AppliedMath

MDPI

Article

Inverses for Fourth-Degree Permutation Polynomials Modulo 32Ψ or 96Ψ, with Ψ as a Product of Different Prime Numbers Greater than Three

Lucian Trifina *, Daniela Tărniceriu and Ana-Mirela Rotopănescu

Department of Telecommunications and Information Technologies, "Gheorghe Asachi" Technical University, 700506 Iasi, Romania; tarniced@etti.tuiasi.ro (D.T.); mrotopanescu@etti.tuiasi.ro (A.-M.R.)
* Correspondence: luciant@etti.tuiasi.ro

Abstract: In this paper, we address the inverse of a true fourth-degree permutation polynomial (4-PP), modulo a positive integer of the form $32k_L\Psi$, where $k_L \in \{1,3\}$ and Ψ is a product of different prime numbers greater than three. Some constraints are considered for the 4-PPs to avoid some complicated coefficients' conditions. With the fourth- and third-degree coefficients of the form $k_{4,f}\Psi$ and $k_{3,f}\Psi$, respectively, we prove that the inverse PP is (I) a 4-PP when $k_{4,f} \in \{1,3\}$ and $k_{3,f} \in \{1,3,5,7\}$ or when $k_{4,f} = 2$ and (II) a 5-PP when $k_{4,f} \in \{1,3\}$ and $k_{3,f} \in \{0,2,4,6\}$.

Keywords: permutation polynomial (PP); fourth-degree PP; inverse PP

check for updates

Citation: Trifina, L.; Tărniceriu, D.; Rotopănescu, A.-M. Inverses for Fourth-Degree Permutation Polynomials Modulo 32Ψ or 96Ψ, with Ψ as a Product of Different Prime Numbers Greater than Three. *AppliedMath* **2024**, *4*, 383–393. https://doi.org/10.3390/appliedmath4010020

Academic Editor: Libor Pekař

Received: 15 January 2024
Revised: 20 February 2024
Accepted: 3 March 2024
Published: 16 March 2024

1. Introduction

Permutation polynomials (PPs) have been studied for a long time [1]. Possible applications of PPs include those in cryptography, those used for sequence generation, or those used for interleavers in turbo codes [2–5].

A well-known result is that a permutation induced by a PP, $\pi(x)$, modulo a positive integer L, has an inverse permutation induced also by a PP, $\rho(x)$, modulo L. The PP $\rho(x)$ that generates the inverse permutation is named the inverse PP modulo L of PP $\pi(x)$. The inverse of a PP is particularly useful for deriving upper bounds of the minimum distance of a turbo code when using a PP interleaver [6].

1.1. Main Contributions

In the following, we list the main contributions of this paper:

- We derive the inverse PPs for fourth-degree PPs (4-PPs) modulo a positive integer of the form 32Ψ or 96Ψ, with Ψ as a product of different prime numbers greater than three. To avoid some complicated conditions on the coefficients, we impose some restrictions when the condition $3 \nmid (p_i - 1)$ or $p_i = 7$ is fulfilled for a prime $p_i \mid \Psi$. In these cases, we consider only the fourth-, third-, and second-degree coefficients that are multiples of p_i. If Ψ is a product of different prime numbers $p_i > 7$ so that $3 \mid (p_i - 1)$, the result in this paper is fully general with respect to the possible coefficients of the 4-PP.
- We give examples showing how to compute the inverse of a 4-PP. If the fourth-, third-, and second-degree coefficients of the 4-PP are of the forms $k_{4,f}\Psi$, $k_{3,f}\Psi$, and $k_{2,f}\Psi$, respectively, the second-to-the highest-degree coefficients of the inverse PP are immediately found using the results obtained depending on the values of $k_{4,f}$, $k_{3,f}$, and $k_{2,f}$. The first-degree coefficient of the inverse PP can be found from a first-degree congruence equation involving the first-degree coefficient of the 4-PP.
- In the "Remarks" section, we show how the inverse of a 4-PP can be found by means of the inverse normalized PPs modulo each factor from the prime decomposition of

L. We have made remarks regarding the facilities of finding the inverse PP using the results derived in this paper.

1.2. Structure of This Paper

The structure of this paper is as follows. Some basic results about 4-PPs are given in Section 2. The main results are obtained in Section 3. Four examples illustrating how we can find the inverse of 4-PP are given in Section 4, and some remarks are made in Section 5.

2. Preliminaries

2.1. Notations

The following notations are used in the paper:

- $\mathbb{N}^*$ stands for the set of positive integers (i.e., the set of natural numbers greater than zero).
- $\pmod{L}$, with $L \in \mathbb{N}^*$, stands for the modulo L operation.
- $a \mid b$, with $a, b \in \mathbb{N}^*$, stands for a divides b.
- $a \nmid b$, with $a, b \in \mathbb{N}^*$, stands for a does not divide b.
- $\gcd(a, b)$, with $a, b \in \mathbb{N}^*$, stands for the greatest common divisor of a and b.
- $a!$, with $a \in \mathbb{N}^*$, stands for the factorial of a (i.e., the product $1 \cdot 2 \cdot 3 \cdot \cdots \cdot a$).

2.2. Results about 4-PPs

A fourth-degree polynomial

$$\pi(x) = (f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4) \pmod{L}, \tag{1}$$

is 4-PP modulo L if for $x \in \{0, 1, \ldots, L-1\}$, values $\pi(x) \pmod{L}$ produce a permutation of the set $\{0, 1, \cdots, L-1\}$.

A 4-PP is *true* if the permutation it performs cannot be accomplished by a permutation polynomial of a degree smaller than four.

Two 4-PPs with different coefficients are called *different* if they perform different permutations.

In [7], conditions on coefficients f_1, f_2, f_3, and f_4 are derived so that the fourth-degree polynomial in (1) is a 4-PP modulo L. As we are interested in positive integers, L, of the form $32 \cdot \prod_{i=1}^{N_p} p_i$ or $96 \cdot \prod_{i=1}^{N_p} p_i$, with N_p as a positive integer, we give in Table 1 conditions for the coefficients only for the primes 2, 3, and p_i, $i = 1, 2, \ldots, N_p$, when L is of the form

$$L = 2^{n_{L,2}} \cdot 3^{n_{L,3}} \cdot \prod_{i=1}^{N_p} p_i, \text{ with } n_{L,2} > 1, n_{L,3} \in \{0, 1\},$$
$$p_i > 3, i = 1, 2, \ldots, N_p, p_1 < p_2 < \cdots < p_{N_p}. \tag{2}$$

Table 1. Conditions for coefficients f_1, f_2, f_3, f_4 so that $\pi(x)$ in (1) is a 4-PP modulo L of the form (2).

