Galois 型移位寄存器可转换为 Fibonacci 型移位寄存器的图条件

王腾艺[1]，刘新芸[2]，邹云蕾[1†]

(1. 扬州大学 数学学院，江苏 扬州 225002；2. 潍坊学院 数学与统计学院，山东 潍坊 261061)

摘　要: 研究 Galois 型非线性反馈移位寄存器可等价转换为 Fibonacci 型非线性反馈移位寄存器的充分必要图条件, 旨在为两类移位寄存器结构间的等价转换提供理论支撑与判定框架. 首先, 基于矩阵半张量积理论, 建立 Galois 型与 Fibonacci 型非线性反馈移位寄存器演化方程的代数形式, 进而推导二者可相互转换的代数判定条件; 然后, 从 Fibonacci 型非线性反馈移位寄存器的状态转移矩阵出发, 深入分析其内在的状态传递特征, 引入集合划分方法, 进而建立两类非线性反馈移位寄存器可相互转换的图论判定准则; 此外, 依据所提出的转换条件, 设计相应的结构转换算法, 实现 Galois 型向 Fibonacci 型非线性反馈移位寄存器的结构转化; 最后, 通过两个具体的数值算例, 验证所提出判定条件与所设计转换算法的可行性和有效性.

关键词: Galois 型移位寄存器；Fibonacci 型移位寄存器；布尔网络；半张量积；集合划分；等价转换图条件

中图分类号: TP273　　**文献标志码:** A

DOI: 10.13195/j.kzyjc.2026.0513

引用格式: 王腾艺, 刘新芸, 邹云蕾. Galois 型移位寄存器可转换为 Fibonacci 型移位寄存器的图条件 [J]. 控制与决策.

Graphical conditions for converting Galois NLFSRs into Fibonacci NLFSRs

WANG Teng-yi[1]，*LIU Xin-yun*[2]，*ZOU Yun-lei*[1†]

(1. School of Mathematics，Yangzhou University，Yangzhou 225002，China；2. School of Mathematics and Statistics，Weifang University，Weifang 261061，China)

Abstract: This paper investigates the necessary and sufficient graphical conditions for converting Galois nonlinear feedback shift registers (NLFSRs) into Fibonacci NLFSRs, aiming to provide theoretical support and a decision framework for the equivalence conversion between these two types of shift register structures. First, using the matrix semi-tensor product theory, the algebraic representations of the evolution equations for both Galois and Fibonacci NLFSRs are established, and then the algebraic criteria for their transformation are derived. Second, based on the state transition matrix of Fibonacci NLFSRs, the intrinsic state transfer properties are analyzed and a set partition method is introduced. Accordingly, graphical criteria for the transformation between the two types of NLFSRs are established. Furthermore, according to the proposed conversion conditions, a corresponding structural conversion algorithm is designed to realize the transformation from Galois to Fibonacci NLFSRs. Finally, two numerical examples are presented to verify the feasibility and effectiveness of the proposed criteria and the designed transformation algorithm.

Keywords: Galois shift register；Fibonacci shift register；Boolean network；semi-tensor product；set partition；equivalent transformation graph condition

0　引　言

在现代密码学研究中, 流密码因具备运算速率高、硬件结构精简、差错传播范围小等优势, 在军事、外交等关键安全领域得到广泛应用. 非线性反馈移位寄存器作为构建流密码密钥流生成器的核心器件, 受到了国内外学者的广泛关注[1]. 近年来, 大量研究将移位寄存器系统建模为布尔网络, 并依托布尔网络理论开展系统特性分析[2]. 此外, 程代展教授提

收稿日期: 2026-05-29；**录用日期:** 2026-09-06.

基金项目: 国家自然科学基金项目 (62376242)；扬州创新能力提升基金项目 (YZ2024245).

责任编委: 冯俊娥.

†通信作者. E-mail: ylzou@yzu.edu.cn.

出的矩阵半张量积理论, 为逻辑动态系统的建模与分析提供了全新的代数工具[3-6]. 借助该理论工具, 可将基于逻辑规则刻画的离散动态系统转化为代数系统, 从而克服传统逻辑分析方法的局限性, 并极大地推动了布尔网络系统在能控性[7]、能观性[8-9]、镇定性[10]、系统辨识[11]、系统分解[12]、最优控制[13-14]、重构[15]、输出跟踪[16-17]、观测器设计[18] 及有限演化博弈[19] 等诸多方面的研究发展. 基于这一代数框架, 移位寄存器的相关研究也取得了重要进展, 例如, 文献 [20] 借助布尔网络的稳定性分析了移位寄存器的稳定性; 文献 [21] 和文献 [22] 进一步讨论了移位寄存器的单调性和非奇异性, 丰富和完善了移位寄存器的动力学分析体系; 文献 [23] 利用布尔网络的相关方法研究移位寄存器, 给出了移位寄存器生成最大长度序列的条件, 这在提升密码学中的安全性强度方面具有重要意义.

非线性反馈移位寄存器是一类离散逻辑动态系统, 其当前状态由前一时刻状态经非线性反馈函数生成. 在非线性反馈移位寄存器中, 最常见的两种类型为 Galois 型和 Fibonacci 型[24]. Galois 型移位寄存器由多个寄存器同时施加反馈, 其在硬件实现过程中的电路深度较小, 从而在密钥序列生成时能够获得更高的运行效率; 但由于其输出序列周期与其状态周期不一定同步, 这大幅增加了系统特性分析的难度. 与之相比, Fibonacci 型移位寄存器仅在最后一位引入反馈函数, 整体结构易于分析与实现, 且其输出序列周期与状态序列周期一致, 因此在理论分析和性质研究中具有独特优势. 若可实现 Galois 型移位寄存器向 Fibonacci 型移位寄存器的等价转换[25-26], 则可借助 Fibonacci 型寄存器成熟的周期性、能观性、稳定性等优良特性, 完成复杂 Galois 型寄存器的特性分析与性能推演. 同时, 该等价转换能够有效解决传统 Galois 型移位寄存器输出序列周期短于状态最大循环周期、无法满足 Golomb 第二随机性公设等缺陷[1], 进而优化密钥序列的随机性与稳定性, 提升流密码系统的抗破译、抗攻击能力. 因此, 研究两类移位寄存器的等价转换理论与方法, 具有重要的理论价值与工程应用意义.

随着布尔网络控制框架下移位寄存器理论的持续发展, 两类移位寄存器的结构等价与相互转换问题逐渐成为研究热点, 国内许多学者已围绕该方向开展系列探索性研究. 文献 [27] 推导了两类移位寄存器可实现绝对等价转换的条件, 并设计了对应的结构转换算法. 文献 [28] 改进了两种移位寄存器转换的方法, 证明了 Fibonacci 型移位寄存器无法转化为级数更低的弱等价 Galois 型寄存器. 文献 [29] 研究了 Galois 移位寄存器的可观测性矩阵的特性, 建立了系统退化判定条件与向 Fibonacci 型寄存器等价转换的准则. 文献 [30] 分析了 Galois 结构与 Fibonacci 结构之间的等价关系和非奇异性, 明确了该研究结果与现有结论之间的包含关系. 文献 [31] 研究了两类移位寄存器的等价性, 构造了两类全新的等价 Galois型寄存器. 综合现有研究可知, 当前两类移位寄存器的转换研究多依托传统算法与复杂组合理论展开. 能否仅基于移位寄存器的结构矩阵, 直观、高效地推演 Galois 型移位寄存器向 Fibonacci 型移位寄存器转换的判定条件, 仍是有待深入探讨的研究方向.

