mathematics

Article

When Is the Number of True Different Permutation Polynomials Equal to 0?

Lucian Trifina * and **Daniela Tarniceriu**

Department of Telecommunications and Information Technologies, "Gheorghe Asachi" Technical University, Iasi 700506, Romania; tarniced@etti.tuiasi.ro
* Correspondence: luciant@etti.tuiasi.ro

Received: 31 July 2019; Accepted: 23 October 2019; Published: 25 October 2019

Abstract: In this paper, we have obtained the prime factorization form of positive integers N for which the number of true different fourth- and fifth-degree permutation polynomials (PPs) modulo N is equal to zero. We have also obtained the prime factorization form of N so that the number of any degree PPs nonreducible at lower degree PPs, fulfilling Zhao and Fan (ZF) sufficient conditions, is equal to zero. Some conclusions are drawn comparing all fourth- and fifth-degree permutation polynomials with those fulfilling ZF sufficient conditions.

Keywords: permutation polynomial; number of PPs equal to 0; Zhao and Fan sufficient conditions

PACS: 11A51; 11T06; 11T71 ; 11C08

1. Introduction

Permutation polynomials (PPs) are used in cryptography, sequence generation, or as interleavers in turbo codes [1–3]. Recently, some results were obtained regarding the number of true different (*td*) PPs modulo a positive integer N, whose definition is provided in Section 2.

In [4], the number of *td* quadratic permutation polynomials (QPPs) was obtained. Then, in [5], the method from [4] was applied to determine the number of *td* cubic permutation polynomials (CPPs) for N equal to a multiple of 8 as interleaver lengths from the long-term evolution (LTE) standard [6]. The method proposed in [7] is based on the Chinese remainder theorem and on two other important theorems regarding PPs, and it aims to get the number of *td* PPs. By using it, the number of *td* QPPs and CPPs for every N were obtained. In [8,9], the method from [7] was used to determine the number of *td* CPPs, fourth-degree PPs (4-PPs), and fifth-degree PPs (5-PPs) under Zhao and Fan (ZF) sufficient conditions given in [10]. In [11], an algorithm to determine the number of *td* PPs of degrees up to five, based on the Weng and Dong (WD) algorithm from [12], was given.

In this paper, we obtain some new results as follows. We determine the form of prime factorization of N so that the number of *td* 4-PPs and 5-PPs is equal to 0, and the form of prime factorization of N so that the number of any degree PPs nonreducible at lower degree PPs, fulfilling ZF sufficient conditions, is equal to 0. Thus, these values of N do not have to be used as 4-PP or 5-PP interleaver lengths because some smaller degree PPs are equivalent to 4-PP or 5-PP, providing the same permutations. A similar conclusion holds when we want to find PP interleavers under ZF sufficient conditions.

The paper is structured as follows. In Section 2, we recall the algorithm from [11], which is based on the WD algorithm [12]. In Section 3, we obtain a necessary condition so that the number of *td* PPs of a certain degree is equal to 0 (Lemma 1). Using the result from Lemma 1 in Sections 3.1–3.4, we obtain the form of N's prime factorization so that the number of *td* QPPs, CPPs, 4-PPs, and 5-PPs is equal to 0, respectively. In Section 4, we obtain the number of null polynomials and the quantities required in the algorithm from [11] to determine the number of any degree *td* PPs fulfilling ZF sufficient conditions.

Then, in Theorem 1, we obtain the prime factorization of N so that the number of any degree *td* PPs fulfilling ZF sufficient conditions is equal to 0. Section 5 concludes the paper.

2. Determining the Number of *td* PPs of Degree Up to Five by Using the WD Algorithm

Definition 1. *The polynomial of degree d, modulo N,*

$$\pi(x) = q_0 + q_1 x + q_2 x^2 + \cdots + q_d x^d \pmod{N}, \tag{1}$$

where N is a positive integer, is a PP if the coefficients q_k, $k = 1, \ldots, d$, are chosen so that the set $\{\pi(0), \pi(1), \ldots, \pi(N-1)\}$, modulo N, is a permutation of the set $\{0, 1, \ldots, N-1\}$ of integers modulo N.

Definition 2. *A PP of degree d (d-PP) is named true if the permutation generated by it can not be generated by a PP of degree smaller than d.*

Definition 3. *Two PPs are referred to as different if they generate two different permutations of the set $\{0, 1, \ldots, N-1\}$.*

Definition 4. *Two d-PPs are referred to as true different if they are both true and different.*

Below, we give the algorithm given in [11] for determining the number of *td* PPs of degree up to five based on the WD algorithm.

(1) Factor the positive integer N as

$$N = \prod_{k=1}^{s_1} p_{1,k} \cdot \prod_{k=s_1+1}^{s_1+s_2} p_{2,k}^{n_{N,p_{2,k}}}, \tag{2}$$

where $n_{N,p_{2,k}} > 1$, $\forall k = s_1+1, \ldots, s_1+s_2$, $s_1 \geq 0$ is the number of prime numbers at power of one in the factorization of N, $s_2 \geq 0$ is the number of prime numbers at power greater than one in the factorization of N, and $s_1 + s_2 \geq 1$.

(2) Compute the number of all d-PPs, for $1 \leq d \leq 5$, with the formula

$$C_{N,d-PPs,\text{all}} = \prod_{k=1}^{s_1} C_{p_{1,k},d-PPs} \cdot \prod_{k=s_1+1}^{s_1+s_2} C_{p_{2,k},d-PPs} \cdot (p_{2,k})^{d\cdot(n_{N,p_{2,k}}-1)}, \tag{3}$$

where $C_{p_{1,k},d-PPs}$ and $C_{p_{2,k},d-PPs}$ are given in Tables 1–3, in columns with $n_{N,p} = 1$ and $n_{N,p} > 1$, respectively, for every prime type at power equal or greater than one and for any degree from one to five. In the first product from (3), quantities $C_{p_{1,k},d-PPs}$ have the values given in Tables 1–3 in columns with $n_{N,p} = 1$. In the second product from (3), quantities $C_{p_{2,k},d-PPs}$ have the values given in Tables 1–3 in columns with $n_{N,p} > 1$.

(3) Compute the number of different d-PPs, for $2 \leq d \leq 5$, with the formula

$$C_{N,d-PPs,\text{diff}} = \frac{C_{N,d-PPs,\text{all}}}{\prod_{k=2}^{d} \gcd(k!, N)}. \tag{4}$$

(4) Compute the number of *td* d-PPs, for $2 \leq d \leq 5$, with the recursive formula

$$C_{N,d-PPs,td} = C_{N,d-PPs,\text{diff}} - \sum_{k=1}^{d-1} C_{N,k-PPs,td}, \tag{5}$$

where $C_{N,1-PPs,td} = C_{N,1-PPs,\text{all}}$.

