entropy

MDPI

Article

Lengths for Which Fourth Degree PP Interleavers Lead to Weaker Performances Compared to Quadratic and Cubic PP Interleavers

Lucian Trifina [1,*], Daniela Tarniceriu [1], Jonghoon Ryu [2] and Ana-Mirela Rotopanescu [1]

[1] 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.)

[2] Samsung Electronics, Inc., Suwon 16677, Korea; jonghoon.ryu@samsung.com

* Correspondence: luciant@etti.tuiasi.ro

Received: 25 November 2019; Accepted: 6 January 2020; Published: 8 January 2020

Abstract: In this paper, we obtain upper bounds on the minimum distance for turbo codes using fourth degree permutation polynomial (4-PP) interleavers of a specific interleaver length and classical turbo codes of nominal 1/3 coding rate, with two recursive systematic convolutional component codes with generator matrix $G = [1, 15/13]$. The interleaver lengths are of the form 16Ψ or 48Ψ, where Ψ is a product of different prime numbers greater than three. Some coefficient restrictions are applied when for a prime $p_i \mid \Psi$, condition $3 \nmid (p_i - 1)$ is fulfilled. Two upper bounds are obtained for different classes of 4-PP coefficients. For a 4-PP $f_4x^4 + f_3x^3 + f_2x^2 + f_1x \pmod{16k_L\Psi}$, $k_L \in \{1, 3\}$, the upper bound of 28 is obtained when the coefficient f_3 of the equivalent 4-permutation polynomials (PPs) fulfills $f_3 \in \{0, 4\Psi\}$ or when $f_3 \in \{2\Psi, 6\Psi\}$ and $f_2 \in \{(4k_L - 1) \cdot \Psi, (8k_L - 1) \cdot \Psi\}$, $k_L \in \{1, 3\}$, for any values of the other coefficients. The upper bound of 36 is obtained when the coefficient f_3 of the equivalent 4-PPs fulfills $f_3 \in \{2\Psi, 6\Psi\}$ and $f_2 \in \{(2k_L - 1) \cdot \Psi, (6k_L - 1) \cdot \Psi\}$, $k_L \in \{1, 3\}$, for any values of the other coefficients. Thus, the task of finding out good 4-PP interleavers of the previous mentioned lengths is highly facilitated by this result because of the small range required for coefficients f_4, f_3 and f_2. It was also proven, by means of nonlinearity degree, that for the considered inteleaver lengths, cubic PPs and quadratic PPs with optimum minimum distances lead to better error rate performances compared to 4-PPs with optimum minimum distances.

Keywords: PP interleaver; 4-PP; minimum distance; upper bound; turbo codes

1. Introduction

Error correcting codes with very good performances are an essential component for modern digital communications systems [1,2]. There are three classes of capacity approaching codes—turbo codes [3], low density parity check codes [4], and polar codes [5]. As a class of capacity approaching error correcting codes, turbo codes have gained much interest since their invention. One of the important research directions is increasing their minimum distances by different approaches. For example, recent works that deal with this topic are [6–9]. In [6], some upper bounds on the minimum distance for 3-dimensional turbo codes (conventional turbo codes with an additional patch) with quadratic permutation polynomial (QPP) interleavers were derived. Some example of QPPs found by random search that lead to significantly improved minimum distances are given. In [7], 4-dimensional (4-D) turbo codes are proposed and upper bounds on bit error rate (BER) performances are derived. These upper bounds imply weight enumerating functions and are derived by a simplified, augmented state-diagram-based method. This method is used to select different parameters of 4-D turbo codes so that they lead to lower BER values or higher minimum distances. In [8], a moment based augmented

state diagram method was proposed to derive tighter upper bounds on BER performance for 4-D turbo codes. It was used to design 4-D turbo codes in order to achieve improved BER performances. In [9], a modified interleaver for a new structure of 4-D turbo codes, based on superposition modulation and grouped power allocation, has been proposed to improve the minimum distance. An appropriate design of interleavers for turbo codes considers the approaches that can lead to higher minimum distances. In this respect, knowing the upper bounds on the minimum distances for different classes of interleavers is important from the perspective of the measurements of their performances or limitations.

Permutation polynomial (PP) interleavers for turbo codes were introduced by Sun and Takeshita in 2005 [10]. They are very attractive because of their fully algebraic description, low memory, and high performance if they are appropriately chosen. Other very high-performing interleavers that are not fully algebraic described, are dithered relative prime (DRP) interleavers [11] and almost regular permutation interleavers [12]. Many results have been obtained regarding QPP interleavers. They have been chosen as interleavers for turbo codes in the long term evolution (LTE) standard [13]. The most notable results regarding QPP interleavers are those from [14,15]. In the last years, analysis and design of PP interleavers of degree greater than two have gained interest. For example, good interleavers based on PPs of degree greater than two have been obtained in [16–18].

In [15], upper bounds of the minimum distance for turbo codes with QPP interleavers and different interleaver lengths were obtained. Some upper bounds for PP interleavers of any degree were obtained in [19]. Recently, some results regarding upper bounds of the minimum distance for turbo codes with cubic permutation polynomial (CPP) interleavers have been acquired [20,21]. In this paper, for the first time, upper bounds of the minimum distance for turbo codes with fourth degree permutation polynomial (4-PP) interleavers of a specific type of interleaver length and for classical turbo codes of nominal $1/3$ coding rate, with two recursive systematic convolutional component codes with generator matrix $G = [1, 15/13]$, were obtained. Specifically, for interleaver lengths of the form 16Ψ or 48Ψ, with Ψ, a product of prime numbers greater than three, the minimum distance is upper bounded by the value of 36 or 28, depending on the 4-PP coefficients. Some coefficient restrictions are applied when for a prime $p_i \mid \Psi$, condition $3 \nmid (p_i - 1)$ is fulfilled. If Ψ is a product of prime numbers $p_i > 7$ so that $3 \mid (p_i - 1)$, the result in the paper is fully general.

The paper is structured as follows. In Section 2, some preliminary results about 4-PPs are given. The main results are worked through in Section 3. Some remarks and examples are given in Section 4, and Section 5 concludes the paper.

2. Preliminaries

2.1. Notation

In the paper we use the following notation:

- $(\text{mod } L)$, with L a positive integer, denotes modulo L operation;
- $a \mid b$, with a and b positive integers, denotes a dividing b;
- $a \nmid b$, with a and b positive integers, denotes that a does not divide; b
- $\gcd(a, b)$, with a and b positive integers, denotes the greatest common divisor of a and b;
- $\log_{10}(\cdot)$ denotes base 10 logarithm;
- e^x is the natural exponential function of variable x.

2.2. Results Regarding 4-PPs

A 4-PP modulo L is a fourth degree polynomial

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

so that for $x \in \{0, 1, \ldots, L-1\}$, values $\pi(x) \ (\text{mod } L)$ perform a permutation of the set $\{0, 1, \cdots, L-1\}$.

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

Two 4-PPs with different coefficients are different if they lead to different permutations.

Conditions on coefficients f_1, f_2, f_3, and f_4 so that the fourth degree polynomial in (1) is a 4-PP modulo L have been obtained in [22]. Because we are interested in interleaver lengths of the form $16 \cdot \prod_{i=1}^{N_p} p_i$ or $48 \cdot \prod_{i=1}^{N_p} p_i$, with N_p a positive integer, in Table 1 we give the coefficient conditions only for the primes 2, 3, and p_i, $i = 1, 2, \ldots, N_p$, when the interleaver length is of the form

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

Table 1. Conditions for coefficients f_1, f_2, f_3, and f_4 so that $\pi(x)$ in (1) is a fourth degree permutation polynomial (4-PP) modulo L of the form (2) (p_i is a prime number so that $p_i \mid L$).

(1)	$p_i = 2$	$n_{L,2} > 1$	$f_1 \neq 0, (f_2 + f_4) = 0, f_3 = 0 \pmod 2$
(2)	$p_i = 3$	$n_{L,3} = 1$	$(f_1 + f_3) \neq 0, (f_2 + f_4) = 0 \pmod 3$
(3)	$3 \mid (p_i - 1)$ $(p_i > 7)$	$n_{L,p_i} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0, f_4 = 0 \pmod{p_i}$
(4)	$3 \nmid (p_i - 1)$	$n_{L,p_i} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0, f_4 = 0 \pmod{p_i}$ or $f_2^2 = 3 f_1 f_3 \pmod{p_i}, f_3 \neq 0, f_4 = 0 \pmod{p_i}$

A 4-PP modulo L

$$\rho(x) = (\rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4) \pmod L, \tag{3}$$

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

In this section, we consider the interleaver lengths of the form

$$L = 16 \cdot \prod_{i=1}^{N_p} p_i = 2^4 \cdot \prod_{i=1}^{N_p} p_i \text{ or } L = 48 \cdot \prod_{i=1}^{N_p} p_i = 2^4 \cdot 3 \cdot \prod_{i=1}^{N_p} p_i, \tag{5}$$

with p_i different prime numbers so that $p_i > 3, \forall i = 1, 2, \ldots, N_p$, and $p_1 < p_2 < \cdots < p_{N_p}$.

For p_i a prime so that $3 \nmid (p_i - 1)$, $i \in \{1, 2, \ldots, N_p\}$, we will consider only the 4-PPs with coefficients fulfilling conditions

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

In the following, we denote

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

The reason for which we focus on the interleaver lengths of the form given in (5) is as follows. In [17], 4-PPs of several lengths that lead to the best minimum distance of 36 were reported. We wanted to see if this minimum distance is a general upper bound for a general form of interleaver lengths. From the lengths in [17] for which the best minimum distance of 4-PPs is 36, we restrict ourselves to those of the form given in (5) and also we restrict ourselves to the coefficients fulfilling conditions (6) when $3 \nmid (p_i - 1)$ because, in this case, the possible coefficients of a true 4-PP are limited to a few values (see Lemma 1). This simplifies finding the coefficients of the inverse 4-PPs, and thus, the proofs for

upper bounds on minimum distance for 4-PPs of the focal interleaver lengths. We note that increasing the power of primes in the product Ψ leads to more values of the possible coefficients of 4-PPs, and thus, finding the inverse 4-PPs is more complicated.

3.1. Methodology

The research methodology is similar to that from [20,21] and it is described in this subsection. To find upper bounds on the minimum distance for turbo codes that have 4-PP interleavers of lengths of the form given in (5), the research methodology assumes the following steps:

(1) For the interleaver lengths of the form given in (5), we found all possible values for the coefficients of true different 4-PPs. Thus, every 4-PP will have the coefficients equivalent to these found values.
(2) We proved that for the interleaver lengths in question, every true 4-PP has an inversely true 4-PP, extending the result from [23].
(3) For some 4-PPs with particular minimum distances, we found the interleaver patterns that lead to these minimum distances. There are several methods to find minimum distance of turbo codes with particular interleavers. The method from [24] or its improved version from [25] allow the determination of the true minimum distance ($d_{\min}$), but their complexity increases rapidly when increasing $d_{\min}$. Methods based on impulses of high amplitude inserted in the all-zero codeword and then decoding this perturbed codeword to give a decoded codeword of low weigth, are faster for high values of $d_{\min}$ and useful for finding interleaver patterns. Double impulse method (DIM) and triple impulse method (TIM) [26] are more reliable among the impulse based methods. An alternative method of TIM is the full range double impulse method from [27] (denoted DIMK in [28]), wherein the reliability of DIM is improved by a full range for the second impulse, instead of a limited range search. The complexity of impulse based methods can be reduced for structured interleavers (such as 4-PP ones) [29]. We have made use of DIMK method for finding the interleaver patterns from Theorems 1 and 2.
(4) Finally, we proved that these critical interleaver patterns always appear for 4-PPs of the interleaver lengths in question and classes of their coefficients.

3.2. Coefficients of 4-PPs for the Interleaver Lengths of the Form 16Ψ *or* 48Ψ

In [23], we derived a pure mathematical result. For interleaver lengths of the form 16Ψ, in Lemma 3.1 from [23], the possible values of the coefficients of a true 4-PP were obtained. Lemma 3.2 provides an equation to determine the coefficients of an inverse true 4-PP without giving all its possible solutions. The next two lemmas are extensions of Lemmas 3.1 and 3.2 from [23]. Lemma 1 gives the coefficients of a true 4-PP and Lemma 2 gives the coefficients of an inverse true 4-PP of a true 4-PP, fulfilling conditions (6) when $3 \nmid (p_i - 1)$, the modulo of an integer of the form given in (5). These two lemmas are necessary to derive the upper bounds on the minimum distance from Section 3.3. We note that because of coefficient conditions 2) from Table 1, the extension of the results from [23] to the interleaver lengths of the form 48Ψ is not straightforward. Because $3 \nmid \Psi$, we can have any of the following combinations of f_4 and f_2 coefficients' conditions: (1) $f_4 = 1 \pmod 3$, $f_2 = 2 \pmod 3$; (2) $f_4 = 2 \pmod 3$, $f_2 = 1 \pmod 3$, with any of the following combinations of f_3 and f_1 coefficients conditions: (1) $f_3 = 0 \pmod 3$ and $f_1 \neq 0 \pmod 3$; (2) $f_3 = 1 \pmod 3$, $f_1 \neq 2 \pmod 3$; (3) $f_3 = 2 \pmod 3$, $f_1 \neq 1 \pmod 3$. Therefore, we will have more different cases to determine the coefficients of an inverse 4-PP, as Tables 5–8 show.

Lemma 1. *Let the interleaver length be of the form given in* (5)*. Then all true different 4-PPs fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, have possible values for coefficients* f_4*,* f_3*, and* f_2 *equivalent to those given in Table 2 from the second, third, and fourth columns, respectively. Coefficient* f_1 *has to 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).

L	f_4	f_3	f_2
16Ψ	Ψ	0 or 2Ψ or 4Ψ or 6Ψ	Ψ or 3Ψ or 5Ψ or 7Ψ
48Ψ	Ψ	0 or 2Ψ or 4Ψ or 6Ψ	5Ψ or 11Ψ or 17Ψ or 23Ψ

Proof. For the interleaver length of the form $L = 16\Psi$, a true 4-PP is equivalent to a 4-PP for which $f_2 < L/2 = 8\Psi$, $f_3 < L/2 = 8\Psi$, and $f_4 < L/8 = 2\Psi$. For the interleaver length of the form $L = 48\Psi$, a true 4-PP is equivalent to a 4-PP for which $f_2 < L/2 = 24\Psi$, $f_3 < L/6 = 8\Psi$, and $f_4 < L/24 = 2\Psi$. Taking into account the coefficient conditions for a 4-PP given in Table 1 and that Ψ is odd, coefficients f_2, f_3, and f_4 from Table 2 follows.

We note that when $L = 16\Psi$ or $L = 48\Psi$, (from condition 1 in Table 1) f_1 becomes odd. □

Lemma 2. *Let the interleaver length be of the form $L = 16 \cdot k_L \cdot \Psi$, with $k_L \in \{1, 3\}$ and Ψ given 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 $3 \nmid (p_i - 1)$, has an inverse true 4-PP $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 + \rho_4 x^4 \pmod L$, with*

$$\rho_4 = f_4, \tag{8}$$

$$\rho_3 = k_{3,\rho} \cdot 2\Psi, \tag{9}$$

$$\rho_2 = (2k_{2,\rho} \cdot k_L - 1) \cdot \Psi. \tag{10}$$

ρ_1 is the unique modulo L solution of the congruence $f_1\rho_1 = \Psi \cdot k + 1 \pmod L$. k, $k_{3,\rho}$, and $k_{2,\rho}$ are given in Tables 3–8, according to the values of $k_{3,f} = f_3/(2\Psi)$, $k_{2,f} = (f_2/\Psi + 1)/(2k_L)$, and $f_1 \pmod{16k_L}$.

Proof. $\rho(x)$ is an inverse 4-PP of $\pi(x)$ if

$$\pi(\rho(x)) = x \pmod L, \forall x \in \{0, 1, \ldots, L-1\}. \tag{11}$$

Taking into account Lemma 1, after some algebraic manipulations, Equation (11) is equivalent to

$$\begin{aligned}
&(f_1\rho_1 - 1) \cdot x + (f_1\rho_2 + f_2\rho_1^2) \cdot x^2 + (f_1\rho_3 + 2f_2\rho_2\rho_1 + f_3\rho_1^3) \cdot x^3 + \\
&+(f_4\rho_1^4 + 3f_3\rho_1^2\rho_2 + 2f_2\rho_3\rho_1 + f_2\rho_2^2 + f_1\rho_4) \cdot x^4 + \\
&+(4f_4\rho_1^3\rho_2 + 3f_3\rho_1^2\rho_3 + 3f_3\rho_1\rho_2^2 + 2f_2\rho_4\rho_1 + 2f_2\rho_3\rho_2) \cdot x^5 + \\
&+(4f_4\rho_1^3\rho_3 + 6f_4\rho_1^2\rho_2^2 + 3f_3\rho_4\rho_1^2 + 6f_3\rho_1\rho_2\rho_3 + f_3\rho_2^3 + 2f_2\rho_4\rho_2 + f_2\rho_3^2) \cdot x^6 + \\
&+(4f_4\rho_4\rho_1^3 + 12f_4\rho_1^2\rho_2\rho_3 + 4f_4\rho_1\rho_2^3 + 6f_3\rho_4\rho_1\rho_2 + 3f_3\rho_1\rho_3^2 + 3f_3\rho_2^2\rho_3 + 2f_2\rho_4\rho_3) \cdot x^7 + \\
&+(12f_4\rho_1^2\rho_2\rho_4 + 6f_4\rho_1^2\rho_3^2 + 12f_4\rho_1\rho_2^2\rho_3 + 6f_3\rho_1\rho_3\rho_4 + f_4\rho_2^4 + 3f_3\rho_2^2\rho_4 + 3f_3\rho_2\rho_3^2 + f_2\rho_4^2) \cdot x^8 + \\
&+(12f_4\rho_1^2\rho_3\rho_4 + 12f_4\rho_1\rho_2^2\rho_4 + 12f_4\rho_1\rho_2\rho_3^2 + 3f_3\rho_1\rho_4^2 + 4f_4\rho_2^3\rho_3 + 6f_3\rho_2\rho_3\rho_4 + f_3\rho_3^3) \cdot x^9 + \\
&+(6f_4\rho_1^2\rho_4^2 + 24f_4\rho_1\rho_2\rho_3\rho_4 + 4f_4\rho_1\rho_3^3 + 4f_4\rho_2^3\rho_4 + 6f_4\rho_2^2\rho_3^2 + 3f_3\rho_2\rho_4^2 + 3f_3\rho_3^2\rho_4) \cdot x^{10} + \\
&+(12f_4\rho_2^2\rho_3\rho_4 + 4f_4\rho_2\rho_3^3 + 12f_4\rho_1\rho_2\rho_4^2 + 12f_4\rho_1\rho_3^2\rho_4 + 3f_3\rho_3\rho_4^2) \cdot x^{11} + \\
&+(6f_4\rho_2^2\rho_4^2 + 12f_4\rho_2\rho_3^2\rho_4 + f_4\rho_3^4 + 12f_4\rho_1\rho_3\rho_4^2 + f_3\rho_4^3) \cdot x^{12} + \\
&+(4f_4\rho_3^3\rho_4 + 12f_4\rho_2\rho_3\rho_4^2 + 4f_4\rho_1\rho_4^3) \cdot x^{13} + (6f_4\rho_3^2\rho_4^2 + 4f_4\rho_2\rho_4^3) \cdot x^{14} + \\
&+(4f_4\rho_3\rho_4^3) \cdot x^{15} + (f_4\rho_4^4) \cdot x^{16} = 0 \pmod L, \forall x \in \{0, 1, \ldots, L-1\}.
\end{aligned} \tag{12}$$

Because $\pi(x)$ and $\rho(x)$ are true 4-PPs, from Lemma 1 it results that $\rho_4 = f_4 = \Psi$, $\rho_3 = k_{3,\rho} \cdot 2\Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, with $k_{3,\rho}, k_{3,f} \in \{0, 1, 2, 3\}$, $\rho_2 = (2k_{2,\rho} \cdot k_L - 1) \cdot \Psi$, and $f_2 = (2k_{2,f} \cdot k_L - 1) \cdot \Psi$,

with $k_{2,\rho}, k_{2,f} \in \{1,2,3,4\}$, $k_L \in \{1,3\}$. Because p_i is odd $\forall i \in \{1,2,\ldots,N_p\}$, Ψ from (7) is also odd. Then, we can have $\Psi = 1 \pmod 8$, $\Psi = 3 \pmod 8$, $\Psi = 5 \pmod 8$, or $\Psi = 7 \pmod 8$. Then, $2\Psi = 2 \pmod 8$ or $2\Psi = 6 \pmod 8$. Because every p_i is odd and $3 \nmid p_i$, we can have $\Psi = 1 \pmod{24}$, $\Psi = 5 \pmod{24}$, $\Psi = 7 \pmod{24}$, $\Psi = 11 \pmod{24}$, $\Psi = 13 \pmod{24}$, $\Psi = 17 \pmod{24}$, $\Psi = 19 \pmod{24}$, or $\Psi = 23 \pmod{24}$. Then, $2\Psi = 2 \pmod{24}$, $2\Psi = 10 \pmod{24}$, $2\Psi = 14 \pmod{24}$, or $2\Psi = 22 \pmod{24}$.

Table 3. Coefficients of an inverse 4-PP for a 4-PP $\pmod{16\Psi}$ (Part I) ($k_{2,f} = (k'_{2,f}+1)/2$ and $k_{2,\rho} = (k'_{2,\rho}+1)/2$). For $f_1 \pmod{16} = f_{1,8}+8$, $\rho_1 \pmod{16} = (\rho_{1,f_{1,8}}+8) \pmod{16}$.

$k_{3,f}$	$k'_{2,f}$	$f_{1,8}$	$k_{3,\rho}$	$k'_{2,\rho}$	$\rho_{1,f_{1,8}}$ for $k_{\Psi,4}=1$	k for $k_{\Psi,4}=1$	$\rho_{1,f_{1,8}}$ for $k_{\Psi,4}=3$	k for $k_{\Psi,4}=3$
0	1	1	0	1	13	12	13	4
		3	2	5	3	8	11	0
		5	0	1	9	12	9	4
		7	2	5	15	8	7	0
	3	1	2	3	13	12	5	12
		3	0	3	11	0	11	0
		5	2	3	1	4	9	4
		7	0	3	15	8	15	8
	5	1	0	5	13	12	13	4
		3	2	1	3	8	11	0
		5	0	5	9	12	9	4
		7	2	1	15	8	7	0
	7	1	2	7	13	12	5	12
		3	0	7	3	8	3	8
		5	2	7	1	4	9	4
		7	0	7	7	0	7	0
1	1	1	1	5	5	4	13	4
		3	3	1	3	8	3	8
		5	1	5	1	4	9	4
		7	3	1	15	8	15	8
	3	1	3	3	5	4	13	4
		3	1	3	3	8	3	8
		5	3	3	9	12	1	12
		7	1	3	7	0	7	0
	5	1	1	1	5	4	13	4
		3	3	5	3	8	3	8
		5	1	1	1	4	9	4
		7	3	5	15	8	15	8
	7	1	3	7	13	12	5	12
		3	1	7	3	8	3	8
		5	3	7	1	4	9	4
		7	1	7	7	0	7	0

Table 4. Coefficients of an inverse 4-PP for a 4-PP $\pmod{16\Psi}$ (Part II) ($k_{2,f} = (k'_{2,f}+1)/2$ and $k_{2,\rho} = (k'_{2,\rho}+1)/2$). For $f_1 \pmod{16} = f_{1,8}+8$, $\rho_1 \pmod{16} = (\rho_{1,f_{1,8}}+8) \pmod{16}$.

