Upper Bounds on the Minimum Distance for Turbo Codes Using CPP Interleavers

Lucian Trifina, Daniela Tarniceriu, Jonghoon Ryu, Ana-Mirela Rotopanescu

August 20, 2019

Abstract

In this paper we have considered turbo codes with component convolutional codes as in the Long Term Evolution (LTE) standard. The interleaver lengths are of the form 16Ψ or 48Ψ, with Ψ a product of different prime numbers greater than three. For these interleaver lengths, we have shown that cubic permutation polynomials (CPP), with some constraints on the coefficients when for a prime $p_i > 3$, $3 \nmid (p_i - 1)$, allways have an inverse true CPP. For the previously mentioned turbo codes and CPP interleavers, we have shown that the minimum distance is upper bounded by the values of 38, 36, and 28, for three different classes of coefficients. Previously it was shown that for the same interleaver lengths and for quadratic PP (QPP) interleavers, the upper bound of the minimum distance is equal to 38. Several examples show that d_{min}-optimal CPP interleavers are better than d_{min}-optimal QPP interleavers because the multiplicities corresponding to the minimum distances for CPPs are about a half of those for QPPs. A theoretical explanation in terms of nonlinearity degrees for this result is given for all considered interleaver lengths and for the class of CPPs for which the upper bound is equal to 38.

Keywords: PP interleaver, CPP, QPP, minimum distance, upper bound, turbo codes.

1 Introduction

Permutation polynomials (PPs) have been studied for many years ago. They are used in cryptography or as interleavers for turbo codes [1]. PP interleavers for turbo codes have some advantages as: fully algebraic description, which made them easy to analyze and design, low power consumption and low memory requirements. Other well known and performant interleavers are dithered relative prime (DRP) [2] and almost regular permutation (ARP) ones [3]. These interleavers can lead to better error correcting performance, but they are not fully algebraic, being a combination of algebraic and random interleavers.

Quadratic PP (QPP) interleavers have been adopted for turbo codes in the Long Term Evolution (LTE) standard of the 3rd Generation Partnership Project [4]. Higher than two degree PP interleavers have received attention in the last years [5–10]. Minimum distance is a well known metric which affects the performance of error correcting codes. Therefore it is beneficial to know the upper bounds of the minimum distance of different codes to know the capabilities in error correction of these codes. Related results for turbo codes with QPP interleavers are given in [11]. Recently, in [12], upper bounds on the minimum distance of turbo codes with cubic PP (CPP) interleavers of lengths of the form $8p$ or $24p$, with p a prime number so that $3 \mid (p-1)$, were established. In this paper, we deal with the upper bounds on the minimum distance of turbo codes using CPP interleavers of lengths of the form $L = 16\Psi$ or $L = 48\Psi$, with Ψ a product of different prime numbers greater than three, and with some constraints for the coefficients when for a prime $p_i > 3$, $3 \nmid (p_i - 1)$. The main contributions in this paper are:

- We have shown that all CPP interleavers for the above interleavers lengths and constraints have an inverse true CPP (i.e. a CPP which can not be reduced to a QPP or a linear PP (LPP)).
- We have obtained three upper bounds of the minimum distance of the turbo codes using the above CPP interleavers. These upper bounds are equal to 38, 36, and 28, for different classes of the CPP' coefficients (as show Tables 10, 11, and 12).
- Some remarks are made for CPP and QPP interleavers from Table III in [13]. The difference in error correction performance of these CPP and QPP interleavers is explained in terms of nonlinearity degrees. This result is proven to be generally valid for all considered interleaver lengths and for the class of CPPs for which the upper bound is equal to 38. An insight to search d_{min}-optimal CPPs among CPPs with the largest spread factor is suggested. This fact along with conditions in Table 10 restricts very much the class of coefficients to find d_{min}-optimal CPPs and thus saves very much time for searching.

The paper is structured as follows. In Section 2, the used notations are given and some required previous results about CPPs are provided. In Section 3, the main results are obtained. In Section 4, some remarks are made for CPP and QPP interleavers from Table III in [13] and Section 5 concludes the paper.

2 Preliminaries

2.1 Notations

In the paper we use the following notations:

- $\pmod{L}$, with L a positive integer, denotes modulo L operation
- $a \mid b$, with a and b positive integers, denotes a divides b
- $a \nmid b$, with a and b positive integers, denotes a does not divide b
- $\gcd(a, b)$, with a and b positive integers, denotes the greatest common divisor of a and b.

2.2 Results about CPPs

A CPP modulo L is a third degree polynomial

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

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

A CPP is *true* if the permutation it performs cannot be performed by a permutation polynomial of degree smaller than three.

Two CPPs with different coefficients are *different* if they lead to different permutations.

Conditions on coefficients f_1, f_2, and f_3 so that the third degree polynomial in (1) is a CPP modulo L have been obtained in [5, 6]. 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 so that $\pi(x)$ in (1) is a CPP modulo L of the form (2)

1)	$p = 2$	$n_{L,2} > 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0 \pmod{2}$
2)	$p = 3$	$n_{L,3} = 1$	$(f_1 + f_3) \neq 0, f_2 = 0 \pmod{3}$
3)	$3 \mid (p_i - 1)$	$n_{L,p_i} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0 \pmod{p_i}$
3)	$3 \nmid (p_i - 1)$	$n_{L,p_i} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0 \pmod{p_i}$ or $f_2^2 = 3f_1f_3 \pmod{p_i}$

A CPP modulo L

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

is an inverse of the CPP 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 CPPs with coefficients fulfilling conditions

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

In the following we will denote

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

Firstly, we prove two lemmas necessary to derive the upper bounds of the minimum distance.

Lemma 3.1. *Let the interleaver length be of the form given in* (5)*. Then all true different CPPs fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, have possible values for coefficients* f_3 *and* f_2 *equivalent to those given in Table 2 from the second and third column, respectively. Coefficient* f_1 *has to fulfill the necessary conditions, but not sufficient, from the fourth column in Table 2.*

Table 2: Possible values for coefficients f_3 and f_2 so that $\pi(x)$ in (1) is a true CPP modulo 16Ψ or 48Ψ. (Conditions for coefficient f_1 from the fourth column are necessary, but not sufficient.)

L	f_3	f_2	f_1
16Ψ	2Ψ or 4Ψ or 6Ψ	0 or 2Ψ or 4Ψ or 8Ψ	1 (mod 8) or 3 (mod 8) or 5 (mod 8) or 7 (mod 8)
48Ψ	2Ψ or 4Ψ or 6Ψ	0 or 6Ψ or 12Ψ or 18Ψ	

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

We note that when $L = 16\Psi$ or $L = 48\Psi$, from condition 1) in Table 1 f_1 results odd. Thus, we can have only $f_1 = 1 \pmod 8$ or $f_1 = 3 \pmod 8$ or $f_1 = 5 \pmod 8$ or $f_1 = 7 \pmod 8$. □

Taking into account the result in Lemma 3.1, for interleaver lengths of the form (5), coefficients f_3 and f_2 of a CPP fulfilling conditions (6) when $3 \nmid (p_i - 1)$ are of the form

$$f_3 = k_3 \cdot 2\Psi, k_3 \in \{1,2,3\}, f_2 = k_2 \cdot 2\Psi, k_2 \in \{0,1,2,3\}, \text{ for } L = 16\Psi, \tag{8}$$

$$f_3 = k_3 \cdot 2\Psi, k_3 \in \{1,2,3\}, f_2 = k_2 \cdot 6\Psi, k_2 \in \{0,1,2,3\}, \text{ for } L = 48\Psi. \tag{9}$$

Lemma 3.2. *Let the interleaver length be of the form given in* (5)*. Then, a true CPP* $\pi(x) = f_1x + f_2x^2 + f_3x^3 \pmod L$*, fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, has an inverse true CPP* $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 \pmod L$*, with*

$$\rho_3 = f_3, \tag{10}$$

$$\rho_2 = f_2 \textit{ or } \rho_2 = f_2 + 4\Psi \pmod{8\Psi}, \textit{ when } L = 16\Psi, \tag{11}$$

$$\rho_2 = f_2 \textit{ or } \rho_2 = f_2 + 12\Psi \pmod{24\Psi}, \textit{ when } L = 48\Psi. \tag{12}$$

ρ_1 *is the unique modulo* L *solution of the congruence* $f_1\rho_1 = 2\Psi \cdot k + 1 \pmod L$*, so that* $\rho_1 = f_1 \pmod{24}$ *when* $L = 48\Psi$*, with* k *from Tables 3-8, according to the coefficients* f_3*,* f_2 *and* f_1*.*

Table 3: Determining coefficients ρ_2 and ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_3, f_2 and f_1 when $L = 16\Psi$ ($k_\Psi = 2\Psi \pmod 8$).

f_3	f_2	Condition for f_1	Congruence for determining ρ_1	ρ_2
2Ψ	0	$f_1 = 3 \pmod 8$ or $f_1 = 7 \pmod 8$	$f_1\rho_1 = 2\Psi \cdot \big((k_\Psi + 6) \pmod 8\big)$ $+1 \pmod{(16 \cdot \Psi)}$	f_2
	2Ψ or 6Ψ	$f_1 = 1 \pmod 8$	$f_1\rho_1 = 1 \pmod{(16 \cdot \Psi)}$	
	0	$f_1 = 1 \pmod 8$ or $f_1 = 5 \pmod 8$	$f_1\rho_1 = 2\Psi \cdot \big((k_\Psi + 2) \pmod 8\big)$ $+1 \pmod{(16 \cdot \Psi)}$	
	4Ψ	-		
	2Ψ or 6Ψ	$f_1 = 5 \pmod 8$	$f_1\rho_1 = 8\Psi + 1 \pmod{(16 \cdot \Psi)}$	
2Ψ or 6Ψ	2Ψ	$f_1 = 3 \pmod 8$	$f_1\rho_1 = 1 \pmod{(16 \cdot \Psi)}$	$f_2 + 4\Psi$ $\pmod{8\Psi}$
	6Ψ	$f_1 = 7 \pmod 8$		
	2Ψ	$f_1 = 7 \pmod 8$	$f_1\rho_1 = 8\Psi + 1 \pmod{(16 \cdot \Psi)}$	
	6Ψ	$f_1 = 3 \pmod 8$		
4Ψ	2Ψ or 6Ψ	$f_1 = 7 \pmod 8$	$f_1\rho_1 = 1 \pmod{(16 \cdot \Psi)}$	f_2
	4Ψ	$f_1 = 1 \pmod 8$ or $f_1 = 5 \pmod 8$		
	0	$f_1 = 1 \pmod 8$	$f_1\rho_1 = 8\Psi + 1 \pmod{(16 \cdot \Psi)}$	
	2Ψ or 6Ψ	$f_1 = 3 \pmod 8$		
	0 or 4Ψ	$f_1 = 3 \pmod 8$ or $f_1 = 7 \pmod 8$		
	0	$f_1 = 5 \pmod 8$		
	2Ψ	$f_1 = 5 \pmod 8$	$f_1\rho_1 = 1 \pmod{(16 \cdot \Psi)}$	$f_2 + 4\Psi$ $\pmod{8\Psi}$
	6Ψ	$f_1 = 1 \pmod 8$		
	2Ψ	$f_1 = 1 \pmod 8$	$f_1\rho_1 = 8\Psi + 1 \pmod{(16 \cdot \Psi)}$	
	6Ψ	$f_1 = 5 \pmod 8$		
6Ψ	0	$f_1 = 1 \pmod 8$ or $f_1 = 5 \pmod 8$	$f_1\rho_1 = 2\Psi \cdot \big((k_\Psi + 6) \pmod 8\big)$ $+1 \pmod{(16 \cdot \Psi)}$	f_2
	4Ψ	-		
	2Ψ or 6Ψ	$f_1 = 1 \pmod 8$	$f_1\rho_1 = 1 \pmod{(16 \cdot \Psi)}$	
	0	$f_1 = 3 \pmod 8$ or $f_1 = 7 \pmod 8$	$f_1\rho_1 = 2\Psi \cdot \big((k_\Psi + 2) \pmod 8\big)$ $+1 \pmod{(16 \cdot \Psi)}$	
	2Ψ or 6Ψ	$f_1 = 5 \pmod 8$	$f_1\rho_1 = 8\Psi + 1 \pmod{(16 \cdot \Psi)}$	

