On the Equivalence of Cubic Permutation Polynomial and ARP Interleavers for Turbo Codes

Lucian Trifina and Daniela Tarniceriu

***Abstract*— Recently, it was shown that the dithered relative prime interleavers and quadratic permutation polynomial (QPP) interleavers can be expressed in terms of almost regular permutation (ARP) interleavers. In this paper, the conditions for a QPP interleaver to be equivalent to an ARP interleaver are extended for cubic permutation polynomial (CPP) interleavers. It is shown that the CPP interleavers are always equivalent to an ARP interleaver with disorder degree greater than one and smaller than the interleaver length, when the prime factorization of the interleaver length contains at least one prime number to a power higher than one and it fulfills the conditions for which there are true CPPs for the considered length. When the prime factorization of the interleaver length contains only prime numbers to the power of one, with at least two prime numbers p_i, fulfilling the conditions $p_i > 3$ and $3 \nmid (p_i - 1)$, values of disorder degree smaller than the interleaver length are possible under some conditions on the coefficients of the second and third degree terms of the CPP.**

***Index Terms*— Turbo codes, ARP interleaver, CPP interleaver, equivalence.**

I. Introduction

THREE of the most common and performant interleavers for Turbo Codes (TCs) are Dithered Relative Prime (DRP) interleavers [1], Almost Regular Permutation (ARP) interleavers [2] and Permutation Polynomial (PP) interleavers, introduced by Sun *et al.* [3], [4].

Recently, in [5], it was shown that DRP and Quadratic Permutation Polynomial (QPP) interleavers can be expressed in terms of ARP interleavers. As a consequence, this proves that ARP interleavers can achieve at least the same distance spectra, and thus the same asymptotic performances, as DRP and QPP interleavers. These equivalences present the advantage of a unified implementation, when these different interleavers are used for some specific applications.

QPP interleavers have been intensively studied in [3], [4], and [6]–[17] and they are used in the Long Term Evolution (LTE) standard [18]. However, in [19] and [20], it was shown that Cubic Permutation Polynomial (CPP) interleavers of small lengths may lead to performances slightly superior to those of QPP ones. Furthermore, in Section VI, we present some significantly better CPPs compared to QPPs in terms of frame error rate (FER) at high signal-to-noise ratio (SNR), for medium lengths. The better performance of CPPs motivates the analysis of the equivalence between CPP and ARP interleavers.

Necessary and sufficient conditions for generating QPPs and CPPs were given in [4], [21], and [22]. In this paper, we present the conditions to express CPP interleavers as ARP interleavers. We prove that CPP interleavers can always be expressed as ARP interleavers, with a disorder degree greater than one and lower than the interleaver length, when its prime factorization contains at least one prime number to a power higher than one and it fulfills the conditions for which there are true CPPs for the considered length. True CPPs are those that cannot be reduced to QPPs or linear PPs (LPPs). When the prime factorization of the interleaver length contains only prime numbers to the power of one, with at least two prime numbers p_i, so that $p_i > 3$ and $3 \nmid (p_i - 1)$, values of disorder degree lower than the interleaver length are possible under some conditions on the coefficients of the second and third degree terms of the CPP. Some specific examples are shown for different lengths.

In the paper, we will use the following notations: $\mathbb{N}$ is the set of natural numbers, $\mathbb{N}^+$ is the set of natural numbers greater than zero, $\mathbb{N}_o$ is the set of odd natural numbers, $\mathbb{Z}$ is the set of integers, $\mathbb{Z}_K = \{0, 1, \cdots, K-1\}$ is the integer ring, where K is a positive integer, $a \bmod b$ denotes a modulo b, $a \mid b$ denotes a divides b, and $a \nmid b$ denotes a does not divide b, where $a, b \in \mathbb{N}$.

The paper is structured as follows. In Section II the mathematical model for ARP and CPP interleavers is presented. Section III provides the conditions for a CPP interleaver to be expressed as an ARP interleaver. These conditions are formulated in terms of prime number powers from the factorization of the interleaver length and of the coefficients of the second and the third degree terms of the CPP, in Section IV. Section V analyzes the cases for which there are true CPPs and valid values of disorder degree lower than the interleaver length. Finally, Section VI presents some CPPs with significantly better FER performances compared to those of QPPs/LPPs of medium lengths and Section VII makes an analysis of evaluation complexity of CPPs and QPPs/LPPs.

Manuscript received April 7, 2016; revised September 12, 2016; accepted November 8, 2016. Date of publication November 15, 2016; date of current version February 14, 2017. The associate editor coordinating the review of this paper and approving it for publication was L. Dolecek.

The authors are with the Faculty of Electronics, Telecommunications and Information Technology, Department of Telecommunications, Gheorghe Asachi Technical University of Iaşi, 700506 Iaşi, Romania (e-mail: luciant@etti.tuiasi.ro; tarniced@etti.tuiasi.ro).

Digital Object Identifier 10.1109/TCOMM.2016.2628744

TABLE I
NECESSARY AND SUFFICIENT CONDITIONS FOR A CPP COEFFICIENTS

1.a)	$p_1 = 2$	$\alpha_{K,1} = 1$	$(f_1 + f_2 + f_3) = 1 \mod 2$
1.b)		$\alpha_{K,1} > 1$	$f_1 = 1 \mod 2$, $f_2 = 0 \mod 2$, $f_3 = 0 \mod 2$
2.a)	$p_2 = 3$	$\alpha_{K,2} = 1$	$(f_1 + f_3) \neq 0 \mod 3$, $f_2 = 0 \mod 3$
2.b)		$\alpha_{K,2} > 1$	$f_1 \neq 0 \mod 3$, $(f_1 + f_3) \neq 0 \mod 3$, $f_2 = 0 \mod 3$
3)	$3 \mid (p_i - 1)$	$\alpha_{K,i} \geq 1$	$f_1 \neq 0 \mod p_i$, $f_2 = 0 \mod p_i$, $f_3 = 0 \mod p_i$
4.a)	$3 \nmid (p_i - 1)$, $p_i > 3$	$\alpha_{K,i} = 1$	$f_2^2 = 3 \cdot f_1 \cdot f_3 \mod p_i$, if $f_3 \neq 0 \mod p_i$
			$f_1 \neq 0 \mod p_i$ and $f_2 = 0 \mod p_i$, if $f_3 = 0 \mod p_i$
4.b)		$\alpha_{K,i} > 1$	$f_1 \neq 0 \mod p_i$, $f_2 = 0 \mod p_i$, $f_3 = 0 \mod p_i$

II. MATHEMATICAL MODEL FOR ARP AND CPP INTERLEAVERS

A. ARP Interleavers

The ARP interleaver was proposed by Berrou *et al.* [2]. It is based on a regular permutation of period P and a vector of shifts S. Its interleaving function is defined as:

$$\Pi_{ARP}(x) = \left(P \cdot x + S_{(x \bmod Q)}\right) \bmod K, \tag{1}$$

where $x = 0, \cdots, K-1$ denotes the address of the data symbol after interleaving and $\Pi_{ARP}(x)$ represents its corresponding address before interleaving. P is a positive integer relatively prime to the interleaver size K. The disorder cycle or disorder degree in the permutation is denoted by Q and it corresponds to the number of shifts in S. K must be a multiple of Q.

B. CPP Interleavers

PP interleavers were proposed by Sun *et al.* [3], [4]. They are based on permutation polynomials over the integer ring $\mathbb{Z}_K$, where K is the interleaver length. For a CPP, the permutation function is defined as

$$\Pi_{CPP}(x) = \left(f_1 \cdot x + f_2 \cdot x^2 + f_3 \cdot x^3\right) \bmod K, \tag{2}$$

where $x = 0, \cdots, K-1$ denotes the address of the data symbol after interleaving and $\Pi_{CPP}(x)$ represents its corresponding address before interleaving. Necessary and sufficient conditions for generating CPPs are given in [21] and [22]. These conditions depend on the prime factorization of the interleaver length K. We consider the factorization of K as follows:

$$K = 2^{\alpha_{K,1}} \cdot 3^{\alpha_{K,2}} \cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{K,i}}, \tag{3}$$

where $\omega(K)$ is a positive integer greater than or equal to 2. If $\omega(K) = 2$, the product $\prod_{i=3}^{\omega(K)} p_i^{\alpha_{K,i}}$ in (3) is considered to be equal to 1. In (3) we could have $\alpha_{K,1} = 0$ and/or $\alpha_{K,2} = 0$, the rest of prime number powers being greater than 0 for $\omega(K) \geq 3$, i.e. $\alpha_{K,i} \geq 1$ for $i = 3, 4, \cdots, \omega(K)$.

The conditions on the coefficients are given in Table I. We specify that these conditions have to be fulfilled only for the prime factors of K. The other prime factors from the factorization of CPP's coefficients are not to be considered when checking the conditions given in Table I.

III. CONDITIONS FOR A CPP INTERLEAVER TO BE EXPRESSED AS AN ARP INTERLEAVER

The aim of this section is to find the conditions a CPP has to meet, so that it can be expressed in terms of an ARP. A first condition resulting from the definition of ARP is that the value of Q is a submultiple of K. In this section, we derive an expression for the value of Q of the equivalent ARP that depends on K, on the coefficient f_3 of the CPP and on a positive integer denoted l. The conditions for the positive integer l are determined considering the equivalence between a CPP and an ARP. As it will be seen, these conditions result in two expressions that depend on the positive integer l, on the interleaver length K and on the coefficients f_2 and f_3 of the CPP and these expressions are positive integers.

