On lattice-based algebraic feedback shift registers synthesis algorithms for multisequences

Li-Ping Wang[1]* Daqing Wan[2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China.

[2]Department of Mathematics, University of California, Irvine, USA

Abstract

In this paper we show that algebraic feedback shift registers synthesis problems over some residue class rings and some quadratic integer rings for multisequences are reduced to the successive minima problem in lattice theory. Therefore they can be solved by polynomial-time algorithms when the number of multiple sequences is fixed.

keywords: Feedback with carry shift registers, Berlekamp-Massey algorithm, simultaneous rational approximation, multisequences.

1 Introduction

Feedback with carry shift registers (FCSRs for short) were introduced by Klapper and Goresky in [17] (see also [12, 18, 19]) . They are very similar to classical linear feedback shift registers (LFSRs) used in many pseudorandom generators. Later Klapper and Xu generalized both LFSRs and FCSRs to algebraic feedback shift registers (AFSRs) in [20]. As we all know, synthesis problem for key streams plays an important role in design and analysis of stream ciphers. It aims to find a generator such as an LFSR, an FCSR or an AFSR, with the shortest length, which is capable of predicting the whole sequence if only a finite prefix of a sequence is obtained.

There are a lot of synthesis algorithms for a single sequence. The famous Berlekamp-Massey algorithm [5, 22] solves LFSRs synthesis problem. There are also many other algorithms such as continued fraction method [25] and Euclidean algorithms [27]. For FCSRs, there are mainly three synthesis methods: the Euclidean algorithm [3], the theory of approximation lattices [18] and Klapper-Xu algorithm [20, 29], which is also used to some AFSRs with certain algebraic properties. Recently, Liu and Klapper proposed a new synthesis algorithm for AFSRs over quadratic integer rings using lattice approximation approach based on low-dimensional lattice basis reduction[21].

With the recent development of parallelization, word-based stream ciphers become popular and there are many LFSRs synthesis algorithms for multisequences [9, 10, 11, 28]. In addition, some researchers considered the bounds for minimal length for FCSRs generating periodic multisequences [15, 30]. However, there is neither AFSRs nor FCSRs synthesis algorithms for finite-length multisequences. In this paper we show that the AFSRs synthesis problems over some residue class rings (that is, FCSRs) and some quadratic integer rings for finite-length multisequences are reduced to the successive minima problem in lattice theory. Therefore, we can give a polynomial-time algorithm to solve the problems when the number of multiple sequences is fixed.

The rest of this paper is organized as follows. In Section 2 we introduce some preliminaries about AFSRs synthesis problems for multisequences. Section 3 recalls some basic results about lattice problems needed in this paper. In section 4 we solve FCSRs synthesis problem for multisequences. Next, we propose an AFSR synthesis algorithm over some quadratic integer rings for multisequences in Section 5. Finally, we give our conclusions in Section 6.

2 Preliminaries

For a positive integer m, consider m infinite sequences $S_1, \ldots, S_m$, where $S_i = a_{i,0}, a_{i,1}, \ldots$ for $1 \leq i \leq m$. Also, they can be denoted by an m-fold multisequence $\mathbf{S} = \mathbf{a}_0, \mathbf{a}_1, \ldots$, where $\mathbf{a}_j = (a_{1,j}, \ldots, a_{m,j})^T$, $j \geq 0$, and T is the transpose of a vector. In this section we introduce the construction of AFSRs for an m-fold multisequence, which is similar to a single sequence, that is, $m = 1$. For more details, refer to [12, 20].

Let R be an integral domain with a principal ideal generated by an element π such that the quotient ring $R/(\pi)$ is finite. Let $U \subset R$ be a complete set of representatives for $R/(\pi)$ (i.e., the composition $U \to R \to R/(\pi)$ is a one-to-one correspondence). The ring of π-adic integers, R_π, is the set of expressions $\gamma = \sum_{i=0}^{\infty} a_i \pi^i$ with all $a_i \in U$.

An AFSR (Fig.1) is determined by $r+1$ coefficients $q_0, q_1, \ldots, q_r \in U$ called taps such that q_0 is invertible modulo π. It is an automation each of whose states consists of r elements $\mathbf{a}_0, \ldots, \mathbf{a}_{r-1} \in U^m$ with an initial memory column vector $\mathbf{z}$. The state is updated by the following steps:

(1) Take the integer sum $\sigma = \sum_{k=1}^{r} q_k \mathbf{a}_{r-k} + \mathbf{z}$.

