Some lengths for which CPP interleavers have weaker minimum distances than QPP interleavers

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

Abstract

In this paper we obtain an upper bound on the minimum distance of turbo codes using true cubic permutation polynomial (CPP) interleavers of some particular lengths. We address interleavers of lengths of the form $8p$ or $24p$, with p a prime number so that $3 \mid (p-1)$, used in classical 1/3 rate turbo codes with recursive systematic convolutional component codes having generator matrix $G = [1, 15/13]$, in octal form. We prove that 27 is an upper bound on the minimum distance for these types of lengths. We also derive the coefficients of the inverse true CPP for a true CPP of the considered lengths.

Keywords: PP interleaver , CPP, QPP, minimum distance, turbo codes

1 Introduction

Permutation polynomials (PPs) used as interleavers for turbo codes [1–10] have gained a high interest because of their advantages as low complexity and algebraic properties so that they are easily to be designed and implemented. Quadratic permutation polynomials (QPPs) have been adopted as interleavers for Long Term Evolution (LTE) standard [11]. Other known performant interleavers, which are not fully algebraic, are dithered relative prime (DRP) interleavers [12] and almost regular permutation (ARP) interleavers [13,14].

In [5] some upper bounds on the minimum distance of turbo codes with QPP interleavers have been obtained. A partial upper bound on the minimum distance of turbo codes with any degree PP interleavers has been obtained later in [9].

In this paper we deal with the minimum distance of turbo codes with true cubic permutation polynomial (CPP) interleavers (detailed in Subsection 2.2) of lengths of the form $8p$ or $24p$, with p a prime number so that $3 \mid (p-1)$.

1.1 Contributions

The main contributions in this paper are:

- we prove that for the above mentioned interleaver lengths, the minimum distance of 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, is upper bounded by the value of 27.
- we prove that for the above mentioned interleaver lengths a true CPP admits a true inverse CPP and we derive the coefficients of this inverse CPP.

- we give some examples of CPPs and QPPs with optimal minimum distance for four small to large interleaver lengths and we make some remarks about PPs of degree higher than three for the conisdered interleaver lengths in the paper.

The paper is structured as follows. In Section 2 some preliminaries about CPPs are presented. The main result is proved in Section 3. In Section 4 we give four examples of CPPs and QPPs with optimal minimum distance, with comments on their performances and in Section 5 some conclusions are drawn.

2 Preliminaries

2.1 Notations

In the paper we use the following notations:

- (mod L), with L a positive integer, denotes modulo L operation
- $a \mid b$, with a and b positive integers, denotes a divides 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 *a true* CPP if the permutation performed by it cannot be performed by a permutation polynomial of degree smaller than three.

Two CPPs with different coefficients are *different* CPPs 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 [15,16]. Because we are interested in interleaver lengths of the form $8p$ or $24p$, with p a prime number so that $3 \mid (p-1)$, in Table 1 we give the coefficient conditions only for the primes 2, 3, and p, with $3 \mid (p-1)$, when the interleaver length is of the form

$$L = 2^{n_{L,2}} \cdot 3^{n_{L,3}} \cdot p, \text{ with } n_{L,2} > 1, n_{L,3} \in \{0, 1\} \text{ and } p \text{ a prime number so that } 3 \mid (p-1). \tag{2}$$

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)	$3 \mid (p-1)$	$n_{L,p} = 1$	$f_1 \neq 0, f_2 = 0, f_3 = 0 \pmod{p}$

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 Result

In this section we prove that for interleaver lengths of the form

$$L = 8p = 2^3 \cdot p \text{ or } L = 24p = 2^3 \cdot 3 \cdot p, \text{ with } p \text{ a prime number so that } 3 \mid (p-1), \tag{5}$$

a true CPP leads to a minimum distance which is upper bounded by the value of 27 for a classical 1/3 rate turbo code with two RSC component codes having generator matrix $G = [1, 15/13]$ in octal form.

Firstly, we prove two lemmas necessary for the main result.

Lemma 3.1. *Let the interleaver length be of the form* (5)*. Then all true different CPPs have possible values for coefficients f_3 and f_2 equivalent to those from the second and third column, respectively, in Table 2. Coefficient f_1 have 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 $8p$ or $24p$. Conditions for coefficient f_1 from the fourth column are necessary, but not sufficient.

L	f_3	f_2	f_1
$8p$	$2p$	0 or $2p$	1 (mod 4) or 3 (mod 4)
$24p$	$2p$	0 or $6p$	1 (mod 4) or 3 (mod 4), 0 (mod 3) or 2 (mod 3)

Proof. For the interleaver length of the form $L = 8p$, a true CPP is equivalent to a CPP for which $f_2 < L/2 = 4p$ and $f_3 < L/2 = 4p$. For the interleaver length of the form $L = 24p$, a true CPP is equivalent to a CPP for which $f_2 < L/2 = 12p$ and $f_3 < L/6 = 4p$. Taking into account the coefficient conditions for a CPP given in Table 1, the result for coefficients f_2 and f_3 from Table 2 follows.

We note that when $L = 8p$ or $L = 24p$, from condition 1) in Table 1 f_1 results odd. Thus, we can have only $f_1 = 1 \pmod{4}$ or $f_1 = 3 \pmod{4}$. When $L = 24p$, from condition 2) in Table 1 it results that $f_1 + f_3 \neq 0 \pmod{3}$. But $f_3 = 2p = 2 \pmod{3}$. Thus, we can only have $f_1 = 0 \pmod{3}$ or $f_1 = 2 \pmod{3}$. □ □

Lemma 3.2. *Let the interleaver length be of the form* (5)*. Then, a true CPP $\pi(x) = f_1 x + f_2 x^2 + f_3 x^3 \pmod{L}$ has an inverse true CPP $\rho(x) = \rho_1 x + \rho_2 x^2 + \rho_3 x^3 \pmod{L}$, with $\rho_3 = f_3$, $\rho_2 = f_2$, and ρ_1 being the unique modulo L solution of the congruences from Table 3, according to the coefficients f_2 and f_1.*

Table 3: Congruences for determining coefficient ρ_1 of the inverse CPP $\rho(x)$ depending on the coefficients f_2 and f_1. When the congruence has more solutions, the valid solution for ρ_1 fulfills the condition in the parenthesis in the third column.