$k_{3,f}$	$k'_{2,f}$	$f_{1,8}$	$k_{3,\rho}$	$k'_{2,\rho}$	$\rho_{1,f_{1,8}}$ for $k_{\Psi,4}=1$	k for $k_{\Psi,4}=1$	$\rho_{1,f_{1,8}}$ for $k_{\Psi,4}=3$	k for $k_{\Psi,4}=3$
2	1	1	2	1	5	4	5	12
		3	0	5	3	8	11	0
		5	2	1	1	4	1	12
		7	0	5	15	8	7	0
	3	1	0	3	5	4	13	4
		3	2	3	11	0	11	0
		5	0	3	9	12	1	12
		7	2	3	15	8	15	8
	5	1	2	5	5	4	5	12
		3	0	1	3	8	11	0
		5	2	5	1	4	1	12
		7	0	1	15	8	7	0
	7	1	0	7	5	4	13	4
		3	2	7	3	8	3	8
		5	0	7	9	12	1	12
		7	2	7	7	0	7	0
3	1	1	3	5	13	12	5	12
		3	1	1	3	8	3	8
		5	3	5	9	12	1	12
		7	1	1	15	8	15	8
	3	1	1	3	13	12	5	12
		3	3	3	3	8	3	8
		5	1	3	1	4	9	4
		7	3	3	7	0	7	0
	5	1	3	1	13	12	5	12
		3	1	5	3	8	3	8
		5	3	1	9	12	1	12
		7	1	5	15	8	15	8
	7	1	1	7	5	4	13	4
		3	3	7	3	8	3	8
		5	1	7	9	12	1	12
		7	3	7	7	0	7	0

Table 5. Coefficients of an inverse 4-PP for a 4-PP $\pmod{48\Psi}$ (Part I). For $f_1 \pmod{48} = f_{1,24} + 24$, $\rho_1 \pmod{48} = (\rho_{1,f_{1,24}} + 24) \pmod{48}$.

$k_{3,f}$	$k_{2,f}$	$f_{1,24}$	$k_{3,\rho}$	$k_{2,\rho}$	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 1$ ($\rho_{1,1}$)	k for $k_{\Psi,12} = 1$ (k_1)	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 7$	k for $k_{\Psi,12} = 7$
0	1	1 / 13	0	1	13 / 1	12 / 12	$\rho_{1,1}$	$(k_1 + 24)$
		5 / 17	0	1	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	2	3	15 / 3	8 / 8	$(\rho_{1,1} + 24)$	
		11 / 23	2	3	43 / 31	40 / 40	$\pmod{48}$	
	2	1 / 13	2	2	45 / 9	44 / 20	$(\rho_{1,1} + 24)$	k_1
		5 / 17	2	2	1 / 13	4 / 28	$\pmod{48}$	$\pmod{48}$
		7 / 19	0	2	31 / 43	24 / 0	$\rho_{1,1}$	
		11 / 23	0	2	35 / 47	0 / 24	$\pmod{48}$	
	3	1 / 13	0	3	13 / 1	12 / 12	$\rho_{1,1}$	$(k_1 + 24)$
		5 / 17	0	3	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	2	1	15 / 3	8 / 8	$(\rho_{1,1} + 24)$	
		11 / 23	2	1	43 / 31	40 / 40	$\pmod{48}$	
	4	1 / 13	2	4	45 / 9	44 / 20	$(\rho_{1,1} + 24)$	k_1
		5 / 17	2	4	1 / 13	4 / 28	$\pmod{48}$	$\pmod{48}$
		7 / 19	0	4	7 / 19	0 / 24	$\rho_{1,1}$	
		11 / 23	0	4	11 / 23	24 / 0	$\pmod{48}$	
1	1	3 / 15	3	1	35 / 23	8 / 8	$\rho_{1,1}$	k_1
		5 / 17	1	3	17 / 5	36 / 36	$(\rho_{1,1} + 24)$	$\pmod{48}$
		9 / 21	1	3	45 / 33	20 / 20	$\pmod{48}$	
		11 / 23	3	1	43 / 31	40 / 40	$\rho_{1,1}$	
	2	3 / 15	1	2	3 / 15	8 / 32	$\rho_{1,1}$	k_1
		5 / 17	3	2	25 / 37	28 / 4	$(\rho_{1,1} + 24)$	$\pmod{48}$
		9 / 21	3	2	29 / 41	20 / 44	$\pmod{48}$	
		11 / 23	1	2	11 / 23	24 / 0	$\rho_{1,1}$	
	3	3 / 15	3	3	35 / 23	8 / 8	$\rho_{1,1}$	k_1
		5 / 17	1	1	17 / 5	36 / 36	$(\rho_{1,1} + 24)$	$\pmod{48}$
		9 / 21	1	1	45 / 33	20 / 20	$\pmod{48}$	
		11 / 23	3	3	43 / 31	40 / 40	$\rho_{1,1}$	
	4	3 / 15	1	4	3 / 15	8 / 32	$\rho_{1,1}$	k_1
		5 / 17	3	4	1 / 13	4 / 28	$(\rho_{1,1} + 24)$	$\pmod{48}$
		9 / 21	3	4	5 / 17	44 / 20	$\pmod{48}$	
		11 / 23	1	4	11 / 23	24 / 0	$\rho_{1,1}$	

Table 6. Coefficients of an inverse 4-PP for a 4-PP $\pmod{48\Psi}$ (Part II). For $f_1 \pmod{48} = f_{1,24} + 24$, $\rho_1 \pmod{48} = (\rho_{1,f_{1,24}} + 24) \pmod{48}$.

$k_{3,f}$	$k_{2,f}$	$f_{1,24}$	$k_{3,\rho}$	$k_{2,\rho}$	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 1$ ($\rho_{1,1}$)	k for $k_{\Psi,12} = 1$ (k_1)	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 7$	k for $k_{\Psi,12} = 7$
2	1	1 / 13	2	1	37 / 25	36 / 36	$\rho_{1,1}$	$(k_1 + 24)$
		3 / 15	0	3	19 / 7	8 / 8	$(\rho_{1,1} + 24)$	$\pmod{48}$
		7 / 19	0	3	47 / 35	40 / 40	$\pmod{48}$	
		9 / 21	2	1	45 / 33	20 / 20	$\rho_{1,1}$	
	2	1 / 13	0	2	5 / 17	4 / 28	$\rho_{1,1} + 24$	k_1
		3 / 15	2	2	27 / 39	32 / 8	$\rho_{1,1}$	$\pmod{48}$
		7 / 19	2	2	31 / 43	24 / 0	$\pmod{48}$	
		9 / 21	0	2	13 / 25	20 / 44	$\rho_{1,1} + 24$	
	3	1 / 13	2	3	37 / 25	36 / 36	$\rho_{1,1}$	$(k_1 + 24)$
		3 / 15	0	1	19 / 7	8 / 8	$(\rho_{1,1} + 24)$	$\pmod{48}$
		7 / 19	0	1	47 / 35	40 / 40	$\pmod{48}$	
		9 / 21	2	3	45 / 33	20 / 20	$\rho_{1,1}$	
	4	1 / 13	0	4	5 / 17	4 / 28	$\rho_{1,1} + 24$	k_1
		3 / 15	2	4	3 / 15	8 / 32	$\rho_{1,1}$	$\pmod{48}$
		7 / 19	2	4	7 / 19	0 / 24	$\pmod{48}$	
		9 / 21	0	4	13 / 25	20 / 44	$\rho_{1,1} + 24$	
3	1	1 / 13	3	3	13 / 1	12 / 12	$(\rho_{1,1} + 24)$	k_1
		5 / 17	3	3	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	1	1	47 / 35	40 / 40	$\rho_{1,1}$	
		11 / 23	1	1	27 / 15	8 / 8	$\pmod{48}$	
	2	1 / 13	1	2	29 / 41	28 / 4	$(\rho_{1,1} + 24)$	k_1
		5 / 17	1	2	33 / 45	20 / 44	$\pmod{48}$	$\pmod{48}$
		7 / 19	3	2	7 / 19	0 / 24	$\rho_{1,1}$	
		11 / 23	3	2	11 / 23	24 / 0	$\pmod{48}$	
	3	1 / 13	3	1	13 / 1	12 / 12	$(\rho_{1,1} + 24)$	k_1
		5 / 17	3	1	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	1	3	47 / 35	40 / 40	$\rho_{1,1}$	
		11 / 23	1	3	27 / 15	8 / 8	$\pmod{48}$	
	4	1 / 13	1	4	5 / 17	4 / 28	$(\rho_{1,1} + 24)$	k_1
		5 / 17	1	4	9 / 21	44 / 20	$\pmod{48}$	$\pmod{48}$
		7 / 19	3	4	7 / 19	0 / 24	$\rho_{1,1}$	
		11 / 23	3	4	11 / 23	24 / 0	$\pmod{48}$	

Table 7. Coefficients of an inverse 4-PP for a 4-PP $\pmod{48\Psi}$ (Part III). For $f_1 \pmod{48} = f_{1,24} + 24$, $\rho_1 \pmod{48} = (\rho_{1,f_{1,24}} + 24) \pmod{48}$.

$k_{3,f}$	$k_{2,f}$	$f_{1,24}$	$k_{3,\rho}$	$k_{2,\rho}$	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 5$ ($\rho_{1,5}$)	k for $k_{\Psi,12} = 5$ (k_5)	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 11$	k for $k_{\Psi,12} = 11$
0	1	1 / 13	0	1	13 / 1	12 / 12	$\rho_{1,5}$	$(k_5 + 24)$
		5 / 17	0	1	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	2	3	47 / 35	8 / 8	$(\rho_{1,5} + 24)$	
		11 / 23	2	3	27 / 15	40 / 40	$\pmod{48}$	
	2	1 / 13	2	2	29 / 41	44 / 20	$(\rho_{1,5} + 24)$	k_5
		5 / 17	2	2	33 / 45	4 / 28	$\pmod{48}$	$\pmod{48}$
		7 / 19	0	2	31 / 43	24 / 0	$\rho_{1,5}$	
		11 / 23	0	2	35 / 47	0 / 24	$\pmod{48}$	
	3	1 / 13	0	3	13 / 1	12 / 12	$\rho_{1,5}$	$(k_5 + 24)$
		5 / 17	0	3	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	2	1	47 / 35	8 / 8	$(\rho_{1,5} + 24)$	
		11 / 23	2	1	27 / 15	40 / 40	$\pmod{48}$	
	4	1 / 13	2	4	29 / 41	44 / 20	$(\rho_{1,5} + 24)$	k_5
		5 / 17	2	4	33/ 45	4 / 28	$\pmod{48}$	$\pmod{48}$
		7 / 19	0	4	7 / 19	0 / 24	$\rho_{1,5}$	
		11 / 23	0	4	11 / 23	24 / 0	$\pmod{48}$	
1	1	1 / 13	1	3	37 / 25	36 / 36	$\rho_{1,5} + 24$	k_5
		3 / 15	3	1	19 / 7	40 / 40	$\rho_{1,5}$	$\pmod{48}$
		7 / 19	3	1	47 / 35	8 / 8	$\pmod{48}$	
		9 / 21	1	3	45 / 33	4 / 4	$\rho_{1,5} + 24$	
	2	1 / 13	3	2	5 / 17	20 / 44	$\rho_{1,5} + 24$	k_5
		3 / 15	1	2	3 / 15	40 / 16	$\rho_{1,5}$	$\pmod{48}$
		7 / 19	1	2	7 / 19	0 / 24	$\pmod{48}$	
		9 / 21	3	2	13 / 25	4 / 28	$\rho_{1,5} + 24$	
	3	1 / 13	1	1	37 / 25	36 / 36	$\rho_{1,5} + 24$	k_5
		3 / 15	3	3	19 / 7	40 / 40	$\rho_{1,5}$	$\pmod{48}$
		7 / 19	3	3	47 / 35	8 / 8	$\pmod{48}$	
		9 / 21	1	1	45 / 33	4 / 4	$\rho_{1,5} + 24$	
	4	1 / 13	3	4	29 / 41	44 / 20	$\rho_{1,5} + 24$	k_5
		3 / 15	1	4	3 / 15	40 / 16	$\rho_{1,5}$	$\pmod{48}$
		7 / 19	1	4	7 / 19	0 / 24	$\pmod{48}$	
		9 / 21	3	4	37 / 1	28 / 4	$\rho_{1,5} + 24$	

Table 8. Coefficients of an inverse 4-PP for a 4-PP $\pmod{48\Psi}$ (Part IV). For $f_1 \pmod{48} = f_{1,24} + 24$, $\rho_1 \pmod{48} = (\rho_{1,f_{1,24}} + 24) \pmod{48}$.

$k_{3,f}$	$k_{2,f}$	$f_{1,24}$	$k_{3,\rho}$	$k_{2,\rho}$	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 5$ ($\rho_{1,5}$)	k for $k_{\Psi,12} = 5$ (k_5)	$\rho_{1,f_{1,24}}$ for $k_{\Psi,12} = 11$	k for $k_{\Psi,12} = 11$
2	1	3 / 15	0	3	35 / 23	40 / 40	$\rho_{1,5} + 24$	$(k_5 + 24)$
		5 / 17	2	1	17 / 5	36 / 36	$\rho_{1,5}$	$\pmod{48}$
		9 / 21	2	1	45 / 33	4 / 4	$\pmod{48}$	
		11 / 23	0	3	43 / 31	8 / 8	$\rho_{1,5} + 24$	
	2	3 / 15	2	2	27 / 39	16 / 40	$\rho_{1,5}$	k_5
		5 / 17	0	2	25 / 37	44 / 20	$(\rho_{1,5} + 24)$	$\pmod{48}$
		9 / 21	0	2	29 / 41	4 / 28	$\pmod{48}$	
		11 / 23	2	2	35 / 47	0 / 24	$\rho_{1,5}$	
	3	3 / 15	0	1	35 / 23	40 / 40	$\rho_{1,5} + 24$	$(k_5 + 24)$
		5 / 17	2	3	17 / 5	36 / 36	$\rho_{1,5}$	$\pmod{48}$
		9 / 21	2	3	45 / 33	4 / 4	$\pmod{48}$	
		11 / 23	0	1	43 / 31	8 / 8	$\rho_{1,5} + 24$	
	4	3 / 15	2	4	3 / 15	40 / 16	$\rho_{1,5}$	k_5
		5 / 17	0	4	25 / 37	44 / 20	$(\rho_{1,5} + 24)$	$\pmod{48}$
		9 / 21	0	4	29 / 41	4 / 28	$\pmod{48}$	
		11 / 23	2	4	11 / 23	24 / 0	$\rho_{1,5}$	
3	1	1 / 13	3	3	13 / 1	12 / 12	$(\rho_{1,5} + 24)$	k_5
		5 / 17	3	3	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	1	1	15 / 3	40 / 40	$\rho_{1,5}$	
		11 / 23	1	1	43 / 31	8 / 8	$\pmod{48}$	
	2	1 / 13	1	2	45 / 9	28 / 4	$(\rho_{1,5} + 24)$	k_5
		5 / 17	1	2	1 / 13	20 / 44	$\pmod{48}$	$\pmod{48}$
		7 / 19	3	2	7 / 19	0 / 24	$\rho_{1,5}$	
		11 / 23	3	2	11 / 23	24 / 0	$\pmod{48}$	
	3	1 / 13	3	1	13 / 1	12 / 12	$(\rho_{1,5} + 24)$	k_5
		5 / 17	3	1	41 / 29	12 / 12	$\pmod{48}$	$\pmod{48}$
		7 / 19	1	3	15 / 3	40 / 40	$\rho_{1,5}$	
		11 / 23	1	3	43 / 31	8 / 8	$\pmod{48}$	
	4	1 / 13	1	4	21 / 33	4 / 28	$(\rho_{1,5} + 24)$	k_5
		5 / 17	1	4	25 / 37	44 / 20	$\pmod{48}$	$\pmod{48}$
		7 / 19	3	4	7 / 19	0 / 24	$\rho_{1,5}$	
		11 / 23	3	4	11 / 23	24 / 0	$\pmod{48}$	

Thus, for $L = 16k_L\Psi$, $k_L \in \{1,3\}$, $\rho_3 = k_{3,\rho} \cdot 2\Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, with $k_{3,\rho}, k_{3,f} \in \{0,1,2,3\}$, $\rho_2 = (2k_{2,\rho}k_L - 1) \cdot \Psi$, and $f_2 = (2k_{2,f}k_L - 1) \cdot \Psi$, with $k_L \in \{1,3\}$, $k_{2,\rho}, k_{2,f} \in \{1,2,3,4\}$, (12) is equivalent to

$$
\begin{aligned}
&(f_1\rho_1 - 1) \cdot x + \Psi \cdot (f_1 \cdot (2k_{2,\rho}k_L - 1) + (2k_{2,f}k_L - 1) \cdot \rho_1^2) \cdot x^2 + \\
&+2\Psi \cdot (f_1 k_{3,\rho} + (2k_{2,f}k_L - 1) \cdot (2k_{2,\rho}k_L - 1)\Psi\rho_1 + k_{3,f}\rho_1^3) \cdot x^3 + \\
&+\Psi \cdot (\rho_1^4 + 6k_{3,f} \cdot (2k_{2,\rho}k_L - 1) \cdot \Psi \cdot \rho_1^2 + 4k_{3,\rho} \cdot (2k_{2,f}k_L - 1) \cdot \Psi \cdot \rho_1 + \\
&+(2k_{2,f}k_L - 1) \cdot (2k_{2,\rho}k_L - 1)^2 \cdot \Psi^2 + f_1) \cdot x^4 + \\
&+2\Psi^2 \cdot (2 \cdot (2k_{2,\rho}k_L - 1) \cdot \rho_1^3 + 6k_{3,f}k_{3,\rho}\rho_1^2 + 3k_{3,f} \cdot (2k_{2,\rho}k_L - 1)^2 \cdot \Psi\rho_1 + (2k_{2,f}k_L - 1) \cdot \rho_1 + \\
&+2 \cdot (2k_{2,f}k_L - 1) \cdot (2k_{2,\rho}k_L - 1) \cdot k_{3,\rho}\Psi) \cdot x^5 + \\
&+2\Psi^2 \cdot (4k_{3,\rho}\rho_1^3 + 3 \cdot (2k_{2,\rho}k_L - 1)^2 \cdot \Psi\rho_1^2 + 3k_{3,f}\rho_1^2 + 12k_{3,f}k_{3,\rho} \cdot (2k_{2,\rho}k_L - 1) \cdot \Psi\rho_1 + \\
&+k_{3,f} \cdot (2k_{2,\rho}k_L - 1)^3 \cdot \Psi^2 + (2k_{2,f}k_L - 1) \cdot (2k_{2,\rho}k_L - 1) \cdot \Psi + 2 \cdot (2k_{2,f}k_L - 1) \cdot k_{3,\rho}^2\Psi) \cdot x^6 + \\
&+4\Psi^2 \cdot (\rho_1^3 + 6k_{3,\rho} \cdot (2k_{2,\rho}k_L - 1) \cdot \Psi\rho_1^2 + (2k_{2,\rho}k_L - 1)^3 \cdot \Psi^2\rho_1 + 3k_{3,f} \cdot (2k_{2,\rho}k_L - 1) \cdot \Psi\rho_1 +
\end{aligned}
$$

$$+6k_{3,f}k_{3,\rho}^2\Psi\rho_1+3k_{3,f}k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi^2+k_{3,\rho}\cdot(2k_{2,f}k_L-1)\cdot\Psi)\cdot x^7+$$
$$+\Psi^3\cdot(12\cdot(2k_{2,\rho}k_L-1)\cdot\rho_1^2+24k_{3,\rho}^2\rho_1^2+24k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi\rho_1+24k_{3,f}k_{3,\rho}\rho_1+$$
$$+(2k_{2,\rho}k_L-1)^4\cdot\Psi^2+6k_{3,f}\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi+24k_{3,f}k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)\cdot\Psi+(2k_{2,f}k_L-1))\cdot x^8+$$
$$+2\Psi^3\cdot(12k_{3,\rho}\rho_1^2+3k_{3,f}\rho_1+24k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)\cdot\Psi\rho_1+6\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi\rho_1+$$
$$+4k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^3\cdot\Psi^2+12k_{3,f}k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot\Psi+8k_{3,f}k_{3,\rho}^3\Psi)\cdot x^9+$$
$$+2\Psi^3\cdot(3\rho_1^2+16k_{3,\rho}^3\Psi\rho_1+24k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot\Psi\rho_1+2\cdot(2k_{2,\rho}k_L-1)^3\cdot\Psi^2+$$
$$+12k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi^2+3k_{3,f}\cdot(2k_{2,\rho}k_L-1)\cdot\Psi+12k_{3,f}k_{3,\rho}^2\Psi)\cdot x^{10}+$$
$$+4\Psi^4\cdot(12k_{3,\rho}^2\rho_1+3\cdot(2k_{2,\rho}k_L-1)\cdot\rho_1+8k_{3,\rho}^3\cdot(2k_{2,\rho}k_L-1)\cdot\Psi+$$
$$+6k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi+3k_{3,f}k_{3,\rho})\cdot x^{11}+$$
$$+2\Psi^4\cdot(12k_{3,\rho}\rho_1+8k_{3,\rho}^4\Psi+3\cdot(2k_{2,\rho}k_L-1)^2\cdot\Psi+24k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)\cdot\Psi+k_{3,f})\cdot x^{12}+$$
$$+4\Psi^4\cdot(\rho_1+8k_{3,\rho}^3\Psi+6k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot\Psi)\cdot x^{13}+4\Psi^5\cdot(6k_{3,\rho}^2+(2k_{2,\rho}k_L-1))\cdot x^{14}+$$
$$+(8k_{3,\rho}\Psi^5)\cdot x^{15}+\Psi^5\cdot x^{16}=0\ (\mathrm{mod}\ 16k_L\Psi),\forall x\in\{0,1,\ldots,16k_L\Psi-1\}. \quad (13)$$

Because $\Psi \mid L$, from (13) we have

$$(f_1\rho_1-1)\cdot x=0\ (\mathrm{mod}\ \Psi),\forall x\in\{0,1,\ldots,16k_L\Psi-1\}. \quad (14)$$

Equation (14) is equivalent to

$$f_1\rho_1=1\ (\mathrm{mod}\ \Psi)\Leftrightarrow f_1\rho_1=\Psi\cdot k+1\ (\mathrm{mod}\ 16k_L\Psi),\ \text{with}\ k\in\{0,1,2,\ldots,16k_L-1\}. \quad (15)$$

We note that when $k_L=1$, we have $\gcd(f_1,16\Psi)=1$. According to Theorem 57 from [30], in this case congruence (15) has only one solution in variable ρ_1. When $k_L=3$, we can have $\gcd(f_1,48\Psi)=3$. Thus, congruence (15) has three solutions, but as we will see, only one solution from the three will be valid.

