2022 International Symposium on Nonlinear Theory and Its Applications,
NOLTA2022, Virtual, December 12-15, 2022

Investigations of degree period of commutative polynomials defined by fourth-order recurrence relations with two variables over Z_{2^k}

Takuma Nishizaka† and Daisaburo Yoshioka‡

†Division of Applied Information Sciences, Sojo University,
‡Department of Computer and Information Sciences, Sojo University,
4-22-1 Ikeda, Nishi-Ku, Kumamoto, Japan
Email: g2211m11@m.sojo-u.ac.jp, yoshioka@cis.sojo-u.ac.jp

Abstract– In recent years, a public-key cryptosystem based on Chebyshev polynomials over Z_{2^k} has been presented. Unfortunately, however, the cryptosystem is broken using knowledge of the periodic properties of Chebyshev polynomials. Although commutative polynomials with two variables can be candidates for the cryptosystem instead of Chebyshev polynomials, the periodic properties of the polynomials should be discussed carefully. In this study, we investigated the degree period of commutative polynomials with two variables over residue ring Z_{2^k}.

1. Introduction

Since the first idea of public-key cryptosystems was introduced by Diffie and Hellman, various public-key cryptosystems have been proposed [1], [2]. In constructing public-key cryptosystems, the commutative property is an essential characteristic. A pure monomial x^n, which appears in the Diffie–Hellman key exchange and RSA algorithms, and Chebyshev polynomials $T_n(x)$ are the only classes of commutative polynomials [3].

Generally, public-key encryptions, such as RSA, are defined over a finite field or finite ring of a large number, which incurs computational cost. When the ring is Z_{2^k}, the remainder operation is equivalent to simply taking the least significant bits, the computational cost of which is negligible. Therefore, a public-key cryptosystem over the ring of Z_{2^k} is very attractive. However, the discrete logarithm problem of x^n over the ring is solved in polynomial time using the Pohlig–Hellman algorithm [4]. A public-key cryptosystem using Chebyshev polynomials over Z_{2^k} has been introduced in [5] as a candidate for such cryptosystems. The cryptosystem can be viewed as chaos-based cryptography because Chebyshev polynomials are a class of well-known chaotic mappings. Due to the sensitive dependence on initial conditions, chaotic systems often exhibit random-like behavior, which makes them popular candidates for building blocks of cryptosystems. However, the cryptosystem has been cryptanalyzed and shown to be insecure [6], which also means that we need commutative polynomials with at least two variables to construct public-key cryptography over Z_{2^k}.

ORCID iDs First Author: 0000-0003-1834-8585,
Second Author: 0000-0001-8322-0938

In recent years, high-dimensional commutative polynomials defined by recurrence relations as extended Chebyshev polynomials have been proposed [7]. The cryptosystem using Chebyshev polynomials has been cryptanalyzed based on knowledge of periodic properties of Chebyshev polynomials over finite sets. It can be presumed from this fact that periodic properties of polynomials may be helpful in the analysis of cryptosystems. Therefore, investigation of the period is very important.

In this study, we clarify some properties of the degree period of commutative polynomials with two variables over the ring Z_{2^k}.

2. Period of linear recurrence relation

For convenience, we briefly introduce a linear recurrence sequence and its period.

Let $n \geq 0$ and $k \geq 1$ be integers. The set $Z_{2^k} = \{0,1,\dots,2^k-1\}$ is defined as the set of remainders of all integers modulo 2^k that forms a ring with respect to addition and multiplication. Let $Z_{2^k}[t]$ be a set of polynomials whose coefficients are the elements in Z_{2^k}. For $a(t), b(t) \in Z_{2^k}[t]$,

$$a(t) \equiv b(t) \bmod (g(t), 2^k) \tag{1}$$

means that there exists $h_1(t), h_2(t)$ such that

$$a(t) - b(t) = h_1(t)g(t) + h_2(t)2^k \tag{2}$$

An n-th order recursive recurrence formula over Z_{2^k}

$$a_{i+n} \equiv -\sum_{j=0}^{n-1} c_j a_{i+j} \bmod 2^k \tag{3}$$

can generate a periodic sequence $\alpha = \{a_i\}_{i=0}^{\infty}$ from an initial value $(a_0, a_1, \dots, a_{n-1})$. From the above formula,

