The Graph Structure of Chebyshev Permutation Polynomials over Ring $\mathbb{Z}_{p^k}$

Chengqing Li, Xiaoxiong Lu, Kai Tan, and Guanrong Chen, Life Fellow, IEEE

Abstract—Understanding the underlying graph structure of a nonlinear map over a certain domain is essential to evaluate its potential for real applications. In this paper, we investigate the structure of the associated functional graph of Chebyshev permutation polynomials over ring $\mathbb{Z}_{p^k}$, where $p$ is a prime number larger than three, every number in the ring is considered as a vertex and the existing mapping relation between two vertices is regarded as a directed edge. Based on some new properties of Chebyshev polynomials and their derivatives, we disclose how the basic structure of the functional graph evolves with respect to parameter $k$. First, we present a complete explicit form of the length of a path starting from any given vertex, i.e., the least period of the sequence generated by iterating a Chebyshev permutation polynomial from an initial state. Then, we show that the strong patterns of the functional graph, e.g., the number of cycles of any given length, is always preserved as $k$ increases. Moreover, we rigorously prove the elegant structure of the functional graph and verify it experimentally. Our results could be useful for studying emergence of complexity of a nonlinear map in digital computer and security analysis of its cryptographical applications.

Index Terms—Chebyshev polynomial, Chebyshev integer sequence, cycle distribution, emergence, functional graph, permutation, pseudorandom number sequence, period.

I. INTRODUCTION

CHEBYSHEV polynomials are named after the Russian mathematician Pafnuty L. Chebyshev [1], which are widely applied in diverse fields, for example function approximation [2], pseudorandom number generator [3], spread-spectrum sequence [4], authentication [5], key exchange protocol [6], and privacy protection [7].

The Chebyshev polynomials of the first kind are defined by recurrence relations as follows:

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x),$$

where $T_0(x) = 1$, $T_1(x) = x$, $x \in [-1, 1]$, and $n$ is the degree of the Chebyshev polynomial. The Chebyshev polynomials of the second kind are defined in a similar form, as follows:

$$U_{n+1}(x) = 2xU_n(x) - U_{n-1}(x),$$

where $U_0(x) = 1$, $U_1(x) = 2x$. Some Chebyshev-like rational maps were introduced and defined by replacing the cosine functions in the trigonometric form of the Chebyshev polynomial with tangent functions [8], [9].

The semi-group property of the Chebyshev polynomials has attracted considerable attention from the field of cryptography, which are used as an alternative way to design public-key encryption algorithms [10]–[13], with the first publication on the polynomials over real number field in 2003 [10]. However, because the degree of a Chebyshev polynomial has an explicit algebraic expression over real number field, lately the security flaws of the algorithm designed in [10] were found [17], [18]. Then, the numerical domain was extended from real number field to ring $\mathbb{Z}_{p^k}$ [13]. The security of the associated algorithms depends on the difficulty in deriving the degree of the Chebyshev polynomial used, which satisfies $y \equiv T_n(x) \mod p^k$ for given $x$, $y$ and $k$. Recently, cryptanalysis on the public-key encryption algorithm has demonstrated that it is insecure when the parameters are improperly selected [14]–[18]. Nevertheless, to present complete security analysis on cryptographical applications of Chebyshev polynomials over $\mathbb{Z}_{p^k}$, disclosure of its graph structure is the precondition.

There are two kinds of sequences produced by Chebyshev polynomials over $\mathbb{Z}_{p^k}$: Chebyshev degree sequence $\{T_i(x) \mod p^k\}_{i \geq 0}$ [14]–[16] and Chebyshev integer sequence $\{T^*_n(x) \mod p^k\}_{n \geq 0}$ [17]–[19]. The former is essentially a homogeneous linear recurring sequence. It is periodic for any parameters and initial states [20]. The period distributions of Chebyshev degree sequences over prime field $\mathbb{F}_p$ [14] and ring $\mathbb{Z}_{p^k}$ [15] have been systematically analyzed by the generating function method, showing that the security of the public-key encryption algorithm based on a Chebyshev polynomial depends on the parameter $p$. Combining the variation rule of the period of a Chebyshev degree sequence with the increase of parameter $k$, a polynomial-time algorithm was designed in [16] to determine the equivalence class of the degree of a Chebyshev polynomial modulo $p^k$ when $p$ is not large.

Chebyshev integer sequence is a nonlinear congruence iterative sequence. It is periodic if and only if the Chebyshev polynomial is a permutation polynomial over $\mathbb{Z}_{p^k}$. The periods of the Chebyshev integer sequences generated by iterating Chebyshev permutation polynomials over rings $\mathbb{Z}_{2^k}$ and $\mathbb{Z}_{p^k}$ were investigated in [17]–[19]. Moreover, an algorithm with time complexity $O(k)$ was developed to identify the degree of the Chebyshev polynomial modulo $2^k$ [17]. In [18], it is
reported that a key exchange protocol based on a Chebyshev polynomial modulo $p^k$ may be fragile against brute-force attack for some parameters. The period of a Chebyshev degree sequence over different domains can be analyzed with the aid of abundant algebraic tools for linear recurring sequences. In contrast, the nonlinear complexity of Chebyshev integer sequences make the period analysis much more difficult.

The graph structure of a nonlinear system over different domains can be used to evaluate the dynamics and the randomness of a system [21]–[26]. In [22], [23], evolution rules on the graph structure of various chaotic maps, including the Logistic map, Tent map, and Cat map, on a finite-precision computer were revealed. In particular, the graph structure of the generalized Cat map over any binary arithmetic domain and the associated evolution rules are completely disclosed. Some periodicity properties of the sequences generated by the Logistic map and Cat map over different rings are presented in [24]–[26]. The graph structure of a linear feedback shift register with arbitrary characteristic polynomial over finite field $\mathbb{F}_p$, is theoretically proved based on cyclotomic classes and decimation sequences [27]. Then, the graph structure of a class of cascaded feedback registers is determined by solving a system of linear equations [28]. Using a special type of trees associated with $v$-series, the functional graphs of Rédei functions [29], Chebyshev polynomials [30], and general linear maps [31] over finite field $\mathbb{F}_p$, were investigated with respect to various metrics: the number of connected components, the lengths of cycles and the average pre-period (transient) lengths. Moreover, a comprehensive review was presented in [32] for studying the dynamics of digitized nonlinear maps via the functional graphs.

Although there have been some investigations on the graph structure of Chebyshev polynomials over finite field $\mathbb{F}_p$, and ring $\mathbb{Z}_{p^k}$ for example in [17], [30], [33], its graph structure over ring $\mathbb{Z}_{p^k}$ is still not clear, due perhaps to the high computational complexity of Chebyshev polynomials with larger degrees. In addition, this study may provide new ideas for the construction of complete permutation polynomial [34]–[36]. In this paper, we first review and improve an explicit periodicity analysis of the Chebyshev integer sequences over ring $\mathbb{Z}_{p^k}$ given in [18]. We then find the periodicity variation rules of the sequences with the increase of parameter $k$. To that end, we analyze the graph structure of Chebyshev permutation polynomials over the ring and reveal how the structure is changed with parameter $k$.

The rest of the paper is organized as follows. Section II derives the period of the Chebyshev integer sequence generated from any initial state over ring $\mathbb{Z}_{p^k}$. The graph structure of Chebyshev permutation polynomials over the ring is completely disclosed in Sec. III. The last section concludes the paper.

II. CHEBYSHEV POLYNOMIAL AND CHEBYSHEV INTEGER SEQUENCE

In this section, we review some existing results about the Chebyshev polynomial, and propose some new properties of its $m$-order derivative, which are useful for analyzing the explicit expression of the least-period Chebyshev integer sequence from a given initial state.

A. Preliminary

For each integer $n > 1$, a Chebyshev polynomial of degree $n$ can be represented in power series form as

$$T_n(x) = \frac{n^2}{2} \sum_{m=0}^{\lfloor n/2 \rfloor} (-1)^m \frac{(n-m-1)!}{m!(n-2m)!} (2x)^{n-2m}$$  \hspace{1cm} (3)

If $n$ is odd, $T_n(x)$ can be represented as

$$T_n(x) = a_1x + a_2x^3 + \cdots + a_nx^n,$$ \hspace{1cm} (4)

where $a_i$ is an integer. Then, for any $x, y \in \mathbb{Z}$,

$$T_n(x+y) = a_1(x+y) + a_3(x+y)^3 + \cdots + a_n(x+y)^n = T_n(x) + y \cdot T_n^{(1)}(x) + \cdots + y^n \cdot \frac{T_n^{(n)}(x)}{n!}$$ \hspace{1cm} (5)

and

$$\frac{T_n^{(m)}(x)}{m!} \in \mathbb{Z},$$ \hspace{1cm} (6)

where $\mathbb{Z}$ is the integer set, $1 \leq m \leq n$, and $T_n^{(m)}(x)$ is the $m$-th derivative of Chebyshev polynomial $T_n(x)$. If $x$ can be expressed as $x = \frac{y+y^{-1}}{2}$, it follows that

$$T_n(x) = T_n\left(\frac{y+y^{-1}}{2}\right) = \frac{y^n + y^{-n}}{2}$$ \hspace{1cm} (7)

and

$$U_n(x) = U_n\left(\frac{y+y^{-1}}{2}\right) = \frac{y^{n+1} - y^{-(n+1)}}{y - y^{-1}}.$$ \hspace{1cm} (8)

The semi-group property is one of the most important properties of Chebyshev polynomials, which is

$$T_n(T_m(x)) = T_m(T_n(x)) = T_{mn}(x)$$

for any two positive integers $m$ and $n$. Thus, the composition of $N$ Chebyshev polynomial $T_n(x)$ can be denoted as $T_{n^N}(x)$.

Let $\mathbb{Z}_{p^k}$ be the ring of residue classes modulo $p^k$ with respect to modular addition and multiplication, where $k$ is a natural number. The semi-group property of Chebyshev polynomials over $\mathbb{Z}_{p^k}$ still holds, namely $T_n(T_m(x)) \equiv T_{mn}(T_n(x)) \equiv T_{mn}(x) \pmod{p^k}$.