With (15) and denoting $\Psi\ (\mathrm{mod}\ 16k_L)=k_\Psi$, (13) is fulfilled if and only if

$$k\cdot x+(f_1\cdot(2k_{2,\rho}k_L-1)+(2k_{2,f}k_L-1)\cdot\rho_1^2)\cdot x^2+$$
$$+2\cdot(f_1k_{3,\rho}+(2k_{2,f}k_L-1)\cdot(2k_{2,\rho}k_L-1)k_\Psi\rho_1+k_{3,f}\rho_1^3)\cdot x^3+$$
$$+(\rho_1^4+6k_{3,f}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi\cdot\rho_1^2+4k_{3,\rho}\cdot(2k_{2,f}k_L-1)\cdot k_\Psi\cdot\rho_1+$$
$$+(2k_{2,f}k_L-1)\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi^2+f_1)\cdot x^4+$$
$$+2k_\Psi\cdot(2\cdot(2k_{2,\rho}k_L-1)\cdot\rho_1^3+6k_{3,f}k_{3,\rho}\rho_1^2+3k_{3,f}\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi\rho_1+(2k_{2,f}k_L-1)\cdot\rho_1+$$
$$+2\cdot(2k_{2,f}k_L-1)\cdot(2k_{2,\rho}k_L-1)\cdot k_{3,\rho}k_\Psi)\cdot x^5+$$
$$+2k_\Psi\cdot(4k_{3,\rho}\rho_1^3+3\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi\rho_1^2+3k_{3,f}\rho_1^2+12k_{3,f}k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi\rho_1+$$
$$+k_{3,f}\cdot(2k_{2,\rho}k_L-1)^3\cdot k_\Psi^2+(2k_{2,f}k_L-1)\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi+2\cdot(2k_{2,f}k_L-1)\cdot k_{3,\rho}^2k_\Psi)\cdot x^6+$$
$$+4k_\Psi\cdot(\rho_1^3+6k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi\rho_1^2+(2k_{2,\rho}k_L-1)^3\cdot k_\Psi^2\rho_1+3k_{3,f}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi\rho_1+$$
$$+6k_{3,f}k_{3,\rho}^2k_\Psi\rho_1+3k_{3,f}k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi^2+k_{3,\rho}\cdot(2k_{2,f}k_L-1)\cdot k_\Psi)\cdot x^7+$$
$$+k_\Psi^2\cdot(12\cdot(2k_{2,\rho}k_L-1)\cdot\rho_1^2+24k_{3,\rho}^2\rho_1^2+24k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi\rho_1+24k_{3,f}k_{3,\rho}\rho_1+$$

$$+(2k_{2,\rho}k_L-1)^4\cdot k_\Psi^2+6k_{3,f}\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi+24k_{3,f}k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi+(2k_{2,f}k_L-1))\cdot x^8+$$
$$+2k_\Psi^2\cdot(12k_{3,\rho}\rho_1^2+3k_{3,f}\rho_1+24k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi\rho_1+6\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi\rho_1+$$
$$+4k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^3\cdot k_\Psi^2+12k_{3,f}k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi+8k_{3,f}k_{3,\rho}^3k_\Psi)\cdot x^9+$$
$$+2k_\Psi^2\cdot(3\rho_1^2+16k_{3,\rho}^3k_\Psi\rho_1+24k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi\rho_1+$$
$$+2\cdot(2k_{2,\rho}k_L-1)^3\cdot k_\Psi^2+12k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi^2+3k_{3,f}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi+12k_{3,f}k_{3,\rho}^2k_\Psi)\cdot x^{10}+$$
$$+4k_\Psi^3\cdot(12k_{3,\rho}^2\rho_1+3\cdot(2k_{2,\rho}k_L-1)\cdot\rho_1+8k_{3,\rho}^3\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi+$$
$$+6k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi+3k_{3,f}k_{3,\rho})\cdot x^{11}+$$
$$+2k_\Psi^3\cdot(12k_{3,\rho}\rho_1+8k_{3,\rho}^4k_\Psi+3\cdot(2k_{2,\rho}k_L-1)^2\cdot k_\Psi+24k_{3,\rho}^2\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi+k_{3,f})\cdot x^{12}+$$
$$+4k_\Psi^3\cdot(\rho_1+8k_{3,\rho}^3k_\Psi+6k_{3,\rho}\cdot(2k_{2,\rho}k_L-1)\cdot k_\Psi)\cdot x^{13}+4k_\Psi^4\cdot(6k_{3,\rho}^2+(2k_{2,\rho}k_L-1))\cdot x^{14}+$$
$$+(8k_{3,\rho}k_\Psi^4)\cdot x^{15}+k_\Psi^4\cdot x^{16}=0\ (\mathrm{mod}\ 16k_L),\forall x\in\{0,1,\ldots,16k_L-1\}. \quad (16)$$

We note that the values of k_L and k_Ψ are given by the interleaver length.

Because Ψ is odd, when $k_L=1$ we can have $k_\Psi\in\{1,3,5,7,9,11,13,15\}$.

For $k_L=1$ we denote $k'_{2,f}=2k_{2,f}-1$ and $k'_{2,\rho}=2k_{2,\rho}-1$.

In this case, the variables from Equation (16) are $f_1\ (\mathrm{mod}\ 16),\rho_1\ (\mathrm{mod}\ 16)\in\{1,3,5,\ldots,15\}$, $k_{3,\rho},k_{3,f}\in\{0,1,2,3\}$, $k'_{2,\rho},k'_{2,f}\in\{1,3,5,7\}$, k, and k_Ψ. The values of $k_{3,f}$, $k'_{2,f}$, and $f_1\ (\mathrm{mod}\ 16)$ are given by the true 4-PP, for which we want to find the inverse 4-PP; and k_Ψ is given by the interleaver length. Given the values of k_Ψ, $k_{3,f}$, $k'_{2,f}$, and $f_1\ (\mathrm{mod}\ 16)$, we can find the coefficients of the inverse 4-PP by exhaustive searching for the rest of variables, $k_{3,\rho}$, $k'_{2,\rho}$, $\rho_1\ (\mathrm{mod}\ 16)$, and k. For each $k_{3,\rho}\in\{0,1,2,3\}$, $k'_{2,\rho}\in\{1,3,5,7\}$, $\rho_1\ (\mathrm{mod}\ 16)\in\{1,3,5,\ldots,15\}$, and $k\in\{0,1,\ldots,15\}$, we test if the left hand side term from (16), evaluated modulo 16, is equal to 0 for each $x\in\{0,1,\ldots,15\}$. For a combination of variables k_Ψ, $k_{3,f}$, $k'_{2,f}$, and $f_1\ (\mathrm{mod}\ 16)$, only a combination of $k_{3,\rho}$, $k'_{2,\rho}$, $\rho_1\ (\mathrm{mod}\ 16)$, and k results in a solution of (16). In this way, using Matlab environment we found all the solutions of Equation (16). Solutions in variables k, $f_1\ (\mathrm{mod}\ 16)$, $\rho_1\ (\mathrm{mod}\ 16)$, $k_{3,\rho}$, $k_{3,f}$, and $k'_{2,\rho}$, $k'_{2,f}$ are the same $\forall k_\Psi\in\{1,5,9,13\}$, and also solutions in the previously mentioned variables are the same $\forall k_\Psi\in\{3,7,11,15\}$. For every $k_\Psi\in\{1,3,5,\ldots,15\}$, solutions of Equation (16) in variables k, $k_{3,\rho},k_{3,f}$, and $k'_{2,\rho},k'_{2,f}$ are the same $\forall f_1\ (\mathrm{mod}\ 16)\in\{1,9\}$, or $\forall f_1\ (\mathrm{mod}\ 16)\in\{3,11\}$, or $\forall f_1\ (\mathrm{mod}\ 16)\in\{5,13\}$, or $\forall f_1\ (\mathrm{mod}\ 16)\in\{7,15\}$. If the solution of Equation (16) in variable $\rho_1\ (\mathrm{mod}\ 16)$ for $f_1\ (\mathrm{mod}\ 16)=f_1\ (\mathrm{mod}\ 8)=f_{1,8}\in\{1,3,5,7\}$ and the other variables with fixed values, is $\rho_{1,f_{1,8}}\ (\mathrm{mod}\ 16)$, then solution of the same equation in variable $\rho_1\ (\mathrm{mod}\ 16)$, for $f_1\ (\mathrm{mod}\ 16)=f_{1,8}+8$, is $(\rho_{1,f_{1,8}}+8)\ (\mathrm{mod}\ 16)$. Thus, for $k_L=1$, we can summarize the solutions of (16) for every $k_\Psi\ (\mathrm{mod}\ 4)=k_{\Psi,4}\in\{1,3\}$ and for every $f_1\ (\mathrm{mod}\ 8)\in\{1,3,5,7\}$. These solutions are given in Tables 3 and 4.

When $k_L=3$, because $3\nmid\Psi$, we can have $k_\Psi\in\{1,5,7,11,13,17,19,23,25,29,31,35,37,41,43,47\}$. We note that in this case, because of condition $(f_1+f_3)\neq 0\ (\mathrm{mod}\ 3)$, we can have only some values for $f_1\ (\mathrm{mod}\ 48)$, not every odd number. Because $3\nmid\Psi$, we can have $\Psi\ (\mathrm{mod}\ 3)\in\{1,2\}$. Because $f_3=k_{3,f}\cdot 2\Psi$, with $k_{3,f}\in\{0,1,2,3\}$, we can have:

(1) $f_1\ (\mathrm{mod}\ 48)\in\{1,5,7,11,13,17,19,23,25,29,31,35,37,41,43,47\}$, when $\Psi\ (\mathrm{mod}\ 3)\in\{1,2\}$ and $k_{3,f}\in\{0,3\}$;

(2) $f_1\ (\mathrm{mod}\ 48)\in\{1,3,7,9,13,15,19,21,25,27,31,33,37,39,43,45\}$, when $\Psi\ (\mathrm{mod}\ 3)=1$ and $k_{3,f}=2$ or when $\Psi\ (\mathrm{mod}\ 3)=2$ and $k_{3,f}=1$;

(3) $f_1\ (\mathrm{mod}\ 48)\in\{3,5,9,11,15,17,21,23,27,29,33,35,39,41,45\}$, when $\Psi\ (\mathrm{mod}\ 3)=1$ and $k_{3,f}=1$ or when $\Psi\ (\mathrm{mod}\ 3)=2$ and $k_{3,f}=2$.

Solutions of Equation (16) for $k_L=3$ were found in the same way as for $k_L=1$, as it was previously explained. Solutions in variables k, $f_1\ (\mathrm{mod}\ 48)$, $\rho_1\ (\mathrm{mod}\ 48)$, $k_{3,\rho},k_{3,f}$, and $k_{2,\rho},k_{2,f}$ are the

same $\forall k_\Psi \in \{1, 13, 25, 37\}$, or $\forall k_\Psi \in \{5, 17, 29, 41\}$, or $\forall k_\Psi \in \{7, 19, 31, 43\}$, or $\forall k_\Psi \in \{11, 23, 35, 47\}$. For every $k_\Psi \in \{1, 5, 7, 11, \ldots, 47\}$, solutions of Equation (16) in variables k, $k_{3,\rho}, k_{3,f}$, and $k_{2,\rho}, k_{2,f}$ are the same $f_1 \pmod{48}$ and for $(f_1 + 24) \pmod{48}$. If the solution of Equation (16) in variable $\rho_1 \pmod{48}$ for $f_1 \pmod{48} = f_1 \pmod{24} = f_{1,24}$ and with the other variables with fixed values, is $\rho_{1,f_{1,24}} \pmod{48}$, then solution of the same equation in variable $\rho_1 \pmod{48}$, for $f_1 \pmod{48} = f_{1,24} + 24$, is $(\rho_{1,f_{1,24}} + 24) \pmod{48}$. Thus, for $k_L = 3$, we can summarize the solutions of (16) for every $k_\Psi \pmod{12} = k_{\Psi,12} \in \{1, 5, 7, 11\}$ and for every $f_1 \pmod{24}$. These solutions, found by means of Matlab software, are given in Tables 5–8. □

We note that the inverse 4-PP from Lemma 2 is a true 4-PP, and thus the 4-PP $\pi(x)$ does not admit an inverse QPP or CPP.

3.3. Upper Bounds on the Minimum Distances for 4-PP-Based Turbo Codes for Interleaver Lengths of the Form 16Ψ *or* 48Ψ

In this subsection, we prove that for the interleaver lengths of the form given in Equation (5), a true 4-PP leads to a minimum distance which is upper bounded by the value of 36 or 28, depending on the classes of coefficients, for a classical 1/3 rate turbo code with two recursive systematic convolutional (RSC) component codes having generator matrix $G = [1, 15/13]$ in octal form.

Theorem 1. *Let the interleaver length be of the form given in* (5)*. Then, the minimum distance of the classical nominal 1/3 rate turbo code with two RSC codes parallel concatenated having the generator matrix* $G = [1, 15/13]$ *(in octal form) and 4-PP interleavers—fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, with coefficients* $f_4 = \Psi$*,* $f_3 = k_{3,f} \cdot 2\Psi$*,* $k_{3,f} \in \{1, 3\}$*,* $f_2 = (2k_{2,f} \cdot k_L - 1) \cdot \Psi$*,* $k_{2,f} \in \{1, 2, 3, 4\}$*, and* $k_L \in \{1, 3\}$*—is upper bounded by the value of 36.*

Proof. We consider the interleaver pattern of size twelve shown in Figure 1.

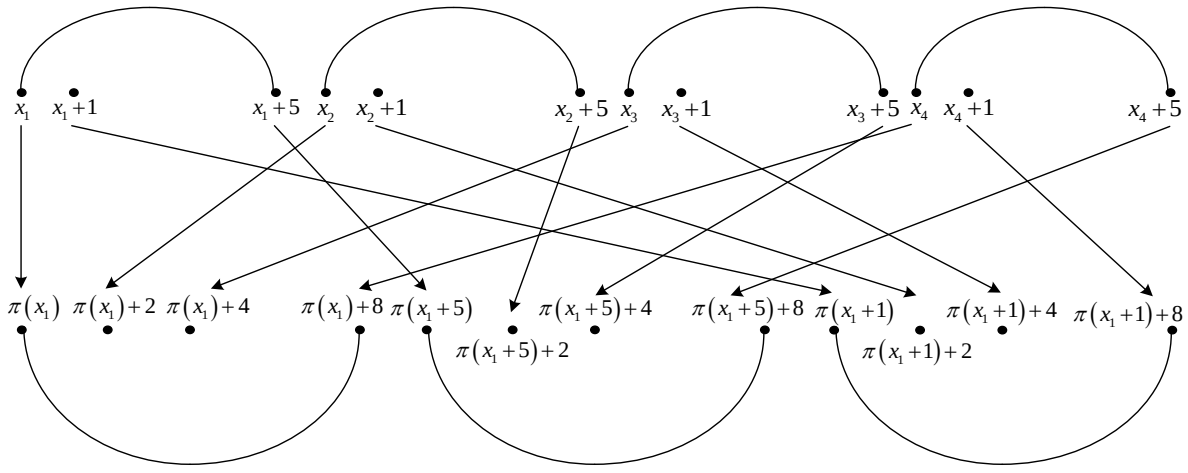

Figure 1. Critical interleaver pattern of size twelve for 4-PP-based interleavers.

The twelve elements of permutation $\pi(\cdot)$ indicated in Figure 1 are written in detail below.

$$\begin{cases} x_1 \to \pi(x_1) \\ x_1+1 \to \pi(x_1+1) \pmod L \\ x_1+5 \to \pi(x_1+5) \pmod L \\ x_2 \to \pi(x_2) = \pi(x_1)+2 \pmod L \\ x_2+1 \to \pi(x_2+1) = \pi(x_1+1)+2 \pmod L \\ x_2+5 \to \pi(x_2+5) = \pi(x_1+5)+2 \pmod L \\ x_3 \to \pi(x_3) = \pi(x_1)+4 \pmod L \\ x_3+1 \to \pi(x_3+1) = \pi(x_1+1)+4 \pmod L \\ x_3+5 \to \pi(x_3+5) = \pi(x_1+5)+4 \pmod L \\ x_4 \to \pi(x_4) = \pi(x_1)+8 \pmod L \\ x_4+1 \to \pi(x_4+1) = \pi(x_1+1)+8 \pmod L \\ x_4+5 \to \pi(x_4+5) = \pi(x_1+5)+8 \pmod L \end{cases} \tag{17}$$

Writing $x_2 = \rho(\pi(x_2)) = \rho(\pi(x_1)+2)$ in the fifth and sixth equations from (17), $x_3 = \rho(\pi(x_3)) = \rho(\pi(x_1)+4)$ in the eighth and ninth equations from (17), and $x_4 = \rho(\pi(x_4)) = \rho(\pi(x_1)+8)$ in the eleventh and twelfth equation from (17), with $x_1 = x$, we have

$$\begin{cases} \pi(\rho(\pi(x)+2)+1) = \pi(x+1)+2 \pmod L \\ \pi(\rho(\pi(x)+2)+5) = \pi(x+5)+2 \pmod L \\ \pi(\rho(\pi(x)+4)+1) = \pi(x+1)+4 \pmod L \\ \pi(\rho(\pi(x)+4)+5) = \pi(x+5)+4 \pmod L \\ \pi(\rho(\pi(x)+8)+1) = \pi(x+1)+8 \pmod L \\ \pi(\rho(\pi(x)+8)+5) = \pi(x+5)+8 \pmod L \end{cases} \tag{18}$$

Taking into account that

$$\pi(a+b) = \pi(a)+\pi(b)+a\cdot b\cdot\left(2f_4\cdot(2a^2+3ab+2b^2)+3f_3\cdot(a+b)+2f_2\right), \tag{19}$$

equations from (18) are equivalent to

$$\begin{cases} \rho(\pi(x)+2)\cdot\left(2f_4\cdot(2\rho^2(\pi(x)+2)+3\rho(\pi(x)+2)+2)+\right. \\ \left.+3f_3\cdot(\rho(\pi(x)+2)+1)+2f_2\right) = x\cdot\left(2f_4\cdot(2x^2+3x+2)+3f_3\cdot(x+1)+2f_2\right) \pmod L \\ 5\cdot\rho(\pi(x)+2)\cdot\left(2f_4\cdot(2\rho^2(\pi(x)+2)+3\cdot5\cdot\rho(\pi(x)+2)+2\cdot5^2)+\right. \\ \left.+3f_3\cdot(\rho(\pi(x)+2)+5)+2f_2\right) = \\ = 5\cdot x\cdot\left(2f_4\cdot(2x^2+3\cdot5\cdot x+2\cdot5^2)+3f_3\cdot(x+5)+2f_2\right) \pmod L \\ \rho(\pi(x)+4)\cdot\left(2f_4\cdot(2\rho^2(\pi(x)+4)+3\rho(\pi(x)+4)+2)+\right. \\ \left.+3f_3\cdot(\rho(\pi(x)+4)+1)+2f_2\right) = x\cdot\left(2f_4\cdot(2x^2+3x+2)+3f_3\cdot(x+1)+2f_2\right) \pmod L \\ 5\cdot\rho(\pi(x)+4)\cdot\left(2f_4\cdot(2\rho^2(\pi(x)+4)+3\cdot5\cdot\rho(\pi(x)+4)+2\cdot5^2)+\right. \\ \left.+3f_3\cdot(\rho(\pi(x)+4)+5)+2f_2\right) = \\ = 5\cdot x\cdot\left(2f_4\cdot(2x^2+3\cdot5\cdot x+2\cdot5^2)+3f_3\cdot(x+5)+2f_2\right) \pmod L \\ \rho(\pi(x)+8)\cdot\left(2f_4\cdot(2\rho^2(\pi(x)+8)+3\rho(\pi(x)+8)+2)+\right. \\ \left.+3f_3\cdot(\rho(\pi(x)+8)+1)+2f_2\right) = x\cdot\left(2f_4\cdot(2x^2+3x+2)+3f_3\cdot(x+1)+2f_2\right) \pmod L \\ 5\cdot\rho(\pi(x)+8)\cdot\left(2f_4\cdot(2\rho^2(\pi(x)+8)+3\cdot5\cdot\rho(\pi(x)+8)+2\cdot5^2)+\right. \\ \left.+3f_3\cdot(\rho(\pi(x)+8)+5)+2f_2\right) = \\ = 5\cdot x\cdot\left(2f_4\cdot(2x^2+3\cdot5\cdot x+2\cdot5^2)+3f_3\cdot(x+5)+2f_2\right) \pmod L \end{cases} \tag{20}$$

or

$$\begin{cases} 4f_4 \cdot \rho^3(\pi(x)+2) + (6f_4+3f_3) \cdot \rho^2(\pi(x)+2) + (4f_4+3f3+2f_2) \cdot \rho(\pi(x)+2) = \\ = 2f_4 \cdot (2x^3+3x^2+2x) + 3f_3 \cdot (x^2+x) + 2f_2 \cdot x \pmod{L} \\ 20f_4 \cdot \rho^3(\pi(x)+2) + (150f_4+15f_3) \cdot \rho^2(\pi(x)+2) + (500f_4+75f3+10f_2) \cdot \rho(\pi(x)+2) = \\ = 10f_4 \cdot (2x^3+15x^2+50x) + 15f_3 \cdot (x^2+5x) + 10f_2 \cdot x \pmod{L} \\ 4f_4 \cdot \rho^3(\pi(x)+4) + (6f_4+3f_3) \cdot \rho^2(\pi(x)+4) + (4f_4+3f3+2f_2) \cdot \rho(\pi(x)+4) = \\ = 2f_4 \cdot (2x^3+3x^2+2x) + 3f_3 \cdot (x^2+x) + 2f_2 \cdot x \pmod{L} \\ 20f_4 \cdot \rho^3(\pi(x)+4) + (150f_4+15f_3) \cdot \rho^2(\pi(x)+4) + (500f_4+75f3+10f_2) \cdot \rho(\pi(x)+4) = \\ = 10f_4 \cdot (2x^3+15x^2+50x) + 15f_3 \cdot (x^2+5x) + 10f_2 \cdot x \pmod{L} \\ 4f_4 \cdot \rho^3(\pi(x)+8) + (6f_4+3f_3) \cdot \rho^2(\pi(x)+8) + (4f_4+3f3+2f_2) \cdot \rho(\pi(x)+8) = \\ = 2f_4 \cdot (2x^3+3x^2+2x) + 3f_3 \cdot (x^2+x) + 2f_2 \cdot x \pmod{L} \\ 20f_4 \cdot \rho^3(\pi(x)+8) + (150f_4+15f_3) \cdot \rho^2(\pi(x)+8) + (500f_4+75f3+10f_2) \cdot \rho(\pi(x)+8) = \\ = 10f_4 \cdot (2x^3+15x^2+50x) + 15f_3 \cdot (x^2+5x) + 10f_2 \cdot x \pmod{L}. \end{cases} \tag{21}$$

