Permutation Polynomials and Polynomial Generators of a General Linear Group

Chris Castillo

Loyola Blakefield

MD-DC-VA Section of the MAA
Fall 2016 Meeting
Johns Hopkins University
November 5, 2016

Finite Fields and Permutation Polynomials

Permutation Polynomials and $GL(\mathbb{F}_{p^2})$

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Let p be prime and consider the finite field $\mathbb{F}_{p^n}$

Finite Fields and Permutation Polynomials

Let p be prime and consider the finite field $\mathbb{F}_{p^n}$

Theorem (Lagrange Interpolation)

Any function $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ may be represented as a polynomial $f(X) \in \mathbb{F}_{p^n}[X]$ according to the formula:

$$f(X) = \sum_{x \in \mathbb{F}_{p^n}} \left(1 - (X - x)^{p^n - 1}\right) \varphi(x).$$

Finite Fields and Permutation Polynomials

Let p be prime and consider the finite field $\mathbb{F}_{p^n}$

Theorem (Lagrange Interpolation)

Any function $\varphi\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ *may be represented as a polynomial* $f(X) \in \mathbb{F}_{p^n}[X]$ *according to the formula:*

$$f(X) = \sum_{x \in \mathbb{F}_{p^n}} \left(1 - (X - x)^{p^n - 1}\right) \varphi(x).$$

Definition (Permutation Polynomial)

A polynomial $f(X) \in \mathbb{F}_{p^n}[X]$ is a *permutation polynomial* if it induces a bijection of $\mathbb{F}_{p^n}$ under evaluation.

Examples of Permutation Polynomials

Permutation Polynomials and $GL(\mathbb{F}_{p^2})$

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Example (Linear polynomials)

$aX + b$ for any $a \in \mathbb{F}_{p^n}^*$ and any $b \in \mathbb{F}_{p^n}$

Examples of Permutation Polynomials

Permutation Polynomials and $GL(\mathbb{F}_{p^2})$

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Example (Linear polynomials)

$aX + b$ for any $a \in \mathbb{F}_{p^n}^*$ and any $b \in \mathbb{F}_{p^n}$

Example (Monomials)

X^m if and only if $(m, p^n - 1) = 1$

Examples of Permutation Polynomials

Example (Linear polynomials)

$aX + b$ for any $a \in \mathbb{F}_{p^n}^*$ and any $b \in \mathbb{F}_{p^n}$

Example (Monomials)

X^m if and only if $(m, p^n - 1) = 1$

Example (All-ones polynomials)

$1 + X + X^2 + \cdots + X^k$ if and only if $k \equiv 1 \pmod{p(p^n - 1)}$

Examples of Permutation Polynomials

Example (Linear polynomials)

$aX + b$ for any $a \in \mathbb{F}_{p^n}^*$ and any $b \in \mathbb{F}_{p^n}$

Example (Monomials)

X^m if and only if $(m, p^n - 1) = 1$

Example (All-ones polynomials)

$1 + X + X^2 + \cdots + X^k$ if and only if $k \equiv 1 \pmod{p(p^n - 1)}$

Example (Dickson polynomials of the first kind)

$$g_k(X, a) := \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j X^{k-2j} \text{ for } a \in \mathbb{F}_q^*$$

if and only if $(k, (p^n)^2 - 1) = 1$

Groups of Permutation Polynomials

Example (Linear monomials)

$\langle aX \rangle \cong C_{p^n-1}$ for a fixed primitive $a \in \mathbb{F}_{p^n}^*$

Groups of Permutation Polynomials

Permutation Polynomials and $GL(\mathbb{F}_{p^2})$

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Example (Linear monomials)

$\langle aX \rangle \cong C_{p^n-1}$ for a fixed primitive $a \in \mathbb{F}_{p^n}^*$

Example (Linear binomials)

$\langle X + b \rangle \cong C_p$ for a fixed $b \in \mathbb{F}_{p^n}^*$

Groups of Permutation Polynomials

Example (Linear monomials)

$\langle aX \rangle \cong C_{p^n-1}$ for a fixed primitive $a \in \mathbb{F}_{p^n}^*$

Example (Linear binomials)

$\langle X + b \rangle \cong C_p$ for a fixed $b \in \mathbb{F}_{p^n}^*$

Example (Linearized polynomials)

$\langle L(X) \rangle \cong GL(\mathbb{F}_{p^n})$ where $L(X) = \sum_{i=0}^{n-1} \ell_i X^{p^i}$ such that the unique zero of $L(X)$ of 0