Given an initial state $x \in \mathbb{Z}_{p^k}$, the $i$-th iteration of $T_n(x)$ over $\mathbb{Z}_{p^k}$ is $T_n(x) = T_n(T_{n^{-1}}(x)) \pmod{p^k}$, where $i \geq 1$ and $T_{n^i}(x) = x \pmod{p^k}$. The least period of a sequence generated by iterating a Chebyshev polynomial is defined as the minimum positive integer $N$ such that $T_n^N(x) \equiv x \pmod{p^k}$. In particular, iterating some functions from any initial state can return it. Such functions are called permutation functions over a domain. They exist if and only if they are bijective over the domain. For a Chebyshev polynomial $T_n(x)$ over $\mathbb{Z}_{p^k}$, it is a permutation polynomial if and only if

$$\gcd(n, p) = \gcd(n, p^2 - 1) = 1,$$ \hspace{1cm} (9)

where $\gcd$ denotes the operator solving the greatest common divisor of two integers [18]. It is assumed that Chebyshev
polynomial $T_n(x)$ satisfies condition (9) and $p > 3$ throughout the rest of this paper unless otherwise indicated. (The graph structure with $p = 2$ is investigated in [17], and that with $p = 3$ requires special analysis as [24] dealing with Logistic map over ring $\mathbb{Z}_n$.)

B. Some properties of the derivative of a Chebyshev polynomial

The relation between different orders of derivative of Chebyshev polynomials $T_n(x)$ is discussed in Lemma 1 and Lemma 2 describes the number of factor $p$ contained in the $m$-order derivative of $T_n(x)$ at $±1$. The equivalence between the first derivatives of $T_n(x)$ at $p − 1$ and $−1$ is analyzed in Lemma 3.

**Lemma 1.** The $m$-order derivative of Chebyshev polynomial $T_n(x)$ satisfies

$$n^2 \left( x^2 - 1 \right) T_n^{(m)}(x) = \left( n^2 - \sum_{i=0}^{m-3} (2t + 1) T_n^{(m-2)}(x) \right) - (2m-3) x T_n^{(m-1)}(x), \quad (10)$$

where $T_n^{(0)}(x) = T_n(x)$ and $m \geq 2$.

**Proof.** The lemma is proved via mathematical induction on $m$. According to the relation between the two kinds of Chebyshev polynomials [37], $T_n(x) = nU_{n-1}(x)$ and $U_{n-1}(x) = \frac{nT_n(x) - xT_n'(x)}{x^2 - 1}$, one has

$$T_n^{(2)}(x) = \frac{n^2 T_n(x) - xT_n'(x)}{x^2 - 1}. \quad (11)$$

So, Eq. (10) holds for $m = 2$. Assume that Eq. (10) holds for $m = s$. When $m = s + 1$, using the quotient rule for differentiation, one obtains

$$\frac{dT_n^{(s)}(x)}{dx} = \frac{(n^2 - \sum_{i=0}^{s-2} (2t + 1) T_n^{(s-2)}(x))}{x^2 - 1} - \frac{(2s-1)x T_n^{(s)}(x)}{x^2 - 1}.$$

Thus, Eq. (10) also holds for $m = s + 1$. The above induction completes the proof of the lemma. \(\blacksquare\)

**Lemma 2.** If the derivative of a Chebyshev polynomial satisfies $T_n^{(m)}(±1) \equiv 1 \pmod{p^w}$, then

$$\frac{T_n^{(m)}(±1) \cdot p^m}{m!} \equiv 0 \pmod{p^{w+2}}$$

for any $m \geq 2$, where $w$ is a positive integer.

**Proof.** Referring to Eq. (6) with $x = ±1$, one has $\frac{T_n^{(m)}(±1)}{m!}$ is an integer. It means that the lemma holds when $m \geq w + 2$.

Now, assume $m < w + 2$. As [37], the $m$-order derivative of Chebyshev polynomial $T_n(x)$ at $±1$ can be expressed as

$$T_n^{(m)}(±1) = (±1)^{n+m} \prod_{j=0}^{m-1} n^2 - j^2 / 2j + 1. \quad (12)$$

When $m = 1$, one has $T_n'(±1) = n^2$. Since $T_n'(±1) \equiv 1 \pmod{p^w}$, one has

$$n^2 - 1 \equiv 0 \pmod{p^w}. \quad (13)$$

Let $E(x) = \max\{t \mid x \equiv 0 \pmod{p^t}\}$. When $m \geq 2$, one has

$$E(\prod_{i=0}^{m-1} (n^2 - i^2)) \geq E(n^2 - 1) \geq w \quad (14)$$

and

$$E(T_n^{(m)}(±1)) = E(\prod_{i=0}^{m-1} (n^2 - i^2)) - E(\prod_{j=0}^{m-1} (2j + 1)). \quad (15)$$

The value of $E(T_n^{(m)}(±1))$ is calculated according to the scope of $m$:

- $2 \leq m < p$: Calculate

$$E\left(\prod_{j=0}^{m-1} (2j + 1)\right) = \begin{cases} 0 & \text{if } 2 \leq m < \frac{p+1}{2}; \\ 1 & \text{if } \frac{p+1}{2} \leq m < p. \end{cases}$$

Referring to the above equation and Eqs. (14) and (15), one has

$$E(T_n^{(m)}(±1)) \geq \begin{cases} w & \text{if } 2 \leq m < \frac{p+1}{2}; \\ w - 1 & \text{if } \frac{p+1}{2} \leq m < p. \end{cases}$$

- $p \leq m < w + 2$: Since $T_n^{(m)}(±1)$ is an integer, if there is $j$ in the denominator $\prod_{j=0}^{m-1} (2j + 1)$ such that $2j + 1 = kp^i$, then

$$E(n^2 - i^2) = \begin{cases} t - 1 & \text{if } k = 1 \text{ and } t \neq 1; \\ t & \text{otherwise}. \end{cases} \quad (16)$$

where $k \pmod{p} \neq 0$ and $i$ belongs to

$$S_j = \begin{cases} \{p - 1\} & \text{if } k = 1 \text{ and } t = 1; \\ \{p + 1\} & \text{if } k = 3 \text{ and } t = 1; \\ \{\frac{p+1}{2}p^{i-1} + 1, \frac{p+1}{2}p^{i-1} - 1\} & \text{if } k = 1 \text{ and } t \neq 1; \\ \{k-1/p^i + 1, k-1/p^i - 1\} & \text{otherwise}. \end{cases}$$

From $m < w + 2$, one can know

$$kp^i = 2j + 1 \leq 2m - 1 < 2w + 3. \quad (17)$$

If $w = 1$, one can get $t \leq w$ from the above inequation. If $w > 1$, one can get $p^w > 3^w > 2w + 3$. It yields from Eq. (17) that $t \leq w$. So, one has $n^2 - 1 \equiv 0 \pmod{p^w}$ from congruence (13). It means that congruence (16) holds and $E(2j + 1) \leq E\left(\prod_{j=0}^{m-1} (2j + 1)\right)$. From the definition of $S_j$, one can know $S_j \cup S_{j'} = \emptyset$ for any $j_1, j_2 \in \{j \mid (2j + 1) \pmod{p} = 0, j \in \mathbb{Z}_m\}$, where $j_1 \neq j_2$. It yields $E\left(\prod_{j=0}^{m-1} (2j + 1)\right) \leq E\left(\prod_{i=2}^{m-1} (n^2 - i^2)\right)$. Since

$$E\left(\prod_{i=0}^{m-1} (n^2 - i^2)\right) = E(n^2 - 1) + E\left(\prod_{i=2}^{m-1} (n^2 - i^2)\right),$$

one has $E\left(\prod_{j=0}^{m-1} (n^2 - i^2)\right) - E\left(\prod_{j=0}^{m-1} (2j + 1)\right) \geq w$ from congruence (14), namely $E(T_n^{(m)}(±1)) \geq w$ by Eq. (15).
Combining the above two cases, one obtains
\[
T_n^{(m)}(±1) ≡ \begin{cases} 0 \pmod{p^m} & \text{if } 2 \leq m < \frac{p+1}{2} \\
0 \pmod{p^{m-1}} & \text{if } \frac{p+1}{2} \leq m < p. \end{cases} \tag{18}
\]

Now, move on to calculate \( E(m!) \). Write the integer \( m \) as a \( p \)-adic representation \( m = \sum_{i=0}^{e} k_ip^i \), where \( k_i \in \mathbb{Z}_p \setminus \{0\} \) and \( k_i \in \mathbb{Z}_p \) for \( i \in \{0, 1, \ldots, e-1\} \). If \( m < p \), one has \( \exp_1(te) = 0 \). Counting the number of integers in \( \{1, 2, \ldots, m\} \) dividing \( p^v \), if \( m \geq p \), one has
\[
E(m!) = \sum_{i=1}^{e} \left\{ \lfloor y \rfloor \mid y \equiv 0 \mod{p^i}; y = 1, 2, \ldots, m \right\} \\
= \sum_{i=1}^{e} \left( k_ip^i \right) \\
= \sum_{i=1}^{e} \left( k_ip^{i-1} + k_ip^{i-2} + \cdots + k_ip^{i-e+1} + k_e \right) \\
= k_e(p^{e-2} + k_{e-1}p^{e-3} + \cdots + k_2p^2 + k_1p) \leq m - 2.
\]
For any prime number \( p > 3 \), it follows from the above equation and \( 1+p+p^2+\cdots+p^{e-1} = (p^e-1)/(p-1) < p^e-2 \) that
\[
E(m!) < k_e(p^{e-2} + k_{e-1}p^{e-3} + \cdots + k_2p^2 + k_1p) \leq m - 2.
\]
Thus,
\[
\frac{p^m}{m!} \equiv \begin{cases} 0 \pmod{p^m} & \text{if } 2 \leq m < p; \\
0 \pmod{p^2} & \text{if } p \leq m \leq n. \tag{19}
\end{cases}
\]
Referring to congruences \( E(2), \) one has \( T_n^{(m)}(±1) \equiv 0 \pmod{m!} \).

**Lemma 3.** Congruence \( T_n^{(m)}(p-1) \equiv 1 \pmod{p^m} \) holds if and only if \( T_n^{(m)}(±1) \equiv 1 \pmod{p^m} \).