(2) Find $\mathbf{a}_r \in U^m$ such that $-q_0 \mathbf{a}_r \equiv \sigma \mod \pi$.

(3) Replace $(\mathbf{a}_0, \ldots, \mathbf{a}_{r-1})$ by $(\mathbf{a}_1, \ldots, \mathbf{a}_r)$ and replace $\mathbf{z}$ by the quotient of $\sigma + q_0 \mathbf{a}_r$ divided by π.

An LFSR over a finite field $\mathbb{F}$ is an AFSR where $R = \mathbb{F}[x]$, $\pi = x$ and $U = \mathbb{F}$, which is the quotient ring $R/(\pi) = \mathbb{F}[x]/(x)$. An FCSR over $\mathbb{Z}/(N)$ for a positive integer N is an AFSR with $R = \mathbb{Z}$, $\pi = N$, and $U = \{0, 1, \ldots, N-1\}$. An AFSR over a quadratic extension of $\mathbb{Z}$ is an AFSR, where $R = \mathbb{Z}[\pi]$, $\pi^2 = d$, $U = \{0, 1, \ldots, |d|-1\}$, where $d \in \mathbb{Z}$ is square free. In this paper we focus on the last two AFSRs synthesis problems for multisequences, in particular, in case N is a prime power and d is a prime, respectively.

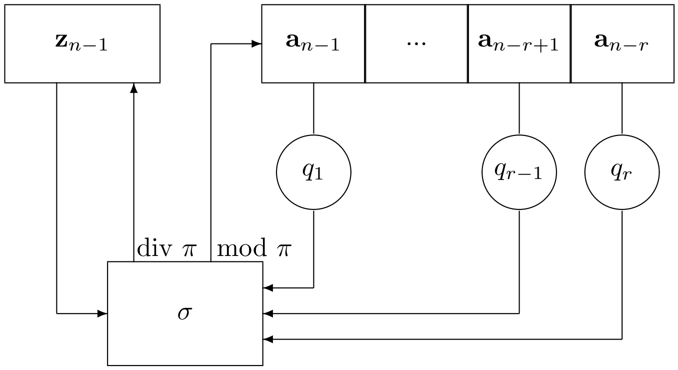

Figure 1: An Algebraic Feedback Shift Register

The register outputs an infinite sequence $\mathbf{a}_0, \mathbf{a}_1, \ldots$ of elements in U^m. The sequence satisfies a linear recurrence with carry, that is, for $n \geq r$,

$$-q_0\mathbf{a}_n + \pi\mathbf{z}_n = q_1\mathbf{a}_{n-1} + \ldots + q_r\mathbf{a}_{n-r} + \mathbf{z}_{n-1}, \tag{1}$$

where $\mathbf{z}_i$ denotes the ith memory vector.

The element $q = q_0 + q_1\pi + q_2\pi^2 + \ldots + q_r\pi^r$ plays a central role in the analysis of AFSRs and is referred as the connection element of the AFSR. The connection element is analogous to the connection polynomial of an LFSR.

We generalize the fundamental theorem on AFSRs from single sequences to multisequences as follows.

Theorem 1 *(Generalization of [Theorem 3, [20]]) Let the output sequence* $\mathbf{S} = \mathbf{a}_0, \mathbf{a}_1, \ldots$ *of an AFSR with connection element* q *and initial state* $(\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_{r-1}; \mathbf{z})$*. Let* $\alpha_i = \sum_{j=0}^{\infty} a_{i,j}\pi^j$ *be the associated formal power series of* S_i *for* $1 \leq i \leq m$ *and* $\alpha = (\alpha_1, \ldots, \alpha_m)^T$ *be the associated vector of* $\mathbf{S}$*. Then*

$$\alpha = \frac{\sum_{n=0}^{r-1}\sum_{i=0}^{n} q_i\mathbf{a}_{n-i}\pi^n - \mathbf{z}\pi^r}{q} = \frac{\mathbf{u}}{q} \in R_\pi^m. \tag{2}$$

The expression $\mathbf{u}/q$ *is called a simultaneous rational expression of* α*.*

If S_i is a periodic sequence with period L, the best rational expression of S_i is then $\alpha_i = \sum_{j=0}^{\infty} a_{i,j}\pi^j = -\frac{\sum_{i=0}^{L-1} a_{i,j}\pi^j}{\pi^L - 1} = -\frac{p_i}{q_i}$ for all i. In the case that R is a principal ideal domain, then $q = lcm(q_1, \ldots, q_m)$, where lcm denotes the least common multiple, is the smallest element such that there exists an AFSR with connection element q which can generate $S_1, \ldots, S_m$ simultaneously.

