Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2014, Article ID 840435, 6 pages
http://dx.doi.org/10.1155/2014/840435

Research Article

Algorithms for Finding Inverse of Two Patterned Matrices over $\mathbb{Z}_p$

Xiaoyu Jiang and Kicheon Hong

Department of Information and Telecommunications Engineering, The University of Suwon, Wau-ri, Bongdam-eup, Hwaseong-si, Gyeonggi-do 445-743, Republic of Korea

Correspondence should be addressed to Kicheon Hong; kchong@suwon.ac.kr

Received 10 April 2014; Accepted 24 May 2014; Published 26 August 2014

Academic Editor: Zidong Wang

Circulant matrix families have become an important tool in network engineering. In this paper, two new patterned matrices over $\mathbb{Z}_p$ which include row skew first-plus-last right circulant matrix and row first-plus-last left circulant matrix are presented. Their basic properties are discussed. Based on Newton-Hensel lifting and Chinese remaindering, two different algorithms are obtained. Moreover, the cost in terms of bit operations for each algorithm is given.

1. Introduction

Circulant matrix families play an important role in network engineering. Basic [1] gave a simple condition for characterizing weighted circulant graphs allowing perfect state transfer in terms of their eigenvalues. Noual et al. [2] showed some preliminary results on the dynamical behaviours of some specific nonmonotone Boolean automata networks that were called xor circulant networks. Using the circulant matrix, the charge transport and the noise of a quantum wire network, made of three semi-infinite external leads attached to a ring crossed by a magnetic flux, were investigated [3]. Based on the circulant adjacency matrices of the networks induced by these interior symmetries, Aguiar and Ruan [4] analyzed the impact of interior symmetries on the multiplicity of the eigenvalues of the Jacobian matrix at a fully synchronous equilibrium for the coupled cell systems associated with homogeneous networks. Involving circulant matrix, the storage of binary cycles in Hopfield-type and other neural networks was investigated [5]. A new structure for the decoupling of circulant symmetric arrays of more than four elements was presented in [6]. Wang and Cheng [7] studied the existence of doubly periodic travelling waves in cellular networks involving the discontinuous Heaviside step function by circulant matrix. Pais et al. [8] proved conditions for the existence of stable limit cycles arising from multiple distinct Hopf bifurcations of the dynamics in the case of circulant fitness matrices. Cho and Chung [9] discussed the routing of a message on circulant networks, that is, a key to the performance of this network. Grassi [10] designed DTCNNs where each trajectory converges to a unique equilibrium point, which depends only on the input and not on the initial state, by exploiting the global asymptotic stability of the equilibrium point of DTCNNs with circulant matrices. Wu [11] obtained the coexistence of multiple large-amplitude wave solutions for the delayed Hopfield-Cohen-Grossberg model of neural networks with a symmetric circulant connection matrix. The system model of the OFDM is based on AF relay networks as well as the strategy of the superimposed training involved circulant matrix [12]. Two-way transmission model was considered in [13] and ensured circular convolution between two frequency selective channels.

In this paper, we give two algorithms for an $n \times n$ nonsingular RSFPLR circulant matrix over $\mathbb{Z}_p$. The primitive problem is transformed into an equivalent problem over $\mathbb{Z}_p[x]$. The first algorithm supposes the factorization of p is given and the costs of multiplications and additions over $\mathbb{Z}_p$ are $n\log^2 n + n \log p$ and $n\log^2 n \log\log n$, respectively. We obtain the bit complexity bound:

$$O\left(\left(n\log^2 n + n \log p\right)\mu\left(\log p\right) + n\log^2 n \log\log n \log p\right), \tag{1}$$

where $\mu(d)$ denotes the bit complexity of multiplying d-bit integers. The second algorithm does not know the factorization of p and its cost is greater, by a factor $\log p$, than in the first algorithm.