For $L = 16 \cdot k_L \cdot \Psi$, $f_4 = \Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, $k_{3,f} \in \{0,1,2,3\}$, $f_2 = (2k_{2,f} \cdot k_L - 1) \cdot \Psi$, $k_{2,f} \in \{1,2,3,4\}$, $k_L \in \{1,3\}$, equations from (21) become

$$\begin{cases} 4\Psi \cdot \rho^3(\pi(x)+2) + 2\Psi \cdot (3+3k_{3,f}) \cdot \rho^2(\pi(x)+2) + 2\Psi \cdot (2+3k_{3,f}+2k_{2,f} \cdot k_L - 1) \cdot \rho(\pi(x)+2) = \\ = 2\Psi \cdot (2x^3+3x^2+2x) + 2\Psi \cdot 3k_{3,f} \cdot (x^2+x) + 2\Psi \cdot (2k_{2,f} \cdot k_L - 1) \cdot x \pmod{16 \cdot k_L \cdot \Psi} \\ 20\Psi \cdot \rho^3(\pi(x)+2) + 2\Psi \cdot (75+15k_{3,f}) \cdot \rho^2(\pi(x)+2) + 2\Psi \cdot (250+75k_{3,f} + \\ +5 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(\pi(x)+2) = 10\Psi \cdot (2x^3+15x^2+50x) + 2\Psi \cdot 15k_{3,f} \cdot (x^2+5x) + \\ +5 \cdot (2k_{2,f} \cdot k_L - 1) \cdot 2\Psi \cdot x \pmod{16 \cdot k_L \cdot \Psi} \\ 4\Psi \cdot \rho^3(\pi(x)+4) + 2\Psi \cdot (3+3k_{3,f}) \cdot \rho^2(\pi(x)+4) + 2\Psi \cdot (2+3k_{3,f}+2f_2) \cdot \rho(\pi(x)+4) = \\ = 2\Psi \cdot (2x^3+3x^2+2x) + 2\Psi \cdot 3k_{3,f} \cdot (x^2+x) + 2\Psi \cdot (2k_{2,f} \cdot k_L - 1) \cdot x \pmod{16 \cdot k_L \cdot \Psi} \\ 20\Psi \cdot \rho^3(\pi(x)+4) + 2\Psi \cdot (75+15k_{3,f}) \cdot \rho^2(\pi(x)+4) + 2\Psi \cdot (250+75k_{3,f}+5 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \\ \rho(\pi(x)+4) = 10\Psi \cdot (2x^3+15x^2+50x) + 2\Psi \cdot 15k_{3,f} \cdot (x^2+5x) + \\ +5 \cdot (2k_{2,f} \cdot k_L - 1) \cdot 2\Psi \cdot x \pmod{16 \cdot k_L \cdot \Psi} \\ 4\Psi \cdot \rho^3(\pi(x)+8) + 2\Psi \cdot (3+3k_{3,f}) \cdot \rho^2(\pi(x)+8) + 2\Psi \cdot (2+3k_{3,f}+2f_2) \cdot \rho(\pi(x)+8) = \\ = 2\Psi \cdot (2x^3+3x^2+2x) + 2\Psi \cdot 3k_{3,f} \cdot (x^2+x) + 2\Psi \cdot (2k_{2,f} \cdot k_L - 1) \cdot x \pmod{16 \cdot k_L \cdot \Psi} \\ 20\Psi \cdot \rho^3(\pi(x)+8) + 2\Psi \cdot (75+15k_{3,f}) \cdot \rho^2(\pi(x)+8) + 2\Psi \cdot (250+75k_{3,f}+5 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \\ \rho(\pi(x)+8) = 10\Psi \cdot (2x^3+15x^2+50x) + 2\Psi \cdot 15k_{3,f} \cdot (x^2+5x) + \\ +5 \cdot (2k_{2,f} \cdot k_L - 1) \cdot 2\Psi \cdot x \pmod{16 \cdot k_L \cdot \Psi}. \end{cases} \tag{22}$$

Equations from (22) are fulfilled if and only if

$$\begin{cases} 2 \cdot \rho^3(\pi(x)+2) + 3 \cdot (k_{3,f}+1) \cdot \rho^2(\pi(x)+2) + (3k_{3,f}+2k_{2,f}k_L+1) \cdot \rho(\pi(x)+2) = \\ = 3k_{3,f} \cdot (x^2+x) + (2k_{2,f} \cdot k_L - 1) \cdot x + (2x^3+3x^2+2x) \pmod{8 \cdot k_L} \\ 10 \cdot \rho^3(\pi(x)+2) + 15 \cdot (k_{3,f}+3) \cdot \rho^2(\pi(x)+2) + 5 \cdot (15k_{3,f}+2k_{2,f} \cdot k_L - 1 + 50) \cdot \rho(\pi(x)+2) = \\ = 15k_{3,f} \cdot (x^2+5x) + 5 \cdot (2k_{2,f} \cdot k_L - 1) \cdot x + 5 \cdot (2x^3+15x^2+50x) \pmod{8 \cdot k_L} \\ 2 \cdot \rho^3(\pi(x)+4) + 3 \cdot (k_{3,f}+1) \cdot \rho^2(\pi(x)+4) + (3k_{3,f}+2k_{2,f} \cdot k_L + 1) \cdot \rho(\pi(x)+4) = \\ = 3k_{3,f} \cdot (x^2+x) + (2k_{2,f} \cdot k_L - 1) \cdot x + (2x^3+3x^2+2x) \pmod{8 \cdot k_L} \\ 10 \cdot \rho^3(\pi(x)+4) + 15 \cdot (k_{3,f}+3) \cdot \rho^2(\pi(x)+4) + (250+75k_{3,f}+5 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(\pi(x)+4) = \\ = 15k_{3,f} \cdot (x^2+5x) + 5 \cdot (2k_{2,f} \cdot k_L - 1) \cdot x + 5 \cdot (2x^3+15x^2+50x) \pmod{8 \cdot k_L} \\ 2 \cdot \rho^3(\pi(x)+8) + 3 \cdot (k_{3,f}+1) \cdot \rho^2(\pi(x)+8) + (3k_{3,f}+2k_{2,f} \cdot k_L + 1) \cdot \rho(\pi(x)+8) = \\ = 3k_{3,f} \cdot (x^2+x) + (2k_{2,f} \cdot k_L - 1) \cdot x + (2x^3+3x^2+2x) \pmod{8 \cdot k_L} \\ 10 \cdot \rho^3(\pi(x)+8) + 15 \cdot (k_{3,f}+3) \cdot \rho^2(\pi(x)+8) + 5 \cdot (15k_{3,f}+2k_{2,f} \cdot k_L - 1 + 50) \cdot \rho(\pi(x)+8) = \\ = 15k_{3,f} \cdot (x^2+5x) + 5 \cdot (2k_{2,f} \cdot k_L - 1) \cdot x + 5 \cdot (2x^3+15x^2+50x) \pmod{8 \cdot k_L}. \end{cases} \tag{23}$$

For $x = 0$, equations from (20) become

$$\begin{cases} 2 \cdot \rho^3(2) + 3 \cdot (k_{3,f}+1) \cdot \rho^2(2) + (3k_{3,f}+2k_{2,f}k_L+1) \cdot \rho(2) = 0 \pmod{8 \cdot k_L} \\ 10 \cdot \rho^3(2) + 15 \cdot (k_{3,f}+3) \cdot \rho^2(2) + 5 \cdot (15k_{3,f}+2k_{2,f} \cdot k_L - 1 + 50) \cdot \rho(2) = 0 \pmod{8 \cdot k_L} \\ 2 \cdot \rho^3(4) + 3 \cdot (k_{3,f}+1) \cdot \rho^2(4) + (3k_{3,f}+2k_{2,f} \cdot k_L + 1) \cdot \rho(4) = 0 \pmod{8 \cdot k_L} \\ 10 \cdot \rho^3(4) + 15 \cdot (k_{3,f}+3) \cdot \rho^2(4) + (250+75k_{3,f}+5 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(4) = 0 \pmod{8 \cdot k_L} \\ 2 \cdot \rho^3(8) + 3 \cdot (k_{3,f}+1) \cdot \rho^2(8) + (3k_{3,f}+2k_{2,f} \cdot k_L + 1) \cdot \rho(8) = 0 \pmod{8 \cdot k_L} \\ 10 \cdot \rho^3(8) + 15 \cdot (k_{3,f}+3) \cdot \rho^2(8) + 5 \cdot (15k_{3,f}+2k_{2,f} \cdot k_L - 1 + 50) \cdot \rho(8) = 0 \pmod{8 \cdot k_L} \end{cases} \tag{24}$$

or

$$\begin{cases} \rho(2)/2 \cdot \left(2\rho^2(2) + 3\rho(2) + 1 + 3k_{3,f} \cdot (\rho(2)+1) + 2k_{2,f} \cdot k_L\right) = 0 \pmod{4 \cdot k_L} \\ 5 \cdot \rho(2)/2 \cdot \left(2\rho^2(2) + 3 \cdot 5 \cdot \rho(2) + 49 + 3k_{3,f} \cdot (\rho(2)+5) + 2k_{2,f} \cdot k_L\right) = 0 \pmod{4 \cdot k_L} \\ \rho(4)/4 \cdot \left(2\rho^2(4) + 3\rho(4) + 1 + 3k_{3,f} \cdot (\rho(4)+1) + 2k_{2,f} \cdot k_L\right) = 0 \pmod{2 \cdot k_L} \\ 5 \cdot \rho(4)/4 \cdot \left(2\rho^2(4) + 3 \cdot 5 \cdot \rho(4) + 49 + 3k_{3,f} \cdot (\rho(4)+5) + 2k_{2,f} \cdot k_L\right) = 0 \pmod{2 \cdot k_L} \\ \rho(8)/8 \cdot \left(2\rho^2(8) + 3\rho(8) + 1 + 3k_{3,f} \cdot (\rho(8)+1) + 2k_{2,f} \cdot k_L\right) = 0 \pmod{k_L} \\ 5 \cdot \rho(8)/8 \cdot \left(2\rho^2(8) + 3 \cdot 5 \cdot \rho(8) + 49 + 3k_{3,f} \cdot (\rho(8)+5) + 2k_{2,f} \cdot k_L\right) = 0 \pmod{k_L}. \end{cases} \tag{25}$$

For $k_L = 1$ and $k'_{2,f} = 2k_{2,f} - 1$, equations from (25) are fulfilled if and only if

$$\begin{cases} (2\rho^2(2) + 3\rho(2) + 2) + 3k_{3,f} \cdot (\rho(2)+1) + k'_{2,f} = 0 \pmod 4 \\ (2\rho^2(2) + 3 \cdot 5 \cdot \rho(2) + 2 \cdot 5^2) + 3k_{3,f} \cdot (\rho(2)+5) + k'_{2,f} = 0 \pmod 4 \\ (2\rho^2(4) + 3\rho(4) + 2) + 3k_{3,f} \cdot (\rho(4)+1) + k'_{2,f} = 0 \pmod 2 \\ (2\rho^2(4) + 3 \cdot 5 \cdot \rho(4) + 2 \cdot 5^2) + 3k_{3,f} \cdot (\rho(4)+5) + k'_{2,f} = 0 \pmod 2 \end{cases} \tag{26}$$

or

$$\begin{cases} 2\rho_1 + 2 + 2k_{3,f} \cdot \rho_1 + 3k_{3,f} + k'_{2,f} = 0 \pmod 4 \\ k_{3,f} + k'_{2,f} = 0 \pmod 2 \end{cases} \tag{27}$$

or

$$\begin{cases} 2\rho_1 \cdot (k_{3,f}+1) + 2 + 3k_{3,f} + k'_{2,f} = 0 \pmod 4 \\ k_{3,f} + k'_{2,f} = 0 \pmod 2. \end{cases} \tag{28}$$

Equations from (28) are fulfilled if and only if $k_{3,f} = 1$ and $k'_{2,f} \in \{3,7\}$, or $k_{3,f} = 3$ and $k'_{2,f} \in \{1,5\}$.

For $k_L = 3$, equations from (25) are fulfilled if and only if

$$\begin{cases} \rho(2)/2 \cdot \left(2\rho^2(2) + 3\rho(2) + 1 + 3k_{3,f} \cdot (\rho(2)+1) + 6k_{2,f}\right) = 0 \pmod{12} \\ \rho(4)/4 \cdot \left(2\rho^2(4) + 3\rho(4) + 1 + 3k_{3,f} \cdot (\rho(4)+1) + 6k_{2,f}\right) = 0 \pmod 6 \\ \rho(8)/8 \cdot \left(2\rho^2(8) + 3\rho(8) + 1 + 3k_{3,f} \cdot (\rho(8)+1) + 6k_{2,f}\right) = 0 \pmod 3 \end{cases} \tag{29}$$

or

$$\begin{cases} \rho(2)/2 \cdot \left(2\rho^2(2) + 3\rho(2) + 1 + 3k_{3,f} \cdot (\rho(2)+1) + 6k_{2,f}\right) = 0 \pmod{12} \\ \rho(4)/4 \cdot \left(2\rho^2(4) + 1 + 3k_{3,f}\right) = 0 \pmod 6 \\ \rho(8)/8 \cdot \left(2\rho^2(8) + 1\right) = 0 \pmod 3. \end{cases} \tag{30}$$

With $\rho_2 = (6k_{2,\rho} - 1) \cdot \Psi$, $\rho_3 = k_{3,\rho} \cdot 2\Psi$, and $\rho_4 = \Psi$, we have

$$\begin{cases} \rho(2)/2 = \rho_1 + 8 \cdot k_{3,\rho} \cdot \Psi + 6 \cdot \Psi \pmod{12} \\ \rho(4)/4 = \rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi \pmod 6 \\ \rho(8)/8 = \rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi \pmod 3 \end{cases} \tag{31}$$

and

$$\begin{cases} 2 \cdot \rho^2(2) = 8 \cdot (\rho_1 + 8 \cdot k_{3,\rho} \cdot \Psi + 6 \cdot \Psi)^2 \pmod{12} \\ 2 \cdot \rho^2(4) = 2 \cdot (\rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi)^2 \pmod 6 \\ 2 \cdot \rho^2(8) = 2 \cdot (\rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi)^2 \pmod 3. \end{cases} \tag{32}$$

With (31) and (32), (30) is equivalent to

$$\begin{cases} 8 \cdot (\rho_1 + 8 \cdot k_{3,\rho} \cdot \Psi + 6 \cdot \Psi)^3 + 6 \cdot (k_{3,f}+1) \cdot (\rho_1 + 8 \cdot k_{3,\rho} \cdot \Psi + 6 \cdot \Psi)^2 + \\ +(3k_{3,f} + 6k_{2,f} + 1) \cdot (\rho_1 + 8 \cdot k_{3,\rho} \cdot \Psi + 6 \cdot \Psi) = 0 \pmod{12} \\ 2 \cdot (\rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi)^3 + (3k_{3,f}+1) \cdot (\rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi) = 0 \pmod 6 \\ 2 \cdot (\rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi)^3 + (\rho_1 + 2 \cdot k_{3,\rho} \cdot \Psi) = 0 \pmod 3. \end{cases} \tag{33}$$

By exhaustive searching by means software programs, it can be verified that equations from (33) are fulfilled if and only if $k_{3,f} = 1$ and $k_{2,f} \in \{2,4\}$, or $k_{3,f} = 3$ and $k_{2,f} \in \{1,3\}$.

For $x = 1$, equations from (20) become

$$\begin{cases} \rho(\pi(1)+2)\cdot\left(2f_4\cdot(2\rho^2(\pi(1)+2)+3\rho(\pi(1)+2)+2)+\right.\\ \left.+3f_3\cdot(\rho(\pi(1)+2)+1)+2f_2\right) = 14f_4+6f_3+2f_2 \pmod L\\ 5\cdot\rho(\pi(1)+2)\cdot\left(2f_4\cdot(2\rho^2(\pi(1)+2)+3\cdot5\cdot\rho(\pi(1)+2)+2\cdot5^2)+\right.\\ \left.+3f_3\cdot(\rho(\pi(1)+2)+5)+2f_2\right) = 5\cdot\left(134f_4+18f_3+2f_2\right) \pmod L\\ \rho(\pi(1)+4)\cdot\left(2f_4\cdot(2\rho^2(\pi(1)+4)+3\rho(\pi(1)+4)+2)+\right.\\ \left.+3f_3\cdot(\rho(\pi(1)+4)+1)+2f_2\right) = 14f_4+6f_3+2f_2 \pmod L\\ 5\cdot\rho(\pi(1)+4)\cdot\left(2f_4\cdot(2\rho^2(\pi(1)+4)+3\cdot5\cdot\rho(\pi(1)+4)+2\cdot5^2)+\right.\\ \left.+3f_3\cdot(\rho(\pi(1)+4)+5)+2f_2\right) = 5\cdot\left(134f_4+18f_3+2f_2\right) \pmod L\\ \rho(\pi(1)+8)\cdot\left(2f_4\cdot(2\rho^2(\pi(1)+8)+3\rho(\pi(1)+8)+2)+\right.\\ \left.+3f_3\cdot(\rho(\pi(1)+8)+1)+2f_2\right) = 14f_4+6f_3+2f_2 \pmod L\\ 5\cdot\rho(\pi(1)+8)\cdot\left(2f_4\cdot(2\rho^2(\pi(1)+8)+3\cdot5\cdot\rho(\pi(1)+8)+2\cdot5^2)+\right.\\ \left.+3f_3\cdot(\rho(\pi(1)+8)+5)+2f_2\right) = 5\cdot\left(134f_4+18f_3+2f_2\right) \pmod L. \end{cases} \tag{34}$$

For $L = 16\cdot k_L\cdot\Psi$, $f_4 = \Psi$, $f_3 = k_{3,f}\cdot2\Psi$, $k_{3,f}\in\{0,1,2,3\}$, $f_2 = (2k_{2,f}\cdot k_L-1)\cdot\Psi$, $k_{2,f}\in\{1,2,3,4\}$, $k_L\in\{1,3\}$, equations from (34) become

$$\begin{cases} \rho(\pi(1)+2)\cdot2\Psi\cdot\left(2\rho^2(\pi(1)+2)+3\rho(\pi(1)+2)+1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+2)+1)+2k_{2,f}k_L\right)-2\Psi\cdot\left(6+6k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{16\cdot k_L\cdot\Psi}\\ 5\cdot2\Psi\cdot\rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+3\cdot5\cdot\rho(\pi(1)+2)+2\cdot5^2-1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+2)+5)+2k_{2,f}k_L\right)-5\cdot2\Psi\cdot\left(66+18k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{16\cdot k_L\cdot\Psi}\\ \rho(\pi(1)+4)\cdot2\Psi\cdot\left(2\rho^2(\pi(1)+4)+3\rho(\pi(1)+4)+1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+4)+1)+2k_{2,f}k_L\right)-2\Psi\cdot\left(6+6k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{16\cdot k_L\cdot\Psi}\\ 5\cdot\rho(\pi(1)+4)\cdot2\Psi\cdot\left(2\rho^2(\pi(1)+4)+3\cdot5\cdot\rho(\pi(1)+4)+2\cdot5^2-1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+4)+5)+2k_{2,f}k_L\right)-5\cdot2\Psi\cdot\left(66+18k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{16\cdot k_L\cdot\Psi}\\ \rho(\pi(1)+8)\cdot2\Psi\cdot\left(2\rho^2(\pi(1)+8)+3\rho(\pi(1)+8)+1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+8)+1)+2k_{2,f}k_L\right)-2\Psi\cdot\left(6+6k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{16\cdot k_L\cdot\Psi}\\ 5\cdot\rho(\pi(1)+8)\cdot2\Psi\cdot\left(2\rho^2(\pi(1)+8)+3\cdot5\cdot\rho(\pi(1)+8)+2\cdot5^2-1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+8)+5)+2k_{2,f}k_L\right)-5\cdot2\Psi\cdot\left(66+18k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{16\cdot k_L\cdot\Psi}. \end{cases} \tag{35}$$

Equations from (35) are fulfilled if and only if

$$\begin{cases} \rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+3\rho(\pi(1)+2)+1+3k_{3,f}\cdot(\rho(\pi(1)+2)+1)+2k_{2,f}k_L\right)-\\ -\left(6+6k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{8\cdot k_L}\\ 5\cdot\rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+3\cdot5\cdot\rho(\pi(1)+2)+2\cdot5^2-1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+2)+5)+2k_{2,f}k_L\right)-5\cdot\left(66+18k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{8\cdot k_L}\\ \rho(\pi(1)+4)\cdot\left(2\rho^2(\pi(1)+4)+3\rho(\pi(1)+4)+1+3k_{3,f}\cdot(\rho(\pi(1)+4)+1)+2k_{2,f}k_L\right)-\\ -\left(6+6k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{8\cdot k_L}\\ 5\cdot\rho(\pi(1)+4)\cdot\left(2\rho^2(\pi(1)+4)+3\cdot5\cdot\rho(\pi(1)+4)+2\cdot5^2-1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+4)+5)+2k_{2,f}k_L\right)-5\cdot\left(66+18k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{8\cdot k_L}\\ \rho(\pi(1)+8)\cdot\left(2\rho^2(\pi(1)+8)+3\rho(\pi(1)+8)+1+3k_{3,f}\cdot(\rho(\pi(1)+8)+1)+2k_{2,f}k_L\right)-\\ -\left(6+6k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{8\cdot k_L}\\ 5\cdot\rho(\pi(1)+8)\cdot\left(2\rho^2(\pi(1)+8)+3\cdot5\cdot\rho(\pi(1)+8)+2\cdot5^2-1+\right.\\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+8)+5)+2k_{2,f}k_L\right)-5\cdot\left(66+18k_{3,f}+2k_{2,f}k_L\right) = 0 \pmod{8\cdot k_L}. \end{cases} \tag{36}$$

For $k_L = 1$ and $k'_{2,f} = 2k_{2,f} - 1$, equations from (36) are fulfilled if and only if

$$\begin{cases} \rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+3\rho(\pi(1)+2)+2+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+2)+1)+k'_{2,f}\right)+\left(1+2k_{3,f}+7k'_{2,f}\right)=0 \pmod 8 \\ 5\cdot\rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+7\cdot\rho(\pi(1)+2)+2+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+2)+5)+k'_{2,f}\right)+\left(1+6k_{3,f}+3k'_{2,f}\right)=0 \pmod 8 \\ \rho(\pi(1)+4)\cdot\left(2\rho^2(\pi(1)+4)+3\rho(\pi(1)+4)+2+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+4)+1)+k'_{2,f}\right)+(1+2k_{3,f}+7k'_{2,f})=0 \pmod 8 \\ 5\cdot\rho(\pi(1)+4)\cdot\left(2\rho^2(\pi(1)+4)+7\cdot\rho(\pi(1)+4)+2+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+4)+5)+k'_{2,f}\right)+\left(1+6k_{3,f}+3k'_{2,f}\right)=0 \pmod 8 \\ \rho(\pi(1)+8)\cdot\left(2\rho^2(\pi(1)+8)+3\rho(\pi(1)+8)+2+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+8)+1)+k'_{2,f}\right)+(1+2k_{3,f}+7k'_{2,f})=0 \pmod 8 \\ 5\cdot\rho(\pi(1)+8)\cdot\left(2\rho^2(\pi(1)+8)+7\cdot\rho(\pi(1)+8)+2+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+8)+5)+k'_{2,f}\right)+\left(1+6k_{3,f}+3k'_{2,f}\right)=0 \pmod 8. \end{cases} \tag{37}$$