Assume R has a norm function $\mathcal{N} : R \to \mathbb{N} \cup \{0\}$ ($\mathbb{N}$ defines the natural numbers). To measure the length of a vector, we need to define a norm in R^{m+1} in terms of $\mathcal{N}$ by

$$\phi(u_1, \ldots, u_{m+1}) = \max(\mathcal{N}(u_1), \ldots, \mathcal{N}(u_{m+1})), \text{ for } (u_1, \ldots, u_{m+1}) \in R^{m+1}.$$

What we focus on in this paper is that only the first n terms of $\mathbf{S}$ are obtained for any non-negative integer n. Our goal of the AFSRs synthesis problem is to find any $(p_1, \ldots, p_m, q) \in R^{m+1}$ with q invertible modulo π such that there exists an AFSR with connection element q which generates the first n terms of $S_1, \ldots, S_m$ simultaneously, and $\phi(p_1, \ldots, p_m, q)$ is minimum in all such AFSRs.

Meanwhile, we describe the above synthesis problem in the mathematical form.

Definition 1 *Let $\alpha = (\alpha_1, \ldots, \alpha_m)$ be an m-dimensional vector of π-adic numbers and n be a non-negative integer. We say $(\frac{p_1}{q}, \ldots, \frac{p_m}{q})$, with $\gcd(q, \pi) = 1$, is a simultaneous rational approximation of order n of α if the first n terms in the π-adic expansions of α_i and $\frac{p_i}{q}$ are equal for any $1 \leq i \leq m$, i.e. π^n divides $\alpha_i - \frac{p_i}{q}$.*

For $1 \leq i \leq m$, we denote

$$\alpha_{i,n} = \sum_{k=0}^{n-1} a_{i,k} \pi^k.$$

In other words, $(\frac{p_1}{q}, \ldots, \frac{p_m}{q})$ is a simultaneous rational approximation of order n of α if and only if $q\alpha_{i,n} \equiv p_i \mod \pi^n$ and $\gcd(q, \pi) = 1$.

The problem of the best (π-adic) simultaneous rational approximation of order n of α is as follows.

Given $(\alpha_{1,n}, \ldots, \alpha_{m,n})$ and n, find all $(p_1, \ldots, p_m, q)$ with $\gcd(\pi, q) = 1$, satisfying $q\alpha_{i,n} \equiv p_i \mod \pi^n$ and minimizing $\phi(p_1, \ldots, p_m, q)$.

The problem of the AFSRs synthesis for a given multisequence $\mathbf{S}$ with finite length n is equivalent to the problem of the best simultaneous rational approximation of order n to α.

3 Some facts about lattices

In this section we introduce several fundamental problems in lattice theory and state some important results we need later.

In lattice problems, one often uses the Euclidean norm l_2, but many applications require other norms like l_p, most generally, the semi-norm. For any real number $1 \leq p \leq \infty$ and a positive integer n, the l_p-norm of a vector $\mathbf{v} \in \mathbb{R}^n$ is defined by $||\mathbf{v}||_p := (\sum_{i=1}^n |v_i|^p)^{1/p}$ and $||\mathbf{v}||_\infty = \max_{i=1,\ldots,n} |v_i|$.

The semi-norm is defined by a convex body $K \subseteq \mathbb{R}^n$, that is, K is convex, compact and full-dimensional, as $||\mathbf{v}||_K = \inf\{r \geq 0 : \mathbf{x} \in rK\}$ for $\mathbf{v} \in \mathbb{R}^n$. The functional $|| \cdot ||_K$ is a semi-norm, i.e., it satisfies the triangular inequality and $||t\mathbf{v}||_K = t||\mathbf{v}||_K$ for $t \geq 0, \mathbf{v} \in \mathbb{R}^n$. If K is centrally symmetric, then $|| \cdot ||_K$ is a norm in the usual norm sense.

Let $B_p^n = \{\mathbf{v} \in \mathbb{R}^n : ||\mathbf{v}||_p \leq 1\}$ denote the l_p ball in $\mathbb{R}^n$. Note from our definitions that $||\mathbf{v}||_{B_p^n} = ||\mathbf{v}||_p$ for $\mathbf{v} \in \mathbb{R}^n$.