Proof. $\rho(x)$ is an inverse CPP of $\pi(x)$ if

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

Taking into account Lemma 3.1, after some algebraic manipulations, equation (13) is equivalent to

$$\begin{aligned}(f_1\rho_1 - 1) \cdot x + (f_1\rho_2 + f_2\rho_1^2) \cdot x^2 + (f_1\rho_3 + 2f_2\rho_2\rho_1 + f_3\rho_1^3) \cdot x^3 + (3f_3\rho_1^2\rho_2 + 2f_2\rho_3\rho_1 + f_2\rho_2^2) \cdot x^4 + \\ +(3f_3\rho_1^2\rho_3 + 3f_3\rho_1\rho_2^2) \cdot x^5 + (f_3\rho_2^3 + f_2\rho_3^2) \cdot x^6 + 3f_3\rho_1\rho_3^2 \cdot x^7 = 0 \pmod L, \forall x \in \{0, 1, \ldots, L-1\}.\end{aligned} \tag{14}$$

Because $\pi(x)$ and $\rho(x)$ are true CPPs, from Lemma 3.1 it results that $\rho_3 = f_3 = k_3 \cdot 2\Psi$, with $k_3 \in \{1, 2, 3\}$. 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,

Table 4: Determining coefficients ρ_2 and ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_3, f_2 and f_1 when $f_3 = 2\Psi$ and $L = 48\Psi$ ($k_\Psi = (2\Psi) \pmod{24}$).

f_3	f_2	Condition for f_1	k_Ψ	k	ρ_2
2Ψ	0	$f_1 \in \{1, 13\} \pmod{24}$	10 or 22	$(k_\Psi + 2) \pmod{24}$	f_2
		$f_1 \in \{9, 21\} \pmod{24}$	2 or 14		
		$f_1 \in \{5, 17\} \pmod{24}$	2 or 14	$(k_\Psi + 10) \pmod{24}$	
		$f_1 \in \{9, 21\} \pmod{24}$	10 or 22		
		$f_1 \in \{3, 15\} \pmod{24}$	2 or 14	$(k_\Psi + 14) \pmod{24}$	
		$f_1 \in \{7, 19\} \pmod{24}$	10 or 22		
		$f_1 \in \{3, 15\} \pmod{24}$	10 or 22	$(k_\Psi + 22) \pmod{24}$	
		$f_1 \in \{11, 23\} \pmod{24}$	2 or 14		
	6Ψ or 18Ψ	$f_1 = 1 \pmod{24}$	22	$(k_\Psi + 2) \pmod{24}$	
		$f_1 = 9 \pmod{24}$	14		
		$f_1 = 13 \pmod{24}$	10		
		$f_1 = 21 \pmod{24}$	2		
		$f_1 = 5 \pmod{24}$	2	$(k_\Psi + 10) \pmod{24}$	
		$f_1 = 9 \pmod{24}$	22		
		$f_1 = 17 \pmod{24}$	14		
		$f_1 = 21 \pmod{24}$	10		
		$f_1 = 1 \pmod{24}$	10	$(k_\Psi + 14) \pmod{24}$	
		$f_1 = 9 \pmod{24}$	2		
		$f_1 = 13 \pmod{24}$	22		
		$f_1 = 21 \pmod{24}$	14		
		$f_1 = 5 \pmod{24}$	14	$(k_\Psi + 22) \pmod{24}$	
		$f_1 = 9 \pmod{24}$	10		
		$f_1 = 17 \pmod{24}$	2		
		$f_1 = 21 \pmod{24}$	22		
	12Ψ	$f_1 \in \{1, 7, 13, 19\} \pmod{24}$	10 or 22	$(k_\Psi + 2) \pmod{24}$	
		$f_1 \in \{3, 9, 15, 21\} \pmod{24}$	2 or 14		
		$f_1 \in \{5, 11, 17, 23\} \pmod{24}$	2 or 14	$(k_\Psi + 10) \pmod{24}$	
		$f_1 \in \{3, 9, 15, 21\} \pmod{24}$	10 or 22		

$2\Psi = 2 \pmod{8}$ 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 $2\Psi = 22 \pmod{24}$.

Thus, for $L = 16\Psi$ and $\rho_2 = f_2 = k_2 \cdot 2\Psi$, with $k_2 \in \{0, 1, 2, 3\}$, (14) is equivalent to

$$\begin{gathered}(f_1\rho_1 - 1) \cdot x + 2k_2\Psi \cdot (f_1 + \rho_1^2) \cdot x^2 + 2\Psi \cdot (k_3 f_1 + 4k_2^2\Psi\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +4k_2\Psi^2 \cdot (3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2\Psi) \cdot x^4 + 4k_3\Psi^2 \cdot (2k_2^2\Psi\rho_1 + 3k_3\rho_1^2) \cdot x^5 + 8k_2k_3^2\Psi^3 \cdot x^6 + \\ +8k_3^3\Psi^3\rho_1 \cdot x^7 = 0 \pmod{16\Psi}, \forall x \in \{0, 1, \ldots, 16\Psi - 1\}.\end{gathered} \tag{15}$$

For $L = 16\Psi$, $f_2 = k_2 \cdot 2\Psi$ and $\rho_2 = ((k_2 + 2) \pmod{4}) \cdot 2\Psi$, with $k_2 \in \{0, 1, 2, 3\}$,

Table 5: Determining coefficients ρ_2 and ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_3, f_2 and f_1 when $f_3 = 2\Psi$ and $L = 48\Psi$ ($k_\Psi = (2\Psi) \pmod{24}$).

f_3	f_2	Condition for f_1	k_Ψ	k	ρ_2
2Ψ	6Ψ	$f_1 = 15 \pmod{24}$	2	$(k_\Psi + 2)$ (mod 24)	$f_2 + 12\Psi$ (mod 24Ψ)
		$f_1 = 7 \pmod{24}$	10		
		$f_1 = 3 \pmod{24}$	14		
		$f_1 = 19 \pmod{24}$	22		
		$f_1 = 23 \pmod{24}$	2	$(k_\Psi + 10)$ (mod 24)	
		$f_1 = 15 \pmod{24}$	10		
		$f_1 = 11 \pmod{24}$	14		
		$f_1 = 3 \pmod{24}$	22		
		$f_1 = 3 \pmod{24}$	2	$(k_\Psi + 14)$ (mod 24)	
		$f_1 = 19 \pmod{24}$	10		
		$f_1 = 15 \pmod{24}$	14		
		$f_1 = 7 \pmod{24}$	22		
		$f_1 = 11 \pmod{24}$	2	$(k_\Psi + 22)$ (mod 24)	
		$f_1 = 3 \pmod{24}$	10		
		$f_1 = 23 \pmod{24}$	14		
		$f_1 = 15 \pmod{24}$	22		
	18Ψ	$f_1 = 3 \pmod{24}$	2	$(k_\Psi + 2)$ (mod 24)	
		$f_1 = 19 \pmod{24}$	10		
		$f_1 = 15 \pmod{24}$	14		
		$f_1 = 7 \pmod{24}$	22		
		$f_1 = 11 \pmod{24}$	2	$(k_\Psi + 10)$ (mod 24)	
		$f_1 = 3 \pmod{24}$	10		
		$f_1 = 23 \pmod{24}$	14		
		$f_1 = 15 \pmod{24}$	22		
		$f_1 = 15 \pmod{24}$	2	$(k_\Psi + 14)$ (mod 24)	
		$f_1 = 7 \pmod{24}$	10		
		$f_1 = 3 \pmod{24}$	14		
		$f_1 = 19 \pmod{24}$	22		
		$f_1 = 23 \pmod{24}$	2	$(k_\Psi + 22)$ (mod 24)	
		$f_1 = 15 \pmod{24}$	10		
		$f_1 = 11 \pmod{24}$	14		
		$f_1 = 3 \pmod{24}$	22		

(14) is equivalent to

$$\begin{gathered}(f_1\rho_1 - 1)\cdot x + 2\Psi\cdot(2f_1 + f_1k_2 + k_2\rho_1^2)\cdot x^2 + 2\Psi\cdot(k_3f_1 + 4k_2^2\Psi\rho_1 + k_3\rho_1^3)\cdot x^3 + \\ +4\Psi^2\cdot(3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3\Psi + 2k_3\rho_1^2)\cdot x^4 + 4k_3\Psi^2\cdot(2k_2^2\Psi\rho_1 + 3k_3\rho_1^2)\cdot x^5 + \\ +8k_2k_3^2\Psi^3\cdot x^6 + 8k_3^3\Psi^3\rho_1\cdot x^7 = 0 \pmod{16\Psi}, \forall x \in \{0,1,\ldots,16\Psi-1\}.\end{gathered} \tag{16}$$

For $L = 48\Psi$, $\rho_2 = f_2 = k_2\cdot 6\Psi$, with $k_2 \in \{0,1,2,3\}$, (14) is equivalent to

$$\begin{gathered}(f_1\rho_1 - 1)\cdot x + 6k_2\Psi\cdot(f_1 + \rho_1^2)\cdot x^2 + 2\Psi\cdot(k_3f_1 + 12k_2^2\Psi\rho_1 + k_3\rho_1^3)\cdot x^3 + \\ +12k_2\Psi^2\cdot(3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2\Psi)\cdot x^4 + 12k_3\Psi^2\cdot(2k_2^2\Psi\rho_1 + k_3\rho_1^2)\cdot x^5 + 24k_2k_3^2\Psi^3\cdot x^6 + \\ +24k_3^3\Psi^3\rho_1\cdot x^7 + 16k_3^4\Psi^4\cdot x^9 = 0 \pmod{48\Psi}, \forall x \in \{0,1,\ldots,48\Psi-1\}.\end{gathered} \tag{17}$$

Table 6: Determining coefficients ρ_2 and ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_3, f_2 and f_1 when $f_3 = 4\Psi$ and $L = 48\Psi$ ($k_\Psi = (2\Psi) \pmod{24}$).

f_3	f_2	Condition for f_1	k_Ψ	k	ρ_2
4Ψ	0	$f_1 \in \{3,9,15,21\} \pmod{24}$	2	$(k_\Psi + 2) \pmod{24}$	f_2
		$f_1 \in \{5,11,17,23\} \pmod{24}$	10		
		$f_1 \in \{1,7,13,19\} \pmod{24}$	2	$(k_\Psi + 10) \pmod{24}$	
		$f_1 \in \{3,9,15,21\} \pmod{24}$	10		
		$f_1 \in \{3,9,15,21\} \pmod{24}$	14	$(k_\Psi + 14) \pmod{24}$	
		$f_1 \in \{5,11,17,23\} \pmod{24}$	22		
		$f_1 \in \{1,7,13,19\} \pmod{24}$	14	$(k_\Psi + 22) \pmod{24}$	
		$f_1 \in \{3,9,15,21\} \pmod{24}$	22		
	6Ψ or 18Ψ	$f_1 = 3 \pmod{24}$	2	$(k_\Psi + 2) \pmod{24}$	
		$f_1 = 11 \pmod{24}$	10		
		$f_1 = 15 \pmod{24}$	14		
		$f_1 = 23 \pmod{24}$	22		
		$f_1 = 3 \pmod{24}$	10	$(k_\Psi + 10) \pmod{24}$	
		$f_1 = 7 \pmod{24}$	14		
		$f_1 = 15 \pmod{24}$	22		
		$f_1 = 19 \pmod{24}$	2		
		$f_1 = 3 \pmod{24}$	14	$(k_\Psi + 14) \pmod{24}$	
		$f_1 = 11 \pmod{24}$	22		
		$f_1 = 15 \pmod{24}$	2		
		$f_1 = 23 \pmod{24}$	10		
		$f_1 = 3 \pmod{24}$	22	$(k_\Psi + 22) \pmod{24}$	
		$f_1 = 7 \pmod{24}$	2		
		$f_1 = 15 \pmod{24}$	10		
		$f_1 = 19 \pmod{24}$	14		
	12Ψ	$f_1 \in \{3,15\} \pmod{24}$	2	$(k_\Psi + 2) \pmod{24}$	
		$f_1 \in \{11,23\} \pmod{24}$	10		
		$f_1 \in \{9,21\} \pmod{24}$	14		
		$f_1 \in \{5,17\} \pmod{24}$	22		
		$f_1 \in \{1,13\} \pmod{24}$	14	$(k_\Psi + 10) \pmod{24}$	
		$f_1 \in \{3,15\} \pmod{24}$	10		
		$f_1 \in \{7,19\} \pmod{24}$	2		
		$f_1 \in \{9,21\} \pmod{24}$	22		
		$f_1 \in \{3,15\} \pmod{24}$	14	$(k_\Psi + 14) \pmod{24}$	
		$f_1 \in \{5,17\} \pmod{24}$	10		
		$f_1 \in \{9,21\} \pmod{24}$	2		
		$f_1 \in \{11,23\} \pmod{24}$	22		
		$f_1 \in \{1,13\} \pmod{24}$	2	$(k_\Psi + 22) \pmod{24}$	
		$f_1 \in \{3,15\} \pmod{24}$	22		
		$f_1 \in \{7,19\} \pmod{24}$	14		
		$f_1 \in \{9,21\} \pmod{24}$	10		

