A Simple Method to Determine the Number of True Different Quadratic and Cubic Permutation Polynomial Based Interleavers for Turbo Codes

Lucian Trifina, Daniela Tarniceriu

Abstract—Interleavers are important blocks of the turbo codes, their types and dimensions having a significant influence on the performances of the mentioned codes. If appropriately chosen, the permutation polynomial (PP) based interleavers lead to remarkable performances of these codes. The most used interleavers from this category are quadratic permutation polynomials (QPPs) and cubic permutation polynomials (CPPs). Based on the necessary and sufficient conditions for the coefficients of the second and third degree polynomials to be QPP and CPP, respectively and on the Chinese remainder theorem, in this paper we determine the number of true different QPPs that cannot be reduced to linear permutation polynomials (LPPs), and the number of true different CPPs that cannot be reduced to QPPs or LPPs. This is of particular interest when we need to find QPP or CPP based interleavers for turbo codes.

Keywords: quadratic permutation polynomial, cubic permutation polynomial, number of true different QPPs or CPPs, Long Term Evolution standard.

1. Introduction

The interleaver is a critical component of a turbo code. The algebraic interleavers are preferred because of several advantages: analytical design, outstanding performances and simple, practical implementation with high-speed, low-power consumption and little memory requirements [1].

From the category of permutation polynomial (PP) based interleavers, the quadratic permutation polynomial (QPPs) based ones [1-15] have got the most attention. They are used in the Long Term Evolution (LTE) standard [16]. Although QPP interleavers have remarkable performances, for some lengths, the cubic permutation polynomial (CPP) interleavers [17-19] bring improvements over QPPs in terms of bit error rate (BER) and frame error rate (FER) for Additive White Gaussian Noise (AWGN) and for independent fading Rayleigh channels, as shown in [17].

This paper proposes a way to determine the number of true different QPPs that cannot be reduced to linear permutation polynomials (LPPs) and the number of true different CPPs that cannot be reduced to QPPs or LPPs. The used method is based on the Chinese remainder theorem and is very simple to be applied. The number of true QPPs was also found in [8] in other way. The number of PPs with degree at most six was addressed in [20], but this approach did not consider the equivalence conditions and nor the number of polynomials, separately, for each polynomial degree.

The paper structure is as follows. QPPs and CPPs over integer rings are reviewed in Section 2. In Section 3, the used method based on the Chinese remainder theorem is presented. Section 4 provides the formulas for the number of true different QPP based interleavers, while Section 5 provides the formulas for the number of true different CPP based interleavers. Section 6 concludes the paper.

2. QPP and CPP Based Interleavers over Integer Rings

A PP based interleaver of degree *n* is of the form:

$$\pi(x) = q_0 + q_1 x + q_2 x^2 + \ldots + q_n x^n \pmod{N}, \tag{1}$$

where N is the interleaver length and the coefficients q_k, $k = \overline{1,n}$ are chosen so that $\pi(x)$ from (1), with $x = 0,1,\ldots,N-1$, is a permutation of the set $\mathbb{Z}_N = \{0,1,\ldots,N-1\}$. Without loss of generality of the problem dealt with in the paper, we consider $q_0 = 0$. For $n = 2$ and $n = 3$ in (1), a QPP and a CPP results, respectively.

The conditions for the coefficients q_1, q_2, so that $\pi(x)$ in (1) with $n = 2$ is a permutation polynomial, are given in [1] and the conditions for the coefficients q_1, q_2, q_3, so that $\pi(x)$ with $n = 3$ is a permutation polynomial, are given in [18-19]. They are summarized in Table 1 for QPPs and in Table 2 for CPPs, respectively, depending on the factors of decomposition in prime factors of the interleaver length N, as:

$$N = \prod_{\substack{p \in \mathrm{P}, \\ p|N}} p^{n_{N,p}}, \tag{2}$$

where P is the set of prime numbers, the notation $p \mid N$ means that p divides N and $n_{N,p} \geq 1$ for a finite number of prime numbers.

Table 1: Conditions for the coefficients q_1, q_2 so that $\pi(x)$ in (1) with $n = 2$ is a permutation polynomial

1.a)	$p = 2$	$n_{N,2} = 1$	$(q_1 + q_2) \neq 0 \pmod 2$
1.b)		$n_{N,2} > 1$	$q_1 \neq 0 \pmod 2$ and $q_2 = 0 \pmod 2$
2.	$p > 2$	$n_{N,p} \geq 1$	$q_1 \neq 0 \pmod p$, $q_2 = 0 \pmod p$

Table 2: Conditions for the coefficients q_1, q_2, q_3 so that $\pi(x)$ in (1) with $n = 3$ is a permutation polynomial

1.a)	$p = 2$	$n_{N,2} = 1$	$(q_1 + q_2 + q_3) \neq 0 \pmod 2$
1.b)		$n_{N,2} > 1$	$q_1 \neq 0, q_2 = 0, q_3 = 0 \pmod 2$
2.a)	$p = 3$	$n_{N,3} = 1$	$(q_1 + q_3) \neq 0, q_2 = 0 \pmod 3$
2.b)		$n_{N,3} > 1$	$q_1 \neq 0, (q_1 + q_3) \neq 0, q_2 = 0 \pmod 3$
3.a)	$3 \mid (p-1)$	$n_{N,p} = 1$	$q_1 \neq 0, q_2 = 0, q_3 = 0 \pmod p$
3.b)		$n_{N,p} > 1$	$q_1 \neq 0, q_2 = 0, q_3 = 0 \pmod p$
4.a)	$3 \nmid (p-1)$ $p > 3$	$n_{N,p} = 1$	$q_2^2 = 3q_1q_3 \pmod p$ if $q_3 \neq 0 \pmod p$ and $q_1 \neq 0 \pmod p, q_2 = 0 \pmod p$ if $q_3 = 0 \pmod p$
4.b)		$n_{N,p} > 1$	$q_1 \neq 0, q_2 = 0, q_3 = 0 \pmod p$

3. A Simple Method for Determining the Number of True Different Permutation Polynomial Based Interleavers Using the Chinese Remainder Theorem

In the following, we recall the result of the Chinese remainder theorem.

Theorem 1. Suppose $n_1, \cdots, n_k$ are positive integers that are pairwise coprime. Then, for any given sequence of integers $a_1, \cdots, a_k$, there is an integer x solving the following system of simultaneous congruences:

$$\begin{cases} x = a_1 \left(\mathrm{mod}\, n_1\right) \\ \cdots\cdots\cdots\cdots \\ x = a_k \left(\mathrm{mod}\, n_k\right) \end{cases} \tag{3}$$

Furthermore, all solutions x of this system are congruent modulo the product $N = n_1 \cdot \cdots \cdot n_k$. Hence

$$x = y \left(\mathrm{mod}\, n_i\right), 1 \le i \le k \qquad \Leftrightarrow \qquad x = y \left(\mathrm{mod}\, N\right) \tag{4}$$

Theorem 1 ensures that for two different sequences $a_1, \cdots, a_k$, two distinct modulo N solutions exist.

The method that we present in this paper uses the result of the following theorem from [2]:

Theorem 2 ([2]). For any $N = \prod_{j=1}^{s} p_j^{n_{N,p_j}}$, such that $s \in \mathbb{N}^*$, $n_{N,p_j} \ge 1$, $\forall j = \overline{1,s}$, $\pi(x)$ is a modulo N PP, iff $\pi(x)$ is also a PP modulo $p_j^{n_{N,p_j}}$, $\forall j = \overline{1,s}$.

Assume that $\pi(x)$ is a PP. Let there be:

$$q_{i,j} = q_i \left(\mathrm{mod}\, p_j^{n_{N,p_j}}\right), \ \forall j = \overline{1,s}, \ \forall i = \overline{1,n}. \tag{5}$$

Since the numbers $p_j^{n_{N,p_j}}$, $j = \overline{1,s}$, are relatively prime to each other, from the Chinese remainder theorem we have that for $\forall i = \overline{1,n}$, if we know the values $q_{i,j} \in \mathbb{Z}_{p_j^{n_{N,p_j}}}$, $j = \overline{1,s}$, then there is a single number $q_i \in \mathbb{Z}_N$, that is precisely the coefficient q_i for the assumed PP.

Since $\left(\sum_{i=1}^{n} q_i \cdot x^i\right)\left(\mathrm{mod}\, p_j^{n_{N,p_j}}\right) = \left(\sum_{i=1}^{n} q_{i,j} \cdot x^i\right)\left(\mathrm{mod}\, p_j^{n_{N,p_j}}\right)$, from the Theorem 2 above, it results that if the coefficients $q_{i,j} \in \mathbb{Z}_{p_j^{n_{N,p_j}}}$, $i = \overline{1,n}$, $\forall j = \overline{1,s}$, are chosen so that the polynomials $\left(\sum_{i=1}^{n} q_{i,j} \cdot x^i\right)\left(\mathrm{mod}\, p_j^{n_{N,p_j}}\right)$, $\forall j = \overline{1,s}$, are modulo $p_j^{n_{N,p_j}}$ PPs, $\forall j = \overline{1,s}$, then the coefficients $q_i \in \mathbb{Z}_N$, $i = \overline{1,n}$ determine a modulo N PP. Therefore, we can determine the number of modulo N PPs in the following way:

a) We decompose the interleaver length in prime factors $N = \prod_{j=1}^{s} p_j^{n_{N,p_j}}$, such that $s \in \mathbb{N}^*$, $n_{N,p_j} \ge 1$, $\forall j = \overline{1,s}$.

b) For any $j = \overline{1,s}$, we find all the coefficients $q_{i,j} \in \mathbb{Z}_{p_j^{n_{N,p_j}}}$, $i = \overline{1,n}$, so that the polynomial $\left(\sum_{i=1}^{n} q_{i,j} \cdot x^i\right)\left(\mathrm{mod}\, p_j^{n_{N,p_j}}\right)$ is a modulo $p_j^{n_{N,p_j}}$ PP. This can be done easily if we know the conditions the coefficients of the PP must met depending on p_j and

n_{N,p_j}, as is the case for QPPs and CPPs. We calculate the number of such modulo $p_j^{n_{N,p_j}}$ PPs from the coefficient conditions.

c) To determine the true number of different PPs, we must take into account the equivalence conditions imposed for PPs of degree n imposed and considering $q_n \neq 0$. For QPPs and CPPs, these equivalence conditions are given in [8-9] and [17], respectively. The condition $q_n = 0$ is met only when $q_{n,j} = 0$, $\forall j = \overline{1,s}$. For the remaining number of coefficients $q_{i,j} \in \mathbb{Z}_{p_j^{n_{N,p_j}}}$, $j = \overline{1,s}$, we compute the total number of combinations that can lead to a modulo N PP. It will be the product of numbers of all coefficient combinations for $j = \overline{1,s}$.

d) In the next section, we apply the method described above for the case of QPPs and CPPs and determine the true number of different QPPs and CPPs, respectively, depending on the types of factors that appear in prime factor decomposition of N. As in [8], we denote by $\Phi(N)$ the Euler function, which is the number of numbers relatively prime with N, smaller than N. It is given by the following equation:

$$\Phi(N) = N \cdot \prod_{\substack{p \in \mathrm{P}, \\ p|N}} \left(1 - \frac{1}{p}\right) \tag{6}$$

4. Determining the Number of True Different Quadratic Permutation Polynomial Based Interleavers

We mention that the equivalence condition of QPPs [8] requires that $q_2 < N/2$, when $2 \mid N$.

