Int. J. Electron. Commun. (AEÜ) xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Short communication

A coefficient test for fourth degree permutation polynomials over integer rings

Lucian Trifina *, Daniela Tarniceriu

"Gheorghe Asachi" Technical University, Faculty of Electronics, Telecommunications and Information Technology, Department of Telecommunications, Bd. Carol I, no. 11, 700506 Iasi, Romania

ARTICLE INFO

Article history:
Received 8 December 2015
Accepted 10 September 2016
Available online xxxx

Keywords:
Fourth degree polynomial
Permutation polynomial
Coefficient test
Turbo codes

ABSTRACT

So far, there are known conditions on a polynomial's coefficients so that it is a permutation polynomial (PP) modulo a given positive integer number only for degrees up to three. For polynomials of degrees higher than three, we only know the conditions so that they are PPs modulo a power of two. In this paper, we propose a coefficient test for fourth degree polynomials to be PPs over integer rings. The test is useful for finding fourth degree PPs for different applications in communications such as interleavers for turbo codes.

1. Introduction

An interleaver is a critical component of a turbo code. The algebraic interleavers, especially permutation polynomial (PP) based ones, are preferred because of several advantages: analytical design, outstanding performances and simple, practical implementation with high-speed, low-power consumption and little memory requirements [1–4].

From the category of PP based interleavers, the quadratic permutation polynomial (QPP) [1–4] and then, the cubic permutation polynomial (CPP) [5,6] based ones received the most attention.

For using PP interleavers in practical applications, it is necessary to know the coefficients of the polynomial describing the interleaver. A brute-force exhaustive search is impractical when the number of PPs is large. Therefore, we require the conditions on a polynomial's coefficients so that it is a PP one. So far, we have known the conditions for a polynomial of any degree to be a PP modulo 2^w, with w a positive integer [7], the conditions for a polynomial of second degree to be QPP [1–4], and the conditions for a polynomial of third degree to be CPP [5,6]. This paper extends the conditions in [5] for polynomials of fourth degree, so that they are PPs (denoted 4-PPs).

2. Results on permutation polynomials over integer rings

A PP based interleaver of degree d is of the form:

$$\pi(x) = q_0 + q_1 x + q_2 x^2 + \cdots + q_d x^d (\text{mod} \quad N) \tag{1}$$

where N is the interleaver length and the coefficients q_k, $k = 1, \ldots, d$ are chosen so that $\pi(x)$ from (1), with $x = 0, 1, \ldots, N-1$, is a permutation of the set of integers modulo N, $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$. Because the free term q_0, only determines a cyclic shift of the permutation elements, we will consider $q_0 = 0$.

Let $\mathbb{P} = \{2, 3, 5, \ldots\}$ be the set of prime numbers. In the following, the notation $p|N$ means that p divides N, the notation $p\nmid N$ means that p does not divide N and $\pi'(x)$ denotes the formal derivative of the polynomial $\pi(x)$. We recall the next two theorems, which are useful for obtaining the results in Section 3, from [5].

Theorem 2.1. *For any* $N = \prod_{p|N, p\in\mathbb{P}} p^{n_{N,p}}$, $\pi(x)$ *is a PP modulo* N *iff* $\pi(x)$ *is also a PP modulo* $p^{n_{N,p}}, \forall p$ *such that* $n_{N,p} \geqslant 1$.

Theorem 2.2. $\pi(x)$ *is a PP modulo* p^n, *with* $n > 1$, *iff* $\pi(x)$ *is a PP modulo* p *and* $\pi'(x) \neq 0 (\text{mod}\ p)$, *for every integer* x.

In this paper, we present a direct test on the coefficients q_1, q_2, q_3, q_4 of a fourth degree polynomial, so that it is a 4-PP.