L	f_2	Condition(s) for f_1	Congruence for determining ρ_1 (valid solution)
$8p$	0	-	$f_1\rho_1 = 1 \pmod{8p}$
	$2p$	$f_1 = 1 \pmod 4$	
	$2p$	$f_1 = 3 \pmod 4$	$f_1\rho_1 = 4p + 1 \pmod{8p}$
$24p$	0	$f_1 = 2 \pmod 3$	$f_1\rho_1 = 1 \pmod{24p}$
	$6p$	$f_1 = 2 \pmod 3$ and $f_1 = 1 \pmod 4$	
	0	$f_1 = 0 \pmod 3$	$f_1\rho_1 = 8p + 1 \pmod{24p}$ ($\rho_1 = 0 \pmod 3$)
	$6p$	$f_1 = 0 \pmod 3$ and $f_1 = 1 \pmod 4$	
	$6p$	$f_1 = 2 \pmod 3$ and $f_1 = 3 \pmod 4$	$f_1\rho_1 = 12p + 1 \pmod{24p}$
	$6p$	$f_1 = 0 \pmod 3$ and $f_1 = 3 \pmod 4$	$f_1\rho_1 = 20p + 1 \pmod{24p}$ ($\rho_1 = 0 \pmod 3$)

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

$$\pi(\rho(x)) = x \pmod L, \forall x \in \{0, 1, \ldots, L-1\}. \tag{6}$$

Taking into account Lemma 3.1, after some algebraic manipulations, equation (6) is equivalent to

$$(f_1\rho_1 - 1)\cdot x + (f_1\rho_2 + f_2\rho_1^2)\cdot x^2 + (f_1\rho_3 + f_3\rho_1^3)\cdot x^3 + 3f_3\rho_1^2\rho_2\cdot x^4 + 3f_3\rho_1^2\rho_3\cdot x^5 + \\ + f_3\rho_3^3\cdot x^9 = 0 \pmod L, \forall x \in \{0, 1, \ldots, L-1\}. \tag{7}$$

Because $\pi(x)$ and $\rho(x)$ are true CPPs, from Lemma 3.1 it results that $\rho_3 = f_3 = 2p$. Because p is odd, we can have $p = 1 \pmod 4$ or $p = 3 \pmod 4$. Then $2p = 2 \pmod 4$. Thus (7) is equivalent to

$$(f_1\rho_1 - 1)\cdot x + (f_1\rho_2 + f_2\rho_1^2)\cdot x^2 + 2p\cdot(f_1 + \rho_1^3)\cdot x^3 + 6p\cdot\rho_1^2\rho_2\cdot x^4 + 12p^2\cdot\rho_1^2\cdot x^5 + \\ + 16p^4\cdot x^9 = 0 \pmod L, \forall x \in \{0, 1, \ldots, L-1\}. \tag{8}$$

Because $(2p) \mid L$, $(2p) \mid f_2$, and $(2p) \mid \rho_2$, from (8) we have

$$(f_1\rho_1 - 1)\cdot x = 0 \pmod{2p}, \forall x \in \{0, 1, \ldots, 2p-1\}. \tag{9}$$

Equation (9) is equivalent to

$$f_1\rho_1 = 1 \pmod{2p} \Leftrightarrow f_1\rho_1 = 2p\cdot k + 1 \pmod L, \text{ with } k \in \{0,1,2,3\} \text{ when } L = 8p, \\ \text{and } k \in \{0, 1, 2, \ldots, 11\} \text{ when } L = 24p. \tag{10}$$

According to Theorem 57 from [17], we note that congruence $f_1\rho_1 = 2p\cdot k+1 \pmod L$ has only one solution modulo L when $L = 8p$ or when $L = 24p$ and $f_1 = 2 \pmod 3$, because $\gcd(f_1, L) = 1$. When $L = 24p$, $f_1 = 0 \pmod 3$, and $k \in \{1, 4, 7, 10\}$, congruence $f_1\rho_1 = 2p\cdot k + 1 \pmod L$ has three solutions modulo L because $\gcd(f_1, L) = 3$ and $3 \mid (2p\cdot k+1)$, but we will show that only the solution which fulfills condition $\rho_1 = 0 \pmod 3$ is valid and it is unique.

In the following we will see which values of k in (10) are valid in different cases. We have three cases.

Case 1: $\rho_2 = f_2 = 0$

In this case $L = 8p$ or $L = 24p$.

Case 1.1: $L = 8p$

For $L = 8p$, $f_2 = \rho_2 = 0$, $f_3 = \rho_3 = 2p$, and $f_1\rho_1 = 2p \cdot k + 1$, (8) is equivalent to

$$2p \cdot \left(kx + (f_1 + \rho_1^3) \cdot x^3 + 2p \cdot \rho_1^2 \cdot x^5\right) = 0 \pmod{8p}, \forall x \in \{0, 1, \ldots, 8p-1\}. \tag{11}$$

Taking into account that $2p = 2 \pmod 4$, (11) is true only if

$$kx + (f_1 + \rho_1^3) \cdot x^3 + 2\rho_1^2 \cdot x^5 = 0 \pmod 4, \forall x \in \{0, 1, 2, 3\}. \tag{12}$$

Because f_1 and ρ_1 can take only values 1 and 3 modulo 4, we can have four possible cases.