Definition 1. A row skew first-plus-last right (RSFPLR) circulant matrix with the first row $(a_0, a_1, \ldots, a_{n-1})$ over $\mathbb{Z}_p$, denoted by RSFPLRcircfr$(a_0, a_1, \ldots, a_{n-1})$, meant a square matrix of the form

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 + a_{n-1} & \ddots & a_{n-2} \\ \vdots & -a_{n-1} + a_{n-2} & \ddots & \vdots \\ -a_2 & \vdots & \ddots & a_1 \\ -a_1 & -a_2 + a_1 & \cdots & a_0 + a_{n-1} \end{pmatrix}_{n\times n}. \quad (2)$$

Obviously, the RSFPLR circulant matrix over a field is a $x^n - x + 1$-circulant matrix [14], and that is neither the extention of circulant matrix over $\mathbb{Z}_p$ [15] nor its special case, and they are two different families of patterned matrices.

We define $\Theta_{(-1,1)}$ as the basic RSFPLR circulant matrix over $\mathbb{Z}_p$; that is,

$$\Theta_{(-1,1)} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ -1 & 1 & 0 & \cdots & 0 \end{pmatrix}_{n\times n} = \text{RSFPLRcircfr}\,(0, 1, 0, \ldots, 0)\,. \quad (3)$$

It is easily verified that $g(x) = x^n - x + 1$ has no repeated roots over $\mathbb{Z}_p$ and $g(x) = x^n - x + 1$ is both the minimal polynomial and the characteristic polynomial of the matrix $\Theta_{(-1,1)}$. In addition, $\Theta_{(-1,1)}$ is nonderogatory and satisfies $\Theta^j_{(-1,1)} = \text{RSFPLRcircfr}(\underbrace{0, \ldots, 0}_{j}, 1, \underbrace{0, \ldots, 0}_{n-j-1})$ and $\Theta^n_{(-1,1)} = I_n - \Theta_{(-1,1)}$. In view of the structure of the powers of the basic RSFPLR circulant matrix $\Theta_{(-1,1)}$ over $\mathbb{Z}_p$, it is clear that

$$A = \text{RSFPLRcircfr}\,(a_0, a_1, \ldots, a_{n-1}) = \sum_{i=0}^{n-1} a_i \Theta^i_{(-1,1)}. \quad (4)$$

Thus, A is a RSFPLR circulant matrix over $\mathbb{Z}_p$ if and only if $A = f(\Theta_{(-1,1)})$ for some polynomial $f(x)$ over $\mathbb{Z}_p$. The polynomial $f(x) = \sum_{i=0}^{n-1} a_i x^i$ will be called the *representer* of the RSFPLR circulant matrix A over $\mathbb{Z}_p$. By Definition 1 and (4), it is clear that A is a RSFPLR circulant matrix over $\mathbb{Z}_p$ if and only if A commutes with $\Theta_{(-1,1)}$; that is, $A\Theta_{(-1,1)} = \Theta_{(-1,1)}A$.

In addition to the algebraic properties that can be easily derived from the representation (4), we mention that RSFPLR circulant matrices have very nice structure. The product of two RSFPLR circulant matrices is a RSFPLR circulant matrix and A^{-1} is a RSFPLR circulant matrix, too. Furthermore, let $\mathbb{Z}_p[\Theta_{(-1,1)}] = \{A \mid A = f(\Theta_{(-1,1)}), f(x) \in \mathbb{Z}_p[x]\}$. It is a routine to prove that $\mathbb{Z}_p[\Theta_{(-1,1)}]$ is a commutative ring with the matrix addition and multiplication.