**Proof.** As \( T_n(x) \) is a polynomial of degree \( n \), one has
\[
T_n^{(m)}(p-1) = T_n^{(p)}(p-1) + \sum_{i=1}^{n-1} \binom{n}{i} p^{i-1} T_n^{(i)}(1). \tag{20}
\]
If \( T_n^{(m)}(p-1) \equiv 1 \pmod{p^m} \), from the above equation and Lemma 2, one has \( T_n^{(p)}(p-1) \equiv 1 \pmod{p^m} \). Hence, the sufficient part of this lemma is proved.
If \( T_n^{(m)}(p-1) \equiv 1 \pmod{p^m} \), one can prove
\[
T_n^{(m)}(±1) \equiv 1 \pmod{p^m} \tag{21}
\]
via mathematical induction on \( m \), where \( 1 \leq m \leq w \). When \( m = 1 \), it follows from Eq. (20) that \( T_n^{(m)}(p-1) \equiv 1 \pmod{p} \), which means congruence \( 21 \) holds for \( m = 1 \). Assume that congruence \( 21 \) holds for \( m = s \leq w-1 \), namely \( T_n^{(m)}(p-1) \equiv 1 \pmod{p^s} \). It means from Lemma 2 that
\[
\frac{p^{i-1}}{(i-1)!} T_n^{(i)}(1) \equiv 0 \pmod{p^{s+1}}
\]
for \( i \geq 2 \). When \( t = s+1 \), referring to the above congruence and Eq. (20), one has \( T_n^{(m)}(p-1) \equiv T_n^{(m)}(±1) \pmod{p^{s+1}} \). Therefore, congruence \( 21 \) also holds for \( t = s+1 \). The above induction completes the proof of congruence \( 21 \), which means \( T_n^{(m)}(±1) \equiv 1 \pmod{p^m} \). Consequently, the necessary part of this lemma is proved.

As for \( x \in \mathbb{Z}_p \) and \( x \not\equiv 0 \pmod{p^m} \), \( x \) can be expressed as
\[
x = \frac{y + y^{-1}}{2} \pmod{p^m}, \tag{22}
\]
where \( y = x + \omega, \ y^{-1} = x - \omega \), and \( \omega^2 = x^2 - 1 \) (mod \( p^m \)).

Now, move on to calculate \( E(2m)! \). Write the integer \( m \) as a \( p \)-adic representation \( m = \sum_{i=0}^{e} k_ip^i \), where \( k_i \in \mathbb{Z}_p \setminus \{0\} \) and \( k_i \in \mathbb{Z}_p \) for \( i \in \{0, 1, \ldots, e-1\} \).[39] Theorem 14.8. If \( m < p \), one has \( E(2m)! = 0 \). Counting the number of integers in \( \{1, 2, \ldots, m\} \) dividing \( p^v \), if \( m \geq p \), one has
\[
E(2m)! = \sum_{i=1}^{e} \left\{ \lfloor y \rfloor \mid y \equiv 0 \mod{p^i}; y = 1, 2, \ldots, m \right\} \\
= \sum_{i=1}^{e} \left( k_ip^i \right) \\
= \sum_{i=1}^{e} \left( k_ip^{i-1} + k_ip^{i-2} + \cdots + k_ip^{i-e+1} + k_e \right) \\
= k_e(p^{e-2} + k_{e-1}p^{e-3} + \cdots + k_2p^2 + k_1p) \leq m - 2.
\]

When \( x \neq 0 \), according to Eq. (22), one can set \( x = \frac{y^2 + 1}{2} \mod p^w \), where \( y \in GR^*(p^w, 2) \). From Eq. (11), one can get the following equivalent congruences:

\[
T_n(x) \equiv x \pmod{p^w}
\]

\[
\Leftrightarrow \frac{y^n + y^{-n}}{2} \equiv \frac{y + y^{-1}}{2} \pmod{p^w}
\]

\[
\Leftrightarrow y^{2n} + 1 \equiv y^{n+1} + y^{-n+1} \pmod{p^w}
\]

\[
\Leftrightarrow (y^{n-1} - 1)(y^{n+1} - 1) \equiv 0 \pmod{p^w}.
\]

In fact, congruence \((y^{n-1} - 1)(y^{n+1} - 1) \equiv 0 \pmod{p^w}\) exists if and only if \(y^{n+1} \equiv 1 \pmod{p^w}\) or

\[
\begin{align*}
(26)
\end{align*}
\]

\[
y^{n-1} &\equiv 1 \pmod{p^w}, \\
y^{n+1} &\equiv 1 \pmod{p^w - w'},
\]

where \( 1 \leq w' < w \). Assume congruence (26) holds, one can obtain \( y^{n-1} \equiv 1 \pmod{p} \) and \( y^{n+1} \equiv 1 \pmod{p} \). So, \( y^{1-n} \equiv 1 \pmod{p} \) or \( y^{2} = y^{1-n+n+1} \equiv 1 \pmod{p} \).

From \( x = \frac{y^2 + 1}{2} \mod p^w \), one has \( y^2 = 2x^2 - 1 \pm 2xw, \) where \( \omega^2 = x^2 - 1 \mod p^w \). Then, one can get \( 2x^2 - 1 \pm 2xw = 1 \pmod{p} \), which means a contradiction \( x^2 - 1 \equiv x^2 \pmod{p} \). Thus, congruence (26) does not hold and

\[
T_n(x) \equiv x \pmod{p^w} \Leftrightarrow y^{n+1} \equiv 1 \pmod{p^w}. \quad (27)
\]

From Eq. (8) and

\[
y^n \equiv \begin{cases} 
0 \pmod{p^w} & \text{if } y^{n-1} \equiv 1 \pmod{p^w}; \\
y^{-1} \pmod{p^w} & \text{if } y^{n+1} \equiv 1 \pmod{p^w},
\end{cases}
\]

one can get

\[
(28)
\]

\[
T_n'(x) = nU_{n-1}(x) = \frac{n}{y} \frac{y^n - y^{-n}}{y - y^{-1}} = \begin{cases}
n \pmod{p^w} & \text{if } y^{n-1} \equiv 1 \pmod{p^w}; \\
-n \pmod{p^w} & \text{if } y^{n+1} \equiv 1 \pmod{p^w}.
\end{cases}
\]

It means this lemma holds for \( x \in \mathbb{Z}_p \setminus \{0, p - 1\} \).

**Lemma 5.** If \( T_n(x) \equiv x \pmod{p^w} \) and \( T_n'(x) \equiv 1 \pmod{p^w} \), one has \( T_n(x + hp) \equiv T_n(x) \pmod{p^w} \), and

\[
T_n^{(m)}(x + hp) \cdot \frac{p^m}{m!} \equiv 0 \pmod{p^{w+2}}
\]

for any \( m \geq 2 \), where \( x \in \mathbb{Z}_p \) and \( h \in \mathbb{N} \).

**Proof.** When \( x \notin \{1, p - 1\} \), referring to Lemma 4, one has \( T_n'(x) \equiv \pm \tilde{n} \pmod{p^w} \), which means \( n^2 \equiv 1 \pmod{p^w} \). So, it follows from Eq. (11) that

\[
(x^2 - 1)T_n^{(2)}(x) = n^2T_n(x) - xT'_n(x)
\]

\[
\equiv (n^2 - T'_n(x)) \pmod{p^w}
\]

\[
\equiv 0 \pmod{p^w}.
\]

From \( x \notin \{p - 1, 1\} \) and the above congruence, one can get \( T_n^{(2)}(x) \equiv 0 \pmod{p^w} \). It yields from Lemma 1 that

\[
(29)
\]

\[
T_n^{(m)}(x) \equiv 0 \pmod{p^w}
\]

for any \( m \geq 2 \). Since \( T_n(x) \) is a polynomial of degree \( n \), \( T_n^{(m)}(x + hp) \) is a polynomial of degree \( n - m \), and its Taylor expansion is

\[
T_n^{(m)}(x + hp) = T_n^{(m)}(x) + \sum_{i=m+1}^{n} \frac{(hp)^{i-m}}{(i-m)!} T_n^{(i)}(x) \quad (30)
\]

Then, combining congruences (19) and (29), one can know

\[
\begin{cases}
T'_n(x + hp) \equiv T'_n(x) \pmod{p^{w+1}} \\
T_n^{(m)}(x + hp) \equiv 0 \pmod{p^w}
\end{cases}
\]

satisfies for any \( m \geq 2 \). So, this lemma holds for \( x \notin \{1, p - 1\} \) from Eq. (19).

When \( x \in \{1, p - 1\} \), combining Lemmas 2-3 and Eq. (30), one can know this lemma also holds.

**Lemma 6.** If \( T_n(x) \equiv x \pmod{p} \) and \( T_n'(x) \equiv 1 \pmod{p^t} \), one has

\[
T_n(x + hp) \equiv x + hp \pmod{p^t}, \quad (31)
\]

where \( x \in \mathbb{Z}_p, h \in \mathbb{N} \), and \( 1 \leq t \leq w + 1 \).

**Proof.** When \( h = 0 \), depending on the value of \( x \), the proof of congruence (31).

\[
T_n(x) \equiv x \pmod{p^t}, \quad (32)
\]

is divided into the following three cases:

- \( x \in \{0, 1\} \): One has \( T_n(x) = x \) from Eq. (1). So, \( T_n(x) \equiv x \pmod{p^t} \).
- \( x = p - 1 \): One has \( T_n'(x) \equiv 1 \pmod{p^t} \) from Lemma 3. Then referring to Eq. (30) and Lemma 2 one can get

\[
T_n(-1 + p) = T_n(-1) + pT'_n(-1) + \sum_{i=2}^{n} \frac{p^i}{i!} \cdot T_n^{(i)}(-1)
\]

\[
\equiv -1 + p \pmod{p^{w+1}}.
\]

So, \( T_n(p - 1) \equiv p - 1 \pmod{p^t} \).

