SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

March 2016, Vol. 59 032107:1–032107:10
doi: 10.1007/s11432-015-5302-1

On the matrix feedback shift register synthesis for matrix sequences

Liping WANG[1*] & Guang ZENG[2]

[1]*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Zhengzhou Information Science and Technology Institute, Zhengzhou* 450002*, China*

Received December 8, 2014; accepted January 4, 2015; published online November 11, 2015

Abstract In this paper, a generalization of the linear feedback shift register synthesis problem is presented for synthesizing minimum-length matrix feedback shift registers (MFSRs for short) to generate prescribed matrix sequences and so a new complexity measure, that is, matrix complexity, is introduced. This problem is closely related to the minimal partial realization in linear systems and so can be solved through any minimal partial realization algorithm. All minimum-length MFSRs capable of generating a given matrix sequence with finite length are characterized and a necessary and sufficient condition for the uniqueness issue is obtained. Furthermore, the asymptotic behavior of the matrix complexity profile of random vector sequences is determined.

Keywords Berlekamp-Massey algorithm, minimal partial realization, multisequences, σ-LFSR

Citation Wang L P, Zeng G. On the matrix feedback shift register synthesis for matrix sequences. Sci China Inf Sci, 2016, 59(3): 032107, doi: 10.1007/s11432-015-5302-1

1 Introduction

The linear feedback shift register (LFSR for short) synthesis problem plays an important role in design and analysis of stream ciphers and decoding theory. With the development of parallelization [1–3], many kinds of extensions of LFSRs are proposed. Niederreiter presented the multiple-recursive matrix method for pseudorandom number generation [4]. Tsaban and Vishne considered the word-oriented linear transformation shift registers (TSRs for short) [5]. Recently σ-LFSRs were studied in [6–8]. Those prompt us to introduce the problem of synthesizing minimum-length matrix feedback shift registers (MFSRs for short) for generating prescribed matrix sequences.

First we give the detailed description of MFSRs. Let $\mathbb{F}_q$ denote a finite field of order q, where q is a prime power. Let $\mathbb{F}_q^{m\times p}$ be the set of all m by p matrices over $\mathbb{F}_q$. All vectors that appear in this paper are assumed to be row vectors if not explicitly indicated. The $m\times m$ identity matrix is denoted by I_m and the $m\times p$ zero matrix by $\mathbf{0}_{m\times p}$. The m-dimensional zero vector is denoted by $\mathbf{0}_m$.

Definition 1. Assume the first n terms of an infinite sequence $\boldsymbol{S}=(S_1, S_2, \ldots, S_n, \ldots)$ with $S_i\in\mathbb{F}_q^{m\times p}$ are given. For a nonnegative integer d with $d\leqslant n$, let $\boldsymbol{C}(x)=C_dx^d-C_{d-1}x^{d-1}-\cdots-C_0$ with $C_i\in\mathbb{F}_q^{m\times m}$ for $0\leqslant i\leqslant d-1$ and $C_d=I_m$. If

$$S_k=C_{d-1}S_{k-1}+\cdots+C_0S_{k-d} \text{ for } d+1\leqslant k\leqslant n, \tag{1}$$

* Corresponding author (email: wangliping@iie.ac.cn)

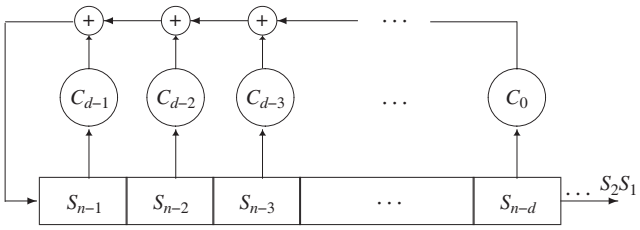

Figure 1 A matrix feedback shift register.

then d and $\boldsymbol{C}(x)$ completely specify the length and the left characteristic polynomial matrix of an MFSR that generates the first n terms of $\boldsymbol{S}$, as shown in Figure 1. The least degree d satisfying (1) is called the nth left matrix complexity of the sequence $\boldsymbol{S}$, denoted by $\mathcal{M}_n^{(m,p)}(\boldsymbol{S})$. The corresponding polynomial is called the nth left minimal polynomial matrix of $\boldsymbol{S}$. The sequence $\{\mathcal{M}_n^{(m,p)}(\boldsymbol{S})\}_{n=1}^{\infty}$ is called the left matrix complexity profile of $\boldsymbol{S}$.

Similarly, we can define an nth right minimal polynomial matrix and the nth right matrix complexity of $\boldsymbol{S}$. However, we do not introduce new notations because the nth right matrix complexity of $\boldsymbol{S}$ is equal to the nth left matrix complexity of $\boldsymbol{S}^{\mathrm{T}}$, that is, $\mathcal{M}_n^{(p,m)}(\boldsymbol{S}^{\mathrm{T}})$, where $\boldsymbol{S}^{\mathrm{T}} = (S_1^{\mathrm{T}}, S_2^{\mathrm{T}}, \ldots)$ and T denotes the transpose of a matrix.

MFSRs can be regarded as a generalization of the classic LFSRs and coincide with them when $m = p = 1$. In this scalar case, the matrix complexity is the linear complexity. If $p = 1$ and $m > 1$, that is, the multisequence case, an MFSR is the so-called multiple-recursive matrix method [4] and its right matrix complexity is the joint linear complexity. Furthermore, if the coefficients C_i are confined in circular rotation operations, shift operations, or AND operations, the model is a σ-LFSR [6–8]. In the same case, if $C_i = a_i D$ where $D \in \mathbb{F}_q^{m\times m}$ and $a_i \in \mathbb{F}_q$ for all i, $0 \leqslant i \leqslant d-1$, an MFSR is a TSR [5].

Now we present the MFSR synthesis problem as follows.

Problem 1. Given the first n terms of a matrix sequence $\boldsymbol{S}$, find a minimum-length MFSR capable of generating these terms.

The well-known Berlekamp-Massey algorithm [9, 10] solves the scalar case of Problem 1. As to the multisequence case, that is, $p = 1$ and $m > 1$, there are also several synthesis algorithms [11–16]. However, they only solved its right case. Recently, in [17, 18] authors considered the similar problem except that the leading coefficient of a minimal polynomial matrix is not required to be an identity matrix. In this paper, we focus on the general MFSR synthesis problem.

Note that the minimal partial realization problem also deals with matrix sequences, which is one of the fundamental problems in linear system theory and a lot of minimal partial realization algorithms were proposed [19–25]. In Section 2, we establish the relationship between two problems and so the MFSR synthesis problem can be solved through a minimal partial realization algorithm.