For $L = 48\Psi$, $f_2 = k_2 \cdot 6\Psi$ and $\rho_2 = ((k_2 + 2) \pmod{4}) \cdot 6\Psi$, with $k_2 \in \{0,1,2,3\}$,

Table 7: Determining coefficients ρ_2 and ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_3, f_2 and f_1 when $f_3 = 4\Psi$ and $L = 48\Psi$ ($k_\Psi = (2\Psi) \pmod{24}$).

f_3	f_2	Condition for f_1	k_Ψ	k	ρ_2
4Ψ	6Ψ	$f_1 = 9 \pmod{24}$	2	$(k_\Psi + 2)$ $\pmod{24}$	$f_2 + 12\Psi$ $\pmod{24\Psi}$
		$f_1 = 17 \pmod{24}$	10		
		$f_1 = 21 \pmod{24}$	14		
		$f_1 = 5 \pmod{24}$	22		
		$f_1 = 1 \pmod{24}$	2	$(k_\Psi + 10)$ $\pmod{24}$	
		$f_1 = 9 \pmod{24}$	10		
		$f_1 = 13 \pmod{24}$	14		
		$f_1 = 21 \pmod{24}$	22		
		$f_1 = 21 \pmod{24}$	2	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 = 5 \pmod{24}$	10		
		$f_1 = 9 \pmod{24}$	14		
		$f_1 = 17 \pmod{24}$	22		
		$f_1 = 13 \pmod{24}$	2	$(k_\Psi + 22)$ $\pmod{24}$	
		$f_1 = 21 \pmod{24}$	10		
		$f_1 = 1 \pmod{24}$	14		
		$f_1 = 9 \pmod{24}$	22		
	18Ψ	$f_1 = 21 \pmod{24}$	2	$(k_\Psi + 2)$ $\pmod{24}$	
		$f_1 = 5 \pmod{24}$	10		
		$f_1 = 9 \pmod{24}$	14		
		$f_1 = 17 \pmod{24}$	22		
		$f_1 = 13 \pmod{24}$	2	$(k_\Psi + 10)$ $\pmod{24}$	
		$f_1 = 21 \pmod{24}$	10		
		$f_1 = 1 \pmod{24}$	14		
		$f_1 = 9 \pmod{24}$	22		
		$f_1 = 9 \pmod{24}$	2	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 = 17 \pmod{24}$	10		
		$f_1 = 21 \pmod{24}$	14		
		$f_1 = 5 \pmod{24}$	22		
		$f_1 = 1 \pmod{24}$	2	$(k_\Psi + 22)$ $\pmod{24}$	
		$f_1 = 9 \pmod{24}$	10		
		$f_1 = 13 \pmod{24}$	14		
		$f_1 = 21 \pmod{24}$	22		

(14) is equivalent to

$$\begin{gathered}(f_1\rho_1 - 1) \cdot x + 6\Psi \cdot (k_2 f_1 + k_2\rho_1^2 + 2f_1) \cdot x^2 + 2\Psi \cdot (k_3 f_1 + 12k_2^2\Psi\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +12\Psi^2 \cdot (3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3\Psi + 2k_3\Psi^2\rho_1^2) \cdot x^4 + 12k_3\Psi^2 \cdot (2k_2^2\Psi\rho_1 + k_3\rho_1^2) \cdot x^5 + \\ +24k_2k_3^2\Psi^3 \cdot x^6 + 24k_3^3\Psi^3\rho_1 \cdot x^7 + 16k_3^4\Psi^4 \cdot x^9 = 0 \pmod{48\Psi}, \forall x \in \{0, 1, \ldots, 48\Psi - 1\}.\end{gathered} \tag{18}$$

Because $(2\Psi) \mid L$, from (15), (16), (17), or (18), we have

$$(f_1\rho_1 - 1) \cdot x = 0 \pmod{2\Psi}, \forall x \in \{0, 1, \ldots, L - 1\}. \tag{19}$$

Table 8: Determining coefficients ρ_2 and ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_3, f_2 and f_1 when $f_3 = 6\Psi$ and $L = 48\Psi$ ($k_\Psi = (2\Psi) \pmod{24}$).

f_3	f_2	Condition for f_1	k_Ψ	k	ρ_2
6Ψ	0	$f_1 \in \{7, 11, 19, 23\} \pmod{24}$	10 or 22	$(k_\Psi + 2)$ $\pmod{24}$	f_2
		$f_1 \in \{7, 11, 19, 23\} \pmod{24}$	2 or 14	$(k_\Psi + 10)$ $\pmod{24}$	
		$f_1 \in \{1, 5, 13, 17\} \pmod{24}$	10 or 22	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 \in \{1, 5, 13, 17\} \pmod{24}$	2 or 14	$(k_\Psi + 22)$ $\pmod{24}$	
	6Ψ or 18Ψ	$f_1 \in \{5, 13\} \pmod{24}$	10	$(k_\Psi + 2)$ $\pmod{24}$	
		$f_1 \in \{1, 17\} \pmod{24}$	22		
		$f_1 \in \{5, 13\} \pmod{24}$	2	$(k_\Psi + 10)$ $\pmod{24}$	
		$f_1 \in \{1, 17\} \pmod{24}$	14		
		$f_1 \in \{1, 17\} \pmod{24}$	10	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 \in \{5, 13\} \pmod{24}$	22		
		$f_1 \in \{1, 17\} \pmod{24}$	2	$(k_\Psi + 22)$ $\pmod{24}$	
		$f_1 \in \{5, 13\} \pmod{24}$	14		
	12Ψ	$f_1 \in \{1, 5, 7, 11, 13,$ $17, 19, 23\} \pmod{24}$	10 or 22	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 \in \{1, 5, 7, 11, 13,$ $17, 19, 23\} \pmod{24}$	2 or 14	$(k_\Psi + 22)$ $\pmod{24}$	
	6Ψ	$f_1 \in \{7, 23\} \pmod{24}$	10	$(k_\Psi + 2)$ $\pmod{24}$	$f_2 + 12\Psi$ $\pmod{24\Psi}$
		$f_1 \in \{11, 19\} \pmod{24}$	22		
		$f_1 \in \{7, 23\} \pmod{24}$	2	$(k_\Psi + 10)$ $\pmod{24}$	
		$f_1 \in \{11, 19\} \pmod{24}$	14		
		$f_1 \in \{7, 23\} \pmod{24}$	22	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 \in \{11, 19\} \pmod{24}$	10		
		$f_1 \in \{7, 23\} \pmod{24}$	14	$(k_\Psi + 22)$ $\pmod{24}$	
		$f_1 \in \{11, 19\} \pmod{24}$	2		
	18Ψ	$f_1 \in \{11, 19\} \pmod{24}$	10	$(k_\Psi + 2)$ $\pmod{24}$	
		$f_1 \in \{7, 23\} \pmod{24}$	22		
		$f_1 \in \{11, 19\} \pmod{24}$	2	$(k_\Psi + 10)$ $\pmod{24}$	
		$f_1 \in \{7, 23\} \pmod{24}$	14		
		$f_1 \in \{11, 19\} \pmod{24}$	22	$(k_\Psi + 14)$ $\pmod{24}$	
		$f_1 \in \{7, 23\} \pmod{24}$	10		
		$f_1 \in \{11, 19\} \pmod{24}$	14	$(k_\Psi + 22)$ $\pmod{24}$	
		$f_1 \in \{7, 23\} \pmod{24}$	2		

Equation (19) is equivalent to

$$f_1\rho_1 = 1 \pmod{2\Psi} \Leftrightarrow f_1\rho_1 = 2\Psi \cdot k + 1 \pmod{L}, \text{ with } k \in \{0, 1, 2, \ldots, 7\} \text{ when } L = 16\Psi, \text{ and } k \in \{0, 1, 2, \ldots, 23\} \text{ when } L = 48\Psi. \tag{20}$$

According to Theorem 57 from [14], we note that congruence $f_1\rho_1 = 2\Psi \cdot k + 1 \pmod{L}$ has only one solution ρ_1 modulo L when $L = 16\Psi$ or when $L = 48\Psi$ and $f_1 = 1 \pmod{3}$

or $f_1 = 2 \pmod 3$, because $\gcd(f_1, L) = 1$. When $L = 48\Psi$, with $\Psi = 1 \pmod 3$, $f_1 = 0 \pmod 3$, and $k \in \{1, 4, 7, \ldots, 22\}$, or when $L = 48\Psi$, with $\Psi = 2 \pmod 3$, $f_1 = 0 \pmod 3$, and $k \in \{2, 5, 8, \ldots, 23\}$, congruence $f_1\rho_1 = 2\Psi \cdot k + 1 \pmod L$ has three solutions modulo L because $\gcd(f_1, L) = 3$ and $3 \mid (2\Psi \cdot k + 1)$, but we will show that only the solution that fulfills condition $\rho_1 = 0 \pmod 3$ is valid and it is unique.

With (20), (15) is fulfilled if and only if

$$\begin{gathered} k \cdot x + k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 4k_2^2\Psi\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +2k_2\Psi \cdot (3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2\Psi) \cdot x^4 + 2k_3\Psi \cdot (2k_2^2\Psi\rho_1 + 3k_3\rho_1^2) \cdot x^5 + 4k_2k_3^2\Psi^2 \cdot x^6 + \\ +4k_3^3\Psi^2\rho_1 \cdot x^7 = 0 \pmod 8, \forall x \in \{0, 1, \ldots, 7\}. \end{gathered} \tag{21}$$

When $2\Psi = 2 \pmod 8$, (21) is equivalent to

$$\begin{gathered} k \cdot x + k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 4k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +2k_2 \cdot (3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2) \cdot x^4 + 2k_3 \cdot (2k_2^2\rho_1 + 3k_3\rho_1^2) \cdot x^5 + 4k_2k_3^2 \cdot x^6 + \\ +4k_3^3\rho_1 \cdot x^7 = 0 \pmod 8, \forall x \in \{0, 1, \ldots, 7\}. \end{gathered} \tag{22}$$

When $2\Psi = 6 \pmod 8$, (21) is equivalent to

$$\begin{gathered} k \cdot x + k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 4k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +2k_2 \cdot (k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2) \cdot x^4 + 2k_3 \cdot (2k_2^2\rho_1 + k_3\rho_1^2) \cdot x^5 + 4k_2k_3^2 \cdot x^6 + \\ +4k_3^3\rho_1 \cdot x^7 = 0 \pmod 8, \forall x \in \{0, 1, \ldots, 7\}. \end{gathered} \tag{23}$$

With (20), (16) is fulfilled if and only if

$$\begin{gathered} k \cdot x + (2f_1 + f_1k_2 + k_2\rho_1^2) \cdot x^2 + (k_3 f_1 + 4k_2^2\Psi\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +2\Psi \cdot (3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3\Psi + 2k_3\rho_1^2) \cdot x^4 + 2k_3\Psi \cdot (2k_2^2\Psi\rho_1 + 3k_3\rho_1^2) \cdot x^5 + \\ +4k_2k_3^2\Psi^2 \cdot x^6 + 4k_3^3\Psi^2\rho_1 \cdot x^7 = 0 \pmod 8, \forall x \in \{0, 1, \ldots, 7\}. \end{gathered} \tag{24}$$