- \( x \notin \{0, 1, p - 1\} \): One can prove congruence (32) holds via mathematical induction on \( t \). When \( t = 1 \), congruence (32) holds from \( T_n(x) \equiv x \pmod{p} \). Assume that congruence (32) holds for \( t = s \leq w \). When \( t = s + 1 \), according to Eq. (22), one can set \( x = \frac{y^2 + 1}{2} \mod p^s+1 \), where \( y \in GR^*(p^s+1, 2) \). From congruence (32) with \( w = s \) and relation (27), one has \( y^{n-1} \equiv 1 \pmod{p^s} \) or \( y^{n+1} \equiv 1 \pmod{p^s} \). Without losing the generality, assume that

\[
y^{n+1} \equiv 1 \pmod{p^s} \quad (33)
\]

From \( T_n'(x) \equiv 1 \pmod{p^s} \) and \( w \leq s \), one has \( T_n'(x) \equiv 1 \pmod{p^s} \). Then, from congruences (28) and (33), one can get \( n \equiv 1 \pmod{p^s} \). It means \( n = b \cdot p^s + 1 \), where \( b \) is a positive integer. So, \( y^b \cdot p^s \equiv y^{n-1} \equiv 1 \pmod{p^s} \) and \( \text{ord}(y)^{p^s} = b \cdot p^s \).

\[
\text{ord}(y)^{p^s} \equiv b \cdot p^s, \quad (34)
\]

From Eqs. (24) and (25), one has \( \text{ord}(y)^{p^s} = k_1\varepsilon_2 k_1 \mid (p^s - 1) \) and \( k_1 \mid p^s - 1 \). Then one can get \( k_1 \mid b \) from condition (34). Thus, \( k_1\varepsilon_2 \mid b \cdot p^s - 1 \) and \( \text{ord}(y)^{p^s} \equiv b \cdot p^{s-1} \). Referring to the definition of \( \text{ord}(y)^{p^s} \), one has

\[
\text{ord}(y)^{p^s} \equiv b \cdot p^{s-1}.
\]
\[ y^{b \cdot p^{s-1}} \equiv 1 \pmod{p^s} \]. Set \( y^{b \cdot p^{s-1}} = 1 + h_1 p^s \), where \( h_1 \) is a positive integer. Then,
\[ y^{n-1} = y^{b \cdot p^{s}} = (1 + h_1 p^s)^p \equiv 1 \pmod{p^{s+1}}, \]

From the above congruence and relation (27), one has \( T_n(x) = x \pmod{p^{s+1}} \). Therefore, congruence (32) also holds for \( t = s + 1 \). The above induction completes the proof of congruence (32) for the third case.

When \( h \neq 0 \), referring to Lemma 5 and congruence (32), one has
\[ T_n(x + hp) = T_n(x) + hpT_n'(x) + \sum_{i=2}^{n} \frac{(hp)^j}{i!} T_n^{(i)}(x) \equiv x + hp \pmod{p^{w+1}}. \]

\[ x \equiv 1 \pmod{p} \]

\[ \text{Proof.} \]

By the semi-group property of Chebyshev polynomials, one has \( T_n^N(x) = T_{n^N}(x) \). Let \( n \) in (18 Eq. (13)) be \( n^N \), one can know this lemma holds.

\begin{lemma}
For any non-negative integer \( x \) satisfying \( x \equiv 1 \pmod{p} \), one has
\[ 1 + x + x^2 + \cdots + x^{p-1} \equiv p \pmod{p^2} \] (39)
and \( p \) is the least positive integer \( j \) such that \( 1 + x + x^2 + \cdots + x^{j-1} \equiv 0 \pmod{p} \).
\end{lemma}

\[ \text{Proof.} \]

Since \( x \equiv 1 \pmod{p} \), one has \( x = c \cdot p + 1 \) and
\[ 1 + x + x^2 + \cdots + x^{p-1} = 1 + (c \cdot p + 1) + (c \cdot p + 1)^2 + \cdots + (c \cdot p + 1)^{j-1} \equiv j + c \cdot p + 2c \cdot p + \cdots + (j-1) \cdot c \cdot p \pmod{p^2} \]
\[ = j + \frac{j(j-1)}{2} c \cdot p \pmod{p^2}, \]
where \( c \) is an integer. Setting \( j = p \), one can obtain congruence (39). Furthermore, from the above congruence, one can verify that \( p \) is the least positive integer \( j \) such that
\[ 1 + x + x^2 + \cdots + x^{j-1} \equiv 0 \pmod{p} \).

\[ \text{Lemma 9.} \]

If two non-negative integers, \( x \) and \( w \), satisfy
\[ T_n^N(x) \equiv x \pmod{p^w}, \]
then
\[ (T_n^N(x))^i \equiv (T_n^N(x))^i \pmod{p} \]
hold for any positive integer \( i \).

\[ \text{Proof.} \]

Let \( n \) in (18 Lemma 6) be \( n^N \), one can get this lemma.

\[ \text{Lemma 10.} \]

The least period of sequence \( \{T_n^N(x) \pmod{p^w} \}_{i \geq 0} \)

is larger than \( N \) when
\[ k > \max\{ t \mid T_n^N(x) \equiv x \pmod{p^t} \}, \]
where \( N \) is the least period of sequence \( \{T_n^N(x) \pmod{p^w} \}_{i \geq 0} \) and \( x \in \mathbb{Z}_{p^k} \setminus \{0,1\} \).

\[ \text{Proof.} \]

Referring to the definition of \( N \), one has \( T_n^N(x) \equiv x \pmod{p^w} \) and \( T_n^N(x) = c \cdot p^w + x \), where \( c \) is an integer. Thus, one can get \( m \geq w \) and \( c = c_p \cdot p^m \), where \( m = \max\{ t \mid T_n^N(x) \equiv x \pmod{p^t} \} \) and \( \gcd(c_p, p) = 1 \).

Let \( N' \) denote the least period of sequence \( \{T_n^N(x) \pmod{p^k} \}_{i \geq 0} \). Assume \( N' < N \) when \( k > m \). Then, \( T_n^N(x) \equiv x \pmod{p^w} \), which means that \( N' \) is the period of the sequence \( \{T_n^N(x) \pmod{p^w} \}_{i \geq 0} \). But this contradicts the definition of \( N \). So, \( N' \geq N \).

Assume \( N' = N \) when \( k > m \). Then, one can get \( T_n^N(x) \equiv x \pmod{p^k} \), which contradicts \( \gcd(c_p, p) = 1 \).

Therefore, \( N' > N \), and the lemma is proved.

\[ \text{Theorem 1.} \]

Given an initial state \( x \in \mathbb{Z}_{p^k} \setminus \{0,1\} \), the least period of sequence \( \{T_n^N(x) \pmod{p^k} \}_{i \geq 0} \) is
\[ N = N_x \cdot l_x \cdot p^{k-v}, \]
where \( k \geq v \), \( N_x \) is the least period of sequence \( \{T_n^N(x) \pmod{p^k} \}_{i \geq 0} \), \( l_x = \gcd(T_n^N(x)), \) and
\[ v = \max\{ t \mid T_n^N(x) \equiv x \pmod{p^t} \}. \]
Proof. According to the permutation property of Chebyshev polynomials over ring \( \mathbb{Z}_p \) and [40] Theorem 5.1.1, one has \( T_{N_N}(x) \equiv x \pmod{p} \) for any \( x \in \mathbb{Z}_p \).

Lemma 10 gives an explicit expression of the integer \( w \), satisfying

\[
\begin{align*}
T_{N_N}(x) &\equiv x \pmod{p^w} \\
T_{N_N}(x) &\not\equiv x \pmod{p^{w+1}}
\end{align*}
\]

for any \( x \in Z_p^\times \setminus \{0, 1\} \). When \( T_{N_N}(x) \equiv 1 \pmod{p} \), namely \( l_x = 1 \), from Lemma [6] and condition [42], one has \( w \geq 2 \). When \( T_{N_N}(x) \not\equiv 1 \pmod{p} \), namely \( l_x \neq 1 \), referring to Lemma [7] and condition [42], one has

\[
T_{N_N^{-1}}(x) \equiv x + b \cdot p^w \sum_{j=0}^{l_x-1} (T_{N_N}(x))^j \pmod{p^{w+1}}.
\]

Since \( \sum_{j=0}^{l_x-1} (T_{N_N}(x))^j \pmod{p} = 0 \) from [18] Lemma 2, the above congruence becomes

\[
T_{N_N^{-1}}(x) \equiv x \pmod{p^{w+1}}.
\]

Then, as \( T_{N_N^{-1}}(x) \not\equiv x \) for all \( x \in Z_p^\times \setminus \{0, 1\} \), one can get

\[
\begin{align*}
T_{N_N^{-1}}(x) &\equiv x \pmod{p^v}, \\
T_{N_N^{-1}}(x) &\not\equiv x \pmod{p^{v+1}},
\end{align*}
\]

where \( v \geq 2 \).

According to the minimum property of \( l_x \) and condition [43], it follows that \( N_x \cdot l_x \) is the least period of the sequence \( \{T_n(x) \pmod{p^v}\}_{i \geq 0} \). To this end, by mathematical induction on \( t \), one can prove that

\[
\begin{align*}
T_{N_N^{-1}}p_i(x) &\equiv x \pmod{p^{v+t}}, \\
T_{N_N^{-1}}p_i(x) &\not\equiv x \pmod{p^{v+t+1}},
\end{align*}
\]

and \( N_x \cdot l_x \cdot p^i \) is the least integer \( i \) satisfying \( T_n(x) \equiv x \pmod{p^{v+i}} \).

First, when \( t = 0 \), the above condition is true under condition [43]. Then, assume that condition [44] holds for \( t = s \), namely

\[
\begin{align*}
T_{N_N^{-1}}p^s(x) &\equiv x \pmod{p^{v+s}}, \\
T_{N_N^{-1}}p^s(x) &\not\equiv x \pmod{p^{v+s+1}},
\end{align*}
\]

and \( N_x \cdot l_x \cdot p^s \) is the least integer \( i \) satisfying \( T_n(x) \equiv x \pmod{p^{v+s}} \). Note that congruence (38) in Lemma 7 also holds with the operation of modulo \( p^{v+s} \) if \( w \geq 2 \). Thus, when \( t = s + 1 \), let \( N = N_x \cdot l_x \cdot p^s \) in Lemma [7] one has

\[
T_{N_N^{-1}}p^{s+1}(x) \equiv x + b \cdot p^{v+s} \sum_{j=0}^{l_x-1} (T_{N_N}(x))^j \pmod{p^{v+s+2}}.
\]

It can be verified, based on Lemma [9] and the definition of \( l_x \), that

\[
T_{N_N^{-1}}p^{s+1}(x) \equiv (T_{N_N}(x))^{l_x-1} \equiv 1 \pmod{p}.
\]

From the above congruence and Lemma [8] one obtains

\[
\sum_{j=0}^{p-1} (T_{N_N^{-1}}p^{s+1}(x))^j \pmod{p^2} = p
\]

and \( p \) is the least positive integer \( h \) such that

\[
\sum_{j=0}^{h-1} (T_{N_N^{-1}}p^{s+1}(x))^j \pmod{p} = 0.
\]

Consequently, it follows from congruence [45] that

\[
\begin{align*}
T_{N_N^{-1}}p^{s+1}(x) &\equiv x \pmod{p^{v+s+1}}, \\
T_{N_N^{-1}}p^{s+1}(x) &\not\equiv x \pmod{p^{v+s+2}},
\end{align*}
\]

and \( N_x \cdot l_x \cdot p^{v+1} \) remains to be the least integer \( i \) satisfying \( T_n(x) \equiv x \pmod{p^{v+i}} \).