$p = 2$	$n_{L,2} > 1$	$f_1 \neq 0, (f_2 + f_4) = 0, f_3 = 0 \pmod{2}$
$p = 3$	$n_{L,3} = 1$	$(f_1 + f_3) \neq 0, (f_2 + f_4) = 0 \pmod{3}$
$3 \mid (p_i - 1)$ $(p_i > 7)$	$n_{L,p_i} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0, f_4 = 0 \pmod{p_i}$
$3 \nmid (p_i - 1)$ $(p_i \geq 5)$	$n_{L,p_i} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0, f_4 = 0 \pmod{p_i}$ or $f_2^2 = 3f_1 f_3 \pmod{p_i}, f_3 \neq 0, f_4 = 0 \pmod{p_i}$

A d-PP modulo L

$$\rho(x) = (\rho_1 x + \rho_2 x^2 + \cdots + \rho_d x^d) \pmod{L}, d \in \mathbb{N}^* \tag{3}$$

is an inverse of the 4-PP in (1) if

$$\pi(\rho(x)) = x \pmod{L}, \forall x \in \{0, 1, \cdots, L-1\}. \tag{4}$$

3. Main Results

The positive integers L will be considered of the form

$$L = 32 \cdot \prod_{i=1}^{N_p} p_i = 2^5 \cdot \prod_{i=1}^{N_p} p_i \text{ or } L = 96 \cdot \prod_{i=1}^{N_p} p_i = 2^5 \cdot 3 \cdot \prod_{i=1}^{N_p} p_i, \tag{5}$$

with $p_1, p_2, \ldots, p_{N_p}$ different prime numbers so that $3 < p_1 < p_2 < \cdots < p_{N_p}$.

To avoid some complicated conditions for the coefficients, if p_i is a prime such that $3 \nmid (p_i - 1)$ and $p_i \geq 5$, $i \in \{1, 2, \ldots, N_p\}$, or if $p_i = 7$, only the following conditions

$$f_1 \neq 0, f_2 = 0, f_3 = 0, f_4 = 0 \pmod{p_i}. \tag{6}$$

will be considered for the 4-PPs' coefficients.

We denote

$$\prod_{i=1}^{N_p} p_i = \Psi. \tag{7}$$

3.1. Coefficients of 4-PPs Modulo a Positive Integer of the Form 32Ψ or 96Ψ

The next lemma gives the possible values of the coefficients for a 4-PP modulo a positive integer of the form (5).

Lemma 1. *Let a positive integer L be of the form given in* (5)*. Then, the possible values for coefficients f_4, f_3, and f_2 for a true different 4-PP fulfilling conditions* (6) *when $3 \nmid (p_i - 1)$ or when $p_i = 7$ are equivalent to those given in Table 2. Coefficient f_1 will always be odd.*

Table 2. Possible values for coefficients f_4, f_3, and f_2 so that $\pi(x)$ in (1) is a true 4-PP modulo L of the form (5) (Ψ is as in (7)).

L	f_4	f_3	f_2
32Ψ	Ψ or 3Ψ	0 or 2Ψ or 4Ψ or 6Ψ or 8Ψ or 10Ψ or 12Ψ or 14Ψ	Ψ or 3Ψ or 5Ψ or 7Ψ or 9Ψ or 11Ψ or 13Ψ or 15Ψ
	2Ψ	0 or 2Ψ or 4Ψ or 6Ψ or 8Ψ or 10Ψ or 12Ψ or 14Ψ	0 or 2Ψ or 4Ψ or 6Ψ or 8Ψ or 10Ψ or 12Ψ or 14Ψ
96Ψ	Ψ	0 or 2Ψ or 4Ψ or 6Ψ or 8Ψ or 10Ψ or 12Ψ or 14Ψ	5Ψ or 11Ψ or 17Ψ or 23Ψ or 29Ψ or 35Ψ or 41Ψ or 47Ψ
	2Ψ	0 or 2Ψ or 4Ψ or 6Ψ or 8Ψ or 10Ψ or 12Ψ or 14Ψ	4Ψ or 10Ψ or 16Ψ or 22Ψ or 28Ψ or 34Ψ or 40Ψ or 46Ψ
	3Ψ	0 or 2Ψ or 4Ψ or 6Ψ or 8Ψ or 10Ψ or 12Ψ or 14Ψ	3Ψ or 9Ψ or 15Ψ or 21Ψ or 27Ψ or 33Ψ or 39Ψ or 45Ψ

Proof of Lemma 1. According to Section 3 from [8], a true 4-PP is equivalent to a 4-PP which has the coefficient $f_k < \frac{L}{\gcd(L,k!)}$, $k = 2, 3, 4$. Thus, for the positive integer L of the form $L = 32\Psi$, a true 4-PP is equivalent to a 4-PP for which $f_2 < L/2 = 16\Psi$, $f_3 < L/2 = 16\Psi$, and $f_4 < L/8 = 4\Psi$. For the positive integer L of the form $L = 96\Psi$, a true 4-PP is equivalent to a 4-PP for which $f_2 < L/2 = 48\Psi$, $f_3 < L/6 = 16\Psi$, and $f_4 < L/24 = 4\Psi$. From the coefficient conditions of a 4-PP in Table 1 and because Ψ is odd, we obtain coefficients f_2, f_3, and f_4 from Table 2.

We note that when $L = 32\Psi$ or $L = 96\Psi$, from condition 1) in Table 1, f_1 is odd. □

Because $\pi(x)$ is a true 4-PP, from Lemma 1, we have that

$$\begin{cases} f_4 = k_{4,f} \cdot \Psi, & \text{with } k_{4,f} \in \{1,2,3\} \\ f_3 = k_{3,f} \cdot 2\Psi, & \text{with } k_{3,f} \in \{0,1,2,3,4,5,6,7\} \\ f_2 = k_{2,f} \cdot \Psi, & \text{with } k_{2,f} = c_2 \cdot k_L + k_{4,f,L}, k_L \in \{1,3\}, \\ & c_2 \in \{1,3,5,7,9,11,13,15\} \end{cases} \tag{8}$$

The values of $k_{4,f,L}$ from (8) are as follows:

$$\begin{cases} k_{4,f,L} = 0, & \text{when } k_L = 1 \text{ and } k_{4,f} \in \{1,3\}, \\ k_{4,f,L} = -1, & \text{when } k_L = 1 \text{ and } k_{4,f} = 2, \\ k_{4,f,L} = 3 - k_{4,f}, & \text{when } k_L = 3. \end{cases} \tag{9}$$

Because p_i is odd $\forall i \in \{1,2,\ldots,N_p\}$, Ψ from (7) is also odd.