Definition 2. A row first-plus-last left (RSLPFL) circulant matrix with the first row $(a_0, a_1, \ldots, a_{n-1})$ over $\mathbb{Z}_p$, denoted by RSLPFLcircfr$(a_0, a_1, \ldots, a_{n-1})$, meant a square matrix of the form

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & \cdots & a_{n-1} + a_0 & -a_0 \\ \vdots & \vdots & \iddots & -a_0 + a_1 & \vdots \\ a_{n-2} & \iddots & \iddots & \vdots & -a_{n-3} \\ a_{n-1} + a_0 & \cdots & \cdots & -a_{n-3} + a_{n-2} & -a_{n-2} \end{pmatrix}_{n\times n}. \quad (5)$$

Lemma 3. *Let*

$$\widehat{I}_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix} \quad (6)$$

be the $n \times n$ matrix of the counteridentity. Then

(i) RSLPFLcircfr$(a_0, a_1, \ldots, a_{n-1})$
$= RSFPLRcircfr(a_{n-1}, \ldots, a_1, a_0)\widehat{I}_n$;

(ii) RSLPFLcircfc$(a_0, a_1, \ldots, a_{n-1})\widehat{I}_n$
$= RSFPLRcircfc(a_{n-1}, \ldots, a_1, a_0)$.

Let A be a nonsingular matrix over $\mathbb{Z}_p$; we explore the problem of finding a RSFPLR circulant matrix $B = \sum_{i=0}^{n-1} b_i \Theta^i_{(-1,1)}$, such that $AB = I$.

Solving A^{-1} is clearly equivalent to finding a polynomial $g(x) = \sum_{i=0}^{n-1} b_i x^i$ in $\mathbb{Z}_p[x]$ such that

$$f(x)\, g(x) \equiv 1 \pmod{x^n - x + 1}. \quad (7)$$

The congruence modulo $x^n - x + 1$ follows from the equality $\Theta^n_{(-1,1)} = I_n - \Theta_{(-1,1)}$. Hence, the problem of solving A^{-1} is equivalent to inversion in the ring $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$.

The following theorem describes a necessary and sufficient condition for the nonsingularity of a RSFPLR circulant matrix over $\mathbb{Z}_p$.

Theorem 4. *Let $A = RSFPLRcircfr(a_0, a_1, \ldots, a_{n-1})$ be a RSFPLR circulant matrix over $\mathbb{Z}_p$; then the matrix A is nonsingular if and only if*

$$gcd\,(f(x), x^n - x + 1) = 1 \quad in\ \mathbb{Z}_{p_i}[x], \quad (8)$$

for $i = 1, \ldots, l$, where $p = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ is the prime powers factorization of p and $f(x) = \sum_{j=0}^{n-1} a_j x^j$.

Proof. If A is nonsingular, by (7), there exists $s(x)$ such that, for $i = 1, \ldots, l$,

$$f(x)\, g(x) + s(x)\,(x^n - x + 1) = 1 \quad \text{in } \mathbb{Z}_{p_i}[x]; \quad (9)$$

that is, $\gcd(f(x), x^n - x + 1) = 1$ in $\mathbb{Z}_{p_i}[x]$.

The proof of sufficient condition for nonsingularity will be given in Section 2 (Lemmas 5 and 6). □

Review of Bit Complexity Results [15]. The sum of two polynomials in $\mathbb{Z}_p[x]$ of degree at most n can be trivially calculated in $O(n\log p)$ bit operations. The product of two such polynomials can be calculated in $O(n\log n)$ multiplications and $O(n\log n\log\log n)$ additions or subtractions in $\mathbb{Z}_p$. Therefore, the cost of polynomial multiplication is $O(\prod(p,n))$ bit operations, where

$$\Pi(p,n) = n\log n\mu(\log p) + n\log n\ \log\ \log\ n\log p. \quad (10)$$

Let $a(x), b(x)$ be two polynomials of degree at most n over $\mathbb{Z}_p[x]$ (p prime); we calculate $d(x) = \gcd(a(x), b(x))$ in $O(\Gamma(p,n))$ bit operations, where

$$\Gamma(p,n) = \Pi(p,n)\log n + n\mu(\log p)\log\ \log\ p. \quad (11)$$

2. Finding Inversion in $\mathbb{Z}_p[x]/\langle x^n-x+1\rangle$ for Factorization of p Given

In this section, let $p = p_1^{k_1}p_2^{k_2}\cdots p_l^{k_l}$ be the given prime powers factorization of p. In the following, we discuss the inverse of a RSFPLR circulant matrix over $\mathbb{Z}_p$ by studying the equivalent problem, that is, finding the inversion of a polynomial $f(x)$ over $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$. We obtain algorithms of calculating the inverse via Chinese remaindering, the extended Euclidean algorithm, and Newton-Hensel lifting.