The above induction completes the proof of condition [44] and \( N_x \cdot l_x \cdot p^i \) is the least period of the sequence \( \{T_n(x) \pmod{p^i}\}_{i \geq 0} \). Setting \( t = v \) completes the proof of the theorem.

To verify Theorem 1, the periods of the sequence \( \{T_n(x) \pmod{p^k}\}_{i \geq 0} \) with \( (n, p) = (43, 5) \) and \((169, 7)\) are listed in Tables I and II, respectively. When \( (n, p) = (43, 5) \), for initial state \( x \in \{2, 3, 5, 7\} \), one has \( N_x = 1, l_x = 4, \) and \( v = 3 \), which means that the period of the sequence \( \{T_{43}(x) \pmod{5^k}\}_{i \geq 0} \) is \( 4 \cdot 5^{k-3} \) for any \( k \geq 3 \). Similarly, for initial state \( x \in \{2, 3, 4, 6, 7\} \), the period of the sequence \( \{T_{169}(x) \pmod{7^k}\}_{i \geq 0} \) is \( 7^{k-2} \) for any \( k \geq 2 \). Moreover, referring to the proof process of Theorem 1, one can observe the following three rules on the periodic change of Chebyshev integer sequence \( \{T_n(x) \pmod{p^k}\}_{i \geq 0} \) with the increase of parameter \( k \):

1) The period of the Chebyshev integer sequence starting from \( x \in \{0, 1\} \) remains unchanged for any \((n, p)\).
2) If \( T_{N_N}(x) \not\equiv 1 \pmod{p} \), the period of Chebyshev integer sequences increases \( l_x \) times with respect to \( k \) when it is less than a threshold corresponding to \( x \). When \( k \) is larger than another threshold, the expansion ratio becomes a fixed value \( p \). The data on \( x = 2, 3, 4, 5, 6, 7 \) shown in Table I follow such rule. Moreover, the two thresholds may be different but the period keeps unchanged between them.
3) If \( T_{N_N}(x) \equiv 1 \pmod{p} \), the period expansion ratio is a fixed value \( p \) when \( k \) is larger than a threshold of a relatively small value. The data on \( x = 2, 3, 4, 5, 6, 7 \) in Table II belong to this case.

As shown in Table II, the least period of sequence \( \{T_{43}(2) \pmod{5^k}\}_{i \geq 0} \) is \( 5^k \), which is the period of the latter of the is larger than 25. This rule is concluded in Corollary II.

**Corollary 1.** If \( N_c \geq p^2 \), then the least period of the sequence \( \{T_n(x) \pmod{p^k}\}_{i \geq 0} \) is \( N_c \cdot p^{k-u} \), for any \( k \geq u \), where \( N_c \) is the least period of sequence \( \{T_n(x) \pmod{p^u}\}_{i \geq 0} \).

**Proof.** For any \( x \in Z_p \), one has \( l_x \) and \( N_x \) in Theorem 1 satisfying \( l_x < p \) and \( N_x < p \) according to [39] Corollary 2.18 and [40] Theorem 5.1.1, respectively.

Assume that \( w \leq \max \{t \mid T_{N_N^{-1}}(x) \equiv x \pmod{p^t} \} \). Then, one has \( N_c \leq N_x \cdot l_x < p^2 \), which contradicts the given condition. So, \( w > v = \max \{t \mid T_{N_N^{-1}}p^i(x) \equiv x \pmod{p^i} \} \).

From condition [43] and the subsequent proof in Theorem 1 one can get \( N_c = N_x \cdot l_x \cdot p^{u-v} \) and the period of sequence \( \{T_n(x) \pmod{p^k}\}_{i \geq 0} \) is \( N_c \cdot p^{k-w} \).
TABLE I: The least period of sequence \( \{T^i_n(x) \mod p^k\}_{i \geq 0} \) with \((n, p) = (43, 5)\).

| Period \( x \) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---------------|---|---|---|---|---|---|---|---|
| \( T^0_{n,p} \) \( (x) \) | 2 | 4 | 3 | 3 | 4 | 2 | 4 | 3 |
| \( T^1_{n,p} \) \( (x) \) | 4 | 2 | 4 | 4 | 2 | 4 | 2 | 4 |
| \( T^3_{n,p} \) \( (x) \) | 4 | 1 | 4 | 4 | 2 | 4 | 2 | 4 |
| \( T^4_{n,p} \) \( (x) \) | 4 | 1 | 20 | 20 | 10 | 20 | 10 | 20 |
| \( T^5_{n,p} \) \( (x) \) | 5 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| \( T^6_{n,p} \) \( (x) \) | 6 | 100 | 500 | 500 | 250 | 500 | 250 | 500 |
| \( T^7_{n,p} \) \( (x) \) | 7 | 2500 | 2500 | 1250 | 2500 | 1250 | 2500 | 2500 |

TABLE II: The least period of sequence \( \{T^i_n(x) \mod p^k\}_{i \geq 0} \) with \((n, p) = (169, 7)\).

| Period \( x \) | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---------------|---|---|---|---|---|---|---|---|
| \( T^0_{n,p} \) \( (x) \) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| \( T^1_{n,p} \) \( (x) \) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| \( T^2_{n,p} \) \( (x) \) | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| \( T^3_{n,p} \) \( (x) \) | 4 | 1 | 49 | 49 | 49 | 7 | 49 | 49 |
| \( T^5_{n,p} \) \( (x) \) | 5 | 1343 | 1343 | 1343 | 49 | 1343 | 1343 |
| \( T^6_{n,p} \) \( (x) \) | 6 | 2401 | 2401 | 2401 | 343 | 2401 | 2401 |

III. FUNCTIONAL GRAPH OF CHEBYSHEV PERMUTATION POLYNOMIAL OVER RING \( \mathbb{Z}_{p^k} \)

Let \( F_{p^k} \) denote the associated functional graph of a Chebyshev permutation polynomial over \( \mathbb{Z}_{p^k} \), constructed as follows: every number in \( \mathbb{Z}_{p^k} \) is considered as a vertex, and vertex \( x \) is directly linked to vertex \( y \) if and only if \( y = T_n(x) \mod p^k \). This section introduces some basic properties of \( F_{p^k} \), and discloses evolution rules of \( F_{p^k} \) with respect to \( k \).

A. Some basic properties of \( F_{p^k} \)

As a typical example, Fig. [1] shows \( F_{p^k} \) with \((n, p) = (13, 7)\) and \( k = 1, 2, 3 \), indicating some general rules: \( F_{p^k} \) is composed of some directed cycles without any transient, as shown in Proposition [1] states \( x \) and \( p^k - x \) belong to cycles of the same length, as shown in Proposition [2] there are some self-loops (i.e., a vertex has a directed edge that links to itself) for arbitrary parameter \( k \), as shown in Proposition [3] for each cycle in \( F_p \), functional graph \( F_{p^k} \) contains a cycle of the same length when \( k \geq 2 \), as shown in Propositions [4] and [5]. In particular, there are some short cycles in \( F_{p^k} \) for any parameter \( k \), which may cause serious security pitfalls in applications using Chebyshev permutation polynomials as sources for pseudo-random number sequences and permutation vectors [3, 4].

Proposition 1. Any vertex of the functional graph of a Chebyshev permutation polynomial belongs to one and only one cycle, which composition a Chebyshev integer sequence.

Proof. According to [40] Theorem 5.1.1], when the Chebyshev polynomial \( T_n(x) \) modulo \( p^k \) satisfies the permutation condition [2], the set \( \{0, 1, \ldots, p^k - 1\} \) can be divided into some disjoint subsets such that the mappings of Chebyshev polynomial on each subset compose a directed cycle. From the definitions of the Chebyshev integer sequence, one can know each directed cycle corresponds to a Chebyshev integer sequence.

Proposition 2. For any \( x \in \mathbb{Z}_{p^k} \), if \( T_n(x) \equiv x \pmod{p^k} \), then \( T_n(p^k - x) \equiv (p^k - x) \pmod{p^k} \).

Proof. It follows from Eq. (4) and \( T_n(x) \equiv x \pmod{p^k} \) that

\[
T_n(p^k - x) = a_1(p^k - x) + a_3(p^k - x)^3 + \cdots + a_{n}(p^k - x)^n \equiv -(a_1x + a_3x^3 + \cdots + a_nx^n) \pmod{p^k}
\]

for any \( x \in \mathbb{Z}_{p^k} \).

Proposition 3. Chebyshev permutation polynomial satisfy

\[
T_n(x) \equiv x \pmod{p^k}
\]

for \( x \in \{0, \frac{1}{2}(p^k + 1)/2, (p^k - 1)/2, p - 1\} \).

Proof. From Eq. (1), the period of the sequence \( \{T_i(\frac{1}{2})\}_{i=1}^\infty \) is 6 and the sequence is

\[
\left\{1, -\frac{1}{2}, -1, -\frac{1}{2}, 1, \frac{1}{2}, \cdots\right\}.
\]

For any prime number \( p \), set \( \{p - 1, p, p + 1\} \) always contains two numbers, \( a, b \), satisfying \( 2 \mid a \) and \( 3 \mid b \). So, one obtains 6 \( \mathbb{Z}_n \) and \( (n \pmod{6}) \in \{1, 5\} \) from condition (9). Consequently, \( T_n(\frac{1}{2}) = \frac{1}{2} \) from sequence (46).

