On Permutation Polynomials of Prescribed Shape

Qiang Wang
School of Mathematics and Statistics
Carleton University
wang@math.carleton.ca

Joint work with Amir Akbary and Dragos Ghioca

FQ9, July 2009

Definitions:

A Permutation Polynomial (PP) of a finite field $\mathbb{F}_q$ is polynomial which permutes the elements of $\mathbb{F}_q$ as an evaluation mapping.

Examples:

- $P(x) = ax + b, a \neq 0$.
- $P(x) = x^n$ is a PP of $\mathbb{F}_q$ iff $(n, q-1) = 1$. (RSA)
- Dickson polynomial $D_n(x, 1)$ is PP of $\mathbb{F}_q$ iff $(n, q^2 - 1) = 1$.
- $P_1 \circ P_2$ is a PP of $\mathbb{F}_q$ iff $P_1(x)$ and $P_2(x)$ are PPs.

Problem

Problem (Lidl-Mullen, 1988)

Let $N_d(q)$ denote the number of permutation polynomials of $\mathbb{F}_q$ which have degree d. We have the trivial boundary conditions: $N_1(q) = q(q-1)$, $N_d(q) = 0$ if d is a divisor of $(q-1)$ larger than 1, and $\sum N_d(q) = q!$ where the sum is over all $1 \leq d < q-1$ such that d is either 1 or it is not a divisor of $(q-1)$. Find $N_d(q)$.

Previous work

- Das [2] 2002 proved that $N_{p-2}(p) \sim (\varphi(p)/p)p!$ as $p \to \infty$, where φ is the Euler function. More precisely he proves that

$$\left| N_{p-2}(p) - \frac{\varphi(p)}{p} p! \right| \leq \sqrt{\frac{p^{p+1}(p-2)+p^2}{p-1}}.$$

Previous work

- Das [2] 2002 proved that $N_{p-2}(p) \sim (\varphi(p)/p)p!$ as $p \to \infty$, where φ is the Euler function. More precisely he proves that

$$\left|N_{p-2}(p) - \frac{\varphi(p)}{p}p!\right| \leq \sqrt{\frac{p^{p+1}(p-2)+p^2}{p-1}}.$$

- Konyagin and Pappalardi [3] 2002 proved that

$$\left|N_{q-2}(q) - \frac{\varphi(q)}{q}q!\right| \leq \sqrt{\frac{2e}{\pi}}q^{\frac{q}{2}}.$$

Previous work

Fix j integers $k_1, \ldots, k_j$ such that $0 < k_1 < \cdots < k_j < q - 1$. Define $N(k_1, \ldots, k_j; q)$ as the number of permutation polynomials h of $\mathbb{F}_q$ of degree less than $(q-1)$ such that the coefficient of x^{k_i} in h equals 0, for $i = 1, \ldots, j$.

Theorem (Konyagin-Pappalardi, [4], 2006)

$$\left| N(k_1, \ldots, k_j; q) - \frac{q!}{q^j} \right| < \left(1 + \sqrt{\frac{1}{e}}\right)^q ((q - k_1 - 1)q)^{q/2}.$$

Note that $N_{q-2}(q) = q! - N(q-2; q)$.

Comments and Questions

- Enumeration of permutation polynomials with a prescribed set of nonzero monomials? Existence?
- What happens when k_1 is small?

Existence of permutation polynomials of certain shapes

- There are no permutation polynomials of $\mathbb{F}_q$ of degree $d > 1$ such that $d \mid (q-1)$.
- For any positive even degree n, there is no permutation polynomial of degree n of $\mathbb{F}_q$ if q is sufficiently large compared to n (Fried, Guralnick, and Saxl, 1993).

Existence of permutation polynomials of certain shapes

On the other hand one can prove the existence of permutation polynomials of varying degrees.

Theorem (Carlitz-Wells, 1966)

(i) Let $\ell > 1$. Then for q sufficiently large such that $\ell \mid (q-1)$, there exists $a \in \mathbb{F}_q$ such that the polynomial $x(x^{(q-1)/\ell} + a)$ is a permutation polynomial of $\mathbb{F}_q$.
(ii) Let $\ell > 1$, $(r, q-1) = 1$, and k be a positive integer. Then for q sufficiently large such that $\ell \mid (q-1)$, there exists $a \in \mathbb{F}_q$ such that the polynomial $x^r(x^{(q-1)/\ell} + a)^k$ is a permutation polynomial of $\mathbb{F}_q$.