We have

$$\begin{aligned} \rho(\pi(1)+2) \pmod 8 &= 1+\rho(2)+2\cdot\pi(1)\cdot(2\rho_4\cdot(2\pi^2(1)+2\cdot 2^2+3\cdot 2\cdot\pi(1))+ \\ &+3\rho_3\cdot(\pi(1)+2)+2\rho_2) \pmod 8 = \\ &= 1+2\cdot(\rho_1+2\rho_2)+6\rho_3\cdot(f_1+f_2+f_3+f_4)^2+(4\rho_3+4\rho_2)\cdot(f_1+f_2+f_3+f_4) \pmod 8 = \\ &= 1+2\cdot(\rho_1+2k_{2,\rho}k_\Psi)+4k_{3,\rho}k_\Psi\cdot(f_1+k'_{2,f}k_\Psi+k_\Psi)^2+4k_{2,\rho}k_\Psi\cdot(f_1+k'_{2,f}k_\Psi+k_\Psi) \pmod 8 = \\ &= 1+2\cdot(\rho_1+2k_{2,\rho}k_\Psi)+4k_{3,\rho}k_\Psi\cdot(1+(k'_{2,f})^2+1+2f_1k'_{2,f}k_\Psi+2f_1k_\Psi+2k'_{2,f})+ \\ &+4f_1k_{2,\rho}k_\Psi+4k_{2,\rho}\cdot(k'_{2,f}+1) \pmod 8 = \\ &= 1+2\rho_1+4k_{3,\rho}(k'_{2,f})^2k_\Psi+4k_{2,\rho}\cdot(k'_{2,f}+1) \pmod 8, \end{aligned} \tag{38}$$

$$\rho^2(\pi(1)+2) \pmod 8 = 5+4\rho_1 \pmod 8, \tag{39}$$

$$\rho^3(\pi(1)+2) \pmod 8 = 5+6\rho_1+4k_{3,\rho}(k'_{2,f})^2k_\Psi+4k_{2,\rho}\cdot(k'_{2,f}+1) \pmod 8, \tag{40}$$

$$\begin{aligned} \rho(\pi(1)+4) \pmod 8 &= 1+\rho(4)+4\cdot\pi(1)\cdot(2\rho_4\cdot(2\pi^2(1)+2\cdot 4^2+3\cdot 4\cdot\pi(1))+ \\ &+3\rho_3\cdot(\pi(1)+4)+2\rho_2) \pmod 8 = 1+4\rho_1 \pmod 8, \end{aligned} \tag{41}$$

$$\rho^2(\pi(1)+4) \pmod 8 = 1 \pmod 8, \tag{42}$$

$$\begin{aligned} \rho(\pi(1)+8) \pmod 8 &= 1+\rho(8)+8\cdot\pi(1)\cdot(2\rho_4\cdot(2\pi^2(1)+2\cdot 8^2+3\cdot 8\cdot\pi(1))+ \\ &+3\rho_3\cdot(\pi(1)+8)+2\rho_2) \pmod 8 = 1 \pmod 8. \end{aligned} \tag{43}$$

Thus, equations from (36) are equivalent to

$$\begin{cases} 2\rho^3(\pi(1)+2)+3\cdot(k_{3,f}+1)\cdot\rho^2(\pi(1)+2)+ \\ +(2+3k_{3,f}+k'_{2,f})\cdot\rho(\pi(1)+2)+\left(1+2k_{3,f}+7k'_{2,f}\right)=0 \pmod 8 \\ 2\rho^3(\pi(1)+2)+(7k_{3,f}+3)\cdot\rho^2(\pi(1)+2)+ \\ +(2+3k_{3,f}+k'_{2,f})\cdot\rho(\pi(1)+2)+\left(1+6k_{3,f}+3k'_{2,f}\right)=0 \pmod 8 \\ (1+4\rho_1)\cdot\left(2+3k_{3,f}+k'_{2,f}\right)+\left(6+5k_{3,f}+7k'_{2,f}\right)=0 \pmod 8 \\ (1+4\rho_1)\cdot\left(2+3k_{3,f}+5k'_{2,f}\right)+\left(6+5k_{3,f}+3k'_{2,f}\right)=0 \pmod 8 \end{cases} \tag{44}$$

or

$$\begin{cases} 2\rho^3(\pi(1)+2)+3\cdot(k_{3,f}+1)\cdot\rho^2(\pi(1)+2)+ \\ +(2+3k_{3,f}+k'_{2,f})\cdot\rho(\pi(1)+2)+\left(1+2k_{3,f}+7k'_{2,f}\right)=0 \pmod 8 \\ 2\rho^3(\pi(1)+2)+(7k_{3,f}+3)\cdot\rho^2(\pi(1)+2)+ \\ +(2+3k_{3,f}+k'_{2,f})\cdot\rho(\pi(1)+2)+\left(1+6k_{3,f}+3k'_{2,f}\right)=0 \pmod 8 \\ 4\rho_1\cdot(k_{3,f}+k'_{2,f})=0 \pmod 8. \end{cases} \tag{45}$$

The third equation from (45) is fulfilled if and only if $k_{3,f}=1$ and $k'_{2,f}\in\{1,5\}$, or $k_{3,f}=3$ and $k'_{2,f}\in\{3,7\}$. It can be verified that these values also fulfill the first two equations from (45).

For $k_L=3$, equations from (36) are fulfilled if and only if

$$\begin{cases} \rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+3\rho(\pi(1)+2)+1+3k_{3,f}\cdot(\rho(\pi(1)+2)+1)+6k_{2,f}\right)+ \\ +18\cdot\left(1+k_{3,f}+k_{2,f}\right)=0 \pmod{24} \\ 5\cdot\rho(\pi(1)+2)\cdot\left(2\rho^2(\pi(1)+2)+15\cdot\rho(\pi(1)+2)+1+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+2)+5)+6k_{2,f}\right)+6\cdot\left(1+k_{3,f}+3k_{2,f}\right)=0 \pmod{24} \\ \rho(\pi(1)+4)\cdot\left(2\rho^2(\pi(1)+4)+3\rho(\pi(1)+4)+1+3k_{3,f}\cdot(\rho(\pi(1)+4)+1)+6k_{2,f}\right)+ \\ +18\cdot(1+k_{3,f}+k_{2,f})=0 \pmod{24} \\ 5\cdot\rho(\pi(1)+4)\cdot\left(2\rho^2(\pi(1)+4)+15\cdot\rho(\pi(1)+4)+1+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+4)+5)+6k_{2,f}\right)+6\cdot\left(1+k_{3,f}+3k_{2,f}\right)=0 \pmod{24} \\ \rho(\pi(1)+8)\cdot\left(2\rho^2(\pi(1)+8)+3\rho(\pi(1)+8)+1+3k_{3,f}\cdot(\rho(\pi(1)+8)+1)+6k_{2,f}\right)+ \\ +18\cdot(1+k_{3,f}+k_{2,f})=0 \pmod{24} \\ 5\cdot\rho(\pi(1)+8)\cdot\left(2\rho^2(\pi(1)+8)+15\cdot\rho(\pi(1)+8)+1+\right. \\ \left.+3k_{3,f}\cdot(\rho(\pi(1)+8)+5)+6k_{2,f}\right)+6\cdot\left(1+k_{3,f}+3k_{2,f}\right)=0 \pmod{24}. \end{cases} \tag{46}$$

With

$$\pi(1) \pmod{24} = (f_1+6k_{2,f}k_\Psi+2k_{3,f}k_\Psi) \pmod{24}, \tag{47}$$

we have

$$\begin{aligned} \rho(\pi(1)+2) \pmod{24} &= 1+\rho(2)+2\cdot\pi(1)\cdot(2\rho_4\cdot(2\pi^2(1)+2\cdot2^2+3\cdot2\cdot\pi(1))+ \\ &+3\rho_3\cdot(\pi(1)+2)+2\rho_2) \pmod{24} = \\ &= 1+2\cdot(\rho_1+2\rho_2+4\rho_3+8\rho_4)+8\rho_4\cdot\pi^3(1)+6\rho_3\pi^2(1)+(8\rho_4+12\rho_3+4\rho_2)\cdot\pi(1) = \\ &= 1+2\rho_1+16k_{3,\rho}k_\Psi+12k_\Psi+8k_\Psi\cdot\pi^3(1)+12k_{3,\rho}k_\Psi\cdot\pi^2(1)+4k_\Psi\cdot(f_1+2k_{3,f}k_\Psi) \pmod{24}, \end{aligned} \tag{48}$$

$$\begin{aligned} \rho^2(\pi(1)+2) \pmod{24} &= 1+4\rho_1\cdot(\rho_1+1)+8k_{3,\rho}k_\Psi\cdot(2k_{3,\rho}k_\Psi+2\rho_1+1)+ \\ &+16k_{3,\rho}^2\cdot\pi^6(1)+16k_\Psi\cdot\pi^4(1)+8k_\Psi\cdot(2+\rho_1+2k_{3,\rho}k_\Psi)\cdot\pi^3(1)+16k_\Psi\cdot\pi^2(1)+ \\ &+8k_\Psi\cdot(1+2\rho_1+k_{3,\rho}k_\Psi)\cdot(f_1+2k_{3,f}k_\Psi) \pmod{24}, \end{aligned} \tag{49}$$

$$\rho^3(\pi(1)+2) \pmod{24} = 1+2\rho_1\cdot(4\rho_1^2+6\rho_1+3)+4k_\Psi\cdot(4k_{3,\rho}^3k_\Psi^2+3)+$$

$$+8k_{\Psi}^{3}\cdot\pi^{9}(1)+16k_{\Psi}^{3}\cdot\pi^{3}(1)+12k_{3,\rho}k_{\Psi}\cdot\pi^{2}(1)+12k_{\Psi}f_{1}\ (\mathrm{mod}\ 24), \tag{50}$$

$$\begin{gathered}\rho(\pi(1)+4)\ (\mathrm{mod}\ 24)=1+\rho(4)+4\cdot\pi(1)\cdot(2\rho_{4}\cdot(2\pi^{2}(1)+2\cdot4^{2}+3\cdot4\cdot\pi(1))+\\+3\rho_{3}\cdot(\pi(1)+4)+2\rho_{2})\ (\mathrm{mod}\ 24)=\\=1+\rho(4)+16\rho_{4}\cdot\pi^{3}(1)+12\rho_{3}\cdot\pi^{2}(1)+(16\rho_{4}+8\rho_{2})\cdot\pi(1)\ (\mathrm{mod}\ 24)=\\=1+4\cdot(\rho_{1}+4\rho_{2}+16\rho_{3}+16\rho_{4})+16\rho_{4}\cdot(f_{1}+f_{2}+f_{3}+f_{4})^{3}+12\rho_{3}\cdot(f_{1}+f_{2}+f_{3}+f_{4})^{2}+\\+(16\rho_{4}+8\rho_{2})\cdot(f_{1}+f_{2}+f_{3}+f_{4})\ (\mathrm{mod}\ 24)=\\=1+4\cdot(\rho_{1}+8k_{3,\rho}k_{\Psi})+16k_{\Psi}\cdot(f_{1}+6k_{2,f}k_{\Psi}+2k_{3,f}k_{\Psi})^{3}+\\+8k_{\Psi}\cdot(f_{1}+2k_{3,f}k_{\Psi})\ (\mathrm{mod}\ 24),\end{gathered} \tag{51}$$

$$\begin{gathered}\rho^{2}(\pi(1)+4)\ (\mathrm{mod}\ 24)=1+8\rho_{1}\cdot(2\rho_{1}+1)+16k_{3,\rho}k_{\Psi}\cdot(k_{3,\rho}k_{\Psi}+\rho_{1}+1)+\\+16k_{3,\rho}^{2}\cdot\pi^{6}(1)+16k_{\Psi}^{2}\cdot\pi^{4}(1)+8k_{\Psi}\cdot(1+\rho_{1}+2k_{3,\rho}k_{\Psi})\cdot\pi^{3}(1)+16k_{\Psi}^{2}\cdot\pi^{2}(1)+\\+8k_{\Psi}\cdot(2+2\rho_{1}+k_{3,\rho}k_{\Psi})\cdot(f_{1}+2k_{3,f}k_{\Psi})\mod 24),\end{gathered} \tag{52}$$

$$\rho^{3}(\pi(1)+4)\ (\mathrm{mod}\ 24)=1+4\rho_{1}\cdot(4\rho_{1}^{2}+3)+8k_{\Psi}^{3}k_{3,\rho}^{3}+16k_{\Psi}^{3}\cdot\pi^{9}(1)+8k_{\Psi}^{3}\cdot\pi^{3}(1)\ (\mathrm{mod}\ 24), \tag{53}$$

$$\begin{gathered}\rho(\pi(1)+8)\ (\mathrm{mod}\ 24)=1+\rho(8)+8\cdot\pi(1)\cdot(2\rho_{4}\cdot(2\pi^{2}(1)+2\cdot8^{2}+3\cdot8\cdot\pi(1))+\\+3\rho_{3}\cdot(\pi(1)+8)+2\rho_{2})\ (\mathrm{mod}\ 24)=1+\rho(8)+8\rho_{4}\cdot\pi^{3}(1)+8\cdot(2\rho_{2}+\rho_{4})\cdot\pi(1)=\\=1+8\cdot(\rho_{1}+2k_{3,\rho}k_{\Psi})+8k_{\Psi}\cdot(f_{1}+6k_{2,f}k_{\Psi}+2k_{3,f}k_{\Psi})^{3}+\\+16k_{\Psi}\cdot(f_{1}+2k_{3,f}k_{\Psi})\ (\mathrm{mod}\ 24),\end{gathered} \tag{54}$$

$$\begin{gathered}\rho^{2}(\pi(1)+4)\ (\mathrm{mod}\ 24)=1+16\rho_{1}\cdot(\rho_{1}+1)+8k_{3,\rho}k_{\Psi}\cdot(2k_{3,\rho}k_{\Psi}+2\rho_{1}+1)+\\+16k_{3,\rho}^{2}\cdot\pi^{6}(1)+16k_{\Psi}^{2}\cdot\pi^{4}(1)+8k_{\Psi}\cdot(2+\rho_{1}+2k_{3,\rho}k_{\Psi})\cdot\pi^{3}(1)+16k_{\Psi}^{2}\cdot\pi^{2}(1)+\\+8k_{\Psi}\cdot(1+2\rho_{1}+k_{3,\rho}k_{\Psi})\cdot(f_{1}+2k_{3,f}k_{\Psi})\mod 24),\end{gathered} \tag{55}$$

$$\rho^{3}(\pi(1)+8)\ (\mathrm{mod}\ 24)=1+8\rho_{1}^{3}+16k_{\Psi}^{3}k_{3,\rho}^{3}+8k_{\Psi}^{3}\cdot\pi^{9}(1)+16k_{\Psi}^{3}\cdot\pi^{3}(1)\ (\mathrm{mod}\ 24). \tag{56}$$

Taking into account Equations (47)–(56), it can be verified, by exhaustive searching by means of Matlab that equations from system (46) are fulfilled if and only if $k_{3,f}=1$ and $k_{2,f}\in\{1,3\}$, or $k_{3,f}=3$ and $k_{2,f}\in\{2,4\}$.

From solutions of (28), (33), (45), and (46), it results that the interleaver pattern from Figure 1 always appears for $x_1=0$ or $x_1=1$, when $k_{3,f}\in\{1,3\}$ and $k_{2,f}\in\{1,2,3,4\}$. For an interleaver pattern as in Figure 1, the weight of the codeword for classical nominal $1/3$ rate turbo codes with two RSC codes having generator matrix $G=[1,15/13]$, is equal to $12+4\cdot3+3\cdot4=36$, because each of the four error patterns with a weight of three leads to a parity weight of three, and each of the three error patterns with a weight of four leads to a parity weight of four. Because the interleaver pattern

from Figure 1 always appears in the previous conditions, it results that the minimum distance is upper bounded by the value of 36. □

Theorem 2. *Let the interleaver length be of the form given in* (5)*. Then, the minimum distance of the classical nominal 1/3 rate turbo code—with two RSC codes concatenated in parallel, having the generator matrix* $G = [1, 15/13]$ *(in octal form), 4-PP interleavers, and fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, with coefficients* $f_4 = \Psi$*,* $f_3 = k_{3,f} \cdot 2\Psi$*,* $f_2 = (2k_{2,f} \cdot k_L - 1) \cdot \Psi$*,* $k_L \in \{1, 3\}$*, when* $k_{3,f} \in \{0, 2\}$ *and* $k_{2,f} \in \{1, 2, 3, 4\}$ *or when* $k_{3,f} \in \{1, 3\}$ *and* $k_{2,f} \in \{2, 4\}$*—is upper bounded by the value of 28.*

Proof. We consider the interleaver patterns of size four shown in Figures 2 and 3.

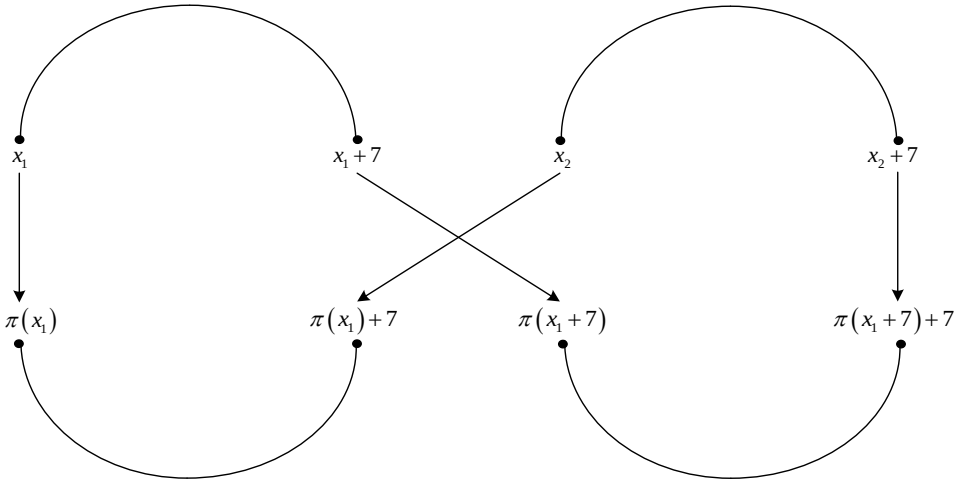

Figure 2. Critical interleaver pattern of size four for 4-PP-based interleavers.

The four elements of permutation $\pi(\cdot)$ indicated in Figure 2 are written in detail below.

$$\begin{cases} x_1 \to \pi(x_1) \\ x_1 + 7 \to \pi(x_1 + 7) \pmod{L} \\ x_2 \to \pi(x_2) = \pi(x_1) + 7 \pmod{L} \\ x_2 + 7 \to \pi(x_2 + 7) = \pi(x_1 + 7) + 7 \pmod{L}. \end{cases} \tag{57}$$

Writing $x_2 = \rho(\pi(x_2)) = \rho(\pi(x_1) + 7)$ in the fourth equation from (57), with $x_1 = x$, we have

$$\pi(\rho(\pi(x) + 7) + 7) = \pi(x + 7) + 7 \pmod{L}. \tag{58}$$

Equation (58) is equivalent to

$$\begin{aligned} 7 \cdot \rho(\pi(x) + 7) \cdot \left(2f_4 \cdot (2\rho^2(\pi(x) + 7) + 3 \cdot 7 \cdot \rho(\pi(x) + 7) + 2 \cdot 7^2) + 3f_3 \cdot (\rho(\pi(x) + 7) + 7) + 2f_2\right) = \\ = 7 \cdot x \cdot \left(2f_4 \cdot (2x^2 + 3 \cdot 7 \cdot x + 2 \cdot 7^2) + 3f_3 \cdot (x + 7) + 2f_2\right) \pmod{L} \end{aligned} \tag{59}$$

or

$$\begin{aligned} 28f_4 \cdot \rho^3(\pi(x) + 7) + (294f_4 + 21f_3) \cdot \rho^2(\pi(x) + 7) + (1372f_4 + 147f_3 + 14f_2) \cdot \rho(\pi(x) + 7) = \\ = 14x \cdot (2x^2 + 21x + 98) \cdot f_4 + 21x \cdot (x + 7) \cdot f_3 + 14x \cdot f_2 \pmod{L}. \end{aligned} \tag{60}$$

For $L = 16 \cdot k_L \cdot \Psi$, $f_4 = \Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, $k_{3,f} \in \{0, 1, 2, 3\}$, $f_2 = (2k_{2,f} \cdot k_L - 1) \cdot \Psi$, $k_{2,f} \in \{1, 2, 3, 4\}$, $k_L \in \{1, 3\}$, Equation (60) becomes

$$14 \cdot 2\Psi \cdot \rho^3(\pi(x) + 7) + 2\Psi \cdot (147 + 21k_{3,f}) \cdot \rho^2(\pi(x) + 7) +$$

$$+2\Psi\cdot(686+147k_{3,f}+7\cdot(2k_{2,f}\cdot k_L-1))\cdot\rho(\pi(x)+7)=$$
$$=7x\cdot(2x^2+21x+98)\cdot 2\Psi+21x\cdot(x+7)\cdot k_{3,f}\cdot 2\Psi+$$
$$+7x\cdot(2k_{2,f}\cdot k_L-1)\cdot 2\Psi\ (\mathrm{mod}\ 16\cdot k_L\cdot\Psi). \tag{61}$$

Equation (61) is fulfilled if and only if

$$14\cdot\rho^3(\pi(x)+7)+(147+21k_{3,f})\cdot\rho^2(\pi(x)+7)+$$
$$+(686+147k_{3,f}+7\cdot(2k_{2,f}\cdot k_L-1))\cdot\rho(\pi(x)+7)=$$
$$=7x\cdot(2x^2+21x+98)+21x\cdot(x+7)\cdot k_{3,f}+7x\cdot(2k_{2,f}\cdot k_L-1)\ (\mathrm{mod}\ 8\cdot k_L), \tag{62}$$

where

$$\rho(\pi(x)+7)\ (\mathrm{mod}\ 8\cdot k_L)=x+\rho(7)+7\cdot\pi(x)\cdot(2\rho_4\cdot(2\pi^2(x)+2\cdot 7^2+3\cdot 7\cdot\pi(x))+$$
$$+3\rho_3\cdot(\pi(x)+7)+2\rho_2)\ (\mathrm{mod}\ 8\cdot k_L)=x+\rho(7)+28\rho_4\cdot\pi^3(x)+$$
$$+21\cdot(14\rho_4+\rho_3)\cdot\pi^2(x)+7\cdot(196\rho_4+21\rho_3+2\rho_2)\cdot\pi(x)\ (\mathrm{mod}\ 8\cdot k_L). \tag{63}$$

For $x=0$, $x=1$, and $x=3$, Equation (62) becomes

$$14\cdot\rho^3(7)+(147+21k_{3,f})\cdot\rho^2(7)+$$
$$+(686+147k_{3,f}+7\cdot(2k_{2,f}\cdot k_L-1))\cdot\rho(7)=0\ (\mathrm{mod}\ 8\cdot k_L), \tag{64}$$
$$14\cdot\rho^3(\pi(1)+7)+(147+21k_{3,f})\cdot\rho^2(\pi(1)+7)+$$
$$+(686+147k_{3,f}+7\cdot(2k_{2,f}\cdot k_L-1))\cdot\rho(\pi(1)+7)=$$
$$=847+168\cdot k_{3,f}+7\cdot(2k_{2,f}\cdot k_L-1)\ (\mathrm{mod}\ 8\cdot k_L), \tag{65}$$

and

$$14\cdot\rho^3(\pi(3)+7)+(147+21k_{3,f})\cdot\rho^2(\pi(3)+7)+$$
$$+(686+147k_{3,f}+7\cdot(2k_{2,f}\cdot k_L-1))\cdot\rho(\pi(3)+7)=$$
$$=3759+630\cdot k_{3,f}+21\cdot(2k_{2,f}\cdot k_L-1)\ (\mathrm{mod}\ 8\cdot k_L), \tag{66}$$

respectively.