$$f(t) = t^n + \sum_{j=0}^{n-1} c_j t^j \tag{4}$$

is called a characteristic polynomial, and we define the binary expansion of $f(t)$ as

$$f(t) = \sum_{i-0}^{k-1} f_i(t)2^k \tag{5}$$

Let T be the minimum positive integer such that

$$t^{T+i} \equiv t^i \bmod (f_0(t), 2) \tag{6}$$

Equation (6) also means that $f_0(t)$ divides t^T-1 mod 2. $T = \mathrm{per}(f_0)$ denotes the period of $f_0(t)$. The sequence period of α is given by the following theorem.

Lemma 1[8] Let $\alpha = \{a_i\}_{i=0}^{\infty}$ be an integer sequence generated by (3) and $f(t)$ be its characteristic function. The period of α is a divisor of $2^{k-1}\mathrm{per}(f_0)$.

In other words, the sequence period of α is given by the period of the characteristic function $f(t)$.

3. Degree period of commutative polynomials with two variables over Z_{2^k}

3.1 Definition

The Chebyshev polynomial is defined by the third-order linear recurrence relation, that is,

$$C_0(x) = 1 \quad (7)$$

$$C_1(x) = x \quad (8)$$

$$C_n(x) = xC_{n-1}(x) - C_{n-2}(x) \quad (9)$$

The Chebyshev polynomials have a commutative property, which is given by

$$C_n\big(C_m(x)\big) = C_m\big(C_n(x)\big) = C_{nm}(x) \quad (10)$$

This property enables us to construct public-key cryptosystems.

In [7], high-dimensional commutative polynomials were proposed as extended Chebyshev polynomials. One was obtained by fourth order recurrence relations with two variables x, y using the following equations:

$$T_0(x,y) = (3,3) \quad (11)$$

$$T_1(x,y) = (x,y) \quad (12)$$

$$T_2(x,y) = (x^2 - 2y, y^2 - 2x) \quad (13)$$

$$T_3(x,y) = (x^3 - 3xy + 3, y^3 - 3xy + 3) \quad (14)$$

$$T_m(x,y) = \begin{pmatrix} xT_{m-1,1}(x,y)_x - yT_{m-2,1}(x,y)_x \\ +T_{m-3},1(x,y)_x, \\ yT_{m-1,2}(x,y)_y - xT_{m-2,2}(x,y)_y \\ +T_{m-3,2}(x,y)_y \end{pmatrix}, \quad (15)$$

where m is a degree of the polynomials. In the definition, when $T_m(x,y) = (a,b)$, we define $T_{m,1}(x,y) = a, T_{m,2}(x,y) = b$.

These polynomials are commute under compositions as with the Chebyshev polynomial, that is,

$$T_m\big(T_n(x,y)\big) = T_n\big(T_m(x,y)\big) = T_{nm}(x,y) \quad (16)$$

The recurrence equation (15) can be rewritten as a matrix equation as follows:

$$\begin{bmatrix} T_{m,1}(x,y) \\ T_{m-1,1}(x,y) \\ T_{m-2,1}(x,y) \end{bmatrix} = \begin{bmatrix} x & -y & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^{m-2} \begin{bmatrix} x^2 - 2y \\ x \\ 3 \end{bmatrix} \quad (17)$$

and

$$\begin{bmatrix} T_{m,2}(x,y) \\ T_{m-1,2}(x,y) \\ T_{m-2,2}(x,y) \end{bmatrix} = \begin{bmatrix} y & -x & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}^{m-2} \begin{bmatrix} y^2 - 2x \\ x \\ 3 \end{bmatrix}, \quad (18)$$

where $m \geq 3$. Hence, we compute the above matrix powering, which can be calculated effectively using the addition chain algorithm [9].