Given linearly independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_l \in \mathbb{R}^n$, the lattice generated by these vectors is defined by

$$L(\mathbf{b}_1, \ldots, \mathbf{b}_l) = \{\sum_{i=1}^{l} z_i \mathbf{b}_i : z_i \in \mathbb{Z}\}.$$

We call $\mathbf{b}_1, \ldots, \mathbf{b}_l$ a basis of the lattice. We say that the rank of lattice is l and its dimension is n. If $l = n$, the lattice is called a full-rank lattice. The determinant of a lattice L with a basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_l)$, denoted by $\det(L)$, is defined by $\det(L) = \sqrt{B^T B}$. Hereafter we only consider full-rank lattices.

The ith successive minimum of a lattice, denoted by $\lambda_i^{(K)}(L)$, with respect to the semi-norm $||\cdot||_K$, is defined by

$$\lambda_i^{(K)}(L) := \inf\{r > 0 : \mathbf{v}_1, \ldots, \mathbf{v}_i \in L \text{ are linearly independent with } ||\mathbf{v}_j||_K \leq r \text{ for } 1 \leq j \leq i.\}$$

The length of the shortest nonzero vector in the lattice is denoted by $\lambda_1^{(K)}(L)$.

In the last 30 years the complexity of the following lattice problems has been studied intensively.

Definition 2 (Shortest Vector problem(SVP)) *Given a lattice L, find a non-zero lattice vector $\mathbf{v} \in L$ such that*

$$||\mathbf{v}||_K \leq ||\mathbf{w}||_K$$

for any $\mathbf{w} \in L \setminus \{0\}$.

Definition 3 (Closest vector problem (CVP)) *Given a lattice L and a target vector $\mathbf{t} \in span(L)$, find a lattice vector $\mathbf{v} \in L$ such that*

$$||\mathbf{v} - \mathbf{t}||_K \leq ||\mathbf{w} - \mathbf{t}||_K$$

for all $\mathbf{w} \in L$.

Definition 4 (Successive Minima Problem (SMP)) *Given a lattice with rank n, find n linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in L$ such that*

$$||\mathbf{v}_i||_K \leq \lambda_i^{(K)}(L)$$

for all $i = 1, \ldots, n$.

The successive minima vectors always exist.

Proposition 1 *([7]) Let L be a lattice of rank n with successive minima $\lambda_1^{(K)}(L)$, $\ldots$, $\lambda_n^{(K)}(L)$. Then there exist linearly independent lattice vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in L$ such that $||v_i||_K = \lambda_i^{(K)}(L)$ for all i, $1 \leq i \leq n$.*

In [26] authors gave an algorithm in quadratic time about the length of input data to reach all the successive minima of a lattice with rank up to four in l_2 norm.

Micciancio [23] gave a polynomial time rank-preseving reduction from SMP to CVP. Hence the algorithms for SMP have the same running time as the algorithms for CVP. For exact CVP in l_2 norm, Kannan's algorithm [16] gives a solution in deterministic $2^{O(n \log n)} b^{O(1)}$ time and poly(n) space, where b is the length of input data. Then it is improved to $n^{n/2} b^{O(1)}$ by Helfrich [14] and hanrot and Stehle [13]. This performance remained essentially unchallenged until the breakthrough randomized sieve algorithm of Ajtai, Kumar and Sivakumar [1] which provides a $2^{O(n)}$-time and -space solution for exact SVP. After modifying this algorithm, a sequence of works [2, 4, 6] can solve CVP exactly in $2^{O(n)}$ time as long as the target point is "very close" to the lattice. It is worth noting that the AKS sieve is a Monte Carlo algorithm: while the output solution is correct with high probability, it is not guaranteed. In a more recent breakthrough, Micciancio and Voulgaris [24] gave a deterministic $2^{O(n)}$-time and -space algorithm for exact CVP in the l_2 norm. In [8] authors gave a deterministic $2^{O(n)}$-time and space algorithm for exact CVP when the target point is sufficient close to the lattice in a semi-norm given by a convex body. We summarize it as follows.