For $k_L=1$, $k'_{2,f}=2k_{2,f}-1$ and $k'_{2,\rho}=2k_{2,\rho}-1$, Equation (63) becomes

$$\rho(\pi(x)+7)\ (\mathrm{mod}\ 8)=x+\rho(7)+4\rho_4\cdot\pi^3(x)+(6\rho_4+5\rho_3)\cdot\pi^2(x)+(4\rho_4+3\rho_3+6\rho_2)\cdot\pi(x)\ (\mathrm{mod}\ 8)=$$
$$=x+7\rho_1+k_\Psi\cdot(6k_{3,\rho}+k'_{2,\rho}+1)+4k_\Psi\cdot\pi^3(x)+$$
$$+2k_\Psi\cdot(k_{3,\rho}+3)\cdot\pi^2(x)+2k_\Psi\cdot(3k_{3,\rho}+3k'_{2,\rho}+2)\cdot\pi(x)\ (\mathrm{mod}\ 8), \tag{67}$$

and Equations (64)–(66) become

$$6\cdot\rho^3(7)+(5k_{3,f}+3)\cdot\rho^2(7)+(3k_{3,f}+7k'_{2,f}+6)\cdot\rho(7)=0\ (\mathrm{mod}\ 8), \tag{68}$$

where

$$\rho(7)\ (\mathrm{mod}\ 8)=7\rho_1+k_\Psi\cdot(6k_{3,\rho}+k'_{2,\rho}+1)\ (\mathrm{mod}\ 8), \tag{69}$$

$$6\cdot\rho^3(\pi(1)+7)+(5k_{3,f}+3)\cdot\rho^2(\pi(1)+7)+$$
$$+(3k_{3,f}+7k'_{2,f}+6)\cdot\rho(\pi(1)+7)+k'_{2,f}+1=0\ (\mathrm{mod}\ 8), \tag{70}$$

where

$$\rho(\pi(1)+7) \pmod 8 = 1+7\rho_1+k_\Psi\cdot(6k_{3,\rho}+k'_{2,\rho}+1)+$$
$$+4k_\Psi\cdot(f_1+k'_{2,f}k_\Psi+k_{3,f}\cdot 2k_\Psi+k_\Psi)^3+2k_\Psi\cdot(k_{3,\rho}+3)\cdot(f_1+k'_{2,f}k_\Psi+k_{3,f}\cdot 2k_\Psi+k_\Psi)^2+$$
$$+2k_\Psi\cdot(3k_{3,\rho}+3k'_{2,\rho}+2)\cdot(f_1+k'_{2,f}k_\Psi+k_{3,f}\cdot 2k_\Psi+k_\Psi) \pmod 8, \quad (71)$$

and

$$6\cdot\rho^3(\pi(3)+7)+(5k_{3,f}+3)\cdot\rho^2(\pi(3)+7)+$$
$$+(3k_{3,f}+7k'_{2,f}+6)\cdot\rho(\pi(3)+7)+2k_{3,f}+3k'_{2,f}+1=0 \pmod 8, \quad (72)$$

where

$$\rho(\pi(3)+7) \pmod 8 = 3+7\rho_1+k_\Psi\cdot(6k_{3,\rho}+k'_{2,\rho}+1)+$$
$$+4k_\Psi\cdot(3f_1+k'_{2,f}k_\Psi+6k_{3,f}k_\Psi+k_\Psi)^3+2k_\Psi\cdot(k_{3,\rho}+3)\cdot(3f_1+k'_{2,f}k_\Psi+6k_{3,f}k_\Psi+k_\Psi)^2+$$
$$+2k_\Psi\cdot(3k_{3,\rho}+3k'_{2,\rho}+2)\cdot(3f_1+k'_{2,f}k_\Psi+6k_{3,f}k_\Psi+k_\Psi) \pmod 8, \quad (73)$$

respectively.

For $k_L=3$, Equation (63) becomes

$$\rho(\pi(x)+7) \pmod{24} = x+\rho(7)+4\rho_4\cdot\pi^3(x)+3\cdot(2\rho_4+7\rho_3)\cdot\pi^2(x)+$$
$$+(4\rho_4+3\rho_3+14\rho_2)\cdot\pi(x) \pmod{24} =$$
$$=x+7\rho_1+2k_\Psi\cdot(7k_{3,\rho}+3k_{2,\rho})+4k_\Psi\cdot\pi^3(x)+6k_\Psi\cdot(7k_{3,\rho}+1)\cdot\pi^2(x)+$$
$$+2k_\Psi\cdot(3k_{3,\rho}+6k_{2,\rho}+7)\cdot\pi(x) \pmod{24} \quad (74)$$

and Equations (64)–(66) become

$$14\cdot\rho^3(7)+3\cdot(7k_{3,f}+1)\cdot\rho^2(7)+(3k_{3,f}+18k_{2,f}+7)\cdot\rho(7)=0 \pmod{24}, \quad (75)$$

where

$$\rho(7) \pmod{24} = 7\rho_1+2k_\Psi\cdot(7k_{3,\rho}+3k_{2,\rho}) \pmod{24}, \quad (76)$$

$$14\cdot\rho^3(\pi(1)+7)+3\cdot(7k_{3,f}+1)\cdot\rho^2(\pi(1)+7)+$$
$$+(3k_{3,f}+18k_2+7)\cdot\rho(\pi(1)+7)+6k_{2,f}=0 \pmod{24}, \quad (77)$$

where

$$\rho(\pi(1)+7) \pmod{24} = 1+7\rho_1+2k_\Psi\cdot(7k_{3,\rho}+3k_{2,\rho})+$$
$$+4k_\Psi\cdot(f_1+6k_{2,f}k_\Psi+2k_{3,f}k_\Psi)^3+6k_\Psi\cdot(7k_{3,\rho}+1)\cdot(f_1+6k_{2,f}k_\Psi+2k_{3,f}k_\Psi)^2+$$
$$+2k_\Psi\cdot(3k_{3,\rho}+6k_{2,\rho}+7)\cdot(f_1+6k_{2,f}k_\Psi+2k_{3,f}k_\Psi) \pmod{24}, \quad (78)$$

and

$$14\cdot\rho^3(\pi(3)+7)+3\cdot(7k_{3,f}+1)\cdot\rho^2(\pi(3)+7)+$$
$$+(3k_{3,f}+18k_2+7)\cdot\rho(\pi(3)+7)+6\cdot(3k_{3,f}+3k_{2,f}+1)=0 \pmod{24}, \quad (79)$$

where

$$\rho(\pi(3)+7) \pmod{24} = 3+7\rho_1+2k_\Psi\cdot(7k_{3,\rho}+3k_{2,\rho})+$$
$$+4k_\Psi\cdot(3f_1+6k_{2,f}k_\Psi+6k_{3,f}k_\Psi)^3+6k_\Psi\cdot(7k_{3,\rho}+1)\cdot(3f_1+6k_{2,f}k_\Psi+6k_{3,f}k_\Psi)^2+$$
$$+2k_\Psi\cdot(3k_{3,\rho}+6k_{2,\rho}+7)\cdot(3f_1+6k_{2,f}k_\Psi+6k_{3,f}k_\Psi) \pmod{24}, \quad (80)$$

respectively.

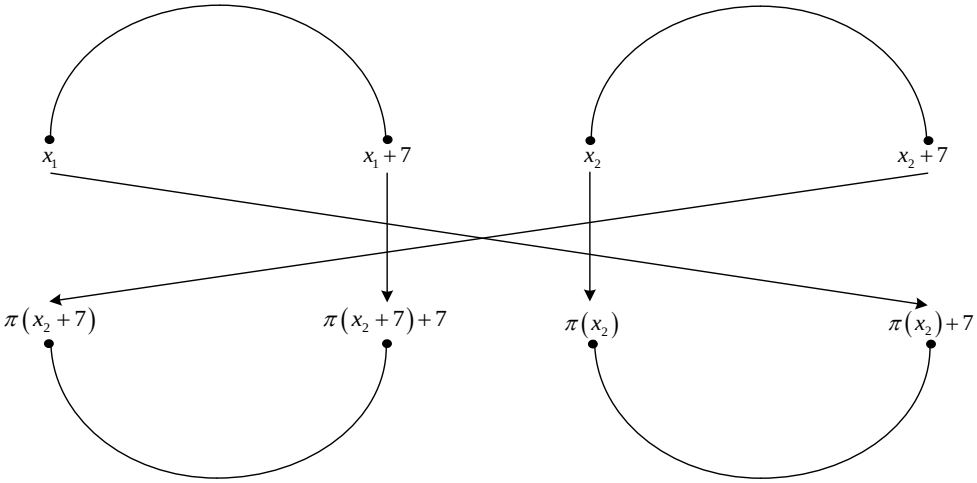

Figure 3. Critical interleaver pattern of size four for 4-PP-based interleavers.

The four elements of permutation $\pi(\cdot)$ indicated in Figure 3 are written in detail below

$$\begin{cases} x_2 \to \pi(x_2) \\ x_2+7 \to \pi(x_2+7) \pmod{L} \\ x_1 \to \pi(x_1) = \pi(x_2)+7 \pmod{L} \\ x_1+7 \to \pi(x_1+7) = \pi(x_2+7)+7 \pmod{L}. \end{cases} \tag{81}$$

Writing $x_2 = \rho(\pi(x_2)) = \rho(\pi(x_1)-7)$ in the fourth equation from (81), with $x_1 = x$, we have

$$\pi(\rho(\pi(x)-7)+7) = \pi(x+7)-7 \pmod{L}. \tag{82}$$

For $L = 16 \cdot k_L \cdot \Psi$, $f_4 = \Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, $k_{3,f} \in \{0,1,2,3\}$, $f_2 = (2k_{2,f} \cdot k_L - 1) \cdot \Psi$, $k_{2,f} \in \{1,2,3,4\}$, $k_L \in \{1,3\}$, Equation (82) is fulfilled if and only if

$$\begin{aligned} &14 \cdot \rho^3(\pi(x)-7) + (147+21k_{3,f}) \cdot \rho^2(\pi(x)-7) + \\ &+(686+147k_{3,f}+7 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(\pi(x)-7) = \\ &= 7x \cdot (2x^2+21x+98) + 21x \cdot (x+7) \cdot k_{3,f} + 7x \cdot (2k_{2,f} \cdot k_L - 1) \pmod{8 \cdot k_L}, \end{aligned} \tag{83}$$

where

$$\begin{aligned} &\rho(\pi(x)-7) \pmod{8 \cdot k_L} = x + \rho(-7) - 7 \cdot \pi(x) \cdot (2\rho_4 \cdot (2\pi^2(x) + 2 \cdot 7^2 - 3 \cdot 7 \cdot \pi(x)) + \\ &+3\rho_3 \cdot (\pi(x)-7) + 2\rho_2) \pmod{8 \cdot k_L} = x + \rho(-7) - 28\rho_4 \cdot \pi^3(x) + 21 \cdot (14\rho_4 - \rho_3) \cdot \pi^2(x) + \\ &- 7 \cdot (196\rho_4 - 21\rho_3 + 2\rho_2) \cdot \pi(x) \pmod{8 \cdot k_L}. \end{aligned} \tag{84}$$

For $x = 0$, $x = 1$, and $x = 3$, Equation (84) becomes

$$\begin{aligned} &14 \cdot \rho^3(-7) + (147+21k_{3,f}) \cdot \rho^2(-7) + \\ &+ (686+147k_{3,f}+7 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(-7) = 0 \pmod{8 \cdot k_L}, \end{aligned} \tag{85}$$

$$\begin{aligned} &14 \cdot \rho^3(\pi(1)-7) + (147+21k_{3,f}) \cdot \rho^2(\pi(1)-7) + \\ &+(686+147k_{3,f}+7 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(\pi(1)-7) = \\ &= 847+168 \cdot k_{3,f}+7 \cdot (2k_{2,f} \cdot k_L - 1) \pmod{8 \cdot k_L}, \end{aligned} \tag{86}$$

and

$$14 \cdot \rho^3(\pi(3)-7) + (147 + 21k_{3,f}) \cdot \rho^2(\pi(3)-7) +$$
$$+(686 + 147k_{3,f} + 7 \cdot (2k_{2,f} \cdot k_L - 1)) \cdot \rho(\pi(3)-7) =$$
$$= 3759 + 630 \cdot k_{3,f} + 21 \cdot (2k_{2,f} \cdot k_L - 1) \pmod{8 \cdot k_L}, \quad (87)$$

respectively.

For $k_L = 1$, $k'_{2,f} = 2k_{2,f} - 1$, and $k'_{2,\rho} = 2k_{2,\rho} - 1$, Equation (84) becomes

$$\rho(\pi(x)-7) \pmod 8 = x + \rho(1) + 4\rho_4 \cdot \pi^3(x) + 3 \cdot (2\rho_4 + \rho_3) \cdot \pi^2(x) +$$
$$+(4\rho_4 + 3\rho_3 + 2\rho_2) \cdot \pi(x) \pmod 8 =$$
$$= x + \rho_1 + k_\Psi \cdot (2k_{3,\rho} + k'_{2,\rho} + 1) + 4k_\Psi \cdot \pi^3(x) + 6k_\Psi \cdot (k_{3,\rho} + 1) \cdot \pi^2(x) +$$
$$+ 2k_\Psi \cdot (3k_{3,\rho} + k'_{2,\rho} + 2) \cdot \pi(x) \pmod 8, \quad (88)$$

and Equations (85)–(87) become

$$6 \cdot \rho^3(1) + (5k_{3,f} + 3) \cdot \rho^2(1) + (3k_{3,f} + 7 \cdot k'_{2,f} + 6) \cdot \rho(1) = 0 \pmod 8, \quad (89)$$

where

$$\rho(1) \pmod 8 = \rho_1 + k_\Psi \cdot (2k_{3,\rho} + k_{2,\rho} + 1) \pmod 8, \quad (90)$$

$$6 \cdot \rho^3(\pi(1)-7) + (5k_{3,f} + 3) \cdot \rho^2(\pi(1)-7) +$$
$$+ (3k_{3,f} + 7 \cdot k'_{2,f} + 6) \cdot \rho(\pi(1)-7) + k'_{2,f} + 1 = 0 \pmod 8, \quad (91)$$

where

$$\rho(\pi(1)-7) \pmod 8 = 1 + \rho_1 + k_{2,\rho}k_\Psi + k_{3,\rho} \cdot 2k_\Psi + k_\Psi + 4k_\Psi \cdot (f_1 + k'_{2,f}k_\Psi + k_{3,f} \cdot 2k_\Psi + k_\Psi)^3 +$$
$$+6k_\Psi \cdot (k_{3,\rho} + 1) \cdot (f_1 + k'_{2,f}k_\Psi + k_{3,f} \cdot 2k_\Psi + k_\Psi)^2 +$$
$$+ 2k_\Psi \cdot (3k_{3,\rho} + k_{2,\rho} + 2) \cdot (f_1 + k'_{2,f}k_\Psi + k_{3,f} \cdot 2k_\Psi + k_\Psi) \pmod 8, \quad (92)$$

and

$$6 \cdot \rho^3(\pi(3)-7) + (5k_{3,f} + 3) \cdot \rho^2(\pi(3)-7) + (3k_{3,f} + 7 \cdot k'_{2,f} + 6) \cdot \rho(\pi(3)-7) +$$
$$+ 2k_{3,f} + 3k'_{2,f} + 1 = 0 \pmod 8, \quad (93)$$

where

$$\rho(\pi(3)-7) \pmod 8 = 3 + \rho_1 + k_\Psi \cdot (2k_{3,\rho} + k_{2,\rho} + 1) + 4k_\Psi \cdot (f_1 + 3k'_{2,f}k_\Psi + k_{3,f} \cdot 2k_\Psi + 3k_\Psi)^3 +$$
$$+6k_\Psi \cdot (k_{3,\rho} + 1) \cdot (f_1 + 3k'_{2,f}k_\Psi + k_{3,f} \cdot 2k_\Psi + 3k_\Psi)^2 +$$
$$+ 2k_\Psi \cdot (3k_{3,\rho} + k_{2,\rho} + 2) \cdot (f_1 + 3k'_{2,f}k_\Psi + k_{3,f} \cdot 2k_\Psi + 3k_\Psi) \pmod 8, \quad (94)$$

respectively.

For $k_L = 3$, Equation (84) becomes

$$\rho(\pi(x)-7) \pmod{24} = x + \rho(-7) + 20\rho_4 \cdot \pi^3(x) + 3 \cdot (2\rho_4 + \rho_3) \cdot \pi^2(x) +$$
$$+(20\rho_4 + 3\rho_3 + 10\rho_2) \cdot \pi(x) \pmod{24} = x + 17 \cdot (\rho_1 + 6k_{2,\rho}k_\Psi + 10k_{3,\rho}k_\Psi) +$$
$$+ 20k_\Psi \cdot \pi^3(x) + 6k_\Psi \cdot (k_{3,\rho} + 1) \cdot \pi^2(x) + 2k_\Psi \cdot (3k_{3,\rho} + 6k_{2,\rho} + 5) \cdot \pi(x) \pmod{24}, \quad (95)$$

and Equations (85)–(87) become

$$14 \cdot \rho^3(-7) + 3 \cdot (7k_{3,f} + 1) \cdot \rho^2(-7) + \\ + (3k_{3,f} + 18k_{2,f} + 7) \cdot \rho(-7) = 0 \pmod{24}, \tag{96}$$

where

$$\rho(-7) \pmod{24} = 17 \cdot (\rho_1 + 6k_{2,\rho}k_\Psi + 10k_{3,\rho}k_\Psi) \pmod{24}, \tag{97}$$

$$14 \cdot \rho^3(\pi(1) - 7) + 3 \cdot (7k_{3,f} + 1) \cdot \rho^2(\pi(1) - 7) + \\ + (3k_{3,f} + 18k_{2,f} + 7) \cdot \rho(\pi(1) - 7) + 6k_{2,f} = 0 \pmod{24}, \tag{98}$$

where

$$\rho(\pi(1) - 7) \pmod{24} = 1 + 17 \cdot (\rho_1 + 6k_{2,\rho}k_\Psi + 10k_{3,\rho}k_\Psi) + \\ + 20k_\Psi \cdot (f_1 + 6k_{2,f}k_\Psi + 2k_{3,f}k_\Psi)^3 + 6k_\Psi \cdot (k_{3,\rho} + 1) \cdot (f_1 + 6k_{2,f}k_\Psi + 2k_{3,f}k_\Psi)^2 + \\ + 2k_\Psi \cdot (3k_{3,\rho} + 6k_{2,\rho} + 5) \cdot (f_1 + 6k_{2,f}k_\Psi + 2k_{3,f}k_\Psi) \pmod{24}, \tag{99}$$

and

$$14 \cdot \rho^3(\pi(3) - 7) + 3 \cdot (7k_{3,f} + 1) \cdot \rho^2(\pi(3) - 7) + \\ + (3k_{3,f} + 18k_{2,f} + 7) \cdot \rho(\pi(3) - 7) + 6 \cdot (3k_{3,f} + 3k_{2,f} + 1) = 0 \pmod{24}, \tag{100}$$

where

$$\rho(\pi(3) - 7) \pmod{24} = 3 + 17 \cdot (\rho_1 + 6k_{2,\rho}k_\Psi + 10k_{3,\rho}k_\Psi) + \\ + 12k_\Psi \cdot (f_1 + 2k_{2,f}k_\Psi + 2k_{3,f}k_\Psi)^3 + 6k_\Psi \cdot (k_{3,\rho} + 1) \cdot (f_1 + 2k_{2,f}k_\Psi + 2k_{3,f}k_\Psi)^2 + \\ + 6k_\Psi \cdot (3k_{3,\rho} + 6k_{2,\rho} + 5) \cdot (f_1 + 2k_{2,f}k_\Psi + 2k_{3,f}k_\Psi) \pmod{24}, \tag{101}$$

respectively.

Solutions of Equations (68), (70), (72), (89), (91), and (93) for variables $k_{3,f}$, $k'_{2,f}$, and $f_1 \pmod 8$, which fulfill the results from Lemma 2, are given in Tables 9 and 10. It can be observed that they can be summarized as in Table 11.

Table 9. Solutions of Equations (68), (70), (72), (89), (91), and (93) for $k_{3,f} \in \{0,2\}$.

Equation	k_Ψ	$k_{3,f}$	$k'_{2,f}$	$f_1 \pmod 8$
(68)	1	0	1 or 5	3
		0	3 or 7	7
		2	1 or 3 or 5 or 7	3
	3	0	1 or 3 or 5 or 7	7
		2	1 or 5	7
		2	3 or 7	3
(70)	1	0	1 or 5	5
		0	3 or 7	1
		2	1 or 3 or 5 or 7	5
	3	0	1 or 3 or 5 or 7	1
		2	1 or 5	1
		2	3 or 7	5
(89)	1	0	1 or 3 or 5 or 7	1
		2	1 or 5	1
		2	3 or 7	5
	3	0	1 or 5	5
		0	3 or 7	1
		2	1 or 3 or 5 or 7	5
(91)	1	0	1 or 3 or 5 or 7	7
		2	1 or 5	7
		2	3 or 7	3
	3	0	1 or 5	3
		0	3 or 7	7
		2	1 or 3 or 5 or 7	3
(93)	1	0	1 or 3 or 5 or 7	3
		2	1 or 5	3
		2	3 or 7	7
	3	0	1 or 5	7
		0	3 or 7	3
		2	1 or 3 or 5 or 7	1

Table 10. Solutions of Equations (68), (70), (72), (89), (91), and (93) for $k_{3,f} \in \{1,3\}$.