Also, if $m = p > 1$, Problem 1 can be regarded as the LFSR synthesis problem for a single sequence over rings of matrices. Decoding generalized Reed-Solomon codes over rings of matrices in [26, 27] can be reduced to solving Problem 1. Therefore, it is also necessary to consider the parametrization and the uniqueness issue about minimal polynomial matrices of matrix sequences with finite length. In Section 3, we characterize all nth minimal polynomial matrices of $\boldsymbol{S}$ and give a necessary and sufficient condition for the uniqueness issue.

In [28–32], some asymptotic results about the joint linear complexity profile of multisequences are given. In Section 4, we further study the asymptotic behavior about the left matrix complexity profile of random column vector sequences. Finally, we propose some open problems for the general matrix case in Section 5.

2 A solution to the MFSR synthesis problem

In this section, we give a solution to the MFSR synthesis problem by establishing the link between the MFSR synthesis problem and the minimal partial realization problem since both of them deal with matrix

sequences. Note that a left minimal partial realization algorithm for matrix sequences rather than the right case facilitates a comparison of two problems and so we briefly recall the left case of results in [24].

Identify the matrix sequence $\boldsymbol{S}$ with a formal power series by $\boldsymbol{S}(x)=\sum_{k=1}^{\infty}S_kx^{-k}$. Furthermore, it also can be written as an m by p matrix over a formal Laurent series field $K=\mathbb{F}_q((x^{-1}))$.

There is a valuation v on K whereby for $\alpha=\sum_{k=k_0}^{\infty}a_kx^{-k}\in K$ we put $v(\alpha)=\max\{-k\in\mathbb{Z}:a_k\neq 0\}$ if $\alpha\neq 0$ and $v(\alpha)=-\infty$ if $\alpha=0$. The valuation $v(\boldsymbol{A})$ of an $m\times p$ matrix $\boldsymbol{A}=(\alpha_{ij})_{m\times p}$ over K is defined as $\max\{v(\alpha_{ij}):1\leqslant i\leqslant m,\ 1\leqslant j\leqslant p\}$. We also use the projection $\theta:K^{m\times p}\to\mathbb{F}_q^{m\times p}$ such that $\gamma=(\alpha_{ij})_{m\times p}\mapsto(a_{i,j,-v(\gamma)})_{m\times p}$, where $\alpha_{ij}=\sum_{k=k_0}^{\infty}a_{i,j,k}x^{-k},\ 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant p$. Thus, the valuation and projection can be seen as the generalization of the degree and the leading coefficient of a polynomial, respectively.

Example 1. Let $\gamma=\begin{pmatrix}x^{-2}&x^{-1}\\x^{-1}&x^{-3}\end{pmatrix}$. We have $v(\gamma)=-1$ and $\theta(\gamma)=\begin{pmatrix}0&1\\1&0\end{pmatrix}$.

For a positive integer n, an $m\times m$ nonsingular polynomial matrix $\boldsymbol{M}_n(x)$, and an $m\times p$ polynomial matrix $\boldsymbol{Y}_n(x)$, if the first n terms of the Laurent expansion of $\boldsymbol{M}_n^{-1}(x)\boldsymbol{Y}_n(x)$ are equal to $S_1,S_2,\ldots,S_n$, then $\boldsymbol{M}_n^{-1}(x)\boldsymbol{Y}_n(x)$ is called an nth left partial realization of $\boldsymbol{S}(x)$ or $\boldsymbol{S}$. If the degree of $\det(\boldsymbol{M}_n(x))$ is minimal, then $\boldsymbol{M}_n^{-1}(x)\boldsymbol{Y}_n(x)$ is an nth left minimal partial realization of $\boldsymbol{S}(x)$ or $\boldsymbol{S}$ and the degree is called the nth left McMillan degree of $\boldsymbol{S}$, denoted by $\mathcal{L}_n^{(m,p)}(\boldsymbol{S})$. The sequence $\{\mathcal{L}_n^{(m,p)}(\boldsymbol{S})\}_{n=1}^{\infty}$ is called the left McMillan degree profile of $\boldsymbol{S}$.

So, the minimal partial realization problem for the left case is given as follows.

Problem 2. Given the first n terms of a matrix sequence $\boldsymbol{S}$, find an nth left minimal partial realization of $\boldsymbol{S}(x)$ or $\boldsymbol{S}$.

Let $\mathbb{F}_q[x]^m$ be the $\mathbb{F}_q[x]$-module of dimension m and let $\mathbb{F}_q^m$ denote the m-dimensional vector space over $\mathbb{F}_q$. Define m classes $[\beta_1],\ldots,[\beta_m]$ by

$$[\beta_i]=\{(\underbrace{0,\ldots,0}_{i-1},1,b_1,\ldots,b_{m-i})\in\mathbb{F}_q^m:b_j\in\mathbb{F}_q\text{ for }1\leqslant j\leqslant m-i\},\ i=1,\ldots,m.$$

A nonzero polynomial vector $\boldsymbol{c}(x)=\sum_{i=0}^{d}\boldsymbol{c}_ix^i\in\mathbb{F}_q[x]^m$, where $\boldsymbol{c}_0,\ldots,\boldsymbol{c}_d\in\mathbb{F}_q^m$ and $\boldsymbol{c}_d\neq\boldsymbol{0}_m$, is called an nth left i-annihilating polynomial vector of $\boldsymbol{S}$ if $\boldsymbol{c}_d\in[\beta_i]$ and

$$\boldsymbol{c}_dS_k+\boldsymbol{c}_{d-1}S_{k-1}+\cdots+\boldsymbol{c}_0S_{k-d}=\boldsymbol{0}_p,\tag{2}$$

for all $d+1\leqslant k\leqslant n$. The nth left i-minimal polynomial vector of $\boldsymbol{S}$ is the nth left i-annihilating polynomial vector with the least valuation.

For each i, $1\leqslant i\leqslant m$, it is clear that there always exists an nth left i-minimal polynomial vector of $\boldsymbol{S}$ and we denote them by $\boldsymbol{M}_{n,1}(x),\ldots,\boldsymbol{M}_{n,m}(x)$, respectively. Let $\boldsymbol{M}_n(x)=(\boldsymbol{M}_{n,1}(x)\cdots\boldsymbol{M}_{n,m}(x))^{\mathrm{T}}$ be a matrix and denote the polynomial part of $\boldsymbol{M}_n(x)\boldsymbol{S}(x)$ by $\mathrm{pol}(\boldsymbol{M}_n(x)\boldsymbol{S}(x))$ and we have the following proposition.

Proposition 1 ([24], Theorem 1)**.** If $\boldsymbol{M}_{n,i}(x)$, $1\leqslant i\leqslant m$, is an nth left i-minimal polynomial vector of $\boldsymbol{S}$ and $\boldsymbol{M}_n(x)$ is constructed as above, $\boldsymbol{M}_n^{-1}(x)\mathrm{pol}(\boldsymbol{M}_n(x)\boldsymbol{S}(x))$ is an nth left minimal partial realization of $\boldsymbol{S}$.