Lemma 5. *Let $g_1(x),\ldots,g_l(x)$ be known such that*

$$f(x)\,g_i(x) \equiv 1\ (mod\ x^n - x + 1) \quad in\ \mathbb{Z}_{p_i^{k_i}}[x], \quad (12)$$

for $i = 1,2,\ldots,l$ and $p = p_1^{k_1}p_2^{k_2}\cdots p_l^{k_l}$ and $f(x)$ is a polynomial in $\mathbb{Z}_p[x]$.

One can solve $g(x) \in \mathbb{Z}_p[x]$ such that

$$f(x)\,g(x) \equiv 1\ (mod\ x^n - x + 1), \quad (13)$$

and the cost of bit operations is $O(nl\mu(\log p) + \mu(\log p)\log\ \log\ p)$.

Proof. Due to $f(x)g_i(x) \equiv 1 (\mathrm{mod}\ x^n - x + 1)$ in $\mathbb{Z}_{p_i^{k_i}}[x]$, we get

$$f(x)\,g_i(x) \equiv 1 + \lambda_i(x)\langle x^n - x + 1\rangle \left(\mathrm{mod}\ p_i^{k_i}\right). \quad (14)$$

Let $\alpha_i = p/p_i^{k_i}$. Distinctly, for $j \neq i$, $\alpha_i \equiv 0\ (\mathrm{mod}\ p_j^{k_j})$. Since $\gcd(\alpha_i, p_i^{k_i}) = 1$, we can solve β_i which satisfies $\alpha_i\beta_i \equiv 1\ (\mathrm{mod}\ p_i^{k_i})$. Let $g(x) = \sum_{i=1}^{l}\alpha_i\beta_i g_i(x)$, $\lambda(x) = \sum_{i=1}^{l}\alpha_i\beta_i\lambda_i(x)$.

By construction, for $i = 1,2,\ldots,l$, we get $g(x) \equiv g_i(x)\ (\mathrm{mod}\ p_i^{k_i})$ and $\lambda(x) \equiv \lambda_i(x)\ (\mathrm{mod}\ p_i^{k_i})$. Then, for $i = 1,2,\ldots,l$, we obtain $f(x)g(x) = \sum_{j=1}^{l}\alpha_j\beta_j f(x)g_j(x) \equiv f(x)g_i(x)(\mathrm{mod}\,p_i^{k_i}) \equiv 1 + \lambda_i(x)\langle x^n - x + 1\rangle(\mathrm{mod}\,p_i^{k_i}) \equiv 1 + \lambda(x)\langle x^n - x + 1\rangle(\mathrm{mod}\,p_i^{k_i})$. We come to the conclusion that

$$f(x)\,g(x) \equiv 1 + \lambda(x)\langle x^n - x + 1\rangle(\mathrm{mod}\,p); \quad (15)$$

that is,

$$f(x)\,g(x) \equiv 1\ (\mathrm{mod}\ x^n - x - 1) \quad \text{in } \mathbb{Z}_p[x]. \quad (16)$$