For $f_1 = \rho_1 = 1 \pmod 4$, (12) is equivalent to $kx = 0$ (mod 4, and thus $k = 0 \pmod 4$), i.e. $k = 0$. From (10) it means that $f_1\rho_1 = 1 \pmod{8p}$. We note that, because $f_1 = \rho_1 = 1 \pmod 4$ it results that $f_1\rho_1 = 1 \pmod 4$, and thus the solution of $f_1\rho_1 = 1 \pmod{8p}$ is valid.

Similarly, for $f_1 = \rho_1 = 3 \pmod 4$, (12) is equivalent to $k = 0$, or to $f_1\rho_1 = 1 \pmod{8p}$. The solution is valid because from $f_1 = \rho_1 = 3 \pmod 4$ it results that $f_1\rho_1 = 1 \pmod 4$.

For $f_1 = 1 \pmod 4$ and $\rho_1 = 3 \pmod 4$ or for $f_1 = 3 \pmod 4$ and $\rho_1 = 1 \pmod 4$, (12) is equivalent to $kx + 2x^5 = 0 \pmod 4$, and thus $k = 2$, or $f_1\rho_1 = 4p + 1 \pmod{8p}$. But in these cases $f_1\rho_1 = 3 \pmod 4$ and so, the solution of $f_1\rho_1 = 4p + 1 \pmod{8p}$ is not valid.

Concluding, the valid solution in this case is that of congruence $f_1\rho_1 = 1 \pmod{8p}$.

Case 1.2: $L = 24p$

For $L = 24p$, $f_2 = \rho_2 = 0$, $f_3 = \rho_3 = 2p$, and $f_1\rho_1 = 2p \cdot k + 1$, (8) is equivalent to

$$2p \cdot \left(kx + (f_1 + \rho_1^3) \cdot x^3 + 6p \cdot \rho_1^2 \cdot x^5 + 8p^3 \cdot x^9\right) = 0 \pmod{24p}, \forall x \in \{0, 1, \ldots, 24p-1\}. \tag{13}$$

(13) is equivalent to

$$kx + (f_1 + \rho_1^3) \cdot x^3 + 6p \cdot \rho_1^2 \cdot x^5 + 8p^3 \cdot x^9 = 0 \pmod{12}, \forall x \in \{0, 1, \ldots, 11\}. \tag{14}$$

(14) is true if and only if

$$\begin{gathered} kx + (f_1 + \rho_1^3) \cdot x^3 + 6p \cdot \rho_1^2 \cdot x^5 + 8p^3 \cdot x^9 = 0 \pmod 3 \Leftrightarrow \\ kx + (f_1 + \rho_1^3) \cdot x^3 + 2 \cdot x^9 = 0 \pmod 3, \forall x \in \{0, 1, 2\}, \end{gathered} \tag{15}$$

and

$$\begin{gathered} kx + (f_1 + \rho_1^3) \cdot x^3 + 6p \cdot \rho_1^2 \cdot x^5 + 8p^3 \cdot x^9 = 0 \pmod 4 \Leftrightarrow \\ kx + (f_1 + \rho_1^3) \cdot x^3 + 2\rho_1^2 \cdot x^5 = 0 \pmod 4, \forall x \in \{0, 1, 2, 3\}. \end{gathered} \tag{16}$$

For $f_1 = \rho_1 = 0 \pmod 3$, (15) is equivalent to $kx + 2x^9 = 0 \pmod 3$, and thus $k = 1 \pmod 3$, or $k \in \{1, 4, 7, 10\}$. We note that for $k = 1 \pmod 3$, $f_1\rho_1 = 2p \cdot k + 1 = 0 \pmod 3$, and the solution is valid.

For $f_1 = \rho_1 = 2 \pmod 3$, (15) is equivalent to $kx + x^3 + 2x^9 = 0 \pmod 3$, and thus $k = 0 \pmod 3$, or $k \in \{0, 3, 6, 9\}$. For $k = 0 \pmod 3$, $f_1\rho_1 = 2p \cdot k + 1 = 1 \pmod 3$, and thus, the solution is valid.

For $f_1 = 0 \pmod 3$ and $\rho_1 = 2 \pmod 3$, and for $f_1 = 2 \pmod 3$ and $\rho_1 = 0 \pmod 3$, (15) is equivalent to $kx + 2x^3 + 2x^9 = 0 \pmod 3$, and thus $k = 2 \pmod 3$. But for $k = 2 \pmod 3$, $f_1\rho_1 = 2p \cdot k + 1 = 2 \pmod 3$, and thus, this solution is not valid.

Now we are interested in the valid solutions of k so that (16) is fulfilled.

For $f_1 = \rho_1 = 1 \pmod 4$, (16) is equivalent to $kx + 2x^3 + 2x^5 = 0 \pmod 4$, and thus $k = 0 \pmod 4$, or $k \in \{0, 4, 8\}$. For $k = 0 \pmod 4$, $f_1\rho_1 = 2p \cdot k + 1 = 1 \pmod 4$, and the solution is valid.

For $f_1 = \rho_1 = 3 \pmod 4$, (16) is also equivalent to $kx+2x^3+2x^5 = 0 \pmod 4$, and thus $k = 0 \pmod 4$, or $k \in \{0, 4, 8\}$. The solution is valid because for $f_1 = \rho_1 = 3 \pmod 4$, $f_1\rho_1 = 1 \pmod 4$.

For $f_1 = 1 \pmod 4$ and $\rho_1 = 3 \pmod 4$, or for $f_1 = 3 \pmod 4$ and $\rho_1 = 1 \pmod 4$, (16) is equivalent to $kx + 2x^5 = 0 \pmod 4$, and thus $k = 2 \pmod 4$. But for $k = 2 \pmod 4$, $f_1\rho_1 = 2p \cdot k + 1 = 1 \pmod 4$, and thus, this solution is not valid.