Quantitative version of Carlitz-Wells's Theorem

- Laigle-Chapuy [1] 2007 gave a quantitative version of Carlitz-Wells's Theorem for $k = 1$ assuming $q > \ell^{2\ell+2}\left(1 + \frac{\ell+1}{\ell^{\ell+2}}\right)^2$.
- Masuda and Zieve [3] obtain a stronger result for more general binomials of the form $x^r(x^{e_1(q-1)/\ell} + a)$. Result: $q > \ell^{2\ell+2}$.
- General polynomials?

Setup–index of a polynomial

- Let $g(x) \in \mathbb{F}_q[x]$ be non-constant and monic with $g(0) = 0$, the index ℓ of $g(x)$ is defined as the least divisor of $q-1$ such that $g(x)$ can be written uniquely as $x^r f(x^{(q-1)/\ell})$ where r is the vanishing order of $g(x)$ at zero.
- Any non-constant polynomial $h(x)$ can be written as $h(x) = ag(x) + b$ where $a \neq 0$ and $g(x)$ is monic with $g(0) = 0$. We define the *index* of $h(x)$ as the index of $g(x)$.
- $h(x)$ can be written uniquely as

$$h(x) = a(x^r f(x^{(q-1)/\ell})) + b.$$

- Clearly, $h(x)$ is a permutation polynomial of $\mathbb{F}_q$, if and only if $g(x) = x^r f(x^{(q-1)/\ell})$ is a permutation polynomial of $\mathbb{F}_q$.

Setup

Let $\ell \geq 2$ be a divisor of $q-1$. We let

$$g_{r,\bar{e}}^{\overline{a}}(x) := x^r \left(x^{e_m s} + a_1 x^{e_{m-1} s} + \cdots + a_{m-1} x^{e_1 s} + a_m\right),$$

where m, r are positive integers, $\overline{a} = (a_1, \ldots, a_m) \in (\mathbb{F}_q{}^*)^m$, and $\bar{e} = (e_1, \ldots, e_m)$ is an m-tuple of integers that satisfy the following conditions:

$$0 < e_1 < e_2 \cdots < e_m \leq \ell - 1 \text{ and } (e_1, \ldots, e_m, \ell) = 1 \text{ and } r + e_m s \leq q - 1, \tag{1}$$

where $s := (q-1)/\ell$.

Main result

Fix $r, m, \overline{e}$, define $N^m_{r,\overline{e}}(\ell, q)$ as the number of all tuples $\overline{a} \in \left(\mathbb{F}_q^*\right)^m$ such that $g^{\overline{a}}_{r,\overline{e}}(x)$ is a permutation polynomial of $\mathbb{F}_q$.
That is, $N^m_{r,\overline{e}}(\ell, q)$ is the number of all monic permutation $(m+1)$-nomials $g^{\overline{a}}_{r,\overline{e}}(x) = x^r f(x^{(q-1)/\ell})$ of $\mathbb{F}_q$ with index ℓ.

Theorem

$$\left| \frac{\frac{\ell^\ell}{\ell!} N^m_{r,\overline{e}}(\ell, q) - q^m}{\ell^{\ell+1} q^{m-1/2}} \right| < 1.$$

Or:

$$\left| N^m_{r,\overline{e}}(\ell, q) - \frac{\ell!}{\ell^\ell} q^m \right| < \ell!\ell q^{m-1/2}.$$

More results

Corollary

For any q, r, $\bar{e}$, m, ℓ *that satisfy* (1), $(r, s) = 1$, *and* $q > \ell^{2\ell+2}$, *there exists an* $\bar{a} \in (\mathbb{F}_q^*)^m$ *such that the* $(m+1)$*-nomial* $g_{r,\bar{e}}^{\bar{a}}(x)$ *is a permutation polynomial of* $\mathbb{F}_q$*.*

Remark

For $q \geq 7$ we have $\ell^{2\ell+2} < q$ as long as $\ell < \frac{\log q}{2 \log \log q}$.

Take $r = 1$ in the above result, we can obtain the existence of permutation $(m+1)$-nomials which have coefficients equal to 0 for their x^k terms, where $2 \leq k \leq s$. This observation addresses one of the questions left open by Konyagin and Pappalardi ($k_1 = 2$, $\ldots$, $k_j = s$).

