Constructing Groups of Permutation Polynomials

Chris Castillo, Dr. Robert S. Coulter

Department of Mathematical Sciences, University of Delaware, Newark, Delaware

Introduction

A central problem in finite field theory is the construction and classification of polynomials with certain properties. One class of particular interest is permutation polynomials, that is, polynomials whose induced function is a bijection on the field. Using a novel algebraic technique, we have constructed a new family of permutation polynomials over each finite field $\mathbb{F}_{p^2}$, where p is an odd prime.

Specifically, we apply Cayley's Theorem to the right regular action of the cyclic group C_{p^2} of order p^2 on the finite field $\mathbb{F}_{p^2}$ of the same order, and then we use interpolation to describe the function induced by the action of each element of C_{p^2} as a polynomial in $\mathbb{F}_{p^2}[X]$. The polynomials generated by this method form the new class of permutation polynomials we have constructed.

Algebraic Tools

Interpolation Formula ([1, p. 348]). *If $\varphi\colon \mathbb{F}_q \to \mathbb{F}_q$ is an arbitrary function, then the unique polynomial $f \in \mathbb{F}_q[X]$ representing φ is given by:*

$$f(X) = \sum_{c\in\mathbb{F}_q} \varphi(c)\big(1-(X-c)^{q-1}\big).$$

Cayley's Theorem ([2, p. 6]). *Every group G can be represented as a group of permutations by letting G act on itself via the right regular action.*

Construction Method

1. **Define a bijection $C_{p^2} \to \mathbb{F}_{p^2}$.**

   Let $C_{p^2} = \langle a\rangle$ and fix a basis $[y, z]$ of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$. For any integer $0 \le k < p^2$, write k in its base-p expansion: $k = m + np$ where $0 \le m, n \le p-1$. Then the function $\sigma\colon C_{p^2} \to \mathbb{F}_{p^2}$ defined by

   $$a^{m+np} \mapsto my + nz$$

   is a bijection.

   Here, the addition $(m + np) + (i + jp)$ is performed base-p, using carries, and then reduced modulo p^2.

2. **Define the action of C_{p^2} on $\mathbb{F}_{p^2}$.**

   Let C_{p^2} act on $\mathbb{F}_{p^2}$ by

   $$(my + nz) * a^{i+jp} = \sigma\big(\sigma^{-1}(my + nz) \cdot a^{i+jp}\big).$$

   By Cayley's Theorem, the action of each element of C_{p^2} produces a permutation, i.e. a bijective function $\mathbb{F}_{p^2} \to \mathbb{F}_{p^2}$.

3. **Apply the interpolation formula.**

   We now apply the Interpolation Formula to obtain a (permutation) polynomial which represents this function.

Next Steps

We would like to use this method to find polynomial representations of the following families of groups:

- C_{p^n} for any positive integer n
- $C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_k}}$
- $C_{p^{n_1}} \rtimes C_{p^{n_2}}$

We would also like to generalize this method to investigate polynomial representations of groups of non prime-power order.

References

[1] R. Lidl & H. Niederreiter. *Finite Fields.* Cambridge: Cambridge University Press, 1997.

[2] J. D. Dixon & B. Mortimer. *Permutation Groups.* Graduate Texts in Mathematics 163. New York: Springer, 1996.

[3] T. Vaughan. Polynomials and linear transformations over finite fields. *J. Reine Angew. Math.* **267** (1974), 179–206.

The Polynomials

Theorem (CC & RSC, 2012). Let $[y, z]$ be a basis of $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$ and let $a^{i+jp} \in C_{p^2}$. Then the polynomial in $\mathbb{F}_{p^2}[X]$ representing the action of a^{i+jp} on $\mathbb{F}_{p^2}$ is:

$$f^{y,z}_{a^{i+jp}}(X) = \begin{cases} X + jz & \text{if } i = 0, \\ X + jz + iy - z\displaystyle\sum_{m=p-i}^{p-1}\sum_{n=0}^{p-1}\big(X-(my+nz)\big)^{p^2-1} & \text{if } i \neq 0. \end{cases}$$

The representation polynomial $f^{y,z}_{a^{i+jp}}(X)$ has the following properties:

- The leading term is $iz^pX^{p^2-p}$ when $i \neq 0$.
- The constant term is $jz + iy$.
- The function induced by the polynomial $f^{y,z}_{a^{i+jp}}(X)$ has no fixed points unless $i = j = 0$.
- Different choices of basis will produce different representation polynomials.
- The subgroup of order p is a (cyclic) group consisting of linear polynomials.
- If we define the "all ones" polynomial to be $h_k(X) = 1 + X + X^2 + \cdots + X^k$, then we obtain the following family of fixed point-free permutation polynomials for $y \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$:

$$f^{y,1}_{a^{p-1}}(X) = X - y - X^{p-1}h_{p-1}(X^{p-1}).$$

The Group

Theorem (CC & RSC, 2012). Let $[y, z]$ be a basis of $\mathbb{F}_{p^2}$. Then the set of representation polynomials

$$\big\{f^{y,z}_{a^k}(X) : 0 \le k \le p^2 - 1\big\}$$

forms a group under composition of polynomials in $\mathbb{F}_{p^2}[X]$ reduced modulo $X^{p^2} - X$. Moreover, this group is cyclic of order p^2:

$$\big\langle f^{y,z}_a(X)\big\rangle \cong C_{p^2}.$$

The conjugacy classes of these groups are classified according to the basis of $\mathbb{F}_{p^2}$ on which the generating representation polynomial is defined:

- The $p-1$ representation groups generated by the bases $[y, \gamma z]$ for $1 \le \gamma \le p-1$ are non-conjugate.
- The p^2-1 representation groups generated by the bases $[\beta y, \beta z]$ for $\beta \in \mathbb{F}^*_{p^2}$ are conjugate to each other according to the relation:

$$\beta X \circ f^{y,z}_a(X) \circ \beta^{-1}X = f^{\beta y,\beta z}_a(X).$$

- The p representation groups generated by the bases $[y + \alpha z, z]$ for $0 \le \alpha \le p-1$ are identical.