As in [5], a sufficient condition for the existence of an ARP-equivalent form of a valid CPP interleaver is that the following equations hold:

$$(P \cdot x) \bmod K = (f_1 \cdot x) \bmod K, \quad \text{for } x = 0, \ldots, K-1 \tag{4}$$

and

$$S_{(x \bmod Q)} \bmod K = \left(f_2 \cdot x^2 + f_3 \cdot x^3\right) \bmod K, \quad \text{for } x = 0, \ldots, K-1. \tag{5}$$

The above equations are satisfied if:

$$P = f_1 \tag{6}$$

and

$$\left(f_2 \cdot x^2 + f_3 \cdot x^3\right) \bmod K = \left(f_2 \cdot (x+Q)^2 + f_3 \cdot (x+Q)^3\right) \bmod K, \quad \forall\, x = 0, \cdots, K-1. \tag{7}$$

Equation (7) is equivalent to

$$\left(f_2 \cdot x^2 + f_3 \cdot x^3\right) \bmod K = \left(f_2 \cdot x^2 + f_3 \cdot x^3 + (f_2 \cdot Q^2 + f_3 \cdot Q^3) + (2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2) \cdot x + (3 \cdot f_3 \cdot Q) \cdot x^2\right) \bmod K, \quad \forall\, x = 0, \cdots, K-1 \tag{8}$$

and (8) is true if

$$\left(f_2 \cdot Q^2 + f_3 \cdot Q^3\right) + \left(2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2\right) \cdot x + \left(3 \cdot f_3 \cdot Q\right) \cdot x^2 = 0 \bmod K, \quad \forall\, x = 0, \cdots, K-1. \tag{9}$$

Equation (9) is true if the second degree polynomial in variable x is a null polynomial modulo K, of degree less than or equal to two. The polynomial $z(x) = 0 \bmod K$ is always a trivial null polynomial. For a null polynomial of any degree, the free term must be equal to zero and null poynomials of first degree do not exist [23]. From [12], we know that the only quadratic null polynomial (QNP) modulo K exists when $2 \mid K$ and it is

$$z_{QNP}(x) = \left(\frac{K}{2} \cdot x + \frac{K}{2} \cdot x^2\right) \bmod K \tag{10}$$

Taking into account the above considerations, (9) is true if and only if

$$\begin{cases} \left(f_2 \cdot Q^2 + f_3 \cdot Q^3\right) = 0 \bmod K, \\ \left(2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2\right) = 0 \bmod K, \\ \left(3 \cdot f_3 \cdot Q\right) = 0 \bmod K \end{cases} \tag{11}$$

or, when $2 \mid K$,

$$\begin{cases} \left(f_2 \cdot Q^2 + f_3 \cdot Q^3\right) = 0 \bmod K, \\ \left(2 \cdot f_2 \cdot Q + 3 \cdot f_3 \cdot Q^2\right) = \dfrac{K}{2} \bmod K, \\ \left(3 \cdot f_3 \cdot Q\right) = \dfrac{K}{2} \bmod K \end{cases} \tag{12}$$

The third equation from system (11) is equivalent to

$$Q = \frac{l \cdot K}{3 \cdot f_3}, l \in \mathbb{N}^+ \tag{13}$$

With (13), system (11) becomes

$$\begin{cases} Q = \dfrac{l \cdot K}{3 \cdot f_3}, l \in \mathbb{N}^+ \\ \dfrac{l^2 \cdot K \cdot (3 \cdot f_2 + l \cdot K)}{3^3 \cdot f_3^2} \in \mathbb{N}^+ \\ \dfrac{l \cdot (2 \cdot f_2 + l \cdot K)}{3 \cdot f_3} \in \mathbb{N}^+ \end{cases} \tag{14}$$

The third equation from system (12) is equivalent to

$$Q = \frac{l_o \cdot K}{2 \cdot 3 \cdot f_3}, l_o \in \mathbb{N}_o \tag{15}$$

With (15), system (12) becomes

$$\begin{cases} Q = \dfrac{l_o \cdot K}{2 \cdot 3 \cdot f_3}, l_o \in \mathbb{N}_o \\ \dfrac{l_o^2 \cdot K \cdot (2 \cdot 3 \cdot f_2 + l_o \cdot K)}{2^3 \cdot 3^3 \cdot f_3^2} \in \mathbb{N}^+ \\ \dfrac{l_o \cdot (2^2 \cdot f_2 + l_o \cdot K)}{2^2 \cdot 3 \cdot f_3} - \frac{1}{2} \in \mathbb{N}^+ \end{cases} \tag{16}$$

IV. CPP Interleavers Seen as Particular Cases of ARP Interleavers

In this section, Theorem 1 expresses the conditions on powers of prime numbers from the factorization of the positive integer l mentioned in Section III for a CPP to be expressed as an ARP. For each different prime number, the powers from the factorization of l depend on the powers of the prime numbers from the factorization of K and on the powers of the prime numbers from the factorization of the coefficients f_2 and f_3 of the CPP.

We consider the prime factorization of K as:

$$K = 2^{\alpha_{K,1}} \cdot 3^{\alpha_{K,2}} \cdot \prod_{i=3}^{\omega(K)-n_{4a}} p_i^{\alpha_{K,i}} \cdot \prod_{i=\omega(K)-n_{4a}+1}^{\omega(K)} p_i, \tag{17}$$

where n_{4a} is the number of prime factors from the factorization of K fulfilling the conditions $3 \nmid (p_i - 1)$, $p_i > 3$ and $\alpha_{K,i} = 1$. These prime factors are written the last in the factorization of K. For $i = 3, \cdots, \omega(K) - n_{4a}$, if $3 \nmid (p_i - 1)$, then $\alpha_{K,i} > 1$. As in (3), $\omega(K)$ from (17) is a positive integer greater than or equal to 2. If $\omega(K) = 2$, the products $\prod_{i=3}^{\omega(K)-n_{4a}} p_i^{\alpha_{K,i}}$ and $\prod_{i=\omega(K)-n_{4a}+1}^{\omega(K)} p_i$ in (17) are considered to be equal to 1. In (17) we could also have $\alpha_{K,1} = 0$ and/or $\alpha_{K,2} = 0$, the rest of prime number powers being greater than 0 for $\omega(K) \geq 3$, i.e. $\alpha_{K,i} \geq 1$, for $i = 3, 4, \cdots, \omega(K) - n_{4a}$.

The decomposition of the coefficients f_j, $j = 2, 3$, is

$$f_j = 2^{\alpha_{f_j,1}} \cdot 3^{\alpha_{f_j,2}} \cdot \prod_{i=3}^{\omega(K)-n_{4a}} p_i^{\alpha_{f_j,i}} \cdot \prod_{i=\omega(K)-n_{4a}+1}^{\omega(K)} p_{i,f_j}^{\alpha_{f_j,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_j)} p_{i,f_j}^{\alpha_{f_j,i}}, \tag{18}$$

where $\omega(f_j)$ is a positive integer greater than or equal to $\omega(K)$. According to Table I, in (18) we could have $\alpha_{f_j,1} = 0$ and/or $\alpha_{f_j,2} = 0$ and/or $\alpha_{f_j,i} = 0$, for some indices $i \in \{3, 4, \cdots, \omega(K)\}$. When $\omega(f_j) > \omega(K)$, the rest of prime number powers are greater than 0, i.e $\alpha_{f_j,i} \geq 1$, for $i = \omega(K) + 1, \cdots, \omega(f_j)$. We have to mention that for a true CPP we could have the coefficient $f_2 = 0$. In this case, the decomposition of f_2 as in (18) is not valid and the terms which contain the variable f_2 in systems (14) and (16) must be removed. Writing f_1 as f_j from (18), with $j = 1$, when $\alpha_{K,2} > 0$, from $(f_1 + f_3) \neq 0 \bmod 3$ in Table I, it results that $\alpha_{f_3,2} = 0$ when $\alpha_{f_1,2} \geq 1$, and $\alpha_{f_3,2} \geq 0$ when $\alpha_{f_1,2} = 0$. When $\alpha_{f_3,i} = 0$ for an $i \in \{\omega(K) - n_{4a} + 1, \cdots, \omega(K)\}$, from the condition $f_2^2 = 3 \cdot f_1 \cdot f_3 \bmod p_i$, we have $\alpha_{f_2,i} = 0$ when $\alpha_{f_1,i} = 0$, and $\alpha_{f_2,i} \geq 1$ when $\alpha_{f_1,i} \geq 1$. The following example shows how the interleaver length K and the CPP coefficients f_2 and f_3 are written according to (17) and (18).

Example 1: Let the interleaver length be $K = 22540 = 2^2 \cdot 3^0 \cdot 7^2 \cdot 5^1 \cdot 23^1$. According to (17), we have $\omega(K) = 5$, $n_{4a} = 2$, $p_3 = 7$, $p_4 = 5$, $p_5 = 23$, $\alpha_{K,1} = 2$, $\alpha_{K,2} = 0$, $\alpha_{K,3} = 2$, $\alpha_{K,4} = 1$ and $\alpha_{K,5} = 1$.

Let the CPP coefficients be $f_1 = 11$, $f_2 = 4186 = 2^1 \cdot 3^0 \cdot 7^1 \cdot 5^0 \cdot 23^1 \cdot 13^1$ and $f_3 = 322 = 2^1 \cdot 3^0 \cdot 7^1 \cdot 5^0 \cdot 23^1$. It is easy to check that these coefficients verify the

conditions 1.b), 3) for $p_i = 7$ and 4.a) for $p_i = 5$ and $p_i = 23$ from Table I. Condition 1.b) is satisfied since $f_1 = 1 \bmod 2$, $f_2 = f_3 = 0 \bmod 2$, condition 3) is satisfied for $p_i = 7$ since $f_1 \neq 0 \bmod 7$, $f_2 = f_3 = 0 \bmod 7$, condition 4.a) is satisfied for $p_i = 5$ since $f_3 \neq 0 \bmod 5$ and $f_2^2 = 3 \cdot f_1 \cdot f_3 = 1 \bmod 5$, and the same condition is satisfied for $p_i = 23$ since $f_1 \neq 0 \bmod 23$, $f_2 = f_3 = 0 \bmod 23$. Thus, these coefficients lead to a valid CPP and, according to (18), we have $\omega(f_2) = 6$, $\omega(f_3) = \omega(K) = 5$, $\alpha_{f_2,1} = 1$, $\alpha_{f_2,2} = 0$, $\alpha_{f_2,3} = 1$, $\alpha_{f_2,4} = 0$, $\alpha_{f_2,5} = 1$, $\alpha_{f_2,6} = 1$, $\alpha_{f_3,1} = 1$, $\alpha_{f_3,2} = 0$, $\alpha_{f_3,3} = 1$, $\alpha_{f_3,4} = 0$ and $\alpha_{f_3,5} = 1$. ■

The decomposition of l from (13) is

$$l = 2^{\alpha_{l,1}} \cdot 3^{\alpha_{l,2}} \cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{l,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{l,i}} \tag{19}$$

and the decomposition of l_o from (15) is

$$l_o = 3^{\alpha_{l_o,2}} \cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{l_o,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{l_o,i}} \tag{20}$$

The following example shows how a valid value of l for the CPP from Example 1 is written according to (19).

Example 2: Let K, f_1, f_2, and f_3 be as in Example 1. Then, a valid value of l is $l = 42 = 2^1 \cdot 3^1 \cdot 7^1 \cdot 5^0 \cdot 23^0$, for which, from (13), $Q = 980$ results. Thus, according to (19), we have $\alpha_{l,1} = 1$, $\alpha_{l,2} = 1$, $\alpha_{l,3} = 1$, $\alpha_{l,4} = 0$, and $\alpha_{l,5} = 0$. ■

Rewriting the conditions from systems (14) and (16) and taking into account (17) - (20), we obtain the conditions for CPP interleavers to be expressed as ARP interleavers. These conditions are given in Theorem 1 below.