The proof is omitted here, see [24] for details.

Note that the valuations of $\boldsymbol{M}_{n,1}(x),\ldots,\boldsymbol{M}_{n,m}(x)$ maybe are not identical and so $\boldsymbol{M}_n(x)$ is not a solution of Problem 1. Therefore, Problems 1 and 2 are not the same problem.

Example 2. Consider a sequence $\boldsymbol{S}=\left(\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\ldots\right)$ over $\mathbb{F}_2$. So, we get a 4th left minimal partial realization of $\boldsymbol{S}$, in which

$$\boldsymbol{M}_4(x)=\begin{pmatrix}x^3+x^2+x+1&x^2+x\\x^2+1&x^2+x+1\end{pmatrix}.$$

However, $\boldsymbol{M}_4(x)$ is not the solution of Problem 1.

Conversely, we have the following proposition. Also, in the sequel we denote the ith row of an $m \times m$ polynomial matrix $\boldsymbol{D}_n(x)$ by $\boldsymbol{D}_{n,i}(x)$ for $1 \leqslant i \leqslant m$.

Proposition 2. If $\boldsymbol{M}_n^{-1}(x)\mathrm{pol}(\boldsymbol{M}_n(x)\boldsymbol{S}(x))$ is an nth left minimal partial realization of $\boldsymbol{S}$, then there exists the same nth left minimal partial realization $\boldsymbol{N}_n^{-1}(x)\mathrm{pol}(\boldsymbol{N}_n(x)\boldsymbol{S}(x))$ of $\boldsymbol{S}$ such that $\boldsymbol{N}_{n,i}(x)$ is an nth left i-minimal polynomial vector of $\boldsymbol{S}$ and the multiset $\{v(\boldsymbol{N}_{n,i}(x)) : 1 \leqslant i \leqslant m\}$ is equal to the multiset $\{v(\boldsymbol{M}_{n,i}(x)) : 1 \leqslant i \leqslant m\}$.

Proof. It is clear that there exists a unimodular matrix $\boldsymbol{U}_n(x)$ (a polynomial matrix is unimodular if its determinant is nonzero element of $\mathbb{F}_q$) such that $\boldsymbol{N}_n(x) = \boldsymbol{U}_n(x)\boldsymbol{M}_n(x)$ satisfying $\boldsymbol{N}_{n,i}(x)$ is an nth left i-minimal polynomial vector of $\boldsymbol{S}$. Furthermore, we have $\boldsymbol{M}_n^{-1}(x)\mathrm{pol}(\boldsymbol{M}_n(x)\boldsymbol{S}(x)) = \boldsymbol{N}_n^{-1}(x)\mathrm{pol}(\boldsymbol{N}_n(x)\boldsymbol{S}(x))$ and so the two multisets are the same.

Example 3. As in Example 2, by Proposition 2 we have

$$\boldsymbol{N}_4(x) = \begin{pmatrix} 0 & 1 \\ 1 & x \end{pmatrix} \boldsymbol{M}_4(x) = \begin{pmatrix} x^2+1 & x^2+x+1 \\ x^2+1 & x^3 \end{pmatrix}.$$

By the above discussion, we get the following theorem.

Theorem 1. If $\boldsymbol{M}_n^{-1}(x)\mathrm{pol}(\boldsymbol{M}_n(x)\boldsymbol{S}(x))$ is an nth left minimal partial realization of $\boldsymbol{S}$, then any nth left minimal polynomial matrix of $\boldsymbol{S}$ has the form $\boldsymbol{C}_n(x) = \boldsymbol{U}_n(x)(f_{n,1}(x)\boldsymbol{M}_{n,1}(x)\cdots f_{n,m}(x)\boldsymbol{M}_{n,m}(x))^{\mathrm{T}}$ and $\mathcal{M}_n^{(m,p)}(\boldsymbol{S}) = \max_{1\leqslant i\leqslant m}\{v(\boldsymbol{M}_{n,i}(x))\}$, where $f_{n,i}(x) \in \mathbb{F}_q[x]$, $\deg(f_{n,i}(x)) = \mathcal{M}_n^{(m,p)}(\boldsymbol{S}) - v(\boldsymbol{M}_{n,i}(x))$, and $U_n(x)$ is unimodular such that $\theta(\boldsymbol{C}_n(x)) = I_m$.

Proof. It is no harm to assume that $\boldsymbol{M}_{n,i}(x)$ is an nth left i-minimal polynomial vector of $\boldsymbol{S}$ by Proposition 2 and so $f_{n,i}(x)\boldsymbol{M}_{n,i}(x)$ satisfies (2) for $1 \leqslant i \leqslant m$. Put $\boldsymbol{D}(x) = (f_{n,1}(x)\boldsymbol{M}_{n,1}(x)\cdots f_{n,m}(x)\boldsymbol{M}_{n,m}(x))^{\mathrm{T}}$ and left multiply $\boldsymbol{D}(x)$ by a unimodular matrix $\boldsymbol{U}_n(x)$ such that

$$\boldsymbol{C}_n(x) = \boldsymbol{U}_n(x)\boldsymbol{D}(x) \text{ and } \theta(\boldsymbol{C}_n(x)) = I_m,$$

and so $\boldsymbol{C}_n(x)$ is an nth left characteristic polynomial matrix of $\boldsymbol{S}$. Suppose that there is an nth left characteristic polynomial matrix $\boldsymbol{C}'_n(x)$ with $v(\boldsymbol{C}'_n(x)) < \mathcal{M}_n^{(m,p)}(\boldsymbol{S}) = v(\boldsymbol{M}_{n,t}(x))$ for some t, $1 \leqslant t \leqslant m$. Thus, $\boldsymbol{C}'_{n,t}(x)$ is an nth left t-annihilating polynomial vector of $\boldsymbol{S}$ with its valuation less than $v(\boldsymbol{M}_{n,t}(x))$. This is impossible.

By Theorem 1, one can solve Problem 1 by simply putting

$$f_{n,i}(x) = x^{\max_{1\leqslant i\leqslant m}\{v(\boldsymbol{M}_{n,i}(x))\}-v(\boldsymbol{M}_{n,i}(x))}$$

once the solution of Problem 2 is obtained.

Example 4. By Theorem 1, we have $\boldsymbol{C}_4(x) = \begin{pmatrix} x^3+x^2+x+1 & x^2+x \\ x^2+1 & x^3 \end{pmatrix}$, which is a 4th left minimal polynomial matrix of $\boldsymbol{S}$ in Example 2.