基于以上讨论, 本文研究 Galois 型非线性反馈移位寄存器向 Fibonacci 型非线性反馈移位寄存器转换的充分必要图论条件. 本文的主要创新点如下:

(i) 构建了 Galois 型移位寄存器向 Fibonacci 型移位寄存器转换的系统性代数分析框架, 为两类移位寄存器的结构等价变换与特性分析提供了统一、完善的理论支撑, 完善了布尔网络框架下移位寄存器之间转换的研究体系;

(ii) 仅依据 Galois 型移位寄存器的状态转移矩阵中非零元素所在的行与列位置指标, 推导得到两类寄存器实现等价转换的图论判定条件, 并给出了用于实现等价转换的置换矩阵的构造方法.

1 预备知识

为了叙述方便, 本文用到的相关符号如下:

1) $\mathcal{D} := \{0, 1\}$;

2) $\mathcal{D}^n := \underbrace{\mathcal{D} \times \ldots \times \mathcal{D}}$;

3) $\Delta_m := \{\delta_m^i \mid^n i = 1, 2, \ldots, m\}$, 其中$\delta_m^i$为单位矩阵$I_m$的第$i$列;

4) $\Delta := \{\delta_2^1, \delta_2^2\}$;

5) $\mathrm{Col}_i(L)$: 矩阵L的第i列;

6) $\mathrm{Col}(L)$: 矩阵L的列向量的集合;

7) $\mathcal{R}_{m\times n}$: 所有$m \times n$实矩阵的集合;

8) $\mathbf{1}_n$: 元素全为1的n维列向量;

9) $\mathbf{0}_n$: 元素全为0的n维列向量;

10) $|S|$: 集合S的基数, 即S中元素的个数;

11) $\oplus$: 模2加法;

12) $A^\top$: 矩阵A的转置.

若矩阵$L \in \mathcal{R}_{m\times n}$满足$\mathrm{Col}(L) \subseteq \Delta_m$, 则称$L$为逻辑矩阵. 记$\mathcal{L}_{m\times n}$为所有$m \times n$逻辑矩阵的集合. 为表达简便, 记$L = [\delta_m^{i_1}\delta_m^{i_2} \ldots \delta_m^{i_n}] := \delta_m[i_1\ i_2\ \ldots\ i_n]$.

定义 1[32] 已知$A \in \mathcal{R}_{a\times b}$, $B \in \mathcal{R}_{c\times d}$, 则矩阵$A$与$B$的半张量积定义为$A \ltimes B = (A \otimes I_{\frac{\alpha}{b}})$

$(B\otimes I_{\frac{\alpha}{c}})$, 其中$\alpha$为$b$和$c$的最小公倍数, $\otimes$表示 Kronecker 积.

当$b=c$时, 矩阵A与B的半张量积退化为普通矩阵乘法, 这表明半张量积是传统矩阵乘法的一种推广. 在不引起歧义的情况下, 在后面的表达中符号"$\ltimes$"通常被省略.

定义 2[33]　已知$A\in\mathcal{R}_{a\times b}$, $B\in\mathcal{R}_{c\times b}$, 则$A$和$B$的 Khatri-Rao 积定义为

$$A*B=[\mathrm{Col}_1(A)\otimes\mathrm{Col}_1(B),\ldots,\mathrm{Col}_b(A)\otimes\mathrm{Col}_b(B)].$$

引理 1[34]　设 $A\in\mathcal{R}_{m\times n}$, $B\in\mathcal{R}_{p\times q}$, $C\in\mathcal{R}_{n\times s}$, $D\in\mathcal{R}_{q\times r}$. Kronecker 积有如下性质$(AC)\otimes(BD)=(A\otimes B)(C\otimes D)$, 其中$AC$与$BD$为普通矩阵乘法.

已知 $X\in\Delta_m$, $Y\in\Delta_n$, $L_1,L_2\in\mathcal{L}_{m\times m}$, 则$Y=(\mathbf{1}_m^\top X)\otimes(I_nY)=(\mathbf{1}_m^\top\otimes I_n)XY$以及$(L_1X)(L_2X)=(L_1*L_2)X$.

将逻辑值1与0等价为向量形式δ_2^1与δ_2^2, 记为$1\sim\delta_2^1$, $0\sim\delta_2^2$, 则对于任意$(i_1,i_2,\ldots,i_n)\in\mathcal{D}^n$, 有$\delta_{2^n}^i=\ltimes_{l=1}^n\delta_2^{2-i_l}\in\Delta_{2^n}$.

引理 2[32]　设$f(X_1,X_2,\ldots,X_n):D^n\to D$为一个逻辑函数, 则存在唯一的逻辑矩阵$F\in\mathcal{L}_{2\times2^n}$, 称为$f$的结构矩阵, 使得$f(x_1,x_2,\ldots,x_n)=Fx_1\ltimes x_2\ldots\ltimes x_n$, 其中$x_i=\delta_2^{2-X_i}\in\Delta$.

一个n阶 Galois 型移位寄存器的逻辑表达式为

$$X_i(t+1)=f_i(X_1(t),X_2(t),\ldots,X_n(t)),\quad i=1,2,\ldots,n,\tag{1}$$

其中$f_i:D^n\to D$是逻辑函数, $X_i(t)\in D$是第i个寄存器在t时刻的值.

设$x_i=\delta_2^{2-X_i}\in\Delta$, $x(t)=\ltimes_{i=1}^n x_i(t)$. 由引理 2, 对于每一个$f_i$, 都存在唯一的结构矩阵$M_{f_i}\in\mathcal{L}_{2\times2^n}$, 使得$x_i(t+1)=M_{f_i}x(t)$. 借助矩阵半张量积, 则 Galois 型移位寄存器 (1) 的等价代数表达形式为

$$x(t+1)=Gx(t),\tag{2}$$

这里$G=M_{f_1}*M_{f_2}*\ldots*M_{f_n}$. $G\in\mathcal{L}_{2^n\times2^n}$称为系统的状态转移矩阵.

一个n阶 Fibonacci 型移位寄存器的逻辑表达式为

$$\begin{cases}Z_i(t+1)=Z_{i+1}(t),\ i=1,2,\ldots,n-1,\\ Z_n(t+1)=f(Z_1(t),Z_2(t),\ldots,Z_n(t)),\end{cases}\tag{3}$$

其中$f:D^n\to D$是逻辑函数, $Z_j(t)\in D$, $j\in\{1,2,\ldots,n\}$是第i个寄存器在t时刻的值. $(Z_1(t),Z_2(t),\ldots,Z_n(t))$表示 Fibonacci 型移位寄存器在$t$时刻的状态.