3.2 Degree period and its symmetry

The commutative polynomials represented by (15) of degree m over residue ring Z_{2^k} are given by

$$T_m(x,y) \bmod 2^k \quad (19)$$

As described in the previous subsection, we can efficiently calculate $T_m(x,y) \equiv (\alpha,\beta) \bmod 2^k$ from $m, x,$ and y using the addition chain algorithm. In contrast, finding m from $x, y,$ and (α,β) such that $T_m(x,y) \equiv (\alpha,\beta) \bmod 2^k$ seems difficult. The problem of solving a degree m is called the degree determination problem. The security of a cryptosystem using the polynomials in (15) depends on the difficulty of the degree determination problem. Knowledge of the properties of the degree period can aid cryptoanalysis; therefore, we investigate the properties of the degree period.

Let $\mathrm{lcm}(a,b)$ be the least common multiple of a and b. Let N, N_x, and N_y be the minimum natural numbers that satisfy

$$\forall i, T_{i+N}(x,y) \equiv T_i(x,y) \bmod 2^k \quad (20)$$

$$\forall i, T_{Nx+i,1}(x,y) \equiv T_{i,1}(x,y) \bmod 2^k \quad (21)$$

$$\forall i, T_{Ny+i,2}(x,y) \equiv T_{i,2}(x,y) \bmod 2^k \quad (22)$$

Namely, $N, N_x,$ and N_y are the degree periods of $T_m(x,y)$, $T_{m,1}(x,y)$, and $T_{m,2}(x,y)$, respectively. N is determined by

$$N = \mathrm{lcm}\big(N_x, N_y\big) \quad (23)$$

These degree periods are dependent on (x,y). Therefore, we denote them as $N(x,y), N_x(x,y),$ and $N_y(x,y)$ if it is needed.

We now present an example, where k = 3, x = 5, and y = 1, as shown in Table 1. It can be observed from this table that $N_x = N_y = N = 4$.

Table 1

Sequences of $T_m(x,y)$ where k = 3, x = 5, y = 1

$T_m(x,y)$	$T_m(x,y) \bmod 2^k$
$T_0(x,y)$	(3,3)
$T_1(x,y)$	(5,1)
$T_2(x,y)$	(7,7)
$T_3(x,y)$	(5,1)
$T_4(x,y)$	(3,3)
$T_5(x,y)$	(5,1)
$T_6(x,y)$	(7,7)
$T_7(x,y)$	(5,1)
$T_8(x,y)$	(3,3)
⋮	⋮

Next, we provide the following proposition.

Proposition 1 $N(x,y) = N(y,x)$

Proof: From the definition,

$$T_{m,1}(x,y) = T_{m,2}(y,x) \quad (24)$$

$$T_{m,2}(x,y) = T_{m,1}(y,x) \quad (25)$$

which means that $N_x(x,y) = N_y(y,x)$ and $N_y(x,y) = N_x(x,y)$. Substituting this into (23), $N(x,y) =$

$\mathrm{lcm}(N_x(x,y), N_y(x,y)) = \mathrm{lcm}(N_y(y,x), (N_x(x,y)) = N(y,x)$. (Q.E.D)

All the results of $N(x,y)$ are summarized in Table 2 when $k = 2$. We confirmed that the degree period $N(x,y)$ is the same as $N(y,x)$.
All the results of $N(x,y)$ are summarized in Table 2 when $k = 2$. We confirmed that the degree period $N(x,y)$ is the same as $N(y,x)$.

Table 2
All degree periods where $k = 2$

x	y	$N(x,y)$
0	0	3
0	1	14
0	2	6
0	3	14
1	0	14
1	1	2
1	2	7
1	3	4
2	0	6
2	1	7
2	2	6
2	3	14
3	0	14
3	1	4
3	2	14
3	3	1

3.3 Possible values of the degree period

Let $f_x(t)$ and $f_y(t)$ be the characteristic functions corresponding to $T_{m,1}(x,y)$ and $T_{m,2}(x,y)$, respectively. From (3) and (4), the characteristic functions are derived as

$$f_x(t) = 1 - xt + yt^2 - t^3 \quad (26)$$
$$f_y(t) = 1 - yt + xt^2 - t^3 \quad (27)$$

Then, we obtain the following proposition.