When $2\Psi = 2 \pmod 8$, (24) is equivalent to

$$\begin{gathered} k \cdot x + 2 \cdot (2f_1 + f_1k_2 + k_2\rho_1^2) \cdot x^2 + (k_3 f_1 + 4k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +2 \cdot (3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3 + 2k_3\rho_1^2) \cdot x^4 + 2k_3 \cdot (2k_2^2\rho_1 + 3k_3\rho_1^2) \cdot x^5 + \\ +4k_2k_3^2 \cdot x^6 + 4k_3^3\rho_1 \cdot x^7 = 0 \pmod 8, \forall x \in \{0, 1, \ldots, 7\} \end{gathered} \tag{25}$$

and when $2\Psi = 6 \pmod 8$, (24) is equivalent to

$$\begin{gathered} k \cdot x + 2 \cdot (2f_1 + f_1k_2 + k_2\rho_1^2) \cdot x^2 + (k_3 f_1 + 4k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +2 \cdot (k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3 + 2k_3\rho_1^2) \cdot x^4 + 2k_3 \cdot (2k_2^2\rho_1 + k_3\rho_1^2) \cdot x^5 + \\ +4k_2k_3^2 \cdot x^6 + 4k_3^3\rho_1 \cdot x^7 = 0 \pmod 8, \forall x \in \{0, 1, \ldots, 7\}. \end{gathered} \tag{26}$$

Solutions (k, ρ_1) of equations (22), (23), (25), and (26) for each value of $f_3 \in \{2\Psi, 4\Psi, 6\Psi\}$, $f_2 \in \{0, 2\Psi, 4\Psi, 6\Psi\}$, and $f_1 \pmod 8 \in \{1, 3, 5, 7\}$, can be found using specific software programs. We have used symbolic calculus in Matlab for this goal. These solutions are unique for each value of $f_1 \pmod 8$ and they are given in Table 3, unified for the cases when $2\Psi = 2 \pmod 8$ and $2\Psi = 6 \pmod 8$.

With (20), (17) is fulfilled if and only if

$$\begin{gathered} k \cdot x + 3k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\Psi\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +6k_2\Psi \cdot (3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2\Psi) \cdot x^4 + 6k_3\Psi \cdot (2k_2^2\Psi\rho_1 + k_3\rho_1^2) \cdot x^5 + 12k_2k_3^2\Psi^2 \cdot x^6 + \\ +12k_3^3\Psi^2\rho_1 \cdot x^7 + 8k_3^4\Psi^3 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}. \end{gathered} \tag{27}$$

When $2\Psi = 2 \pmod{24}$, (27) is equivalent to

$$\begin{gathered}
k \cdot x + 3k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6k_2 \cdot (3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + k_3\rho_1^2) \cdot x^5 + 12k_2k_3^2 \cdot x^6 + \\
+12k_3^3\rho_1 \cdot x^7 + 8k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{28}$$

When $2\Psi = 10 \pmod{24}$, (27) is equivalent to

$$\begin{gathered}
k \cdot x + 3k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6k_2 \cdot (3k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + k_3\rho_1^2) \cdot x^5 + 12k_2k_3^2 \cdot x^6 + \\
+12k_3^3\rho_1 \cdot x^7 + 16k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{29}$$

When $2\Psi = 14 \pmod{24}$, (27) is equivalent to

$$\begin{gathered}
k \cdot x + 3k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6k_2 \cdot (k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + 3k_3\rho_1^2) \cdot x^5 + 12k_2k_3^2 \cdot x^6 + \\
+12k_3^3\rho_1 \cdot x^7 + 8k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{30}$$

When $2\Psi = 22 \pmod{24}$, (27) is equivalent to

$$\begin{gathered}
k \cdot x + 3k_2 \cdot (f_1 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6k_2 \cdot (k_3\rho_1^2 + 2k_3\rho_1 + 2k_2^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + 3k_3\rho_1^2) \cdot x^5 + 12k_2k_3^2 \cdot x^6 + \\
+12k_3^3\rho_1 \cdot x^7 + 16k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{31}$$

With (20), (18) is fulfilled if and only if

$$\begin{gathered}
k \cdot x + 3 \cdot (2f_1 + 3f_1k_2 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\Psi\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6\Psi \cdot (3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3\Psi + 2k_3\rho_1^2) \cdot x^4 + 6k_3\Psi \cdot (2k_2^2\Psi\rho_1 + k_3\rho_1^2) \cdot x^5 + \\
+12k_2k_3^2\Psi^2 \cdot x^6 + 12k_3^3\Psi^2\rho_1 \cdot x^7 + 8k_3^4\Psi^3 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{32}$$

When $2\Psi = 2 \pmod{24}$, (32) is equivalent to

$$\begin{gathered}
k \cdot x + 3 \cdot (2f_1 + 3f_1k_2 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6 \cdot (3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3 + 2k_3\rho_1^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + k_3\rho_1^2) \cdot x^5 + 12k_2k_3^2 \cdot x^6 + \\
+12k_3^3\rho_1 \cdot x^7 + 8k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{33}$$

When $2\Psi = 10 \pmod{24}$, (32) is equivalent to

$$\begin{gathered}
k \cdot x + 3 \cdot (2f_1 + 3f_1k_2 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6 \cdot (3k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3 + 2k_3\rho_1^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + k_3\rho_1^2) \cdot x^5 + \\
+12k_2k_3^2 \cdot x^6 + 12k_3^3\rho_1 \cdot x^7 + 16k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{34}$$

When $2\Psi = 14 \pmod{24}$, (32) is equivalent to

$$\begin{gathered}
k \cdot x + 3 \cdot (2f_1 + 3f_1k_2 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\
+6 \cdot (k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3 + 2k_3\rho_1^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + 3k_3\rho_1^2) \cdot x^5 + \\
+12k_2k_3^2 \cdot x^6 + 12k_3^3\rho_1 \cdot x^7 + 8k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}.
\end{gathered} \tag{35}$$

When $2\Psi = 22 \pmod{24}$, (32) is equivalent to

$$\begin{gathered} k \cdot x + 3 \cdot (2f_1 + 3f_1k_2 + \rho_1^2) \cdot x^2 + (k_3 f_1 + 12k_2^2\rho_1 + k_3\rho_1^3) \cdot x^3 + \\ +6 \cdot (k_2k_3\rho_1^2 + 2k_2k_3\rho_1 + 2k_2^3 + 2k_3\rho_1^2) \cdot x^4 + 6k_3 \cdot (2k_2^2\rho_1 + 3k_3\rho_1^2) \cdot x^5 + \\ +12k_2k_3^2 \cdot x^6 + 12k_3^3\rho_1 \cdot x^7 + 16k_3^4 \cdot x^9 = 0 \pmod{24}, \forall x \in \{0, 1, \ldots, 23\}. \end{gathered} \tag{36}$$

Solutions (k, ρ_1) of equations (28)-(31) and (33)-(36) for each value of $f_3 \in \{2\Psi, 4\Psi, 6\Psi\}$, $f_2 \in \{0, 6\Psi, 12\Psi, 18\Psi\}$, and $f_1 \pmod{24} \in \{1, 3, \ldots, 23\}$, found by software means, are given in Tables 4-8. When the congruence equation $f_1\rho_1 = 2\Psi \cdot k + 1 \pmod{48\Psi}$ has three solutions in variable $\rho_1 \pmod{48\Psi}$, the valid solution (i.e. that which fulfills one of the equations (28)-(31)) is only $\rho_1 = f_1 \pmod{24}$. We note that, because of condition $(f_1 + f_3) \neq 0 \pmod 3$ for $L = 48\Psi$, for a certain value of f_3, $f_1 \pmod{24}$ can take only 8 different values from the 12 ones from the set $\{1, 3, \ldots, 23\}$. For example, if $f_3 = 2\Psi$ and $k_\Psi = (2\Psi) \pmod{24} = 2$, then $f_3 = 2 \pmod 3$ and $f_1 \pmod{24} \in \{3, 5, 9, 11, 15, 17, 21, 23\}$. □

We note that the inverse CPP from Lemma 3.2 is a true CPP and thus the CPP $\pi(x)$ does not admit an inverse QPP.

From Lemma 3.2, when $L = 16\Psi$, we have $f_1\rho_1 = k_\Psi \cdot (k_\Psi + 2) + 1 \pmod 8$ or $f_1\rho_1 = k_\Psi \cdot (k_\Psi + 6) + 1 \pmod 8$, with $k_\Psi = 2\Psi \pmod 8 \in \{2, 6\}$. Thus, we always have $f_1\rho_1 = 1 \pmod 8$ when $L = 16\Psi$. Also, from Lemma 3.2, when $L = 48\Psi$ we have $f_1\rho_1 = k_\Psi \cdot (k_\Psi + 2) + 1 \pmod{24}$ or $f_1\rho_1 = k_\Psi \cdot (k_\Psi + 10) + 1 \pmod{24}$ or $f_1\rho_1 = k_\Psi \cdot (k_\Psi + 14) + 1 \pmod{24}$ or $f_1\rho_1 = k_\Psi \cdot (k_\Psi + 22) + 1 \pmod{24}$, with $k_\Psi = 2\Psi \pmod{24} \in \{2, 10, 14, 22\}$. This means that $f_1\rho_1 \pmod{24} \in \{1, 9, 17\}$, and thus $f_1\rho_1 = 1 \pmod 8$ and $f_1 = \rho_1 \pmod 8$. In the following theorems we require the values of $f_1 = \rho_1 \pmod 8$ depending on the values of coefficients f_3, f_2, and ρ_2, and on the interleaver length $L \in \{16\Psi, 48\Psi\}$. For CPP interleavers of lengths of the form $L = k_L \cdot 16\Psi$, $k_L \in \{1, 3\}$, fulfilling conditions (6) when $3 \nmid (p_i - 1)$, we have $f_3 = \rho_3 = k_3 \cdot 2\Psi$, with $k_3 \in \{1, 2, 3\}$, $f_2 = k_2 \cdot k_L \cdot 2\Psi$, $\rho_2 = k_2 \cdot k_L \cdot 2\Psi$ or $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi \pmod L$, with $k_2 \in \{0, 1, 2, 3\}$. Values of $f_1 = \rho_1 \pmod 8$ depending on the values of $k_3 \in \{1, 2, 3\}$, $k_2 \in \{0, 1, 2, 3\}$, and ρ_2, for $L = k_L \cdot 16\Psi$, $k_L \in \{1, 3\}$, are given in Table 9.

Table 9: Values of $f_1 = \rho_1 \pmod 8$ depending on the values of $k_2 \in \{0, 1, 2, 3\}$ and of $k_3 \in \{1, 2, 3\}$ for $L = k_L \cdot 16\Psi$, $k_L \in \{1, 3\}$.

k_3	k_2	ρ_2	$f_1 = \rho_1 \pmod 8$
1 or 2 or 3	0 or 2	f_2	1, 3, 5, or 7
1 or 3	1 or 3	f_2	1 or 5
		$f_2 + k_L \cdot 4p \pmod L$	3 or 7
2	1 or 3	f_2	3 or 7
		$f_2 + k_L \cdot 4p \pmod L$	1 or 5

Theorem 3.3. *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 recursive systematic convolutional codes parallel concatenated having the generator matrix* $G = [1, 15/13]$ *(in octal form) and CPP interleavers, fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, with coefficients* $f_3 = k_3 \cdot 2\Psi$*,* $f_2 = k_2 \cdot k_L \cdot 2\Psi$*,* $k_L \in \{1, 3\}$*, and the values of* k_3*,* k_2*,* $k_p = 2\Psi \pmod 8$*, and of coefficient* $f_1 = \rho_1 \pmod 8$ *from Table 10, is upper bounded by the value of 38.*

Table 10: Values of k_3, k_2, k_p, and $f_1 = \rho_1 \pmod 8$ for which the upper bound of the minimum distance for CPP interleavers of lengths of the form (5) is equal to 38 ($f_3 = k_3 \cdot 2\Psi$, $k_3 \in \{1,3\}$, $f_2 = k_2 \cdot k_L \cdot 2\Psi$, $k_2 \in \{0,1,2,3\}$, $k_L \in \{1,3\}$, $k_\Psi = 2\Psi \pmod 8$).