Table 1. The number of all linear permutation polynomials (LPPs) and quadratic permutation polynomials (QPPs) over $\mathbb{Z}_p$ permuting $\mathbb{Z}_{p^{n_{N,p}}}$, with $n_{N,p} \geq 1$.

p	$n_{N,p} = 1$		$n_{N,p} > 1$	
	$C_{p,LPPs}$	$C_{p,QPPs}$	$C_{p,LPPs}$	$C_{p,QPPs}$
2	1	2	1	1
$p > 2$	$p-1$	$p-1$	$p-1$	$p-1$

Table 2. The number of all cubic permutation polynomials (CPPs) and fourth-degree permutation polynomials (4-PPs) over $\mathbb{Z}_p$ permuting $\mathbb{Z}_{p^{n_{N,p}}}$, with $n_{N,p} \geq 1$.

p	$n_{N,p} = 1$		$n_{N,p} > 1$	
	$C_{p,CPPs}$	$C_{p,4-PPs}$	$C_{p,CPPs}$	$C_{p,4-PPs}$
2	4	8	1	2
3	6	18	4	4
5	24	24	4	4
7	6	90	6	6
1 (mod 3), $p > 7$	$p-1$	$p-1$	$p-1$	$p-1$
2 (mod 3), $p > 5$	p^2-1	p^2-1	$p-1$	$p-1$

Table 3. The number of all fifth-degree permutation polynomials (5-PPs) over $\mathbb{Z}_p$ permuting $\mathbb{Z}_{p^{n_{N,p}}}$, with $n_{N,p} \geq 1$.

p	$n_{N,p} = 1$	$n_{N,p} > 1$
	$C_{p,5-PPs}$	$C_{p,5-PPs}$
2	16	4
3	54	16
5	120	56
7	720	258
13	2976	1884
1 (mod 15)	$p-1$	$p-1$
11 (mod 15)	p^2-1	$p-1$
7 (mod 15) or 13 (mod 15), $p > 13$	p^3-p^2+p-1	p^3-2p^2+2p-1
2 (mod 15) or 8 (mod 15), $p > 2$	p^3-1	p^3-2p^2+2p-1
4 (mod 15)	p^2-1	$p-1$
14 (mod 15)	$(p-1)(2p+1)$	$p-1$

3. Determining Positive Integers N so that the Number of *td* PPs of Degree Up to Five Is Equal to 0

Below, we first obtain a formula equivalent to (5), which is more appropriate for the aim of this paper. We use (4) in (5) when $d = 2$, and we obtain

$$C_{N,QPPs,td} = \frac{C_{N,2-PPs,\text{all}}}{\gcd(2,N)} - C_{N,1-PPs,\text{all}}. \tag{6}$$

We use (4) and (6) in (5) when $d = 3$, and we obtain

$$C_{N,CPPs,td} = \frac{C_{N,3-PPs,\mathrm{all}}}{\gcd(2,N)\cdot\gcd(6,N)} - \frac{C_{N,2-PPs,\mathrm{all}}}{\gcd(2,N)}. \tag{7}$$

Using (4) and (7) in (5) when $d = 4$, we obtain

$$C_{N,4-PPs,td} = \frac{C_{N,4-PPs,\mathrm{all}}}{\gcd(2,N)\cdot\gcd(6,N)\cdot\gcd(24,N)} - \frac{C_{N,3-PPs,\mathrm{all}}}{\gcd(2,N)\cdot\gcd(6,N)}, \tag{8}$$

and using (4) and (8) in (5) when $d = 5$, we obtain

$$C_{N,5-PPs,td} = \frac{C_{N,5-PPs,\mathrm{all}}}{\gcd(2,N)\cdot\gcd(6,N)\cdot\gcd(24,N)\cdot\gcd(120,N)} - \\ - \frac{C_{N,4-PPs,\mathrm{all}}}{\gcd(2,N)\gcd(6,N)\cdot\gcd(24,N)}. \tag{9}$$

We note that the formula

$$C_{N,d-PPs,td} = \frac{C_{N,d-PPs,\mathrm{all}}}{\prod_{k=2}^{d}\gcd(k!,N)} - \frac{C_{N,(d-1)-PPs,\mathrm{all}}}{\prod_{k=2}^{d-1}\gcd(k!,N)} \tag{10}$$

is valid for each degree $d \geq 2$, but the quantities $C_{p_{1,k},d-PPs}$ and $C_{p_{2,k},d-PPs}$ in (3) are not known, as in Tables 1–3, for each degree d.

The values of N such that the number of *td* PPs of degrees up to five is equal to 0 can be derived by using Equations (3), (6)–(9), and Tables 1–3.

In the following, a lemma that states a necessary condition to obtain $C_{N,d-PPs,td} = 0$, required to obtain the sought results, is given.

Lemma 1. *The number of td d-PPs is equal to 0 only if* $n_{N,p_k} = 1$ *and only if* $C_{p_k,d-PPs} = C_{p_k,(d-1)-PPs}$*, or at most* $\frac{C_{p_k,d-PPs}}{C_{p_k,(d-1)-PPs}} \mid \gcd(d!,N)$ *for each* $p_k \mid N$ *so that* $p_k \nmid \gcd(d!,N)$.

Proof. Condition $C_{N,d-PPs,td} = 0$ in (10) is equivalent to

$$\frac{C_{N,d-PPs,\mathrm{all}}}{C_{N,(d-1)-PPs,\mathrm{all}}} = \gcd(d!,N), \tag{11}$$

or taking into account (3),

$$\prod_{k=1}^{s_1}\frac{C_{p_{1,k},d-PPs}}{C_{p_{1,k},(d-1)-PPs}}\cdot\prod_{k=s_1+1}^{s_1+s_2}\frac{C_{p_{2,k},d-PPs}}{C_{p_{2,k},(d-1)-PPs}}\cdot(p_{2,k})^{(n_{N,p_{2,k}}-1)} = \gcd(d!,N). \tag{12}$$

Clearly, $C_{p_{1,k},d-PPs} \geq C_{p_{1,k},(d-1)-PPs}$ $\forall k = \overline{1,s_1}$, and $C_{p_{2,k},d-PPs} \geq C_{p_{2,k},(d-1)-PPs}$, and $(p_{2,k})^{(n_{N,p_{2,k}}-1)} > 1$ for $n_{N,p_{2,k}} > 1$ $\forall k = \overline{s_1+1, s_1+s_2}$. Notation $\forall k = \overline{1,L}$, with L a positive integer, means $\forall k = 1,2,\ldots,L$. Then, if $p_{2,k} \nmid \gcd(d!,N)$ for some $k \in \{s_1+1,\ldots,s_1+s_2\}$, Equation (12) can be fulfilled only if $n_{N,p_{2,k}} = 1$, and $C_{p_{2,k},d-PPs} = C_{p_{2,k},(d-1)-PPs}$ or $\frac{C_{p_{2,k},d-PPs}}{C_{p_{2,k},(d-1)-PPs}} \mid \gcd(d!,N)$, and if $p_{1,k} \nmid \gcd(d!,N)$ for some $k \in \{1,\ldots,s_1\}$, Equation (12) can be fulfilled only if $C_{p_{1,k},d-PPs} = C_{p_{1,k},(d-1)-PPs}$ or $\frac{C_{p_{1,k},d-PPs}}{C_{p_{1,k},(d-1)-PPs}} \mid \gcd(d!,N)$. □

The cases when $p_k \mid N$ and $p_k \mid \gcd(d!, N)$, for degrees of 2 up to 5, are approached separately in Sections 3.1–3.4. To help in this purpose, in Tables 4 and 5 the values of $\frac{C_{p_{1,k},d-PPs}}{C_{p_{1,k},(d-1)-PPs}}$ and $\frac{C_{p_{2,k},d-PPs}}{C_{p_{2,k},(d-1)-PPs}}$, for $d = 2, 3, 4, 5$, are given.