Groups of Permutation Polynomials

Example (Linear monomials)

$\langle aX \rangle \cong C_{p^n-1}$ for a fixed primitive $a \in \mathbb{F}_{p^n}^*$

Example (Linear binomials)

$\langle X+b \rangle \cong C_p$ for a fixed $b \in \mathbb{F}_{p^n}^*$

Example (Linearized polynomials)

$\langle L(X) \rangle \cong GL(\mathbb{F}_{p^n})$ where $L(X) = \sum_{i=0}^{n-1} \ell_i X^{p^i}$ such that the unique zero of $L(X)$ of 0

Example (Dickson polynomials of the first kind)

$g_k(X, a)$ is an abelian group if and only if $a \in \{-1, 0, 1\}$

Constructing Groups of Permutation Polynomials

Introduction
Permutation Polynomials Representing Groups
Equivalence of Groups of Polynomials
An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Let G be a group of order at most p^n

Constructing Groups of Permutation Polynomials

Permutation Polynomials and $GL(\mathbb{F}_{p^2})$

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Let G be a group of order at most p^n

1. **Injection**: $\sigma : G \hookrightarrow \mathbb{F}_{p^n}$

Constructing Groups of Permutation Polynomials

Let G be a group of order at most p^n

1. **Injection**: $\sigma : G \hookrightarrow \mathbb{F}_{p^n}$
2. **Action** of G on $\mathbb{F}_{p^n}$:

$$g * x := \begin{cases} \sigma\left(g \cdot \sigma^{-1}(x)\right), & x \in \sigma(G) \\ x, & x \notin \sigma(G) \end{cases}$$

Constructing Groups of Permutation Polynomials

Let G be a group of order at most p^n

1. **Injection**: $\sigma : G \hookrightarrow \mathbb{F}_{p^n}$
2. **Action** of G on $\mathbb{F}_{p^n}$:

$$g * x := \begin{cases} \sigma\left(g \cdot \sigma^{-1}(x)\right), & x \in \sigma(G) \\ x, & x \notin \sigma(G) \end{cases}$$

3. **Interpolation**:

$$f_g(X) = \sum_{x \in \mathbb{F}_{p^n}} \left(1 - (X - x)^{q-1}\right)(g * x)$$

Constructing Groups of Permutation Polynomials

Let G be a group of order at most p^n

1. **Injection**: $\sigma : G \hookrightarrow \mathbb{F}_{p^n}$
2. **Action** of G on $\mathbb{F}_{p^n}$:

$$g * x := \begin{cases} \sigma\left(g \cdot \sigma^{-1}(x)\right), & x \in \sigma(G) \\ x, & x \notin \sigma(G) \end{cases}$$

3. **Interpolation**:

$$f_g(X) = \sum_{x \in \mathbb{F}_{p^n}} \left(1 - (X - x)^{q-1}\right)(g * x)$$

4. **Operation**: composition and reduction modulo $X^{p^n} - X$

Constructing Groups of Permutation Polynomials

- $f_g\left(f_h(X)\right) = f_{gh}(X)$ (closure)

Constructing Groups of Permutation Polynomials

Permutation Polynomials and $GL(\mathbb{F}_{p^2})$

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

- $f_g\big(f_h(X)\big) = f_{gh}(X)$ (closure)
- $f_e(X) = X$ (identity)

Constructing Groups of Permutation Polynomials

- $f_g\big(f_h(X)\big) = f_{gh}(X)$ (closure)
- $f_e(X) = X$ (identity)
- $f_g(X)^{[-1]} = f_{g^{-1}}(X)$ (inverse)

Constructing Groups of Permutation Polynomials

- $f_g\left(f_h(X)\right) = f_{gh}(X)$ (closure)
- $f_e(X) = X$ (identity)
- $f_g(X)^{[-1]} = f_{g^{-1}}(X)$ (inverse)

Theorem

The representation polynomials form a group under composition modulo $X^{p^n} - X$ which is isomorphic to G:

$$G \cong \{f_g(X) : g \in G\}.$$

Examples

Example (Cyclic group of order p^n)

For any $z \in \{1, 2, \ldots, p^n - 1\}$ and any primitive element $\xi \in \mathbb{F}_{p^n}$, the polynomials

$$\xi X + \xi^z \left(1 + \xi^{1-z} X + (\xi^{1-z} X)^2 + \cdots + (\xi^{1-z} X)^{p^n - 2}\right)$$

are permutation polynomials over $\mathbb{F}_{p^n}$.

