An index approach on distribution of permutation polynomials over finite fields

Qiang Wang

School of Mathematics and Statistics
Carleton University
Ottawa, Canada

Carleton Finite Fields Day, September 29, 2017
In honor of Gary L. Mullen's 70th birthday!

Outline

Outline

Gary L. Mullen

- As of September 2017, Gary has published 154 research papers from MathSciNet database.
- Around 10% of them contain the keyword “permutation polynomials” in their titles.
- One of his earliest papers is on permutation polynomials in several variables (1976).
- Many surveys, problems, and conjectures have inspiring and significant impact in this area.

Introduction

Definition

A polynomial $P(x) \in \mathbb{F}_q[x]$ is a permutation polynomial (PP) of $\mathbb{F}_q$ if P permutes the elements of $\mathbb{F}_q$. Equivalently,

- the function $P : c \mapsto f(c)$ is onto;
- the function $P : c \mapsto f(c)$ is one-to-one;
- $P(x) = a$ has a (unique) solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.
- the plane curve $P(x) - P(y) = 0$ has no $\mathbb{F}_q$-rational point other than points on the diagonal $x = y$.

Applications: Almost perfect nonlinear power functions (e.g., Dobbertin, 99), skew Hadamard difference sets (Ding and Yuan, 07), among other.

Lagrange interpolation

Lagrange Interpolation

There exists exactly one polynomial P of degree $\leq q-1$ such that $f(a_i) = b_i$ with $i = 0, \cdots, q-1$ given by

$$P(x) = \sum_{i=0}^{q-1} b_i \prod_{\substack{k=0 \\ k \neq i}}^{q-1} \frac{x - a_k}{a_i - a_k}$$

$$P(x) = \sum_{c \in \mathbb{F}_q} P(c)(1 - (x-c)^{q-1})$$

A few well-known classes

Monomials: x^n is a PP of $\mathbb{F}_q$ if and only if $(n, q-1) = 1$.

Dickson: $D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}$ $(a \neq 0 \in \mathbb{F}_q)$ is a PP of $\mathbb{F}_q$ if and only if $(n, q^2 - 1) = 1$.

Linearized: The polynomial $L(x) = \sum_{s=0}^{n-1} a_s x^{q^s} \in \mathbb{F}_{q^n}[x]$ is a PP of $\mathbb{F}_{q^n}$ if and only if $\det(a_{i-j}^{q^j}) \neq 0$, $0 \leq i, j \leq n-1$.

Low degree: Dickson (1896/97), Lidl - Niederreiter (1997), Li-Chandler-Xiang (2010), Shallue-Wanless (2012).

Some surveys

- R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? The American Mathematical Monthly, vol. 95, no. 3, pp. 243-246, 1988.
- R. Lidl and G. L. Mullen, When does a polynomial over a finite field permute the elements of the field? II, The American Mathematical Monthly, vol. 100, no. 1, pp. 71-74, 1993.
- G. L. Mullen, Permutation polynomials over finite fields, in Finite Fields, Coding Theory, and Advances in Communications and Computing, vol. 141, pp. 131-151, Marcel Dekker, New York, NY, USA, 1993

Some surveys

- G. L. Mullen, Permutation polynomials: a matrix analogue of Schur's conjecture and a survey of recent results. Special issue dedicated to Leonard Carlitz. Finite Fields Appl. 1 (1995), no. 2, 242-258.
- R. Lidl and H. Niederreiter, Finite Fields, vol. 20 of Encyclopedia of Mathematics and Its Applications, Cambridge University Press, Cambridge, UK, 2nd edition, 1997.
- G. L. Mullen and Q. Wang, Permutation polynomials of one variable, Section 8.1 in Handbook of Finite Fields, CRC Press, Boca Raton, FL, 2013.
- X. Hou, Permutation polynomials over finite fields-a survey of recent advances. Finite Fields Appl. 32 (2015), 82-119.

Outline

An open problem

Problem 6 (Lidl-Mullen, 1988)

Let $N_q(n)$ be the number of PPs of $\mathbb{F}_q$ of degree n. Find $N_q(n)$.

- $N_q(1) = q(q-1)$.
- $N_q(n) = 0$ if $n \mid q-1$ and $n > 1$.
- $\sum N_q(n) = q!$

Exceptional polynomials

- A permutation polynomial f over $\mathbb{F}_q$ is exceptional if it induces a permutation of infinitely many extensions of $\mathbb{F}_q$.
- Any exceptional polynomial is a PP, and the converse holds if q is large compared to the degree of the polynomial (Cohen 1995).
- Carlitz's Conjecture (1966): for each even integer n, there is a constant C_n so that for each finite field of odd order $q > C_n$, there does not exist a PP of degree n over $\mathbb{F}_q$.

Theorem (Fried, Guralnick and Saxl 1993)

There are no exceptional polynomials of even degree n over $\mathbb{F}_q$ if q is odd.