Table 4. The values $\frac{C_{p,d-PPs}}{C_{p,(d-1)-PPs}}$ for $d = 2, 3, 4$.

p	$n_{N,p} = 1$	$n_{N,p} > 1$	$n_{N,p} = 1$	$n_{N,p} > 1$	$n_{N,p} = 1$	$n_{N,p} > 1$
	$\frac{C_{p,QPPs}}{C_{p,LPPs}}$	$\frac{C_{p,QPPs}}{C_{p,LPPs}}$	$\frac{C_{p,CPPs}}{C_{p,QPPs}}$	$\frac{C_{p,CPPs}}{C_{p,QPPs}}$	$\frac{C_{p,4-PPs}}{C_{p,CPPs}}$	$\frac{C_{p,4-PPs}}{C_{p,CPPs}}$
2	2	1	2	1	2	2
3	1	1	3	2	3	1
5	1	1	6	1	1	1
7	1	1	1	1	15	1
1 (mod 3), $p > 7$	1	1	1	1	1	1
2 (mod 3), $p > 5$	1	1	$p + 1$	1	1	1

Table 5. The values $\frac{C_{p,5-PPs}}{C_{p,4-PPs}}$.

p	$n_{N,p} = 1$	$n_{N,p} > 1$
	$\frac{C_{p,5-PPs}}{C_{p,4-PPs}}$	$\frac{C_{p,5-PPs}}{C_{p,4-PPs}}$
2	2	2
3	3	4
5	5	14
7	8	43
13	248	157
1 (mod 15)	1	1
11 (mod 15)	1	1
7 (mod 15) or 13 (mod 15), $p > 13$	$p^2 + 1$	$p^2 - p + 1$
2 (mod 15) or 8 (mod 15), $p > 2$	$(p^2 + p + 1)/(p + 1)$	$p^2 - p + 1$
4 (mod 15)	$p + 1$	1
14 (mod 15)	$(2p + 1)/(p + 1)$	1

3.1. Determining Positive Integers N so That the Number of td QPPs Is Equal to 0

As can be seen from Table 4, the conditions in Lemma 1 are satisfied for each prime $p > 2$.

When $\gcd(2!, N) = 2$, it results that $2 \mid N$. Two subcases result.

When $p = 2$ and $n_{N,2} = 1$, equality $C_{N,QPPs,td} = 0$ implies $\frac{C_{2,QPPs}}{C_{2,LPPs}} = 2$. As we see in Table 4, the last condition is true.

When $p = 2$ and $n_{N,2} > 1$, equality $C_{N,QPPs,td} = 0$ implies $\frac{C_{2,QPPs}}{C_{2,LPPs}} \cdot 2^{n_{N,2}-1} = 2$, or, equivalently, $1 \cdot 2^{n_{N,2}-1} = 2$, or $n_{N,2} = 2$. Thus, this solution is valid.

Concluding, the number of *td* QPPs results equal to 0 when N is of the form

$$N_{C_{N,QPPs,td}=0} = 2^{n_{N,2}} \cdot \prod_{k=2}^{s} p_k, \text{ with } n_{N,2} = \overline{0,2}, p_k > 2, \forall k = \overline{2,s}, \tag{13}$$

as was previously obtained by a different method given in [7].

3.2. Determining Positive Integers N so That the Number of td CPPs Is Equal to 0

As can be seen from Table 4, the conditions in Lemma 1 are satisfied for primes of type $p = 1 \pmod 3$. In addition, if $\gcd(3!, N) = 6$, condition $\frac{C_{p,CPPs}}{C_{p,QPPs}} \mid \gcd(3!, N)$ is met for $p = 5$.

When $\gcd(3!, N) > 1$, the following cases result.

(1) $\gcd(3!, N) = 2$, i.e., $2 \mid N$ and $3 \nmid N$

When $p = 2$ and $n_{N,2} = 1$, equality $C_{N,CPPs,td} = 0$ implies $\frac{C_{2,CPPs}}{C_{2,QPPs}} = 2$. As we see in Table 4, the last condition is true.

When $p = 2$ and $n_{N,2} > 1$, equality $C_{N,CPPs,td} = 0$ implies $\frac{C_{2,CPPs}}{C_{2,QPPs}} \cdot 2^{n_{N,2}-1} = 2$, or, equivalently, $1 \cdot 2^{n_{N,2}-1} = 2$ or $n_{N,2} = 2$, a valid solution.

(2) $\gcd(3!, N) = 3$, i.e., $2 \nmid N$ and $3 \mid N$

When $p = 3$ and $n_{N,3} = 1$, equality $C_{N,CPPs,td} = 0$ implies $\frac{C_{3,CPPs}}{C_{3,QPPs}} = 3$. As we see in Table 4, the last condition is true.

When $p = 3$ and $n_{N,3} > 1$, equality $C_{N,CPPs,td} = 0$ implies $\frac{C_{3,CPPs}}{C_{3,QPPs}} \cdot 3^{n_{N,3}-1} = 3$, or, equivalently, $2 \cdot 3^{n_{N,3}-1} = 3$. Thus, no integer solution $n_{N,3}$ of the last equation exists such that $n_{N,3} > 1$.

(3) $\gcd(3!, N) = 6$, i.e., $2 \mid N$ and $3 \mid N$

In the cases when $p = 2$ and $n_{N,2} \in \{1, 2\}$, and when $p = 3$ and $n_{N,3} = 1$, only one solution exists. Thus, we have to consider only the case when $n_{N,2} > 2$ and $n_{N,3} > 1$.

When $n_{N,2} > 2$ and $n_{N,3} > 1$, equality $C_{N,CPPs,td} = 0$ implies $\frac{C_{2,CPPs}}{C_{2,QPPs}} \cdot 2^{n_{N,2}-1} \cdot \frac{C_{3,CPPs}}{C_{3,QPPs}} \cdot 3^{n_{N,3}-1} = 2 \cdot 3$, or, equivalently, $1 \cdot 2^{n_{N,2}-1} \cdot 2 \cdot 3^{n_{N,3}-1} = 2 \cdot 3$. The last equation has no integer solutions so that $n_{N,2} > 2$ and $n_{N,3} > 1$. If $5 \mid N$, $n_{N,5} = 1$, $n_{N,2} > 2$ and $n_{N,3} > 1$, condition $C_{N,CPPs,td} = 0$ implies $\frac{C_{2,CPPs}}{C_{2,QPPs}} \cdot 2^{n_{N,2}-1} \cdot \frac{C_{3,CPPs}}{C_{3,QPPs}} \cdot 3^{n_{N,3}-1} \cdot \frac{C_{5,CPPs}}{C_{5,QPPs}} = 2 \cdot 3$, or, equivalently, $1 \cdot 2^{n_{N,2}-1} \cdot 2 \cdot 3^{n_{N,3}-1} \cdot 6 = 2 \cdot 3$. The last equation has also no solutions such that $n_{N,2} > 2$ and $n_{N,3} > 1$.