The computation of $g(x)$ consists in n (one for each coefficient) applications of Chinese remaindering. Obviously, the computation of α_i, β_i, $i = 1,\ldots,l$ should be done only once. Since integer division has the same asymptotic cost as multiplication, the cost of bit operations for $\alpha_i,\ldots,\alpha_l$ is $O(l\mu(\log p))$. Because each β_i is got via an inversion in $\mathbb{Z}_{p_i^{k_i}}$, the cost of bit operations for $\beta_1,\ldots,\beta_l$ is $O(\sum_{j=1}^{l}\mu(\log p_j^{k_j})\log\log p_j^{k_j})$. Finally, the cost of bit operations for calculating $g(x)$ is $O(nl\mu(\log p))$ by using $\alpha_1,\ldots,\alpha_l,\beta_1,\ldots,\beta_l,g_1(x),\ldots,g_l(x)$. The thesis follows using the inequality

$$\mu(\log a)\log\ \log\ a + \mu(\log b)\log\ \log\ b \le \mu(\log(ab))\log\ \log(ab). \quad (17)$$

□

By Lemma 5, we can find the inversion of a polynomial over $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$ when $p = r^k$ is a prime power. The following lemma presents how to solve this special problem.

Lemma 6. *Suppose $gcd(f(x), x^n - x + 1) = 1$ in $\mathbb{Z}_r[x]$; then $f(x)$ is invertible in $\mathbb{Z}_{r^k}[x]/\langle x^n - x + 1\rangle$, where $f(x)$ is a polynomial in $\mathbb{Z}_{r^k}[x]$. In this case, the cost of bit operations for the inverse of $f(x)$ is $O(\Gamma(r,n) + \Pi(r^k,n))$, where $\Gamma(r,n)$ and $\Pi(r^k,n)$ are the same as* (11) *and* (10)*, respectively.*

Proof. Suppose $\gcd(f(x), x^n - x + 1) = 1$ in $\mathbb{Z}_r[x]$; by Bezout's lemma, there exist $s(x), t(x)$ which satisfy

$$f(x)\,s(x) + \langle x^n - x + 1\rangle\,t(x) \equiv 1\ (\mathrm{mod}\ r). \quad (18)$$

In the following, we consider Newton-Hensel lifting; that is,

$$g_0(x) = s(x), \qquad g_i(x) = 2g_{i-1}(x) - [g_{i-1}(x)]^2 f(x)\ \mathrm{mod}\ x^n - x + 1. \quad (19)$$

It is easy to verify by induction that $g_i(x)f(x) \equiv 1 + r^{2^i}\lambda_i(x)(\mathrm{mod}\,x^n - x + 1)$. Therefore, the inverse element of $f(x)$ in $\mathbb{Z}_{r^k}[x]/\langle x^n - x + 1\rangle$ is $g_{\lceil\log k\rceil}(x)$.

The cost of bit operations for calculating $s(x)$ is $O(\Gamma(r,n))$. Calculating $g_1(x), g_2(x),\ldots,g_{\lceil\log k\rceil}(x)$ is calculating each g_i modulo r^{2^i}. Therefore, the cost of bit operations for the whole sequence is $O(\Pi(r^2,n) + \Pi(r^4,n) + \cdots + \Pi(r^{2^{\lceil\log k\rceil}},n)) = O(\Pi(r^k,n))$. □

By Theorem 4 and Lemmas 5 and 6, we obtain Algorithm 1 for the inversion of a polynomial $f(x)$ over $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$. The cost of bit operations for the algorithm is $T(p,n) = O(nl\mu(\log p) + \mu(\log p)\log\ \log p + \sum_{j=1}^{l}\Gamma(p_j,n) + \Pi(p_j^{k_j},n))$, where l and p_j are bounded by $\log\ p$ and $p_j^{k_j}$, respectively. On the side, by using $\Pi(a,n) + \Pi(b,n) \le \Pi(ab,n)$ and $\Gamma(a,n) + \Gamma(b,n) \le \Gamma(ab,n)$, we get

$$T(p,n) = O(n\log p\mu(\log p) + \mu(\log p)\log\ \log p + \Gamma(p,n) + \Pi(p,n)) = O(n\log p\mu(\log p) + \Pi(p,n)\log n). \quad (20)$$