设$z_i=\delta_2^{2-Z_i}\in\Delta$, $z(t)=\ltimes_{i=1}^n z_i(t)$, 则存在唯一的结构矩阵$M_f\in\mathcal{L}_{2\times2^n}$, 使得$z_n(t+1)=M_fz(t)$. 因此 Fibonacci 型移位寄存器 (3) 的等价代数形式为

$$\begin{cases}z_i(t+1)=z_{i+1}(t),\ i=1,2,\ldots,n-1,\\ z_n(t+1)=M_fz(t).\end{cases}\tag{4}$$

由 (4) 得 $\ltimes_{i=1}^{n-1}z_i(t+1)=\ltimes_{i=2}^n z_i(t)=(\mathbf{1}_2^\top\otimes I_{2^{n-1}})\ltimes_{i=1}^n z_i(t)$. 因而系统 (4) 可转化为

$$z(t+1)=Fz(t),\tag{5}$$

其中 $F=(\mathbf{1}_2^\top\otimes I_{2^{n-1}})*M_f$. $F\in\mathcal{L}_{2^n\times2^n}$称为 Fibonacci 型移位寄存器的状态转移矩阵.

推论 1　设 Fibonacci 型移位寄存器 (4) 的反馈函数的结构矩阵为$M_f=\delta_2[i_1\ i_2\ \ldots\ i_n]$, 则其状态转移矩阵$F$有如下形式:

$$F=[\delta_{2^{n-1}}^1\delta_2^{i_1}\quad\delta_{2^{n-1}}^2\delta_2^{i_2}\quad\ldots\quad\delta_{2^{n-1}}^{2^{n-1}}\delta_2^{i_{2^{n-1}}}\to\ \leftarrow\delta_{2^{n-1}}^1\delta_2^{i_{2^{n-1}+1}}\quad\delta_{2^{n-1}}^2\delta_2^{i_{2^{n-1}+2}}\quad\ldots\quad\delta_{2^{n-1}}^{2^{n-1}}\delta_2^{i_{2^n}}],\tag{6}$$

其中$i_j\in\{1,2\}$, $j=1,2,\ldots,2^n$.

定义 3[35]　已知逻辑映射

$$Z_i=g_i(X_1,X_2,\ldots,X_n),i=1,2,\ldots,n,\tag{7}$$

其中$X_i,Z_i\in D$. 若逻辑函数$g=(g_1,g_2,\ldots,g_n)^\top$为双射, 则称$g$为逻辑坐标变换.

设$x_i=\delta_2^{2-X_i}$, $z_i=\delta_2^{2-Z_i}$, 记$x(t)=\ltimes_{i=1}^n x_i(t)$, $z(t)=\ltimes_{i=1}^n z_i(t)$, 则 (7) 式的代数形式可表示为$z(t)=Tx(t)$, 其中$T\in\mathcal{L}_{2^n\times2^n}$是逻辑坐标变换 (7) 的结构矩阵. 逻辑映射$g$是逻辑坐标变换当且仅当$T$是置换矩阵.

2　主要结果

本节将利用 Fibonacci 型移位寄存器的状态转移矩阵的性质, 通过分析 Fibonacci 型移位寄存器的状态转移矩阵的行指标与列指标之间的关系, 推导 Galois 型移位寄存器与 Fibonacci 型移位寄存器之间可相互转换的图条件.

定义 4　若存在逻辑坐标变换$g:\mathcal{D}^n\to\mathcal{D}^n$, 使得系统 (1) 可以被转换为系统 (3), 则称 Galois 型移位寄存器 (1) 可被转换为 Fibonacci 型移位寄器 (3).

定理 1　Galois 型移位寄存器 (2) 可转换成 Fibonacci 型移位寄存器 (5) 当且仅当存在置换矩阵$T\in\mathcal{L}_{2^n\times2^n}$使得$TGT^\top=F$.

证明　由定义 4 得, 存在逻辑坐标变换$g:\mathcal{D}^n\to\mathcal{D}^n$使得系统 (1) 可以被转换为系统 (3). 利用矩阵半张量积, 可得$g:\mathcal{D}^n\to\mathcal{D}^n$的代数形式$z(k)=Tx(k)$, 其中$T\in\mathcal{L}_{2^n\times2^n}$是置换矩阵. 在该变换下, 系

统 (2) 被转换为$z(k+1)=TGT^{\top}z(k)$的形式. 进而可得 Galois 型移位寄存器 (2) 可以被转换为 Fibonacci 型移位寄存器 (4) 的充要条件为$TGT^{\top}=F$. □

给定一个置换矩阵T. 设

$$\begin{aligned}&T^{\top}=\delta_{2^n}[j_1\quad j_2\quad\ldots\quad j_{2^n}],\\&G=[G_1^{\top}\quad G_2^{\top}\quad\ldots\quad G_{2^n}^{\top}]^{\top},\end{aligned}\tag{8}$$

其中$G_i(i\in\{1,2,\ldots,2^n\})$为$G$的第$i$行. 进而可得

$$\begin{aligned}&TGT^{\top}=\\&([G_1^{\top}\quad G_2^{\top}\quad\ldots\quad G_{2^n}^{\top}]\delta_{2^n}[j_1\quad j_2\quad\ldots\rightarrow\\&\leftarrow j_{2^n}])^{\top}T^{\top}=[G_{j_1}^{\top}\quad G_{j_2}^{\top}\quad\ldots\quad G_{j_{2^n}}^{\top}]^{\top}T^{\top}.\end{aligned}\tag{9}$$

由定理 1 可得, 若 Galois 型移位寄存器 (2) 可转换成 Fibonacci 型移位寄存器 (5), 则矩阵 (9) 具有 (6) 所示的形式.

考虑系统 (2) 的状态转移矩阵G, 令

$$S=\{1,2,\ldots,2^n\}.\tag{10}$$

根据矩阵G中非零元素所在的行与列, 定义集合族:

$$S_i=\{j\mid(G)_{ij}=1\},\tag{11}$$

其中$i\in S$. 进而由 (8) 可得

$$\begin{cases}S_{j_{2l-1}}=\{j\mid\mathrm{Col}_j(G_{j_{2l-1}})=1\},\\S_{j_{2l}}=\{j\mid\mathrm{Col}_j(G_{j_{2l}})=1\},\end{cases}\tag{12}$$

其中$j_{2l-1},j_{2l}\in S$.

定义 5 集合族$\{P_i\}_{i=1}^{\mu}$称为$S=\{1,2,\ldots,2^n\}$的等点划分, 若$\bigcup\limits_{l=1}^{\mu}P_l=S$且$|P_l|=\dfrac{2^n}{\mu}$.

由 (10) 定义的集合S表示逻辑矩阵G的所有行指标, 由 (11) 定义的集合S_i表示逻辑矩阵G的第i行中非零元素所在的列指标. 基于集合S和集合族$\bigcup\limits_{i=1}^{2^n}S_i$以及定义 5, 我们有下面的结论.