Proposition 2 *Let $L \in \mathbb{R}^n$ be a lattice. The best deterministic algorithm for computing all exact successive minima vectors of L has a running time of $2^{O(n)} b^{O(1)}$ with respect to a semi-norm given by a convex body, where b is the length of input data.*

4 FCSRs synthesis for multisequences

In this section we consider the FCSRs synthesis problem for an m-fold multisequence $\mathbf{S}$ given in Section 2, that is, an AFSR with $R = \mathbb{Z}$, $\pi = N$, $U = \{0, 1, \ldots, N-1\}$ and $\phi = l_\infty$, where N is a prime power. Consider this problem using approximation lattices defined by

$$L_n(\alpha) = \{(p_1, \ldots, p_m, q) \in \mathbb{Z}^{m+1} |\, q\alpha_{i,n} \equiv p_i \mod N^n \text{ for all } i, 1 \le i \le m\},$$

where α and $\alpha_{i,n}$ are defined in Section 2.

The approximation lattices satisfy the following properties. The proof is left to the readers.

Lemma 1 *(i) L_0 is a lattice in $\mathbb{Z}^{m+1}$ of rank $m+1$.*

(ii) $L_{n+1} \subset L_n$.

(iii) The determinant of L_n is N^{mn}.

(iv) Let $\omega_1, \ldots, \omega_{m+1}$ be in L_n and $\omega = (\omega_1 \;\ldots\; \omega_{m+1})$ be the matrix made of $\omega_1, \ldots, \omega_{m+1}$. Then they form a basis of L_n if and only if $|\omega| = N^{mn}$.

(v) $\omega_1 = N^n \varepsilon_1$, …, $\omega_m = N^n \varepsilon_m$, where $\varepsilon_1, \ldots, \varepsilon_m$ is the standard vector of dimension $m+1$, $\omega_{m+1} = (\alpha_{1,n}, \ldots, \alpha_{m,n}, 1)^T$ is a basis of L_n.

The lattice $L_n(\alpha)$ can be partitioned into two parts

$$\begin{aligned} L_n^{(0)}(\alpha) &= \{(p_1, \ldots, p_m, q) \in \mathbb{Z}^{m+1} | \gcd(q, N) > 1\} \text{ and} \\ L_n^{(1)}(\alpha) &= \{(p_1, \ldots, p_m, q) \in \mathbb{Z}^{m+1} | \gcd(q, N) = 1\}. \end{aligned}$$

The set $L_n^{(1)}(\alpha)$ is the set of simultaneous rational approximation of α at order n. The best simultaneous rational approximation is then a minimal element of $L_n^{(1)}(\alpha)$ under l_∞ norm.

Theorem 2 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$ be the successive minimum vectors in $L_n(\alpha)$ under l_∞ norm and k, $1 \leq k \leq m+1$, be the smallest integer such that the $m+1$-th component of $\mathbf{v}_k$ is coprime to N. Then $\mathbf{v}_k$ is a minimal element of $L_n^{(1)}(\alpha)$.*

Proof. First we show that such k must exist. Suppose $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$ in $L_n(\alpha)$ with $\mathbf{v}_i = (p_{i,1}, \ldots, p_{i,m}, q_i)$ and $\gcd(N, q_i) \neq 1$ for $1 \leq i \leq m+1$. Since $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$ are linear independent over $\mathbb{R}$, the vector $(\alpha_{1,n}, \ldots, \alpha_{m,n}, 1)$ must be a linear combination of $\mathbf{v}_1, \ldots, \mathbf{v}_{m+1}$, which is impossible.

If $\mathbf{v}_1 \in L_n^{(1)}(\alpha)$, that is, $k = 1$, it is the minimal element in $L_n^{(1)}(\alpha)$.

If $k \geq 2$, that is, $\mathbf{v}_k \in L_n^{(1)}(\alpha)$, we show it is the minimal element in $L_n^{(1)}(\alpha)$. Otherwise, assume that ξ is the minimal element in $L_n^{(1)}(\alpha)$ i.e., $||\xi||_{l_\infty} < ||\mathbf{v}_k||_{l_\infty}$ and $||v_{s-1}||_{l_\infty} < ||v_s||_{l_\infty} = \ldots = ||v_k||_{l_\infty}$ for some s, $2 \leq s \leq k$. Then $v_1, \ldots, v_{s-1}, \xi$ are linearly independent and $||v_i||_{l_\infty} < \lambda_s(L_n(\alpha))$ and $||\xi||_{l_\infty} < \lambda_s(L_n(\alpha))$, which contradicts with the definition of successive minima. □

By Theorem 2, the FCSRs synthesis problem for $\mathbf{S}$ of order n, which is equivalent to the best simultaneous rational approximation of order n for α, is reduced to the SMP in lattice $L_n(L)$. By Proposition 2 and Lemma 1, we get our results as follows.