Theorem 1 (CPP expressed as ARP): Let K, f_j, $j = 2, 3$, and l be as in (17)-(19). A CPP can always be expressed as an ARP with $P = f_1$ and Q as in (13), where:

1) the valid range for $\alpha_{l,1}$ is

$$\alpha_{f_3,1} - \min\left\{\alpha_{K,1}, \min\left\{\alpha_{f_2,1} + 1, \alpha_{l,1} + \alpha_{K,1}\right\}, \frac{\alpha_{K,1} + \min\left\{\alpha_{f_2,1}, \alpha_{l,1} + \alpha_{K,1}\right\}}{2}\right\} \leq \alpha_{l,1} \leq \alpha_{f_3,1} \tag{21}$$

1.1) if $2 \nmid K$ and/or $\alpha_{K,1} < \alpha_{f_3,1} + 3$ and/or $\alpha_{f_3,1} \neq \alpha_{f_2,1} + 1$, and
1.2) if $2 \nmid K$, and/or $\alpha_{K,1} \neq \alpha_{f_3,1} + 1$ and/or $\alpha_{f_3,1} \neq \alpha_{f_2,1}$, and

$$-1 \leq \alpha_{l,1} \leq \alpha_{f_3,1} \tag{22}$$

1.3) if $2 \mid K$, $\alpha_{K,1} \geq \alpha_{f_3,1} + 3$ and $\alpha_{f_3,1} = \alpha_{f_2,1} + 1$, or
1.4) if $2 \mid K$, $\alpha_{K,1} = \alpha_{f_3,1} + 1$ and $\alpha_{f_3,1} = \alpha_{f_2,1}$.

2) the valid range for $\alpha_{l,2}$ is

$$\alpha_{f_3,2} + 1 - \min\left\{\alpha_{K,2}, \min\left\{\alpha_{f_2,2}, \alpha_{l,2} + \alpha_{K,2}\right\}, \frac{\alpha_{K,2} + \min\left\{\alpha_{f_2,2}, \alpha_{l,2} + \alpha_{K,2} - 1\right\}}{2}\right\} \leq \alpha_{l,2} \leq \alpha_{f_3,2} + 1 \tag{23}$$

3) the valid ranges for $\alpha_{l,i}$, $i = 3, 4, \cdots, \omega(K)$, are

$$\alpha_{f_3,i} - \min\left\{\alpha_{K,i}, \min\left\{\alpha_{f_2,i}, \alpha_{l,i} + \alpha_{K,i}\right\}, \frac{\alpha_{K,i} + \min\left\{\alpha_{f_2,i}, \alpha_{l,i} + \alpha_{K,i}\right\}}{2}\right\} \leq \alpha_{l,i} \leq \alpha_{f_3,i} \tag{24}$$

4) the values for $\alpha_{l,i}$, $i = \omega(K) + 1, \cdots, \omega(f_3)$, are

$$\alpha_{l,i} = \alpha_{f_3,i}. \tag{25}$$

Proof: See Appendix A-A. ■

If the coefficient $f_2 = 0$ then, by removing the terms containing the powers $\alpha_{f_2,1}$, $\alpha_{f_2,2}$, and $\alpha_{f_2,i}$ in the small brackets of equations (21), (23), and (24), respectively, we obtain that:

1) the valid ranges for $\alpha_{l,i}$, $i = 1, 3, 4, \cdots, \omega(K)$, are

$$\alpha_{f_3,i} - \alpha_{K,i} \leq \alpha_{l,i} \leq \alpha_{f_3,i} \tag{26}$$

2) the valid range for $\alpha_{l,2}$ is

$$\alpha_{f_3,2} + 1 - \min\left\{\alpha_{K,2}, \alpha_{K,2} + \frac{\alpha_{l,2} - 1}{2}\right\} \leq \alpha_{l,2} \leq \alpha_{f_3,2} + 1 \tag{27}$$

The values for $\alpha_{l,i}$, $i = \omega(K) + 1, \cdots, \omega(f_3)$, when $f_2 = 0$, are the same as in (25).

We mention that if the left-hand side of the double inequalities (21), (23), (24), (26) and (27) is negative, it is considered to be equal to 0. We specify that for the range of $\alpha_{l,1}$ given in (22), the value of l given in (19) is not a positive integer for $\alpha_{l,1} = -1$.

V. Conditions for the Interleaver Length K so That There Are Valid Values $Q < K$

Obviously, for $\alpha_{l,i} = \alpha_{f_3,i}$, with $i = 1, 3, \cdots, \omega(K)$, and $\alpha_{l,2} = \alpha_{f_3,2} + 1$, we have $Q = K$ from (13). For practical implementations, values $Q < K$ are desired. If $Q = 1$, the corresponding ARP is equivalent to a LPP and this case is trivial.

In the following, we demonstrate that, under conditions in Theorem 1, there are always valid values of Q so that $1 < Q < K$, when the prime factorization of K contains at least one prime number to a power higher than one and it fulfills the conditions for which there are true CPPs for this interleaver length. When the prime factorization of K contains only prime numbers to the power of one, with at least two prime numbers of type 4.a), values $Q < K$ are possible under some conditions on the coefficients of the second and third degree terms of the CPP, as will be shown below.

Recently, in [24], it was shown that the number of true CPPs is zero only when the interleaver length is of the form

$$K = 2^{\alpha_{K,1}} \cdot 3^{\alpha_{K,2}} \cdot \prod_{i=3}^{\omega(K)-n_{4a}} p_i, \quad \text{with } \alpha_{K,1} \in \{0, 1, 2\}, \alpha_{K,2} \in \{0, 1\}, 3 \mid (p_i - 1) \text{ and } p_i > 3, \text{ for } i = 3, 4, \cdots, \omega(K) - n_{4a} \tag{28}$$

TABLE II
CONDITIONS FOR VALID VALUES OF $Q < K$ FOR DIFFERENT PRIME FACTORIZATIONS OF K

	Indexes i of p_i	$i = 1$	$i = 2$	$i = 3, 4, \cdots, \omega(K) - n_{4a}$		$i = \omega(K) - n_{4a} + 1, \cdots, \omega(K)$	Conditions for $Q < K$
	Type of prime number p_i	$p_1 = 2$	$p_2 = 3$	Type 3) in Table I	Type 4.b) in Table I	Type 4.a) in Table I	
Case A	The power $\alpha_{K,i}$ of p_i	$\alpha_{K,1} \leq 2$	$\alpha_{K,2} \leq 1$	$\alpha_{K,i} \geq 1$	$\alpha_{K,i} \geq 2$	$\alpha_{K,i} = 0$ ($n_{4a} = 0$)	$\alpha_{K,i} \geq 2$ for at least $i \in \{3, 4, \cdots, \omega(K)\}$
Case B	The power $\alpha_{K,i}$ of p_i	$\alpha_{K,1} \leq 2$	$\alpha_{K,2} \leq 1$	$\alpha_{K,i} = 0$ ($\omega(K) - n_{4a} = 2$)		$\alpha_{K,i} = 1$	$\alpha_{f_3,i} \geq 1$ for at least $i \in \{3, 4, \cdots, \omega(K)\}$ or $\alpha_{K,1} = 2$ or ($\alpha_{K,2} = 1$ and $\alpha_{f_3,2} \geq 1$) or ($\alpha_{K,1} = 1$ and $\alpha_{f_2,1} \geq 1$ and $\alpha_{f_3,1} \geq 1$) or ($\alpha_{K,1} = 1$ and $\alpha_{f_2,1} = 0$ and $\alpha_{f_3,1} = 0$)
Case C	The power $\alpha_{K,i}$ of p_i	$\alpha_{K,1} \leq 2$	$\alpha_{K,2} \leq 1$	$\alpha_{K,i} \geq 1$	$\alpha_{K,i} \geq 2$	$\alpha_{K,i} = 1$	allways there is a value $Q < K$
Case D	The power $\alpha_{K,i}$ of p_i	$\alpha_{K,1} \geq 3$	$\alpha_{K,2} \geq 0$	$\alpha_{K,i} \geq 0$	$\alpha_{K,i} = 0$ or $\alpha_{K,i} \geq 2$	$0 \leq \alpha_{K,i} \leq 1$	allways there is a value $Q < K$
Case E	The power $\alpha_{K,i}$ of p_i	$\alpha_{K,1} \geq 0$	$\alpha_{K,2} \geq 2$	$\alpha_{K,i} \geq 0$	$\alpha_{K,i} = 0$ or $\alpha_{K,i} \geq 2$	$0 \leq \alpha_{K,i} \leq 1$	allways there is a value $Q < K$

From (28), we have that there are true CPPs, when $\alpha_{K,1} \geq 3$ and/or $\alpha_{K,2} \geq 2$ and/or $\alpha_{K,i} \geq 2$, for at least one index $i \in \{3, 4, \cdots, \omega(K) - n_{4a}\}$, and when the prime factorization of K contains at least one prime factor of type 4.a), i.e. $n_{4a} \geq 1$.

As the factorization of K contains the prime numbers 2, 3, and factors of type 3) or 4.b) and of type 4.a), we distinguish five cases for which Table II shows the conditions for existence valid values $Q < K$. These cases are analyzed below. Every combination of these cases in the factorization of K is immediate.

A. The Prime Factorization of K Contains Prime Factors of Type 3) or 4.b) and None Factor of Type 4.a)

If the prime factorization of K contains prime factors of type 3) or 4.b) and none factor of type 4.a) (i.e. $n_{4a} = 0$), and, possibly, the factors 2 and 3 fulfilling the conditions $\alpha_{K,1} \leq 2$ and $\alpha_{K,2} \leq 1$, considering (28), we have that true CPPs exist if $\alpha_{K,i} \geq 2$, for at least one index $i \in \{3, 4, \cdots, \omega(K) - n_{4a}\}$. For this case it means $i \in \{3, 4, \cdots, \omega(K)\}$, since $n_{4a} = 0$. From Table I, type 3), we have $\alpha_{f_2,i} \geq 1$ and $\alpha_{f_3,i} \geq 1$, for all $i = 3, 4, \cdots, \omega(K)$. Since the minimum value of quantities in the big brackets of relation (24) are greater than or equal to one, $\alpha_{l,i} = \alpha_{f_3,i} - 1$ verifies the first inequality in (24). Since $\alpha_{K,i} \geq 1$, it results that $\alpha_{l,i} = \alpha_{f_3,i} - 1$ also verifies (26). Therefore, the value of prime factor powers of Q is $\alpha_{l,i} + \alpha_{K,i} - \alpha_{f_3,i} = \alpha_{f_3,i} - 1 + \alpha_{K,i} - \alpha_{f_3,i} = \alpha_{K,i} - 1$ and thus, $Q < K$. The values of $Q > 1$ are provided due to the factor (or factors) to a power at least equal to 2 in the decomposition of K.