As for \( T_n(\frac{p^k + 1}{2}) = \sum_{i=1}^n \alpha_i (\frac{p^k + 1}{2})^i \), one can ensure that \( 2^{i-1} \) divides \( \alpha_i \), for any \( i \) from Eq. (45), where \( \frac{(n-m-1)!}{m!(n-2m)!} \) is an integer. Furthermore, one has

\[
T_n(\frac{p^k + 1}{2}) = \frac{p^k + 1}{2} \sum_{i=1}^n \alpha_i \frac{1}{2^{i-1}} (p^k + 1)^{i-1} \equiv \frac{p^k + 1}{2} \sum_{i=1}^n \alpha_i (p^k)^{i-1} \pmod{p^k}
\]

\[
\equiv \frac{p^k + 1}{2} \cdot T_n(\frac{1}{2}) \pmod{p^k}
\]

\[
\equiv \frac{p^k + 1}{2} \pmod{p^k}.
\]

When \( x \in \{0, 1\} \), it follows from Eq. (1) that \( T_n(x) = x \) for \( n \geq 1 \). Thus, one obtains

\[
T_n(\frac{p^k - 1}{2}) \equiv \frac{p^k - 1}{2} \pmod{p^k}
\]

and \( T_n(p^k - 1) \equiv (p^k - 1) \pmod{p^k} \) from Proposition [2].

Proposition 4. If \( T_n(x) \equiv x \pmod{p} \) and \( T_n'(x) \equiv 1 \pmod{p} \), there exists \( X_k \in \mathbb{Z}_{p^k} \) such that \( T_n(X_k) \equiv X_k \pmod{p^k} \), where

\[
X_k = \begin{cases} x & \text{if } k \leq w + 1; \\ x + \sum_{i=1}^{k-w-1} j_i p^i & \text{if } k > w + 1, \end{cases}
\]

\( k \geq 2, \ w = E(T_n'(x) - 1), j_i^* = (\alpha \cdot \frac{T_n(X_{i+w}) - X_{i+w}}{p^{w+i}}) \pmod{p} \), and \( \alpha \) is the inverse of \( \frac{T_n'(x) - 1}{p^w} \) in \( \mathbb{Z}_{p^w} \).
Proof. This proposition is proved via mathematical induction on \( k \). Since \( w = E(T'_n(x) - 1) \), one has

\[
T'_n(x) \equiv 1 \pmod{p^w}
\]

and

\[
T'_n(x) = 1 + dp^w,
\]

where \( d \mod p \neq 0 \). It yields from Lemma [6] that \( T_n(x) \equiv x \pmod{p^k} \) for \( k \leq w + 1 \), which means this proposition holds for \( k \leq w + 1 \). Assume that this proposition holds for \( k = s > w + 1 \), namely \( T_n(X_s) \equiv X_s \pmod{p^{s'}} \), where \( X_s = x + \sum_{i=1}^{s-w-1} j^i \cdot p^i \). Set

\[
T_n(X_s) = X_s + h_s p^s,
\]

where \( h_s \) is an integer. Referring to congruence \([47]\) and Lemma [5] one has

\[
T_n'(X_s) \equiv T'_n(x) \pmod{p^{w+1}}
\]

and

\[
\frac{T_n^{(m)}(X_s) \cdot p^m}{m!} \equiv 0 \pmod{p^{w+2}}
\]

for \( m \geq 2 \). When \( k = s + 1 \), one can calculate

\[
T_n(X_s + j_{s-w} p^{s-w})
\]

\[
= T_n(X_s) + \sum_{m=1}^{n} \frac{(j_{s-w} p^{s-w})^m}{m!} T_n^{(m)}(X_s)
\]

\[
= T_n(X_s) + \sum_{m=1}^{n} \frac{(j_{s-w} p^{s-w-1})^m \cdot p^m}{m!} T_n^{(m)}(X_s)
\]

from Eq. [5]. Substituting Eqs. [48], [49], and congruences \([50], [51]\) into the above equation, one has

\[
T_n(X_s + j_{s-w} p^{s-w})
\]

\[
\equiv X_s + h_s p^s + j_{s-w} p^{s-w} T_n'(x) \pmod{p^{s+1}}
\]

\[
\equiv X_s + h_s p^s + j_{s-w} p^{s-w} (1 + d^s \cdot p^w) \pmod{p^{s+1}}
\]

\[
\equiv X_s + j_{s-w} p^{s-w} + (h_s + d \cdot j_{s-w}) p^s \pmod{p^{s+1}}.
\]

Thus, when \( j^s = \left( \frac{T_n(X_s) - X_s}{p^w} \cdot d^w \right) \mod p \) and \( X_{s+1} = X_s + j_{s-w} p^{s-w} \), one has \( T_n(X_{s+1}) \equiv X_s + j_{s-w} p^{s-w} \pmod{p^{s+1}} \). Therefore, this proposition also holds for \( k = s + 1 \). The above induction completes the proof of the proposition.

Proposition 5. If \( T_n(x) \equiv x \pmod{p} \) and \( T'_n(x) \not\equiv 1 \pmod{p} \), there is only one element in \( \mathbb{Z}_{p^k} \), \( X_k \), such that
$X_k \mod p = x$ and $T_n(X_k) \equiv X_k \mod p^k$, where

$$X_k = x + \sum_{i=1}^{k-1} j_i p^i,$$

$k \geq 2$, $j_i^* = (\beta \cdot \frac{T_n(X_i) - X_i}{p^i}) \mod p$, and $\beta$ is the inverse of $(1 - T_n(x))$ in $\mathbb{Z}_p$.

**Proof.** This proposition is proved via mathematical induction on $k$. When $k = 1$, this proposition holds from $T_n(x) \equiv x \mod p$. Assume that this proposition holds for $k = s$, namely $T_n(X_s) \equiv X_s \mod p^s$, where $X_s = x + \sum_{i=1}^{s-1} j_i^* p^i$. Set

$$T_n(X_s) = X_s + h_s p^s,$$

where $h_s$ is an integer. When $k = s + 1$, from Eqs. (5) and (6), one can get

$$T_n(X_s + j_s p^s) \equiv T_n(X_s) + j_s p^s \cdot T_n(0) \equiv T_n(X_s) + j_s p^s \cdot T_n(x) \mod p^{s+1}.$$

Substituting Eq. (52) and $d = T_n(x) \mod p$ into the above congruence, one has

$$T_n(X_s + j_s p^s) \equiv X_s + (h_s + dj_s) p^s \mod p^{s+1}.$$

Thus, if and only if $j_s^* = ((1 - d)^{-1} \cdot \frac{T_n(X_s) - X_s}{p^s}) \mod p$, one has $T_n(X_s + j_s^* p^s) \equiv X_s + j_s^* p^s \mod p^{s+1}$. Let $X_{s+1} = X_s + j_s^* p^s$, then $X_{s+1} \mod p = x$ and $T_n(X_{s+1}) \equiv X_{s+1} \mod p^{s+1}$. Therefore, this proposition also holds for $k = s + 1$. The above induction completes the proof of the proposition.

**B. Evolution rules of $F_{p^k}$ with respect to $k$**

This subsection deals with how the graph structure of Chebyshev permutation polynomial changes with parameter $k$. From numerous experiments about the graph structure of Chebyshev permutation polynomials with random parameters, it is found that the cycle distribution of $F_{p^k}$ is very regular with increase of $k$. As shown in Table III, the number of cycles with period $T_c$ in $F_{p^k}$ is equal to that with period $p \cdot T_c$ in $F_{p^{k+1}}$ when $T_c \geq p^2$, which is summarized in Theorem 3.

| $N_{T_c,k}$ | 1 | 2 | 7 | 14 | 49 | 98 | 343 | 686 | 2401 | 4802 |
|-------------|---|---|---|---|----|----|-----|-----|------|------|
| $k$         | 1 | 5 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
|             | 2 | 5 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
|             | 3 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
|             | 4 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
|             | 5 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
|             | 6 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |

**Theorem 2.** Let $N_{x,y}$ denote the number of cycles with period $x$ in the functional graph of Chebyshev permutation polynomials over $\mathbb{Z}_{p^r}$. Then, one has

$$N_{p \cdot T_c,k+1} = N_{T_c,k},$$

where $T_c \geq p^2$.

**Proposition 6.** The connected components of $F_{p^k}$, to which all states $X$ satisfying $(X \mod p) \in \{T_n^p(x) \mod p \}_{j=0}^{N_{x,y} - 1}$ belong, are composed of $(p-1)p^{i-1}$ cycles of length $N_{x,z_p} p^i$, $p^{w-1}$ cycles of length $N_{x,k}$, and one cycle of length $N_{e}$ when $k > w + 1$; $p^{w-1}$ cycles of length $N_{x,z_p}$ and one cycle of length $N_{e}$ otherwise, where $x \in \mathbb{Z}_p$, $T_n^{N_x} (x) \equiv x \mod p$, $l_x = \text{ord}(T_n^{N_x},\mathbb{Z}_p)$, $w = \text{max} \{ t \mid T_{n \cdot l_x} (x) \equiv 1 \mod p^t \}$, and $i \in \{1, 2, \ldots, k - w - 1\}$.

**Proof.** When $N_{x} = 1$, from the definition of $w$, one has

$$\begin{cases} T_{n \cdot l_x}(x) \equiv 1 \mod p^w; \\ T_{n \cdot l_x}(x) \not\equiv 1 \mod p^{w+1}. \end{cases}$$

(53)
Fig. 2: The cycles distribution of the Chebyshev polynomial $T_n(x)$ over $\mathbb{Z}_{p^k}$, $k = 1 \sim 11$: a) $(n, p) = (13, 7)$; b) $(n, p) = (43, 5)$; c) $(n, p) = (19, 7)$; d) $(n, p) = (443, 5)$.