Equation	k_Ψ	$k_{3,f}$	$k'_{2,f}$	$f_1 \pmod 8$
(68)	1 or 3	1	7	1 or 3 or 5 or 7
		3	3	3 or 7
		3	7	1 or 5
(70)	1 or 3	1	3	1 or 5
		1	7	3 or 7
		3	7	1 or 3 or 5 or 7
(89)	1 or 3	1	7	1 or 3 or 5 or 7
		3	3	1 or 5
		3	7	3 or 7
(91)	1 or 3	1	3	3 or 7
		1	7	1 or 5
		3	7	1 or 3 or 5 or 7
(93)	1 or 3	1	3	1 or 5
		1	7	3 or 7
		3	3	1 or 3 or 5 or 7

Table 11. Solutions of Equations (68), (70), (72), (89), (91), and (93) summarized from Tables 9 and 10.

$k_{3,f}$	$k'_{2,f}$	$f_1 \pmod 8$
0 or 2	1 or 3 or 5 or 7	1 or 3 or 5 or 7
1 or 3	3 or 7	1 or 3 or 5 or 7

Solutions of equations (75), (77), (79), (96), (98), and (100) in variables $k_{3,f}$, $k_{2,f}$, $f_1 \pmod{48}$, which fulfill the results from Lemma 2, are given in Tables 12 and 13. It can be observed that they can be summarized as in Table 14.

Table 12. Solutions of Equations (75), (77), and (79).

Equation	$k_\Psi \in$	$k_{3,f}$	$k_{2,f}$	$f_1 \pmod{48} \in$
(75)	$\{1,5,7,11\}$	0	1 or 3	$\{11,19\}$ for $k_\Psi \in \{1,5\}$, $\{7,23\}$ for $k_\Psi \in \{7,11\}$
			2 or 4	$\{7,23\}$
		1	4	$\{3,5,9,11,15,17,21,23\}$ for $k_\Psi \in \{1,7\}$, $\{1,3,7,9,13,15,19,21\}$ for $k_\Psi \in \{5,11\}$
		2	1 or 3	$\{3,19\}$ for $k_\Psi = 1$, $\{3,11\}$ for $k_\Psi = 5$, $\{7,15\}$ for $k_\Psi = 7$, $\{15,23\}$ for $k_\Psi = 11$
			2 or 4	$\{3,19\}$ for $k_\Psi \in \{1,7\}$, $\{3,11\}$ for $k_\Psi \in \{5,11\}$
		3	2	$\{7,11,19,23\}$
			4	$\{1,5,13,17\}$
(77)	$\{1,5,7,11\}$	0	1 or 3	$\{5,13\}$ for $k_\Psi \in \{1,5\}$, $\{1,17\}$ for $k_\Psi \in \{7,11\}$
			2 or 4	$\{1,17\}$
		1	2	$\{5,9,17,21\}$ for $k_\Psi \in \{1,7\}$, $\{1,9,13,21\}$ for $k_\Psi \in \{5,11\}$,
			4	$\{3,11,15,23\}$ for $k_\Psi \in \{1,7\}$, $\{3,7,15,19\}$ for $k_\Psi \in \{5,11\}$
		2	1 or 3	$\{13,21\}$ for $k_\Psi = 1$, $\{5,21\}$ for $k_\Psi = 5$, $\{1,9\}$ for $k_\Psi = 7$, $\{9,17\}$ for $k_\Psi = 11$
			2 or 4	$\{13,21\}$ for $k_\Psi \in \{1,7\}$, $\{5,21\}$ for $k_\Psi \in \{5,11\}$
		3	4	$\{1,5,7,11,13,17,19,23\}$
(79)	$\{1,5,7,11\}$	0	1 or 3	$\{1,17\}$ for $k_\Psi \in \{1,5\}$, $\{5,13\}$ for $k_\Psi \in \{7,11\}$
			2 or 4	$\{5,13\}$
		1	2	$\{3,11,15,23\}$ for $k_\Psi \in \{1,7\}$, $\{3,7,15,19\}$ for $k_\Psi \in \{5,11\}$,
			4	$\{5,9,17,21\}$ for $k_\Psi \in \{1,7\}$, $\{1,9,13,21\}$ for $k_\Psi \in \{5,11\}$
		2	1 or 3	$\{1,9\}$ for $k_\Psi = 1$, $\{9,17\}$ for $k_\Psi = 5$, $\{13,21\}$ for $k_\Psi = 7$, $\{5,21\}$ for $k_\Psi = 11$
			2 or 4	$\{1,9\}$ for $k_\Psi \in \{1,7\}$, $\{9,17\}$ for $k_\Psi \in \{5,11\}$
		3	2	$\{1,5,7,11,13,17,19,23\}$

Table 13. Solutions of Equations (96), (98), and (100).

Equation	$k_\Psi \in$	$k_{3,f}$	$k_{2,f}$	$f_1 \pmod{48} \in$
(96)	$\{1,5,7,11\}$	0	1 or 3	$\{1,17\}$ for $k_\Psi \in \{1,5\}$, $\{5,13\}$ for $k_\Psi \in \{7,11\}$
			2 or 4	$\{5,13\}$
		1	4	$\{3,5,9,11,15,17,21,23\}$ for $k_\Psi \in \{1,7\}$, $\{1,3,7,9,13,15,19,21\}$ for $k_\Psi \in \{5,11\}$
		2	1 or 3	$\{13,21\}$ for $k_\Psi = 1$, $\{5,21\}$ for $k_\Psi = 5$, $\{1,9\}$ for $k_\Psi = 7$, $\{9,17\}$ for $k_\Psi = 11$
			2 or 4	$\{13,21\}$ for $k_\Psi \in \{1,7\}$, $\{5,21\}$ for $k_\Psi \in \{5,11\}$
		3	2	$\{7,11,19,23\}$
			4	$\{1,5,13,17\}$
(98)	$\{1,5,7,11\}$	0	1 or 3	$\{7,23\}$ for $k_\Psi \in \{1,5\}$, $\{11,19\}$ for $k_\Psi \in \{7,11\}$
			2 or 4	$\{7,23\}$
		1	2	$\{3,11,15,23\}$ for $k_\Psi \in \{1,7\}$, $\{3,7,15,19\}$ for $k_\Psi \in \{5,11\}$,
			4	$\{5,9,17,21\}$ for $k_\Psi \in \{1,7\}$, $\{1,9,13,21\}$ for $k_\Psi \in \{5,11\}$
		2	1 or 3	$\{7,15\}$ for $k_\Psi = 1$, $\{15,23\}$ for $k_\Psi = 5$, $\{3,19\}$ for $k_\Psi = 7$, $\{3,11\}$ for $k_\Psi = 11$
			2 or 4	$\{3,19\}$ for $k_\Psi \in \{1,7\}$, $\{3,11\}$ for $k_\Psi \in \{5,11\}$
		3	4	$\{1,5,7,11,13,17,19,23\}$
(100)	$\{1,5,7,11\}$	0	1 or 3	$\{11,19\}$ for $k_\Psi \in \{1,5\}$, $\{7,23\}$ for $k_\Psi \in \{7,11\}$
			2 or 4	$\{11,19\}$
		1	2	$\{5,9,17,21\}$ for $k_\Psi \in \{1,7\}$, $\{1,9,13,21\}$ for $k_\Psi \in \{5,11\}$,
			4	$\{3,11,15,23\}$ for $k_\Psi \in \{1,7\}$, $\{3,7,15,19\}$ for $k_\Psi \in \{5,11\}$
		2	1 or 3	$\{3,19\}$ for $k_\Psi = 1$, $\{3,11\}$ for $k_\Psi = 5$, $\{7,15\}$ for $k_\Psi = 7$, $\{15,23\}$ for $k_\Psi = 11$
			2 or 4	$\{7,15\}$ for $k_\Psi \in \{1,7\}$, $\{15,23\}$ for $k_\Psi \in \{5,11\}$
		3	2	$\{1,5,7,11,13,17,19,23\}$

Table 14. Solutions of Equations (75), (77), (79), (96), (98), and (100) summarized from Tables 12 and 13.

$k_{3,f}$	$k_{2,f}$	$f_1 \pmod{48} \in$
0	1 or 2 or 3 or 4	$\{1,5,7,11,13,17,19,23\}$
2	1 or 2 or 3 or 4	$\{1,3,7,9,13,15,19,21\}$ for $k_\Psi \in \{1,7\}$, $\{3,5,9,11,15,17,21,23\}$ for $k_\Psi \in \{5,11\}$
1	2 or 4	$\{3,5,9,11,15,17,21,23\}$ for $k_\Psi \in \{1,7\}$, $\{1,3,7,9,13,15,19,21\}$ for $k_\Psi \in \{5,11\}$
3	2 or 4	$\{1,5,7,11,13,17,19,23\}$

From Tables 11 and 14, it results that an interleaver pattern as in Figure 2 or Figure 3 always appears for $x_1 = 0$ or $x_1 = 1$ or $x_1 = 3$, when $k_{3,f} \in \{0,2\}$ and $k_{2,f} \in \{1,2,3,4\}$ or when $k_{3,f} \in \{1,3\}$ and $k_{2,f} \in \{2,4\}$. For an interleaver pattern as in Figure 2 or Figure 3, the weight of the codeword for classical nominal 1/3 rate turbo codes with two RSC codes having generator matrix $G = [1, 15/13]$, is equal to $4 + 4 \cdot 6 = 28$, because each of the four error patterns with weight of 2 lead to parity weight of 6. Because an interleaver pattern as in Figure 2 or Figure 3 always appears in the previous conditions, it results that the minimum distance is upper bounded by the value of 28. □

Combining the results from Theorems 1 and 2, it results that the upper bound of 36 is reached only for $k_{3,f} \in \{1,3\}$ and $k_{2,f} \in \{1,3\}$, $\forall k_L \in \{1,3\}$. Thus, the task for finding good 4-PPs is facilitated with this result, because coefficients f_4, f_3, and f_2 have only four possible combinations.

We note that from the LTE interleaver lengths [13], there exist 25 lengths of the form (5); namely 48, 80, 112, 176, 208, 240, 272, 304, 336, 368, 464, 496, 528, 560, 592, 624, 656, 688, 752, 816, 848, 880, 912, 944, and 976. From these, for the lengths 40, 208, 304, 496, 592, 624, 688, 912, and 976,

restriction conditions (6) on coefficients are not required, and thus, the result in the paper is fully general. Examples of 4-PP interleavers that reach the upper bound of 36 are those from [17] for the interleaver lengths 368, 464, and 496, when dual trellis termination [31] is used.

4. Remarks and Examples

4.1. Remarks

In this subsection, we make some remarks regarding the upper bounds on the minimum distance derived in [19] and those on the minimum distance derived in this paper. From Lemma 3.2 and Table 2 in [19], it results that an upper bound on minimum distance for turbo codes with any degree PP interleavers is equal to 36 in the following conditions:

(1) The PPs can be represented by a parallel linear PP (PLPP) with the minimum number of linear PPs (LPPs) from the PLPP representation equal to two or 14.

(2) The coefficients of the first degree term of LPPs from the PLPP representation are all equal to each other. We denote by D_{eq} the minimum number of LPPs from the PLPP representation fulfilling this condition.

In the following, we prove that 4-PPs fulfilling the conditions from Theorem 1 can be represented by PLPPs with the value of D_{eq} greater than two. For this task, it is enough to prove that these 4-PPs do not allow a PLPP representation with $D_{eq} = 2$ LPPs. A 4-PP allows a PLPP representation with D_{eq} component LPPs if and only if the following condition is fulfilled

$$f(D_{eq} \cdot y + D_{eq} + i) - f(D_{eq} \cdot y + i) = f(D_{eq} + i) - f(i) \pmod{L},$$
$$\forall i \in \{0, 1, \ldots, D_{eq} - 1\}, \forall y \in \{1, 2, \ldots, L/D_{eq} - 2\}. \quad (102)$$

With $f(x)$ from (1) fulfilling conditions (6) when $3 \nmid (p_i - 1)$ and with L as in (5), Equation (102) is equivalent to

$$\Psi \cdot \left(2D_{eq}^4 y \cdot (2y^2 + 3y + 2) + 12D_{eq}^3 iy \cdot (y + 1) + 12D_{eq}^2 i^2 y\right) + 2k_{3,f}\Psi \cdot \left(3D_{eq}^3 y \cdot (y + 1) + 6D_{eq}^2 iy\right) +$$
$$+ k'_{2,f}\Psi \cdot D_{eq}^2 \cdot 2y = 0 \pmod{16k_L\Psi}, \forall i \in \{0, 1, \ldots, D_{eq} - 1\}, \forall y \in \{1, 2, \ldots, 16k_L\Psi/D_{eq} - 2\}, \quad (103)$$

or

$$D_{eq}^4 y \cdot (2y^2 + 3y + 2) + 6D_{eq}^3 iy \cdot (y + 1) + 6D_{eq}^2 i^2 y + k_{3,f} \cdot 3D_{eq}^2 y \cdot \left(D_{eq} \cdot (y + 1) + 2i\right) + k'_{2,f} D_{eq}^2 \cdot y =$$
$$= 0 \pmod{8k_L}, \forall i \in \{0, 1, \ldots, D_{eq} - 1\}, \forall y \in \{1, 2, \ldots, 8k_L - 1\}. \quad (104)$$

Because $k_L \in \{1, 3\}$, we can write $3 = k_L \cdot (k_L - 1)$. Thus, Equation (104) is equivalent to

$$D_{eq}^4 y \cdot (2y^2 + 3y + 2) + 2 \cdot k_L \cdot (k_L - 1) \cdot D_{eq}^3 iy \cdot (y + 1) + 2 \cdot k_L \cdot (k_L - 1) \cdot D_{eq}^2 i^2 y +$$
$$+ k_{3,f} \cdot k_L \cdot (k_L - 1) \cdot D_{eq}^2 y \cdot \left(D_{eq} \cdot (y + 1) + 2i\right) + k'_{2,f} D_{eq}^2 \cdot y = 0 \pmod{8k_L},$$
$$\forall i \in \{0, 1, \ldots, D_{eq} - 1\}, \forall y \in \{1, 2, \ldots, 8k_L - 1\}. \quad (105)$$

For $D_{eq} = 2$, Equation (105) is equivalent to

$$8y^3 + 4 \cdot (k'_{2,f} + 2) \cdot y = 0 \pmod{8k_L}, \forall y \in \{1, 2, \ldots, 8k_L - 1\}, \quad (106)$$

or

$$2y^3 + (k'_{2,f} + 2) \cdot y = 0 \pmod{2k_L}, \forall y \in \{1, \ldots, 2k_L - 1\}. \quad (107)$$

For the coefficients of 4-PPs given in Theorem 1 we have $k'_{2,f} \pmod 2 = 1$ when $k_L = 1$ and $k'_{2,f} \pmod 6 = 5$ when $k_L = 3$. Thus (107) is equivalent to

$$y = 0 \pmod 2, \text{ for } y = 1, \tag{108}$$

when $k_L = 1$, and to

$$2y^3 + y = 0 \pmod 6, \forall y \in \{1, 2, \ldots, 5\}, \tag{109}$$

when $k_L = 3$.

It is clear that equalities (108) and (109) are not fulfilled for $y = 1$. Therefore, it results that the 4-PPs given in Theorem 1 do not allow a PLPP representation with $D_{eq} = 2$ component LPPs.

We can have $D_{eq} = 3$ only when $k_L = 3$, because $3 \nmid L$ for $k_L = 1$. For $D_{eq} = 3$ and $k_L = 3$, Equation (105) is equivalent to

$$18y^3 + 3y^2 \cdot (1 + 6i + 2i^2 + 3k_{3,f}) + 3y \cdot (6 + 6i + 3k_{3,f} + 2ik_{3,f} + 3k'_{2,f}) = 0 \pmod{24},$$
$$\forall i \in \{0, 1, 2\}, \forall y \in \{1, 2, \ldots, 23\}, \tag{110}$$

or

$$6y^3 + y^2 \cdot (1 + 6i + 2i^2 + 3k_{3,f}) + y \cdot (6 + 6i + 3k_{3,f} + 2ik_{3,f} + 3k'_{2,f}) = 0 \pmod 8,$$
$$\forall i \in \{0, 1, 2\}, \forall y \in \{1, 2, \ldots, 7\}. \tag{111}$$

Because there is no cubic null polynomial modulo 8 with the coefficient of the third term degree equal to six, it results that the 4-PPs from Theorem 1 can not be represented by a PLPP with three component LPPs.

For $D_{eq} = 4$, Equation (105) is equivalent to

$$8y^3 + 8 \cdot (2k'_{2,f} + 1) \cdot y = 0 \pmod{8k_L}, \forall y \in \{1, 2, \ldots, 8k_L - 1\}, \tag{112}$$

or

$$y^3 + (2k'_{2,f} + 1) \cdot y = 0 \pmod{k_L}, \forall y \in \{1, \ldots, k_L - 1\}. \tag{113}$$

For $k_L = 1$, Equation (113) is, obviously, fulfilled. For $k_L = 3$, because $k'_{2,f} \pmod 3 = 2$, Equation (113) becomes

$$y^3 + 2y = 0 \pmod 3, \forall y \in \{1, 2\}. \tag{114}$$

It can be easily verified that the equality from (114) is fulfilled for $y \in \{1, 2\}$.

To show that the 4-PPs established in Theorem 1 can be represented by a PLPP with $D_{eq} = 4$ LPPs, we still have to prove that all the coefficients of the first term degree of the four LPPs are equal to each other. For that, we have to show that

$$f(y + 4) - f(y) = f(4) - f(0) \pmod L, \forall y \in \{1, 2, 3\}. \tag{115}$$

Equation (115) is equivalent to

$$f_4 \cdot (4 \cdot y^3 \cdot 4 + 6 \cdot y^2 \cdot 4^2 + 4 \cdot y \cdot 4^3) + f_3 \cdot (3 \cdot y^2 \cdot 4 + 3 \cdot y \cdot 4^2) + f_2 \cdot 2 \cdot y \cdot 4 = 0 \pmod L, \forall y \in \{1, 2, 3\}; \tag{116}$$

or, with $f_4 = \Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, $f_2 = k'_{2,f} \cdot \Psi$, and $L = 16k_L\Psi$,

$$2y^3 + 3k_{3,f}y^2 + (k'_{2,f} + 2) \cdot y = 0 \pmod{2k_L}, \forall y \in \{1, 2, 3\}. \tag{117}$$

For the 4-PPs established in Theorem 1, we have $3k_{3,f} \pmod{2k_L} = k_L$ and $(k'_{2,f} + 2) \pmod{2k_L} = 1, \forall k_L \in \{1, 3\}$. Then, for $k_L = 1$ and $k_L = 3$, Equation (117) becomes

$$y^2 + y = 0 \pmod 2, \forall y \in \{1, 2, 3\} \tag{118}$$

and

$$2y^3 + 3y^2 + y = 0 \pmod 6, \forall y \in \{1, 2, 3\}, \tag{119}$$

respectively. It can be easily verified that the equalities from (118) and (119) are fulfilled for $y \in \{1, 2, 3\}$. Thus, the 4-PPs established in Theorem 1 always allow a PLPP representation with $D_{eq} = 4$ LPPs. Therefore, from Table 2 in [19] it results that the tightest upper bound derived in [19] is equal to 52. Thus, the upper bound of 36, derived in Theorem 1, is much tighter. The examples of 4-PPs given in the next subsection show that this upper bound can be reached.

4.2. Examples

Table 15 shows some CPPs and 4-PPs with optimum minimum distance for several LTE interleaver lengths of the form given in (5). We note that for all these 4-PPs we have $D_{eq} = 4$, and thus, the best upper bound derived in [19] is equal to 52. Minimum distances (d_{min}) and corresponding multiplicities ($N_{d_{min}}$), spread factors (D), nonlinearity degrees (ζ), and refined nonlinearity degrees (ζ') for each CPP and each 4-PP are also given in Table 15. As it can be observed, CPPs have optimum distances greater than those of 4-PPs (38 compared to 36) and the corresponding multiplicities for CPPs are equal to about a half of those for 4-PPs. These relation between the multiplicities for CPPs and 4-PPs with optimum distances is explained by means of nonlinearity degrees. In [21], it was proven that CPPs with optimum distance have the nonlinearity degree equal to $\zeta_{CPP,d_{min}-opt} = 8$. In Appendix A, it is proven that the nonlinearity degree of 4-PPs for interleaver lengths of the form (5), fulfilling conditions (6) when $3 \nmid (p_i - 1)$, is equal to

$$\zeta_{4-PP} = \begin{cases} 4 \text{ when } k_{3,f} \in \{1, 3\} \\ 8 \text{ when } k_{3,f} \in \{0, 2\}, \end{cases} \tag{120}$$

where the coefficient of the third term of 4-PP is $f_3 = k_{3,f} \cdot 2\Psi$. Because 4-PPs with optimum distance have $k_{3,f} \in \{1, 3\}$, it results that their nonlinearity degree is equal to $\zeta_{4-PP_{d_{min}-opt}} = 4 = \zeta_{CPP_{d_{min}-opt}}/2$. Thus, the result for the multiplicities is explained.

We also note that the good QPPs reported in Table XIII from [21] have the minimum distance equal to 38 and the corresponding multiplicities are approximately equal to those for 4-PPs from Table 15 in this paper. The results for multiplicities are explained by the fact that QPPs given in [21] have the nonlinearity degree $\zeta_{QPP_{d_{min}-opt}} = 4 = \zeta_{4-PP_{d_{min}-opt}}$.

Taking into account the above, it is expected that CPPs and QPPs for these interleaver lengths to lead to better error rate performances compared to 4-PPs.

An estimation of asymptotic improvement in terms of the error rate for CPP and QPP interleavers compared to 4-PP interleavers can be given if we compare the upper bounds on error rates for distance spectra of the turbo codes truncated at the first term. For an additive white Gaussian noise (AWGN) channel with the signal to noise ratio SNR, the frame error rate (FER) for a block code with coding rate R_c, minimum distance $d_{\min}$, and the corresponding multiplicity $N_{d_{\min}}$, is upper bounded by

$$FER \leq TUB_{erfc}(FER) < TUB_{exp}(FER), \tag{121}$$

where

$$TUB_{erfc}(FER) = 0.5 \cdot N_{d_{\min}} \cdot erfc\left(\sqrt{R_c \cdot d_{\min} \cdot SNR}\right) = N_{d_{\min}} \cdot \frac{1}{\sqrt{\pi}} \cdot \int_{\sqrt{R_c \cdot d_{\min} \cdot SNR}}^{+\infty} e^{-t^2} dt \tag{122}$$

and

$$TUB_{exp}(FER) = 0.5 \cdot N_{d_{\min}} \cdot e^{-R_c \cdot d_{\min} \cdot SNR}. \quad (123)$$

From Table 15 it results that the multiplicity of the codewords of weight $d_{\min}$ is approximately equal to L for CPP interlevears and to $2L$ for 4-PP interleavers. From the QPPs reported in Table XIII from [21], it results that for QPPs, the best minimum distance is equal to 38 and the corresponding multiplicity is approximately equal to $2L$. Thus, if we use the upper bounds with $TUB_{exp}(FER)$ from (123), the FER for QPP, CPP, and 4-PP interleavers, is approximately upper bounded by

$$FER_{QPP} < 0.5 \cdot 2L \cdot e^{-R_c \cdot 38 \cdot SNR}, \quad (124)$$

$$FER_{CPP} < 0.5 \cdot L \cdot e^{-R_c \cdot 38 \cdot SNR}, \quad (125)$$

and

$$FER_{4-PP} < 0.5 \cdot 2L \cdot e^{-R_c \cdot 36 \cdot SNR}, \quad (126)$$

respectively.