B. The Prime Factorization of K Contains at Least Two Prime Factors of Type 4.a)

If the prime decomposition of K contains at least two prime factors of type 4.a) and, possibly, the factors 2 and 3 fulfilling the conditions $\alpha_{K,1} \leq 2$ and $\alpha_{K,2} \leq 1$, considering (28), we have that true CPPs always exist. For the factors of type 4.a), we can have $\alpha_{f_3,i} \geq 1$ or $\alpha_{f_3,i} = 0$. If $\alpha_{f_3,i} \geq 1$, then $\alpha_{f_2,i} \geq 1$, and this happens for at most $n_{4a} - 1$ of the n_{4a} factors, because, otherwise, it would mean that $f_3 \in \{K/3, K/2, K\}$, which does not lead to a true CPP [19]. Therefore, for at least one factor of type 4.a) we have $\alpha_{f_3,i} = 0$, and hence $\alpha_{l,i} = 0$. If for all factors of type 4.a) we have $\alpha_{f_3,i} = 0$ (i.e. f_3 does not divide any prime factor of type 4.a)), then the minimum value of powers of the corresponding factors from the factorization of Q is $\alpha_{l,i} + \alpha_{K,i} - \alpha_{f_3,i} = 0 + 1 - 0 = 1$. In this case we have the following subcases:

1) If $\alpha_{K,1} = \alpha_{K,2} = 0$, the only valid value of Q is $Q = K$.
2) If $\alpha_{K,1} = 2$ and $\alpha_{K,2} = 0$, from Table I, case 1.b), we have that $\alpha_{f_3,1} \geq 1$ and $\alpha_{f_2,1} \geq 1$ or $f_2 = 0$ and, because $\alpha_{l,1} = \alpha_{f_3,1} - 1$ verifies the first inequality in (21) or (26) for $i = 1$, a valid value $Q < K$ is $K/2$.
3) If $\alpha_{K,1} = 1$ and $\alpha_{K,2} = 0$, from Table I, case 1.a), we could have $\alpha_{f_3,1} \geq 0$ and $\alpha_{f_2,1} \geq 0$. Then, we have:
   a) If $\alpha_{f_2,1} = 0$ and $\alpha_{f_3,1} \geq 1$, or if $\alpha_{f_2,1} \geq 1$ and $\alpha_{f_3,1} = 0$, or if $f_2 = 0$ and $\alpha_{f_3,1} = 0$, from (21) or (26) for $i = 1$, we have that $\alpha_{f_3,1}$ is the single value for $\alpha_{l,1}$ and thus, the only valid value of Q is $Q = K$.
   b) If $\alpha_{f_2,1} = 0$ and $\alpha_{f_3,1} = 0$, the valid range for $\alpha_{l,1}$ is as in (22), and thus, if $\alpha_{l,1} = -1$, a valid value of Q is $Q = K/2$.
   c) If $\alpha_{f_2,1} \geq 1$ and $\alpha_{f_3,1} \geq 1$, or if $f_2 = 0$ and $\alpha_{f_3,1} \geq 1$, as in the subcase 2), when $\alpha_{K,1} = 2$, a valid value $Q < K$ is $K/2$.
4) If $\alpha_{K,2} = 1$ and $\alpha_{K,1} = 0$, from Table I, case 2.a), we have that $\alpha_{f_2,2} \geq 1$ or $f_2 = 0$ and we could have $\alpha_{f_3,2} \geq 0$. Then, we have:

a) If $\alpha_{f_3,2} = 0$, as $\alpha_{l,2} = 0$ does not fulfill the first inequality in (23) or (27), the only valid value of Q is $Q = K$.
b) If $\alpha_{f_3,2} \geq 1$, as $\alpha_{l,2} = \alpha_{f_3,2}$ fulfills the first inequality in (23) or (27), a valid value $Q < K$ is $K/3$.

The subcases when $\alpha_{K,1} = 1$ and $\alpha_{K,2} = 1$, or when $\alpha_{K,1} = 2$ and $\alpha_{K,2} = 1$ are immediate.

If $\alpha_{f_3,i} \geq 1$ for at least one factor of type 4.a), we have at least one value $Q < K$, because the value $\alpha_{l,i} = \alpha_{f_3,i} - 1$ verifies the first inequality from (24) or (26). The values of $Q > 1$ are provided due to the factor (or factors) of type 4.a) from the decomposition of K for which $\alpha_{f_3,i} = 0$.

In the final of this subsection, we mention that true CPPs also exist when the decomposition of K contains only one prime factor of type 4.a). If K is a prime number of type 4.a), the only valid value of Q is $Q = K$. If K is a prime number of type 4.a) multiplied by $2^{\alpha_{K,1}}$ and/or $3^{\alpha_{K,2}}$, with $\alpha_{K,1} \in \{1, 2\}$ and $\alpha_{K,2} = 1$, then we have $\alpha_{f_3,3} = 0$ (p_3 is the prime number of type 4.a)) and the subcases 1) up to 4) above also hold. The smallest valid value of Q can be only p_3, which can be very large.

C. The Prime Factorization of K Contains at Least Two Prime Factors Greater Than 3, of Which at Least One of Type 4.a) and at Least One of Other Type

If the prime decomposition of K contains prime factors greater than 3, of which at least one of type 4.a) (i.e. $n_{4a} \geq 1$) and at least one of other type and, possibly, the factors 2 and 3 fulfilling the conditions $\alpha_{K,1} \leq 2$ and $\alpha_{K,2} \leq 1$, then, considering (28), we have that there are always true CPPs. Due to the prime factor or factors greater than 3, which are not of type 4.a), we have that at least one value $Q < K$ exists. Since for these factors the value $\alpha_{l,i} = \alpha_{f_3,i} - 1$ verifies the first inequality from (24) or (26), we have that the power of the corresponding prime factors from the factorization of Q is equal to $\alpha_{K,i} - 1$, that is $Q < K$. The values $Q > 1$ are provided due to the factor (or factors) of type 4.a) from the decomposition of K for which $\alpha_{f_3,i} = 0$.

D. The Prime Factorization of K Contains the Prime Factor 2 to the Power at Least 3

If the prime decomposition of K contains the prime factor 2 to the power at least 3 (i.e. $\alpha_{K,1} \geq 3$), considering (28), true CPPs always exist. In this case, from Table I, case 1.b), we have $\alpha_{f_2,1} \geq 1$ and $\alpha_{f_3,1} \geq 1$. Therefore, to show that there are valid values $Q < K$, it is sufficient to show that $\alpha_{l,1} = \alpha_{f_3,1} - 1$ verifies the first inequality from (21). Indeed, because $\alpha_{K,1} \geq 3$, $\alpha_{f_2,1} \geq 1$ and $\alpha_{f_3,1} \geq 1$, by replacing $\alpha_{l,1} = \alpha_{f_3,1} - 1$ into the left-hand side of (21), we have

$$\alpha_{f_3,1} - \min\left\{\alpha_{K,1}, \min\left\{\alpha_{f_2,1} + 1, \alpha_{f_3,1} - 1 + \alpha_{K,1}\right\}, \frac{\alpha_{K,1} + \min\left\{\alpha_{f_2,1}, \alpha_{f_3,1} - 1 + \alpha_{K,1}\right\}}{2}\right\} \leq \alpha_{f_3,1} - 2, \quad (29)$$

because each of the three terms between the big brackets are greater than or equal to two. Similarly, $\alpha_{l,1} = \alpha_{f_3,1} - 1$ verifies (26) for $i = 1$. The values $Q > 1$ are provided due to the condition $\alpha_{K,1} \geq 3$. In the case when $\alpha_{f_3,1} = \alpha_{f_2,1} + 1$ and $\alpha_{K,1} \geq \alpha_{f_3,1} + 3$, it results that $\alpha_{f_3,1} \geq 2$ and $\alpha_{K,1} \geq 5$ and, because the minimum value of $\alpha_{l,1}$ is -1, it results that the minimum value of the power of 2 in the factorization of Q is 2 and, hence, $Q < K$. If $\alpha_{K,1} = \alpha_{f_3,1} + 1$, then, because for true CPPs $f_3 < K/2$, it results that K contains other prime factors greater than 2, corresponding to the other analyzed cases.

E. The Prime Factorization of K Contains the Prime Factor 3 to the Power at Least 2

If the prime decomposition of K contains the prime factor 3 to the power at least 2 (i.e. $\alpha_{K,2} \geq 2$), considering (28), true CPPs always exist. In this case, it is sufficient to show that $\alpha_{l,2} = \alpha_{f_3,2}$ verifies the first inequality from (23) or (27). Considering $\alpha_{f_2,2} \geq 1$ and $\alpha_{f_3,2} \geq 0$, from case 2.b) in Table I, and $\alpha_{l,2} = \alpha_{f_3,2}$ into the left hand side of (23), we have

$$\alpha_{f_3,2} + 1 - \min\left\{\alpha_{K,2}, \min\left\{\alpha_{f_2,2}, \alpha_{f_3,2} + \alpha_{K,2}\right\}, \frac{\alpha_{K,2} + \min\left\{\alpha_{f_2,2}, \alpha_{f_3,2} + \alpha_{K,2} - 1\right\}}{2}\right\} \leq \alpha_{f_3,2}, \quad (30)$$

because each from the three terms between the big brackets are greater than or equal to one. Similarly, $\alpha_{l,2} = \alpha_{f_3,2}$ verifies (27). Values $Q > 1$ are provided because $\alpha_{K,2} \geq 2$.

In Appendix A-B we give three examples, for three different lengths of CPP interleavers, in which we calculate the values of Q and of S vector components for ARP equivalent interleavers, when the length of Q is reasonably small.

VI. Simulation Results

In this section, we give some CPPs that we found with better FER performances compared to those of QPPs or LPPs of some small and medium lengths from the LTE standard [18], and minimum values of Q for their ARP representations. We denote by Q_s the minimum value of Q. We compare the CPPs with QPPs/LPPs in terms of FER at high SNR in deciBells (dB) and in terms of minimum values of Q. In simulations, we considered a binary phase shift keying (BPSK) modulation and an additive white Gaussian noise (AWGN) channel. The generator matrix of the recursive convolutional component codes of the turbo code and the trellis termination method are as in LTE standard [18]. Thus, the coding rate of the turbo code is $R_c = K/(3 \cdot K + 12)$. We used the maximum a posteriori (MAP) decoding algorithm with an iteration stopping criterion based on the maximum absolute value of logarithm likelihood ratio (LLR). The threshold of LLR was set to 15. Each line of Table III shows: the interleaver length K, the value of SNR in dB, the number of distances (n_{dist}) in the distance spectra used in searching PPs, simulated FER, and for QPP/LPP and CPP we found the truncated upper bounds of FER, and the value of Q_s. The distance spectra of turbo codes were computed using the method from [25] and the C program available at [26]. At least 50 frame erros