It is useful to determine the values $q_{i,j}$, $i = \overline{1,2}$, $j = \overline{1,s}$, for the Quadratic Null Polynomial (QNP). From [8], it is known that the only QNP is obtained for $q_1, q_2 = N/2$, when $2 \mid N$. Therefore, in this case the same QPP interleaver results, if the QPP coefficients change from (q_1, q_2) to $\left((q_1 + N/2) \pmod N, (q_2 + N/2) \pmod N\right)$. Thus, if $N = 2^{n_{N,2}} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $n_{N,2} \geq 1$, $p_j > 2$ and $n_{N,p_j} \geq 1$, $j = \overline{2,s}$, then $N/2 = 2^{n_{N,2}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$ and we have:

- For $n_{N,2} = 1$: $q_{i,1} = 1$ and $q_{i,j} = 0$, $\forall i = \overline{1,2}$, $\forall j = \overline{2,s}$. Therefore, in this case the same QPP interleaver results, if the values $q_{i,j}$, with $i = \overline{1,2}$ and $j = \overline{2,s}$, remain the same and the values $q_{i,1}$, $i = \overline{1,2}$, change to $(q_{i,1} + 1) \pmod 2$, $i = \overline{1,2}$.

- For $n_{N,2} > 1$: $q_{i,1} = 0$ and $q_{i,j} = 0$, $\forall i = \overline{1,2}$, $\forall j = \overline{2,s}$. In this case, all the coefficients $q_{i,j}$, $i = \overline{1,2}$, $j = \overline{1,s}$, remain the same for equivalent QPPs.

In the case of QPPs, we have three types of factors as shown in Table 1. These are considered in the following and for each type of prime factor, the number of QPPs is determined.

Case 1.a). If $p=2$ and $n_{N,2}=1$, the coefficients $q_{i,1}\in\mathbb{Z}_2=\{0,1\}$, $i=\overline{1,2}$. The condition $\left(q_{1,1}+q_{2,1}\right)\neq 0\left(\mathrm{mod}\,2\right)$ is met for $q_{1,1}=0,q_{2,1}=1$ or $q_{1,1}=1,q_{2,1}=0$. Since the two sets of coefficients lead to equivalent QPPs, from the two combinations only one must be kept, for example $q_{1,1}=1,q_{2,1}=0$, combined with other prime factors.

Case 1.b). If $p=2$ and $n_{N,2}>1$, the coefficients $q_{i,1}\in\mathbb{Z}_{2^{n_{N,2}}}$, $i=\overline{1,2}$. The condition $q_{1,1}\neq 0\left(\mathrm{mod}\,2\right)$ is met for $\Phi\left(2^{n_{N,2}}\right)=2^{n_{N,2}-1}$ coefficients. The condition $q_{2,1}=0\left(\mathrm{mod}\,2\right)$ is met for $\frac{2^{n_{N,2}}}{2}=2^{n_{N,2}-1}$ coefficients, from which one is zero. In this case, from the equivalence conditions of QPPs, it results that all values greater or equal to $\frac{2^{n_{N,2}}}{2}=2^{n_{N,2}-1}$ have to be removed, i.e. $\frac{2^{n_{N,2}-1}}{2}=2^{n_{N,2}-2}$ values, leading to $\frac{2^{n_{N,2}-1}}{2}=2^{n_{N,2}-2}$ values for $q_{2,1}$.

Case 2). If $p>2$ and $n_{N,p}\geq 1$, the coefficients $q_{i,j}\in\mathbb{Z}_{p^{n_{N,p}}}$, $i=\overline{1,2}$. The condition $q_{1,j}\neq 0\left(\mathrm{mod}\,p\right)$ is met for $\Phi\left(p^{n_{N,p}}\right)=p^{n_{N,p}-1}\cdot\left(p-1\right)$ coefficients. The condition $q_2=0\left(\mathrm{mod}\,p\right)$ is met for $\frac{p^{n_{N,p}}}{p}=p^{n_{N,p}-1}$ coefficients, from which one is zero.

We apply the method described in Section 3 and distinguish three situations for the decomposition in prime factors of N, namely:

a) $2\nmid N$, that is $N=\prod_{j=1}^{s}p_j^{n_{N,p_j}}$, with $p_j>2$ and $n_{N,p_j}\geq 1$. Then, from Case 2) above, the number of possible combinations for the coefficient q_1 results equal to $\prod_{j=1}^{s}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ and the number of coefficients q_2 is equal to $\prod_{j=1}^{s}p_j^{n_{N,p_j}-1}$. The value $q_2=0$ results only when $q_{2,j}=0,\forall j=\overline{1,s}$, that is for only one combination of the coefficients $q_{2,j}, j=\overline{1,s}$, which has to be removed. The number of QPPs will be:

$$C_{N,QPPs}=\prod_{j=1}^{s}\left(p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=1}^{s}p_j^{n_{N,p_j}-1}-1\right) \tag{7}$$

Equation (7) is equivalent to Theorem 6, case a) from [8].

From (7) we see that the number of QPPs is equal to 0, when the interleaver length is a product of prime numbers greater than 2, each of them to the power 1.

b) $4\mid N$, that is $N=2^{n_{N,2}}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}}$, with $n_{N,2}>1$, $p_j>2$ and $n_{N,p_j}\geq 1$, $j=\overline{2,s}$. From the cases 1.b) and 2) above, the number of possible combinations for the

coefficient q_1 results equal to $2^{n_{N,2}-1}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ and the number of coefficients q_2, equal to $2^{n_{N,2}-1}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}$. Since from the equivalence condition of QPPs we must have $q_2 < N/2$, a number of $\frac{1}{2}\cdot 2^{n_{N,2}-1}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}-1} = 2^{n_{N,2}-2}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}$ coefficients remain, from which the value $q_2 = 0$ has to be removed, finaly remaining $2^{n_{N,2}-2}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}-1$ values for true different QPPs. Then, the number of QPPs will be:

$$C_{N,QPPs} = 2^{n_{N,2}-1}\cdot\prod_{j=2}^{s}\left(p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(2^{n_{N,2}-2}\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}-1\right) \tag{8}$$

Equation (8) is equivalent to Theorem 6, case b) from [8].

From (8), we see that the number of QPPs is equal to 0 when the interleaver length is a multiple of 4 of a product of prime numbers greater than 2, each of them to the power 1.

c) $2 \mid N$ and $4 \nmid N$, that is $N = 2\cdot\prod_{j=2}^{s}p_j^{n_{N,p_j}}$, with $p_j > 2$ and $n_{N,p_j} \geq 1$, $j = \overline{2,s}$. From the cases 1.a) and 2) above the number of possible combinations for the coefficient q_1 results equal to $\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ and the number of coefficients q_2 equal to $\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}$. We mention that in this case all the $\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}$ coefficients q_2 are equal modulo N to $\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}$ different coefficients $q_2 < N/2$. Therefore, we have to only remove the value $q_2 = 0$, finally leading to $\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}-1$ values for the coefficient q_2 of true different QPPs. Then the number of QPPs will be:

$$C_{N,QPPs} = \prod_{j=2}^{s}\left(p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=2}^{s}p_j^{n_{N,p_j}-1}-1\right) \tag{9}$$

Equation (9) is equivalent to Theorem 6, case c) from [8].

From (9) we see that the number of QPPs is equal to 0 when the interleaver length is a multiple of 2 of a product of prime numbers greater than 2, each of them to the power 1.

From the cases a), b) and c), we conclude that the number of QPPs is 0 when the interleaver length is

$$N = 2^{n_{N,2}}\cdot\prod_{j=2}^{s}p_j \text{, with } n_{N,2} = \overline{0,2},\ p_j > 2,\ j = \overline{2,s} \tag{10}$$

Such lengths have to be avoided in designing QPP based interleavers.

5. Determining the Number of True Different Cubic Permutation Polynomial Based Interleavers

We note that from the equivalence conditions for CPPs [17], we must have:

- $q_2 < N/2$ and $q_3 < N/2$, when $2 \mid N$ and $3 \nmid N$.
- $q_3 < N/3$, when $3 \mid N$ and $2 \nmid N$.
- $q_2 < N/2$ and $q_3 < N/6$, when $6 \mid N$.

The 10 Cubic Null Polynomials (CNPs) are given in [17]. The values $q_{i,j}$, $i = \overline{1,2,3}$, $j = \overline{1,s}$, for these CNPs are given below, where the order of CNPs is that from [17] and the only QNP is left the last.

- If $2 \mid N$ and $3 \nmid N$, that is $N = 2^{n_{N,2}} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $n_{N,2} \geq 1$, $p_j > 2$ and $n_{N,p_j} \geq 1$, $j = \overline{2,s}$, there are two CNPs to which the only QNP is added. For these three NPs of degree at most equal to 3, the values of the coefficients $q_{i,j}$, $i = \overline{1,2,3}$, $j = \overline{1,s}$, are, in terms of $n_{N,2}$:

  1) when $n_{N,2} = 1$, we have: 1.I) $q_{1,1} = q_{3,1} = 1$, $q_{2,1} = 0$ and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$; 1.II) $q_{2,1} = q_{3,1} = 1$, $q_{1,1} = 0$ and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$; 1.III) $q_{1,1} = q_{2,1} = 1$, $q_{3,1} = 0$ and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$.

  2) when $n_{N,2} > 1$ for all the three NPs we have: 2.I), 2.II), 2.III) $q_{1,1} = q_{2,1} = q_{3,1} = 0$, and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$.