Particularly, if $p = O(n)$, the ascendent term is $\Pi(p,n)\log n$. That is, the cost of calculating the inverse of $f(x)$ is gradually

Inverse1 $(f(x), p, n) \rightarrow g(x)$
{Calculates the inverse $g(x)$ of $f(x)$ in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$}
(1) **let** $p = p_1^{k_1} p_2^{k_2}, \ldots, p_l^{k_l}$;
(2) **for** $j = 1, 2, \ldots, l$ do
(3) **if** $\gcd(f(x), x^n - x + 1) = 1$ in $\mathbb{Z}_{p_j}[x]$ then
(4) calculate $g_j(x)$ which satisfy
$f(x)g_j(x) \equiv 1 (\mathrm{mod}\ x^n - x + 1)$ in $\mathbb{Z}_{p_j^{k_j}}[x]$
(5) using Newton-Hensel lifting (Lemma 6);
(6) **else**
(7) **return** "$f(x)$ is not invertible";
(8) **endif**
(9) **endfor**
(10) calculate $g(x)$ using Chinese remaindering (Lemma 5).

Algorithm 1: Finding inversion in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$ for factorization of p given.

Inverse2 $(f(x), p) \rightarrow g(x)$
{Calculates the inverse $g(x)$ of $f(x)$ in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$}
(1) **if** $\gcd(f(x), x^n - x + 1) = 1$ **then**
(2) **let** $s(x), t(x)$ which satiefy $f(x)s(x) + (x^n - x + 1)t(x) = 1$ in $\mathbb{Z}_p[x]$;
(3) **return** $s(x)$;
(4) **else if** $\gcd(f(x), x^n - x + 1) = a(x)$, $\deg(a(x)) > 0$ **then**
(5) **return** "$f(x)$ is not invertible";
(6) **else if** $\gcd(f(x), x^n - x + 1)$ fails let d satisfy $d \mid p$;
(7) **let** $(m_1, m_2) \leftarrow$ **GetFactors** (p, d);
(8) **if** $m_2 \neq 1$, **then**
(9) $g_1(x) \leftarrow$ **Inverse2** $(f(x), m_1)$;
(10) $g_2(x) \leftarrow$ **Inverse2** $(f(x), m_2)$;
(11) calculate $g(x)$ using Chinese remaindering (Lemma 5);
(12) **else**
(13) $g_1(x) \leftarrow$ **Inverse2** $(f(x), m_1)$;
(14) calculate $g(x)$ using Newton-Hensel lifting (Lemma 6);
(15) **endif**
(16) **return** $g(x)$;
(17) **endif**
GetFactors $(p, d) \rightarrow (m_1, m_2)$
(18) **let** $m_1 \leftarrow \gcd(p, d^{\lfloor \log p \rfloor})$;
(19) **if** $(p/m_1) \neq 1$ **then**
(20) **return** $(m_1, p/m_1)$;
(21) **endif**
(22) **let** $e \leftarrow p/d$;
(23) **let** $m_1 \leftarrow \gcd(p, e^{\lfloor \log p \rfloor})$;
(24) if $(p/m_1) \neq 1$ **then**
(25) **return** $(m_1, p/m_1)$;
(26) **endif**
(27) **let** $m_1 \leftarrow \mathrm{lcm}(d, e)$;
(28) **return** $(m_1, 1)$;

Algorithm 2: Finding inversion in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$ for factorization of p unknown.

bounded by the cost of executing $\log n$ multiplications in $\mathbb{Z}_p[x]$.

3. Algorithm of Finding Inversion in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$ for Factorization of p Unknown

In this section, we show how to compute the inverse of $f(x)$ without knowing the factorization of the modulus. The number of bit operations of the new algorithm is only a factor $O(\log p)$ greater than in the previous case.