3 Parametrization and uniqueness of nth left minimal polynomial matrices of $\boldsymbol{S}$

In this section, we recall a lattice-based minimal partial realization algorithm in [24,25] and deduce a new result, that is, Theorem 2, from which we determine the more detailed parametrization and uniqueness issue about the nth left minimal polynomial matrices of $\boldsymbol{S}$.

3.1 A lattice-based minimal partial realization

A subset Λ of K^{p+m} is called an $\mathbb{F}_q[x]$-lattice if there exists a basis $\omega_1, \ldots, \omega_{p+m}$ of K^{p+m} such that

$$\Lambda = \left\{ \sum_{i=1}^{p+m} f_i(x)\,\omega_i : f_i(x) \in \mathbb{F}_q[x], \quad i = 1, \ldots, p+m \right\}.$$

In this situation, we say that $\omega_1,\ldots,\omega_{p+m}$ form a basis for Λ. For $i\in\{1,\ldots,p+m\}$, the value

$$\lambda_i(\Lambda):=\min\{\lambda\in\mathbb{Z}|\text{ there exist }\mathbb{F}_q[x]\text{-linearly independent }\alpha_1,\ldots,\alpha_i\in\Lambda\text{ with }v(\alpha_j)\leqslant\lambda,\ 1\leqslant j\leqslant i\}$$

is called the ith successive minimum of Λ. A basis $\omega_1,\ldots,\omega_{p+m}$ is reduced if $\theta(\omega_1),\ldots,\theta(\omega_{p+m})$ are linearly independent over $\mathbb{F}_q$. It is not unique, but the numbers $\lambda_i=v(\omega_i)$ are successive minima of the lattice if one rearranges the order of elements in the reduced basis such that $v(\omega_1)\leqslant\cdots\leqslant v(\omega_{p+m})$. The determinant of the lattice is defined by $\det(\Lambda)=v(\det(\omega_1,\ldots,\omega_{p+m}))$ and is independent of the choice of the basis. In [33], it was proved that

$$\sum_{i=1}^{p+m}v(\omega_i)=\det(\Lambda)\tag{3}$$

if the basis $\omega_1,\ldots,\omega_{p+m}$ is reduced. For any vector γ, let $\overline{\gamma}$ be the vector containing only the last m components of γ. The reduced basis is normal if $\overline{\theta(\omega_i)}=\mathbf{0}_m$ for $1\leqslant i\leqslant p$ and $\overline{\theta(\omega_{p+i})}\in[\beta_i]$ for $1\leqslant i\leqslant m$.

Consider the matrix

$$\begin{pmatrix}I_p & \mathbf{0}_{p\times m}\\ \boldsymbol{S}(x) & I_m x^{-n-1}\end{pmatrix}$$

and denote its $p+m$ rows by $\varepsilon_1,\ldots,\varepsilon_p,\alpha_{n,1},\ldots,\alpha_{n,m}$, which span an $\mathbb{F}_q[x]$-lattice, simply denoted by $\Lambda_n(\boldsymbol{S})$. By (3), it is clear that

$$\det(\Lambda_n(\boldsymbol{S}))=-m(n+1).\tag{4}$$

The mapping $\eta:\Lambda_n(\boldsymbol{S})\to\mathbb{F}_q[x]^m$ is given by

$$f_1(x)\varepsilon_1+\cdots+f_p(x)\varepsilon_p+f_{p+1}(x)\alpha_{n,1}+\cdots+f_{p+m}(x)\alpha_{n,m}\mapsto(f_{p+1}(x),\ldots,f_{p+m}(x)),$$

where $f_1(x),\ldots,f_{p+m}(x)\in\mathbb{F}_q[x]$. Conversely, a nonzero polynomial vector $\boldsymbol{c}(x)\in\mathbb{F}_q[x]^m$ completely determines its associated element in $\Lambda_n(\boldsymbol{S})$ which is given by

$$\sigma(\boldsymbol{c}(x))|_{\Lambda_n(\boldsymbol{S})}:=(\boldsymbol{c}(x)\boldsymbol{S}(x)-\mathrm{Pol}(\boldsymbol{c}(x)\boldsymbol{S}(x)),\boldsymbol{c}(x)x^{-n-1}).$$

By the definition of the normal basis, the following proposition can be obtained, see [24] for a detailed proof.

Proposition 3 ([24], Theorem 3)**.** Let $\omega_1,\ldots,\omega_{p+m}$ be a normal basis for $\Lambda_n(\boldsymbol{S})$. Then, $\eta(\omega_{p+i})$ for $1\leqslant i\leqslant m$ is an nth left i-minimal polynomial vector of $\boldsymbol{S}$.

By Propositions 1 and 3, one can solve Problem 2. Also, by Proposition 3, the set $\{v(\eta(\omega_{p+i})):1\leqslant i\leqslant m\}$ is completely determined by the sequence $\boldsymbol{S}$ and is called the nth left complexity multiset of $\boldsymbol{S}$, denoted by $\{\mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}):1\leqslant i\leqslant m\}$. By the construction of $\boldsymbol{M}_n(x)$, we have

$$\mathcal{L}_n^{(m,p)}(\boldsymbol{S})=\sum_{i=1}^{m}\mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}).\tag{5}$$

For a lattice Λ in K^{p+m}, its dual lattice Λ' is defined by

$$\Lambda'=\{\gamma'\in K^{p+m}:\gamma\cdot\gamma'\in\mathbb{F}_q[x],\text{ for all }\gamma\in\Lambda\},$$

where $\gamma\cdot\gamma'=\sum_{j=1}^{p+m}\gamma_j(x)\gamma'_j(x)$ for $\gamma=(\gamma_1(x),\ldots,\gamma_{p+m}(x))$ and $\gamma'=(\gamma'_1(x),\ldots,\gamma'_{p+m}(x))$.

Thus, the vectors $(\underbrace{-1,0,\ldots,0}_{p},S_{11}(x)x^{n+1},S_{21}(x)x^{n+1},\ldots,S_{m1}(x)x^{n+1})$, $(\underbrace{0,-1,\ldots,0}_{p},\ S_{12}(x)x^{n+1},$ $S_{22}(x)x^{n+1},\ldots,S_{m2}(x)x^{n+1}),\ldots,(\underbrace{0,\ldots,-1}_{p},S_{1p}(x)x^{n+1},\ \ \ldots,\ \ S_{mp}(x)x^{n+1})$, $(\underbrace{0,\ldots,0}_{p},x^{n+1},0,\ldots,0)$,

$(\underbrace{0,\ldots,0}_{p},0,\ x^{n+1},\ \ldots,0),\ldots,(\underbrace{0,\ldots,0}_{p},0,\ldots,0,\ x^{n+1})$ form the basis for the dual lattice $\Lambda'_n(\boldsymbol{S})$ of $\Lambda_n(\boldsymbol{S})$ and so we have

$$\Lambda'_n(\boldsymbol{S}) = x^{n+1}\Lambda_n(\boldsymbol{S}^{\mathrm{T}}). \tag{6}$$