TABLE III
FER (TUB(FER)) FOR CPPS AND QPPS/LPPS

K	SNR [dB]	n_{dist}	QPP or LPP	Q_s	$10^6\times$ FER (TUB(FER)) for QPP or LPP	CPP	Q_s	$10^6\times$ FER (TUB(FER)) for CPP
48	5.0	9	$11x$	1	1.5059 (0.1306)	$13x + 6x^2 + 4x^3$	12	0.9258 (0.1556)
120	4.0	7	$11x$	1	0.5223 (0.0624)	$45x + 0x^2 + 8x^3$	15	0.2577 (0.0560)
448	2.5	3	$139x + 112x^2$	2	1.8168 (0.3267)	$251x + 56x^2 + 112x^3$	4	1.2802 (0.0308)
592	2.0	3	$129x + 74x^2$	4	3.0400 (0.2896)	$315x + 0x^2 + 74x^3$	8	0.6657 (0.2193)
656	2.0	3	$21x + 246x^2$	4	1.9669 (0.0428)	$185x + 164x^2 + 82x^3$	8	0.5617 (0.0428)
688	2.2	3	$365x + 86x^2$	4	0.6749 (0.0272)	$323x + 0x^2 + 258x^3$	8	0.1793 (0.0278)
752	2.0	3	$165x + 94x^2$	4	1.8191 (0.2405)	$541x + 188x^2 + 94x^3$	8	0.5096 (0.1296)
816	2.2	3	$229x + 102x^2$	4	1.0478 (0.0145)	$399x + 102x^2 + 34x^3$	24	0.3181 (0.0126)
848	2.2	3	$185x + 318x^2$	4	0.8330 (0.0176)	$157x + 212x^2 + 318x^3$	8	0.1390 (0.0202)
912	1.8	3	$29x + 114x^2$	4	5.7172 (0.0494)	$287x + 114x^2 + 114x^3$	8	0.9350 (0.2885)
944	2.2	3	$265x + 118x^2$	4	1.0497 (0.0027)	$179x + 0x^2 + 354x^3$	8	0.1557 (0.0027)
976	2.3	3	$59x + 122x^2$	4	0.6804 (0.0086)	$307x + 0x^2 + 122x^3$	8	0.0751 (0.0016)

TABLE IV
NUMBER OF FRAME ERRORS (n_{er}) COUNTED IN SIMULATION OF CPPS WITH VERY LOW FER FROM TABLE III

CPP interleaver length K	688	816	848	944	976
Number of frame errors n_{er}	46	35	31	18	19

were counted for each simulation, except the CPPs with very low FER for which the number of frame errors are given in Table IV. The truncated upper bound of the FER (TUB(FER)) for AWGN channel is given by [27]:

$$\text{TUB(FER)} = 0.5 \cdot \sum_{i=1}^{n_{dist}} N_{d_i} \cdot \text{erfc}(\sqrt{R_c \cdot d_i \cdot SNR}) \quad (31)$$

In (31), d_i is the ith distance in the distance spectrum (d_1 being the minimum distance), N_{d_i} is the corresponding codeword multiplicity, R_c is the coding rate of the turbo code, SNR is the signal-to-noise ratio and erfc(·) is the complementary error function.

These QPPs/LPPs and CPPs were found using the method from [17] applied for two different classes of interleavers, as follows:

- for lengths smaller than or equal to 448, by maximizing the spread factor and then by minimizing the TUB(FER) value;

- for lengths greater than or equal to 592, by maximizing the Ω' metric among the interleavers with spread factor greater than or equal to $0.45 \cdot \sqrt{2K}$ [10] and then, by minimizing the TUB(FER) value.

From Table III, we observe that CPPs of medium lengths can achieve a FER at high SNR from approximately 3 up to 9 times smaller than for QPPs. For these lengths, the spread factor of CPPs is always greater than or equal to that of QPPs, while the nonlinearity degree of CPPs is always greater than that of QPPs. This fact togheter with small TUB(FER) values for these CPPs explains the FER performance differences [10]. For small lengths, the FER for CPPs is slightly smaller than FER for good QPPs or LPPs. Except the lengths 48, 120, and 816, the values of Q_s for CPPs in Table III are two times greater than the values of Q_s for QPPs. This difference is explained by better FER performances of CPPs compared to QPPs for these lengths. It is known that the increase of the number of ARP interleaver parameters can lead to better performances in terms of error rate.

In Section V, we shown that there are interleaver lengths K for which some CPPs lead only to values $Q = K$. It is interesting to see the performance differences between CPPs allowing just $Q = K$ and those allowing values $Q < K$. For this, we performed a search using the method described above among such several lengths, namely 55, 110, 187, 330, 374, 759, and 943. Firstly, the search was made among all CPPs of a certain length of the above ones and then only among the CPPs that can not be expressed as ARPs with $Q < K$. The search results are given in Table V with the same structure as Table III. From this table, we can see that CPPs that can be expressed as ARPs with $Q < K$ lead to significantly lower FER than those that can not be expressed as ARPs.

VII. ANALYSIS OF EVALUATION COMPLEXITY OF CPPS AND QPPS/LPPS

The complexity of QPPs and CPPs was evaluated in subsection V.B from [15]. From a mathematical point of view, a QPP can be evaluated at every point $x = 0, 1, \cdots, K-1$ with two multiplications, one addition and one modulo operation, while a CPP can be evaluated with three multiplications, two additions and one modulo operation. From a hardware perspective, a PP can be efficiently implemented using a recursive formula, given in [28] and [29] for QPPs and generalized in [15] for PPs of arbitrary degree, with a step size s equal to an arbitrary positive integer less than K. Thus, a QPP implementation requires precomputing and storage of three constants and then, for each step, two additions and two modulo operations. The implementation of a CPP requires precomputing and storage of four constants and then, for each step, three additions and three modulo operations.

TABLE V
FER (TUB(FER)) FOR CPPS WHICH CAN NOT BE EXPRESSED AS ARPS WITH $Q < K$ AND FOR CPPS WHICH CAN BE EXPRESSED AS ARPS WITH $Q < K$

K	SNR_{dB} [dB]	n_{dist}	CPP not expressed as ARP with $Q < K$	Q_s	$10^6\times$ FER (TUB(FER)) for CPP not expressed as ARP with $Q < K$	CPP expressed as ARP with $Q < K$	Q_s	$10^6\times$ FER (TUB(FER)) for CPP expressed as ARP with $Q < K$
55	5.0	9	$28x + 8x^2 + 6x^3$	55	3.1544 (0.5876)	$27x + 11x^2 + 11x^3$	5	0.7900 (0.2107)
110	3.5	9	$26x + 52x^2 + 53x^3$	110	23.702 (5.5831)	$38x + 11x^2 + 44x^3$	10	3.1769 (2.8624)
187	3.0	7	$123x + 10x^2 + 167x^3$	187	56.932 (14.228)	$124x + 51x^2 + 102x^3$	11	6.3537 (1.2211)
330	2.5	5	$126x + 114x^2 + 37x^3$	330	40.567 (2.7973)	$75x + 0x^2 + 44x^3$	15	6.0410 (0.4342)
374	2.5	5	$318x + 75x^2 + 50x^3$	374	183.88 (171.419)	$316x + 170x^2 + 51x^3$	22	1.5615 (1.0569)
759	2.0	3	$506x + 0x^2 + 80x^3$	759	339.41 (385.58)	$460x + 0x^2 + 22x^3$	69	2.7018 (2.9129)
943	2.0	3	$0x + 0x^2 + 663x^3$	943	68.492 (18.342)	$598x + 0x^2 + 697x^3$	23	2.7579 (3.6893)

TABLE VI
SUMMARY OF OPERATIONS AND STORAGE REQUIREMENTS FOR EVALUATION OF QPPS, CPPS, ARPS AND PLPPS. K IS THE INTERLEAVER LENGTH, s IS THE STEP SIZE FOR IMPLEMENTATION OF PPS WITH RECURSIVE FORMULAS GIVEN IN [15], [28], AND [29], Q IS THE PARAMETER FROM THE DEFINITION OF ARP INTERLEAVER (SEE (1)) AND L IS THE NUMBER OF LPPS FROM PLPP REPRESENTATION OF PPS (SEE [30])

	QPPs	CPPs	ARPs	PLPPs
Number of precomputed and stored constants	$3 \cdot s$	$4 \cdot s$	$Q + 1$	$2 \cdot L$
Number of additions	$2 \cdot (K - s)$	$3 \cdot (K - s)$	$K - Q$	$K - L$
Number of modulo operations	$2 \cdot (K - s)$	$3 \cdot (K - s)$	$K - Q$	$K - L$

Using ARP representations of QPPs and CPPs, from (1), we need one multiplication, one addition and one modulo operation for evaluation at every point $x = 0, 1, \cdots, K-1$. In addition, we need to store $Q+1$ values. Using the recursive formula:

$$\Pi_{ARP}(x + Q) = (\Pi_{ARP}(x) + P \cdot Q) \bmod K, \qquad (32)$$

after precomputing and storage the first Q values of $\Pi_{ARP}(x)$ (i.e. $\Pi_{ARP}(0)$, $\Pi_{ARP}(1)$, ..., $\Pi_{ARP}(Q-1)$) and precomputing and storage the value $(P \cdot Q) \bmod K$, we need only one addition and one modulo operation for evaluation at every point $x = Q, Q+1, \cdots, K-1$. A formula similar to (32), with $Q = s$, where s is an arbitrary positive integer, can be used for a LPP implementation. The evaluation of an ARP with $Q \geq 2$ is definitely more complex than that of a LPP with $s = 1$.

The number of additions and modulo operations as well as the number of precomputed and stored constants required for implementation of QPPs or CPPs are summarized in Table VI, when using the same step size s. From this table, we see that ARP representations of QPPs and CPPs are always more efficient in terms of the number of additions and modulo operations. ARP representations of QPPs and CPPs are more efficient in terms of the number of precomputed and stored constants when $s > (Q+1)/3$ and $s > (Q+1)/4$, respectively. For QPPs from Table III this means $s \geq 2$, and for CPPs of medium lengths, except the length 816, this means $s \geq 2$ or $s \geq 3$. ARP representations of CPPs from Table III require about two times more precomputed and stored constants and slightly fewer additions and modulo operations compared to ARP representations of QPPs.

Some PPs can also be represented by means of Parallel Linear Permutation Polynomials (PLPPs), consisting of L LPPs, introduced in [30] and named Generalized LPPs in [23], subsection 4.4. It was shown that an ARP is actually a particular PLPP with the linear term coefficients of the component LPPs equal to the value of P from (1) and $L = Q$. Using the recursive formula (32) for each of the L LPPs, the required number of additions, of modulo operations and of precomputed and stored constants for evaluation of a PLPP are also shown in Table VI. [[30], Lemma 3.3] gives a value of L in terms of the prime factorization of the interleaver length K, so that a PP of arbitrary degree can be decomposed into L LPPs. The values of L for the CPPs from Table III, computed using this Lemma, are equal to $Q_s/2$, except the lengths 48, 120 and 448 for which $L = Q_s$. Thus, for lengths for which $L = Q_s/2$, the ARP and PLPP representations of the CPPs lead to approximately the same storage requirements and computational complexity.