$f_1 = \rho_1 \pmod 8$ (from eq. (50); $\rho_2 = k_2 k_L 2\Psi$)	$f_1 = \rho_1 \pmod 8$ (from eq. (52); $\rho_2 = k_2 k_L 2\Psi$)	$f_1 = \rho_1 \pmod 8$ (from eq. (51); $\rho_2 = (k_2+2)\cdot$ $\cdot k_L 2\Psi \pmod L$)	k_3	k_2	k_Ψ
3	1	-	1	0 or 2	2
7	5	-	1	0 or 2	6
-	1	7	1 or 3	1 or 3	2 or 6
7	5	-	3	0 or 2	2
3	1	-	3	0 or 2	6

Proof. We consider the interleaver pattern of size nine shown in Fig. 1. We note that this interleaver pattern is similar to that in Fig. 1 from [11], but here we consider true CPP-based interleavers instead of QPP-based ones.

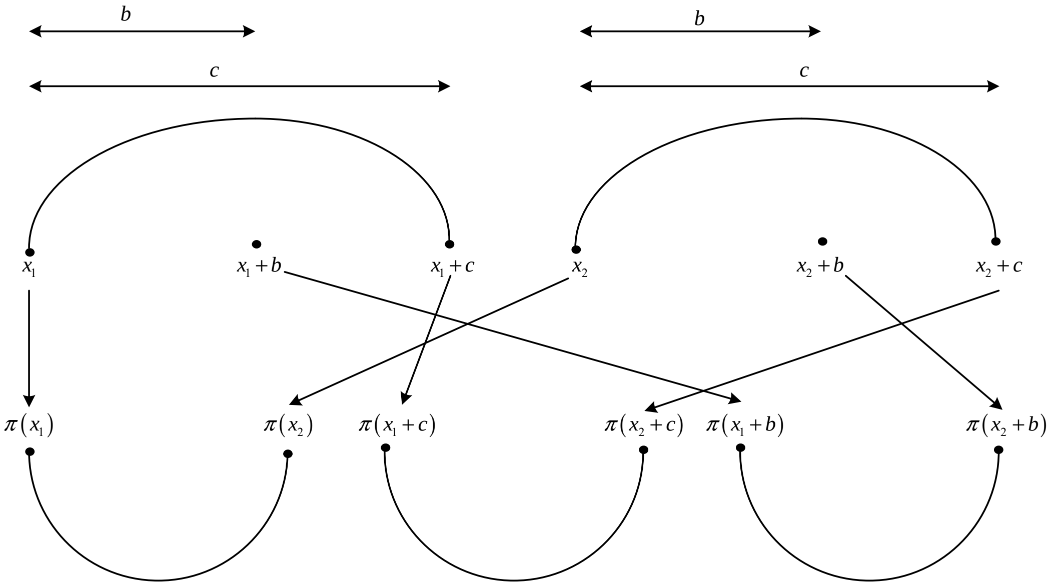

Figure 1: Critical interleaver pattern of size six for CPP-based interleavers

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

$$\begin{cases} x_1 \to \pi(x_1) \\ x_1 + b \to \pi(x_1 + b) \\ x_1 + c \to \pi(x_1 + c) \\ x_2 \to \pi(x_2) = \pi(x_1) + a \\ x_2 + b \to \pi(x_2 + b) = \pi(x_1 + b) + a \\ x_2 + c \to \pi(x_2 + c) = \pi(x_1 + c) + a \end{cases} \tag{37}$$

Writing $x = \rho(\pi(x))$, for $x = x_1$ and $x = x_2$, the equations corresponding to points

x_2+b and x_2+c from (37) are written as

$$\begin{cases} \pi(\rho(\pi(x_2))+b)=\pi(\rho(\pi(x_1))+b)+a \pmod{L} \\ \pi(\rho(\pi(x_2))+c)=\pi(\rho(\pi(x_1))+c)+a \pmod{L} \end{cases} \tag{38}$$

Using the equation corresponding to the point x_2 from (37) in (38), and then replacing $\pi(x_1)$ by x, we have

$$\begin{cases} \pi(\rho(x+a)+b)=\pi(\rho(x)+b)+a \pmod{L} \\ \pi(\rho(x+a)+c)=\pi(\rho(x)+c)+a \pmod{L} \end{cases} \tag{39}$$

For $x=0$ in (39), we have

$$\begin{cases} \pi(\rho(a)+b)=\pi(b)+a \pmod{L} \\ \pi(\rho(a)+c)=\pi(c)+a \pmod{L} \end{cases} \tag{40}$$

and for $x=1$ in (39), we have

$$\begin{cases} \pi(\rho(1+a)+b)=\pi(\rho(1)+b)+a \pmod{L} \\ \pi(\rho(1+a)+c)=\pi(\rho(1)+c)+a \pmod{L} \end{cases} \tag{41}$$

Equations in (40) are equivalent to

$$\begin{cases} b\cdot\rho(a)\cdot\big(2\cdot f_2+3\cdot f_3\cdot(b+\rho(a))\big)=0 \pmod{L} \\ c\cdot\rho(a)\cdot\big(2\cdot f_2+3\cdot f_3\cdot(c+\rho(a))\big)=0 \pmod{L} \end{cases} \tag{42}$$

and equations in (41) are equivalent to

$$\begin{cases} 2\cdot b\cdot f_2\cdot(\rho(a+1)-\rho(1))+ \\ +3\cdot b\cdot f_3\cdot(b\cdot\rho(a+1)+\rho^2(a+1)-b\cdot\rho(1)-\rho^2(1))=0 \pmod{L} \\ 2\cdot c\cdot f_2\cdot(\rho(a+1)-\rho(1))+ \\ +3\cdot c\cdot f_3\cdot(c\cdot\rho(a+1)+\rho^2(a+1)-c\cdot\rho(1)-\rho^2(1))=0 \pmod{L} \end{cases} \tag{43}$$

Because for the lengths considered in (5), and for conditions (6) when $3 \nmid (p_i-1)$, coefficients f_2 and f_3 are multiples of 2Ψ, coefficient f_2 is multiple of 3 for $n_{L,3}=1$, then the congruences from (42) and (43) are fulfilled if the left hand terms are divisible by 8.

In (42) and (43) we consider $a=7$, $b=5$ and $c=8$, for which the interleaver pattern from Fig. 1 leads to minimum distance of $6+2\cdot 7+3\cdot 6=38$, because each of the two 3-weight input error patterns leads to a parity sequence of weight 7 and each of the three 2-weight input error patterns leads to a parity sequence of weight 6.

For $a=7$, $b=5$ and $c=8$, equations in (42) are equivalent to

$$\begin{cases} 5\cdot\rho(7)\cdot\big(2\cdot f_2+3\cdot f_3\cdot(5+\rho(7))\big)=0 \pmod{L} \\ 8\cdot\rho(7)\cdot\big(2\cdot f_2+3\cdot f_3\cdot(8+\rho(7))\big)=0 \pmod{L} \end{cases} \tag{44}$$

and equations in (43) are equivalent to

$$\begin{cases} 5\cdot(\rho(8)-\rho(1))\cdot(2\cdot f_2+3\cdot f_3\cdot(5+\rho(8)+\rho(1)))=0 \pmod{L} \\ 8\cdot(\rho(8)-\rho(1))\cdot(2\cdot f_2+3\cdot f_3\cdot(8+\rho(8)+\rho(1)))=0 \pmod{L} \end{cases} \tag{45}$$

With conditions $f_3=\rho_3=k_3\cdot 2\Psi$, with $k_3\in\{1,2,3\}$, $f_2=k_2\cdot k_L\cdot 2\Psi$, $\rho_2=k_2\cdot k_L\cdot 2\Psi$ or $\rho_2=(k_2+2)\cdot k_L\cdot 2\Psi \pmod{L}$, with $k_2\in\{0,1,2,3\}$, $k_L\in\{1,3\}$, it is obviously that the second equation from (44) and (45) is fulfilled.

With the above coefficients f_3 and f_2, for $\rho_2 = k_2 \cdot k_L \cdot 2\Psi$ the first equation from (44) becomes

$$\begin{gathered}5 \cdot 7 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot 2\Psi + 7^2 \cdot k_3 \cdot 2\Psi) \cdot k_L \cdot 2\Psi \cdot \\ \cdot \big(2 \cdot k_2 + (4 - k_L) \cdot k_3 \cdot (5 + 7\rho_1 + 7^2 \cdot k_2 \cdot k_L \cdot 2\Psi + 7^3 \cdot k_3 \cdot 2\Psi)\big) = 0 \pmod{(k_L \cdot 16\Psi)}\end{gathered} \tag{46}$$

For $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi \pmod{L}$ the first equation from (44) becomes

$$\begin{gathered}5 \cdot 7 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot 2\Psi + 7^2 \cdot k_3 \cdot 2\Psi) \cdot k_L \cdot 2\Psi \cdot \\ \big(2 \cdot k_2 + (4 - k_L) \cdot k_3 \cdot (5 + 7\rho_1 + 7^2 \cdot (k_2 + 2) \cdot k_L \cdot 2\Psi + 7^3 \cdot k_3 \cdot 2\Psi)\big) = 0 \pmod{(k_L \cdot 16\Psi)}\end{gathered} \tag{47}$$

(46) is fulfilled if and only if

$$\begin{gathered}5 \cdot 7 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot 2\Psi + 7^2 \cdot k_3 \cdot 2\Psi) \cdot (2 \cdot k_2 + (4 - k_L) \cdot 5 \cdot k_3 + \\ +(4 - k_L) \cdot 7 \cdot k_3 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot 2\Psi + 7^2 \cdot k_3 \cdot 2\Psi)) = 0 \pmod{8}\end{gathered} \tag{48}$$

and (47) is fulfilled if and only if

$$\begin{gathered}5 \cdot 7 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot 2\Psi + 7^2 \cdot k_3 \cdot 2\Psi) \cdot (2 \cdot k_2 + (4 - k_L) \cdot 5 \cdot k_3 + \\ +(4 - k_L) \cdot 7 \cdot k_3 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot 2\Psi + 7^2 \cdot k_3 \cdot 2\Psi)) = 0 \pmod{8}\end{gathered} \tag{49}$$

With $k_\Psi = 2\Psi \pmod{8}$, (48) and (49) are equivalent to

$$\begin{gathered}3 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot (2 \cdot k_2 + (4 + 3k_L) \cdot k_3 + \\ +(4 + k_L) \cdot k_3 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi)) = 0 \pmod{8}\end{gathered} \tag{50}$$

and

$$\begin{gathered}3 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot (2 \cdot k_2 + (4 + 3k_L) \cdot k_3 + \\ +(4 + k_L) \cdot k_3 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi)) = 0 \pmod{8},\end{gathered} \tag{51}$$

respectively.

Similarly, for $\rho_2 = k_2 \cdot k_L \cdot 2\Psi$ the first equation from (45) is fulfilled if and only if

$$\begin{gathered}3 \cdot (\rho_1 + k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot \\ \cdot (2 \cdot k_2 + (4 - k_L) \cdot k_3 \cdot (5 + \rho_1 + k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi)) = 0 \pmod{8}\end{gathered} \tag{52}$$

and for $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi \pmod{L}$ the first equation from (45) is fulfilled if and only if

$$\begin{gathered}3 \cdot (\rho_1 + (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot \\ \cdot (2 \cdot k_2 + (4 - k_L) \cdot k_3 \cdot (5 + \rho_1 + (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi)) = 0 \pmod{8}\end{gathered} \tag{53}$$

Solutions of equations (50)-(52) in variable $\rho_1 = f_1 \pmod{8}$, found by software means, are given in Tables 10 for possible values of k_3, k_2, and k_Ψ. We note that equation (53) has no solutions.

Thus, for CPPs with values of coefficient $f_1 = \rho_1 \pmod{8}$ according to Table 10, we have the upper bound of the minimum distance equal to 38.