定理 2 Galois 型移位寄存器 (2) 可转换为 Fibonacci 型移位寄存器 (5) 当且仅当存在集合 (10) 的等点划分$\{k_1,k_2\},\{k_3,k_4\},\ldots,\{k_{2^n-1},k_{2^n}\}$, 使得由 (11) 定义的集合族满足以下条件

$$\begin{cases}S_{k_1}\bigcup S_{k_2}=\{k_1,k_{2^{n-1}+1}\},\\S_{k_3}\bigcup S_{k_4}=\{k_2,k_{2^{n-1}+2}\},\\\quad\vdots\\S_{k_{2^{n-1}-1}}\bigcup S_{k_{2^{n-1}}}=\{k_{2^{n-2}},k_{2^{n-1}+2^{n-2}}\},\\S_{k_{2^{n-1}+1}}\bigcup S_{k_{2^{n-1}+2}}=\{k_{2^{n-2}+1},k_{2^{n-1}+2^{n-2}+1}\},\\\quad\vdots\\S_{k_{2^n-1}}\bigcup S_{k_{2^n}}=\{k_{2^{n-1}},k_{2^n}\}.\end{cases}\tag{13}$$

证明 (充分性) 在 (8) 中令$j_i=k_i$, $i=1,2,\ldots,2^n$, 即$T^{\top}=\delta_{2^n}[k_1\ \ k_2\ldots k_{2^n}]$, 进而由 (9) 得

$$TGT^{\top}=[G_{k_1}^{\top}\ G_{k_2}^{\top}\ldots G_{k_{2^n}}^{\top}]^{\top}\delta_{2^n}[k_1\ k_2\ldots k_{2^n}]\tag{14}$$

且

$$\begin{cases}S_{k_{2l-1}}=\{j\mid\mathrm{Col}_j(G_{k_{2l-1}})=1\},\\S_{k_{2l}}=\{j\mid\mathrm{Col}_j(G_{k_{2l}})=1\}.\end{cases}\tag{15}$$

由 (13) 可得, $S_{k_{2l-1}}\bigcup S_{k_{2l}}=\{k_l,k_{2^{n-1}+l}\}$, $l=1,2,\ldots,2^{n-1}$. 基于 (14) 和 (15) 可得

$$\begin{aligned}&\begin{bmatrix}G_{k_{2l-1}}\\G_{k_{2l}}\end{bmatrix}\delta_{2^n}[k_1\quad k_2\quad\ldots\quad k_{2^n}]=\\&[\underbrace{\mathbf{0}_2\ \ldots\ \mathbf{0}_2}_{l-1}\ \ \delta_2^{p_l}\ \mathbf{0}_2\ \ldots\ \mathbf{0}_2\ \delta_2^{p_{2^{n-1}+l}}\ \ \underbrace{\mathbf{0}_2\ \ldots\ \mathbf{0}_2}_{2^n-(2^{n-1}+l)}],\end{aligned}\tag{16}$$

其中, p_l和$p_{2^{n-1}+l}$的值按如下规则确定:

a) 若 $k_l\in S_{k_{2l-1}}$, 则 $p_l=1$; 若 $k_l\in S_{k_{2l}}$, 则 $p_l=2$;

b) 若 $k_{2^{n-1}+l}\in S_{k_{2l-1}}$, 则 $p_{2^{n-1}+l}=1$; 若 $k_{2^{n-1}+l}\in S_{k_{2l}}$, 则$p_{2^{n-1}+l}=2$.

由 (16) 得

$$\begin{aligned}&TGT^{\top}=\\&[\delta_{2^{n-1}}^1\delta_2^{p_1}\quad\delta_{2^{n-1}}^2\delta_2^{p_2}\quad\ldots\quad\delta_{2^{n-1}}^{2^{n-1}}\delta_2^{p_{2^{n-1}}}\rightarrow\\&\leftarrow\delta_{2^{n-1}}^1\delta_2^{p_{2^{n-1}+1}}\quad\delta_{2^{n-1}}^2\delta_2^{p_{2^{n-1}+2}}\quad\ldots\quad\delta_{2^{n-1}}^{2^{n-1}}\delta_2^{p_{2^n}}],\end{aligned}$$

其中$p_i\in\{1,2\}$, 这表明矩阵 (14) 具有 (6) 所示的形式, 即存在一个置换矩阵T使得$TGT^{\top}=F$. 由定理 1, Galois 型移位寄存器 (2) 可以转换为 Fibonacci 型移位寄存器 (5). 充分性得证.

(必要性) 假设 Galois 型移位寄存器 (2) 能够转换为 Fibonacci 型移位寄存器 (5), 根据定理 1, 存在一个置换矩阵$T^{\top}=\delta_{2^n}[k_1\ \ k_2\ldots k_{2^n}]$使得矩阵$TGT^{\top}$具有 (6) 所示的形式. 由 (6) 和 (9) 可得

$$\begin{aligned}&[G_{k_1}^{\top}\quad G_{k_2}^{\top}\quad\ldots\quad G_{k_{2^n}}^{\top}]^{\top}\delta_{2^n}[k_1\quad k_2\quad\ldots\quad k_{2^n}]=\\&[\delta_{2^{n-1}}^1\delta_2^{i_1}\quad\delta_{2^{n-1}}^2\delta_2^{i_2}\quad\ldots\quad\delta_{2^{n-1}}^{2^{n-1}}\delta_2^{i_{2^{n-1}}}\rightarrow\\&\leftarrow\delta_{2^{n-1}}^1\delta_2^{i_{2^{n-1}+1}}\quad\delta_{2^{n-1}}^2\delta_2^{i_{2^{n-1}+2}}\quad\ldots\quad\delta_{2^{n-1}}^{2^{n-1}}\delta_2^{i_{2^n}}],\end{aligned}$$

进而

$$\begin{aligned}&\begin{bmatrix}G_{k_{2l-1}}\\G_{k_{2l}}\end{bmatrix}\delta_{2^n}[k_1\quad k_2\quad\ldots\quad k_{2^n}]=\\&[\underbrace{\mathbf{0}_2\ \ldots\ \mathbf{0}_2}_{l-1}\ \ \delta_2^{i_l}\ \mathbf{0}_2\ \ldots\ \mathbf{0}_2\ \delta_2^{i_{2^{n-1}+l}}\ \ \underbrace{\mathbf{0}_2\ \ldots\ \mathbf{0}_2}_{2^n-(2^{n-1}+l)}],\end{aligned}\tag{17}$$

其中 $l=1,2,\ldots,2^{n-1}$. 由 (17) 得 $\{j|\mathrm{Col}_j(G_{k_{2l-1}})=1\}\bigcup\{j|\mathrm{Col}_j(G_{k_{2l}})=1\}=\{k_l,k_{2^{n-1}+l}\}$. 进而, 基于 (12) 得$S_{k_{2l-1}}\bigcup S_{k_{2l}}=\{k_l,k_{2^{n-1}+l}\}$, 即 (13) 满足. 必要性得证. □

记 Galois 型移位寄存器 (2) 的状态转移图为$\mathcal{G}(V,E)$, 其由顶点集V和有向边集E构成, 其中$V=\{1,2,\ldots,2^n\}$, $\mathcal{G}(V,E)$有一条有向边$(j,i)\in E$当且仅当$(G)_{ij}=1$. 若$(G)_{ij}=1$, 则称顶点i为顶

点j的一个出邻点. 设V_1为V的一个子集, 并令

$$\mathcal{N}(V_1)=\{i|(G)_{ij}=1,\ j\in V_1\},\tag{18}$$

则称$\mathcal{N}(V_1)$是V_1的出邻居. 由 (18) 得, 集合$\{k_{2i-1}, k_{2i}\}$是集合$\{k_i, k_{2^{n-1}+i}\}$中点的出邻居集. 基于以上讨论, 满足条件 (13) 的 Galois 型移位寄存器的状态转移矩阵的状态转移图如图 1 所示, 箭头的含义为箭头尾部所连顶点集的出邻居即为箭头头部所连的顶点集.