Taking into account that both (15) and (16) must be fulfilled, combining the above solutions, we have $k = 0$ or $f_1\rho_1 = 1 \pmod{24p}$ when $f_1 = 2 \pmod 3$ and $f_1 = 1 \text{ or } 3 \pmod 4$, and $k = 4$ or $f_1\rho_1 = 8p + 1 \pmod{24p}$, with $\rho_1 = 0 \pmod 3$, when $f_1 = 0 \pmod 3$ and $f_1 = 1 \text{ or } 3 \pmod 4$.

Case 2: $\rho_2 = f_2 = 2p$

In this case $L = 8p$ and for $\rho_3 = f_3 = 2p$ and $f_1\rho_1 = 2p \cdot k + 1 \pmod{8p}$, (8) is equivalent to

$$2p \cdot \left(kx + (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 + 6p \cdot \rho_1^2 \cdot x^4 + 2p \cdot \rho_1^2 \cdot x^5\right) = 0 \pmod{8p}, \quad \forall x \in \{0, 1, \ldots, 8p - 1\}. \tag{17}$$

(17) holds if and only if

$$kx + (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 + 2 \cdot \rho_1^2 \cdot x^4 + 2 \cdot \rho_1^2 \cdot x^5 = 0 \pmod 4, \quad \forall x \in \{0, 1, 2, 3\}. \tag{18}$$

But $2 \cdot \rho_1^2 \cdot x^4 + 2 \cdot \rho_1^2 \cdot x^5 = 2 \cdot \rho_1^2 \cdot x^4 \cdot (x + 1) = 0 \pmod 4$, and thus, (18) is equivalent to

$$kx + (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 = 0 \pmod 4, \forall x \in \{0, 1, 2, 3\}. \tag{19}$$

For $f_1 = \rho_1 = 1 \pmod 4$, (19) is equivalent to $kx + 2x^2 + 2x^3 = 0 \pmod 4$, and thus $k = 0$, or $f_1\rho_1 = 1 \pmod{8p}$, which is a valid solution.

For $f_1 = \rho_1 = 3 \pmod 4$, (19) is equivalent to $kx + 2x^3 = 0 \pmod 4$, and thus $k = 2$, or $f_1\rho_1 = 4p + 1 \pmod{8p}$, which is a valid solution.

For $f_1 = 1 \pmod 4$ and $\rho_1 = 3 \pmod 4$, (19) is equivalent to $kx + 2x^2 = 0 \pmod 4$, and thus $k = 2$, which is not a valid solution.

For $f_1 = 3 \pmod 4$ and $\rho_1 = 1 \pmod 4$, (19) is equivalent to $kx = 0 \pmod 4$, and thus $k = 0$, which also is not a valid solution.

Thus the valid solutions in this case are those of congruence $f_1\rho_1 = 1 \pmod{8p}$ when $f_1 = 1 \pmod 4$ and of congruence $f_1\rho_1 = 4p + 1 \pmod{8p}$ when $f_1 = 3 \pmod 4$.

Case 3: $\rho_2 = f_2 = 6p$

In this case $L = 24p$ and for $\rho_3 = f_3 = 2p$ and $f_1\rho_1 = 2p \cdot k + 1 \pmod{24p}$, (8) is equivalent to

$$2p \cdot \left(kx + 3 \cdot (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 + 18p \cdot \rho_1^2 \cdot x^4 + 6p \cdot \rho_1^2 \cdot x^5 + 8p^3 \cdot x^9\right) = = 0 \pmod{24p}, \forall x \in \{0, 1, \ldots, 24p - 1\}. \tag{20}$$

(20) holds if and only if

$$kx + 3 \cdot (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 + 6p \cdot \rho_1^2 \cdot x^4 + 6p \cdot \rho_1^2 \cdot x^5 + 8p^3 \cdot x^9 = \\ = 0 \pmod{12}, \forall x \in \{0, 1, \ldots, 11\}. \quad (21)$$

Quantity $6p \cdot \rho_1^2 \cdot x^4 + 6p \cdot \rho_1^2 \cdot x^5 = 6p \cdot \rho_1^2 \cdot x^4 \cdot (x+1)$, and thus it is equal to 0 modulo 12. Then (21) is equivalent to

$$kx + 3 \cdot (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 + 8p^3 \cdot x^9 = 0 \pmod{12}, \forall x \in \{0, 1, \ldots, 11\}. \quad (22)$$

(22) holds if and only if

$$kx + (f_1 + \rho_1^3) \cdot x^3 + 2 \cdot x^9 = 0 \pmod 3, \forall x \in \{0, 1, 2\}. \quad (23)$$

and

$$kx + 3 \cdot (f_1 + \rho_1^2) \cdot x^2 + (f_1 + \rho_1^3) \cdot x^3 = 0 \pmod 4, \forall x \in \{0, 1, 2, 3\}. \quad (24)$$

For $f_1 = \rho_1 = 0 \pmod 3$, (23) is equivalent to $kx + 2 \cdot x^9 = 0 \pmod 3$, and thus $k = 1 \pmod 3$, or $k \in \{1, 4, 7, 10\}$. Following a similar analysis as that in case 1.2, the solution results valid.

For $f_1 = \rho_1 = 2 \pmod 3$, (23) is equivalent to $kx + x^3 + 2 \cdot x^9 = 0 \pmod 3$, and thus $k = 0 \pmod 3$, or $k \in \{0, 3, 6, 9\}$, which is a valid solution.

For $f_1 = 0 \pmod 3$ and $\rho_1 = 2 \pmod 3$, and for $f_1 = 2 \pmod 3$ and $\rho_1 = 0 \pmod 3$, (23) is equivalent to $kx + 2x^3 + 2x^9 = 0 \pmod 3$, and thus $k = 2 \pmod 3$, which is not a valid solution.

For $f_1 = \rho_1 = 1 \pmod 4$, (24) is equivalent to $kx + 2x^2 + 2x^3 = 0 \pmod 4$, and thus $k = 0 \pmod 4$, or $k \in \{0, 4, 8\}$, which is a valid solution.