Lemma 1 ([34], Corollary 1)**.** Let $\lambda_1,\ldots,\lambda_{p+m}$ be the successive minima of a lattice Λ, and $\lambda'_1,\ldots,\lambda'_{p+m}$ be the successive minima of its dual lattice Λ'. We have

$$\lambda_i + \lambda'_{p+m-i+1} = 0,\ \text{for } i = 1,2,\ldots,p+m.$$

Theorem 2. Let $\omega_1,\ldots,\omega_{p+m}$ be a normal basis of the lattice $\Lambda_n(\boldsymbol{S})$. Then, the multiset $\{v(\omega_1),\ldots,v(\omega_p)\} = \{-\mathcal{L}_{n,1}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}),\ldots,-\mathcal{L}_{n,p}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}})\}$, and $\{v(\omega_{p+1}),\ldots,v(\omega_{p+m})\} = \{-n-1+\mathcal{L}_{n,1}^{(m,p)}(\boldsymbol{S}),\ldots,-n-1+\mathcal{L}_{n,m}^{(m,p)}(\boldsymbol{S})\}$.

Proof. Let $\tau_1,\ldots,\tau_{p+m}$ be a normal basis for the lattice $\Lambda_n(\boldsymbol{S}^{\mathrm{T}})$ and so the multiset $\{n+1+v(\tau_1),\ldots,n+1+v(\tau_m),\mathcal{L}_{n,1}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}),\ldots,\mathcal{L}_{n,p}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}})\}$ is a permutation of the successive minima of $\Lambda'_n(\boldsymbol{S})$ by (6). The multiset $\{v(\omega_1),\ldots,v(\omega_p),\ -n-1+\mathcal{L}_{n,1}^{(m,p)}(\boldsymbol{S}),\ldots,-n-1+\mathcal{L}_{n,m}^{(m,p)}(\boldsymbol{S})\}$ is a permutation of the successive minima of $\Lambda_n(\boldsymbol{S})$. Let $\boldsymbol{S}_0$ be the matrix sequence obtained by the nth minimal partial realization of $\boldsymbol{S}$ from the normal basis. For any integer $l \geqslant n$, the multiset $\{v(\omega_1),\ldots,v(\omega_p),\ -l-1+\mathcal{L}_{n,1}^{(m,p)}(\boldsymbol{S}),\ldots,-l-1+\mathcal{L}_{n,m}^{(m,p)}(\boldsymbol{S})\}$ is a permutation of the successive minima of $\Lambda_l(\boldsymbol{S}_0)$ and the multiset $\{l+1+v(\tau_1),\ldots,l+1+v(\tau_m),\mathcal{L}_{n,1}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}),\ldots,\mathcal{L}_{n,p}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}})\}$ is a permutation of the successive minima of $\Lambda'_l(\boldsymbol{S}_0)$. Therefore, by Lemma 1, we obtain the required results.

Corollary 1. For the matrix sequence $\boldsymbol{S}$, we have

$$\mathcal{L}_n^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) = \sum_{j=1}^{p}\mathcal{L}_{n,j}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) = \sum_{i=1}^{m}\mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}) = \mathcal{L}_n^{(m,p)}(\boldsymbol{S}).$$

3.2 Characterization of all nth left minimal polynomial matrices of $\boldsymbol{S}$

In this section, we characterize all nth left minimal polynomial matrices of $\boldsymbol{S}$ as follows.

Theorem 3. Let $\omega_1,\ldots,\omega_{p+m}$ be a normal basis of $\Lambda_n(\boldsymbol{S})$ and assume that $v(\omega_j) = -\mathcal{L}_{n,j}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}})$ for $1 \leqslant j \leqslant p$. Then, any nth left minimal polynomial matrix of $\boldsymbol{S}$ can be obtained by

$$\boldsymbol{C}_n(x) = \boldsymbol{U}_n(x)\begin{pmatrix} f_{n,1}(x)(\eta(\omega_{p+1}) + \sum_{j=1}^{p} g_{1,j}^{(n)}(x)\eta(\omega_j)) \\ \cdots \\ f_{n,m}(x)(\eta(\omega_{p+m}) + \sum_{j=1}^{p} g_{m,j}^{(n)}(x)\eta(\omega_j)) \end{pmatrix},$$

where for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant p$, $f_{n,i}(x)$ and $g_{i,j}^{(n)}(x) \in \mathbb{F}_q[x]$ such that $\deg(g_{i,j}^{(n)}(x)) \leqslant -n-1+\mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}) + \mathcal{L}_{n,j}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}})$, $\deg(f_{n,i}(x)) = \mathcal{M}_n^{(m,p)}(\boldsymbol{S}) - \mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S})$, and $\boldsymbol{U}_n(x)$ is unimodular such that $\theta(\boldsymbol{C}_n(x)) = I_m$.

Proof. Since $\omega_1,\ldots,\omega_{p+m}$ is a normal basis for $\Lambda_n(\boldsymbol{S})$, the associated element $\sigma(\boldsymbol{M}_{n,i}(x))|_{\Lambda_n(\boldsymbol{S})}$ of $\boldsymbol{M}_{n,i}(x)$, which is the ith row of an nth left minimal partial realization $\boldsymbol{M}_n^{-1}(x)\mathrm{pol}(\boldsymbol{M}_n(x)\boldsymbol{S}(x))$ of $\boldsymbol{S}$, must be a linear combination of $\omega_1,\ldots,\omega_p$ over $\mathbb{F}_q[x]$, that is, $\sigma(\boldsymbol{M}_{n,i}(x))|_{\Lambda_n(\boldsymbol{S})} = \omega_{p+i} + \sum_{j=1}^{p} g_{i,j}^{(n)}(x)\omega_j$, where $g_{i,j}^{(n)}(x)$ is required as above by Theorem 2. By Theorem 1, we have

$$\sigma(\boldsymbol{C}_{n,i}(x))|_{\Lambda_n(\boldsymbol{S})} = f_{n,i}(x)\sigma(\boldsymbol{M}_{n,i}(x))|_{\Lambda_n(\boldsymbol{S})},$$

where the requirement of $f_{n,i}(x)$ can be easily obtained. As to the choice of $\boldsymbol{U}_n(x)$, it is similar to that in Theorem 1.