From Table 1 in reference [7], we can see that, if for a prime $p_i \mid \Psi$ with $3 \nmid (p_i - 1)$ and $p_i > 3$, coefficient $f_3 \neq 0 \pmod{p_i}$, condition $(f_2)^2 = 3f_1f_3 \pmod{p_i}$ has to be fulfilled. A similar remark is valid for $p_i = 7$ when $f_4 \neq 0 \pmod 7$. Thus, in these cases, coefficients f_2 and f_3 are not multiples of Ψ and the results derived in the next subsection are not applicable.

3.2. The Inverse PP of a 4-PP Modulo a Positive Integer of the Form 32Ψ or 96Ψ

The next lemma gives the coefficients of an inverse true 4-PP or 5-PP for a true 4-PP, fulfilling conditions (6) when $3 \nmid (p_i - 1)$ or when $p_i = 7$, modulo an integer of the form given in (5). In a previous result, we proved that a 4-PP modulo a positive integer of the form 16Ψ or 48Ψ always has an inverse true 4-PP. It is interesting that, unlike this previous result, for a 4-PP modulo, a positive integer of the form 32Ψ or 96Ψ, the inverse can be a true 4-PP or a true 5-PP.

In this lemma, an inverse true 4-PP is denoted as in Equation (3), with $d = 4$, and it has the possible coefficients

$$\begin{cases} \rho_4 = k_{4,\rho} \cdot \Psi, & \text{with } k_{4,\rho} \in \{1,2,3\} \\ \rho_3 = k_{3,\rho} \cdot 2\Psi, & \text{with } k_{3,\rho} \in \{0,1,2,3,4,5,6,7\} \\ \rho_2 = k_{2,\rho} \cdot \Psi, & \text{with } k_{2,\rho} = c_2 \cdot k_L + k_{4,\rho,L}, k_L \in \{1,3\}, \\ & c_2 \in \{1,3,5,7,9,11,13,15\} \end{cases} \tag{10}$$

and the values of $k_{4,\rho,L}$ from (10) as follows:

$$\begin{cases} k_{4,\rho,L} = 0, & \text{when } k_L = 1 \text{ and } k_{4,\rho} \in \{1,3\}, \\ k_{4,\rho,L} = -1, & \text{when } k_L = 1 \text{ and } k_{4,\rho} = 2, \\ k_{4,\rho,L} = 3 - k_{4,\rho}, & \text{when } k_L = 3. \end{cases} \tag{11}$$

Similarly, an inverse true 5-PP is denoted as in Equation (3), with $d = 5$, and has the following possible coefficients:

$$\begin{cases} \rho_5 = k_{5,\rho} \cdot \Psi, & \text{with } k_{5,\rho} \in \{1,2,3\} \\ \rho_4 = k_{4,\rho} \cdot \Psi, & \text{with } k_{4,\rho} \in \{0,1,2,3\} \\ \rho_3 = k_{3,\rho} \cdot \Psi, & \text{with } k_{3,\rho} \in \{1,3,5,\ldots,15\} \text{ when } k_{5,\rho} \in \{1,3\} \\ & \text{and } k_{3,\rho} \in \{0,2,4,\ldots,14\} \text{ when } k_{5,\rho} = 2 \\ \rho_2 = k_{2,\rho} \cdot \Psi, & \text{with } k_{2,\rho} \in \{1,3,5,\ldots,15\} \text{ when } k_{4,\rho} \in \{1,3\} \\ & \text{and } k_{2,\rho} \in \{0,2,4,\ldots,14\} \text{ when } k_{4,\rho} \in \{0,2\} \end{cases} \tag{12}$$

We note that a 5-PP modulo a positive integer of the form (5) has more possible coefficients, but as we will see, the inverse 5-PP of a 4-PP has coefficients only of the form in (12). The particular conditions for coefficients of a 5-PP, as in (12), are given in Table 3.

Table 3. Particular conditions for coefficients $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ so that $\rho(x)$ in (3), with $d = 5$, is a 5-PP modulo L of the form (2).

$p = 2$	$n_{L,2} > 1$	$\rho_1 \neq 0, (\rho_2 + \rho_4) = 0, (\rho_3 + \rho_5) = 0 \pmod 2$
$p = 3$	$n_{L,3} = 1$	$(\rho_1 + \rho_3 + \rho_5) \neq 0, (\rho_2 + \rho_4) = 0 \pmod 3$
$p = 5$	$n_{L,5} = 1$	$(\rho_1 + \rho_5) \neq 0, \rho_2 = 0, \rho_3 = 0, \rho_4 = 0 \pmod 5$
$p_i > 5$	$n_{L,p_i} = 1$	$\rho_1 \neq 0, \rho_2 = 0, \rho_3 = 0, \rho_4 = 0, \rho_5 = 0 \pmod{p_i}$

We note that, when $5|\Psi$, a true 5-PP is equivalent to a 5-PP which has the coefficient $\rho_5 < \frac{L}{\gcd(L,5!)}$. For $L = 32 \cdot k_L \cdot \Psi$, $k_L \in \{1,3\}$, this means that $\rho_5 < 4 \cdot \frac{\Psi}{5}$. But, from (12), $\rho_5 = k_{5,\rho} \cdot \Psi$, with $k_{5,\rho} \in \{1,2,3\}$, and thus, we have $\rho_5 > 4 \cdot \frac{\Psi}{5}$. However, from Section 3 in [8], an equivalent PP with $\rho(x)$, with the coefficient $\rho_5 < 4 \cdot \frac{\Psi}{5}$, can be obtained if we subtract from $\rho(x)$ a null polynomial modulo L, $z(x)$, with the coefficient $z_5 = k_{5,\rho} \cdot 4 \cdot \frac{\Psi}{5}$. Then, the resulting 5-PP has the coefficient $\rho_5 = k_{5,\rho} \cdot \frac{\Psi}{5}$, with $k_{5,\rho} \in \{1,2,3\}$, and thus, it is a true 5-PP.

