Finite Fields and Their Applications 35 (2015) 172–203

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A general representation theory for constructing groups of permutation polynomials

Chris Castillo *, Robert S. Coulter [1]

Department of Mathematical Sciences, University of Delaware, United States

ARTICLE INFO

Article history:
Received 20 October 2014
Received in revised form 10 March 2015
Accepted 17 March 2015
Available online 17 May 2015
Communicated by Rudi Lidl

MSC:
11T06
12E10
20C99

Keywords:
Finite field
Permutation polynomial
Regular representation
Equivalent representations

ABSTRACT

Using the left regular action of a group on itself, we develop a general representation theory for constructing groups of permutation polynomials. As an application of the method, we compute polynomial representations of several abelian and nonabelian groups, and we determine the equivalence classes of the groups of polynomials we construct. In particular, when the size of the group is equal to the size of the field in which the group is represented, all non-identity representation polynomials are necessarily fixed-point free permutation polynomials.

1. Introduction

We begin by fixing some notation. Throughout, we will let $q = p^n$ for some prime p and let $\mathbb{F}_q$ denote the finite field of order q. The multiplicative group of $\mathbb{F}_q$ will be denoted $\mathbb{F}_q^\times = \langle \zeta \rangle$ for some fixed, but arbitrary, primitive element ζ of $\mathbb{F}_q$. We will be concerned

* Corresponding author.
E-mail addresses: castillo@math.udel.edu (C. Castillo), coulter@math.udel.edu (R.S. Coulter).

[1] The work of the second author was partially supported by the National Science Foundation (NSF).

http://dx.doi.org/10.1016/j.ffa.2015.03.006
1071-5797/

with elements of $\mathbb{F}_q[X]$, the ring of polynomials over $\mathbb{F}_q$ in the indeterminate X. Any function $\varphi: \mathbb{F}_q \to \mathbb{F}_q$ can be represented by a polynomial $f \in \mathbb{F}_q[X]$, for example, via the interpolation formula

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

This representation is unique if one restricts the degree of the polynomials to less than q; polynomials in $\mathbb{F}_q[X]$ with degree less than q are called *reduced*. If, under evaluation, a polynomial $f \in \mathbb{F}_q[X]$ induces a bijection on $\mathbb{F}_q$, then we call $f(X)$ a *permutation polynomial* over $\mathbb{F}_q$.

This paper is motivated by two problems concerning permutation polynomials. The first problem is to find new classes of permutation polynomials (problem P2 in [9]). Permutation polynomials are a central object of study in finite field theory, and determining whether a given polynomial is a permutation polynomial is a non-trivial task. Hermite [8] proved the initial results over prime fields, introducing the criterion that now bears his name, and Dickson [6] expanded these to arbitrary finite fields. While it is a simple exercise to show that the monomial X^k is a permutation polynomial over $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$, much less simple is the result by Matthews [11] that the "all-ones" polynomial $h_k(X) = 1 + X + X^2 + \cdots + X^k$ is a permutation polynomial over $\mathbb{F}_q$ (of odd characteristic) if and only if $k \equiv 1 \pmod{p(q-1)}$. The reader who is interested in the basic theory of permutation polynomials is referred to Chapter 7 of [10], which is a standard reference in the field.

The second problem is concerned with representation theory and the structure of permutation polynomials. A *representation* is a homomorphism $G \to \mathrm{Sym}(S)$ of a group G into the group of symmetries of some object S. When G is finite and S is a set of cardinality $|G|$, the representation is called a *permutation representation*. In this paper, we will investigate a certain type of permutation representation. Taking the set S to be the underlying set of a finite field $\mathbb{F}_q$, we can consider $\mathrm{Sym}(S)$ to be the set of reduced permutation polynomials over $\mathbb{F}_q$. Since two reduced permutation polynomials can be composed and reduced modulo $X^q - X$ to produce another, it is natural to investigate the types of permutation groups that can be represented by certain permutation polynomials.

There are several other results describing groups of permutation polynomials with relatively simple polynomial generators. For example, Carlitz [4] showed the full symmetric group on q letters can be generated by X^{q-2} and all linear polynomials in $\mathbb{F}_q[X]$, while Wells determined polynomial generators for several small-index subgroups of S_q in [15]. Additionally, Wan and Lidl [14], in the course of proving when polynomials of the form $X^r f(X^s)$ were permutation polynomials, also determined that they have the group structure of a generalized wreath product.

We are interested specifically in whether it is possible to represent given groups of order roughly q by permutation polynomials over $\mathbb{F}_q$. This is possible in the loosest