Our idea consists in trying to compute $\gcd(f(x), x^n - x + 1)$ in $\mathbb{Z}_p[x]$ using the gcd algorithm for $\mathbb{Z}_p[x]$. Such algorithm requires the inversion of some scalars, which is not a problem in $\mathbb{Z}_p[x]$, but it is not always possible if p is not prime. Therefore, the computation of $\gcd(f(x), x^n - x + 1)$ may fail. However, if the gcd algorithm terminates, we have solved the problem. In fact, together with the alleged gcd $a(x)$, the

algorithm also returns $s(x), t(x)$ such that $f(x)s(x)+(x^n-x+1)t(x) = a(x)$ in $\mathbb{Z}_p[x]$. If $a(x) = 1$, then $s(x)$ is the inverse of $f(x)$. If $\deg(a(x)) \neq 0$, one can easily prove that $f(x)$ is not invertible in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$. Note that we must force the gcd algorithm to return a monic polynomial.

If the computation of $\gcd(f(x), x^n - x + 1)$ fails, we use recursion. In fact, the gcd algorithm fails if it cannot invert an element $y \in \mathbb{Z}_p$. Inversion is done by using the integer gcd algorithm. If y is not invertible, the integer gcd algorithm returns $d = \gcd(p, y)$, with $d > 1$. Hence, d is a nontrivial factor of p. We use d to compute either a pair m_1, m_2, such that $\gcd(m_1, m_2) = 1$ and $m_1 m_2 = p$, or a single factor m_1, such that $m_1 \mid p$ and $p \mid (m_1)^2$. In the first case, we invert $f(x)$ in $\mathbb{Z}_{m_1}[x]/\langle x^n - x + 1\rangle$ and $\mathbb{Z}_{m_2}[x]/\langle x^n - x + 1\rangle$, and we use Chinese remaindering to get the desired result. In the second case, we invert $f(x)$ in $\mathbb{Z}_{m_1}[x]/\langle x^n - x + 1\rangle$ and we use one step of Newton-Hensel lifting to get the inverse in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$.

The computation of the factors p_1, p_2 is done by procedure GetFactors whose correctness is proven by Lemmas 4.1 and 4.2 in [15]. Combining these procedures together, we get Algorithm 2.

Theorem 7. *Suppose $f(x)$ is invertible in $\mathbb{Z}_p[x]/\langle x^n - x + 1\rangle$; the cost of bit operations for Algorithm 2 which returns the inverse $g(x)$ is $O(\Gamma(p, n)\log p)$.*

Proof. It is similar to the proof of Theorem 4.3 in [15]. □

In addition, by Lemma 3 and Algorithms 1 and 2, it is easy to get two algorithms for inverting RSLPFL circulant matrices over $\mathbb{Z}_p$, respectively.

4. Conclusion

In this paper, we consider the problem of finding inverse matrix for a $n \times n$ RSFPLR circulant matrix with entries over $\mathbb{Z}_p$. We present two different algorithms. Our algorithms require different degrees of knowledge of p and n, and their costs range, roughly, from $n \log n \log\log n$ to $n \log^2 n \log\log n \log p$ operations over $\mathbb{Z}_p$. Moreover, for each algorithm, we give the cost in terms of bit operations. Finally, the extended algorithms are used to solve the problem of inverting RSLPFL circulant matrices over $\mathbb{Z}_p$. Based on the existing problem in [16–19], we will develop solving these problems by circulant matrices technology.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the GRRC program of Gyeonggi province [(GRRC SUWON 2014-B3), Development of Cloud Computing-Based Intelligent Video Security Surveillance System with Active Tracking Technology]. Their support is gratefully acknowledged.

References

[1] M. Basic, "Which weighted circulant networks have perfect state transfer?" *Information Sciences*, vol. 257, pp. 193–209, 2014.

[2] M. Noual, D. Regnault, and S. Sené, "About non-monotony in Boolean automata networks," *Theoretical Computer Science*, vol. 504, pp. 12–25, 2013.