- If $3 \mid N$ and $2 \nmid N$, that is $N = 3^{n_{N,3}} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $n_{N,3} \geq 1$, $p_j > 2$ and $n_{N,p_j} \geq 1$, $j = \overline{2,s}$, there are two CNPs. The values of the coefficients $q_{i,j}$, $i = \overline{1,2,3}$, $j = \overline{1,s}$, for these two CNPs are given in terms of $n_{N,3}$:

  1) when $n_{N,3} = 1$, we have: 1.III) $q_{1,1} = 2; q_{3,1} = 1$ or $q_{1,1} = 1; q_{3,1} = 2$, depending on the product $\prod_{j=2}^{s} p_j^{n_{N,p_j}}$, $q_{2,1} = 0$ and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$; 1.IV) $q_{1,1} = 1; q_{3,1} = 2$ or $q_{1,1} = 2; q_{3,1} = 1$, depending on the product $\prod_{j=2}^{s} p_j^{n_{N,p_j}}$, $q_{2,1} = 0$ and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$.

  2) when $n_{N,3} > 1$, for both CNPs, we have: 2.III), 2.IV) $q_{1,1} = q_{2,1} = q_{3,1} = 0$, and $q_{i,j} = 0$, $\forall i = \overline{1,3}$, $\forall j = \overline{2,s}$.

- If $6 \mid N$, that is $N = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}}$, with $n_{N,2} \geq 1$, $n_{N,3} \geq 1$, $p_j > 2$ and $n_{N,p_j} \geq 1$, $j = \overline{3,s}$, there are 10 CNPs, to which the only QNP is added. The values of

the coefficients $q_{i,j}$, $i=\overline{1,2,3}$, $j=\overline{1,s}$, for these 11 NPs of degree at most equal to 3 are given in terms of $n_{N,2}$ and $n_{N,3}$:

1) when $n_{N,2}=1$ and $n_{N,3}=1$, we have: 1.I) $q_{1,1}=q_{3,1}=1$, $q_{2,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 1.II) $q_{2,1}=q_{3,1}=1$, $q_{1,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 1.III) $q_{1,1}=q_{2,1}=q_{3,1}=0$, $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.IV) $q_{1,1}=q_{2,1}=q_{3,1}=0$, $q_{1,2}=1; q_{3,2}=2$ or $q_{1,2}=2; q_{3,2}=1$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.V) $q_{1,1}=q_{3,1}=1$, $q_{2,1}=0$, $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.VI) $q_{1,1}=0$, $q_{2,1}=1$, $q_{3,1}=1$; $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.VII) $q_{1,1}=1$, $q_{2,1}=1$, $q_{3,1}=0$; $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.VIII) $q_{1,1}=1$, $q_{2,1}=1$, $q_{3,1}=0$; $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.IX) $q_{1,1}=1$, $q_{2,1}=0$, $q_{3,1}=1$; $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.X) $q_{1,1}=0$, $q_{2,1}=1$, $q_{3,1}=1$; $q_{1,2}=2; q_{3,2}=1$ or $q_{1,2}=1; q_{3,2}=2$, depending on the product $\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 1.XI) $q_{1,1}=q_{2,1}=1$, $q_{3,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$.

2) when $n_{N,2}=1$ and $n_{N,3}>1$, we have: 2.I) $q_{1,1}=q_{3,1}=1$, $q_{2,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 2.II) $q_{2,1}=q_{3,1}=1$, $q_{1,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 2.III) and 2.IV) $q_{1,1}=q_{2,1}=q_{3,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 2.V) and 2.IX) $q_{1,1}=q_{3,1}=1$, $q_{2,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 2.VI) and 2.X) $q_{1,1}=0$, $q_{2,1}=1$, $q_{3,1}=1$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 2.VII) and 2.VIII) $q_{1,1}=1$, $q_{2,1}=1$, $q_{3,1}=0$; and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 2.XI) $q_{1,1}=q_{2,1}=1$, $q_{3,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$.

3) when $n_{N,2}>1$ and $n_{N,3}=1$, we have: 3.I) and 3.II) $q_{1,1}=q_{2,1}=q_{3,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$; 3.III) - 3.X) $q_{1,1}=q_{2,1}=q_{3,1}=0$, $q_{1,2}=2;q_{3,2}=1$ or $q_{1,2}=1;q_{3,2}=2$, depending on the product $\prod_{j=3}^{s}p_j^{n_{N,p_j}}$, $q_{2,2}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{3,s}$; 3.XI) $q_{1,1}=q_{2,1}=q_{3,1}=0$, and $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{2,s}$.

4) when $n_{N,2}>1$ and $n_{N,3}>1$, we have: 4.I) - 4.XI) $q_{i,j}=0$, $\forall i=\overline{1,3}$, $\forall j=\overline{1,s}$.

In the case of CPPs, there are four types of prime factors, as shown in Table 2. They are considered below and we determine the number of CPPs for each type of prime factor. The prime factor 2 is considered the first one, the prime factor 3 is considered the second one and the other prime factors are considered with arbitrary indices $j>3$.

Case 1.a). If $p=2$ and $n_{N,2}=1$, the coefficients $q_{i,1}\in\mathbb{Z}_2=\{0,1\}$, $i=\overline{1,2,3}$. The condition $(q_{1,1}+q_{2,1}+q_{3,1})\neq 0(\bmod 2)$ is met for the following coefficient combinations: $q_{i,1}$, $i=\overline{1,2,3}$: $q_{1,1}=0,q_{2,1}=0,q_{3,1}=1$ or $q_{1,1}=0,q_{2,1}=1,q_{3,1}=0$ or $q_{1,1}=1,q_{2,1}=0,q_{3,1}=0$ or $q_{1,1}=1,q_{2,1}=1,q_{3,1}=1$. Since the four sets of coefficients lead to equivalent CNPs, only one must be kept in combination with other types of prime factors.

Case 1.b). If $p=2$ and $n_{N,2}>1$, the coefficients $q_{i,1}\in\mathbb{Z}_{2^{n_{N,2}}}$, $i=\overline{1,3}$. The condition $q_{1,1}\neq 0(\bmod 2)$ is met for $\Phi\left(2^{n_{N,2}}\right)=2^{n_{N,2}-1}$ coefficients. The condition $q_{2,1}=0(\bmod 2)$ or $q_{3,1}=0(\bmod 2)$ is met for $\frac{2^{n_{N,2}}}{2}=2^{n_{N,2}-1}$ coefficients. From the equivalence conditions of CPPs for $2\mid N$ and $3\not\mid N$, it results that from the values of $q_{2,1}$ and $q_{3,1}$ only $\frac{2^{n_{N,2}-1}}{2}=2^{n_{N,2}-2}$ lead to different permutations.

Case 2.a). If $p=3$ and $n_{N,3}=1$, the coefficients $q_{i,2}\in\mathbb{Z}_3=\{0,1,2\}$, $i=\overline{1,3}$. The condition $(q_{1,2}+q_{3,2})\neq 0(\bmod 3)$ is met for the following coefficient combinations: $q_{i,2}$, $i=\overline{1,3}$: $q_{1,2}=0,q_{3,2}=1$, or $q_{1,2}=0,q_{3,2}=2$, or $q_{1,2}=1,q_{3,2}=0$, or $q_{1,2}=1,q_{3,2}=1$, or $q_{1,2}=2,q_{3,2}=0$, or $q_{1,2}=2,q_{3,2}=2$. The condition $q_{2,2}=0(\bmod 3)$ is met only for $q_{2,2}=0$. From the equivalence conditions of CPPs for $2\not\mid N$ and $3\mid N$, it results that the six sets of coefficients $q_{i,2}$, $i=\overline{1,3}$, lead to only two distinct permutations that can be considered for $q_{1,2}=1,q_{3,2}=0$ or $q_{1,2}=2,q_{3,2}=0$ and $q_{2,2}=0$. Because for these two sets we have $q_{3,2}=q_{2,2}=0$, only $q_{1,2}$ being different, in combination with other prime factors we must consider two coefficients for $q_{1,2}$ and only one for $q_{2,2}$ and $q_{3,2}$, respectively.

Case 2.b). If $p=3$ and $n_{N,3}>1$ the coefficients $q_{i,2}\in\mathbb{Z}_{3^{n_{N,3}}}$, $i=\overline{1,3}$. The condition $q_{2,2}=0(\mathrm{mod}\,3)$ is met for $3^{n_{N,3}-1}$ values. The condition $q_{1,2}\neq 0(\mathrm{mod}\,3)$ is met for $\Phi\left(3^{n_{N,3}}\right)=2\cdot 3^{n_{N,3}-1}$ values. The set of values for $q_{1,2}$ is $\left\{1,2,4,5,7,8,\ldots,3^{n_{N,3}}-2,3^{n_{N,3}}-1\right\}$, of which $3^{n_{N,3}-1}$ values are equal to 1 modulo 3 and also $3^{n_{N,3}-1}$ values are equal to 2 modulo 3. As $q_{3,2}\in\mathbb{Z}_{3^{n_{N,3}}}$, the condition $\left(q_{1,2}+q_{3,2}\right)\neq 0(\mathrm{mod}\,3)$, for a fixed value of $q_{1,2}$, will be fullfiled for $3^{n_{N,3}-1}+3^{n_{N,3}-1}=2\cdot 3^{n_{N,3}-1}$ coefficients $q_{3,2}$. However, as $3^{n_{N,3}-1}$ is multiple of 3, from the equivalence conditions of CPPs for $2\not| N$ and $3|N$, it results that of the $2\cdot 3^{n_{N,3}-1}$ coefficients $q_{3,2}$ only $\frac{1}{3}\cdot 2\cdot 3^{n_{N,3}-1}=2\cdot 3^{n_{N,3}-2}$ lead to distinct permutations.

Cases 3.a), 3.b), 4.b). If $p>3$ and $n_{N,p}\geq 1$ when $p=3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p}>1$ when $p=3\cdot k+2, k\in\mathbb{N}$, the coefficients $q_{i,j}\in\mathbb{Z}_{p^{n_{N,p}}}$, $i=\overline{1,3}$. The condition $q_{1,j}\neq 0(\mathrm{mod}\,p)$ is met for $\Phi\left(p^{n_{N,p}}\right)=p^{n_{N,p}-1}\cdot(p-1)$ coefficients. The condition $q_{2,j}=0(\mathrm{mod}\,p)$ or $q_{3,j}=0(\mathrm{mod}\,p)$ is met for $\frac{p^{n_{N,p}}}{p}=p^{n_{N,p}-1}$ coefficients, of which one is zero.