For $f_1 = \rho_1 = 3 \pmod 4$, (24) is equivalent to $kx + 2x^3 = 0 \pmod 4$, and thus $k = 2 \pmod 4$, or $k \in \{2, 6, 10\}$, which is a valid solution.

For $f_1 = 1 \pmod 4$ and $\rho_1 = 3 \pmod 4$, (24) is equivalent to $kx + 2x^2 = 0 \pmod 4$, and thus $k = 2 \pmod 4$, which is not a valid solution.

For $f_1 = 3 \pmod 4$ and $\rho_1 = 1 \pmod 4$, (24) is equivalent to $kx = 0 \pmod 4$, and thus $k = 0 \pmod 4$, which is not a valid solution.

Combining the above solutions, we have

1) $k = 4$ or $f_1\rho_1 = 8p + 1 \pmod{24p}$, with $\rho_1 = 0 \pmod 3$, when $f_1 = 0 \pmod 3$ and $f_1 = 1 \pmod 4$,

2) $k = 10$ or $f_1\rho_1 = 20p + 1 \pmod{24p}$, with $\rho_1 = 0 \pmod 3$, when $f_1 = 0 \pmod 3$ and $f_1 = 3 \pmod 4$,

3) $k = 0$ or $f_1\rho_1 = 1 \pmod{24p}$, when $f_1 = 2 \pmod 3$ and $f_1 = 1 \pmod 4$, and

4) $k = 6$ or $f_1\rho_1 = 12p + 1 \pmod{24p}$, when $f_1 = 2 \pmod 3$ and $f_1 = 3 \pmod 4$.

Thus, the lemma is proved. □ □

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. We also note that, because the inverse CPP is a true CPP, then we don't need to consider cases when $f_2 = 0$ and $\rho_2 = 2p$, or $f_2 = 2p$ and $\rho_2 = 0$, for $L = 8p$, and cases when $f_2 = 0$ and $\rho_2 = 6p$, or $f_2 = 6p$ and $\rho_2 = 0$, for $L = 24p$. If $\rho_2 \neq f_2 \pmod{L/2}$ then the resulted CPP $\rho(x)$ is a true CPP different from the one corresponding to the inverse permutation.

Now we give the theorem containing the main result in this paper.

Theorem 3.3. *Let the interleaver length be of the form* (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) is upper bounded by the value of 27.*

Proof. We consider the interleaver pattern of size nine from Fig. 1. We note that this interleaver pattern is similar to that in Fig. 2 from [5], but for true CPP-based interleavers it leads to other minimum distance of the turbo code.

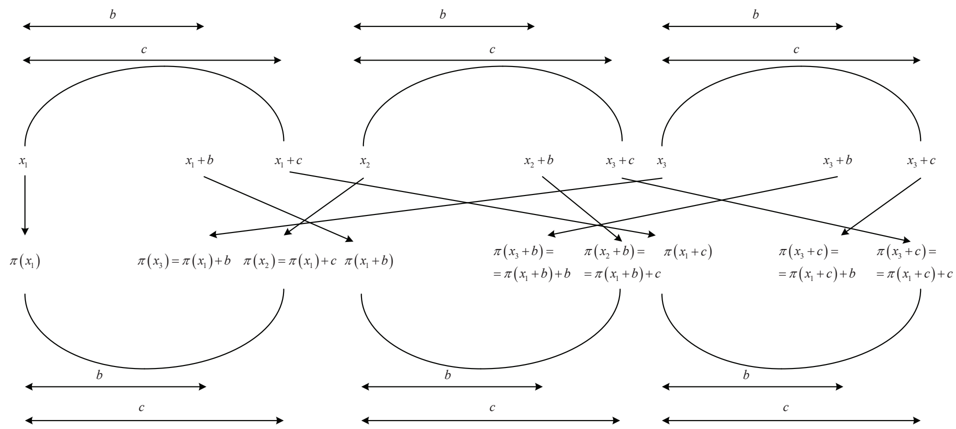

Figure 1: Critical interleaver pattern of size nine for CPP-based interleavers

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

$$\begin{cases} x_1 \to \pi(x_1) \\ x_1 + b \to \pi(x_1 + b) \\ x_1 + c \to \pi(x_1 + c) \\ x_2 \to \pi(x_2) = \pi(x_1) + c \\ x_2 + b \to \pi(x_2 + b) = \pi(x_1 + b) + c \\ x_2 + c \to \pi(x_2 + c) = \pi(x_1 + c) + c \\ x_3 \to \pi(x_3) = \pi(x_1) + b \\ x_3 + b \to \pi(x_3 + b) = \pi(x_1 + b) + b \\ x_3 + c \to \pi(x_3 + c) = \pi(x_1 + c) + b \end{cases} \tag{25}$$

Writing $x = \rho(\pi(x))$, for $x = x_1$, $x = x_2$, and $x = x_3$, the equations corresponding to points $x_2 + b$, $x_2 + c$, $x_3 + b$, and $x_3 + c$ from (25) are written as

$$\begin{cases} \pi(\rho(\pi(x_2)) + b) = \pi(\rho(\pi(x_1)) + b) + c \pmod{L} \\ \pi(\rho(\pi(x_2)) + c) = \pi(\rho(\pi(x_1)) + c) + c \pmod{L} \\ \pi(\rho(\pi(x_3)) + b) = \pi(\rho(\pi(x_1)) + b) + b \pmod{L} \\ \pi(\rho(\pi(x_3)) + c) = \pi(\rho(\pi(x_1)) + c) + b \pmod{L} \end{cases} \tag{26}$$

Using the equations corresponding to points x_2 and x_3 from (25) in (26), and then replacing $\pi(x_1)$ by x, we have

$$\begin{cases} \pi(\rho(x + c) + b) = \pi(\rho(x) + b) + c \pmod{L} \\ \pi(\rho(x + c) + c) = \pi(\rho(x) + c) + c \pmod{L} \\ \pi(\rho(x + b) + b) = \pi(\rho(x) + b) + b \pmod{L} \\ \pi(\rho(x + b) + c) = \pi(\rho(x) + c) + b \pmod{L} \end{cases} \tag{27}$$