Concluding, the number of *td* CPPs results equal to 0 when N is of the form

$$N_{C_{N,CPPs,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot \prod_{k=3}^{s} p_k,$$

$$\text{with } n_{N,2} = \overline{0,2}, n_{N,3} = \overline{0,1}, p_k > 3, \text{ with } p_k = 1 \pmod 3), k = \overline{3,s}, \tag{14}$$

as was previously obtained by a different method given in [7].

3.3. Determining Positive Integers N so That the Number of td 4-PPs Is Equal to 0

From Table 4, we note that the conditions from Lemma 1 are fulfilled for each prime $p > 7$ and for prime $p = 5$.

When $\gcd(4!, N) > 1$, the following cases result:

(1) $\gcd(4!, N) = 2^{n_{N,2}}$, with $n_{N,2} \in \{1, 2, 3\}$, i.e., $2^{n_{N,2}} \mid N$

When $p = 2$ and $n_{N,2} = 1$, equality $C_{N,4-PPs,td} = 0$ implies $\frac{C_{2,4-PPs}}{C_{2,CPPs}} = 2$. As we see in Table 4, the last condition is true.

When $p = 2$ and $n_{N,2} \in \{2,3\}$, equality $C_{N,4-PPs,td} = 0$ implies $\frac{C_{2,4-PPs}}{C_{2,CPPs}} \cdot 2^{n_{N,2}-1} = 2^{n_{N,2}}$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} = 2^{n_{N,2}}$. The last equation has as solutions both $n_{N,2} = 2$ and $n_{N,2} = 3$.

When $p = 2$ and $n_{N,2} > 3$, equality $C_{N,4-PPs,td} = 0$ implies $\frac{C_{2,4-PPs}}{C_{2,CPPs}} \cdot 2^{n_{N,2}-1} = 2^3$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} = 2^3$. The last equation has no integer solutions such that $n_{N,2} > 3$.

(2) $\gcd(4!, N) = 3$, i.e., $2 \nmid N$ and $3 \mid N$

When $p = 3$ and $n_{N,3} = 1$, equality $C_{N,4-PPs,td} = 0$ implies $\frac{C_{3,4-PPs}}{C_{3,CPPs}} = 3$. As we see in Table 4, the last condition is true.

When $p = 3$ and $n_{N,3} > 1$, equality $C_{N,4-PPs,td} = 0$ implies $\frac{C_{3,4-PPs}}{C_{3,CPPs}} \cdot 3^{n_{N,3}-1} = 3$, or, equivalently, $1 \cdot 3^{n_{N,3}-1} = 3$. The last equation has as a valid solution $n_{N,3} = 2$.

(3) $\gcd(4!, N) = 2^{n_{N,2}} \cdot 3$, with $n_{N,2} \in \{1,2,3\}$, i.e., $2^{n_{N,2}} \mid N$ and $3 \mid N$

Each of the above cases have solutions. Therefore, we do not have to consider this case because the same solutions result.

Concluding, the number of *td* 4-PPs results equal to 0 when N is of the form

$$N_{C_{N,4-PPs,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot 5^{n_{N,5}} \cdot \prod_{k=4}^{s} p_k,$$

$$\text{with } n_{N,2} = \overline{0,3}, n_{N,3} = \overline{0,2}, n_{N,5} = \overline{0,1}, p_k > 7, k = \overline{4,s}. \quad (15)$$

3.4. Determining Positive Integers N so That the Number of td 5-PPs Is Equal to 0

As can be seen from Table 5, the conditions in Lemma 1 are satisfied for primes p of types $p = 1 \pmod{15}$ and $p = 11 \pmod{15}$. In addition, if $8 \mid \gcd(5!, N)$, condition $\frac{C_{p,5-PPs}}{C_{p,4-PPs}} \mid \gcd(5!, N)$ is fulfilled for $p = 7$, and if $20 \mid \gcd(5!, N)$, condition $\frac{C_{p,5-PPs}}{C_{p,4-PPs}} \mid \gcd(5!, N)$ is fulfilled for $p = 19$.

When $\gcd(5!, N) > 1$, the following cases result:

(1) $\gcd(5!, N) = 2^{n_{N,2}}$, with $n_{N,2} \in \{1,2,3\}$, i.e., $2^{n_{N,2}} \mid N$, $3 \nmid N$, and $5 \nmid N$

When $p = 2$ and $n_{N,2} = 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{2,5-PPs}}{C_{2,4-PPs}} = 2$. As we see in Table 5, the last condition is true.

When $p = 2$ and $n_{N,2} \in \{2,3\}$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{2,5-PPs}}{C_{2,4-PPs}} \cdot 2^{n_{N,2}-1} = 2^{n_{N,2}}$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} = 2^{n_{N,2}}$. The last equation has as solutions both $n_{N,2} = 2$ and $n_{N,2} = 3$.

When $p = 2$ and $n_{N,2} > 3$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{2,5-PPs}}{C_{2,4-PPs}} \cdot 2^{n_{N,2}-1} = 2^3$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} = 2^3$. The last equation has no integer solutions such that $n_{N,2} > 3$.

When $7 \mid N$, $n_{N,7} = 1$, and $n_{N,2} > 3$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{2,5-PPs}}{C_{2,4-PPs}} \cdot 2^{n_{N,2}-1} \cdot \frac{C_{7,5-PPs}}{C_{5,4-PPs}} = 2^3$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} \cdot 8 = 2^3$. The last equation has no integer solutions such that $n_{N,2} > 3$.

(2) $\gcd(3!, N) = 3$, i.e., $2 \nmid N$, $3 \mid N$, and $5 \nmid N$

When $p = 3$ and $n_{N,3} = 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{3,5-PPs}}{C_{3,4-PPs}} = 3$. As we see in Table 5, the last condition is true.

When $p = 3$ and $n_{N,3} > 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{3,5-PPs}}{C_{3,4-PPs}} \cdot 3^{n_{N,3}-1} = 3$, or, equivalently, $4 \cdot 3^{n_{N,3}-1} = 3$. The last equation has no integer solutions such that $n_{N,3} > 1$.

(3) $\gcd(5!, N) = 2^{n_{N,2}} \cdot 3$, with $n_{N,2} \in \{1,2,3\}$, i.e., $2^{n_{N,2}} \mid N$, $3 \mid N$, and $5 \nmid N$

Each of the cases when $p = 2$ and $n_{N,2} \in \{1,2,3\}$, and when $p = 3$ and $n_{N,3} = 1$, have one solution. Thus, we have to consider only the case when $n_{N,2} > 3$ and $n_{N,3} > 1$.