Table 15. Minimum distances (d_{min}) and corresponding multiplicities ($N_{d_{min}}$), spread factors (D), nonlinearity degrees (ζ), and refined nonlinearity degrees (ζ') for cubic permutation polynomials (CPPs) and for fourth degree permutation polynomials (4-PPs) with optimum minimum distance.

L	CPP	d_{min}	$N_{d_{min}}$	ζ	ζ'	D	4-PP	d_{min}	$N_{d_{min}}$	ζ	ζ'	D
592	$222x^3 + 148x^2 + 39x$	38	625	8	5	20	$37x^4 + 222x^3 + +37x^2 + 393x$	36	1102	4	4	30
656	$82x^3 + 164x^2 + 185x$ (from [18])	38	620	8	5	22	$41x^4 + 246x^3 + +41x^2 + 217x$	36	1230	4	4	32
688	$86x^3 + 0x^2 + 21x$	38	652	8	5	24	$43x^4 + 258x^3 + +43x^2 + 137x$	36	1294	4	4	32
752	$94x^3 + 188x^2 + 541x$ (from [18])	38	716	8	5	26	$47x^4 + 282x^3 + +47x^2 + 249x$	36	1422	4	4	32
816	$34x^3 + 0x^2 + 19x$	38	782	8	7	28	$17x^4 + 34x^3 + +85x^2 + 9x$	36	1556	4	4	30
848	$318x^3 + 212x^2 + 157x$ (from [18])	38	812	8	5	28	$53x^4 + 318x^3 + +53x^2 + 169x$	36	1614	4	4	32
912	$114x^3 + 114x^2 + 287x$ (from [18])	38	878	8	4	30	$19x^4 + 38x^3 + +95x^2 + 5x$	36	1748	4	4	18
944	$354x^3 + 0x^2 + 179x$ (from [18])	38	910	8	5	32	$59x^4 + 354x^3 + +59x^2 + 317x$	36	1806	4	4	38
976	$122x^3 + 0x^2 + 307x$ (from [18])	38	942	8	5	32	$61x^4 + 366x^3 + +61x^2 + 389x$	36	1870	4	4	38

From (124)–(126), it results that when considering the interleaver lengths of the form given in (5) and turbo codes of nominal 1/3 coding rate with RSC component codes with generator matrix $G = [1, 15/13]$, the asymptotic coding gain for QPPs compared to 4-PPs, is equal to

$$G_{c_{QPP,4-PP}}(TUB_{exp}(FER)) = 10 \cdot \log_{10}\left(\frac{38}{36}\right) \cong 0.235 \text{ dB} \quad (127)$$

and the asymptotic coding gain for CPPs compared to 4-PPs, for a given FER value, is equal to

$$G_{c_{CPP,4-PP}}(TUB_{exp}(FER)) = 10 \cdot \log_{10}\left(\frac{38}{36}\right) - 10 \cdot \log_{10}\left(1 + \frac{\log_{10}(2)}{\log_{10}(FER/L)}\right). \quad (128)$$

For example, for a target $FER = 3 \cdot 10^{-6}$ and for interleaver length $L = 656$, the coding gain from (128) becomes $G_{c_{CPP,4-PP}}(TUB_{exp}(FER)) \cong 0.395$ dB. Increasing the interleaver length, $G_{c_{CPP,4-PP}}(TUB_{exp}(FER))$ resulting from (128) decreases easily. For an increase of interleaver length

with a factor of approximately 25 compared to 656, the coding gain from (128) decreases with about 0.023 dB.

In Figure 4, the FER, $TUB_{erfc}(FER)$, and $TUB_{exp}(FER)$ curves for 4-PP, CPP, and QPP of interleaver length L = 656 are shown. The 4-PP and the CPP are those from Table 15, and the QPP is $246x^2 + 21x \pmod{656}$ given in [21]. For FER curves, the Max-Log-MAP algorithm with a scaling coefficient of the extrinsec information of 0.75 was used. We note that the considered multiplicities for $TUB_{erfc}(FER)$ and $TUB_{exp}(FER)$ curves are the estimated ones; i.e., $2L$, L, and $2L$, for 4-PP, CPP, and QPP, respectively. For $FER = 3 \cdot 10^{-6}$, from Figure 4, it results that

(1) The coding gains resulting from FER curves are $G_{c_{CPP,4-PP}}(FER) = 0.393$ dB and $G_{c_{QPP,4-PP}}(FER) = 0.229$ dB and

(2) The coding gains resulting from $TUB_{erfc}(FER)$ curves are $G_{c_{CPP,4-PP}}(TUB_{erfc}(FER)) = 0.409$ dB and $G_{c_{QPP,4-PP}}(TUB_{erfc}(FER)) = 0.235$ dB.

We observe that these coding gains are very close to those previously estimated by the $TUB_{exp}(FER)$ upper bounds.

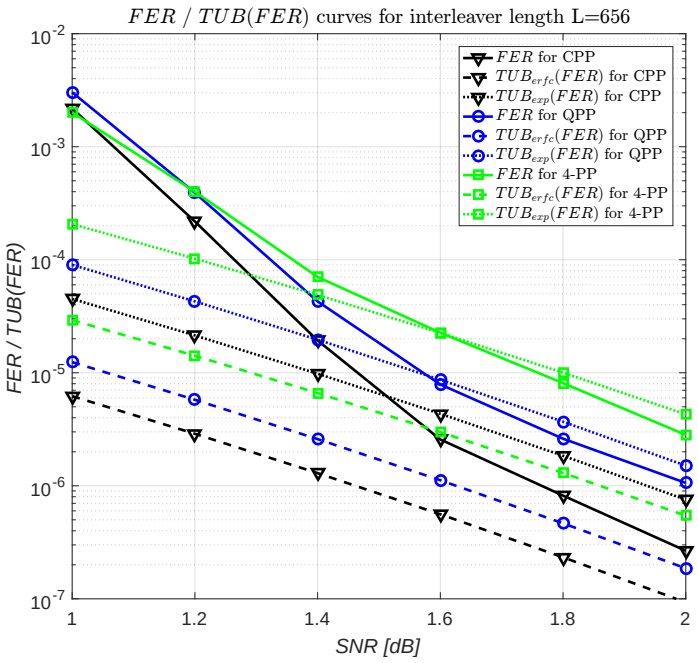

Figure 4. Frame error rate (FER) and truncated upper bound of FER ($TUB(FER)$) curves for interleaver length L = 656.

5. Conclusions

In this paper, we obtained the upper bounds of the minimum distance for turbo codes when using 4-PP interleavers. The component RSC codes were those from the LTE standard and 1/3 nominal coding rate. The interleaver lengths in question were of the form (5), and condition (6) was applied for 4-PP coefficients when for a prime p_i, $3 \nmid (p_i - 1)$. The two obtained upper bounds have the values of 28 and 36 for different classes of 4-PP coefficients. The result obtained in this paper has theoretical importance. The highest upper bound for 4-PPs (i.e., 36) is smaller than that for CPPs or QPPs (i.e., 38), while the corresponding multiplicities are about twice as high as those for CPPs and approximately equal to those for QPPs. Thus, it is expected that CPPs and QPPs for the interleaver lengths in question are better compared to 4-PPs.

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

Funding: This work was supported by a National Research Grant—ARUT of the TUIASI, project number GnaC2018_39.

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

Appendix A

In [32], an efficient algorithm for the computing nonlinearity degree of a 4-PP was given. We remember that for interleaver lengths of the form (5), the coefficients of 4-PPs fulfilling conditions (6) when $3 \nmid (p_i - 1)$, are equivalent to the following ones: $f_4 = \Psi$, $f_3 = k_{3,f} \cdot 2\Psi$, with $k_{3,f} \in \{0, 1, 2, 3\}$, $f_2 = (2k_L k_{2,f} - 1) \cdot \Psi$, with $k_{2,f} \in \{1, 2, 3, 4\}$ and $k_L \in \{1, 3\}$. Then, we have

$$\gcd(4f_4, L) = 4\Psi, \tag{A1}$$

$$\gcd(6, L) = 2k_L, \tag{A2}$$

$$\gcd(2, L) = 2. \tag{A3}$$

$$\begin{aligned} k_{0,f_4} &= \left(\frac{4f_4}{\gcd(4f_4, L)}\right)^{-1} \cdot \frac{L/\gcd(6, L) \cdot \tau_3}{\gcd(4f_4, L)} \left(\mathrm{mod}\ \frac{L}{\gcd(4f_4, L)}\right) = \\ &= \left(\frac{4\Psi}{4\Psi}\right)^{-1} \cdot \frac{8\Psi \cdot \tau_3}{4\Psi} \left(\mathrm{mod}\ \frac{16k_L\Psi}{4\Psi}\right) = 2\tau_3 \pmod{4k_L} = 2\tau_3. \end{aligned} \tag{A4}$$

For

$$k_0 = k_{0,f_4} + L/\gcd(4f_4, L) \cdot i = 2\tau_3 + 4k_L \cdot i, \tag{A5}$$

we have

$$\begin{aligned} 3f_3k_0 - 6f_4k_0^2 \pmod{L} &= 3k_{3,f} \cdot 2\Psi \cdot (2\tau_3 + 4k_L \cdot i) - 6\Psi \cdot (2\tau_3 + 4k_L \cdot i)^2 \pmod{16k_L\Psi} = \\ &= 12\Psi \cdot (\tau_3 + 2k_L \cdot i) \cdot (k_{3,f} - 2\tau_3 - 4k_L \cdot i) \pmod{16k_L\Psi}, \end{aligned} \tag{A6}$$

$$L/\gcd(2, L) \cdot \tau_2 \pmod{L} = 8k_L\Psi \cdot \tau_2 \pmod{16k_L\Psi}, \tag{A7}$$

$$\begin{aligned} 2f_2k_0 - 3f_3k_0^2 + 4f_4k_0^3 \pmod{L} &= 2 \cdot (2k_Lk_{2,f} - 1) \cdot \Psi \cdot (2\tau_3 + 4k_L \cdot i) - 3k_{3,f} \cdot 2\Psi \cdot (2\tau_3 + 4k_L \cdot i)^2 + \\ &+ 4\Psi \cdot (2\tau_3 + 4k_L \cdot i)^3 \pmod{16k_L\Psi} = 4\Psi \cdot (\tau_3 + 2k_L \cdot i) \cdot \\ &\cdot \left(2k_Lk_{2,f} - 1 - 3k_{3,f} \cdot (2\tau_3 + 4k_L \cdot i) + (2\tau_3 + 4k_L \cdot i)^2\right) \pmod{16k_L\Psi} \end{aligned} \tag{A8}$$

$$\begin{aligned} (-L/\gcd(6, L) \cdot \tau_3 - L/\gcd(2, L) \cdot \tau_2) \pmod{L} &= \\ = -8\Psi \cdot (\tau_3 + k_L \cdot \tau_2) \pmod{16k_L\Psi}. \end{aligned} \tag{A9}$$

Then condition $3f_3k_0 - 6f_4k_0^2 \pmod{L} = L/\gcd(2, L) \cdot \tau_2 \pmod{L}$ is equivalent to

$$12\Psi \cdot (\tau_3 + 2k_L \cdot i) \cdot (k_{3,f} - 2\tau_3 - 4k_L \cdot i) \pmod{16k_L\Psi} = 8k_L\Psi \cdot \tau_2 \pmod{16k_L\Psi}$$

or

$$3 \cdot (\tau_3 + 2k_L \cdot i) \cdot (k_{3,f} - 2\tau_3 - 4k_L \cdot i) \pmod{4k_L} = 2k_L \cdot \tau_2 \pmod{4k_L}$$

or

$$3 \cdot (\tau_3 + 2k_L \cdot i) \cdot (k_{3,f} - 2\tau_3) \pmod{4k_L} = 2k_L \cdot \tau_2 \pmod{4k_L}; \tag{A10}$$

and condition $2f_2k_0 - 3f_3k_0^2 + 4f_4k_0^3 \pmod{L} = (-L/\gcd(6,L) \cdot \tau_3 - L/\gcd(2,L) \cdot \tau_2) \pmod{L}$ is equivalent to

$$4\Psi \cdot (\tau_3 + 2k_L \cdot i) \cdot \left(2k_Lk_{2,f} - 1 - 3k_{3,f} \cdot (2\tau_3 + 4k_L \cdot i) + (2\tau_3 + 4k_L \cdot i)^2\right) \pmod{16k_L\Psi} =$$

$$= -8\Psi \cdot (\tau_3 + k_L \cdot \tau_2) \pmod{16k_L\Psi}$$

or

$$(\tau_3 + 2k_L \cdot i) \cdot \left(2k_Lk_{2,f} - 1 - 3k_{3,f} \cdot (2\tau_3 + 4k_L \cdot i) + (2\tau_3 + 4k_L \cdot i)^2\right) \pmod{4k_L} =$$

$$= -2 \cdot (\tau_3 + k_L \cdot \tau_2) \pmod{4k_L}$$

or

$$(\tau_3 + 2k_L \cdot i) \cdot \left(2k_Lk_{2,f} - 1 - 6k_{3,f} \cdot \tau_3 + 8\tau_3^2\right) \pmod{4k_L} = -2 \cdot (\tau_3 + k_L \cdot \tau_2) \pmod{4k_L}. \tag{A11}$$

Because $L/\gcd(6,L) \cdot \tau_3 = 8\Psi \cdot \tau_3$, we have $\gcd(4f_4, L) \mid L/\gcd(6,L) \cdot \tau_3$, $\forall \tau_3 \in \{0,1,\ldots,2k_L - 1\}$. Then, with Equations (A1)–(A11), Algorithm 2 from [32] becomes Algorithm A1 in this paper. Run Algorithm A1 for every $k_{3,f} \in \{0,1,2,3\}$, $k_{2,f} \in \{1,2,3,4\}$, and $k_L \in \{1,3\}$, (120) result.

Algorithm A1: Algorithm for computing the nonlinearity degree ζ for a 4-PP for interleaver lengths of the form (5) and the coefficients of 4-PP fulfilling conditions (6) when $3 \nmid (p_i - 1)$.

input : Values k_L for the interleaver length, and $k_{3,f}$, $k_{2,f}$ for the 4-PP.
output: Nonlinearity degree ζ for the 4-PP.

```
N_{k_0} ← 0; for τ_3 = 0 : 2k_L − 1 do
    for i = 0 : 3 do
        for τ_2 = 0 : 1 do
            if 3 · (τ_3 + 2k_L · i) · (k_{3,f} − 2τ_3) (mod 4k_L) = 2k_L · τ_2 (mod 4k_L) then
                if (τ_3 + 2k_L · i) · (2k_L k_{2,f} − 1 − 6k_{3,f} · τ_3 + 8τ_3^2) (mod 4k_L) =
                  −2 · (τ_3 + k_L · τ_2) (mod 4k_L) then
                    N_{k_0} ← (N_{k_0} + 1); break;
                end
            end
        end
    end
end
ζ ← 16k_L / N_{k_0};
```

References

1. Shao, S.; Hailes, P.; Wang, Y.-Y.; Wu, J.-Y.; Maunder, R.G.; Al-Hashimi, B.M.; Hanzo, L. Survey of turbo, LDPC, and polar decoder ASIC implementations. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2309–2333. [CrossRef]
2. Arora, K.; Singh, J.; Randhawa, Y.S. A survey on channel coding techniques for 5G wireless networks. *Telecommun. Syst.* **2019**. [CrossRef]
3. Berrou, C.; Glavieux, A.; Thitimajshima, P. Near Shannon limit error-correcting coding and decoding: Turbo-codes. In Proceedings of the IEEE International Conference on Communications (ICC 1993), Geneva, Switzerland, 23–26 May 1993; pp. 1064–1070.
4. MacKay, D.J.C.; Neal, R.M. Near Shannon limit performance of low density parity check codes. *Electron. Lett.* **1996**, *32*, 457–458. [CrossRef]
5. Arikan, E. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Trans. Inform. Theory* **2009**, *55*, 3051–3073. [CrossRef]
6. Rosnes, E.; i Amat, A.G. Performance analysis of 3-D turbo codes. *IEEE Trans. Inform. Theory* **2011**, *57*, 3707–3720. [CrossRef]
7. Banerjee, S.; Chattopadhyay, S. Evaluation of system performance by adding a fourth dimension to turbo code. *Int. J. Commun. Syst.* **2018**, *31*, ID e3450. [CrossRef]
8. Banerjee, S.; Chattopadhyay, S. Performance analysis of four dimensional turbo code (4D-TC) using moment based simplified augmented state diagram (MSASD) approach: Extension to LTE system. *Wirel. Person. Commun.* **2019**, *108*, 2077–2102. [CrossRef]
9. Banerjee, S.; Chattopadhyay, S. Superposition modulation-based new structure of four-dimensional turbo code (4D-TC) using modified interleaver and its application in WiMAX & LTE systems. *Person. Ubiquitous Comput.* **2019**, *23*, 943–959.
10. Sun, J.; Takeshita, O.Y. Interleavers for turbo codes using permutation polynomials over integer rings. *IEEE Trans. Inform. Theory* **2005**, *51*, 101–119.
11. Crozier, S.; Guinand, P. High-performance low-memory interleaver banks for turbo-codes. In Proceedings of the IEEE 54th Vehicular Technology Conference. VTC Fall 2001. , Atlantic City, NJ, USA, 7–11 October 2001; pp. 2394–2398.
12. Berrou, C.; Saoter, Y.; Douillard, C.; Kerouedan, S.; Jezequel, M. Designing good permutations for turbo codes: Towards a single model. In Proceedings of the 2004 IEEE International Conference on Communications, Paris, France, 20–24 June 2004; pp. 341–345.
13. 3GPP TS 36.212 V8.3.0, 3rd Generation Partnership Project, Multiplexing and channel coding (Release 8), 2008. Available Online: http://www.etsi.org. (accessed on 23 July 2009).
14. Takeshita, O.Y. Permutation polynomial interleavers: An algebraic-geometric perspective. *IEEE Trans. Inform. Theory* **2007**, *53*, 2116–2132. [CrossRef]
15. Rosnes, E. On the minimum distance of turbo codes with quadratic permutation polynomial interleavers. *IEEE Trans. Inform. Theory* **2012**, *58*, 4781–4795. [CrossRef]
16. Ryu, J. Permutation polynomials of higher degrees for turbo code interleavers. *IEICE Trans. Commun.* **2012**, *E95-B*, 3760–3762. [CrossRef]
17. Trifina, L.; Ryu, J.; Tarniceriu, D. Up to five degree permutation polynomial interleavers for short length LTE turbo codes with optimum minimum distance. In Proceedings of the 13th IEEE International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 13–14 July 2017.
18. Trifina, L.; Tarniceriu, D. On the equivalence of cubic permutation polynomial and ARP interleavers for turbo codes. *IEEE Trans. Commun.* **2017**, *65*, 473–485. [CrossRef]
19. Ryu, J.; Trifina, L.; Balta, H. The limitation of permutation polynomial interleavers for turbo codes and a scheme for dithering permutation polynomials. *AEU Int. J. Electron. Commun.* **2015**, *69*, 1550–1556. [CrossRef]
20. Trifina, L.; Tarniceriu, D.; Ryu, J.; Rotopanescu, A.-M. Some Lengths for Which CPP Interleavers Have Weaker Minimum Distances Than QPP Interleavers. Available online: http://telecom.etti.tuiasi.ro/tti/papers/PDFs/Some%20lengths%20for%20which%20CPPs%20have%20weaker%20minimum%20distances%20than%20QPPs.pdf (accessed on 7 December 2019).

21. Trifina, L.; Tarniceriu, D.; Ryu, J.; Rotopanescu, A.-M. Upper Bounds on the Minimum Distance for Turbo Codes Using CPP Interleavers. Available online: http://telecom.etti.tuiasi.ro/tti/papers/PDFs/UB%20of%20dmin%20for%20CPPs%20of%20L_16p_48p.pdf (accessed on 7 December 2019).
22. 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]
23. Trifina, L.; Tarniceriu, D.; Rotopanescu, A.-M.; Ursu, E. The inverse of a fourth degree permutation polynomial. In Proceedings of the Fifth Conference of Mathematical Society of Moldova, Chisinau, Moldova, 28 September–1 October 2019; pp. 255–260.
24. Garello, R.; Pierleoni, P.; Benedetto, S. Computing the free distance of turbo codes and serially concatenated codes with interleavers: Algorithms and applications. *IEEE J. Sel. Areas Commun.* **2001**, *19*, 800–812. [CrossRef]
25. Rosnes, E.; Ytrehus, Y. Improved algorithms for the determination of turbo-code weight distributions. *IEEE Trans. Commun.* **2005**, *53*, 20–26. [CrossRef]
26. Crozier, S.; Guinand, P.; Hunt, A. Computing the minimum distance of turbo-codes using iterative decoding techniques. In Proceedings of the 22th Biennial Symposium on Communications, Kingston, ON, Canada, 31 May–3 June 2004; pp. 306–308.
27. Ould-Cheikh-Mouhamedou, Y.; Crozier, S.; Guinand, P.; Kabal, P. Comparison of distance measurement methods for turbo codes. In Proceedings of the 9th Canadian Workshop on Information Theory (CWIT-05), Montreal, QC, Canada, 5–8 June 2005; pp. 36–39.
28. Crozier, S.; Guinand, P.; Hunt, A. Estimating the minimum distance of large-block turbo codes using iterative multiple-impulse methods. In Proceedings of the 4th International Symposium on Turbo Codes and Related Topics, Munich, Germany, 3–7 April 2006.
29. Ould-Cheikh-Mouhamedou, Y. Reducing the complexity of distance measurement methods for circular turbo codes that use structured interleavers. *Int. J. Commun. Syst.* **2015**, *28*, 1572–1579. [CrossRef]
30. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*; Oxford University Press: Oxford, UK, 1975.
31. Guinand, P.; Lodge, J. Trellis termination for turbo encoders. In Proceedings of the 17th Biennial Symposium on Communications, Kingston, ON, Canada, 29 May–1 June 1994; pp. 389–392.
32. Trifina, L.; Tarniceriu, D.; Rotopanescu, A.-M. Nonlinearity degree for CPP, 4-PP, and 5-PP interleavers for turbo codes. In Proceedings of the 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 27–29 June 2019.