Corollary 2. The number of all nth left minimal polynomial matrices of $\boldsymbol{S}$ is

$$q^{m\mathcal{M}_n^{(m,p)}(\boldsymbol{S}) - \mathcal{L}_n^{(m,p)}(\boldsymbol{S}) + \sum_{i=1}^{m}\sum_{j=1}^{p}(\delta_{i,j}+1)(\mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}) + \mathcal{L}_{n,j}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) - n)},$$

where $\delta_{i,j} = \begin{cases} -1, & \text{if } \mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}) + \mathcal{L}_{n,j}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) - n - 1 < 0, \\ 0, & \text{else.} \end{cases}$

Table 1 Example 5.

$\begin{pmatrix} x^3+x+1 & x^3+x^2+x+1 \\ x^2 & x^3+1 \end{pmatrix}$	$\begin{pmatrix} x^3+x^2+1 & x^3+1 \\ 1 & x^3+x^2+x \end{pmatrix}$	$\begin{pmatrix} x^3 & x^3+x^2+x \\ 1 & x^3+x^2+x \end{pmatrix}$
$\begin{pmatrix} x^3+x^2+1 & x^3+1 \\ x & x^3+x^2+x+1 \end{pmatrix}$	$\begin{pmatrix} x^3 & x^3+x^2+x \\ x^2+x+1 & x^3 \end{pmatrix}$	$\begin{pmatrix} x^3 & x^3+x^2+x \\ x^2 & x^3+1 \end{pmatrix}$
$\begin{pmatrix} x^3+x+1 & x^3+x^2+x+1 \\ x^2+x+1 & x^3 \end{pmatrix}$	$\begin{pmatrix} x^3+x^2+x & x^3 \\ 1 & x^3+x^2+x \end{pmatrix}$	$\begin{pmatrix} x^3+x^2+x & x^3 \\ x^2+x+1 & x^3 \end{pmatrix}$
$\begin{pmatrix} x^3+x^2+x & x^3 \\ x & x^3+x^2+x+1 \end{pmatrix}$	$\begin{pmatrix} x^3+x^2+1 & x^3+1 \\ x^2 & x^3+1 \end{pmatrix}$	$\begin{pmatrix} x^3 & x^3+x^2+x \\ x & x^3+x^2+x+1 \end{pmatrix}$
$\begin{pmatrix} x^3+x+1 & x^3+x^2+x+1 \\ 1 & x^3+x^2+x \end{pmatrix}$	$\begin{pmatrix} x^3+x^2+1 & x^3+1 \\ x^2+x+1 & x^3 \end{pmatrix}$	$\begin{pmatrix} x^3+x^2+x & x^3 \\ x^2 & x^3+1 \end{pmatrix}$
$\begin{pmatrix} x^3+x+1 & x^3+x^2+x+1 \\ x & x^3+x^2+x+1 \end{pmatrix}$		

Example 5. By the algorithm in [24], a normal basis of the lattice $\Lambda_5(\boldsymbol{S})$ in Example 2 is

$$\begin{aligned}
&\omega_1 = (x^{-4}, x^{-3}+x^{-4}+x^{-5}, x^{-5}+x^{-6}, x^{-6}),\\
&\omega_2 = (x^{-3}+x^{-4}, x^{-3}+x^{-5}, x^{-4}+x^{-6}, x^{-4}+x^{-5}+x^{-6}),\\
&\omega_3 = (x^{-4}, x^{-3}+x^{-4}, x^{-3}+x^{-4}+x^{-5}+x^{-6}, x^{-4}+x^{-5}),\\
&\omega_4 = (x^{-4}, x^{-3}+x^{-5}, x^{-3}+x^{-5}+x^{-6}, x^{-3}+x^{-4}+x^{-5}+x^{-6}).
\end{aligned}$$

By Theorem 3, we list all 5th left minimal polynomial matrices of $\boldsymbol{S}$ in Table 1.

3.3 Uniqueness issue

By Theorem 3, we get the following theorem.

Theorem 4. The nth left minimal polynomial matrix of $\boldsymbol{S}$ is unique if and only if $\mathcal{M}_n^{(m,p)}(\boldsymbol{S}) + \mathcal{M}_n^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) < n+1$ and $\mathcal{L}_{n,1}^{(m,p)}(\boldsymbol{S}) = \cdots = \mathcal{L}_{n,m}^{(m,p)}(\boldsymbol{S})$.

The following corollaries follow from Theorem 4.

Corollary 3. If $(m+1)\mathcal{M}_n^{(m,p)}(\boldsymbol{S}) < n+1$ and $\mathcal{L}_{n,1}^{(m,p)}(\boldsymbol{S}) = \cdots = \mathcal{L}_{n,m}^{(m,p)}(\boldsymbol{S})$, then the nth minimal polynomial matrix of the sequence $\boldsymbol{S}$ is unique.

Proof. It follows from Corollary 1 that

$$\mathcal{M}_n^{(m,p)}(\boldsymbol{S}) + \mathcal{M}_n^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) \leqslant \mathcal{M}_n^{(m,p)}(\boldsymbol{S}) + \sum_{j=1}^{p} \mathcal{L}_{n,j}^{(p,m)}(\boldsymbol{S}^{\mathrm{T}}) \leqslant \mathcal{M}_n^{(m,p)}(\boldsymbol{S}) + \sum_{i=1}^{m} \mathcal{L}_{n,i}^{(m,p)}(\boldsymbol{S}) < n+1.$$

So, we obtain the required result by applying Theorem 4.

Corollary 4. If $p=1$ and $\mathcal{L}_{n,1}^{(m,p)}(\boldsymbol{S}) = \cdots = \mathcal{L}_{n,m}^{(m,p)}(\boldsymbol{S})$, then the nth left minimal polynomial matrix of $\boldsymbol{S}$ is unique if and only if $(m+1)\mathcal{M}_n^{(m,p)}(\boldsymbol{S}) < n+1$.

Proof. The sufficient condition is obtained by Corollary 3. Conversely, by Corollary 1 we get

$$(m+1)\mathcal{M}_n^{(m,1)}(\boldsymbol{S}) = \mathcal{M}_n^{(m,1)}(\boldsymbol{S}) + \mathcal{L}_{n,1}^{(1,m)}(\boldsymbol{S}^{\mathrm{T}}).$$

The required result is obtained by Theorem 4.