Lemma 2. *Let a positive integer be of the form $L = 32 \cdot k_L \cdot \Psi$, with $k_L \in \{1,3\}$ and Ψ as in (7). Then, a true 4-PP $\pi(x) = f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 \pmod{L}$, fulfilling conditions (6) when $3 \nmid (p_i - 1)$ or when $p_i = 7$, has*

1. *A true inverse 4-PP $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 \pmod{L}$ when $k_{4,f} \in \{1,3\}$ and $k_{3,f} \in \{1,3,5,7\}$ or when $k_{4,f} = 2$;*
2. *A true inverse 5-PP $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 + \rho_5 x^5 \pmod{L}$ when $k_{4,f} \in \{1,3\}$ and $k_{3,f} \in \{0,2,4,6\}$.*

Proof of Lemma 2. $\pi(x)$ has the inverse PP $\rho(x)$ if

$$\pi(\rho(x)) = x \pmod{L}, \forall x \in \{0,1,\ldots,L-1\}. \tag{13}$$

With Lemma 1, for $\rho(x)$ a 5-PP, after some algebraic manipulations, Equation (13) is equivalent to

$$(f_1\rho_1 - 1) \cdot x + \Theta(x) = 0 \pmod{L}, \forall x \in \{0,1,\ldots,L-1\}, \tag{14}$$

where

$$\begin{gathered}
\Theta(x) = (f_1\rho_2 + f_2\rho_1^2) \cdot x^2 + (f_1\rho_3 + 2f_2\rho_2\rho_1 + f_3\rho_1^3) \cdot x^3 + \\
(f_4\rho_1^4 + 3f_3\rho_1^2\rho_2 + 2f_2\rho_3\rho_1 + f_2\rho_2^2 + f_1\rho_4) \cdot x^4 + \\
(4f_4\rho_1^3\rho_2 + 3f_3\rho_1^2\rho_3 + 3f_3\rho_1\rho_2^2 + 2f_2\rho_4\rho_1 + 2f_2\rho_3\rho_2 + f_1\rho_5) \cdot x^5 + \\
(4f_4\rho_1^3\rho_3 + 6f_4\rho_1^2\rho_2^2 + 3f_3\rho_4\rho_1^2 + 6f_3\rho_1\rho_2\rho_3 + 2f_2\rho_5\rho_1 + f_3\rho_2^3 + 2f_2\rho_4\rho_2 + f_2\rho_3^2) \cdot x^6 + \\
(4f_4\rho_4\rho_1^3 + 12f_4\rho_1^2\rho_2\rho_3 + 3f_3\rho_5\rho_1^2 + 4f_4\rho_1\rho_2^3 + 6f_3\rho_4\rho_1\rho_2 + \\
3f_3\rho_1\rho_3^2 + 3f_3\rho_2^2\rho_3 + 2f_2\rho_5\rho_2 + 2f_2\rho_4\rho_3) \cdot x^7 + \\
(4f_4\rho_5\rho_1^3 + 12f_4\rho_1^2\rho_2\rho_4 + 6f_4\rho_1^2\rho_3^2 + 12f_4\rho_1\rho_2^2\rho_3 + 6f_3\rho_5\rho_1\rho_2 + 6f_3\rho_1\rho_3\rho_4 + \\
f_4\rho_2^4 + 3f_3\rho_2^2\rho_4 + 3f_3\rho_2\rho_3^2 + 2f_2\rho_5\rho_3 + f_2\rho_4^2) \cdot x^8 + \\
(12f_4\rho_5\rho_1^2\rho_2 + 12f_4\rho_1^2\rho_3\rho_4 + 12f_4\rho_1\rho_2^2\rho_4 + 12f_4\rho_1\rho_2\rho_3^2 + 6f_3\rho_5\rho_1\rho_3 + \\
3f_3\rho_1\rho_4^2 + 4f_4\rho_2^3\rho_3 + 3f_3\rho_5\rho_2^2 + 6f_3\rho_2\rho_3\rho_4 + f_3\rho_3^3 + 2f_2\rho_5\rho_4) \cdot x^9 + \\
(12f_4\rho_1^2\rho_3\rho_5 + 6f_4\rho_1^2\rho_4^2 + 12f_4\rho_1\rho_2^2\rho_5 + 24f_4\rho_1\rho_2\rho_3\rho_4 + 4f_4\rho_1\rho_3^3 + 6f_3\rho_1\rho_4\rho_5 + \\
4f_4\rho_2^3\rho_4 + 6f_4\rho_2^2\rho_3^2 + 6f_3\rho_2\rho_3\rho_5 + 3f_3\rho_2\rho_4^2 + 3f_3\rho_3^2\rho_4 + f_2\rho_5^2) \cdot x^{10} + \\
(12f_4\rho_1^2\rho_4\rho_5 + 24f_4\rho_1\rho_2\rho_3\rho_5 + 12f_4\rho_2^2\rho_3\rho_4 + 4f_4\rho_2\rho_3^3 + 12f_4\rho_1\rho_2\rho_4^2 + \\
12f_4\rho_1\rho_3^2\rho_4 + 3f_3\rho_1\rho_5^2 + 6f_3\rho_2\rho_4\rho_5 + 3f_3\rho_3^2\rho_5 + 3f_3\rho_3\rho_4^2) \cdot x^{11} + \\
(6f_4\rho_1^2\rho_5^2 + 24f_4\rho_1\rho_2\rho_4\rho_5 + 12f_4\rho_1\rho_3^2\rho_5 + 6f_4\rho_2^2\rho_4^2 + 12f_4\rho_2\rho_3^2\rho_4 + \\
f_4\rho_3^4 + 12f_4\rho_1\rho_3\rho_4^2 + 12f_4\rho_2^2\rho_3\rho_5 + 3f_3\rho_2\rho_5^2 + 6f_3\rho_3\rho_4\rho_5 + f_3\rho_4^3) \cdot x^{12} + \\
(12f_4\rho_2^2\rho_4\rho_5 + 12f_4\rho_2\rho_3^2\rho_5 + 4f_4\rho_3^3\rho_4 + 12f_4\rho_2\rho_3\rho_4^2 + 12f_4\rho_1\rho_2\rho_5^2 + \\
24f_4\rho_1\rho_3\rho_4\rho_5 + 3f_3\rho_3\rho_5^2 + 4f_4\rho_1\rho_4^3 + 3f_3\rho_4^2\rho_5) \cdot x^{13} + \\
(6f_4\rho_2^2\rho_5^2 + 24f_4\rho_2\rho_3\rho_4\rho_5 + 6f_4\rho_3^2\rho_4^2 + 4f_4\rho_2\rho_4^3 + 4f_4\rho_3^3\rho_5 + \\
12f_4\rho_1\rho_3\rho_5^2 + 12f_4\rho_1\rho_4^2\rho_5 + 3f_3\rho_4\rho_5^2) \cdot x^{14} + \\
(12f_4\rho_3^2\rho_4\rho_5 + 4f_4\rho_3\rho_4^3 + 12f_4\rho_2\rho_3\rho_5^2 + 12f_4\rho_2\rho_4^2\rho_5 + 12f_4\rho_1\rho_4\rho_5^2 + f_3\rho_5^3) \cdot x^{15} + \\
(6f_4\rho_3^2\rho_5^2 + 12f_4\rho_3\rho_4^2\rho_5 + f_4\rho_4^4 + 12f_4\rho_2\rho_4\rho_5^2 + 4f_4\rho_1\rho_5^3) \cdot x^{16} + \\
(4f_4\rho_4^3\rho_5 + 12f_4\rho_3\rho_4\rho_5^2 + 4f_4\rho_2\rho_5^3) \cdot x^{17} + \\
(6f_4\rho_4^2\rho_5^2 + 4f_4\rho_3\rho_5^3) \cdot x^{18} + (4f_4\rho_4\rho_5^3) \cdot x^{19} + (f_4\rho_5^4) \cdot x^{20}.
\end{gathered} \tag{15}$$

For $\rho(x)$ a 4-PP, Equation (13) is equivalent to Equation (14) with $\rho_5 = 0$ in $\Theta(x)$.