Case 4.a). If $3\not|\,(p-1)$, $p>3$ and $n_{N,p}=1$, the coefficients $q_{i,j}\in\mathbb{Z}_p$, $i=\overline{1,3}$. The condition $q_{1,j}\neq 0(\mathrm{mod}\,p)$ is met for $\Phi(p)=p-1$ coefficients. The condition $q_{2,j}=0(\mathrm{mod}\,p)$ or $q_{3,j}=0(\mathrm{mod}\,p)$ is obviously met only for the value zero. When $q_{3,j}\neq 0(\mathrm{mod}\,p)$ (for $\Phi(p)=p-1$ values), the condition $q_{2,j}^2=3q_{1,j}q_{3,j}(\mathrm{mod}\,p)$ has to be fulfilled. This congruence equation, for fixed $q_{2,j}$ and $q_{3,j}$, has only one modulo p solution in the variable $q_{1,j}$ [21]. Therefore, by considering all the p possible values for $q_{2,j}$, a number of $p\cdot(p-1)$ coefficient combinations $q_{i,j}\in\mathbb{Z}_p$, $i=\overline{1,3}$, results, that verifies the condition $q_{2,j}^2=3q_{1,j}q_{3,j}(\mathrm{mod}\,p)$.

For this case, it is useful to see how many coefficient combinations result when the product of factors is of the type 4.a), that is $N=\prod_{j=1}^{n_{4a}}p_j$, with $p_j=3\cdot k+2, k\in\mathbb{N}^*$, $j=\overline{1,n_{4a}}$. The conditions $q_{1,j}\neq 0(\mathrm{mod}\,p)$, $q_{2,j}=0(\mathrm{mod}\,p)$ and $q_{3,j}=0(\mathrm{mod}\,p)$, have to be considered for each group of $n_{4a,0}$ prime factors of type 4.a), with $n_{4a,0}=\overline{1,n_{4a}}$. We denote by $I_{n_{4a}}=\{1,2,\ldots,n_{4a}\}$ the set of indices corresponding to those n_{4a} prime factors.

We firstly consider the case of groups consisting of only one prime factor, p_{j_1}. Thus, if $q_{3,j_1}=0(\mathrm{mod}\,p_{j_1})$, the following conditions must be meet $q_{1,j_1}\neq 0(\mathrm{mod}\,p_{j_1})$ and $q_{2,j_1}=0(\mathrm{mod}\,p_{j_1})$, and if $q_{3,j}\neq 0(\mathrm{mod}\,p_j)$, the condition $q_{2,j}^2=3q_{1,j}q_{3,j}(\mathrm{mod}\,p_j)$,

$\forall j \in I_{n_{4a}}$, $j \neq j_1$ must be met. The first set of conditions is met for $p_{j_1} - 1$ coefficients q_1 and a single value for q_2 and q_3, respectively, which is zero. The second set of conditions is met for $\prod_{\substack{j=1,\\ j\neq j_1}}^{n_{4a}} \left(p_j - 1\right)$ coefficients q_3, and the congruence equation has one solution in the variable $q_{1,j}$, for each of the $\prod_{\substack{j=1,\\ j\neq j_1}}^{n_{4a}} p_j$ coefficients q_2, and the $\prod_{\substack{j=1,\\ j\neq j_1}}^{n_{4a}} \left(p_j - 1\right)$ coefficients q_3. Therefore, in total, for the groups consisting of one factor p_{j_1}, for which $q_{3,j_1} = 0 \left(\mathrm{mod}\, p_{j_1}\right)$, we have $\left(p_{j_1} - 1\right) \cdot \prod_{\substack{j=1,\\ j\neq j_1}}^{n_{4a}} p_j \cdot \prod_{\substack{j=1,\\ j\neq j_1}}^{n_{4a}} \left(p_j - 1\right)$ combinations of coefficients q_i, $i = \overline{1,3}$.

In the following, we consider the case of groups consisting of two prime factors, p_{j_1} and p_{j_2} Thus, if $q_{3,j} = 0 \left(\mathrm{mod}\, p_j\right)$, for $j \in \{j_1, j_2\}$ the conditions $q_{1,j} \neq 0 \left(\mathrm{mod}\, p_j\right)$ and $q_{2,j} = 0 \left(\mathrm{mod}\, p_j\right)$ must be met for $j \in \{j_1, j_2\}$, and if $q_{3,j} \neq 0 \left(\mathrm{mod}\, p_j\right)$, the condition $q_{2,j}^2 = 3 q_{1,j} q_{3,j} \left(\mathrm{mod}\, p_j\right)$, $\forall j \in I_{n_{4a}}$, $j \neq j_1$ and $j \neq j_2$ must be met. The first set of conditions is met for $\left(p_{j_1} - 1\right) \cdot \left(p_{j_2} - 1\right)$ coefficients q_1 and a single value for q_2 and q_3, respectively, which is zero. The second set of conditions is met for $\prod_{\substack{j=1,\\ j\neq j_1,\\ j\neq j_2}}^{n_{4a}} \left(p_j - 1\right)$ coefficients q_3, and the congruence equation has one solution in the variable $q_{1,j}$, for each of the $\prod_{\substack{j=1,\\ j\neq j_1,\\ j\neq j_2}}^{n_{4a}} p_j$ coefficients q_2 and the $\prod_{\substack{j=1,\\ j\neq j_1,\\ j\neq j_2}}^{n_{4a}} \left(p_j - 1\right)$ coefficients q_3. Thus, in total, for the groups consisting of two factors, p_{j_1} and p_{j_2}, for which $q_{3,j} = 0 \left(\mathrm{mod}\, p_j\right)$, $j \in \{j_1, j_2\}$, we have $\left(p_{j_1} - 1\right) \cdot \left(p_{j_2} - 1\right) \cdot \prod_{\substack{j=1,\\ j\neq j_1,\\ j\neq j_2}}^{n_{4a}} p_j \cdot \prod_{\substack{j=1,\\ j\neq j_1,\\ j\neq j_2}}^{n_{4a}} \left(p_j - 1\right)$ combinations of coefficients q_i, $i = \overline{1,3}$.

Let the set $I_{n_{4a,0}} \subseteq I_{n_{4a}}$, with $1 \leq n_{4a,0} < n_{4a}$ (the notation 0 derives from the fact that $q_{3,j} = 0 \left(\mathrm{mod}\, p_j\right)$, for $j \in I_{n_{4a,0}}$). Then, if there are groups of $n_{4a,0}$ prime factors of type 4.a), it means that the following conditions have to be met: $q_{1,j} \neq 0 \left(\mathrm{mod}\, p_j\right)$, $q_{2,j} = 0 \left(\mathrm{mod}\, p_j\right)$, if $q_{3,j} = 0 \left(\mathrm{mod}\, p_j\right)$, $\forall j \in I_{n_{4a,0}}$, and $q_{2,j}^2 = 3 q_{1,j} q_{3,j} \left(\mathrm{mod}\, p_j\right)$, if $q_{3,j} \neq 0 \left(\mathrm{mod}\, p_j\right)$, $\forall j \in I_{n_{4a}} - I_{n_{4a,0}}$.

The first set of conditions is met for $\prod_{j\in I_{n_{4a},0}}\left(p_j-1\right)$ coefficients q_1 and one value for q_2 and q_3, respectively, which is zero. The second set of conditions is met for $\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}\left(p_j-1\right)$ coefficients q_3, and the congruence equation has one solution in the variable $q_{1,j}$, for each of the $\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}p_j$ coefficients q_2 and the $\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}\left(p_j-1\right)$ coefficients q_3. Thus, in total, for groups consisting of $n_{4a,0}$ factors, for which $q_{3,j}=0\left(\mathrm{mod}\,p_j\right),\quad j\in I_{n_{4a,0}}$, we will have $\prod_{j\in I_{n_{4a},0}}\left(p_j-1\right)\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}^{n_{4a}}p_j\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}\left(p_j-1\right)$ combinations of coefficients q_i, $i=\overline{1,3}$. If $I_{n_{4a,0}}=I_{n_{4a}}$, that is $n_{4a,0}=n_{4a}$, we have $\prod_{j=1}^{n_{4a}}\left(p_j-1\right)$ coefficients q_1 and one coefficient q_2 and q_3, respectively (namely, the value zero that will be removed from the combinations with other prime factors).

In the case of CPPs, there are four types of prime numbers that are considered in stating the conditions in Table 2, each with two distinct sets of values of power of the prime number. As the conditions for the cases 1.b) 3.a), 3.b) and 4.b) are the same, there are 23 possible cases of decomposition of the number N in prime factors, which lead to combinations of different conditions on the coefficients q_1,q_2,q_3. Some of these cases are for very small values of the number N, being trivial cases.

Firstly, the cases excluding the factors of types 3.a) or 3.b) or 4.b) are shown (cases 4-11). However, because they are particular cases of the situations including these factors, the number of CPPs can be obtained using the same formulas, but replacing products including these factors by 1. This is the reason for which for cases 4-11 we will refer the next cases, that is, 12-23.

We analyse separately each case.

Case 1) The decomposition of N contains prime factors of type 1.a.), that is $N=2$.

Since $N=2$ is even, it requires that $q_3<N/2=1$. As q_3 can not be 0, there is no CPP in this case, i.e. $C_{2,CPPs}=0$.

Case 2) The decomposition of N contains prime factors of type 2.a), that is N=3.

Since $N=3$, from the equivalence conditions, it requires that $q_3<N/3=1$. As q_3 can not be 0, there is no CPP in this case, i.e. $C_{3,CPPs}=0$.

Case 3) The decomposition of N containes prime factors of the type 1.a) and 2.a), that is $N=6$.

Because in this case from the equivalence conditions of CPPs it requires that $q_3<\frac{N}{6}=1$, there is no CPP, i.e. $C_{6,CPPs}=0$.

Case 4) The decomposition of N containes prime factors of the type 2.b), that is N is a power of 3, greater than 1.

This is a particular case of 16), for odd *N*, therefore we can use equation (17) in which the products $\prod_{j=2}^{s} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 5) The decomposition of N containes prime factors of the type 1.a) and 2.b).

This is a particular case of 17), therefore we can use equation (19) in which the products $\prod_{j=3}^{s} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 6) The decomposition of N containes prime factors of the type 4.a).

This is a particular case of 18), for odd *N*, therefore we can use equation (23) in which the products $\prod_{j=1}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$, $\prod_{j=1}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 7) The decomposition of N containes prime factors of the type 1.a) and 4.a).

This is a particular case of 19), therefore we can use equation (25), in which the products $\prod_{j=2}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$, $\prod_{j=2}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 8) The decomposition of N containes prime factors of the type 2.a) and 4.a).

This is a particular case of 20), for odd *N*, therefore we can use equation (29) in which the products $\prod_{j=2}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$, $\prod_{j=2}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 9) The decomposition of N containes prime factors of the type 1.a) and 2.a) and 4.a).