Since $T_n(x) \equiv x \pmod{p}$, $T^p_{n'}(x) = T^n_{n'}(x) \equiv x \pmod{p}$. Setting $n = n^{l_x}$ in Lemmas 5 and 6 from condition $53$, one has $T^m_{n^{l_x}}(x) \equiv x \pmod{p^{w+1}}$.

\[ T_{n^{l_x}}(x) \equiv T^l_{n^{l_x}}(x) \pmod{p^{w+1}}, \quad (54) \]

and

\[ \frac{T^{(m)}(x) \cdot p^m}{m!} \equiv 0 \pmod{p^{w+2}} \quad (55) \]

for $m \geq 2$, where $X \equiv x \pmod{p}$. Setting $n = n^{l_x}$ in Eq. (5), one can get

\[ T_{n^{l_x}}(x + jp^i) = T_{n^{l_x}}(x) + \sum_{m=1}^{n^{l_x}} \frac{(jp^i)^m}{m!} T^{(m)}_{n^{l_x}}(x) \]

\[ = T_{n^{l_x}}(x) + \sum_{m=1}^{n^{l_x}} \frac{(jp^i-1)^m \cdot p^m}{m!} T^{(m)}_{n^{l_x}}(x), \]

where $i$ and $j$ are integers. Substituting congruences (54) and (55) into the above equation, one has

\[ T_{n^{l_x}}(x + jp^i) \equiv T_{n^{l_x}}(x) + jp^i T^l_{n^{l_x}}(x) \pmod{p^{w+i+1}} \quad (56) \]

for $i \geq 1$. Depending on the value of $l_x$, the proof is divided into the following two cases:

- $l_x = 1$: Referring to Proposition 4, one can know that there exists $X_k \in \mathbb{Z}_{p^k}$ such that $X_k \equiv x \pmod{p}$ and

\[ T_n(X_k) \equiv X_k \pmod{p^k}. \quad (57) \]

Specially, when $k \leq w + 1$, $X_k = x$. Let $j$ go through $\mathbb{Z}_{p^{k-w} - 1}$, $X = x$, and $i = 1$ in congruence (56). From condition 53 and congruence (57), one obtains

\[ T_n(x + j) \equiv T_n(x + j p^i) \equiv x + j p^i T_n(x) \pmod{p^{w+2}} \equiv x + j p^i \pmod{p^k}. \]

Thus, when $k \leq w + 1$, all states $X$ satisfying $X \equiv x \pmod{p}$ in $F_{p^k}$ make up $p^{k-1}$ self-loops.

When $k > w + 1$, let $j$ go through $\mathbb{Z}_{p^{w} - 1}$, $X = X_k$ and $i = k - w$ in congruence (56), it yields from condition (53) that

\[ T_n(X_k + j p^{k-w}) \equiv T_n(X_k + j p^{k-w} T_n(x)) \ \pmod{p^{k+1}} \equiv X_k + j p^{k-w} \pmod{p^k}. \quad (58) \]

It means that all states $X$ satisfying $(X - X_k) \equiv 0 \pmod{p^{k-w}}$ in $F_{p^k}$ make up $p^w$ self-loops. In addition, from condition (53) and congruence (56), one has

\[ T_n(X_k + j_1 p^i) \equiv X_k + j_1 p^i \pmod{p^{w+i+1}}, \]

\[ T_n(X_k + j_1 p^i) \neq X_k + j_1 p^i \pmod{p^{w+i+1}}, \quad (59) \]

where $1 \leq i \leq k - w - 1$ and $j_1 \pmod{p} \neq 0$. Since $X_k + j_1 p^i \in \mathbb{Z}_{p^{k-1}}$, one has $j_1 \in \mathbb{Z}_{p^{k-1}}$. According to Theorem 1 and condition (59), one has the least period of sequence $\{T^t_n(X_k + j_1 p^i) \pmod{p^k} \}_{t \geq 0}$ is $p^{k-w-1}$. It yields from $j_1 \in \mathbb{Z}_{p^{k-1}}$ that the number of states of period $p^{k-w-1}$ is $|\mathbb{Z}_{p^{k-1}}|$. So, all states $X$ satisfying $(X - X_k) \pmod{p^w} = 0$ and $(X - X_k) \pmod{p^w} \neq 0$ in $F_{p^k}$ make up

\[ \frac{|\mathbb{Z}_{p^{k-1}}|}{p^{k-w-1}} = \frac{(p-1)p^{k-1-1}}{p^{k-w-1}} = (p-1)\frac{p}{p^{k-w-1}} \]
cycles of length $k^{w-1}$.

- $l_x \neq 1$: From Proposition 5 one can know there is only one possible value of $X_k$ satisfying congruence (57), which means there is only one self-loop in $F_{r_k}$. When $k \leq w + 1$, let $X = X_0$ and $i = 1$ in congruence (56), from condition (53), one has

$$T_n(x_j + jp) = T_n(x_j + jp) \pmod{p^{w+2}}$$

where $j \in \mathbb{Z}_{p^{k-1}} \setminus \{0\}$. Thus, when $k \leq w + 1$, all states $X$ satisfying $(X - X_0) \equiv 0 \pmod{p}$ make up $k^{w-1}$ cycles of length $l_x$ and one self-loop.

When $k > w + 1$, similar to congruence (58) and condition (59), one can get

$$T_n'(x_j + j p^{k-w}) \equiv X_j \cdot p^{k-w} \pmod{p^k} \quad (60)$$

and

$$\begin{cases} T_n'(x_j + j p^i) \equiv X_j + j p^i \pmod{p^{w+i}}; \\ T_n'(x_j + j p^{i+1}) \equiv X_j + j p^{i+1} \pmod{p^{w+i+1}}, \end{cases}$$

where $j \in \mathbb{Z}_{p^{w-1}} \setminus \{0\}$ and $j_1 \in \mathbb{Z}_{p^{w-1}}$. From congruence (60), one has all states $X$ satisfying $(X - X_0) \equiv 0 \pmod{p}$ make up $k^{w-1}$ cycles of length $l_x$ and one self-loop. According to Theorem 1 and condition (61), one has the least period of sequence $\{T_n'(x_j + j p^i) \equiv X_j \pmod{p^k}\} \geq 0$, it yields from $j_1 \in \mathbb{Z}_{p^{w-1}}$, that the number of states of period $l_x \cdot k^{w-1}$ is $|Z_{p^{w-1}}|$. So, all states $X$ satisfying $(X - X_0) \equiv 0 \pmod{p}$ make up

$$\frac{|Z_{p^{w-1}}|}{l_x \cdot k^{w-1}} = \frac{(p-1)p^{k-1}-1}{l_x \cdot k^{w-1}}$$

cycles of length $l_x \cdot k^{w-1}$. In either case, this proposition both holds for $N_x = 1$.

When $N_x \neq 1$, the proof is similar to the case $N_x = 1$ by replacing $n$ with $N_x$.

As a typical example, when $(n, p) = (13, 7)$ and $x = 2$, one can calculate $N_x = 2$, $l_x = 1$, $\{T_n'(2) \pmod{7}\} = \{2, 5\}$, and $w = \max\{t | T_{n_2}(2) \equiv 1 \pmod{7^t}\} = 1$. As shown in the solid rectangle box in Fig. 1 all states $X$ satisfying $X \equiv 0 \pmod{7^2}$ in $F_{r_7}$ make up six cycles of length 14 and seven cycles of length two. When $x = 0$, one can calculate $N_x = 1$, $l_x = 2$, $\{T_n'(0) \pmod{7}\} = \{0\}$, and $w = \max\{t | T_{n_2}(0) \equiv 0 \pmod{7^t}\} = 1$. As shown in the dashed rectangle box in Fig. 1 all states $X$ satisfying $X \equiv 0 \pmod{7^2}$ in $F_{r_7}$ make up three cycles of length 14, three cycles of length two and one self-loop. The results are consistent with Proposition 5.

Lemma 11. If $T_{n,N_x,i}(x) \equiv x \pmod{p^w}$, then

$$T_{n,N_x,i}(x) \equiv (T_n(x) \pmod{p^w})$$

where $x \in \mathbb{Z}_{p^t} \setminus \{0\}$.

Proof. When $x = 0, N_x = 1$, and $T_n'(0) = (-1)^{\frac{1}{2}} n$ and $T_{n,u}(0) = (-1)^{\frac{1}{2}} n^{u-1}$. Since $n$ is odd, $l_0 = \sum_{i=0}^{l_0-1} n^i$ (mod 2). It means $\frac{n-1}{2} \cdot l_0 \equiv \frac{n-1}{2} (\sum_{i=0}^{l_0-1} n^i) \equiv \frac{n^{l_0-1}}{2}$ (mod 2). Thus,$$(T_n'(0))^i \equiv (-1)^{l_0} (-1)^{\frac{n-1}{2} \cdot n^i} \equiv \frac{n^{l_0}}{2}$$

and the lemma holds for $x = 0$.

When $x \neq 0$, referring to $T_{n,N_x,i}(x) \equiv x \pmod{p^w}$ and relation (27),

$$y_n^{N_x+\pm1} \equiv 1 \pmod{p^w}, \quad (62)$$

where $x = \pm 1 \pmod{p^w}$. From the definition of $N_x$, one has $T_{n,N_x}(x) \equiv T_{n,N_x}(x) \pmod{p^w}$. It yields from relation (27) and congruence (28) that $y_n^{N_x \pm 1} \equiv 1 \pmod{p^w}$ and

$$T_{n,N_x}(x) \equiv \begin{cases} n_x \pmod{p} \text{ if } y_n^{N_x} \equiv 1 \pmod{p}; \\ -n_x \pmod{p} \text{ if } y_n^{N_x} \equiv 1 \pmod{p}. \end{cases} \quad (63)$$

According to congruence (63), the proof of the lemma is divided into the following two cases:

- $T_{n,N_x}(x) \equiv n_x \pmod{p}$: One has $y_n^{N_x} \equiv 1 \pmod{p}$. Since $(n_x - 1) | (n_x l_x - 1)$, $y_n^{N_x l_x - 1} \equiv 1 \pmod{p}$. Then one can get $y_n^{N_x l_x - 1} \equiv 1 \pmod{p^w}$ from congruence (62). It yields from congruence (28) that $T_{n,N_x}(x) \equiv n_x \pmod{p^w}$.

- $T_{n,N_x}(x) \equiv -n_x \pmod{p}$: One has $y_n^{N_x} \equiv 1 \pmod{p}$. Furthermore,

$$\begin{cases} (n_x + 1) | (n_x l_x + 1) \text{ if } l_x \text{ is odd}; \\ (n_x + 1) | (n_x l_x - 1) \text{ if } l_x \text{ is even}. \end{cases} \quad (64)$$

It follows from congruence (62) and congruence (64) that

$$y_n^{N_x l_x - 1} \equiv 1 \pmod{p^w} \text{ if } l_x \text{ is odd}; \quad y_n^{N_x l_x - 1} \equiv 1 \pmod{p^w} \text{ if } l_x \text{ is even.}$$

Then referring to congruence (28), one has

$$T_{n,N_x,i}(x) \equiv -n_x \pmod{p^w} \text{ if } l_x \text{ is odd}; \quad T_{n,N_x,i}(x) \equiv n_x \pmod{p^w} \text{ if } l_x \text{ is even.}$$

In all, the lemma holds for either case.