We note that the polynomial of degree 20 from the left-hand side of (14) (i.e., $(f_1\rho_1 - 1) \cdot x + \Theta(x)$) can be easily found by means of a symbolic calculus software.

Because all the coefficients of PPs $f(x)$ and $\rho(x)$, except for f_1 and ρ_1, are multiples of Ψ, we have that $\Psi | \Theta(x)$. Therefore, from (14), we have that

$$(f_1\rho_1 - 1) \cdot x = 0 \pmod{\Psi}, \forall x \in \{0, 1, \ldots, 32k_L - 1\}. \tag{16}$$

From (16), we have that

$$f_1\rho_1 = 1 \pmod{\Psi} \Leftrightarrow f_1\rho_1 = \Psi \cdot k_1 + 1 \pmod{32k_L\Psi}, \text{ with } k_1 \in \{0, 1, 2, \ldots, 32k_L - 1\} \tag{17}$$

If $k_L = 1$, then $\gcd(f_1, 32\Psi) = 1$. From Theorem 57 in [9], we see that congruence (17) has only one solution in variable ρ_1. If $k_L = 3$, then $\gcd(f_1, 96\Psi) = 3$. In this case, congruence (17) has three solutions. From these three solutions, only one of them will be valid.

With (17), Equation (14) is fulfilled if and only if

$$k_1 \cdot x + \Theta(x)/\Psi = 0 \pmod{32k_L}, \forall x \in \{0, 1, \ldots, 32k_L - 1\}, \tag{18}$$

We denote $\Psi \pmod{32k_L} = k_\Psi$ and write the coefficients f_2, f_3, and f_4 as in (8) and the coefficients ρ_2, ρ_3, ρ_4, and ρ_5 as in (10) or (12). The solutions of Equation (18) in terms of $k_{5,\rho}$, $k_{4,\rho}$, $k_{3,\rho}$, $k_{2,\rho}$, $\rho_1 \pmod{32k_L}$, and k_1 can be found by means of software exhaustive searching for each set of values for k_L, k_Ψ, $k_{4,f}$, $k_{3,f}$, $k_{2,f}$, and $f_1 \pmod{32k_L}$. These solutions are given in the file available at the link in [10] for $L = 32\Psi$ and at the link in [11] for $L = 96\Psi$. As we can see from these files, the inverse PP of a 4-PP modulo a positive integer of the form (5) is a true 4-PP when $k_{4,f} \in \{1, 3\}$ and $k_{3,f} \in \{1, 3, 5, 7\}$ or when $k_{4,f} = 2$, and a true 5-PP when $k_{4,f} \in \{1, 3\}$ and $k_{3,f} \in \{0, 2, 4, 6\}$.

We note that if at least one of the coefficients f_2, f_3, and f_4 is not a multiple of Ψ, we cannot derive Equation (18). Thus, in this case, the solutions of Equation (15) in terms of $\rho_1, \rho_2, \rho_3, \rho_4$, and ρ_5 are much more complicated. □

4. Examples

In this section, we give two examples showing how we can find the inverse 4-PP or 5-PP for a 4-PP modulo a positive integer of the form (5) with $k_L = 1$ (Examples 1 and 2) and two examples for a positive integer of the form (5) with $k_L = 3$ (Examples 3 and 4).

Example 1. *Let* $\pi(x) = 187x^4 + 1122x^3 + 2431x^2 + 5975x \pmod{5984}$ *be the 4-PP. Because* $L = 5984 = 2^5 \cdot 11 \cdot 17$, *we have* $k_L = 1$, $\Psi = 11 \cdot 17 = 187$, $k_\Psi = 187 \pmod{32} = 27$, $k_{4,f} = f_4/\Psi = 1$, $k_{3,f} = f_3/(2\Psi) = 3$, $k_{2,f} = f_2/\Psi = 13$, *and* $f_1 \pmod{32} = 23$. *From the file available at the link in [10], we see that the inverse PP is a 4-PP* $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 \pmod{L}$, *with the coefficients derived from* $k_{4,\rho} = \rho_4/\Psi = 1$, $k_{3,\rho} = \rho_3/(2\Psi) = 1$, $k_{2,\rho} = \rho_2/\Psi = 5$, $\rho_1 \pmod{32} = 7$, *and* $k_1 = 0$. *Thus, we have that* $\rho_4 = \Psi = 187$, $\rho_3 = 2\Psi = 374$, *and* $\rho_2 = 5\Psi = 935$. *The coefficient* ρ_1 *results from Equation (17), with* $f_1 = 5975$, $\Psi = 187$, *and* $k_1 = 0$, *i.e.,* $5975 \cdot \rho_1 = 1 \pmod{5984}$. *This equation has only the solution modulo 5984,* $\rho_1 = 5319$. *So, the inverse 4-PP is* $\rho(x) = 187x^4 + 374x^3 + 935x^2 + 5319x \pmod{5984}$.

Example 2. *Now, let* $\pi(x) = 561x^4 + 748x^3 + 935x^2 + 3059x \pmod{5984}$ *be the 4-PP. We have again* $k_L = 1$, $\Psi = 187$, *and* $k_\Psi = 27$, *but* $k_{4,f} = f_4/\Psi = 3$, $k_{3,f} = f_3/(2\Psi) = 2$, $k_{2,f} = f_2/\Psi = 5$, *and* $f_1 \pmod{32} = 19$. *From the file available at the link in [10], we have that the inverse PP is a 5-PP* $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 + \rho_5 x^5 \pmod{L}$, *with the coefficients derived from* $k_{5,\rho} = \rho_5/\Psi = 2$, $k_{4,\rho} = \rho_4/\Psi = 3$, $k_{3,\rho} = \rho_3/\Psi = 10$, $k_{2,\rho} = \rho_2/\Psi = 5$, $\rho_1 \pmod{32} = 11$, *and* $k_1 = 16$. *Thus, we have that* $\rho_5 = 2\Psi = 374$, $\rho_4 = 3\Psi = 561$, $\rho_3 = 10\Psi = 1870$, *and* $\rho_2 = 5\Psi = 935$. *The coefficient* ρ_1 *results from Equation (17), with* $f_1 = 3059$, $\Psi = 187$, *and* $k_1 = 16$, *i.e.,* $3059 \cdot \rho_1 = 2993 \pmod{5984}$. *This equation has only* *the solution modulo 5984, $\rho_1 = 4555$. So, the inverse 5-PP is $\rho(x) = 374x^5 + 561x^4 + 1870x^3 + 935x^2 + 4555x \pmod{5984}$.*