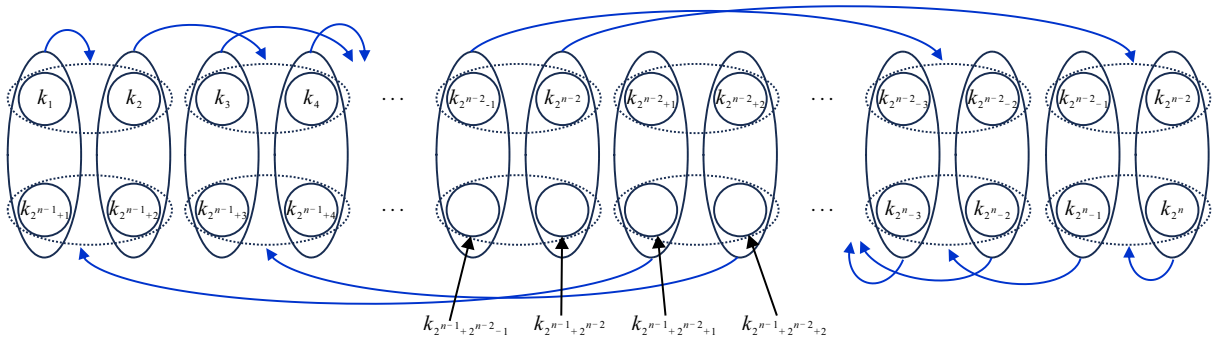

图 1　满足条件 (13) 的系统的状态转移图

注 1　定理 2 提出的基于集合划分条件 (13) 的判定准则, 完善并拓展了已有研究成果. 文献 [27] 给出了 Galois 型移位寄存器向 Fibonacci 型移位寄存器转换的显式算法, 该算法的有效性受反馈函数稀疏性约束且所得条件为充分条件; 文献 [28] 拓宽了文献 [27] 中显式算法的适用范围, 但其侧重点在于弱等价关系与模型降阶优化; 文献 [29] 的结果基于能观矩阵的秩以及状态图的同构关系; 文献 [30] 建立了基于可观测性的等价充要条件; 文献 [31] 则构建了较为完备的代数理论体系. 相较于上述已有研究, 本文通过状态集合配对问题推导得到两类移位寄存器可相互转换的充要条件, 建立了严格的等价关系并给出了置换矩阵的具体构造方法. 本文所提条件 (13) 仅依赖状态矩阵的行指标与列指标, 形式简洁、适用性强. 本文在保证理论严谨性的基础上, 有效提升了算法的实际应用价值, 为两类移位寄存器的等价转换构建了一套统一、简洁且高效的图论求解框架.

定理 2 表明判断 Galois 型移位寄存器能否转换为 Fibonacci 型移位寄存器的关键在于能否在 Galois 型移位寄存器的结构矩阵的行指标集中, 找到一个满足条件 (13) 的等点划分. 下面先给出 Galois 型移位寄存器可转换为 Fibonacci 型移位寄存器的一些必要条件.

推论 2　若 Galois 型移位寄存器 (2) 能够转换为 Fibonacci 型移位寄存器 (5), 则下列结论成立:

(i) $G\mathbf{1}_{2^n}=[l_1\ \ l_2\ldots l_{2^n}]^{\top}$, 其中$l_i\in\{0,1,2\}$, $i=1,2,\ldots,2^n$;

(ii) 在 (11) 定义的集合中, 满足$\{i\}\bigcap S_i=\{i\}$的S_i至多只有两个;

(iii) 在 (11) 定义的集合中, 若存在集合S_i满足$\{i\}\bigcap S_i=\{i\}$, 则$i=k_1$或$i=k_{2^n}$.

证明　(i) 由 (13) 得, $|S_i|\leqslant 2$, $i=1,2,\ldots,2^n$. 由于G是逻辑矩阵, 因此$l_i\in\{0,1,2\}$.

(ii) 由 (13) 得, $S_{k_{2l-1}}\bigcup S_{k_{2l}}=\{k_l, k_{2^{n-1}+l}\}$, $l=1,2,\ldots,2^{n-1}$. 当 $l=1$时, $\{k_1,k_2\}\bigcap\{k_1,k_{2^{n-1}+1}\}=k_1$. 当 $l=2^{n-1}$时, $\{k_{2^n-1},k_{2^n}\}\bigcap\{k_{2^{n-1}},k_{2^n}\}=k_{2^n}$. 当 $l\neq 1$且 $l\neq 2^{n-1}$时, 得 $\{k_{2l-1},k_{2l}\}\bigcap\{k_l,k_{2^{n-1}+l}\}=\varnothing$. 因此, 在 (11) 定义的集合中, 至多存在两个集合满足$\{i\}\bigcap S_i\neq\varnothing$.

(iii) 由 (13) 得, 当$i=k_1$或$i=k_{2^n}$时, 结论成立. □

推论 2 给出了 Galois 型移位寄存器可转换为 Fibonacci 型移位寄存器的若干必要条件. 由于原命题与其逆否命题等价, 因此若矩阵G不满足推论 2 中任意一个结论, 则系统 (2) 不能被转换为 Fibonacci 型移位寄存器. 反之, 从这些必要条件出发, 并结合矩阵G的结构, 可以设计算法在集合 (10) 中寻找满足条件 (13) 的等点划分.