3. A coefficient test for fourth degree PPs

This section is similar to Section III in [5], but considers 4-PPs instead of CPP. We still use the same three-step algorithm (given

* Corresponding author.
E-mail addresses: luciant@etti.tuiasi.ro (L. Trifina), tarniced@etti.tuiasi.ro (D. Tarniceriu).

http://dx.doi.org/10.1016/j.aeue.2016.09.006
1434-8411/

Table 1
A coefficient test for fourth degree PPs modulo p^n

$p=2$	$n=1$	$(q_1+q_2+q_3+q_4)$ is odd
	$n>1$	q_1 is odd, (q_2+q_4) is even, q_3 is even
$p=3$	$n=1$	$(q_1+q_3)\neq 0 \pmod 3$, $(q_2+q_4)=0 \pmod 3$
	$n>1$	$q_1\neq 0 \pmod 3$, $(q_1+q_3)\neq 0 \pmod 3$, $q_2=q_4=0 \pmod 3$
$p=7$	$n=1$	(1) If $q_4\neq 0 \pmod 7$, then (1.1) $3(q_3)^2=q_2q_4 \pmod 7$, and (1.2) $2q_1(q_4)^2=(q_3)^3+(q_4)^3 \pmod 7$ or $2q_1(q_4)^2=(q_3)^3+6(q_4)^3 \pmod 7$. (2) If $q_4=0 \pmod 7$ then $q_1\neq 0 \pmod 7$ and $q_2=q_3=0 \pmod 7$.
	$n>1$	$q_1\neq 0 \pmod 7, q_2=q_3=q_4=0 \pmod 7$
$3\nmid(p-1)$ ($p=5$ or $p>7$)	$n=1$	$q_4=0 \pmod p$ and (1) If $q_3=0 \pmod p$ then $q_1\neq 0 \pmod p$ and $q_2=0 \pmod p$. (2) If $q_3\neq 0 \pmod p$ then $(q_2)^2=3q_1q_3 \pmod p$.
	$n>1$	$q_1\neq 0 \pmod p, q_2=q_3=q_4=0 \pmod p$
$3\mid(p-1)$ $(p>7)$	$n\geqslant 1$	$q_1\neq 0 \pmod p, q_2=q_3=q_4=0 \pmod p$

below) to check if a fourth degree polynomial $\pi(x)$ is 4-PP, but the conditions from Table 1 are different.

(1) Factor N as $N=\prod_{p\in\mathbb{P},\, p\mid N} p^{n_{N,p}}$.
(2) For each p and the corresponding $n_{N,p}$ from the previous step, test if the conditions in Table 1 are satisfied.
(3) $\pi(x)$ is a 4-PP iff all tests in step 2 are satisfied.

In the following, we prove that Table 1 is equivalent to Theorem 2.2 for 4-PPs. The cases $p=2$ with $n\geqslant 1$, $p=3$ with $n\geqslant 1$ and $p=7$ with $n=1$ are addressed in Sections 3.1, 3.2 and 3.3, respectively. Because of the similarity of the cases $p=7$ and $n>1$, $3\mid(p-1)$ with $p>7$ and $n\geqslant 1$, $3\nmid(p-1)$ with $p=5$ or $p>7$ and $n>1$, they are addressed together in Section 3.4. The last case, when $3\nmid(p-1)$ with $p=5$ or $p>7$ and $n=1$, is addressed in Section 3.5.

3.1. p = 2

For $p=2$, a simple test on the coefficients is given in [7], for any degree of the polynomial. For the fourth degree, the conditions are given in Table 1.

3.2. p = 3

3.2.1. p = 3 and n = 1

Theorem 3.1. *$\pi(x)=q_1x+q_2x^2+q_3x^3+q_4x^4 \pmod 3$ is a PP iff $(q_1+q_3)\neq 0 \pmod 3$ and $(q_2+q_4)=0 \pmod 3$.*

Proof. As $\pi(0)=0$, it requires that

$$\pi(1)=q_1+q_2+q_3+q_4\neq 0 \pmod 3, \tag{2}$$

$$\pi(2)=2q_1+q_2+2q_3+q_4\neq 0 \pmod 3, \tag{3}$$

and

$$\pi(1)\neq\pi(2) \pmod 3. \tag{4}$$

Replacing (2) and (3) in (4), we have

$$(q_1+q_3)\neq 0 \pmod 3. \tag{5}$$

If $q_1+q_3=1 \pmod 3$, then, from (2) it follows that $q_2+q_4=0 \pmod 3$ or $q_2+q_4=1 \pmod 3$, and from (3) it follows that $q_2+q_4=0 \pmod 3$ or $q_2+q_4=2 \pmod 3$. Therefore, $q_2+q_4=0 \pmod 3$. For the case $q_1+q_3=2 \pmod 3$ we can obtain the same result in a similar way. □

