Math. Maced.
Vol. 5 (2007)
77-81

POLYNOMIAL n-ARY QUASIGROUPS

SIMONA SAMARDZISKA[1] AND SMILE MARKOVSKI[2]

Abstract. A polynomial quasigroup is said to be a quasigroup $(Q, *)$ defined by a multivariate polynomial $P(x, y)$ by $x * y = P(x, y)$ for each $x, y \in Q$. We give a generalization of the notion of polynomial quasigroups, for the case of n-ary quasigroups, and we characterize them exactly by providing necessary and sufficient conditions for their existence.

1. Introduction

A polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ in a finite ring R is said to be a *permutation polynomial* if P permutes the elements of R.

We say that an n-ary quasigroup (Q, f) is a *polynomial n-ary quasigroup* if there is a ring $(Q, +, \cdot)$ and a polynomial $P(x_1, x_2, \ldots, x_n) \in Q[x_1, x_2, \ldots, x_n]$ such that $f(x_1, x_2, \ldots, x_n) = P(x_1, x_2, \ldots, x_n)$ for every $x_1, x_2, \ldots, x_n \in Q$. Note that for $n = 1$ we have a set Q endowed with a permutation f, and for $n = 2$ we have a usual binary quasigroup.

In the sequel we consider only the case when the ring is $R = \mathbb{Z}_{p^w}$, where p is prime and w is a positive integer.

Rivest [3] considers polynomials over $\mathbb{Z}_{2^w}$ that define binary quasigroups of order 2^w. He proves the following statement.

Theorem 1. (a) *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients. Then $P(x)$ is a permutation polynomial modulo 2^w, $w \geq 2$, if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \ldots)$ is even, and $(a_3 + a_5 + a_7 + \ldots)$ is even.*

(b) *A bivariate polynomial $P(x, y) = \sum_{i,j} a_{i,j} x^i y^j$, represents a quasigroup operation in $\mathbb{Z}_{2^w}$, $w \geq 2$, if and only if the four univariate polynomials $P(x, 0)$, $P(x, 1)$, $P(0, y)$ and $P(1, y)$, are all permutation polynomials in $\mathbb{Z}_{2^w}$.*

The key result of this article, given in Section 2, is the generalization of the Rivest's theorem, for polynomials of n variables over the ring $\mathbb{Z}_{2^w}$. In Section 3 we give one more generalization, where we consider the ring $\mathbb{Z}_{p^w}$ for prime p.

2. Polynomial n-ary quasigroups on $\mathbb{Z}_{2^w}$

An n-ary quasigroup is a pair (Q, f) of a nonempty set Q and an n-ary operation f with the property that for any given n elements $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_{n+1} \in Q$

2000 *Mathematics Subject Classification.* 20N05;20N15.
Key words and phrases. Permutation polynomial, n-ary quasigroup, polynomial quasigroup.

and any $i = 1, 2, \ldots, n$, there is a uniquely determined element $a_i \in Q$ such that

$$f(a_1, a_2, \ldots, a_n) = a_{n+1}.$$

Equivalently, (Q, f) is an n-ary quasigroup if the unary operations

$$f_{a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n}(x) = f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n)$$

are permutations of Q.

Clearly, the following is true:

Proposition 2.1. *Given an n-ary quasigroup (Q, f) and given any fixed elements $a_{i_1}, \ldots, a_{i_k} \in Q$, the projection operation*

$$\begin{aligned} & f_{a_{i_1},\ldots,a_{i_k}}(x_1, \ldots, x_{i_1-1}, x_{i_1+1}, \ldots, x_{i_k-1}, x_{i_k+1}, \ldots, x_n) = \\ = \quad & f(x_1, \ldots, x_{i_1-1}, a_{i_1}, x_{i_1+1}, \ldots, x_{i_k-1}, a_{i_k}, x_{i_k+1}, \ldots, x_n) \end{aligned}$$

defines an $(n-k)$-ary quasigroup $(Q, f_{a_{i_1},\ldots,a_{i_k}})$, for each $k = 1, 2, \ldots, n-1$.

Now, let $P(x_1, x_2, \ldots, x_n)$ be a polynomial over the ring $(\mathbb{Z}_{2^w}, +, \cdot)$. We are interested, under what conditions P defines an n-ary quasigroup.

We will need the following lemma:

Lemma 1. [3] *Let $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ be a polynomial with integral coefficients, and let $n = 2m$, where m is even.*
If $P(x)$ is a permutation polynomial modulo m, then $P(x)$ is a permutation polynomial modulo n if and only if $(a_3 + a_5 + a_7 + \ldots)$ is even.