称集合S_{k_i}与S_{k_j}是相关的, 若其满足

$$|\{k_i,k_j\}\bigcap(S_{k_i}\bigcup S_{k_j})|=1,\ |S_{k_i}\bigcup S_{k_j}|=2,$$

记为$S_{k_i}\dot{\sim}S_{k_j}$. 定义集合族$\mathscr{S}=\{\{k_i,k_j\}|S_{k_i}\dot{\sim}S_{k_j}\}$. 由 (13) 可得 $S_{k_1}\dot{\sim}S_{k_2}$且 $S_{k_{2^n-1}}\dot{\sim}S_{k_{2^n}}$. 若集合$\{k_1,k_2\}$, $\{k_{2^n-1},k_{2^n}\}$被确定, 则可确定$k_{2^{n-1}+1}$与$k_{2^{n-1}}$. 由

$$\begin{aligned}&S_{k_3}\bigcup S_{k_4}=\{k_2,k_{2^{n-1}+2}\},\\&S_{k_{2^{n-1}+1}}\bigcup S_{k_{2^{n-1}+2}}=\{k_{2^{n-2}+1},k_{2^{n-1}+2^{n-2}+1}\},\end{aligned}\tag{19}$$

$$\begin{aligned}&S_{k_{2^n-3}}\bigcup S_{k_{2^n-2}}=\{k_{2^n-1},k_{2^{n-1}-1}\},\\&S_{k_{2^{n-1}-1}}\bigcup S_{k_{2^{n-1}}}=\{k_{2^n-2},k_{2^{n-1}+2^{n-2}}\}.\end{aligned}\tag{20}$$

可确定$k_{2^{n-1}+2}$与$k_{2^{n-1}-1}$, 进一步可以确定

$$\{k_3,k_4\},\ \{k_{2^{n-2}+1},\ k_{2^{n-1}+2^{n-2}+1}\},$$
$$\{k_{2^n-3},k_{2^n-2}\},\ \{k_{2^{n-2}},k_{2^{n-1}+2^{n-2}}\}.$$

算法 1 step 1: 设$S=\{1,2,\ldots,2^n\}$. 令$S_i=\{j|\mathrm{Col}_j(G)=\delta_{2^n}^i\}, i\in S$, 集合族$\{S_i\}_{i=1}^{2^n}$满足$|S_i|\in\{0,1,2\}$且至多存在两个集合满足$\{i\}\bigcap S_i=\{i\}$. 构造集合族$\mathscr{S}=\{\{k_i,k_j\}|S_{k_i}\dot{\sim}S_{k_j}\}$;

step 2: 根据推论 2, 首先选择集合$\{k_{i_1},k_{i_2}\}$, $\{k_{i_3},k_{i_4}\}\in\mathscr{S}$, 使得$\{k_{i_1},k_{i_2}\}\bigcap\{k_{i_3},k_{i_4}\}=\varnothing$. 然后将两个集合分别重新标记为$\{k_1,k_2\}$和$\{k_{2^n-1},k_{2^n}\}$, 其中$\{k_1,k_2\}\bigcap\{k_1,k_{2^{n-1}+1}\}=k_1$, $\{k_{2^n-1},k_{2^n}\}\bigcap\{k_{2^n},k_{2^{n-1}}\}=k_{2^n}$. 进一步确定$k_{2^{n-1}+1}$和$k_{2^{n-1}}$的取值;

step 3: 根据 (19) 式和 (20) 式进一步为$k_{2^{n-1}+2}$, $k_{2^{n-1}-1}$赋值, 并确定

$$\{k_3,k_4\},\ \{k_{2^{n-2}+1},k_{2^{n-1}+2^{n-2}+1}\},$$
$$\{k_{2^n-3},k_{2^n-2}\},\ \{k_{2^{n-2}},k_{2^{n-1}+2^{n-2}}\}.$$

随后继续搜索

$$\{k_5,\ k_6\},\ \ldots,\ \{k_{2^{n-1}-3},\ k_{2^{n-1}-2}\},$$
$$\{k_{2^{n-1}+3},\ k_{2^{n-1}+4}\},\ \ldots,\ \{k_{2^n-3},\ k_{2^n-2}\}.$$

最终使得 (13) 式成立;

step 4: 基于满足条件 (13) 的等点划分$\{k_1,\ k_2\}$, $\{k_3,\ k_4\}$, $\ldots$, $\{k_{2^n-1},\ k_{2^n}\}$, 令$T^\top=\delta_{2^n}[k_1\ \ k_2\ldots k_{2^n}]$.

注 2 算法 1 给出了构造满足条件 (13) 的等点划分的系统性步骤. 需要指出的是, 满足条件 (13) 的等点划分不是唯一的, 因而满足$TGT^T=F$的非奇异逻辑矩阵T也可能存在多个. 不同的T对应不同的 Fibonacci 型反馈函数实现, 然而所有实现对应的系统状态转移图相互同构, 故其循环结构与周期特征维持不变. 此外, 构造集合族$\{S_i\}_{i=1}^{2^n}$需遍历状态转移矩阵$G\in\mathcal{L}_{2^n\times 2^n}$的所有行和列, 且最坏情况下需遍历$O(2^{2n})$个集合配对, 因此算法 1 至少具有指数阶计算复杂度.

3 数值算例

本节将通过具体实例, 展示 Galois 型移位寄存器转换为 Fibonacci 型移位寄存器的过程.

例 1 考虑 Galois 型移位寄存器

$$\begin{cases}x_1(t+1)=x_2(t)\wedge x_3(t),\\ x_2(t+1)=\neg x_1(t),\\ x_3(t+1)=x_2(t)\vee x_3(t),\end{cases}\tag{21}$$

其代数形式为$x(t+1)=Gx(t)$, 其中$G=\delta_8[3\ 7\ 7\ 8\ 1\ 5\ 5\ 6]$. 借助$G$中每一行中非零元素所在的列指标, 得到集合

$$S_1=\{5\},\ S_2=\varnothing,\ S_3=\{1\},\ S_4=\varnothing,$$
$$S_5=\{6,7\},\ S_6=\{8\},\ S_7=\{2,3\},\ S_8=\{4\}.$$

基于上述集合, 寻找满足$TGT^\top=F$的置换矩阵T的具体步骤如下:

a) 由 $S_1\dot{\sim}S_3$且 $S_6\dot{\sim}S_8$, 取 $k_1=1$, $k_2=3$, $k_7=6$, $k_8=8$. 由$S_{k_1}\bigcup S_{k_2}=\{k_1,k_5\}$及$S_{k_7}\bigcup S_{k_8}=\{k_4,k_8\}$, 得$k_5=5$, $k_4=4$.

b) 由 $S_{k_3}\bigcup S_{k_4}=\{k_2,k_6\}$, 且 $S_{k_4}=S_4=\varnothing$, $k_2=3$, 可得$S_{k_3}=S_7$从而$k_6=2$.