Examples

Example (Cyclic group of order p^n)

For any $z \in \{1, 2, \ldots, p^n - 1\}$ and any primitive element $\xi \in \mathbb{F}_{p^n}$, the polynomials

$$\xi X + \xi^z \left(1 + \xi^{1-z} X + (\xi^{1-z} X)^2 + \cdots + (\xi^{1-z} X)^{p^n - 2}\right)$$

are permutation polynomials over $\mathbb{F}_{p^n}$.

Example (Cyclic group of order p^2)

The polynomials

$$1 \pm X + X^{p-1} + X^{2(p-1)} + \cdots + X^{p^2 - p}$$

are permutation polynomials over $\mathbb{F}_{p^2}$.

The Example of Interest: C_{p^2}

Introduction
Permutation Polynomials Representing Groups
Equivalence of Groups of Polynomials
An Unexpected Result about $GL(\mathbb{F}_{p^2})$

- Let $C_{p^2} = \langle g \rangle$

The Example of Interest: C_{p^2}

- Let $C_{p^2} = \langle g \rangle$
- Fix a basis $[\beta] = [\beta_0, \beta_1]$ of $(\mathbb{F}_{p^2}, +)$ over $\mathbb{F}_p$

The Example of Interest: C_{p^2}

- Let $C_{p^2} = \langle g \rangle$
- Fix a basis $[\beta] = [\beta_0, \beta_1]$ of $(\mathbb{F}_{p^2}, +)$ over $\mathbb{F}_p$
- Write the p-adic expansion of k as $k = \kappa_0 + \kappa_1 p$

The Example of Interest: C_{p^2}

- Let $C_{p^2} = \langle g \rangle$
- Fix a basis $[\beta] = [\beta_0, \beta_1]$ of $(\mathbb{F}_{p^2}, +)$ over $\mathbb{F}_p$
- Write the p-adic expansion of k as $k = \kappa_0 + \kappa_1 p$
- Write $x \in \mathbb{F}_{p^2}$ and $x = \lambda_0\beta_0 + \lambda_1\beta_1$

The Example of Interest: C_{p^2}

Injection:

$$\sigma(g^k) = \sigma\left(g^{\kappa_0+\kappa_1 p}\right) = \kappa_0\beta_0 + \kappa_1\beta_1$$

The Example of Interest: C_{p^2}

Injection:

$$\sigma(g^k) = \sigma\left(g^{\kappa_0+\kappa_1 p}\right) = \kappa_0\beta_0 + \kappa_1\beta_1$$

Action:

$$\begin{aligned}
g^k * x &= \sigma\left(g^k \cdot \sigma^{-1}\left(\lambda_0\beta_0 + \lambda_1\beta_1\right)\right) \\
&= \sigma\left(g^{\kappa_0+\kappa_1 p} \cdot g^{\lambda_0+\lambda_1 p}\right) \\
&= \sigma\left(g^{(\kappa_0+\lambda_0)+(\kappa_1+\lambda_1)p}\right) \\
&= \begin{cases} (\kappa_0+\lambda_0)\beta_0 + (\kappa_1+\lambda_1)\beta_1, & \kappa_0+\lambda_0 < p \\ (\kappa_0+\lambda_0)\beta_0 + (\kappa_1+\lambda_1+1)\beta_1, & \kappa_0+\lambda_0 \geq p \end{cases} \\
&= \begin{cases} x + (\kappa_0\beta_0 + \kappa_1\beta_1), & \lambda_0 < p - \kappa_0 \\ x + (\kappa_0\beta_0 + \kappa_1\beta_1) + \beta_1, & \lambda_0 \geq p - \kappa_0 \end{cases}
\end{aligned}$$

The Example of Interest: C_{p^2}

- $C_{p^2} = \langle g \rangle$
- Let $[\beta] = [\beta_0, \beta_1]$ be a basis of $(\mathbb{F}_{p^2}, +)$ over $\mathbb{F}_p$
- Write $k = \kappa_0 + \kappa_1 p$

Example (The "Additive Representation" of C_{p^2})

$$f^{[\beta_0,\beta_1]}_{g^{\kappa_0+\kappa_1 p}}(X) = X + \kappa_0\beta_0 + \kappa_1\beta_1 - \beta_1 \sum_{\lambda_0=p-\kappa_0}^{p-1} \sum_{\lambda_1=0}^{p-1} \sum_{\ell=0}^{p^2-2} \left((\lambda_0\beta_0 + \lambda_1\beta_1)^{-1} X\right)^{\ell}$$