We will prove the next:

Theorem 2. *Let $P(x_1, x_2, \ldots, x_n)$ be a polynomial over the ring $(\mathbb{Z}_{2^w}, +, \cdot)$. $P(x_1, x_2, \ldots, x_n)$ is a polynomial that defines an n-ary quasigroup, $n \geq 2$, if and only if for every $(a_1, \ldots, a_{n-1}) \in \{0,1\}^{n-1}$ each of the polynomials*

$$\begin{aligned} P_1(x_1) &= P(x_1, a_1, \ldots, a_{n-1}), \\ P_2(x_2) &= P(a_1, x_2, \ldots, a_{n-1}), \\ &\vdots \\ P_n(x_n) &= P(a_1, \ldots, a_{n-1}, x_n). \end{aligned} \tag{2.1}$$

is a permutation polynomial.

Proof. The necessary condition comes as a direct consequence of Proposition 2.1.

For the opposite direction, we will use induction on the number of variables n of the polynomial P.

The first step, when $n = 2$, is given by Theorem 1(b).

Let the theorem hold for $n - 1$.

Let us assume that (2.1) are permutation polynomials, but $P(x_1, x_2, \ldots, x_n)$ does not define an n-ary quasigroup. This means that there exists $c \in \mathbb{Z}_{2^w}$, such that some of the polynomials $P(c, x_2, \ldots, x_n)$, $P(x_1, c, x_3, \ldots, x_n)$, $P(x_1, \ldots, x_{n-1}, c)$ does not define a $n-1$ - ary quasigroup. Without loss of generality, we may

assume that it is the polynomial $P'(x_1,\dots,x_{n-1}) = P(x_1,\dots,x_{n-1},c)$. From the inductive hypothesis, some of the polynomials

$$P(x_1,a_1,\dots,a_{n-2},c),\ \ P(a_1,x_2,\dots,a_{n-2},c),\ \dots,\ P(a_1,\dots,a_{n-2},x_{n-1},c),$$

where $(a_1,\dots,a_{n-2}) \in \{0,1\}^{n-2}$, is not a permutation.

Again, without loss of generality, this polynomial may be considered as the polynomial $P(\mathbf{x},c)$.

From the assumption , $P(\mathbf{x},0)$ and $P(\mathbf{x},1)$ are permutation polynomials modulo 2^w, hence permutation polynomials modulo 2. Since $c = 2c_1 + b$ where $b \in \{0,1\}$, we have:

$$P(\mathbf{x},c) = \sum_i p_i(\mathbf{x})c^i = \sum_i p_i(\mathbf{x})b^i = P(\mathbf{x},b) \quad (mod 2)$$

Therefore, $P(\mathbf{x},c)$ is a permutation polynomial modulo 2.

Also, $P(\mathbf{x},c)$ can be rewritten as:

$$P(\mathbf{x},c) = \sum_i (\sum_j a_{ij}c^j)x^i$$

From Lemma 1 this is permutation polynomial modulo 2^w, if and only if

$$\sum_{i\geq 3, i-odd} a_{ij}c^j = 0 \quad (mod 2)$$

But,

$$\sum_{i\geq 3, i-odd} a_{ij}c^j = \sum_{i\geq 3, i-odd} a_{ij}b^j = 0 \quad (mod 2)$$

since $P(\mathbf{x},b)$ is permutation polynomial modulo 2^w.

It follows that $P(\mathbf{x},c)$ is permutation polynomial modulo 2^w, a contradiction with our assumption. Hence, the theorem is proven. □

The next natural step is to see what do the conditions of Theorem 2 look like for the more general case of polynomials over the ring $(\mathbb{Z}_{p^w},+,\cdot)$, p - prime.

3. Quasigroups and polynomials over the ring $(\mathbb{Z}_{p^w},+,\cdot)$, p - prime

In chapter VIII of [1], Hardy and Wright, study the solutions of a congruence to a prime-power modulus. As a direct consequence of Theorem 123 (also noted in [2]), a polynomial $P(x)$ in one variable permutes the elements of $\mathbb{Z}_{p^w}$, if and only if it permutes the elements of $\mathbb{Z}_p$, and $P'(i) \neq 0\ (modp)$ for every integer i. In other words:

Proposition 3.1. *A polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo p^w, p-prime,$w \geq 2$ if and only if the following two conditions are true simultaneously:*

1. *$P(x)$ is a permutation polynomial modulo p, i.e. $\forall i,j \in \{0,1,\dots,p-1\}$ and $i \neq j$, $P(j) - P(i) \neq 0\ (modp)$*
2. *$\forall i \in \{0,1,\dots,p-1\}$, $P'(i) = a_1 + 2ia_2 + \cdots + di^{d-1}a_d \neq 0\ (modp)$*

Remark 3.1: It is easy to establish, that the main theorem from [3], i.e. Theorem 1(a), is a direct consequence of Proposition 3.1.