因此, 存在如下等点划分

$$\{1,\ 3\},\ \{7,\ 4\},\ \{5,2\},\ \{6,\ 8\}.\tag{22}$$

该划分满足 (13) 式. 系统 (21) 的状态转移图如图 2 所示, 箭头的含义为箭头尾部所连顶点集的出邻居即为箭头头部所连的顶点集. 由 (22) 构造置换矩阵$T^\top=\delta_8[1\ 3\ 7\ 4\ 5\ 2\ 6\ 8]$. 经计算可得$F=TGT^\top=\delta_8[2\ 3\ 5\ 8\ 1\ 3\ 5\ 7]$. 因而, Galois 型移位寄存器 (21) 可转换为 Fibonacci 型移位寄存器, 其表达式如下:

$$\begin{cases}z_i(t+1)=z_{i+1}(t),\ i=1,2,\\ z_3(t+1)=\neg z_1(t)\vee(z_2(t)\oplus z_3(t)).\end{cases}\tag{23}$$

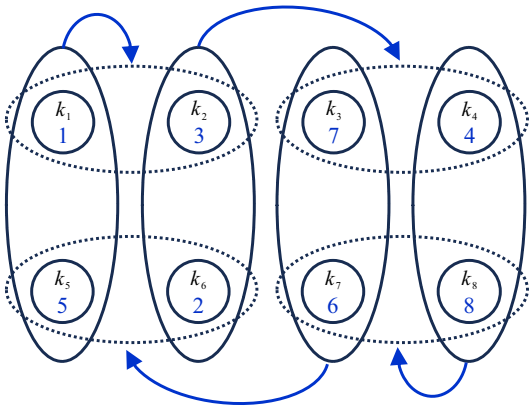

图 2 系统 (21) 的状态转移图

例 2 考虑 Galois 型移位寄存器

$$\begin{cases}x_1(t+1)=x_2(t)\oplus x_1(t),\\ x_2(t+1)=x_3(t),\\ x_3(t+1)=x_4(t),\\ x_4(t+1)=x_1(t)\oplus x_3(t)x_4(t),\end{cases}\tag{24}$$

其代数形式为$x(t+1)=Gx(t)$, 其中

$$G=\delta_{16}[10\ 11\ 13\ 15\ 2\ 3\ 5\ 7\ 1\ 4\ 6\ 8\ 9\ 12\ 14\ 16].$$

由G中每一行中非零元素所在的列指标, 得到集合

$$S_1=\{9\},\ S_2=\{5\},\ S_3=\{6\},\ S_4=\{10\},$$
$$S_5=\{7\},\ S_6=\{11\},\ S_7=\{8\},\ S_8=\{12\},$$
$$S_9=\{13\},\ S_{10}=\{1\},\ S_{11}=\{2\},\ S_{12}=\{14\},$$
$$S_{13}=\{3\},\ S_{14}=\{15\},\ S_{15}=\{4\},\ S_{16}=\{16\}.$$

根据上述集合, 可给出构造置换矩阵T的具体步骤:

a) 根据$S_{16}=\{16\}$和推论 2, 取$k_1=16$. 由于$S_1\dot{\sim}S_{16}$且$S_2\dot{\sim}S_5$, 因而令$k_2=1$, $k_{15}=2$, $k_{16}=5$. 由 $S_{k_1}\bigcup S_{k_2}=\{k_1,k_9\}$和 $S_{k_{15}}\bigcup S_{k_{16}}=\{k_7,k_{16}\}$, 可得$k_9=9$, $k_7=7$.

b) 基于集合 (19) 和集合 (20), 可得$10\in\{k_3,k_4\}$, $11\in\{k_{13},k_{14}\}$, $8\in\{k_4,k_{12}\}$, $13\in\{k_5,k_{13}\}$. 进而得到$k_{10},k_7\in\{3,4,6,12,14,15\}$.

c) 取$k_{10}=6$, 由 (13) 可依次确定$k_3=3$, $k_4=10$, $k_5=13$, $k_6=12$, $k_7=4$, $k_{11}=14$, $k_{12}=8$, $k_{13}=11$和$k_{14}=15$.

由此得到满足条件 (13) 的划分

$$\{16,\ 1\},\ \{3,\ 10\},\ \{13,12\},\ \{4,\ 7\},\\ \{9,\ 6\},\ \{14,\ 8\},\ \{11,15\},\ \{2,\ 5\}. \tag{25}$$

图 3 是系统 (24) 的状态转移图, 图中箭头的含义为箭头尾部所连顶点集的出邻居即为箭头头部所连顶点集. 由 (25) 可得置换矩阵T为

$$T=\delta_{16}[2\ 15\ 3\ 7\ 16\ 10\ 8\ 12\ 9\ 4\ 13\ 6\ 5\ 11\ 14\ 1].$$

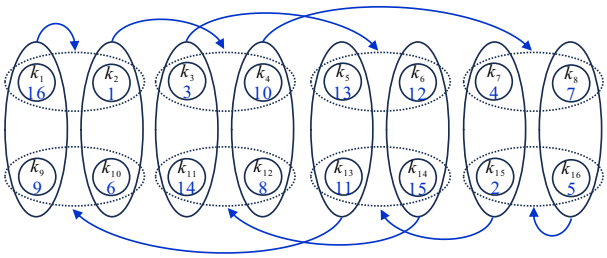

图 3　系统 (24) 的状态转移图

由$F=TGT^{\top}$得

$$F=\delta_{16}[1\ 4\ 5\ 7\ 9\ 12\ 14\ 16\ 2\ 3\ 6\ 8\ 10\ 11\ 13\ 15].$$

因而, Galois 型移位寄存器 (21) 可转换为 Fibonacci 型移位寄存器, 其表达式如下:

$$\begin{cases} z_i(t+1)=z_{i+1}(t), i=1,2,3,\\ z_4(t+1)=\neg z_1(t)\oplus((z_2(t)\wedge(z_3(t)\vee\neg z_4(t)))\\ \qquad\qquad\vee(\neg z_2(t)\wedge(z_3(t)\wedge z_4(t)))). \end{cases}$$

注 3　例 2 中设计的置换矩阵T并不唯一. 在文献 [26 28] 中, 置换矩阵T被设计为$T=\delta_{16}[6\ 5\ 7\ 8\ 3\ 4\ 2\ 1\ 11\ 12\ 10\ 9\ 14\ 13\ 15\ 16]$, 此时 $F=\delta_{16}[2\ 3\ 5\ 7\ 10\ 12\ 14\ 15\ 1\ 4\ 6\ 8\ 9\ 11\ 13\ 16]$. 尽管例 2 和文献 [26, 28] 得到的$F$矩阵不同, 但均满足 Fibonacci 结构且状态转移图同构.

4　结　论

本文提出了一种将 Galois 型非线性反馈移位寄存器转换为 Fibonacci 型非线性反馈移位寄存器的新方法. 研究结合两类移位寄存器的结构矩阵、集合理论以及图论方法, 推导出 Galois 型移位寄存器可转换为 Fibonacci 型移位寄存器的充分必要图条件, 进一步给出了置换矩阵的构造方法. 与已有研究方法相比, 本文所提出的方法仅依赖于 Galois 型移位寄存器的结构矩阵中非零元素的行和列的位置信息, 这有效丰富了布尔网络体系下移位寄存器相互转换的理论框架. 后续研究将进一步探究含控制输入的 Galois 型移位寄存器向反馈函数为$f(x,u)$的 Fibonacci 型移位寄存器转化的可行性.

参考文献 (References)

[1] Golomb S W. Shift register sequences[M]. The 3rd edition. Singapore: World Scientific, 2017.

[2] 王海燕. 基于半张量积方法的反馈移位寄存器研究[D]. 北京: 中国科学院大学, 2017.
(Wang H Y. Research on feedback shift register via semi-tensor product approach[D]. Beijing: University of Chinese Academy of Sciences, 2017.)