Unlike [5] we consider both $x = 0$ and $x = 1$ in (27). For $x = 0$ in (27) we have

$$\begin{cases} \pi(\rho(c) + b) = \pi(b) + c \pmod{L} \\ \pi(\rho(c) + c) = \pi(c) + c \pmod{L} \\ \pi(\rho(b) + b) = \pi(b) + b \pmod{L} \\ \pi(\rho(b) + c) = \pi(c) + b \pmod{L} \end{cases} \tag{28}$$

and for $x = 1$ in (27) we have

$$\begin{cases} \pi(\rho(1 + c) + b) = \pi(\rho(1) + b) + c \pmod{L} \\ \pi(\rho(1 + c) + c) = \pi(\rho(1) + c) + c \pmod{L} \\ \pi(\rho(1 + b) + b) = \pi(\rho(1) + b) + b \pmod{L} \\ \pi(\rho(1 + b) + c) = \pi(\rho(1) + c) + b \pmod{L} \end{cases} \tag{29}$$

Equations in (28) are equivalent to

$$\begin{cases} b \cdot \rho(b) \cdot \big(2 \cdot f_2 + 3 \cdot f_3 \cdot (b + \rho(b))\big) = 0 \pmod{L} \\ c \cdot \rho(c) \cdot \big(2 \cdot f_2 + 3 \cdot f_3 \cdot (c + \rho(c))\big) = 0 \pmod{L} \\ b \cdot \rho(c) \cdot \big(2 \cdot f_2 + 3 \cdot f_3 \cdot (b + \rho(c))\big) = 0 \pmod{L} \\ c \cdot \rho(b) \cdot \big(2 \cdot f_2 + 3 \cdot f_3 \cdot (c + \rho(b))\big) = 0 \pmod{L} \end{cases} \tag{30}$$

and equations in (29) are equivalent to

$$\begin{cases} 2 \cdot b \cdot f_2 \cdot (\rho(b + 1) - b \cdot \rho(1)) + \\ +3 \cdot b \cdot f_3 \cdot (b \cdot \rho(b + 1) + \rho^2(b + 1) - b \cdot \rho(1) - \rho^2(1)) = 0 \pmod{L} \\ 2 \cdot c \cdot f_2 \cdot (\rho(c + 1) - b \cdot \rho(1)) + \\ +3 \cdot c \cdot f_3 \cdot (c \cdot \rho(c + 1) + \rho^2(c + 1) - c \cdot \rho(1) - \rho^2(1)) = 0 \pmod{L} \\ 2 \cdot b \cdot f_2 \cdot (\rho(c + 1) - b \cdot \rho(1)) + \\ +3 \cdot b \cdot f_3 \cdot (b \cdot \rho(c + 1) + \rho^2(c + 1) - b \cdot \rho(1) - \rho^2(1)) = 0 \pmod{L} \\ 2 \cdot c \cdot f_2 \cdot (\rho(b + 1) - c \cdot \rho(1)) + \\ +3 \cdot c \cdot f_3 \cdot (c \cdot \rho(b + 1) + \rho^2(b + 1) - c \cdot \rho(1) - \rho^2(1)) = 0 \pmod{L} \end{cases} \tag{31}$$

Because for the considered lengths, as in (5), coefficients f_2 and f_3 are multiples of $2p$, coefficient f_2 is multiple of 3 for $n_{L,3} = 1$, then the congruences from (30) and (31) are fulfilled if the left hand terms are divisible by 8.

In (30) and (31) we consider $b = 1$ and $c = 5$, for which the interleaver pattern from Fig. 1 leads to minimum distance of $9 + 6 \cdot 3 = 27$, because each of the six 3-weight input error patterns leads to a parity sequence of weight 3.

As in the proof of Lemma 3.2 we have three cases. In each of these cases $f_3 = \rho_3 = 2p = 2 \pmod{4}$ and $f_1 = \rho_1 = 1 \pmod{4}$ or $f_1 = \rho_1 = 3 \pmod{4}$. We will prove that congruences from (30) and (31) are fulfilled for $f_1 = \rho_1 = 1 \pmod{4}$ or for $f_1 = \rho_1 = 3 \pmod{4}$. Thus the interleaver pattern from Fig. 1 appears for $x = 0$ or for $x = 1$, and thus, the upper bound of the minimum distance is 27.

Case 1: $f_2 = \rho_2 = 0$

This case has two subcases.

Case 1.1: $L = 8p$

In this case, for $b = 1$ and $c = 5$, the left hand terms from the four congruences from (30), divided by $2p$, are equivalent modulo 4 to

$$\begin{aligned} \rho(1) \cdot 3 \cdot (1 + \rho(1)) \pmod{4} = 3 \cdot \rho(1) \cdot (1 + \rho_1 + \rho_2 + \rho_3) \pmod{4} = \\ = 3 \cdot \rho(1) \cdot (3 + \rho_1) \pmod{4} = 0, \text{ for } \rho_1 = f_1 = 1 \pmod{4}. \end{aligned} \tag{32}$$

For $b = 1$ and $c = 5$, the left hand terms from the four congruences in (31), divided by $2p$, are equivalent modulo 4 to

$$\begin{gathered} 3 \cdot (\rho(2) - \rho(1)) \cdot (1 + \rho(1) + \rho(2)) \pmod 4 = \\ = 3 \cdot (\rho(2) - \rho(1)) \cdot (1 + 3\rho_1 + \rho_2 + \rho_3) \pmod 4 = \\ = 3 \cdot (\rho(2) - \rho(1)) \cdot (3 + 3\rho_1) \pmod 4 = 0, \text{ for } \rho_1 = f_1 = 3 \pmod 4. \end{gathered} \tag{33}$$

