Available online at www.sciencedirect.com
ScienceDirect
Finite Fields and Their Applications 13 (2007) 113–120
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

On strong orthogonal systems and weak permutation polynomials over finite commutative rings☆

Qijiao Wei[a,b], Qifan Zhang[a,*]

[a]*College of Mathematics, Sichuan University, Chengdu 610064, China*
[b]*Department of Computation Science, Chengdu University of Information Technology, Chengdu, China*

Received 5 March 2005; revised 31 July 2005

Communicated by Rudolf Lidl

Available online 22 September 2005

Abstract

We study two kinds of orthogonal systems of polynomials over finite commutative rings and get two fundamental results. Firstly, we obtain a necessary and sufficient condition for a system of polynomials (over a fixed finite commutative ring R) to form a strong orthogonal system. Secondly, for a pair (R, n) of a finite local ring R and an integer $n > 1$, we get an easy criterion to check whether every weak permutation polynomial in n variables over R is strong.

Keywords: Permutation polynomial; Orthogonal system; Finite field; Finite local ring

1. Introduction

Let R be a finite commutative ring with identity. A polynomial in $R[X]$ is called a permutation polynomial if it induces a permutation of R. This notion has been generalized to polynomials or polynomial systems in $n > 1$ variables in two different ways.

☆ This work is supported by the national science foundation of China (Numbers 10128103 and 19901023).
* Corresponding author.
E-mail address: sszibbh@mail.sc.cninfo.net (Q. Zhang).

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2005.08.005

See [7] for a comprehensive account of permutation polynomials and [8] for a survey. The notion, regarded as *weak permutation polynomial* in this paper (also in [3]), is called *permutation polynomial* in most references.

Definition. A map between two finite sets is said to be uniform if all fibers have the same sizes. Let $f_1, \ldots, f_k$ be polynomials in n variables. Then they are said to form a weak orthogonal system over R if they induce a uniform map from R^n to R^k. They are said to form a strong orthogonal system if there exist polynomials $f_{k+1}, \ldots, f_n$ such that the n polynomials $f_1, \ldots, f_n$ induce a permutation of R^n. Specially, it is called a weak permutation polynomial or strong permutation polynomial if $k = 1$. If $f_1, \ldots, f_n$ induce a permutation of R^n, we call $(f_1, \ldots, f_n)$ a permutation polynomial vector.

It is easy to see that $f_1, \ldots, f_k$ form a weak orthogonal system over R if and only if there exist functions (may not be polynomial) $f_{k+1}, \ldots, f_n$ such that $f_1, \ldots, f_n$ induce a permutation of R^n. One has the following basic facts:

(1) A strong orthogonal system is weak.

(2) Every weak orthogonal system over a finite field is strong (as every function over a finite field is a polynomial function).

Fact (2) was first shown by Carlitz [2]. Frisch [3] characterized all R over which every weak permutation polynomial is strong. Kaiser and Nöbauer [4] proved the special case $R = \mathbb{Z}/m\mathbb{Z}$ earlier. Since every finite commutative ring is a direct sum of several finite local rings, we can consider only finite commutative local rings. From now on, we make conventions without a special statement, as follows:

Let $\mathbb{F}_q$ denote a finite field with q elements. Let R denote a finite commutative local ring with maximum ideal $\mathcal{M}$. Let r denote the least number such that there exist r elements to generate $\mathcal{M}$. Moreover, we will abbreviate a polynomial $f(X_1, \ldots, X_n)$ to *$f(X)$, and denote by $f'(X)$, the column vector of polynomials*

$$\begin{pmatrix} \dfrac{\partial f}{\partial X_1} \\ \dfrac{\partial f}{\partial X_2} \\ \vdots \\ \dfrac{\partial f}{\partial X_n} \end{pmatrix}.$$

For any $x \in R^n$, $f(x)$ and $f'(x)$ have the natural meaning. For any ideal $\mathcal{I}$ of R and two elements $a = (a_1, \ldots, a_n)$, $b = (b_1, \ldots, b_n)$ in R^n, we say $a \equiv b \pmod{\mathcal{I}}$ if $a_i \equiv b_i \pmod{\mathcal{I}}$ for all i. For an element λ in R or $R[X_1, \ldots, X_n]$, we always denote by $\overline{\lambda}$, its reduction mod $\mathcal{M}$.

Frisch's result is, in nature, the following:

(3) If R is not a field and $n > r$, then there exist a weak permutation polynomial in $R[X_1, \ldots, X_n]$ which is not strong.

In this paper, we will prove that for $n \leqslant r$, all weak permutation polynomials in $R[X_1, \ldots, X_n]$ are strong. In some sense, it is easy to understand strong