Example 3. *Let $\pi(x) = 759x^4 + 2530x^3 + 2277x^2 + 10{,}815x \pmod{24{,}288}$ be the 4-PP. Because $L = 24{,}288 = 2^5 \cdot 3 \cdot 11 \cdot 23$, we have $k_L = 3$, $\Psi = 11 \cdot 23 = 253$, $k_\Psi = 253 \pmod{96} = 61$, $k_{4,f} = f_4/\Psi = 3$, $k_{3,f} = f_3/(2\Psi) = 5$, $k_{2,f} = f_2/\Psi = 9$, and $f_1 \pmod{96} = 63$. From the file available at the link in [11], we have that the inverse PP is a 4-PP $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 \pmod{L}$, with the coefficients derived from $k_{4,\rho} = \rho_4/\Psi = 3$, $k_{3,\rho} = \rho_3/(2\Psi) = 1$, $k_{2,\rho} = \rho_2/\Psi = 33$, $\rho_1 \pmod{96} = 47$, and $k_1 = 80$. Thus, we have that $\rho_4 = 3\Psi = 759$, $\rho_3 = 2\Psi = 506$, and $\rho_2 = 33\Psi = 8349$. The coefficient ρ_1 results from Equation (17), with $f_1 = 10{,}815$, $\Psi = 253$, and $k_1 = 80$, i.e., $10{,}815 \cdot \rho_1 = 20{,}241 \pmod{24{,}288}$. This equation has the next three solutions modulo $24{,}288$, $\rho_1 \in \{3119; 11{,}215; 19{,}311\}$. But, from the file available at the link [11], we have that $\rho_1 \pmod{96} = 47$. Thus, the only valid solution is $\rho_1 = 3119$. So, the inverse 4-PP is $\rho(x) = 759x^4 + 506x^3 + 8349x^2 + 3119x \pmod{24{,}288}$.*

Example 4. *Now, let $\pi(x) = 253x^4 + 2024x^3 + 11{,}891x^2 + 12{,}087x \pmod{24{,}288}$ be the 4-PP. We have again $k_L = 3$, $\Psi = 253$, and $k_\Psi = 61$, but $k_{4,f} = f_4/\Psi = 1$, $k_{3,f} = f_3/(2\Psi) = 4$, $k_{2,f} = f_2/\Psi = 47$, and $f_1 \pmod{96} = 87$. From the file available at the link in [11], we have that the inverse PP is a 5-PP $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 + \rho_5 x^5 \pmod{L}$, with the coefficients derived from $k_{5,\rho} = \rho_5/\Psi = 2$, $k_{4,\rho} = \rho_4/\Psi = 1$, $k_{3,\rho} = \rho_3/\Psi = 14$, $k_{2,\rho} = \rho_2/\Psi = 47$, $\rho_1 \pmod{96} = 79$, and $k_1 = 56$. Thus, we have $\rho_5 = 2\Psi = 506$, $\rho_4 = \Psi = 253$, $\rho_3 = 14\Psi = 3542$, and $\rho_2 = 47\Psi = 11{,}891$. The coefficient ρ_1 results from Equation (17), with $f_1 = 12{,}087$, $\Psi = 253$, and $k_1 = 56$, i.e., $12{,}087 \cdot \rho_1 = 14{,}169 \pmod{24{,}288}$. This equation has the next three solutions modulo $24{,}288$, $\rho_1 \in \{2095; 10{,}191; 18{,}287\}$. But, from the file available at the link [11], we have that $\rho_1 \pmod{96} = 79$. Thus, the only valid solution is $\rho_1 = 2095$. So, the inverse 5-PP is $\rho(x) = 506x^5 + 253x^4 + 3542x^3 + 11{,}891x^2 + 2095x \pmod{24{,}288}$.*

5. Remarks

We note that the inverse of a PP can be found by means of the Chinese Remainder Theorem (CRT), finding, firstly, the inverses of the PPs modulo p_i^{N,p_i}, for each factor p_i^{N,p_i} from the prime decomposition of the positive integer L. For L decomposed as in (2), we denote the following:

$$\begin{cases} \pi^{(2)}(x) = \pi(x) \pmod{2^{n_{L,2}}} \\ \pi^{(3)}(x) = \pi(x) \pmod{3^{n_{L,3}}} \\ \pi^{(p_i)}(x) = \pi(x) \pmod{p_i}, \forall i = 1, 2, \ldots, N_p \end{cases} \tag{19}$$

Then, if the inverses of the PPs in (19) are

$$\begin{cases} \rho^{(2)}(x) = \left(\pi^{(2)}(x)\right)^{-1} = \sum_{i=0}^{d_{\rho,2}} \rho_i^{(2)} \cdot x^i \pmod{2^{n_{L,2}}} \\ \rho^{(3)}(x) = \left(\pi^{(3)}(x)\right)^{-1} = \sum_{i=0}^{d_{\rho,3}} \rho_i^{(3)} \cdot x^i \pmod{3^{n_{L,3}}} \\ \rho^{(p_i)}(x) = \left(\pi^{(p_i)}(x)\right)^{-1} = \sum_{i=0}^{d_{\rho,p_i}} \rho_i^{(p_i)} \cdot x^i \pmod{p_i}, \forall i = 1, 2, \ldots, N_p \end{cases} \tag{20}$$

and the maximum degree of the inverse PPs is $d = \max\{d_{\rho,2}, d_{\rho,3}, d_{\rho,p_1}, d_{\rho,p_2}, \ldots, d_{\rho,p_{N_p}}\}$, the coefficients of the inverse PP modulo L are derived by means of the solutions of the next system:

$$\begin{cases} \rho_i = \rho_i^{(2)} \pmod{2^{n_{L,2}}} \\ \rho_i = \rho_i^{(3)} \pmod{3^{n_{L,3}}} \\ \rho_i = \rho_i^{(p_1)} \pmod{p_1} \\ \rho_i = \rho_i^{(p_2)} \pmod{p_2} \\ \ldots \\ \rho_i = \rho_i^{(p_{N_p})} \pmod{p_i} \end{cases} \tag{21}$$

for every $i = 0, 1, \ldots, d$. In (21), if $d_{\rho,p_i} < d$, then the coefficients $\rho_i^{(p_i)} = 0$, $\forall i > d_{\rho,p_i}$.