Lemma 12. If $n, k_2 \equiv 1 \pmod{p^u}$ and $k_1 \equiv 1 \pmod{p}$, then $n^{k_1} \equiv 1 \pmod{p^u}$, where $k_1, k_2, w$ are integers and $k_2 \pmod{p} \neq 0$.

Proof. Let $n^{k_1} = 1 + hp$, where $h$ is an integer. Then,

$$n^{k_1}k_2 = (1 + hp)k_2 = 1 + \sum_{i=1}^{k_2} \binom{k_2}{i} (hp)^i$$

$$= 1 + (hp) \cdot (k_2 + \sum_{i=2}^{k_2} \binom{k_2}{i} (hp)^{i-1}).$$

Since $n^{k_1} - 1 \equiv 1 \pmod{p^u}$ and the above equation, one has $p^u \mid (hp) \cdot (k_2 + \sum_{i=2}^{k_2} \binom{k_2}{i} (hp)^{i-1})$. As $p \nmid k_2$ and
According to Lemma 13, the necessary and sufficient parts of this lemma are equivalent for $x \in \{1, p - 1\}$. When $x \notin \{1, p - 1\}$, from Lemma 11 and congruence (63),

$$T'_{n,N_x} (x) \equiv (T'_n N_x (x) \mod p)^{|x|} \equiv \pm |N_x|^{1/2} \mod p.$$

Without loss of generality, here we only present the proof for the case $T'_{n,N_x} (x) \equiv -N_x (\mod p)$. Let $l = \text{ord}(N_x)$, one has $\left(\frac{N_x}{l}\right)^l \equiv 1 (\mod p)$ and $\left(-\frac{N_x}{l}\right)^{2l} \equiv 1 (\mod p)$. Then from $l_x = \text{ord}(T'_n N_x) = \text{ord}(-N_x)$, one can get $l_x \mid 2l$. Referring to Theorem 1.15, one obtains

$$l = \frac{\text{ord}(n^2)}{\text{gcd}(N_x, \text{ord}(n^2))} \quad \text{and} \quad \text{ord}(n^2) = \frac{\text{ord}(n)}{\text{gcd}(2, \text{ord}(n))}.$$

It means

$$l = \begin{cases} \frac{\text{ord}(n^2)}{2} & \text{if ord}(n) \text{ is odd;} \\ \frac{\text{ord}(n^2)}{k} & \text{if ord}(n) \text{ is even}, \end{cases} \quad (65)$$

where $k = \text{gcd}(N_x, \text{ord}(n))$.

If $T'_{n,N_x} (x) \equiv 1 (\mod p)$, one has $\left(\frac{-N_x}{l}\right)^{2l} \equiv 1 (\mod p)$.

Combining Eq. (65), one has

$$\begin{cases} n^{\text{ord}(n^2)/2} \equiv 1 (\mod p) & \text{if ord}(n) \text{ is odd;} \\ n^{\text{ord}(n^2)/k} \equiv 1 (\mod p) & \text{if ord}(n) \text{ is even}. \end{cases} \quad (66)$$

From the definition of $N_x$, one has $N_x \mod p \neq 0$. Then, according to $n^{\text{ord}(n^2)/2} \equiv 1 (\mod p)$ and Lemma 12, one has

$$n^{\text{ord}(n^2)/k} \equiv 1 (\mod p). \quad (67)$$

So, the necessary part of this lemma is proved for $x \in \{1, p - 1\}$. If $n^{\text{ord}(n^2)/k} \equiv 1 (\mod p)$, then congruences (66), (67) hold. Since $l_x \mid 2l$ and $l \mid p$, one has $2l = l_x \cdot h$ and $h \mod p \neq 0$. Thus, congruence (66) becomes

$$\left(\frac{-N_x}{l}\right)^{2l} \equiv 1 (\mod p).$$

Then, according to $\left(\frac{-N_x}{l}\right)^{1/2} \equiv 1 (\mod p)$ and Lemma 12, one has $\left(\frac{-N_x}{l}\right)^{1/2} \equiv 1 (\mod p)$, which means

$$T'_{n,N_x} (x) \equiv \left(\frac{-N_x}{l}\right)^{1/2} \equiv 1 (\mod p).$$

Consequently, the sufficient part of this lemma is proved for $x \in \{1, p - 1\}$.

**Theorem 3.** The number of cycles of length $T_x$ in the functional graph of the Chebyshev permutation polynomial $T_x(n)$ over $\mathbb{Z}_p$, $N_{T_x,k}$, is a constant when $k > k_x$, i.e.

$$N_{T_x,k} = N_{T_x,k_x}.$$
polynomials over various algebraic domains, such as ring $\mathbb{Z}/n\mathbb{Z}$, where $N = p_1^{e_1}p_2^{e_2} \cdots p_n^{e_n}$ is a general composition, $p_i$ is a prime number and $e_i$ is a positive integer.

REFERENCES

[1] P. Butzer and F. Jongmans, "P. L. Chebyshev (1821–1894): a guide to his life and work," Journal of Approximation Theory, vol. 96, no. 1, pp. 111–138, 1999.
[2] T. Lee and J. Jeng, "The Chebyshev-polynomials-based unified model neural networks for function approximation," IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 28, no. 6, pp. 925–935, 1998.
[3] N. sheng Liu, "Pseudo-randomness and complexity of binary sequences generated by the chaotic system," Communications in Nonlinear Science and Numerical Simulation, vol. 16, no. 2, pp. 761–768, 2011.
[4] C.-C. Chen, K. Yao, K. Uneno, and E. Biglieri, "Design of spread-spectrum sequences using chaotic dynamical systems and ergodic theory," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 48, no. 9, pp. 1100–1114, 2001.
[5] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 824–839, 2018.
[6] D. Yoshioka, Y. Dainobu, K. Tan, and B. Feng, "Periodic properties of Chebyshev polynomials modulo $p$," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 63, no. 8, pp. 778–782, 2016.
[7] L. Zhang, W. Gao, S. Chen, W. Ren, K.-K. R. Choo, and N. N. Xiong, "The graph structure of the generalized discrete Arnold’s Cat map," IEEE Transactions on Information Theory, vol. 58, no. 1, pp. 445–452, 2012.
[8] C. Qureshi and D. Panario, "Rede actions on finite fields and multiplication map in cyclic group," SIAM Journal on Discrete Mathematics, vol. 29, pp. 1486–1503, 2015.
[9] Z.-X. Wan, "Introduction to finite fields and their applications," 3rd ed. Springer, 2012.
[10] M. Nikooghadam, "Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections," Dependable and Secure Computing, vol. 16, no. 2, pp. 761–768, 2011.
[11] Z. Chang, Q. Wang, and W. Jiang, "Cycle structure of LFSR with arbitrary characteristic polynomial over finite fields," Cryptography and Communications, vol. 10, no. 6, pp. 1183–1202, 2018.
[12] Z. Chang, G. Gong, and Q. Wang, "Cycle structures of a class of cascaded FSRs," IEEE Transactions on Information Theory, vol. 64, no. 2, pp. 1376–1377, 2019.
[13] C. Li, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold Cat map for $n = 2^k$," IEEE Transactions on Information Theory, vol. 58, no. 1, pp. 143–149, 2012.
[14] Z. Zhang, S. Chen, S. Ma, Z. Qiu, B. Zhu, Z. Xiao, and M. Liu, "A low complexity and long period digital random sequence generator based on residue number system and permutation polynomial," IEEE Transactions on Computers, vol. 71, no. 11, pp. 2008–2017, 2022.
[15] S. Chatterjee, S. Roy, A. K. Das, S. Chattopadhyay, N. Kumar, and A. V. Vasilakos, "Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment," IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 824–839, 2018.
[16] D. Yoshioka, Y. Dainobu, K. Tan, and B. Feng, "Periodic properties of Chebyshev polynomials modulo $p$," IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 63, no. 8, pp. 778–782, 2016.
[17] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev polynomials," IEEE Transactions on Computers, vol. 54, no. 9, pp. 4388–4397, 2005.
[18] A. Iwasaki and K. Uneno, "Three theorems on odd degree Chebyshev polynomials and more generalized permutation polynomials over a ring of module $2^n$", Japan Journal of Industrial and Applied Mathematics, vol. 35, pp. 49–69, 2018.
[19] [20] R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications," 2nd ed. Cambridge, UK: Cambridge University Press, 1994.
[21] [22] C. Li, K. Tan, B. Feng, and J. Lu, "The graph structure of the generalized discrete Arnold’s Cat map," IEEE Transactions on Computers, vol. 71, no. 2, pp. 364–377, 2022.
[23] X. Lu, E. Y. Xie, and C. Li, "Periodicity analysis of Logistic map over ring $\mathbb{Z}_p$," International Journal of Bifurcation and Chaos, vol. 33, no. 5, p. art. no. 2350063, 2023.
[24] C. Li, K.-W. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold Cat map for $n = 2^k$," IEEE Transactions on Information Theory, vol. 58, no. 1, pp. 445–452, 2012.
[25] C. Qureshi and D. Panario, "Rede actions on finite fields and multiplication map in cyclic group," SIAM Journal on Discrete Mathematics, vol. 29, pp. 1486–1503, 2015.
[26] Z. Zhang, S. Chen, S. Ma, Z. Qiu, B. Zhu, Z. Xiao, and M. Liu, "A low complexity and long period digital random sequence generator based on residue number system and permutation polynomial," IEEE Transactions on Computers, vol. 71, no. 11, pp. 2008–2017, 2022.
[27] Z. Chang, M. F. Ezzerman, S. Ling, and H. Wang, "The cycle structure of LFSR with arbitrary characteristic polynomial over finite fields," Cryptography and Communications, vol. 10, no. 6, pp. 1183–1202, 2018.
[28] Z. Chang, G. Gong, and Q. Wang, "Cycle structures of a class of cascaded FSRs," IEEE Transactions on Information Theory, vol. 66, no. 2, pp. 3766–3774, 2020.
[29] C. Qureshi and D. Panario, "Rede actions on finite fields and multiplication map in cyclic group," SIAM Journal on Discrete Mathematics, vol. 29, pp. 1486–1503, 2015.
[30] Z. Zhang, S. Chen, S. Ma, Z. Qiu, B. Zhu, Z. Xiao, and M. Liu, "A low complexity and long period digital random sequence generator based on residue number system and permutation polynomial," IEEE Transactions on Computers, vol. 71, no. 11, pp. 2008–2017, 2022.