When $n_{N,2} > 3$ and $n_{N,3} > 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{2,5-PPs}}{C_{2,4-PPs}} \cdot 2^{n_{N,2}-1} \cdot \frac{C_{3,5-PPs}}{C_{3,4-PPs}} \cdot 3^{n_{N,3}-1} = 2^3 \cdot 3$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} \cdot 4 \cdot 3^{n_{N,3}-1} = 2^3 \cdot 3$. The last equation has no integer solutions such that $n_{N,2} > 3$ and $n_{N,3} > 1$.

When $7 \mid N$, $n_{N,7} = 1$, $n_{N,2} > 3$ and $n_{N,3} > 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{2,5-PPs}}{C_{2,4-PPs}} \cdot 2^{n_{N,2}-1} \cdot \frac{C_{3,5-PPs}}{C_{3,4-PPs}} \cdot 3^{n_{N,3}-1} \cdot \frac{C_{7,5-PPs}}{C_{5,4-PPs}} = 2^3 \cdot 3$, or, equivalently, $2 \cdot 2^{n_{N,2}-1} \cdot 4 \cdot 3^{n_{N,3}-1} \cdot 8 = 2^3 \cdot 3$. The last equation has no integer solutions such that $n_{N,2} > 3$ and $n_{N,3} > 1$.

(4) $\gcd(5!, N) = 5$, i.e., $2 \nmid N$, $3 \nmid N$, and $5 \mid N$

When $p = 5$ and $n_{N,5} = 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{5,5-PPs}}{C_{5,4-PPs}} = 5$. As we see in Table 5, the last condition is true. When $p = 5$ and $n_{N,5} > 1$, equality $C_{N,5-PPs,td} = 0$ implies $\frac{C_{5,5-PPs}}{C_{5,4-PPs}} \cdot 5^{n_{N,5}-1} = 5$, or, equivalently, $14 \cdot 5^{n_{N,5}-1} = 5$. The last equation has no integer solutions such that $n_{N,5} > 1$.

The cases of other combinations of prime factors 2, 3, and 5, do not have to be considered because the same solutions result.

Concluding, the number of *td* 5-PPs results equal to 0 when N is of the form

$$N_{C_{N,5-PPs,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot 5^{n_{N,5}} \cdot \prod_{k=4}^{s} p_k, \text{ with } n_{N,2} = \overline{0,3}, n_{N,3} = \overline{0,1}, n_{N,5} = \overline{0,1},$$

$$p_k > 5, \text{ with } p_k = 1 \pmod{15} \text{ or } p_k = 11 \pmod{15}, k = \overline{4,s}. \tag{16}$$

4. Determining Positive Integers N so That the Number of *td* d-PPs Fulfilling ZF Sufficient Conditions Is Equal to 0

With the algorithm from Section 2, we can determine the number of *td* PPs fulfilling ZF sufficient conditions for an arbitrary degree d of PPs. The values used in (3) are denoted by $C_{p_k,d-PPs,ZF}$ in this case. We consider the sufficient coefficient conditions from [10] to find the values for $C_{p_k,d-PPs,ZF}$, depending on the degree d of PPs.

Let it be a PP of degree d modulo N as in Equation (1).

For $p = 2$ and $n_{N,p} = 1$, the condition is $(q_1 + q_2 + \cdots + q_d) \neq 0 \pmod 2$. It is fulfilled for $2^d/2 = 2^{d-1}$ combinations of coefficients $(q_1, q_2, \ldots, q_d)$.

For $p = 2$ and $n_{N,p} > 1$, the conditions are $q_1 \neq 0 \pmod 2$, $(q_2 + q_4 + q_6 + \ldots) = 0 \pmod 2$ and $(q_3 + q_5 + q_7 + \ldots) = 0 \pmod 2$.

Condition $q_1 \neq 0 \pmod 2$, with $q_1 \in \mathbb{Z}_2$, is met only for $q_1 = 1$.

Furthermore, we consider the degree d odd and even, respectively, in the other two conditions.

When d is odd ($d \geq 3$), i.e., $d = 2 \cdot k + 1$, $k \in \mathbb{N}^*$, each of the sums $(q_2 + q_4 + q_6 + \ldots)$ and $(q_3 + q_5 + q_7 + \ldots)$ contain k coefficients, each of them being satisfied for $2^k/2 = 2^{k-1}$ combinations of coefficients. It results that $C_{p_k,d-PPs,ZF} = 1 \cdot 2^{k-1} \cdot 2^{k-1} = 2^{2k-2} = 2^{d-3}$, for d odd.

When d is even ($d \geq 4$), i.e., $d = 2 \cdot k$, with $k \in \mathbb{N}$, $k \geq 2$, the sum $(q_2 + q_4 + q_6 + \ldots)$ contains k coefficients and the sum $(q_3 + q_5 + q_7 + \ldots)$ contains $k - 1$ coefficients. The first sum is fulfilled for $2^k/2 = 2^{k-1}$ combinations of coefficients and the second one for $2^{k-1}/2 = 2^{k-2}$ combinations of coefficients. It results that $C_{p_k,d-PPs,ZF} = 1 \cdot 2^{k-1} \cdot 2^{k-2} = 2^{2k-3} = 2^{d-3}$, for d even.

When $p > 2$ and $n_{N,p} \geq 1$, the conditions become $q_1 \neq 0 \pmod p$ and $q_2 = q_3 = \cdots = q_d = 0 \pmod p$. Condition $q_1 \neq 0 \pmod p$, with $q_1 \in \mathbb{Z}_p$, is fulfilled for $p - 1$ values. Condition $q_2 = q_3 = \cdots = q_d = 0 \pmod p$, with $q_i \in \mathbb{Z}_p$, $\forall i = \overline{2,d}$, is fulfilled only for $q_2 = q_3 = \cdots = q_d = 0$. In this case, $C_{p_k,d-PPs,ZF} = (p-1) \cdot 1 = p - 1$.

Table 6 summarizes the values of $C_{p_k,d-PPs}$ used in (3) in the case of ZF sufficient conditions.

We note that the ZF sufficient conditions also become necessary for LPPs and QPPs. Thus, the same values of $C_{p_k,d-PPs}$ from Table 1 can be used.

The values $\frac{C_{p_{1,k},d-PPs,ZF}}{C_{p_{1,k},(d-1)-PPs,ZF}}$ and $\frac{C_{p_{2,k},d-PPs,ZF}}{C_{p_{2,k},(d-1)-PPs,ZF}}$, for $d \geq 3$, are given in Table 7 .