APPENDIX A
PROOF AND EXAMPLES FOR THEOREM 1

A. Proof of Theorem 1

From (13) and (17)-(19), we have

$$Q = \frac{l \cdot K}{3 \cdot f_3} = 2^{\alpha_{l,1}+\alpha_{K,1}-\alpha_{f_3,1}} \cdot 3^{\alpha_{l,2}+\alpha_{K,2}-\alpha_{f_3,2}-1} \cdot \prod_{i=3}^{\omega(K)-n_{4a}} p_i^{\alpha_{l,i}+\alpha_{K,i}-\alpha_{f_3,i}} \cdot \prod_{i=\omega(K)-n_{4a}+1}^{\omega(K)} p_i^{\alpha_{l,i}+1-\alpha_{f_3,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{l,i}-\alpha_{f_3,i}} \qquad (33)$$

or, from (15), (17), (18) and (20), when $2 \mid K$, we have

$$Q = \frac{l_o \cdot K}{2 \cdot 3 \cdot f_3} = 2^{\alpha_{K,1}-\alpha_{f_3,1}-1} \cdot 3^{\alpha_{l_o,2}+\alpha_{K,2}-\alpha_{f_3,2}-1} \cdot \prod_{i=3}^{\omega(K)-n_{4a}} p_i^{\alpha_{l_o,i}+\alpha_{K,i}-\alpha_{f_3,i}} \cdot \prod_{i=\omega(K)-n_{4a}+1}^{\omega(K)} p_i^{\alpha_{l_o,i}+1-\alpha_{f_3,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{l_o,i}-\alpha_{f_3,i}} \tag{34}$$

Since Q has to be a divisor of K, from (33), we have

$$\begin{aligned} &0 \le \alpha_{l,i} + \alpha_{K,i} - \alpha_{f_3,i} \le \alpha_{K,i} \\ &\Leftrightarrow \alpha_{f_3,i} - \alpha_{K,i} \le \alpha_{l,i} \le \alpha_{f_3,i}, \quad \text{for } i = 1, 3, 4, \cdots, \omega(K) \end{aligned} \tag{35}$$

$$\begin{aligned} &0 \le \alpha_{l,2} + \alpha_{K,2} - \alpha_{f_3,2} - 1 \le \alpha_{K,2} \\ &\Leftrightarrow \alpha_{f_3,2} + 1 - \alpha_{K,2} \le \alpha_{l,2} \le \alpha_{f_3,2} + 1 \end{aligned} \tag{36}$$

and

$$\alpha_{l,i} = \alpha_{f_3,i}, \quad \text{for } i = \omega(K) + 1, \cdots, \omega(f_3) \tag{37}$$

In (35) we have $\alpha_{K,i} = 1$, for all $i = \omega(K) - n_{4a} + 1, \cdots, \omega(K)$.

When $2 \mid K$, from (34) we have the same conditions for $\alpha_{l_o,i}$, with $i = 2, 3, \cdots, \omega(f_3)$ as for $\alpha_{l,i}$ from (35)-(37), and for $i = 1$, the next condition has to be fulfilled

$$0 \le \alpha_{K,1} - \alpha_{f_3,1} - 1 \le \alpha_{K,1} \Leftrightarrow \alpha_{K,1} \ge \alpha_{f_3,1} + 1 \tag{38}$$

Considering (37), from the second equation in system (14), we have:

$$\begin{aligned} &\frac{l^2 \cdot K \cdot (3 \cdot f_2 + l \cdot K)}{3^3 \cdot f_3^2} \\ &= 2^{2\alpha_{l,1}+\alpha_{K,1}+\alpha_{f_2,1}-2\alpha_{f_3,1}} \cdot 3^{2\alpha_{l,2}+\alpha_{K,2}+\alpha_{f_2,2}-2\alpha_{f_3,2}-2} \cdot \prod_{i=3}^{\omega(K)} p_i^{2\alpha_{l,i}+\alpha_{K,i}+\alpha_{f_2,i}-2\alpha_{f_3,i}} \\ &\cdot \prod_{i=\omega(K)+1}^{\omega(f_2)} p_{i,f_2}^{\alpha_{f_2,i}} + 2^{3\alpha_{l,1}+2\alpha_{K,1}-2\alpha_{f_3,1}} \cdot 3^{3\alpha_{l,2}+2\alpha_{K,2}-2\alpha_{f_3,2}-3} \\ &\cdot \prod_{i=3}^{\omega(K)} p_i^{3\alpha_{l,i}+2\alpha_{K,i}-2\alpha_{f_3,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{f_3,i}} \\ &= 2^{2\alpha_{l,1}+\alpha_{K,1}-2\alpha_{f_3,1}} \cdot 3^{2\alpha_{l,2}+\alpha_{K,2}-2\alpha_{f_3,2}-2} \\ &\cdot \prod_{i=3}^{\omega(K)} p_i^{2\alpha_{l,i}+\alpha_{K,i}-2\alpha_{f_3,i}} \cdot \left\{ 2^{\alpha_{f_2,1}} \cdot 3^{\alpha_{f_2,2}} \cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{f_2,i}} \right. \\ &\cdot \left. \prod_{i=\omega(K)+1}^{\omega(f_2)} p_{i,f_2}^{\alpha_{f_2,i}} + 2^{\alpha_{l,1}+\alpha_{K,1}} \cdot 3^{\alpha_{l,2}+\alpha_{K,2}-1} \right. \\ &\cdot \left. \prod_{i=3}^{\omega(K)} p_i^{\alpha_{l,i}+\alpha_{K,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{f_3,i}} \right\} \in \mathbb{N}^+ \end{aligned} \tag{39}$$

The sufficient conditions for (39) to be a positive natural number are:

$$\alpha_{l,i} \ge \alpha_{f_3,i} - \frac{\alpha_{K,i} + \min\left\{\alpha_{f_2,i}, \alpha_{l,i} + \alpha_{K,i}\right\}}{2}, \quad \text{for } i = 1, 3, 4, \cdots, \omega(K) \tag{40}$$

and

$$\alpha_{l,2} \ge \alpha_{f_3,2} + 1 - \frac{\alpha_{K,2} + \min\left\{\alpha_{f_2,2}, \alpha_{l,2} + \alpha_{K,2} - 1\right\}}{2} \tag{41}$$

In (39) and (40), we have $\alpha_{K,i} = 1$, for all $i = \omega(K) - n_{4a} + 1, \cdots, \omega(K)$. Conditions (40) and (41) are also necessary when the two terms in the brackets of the $\min\{\cdot,\cdot\}$ functions are not equal, i.e. when:

$$\begin{cases} \alpha_{f_2,i} \ne \alpha_{l,i} + \alpha_{K,i}, & \text{for } i = 1, 3, 4, \cdots, \omega(K), \\ \alpha_{f_2,2} \ne \alpha_{l,2} + \alpha_{K,2} - 1 \end{cases} \tag{42}$$

If $\alpha_{f_2,i} = \alpha_{l,i} + \alpha_{K,i}$ for an $i \in \{1, 3, 4, \cdots, \omega(K)\}$, then the term in the big brackets of (39) may be a multiple of p_i. Thus, in the right-hand side of the inequality (40) a positive number is substracted. In this case, the left-hand side of the double inequality (35) is greater than the right-hand side of the inequality (40) and hence, (35) is a necessary and sufficient condition for the range of $\alpha_{l,i}$ resulted from the first two equations of system (14). Similarly, if $\alpha_{f_2,2} = \alpha_{l,2} + \alpha_{K,2} - 1$, (36) is a necessary and sufficient condition for the range of $\alpha_{l,2}$. So, the final range for $\alpha_{l,i}$ is not affected whether the conditions from (42) are fulfilled, when only (40) and (41) are considered.

When $2 \mid K$, from the second equation in system (16) we have the same conditions for $\alpha_{l_o,i}$, with $i = 2, 3, \cdots, \omega(K)$ as for $\alpha_{l,i}$ from (40)-(41), and for $i = 1$, the next condition has to be fulfilled

$$\min\left\{\alpha_{K,1} + \alpha_{f_2,1} - 2\alpha_{f_3,1} - 2, 2\alpha_{K,1} - 2\alpha_{f_3,1} - 3\right\} \ge 0 \tag{43}$$

(43) holds when

$$\begin{cases} \alpha_{K,1} \ge 2\alpha_{f_3,1} + 2 - \alpha_{f_2,1}, \\ \alpha_{K,1} \ge \alpha_{f_3,1} + 2 \end{cases} \tag{44}$$

Since the sum of two odd numbers is an even number, for $i = 1$, the next two conditions are also valid:

$$\begin{cases} \alpha_{K,1} \ge \alpha_{f_3,1} + 1, \\ \alpha_{K,1} = \alpha_{f_2,1} + 1 \end{cases} \tag{45}$$

Considering (37), from the third equation in system (14) we have:

$$\begin{aligned} &\frac{l \cdot (2 \cdot f_2 + l \cdot K)}{3 \cdot f_3} \\ &= 2^{\alpha_{l,1}+\alpha_{f_2,1}-\alpha_{f_3,1}+1} \cdot 3^{\alpha_{l,2}+\alpha_{f_2,2}-\alpha_{f_3,2}-1} \\ &\cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{l,i}+\alpha_{f_2,i}-\alpha_{f_3,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_2)} p_{i,f_2}^{\alpha_{f_2,i}} + 2^{2\alpha_{l,1}+\alpha_{K,1}-\alpha_{f_3,1}} \\ &\cdot 3^{2\alpha_{l,2}+\alpha_{K,2}-\alpha_{f_3,2}-1} \cdot \prod_{i=3}^{\omega(K)} p_i^{2\alpha_{l,i}+\alpha_{K,i}-\alpha_{f_3,i}} \\ &\cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{f_3,i}} = 2^{\alpha_{l,1}-\alpha_{f_3,1}} \cdot 3^{\alpha_{l,2}-\alpha_{f_3,2}-1} \end{aligned}$$

$$\cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{l,i}-\alpha_{f_3,i}} \cdot \left\{ 2^{\alpha_{f_2,1}+1} \cdot 3^{\alpha_{f_2,2}} \cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{f_2,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_2)} p_{i,f_2}^{\alpha_{f_2,i}} + 2^{\alpha_{l,1}+\alpha_{K,1}} \cdot 3^{\alpha_{l,2}+\alpha_{K,2}} \cdot \prod_{i=3}^{\omega(K)} p_i^{\alpha_{l,i}+\alpha_{K,i}} \cdot \prod_{i=\omega(K)+1}^{\omega(f_3)} p_{i,f_3}^{\alpha_{f_3,i}} \right\} \in \mathbb{N}^+ \quad (46)$$

The sufficient conditions for (46) to be a positive natural number are:

$$\alpha_{l,1} \geq \alpha_{f_3,1} - \min\left\{\alpha_{f_2,1}+1, \alpha_{l,1}+\alpha_{K,1}\right\} \quad (47)$$

$$\alpha_{l,2} \geq \alpha_{f_3,2} + 1 - \min\left\{\alpha_{f_2,2}, \alpha_{l,2}+\alpha_{K,2}\right\} \quad (48)$$

$$\alpha_{l,i} \geq \alpha_{f_3,i} - \min\left\{\alpha_{f_2,i}, \alpha_{l,i}+\alpha_{K,i}\right\}, \quad \text{for } i = 3, 4, \cdots, \omega(K) \quad (49)$$

In (46) and (49) we have $\alpha_{K,i} = 1$, for all $i = \omega(K) - n_{4a} + 1, \cdots, \omega(K)$. The conditions (47)-(49) are also necessary when:

$$\begin{cases} \alpha_{f_2,1}+1 \neq \alpha_{l,1}+\alpha_{K,1}, \\ \alpha_{f_2,i} \neq \alpha_{l,i}+\alpha_{K,i}, \quad \text{for } i = 2, 3, 4, \cdots, \omega(K) \end{cases} \quad (50)$$

With a similar reasoning as that after equation (42), the final range for $\alpha_{l,i}$ is not affected whether the conditions from (50) are fulfilled, when only (47)-(49) are considered.