Case 1.2: $L = 24p$

In this case, for $b = 1$ and $c = 5$, the left hand terms from the four congruences in (30), divided by $6p$, are equivalent modulo 4 to

$$\rho(1) \cdot (1 + \rho(1)) \pmod 4 = \rho(1) \cdot (3 + \rho_1) \pmod 4 = 0, \text{ for } \rho_1 = f_1 = 1 \pmod 4. \tag{34}$$

For $b = 1$ and $c = 5$, the left hand terms from the four congruences in (31), divided by $6p$, are equivalent modulo 4 to

$$\begin{gathered} (\rho(2) - \rho(1)) \cdot (1 + \rho(1) + \rho(2)) \pmod 4 = \\ = (\rho(2) - \rho(1)) \cdot (3 + 3\rho_1) \pmod 4 = 0, \text{ for } \rho_1 = f_1 = 3 \pmod 4. \end{gathered} \tag{35}$$

Case 2: $f_2 = \rho_2 = 2p$ $(L = 8p)$

For $b = 1$ and $c = 5$, the left hand terms from the four congruences in (30), divided by $2p$, are equivalent modulo 4 to

$$\begin{gathered} \rho(1) \cdot (2 + 3 \cdot (1 + \rho(1))) \pmod 4 = \rho(1) \cdot (1 + 3\rho_1 + 3\rho_2 + 3\rho_3) \pmod 4 = \\ = \rho(1) \cdot (1 + 3\rho_1 + 2 + 2) \pmod 4 = \rho(1) \cdot (1 + 3\rho_1) \pmod 4 = 0, \\ \text{for } \rho_1 = f_1 = 1 \pmod 4. \end{gathered} \tag{36}$$

For $b = 1$ and $c = 5$, the left hand terms from the four congruences in (31), divided by $2p$, are equivalent modulo 4 to

$$\begin{gathered} (\rho(2) - \rho(1)) \cdot (2 + 3 \cdot (1 + \rho(1) + \rho(2))) \pmod 4 = \\ = (\rho(2) - \rho(1)) \cdot (1 + 9\rho_1 + 3\rho_2 + 3\rho_3) \pmod 4 = \\ = (\rho(2) - \rho(1)) \cdot (1 + \rho_1) \pmod 4 = 0, \text{ for } \rho_1 = f_1 = 3 \pmod 4. \end{gathered} \tag{37}$$

Case 3: $f_2 = \rho_2 = 6p$ $(L = 24p)$

For $b = 1$ and $c = 5$, the left hand terms from the four congruences in (30), divided by $6p$, are equivalent modulo 4 to

$$\rho(1) \cdot (2 + 1 + \rho(1)) \pmod 4 = \rho(1) \cdot (3 + \rho_1) \pmod 4 = 0, \text{ for } \rho_1 = f_1 = 1 \pmod 4. \tag{38}$$

For $b = 1$ and $c = 5$, the left hand terms from the four congruences in (31), divided by $6p$, are equivalent modulo 4 to

$$\begin{gathered} (\rho(2) - \rho(1)) \cdot (2 + 1 + \rho(1) + \rho(2)) \pmod 4 = \\ = (\rho(2) - \rho(1)) \cdot (3 + 3\rho_1) \pmod 4 = 0, \text{ for } \rho_1 = f_1 = 3 \pmod 4. \end{gathered} \tag{39}$$

Thus, the theorem is proved. □ □

4 Remarks and Examples

In this section we make some remarks about our main result in this paper. According to Table II from [5], for the interleaver lengths considered in (5), the minimum distance of the turbo codes with QPP interleavers is upper bounded by the value of 36. This upper bound, as that obtained in this paper, is achievable for sufficiently large interleaver lengths and for dual trellis termination [18]. In Table 4 we give QPPs and CPPs for four interleaver lengths with optimal minimum distance (denoted d_{min}), i.e. 36 for QPPs and 27 for CPPs. The codeword multiplicities are also given in Table 4. In the second column the value of p in (5) is given. To emphasize the difference in error correction capabilities, frame error rates (FER) at high signal-to-noise ratio (SNR) are also provided in Table 4. An additive white Gaussian noise (AWGN) channel and a Max-Log-MAP algorithm, with a scaling coefficient of 0.7 for the extrinsec information, are considered in simulations. Other CPPs with optimal minimum distance equal to 27 are those given in [10] for the interleaver lengths 248, 296, 344, 456, and 488.

Table 4: Simulation results for d_{min}-optimal QPPs and CPPs of interleaver lengths 312, 1608, 4184, and 10104

L	p	SNR [dB]	d_{min}-optimal QPP	$N_{d_{min}}$ for QPP	FER for QPP	d_{min}-optimal CPP	$N_{d_{min}}$ for CPP	FER for CPP
312	13	2.75	$115x + 78x^2$	558	$1.64 \cdot 10^{-7}$	$11x + 0x^2 + 26x^3$	142	$1.84 \cdot 10^{-6}$
1608	67	2.0	$701x + 402x^2$	3142	$1.70 \cdot 10^{-5}$	$3x + 0x^2 + 134x^3$	790	$1.57 \cdot 10^{-4}$
4184	523	2.5	$13x + 1046x^2$	18660	$3.70 \cdot 10^{-6}$	$3x + 0x^2 + 1046x^3$	2078	$4.48 \cdot 10^{-4}$
10104	421	2.3	$23x + 2526x^2$	104811	$2.17 \cdot 10^{-5}$	$3x + 0x^2 + 842x^3$	5038	$2.85 \cdot 10^{-4}$

Table 5: Simulation results for better 5-PPs compared to d_{min}-optimal QPPs of interleaver lengths 312 and 1608

L	SNR [dB]	5-PP	d_{min}	$N_{d_{min}}$	FER
312	2.75	$183x + 0x^2 + 49x^3 + 0x^4 + 7x^5$	30	20	$7.93 \cdot 10^{-8}$
1608	2.0	$199x + 767x^2 + 153x^3 + x^4 + x^5$	35	46	$3.16 \cdot 10^{-7}$