Exceptional polynomials

- Wan (1993) generalized Carlitz's conjecture proving that if $q > n^4$ and $(n, q-1) > 1$ then there is no PP of degree n over $\mathbb{F}_q$.
- Cohen and Fried (1995) gave an elementary proof of Wan's conjecture following an argument of Lenstra and this result was stated in terms of exceptional polynomials.

Theorem (Cohen-Fried (1995), Wan (1993))

There are no exceptional polynomials of degree n over $\mathbb{F}_q$ if $(n, q-1) > 1$.

Enumeration of PPs with degree $q-2$

$N_q(n)$– the number of PPs over $\mathbb{F}_q$ with degree n and $f(0)=0$.

Theorem (Konyagin-Pappalardi 2002)

Let q be a prime power. Then $\left|N_{<q-2}(q)-(q-1)!\right| \leq \sqrt{\frac{2e}{\pi}}q^{\frac{q}{2}}$.

Theorem (Das 2002)

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

Theorem (Kim-Kim-Kim 2016)

$$\left|N_q(q-2)-(1-\tfrac{1}{q})(q-1)!\right| \leq (1-\tfrac{1}{q})q^{q/2}.$$

Enumeration with prescribed zero coefficients

Theorem (Konyagin-Pappalardi 2006)

Fix j integers $k_1, \ldots, k_j$ with the property that $0 < k_1 < \cdots < k_j < q-1$ and define $N(k_1, \ldots, k_j; q)$ as the number of PPs of $\mathbb{F}_q$ of degree less than $q-1$ such that the coefficient of x^{k_i} equals 0, for $i = 1, \ldots, j$. Then

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

In particular, $N_{q-2}(q) = q! - N(q-2; q)$.

This implies that the number of permutation polynomials for which $\deg(f) < q - t - 1$ is asymptotic equal to $\frac{q!}{q^t}$ whenever $q \to \infty$ and $t \leq 0.03983\, q$.

Outline

Index of a polynomial

Any polynomial $h(x)$ can be written uniquely as

$$\begin{aligned} h(x) &= a_n x^n + a_{n_1} x^{n_1} + \cdots + a_{n_t} x^{n_t} + a_r x^r + a_0 \\ &= a_n x^r (x^{n-r} + b_{n_1} x^{n_1 - r} + \cdots + b^{n_t} x^{n_t - r} + b_r) + a_0 \end{aligned}$$

Let $s = \gcd(n-r, n_1 - r, \ldots, n_t - r, q-1)$ and $\ell = \frac{q-1}{s}$ (index).

$$\begin{aligned} &= a_n x^r (x^{e_m s} + b_{n_1} x^{e_{m-1} s} + \cdots + b^{n_t} x^{e_0 s} + b_r) + a_0 \\ &= a_n x^r f(x^s) + a_0, \end{aligned}$$

Examples: 1) Any monomial $ax^n + b$ has index 1.
2) $x^{19} + ax^4 + b$ over $\mathbb{F}_{25}$ has index $\ell = 8$ because
$x^{19} + ax^4 + b = x^4(x^{15} + a) + b$ and $s = \gcd(15, 24) = 3$.
$h(x)$ is a PP of $\mathbb{F}_q$ iff $x^r f(x^s)$ is a PP of $\mathbb{F}_q$. ($(r, s) = 1$).

Cyclotomic mappings

- Let γ be a primitive element of $\mathbb{F}_q$ and $q-1=\ell s$.
- $C_0=\{\gamma^{\ell j}: j=0,1,\cdots,s-1\}$, the set of all nonzero ℓ-th powers of $\mathbb{F}_q$.
- *cyclotomic cosets* $C_i := \gamma^i C_0, \quad i=0,1,\cdots,\ell-1.$
- For any integer $r>0$ and any $A_0, A_1, \cdots, A_{\ell-1}\in\mathbb{F}_q$, we define an *$r$-th order cyclotomic mapping $f^r_{A_0,A_1,\cdots,A_{\ell-1}}$ of index ℓ* from $\mathbb{F}_q$ to itself by $f^r_{A_0,A_1,\cdots,A_{\ell-1}}(0)=0$ and

$$f^r_{A_0,A_1,\cdots,A_{\ell-1}}(x)=\begin{cases} A_0x^r, & \text{if } x\in C_0=<\gamma^\ell>\leq\mathbb{F}_q^*=<\gamma>;\\ \vdots & \vdots\\ A_ix^r, & \text{if } x\in C_i=\gamma^iC_0;\\ \vdots & \vdots\\ A_{\ell-1}x^r, & \text{if } x\in C_{\ell-1}=\gamma^{\ell-1}C_0,\end{cases}$$

Relations to polynomials of the form $x^r f(x^s)$

The polynomial $f^r_{A_0, A_1, \cdots, A_{\ell-1}}(x) \in \mathbb{F}_q[x]$ of degree at most $q-1$ representing the cyclotomic mapping $f^r_{A_0, A_1, \cdots, A_{\ell-1}}$ is called an r-th order cyclotomic mapping polynomial of index ℓ.