Theorem 3 *The FCSRs synthesis problem for m-fold multisequence $\mathbf{S}$ of order n can be solved by a polynomial-time algorithm when m is fixed. The time complexity is $2^{O(m)}(mn \log N)^{O(1)}$.*

5 AFSRs synthesis over some quadratic integer rings for multisequences

In this section we consider the AFSRs synthesis problem over a quadratic extension of $\mathbb{Z}$ for m-fold sequences $\mathbf{S}$. To be specific, $R = \mathbb{Z}[\pi]$, $\pi^2 = d$, $U = \{0, 1, \ldots, |d| - 1\}$, where d is a prime.

In [21] authors gave such AFSRs synthesis algorithm for a single sequence using approximation lattices method. We use the similar method to construct approximation lattices for multisequences. The nth approximation lattice of α is defined by

$$\begin{aligned} L_n(\alpha) = \{&(p_{1,1}, \sqrt{|d|}\, p_{1,2}, \ldots, p_{m,1}, \sqrt{|d|}\, p_{m,2}, q_1, \sqrt{|d|} q_2) \in \mathbb{R}^{2m+2} : \alpha_{i,n}(q_1 + q_2\pi) \\ &-(p_{i,1} + p_{i,2}\pi) \equiv 0 \mod \pi^n, p_{i,j}, q_j \in \mathbb{Z} \text{ for all } 1 \leq i \leq m, 1 \leq j \leq 2.\} \end{aligned}$$

In the following denote $\mathbf{u} = (p_{1,1}, \sqrt{|d|}\, p_{1,2}, \ldots, p_{m,1}, \sqrt{|d|}\, p_{m,2}, q_1, q_2\sqrt{|d|})$ just for brevity. For $d < 0$, we consider imaginary quadratic integer rings such as $d = -2, -3, -5$ and use the common norm $\mathcal{N}(a + b\pi) = \sqrt{a^2 - db^2}$ over $\mathbb{Z}[\pi]$. Thus we can define $\phi(p_{1,1} + \pi p_{1,2}, \ldots, p_{m,1} + \pi p_{m,2}, q_1 + q_2\pi) = \max\{\mathcal{N}(p_{1,1}+\pi p_{1,2}), \ldots, \mathcal{N}(p_{m,1}+\pi p_{m,2}), \mathcal{N}(q_1+q_2\pi)\}$. That is, we have such a norm in the lattice defined by $||\mathbf{u}||_d = \max\{\sqrt{p_{1,1}^2 - d\,p_{1,2}^2}, \ldots, \sqrt{p_{m,1}^2 - d\,p_{m,2}^2}, \sqrt{q_1^2 - d\,p_2^2}\}$ since it is verified that $||\cdot||_d$ satisfies the triangular inequality and $||t\mathbf{u}||_d = t||\mathbf{u}||_d$. In addition, if $||\mathbf{u}||_d = 0$, then $\mathbf{u} = 0$. Note that there is a little abuse of notation about $||\cdot||_d$ since it is different from the norm $||\cdot||_p$ in Section 2 just for simplification of symbols.

For $d > 0$, we define the norm on the real quadratic integer rings by $\mathcal{N}(a + b\pi) = \max\{|a + b\pi|, |a - b\pi|\}$. Likewise, we have a norm in the lattice defined by $||\mathbf{u}||_d = \max\{|\,p_{1,1} + p_{1,2}\sqrt{d}\,|, |\,p_{1,1} - p_{1,2}\sqrt{d}\,|, \ldots, |\,p_{m,1} + p_{m,2}\sqrt{d}\,|, |\,p_{m,1} - p_{m,2}\sqrt{d}\,|, |\,q_1 + q_2\sqrt{d}\,|, |\,q_1 - q_2\sqrt{d}\,|\}$ since it is also verified that $||\cdot||_d$ satisfies that the triangular inequality, $||t\mathbf{u}||_d = t||\mathbf{u}||_d$, and $\mathbf{u} = 0$ if $||\mathbf{u}||_d = 0$.

Since $q_1 + q_2\pi$ is invertible modulo π if and only if $\gcd(q_1, d) = 1$, the AFSR synthesis problem for the multisequence $\mathbf{S}$ can be reformulated as follows:

Given the first n prefix of the multisequence $\mathbf{S}$, the AFSR synthesis problem is to find $p_{1,1} + p_{1,2}\pi$, ..., $p_{m,1} + p_{m,2}\pi$ and $q_1 + q_2\pi$ such that $(q_1 + q_2\pi)\alpha_{i,n} = p_{i,1} + p_{i,2}\pi \mod \pi^n$ with $\gcd(q_1, d) = 1$ for all i and its ϕ value is minimum.