3.2.2. p = 3 and n > 1

Theorem 3.2. *$\pi(x)=q_1x+q_2x^2+q_3x^3+q_4x^4 \pmod{3^n}$, with $n>1$, is a PP iff $(q_1+q_3)\neq 0 \pmod 3$, $q_2=q_4=0 \pmod 3$ and $q_1\neq 0 \pmod 3$.*

Proof. For the direct proof, we consider that $\pi(x)$ is a PP $\pmod{3^n}$, with $n>1$. Then, according to Theorem 2.2, $\pi(x)$ is a PP $\pmod 3$ and

$$\begin{aligned}\pi'(x)&=q_1+2q_2x+3q_3x^2+4q_4x^3 \pmod 3\\ &=q_1+2q_2x+q_4x^3\neq 0 \pmod 3.\end{aligned} \tag{6}$$

As $\pi(x)$ is a PP $\pmod 3$, from Theorem 3.1,, we have $(q_1+q_3)\neq 0 \pmod 3$ and $(q_2+q_4)=0 \pmod 3$. Replacing $x=0$ in (6), we have $\pi'(0)=q_1\neq 0 \pmod 3$. Replacing $x=1$ in (6), we have $\pi'(1)=q_1+2q_2+q_4\neq 0 \pmod 3$. Because $(q_2+q_4)=0 \pmod 3$, it follows that

$$\pi'(1)=q_1+q_2\neq 0 \pmod 3. \tag{7}$$

Replacing $x=2$ in (6), we have $\pi'(2)=q_1+q_2+2q_4\neq 0 \pmod 3$ and, because $(q_2+q_4)=0 \pmod 3$, it follows that

$$\pi'(2)=q_1+q_4\neq 0 \pmod 3. \tag{8}$$

Relations (7) and (8) must hold for any $q_1\neq 0 \pmod 3$. For $q_1=1 \pmod 3$, from (7) it follows that $q_2=0 \pmod 3$ or $q_2=1 \pmod 3$, and from (8) that $q_4=0 \pmod 3$ or $q_4=1 \pmod 3$. For $q_1=2 \pmod 3$, from (7), it follows that $q_2=0 \pmod 3$ or $q_2=2 \pmod 3$, and from (8) that $q_4=0 \pmod 3$ or $q_4=2 \pmod 3$. Therefore, only the values $q_2=0 \pmod 3$ and $q_4=0 \pmod 3$ meet (7) and (8) for any $q_1\neq 0 \pmod 3$.

For the converse proof, because $(q_1+q_3)\neq 0 \pmod 3$ and $q_2=q_4=0 \pmod 3$, it follows from Theorem 3.1 that $\pi(x)$ is a PP $\pmod 3$.

For $q_2=q_4=0 \pmod 3$, from (6) we have that $\pi'(x)=q_1\neq 0 \pmod 3$. Then, according to Theorem 2.2, it results that $\pi(x)$ is a PP $\pmod{3^n}$, with $n>1$. □

3.3. p = 7 and n = 1

For this case, we need the following lemmas and propositions.

Proposition 3.3 [8]. *A polynomial $\pi(x)$ is a PP $\pmod p$, with $p\nmid d$, iff $a\pi(x+b)+c$ is PP for all $a\neq 0, b, c\in\mathbb{Z}_p$.*

Definition 3.4 [8]. Let $\bar{\pi}(x)=\sum_{k=1}^{d}q_kx^k \pmod{p^n}$. The polynomial $\bar{\pi}(x)$ is a normalized PP if $q_d=1$, $\bar{\pi}(0)=0$, and if $p\nmid d$, then $q_{d-1}=0$.

Proposition 3.5 [9]. *The only normalized fourth degree $\pmod 7$ PPs are $\bar{\pi}(x)=x^4\pm 3x \pmod 7$.*

Lemma 3.6. *Let $\pi(x)=q_1x+q_2x^2+q_3x^3+q_4x^4 \pmod 7$, where $q_4\neq 0 \pmod 7$. Then, $\pi(x)$ can be factorized as $\pi(x)=a\big((x+b)^4\pm 3(x+b)\big)+c \pmod 7$, iff the following two conditions are fulfilled:*

Please cite this article in press as: Trifina L, Tarniceriu D. A coefficient test for fourth degree permutation polynomials over integer rings. Int J Electron Commun (AEÜ) (2016), http://dx.doi.org/10.1016/j.aeue.2016.09.006