The authors are grateful to the referee for a careful reading of the paper. Due to his (or her) remarks, a series of shortcomings have been corrected. Also, we would like to thank Igor Shparlinski and Mike Zieve for useful comments on the first draft of this paper. The project was performed during the visit of the first author to the Università Roma Tre in April 2003 supported in part by G.N.S.A.G.A. from Instituto Nazionale di Alta Matematica.

References

[1] Das P., *The number of permutation polynomials of a given degree over a finite field*, Finite Fields Appl., **8**, No 4, (2002) 478–490.

[2] Konyagin S. & Pappalardi F., *Enumerating permutation polynomials over finite fields by degree*, Finite Fields and Appl. **8** (2002) 548–553.

[3] Lidl R. & Niederreiter H., *Finite fields*, Second edition, Cambridge Univ. Press, Cambridge, 1997.

(Konyagin) Department of Mechanics and Mathematics, Moscow State University, Vorobjovy Gory, 119992, Moscow, Russia

E-mail address: konyagin@ok.ru

(Pappalardi) Dipartimento di Matematica, Università degli Studi Roma Tre, Largo S. L. Murialdo, 1, I–00146 Roma, Italia

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