More results

Next note that for $1 \leq t \leq q-2$ the number of permutation polynomials of degree at least $(q-t-1)$ is

$$q! - N(q-t-1, q-t, \ldots, q-2; q).$$

In [4, Corollary 2] Konyagin and Pappalardi proved that

$$N(q-t-1, q-t, \ldots, q-2; q) \sim \frac{q!}{q^t}$$

holds for $q \to \infty$ and $t \leq 0.03983\, q$. This result will guarantee the existence of permutation polynomials of degree at least $(q-t-1)$ for $t \leq 0.03983\, q$ (as long as q is sufficiently large).

Results

Theorem

Let $m \geq 1$. Let q be a prime power such that $(q-1)$ has a divisor ℓ with $m < \ell$ and $\ell^{2\ell+2} < q$. Then for every $1 \leq t < \frac{(\ell-m)}{\ell}(q-1)$ coprime with $(q-1)/\ell$ there exists an $(m+1)$-nomial $g^{\bar{a}}_{r,\bar{e}}(x)$ of degree $(q-t-1)$ which is a permutation polynomial of $\mathbb{F}_q$.

Note that this theorem establishes the existence of permutation polynomials withe exact degree $q-t-1$.

Corollary

Let $m \geq 1$ be an integer, and let q be a prime power such that $(m+1) \mid (q-1)$. Then for all $n \geq 2m+4$, there exists a permutation $(m+1)$-nomial of $\mathbb{F}_{q^n}$ of degree $(q-2)$.

Sketch of proof of the main theorem

Criterion (Wan & Lidl, 91): Let $(r, s) = 1$ and α be a generator of ${\mathbb{F}_q}^*$. The polynomial $g^{\overline{a}}$ permutes $\mathbb{F}_q$ if and only if the following two conditions are satisfied:

(i) $\alpha^{ie_m s} + a_1\alpha^{ie_{m-1}s} + \cdots + a_{m-1}\alpha^{ie_1 s} + a_m \neq 0$, for each $i = 1, \ldots, \ell$;

(ii) $g^{\overline{a}}(\alpha^i)^s \neq g^{\overline{a}}(\alpha^j)^s$, for $1 \leq i < j \leq \ell$.

$$N^m_{r,\overline{e}}(\ell, q) = \frac{1}{\ell^\ell} \sum_{\substack{\overline{a}\in(\mathbb{F}_q^*)^m \\ \overline{a} \text{ satisfies (i)}}} \sum_{\sigma\in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s\right). \quad (2)$$

where ψ be a multiplicative character of order ℓ of the set μ_ℓ of all ℓth root of unity in ${\mathbb{F}_q}^*$ and

$$P_\sigma(\beta_1, \ldots, \beta_\ell) = \prod_{i=1}^{\ell} \left(\sum_{j=0}^{\ell-1} \left(\psi(\beta_i)\psi(\alpha^s)^{-\sigma(i)}\right)^j \right).$$

Sketch of proof of the main theorem

Lemma

Let $\beta_1, \ldots, \beta_\ell \in \mu_\ell$. *Then*

$$\frac{1}{\ell^\ell} \sum_{\sigma \in S_\ell} P_\sigma(\beta_1, \ldots, \beta_\ell) = \begin{cases} 1 & \text{if } \{\beta_1, \ldots, \beta_\ell\} = \mu_\ell \\ 0 & \text{otherwise} \end{cases}.$$

Lemma

If $\beta_i \in \mu_\ell \cup \{0\}$ *for each* $1 \leq i \leq \ell$, *and at least one* β_i *is zero, then*

$$0 \leq \frac{1}{\ell^\ell} \sum_{\sigma \in S_\ell} P_\sigma(\beta_1, \ldots, \beta_\ell) \leq \frac{1}{\ell}.$$

Sketch of proof of main theorem

Combinatorial arguments.

$$
\begin{aligned}
& \frac{1}{\ell^\ell} \sum_{\overline{a} \in \mathbb{F}_q^m} \sum_{\sigma \in S_\ell} P_\sigma \left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s \right) - \frac{q^{m+1} - (q-1)^{m+1} - (-1)^m}{q} \\
\leq \quad & N^m_{r,\overline{e}}(\ell, q) \\
\leq \quad & \frac{1}{\ell^\ell} \sum_{\overline{a} \in \mathbb{F}_q^m} \sum_{\sigma \in S_\ell} P_\sigma \left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s \right).
\end{aligned}
$$