Table 6. The number of d-permutation polynomials (PPs) ($d \geq 3$) fulfilling ZF sufficient conditions over $\mathbb{Z}_p$ permuting $\mathbb{Z}_{p^{n_{N,p}}}$, with $n_{N,p} \geq 1$.

p	$n_{N,p} = 1$	$n_{N,p} > 1$
	$C_{p,d-PPs,ZF}$	$C_{p,d-PPs,ZF}$
2	2^{d-1}	2^{d-3}
$p > 2$	$p-1$	$p-1$

Table 7. The values $\frac{C_{p,d-PPs}}{C_{p,(d-1)-PPs}}$ for d-PPs ($d \geq 3$) fulfilling Zhao and Fan (ZF) sufficient conditions.

p	$n_{N,p} = 1$	$n_{N,p} > 1$
	$\frac{C_{p,d-PPs}}{C_{p,(d-1)-PPs}}$	$\frac{C_{p,d-PPs}}{C_{p,(d-1)-PPs}}$
2	2	$\begin{cases} 2, & \text{if } d > 3, \\ 1, & \text{if } d = 3. \end{cases}$
$p > 2$	1	1

Let there be

$$z(x) = \sum_{k=1}^{d} z_k \cdot x^k \ (\text{mod } N), \tag{17}$$

a null polynomial (NP) of degree d modulo N, i.e., $z(x) = 0, \forall x = \overline{0, N-1}$.

As we pointed out in [9], the null polynomials (NPs) under ZF sufficient conditions have to fulfill conditions

$$z_1 \neq (-q_1) \ (\text{mod } p), z_2 = z_3 = \cdots = z_d = 0 \ (\text{mod } p), \forall p \mid N, p > 2. \tag{18}$$

Thus, the number of NPs of degrees smaller than or equal to d fulfilling ZF sufficient conditions will not be equal to $\prod_{k=2}^{d} \gcd(k!, N)$ as used in (4). This number is obtained in the following. The general form of NPs of degrees up to d is known from [13,14]:

$$z(x) = \sum_{k=1}^{d} \left\{ \frac{N}{\gcd(k!, N)} \cdot \tau_k \cdot \prod_{m=0}^{k-1} (x - m) \right\} (\text{mod } N),$$
$$\text{where } 0 \leq \tau_k \leq \gcd(k!, N) - 1. \tag{19}$$

The quantity $\gcd(k!, N), k \geq 3$ is denoted by g_k in the following. Let

$$g_k = \gcd(k!, N) = 2^{n_{g_k,2}} \cdot \prod_{j=2}^{s_{g_k}} p_{j,g_k}^{n_{g_k,p_j}}, \text{ with } s_{g_k} \geq 2, n_{g_k,2} \geq 1, n_{g_k,p_j} \geq 1, \text{ and}$$
$$p_{j,g_k} > 2, \forall j = 2, 3, \ldots, s_{g_k}, \tag{20}$$

be the factorization of g_k.

The truth value function $||x \star y||$, with $\star$ being an operator between two positive integers x and y, is defined as

$$||x \star y|| = \begin{cases} 1, & \text{if } x \star y \text{ have a true value of truth,} \\ 0, & \text{if } x \star y \text{ have a false value of truth.} \end{cases} \tag{21}$$

We will use the function in (21) with the "equality operator" (==) and "greater than or equal to" operator ($\geq$).

Similarly to [9], if a prime $p \leq d$ exists, such that $n_{g_d,p} = n_{N,p}$, then for NPs fulfilling ZF sufficient conditions, we have to impose that $p \mid \tau_k$, $\forall k = k', k'+1, \ldots, d$, where k' is the lowest integer such that $n_{g_{k'},p} = n_{g_d,p}$. Thus, prime p will reduce the number of NPs by $p^{d-k'+1}$. With g_d as in (20) for $k = d$, the number of NPs fulfilling ZF sufficient conditions will be equal to

$$C_{NPs,ZF} = \frac{\prod_{k=2}^{d} \gcd(k!, N)}{\prod_{k=2}^{s_{g_d}} (p_{k,g_d})^{(d-k'_d+1)\cdot||n_{g_d,p_k}==n_{N,p_k}||}}, \tag{22}$$

where k'_d is the lowest integer such that $n_{g_{k'_d},p_k} = n_{g_d,p_k}$.

Then the formula for the number of *td* $d-PPs$ fulfilling ZF sufficient conditions is

$$\begin{aligned} C_{N,d-PPs,ZF,td} = {} & C_{N,d-PPs,ZF,\text{all}} \cdot \frac{\prod_{k=2}^{s_{g_d}} (p_{k,g_d})^{(d-k'_d+1)\cdot||n_{g_d,p_k}==n_{N,p_k}||}}{\prod_{k=2}^{d} \gcd(k!, N)} - \\ & - C_{N,(d-1)-PPs,\text{all}} \cdot \frac{\prod_{k=2}^{s_{g_{d-1}}} (p_{k,g_{d-1}})^{(d-k'_{d-1})\cdot||n_{g_{d-1},p_k}==n_{N,p_k}||}}{\prod_{k=2}^{d-1} \gcd(k!, N)}. \end{aligned} \tag{23}$$

Theorem 1. *Let the prime factorization of* $d!$ *be*

$$d! = 2^{n_{d!,2}} \cdot \prod_{k=2}^{s_{d!}} p_{k,d!}^{n_{d!,p_k}},$$

$$\textit{with } s_{d!} \geq 2, n_{d!,2} \geq 1, n_{d!,p_k} \geq 1, \textit{ and } 2 < p_{k,d!} \leq d, \forall k = 2, 3, \ldots, s_{d!}. \tag{24}$$

Then the number of td d-PPs fulfilling ZF sufficient conditions is equal to zero ($C_{N,d-PPs,ZF,td} = 0$) *if the factorization of* N *is*

$$N_{C_{N,d-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot \prod_{k=2}^{s_{d!}} p_{k,d!}^{n_{N,p_k}} \cdot \prod_{k=s_{d!}+1}^{s} p_k,$$

$$\textit{with } 0 \leq n_{N,2} \leq n_{d!,2} \textit{ for } d > 3 \textit{ and } 0 \leq n_{N,2} \leq 2 \textit{ for } d = 3,$$

$$0 \leq n_{N,p_k} \leq n_{d!,p_k} + 1, 2 < p_{k,d!} < d, \forall k = 2, 3, \ldots, s_{d!}, \textit{ and } p_k > d, \forall k = s_{d!}+1, \ldots, s. \tag{25}$$

Proof. Imposing that $C_{N,d-PPs,ZF,td} = 0$ in (23), we obtain

$$\frac{C_{N,d-PPs,ZF,\text{all}}}{C_{N,(d-1)-PPs,\text{all}}} = \gcd(d!, N) \cdot \frac{\prod_{k=2}^{s_{g_{d-1}}} (p_{k,g_{d-1}})^{(d-k'_{d-1})\cdot||n_{g_{d-1},p_k}==n_{N,p_k}||}}{\prod_{k=2}^{s_{g_d}} (p_{k,g_d})^{(d-k'_d+1)\cdot||n_{g_d,p_k}==n_{N,p_k}||}}. \tag{26}$$

The cases when d is a prime number and d is not a prime number are analyzed in the following.