When $2 \mid K$, the third condition from system (16) is true if the quantity $\frac{l_o \cdot (2^2 \cdot f_2 + l_o \cdot K)}{2^2 \cdot 3 \cdot f_3}$ is an odd natural number multiplied by 2^{-1}. Thus, we have the same conditions for $\alpha_{l_o,i}$, with $i = 2, 3, \cdots, \omega(K)$, as for $\alpha_{l,i}$ in (48)-(49), and for $i = 1$, the next condition has to be fulfilled

$$\min\left\{\alpha_{f_2,1} - \alpha_{f_3,1}, \alpha_{K,1} - \alpha_{f_3,1} - 2\right\} = -1 \quad (51)$$

Again, since the sum of two odd numbers is an even number, for $i = 1$, the next condition is also valid:

$$\alpha_{K,1} = \alpha_{f_3,1} = \alpha_{f_2,1} + 2 \quad (52)$$

If (52) is true, then none of the conditions from systems (44) or (45) will hold.

Firstly, we consider the joint conditions from system (44) and equation (51). Since from the second inequality from (44) we have $\alpha_{K,1} - \alpha_{f_3,1} - 2 \geq 0$, (51) is true only if

$$\alpha_{f_2,1} - \alpha_{f_3,1} = -1 \Leftrightarrow \alpha_{f_3,1} = \alpha_{f_2,1} + 1 \quad (53)$$

With (53), the first inequality from (44) becomes $\alpha_{K,1} \geq \alpha_{f_3,1} + 3$ and thus, from (44) and (51), we have the next two conditions:

$$\begin{cases} \alpha_{K,1} \geq \alpha_{f_3,1} + 3, \\ \alpha_{f_3,1} = \alpha_{f_2,1} + 1 \end{cases} \quad (54)$$

Secondly, we consider the joint conditions from system (45) and equation (51), from which we obtain the next two conditions:

$$\begin{cases} \alpha_{K,1} = \alpha_{f_3,1} + 1, \\ \alpha_{f_3,1} = \alpha_{f_2,1} \end{cases} \quad (55)$$

TABLE VII
POSSIBLE VALUES OF Q FOR THE CPP WITH $K = 1696$, $f_1 = 55$, $f_2 = 954$ AND $f_3 = 1272$

l	18	36	72	954	1908	3816
Q	8	16	32	424	848	1696

TABLE VIII
EQUIVALENT ARP INTERLEAVER WITH $P = f_1$, $Q_s = 8$ AND $S(0) = S(4) = 0$

K	f_1	f_2	f_3	$S(1)$	$S(2)$	$S(3)$	$S(5)$	$S(6)$	$S(7)$
1696	55	954	1272	530	424	530	1378	424	1378

If the coefficient $f_2 = 0$, the second condition of the system (16) leads only to the inequality $\alpha_{K,1} \geq \alpha_{f_3,1}+2$, while the third condition of this system becomes $\alpha_{K,1} = \alpha_{f_3,1} + 1$. Thus, if $f_2 = 0$, we have not a particular range for $\alpha_{l,1}$.

Now, we want to derive the range for $\alpha_{l,1}$, resulted from the trivial null polynomial, when $2 \mid K$ and the conditions from systems (54) or (55) are true. Thus, rejoining the conditions (35) for $i = 1$, (40) for $i = 1$, and (47), we obtain

$$\alpha_{f_3,1} - \min\left\{\alpha_{K,1}, \min\left\{\alpha_{f_2,1}+1, \alpha_{l,1}+\alpha_{K,1}\right\}, \frac{\alpha_{K,1} + \min\left\{\alpha_{f_2,1}, \alpha_{l,1}+\alpha_{K,1}\right\}}{2}\right\} \leq \alpha_{l,1} \leq \alpha_{f_3,1} \quad (56)$$

We consider the conditions from the system (54). By replacing (53) in the left-hand side of the double inequality (56) and taking into account the first condition from (54), we have

$$\begin{aligned} &\alpha_{f_3,1} - \min\left\{\alpha_{K,1}, \min\left\{\alpha_{f_3,1}, \alpha_{l,1}+\alpha_{K,1}\right\}, \frac{\alpha_{K,1} + \min\left\{\alpha_{f_3,1}-1, \alpha_{l,1}+\alpha_{K,1}\right\}}{2}\right\} \\ &= \alpha_{f_3,1} - \min\left\{\alpha_{K,1}, \alpha_{f_3,1}, \frac{\alpha_{K,1}+\alpha_{f_3,1}-1}{2}\right\} \\ &= \alpha_{f_3,1} - \alpha_{f_3,1} = 0 \end{aligned} \quad (57)$$

and (56) becomes

$$0 \leq \alpha_{l,1} \leq \alpha_{f_3,1} \quad (58)$$

By replacing the conditions from the system (55) in the left-hand side of the double inequality (56), it results equal to 0 and thus, we also obtain the range for $\alpha_{l,1}$ as in (58).

Then, from (33), the power of 2 from the factorization of Q, denoted by $\alpha_{Q,1}$, is in the range $\alpha_{K,1} - \alpha_{f_3,1} \leq \alpha_{Q,1} \leq \alpha_{K,1}$. However, when $2 \mid K$ and (54) or (55) are true, from (34), the power of 2 from the factorization of Q can also take the value $\alpha_{K,1} - \alpha_{f_3,1} - 1$. Thus, when $2 \mid K$ and the sets of conditions (54) or (55) are true, the valid range for $\alpha_{l,1}$ is

$$-1 \leq \alpha_{l,1} \leq \alpha_{f_3,1} \quad (59)$$

In conclusion, rejoining the conditions (35)-(37), (40)-(41), (47)-(49), (54), (55) and (59), we have the conditions (21)-(25) given in Theorem 1.

TABLE IX
POSSIBLE VALUES OF Q FOR THE CPP WITH $K = 22540$, $f_1 = 11$, $f_2 = 4186$ AND $f_3 = 322$

l	3/2	3	6	21/2	21	69/2	42	69	138	483/2	483	966
Q	35	70	140	245	490	805	980	1610	3220	5635	11270	22540

B. Examples for Theorem 1

Example 3: Let the interleaver length be $K = 1696 = 2^5 \cdot 3^0 \cdot 53^1$ and the CPP coefficients be $f_1 = 55 = 5^1 \cdot 11^1$, $f_2 = 954 = 2^1 \cdot 3^2 \cdot 53^1$ and $f_3 = 1272 = 2^3 \cdot 3^1 \cdot 53^1$. These coefficients meet the conditions from Table I, resulting in a valid true CPP.

The values of l leading to valid values for Q are factorized as follows:

$$l = 2^{\alpha_{l,1}} \cdot 3^{\alpha_{l,2}} \cdot 53^{\alpha_{l,3}} \tag{60}$$

We have to impose the conditions (21), (23) and (24).

From (23), because $\alpha_{K,2} = 0$, we have

$$\alpha_{l,2} = \alpha_{f_3,2} + 1 = 2, \tag{61}$$

so that the factorization of Q is

$$Q = 2^{\alpha_{l,1}+2} \cdot 53^{\alpha_{l,3}} \tag{62}$$

Condition (21) can be written as:

$$3 - \min\left\{5, \min\left\{1+1, \alpha_{l,1}+5\right\}, \frac{5+\min\left\{1, \alpha_{l,1}+5\right\}}{2}\right\} \leq \alpha_{l,1} \leq 3 \Leftrightarrow 1 \leq \alpha_{l,1} \leq 3 \tag{63}$$

Condition (24) can be written as:

$$1 - \min\left\{1, \min\left\{1, \alpha_{l,3}+1\right\}, \frac{1+\min\left\{1, \alpha_{l,3}+1\right\}}{2}\right\} \leq \alpha_{l,3} \leq 1 \Leftrightarrow 0 \leq \alpha_{l,3} \leq 1 \tag{64}$$

From (63) and (64), we see that there are 6 possible values for l and, consequently, for Q, given in Table VII. The possible values for the vector S for this interleaver, for which $Q_s = 8$, are given in Table VIII.

Example 4: Let the interleaver length be $K = 22540 = 2^2 \cdot 7^2 \cdot 5^1 \cdot 23^1$ and the CPP coefficients be $f_1 = 11$, $f_2 = 4186 = 2^1 \cdot 7^1 \cdot 23^1 \cdot 13^1$ and $f_3 = 322 = 2^1 \cdot 7^1 \cdot 23^1$. These coefficients meet the conditions from Table I, resulting in a valid true CPP. We mention that this interleaver length and these CPP coefficients were also used in Example 1 from Section IV.

The values of l leading to valid values for Q are factorized as follows:

$$l = 2^{\alpha_{l,1}} \cdot 3^{\alpha_{l,2}} \cdot 7^{\alpha_{l,3}} \cdot 5^{\alpha_{l,4}} \cdot 23^{\alpha_{l,5}} \tag{65}$$

In the following relations, we consider $\alpha_{K,2} = 0$, $\alpha_{f_2,2} = \alpha_{f_2,4} = 0$ and $\alpha_{f_3,2} = \alpha_{f_3,4} = 0$.

From condition (23), because $\alpha_{K,2} = 0$ and $\alpha_{f_3,2} = 0$, we have

$$\alpha_{l,2} = 0 + 1 = 1, \tag{66}$$

so that the factorization of Q is

$$Q = 2^{\alpha_{l,1}+1} \cdot 7^{\alpha_{l,3}+1} \cdot 5^{\alpha_{l,4}+1} \cdot 23^{\alpha_{l,5}} \tag{67}$$

TABLE X
POSSIBLE VALUES OF Q FOR THE CPP WITH $K = 165$, $f_1 = 3$, $f_2 = 33$ AND $f_3 = 11$

l	3	33
Q	15	165

Since $\alpha_{K,1} = \alpha_{f_3,1} + 1$ and $\alpha_{f_3,1} = \alpha_{f_2,1}$, we have the range (22) for $\alpha_{l,1}$, i.e.

$$-1 \leq \alpha_{l,1} \leq 1 \tag{68}$$

Since $\alpha_{f_3,4} = 0$, from (24) we have

$$\alpha_{l,4} = 0 \tag{69}$$

Now, we have to impose condition (24) for $i = 3$ and $i = 5$. This condition can be written as:

$$1 - \min\left\{2, \min\left\{1, \alpha_{l,3}+2\right\}, \frac{2+\min\left\{1, \alpha_{l,3}+2\right\}}{2}\right\} \leq \alpha_{l,3} \leq 1 \Leftrightarrow 0 \leq \alpha_{l,3} \leq 1 \tag{70}$$

$$1 - \min\left\{1, \min\left\{1, \alpha_{l,5}+1\right\}, \frac{1+\min\left\{1, \alpha_{l,5}+1\right\}}{2}\right\} \leq \alpha_{l,5} \leq 1 \Leftrightarrow 0 \leq \alpha_{l,5} \leq 1 \tag{71}$$

From (68)-(71), we see that there are 12 possible values for l and, consequently, for Q, given in Table IX. As the minimum value of Q is too large, namely $Q_s = 35$, we have not given the possible values for the vector S for this interleaver.