Sketch of proof of the main theorem

Theorem (Weil)

Let Ψ be a multiplicative character of $\mathbb{F}_q$ of order $\ell > 1$ and let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree that is not an ℓ-th power of a polynomial. Let d be the number of distinct roots of $f(x)$ in its splitting field over $\mathbb{F}_q$. Then for every $t \in \mathbb{F}_q$ we have

$$\left| \sum_{a \in \mathbb{F}_q} \Psi(tf(a)) \right| \leq (d-1)\sqrt{q}.$$

Sketch of proof of the main theorem

$$\sum_{a_m \in \mathbb{F}_q} \prod_{i=1}^{\ell} \left(\psi(g^{\overline{a}}(\alpha^i)^s) \psi(\alpha^s)^{-\sigma(i)} \right)^{k_i} =$$

$$\sum_{a_m \in \mathbb{F}_q} \psi \left(\beta^{\sum_{i=1}^{\ell}(rik_i - \sigma(i)k_i)} \cdot \prod_{i=1}^{\ell} \left(\beta^{e_m i} + a_1 \beta^{e_{m-1} i} + \cdots + a_{m-1} \beta^{e_1 i} + a_m \right)^{k_i s} \right) \tag{3}$$

which can be written as a character sum

$$\sum_{a_m \in \mathbb{F}_q} \Psi \left(t \prod_{i=1}^{\ell} \left(\beta^{e_m i} + a_1 \beta^{e_{m-1} i} + \cdots + a_{m-1} \beta^{e_1 i} + a_m \right)^{k_i} \right),$$

where $t := \alpha^{\sum_{i=1}^{\ell}(rik_i - \sigma(i)k_i)} \in \mathbb{F}_q$.

Sketch of proof of the main theorem

Let $m > 1$. Let $\beta := \alpha^s$ be a fixed generator of μ_ℓ. We call a $(m-1)$-tuple $(a_1, \ldots, a_{m-1}) \in (\mathbb{F}_q)^{m-1}$ *good* if there is no $1 \leq i_1 < i_2 \leq \ell$ such that

$$\beta^{i_1 e_m} + a_1 \beta^{i_1 e_{m-1}} + \cdots + a_{m-1}\beta^{i_1 e_1} = \beta^{i_2 e_m} + a_1 \beta^{i_2 e_{m-1}} + \cdots + a_{m-1}\beta^{i_2 e_1}.$$

$$\frac{1}{\ell^\ell} \sum_{\substack{a_m \in \mathbb{F}_q \\ (a_1,\ldots,a_{m-1}) \text{ is good}}} \sum_{\sigma \in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s\right) - \frac{q^{m+1} - (q-1)^{m+1} - (-1)^{m}}{q}$$

$$\leq N^m_{r,\overline{e}}(\ell, q)$$

$$\leq \binom{\ell}{2} q^{m-1} + \frac{1}{\ell^\ell} \sum_{\substack{a_m \in \mathbb{F}_q \\ (a_1,\ldots,a_{m-1}) \text{ is good}}} \sum_{\sigma \in S_\ell} P_\sigma\left(g^{\overline{a}}(\alpha^1)^s, \ldots, g^{\overline{a}}(\alpha^\ell)^s\right).$$

A. Akbary, G. Ghioca, Q. Wang,
On permutation polynomials of prescribed shape, Finite Fields Appl. **15** (2009), 195-206.

P. Das,
The number of permutation polynomials of a given degree over a finite field, Finite Fields Appl. **8** (2002), 478–490.

S. Konyagin and F. Pappalardi,
Enumerating permutation polynomials over finite fields by degree, Finite Fields Appl. **8** (2002), no. 4, 548–553.

S. Konyagin and F. Pappalardi,
Enumerating permutation polynomials over finite fields by degree. II, Finite Fields Appl. **12** (2006), no. 1, 26–37.

Y. Laigle-Chapuy,
Permutation polynomials and applications to coding theory, Finite Fields Appl. **13** (2007), no. 1, 58–70.

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.

A. Masuda and M. E. Zieve,
Permutation binomials over finite fields, Trans. Amer. Math. Soc. **361** (2009), no. 8, 4169–4180.

D. Wan and R. Lidl,
Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, Monatsh. Math. **112** (1991), 149–163.