Let $q - 1 = \ell s$, γ be a given primitive element of $\mathbb{F}_q$ and $\zeta = \gamma^s$ be a primitive ℓ-th root of unity.

$$x^r f(x^{(q-1)/\ell}) = f^r_{A_0, A_1, \cdots, A_{\ell-1}}(x)$$

where $A_i = f(\zeta^i)$ for $0 \leq i \leq \ell - 1$.

Index of a polynomial corresponds to the least index of a cyclotomic mapping.

Remarks

$P(x) = x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$ iff $(r,s)=1$ and $\{A_0^s, A_1^s\zeta^r, \cdots, A_{\ell-1}^s\zeta^{(\ell-1)r}\} = \mu_\ell$, where μ_ℓ is the set of all distinct ℓ-th roots of unity.

Corollary (Park-Lee 2001, Wang 2007, Zieve 2009)

Let $q-1=\ell s$ for some positive integers ℓ and s. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r,s)=1$ and $x^r f(x)^s$ permutes the set μ_ℓ of all distinct ℓ-th roots of unity.

Corollary (W. 2007)

Let $q-1=\ell s$ for some positive integers ℓ and s. Then $P(x) = x^r f(x^s)$ is a PP of $\mathbb{F}_q$ if and only if $(r,s)=1$ and $\{Ind_\gamma(f(\zeta^i)) + ir \mid i = 0, \ldots, \ell-1\} = \mathbb{Z}_\ell$.

Estimation of numbers of PPs with prescribed index

Corollary (Wang 2007)

Let p be prime, $q = p^m$, and $\ell \mid q-1$ for some positive integer ℓ. For each positive integer r such that $(r,s)=1$, there are $P_\ell = \ell!(\frac{q-1}{\ell})^\ell$ distinct r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of index ℓ. Moreover, the number Q_ℓ of r-th order cyclotomic mapping permutation polynomials of $\mathbb{F}_q$ of least index ℓ is

$$Q_\ell = \sum_{\substack{d\mid\ell \\ (r,(q-1)/d)=1}} \mu\left(\frac{\ell}{d}\right)\left(\frac{q-1}{d}\right)^d d!.$$

Estimation of numbers of PPs with prescribed index and exponents

Let

$$x^r f(x^s) = x^r \left(x^{e_m s} + b_{n_1} x^{e_{m-1} s} + \cdots + b_{n_{m-1}} x^{e_1 s} + b_{n_m} \right),$$

where $r + e_m s \leq q - 1$, $0 < e_1 < e_2 < \cdots < e_m \leq \ell - 1$, and $(e_1, \ldots, e_m, \ell) = 1$.
Let $N^m_{r,\bar{e}}(\ell, q)$ be the number of all tuples of coefficients $(b_{n_1}, b_{n_2}, \ldots, b_{n_m})$ such that $x^r f(x^s)$ is a PP of $\mathbb{F}_q$.

Theorem (Akbary-Ghioca-Wang 2009)

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

Existence of PPs with prescribed index and exponents

Theorem (Akbary-Ghioca-Wang 2009)

For any q, r, $\bar{e}$, m, ℓ that satisfy above trivial conditions, $(r, s) = 1$, and $q > \ell^{2\ell+2}$, there exists an $(b_{n_1}, b_{n_2}, \ldots, b_{n_m}) \in (\mathbb{F}_q^*)^m$ such that the $(m+1)$-nomial of the form $x^r f(x^s)$ is a permutation polynomial of $\mathbb{F}_q$.

- There exists permutation polynomials of index ℓ for any prescribed exponents $(e_1, \ldots, e_m)$ as above over finite field $\mathbb{F}_q$ when $q > \ell^{2\ell+2}$. (Akbary-Ghioca-Wang 2009)
- For $q \geq 7$ we have $\ell^{2\ell+2} < q$ if $\ell < \frac{\log q}{2 \log \log q}$.

Existence of PPs with prescribed index and degree

Konyagin and Pappalardi proved for $q \to \infty$ and $t \leq 0.03983\, q$ that $N(q-t-1, q-t, \ldots, q-2; q) \sim \frac{q!}{q^t}$ holds. This result guarantees the existence of PPs of degree at least $q-t-1$ for $t \leq 0.03983\, q$ (as long as q is sufficiently large).

Theorem (Akbary-Ghioca-Wang 2009)

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 of degree $q-t-1$ which is a PP of $\mathbb{F}_q$.

Corollary (Akbary-Ghioca-Wang 2009)

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 $q-2$.

Outline

Conclusion and Problems

- Distribution of PPs and an analogue of Mullen's enumeration problem.
- Construction/Classification of PPs by indices
- The index of any permutation binomial over finite prime field $\mathbb{F}_p$ must satisfy $\ell < \sqrt{p} + 1$. (Masuda and Zieve 2009)
- Question: the index of permutation fewnomials over finite prime field $\mathbb{F}_p$ must be "small"?

Conclusion and Problems

Thank you all for your attention!

Thank you, Gary, for creating jobs for us!

Happy 70th Birthday!