The lattice $L_n(\alpha)$ can be partitioned into two parts

$$\begin{aligned} L_n^{(0)}(\alpha) &= \{\mathbf{u} \in \mathbb{Z}^{2m+2}|\ \gcd(q_1, d) > 1\} \text{ and} \\ L_n^{(1)}(\alpha) &= \{\mathbf{u} \in \mathbb{Z}^{2m+2}|\ \gcd(q_1, d) = 1\}. \end{aligned}$$

This AFSR synthesis problem for the multisequence $\mathbf{S}$ is reduced to finding the minimal element in $L_n^{(1)}(\alpha)$ under the $||\cdot||_d$ norm.

Similar to Theorem 2, we can have the following theorem.

Theorem 4 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_{2m+2}$ be the successive minimum vectors of $L_n(\alpha)$ under $||\cdot||_d$ norm and k, $1 \le k \le m+1$, be the smallest integer such that the $2m+1$-th component of v_k is coprime to d. Then $\mathbf{v}_k$ is a minimal element of $L_n^{(1)}(\alpha)$.*

By Theorem 4 and Proposition 2, we get the below theorem.

Theorem 5 *The AFSR synthesis problem over quadratic integer rings for the m-fold multisequence $\mathbf{S}$ of order n can be solved by a polynomial-time algorithm when m is fixed.*

Note. If we define the approximation lattice by

$$\begin{aligned} L_n(\alpha) = \{&(p_{1,1}, p_{1,2}, \ldots, p_{m,1}, p_{m,2}, q_1, q_2) \in \mathbb{R}^{2m+2} : \alpha_{i,n}(q_1 + q_2\pi) \\ &-(p_{i,1} + p_{i,2}\pi) \equiv 0 \mod \pi^n, \text{ for all } 1 \le i \le m\} \end{aligned}$$

and use the norm $\mathcal{N}(a+b\pi)=\sqrt{a^2+b^2}$ and define $\phi(p_{1,1}+\pi p_{1,2},\ldots,p_{m,1}+\pi p_{m,2},q_1+q_2\pi)=\sqrt{\sum_{i=1}^{m}(p_{i,1}^2+p_{i,2}^2)+q_1^2+q_2^2}$, we can get the same result with respect to the ϕ since Theorem 4 is also applicable to l_2. In [21] authors considered this kind of AFSR synthesis problem for a single sequence with respect to the norm assuming that the length of the sequence are long enough such that the AFSR is unique. However, our synthesis algorithm enumerates all possible solutions for any length n.

Likewise, we can also solve the AFSR synthesis problem for multisequences with respect to other norms such as $\phi(p_{1,1}+\pi p_{1,2},\ldots,p_{m,1}+\pi p_{m,2},q_1+q_2\pi)=\max\{\mathcal{N}(p_{1,1}+\pi p_{1,2}),\ldots,\mathcal{N}(p_{m,1}+\pi p_{m,2}),\mathcal{N}(q_1+q_2\pi)\}$ where $\mathcal{N}(a+\pi b)=\max\{|a|,|b|\}$ and $\phi(p_{1,1}+\pi p_{1,2},\ldots,p_{m,1}+\pi p_{m,2},q_1+\pi q_2)=\max\{|p_{1,1}|,|p_{1,2}|,\cdots,|p_{m,1}|,|p_{m,2}|,|q_1|,|q_2|\}$.

6 Conclusions

In this paper, we solve the AFSRs synthesis problems over some residue class rings and some quadratic integer rings for multisequences when the number of multiple sequences is fixed. A natural problem is how about the complexity of this problem when the number varies. We believe that the problem in this case is NP-hard, just as the simultaneous Diophantine approximation problem. This problem and the AFSR synthesis problem over other algebraic structures will be our future work.

Acknowledgement

We gratefully thank Daniele Micciancio and Weihua Liu for fruitful discussions. The research was partially supported by National Natural Science Foundation of China (No. 61170289) and 973 Program (2013CB834203).

References

[1] M. Ajtai, R. Kumar and D. Sivakumar, A sieve algorithm for the shortest lattice vector problem, In Proceedings of STOC'01, pp: 601-610, ACM, July 2001.

[2] M. Ajtai, R. Kumar, D. Sivakumar, Sampling short lattice vectors and the closest lattice vector problem. In Proceedings of the 17th IEEE Annual Conference on Computational Complexity-CCC, 53-57, 2002.