Example 6. A normal basis of the lattice $\Lambda_6(\boldsymbol{S})$ in Example 2 is

$$\begin{aligned}
&\omega_1 = (x^{-4}, x^{-3}+x^{-4}+x^{-6}, x^{-6}+x^{-7}, x^{-7}),\\
&\omega_2 = (x^{-2}+x^{-3}+x^{-4}, x^{-2}+x^{-3}+x^{-4}+x^{-5}+x^{-6}, x^{-7}, x^{-7}),\\
&\omega_3 = (x^{-4}, x^{-5}+x^{-6}, x^{-4}+x^{-5}+x^{-6}+x^{-7}, x^{-5}+x^{-6}),\\
&\omega_4 = (x^{-4}, x^{-6}, x^{-4}+x^{-6}+x^{-7}, x^{-4}+x^{-5}+x^{-6}+x^{-7}).
\end{aligned}$$

Therefore, the 6th left minimal polynomial matrix $\begin{pmatrix} x^3+x^2+x+1 & x^2+x \\ x^2 & x^3+1 \end{pmatrix}$ of $\boldsymbol{S}$ is unique by Theorem 4 because $\mathcal{M}_6^{(2,2)}(\boldsymbol{S})+\mathcal{M}_6^{(2,2)}(\boldsymbol{S}^{\mathrm{T}})=3+3<6+1$ and $\mathcal{L}_{6,1}^{(2,2)}(\boldsymbol{S})=\mathcal{L}_{6,2}^{(2,2)}(\boldsymbol{S})=3$.

4 The asymptotic behavior of the matrix complexity profile for random vector sequences

In this section, let $\boldsymbol{S}$ denote a random column vector sequence over $\mathbb{F}_q$. We present the asymptotic behavior of the left matrix complexity profile of $\boldsymbol{S}$ by first deducing the result for the left McMillan degree profile of $\boldsymbol{S}$.

Let $(\mathbb{F}_q^{m\times p})^\infty$ be the m by p matrix sequence space over $\mathbb{F}_q$. Let $\mu_{q,pm}$ be the uniform probability measure on $\mathbb{F}_q^{m\times p}$ which assigns the measure q^{-pm} to each element of $\mathbb{F}_q^{m\times p}$. Then, $\mu_{q,pm}^\infty$ is the complete product measure on $(\mathbb{F}_q^{m\times p})^\infty$ induced by $\mu_{q,pm}$. In particular, when $p=1$, we use $\mu_{q,m}^\infty$.

In [29] it was proved that we have $\mu_{q,m}^\infty$-almost everywhere (abbreviated $\mu_{q,m}$-a.e.),

$$\lim_{n\to\infty}\frac{\mathcal{L}_n^{(1,m)}(\boldsymbol{S}^{\mathrm{T}})}{n}=\frac{m}{m+1}.$$

Later, the following refinement of the bounds was shown in [30,31]: we have $\mu_{q,m}^\infty$-a.e.,

$$-\frac{1}{m+1}\leqslant\liminf_{n\to\infty}\frac{\mathcal{L}_n^{(1,m)}(\boldsymbol{S}^{\mathrm{T}})-\frac{mn}{m+1}}{\log_q n}\leqslant\limsup_{n\to\infty}\frac{\mathcal{L}_n^{(1,m)}(\boldsymbol{S}^{\mathrm{T}})-\frac{mn}{m+1}}{\log_q n}\leqslant\frac{1}{m+1},$$

where $\log_q$ denotes the logarithm to the base q.

By Corollary 1, the following theorem is obtained.

Theorem 5. For any prime power q and any integer $m\geqslant 1$, we have $\mu_{q,m}^\infty$-a.e.,

$$-\frac{1}{m+1}\leqslant\liminf_{n\to\infty}\frac{\mathcal{L}_n^{(m,1)}(\boldsymbol{S})-\frac{mn}{m+1}}{\log_q n}\leqslant\limsup_{n\to\infty}\frac{\mathcal{L}_n^{(m,1)}(\boldsymbol{S})-\frac{mn}{m+1}}{\log_q n}\leqslant\frac{1}{m+1}.$$

In particular, we have $\mu_{q,m}^\infty$-a.e.,

$$\lim_{n\to\infty}\frac{\mathcal{L}_n^{(m,1)}(\boldsymbol{S})}{n}=\frac{m}{m+1}.$$

Let $E(\xi)$ denote the expected value of a random variable ξ. In [29,31] it was shown that

$$E(\mathcal{L}_n^{(1,m)}(\boldsymbol{S}^{\mathrm{T}}))=\frac{mn}{m+1}+O(1)\ \text{ as } n\to\infty. \tag{7}$$

Also by Corollary 1, we give the result about the expected value of $\mathcal{L}_n^{(m,1)}(\boldsymbol{S})$.

Theorem 6. For any prime power q and any integer $m\geqslant 1$, we have

$$E(\mathcal{L}_n^{(m,1)}(\boldsymbol{S}))=\frac{mn}{m+1}+O(1)\ \text{ as } n\to\infty.$$

Theorem 7. For any prime power q, any integer $m\geqslant 1$, and any integer i with $1\leqslant i\leqslant m$, we have

$$E(\mathcal{L}_{n,i}^{(m,1)}(\boldsymbol{S}))=\frac{n}{m+1}+O(1)\ \text{ as } n\to\infty.$$

Proof. It follows from (5) that

$$E(\mathcal{L}_n^{(m,1)}(\boldsymbol{S}))=\sum_{i=1}^m E(\mathcal{L}_{n,i}^{(m,1)}(\boldsymbol{S})).$$

In view of the symmetry of $\mathcal{L}_{n,1}^{(m,1)}(\boldsymbol{S}),\ldots,\mathcal{L}_{n,m}^{(m,1)}(\boldsymbol{S})$, they have the same probability distribution. Thus, we get the required result by applying Theorem 6.

Theorem 7 shows that each element of complexity multiset of the vast majority of m-dimensional column vector sequences should be close to the line $\frac{n}{m+1}$.

Table 2 Data distribution.

$L=L_n^{(m,p)}(\boldsymbol{S})$	$N_7^{(2,2)}(L)$	$N_6^{(2,2)}(L)$	$N_2^{(3,3)}(L)$	$N_2^{(3,2)}(L)$
0	1	1	1	1
1	18	18	98	42
2	312	312	5341	861
3	5184	5184	118650	2646
4	83904	80016	124950	546
5	1254672	991044	12936	
6	16111428	8069397	168	
7	106094997	6578442		
8	128095242	978792		
9	15524712	69984		
10	1189536	3840		
11	71424	180		
12	3840	6		
13	180			
14	6			

Theorem 8. For any prime power q and any integer $m \geqslant 1$, we have

$$E(\mathcal{M}_n^{(m,1)}(\boldsymbol{S})) = \frac{n}{m+1} + O(1) \ \text{ as } n \to \infty.$$

Proof. The result follows Theorem 7 since $E(\mathcal{M}_n^{(m,1)}(\boldsymbol{S})) = \max\{E(\mathcal{L}_{n,i}^{(m,1)}(\boldsymbol{S})) : 1 \leqslant i \leqslant m\}$.

Theorem 8 and Eq. (7) show that the left matrix complexity and the right matrix complexity of the vast majority of m-dimensional column vector sequences should be close to the line $\frac{n}{m+1}$ and the line $\frac{mn}{m+1}$, respectively.