We note that for the interleaver lengths considered in (5) there are not true fourth degree PPs [19, 20]. For interleaver lengths as in (5) fifth degree PPs [21] exists only if $p \neq 1 \pmod{15}$ [20]. Thus, to find a PP possible better than QPP interleavers for lengths as in (5), we have to consider the degree of PP at least five when $p \neq 1 \pmod{15}$ and at least six when $p = 1 \pmod{15}$. To give a result in this direction, in Table 5 we provide 5-PPs better than QPPs for interleaver lengths 312 and 1608. We note that for interleaver length of 312 the three PPs in Tables 4 and 5 were optimised by the first method given in [8] with the distance spectra for AWGN channel truncated at the first three terms. For interleaver length of 1608 the QPP was optimised selecting firstly QPPs with maximum metric Ω' and then, among these QPPs, those with the best distance spectrum truncated at the first three terms. The CPP and the 5-PP of length of 1608 were selected choosing the PP of highest minimum distance and lowest multiplicity among some PPs.

5 Conclusions

In this paper we have considered the interleaver lengths of the form $8p$ or $24p$, wih p a prime number such that $3 \mid (p-1)$. We have proved that the minimum distance of a classical 1/3 rate turbo code with component codes as those for LTE standard [11] and true CPP interleavers of the considered lengths is upper bounded by the value of 27. This upper bound is significantly weaker than that for QPP interleavers, i.e. 36 as it was shown in [5].

We have obtained the coefficients of the inverse true CPP of a true CPP for the considered interleaver lengths.

Finally, we have given four examples of CPPs and QPPs of small to high interleaver lengths with optimal minimum distance and we have compared their error rate performance at high SNR. We also have made some remarks about PP interleavers of degree higher than three. As a conclusion in this regard, to find a PP possible better than QPP interleavers for the interleaver lengths in the paper, a degree of PP equal to at least five when prime $p \neq 1 \pmod{15}$ and at least six when $p = 1 \pmod{15}$ has to be considered. Better 5-PPs are provided for two of the four considered interleaver lengths.

Acknowledgements

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

References

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

[2] O.Y. Takeshita, "On maximum contention-free interleavers and permutation polynomials over integer rings", *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1249-1253, Mar. 2006.

[3] O.Y. Takeshita, "Permutation polynomial interleavers: An algebraic-geometric perspective", *IEEE Transactions on Information Theory*, vol. 53, no. 6, pp. 2116-2132, Jun. 2007.

[4] D. Tarniceriu, L. Trifina, and V. Munteanu, "About minimum distance for QPP interleavers", *Annals of Telecommunications*, vol. 64, nos. 11-12, pp. 745-751, Dec. 2009.

[5] E. Rosnes, "On the minimum distance of turbo codes with quadratic permutation polynomial interleavers", *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4781-4795, July 2012.

[6] J. Ryu, "Permutation polynomials of higher degrees for turbo code interleavers", *IEICE Transactions on Communications*, vol. E95-B, no. 12, pp. 3760-3762, Dec. 2012.

[7] L. Trifina, and D. Tarniceriu, “Analysis of cubic permutation polynomials for turbo codes”, *Wireless Personal Communications*, vol. 69, no. 1, pp. 1-22, Mar. 2013.

[8] L. Trifina, and D. Tarniceriu, “Improved method for searching interleavers from a certain set using Garello’s method with applications for the LTE standard”, *Annals of Telecommunications*, vol. 69, nos. 5-6, pp. 251-272, Jun. 2014.

[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 *Proceedings of IEEE International Symposium on Signals, Circuits and Systems (ISSCS 2017)*, Iasi, Romania, 6 pages, July 13-14, 2017.

[11] 3GPP TS 36.212 V8.3.0, 3rd Generation Partnership Project, Multiplexing and channel coding (Release 8), 2008. [Online] `http://www.etsi.org`.

[12] S. Crozier, and P. Guinand, “High-Performance Low-Memory Interleaver Banks for Turbo-Codes”, in Proc. *IEEE 54^{th} Vehicular Technology Conference*, VTC 2001 Fall, Atlantic City, NJ, USA, vol. 4, pp. 2394-2398, 7-11 October 2001.

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

[14] R. Garzon-Bohorquez, C. Abdel Nour, and C. Douillard, “Protograph-Based Interleavers for Punctured Turbo Codes”, *IEEE Transactions on Communications*, vol. 66, no. 5, pp. 1833-1844, May 2018.

[15] Y.-L. Chen, J. Ryu, and O.Y. Takeshita, “A simple coefficient test for cubic permutation polynomials over integer rings”, *IEEE Communications Letters*, vol. 10, no. 7, pp. 549-551, Jul. 2006.

[16] H. Zhao, and P. Fan, “A note on “A simple coefficient test for cubic permutation polynomials over integer rings””, *IEEE Communications Letters*, vol. 11, no. 12, p. 991, Dec. 2007.

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

[18] P. Guinand, and J. Lodge, “Trellis termination for turbo encoders”, in Proc. *17^{th} Biennial Symposium on Communications*, Queen’s University, Kingston, Canada, pp. 389-392, 30 May - 1 June, 1994.

[19] L. Trifina, and D. Tarniceriu, “A coefficient test for fourth degree permutation polynomials over integer rings”, *AEU Int. J. Electron. Commun.*, vol. 70, no. 11, pp. 1565-1568, Nov. 2016.

[20] L. Trifina, and D. Tarniceriu, “When is the number of true different permutation polynomials is equal to 0?”, *Mathematics*, vol. 7, no. 11, ID 1018, Nov. 2019.

[21] L. Trifina, and D. Tarniceriu, “A coefficient test for quintic permutation polynomials over integer rings”, *IEEE Access*, vol. 6, pp. 37893-37909, 2018.