Next, we state and prove the equivalence of Theorem 1(b), for the ring $\mathbb{Z}_{p^w}$.

Theorem 3. *A bivariate polynomial $P(x,y) = \sum_{i,j} a_{i,j} x^i y^j$, represents a quasigroup modulo p^w, p-prime, $w \geq 2$, if and only if the $2p$ univariate polynomials*

$$\begin{aligned} &P(x,0), P(x,1), \ldots, P(x,p-1), \\ &P(0,y), P(1,y), \ldots, P(p-1,y), \end{aligned} \tag{3.1}$$

are all permutation polynomials modulo p^w.

Proof. It is clear that "the only if" part holds.
Assume now that the polynomials (3.1) are permutation polynomials modulo p^w, but $P(x,y)$ is not a representation of a quasigroup. That means that there exists $c \in \mathbb{Z}_{p^w}$, such that at least one of $P(x,c)$ or $P(c,y)$ is not a permutation polynomial. Without loss of generality, let that polynomial be $P_c(x) = P(x,c)$. Since $c = p\,c_1 + b$ where $b \in \{0,1,\ldots p-1\}$, we have:

$$P_c(x) = P(x,c) = \sum_i p_i(x) c^i = \sum_i p_i(x) b^i = P(x,b) \quad (modp)$$

hence, $P(x,c)$ is a permutation polynomial modulo p. And since:

$$\begin{aligned} P_c'(x) &= (\sum_i (\sum_j a_{ij} c^j) x^i)' = \sum_i i \cdot (\sum_j a_{ij} c^j) x^{i-1} = \\ &= \sum_i i \cdot (\sum_j a_{ij} b^j) x^{i-1} = (\sum_i (\sum_j a_{ij} b^j) x^i)' = P_b'(x) \quad (modp) \end{aligned}$$

where $P_b(x) = P(x,b)$, it follows that $P_c'(i) \neq 0 \ (modp), \forall i \in \{0,1,\ldots,p-1\}$. From Proposition 3.1, we conclude that $P_c(x) = P(x,c)$ is a permutation polynomial modulo p^w. Therefore, our assumption is wrong, and this proofs the "if" part of the theorem. □

Now we can state the conditions for an n-variate polynomial over the ring $\mathbb{Z}_{p^w}$ to be a representation of an n-ary quasigroup. (the proof is omitted due to the similarity of the proof of Theorem 2)

Theorem 4. *Let $P(x_1, x_2, \ldots, x_n)$ be a polynomial over the ring $(\mathbb{Z}_{p^w}, +, \cdot)$, p-prime. $P(x_1, x_2, \ldots, x_n)$ is a polynomial that defines an n-ary quasigroup, $n \geq 2$, if and only if for every $(a_1, \ldots, a_{n-1}) \in \{0,1,\ldots,p-1\}^{n-1}$ each of the polynomials*

$$\begin{aligned} &P_1(x_1) = P(x_1, a_1, \ldots, a_{n-1}), \\ &P_2(x_2) = P(a_1, x_2, \ldots, a_{n-1}), \\ &\vdots \\ &P_n(x_n) = P(a_1, \ldots, a_{n-1}, x_n). \end{aligned}$$

is a permutation polynomial over the ring $(\mathbb{Z}_{p^w}, +, \cdot)$.

References

[1] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon, Oxford, 4th ed., 1975.
[2] G. Mullen and H. Stevens, *Polynomial functions (mod m)*, Acta Math. Hungar. 44, (Nos. 3 - 4) (1984), 237-241.
[3] Ronald L. Rivest , *Permutation polynomials modulo* 2^w, Finite Fields and Their Applications 7 (2001), 287-292.

[1] FON University, Faculty of Communication and IT, Skopje, Macedonia
E-mail address: simona.samardziska@fon.edu.mk

[2] University Ss Cyril and Methodius, Faculty of Sciences, Institute of Informatics, Skopje, Macedonia
E-mail address: smile@ii.edu.mk