This is a particular case of 21), therefore we can use equation (31) in which the products $\prod_{j=3}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$, $\prod_{j=3}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 10) The decomposition of N containes prime factors of the type 2.b) and 4.a).

This is a particular case of 22) for odd N , therefore we can use equation (35) in which the products $\prod_{j=2}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$, $\prod_{j=2}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 11) The decomposition of N containes prime factors of the type 1.a) and 2.b) and 4.a).

This is a particular case of 23), therefore we can use equation (37) in which the products $\prod_{j=3}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$, $\prod_{j=3}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)$ and $\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}$ are replaced by 1.

Case 12) The decomposition of N containes prime factors of the type 1.b) or 3.a) or 3. b) or 4.b).

In this case, depending whether the factor of type 1.b) is present, there are two situations.

When there is no factor of type 1.b), N is odd, $2 \not| N$ and $3 \not| N$, and we can write $N = \prod_{j=1}^{s} p_j^{n_{N,p_j}}$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{1,s}$. Then, from the cases 3.a), 3.b) and 4.b) above, the number of possible combinations for the q_1 is equal to $\prod_{j=1}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)$ and the total number of coefficients q_2 and q_3, respectively, are equal to $\prod_{j=1}^{s} p_j^{n_{N,p_j}-1}$. The value $q_3 = 0$ results only when $q_{3,j} = 0, \forall j = \overline{1,s}$, that is, for a single combination of coefficients $q_{3,j}, j = \overline{1,s}$, that has to be removed. The number of CPPs will be equal to:

$$C_{N,CPPs} = \prod_{j=1}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \cdot \left(\prod_{j=1}^{s} p_j^{n_{N,p_j}-1} - 1 \right) \tag{11}$$

From (11), we see that the number of CPPs is equal to 0 if the interleaver length is a product of prime numbers greater than 3, of the form $3 \cdot k + 1, k \in \mathbb{N}$, each of them to power 1.

When there is a factor of the type 1.b), N is even, $2 \mid N$ and $3 \not| N$ and we can write $N = 2^{n_{N,2}} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $n_{N,2} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{2,s}$. Then, from the cases 1.b), 3.a), 3.b) and 4.b) above, the number of possible combinations for the coeffcient q_1 is equal to $\Phi(N) = 2^{n_{N,2}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)$ and the total number of coefficients q_2 and q_3, respectively, is equal to $2^{n_{N,2}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$. Because this case requires from the equivalence conditions that $q_2 < N/2$ and $q_3 < N/2$, a number of $\frac{1}{2} \cdot 2^{n_{N,2}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} = 2^{n_{N,2}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$ possible coefficients q_2 and q_3, respectively, remains, from which one is zero. By removing the value $q_3 = 0$, the number of CPPs will be equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(2^{n_{N,2}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1 \right) = \\ &= 2^{2 \cdot n_{N,2}-3} \cdot \prod_{j=2}^{s} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1 \right) \end{aligned} \tag{12}$$

From (12), we see that the number of CPPs is equal to 0 if the interleaver length is 4 times a product of prime numbers greater than 3, of the form $3 \cdot k + 1, k \in \mathbb{N}$, each of them to power 1.

Case 13) The decomposition of N containes prime factors of the type 1.a) and 3.a) or 3. b) or 4.b).

In this case, $2 \mid N$ and $3 \nmid N$ and we can write $N = 2 \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{2,s}$. From the analysis for the cases 1.a) and 3.a), 3.b), 4.b), the number of possible combinations for the coefficient q_1 is equal to $1 \cdot \Phi(N/2) = \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)$ and the total number of coefficients q_2 and q_3, respectively, is equal to $1 \cdot \frac{N}{2 \cdot t_N} = \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, from which one value is 0. By removing the value $q_3 = 0$ the number of CPPs will be equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1 \right) = \\ &= \left(\prod_{j=2}^{s} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1 \right) \end{aligned} \tag{13}$$

From (13), we see that the number of CPPs is equal to 0 if the interleaver length is 2 times a product of prime numbers greater than 3, of the form $3 \cdot k + 1, k \in \mathbb{N}$, each of them to power 1.

Caz 14) The decomposition of N containes prime factors of the type 2.a) and 1.b) or 3.a) or 3.b) or 4.b).

When there is no factor of type 1.b), N is odd, $2 \nmid N$ and $3 \mid N$ and we can write $N = 3 \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{2,s}$. In determining the number of coefficients, we consider that for the two sets of coefficients valid for the factor of type 2.a), we have only a single value for q_2 and q_3. The number of possible combinations for the coefficient q_1 is equal to $2 \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)$, the number of coefficients q_2 is equal to $\prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$ and the number of coefficients q_3 is equal to $\prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, from which one is 0. By removing the value $q_3 = 0$, the number of CPPs will be equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(2 \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1 \right) = \\ &= \left(2 \cdot \prod_{j=2}^{s} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1 \right) \end{aligned} \tag{14}$$

From (14), we see that the number of CPPs is equal to 0 if the interleaver length is 3 times a product of prime numbers greater than 3, of the form $3 \cdot k + 1, k \in \mathbb{N}$, each of them to power 1.

When there is a factor of type 1.b), N is even, $6 \mid N$ and we can write $N = 2^{n_{N,2}} \cdot 3 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}}$, with $n_{N,2} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{3,s}$. In determining the number of coefficients, we consider that for the two sets of coefficients valid for the factor of type 2.a) we always have $q_{2,1} = q_{3,1} = 0$. From the two sets we have to keep only one for the coefficients q_2 and q_3. The number of possible combinations for the coefficient q_1 is equal to $2^{n_{N,2}-1} \cdot 2 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) = 2^{n_{N,2}} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)$, the number of coefficients q_2 and q_3 is equal to $2^{n_{N,2}-2} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1}$, from which one is 0. By removing the value $q_3 = 0$ the number of CPPs will be equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(2^{n_{N,2}} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)\right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} - 1\right) = \\ &= \left(2^{2 \cdot n_{N,2}-2} \cdot \prod_{j=3}^{s} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1)\right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} - 1\right) \end{aligned} \tag{15}$$

From (15), we see that the number of CPPs is equal to 0 if the interleaver length is 12 times a product of prime numbers greater than 3, of the form $3 \cdot k + 1, k \in \mathbb{N}$, each of them to power 1.

Case 15) The decomposition of N containes prime factors of the type 1.a) and 2.a) and 3.a) or 3.b) or 4.b).

In this case $6 \mid N$ and we can write $N = 2 \cdot 3 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}}$, with $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{3,s}$. The number of possible conmbinations for the coefficient q_1 results equal to $1 \cdot 2 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) = 2 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)$, the number of coefficients q_2 and q_3 is equal to $1 \cdot 1 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} = \prod_{j=3}^{s} p_j^{n_{N,p_j}-1}$, from which one is 0. After removing the value $q_3 = 0$ the number of CPPs will be equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(2 \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)\right) \cdot \left(\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\right) \cdot \left(\prod_{j=3}^{s} p_j^{n_{N,p_j}-1} - 1\right) = \\ &= \left(2 \cdot \prod_{j=3}^{s} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1)\right) \cdot \left(\prod_{j=3}^{s} p_j^{n_{N,p_j}-1} - 1\right) \end{aligned} \tag{16}$$

From (16), we see that the number of CPPs is equal to 0 if the interleaver length is 6 times a product of prime numbers greater than 3, of the form $3 \cdot k + 1, k \in \mathbb{N}$, each of them to power 1.

Case 16) The decomposition of N containes prime factors of the type 2.b) and 1.b) or 3.a) or 3.b) or 4.b).

When there is no factor of the type 1.b), N is odd, $2 \nmid N$ and $3 \mid N$ and we can write $N = 3^{n_{N,3}} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}}$, with $n_{N,3} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{2,s}$. It follows that the number of possible combinations for the coefficient q_1 is equal to $2 \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$, the number of coefficients q_2 is equal to $3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$ and the number of coefficients q_3 is equal to $2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, for $3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$ of the $2 \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$ values for the coefficients q_1 and it is equal to $2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, for the other $3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$ values for the coefficients q_1, from which one is 0. By removing the value $q_3 = 0$ the number of CPPs will be equal to:

$$C_{N,CPPs} = \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)\right) \cdot \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}\right) \cdot \left(2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1\right) +$$

$$+ \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)\right) \cdot \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}\right) \cdot \left(2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1\right) = \quad (17)$$

$$= \left(2 \cdot 3^{2 \cdot \left(n_{N,3}-1\right)} \cdot \prod_{j=2}^{s} p_j^{2 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) \cdot \left(2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1} - 1\right)$$

From (17), we see that in this case the number of CPPs is always greater than 0.

When there is a factor of the type 1.b), N is even, $6 \mid N$ and we can write $N = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}}$, with $n_{N,2} > 1$, $n_{N,3} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{3,s}$. It follows that the numbers of possible combinations for the coefficient q_1 is equal to $2^{n_{N,2}-1} \cdot 2 \cdot 3^{n_{N,3}-1} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$, the number of coefficients q_2 is equal to $2^{n_{N,2}-2} \cdot 3^{n_{N,3}-1} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1}$ and the number of coefficients q_3 is equal to $2^{n_{N,2}-2} \cdot 2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, for $2^{n_{N,2}-1} \cdot 3^{n_{N,3}-1} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$ of the $2^{n_{N,2}-1} \cdot 2 \cdot 3^{n_{N,3}-1} \cdot \prod_{j=3}^{s} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)$ values for the

coefficient q_1 and equal to $2^{n_{N,2}-2}\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, for the other $2^{n_{N,2}-1}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ values of the coefficient q_1, from which one is 0. By removing the value $q_3=0$ the number of CPPs will be equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(2^{n_{N,2}-1}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(2^{n_{N,2}-2}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\right)\cdot \\ &\cdot\left(2^{n_{N,2}-2}\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}-1\right)+\left(2^{n_{N,2}-1}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot \\ &\cdot\left(2^{n_{N,2}-2}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\right)\cdot\left(2^{n_{N,2}-2}\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}-1\right)= \\ &=\left(2^{2\cdot\left(n_{N,2}-1\right)}\cdot 3^{2\cdot\left(n_{N,3}-1\right)}\cdot\prod_{j=3}^{s} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)\cdot\left(2^{n_{N,2}-1}\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}-1\right) \end{aligned} \tag{18}$$

From (18), we see that in this case the number of CPPs is always greater than 0.

Case 17) The decomposition of N containes prime factors of the type 1.a) and 2.b) and 3.a) or 3.b) or 4.b).