5 Some open problems

Let $N_n^{(m,p)}(L)$ denote the number of $m \times p$ matrix sequences with length n over $\mathbb{F}_q$ whose McMillan degree is L. In Table 2, we demonstrate the data distribution of $N_n^{(m,p)}(L)$ for all possible L when $q=2$, and some specified n, m, p.

So, we propose three open problems for the general case as our future work. In this section, let $\boldsymbol{S}$ denote a random $m \times p$ matrix sequence over $\mathbb{F}_q$.

1. How to get the bound for $N_n^{(m,p)}(L)$.
2. For any prime power q and any integers m and p, we guess

$$\lim_{n\to\infty} \frac{L_n^{(m,p)}(\boldsymbol{S})}{n} = \frac{pm}{p+m} \quad \mu_{q,pm}^{\infty} - \text{a.e.}$$

3. The expected value of the nth McMillan degree of random $m \times p$ matrix sequence $\boldsymbol{S}$ with length n is guessed by

$$E(L_n^{(m,p)}(\boldsymbol{S})) = \frac{pmn}{p+m} + O(1) \quad n \to \infty.$$

Generally speaking, we guess that the left matrix complexity and the right matrix complexity of the vast majority of $m \times p$ matrix sequences should be very close to the line $\frac{pn}{p+m}$ and the line $\frac{mn}{p+m}$, respectively.

Acknowledgements This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2013CB834203) and National Natural Science Foundation of China (Grant Nos. 61170289, 61003291).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Dawson E, Simpson L. Analysis and design issues for synchronous stream ciphers. In: Niederreiter H, ed. Coding Theory and Cryptology. Singapore: World Scientific, 2002. 49–90
2 Ekdahl P, Johansson T. A new version of the stream ciphers SNOW. In: Proceedings of 9th Annual International Workshop on Selected Areas in Cryptography, Newfoundland, 2002. 47–61
3 Hawkes P, Rose G G. Exploiting multiples of the connection polynomial in word-oriented stream ciphers. In: Proceedings of 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, 2000. 303–316
4 Niederreiter H. Factorization of polynomials and some linear algebra problems over finite fields. Linear Alg Appl, 1993, 192: 301–328
5 Tsaban B, Vishne U. Efficient linear feedback shift registers with maximal period. Finite Fields Appl, 2002, 8: 256–267
6 Zeng G, Han W, He K. High efficiency feedback shift register: σ-LFSR. Cryptology ePrint Archive, Report 2007/114, 2007
7 Zeng G, He K, Han W. A trinomial type of σ-LFSR oriented toward software implementation. Sci China Ser-F: Inf Sci, 2007, 50: 359–372
8 Zeng G, Yang Y, Han W , et al. Word oriented cascade jump σ-LFSR. In: Proceedings of 18th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Tarragona, 2009. 127–136
9 Berlekamp E R. Algebraic Coding Theory. New York: McGraw-Hill, 1968
10 Massey J L. Shift-register synthesis and BCH decoding. IEEE Trans Inform Theory, 1969, 15: 122–127
11 Dai Z D, Wang K P, Ye D F. m-Continued fraction expansions of multi-Laurent series (in Chinese). Adv Math, 2004, 33: 246–248
12 Dai Z D, Wang K P, Ye D F. Multi-continued fraction algorithm on multi-formal Laurent series. Acta Arithmet, 2006, 122: 1–16
13 Dai Z D, Yang J H. Multi-continued fraction algorithm and generalized B-M algorithm over F_q. Finite Fields Appl, 2006, 12: 379–402
14 Ding C S. Proof of Massey's conjectured algorithm. In: Proceedings of Workshop on the Theory and Application of Cryptographic Techniques, Davos, 1988. 345–349
15 Feng G L, Tzeng K K. A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes. IEEE Trans Inform Theory, 1991, 37: 1274–1287
16 Wang L P, Zhu Y F, Pei D Y. On the lattice basis reduction multisequence synthesis algorithm. IEEE Trans Inform Theory, 2004, 50: 2905–2910
17 Kaltofen F, Yuhasz G. On the matrix Berlekamp-Massey algorithm. ACM Trans Algorithm, 2013, 9: 33
18 Kaltofen F, Yuhasz G. A fraction free matrix Berlekamp/Massey algorithm. Linear Alg Appl, 2013, 439: 2515–2526
19 Antoulas A C. On recursiveness and related topics in linear systems. IEEE Trans Automat Control, 1985, 31: 1121–1135
20 Dickinson B W, Morf M, Kailath D. A minimal realization algorithm for matrix sequences. IEEE Trans Automat Control, 1974, 19: 31–38
21 Gragg W B, Lindquist A. On the partial realization problem. Linear Alg Appl, 1983, 50: 277–319
22 Kuijper M. An algorithm for constructing a minimal partial realization in the multivariable case. Syst Contr Lett, 1997, 31: 225–233
23 van Barel M, Bultheel M A. A generalized minimal partial realization problem. Linear Alg Appl, 1997, 254: 527–551
24 Wang L P. A lattice-based minimal partial realization algorithm. In: Proceedings of 5th International Conference on Sequences and Their Applications, Lexington, 2008. 278–289
25 Wang L P. A lattice-based minimal partial realization algorithm for matrix sequences of varying length. Cryptogr Commun, 2011, 3: 29–42
26 Wang L P. Lagrange interpolation polynomials and generalized Reed-Solomon codes over rings of matrices. In: Proceedings of IEEE International Symposium on Information Theory, Cambridge, 2012. 3098–3100
27 Quintin G, Barbier M, Chabot C. On generalized Reed-Solomon codes over commutative and noncommutative rings. IEEE Trans Inform Theory, 2013, 59: 5882–5897
28 Dai Z D, Imamura K, Yang J H. Asymptotic behavior of normalized linear complexity of multi-sequences. In: Proceeding of 3rd International Conference on Sequences and Their Applications, Seoul, 2004. 126–142
29 Niederreiter H, Wang L P. Proof of a conjecture on the joint linear complexity profile of multisequences. In: Proceeding of 6th International Conference on Cryptology in India, Bangalore, 2005. 13–22
30 Niederreiter H, Wang L P. The asymptotic behavior of the joint linear complexity profile of multisequences. Monatsh Math, 2007, 150: 141–155
31 Niederreiter H, Vielhaber M, Wang L P. Improved results on the probabilistic theory of the joint linear complexity of multisequences. Sci China Inf Sci, 2012, 55: 165–170
32 Wang L P, Niederreiter H. Enumeration results on the joint linear complexity of multisequences. Finite Fields Appl, 2006, 12: 613–637
33 Mahler K. An analogue to Minkowski's geometry of numbers in a field of series. Ann Math, 1941, 42: 488–522
34 Couture R, L'Ecuyer P. Lattice computations for random numbers. Math Comput, 2000, 69: 757–765