Proposition 2 Degree period N is a divisor of the values given in Table 3.

Table 3
Degree period N when each of x, y is even or odd

(x,y)	
(even, even)	$3 \cdot 2^{k-1}$
(even, odd)	$7 \cdot 2^{k-1}$
(odd, even)	$7 \cdot 2^{k-1}$
(odd, odd)	$4 \cdot 2^{k-1}$

Proof: From Lemma 1, $N_x | 2^{k-1}\mathrm{per}(f_0^x)$, where $f_0^x = f_x(t) \bmod 2$ and $a|b$ means that a is a divisor of b. When both x and y are even numbers, $\mathrm{per}(f_0^x) = 3$ because $f_0^x(t) = 1 - t^3$. When x is an even number and y is an odd number, $\mathrm{per}(f_0^x) = 7$ because $f_0^x(t) = 1 + t^2 + t^3$ satisfies $f_0^x(t) | 1 - t^7$. When x is an odd number and y is an even number, $\mathrm{per}(f_0^x) = 7$ because we obtain $f_0^x(t) = 1 + t + t^3$ satisfying $f_0^x(t) | 1 - t^7$. When both x and y are odd numbers, $\mathrm{per}(f_0^x) = 4$ because $f_0^x(t) = 1 + t + t^2 + t^3$, which satisfies $f_0^x(t) | 1 - t^4$. Using the same discussion above, it can be said that N_y has the same result as N_x. Because $N = \mathrm{lcm}(N_x, N_y)$, this assertion is verified. (Q.E.D)

To confirm Proposition 2, we evaluate the period N for all (x,y) with $k = 4$ and summarize the number of (x,y) possessing each value of N in Tables 4 to 7. It can be verified that the theoretical results agree with the experimental results.

Table 4
Distribution when x, y = (even, even) and $k = 4$

N	The number of (x, y)
3	1
6	7
12	14
24	32

Table 5
Distribution when x, y = (even, odd) and $k = 4$

N	The number of (x, y)
7	1
14	3
28	12
56	48

Table 6
Distribution when x, y = (odd, even) and $k = 4$

N	The number of (x, y)
7	1
14	3
28	12
56	48

Table 7
Distribution when x, y = (odd, odd) and $k = 4$

N	The number of (x, y)
1	1
2	3
4	20
8	8
16	32

From Proposition 2, the maximum length of N is

$$N_{\max} = 7 \cdot 2^{k-1} \quad (28)$$

which can be obtained when x or y is an odd number over Z_{2^k}.

Finally, we investigated the distribution of the period N for k = 5 to 8. Figures 1 to 4 show the distributions of N, where the horizontal axis denotes the value of period N and the vertical axis denotes the number of (x,y) possessing such a period. It can be seen from these figures that there are many long periods, and the occurrence of the maximum

length is the highest. Because short periods are not secure from a cryptographic point of view, there might be no problem regarding the length of the degree period.