□

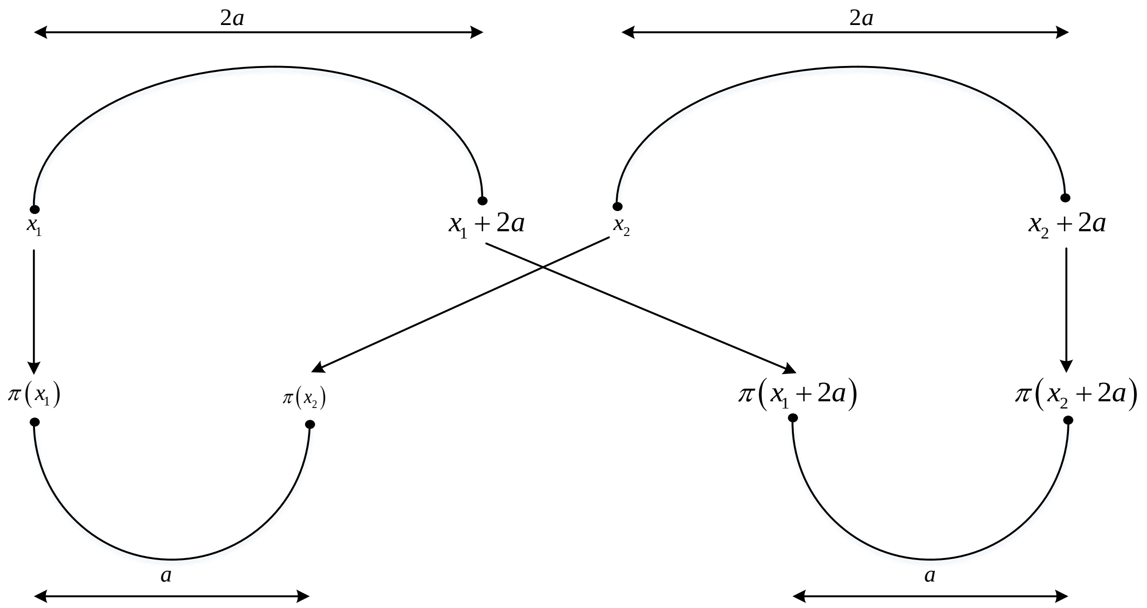

Figure 2: Critical interleaver pattern of size four for CPP-based interleavers

Theorem 3.4. *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 recursive systematic convolutional codes parallel concatenated having the generator matrix* $G = [1, 15/13]$ *(in octal form) and CPP interleavers, fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$, *with coefficients* $f_3 = 2 \cdot k_L \cdot 2\Psi$ *and* $f_2 = k_L \cdot 2\Psi$ *or* $f_2 = 3 \cdot k_L \cdot 2\Psi$, $k_L \in \{1, 3\}$, *is upper bounded by the value of 36.*

Proof. We consider the interleaver pattern of size four shown in Fig. 2.

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

$$\begin{cases} x_1 \to \pi(x_1) \\ x_1 + 2a \to \pi(x_1 + 2a) \\ x_2 \to \pi(x_2) = \pi(x_1) + a \\ x_2 + 2a \to \pi(x_2 + 2a) = \pi(x_1 + 2a) + a \end{cases} \tag{54}$$

Writing $x = \rho(\pi(x))$, for $x = x_2$ the equation corresponding to points $x_2 + 2a$ from (54) is written as

$$\pi(\rho(\pi(x) + a) + 2a) = \pi(x + 2a) + a \pmod{L} \tag{55}$$

For $x = 0$ in (55), we have

$$\pi(\rho(a) + 2a) = \pi(2a) + a \pmod{L} \tag{56}$$

Equation (56) is equivalent to

$$2a \cdot \rho(a) \cdot (2f_2 + 3f_3 \cdot (\rho(a) + 2a)) = 0 \pmod{L} \tag{57}$$

or

$$2a^2 \cdot (\rho_1 + \rho_2 a + \rho_3 a^2) \cdot (2f_2 + 3f_3 \cdot a \cdot (\rho_1 + \rho_2 a + \rho_3 a^2 + 2)) = 0 \pmod{L} \tag{58}$$

As in Theorem 3.3, for $f_3 = \rho_3 = 2 \cdot 2\Psi$, $f_2 = \rho_2 = k_2 \cdot k_L \cdot 2\Psi$, with $k_2 \in \{1, 3\}$, equation (58) becomes

$$\begin{gathered} 2a^2 \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot 2\Psi + a^2 \cdot 2 \cdot 2\Psi) \cdot k_L \cdot 2\Psi \cdot \\ \cdot (2k_2 + (4 - k_L) \cdot 2 \cdot a \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot 2\Psi + a^2 \cdot 2 \cdot 2\Psi + 2)) = 0 \ (\mathrm{mod}\ (k_L \cdot 16\Psi)) \end{gathered} \tag{59}$$

For $f_3 = \rho_3 = 2 \cdot 2\Psi$, $f_2 = k_2 \cdot k_L \cdot 2\Psi$, and $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi \pmod{L}$, with $k_2 \in \{1, 3\}$, equation (58) becomes

$$\begin{gathered} 2a^2 \cdot (\rho_1 + a \cdot (k_2 + 2) \cdot k_L \cdot 2\Psi + a^2 \cdot 2 \cdot 2\Psi) \cdot k_L \cdot 2\Psi \cdot \\ \cdot (2k_2 + (4 - k_L) \cdot 2 \cdot a \cdot (\rho_1 + a \cdot (k_2 + 2) \cdot k_L \cdot 2\Psi + a^2 \cdot 2 \cdot 2\Psi + 2)) = 0 \ (\mathrm{mod}\ (k_L \cdot 16\Psi)) \end{gathered} \tag{60}$$

With $k_p = 2\Psi \pmod{8}$, (59) is fulfilled if and only if

$$\begin{gathered} 2a^2 \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot k_\Psi + a^2 \cdot 2 \cdot k_\Psi) \cdot \\ \cdot (2k_2 + (4 - k_L) \cdot 2 \cdot a \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot k_\Psi + a^2 \cdot 2 \cdot k_\Psi + 2)) = 0 \pmod{8} \end{gathered} \tag{61}$$

and (60) is fulfilled if and only if

$$\begin{gathered} 2a^2 \cdot (\rho_1 + a \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + a^2 \cdot 2 \cdot k_\Psi) \cdot \\ \cdot (2k_2 + (4 - k_L) \cdot 2 \cdot a \cdot (\rho_1 + a \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + a^2 \cdot 2 \cdot k_\Psi + 2)) = 0 \pmod{8} \end{gathered} \tag{62}$$

For $a = 7$, (61) and (62) become

$$\begin{gathered} 2 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot k_\Psi + 2 \cdot k_\Psi) \cdot \\ \cdot (2k_2 + 2k_L \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot k_\Psi + 2 \cdot k_\Psi + 2)) = 0 \pmod{8} \end{gathered} \tag{63}$$

and

$$\begin{gathered} 2 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + 2 \cdot k_\Psi) \cdot \\ \cdot (2k_2 + 2k_L \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + 2 \cdot k_\Psi + 2)) = 0 \pmod{8}, \end{gathered} \tag{64}$$

respectively.

Solutions in variable $\rho_1 = f_1 \pmod{8}$ of equations (63) and (64), for $k_2, k_L \in \{1, 3\}$ and $k_\Psi \in \{2, 6\}$, found by software means, are given in Table 11. We see that we have all possible values of $\rho_1 \pmod{8}$ for the corresponding values of k_3, k_2, and ρ_2, given in Table 9.

Table 11: Values of $\rho_1 \pmod{8}$ fulfilling equation (63) for $\rho_2 = k_2 \cdot k_L \cdot 2\Psi$ and equation (64) for $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi \pmod{L}$, $k_2, k_L \in \{1, 3\}$, for $f_3 = 4\Psi$ (the upper bound of the minimum distance for CPP interleavers of lengths of the form (5) is equal to 36).

$\rho_1 = f_1 \pmod{8}$ (from eq. (63); $\rho_2 = k_2 k_L 2\Psi$)	$\rho_1 = f_1 \pmod{8}$ (from eq. (64); $\rho_2 = (k_2 + 2)\cdot$ $\cdot k_L \cdot 2\Psi \pmod{L}$)	k_3	k_2	k_Ψ
3 or 7	1 or 5	2	1 or 3	2 or 6

For $a = 7$ in (54), the interleaver pattern from Fig. 2 leads to minimum distance of $4 + 2 \cdot 10 + 2 \cdot 6 = 36$, because each of the two 2-weight input error patterns before interleaving leads to a parity sequence of weight 10 and each of the two 2-weight input error patterns after interleaving leads to a parity sequence of weight 6. Thus, the theorem is proven.

□

Theorem 3.5. *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 recursive systematic convolutional codes parallel concatenated having the generator matrix* $G = [1, 15/13]$ *(in octal form) and CPP interleavers, fulfilling conditions* (6) *when* $3 \nmid (p_i - 1)$*, with coefficients* $f_3 = k_3 \cdot 2\Psi$*,* $f_2 = k_2 \cdot k_L \cdot 2\Psi$*,* $k_L \in \{1, 3\}$*, and the values of* k_3*,* k_2*,* $k_p = 2\Psi \pmod 8$*, and coefficient* $f_1 = \rho_1 \pmod 8$ *from Table 12, is upper bounded by the value of 28.*

Table 12: Values of k_3, k_2, $k_\Psi = 2\Psi \pmod 8$, and of $f_1 = \rho_1 \pmod 8$ for which the upper bound of the minimum distance for CPP interleavers of lengths of the form (5) is equal to 28 ($f_3 = k_3 \cdot 2\Psi$, $f_2 = k_2 \cdot k_L \cdot 2\Psi$, $k_L \in \{1, 3\}$).

$f_1 = \rho_1 \pmod 8$ (from eq. (71); $\rho_2 = k_2 k_L 2\Psi$)	$f_1 = \rho_1 \pmod 8$ (from eq. (79) with (80); $\rho_2 = k_2 k_L 2\Psi$)	$f_1 = \rho_1 \pmod 8$ (from eq. (79) with (81); $\rho_2 = (k_2 + 2)\cdot$ $\cdot k_L 2\Psi \pmod L$)	k_3	k_2	k_Ψ
5	7	-	1	0 or 2	2
1	3	-	1	0 or 2	6
5	-	3	1 or 3	1 or 3	2 or 6
3 or 7	1 or 5	-	2	0	2 or 6
1 or 5	3 or 7	-	2	2	2 or 6
1	3	-	3	0 or 2	2
5	7	-	3	0 or 2	6

Proof. We consider again the interleaver pattern of size four shown in Fig. 2, but with the values $2a$ from the two 2-input weight patterns before interleaving replaced by value a. Then equation (55) becomes

$$\pi(\rho(\pi(x) + a) + a) = \pi(x + a) + a \pmod L \tag{65}$$

For $x = 0$ in (65), we have

$$\pi(\rho(a) + a) = \pi(a) + a \pmod L \tag{66}$$

Equation (66) is equivalent to

$$a \cdot \rho(a) \cdot (2f_2 + 3f_3 \cdot (\rho(a) + a)) = 0 \pmod L \tag{67}$$

or

$$a^2 \cdot (\rho_1 + \rho_2 a + \rho_3 a^2) \cdot (2f_2 + 3f_3 \cdot a \cdot (\rho_1 + \rho_2 a + \rho_3 a^2 + 1)) = 0 \pmod L \tag{68}$$

With $f_3 = \rho_3 = k_3 \cdot 2\Psi$, $k_3 \in \{1, 3\}$, and $f_2 = \rho_2 = k_2 \cdot k_L \cdot 2\Psi$, $k_2 \in \{0, 1, 2, 3\}$, $k_L \in \{1, 3\}$, equation (68) becomes

$$\begin{gathered} a^2 \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot 2\Psi + a^2 \cdot k_3 \cdot 2\Psi) \cdot k_L \cdot 2\Psi \cdot \\ (2k_2 + (4 - k_L) \cdot k_3 \cdot a \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot 2\Psi + a^2 \cdot k_3 \cdot 2\Psi + 1)) = 0 \pmod{(k_L \cdot 16\Psi)} \end{gathered} \tag{69}$$