In this case $6\,|\,N$ and we can write $N=2\cdot 3^{n_{N,3}}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}}$, $n_{N,3}>1$, $p_j>3$, $n_{N,p_j}\geq 1$ when $p_j=3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p_j}>1$ when $p_j=3\cdot k+2, k\in\mathbb{N}$, $j=\overline{3,s}$. From the analysis of the cases 1.a), 2.b) and 3.a), 3.b), 4.b), it follows that the number of possible combinations for the coefficient q_1 is equal to $1\cdot 2\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$, the number of coefficients q_2 is equal to $1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}$ and a number of coefficients q_3 is equal to $1\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, for $1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ of the $1\cdot 2\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ values for the coefficient q_1 and equal to $1\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=2}^{s} p_j^{n_{N,p_j}-1}$, for the other $1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$ values for the coefficient q_1, from which one is 0. By removing the value $q_3=0$ the number of CPPs results equal to:

$$\begin{aligned} C_{N,CPPs} &= \left(1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\right)\cdot \\ &\cdot\left(1\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}-1\right)+\left(1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot \end{aligned}$$

$$\cdot\left(1\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s}p_j^{n_{N,p_j}-1}\right)\cdot\left(1\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s}p_j^{n_{N,p_j}-1}-1\right)=$$

$$=\left(2\cdot 3^{2\cdot\left(n_{N,3}-1\right)}\cdot\prod_{j=3}^{s}p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)\cdot\left(2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s}p_j^{n_{N,p_j}-1}-1\right) \quad (19)$$

From (19), we see that in this case the number of CPPs is always greater than 0.

Case 18) The decomposition of N containes prime factors of the type 1.b) or 3.a) or 3.b) or 4.b) and 4.a).

In this case, as we have to address separately the factors of type 4.a), it is useful to denote the number of such factors by n_{4a}.

When there is no factor of the type 1.b), N is odd, $2\nmid N$ and $3\nmid N$ and we can write $N=\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}}\cdot\prod_{j=s-n_{4a}+1}^{s}p_j$, $p_j>3$, $n_{N,p_j}\geq 1$ when $p_j=3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p_j}>1$ when $p_j=3\cdot k+2, k\in\mathbb{N}$, $j=\overline{1,s-n_{4a}}$, and $p_j=3\cdot k+2, k\in\mathbb{N}^*$, $j=\overline{s-n_{4a}+1,s}$. We consider the analysis of the case 4.a), and denote by $I_{n_{4a}}=\{s-n_{4a}+1,s-n_{4a}+2,\ldots,s\}$ the set of indices corresponding to the n_{4a} prime factors of type 4.a) and by $I_{n_{4a,0}}\subseteq I_{n_{4a}}$, with $1\leq n_{4a,0}<n_{4a}$, the set of indices for which $q_{3,j}=0\left(\mathrm{mod}\,p_j\right)$, $j\in I_{n_{4a,0}}$. It follows that for a group of $n_{4a,0}$ prime factors of type 4.a) the number of possible combinations for the coefficient q_1 is equal to $\prod_{j\in I_{n_{4a,0}}}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)$, the number of coefficients q_2 is equal to $\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}}p_j\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}$ and the number of coefficients q_3 is equal to $\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}$. In total, for a group of $n_{4a,0}$ prime factors of the type 4.a), the number of CPPs will be equal to:

$$C_{N,CPPs,n_{4a,0}}=\left(\prod_{j\in I_{n_{4a,0}}}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot$$
$$\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}}p_j\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right) \quad (20)$$

For a group of n_{4a} prime factors of the type 4.a), we have to remove the case when $q_3=0$ and the number of CPPs will be:

$$C_{N,CPPs,n_{4a}}=\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j=1}^{s-n_{4a}}p_j^{n_{N,p_j}-1}-1\right) \quad (21)$$

When the condition $q_{3,j}=0\left(\mathrm{mod}\,p_j\right)$ is not met for any of the n_{4a} prime factors of the type 4.a), according to the condition 4.a) above, the number of CPPs will be:

$$C_{N,CPPs,0}=\left(\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=s-n_{4a}+1}^{s} p_j\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot$$
$$\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)=\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot\left(p_j-1\right)\right)\cdot\prod_{j=1}^{s-n_{4a}}\left(p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right) \quad (22)$$

The final number of CPPs results by summing the quantities from (20)-(22) for $n_{4a,0}=0,1,2,\ldots,n_{4a}$,

$$C_{N,CPPs}=\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot\left(p_j-1\right)\right)\cdot\prod_{j=1}^{s-n_{4a}}\left(p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+$$
$$+\sum_{n_{4a,0}=1}^{n_{4a}-1}\left[\left(\prod_{j\in I_{n_{4a,0}}}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\right.$$
$$\left.\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}} p_j\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\right]+$$
$$+\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right)=$$
$$=\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot\left(p_j-1\right)\right)\cdot\prod_{j=1}^{s-n_{4a}}\left(p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+$$
$$+\sum_{n_{4a,0}=1}^{n_{4a}-1}\left(\prod_{j\in I_{n_{4a}}}\left(p_j-1\right)\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}} p_j\cdot\prod_{j=1}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+ \quad (23)$$
$$+\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot\prod_{j=1}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right)$$

From (23), we see that in this case the number of CPPs is always greater than 0.

When there is a factor of the type 1.b), N is even, $2\,|\,N$ and $3\not|\,N$ and we can write $N=2^{n_{N,2}}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}}\cdot\prod_{j=s-n_{4a}+1}^{s} p_j$, with $n_{N,2}>1$, $p_j>3$, $n_{N,p_j}\geq 1$ when $p_j=3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p_j}>1$ when $p_j=3\cdot k+2, k\in\mathbb{N}$, $j=\overline{2,s-n_{4a}}$, and $p_j=3\cdot k+2, k\in\mathbb{N}^*$, $j=\overline{s-n_{4a}+1,s}$. We consider the case when N is odd and the additional case 1.b), and use the same notations as above. The number of CPPs will be equal to:

$$C_{N,CPPs}=\left(2^{n_{N,2}-1}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=s-n_{4a}+1}^{s} p_j\cdot 2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot$$
$$\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)+$$
$$+\sum_{n_{4a,0}=1}^{n_{4a}-1}\left[\left(\prod_{j\in I_{n_{4a,0}}}\left(p_j-1\right)\cdot 2^{n_{N,2}-1}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\right.$$

$$\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}} p_j\cdot 2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}(p_j-1)\cdot 2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\Bigg]+$$

$$+\left(\prod_{j=s-n_{4a}+1}^{s}(p_j-1)\cdot 2^{n_{N,2}-1}\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot(p_j-1)\right)\cdot$$

$$\cdot\left(2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right)=$$

$$=\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot(p_j-1)\right)\cdot 2^{3\cdot n_{N,2}-5}\cdot\prod_{j=2}^{s-n_{4a}}\left(p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot(p_j-1)\right)+$$

$$+\sum_{n_{4a,0}=1}^{n_{4a}-1}\left(\prod_{j\in I_{n_{4a},0}}(p_j-1)\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}} p_j\cdot 2^{3\cdot n_{N,2}-5}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot(p_j-1)\right)+ \tag{24}$$

$$+\left(\prod_{j=s-n_{4a}+1}^{s}(p_j-1)\cdot 2^{2\cdot n_{N,2}-3}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot(p_j-1)\right)\cdot\left(2^{n_{N,2}-2}\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right)$$

From (24), we see that in this case the number of CPPs is always greater than 0.

Case 19) The decomposition of N containes prime factors of the type 1.a) and 3.a) or 3.b) or 4.b) and 4.a).

In this case $2\,|\,N$ and $3\nmid N$ and we can write $N=2\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}}\cdot\prod_{j=s-n_{4a}+1}^{s} p_j$, with $p_j>3$, $n_{N,p_j}\geq 1$ when $p_j=3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p_j}>1$ when $p_j=3\cdot k+2, k\in\mathbb{N}$, $j=\overline{2,s-n_{4a}}$, and $p_j=3\cdot k+2, k\in\mathbb{N}^*$, $j=\overline{s-n_{4a}+1,s}$. The number of CPPs results by considering the previous case and the case 1.a), with the same notations used above:

$$C_{N,CPPs}=\left(1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot(p_j-1)\right)\cdot\left(\prod_{j=s-n_{4a}+1}^{s} p_j\cdot 1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot$$

$$\cdot\left(\prod_{j=s-n_{4a}+1}^{s}(p_j-1)\cdot 1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)+\sum_{n_{4a,0}=1}^{n_{4a}-1}\Bigg[\left(\prod_{j\in I_{n_{4a},0}}(p_j-1)\cdot 1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot(p_j-1)\right)\cdot$$

$$\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}} p_j\cdot 1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}(p_j-1)\cdot 1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\Bigg]+$$

$$+\left(\prod_{j=s-n_{4a}+1}^{s}(p_j-1)\cdot 1\cdot\prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot(p_j-1)\right)\cdot\left(1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(1\cdot\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right)=$$

$$=\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot(p_j-1)\right)\cdot\prod_{j=2}^{s-n_{4a}}\left(p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot(p_j-1)\right)+$$

$$+\sum_{n_{4a,0}=1}^{n_{4a}-1}\left(\prod_{j\in I_{n_{4a}}}(p_j-1)\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}} p_j\cdot\prod_{j=2}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot(p_j-1)\right)+$$

$$+\left(\prod_{j=s-n_{4a}+1}^{s}(p_j-1)\cdot\prod_{j=2}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot(p_j-1)\right)\cdot\left(\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right) \tag{25}$$

From (25) we see that in this case the number of CPPs is always greater than 0.

Case 20) The decomposition of N contains prime factors of the type 2.a) and 1.b) or 3.a) or 3.b) or 4.b) and 4.a).