[3] V. Caudrelier, M. Mintchev, and E. Ragoucy, "Quantum wire network with magnetic flux," *Physics Letters A*, vol. 377, no. 31–33, pp. 1788–1793, 2013.

[4] M. A. D. Aguiar and H. Ruan, "Interior symmetries and multiple eigenvalues for homogeneous networks," *SIAM Journal on Applied Dynamical Systems*, vol. 11, no. 4, pp. 1231–1269, 2012.

[5] C. Zhang, G. Dangelmayr, and I. Oprea, "Storing cycles in Hopfield-type networks with pseudoinverse learning rule: admissibility and network topology," *Neural Networks*, vol. 46, pp. 283–298, 2013.

[6] J. C. Coetzee, J. D. Cordwell, E. Underwood, and S. L. Waite, "Single-layer decoupling networks for circulant symmetric arrays," *IETE Technical Review*, vol. 28, no. 3, pp. 232–239, 2011.

[7] G. Wang and S. S. Cheng, "6-periodic travelling waves in an artificial neural network with bang-bang control," *Journal of Difference Equations and Applications*, vol. 18, no. 2, pp. 261–304, 2012.

[8] D. Pais, C. H. Caicedo-Núñez, and N. E. Leonard, "Hopf bifurcations and limit cycles in evolutionary network dynamics," *SIAM Journal on Applied Dynamical Systems*, vol. 11, no. 4, pp. 1754–1784, 2012.

[9] Y. Cho and I. Chung, "A parallel routing algorithm on circulant networks employing the Hamiltonian circuit Latin square," *Information Sciences*, vol. 176, no. 21, pp. 3132–3142, 2006.

[10] G. Grassi, "On the design of discrete-time cellular neural networks with circulant matrices," *International Journal of Circuit Theory and Applications*, vol. 28, pp. 193–202, 2000.

[11] J. Wu, "Symmetric functional-differential equations and neural networks with memory," *Transactions of the American Mathematical Society*, vol. 350, no. 12, pp. 4799–4838, 1998.

[12] F. Gao, B. Jiang, X. Gao, and X. Zhang, "Superimposed training based channel estimation for OFDM modulated amplify-and-forward relay networks," *IEEE Transactions on Communications*, vol. 59, no. 7, pp. 2029–2039, 2011.

[13] G. Wang, F. Gao, Y. Wu, and C. Tellambura, "Joint CFO and channel estimation for OFDM-based two-way relay networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 456–465, 2011.

[14] D. Chillag, "Regular representations of semisimple algebras, separable field extensions, group characters, generalized circulants, and generalized cyclic codes," *Linear Algebra and Its Applications*, vol. 218, pp. 147–183, 1995.

[15] D. Bini, G. M. D. Corso, G. Manzini, and L. Margara, "Inversion of circulant matrices over Zm," *Mathematics of Computation*, vol. 70, pp. 1169–1182, 2000.

[16] H. Dong, Z. Wang, and H. Gao, "Distributed H_∞ filtering for a class of markovian jump nonlinear time-delay systems over lossy sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 10, pp. 4665–4672, 2013.

[17] Z. Wang, H. Dong, B. Shen, and H. Gao, "Finite-horizon H_∞ filtering with missing measurements and quantization effects," *IEEE Transactions on Automatic Control*, vol. 58, no. 7, pp. 1707–1718, 2013.

[18] D. Ding, Z. Wang, J. Hu, and H. Shu, "Dissipative control for state-saturated discrete time-varying systems with randomly occurring nonlinearities and missing measurements," *International Journal of Control*, vol. 86, no. 4, pp. 674–688, 2013.

[19] J. Hu, Z. Wang, B. Shen, and H. Gao, "Quantised recursive filtering for a class of nonlinear systems with multiplicative noises and missing measurements," *International Journal of Control*, vol. 86, no. 4, pp. 650–663, 2013.