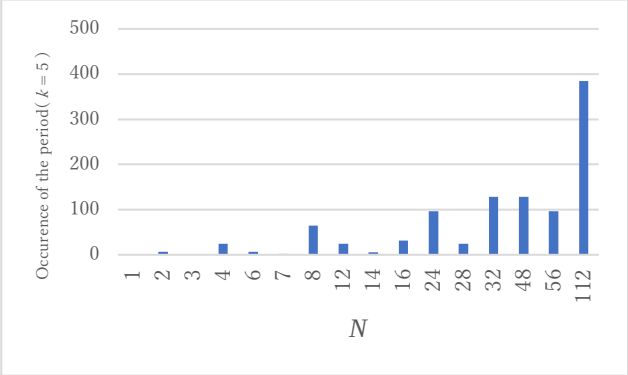

Fig. 1. Distribution of period N when k = 5

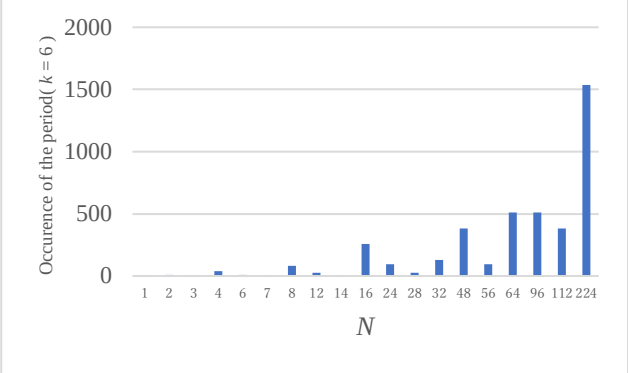

Fig. 2. Distribution of period N when k = 6

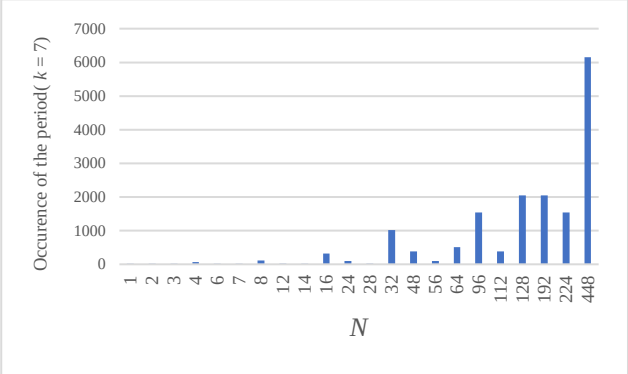

Fig. 3. Distribution of period N when k = 7

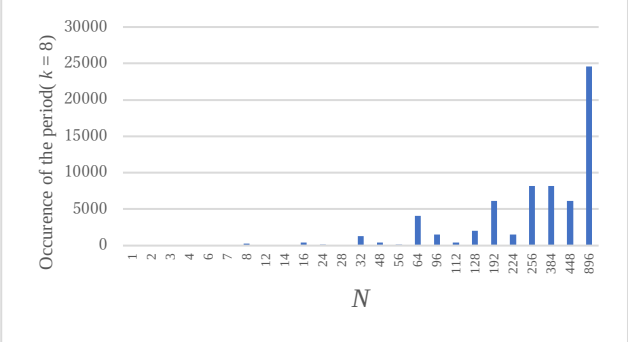

Fig. 4. Distribution of period N when k = 8

4. Conclusion

In this study, we have clarified some periodic properties of the commutative polynomials defined by the fourth-order linear recurrence relation over the residue ring Z_{2^k}.

Another important problem is the characterization of the sequence period generated by the polynomials. However, this topic requires further investigation.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 20K11824.

References

[1] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, vol.IT-22, No.6, pp.644-654, Nov, 1976.

[2] R. L. Rivest, A. Shamir, L. M. Adelman, “A method for obtaining digital signature and public-key cryptosystems,” *Communications of the ACM*, vol.21, no.2, pp.120–126, 1977.

[3] H. D. Block and H. P. Thielman, “Commutative polynomials,” The quarterly journal of mathematics, vol.2, pp.241–243, 1951.

[4] S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Significance," *IEEE Transactions on Information Theory*, vol.24, pp.106–110, 1978.

[5] K. Umeno, “Key exchange by Chebyshev polynomials modulo 2^w,” *Proc. of INA-CISC*, pp.95–97, 2005.

[6] D. Yoshioka and K. Kawano,” Periodic properties of Chebyshev polynomial sequences over the residue ring $Z=2^kZ$,” *IEEE Trans. Circuits and Systems II*, vol.63, no.8, pp-57—61, 2016.

[7] M. Ishii and A. Yoshimoto, “High−DimensionalCommuting Polynomial Mappings as Extended Chebyshev Polynomials,” *The japan society for industrial and applied mathematics*, vol.25, no.2, pp.59—90, 2015. (in Japanese)

[8] Z. Dai, “Binary sequences derived from ML-sequences over Rings I: Periods and minimal polynomials,” *Journal of Cryptology*, vol.5, pp.193—207, 1992.

[9] D.E.Knuth, “The art of computer programming, “ vol.2,1977