In the following, we explain how the inverse PPs of the 4-PPs can be found from Examples 1 and 4.

Example 1 (continued). *For the 4-PP* $\pi(x) = 187x^4 + 1122x^3 + 2431x^2 + 5975x \pmod{5984}$, *because* $5984 = 2^5 \cdot 11 \cdot 17$, *we have the following:*

$$\begin{cases} \pi^{(2)}(x) = \pi(x) \pmod{2^5} = 27x^4 + 2x^3 + 31x^2 + 23x \pmod{32} \\ \pi^{(11)}(x) = \pi(x) \pmod{11} = 2x \pmod{11} \\ \pi^{(17)}(x) = \pi(x) \pmod{17} = 8x \pmod{17} \end{cases} \tag{22}$$

The inverses of the PPs from (22) *are as follows:*

$$\begin{cases} \rho^{(2)}(x) = \left(\pi^{(2)}(x)\right)^{-1} = 3x^4 + 6x^3 + 15x^2 + 7x \pmod{32} \\ \rho^{(11)}(x) = \left(\pi^{(11)}(x)\right)^{-1} = 2^{-1}x \pmod{11} = 6x \pmod{11} \\ \rho^{(17)}(x) = \left(\pi^{(17)}(x)\right)^{-1} = 8^{-1}x \pmod{17} = 15x \pmod{17} \end{cases} \tag{23}$$

Then, the degree of the inverse PP modulo 5984 is $d = \max\{4, 1, 1\} = 4$, *and the coefficients of this PP* ($\rho(x)$) *result from the following systems:*

$$\begin{cases} \rho_1 = \rho_1^{(2)} \pmod{32} = 7 \pmod{32} \\ \rho_1 = \rho_1^{(11)} \pmod{11} = 6 \pmod{11} \\ \rho_1 = \rho_1^{(17)} \pmod{17} = 15 \pmod{17} \end{cases} \text{, with solution } \rho_1 = 5319 \pmod{5984} \tag{24}$$

$$\begin{cases} \rho_2 = \rho_2^{(2)} \pmod{32} = 15 \pmod{32} \\ \rho_2 = \rho_2^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_2 = \rho_2^{(17)} \pmod{17} = 0 \pmod{17} \end{cases} \text{, with solution } \rho_2 = 5423 \pmod{5984} \tag{25}$$

$$\begin{cases} \rho_3 = \rho_3^{(2)} \pmod{32} = 6 \pmod{32} \\ \rho_3 = \rho_3^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_3 = \rho_3^{(17)} \pmod{17} = 0 \pmod{17} \end{cases} \text{, with solution } \rho_3 = 3366 \pmod{5984} \tag{26}$$

and

$$\begin{cases} \rho_4 = \rho_4^{(2)} \pmod{32} = 3 \pmod{32} \\ \rho_4 = \rho_4^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_4 = \rho_4^{(17)} \pmod{17} = 0 \pmod{17} \end{cases} \text{, with solution } \rho_4 = 4675 \pmod{5984}. \tag{27}$$

Thus, the inverse PP is $\rho(x) = 4675x^4 + 3366x^3 + 5423x^2 + 5319x \pmod{5984}$. *This polynomial is different from that in Section 4, but the permutation induced by it modulo 5984 is the same. If we add to it the null polynomial* $z(x) = 1496x^4 + 2992x^3 + 1496x^2 + 0x \pmod{5984}$ *(i.e.,* $z(x) = 0$, $\forall x = 0, 1, \ldots, 5983$*), we obtain the same polynomial:* $\rho(x) + z(x) \pmod{5984} =$

$187x^4 + 374x^3 + 935x^2 + 5319x \pmod{5984}$.

Example 4 (continued). *For the 4-PP* $\pi(x) = 253x^4 + 2024x^3 + 11{,}891x^2 + 12{,}087x \pmod{24{,}288}$, *because* $24{,}288 = 2^5 \cdot 3 \cdot 11 \cdot 23$, *we have the following:*

$$\begin{cases} \pi^{(2)}(x) = \pi(x) \pmod{2^5} = 29x^4 + 8x^3 + 19x^2 + 23x \pmod{32} \\ \pi^{(3)}(x) = \pi(x) \pmod{3} = x^4 + 2x^3 + 2x^2 \pmod{3} = 2x \pmod{3} \\ \pi^{(11)}(x) = \pi(x) \pmod{11} = 9x \pmod{11} \\ \pi^{(23)}(x) = \pi(x) \pmod{23} = 12x \pmod{23} \end{cases} \tag{28}$$

The inverses of the PPs from (28) *are as follows:*

$$\begin{cases} \rho^{(2)}(x) = \left(\pi^{(2)}(x)\right)^{-1} = 2x^5 + x^4 + 6x^3 + 15x^2 + 23x \pmod{32} \\ \rho^{(3)}(x) = \left(\pi^{(3)}(x)\right)^{-1} = 2^{-1}x \pmod{3} = 2x \pmod{3} \\ \rho^{(11)}(x) = \left(\pi^{(11)}(x)\right)^{-1} = 9^{-1}x \pmod{11} = 5x \pmod{11} \\ \rho^{(23)}(x) = \left(\pi^{(23)}(x)\right)^{-1} = 12^{-1}x \pmod{23} = 2x \pmod{23} \end{cases} \tag{29}$$

Then, the degree of the inverse PP modulo 24,288 is $d = \max\{5, 1, 1, 1\} = 5$, *and the coefficients of this PP* ($\rho(x)$) *result from the following systems:*

$$\begin{cases} \rho_1 = \rho_1^{(2)} \pmod{32} = 23 \pmod{32} \\ \rho_1 = \rho_1^{(3)} \pmod{3} = 2 \pmod{3} \\ \rho_1 = \rho_1^{(11)} \pmod{11} = 5 \pmod{11} \\ \rho_1 = \rho_1^{(23)} \pmod{23} = 2 \pmod{23} \end{cases} \text{, with solution } \rho_1 = 12{,}215 \pmod{24{,}288} \tag{30}$$

$$\begin{cases} \rho_2 = \rho_2^{(2)} \pmod{32} = 15 \pmod{32} \\ \rho_2 = \rho_2^{(3)} \pmod{3} = 0 \pmod{3} \\ \rho_2 = \rho_2^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_2 = \rho_2^{(23)} \pmod{23} = 0 \pmod{23} \end{cases} \text{, with solution } \rho_2 = 6831 \pmod{24{,}288} \tag{31}$$