(1) d—a prime number

The prime factorizations of g_{d-1} and $g_d/d^{(||n_{N,d}\geq 1||)}$ are the same if d is a prime number. Moreover, $n_{g_d,d} = 1$ and $k'_d = d$. Therefore, we have

$$\frac{\prod_{k=2}^{s_{g_{d-1}}} (p_k)^{(d-k'_{d-1})\cdot||n_{g_{d-1},p_k}==n_{N,p_k}||}}{\prod_{k=2}^{s_{g_d}} (p_k)^{(d-k'_d+1)\cdot||n_{g_d,p_k}==n_{N,p_k}||}} = \frac{1}{d^{(||n_{N,d}==1||)}}. \tag{27}$$

In this case, condition (26) becomes

$$\frac{C_{N,d-PPs,ZF,\text{all}}}{C_{N,(d-1)-PPs,\text{all}}} = \frac{\gcd(d!,N)}{d^{(||n_{N,d}==1||)}}. \tag{28}$$

Taking into account Equation (3) and the values in Table 7, for $d = 3$ we obtain $C_{N,CPPs,ZF,td} = 0$ if the factorization of N is

$$N_{C_{N,CPPs,ZF,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot \prod_{k=3}^{s} p_k, \text{ with } n_{N,2} = \overline{0,2}, n_{N,3} = \overline{0,2},$$

$$p_k > 3, \forall k = \overline{3,s}, \tag{29}$$

as in (25) for $d = 3$. The same result was obtained in [9].

If d is a prime number, $d > 3$, considering (3) and the values in Table 7, (28) is equivalent to

$$2 \cdot 2^{n_{N,2}-1} \cdot \prod_{k=s_1+1}^{s_1+s_2} 1 \cdot (p_{2,k})^{(n_{N,p_{2,k}}-1)} = 2^{n_{g_d,2}} \cdot \prod_{k=2}^{s_{d!}-1} p_{k,d!}^{n_{g_d,p_k}} \cdot d^{(||n_{N,d}\geq 1||)-(||n_{N,d}==1||)},$$

$$\text{with } 0 \leq n_{g_d,2} \leq n_{d!,2}, 0 \leq n_{g_d,p_k} \leq n_{d!,p_k}, \text{ and } 2 < p_{k,d!} < d, \forall k = 2,3,\ldots,s_{d!}-1. \tag{30}$$

For d a prime number, $d > 3$, from (30) it results that $C_{N,d-PPs,ZF,td} = 0$ if the factorization of N is

$$N_{C_{N,d-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot \prod_{k=2}^{s_{d!}-1} p_{k,d!}^{n_{N,p_k}} \cdot d^{n_{N,d}} \cdot \prod_{k=s_{d!}+1}^{s} p_k,$$

$$\text{with } 0 \leq n_{N,2} \leq n_{d!,2}, 0 \leq n_{N,p_k} \leq n_{d!,p_k}+1, \text{ and } 2 < p_{k,d!} < d, \forall k = 2,3,\ldots,s_{d!}-1,$$

$$0 \leq n_{N,d} \leq 2, p_k > d, \forall k = s_{d!}+1,\ldots,s. \tag{31}$$

(31) is the same as (25) for d a prime number.

(2) d—not a prime number

The prime factors from the factorization of g_d are the same as those from the prime factorization of g_{d-1}, possibly with greater powers of some factors, if d is not a prime number. The maximum powers of the primes $p_{k,d!}$ in the factorization of g_d are $n_{d!,p_k}$, $\forall k = 2,3,\ldots,s_{d!}$.

If $p_{k,d!} \mid g_d$, $p_{k,d!} \nmid d$, and $n_{d!,p_k} \geq n_{N,p_k}$, then $n_{g_{d-1},p_k} = n_{g_d,p_k} = n_{N,p_k}$ and $k'_{d-1} = k'_d$. Thus, the term corresponding to factor $p_{k,d!}$ in the ratio from the right-hand side of (26) is $\dfrac{1}{p_{k,d!}}$. The same observation is valid if $p_{k,d!} \mid g_d$, $p_{k,d!} \mid d$, and $n_{d!,p_k} - n_{d,p_k} \geq n_{N,p_k}$.

If $p_{k,d!} \mid g_d$, $p_{k,d!} \mid d$ and $n_{d!,p_k} - n_{d,p_k} < n_{N,p_k} \leq n_{d!,p_k}$, then $n_{g_{d-1},p_k} < n_{g_d,p_k} = n_{N,p_k}$, $||n_{g_{d-1},p_k} == n_{N,p_k}|| = 0$, $||n_{g_d,p_k} == n_{N,p_k}|| = 1$, and $k'_d = d$. Thus, the term corresponding to factor $p_{k,d!}$ in the ratio from the right-hand side of (26) is also $\dfrac{1}{p_{k,d!}}$.

If $p_{k,d!} \mid g_d$ and $n_{N,p_k} > n_{d!,p_k}$, then $n_{g_{d-1},p_k} < n_{N,p_k}$, $n_{g_d,p_k} < n_{N,p_k}$, $||n_{g_{d-1},p_k} == n_{N,p_k}|| = 0$, and $||n_{g_d,p_k} == n_{N,p_k}|| = 0$. Thus, the term corresponding to factor $p_{k,d!}$ in the ratio from the right-hand side of (26) is equal to 1.

Concluding, if d is not a prime number, (26) is equivalent to

$$\frac{C_{N,d-PPs,ZF,\text{all}}}{C_{N,(d-1)-PPs,\text{all}}} = \gcd(d!,N) \cdot \frac{1}{\prod_{k=2}^{s_{d!}} (p_{k,d!})^{||n_{d!,p_k} \geq n_{N,p_k}||}}. \tag{32}$$

Similarly to (30), (32) is equivalent to

$$2 \cdot 2^{n_{N,2}-1} \cdot \prod_{k=s_1+1}^{s_1+s_2} 1 \cdot (p_{2,k})^{(n_{N,p_{2,k}}-1)} = 2^{n_{g_d,2}} \cdot \frac{\prod_{k=2}^{s_{d!}} p_{k,d!}^{n_{g_d,p_k}}}{\prod_{k=2}^{s_{d!}} (p_{k,d!})^{||n_{d!,p_k} \geq n_{N,p_k}||}},$$

$$\text{with } 0 \leq n_{g_d,2} \leq n_{d!,2}, 0 \leq n_{g_d,p_k} \leq n_{d!,p_k}, \text{ and } 2 < p_{k,d!} < d, \forall k = 2,3,\ldots,s_{d!}. \tag{33}$$

If d is not a prime number, from (33) it results that $C_{N,d-PPs,ZF,td} = 0$ if the factorization of N is

$$N_{C_{N,d-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot \prod_{k=2}^{s_{d!}} p_{k,d!}^{n_{N,p_k}} \cdot \prod_{k=s_{d!}+1}^{s} p_k,$$

$$\text{with } 0 \leq n_{N,2} \leq n_{d!,2}, 0 \leq n_{N,p_k} \leq n_{d!,p_k} + 1, \text{ and } 2 < p_{k,d!} < d, \forall k = 2,3,\ldots,s_{d!},$$
$$p_k > d, \forall k = s_{d!}+1,\ldots,s. \tag{34}$$

We mention that formula (34) is also valid if d is a prime number. Thus, the theorem is proved.
□

Two examples for the form of N when d is a prime number and when d is not a prime number are given in the following.