[3] F. Arnault, T.P. Berger and A. Necer, Feedback with carry shift registers synthesis with the Euclidean algorithm, IEEE Trans. Inform. Theory IT-50 (2004) 910-917.

[4] V. Arvind and P. S. Joglekar, Some sieving algorithms for lattice problems. In FSTTCS, 25-36, 2008.

[5] E. R. Berlekamp, Algebraic coding theory. McGraw-Hill, New York (1968).

[6] J. Blömer, S. Naew, Sampling methods for shortest vectors, closest vectors and successive minima of lattices, Theoretical Computer Science 410 (2009) 1648-1665.

[7] J. W. Cassels, An introduction to the geometry of numbers, Springer, 1971.

[8] D. Dadush, C. Peikert, S. Vempala, Enumerative lattice algorithms in any norm via M-Ellipsoid coverings, arXiv: 1011.5666v4.

[9] C. S. Ding, Proof of Massey's conjectured algorithm, Advances in Cryptology, Lecture Notes in Computer Science, vol. 330, Springer, Berlin, 1988, pp. 345-349.

[10] G. L. Feng and K. K. Tzeng, A generalized Euclidean algorithm for multisequence shift-register synthesis, IEEE Trans. Inform. Theory, IT-35 (1989) 584-594.

[11] G. L. Feng and K. K. Tzeng, A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes, IEEE Trans. Inform. Theory, IT-37 (1991) 1274-1287.

[12] M. Goresky and A. Klapper, Algebraic shift register sequences, Cambridge University Press, Cambridge, 2012.

[13] G. Hanrot and D. Stehle, Improved analysis of Kannan's shortest lattice vector algorithm, in: Procedings of Crypto 2007, LNCS 4622, 170-186, 2007.

[14] B. Helfrich, Algorithms to construct Minkowski reduced and Hermite reduced bases, Theoretical Computer Science 41 (1985) 125-139.

[15] H. Hu, L. Hu and D. Feng, On the expected value of the joint 2-adic complexity of periodic binary multisequences, SETA 2006, LNCS 4086, 199-208, 2006.

[16] R. Kannan, Minkowski's convex body theorem and integer programming, Mathematics of Operations Research 12 (1987) 415-440.

[17] A. Klapper, M. Goresky, 2-adic shift registers, Fast software encryption, In Proc. 1993, vol. 809, Cambridge, U.K, 1994, pp. 174-178.

[18] A. Klapper, M. Goresky, Cryptanalysis based on 2-adic rational approxiamtion, In CRYPTO 1995, LNCS 963, 262-273, 1995.

[19] A. Klapper, M. Goresky, Feedback shift registers, 2-adic span, and combiners with memeory, J. Cryptology, vol.10, 11-47, 1997.

[20] A. Klapper and J. Xu, Algebraic feedback shift registers, Theoretical Computer Sciences 226 (1999) 61-92.

[21] W. Liu and A. Klapper, A lattice rational approximation algorithm for AFSRs over quadratic integer rings, SETA 2014, LNCS 8865, pp. 200-211, 2014.

[22] J. L. Massey, Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory 15, 122-127 (1969).

[23] D. Micciancio, Efficient reductions among lattice problems, In: Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2008, Society for Industrial and Applied Mathematics, 84-93, 2008.

[24] D. Micciancio and P. Voulgaris, A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations, In STOC, 351-358, 2010.

[25] W. H. Mill, Continued fractions and linear recurrences, Math. Computation 29 (1975)173-180.

[26] P. Q. Nguyen and D. Stehle, Low-dimensional lattice basis reduction revisited, In Buell, D. A. (ed.) ANTS 2004, LNCS 3076, pp. 338-357, Springer, Heidelberg, 2004.

[27] Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa, A method for solving key equation for decoding Goppa codes, Inform. Contr. 27(1975) 87-99.

[28] L.-P. Wang, Y.-F. Zhu, and D.-Y. Pei, On the lattice basis reduction multisequence synthesis algorithm, IEEE Trans. Inform. Theory 50 (2004) 2905-2910.

[29] J. Xu and A. Klapper, Feedback with carry shift registers over $Z/(N)$, in Proc. SETA'98, New York: Springer-Verleg, 1998.

[30] L. Zhao, Q. Wen, On the joint 2-adic complexity of binary multisequences, RAIRO-Theor. Appl. 46 (2012) 401-412.