Equation (69) is fulfilled if and only if

$$\begin{gathered} a^2 \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot 2\Psi + a^2 \cdot k_3 \cdot 2\Psi) \cdot \\ (2k_2 + (4 - k_L) \cdot k_3 \cdot a \cdot (\rho_1 + a \cdot k_2 \cdot k_L \cdot 2\Psi + a^2 \cdot k_3 \cdot 2\Psi + 1)) = 0 \pmod 8 \end{gathered} \tag{70}$$

For $a = 7$ and with $k_\Psi = 2\Psi \pmod 8$, equation (70) becomes

$$\begin{gathered} (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot \\ (2k_2 + (4 + k_L) \cdot k_3 \cdot (\rho_1 + 7 \cdot k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi + 1)) = 0 \pmod 8 \end{gathered} \tag{71}$$

For $f_3 = \rho_3 = k_3 \cdot 2\Psi$, $k_3 \in \{1, 3\}$, and $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi$, $k_2 \in \{0, 1, 2, 3\}$, $k_L \in \{1, 3\}$, equation (68) is fulfilled if and only if

$$\begin{gathered} (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot \\ (2k_2 + (4 + k_L) \cdot k_3 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi + 1)) = 0 \pmod 8 \end{gathered} \tag{72}$$

Now we consider $x = 1$ in equation (65). Then, we have

$$\pi(\rho(\pi(1) + a) + a) = \pi(a + 1) + a \pmod L \tag{73}$$

Equation (73) is equivalent to

$$\begin{gathered} \pi(1) + a + \pi(a) + a \cdot \rho(\pi(1) + a) \cdot (2f_2 + 3f_3 \cdot (\rho(\pi(1) + a) + a)) = \\ = \pi(a) + \pi(1) + a \cdot (2f_2 + 3f_3 \cdot (a + 1)) + a \pmod L \end{gathered} \tag{74}$$

or

$$a \cdot (2f_2 \cdot (\rho(\pi(1) + a) - 1) + 3f_3 \cdot (\rho(\pi(1) + a) \cdot (\rho(\pi(1) + a) + a) - (a + 1)) = 0 \pmod L \tag{75}$$

With $f_3 = k_3 \cdot 2\Psi$, $k_3 \in \{1, 3\}$, and $f_2 = k_2 \cdot k_L \cdot 2\Psi$, $k_2 \in \{0, 1, 2, 3\}$, $k_L \in \{1, 3\}$, equation (75) becomes

$$\begin{gathered} a \cdot k_L \cdot 2\Psi \cdot (2k_2 \cdot (\rho(\pi(1) + a) - 1) + \\ +(4 - k_L) \cdot k_3 \cdot (\rho(\pi(1) + a) \cdot (\rho(\pi(1) + a) + a) - (a + 1)) = 0 \pmod{(k_L \cdot 16\Psi)} \end{gathered} \tag{76}$$

Equation (76) is fulfilled if and only if

$$\begin{gathered} a \cdot (2k_2 \cdot (\rho(\pi(1) + a) - 1) + \\ +(4 - k_L) \cdot k_3 \cdot (\rho(\pi(1) + a) \cdot (\rho(\pi(1) + a) + a) - (a + 1)) = 0 \pmod 8 \end{gathered} \tag{77}$$

For $a = 7$ and $k_\Psi = 2\Psi \pmod 8$, equation (77) becomes

$$\begin{gathered} 7 \cdot (2k_2 \cdot (\rho(\pi(1) + 7) - 1) + \\ +(4 - k_L) \cdot k_3 \cdot \rho(\pi(1) + 7) \cdot (\rho(\pi(1) + 7) + 7) = 0 \pmod 8, \end{gathered} \tag{78}$$

or

$$2k_2 + 7 \cdot \rho(\pi(1) + 7) \cdot (2k_2 + (4 - k_L) \cdot k_3 \cdot (\rho(\pi(1) + 7) + 7) = 0 \pmod 8, \tag{79}$$

where for $\rho_3 = k_3 \cdot 2\Psi$, $k_3 \in \{1, 3\}$, $\rho_2 = k_2 \cdot k_L \cdot 2\Psi$, $k_2 \in \{0, 1, 2, 3\}$, $k_L \in \{1, 3\}$, and taking into account that $f_1 = \rho_1 \pmod 8$,

$$\begin{gathered} \rho(\pi(1) + 7) \pmod 8 = 1 + \rho(7) + 7 \cdot \pi(1) \cdot (2\rho_2 + 3\rho_3 \cdot (\pi(1) + 7)) \pmod 8 = \\ = 1 + 7 \cdot (\rho_1 + 7\rho_2 + \rho_3) + 7 \cdot (f_1 + f_2 + f_3) \cdot (2\rho_2 + 3\rho_3 \cdot (f_1 + f_2 + f_3 + 7)) \pmod 8 = \\ = 1 + 7 \cdot (\rho_1 + 7k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) + 7 \cdot (\rho_1 + k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot k_L \cdot k_\Psi \cdot \\ \cdot (2k_2 + (4 - k_L) \cdot k_3 \cdot (\rho_1 + k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi + 7)) \pmod 8 \end{gathered} \tag{80}$$

and for $\rho_3 = k_3 \cdot 2\Psi$, $k_3 \in \{1, 3\}$, $\rho_2 = (k_2 + 2) \cdot k_L \cdot 2\Psi$, $k_2 \in \{0, 1, 2, 3\}$, $k_L \in \{1, 3\}$, and $f_1 = \rho_1 \pmod 8$,

$$\begin{aligned} \rho(\pi(1) + 7) \pmod 8 = 1 + 7 \cdot (\rho_1 + 7 \cdot (k_2 + 2) \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) + \\ +7 \cdot (\rho_1 + k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi) \cdot k_L \cdot k_\Psi \cdot \\ \cdot (2 \cdot (k_2 + 2) + (4 - k_L) \cdot k_3 \cdot (\rho_1 + k_2 \cdot k_L \cdot k_\Psi + k_3 \cdot k_\Psi + 7)) \pmod 8 \end{aligned} \tag{81}$$

Solutions in variable $\rho_1 = f_1 \pmod 8$ of equations (71) and (79), with (80) or (81), found by software means, are given in Tables 12 in terms of possible values of k_3, k_2, and k_Ψ. We note that equation (72) has no solutions.

□

From Theorems 3.3, 3.4, and 3.5 it results that for all CPP interleavers of lengths of the form given in (5), fulfilling conditions (6) when $3 \nmid (p_i - 1)$, the global upper bound of the minimum distance is equal to 38. To get this global upper bound CPP interleavers have to be searched among those with coefficients given in to Table 10.

4 Remarks and Examples

In this section we analyze QPPs and CPPs from [13] (Table III) of interleaver lengths greater than or equal to 592. All these lengths are of the form (5) with $N_p = 1$, and thus $\Psi = p_1 = p$.

Table 13: Minimum distances (d_{min}) and corresponding multiplicities ($N_{d_{min}}$), spread factors (D), nonlinearity degrees (ζ) and refined nonlinearity degrees (ζ') for QPPs and CPPs from [13] (Table III).

L	QPP	d_{min}	$N_{d_{min}}$	ζ	ζ'	CPP	d_{min}	$N_{d_{min}}$	ζ	ζ'	D
592	$74x^2 + 129x$ ([13])	35	276	4	3	$74x^3 + 0x^2 + 315x$	38	558	8	5	20
	$74x^2 + 93x$ (d_{min}-opt-QPP)	38	960								
656	$246x^2 + 21x$	38	1226	4	3	$82x^3 + 164x^2 + 185x$	38	620	8	5	22
688	$86x^2 + 365x$	38	1290	4	3	$258x^3 + 0x^2 + 323x$ ([13])	37	79	8	5	24
						$86x^3 + 0x^2 + 21x$ (d_{min}-opt-CPP)	38	652	8	5	
752	$94x^2 + 165x$	38	1418	4	3	$94x^3 + 188x^2 + 541x$	38	716	8	5	26
816	$102x^2 + 229x$	35	194	4	3	$34x^3 + 102x^2 + 399x$ ([13])	35	98	8	5	28
	$102x^2 + 49x$ (d_{min}-opt-QPP)	38	1546	4	3	$34x^3 + 0x^2 + 19x$ (d_{min}-opt-CPP)	38	782	8	7	
848	$318x^2 + 185x$	38	1610	4	3	$318x^3 + 212x^2 + 157x$	38	812	8	5	28
912	$114x^2 + 29x$	38	1738	4	3	$114x^3 + 114x^2 + 287x$	38	878	8	4	30
944	$118x^2 + 265x$	38	1802	4	3	$354x^3 + 0x^2 + 179x$	38	910	8	5	32
976	$122x^2 + 59x$	38	1866	4	3	$122x^3 + 0x^2 + 307x$	38	942	8	5	32

In Table 13 we have tabulated QPPs and CPPs from [13] (Table III) and we have given the minimum distances (d_{min}) and the corresponding multipicities ($N_{d_{min}}$) for dual trellis termination [15], as well as the spread factors (D), the nonlinearity degrees (ζ) and the refined nonlinearity degrees (ζ') for each PP. In Theorem 1 from [11] it was shown that the upper bound for QPP interleavers and lengths of the form (5), the upper bound of the minimum distance is equal to 38. We note that QPPs of length 592 and 816 and CPPs of lengths 688 and 816, from [13], are not optimal from the point of view of minimum distance. Therefore we also give in Table 13 d_{min}-optimal QPP and CPPs for these lentghs (denoted d_{min}-opt-QPP or d_{min}-opt-CPP). In [13] it was shown that all CPPs from Table 13 are better in terms of frame error rate (FER), than the corresponding QPPs. It is interesting that these better CPPs were found even for interleaver lengths of the form (5) without knowing the results in this paper. This difference in FER performance is explained in that for the same minimum distance, the corresponding multipicities of CPPs are about a half of those of QPPs. We also see that the nonlinearity degree for CPPs is twice that for QPPs. In [16] it was stated that the multiplicity of low-weight codewords is typically a multiple of L/ζ. Thus, the double value of ζ for CPPs compared to that for QPPs explains the values of multiplicities for CPPs as being about a half of those for QPPs. We note that, for interleaver lengths of the form given in (5), this result is general for all QPPs and for all CPPs with coefficients from Table 10. Indeed, nonlinearity degree for QPPs of the interleaver lengths of the form given in (5) is equal to [16]

$$\begin{aligned} \zeta_{QPP} &= \frac{L}{\gcd(2f_2, L)} = \frac{16 \cdot k_L \cdot \Psi}{\gcd(2k_2 \cdot k_L \cdot 2\Psi, 16 \cdot k_L \cdot \Psi)} = \\ &= \begin{cases} (16 \cdot k_L \cdot \Psi)/(4 \cdot k_L \cdot \Psi) = 4 & \text{, for } k_2 \in \{1, 3\} \\ (16 \cdot k_L \cdot \Psi)/(8 \cdot k_L \cdot \Psi) = 2 & \text{, for } k_2 = 2 \end{cases} \end{aligned} \tag{82}$$

In Appendix 1 we proved that nonlinearity degree for CPPs of the interleaver lengths of the form (5), with coefficients from Table 10, is equal to $\zeta_{CPP} = 8$. This assure that we can find better CPPs than QPPs for interleaver lengths of the form (5).

In Table 14 we give the values of p, k_L, k_3, k_2, k_p, and $f_1 = \rho_1 \pmod 8$, defined in Section 3, for CPPs from Table 13. We can see that for all d_{min}-optimal CPPs, values of $f_1 = \rho_1 \pmod 8$ for the corresponding values of k_3, k_2, and k_p, are found among those from Table 10.

Table 14: Values of p, k_L, k_3, k_2, k_p, and $f_1 = \rho_1 \pmod 8$ for CPPs from Table 13.