Example 1 (Example of N so that $C_{N,11-PPs,ZF,td} = 0$). *For $d = 11$, we have*

$$11! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1 \cdot 11^1, \tag{35}$$

and $C_{N,11-PPs,ZF,td} = 0$ if N is of the form

$$N_{C_{N,11-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot 5^{n_{N,5}} \cdot 7^{n_{N,7}} \cdot 11^{n_{N,11}} \cdot \prod_{k=6}^{s} p_k,$$

$$\textit{with } 0 \leq n_{N,2} \leq 8, 0 \leq n_{N,3} \leq 5, 0 \leq n_{N,5} \leq 3, 0 \leq n_{N,7} \leq 2, 0 \leq n_{N,11} \leq 2,$$
$$\textit{and } p_k > 11, \forall k = 6,\ldots,s. \tag{36}$$

Example 2 (Example of N such that $C_{N,12-PPs,ZF,td} = 0$). *For $d = 12$, we have*

$$12! = 2^{10} \cdot 3^5 \cdot 5^2 \cdot 7^1 \cdot 11^1, \tag{37}$$

and $C_{N,12-PPs,ZF,td} = 0$ if N is of the form

$$N_{C_{N,12-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot 5^{n_{N,5}} \cdot 7^{n_{N,7}} \cdot 11^{n_{N,11}} \cdot \prod_{k=6}^{s} p_k,$$

$$\textit{with } 0 \leq n_{N,2} \leq 10, 0 \leq n_{N,3} \leq 6, 0 \leq n_{N,5} \leq 3, 0 \leq n_{N,7} \leq 2, 0 \leq n_{N,11} \leq 2,$$
$$\textit{and } p_k > 11, \forall k = 6,\ldots,s. \tag{38}$$

We mention that the same results as in [9] for degrees $d = 4$ and $d = 5$ are obtained, i.e.,

$$N_{C_{N,4-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot \prod_{k=3}^{s} p_k,$$

$$\text{with } 0 \leq n_{N,2} \leq 3, 0 \leq n_{N,3} \leq 2,$$

$$\text{and } p_k > 3, \forall k = 3, \ldots, s, \tag{39}$$

and

$$N_{C_{N,5-PPs,ZF,td=0}} = 2^{n_{N,2}} \cdot 3^{n_{N,3}} \cdot 5^{n_{N,5}} \cdot \prod_{k=4}^{s} p_k,$$
$$\text{with } 0 \leq n_{N,2} \leq 3, 0 \leq n_{N,3} \leq 2, 0 \leq n_{N,5} \leq 2,$$
$$\text{and } p_k > 5, \forall k = 4, \ldots, s. \tag{40}$$

5. Conclusions

In this paper, we obtained the form of N's prime factorization for which the number of *td* fourth- and fifth-degree permutation polynomials is equal to zero. These values of N do not have to be used as fourth- and fifth-degree PP interleaver lengths because some PPs of smaller degree are equivalent to the fourth- or fifth-degree PPs, providing the same permutations.

We have particularized the algorithm from [11] for permutation polynomials under ZF sufficient conditions, and we obtained the number of null polynomials and the quantities $C_{p,d-PPs,ZF}$ required in the algorithm. We have also obtained the form of N's prime factorization such that the number of *td* PPs of any degree, fulfilling ZF sufficient conditions, is equal to zero. Similarly to those above, these values of N do not have to be used as PP interleaver lengths when we search for PP interleavers under ZF sufficient conditions.

Comparing (15) with (39), we conclude that there are no *td* 4-PPs fulfilling ZF sufficient conditions, but there are *td* 4-PPs fulfilling other conditions, only when $7 \mid N$.

Comparing (16) with (40), we conclude that there are no *td* 5-PPs fulfilling ZF sufficient conditions, but there are *td* 5-PPs fulfilling other conditions, only when $9 \mid N$, or $25 \mid N$, or $p \mid N$ with $p \neq 1 \pmod{15}$ and $p \neq 11 \pmod{15}$.

Author Contributions: Both authors contributed equally to this work.

Funding: This research received no external funding.

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

References

1. Cohen, S.D. *Permutation Group Theory and Permutation Polynomials, Algebras and Combinatorics: An International Congress*; Springer: Singapore, 1999; pp. 133–146.
2. Lidl, R.; Niederriter, H. *Finite Fields*; Cambridge Univ. Press: Cambridge, UK, 1997.
3. Sun, J.; Takeshita, O.Y. Interleavers for turbo codes using permutation polynomials over integer ring. *IEEE Trans. Inform. Theory* **2005**, *51*, 101–119.
4. Zhao, H.; Fan, P.; Tarokh, V. On the equivalence of interleavers for turbo codes using quadratic permutation polynomials over integer rings. *IEEE Commun. Lett.* **2010**, *14*, 236–238 . [CrossRef]
5. Trifina, L.; Tarniceriu, D.; Andrei, M. Determining the number of different cubic permutation polynomial based interleavers for lengths in the LTE standard. In Proceedings of the 2015 International Symposium on Signals, Circuits and Systems (ISSCS), Iasi, Romania, 9–10 July 2015; 4p.
6. 3GPP TS 36.212 V8.3.0, 3rd Generation Partnership Project, Multiplexing and channel coding (Release 8). 2008. Available online: http://www.etsi.org/deliver/etsi_ts/136200_136299/136212/08.03.00_60/ts_136212v080300p.pdf (accessed on 5 June 2015).
7. Trifina, L.; Tarniceriu, D. A simple method to determine the number of true different quadratic and cubic permutation polynomial based interleavers for turbo codes. *Telecommun. Syst.* **2017**, *64*, 147–171. [CrossRef]
8. Trifina, L.; Tarniceriu, D. The number of different true permutation polynomial based interleavers under Zhao and Fan sufficient conditions. *Telecommun. Syst.* **2016**, *63*, 593–623. [CrossRef]
9. Trifina, L.; Tarniceriu, D. Correction for the paper "The number of different true permutation polynomial based interleavers under Zhao and Fan sufficient conditions". *Telecommun. Syst.* **2019**, *70*, 141–158. [CrossRef]

10. Zhao, H.; Fan, P. Simple method for generating mth-order permutation polynomials over integer rings. *IEE Electron. Lett.* **2007**, *43*, 449–451. [CrossRef]
11. Trifina, L.; Tarniceriu, D. Determining the number of true different permutation polynomials of degrees up to five by Weng and Dong algorithm. *Telecommun. Syst.* **2018**, *67*, 211–215. [CrossRef]
12. Weng, G.; Dong, C. A note on permutation polynomials over $\mathbb{Z}_n$. *IEEE Trans. Inform. Theory* **2008**, *54*, 4388–4390. [CrossRef]
13. Singmaster, D. On polynomial functions $\pmod{m}$. *J. Number Theory* **1974**, *6*, 345–352. [CrossRef]
14. Ryu, J. Permutation Polynomial Based Interleavers for Turbo Codes Over Integer Rings. Ph.D. Thesis, Ohio State University, Columbus, OH, USA, 2007. Available online: https://etd.ohiolink.edu/rws_etd/document/get/osu1181139404/inline (accessed on 18 July 2019).