Finite Fields and Their Applications 49 (2018) 198–211

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Permutation polynomials over finite rings

Dalma Görcsös, Gábor Horváth [*], Anett Mészáros

Institute of Mathematics, University of Debrecen, Pf. 400, Debrecen, 4002, Hungary

ARTICLE INFO

Article history:
Received 23 March 2017
Received in revised form 9 September 2017
Accepted 21 October 2017
Available online xxxx
Communicated by Rudolf Lidl

MSC:
13M10
11T06

Keywords:
Permutation polynomials
Local rings
Group of permutation polynomial functions

ABSTRACT

Let PPol(R) denote the group of permutation polynomial functions over the finite, commutative, unital ring R under composition. We generalize numerous results about permutation polynomials over $\mathbb{Z}_{p^n}$ to local rings by treating them under a unified manner. In particular, we provide a natural wreath product decomposition of permutation polynomial functions over the maximal ideal M and over the finite field R/M. We characterize the group of permutation polynomial functions over M whenever the condition $M^{|R/M|} = \{0\}$ applies. Then we derive the size of PPol(R), thereby generalizing the same size formulas for $\mathbb{Z}_{p^n}$. Finally, we completely characterize when the group PPol(R) is solvable, nilpotent, or abelian.

1. Introduction

Let R be a finite, commutative, unital ring. A polynomial $f \in R[x]$ is called a *permutation polynomial* if the function induced by f permutes the elements of R. An $R \to R$ function is a *permutation polynomial function* if it is induced by a permutation polyno-

[*] Corresponding author.
E-mail addresses: gorcsosdalma@gmail.com (D. Görcsös), ghorvath@science.unideb.hu (G. Horváth), m.anett.ani95@gmail.com (A. Mészáros).

https://doi.org/10.1016/j.ffa.2017.10.004
1071-5797/© 2017 Elsevier Inc. All rights reserved.

mial from $R[x]$. The permutation polynomial functions form a group under composition. We denote this group by $\mathrm{PPol}(R)$.

Permutation polynomials have several applications in cryptography and coding theory: mostly when R is a finite field (see e.g. [1–5], and for most recent results see e.g. [6, Chapter VIII]), but even when R is a certain residue class ring [7,8]. The picture is less clear when it comes to arbitrary commutative rings. Many of the existing results on permutation polynomials are only about residue class rings.

Let f be a polynomial with integer coefficients, $f(x) = a_d x^d + \cdots + a_1 x + a_0$. Rivest [9] proved that f is a permutation polynomial modulo 2^n if and only if a_1 is odd, and $(a_2 + a_4 + \dots)$ is even and $(a_3 + a_5 + \dots)$ is even, as well. This is a special case of a more general result by Nöbauer (see e.g. [10, Hilfsatz 8]): the polynomial f is a permutation polynomial modulo p^n for some prime p if and only if it permutes the elements of the finite field $\mathbb{F}_p$, and if $f'(x) = 0$ has no solutions in $\mathbb{F}_p$. Singh and Maity [11] used this characterization to obtain conditions modulo 3^n and 5^n, similar to those gave by Rivest for modulo 2^n.

Mullen and Stevens [12] applied these characterizations to compute the number of permutation polynomial functions over the residue class ring $\mathbb{Z}_{p^n}$. For a set S we denote the size of S by $|S|$. Let $\nu(s)$ be the largest positive integer for which $p^{\nu(s)} \mid s!$. That is, $\nu(s) = \sum_{r=1}^{\infty} [\frac{s}{p^r}]$. Let N be the biggest positive integer for which $\nu(N) < n$. Then

$$|\mathrm{PPol}(\mathbb{Z}_{p^n})| = p!(p-1)^p p^{-2p} \prod_{j=0}^{N} p^{n-\nu(j)}. \tag{1}$$

Furthermore, for $\delta(N) = \frac{1}{2} \sum_{r=1}^{\infty} p^r [\frac{N}{p^r}]\big([\frac{N}{p^r}] + 1\big)$ one has

$$|\mathrm{PPol}(\mathbb{Z}_{p^n})| = p!(p-1)^p p^{(N+1)(n-\nu(N))+\delta(N)-2p}. \tag{2}$$

These formulas have been generalized by Nöbauer for finite quotients of Dedekind domains [13, p. 176, Chapter 4, Corollary 5.72]. Frisch [14] considered “suitable” finite, commutative, unital, local rings, and computed the number of permutation polynomial functions for such rings. However, a formula describing $|\mathrm{PPol}(R)|$ for not necessarily suitable, but arbitrary local rings R has been elusive so far.

Determining the structure of $\mathrm{PPol}(R)$ would be a natural step after computing its size. However, by looking at formulas (1) and (2), one cannot hope to obtain very nice descriptions in the general case. Indeed, even to enumerate and describe the p-Sylow subgroups of $\mathrm{PPol}(\mathbb{Z}_{p^n})$ took considerable effort by Frisch and Krenn [15]. There exist some results on the structure, though. Frisch [14] characterized $\mathrm{PPol}(R)$ as a wreath product when R is a finite, commutative, unital, local ring with maximal ideal of nilpotency class 2. There is another wreath product characterization by Nöbauer for the residue class rings $\mathbb{Z}_{p^n}$ [16], or for polynomials permuting prime residue classes see [17], and more generally for finite quotients of Dedekind domains [13, p. 180, Chapter 4, Theorem 5.94].