L	p	k_L	CPP	k_3	k_2	k_p	$f_1 = \rho_1 \pmod 8$
592	37	1	$74x^3 + 0x^2 + 315x$	1	0	2	3
656	41	1	$82x^3 + 164x^2 + 185x$	1	2	2	1
688	43	1	$258x^3 + 0x^2 + 323x$	3	0	6	3
			$86x^3 + 0x^2 + 21x$	1	0	6	5
752	47	1	$94x^3 + 188x^2 + 541x$	1	2	6	5
816	17	3	$34x^3 + 102x^2 + 399x$	1	1	2	7
			$34x^3 + 0x^2 + 19x$	1	0	2	3
848	53	1	$318x^3 + 212x^2 + 157x$	3	2	2	5
912	19	3	$114x^3 + 114x^2 + 287x$	3	1	6	7
944	59	1	$354x^3 + 0x^2 + 179x$	3	0	6	3
976	61	1	$122x^3 + 0x^2 + 307x$	1	0	2	3

We have observed that choosing coefficients of CPP interleavers according to Table 10 and maximizing the spread factor, the most of CPPs lead to the optimal minimum distance of 38. In Theorem 7 from [16], a procedure to efficiently compute the spread factor for PP interleavers is shown. This procedure requires to know the nonlinearity degree of the PP. For QPP interleavers, a closed mathematical formula for ζ of QPP interleavers is achieved. Recently, in [17], we have obtained an algorithm to efficiently compute the nonlinearity degree of CPP interleavers. Thus, we easily can found d_{min}-optimal CPP interleavers for interleaver lengths of the form (5).

5 Conclusions

In this paper we deal with minimum distance of turbo codes with CPP interleavers of length of the form 16Ψ or 48Ψ, with Ψ a product of different prime numbers greater than three, fulfilling conditions (6) when $3 \nmid (p_i - 1)$.

Firstly, we have shown that all these CPPs have an inverse true CPP.

Then, we have obtained three possible upper bounds of the minimum distance (38, 36, and 28) according to different classes of coefficients (as show Tables 10, 11, and 12). Thus, to get d_{min}-optimal CPPs we require to restrict to a smaller class of coefficients, which is beneficial because it fact saves the searching time. Some remarks about CPPs better than QPPs from [13] are made. An insight which saves more of the searching time is to search d_{min}-optimal CPPs among those with the largest spread factor, thus restricting additionally the class of required CPP interleavers.

Acknowledgements

This work was supported by a National Research Grants - ARUT of the TUIASI, project number GnaC2018_39.

Appendix 1

According to the results from [17] the nonlinearity degree of CPP interleavers of even lengths is equal to

$$\zeta_{CPP} = L/(\gcd\big(\gcd(3f_3, L), \gcd(2f_2, L)) + N_{k_0,QNP_1}\big), \tag{83}$$

where N_{k_0,QNP_1} is the number of the common solutions k_0 of congruence equations

$$\begin{cases} 3f_3k_0 = L/2 \pmod{L} \\ (2f_2 + L/2)k_0 = L/2 \pmod{L}. \end{cases} \tag{84}$$

For coefficients given in Table 10, we have

$$\gcd(3f_3, L) = \gcd((4 - k_L) \cdot k_L \cdot k_3 \cdot 2\Psi, k_L \cdot 16\Psi) = k_L \cdot 2\Psi. \tag{85}$$

Because $\gcd(3f_3, L) \mid (L/2)$, the solutions of the first equation from (84) are of the form

$$k_{0,\mathrm{eq1}}(i) = k_{0,f_3} + L \cdot i/\gcd(3f_3, L) = k_{0,f3} + 8 \cdot i, \text{ with } i = 0, 1, \ldots, \gcd(3f_3, L) - 1, \tag{86}$$

where $k_{0,f3}$ is equal to

$$\begin{aligned} k_{0,f_3} = \left(\frac{3f_3}{\gcd(3f_3, L)}\right)^{-1} \cdot \frac{L}{2 \cdot \gcd(3f_3, L)} \pmod{(L/\gcd(3f_3, L))} = \\ = ((4 - k_L) \cdot k_3)^{-1} \cdot 4 \pmod{8} = \\ = \begin{cases} 1 \cdot 4 \pmod{8} = 4, \text{ for } k_L = 3 \text{ and } k_3 = 1, \text{ or } k_L = 1 \text{ and } k_3 = 3, \\ 3 \cdot 4 \pmod{8} = 4, \text{ for } k_L = 1 \text{ and } k_3 = 1, \text{ or } k_L = 3 \text{ and } k_3 = 3. \end{cases} \end{aligned} \tag{87}$$

Thus, the solutions of the first equation from (84) are

$$k_{0,\mathrm{eq1}}(i) = 4 + 8 \cdot i, \text{ with } i = 0, 1, \ldots, k_L \cdot 2\Psi - 1. \tag{88}$$

Similarly, we have

$$\gcd(2f_2 + L/2, L) = \gcd(k_L \cdot 4\Psi \cdot (k_2 + 2), k_L \cdot 16\Psi) = \begin{cases} k_L \cdot 4\Psi, \text{ for } k_2 \in \{1,3\}, \\ k_L \cdot 8\Psi, \text{ for } k_2 = 0, \\ k_L \cdot 16\Psi, \text{ for } k_2 = 2. \end{cases} \tag{89}$$

Because $\gcd(2f_2 + L/2, L) \mid (L/2)$ only for $k_2 \in \{0, 1, 3\}$, the second equation from (84) has solutions only for these three values of k_2. These solutions are of the form

$$k_{0,\mathrm{eq2}}(i) = k_{0,f_2} + L \cdot i / \gcd(2f_2 + L/2, L), \text{ with } i = 0, 1, \ldots, \gcd(2f_2 + L/2, L) - 1, \tag{90}$$

where k_{0,f_2} is equal to

$$\begin{aligned} k_{0,f_2} &= \left(\frac{2f_2 + L/2}{\gcd(2f_2 + L/2, L)}\right)^{-1} \cdot \frac{L}{2 \cdot \gcd(2f_2 + L/2, L)} \pmod{(L/\gcd(2f_2 + L/2, L))} = \\ &= \begin{cases} (k_2 + 2)^{-1} \cdot 2 \pmod 4 = (k_2 + 2) \cdot 2 \pmod 4 = 2, \text{ for } k_2 \in \{1,3\}, \\ 1 \cdot 1 \pmod 2 = 1, \text{ for } k_2 = 0. \end{cases} \end{aligned} \tag{91}$$

Thus, the solutions of the second equation from (84) are

$$k_{0,\mathrm{eq2}}(i) = \begin{cases} 2 + 4 \cdot i, \text{ with } i = 0, 1, \ldots, k_L \cdot 4\Psi - 1, \text{ for } k_2 \in \{1,3\}, \\ 1 + 2 \cdot i, \text{ with } i = 0, 1, \ldots, k_L \cdot 8\Psi - 1, \text{ for } k_2 = 0. \end{cases} \tag{92}$$

Because

$$k_{0,\mathrm{eq1}}(i) \pmod 8 = 4, \forall i = 0, 1, \ldots, k_L \cdot 2\Psi - 1, \tag{93}$$

and

$$\begin{cases} k_{0,\mathrm{eq2}}(i) \pmod 8 \in \{2, 6\}, \forall i = 0, 1, \ldots, k_L \cdot 4\Psi - 1, \text{ for } k_2 \in \{1,3\}, \\ k_{0,\mathrm{eq2}}(i) \pmod 8 \in \{1, 3, 5, 7\}, \forall i = 0, 1, \ldots, k_L \cdot 8\Psi - 1, \text{ for } k_2 = 0, \end{cases} \tag{94}$$

it results that the two equations from (84) have no common solutions, i.e. $N_{k_0,QNP_1} = 0$. Because for $k_3 \in \{1, 3\}$

$$\gcd\big(\gcd(3f_3, L), \gcd(2f_2, L)\big) = \begin{cases} \gcd\big(k_L \cdot 2\Psi, k_L \cdot 4\Psi\big) = k_L \cdot 2\Psi, \text{ for } k_2 \in \{1,3\}, \\ \gcd\big(k_L \cdot 2\Psi, k_L \cdot 16\Psi\big) = k_L \cdot 2\Psi, \text{ for } k_2 = 0, \\ \gcd\big(k_L \cdot 2\Psi, k_L \cdot 8\Psi\big) = k_L \cdot 2\Psi, \text{ for } k_2 = 2, \end{cases} \tag{95}$$

from (83) we have

$$\zeta_{CPP} = \frac{L}{\gcd\big(\gcd(3f_3, L), \gcd(2f_2, L)\big)} = \frac{k_L \cdot 16\Psi}{k_L \cdot 2\Psi} = 8. \tag{96}$$

References

[1] J. Sun, and O.Y. Takeshita, "Interleavers for turbo codes using permutation polynomials over integer rings", *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 101-119, Jan. 2005.

[2] S. Crozier, and P. Guinand, “High-Performance Low-Memory Interleaver Banks for Turbo-Codes”, in *Proc. IEEE 54th Vehic. Technology Conf., VTC 2001 Fall*, Atlantic City, NJ, USA, vol. 4, pp. 2394-2398, 7-11 Oct. 2001.

[3] C. Berrou, Y. Saoter, C. Douillard, S. Kerouedan, and M. Jezequel, “Designing Good Permutations for Turbo Codes: Towards A Single Model”, in *Proc. IEEE Int. Conf. Commun. (ICC’04)*, vol. 1, Paris, France, pp. 341-345, 2004.

[4] 3GPP TS 36.212 V8.3.0, 3rd Generation Partnership Project, Multiplexing and channel coding (Release 8), 2008. [Online] `http://www.etsi.org`.

[5] Y.-L. Chen, J. Ryu, and O.Y. Takeshita, “A Simple Coefficient Test for Cubic Permutation Polynomials over Integer Rings”, *IEEE Comm. Lett.*, vol. 10, no. 7, pp. 549-551, Jul. 2006.

[6] H. Zhao, and P. Fan, “A Note on “A Simple Coefficient Test for Cubic Permutation Polynomials over Integer Rings””, *IEEE Comm. Lett.*, vol. 11, no. 12, p. 991, Dec. 2007.

[7] J. Ryu, “Permutation polynomials of higher degrees for turbo code interleavers”, *IEICE Trans. Commun.*, vol. E95-B, no. 12, pp. 3760-3762, Dec. 2012.

[8] L. Trifina, and D. Tarniceriu, “Analysis of cubic permutation polynomials for turbo codes”, *Wirel. Person. Commun.*, vol. 69, no. 1, pp. 1-22, Mar. 2013.

[9] J. Ryu, L. Trifina, and H. Balta, “The limitation of permutation polynomial interleavers for turbo codes and a scheme for dithering permutation polynomials”, *AEU Int. J. Electron. Commun.*, vol. 69, no. 10, pp. 1550-1556, Oct. 2015.

[10] L. Trifina, J. Ryu, and D. Tarniceriu, “Up to five degree permutation polynomial interleavers for short length LTE turbo codes with optimum minimum distance”, In *Proc. IEEE Int. Symp. Signals, Circ., Syst. (ISSCS 2017)*, Iasi, Romania, 6 pages, July 13-14, 2017.

[11] E. Rosnes, “On the minimum distance of turbo codes with quadratic permutation polynomial interleavers”, *IEEE Trans. Inform. Theory*, vol. 58, no. 7, pp. 4781-4795, Jul. 2012.

[12] L. Trifina, J. Ryu, D. Tarniceriu, and A.-M. Rotopanescu, “Some lengths for which CPP interleavers have weaker minimum distances than QPP interleavers”, submitted for possible publication (under review), 2019.

[13] L. Trifina, and D. Tarniceriu, “On the Equivalence of Cubic Permutation Polynomial and ARP Interleavers for Turbo Codes”, *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 473-485, Feb. 2017.

[14] G. H. Hardy, and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford University Press, 1975.

[15] P. Guinand, and J. Lodge, “Trellis termination for turbo encoders”, in *Proc. 17th Biennial Symp. Commun.*, Queen’s University, Kingston, Canada, pp. 389-392, 30 May - 1 June, 1994.

[16] O.Y. Takeshita, “Permutation Polynomial Interleavers: An Algebraic-Geometric Perspective”, *IEEE Trans. Inform. Theory*, vol. 53, no. 6, pp. 2116-2132, Jun. 2007.

[17] L. Trifina, D. Tarniceriu, and A.-M. Rotopanescu, “Nonlinearity Degree for CPP, 4-PP, and 5-PP Interleavers for Turbo Codes”, *Int. Conf. Electron., Comput., Artif. Intell. (ECAI)*, Pitesti, Romania, 8 pages, 27 Jun.-29 Jun. 2019.