When there is no factor of the type 1.b), N is odd, $2 \nmid N$ and $3 \mid N$ and we can write $N = 3 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}} \cdot \prod_{j=s-n_{4a}+1}^{s} p_j$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{2, s - n_{4a}}$, and $p_j = 3 \cdot k + 2, k \in \mathbb{N}^*$, $j = \overline{s - n_{4a} + 1, s}$. We consider the analysis from the case 18 and the conditions from the case 2.a). For a group of $n_{4a,0}$ prime factors of the type 4.a), the number of CPPs is equal to:

$$C_{N,CPPs,n_{4a,0}} = \left(\prod_{j \in I_{n_{4a,0}}} (p_j - 1) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} (p_j - 1) \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \tag{26}$$

For group of n_{4a} prime factors of the type 4.a), we have to remove the case when $q_3 = 0$ and the number of CPPs will be equal to:

$$C_{N,CPPs,n_{4a}} = \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1 \right) \tag{27}$$

When the condition $q_{3,j} = 0 \pmod{p_j}$ is not met for any of the n_{4a} prime factors of the type 4.a), the number of CPPs will be:

$$C_{N,CPPs,0} = \left(2 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} p_j \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \tag{28}$$

The number of CPPs results by summing the quantities in (27)-(28) for $n_{4a,0} = 0, 1, 2, \ldots, n_{4a}$:

$$\begin{aligned} C_{N,CPPs} = & \prod_{j=s-n_{4a}+1}^{s} \left(p_j \cdot (p_j - 1) \right) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} \left(p_j^{3 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \right) + \\ & + \sum_{n_{4a,0}=1}^{n_{4a}-1} \left[\left(\prod_{j \in I_{n_{4a,0}}} (p_j - 1) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} (p_j - 1) \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \right] + \\ & + \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1 \right) = \end{aligned}$$

$$= \prod_{j=s-n_{4a}+1}^{s} \left(p_j \cdot \left(p_j - 1\right)\right) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} \left(p_j^{3 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) +$$

$$+ \sum_{n_{4a,0}=1}^{n_{4a}-1} \left(\prod_{j \in I_{n_{4a}}} \left(p_j - 1\right) \cdot 2 \cdot \prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot \prod_{j=2}^{s-n_{4a}} p_j^{3 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) + \tag{29}$$

$$+ \left(\prod_{j=s-n_{4a}+1}^{s} \left(p_j - 1\right) \cdot 2 \cdot \prod_{j=2}^{s-n_{4a}} p_j^{2 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) \cdot \left(\prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1\right)$$

From (29) we see that in this case the number of CPPs is always greater than 0.

When there is a factor of the type 1.b), N is even, $6 \mid N$ and we can write $N = 2^{n_{N,2}} \cdot 3 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}} \cdot \prod_{j=s-n_{4a}+1}^{s} p_j$, with $n_{N,2} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{3, s - n_{4a}}$, and $p_j = 3 \cdot k + 2, k \in \mathbb{N}^*$, $j = \overline{s - n_{4a} + 1, s}$. We consider the subcase when N is odd and the additional case 1.b). The number of CPPs results equal to:

$$C_{N,CPPs} = \left(2^{n_{N,2}-1} \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)\right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} p_j \cdot 2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot$$

$$\cdot \left(\prod_{j=s-n_{4a}+1}^{s} \left(p_j - 1\right) \cdot 2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) +$$

$$+ \sum_{n_{4a,0}=1}^{n_{4a}-1} \left[\left(\prod_{j \in I_{n_{4a,0}}} \left(p_j - 1\right) \cdot 2^{n_{N,2}-1} \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)\right) \cdot \right.$$

$$\left. \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot 2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} \left(p_j - 1\right) \cdot 2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\right] +$$

$$+ \left(\prod_{j=s-n_{4a}+1}^{s} \left(p_j - 1\right) \cdot 2^{n_{N,2}-1} \cdot 2 \cdot \prod_{j=1}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot \left(p_j - 1\right)\right) \cdot$$

$$\cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1\right) =$$

$$= \prod_{j=s-n_{4a}+1}^{s} \left(p_j \cdot \left(p_j - 1\right)\right) \cdot 2^{3 \cdot n_{N,2}-4} \cdot \prod_{j=3}^{s-n_{4a}} \left(p_j^{3 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) +$$

$$+ \sum_{n_{4a,0}=1}^{n_{4a}-1} \left(\prod_{j \in I_{n_{4a}}} \left(p_j - 1\right) \cdot \prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot 2^{3 \cdot n_{N,2}-4} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{3 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) +$$

$$+ \left(\prod_{j=s-n_{4a}+1}^{s} \left(p_j - 1\right) \cdot 2^{2 \cdot \left(n_{N,2}-1\right)} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{2 \cdot \left(n_{N,p_j}-1\right)} \cdot \left(p_j - 1\right)\right) \cdot \left(2^{n_{N,2}-2} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1\right) \tag{30}$$

From (30) we see that in this case the number of CPPs is always greater than 0.

Case 21) The decomposition of N contains prime factors of the type 1.a) and 2.a) and 3.a) or 3.b) or 4.b) and 4.a).

In this case $6 \mid N$ and we can write $N = 2 \cdot 3 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}} \cdot \prod_{j=s-n_{4a}+1}^{s} p_j$, with $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{3, s - n_{4a}}$, and $p_j = 3 \cdot k + 2, k \in \mathbb{N}^*$, $j = \overline{s - n_{4a} + 1, s}$. In determining the number of CPPs, we consider the case 20) for *N* odd and that for the case 1.a), there is a single set of valid coefficients. The number of CPPs will be:

$$C_{N,CPPs} = \left(2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)\right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} p_j \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) +$$
$$+ \sum_{n_{4a,0}=1}^{n_{4a}-1} \left[\left(\prod_{j \in I_{n_{4a,0}}} (p_j - 1) \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)\right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot \right.$$
$$\left. \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} (p_j - 1) \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\right] +$$
$$+ \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)\right) \cdot \left(\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot \left(\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1\right)$$
$$= \prod_{j=s-n_{4a}+1}^{s} \left(p_j \cdot (p_j - 1)\right) \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} \left(p_j^{3 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1)\right) +$$
$$+ \sum_{n_{4a,0}=1}^{n_{4a}-1} \left(\prod_{j \in I_{n_{4a}}} (p_j - 1) \cdot \prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{3 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1)\right) + \quad (31)$$
$$+ \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 2 \cdot \prod_{j=3}^{s-n_{4a}} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1)\right) \cdot \left(\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1\right)$$

From (31) we see that in this case the number of CPPs is always greater than 0.

Case 22) The decomposition of N contains prime factors of the type 2.b) and 1.b) or 3.a) or 3.b) or 4.b) and 4.a).

When the is no factor of the type 1.b), N is odd, $2 \nmid N$ and we can write $N = 3^{n_{N,3}} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}} \cdot \prod_{j=s-n_{4a}+1}^{s} p_j$, $n_{N,3} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when $p_j = 3 \cdot k + 1, k \in \mathbb{N}$ and $n_{N,p_j} > 1$ when $p_j = 3 \cdot k + 2, k \in \mathbb{N}$, $j = \overline{2, s - n_{4a}}$, and $p_j = 3 \cdot k + 2, k \in \mathbb{N}^*$, $j = \overline{s - n_{4a} + 1, s}$. We consider the analysis from the case 18 and the conditions from the case 2.b). For a group of $n_{4a,0}$ prime factors of the type 4.a), the number of CPPs is equal to:

$$C_{N,CPPs,n_{4a,0}} = 2 \cdot \left(\prod_{j \in I_{n_{4a,0}}} (p_j - 1) \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1)\right) \cdot$$
$$\cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} (p_j - 1) \cdot 2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right) \quad (32)$$

For a group of n_{4a} prime factors of the type 4.a), we have to remove the case when $q_3 = 0$ and the number of CPPs will be equal to:

$$C_{N,CPPs,n_{4a}} = 2 \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \\ \cdot \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1 \right) \tag{33}$$

When the condition $q_{3,j} = 0 \pmod{p_j}$ is not met for any of the n_{4a} prime factors of the type 4.a), the number of CPPs will be:

$$C_{N,CPPs,0} = 2 \cdot \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} p_j \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \\ \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \tag{34}$$

The number of CPPs results by summing the quantities in (32)-(34) for $n_{4a,0} = 0,1,2,\ldots,n_{4a}$:

$$C_{N,CPPs} = 2 \cdot \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(\prod_{j=s-n_{4a}+1}^{s} p_j \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \\ \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) + \\ + 2 \cdot \sum_{n_{4a,0}=1}^{n_{4a}-1} \left[\left(\prod_{j \in I_{n_{4a,0}}} (p_j - 1) \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \right. \\ \left. \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(\prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} (p_j - 1) \cdot 2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \right] + \\ + 2 \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \cdot (p_j - 1) \right) \cdot \left(3^{n_{N,3}-1} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} \right) \cdot \left(2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1 \right) = \\ = 4 \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j \cdot (p_j - 1)) \cdot 3^{3 \cdot n_{N,3}-4} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{3 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \right) + \\ + 4 \cdot \sum_{n_{4a,0}=1}^{n_{4a}-1} \left(\prod_{j \in I_{n_{4a}}} (p_j - 1) \cdot 3^{3 \cdot n_{N,3}-4} \cdot \prod_{j \in I_{n_{4a}} - I_{n_{4a,0}}} p_j \cdot \prod_{j=2}^{s-n_{4a}} p_j^{3 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \right) + \\ + 2 \cdot \left(\prod_{j=s-n_{4a}+1}^{s} (p_j - 1) \cdot 3^{2 \cdot (n_{N,3}-1)} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{2 \cdot (n_{N,p_j}-1)} \cdot (p_j - 1) \right) \cdot \left(2 \cdot 3^{n_{N,3}-2} \cdot \prod_{j=2}^{s-n_{4a}} p_j^{n_{N,p_j}-1} - 1 \right) \tag{35}$$

From (35) we see that 0 in this case the number of CPPs is always greater than.

When there is a factor of the type 1.b), N is even, $6 \mid N$ and we can write $N = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot \prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}} \cdot \prod_{j=s-n_{4a}+1}^{s} p_j$, with $n_{N,2} > 1$, $n_{N,3} > 1$, $p_j > 3$, $n_{N,p_j} \geq 1$ when

$p_j = 3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p_j}>1$ when $p_j = 3\cdot k+2, k\in\mathbb{N}$, $j=\overline{3, s-n_{4a}}$, and $p_j = 3\cdot k+2, k\in\mathbb{N}^*$, $j=\overline{s-n_{4a}+1, s}$.