Equivalence of Representations

Definition (Equivalence)

The polynomial representations f, f' generated by $\sigma, \sigma' \colon G \hookrightarrow \mathbb{F}_{p^n}$, respectively, are *equivalent* if there exists a group automorphism $\alpha \colon (\mathbb{F}_{p^n}, +) \to (\mathbb{F}_{p^n}, +)$ such that for all $g \in G$,

$$f_g(X) = \left(\alpha^{-1} \circ f'_g \circ \alpha\right)(X).$$

Equivalence of Polynomials Representing C_{p^2}

Theorem

The "additive representations" of C_{p^2} in any two bases $[\beta]$ and $[\gamma]$ of $(\mathbb{F}_{p^2}, +)$ over $\mathbb{F}_p$ are equivalent.

Equivalence of Polynomials Representing C_{p^2}

Theorem

The "additive representations" of C_{p^2} in any two bases $[\beta]$ and $[\gamma]$ of $(\mathbb{F}_{p^2},+)$ over $\mathbb{F}_p$ are equivalent. Moreover,

$$f_g^{[\gamma]}(X) = L(X)^{[-1]} \circ f_g^{[\beta]}(X) \circ L(X),$$

where $L(X)$ is a polynomial of the form

$$L(X) = \ell_1 X^p + \ell_0 X$$

that represents the change of basis of $(\mathbb{F}_{p^2},+)$ from $[\gamma]$ to $[\beta]$.

Equivalence of Polynomials Representing C_{p^n}

Theorem

The "additive representations" of C_{p^n} in any two bases $[\beta]$ and $[\gamma]$ of $(\mathbb{F}_{p^n}, +)$ over $\mathbb{F}_p$ are equivalent. Moreover,

$$f_g^{[\gamma]}(X) = L(X)^{[-1]} \circ f_g^{[\beta]}(X) \circ L(X),$$

where $L(X)$ is a polynomial of the form

$$L(X) = \sum_{i=0}^{n-1} \ell_i X^{p^i}$$

that represents the change of basis of $(\mathbb{F}_{p^n}, +)$ from $[\gamma]$ to $[\beta]$.

Equivalence of Polynomials Representing C_{p^2}

Theorem

Let $[\beta_0, \beta_1]$ and $[\gamma_0, \gamma_1]$ be two bases of $(\mathbb{F}_{p^2}, +)$ over $\mathbb{F}_p$. Then there exist unique $r \in \mathbb{F}_{p^2}^*$, $s \in \mathbb{F}_p$, and $t \in \mathbb{F}_p^*$ such that

$$f_g^{[\gamma_0,\gamma_1]}(X) = \left(N_t(M_s(rX))\right)^{[-1]} \circ f_g^{[\beta_0,\beta_1]}(X) \circ N_t(M_s(rX)),$$

where

$$M_s(X) = \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(s\beta_1^2X^p + (\beta_0^p\beta_1 - \beta_0\beta_1^p - s\beta_1^{p+1})X\right)$$

and

$$N_t(X) = \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}}\left((t-1)X^p + (\beta_0^{p-1} - t\beta_1^{p-1})X\right).$$

The Unexpected Result

Theorem (Generators of $GL(\mathbb{F}_{p^2})$)

Let $\beta_0, \beta_1 \in \mathbb{F}_{p^2}$ be linearly independent over $\mathbb{F}_p$, let $\rho \in \mathbb{F}_{p^2}^*$ be primitive, and let $\psi, \tau \in \mathbb{F}_p$ with τ nonzero. Then the polynomials ρX,

$$M_\psi(X) = \frac{1}{\beta_0^p\beta_1 - \beta_0\beta_1^p}\left(\psi\beta_1^2X^p + (\beta_0^p\beta_1 - \beta_0\beta_1^p - \psi\beta_1^{p+1})X\right)$$

and

$$N_\tau(X) = \frac{1}{\beta_0^{p-1} - \beta_1^{p-1}}\left((\tau - 1)X^p + (\beta_0^{p-1} - \tau\beta_1^{p-1})X\right)$$

generate a group of permutation polynomials isomorphic to the general linear group $GL(\mathbb{F}_{p^2})$.

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Thank you for attending!

Introduction

Permutation Polynomials Representing Groups

Equivalence of Groups of Polynomials

An Unexpected Result about $GL(\mathbb{F}_{p^2})$

Thank you for attending!

Are there any questions?