Example 5: Let the interleaver length be $K = 165 = 3^1 \cdot 5^1 \cdot 11^1$ and the CPP coefficients be $f_1 = 3$, $f_2 = 33 = 3^1 \cdot 11^1$ and $f_3 = 11$. These coefficients meet the conditions from Table I, resulting in a valid true CPP.

The values of l leading to valid values for Q are factorized as follows:

$$l = 2^{\alpha_{l,1}} \cdot 3^{\alpha_{l,2}} \cdot 5^{\alpha_{l,3}} \cdot 11^{\alpha_{l,4}} \tag{72}$$

In the following relations, we consider $\alpha_{K,1} = 0$, $\alpha_{f_2,1} = \alpha_{f_2,3} = 0$ and $\alpha_{f_3,1} = \alpha_{f_3,2} = \alpha_{f_3,3} = 0$.

We have to impose the conditions (21), (23) and (24).

From (21), because $\alpha_{f_3,1} = 0$, we have

$$\alpha_{l,1} = 0, \tag{73}$$

so that the factorization of Q is

$$Q = 3^{\alpha_{l,2}} \cdot 5^{\alpha_{l,3}+1} \cdot 11^{\alpha_{l,4}} \tag{74}$$

Condition (23) can be written as:

$$0 + 1 - \min\left\{1, \min\left\{1, \alpha_{l,2}+1\right\}, \frac{1+\min\left\{1, \alpha_{l,2}+1-1\right\}}{2}\right\} \leq \alpha_{l,2} \leq 0 + 1$$

TABLE XI
EQUIVALENT ARP INTERLEAVER WITH $P = f_1$, $Q_s = 15$ AND $S(0) = S(12) = 0$

K	f_1	f_2	f_3	$S(1)$	$S(2)$	$S(3)$	$S(4)$	$S(5)$	$S(6)$	$S(7)$	$S(8)$	$S(9)$	$S(10)$	$S(11)$	$S(13)$	$S(14)$
165	3	33	11	44	55	99	77	55	99	110	154	132	110	154	44	22

$$\Leftrightarrow 1 - \min\left\{1, \min\left\{1, \alpha_{l,2}+1\right\}, \frac{1+\min\left\{1,\alpha_{l,2}\right\}}{2}\right\} \leq \alpha_{l,2} \leq 1 \Leftrightarrow \alpha_{l,2} = 1 \quad (75)$$

Condition (24) can be written as:

$$0 - \min\left\{1, \min\left\{0, \alpha_{l,3}+1\right\}, \frac{1+\min\left\{0,\alpha_{l,3}+1\right\}}{2}\right\} \leq \alpha_{l,3} \leq 0 \Leftrightarrow \alpha_{l,3} = 0 \quad (76)$$

and

$$1 - \min\left\{1, \min\left\{1, \alpha_{l,4}+1\right\}, \frac{1+\min\left\{1,\alpha_{l,4}+1\right\}}{2}\right\} \leq \alpha_{l,4} \leq 1 \Leftrightarrow 0 \leq \alpha_{l,4} \leq 1, \quad (77)$$

for $i = 3$ and $i = 4$, respectively.

From (75)-(77), we see that there are 2 possible values for l and, consequently, for Q, given in Table X. The possible values for the vector S for this interleaver, for which $Q_s = 15$, are given in Table XI.

For the same interleaver length $K = 165$, we consider the CPP coefficients $f_1 = 99$, $f_2 = 33$ and f_3=7. Because $\alpha_{f_3,1} = \alpha_{f_3,2} = \alpha_{f_3,3} = \alpha_{f_3,4} = 0$, the only value of Q for which we can express this CPP as an ARP is $Q = K = 165$.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpfull comments and suggestions that greatly improved this paper.

REFERENCES

[1] S. Crozier and P. Guinand, "High-performance low-memory interleaver banks for turbo-codes," in *Proc. IEEE 54th Veh. Technol. Conf. (VTC-Fall)*, vol. 4. Atlantic City, NJ, USA, Oct. 2001, pp. 2394–2398.

[2] C. Berrou, Y. Saouter, C. Douillard, S. Kerouédan, and M. Jézéquel, "Designing good permutations for turbo codes: Towards a single model," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 1. Paris, France, Jun. 2004, pp. 341–345.

[3] J. Sun, O. Y. Takeshita, and M. P. Fitz, "Permutation polynomial based deterministic interleavers for turbo codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Yokohama, Japan, Jul. 2003, p. 319.

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

[5] R. G. Bohórquez, C. A. Nour, and C. Douillard, "On the equivalence of interleavers for turbo codes," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 58–61, Feb. 2015.

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

[7] J. Ryu and O. Y. Takeshita, "On quadratic inverses for quadratic permutation polynomials over integer rings," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1254–1260, Mar. 2006.

[8] O. Y. Takeshita, "A new metric for permutation polynomial interleavers," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, Jul. 2006, pp. 1983–1987.

[9] E. Rosnes and O. Y. Takeshita, "Optimum distance quadratic permutation polynomial-based interleavers for turbo codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, USA, Jul. 2006, pp. 1988–1992.

[10] O. Y. Takeshita, "Permutation polynomial interleavers: An algebraic-geometric perspective," *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2116–2132, Jun. 2007.

[11] D. Tarniceriu, L. Trifina, and V. Munteanu, "About minimum distance for QPP interleavers," *Ann. Telecommun.*, vol. 64, nos. 11–12, pp. 745–751, Dec. 2009.

[12] H. Zhao, P. Fan, and V. Tarokh, "On the equivalence of interleavers for turbo codes using quadratic permutation polynomials over integer rings," *IEEE Commun. Lett.*, vol. 14, no. 3, pp. 236–238, Mar. 2010.

[13] L. Trifina, D. Tarniceriu, and V. Munteanu, "Improved QPP interleavers for LTE standard," in *Proc. IEEE Int. Symp. Signals, Circuits Syst. (ISSCS)*, Iasi, Romania, Jul. 2011, pp. 403–406.

[14] J. Lahtonen, J. Ryu, and E. Suvitie, "On the degree of the inverse of quadratic permutation polynomial interleavers," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3925–3932, Jun. 2012.

[15] E. Rosnes, "On the minimum distance of turbo codes with quadratic permutation polynomial interleavers," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4781–4795, Jul. 2012.

[16] L. Trifina, D. Tarniceriu, and V. Munteanu, "On dispersion and nonlinearity degree of QPP interleavers," *Appl. Math. Inf. Sci.*, vol. 6, no. 3, pp. 397–400, Sep. 2012.

[17] L. Trifina and D. Tarniceriu, "Improved method for searching interleavers from a certain set using Garello's method with applications for the LTE standard," *Ann. Telecommun.*, vol. 69, nos. 5–6, pp. 251–272, Jun. 2014.

[18] *3rd Generation Partnership Project, Multiplexing and channel coding (Release 8)*, document 3GPP TS 36.212 V8.3.0, 2015. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/136200_136299/136212/08.03.00_60/ts_136212v080300p.pdf

[19] L. Trifina and D. Tarniceriu, "Analysis of cubic permutation polynomials for turbo codes," *Wireless Pers. Commun.*, vol. 69, no. 1, pp. 1–22, Mar. 2013.

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

[21] Y.-L. Chen, J. Ryu, and O. Y. Takeshita, "A simple coefficient test for cubic permutation polynomials over integer rings," *IEEE Commun. Lett.*, vol. 10, no. 7, pp. 549–551, Jul. 2006.

[22] H. Zhao and P. Fan, "A note on 'A simple coefficient test for cubic permutation polynomials over integer rings,"' *IEEE Commun. Lett.*, vol. 11, no. 12, p. 991, Dec. 2007.

[23] J. Ryu, "Permutation polynomial based interleavers for turbo codes over integer rings," Ph.D. dissertation, Dept. Elect. Comput. Eng., Ohio State Univ., Columbus, OH, USA, 2007.

[24] L. Trifina and D. Tarniceriu, "A simple method to determine the number of true different quadratic and cubic permutation polynomial based interleavers for turbo codes," *Telecommun. Syst.*, to be published. [Online]. Available: http://link.springer.com/article/10.1007/s11235-016-0166-2

[25] R. Garello, P. Pierleoni, and S. Benedetto, "Computing the free distance of turbo codes and serially concatenated codes with interleavers: Algorithms and applications," *IEEE J. Sel. Areas Commun.*, vol. 19, no. 5, pp. 800–812, May 2001.

[26] *The Turbo Code Minimum Distance Algorithm—C-Program*, accessed on Sep. 2004. [Online]. Available: http://www.tlc.polito.it/garello/turbodistance/turbodistance.html

[27] J. G. Proakis, *Digital Communications*, 3rd ed. New York, NY, USA: McGraw-Hill, 1995.

[28] M. Cheng, M. Nakashima, J. Hamkins, B. Moision, and M. Barsoum, "A decoder architecture for high-speed free-space laser communications," *Proc. SPIE*, vol. 5712, pp. 174–185, Apr. 2005.

[29] Y. Sun and J. R. Cavallaro, "Efficient hardware implementation of a highly-parallel 3GPP LTE/LTE-advance turbo decoder," *Integr., VLSI J.*, vol. 44, no. 4, pp. 305–315, Sep. 2011.

[30] J. Ryu, "Efficient address generation for permutation polynomial based interleavers over integer rings," *IEICE Trans. Fundam.*, vol. E95-A, no. 1, pp. 421–424, Jan. 2012.

Lucian Trifina was born in Fălticeni, Romania, in 1976. He received the B.Sc. degree in electronics and telecommunications engineering, the M.Sc. degree in modern techniques for signal processing from the Gheorghe Asachi Technical University of Iaşi, Romania, in 2002 and 2003, respectively, and the Ph.D. degree, with the doctoral thesis "Turbo Codes—Theoretical and Practical Aspects" in 2007. He is currently with the Faculty of Electronics, Telecommunications and Information Technology, Department of Telecommunications, Gheorghe Asachi Technical University of Iaşi, as an Assistant Professor. His research interests are in coding theory with emphasis on turbo codes and space-time turbo codes.

Daniela Tarniceriu was born in Iaşi, Romania, in 1960. She received the M.Sc. degree in electrical engineering and the Ph.D. degree in electronics and telecommunications from the Gheorghe Asachi Technical University of Iaşi, Romania, in 1983 and 1997, respectively. In 1991, she joined the Faculty of Electronics and Telecommunications, Department of Communications, Gheorghe Asachi Technical University of Iaşi, and received the title of Professor in 2000. From 2005 to 2008 she was the Vice–Dean of the Faculty and from 2008 to 2016 she was the Head of the Department of Telecommunications, Gheorghe Asachi Technical University of Iaşi. In 2016, she became the Dean of the Faculty. Her research interests currently include digital signal processing and coding theory with emphasis on turbo coding and wireless systems.