$$\begin{cases} \rho_3 = \rho_3^{(2)} \pmod{32} = 6 \pmod{32} \\ \rho_3 = \rho_3^{(3)} \pmod{3} = 0 \pmod{3} \\ \rho_3 = \rho_3^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_3 = \rho_3^{(23)} \pmod{23} = 0 \pmod{23} \end{cases} \text{, with solution } \rho_3 = 7590 \pmod{24{,}288} \tag{32}$$

$$\begin{cases} \rho_4 = \rho_4^{(2)} \pmod{32} = 1 \pmod{32} \\ \rho_4 = \rho_4^{(3)} \pmod{3} = 0 \pmod{3} \\ \rho_4 = \rho_4^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_4 = \rho_4^{(23)} \pmod{23} = 0 \pmod{23} \end{cases} \text{, with solution } \rho_4 = 5313 \pmod{24{,}288} \tag{33}$$

and

$$\begin{cases} \rho_5 = \rho_5^{(2)} \pmod{32} = 2 \pmod{32} \\ \rho_5 = \rho_5^{(3)} \pmod{3} = 0 \pmod{3} \\ \rho_5 = \rho_5^{(11)} \pmod{11} = 0 \pmod{11} \\ \rho_5 = \rho_5^{(23)} \pmod{23} = 0 \pmod{23} \end{cases} \text{, with solution } \rho_4 = 10{,}626 \pmod{24{,}288}. \tag{34}$$

Thus, the inverse PP is $\rho(x) = 10{,}626x^5 + 5313x^4 + 7590x^3 + 6831x^2 + 12{,}215x \pmod{24{,}288}$. *This polynomial is different from that in Section 4, but the permutation induced by it modulo 24,288 is the same. If we add to it the null polynomial* $z(x) = 14{,}168x^5 + 19{,}228x^4 + 20{,}240x^3 + 5060x^2 + 14{,}168x \pmod{24{,}288}$, *we obtain the same polynomial:* $\rho(x) + z(x) \pmod{24{,}288} =$

$$506x^5 + 253x^4 + 3542x^3 + 11{,}891x^2 + 2095x \pmod{24{,}288}.$$

In [12], Table I shows the inverses of the normalized PPs of degree ≤ 5. For the positive integers of the form in (2), the normalized PP modulo p_i, with $p_i \geq 3$, is $x \pmod{p_i}$ with the simple inverse $x \pmod{p_i}$. Additionally, the PP $a \cdot x \pmod{p_i}$, $a \neq 0$, has the inverse PP $a^{-1} \cdot x \pmod{p_i}$. However, the normalized PP modulo 32 is $x^4 + cx^3 + bx^2 + ax$, where $a \pmod 2 = b \pmod 2 = 1$ and $c \pmod 2 = 0$, and it is not given in that table. Further, finding the inverse PPs by means of normalized PPs and the CRT is not appropriate for deriving the upper bounds of the minimum distance of the turbo codes using PP interleavers, which is the main goal of the results obtained in this paper.

Author Contributions: Conceptualization, L.T. and D.T.; methodology, L.T.; software, L.T.; validation, L.T., D.T. and A.-M.R.; formal analysis, L.T.; investigation, L.T.; resources, L.T.; data curation, L.T.; writing—original draft preparation, L.T.; writing—review and editing, L.T.; visualization, L.T., D.T., and A.-M.R.; supervision, D.T.; project administration, L.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Publicly available datasets were analyzed in this study. This data can be found here: http://telecom.etti.tuiasi.ro/tti/papers/Text_files/solutii_kL_kp_k1_f1_r1_inv_4PP_or_5PP_for_4PP_L_32p.txt and http://telecom.etti.tuiasi.ro/tti/papers/Text_files/solutii_kL_kp_k1_f1_r1_inv_4PP_or_5PP_for_4PP_L_96p.txt.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

PP	Permutation polynomial
4-PP	Fourth-degree permutation polynomial
5-PP	Fifth-degree permutation polynomial
d-PP	Permutation polynomial of degree d
CRT	Chinese Remainder Theorem

References

1. Dickson, L.E. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. Math.* **1896–1897**, *11*, 65–120. [CrossRef]
2. Cohen, S.D. *Permutation Group Theory and Permutation Polynomials. Algebras and Combinatorics*; Springer: Singapore, 1999; pp. 133–146.
3. Lidl, R.; Niederriter, H. *Finite Fields*; Cambridge University Press: Cambridge, UK, 1997.
4. Sun, J.; Takeshita, O.Y.; Fitz M.P. Permutation polynomials based deterministic interleavers for turbo codes. In Proceedings of the IEEE International Symposium on Information Theory, Yokohama, Japan , 29 June–4 July 2003; p. 319. [CrossRef]
5. Sun, J.; Takeshita, O.Y. Interleavers for turbo codes using permutation polynomials over integer ring. *IEEE Trans. Inform. Theory* **2005**, *51*, 101–119. [CrossRef]
6. Rosnes, E. On the minimum distance of turbo codes with quadratic permutation polynomial interleavers. *IEEE Trans. Inform. Theory* **2012**, *58*, 4781–4795. [CrossRef]
7. Trifina, L.; Tarniceriu, D. A coefficient test for fourth degree permutation polynomials over integer rings. *AEU Int. J. Electron. Commun.* **2016**, *70*, 1565–1568. [CrossRef]
8. Trifina, L.; Tarniceriu, D. The number of different true permutation polynomial based interleavers under Zhao and Fan sufficient conditions. *Telecommun. Syst.* **2016**, *63*, 593–623. [CrossRef]
9. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*, 4th ed.; Oxford University Press: Oxford, UK, 1975.
10. A Text File with the Variables that Give the Inverse 4-PP or the Inverse 5-PP for a 4-PP Modulo 32Ψ, with Ψ a Product of Prime Numbers Greater than Three. Available Online: http://telecom.etti.tuiasi.ro/tti/papers/Text_files/solutii_kL_kp_k1_f1_r1_inv_4PP_or_5PP_for_4PP_L_32p.txt (accessed on 30 December 2023).

11. A Text File with the Variables That Give the Inverse 4-PP or the Inverse 5-PP for a 4-PP Modulo 96Ψ, with Ψ a Product of Prime Numbers Greater than Three. Available Online: http://telecom.etti.tuiasi.ro/tti/papers/Text_files/solutii_kL_kp_k1_f1_r1_inv_4PP_or_5PP_for_4PP_L_96p.txt (accessed on 30 December 2023).
12. Zheng, Y. ;Wang, Q. ;Wei, W. On inverses of permutation polynomials of small degree over finite fields. *IEEE Trans. Inform. Theory* **2020**, *66*, 914–922. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.