We consider the subcase when N is odd and the additional case 1.b). The number of CPPs results equal to:

$$C_{N,CPPs} = \left(2\cdot 2^{n_{N,2}-1}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=s-n_{4a}+1}^{s} p_j\cdot 2^{n_{N,2}-2}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot$$
$$\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 2^{n_{N,2}-2}\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)+$$
$$+2\cdot\sum_{n_{4a,0}=1}^{n_{4a}-1}\left[\left(\prod_{j\in I_{n_{4a,0}}}\left(p_j-1\right)\cdot 2^{n_{N,2}-1}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\right.$$
$$\left.\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}} p_j\cdot 2^{n_{N,2}-2}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}}\left(p_j-1\right)\cdot 2^{n_{N,2}-2}\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\right]+$$
$$+2\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 2^{n_{N,2}-1}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(2^{n_{N,2}-2}\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot$$
$$\cdot\left(2^{n_{N,2}-2}\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right)=$$
$$=\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot\left(p_j-1\right)\right)\cdot 2^{3\cdot\left(n_{N,2}-1\right)}\cdot 3^{3\cdot n_{N,3}-4}\cdot\prod_{j=3}^{s-n_{4a}}\left(p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+$$
$$=\sum_{n_{4a,0}=1}^{n_{4a}-1}\left(\prod_{j\in I_{n_{4a}}}\left(p_j-1\right)\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a,0}}} p_j\cdot 2^{3\cdot\left(n_{N,2}-1\right)}\cdot 3^{3\cdot n_{N,3}-4}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+$$
$$+\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 2^{2\cdot\left(n_{N,2}-1\right)}\cdot 3^{2\cdot\left(n_{N,3}-1\right)}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)\cdot$$
$$\cdot\left(2^{n_{N,2}-1}\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}-1\right) \qquad (36)$$

From (36) we see that in this case the number of CPPs is always greater than 0.

Case 23) The decomposition of N contains prime factors of the type 1.a) and 2.b) and 3.a) or 3.b) or 4.b) and 4.a).

In this case N is even, $6\,|\,N$ and we can write $N = 2\cdot 3^{n_{N,3}}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}}\cdot\prod_{j=s-n_{4a}+1}^{s} p_j$, with $n_{N,3}>1$, $p_j>3$, $n_{N,p_j}\geq 1$ when $p_j = 3\cdot k+1, k\in\mathbb{N}$ and $n_{N,p_j}>1$ when $p_j = 3\cdot k+2, k\in\mathbb{N}$, $j=\overline{3, s-n_{4a}}$, and $p_j = 3\cdot k+2, k\in\mathbb{N}^*$, $j=\overline{s-n_{4a}+1, s}$. In determining the number of CPPs we consider the case 22) for odd N and that for the case 1.a), there is a single set of valid coefficients. The number of CPPs will be:

$$C_{N,CPPs} = 2\cdot\left(3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\left(\prod_{j=s-n_{4a}+1}^{s} p_j\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}} p_j^{n_{N,p_j}-1}\right)\cdot$$

$$\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right)+$$

$$+2\cdot\sum_{n_{4a,0}=1}^{n_{4a}-1}\left[\left(\prod_{j\in I_{n_{4a},0}}\left(p_j-1\right)\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot\right.$$

$$\left.\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}p_j\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right)\cdot\left(\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}\left(p_j-1\right)\cdot 2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right)\right]+$$

$$+2\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\cdot\left(p_j-1\right)\right)\cdot$$

$$\cdot\left(3^{n_{N,3}-1}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}\right)\cdot\left(2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}-1\right)=$$

$$=4\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j\cdot\left(p_j-1\right)\right)\cdot 3^{3\cdot n_{N,3}-4}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+$$

$$+4\cdot\sum_{n_{4a,0}=1}^{n_{4a}-1}\left(\prod_{j\in I_{n_{4a}}}\left(p_j-1\right)\cdot 3^{3\cdot n_{N,3}-4}\cdot\prod_{j\in I_{n_{4a}}-I_{n_{4a},0}}p_j\cdot\prod_{j=3}^{s-n_{4a}}p_j^{3\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)+ \tag{37}$$

$$+2\cdot\left(\prod_{j=s-n_{4a}+1}^{s}\left(p_j-1\right)\cdot 3^{2\cdot\left(n_{N,3}-1\right)}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{2\cdot\left(n_{N,p_j}-1\right)}\cdot\left(p_j-1\right)\right)\cdot\left(2\cdot 3^{n_{N,3}-2}\cdot\prod_{j=3}^{s-n_{4a}}p_j^{n_{N,p_j}-1}-1\right)$$

From (37) we see that in this case the number of CPPs is always greater than 0.

We bring together the conclusions from all previous cases and conclude that the number of CPPs is equal to 0 if the interleaver length is of the form:

$$N=2^{n_{N,2}}\cdot 3^{n_{N,3}}\cdot\prod_{j=3}^{s}p_j,\ \text{with}\ n_{N,2}=\overline{0,2},\ n_{N,3}=\overline{0,1},\ p_j>3,\ \text{with}\ p_j=3\cdot k+1,k\in\mathbb{N},$$

$$j=\overline{3,s} \tag{38}$$

Such lengths have to be avoided in designing CPP based interleavers.

By comparing equations (10) and (38), it can be concluded that for any interleaver length for which the number of CPPs is 0, the number of QPPs is also 0. But there are lengths for which the number of QPPs is 0, but the number of CPPs is greater than 0. Such lengths are generated by multiplying by one, two or four products of prime numbers greater than 2, each to the power 1. In each product, there should be at least a prime number of the form $3\cdot k+2,k\in\mathbb{N}^*$, so that:

$$N=2^{n_{N,2}}\cdot 3^{n_{N,3}}\cdot\prod_{j=3}^{s-n_{4a}}p_j\cdot\prod_{j=s-n_{4a}+1}^{s}p_j,\ \text{with}\ n_{N,2}=\overline{0,2},\ n_{N,3}=\overline{0,1},\ p_j>3,\ \text{with}$$

$$p_j=3\cdot k+1,k\in\mathbb{N},\ \text{if}\ j=\overline{3,s-n_{4a}}\ \text{and}\ p_j=3\cdot k+2,k\in\mathbb{N}^*,\ \text{if}\ j=\overline{s-n_{4a}+1,s},\ s\geq n_{4a}\geq 1 \tag{39}$$

For the lengths of the type in (39) the CPP based interleavers can be used instead of QPP based ones. The number of lengths for which the number of QPPs is 0 is significantly greater than the number of lengths for which the number of CPPs is

greater than 0. For example, from 2 to 10,000 there are 7098 lengths for which the number of QPPs is 0 and only 2264 lengths for which the number of CPPs is 0.

6. Conclusions

This paper presents a method for determining the number of true different modulo N PPs using the Chinese remainder theorem, when the conditions for the coeficients of PPs are known, such as for QPPs or CPPs. The method was applied to determine the number of true different QPPs or CPPs. This number is useful when QPPs or CPPs are used for turbo code interleavers and we choose a certain length of interleaver N. If the number of true different QPPs or CPPs is large, we could have a large number of good interleavers with the desired length. If this number is small, the possibility to find good interleavers for turbo codes is low and if this number is 0, obviously, there is no interleaver with that length.

Referrences

[1] Takeshita, O.Y. (2007). Permutation polynomial interleavers: an algebraic-geometric perspective. *IEEE Transactions Information Theory* **53**(6), 2116-2132.

[2] Sun, J., & Takeshita, O.Y. (2005). Interleavers for turbo codes using permutation polynomial over integer rings. *IEEE Transactions Information Theory* **51**(1), 101-119.

[3] Takeshita, O.Y. (2006). On maximum contention-free interleavers and permutation polynomials over integer rings. *IEEE Transactions Information Theory* **52**(3), 1249-1253.

[4] Ryu, J., & Takeshita, O.Y. (2006). On quadratic *inverse* for quadratic permutation polynomials over integer rings. *IEEE Transactions Information Theory* **52**(3), 1254-1260.

[5] Takeshita, O.Y. (2006). A new metric for permutation polynomial interleavers. Proc. of *IEEE International Symposium of Information Theory* (ISIT), Seattle, USA, pp. 1983-1987.

[6] Rosnes, E., & Takeshita, O.Y. (2006). Optimum distance quadratic permutation polynomial-based interleavers for turbo codes. Proc. of *IEEE International Symposium of Information Theory* (ISIT), Seattle, USA, pp. 1988-1992.

[7] Tărniceriu, D., Trifina, L., & Munteanu, V. (2009). About minimum distance for QPP interleavers. *Annals of Telecommunications* **64**(11-12), 745-751.

[8] Zhao, H., Fan, P., & Tarokh, V. (2010). On the equivalence of interleavers for turbo codes using quadratic permutation polynomials over integer rings. *IEEE Communications Letters* **14**(3), 236-238.

[9] Trifina, L., Tărniceriu, D., & Munteanu, V. (2011). Improved QPP interleavers for LTE Standard. Proc. of *IEEE International Symposium of Signals, Circuits and Systems* (ISSCS), Iasi, Romania, pp. 403-406.

[10] Ryu, J. (2012). Efficient address generation for permutation polynomial based interleavers over integer rings. *IEICE Transactions on Fundamentals* **E95-A**(1), 421-424.

[11] Lahtonen, J., Ryu, J., & Suvitie, E. (2012). On the degree of the inverse of quadratic permutation polynomial interleavers. *IEEE Transactions Information Theory* **58**(6), 3925-3932.

[12] Rosnes, E. (2012). On the minimum distance of turbo codes with quadratic permutation polynomial interleavers. *IEEE Transactions Information Theory* **58**(7), 4781-4795.

[13] Trifina, L., Tărniceriu, D., & Munteanu, V. (2012). On dispersion and nonlinearity degree of QPP Interleavers. *Applied Mathematics & Information Sciences* **6**(3), 397-400.
[14] Ryu, J. (2012). Permutation polynomial of higher degrees for turbo code interleavers. *IEICE Transactions on Communications* **E95-B**(12), 3760-3762.
[15] Trifina, L., & Tărniceriu, D. (2014). Improved method for searching interleavers from a certain set using Garello's method with applications for the LTE Standard. *Annals of Telecommunications* **69**(5-6), 251-272.
[16] 3GPP TS 36.212 V8.3.0, 3rd Generation Partnership Project, Multiplexing and channel coding (Release 8), 2005. http://www.etsi.org/deliver/etsi_ts/136200_136299/136212/08.03.00_60/ts_136212v080300p.pdf. Accessed 05 June 2015.
[17] Trifina, L., & Tărniceriu, D. (2013). Analysis of cubic permutation polynomials for turbo codes. *Wireless Personal Communications* **69**(1), 1-22.
[18] Chen, Y.-L., Ryu, J., & Takeshita, O.Y. (2006). A simple coefficient test for cubic permutation polynomials over integer rings. *IEEE Communications Letters* **10**(7), 549-551.
[19] Zhao, H., & Fan, P. (2007). A Note on A simple coefficient test for cubic permutation polynomials over integer rings. *IEEE Communications Letters* **11**(12), 991.
[20] Weng, G., & Dong, C. (2008). A note on permutation polynomial over $\mathbb{Z}_n$. *IEEE Trans. Inf. Theory* **54**(9), 4388-4390.
[21] Hardy, G.H., & Wright, E.M. (1975). *An Introduction to the Theory of Numbers*. fourth edition, Oxford University Press.