[3] 程代展, 齐洪胜, 刘挺, 等. 从矩阵半张量积到逻辑控制系统[J]. 中国科学: 数学, 2016, 46(10): 1401-1424.
(Cheng D Z, Qi H S, Liu T, et al. From semi-tensor product of matrices to logical control systems. Scientia Sinica: Mathematica, 2016, 46(10): 1401-1424.)

[4] 冯俊娥, 赵荣, 孙菁涵, 等. 逻辑动态系统拓扑结构的多角度分析[J]. 控制与决策, 2025, 40(9): 2625-2638.
(Feng J E, Zhao R, Sun J H, et al. Multi-perspective analysis of topological structure of logical dynamical systems[J]. Control and Decision, 2025, 40(9): 2625-2638.)

[5] 程代展, 齐洪胜, 赵寅. 布尔网络的分析与控制——矩阵半张量积方法[J]. 自动化学报, 2011, 37(5): 529-540.
(Cheng D Z, Qi H S, Zhao Y. Analysis and control of Boolean networks: A semi-tensor product approach[J]. Acta Automatica Sinica, 2011, 37(5): 529-540.)

[6] 冯俊娥, 李怡靓, 赵荣. 基于矩阵半张量积的有限值动态系统的最新进展[J]. 控制与决策, 2022, 37(2): 267-277.
(Feng J E, Li Y L, Zhao R. Recent developments of finite-valued dynamic systems based on semi-tensor product of matrices[J]. Control and Decision, 2022, 37(2): 267-277.)

[7] Liang J L, Chen H W, Lam J. An improved criterion for controllability of Boolean control networks[J]. IEEE Transactions on Automatic Control, 2017, 62(11): 6012-6018.

[8] Zhang X, Meng M, Wang Y H, et al. Criteria for observability and reconstructibility of Boolean control networks *via* set controllability[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2021, 68(4): 1263-1267.

[9] 王彪, 冯俊娥. 关于布尔控制网络的能观性和能检性的研究现状[J]. 控制与决策, 2020, 35(9): 2049-2058.
(Wang B, Feng J E. Recent development on observability and detectability of Boolean control networks[J]. Control and Decision, 2020, 35(9): 2049-

2058.)

[10] 白博文, 王金环. 非周期性 DoS 攻击下布尔控制网络的镇定控制[J]. 控制与决策, 2025, 40(7): 2168-2174.
(Bai B W, Wang J H. Stabilization of Boolean control networks under aperiodic DoS attacks[J]. Control and Decision, 2025, 40(7): 2168-2174.)

[11] Zhang X H, Han H X, Zhang W D. Identification of Boolean networks using premined network topology information[J]. IEEE Transactions on Neural Networks and Learning Systems, 2017, 28(2): 464-469.

[12] Zou Y L, Zhu J D. Kalman decomposition for Boolean control networks[J]. Automatica, 2015, 54: 65-71.

[13] Laschov D, Margaliot M. A maximum principle for single-input Boolean control networks[J]. IEEE Transactions on Automatic Control, 2011, 56(4): 913-917.

[14] Wu Y H, Shen T L. A finite convergence criterion for the discounted optimal control of stochastic logical networks[J]. IEEE Transactions on Automatic Control, 2018, 63(1): 262-268.

[15] 杨俊起, 李浩, 陈志. 基于控制的弱可重构布尔控制网络状态可重构性与估计[J]. 控制理论与应用, 2026, 43(7): 1506-1512.
(Yang J Q, Li H, Chen Z. Control-based state reconstructibility and estimation of weakly reconstructible Boolean control networks[J]. Control Theory & Applications, 2026, 43(7): 1506-1512.)

[16] 徐勇, 朱万里, 李杰. 基于事件触发和状态翻转的布尔控制网络输出跟踪[J]. 控制与决策, 2023, 38(5): 1258-1266.
(Xu Y, Zhu W L, Li J. Output tracking of Boolean control networks based on event-triggered and state-flipped[J]. Control and Decision, 2023, 38(5): 1258-1266.)

[17] Li H T, Xie L H, Wang Y Z. Output regulation of Boolean control networks[J]. IEEE Transactions on Automatic Control, 2017, 62(6): 2993-2998.

[18] Zou Y L, Yang S J, Liu Y R. Functional observer design for Boolean control networks with unknown structures[J]. Journal of the Franklin Institute, 2024, 361(4): 106649.

[19] Liu X Y, Zhu J D. On potential equations of finite games[J]. Automatica, 2016, 68: 245-253.

[20] Zhong J H, Lin D D. Stability of nonlinear feedback shift registers[J]. Science China Information Sciences, 2016, 59(1): 1-12.

[21] Ren B B, Liu Y, Lu J Q, et al. A novel analysis method for grain-like cascade FSRs[C]. 2020 12th International Conference on Advanced Computational Intelligence. Dali, 2020: 597-601.

[22] Lu J Q, Li M L, Liu Y, et al. Nonsingularity of grain-like cascade FSRs via semi-tensor product[J]. Science China Information Sciences, 2018, 61(1): 010204.

[23] Zhong J H, Lin D D. On maximum length nonlinear feedback shift registers using a Boolean network approach[C]. Proceedings of the 33rd Chinese Control Conference. Nanjing, 2014: 2502-2507.

[24] Goresky M, Klapper A M. Fibonacci and Galois representations of feedback-with-carry shift registers[J]. IEEE Transactions on Information Theory, 2002, 48(11): 2826-2836.

[25] Dubrova E. A transformation from the fibonacci to the Galois NLFSRs[J]. IEEE Transactions on Information Theory, 2009, 55(11): 5263-5271.

[26] Lin Z Q. The transformation from the Galois NLFSR to the fibonacci configuration[C]. Proceedings of the 4th International Conference on Emerging Intelligent Data and Web Technologies. Xi'an, 2013: 335-339.

[27] Lu J Q, Li M L, Huang T W, et al. The transformation between the Galois NLFSRs and the Fibonacci NLFSRs via semi-tensor product of matrices[J]. Automatica, 2018, 96: 393-397.

[28] Li B W, Zhu S Y, Lu J Q. Improved transformation between Fibonacci FSRs and Galois FSRs based on semi-tensor product[J]. Journal of the Franklin Institute, 2022, 359(1): 224-239.

[29] Zhao X Y, Wang B, Yan Y Y, et al. The equivalence transformation between Galois NFSRs and fibonacci NFSRs[J]. Asian Journal of Control, 2021, 23(6): 2865-2873.

[30] Zhao X X, Qi W F, Zhang J M. Further results on the equivalence between Galois NFSRs and fibonacci NFSRs[J]. Designs, Codes and Cryptography, 2020, 88(1): 153-171.

[31] Pan Y Y, Zhong J H, Lin D D. The equivalence between Galois and fibonacci NFSRs[J]. Theoretical Computer Science, 2024, 1003: 114620.

[32] Cheng D Z, Qi H S, Zhao Y. An introduction to semi-tensor product of matrices and its applications[M]. Hackensack: World Scientific Publishing Company, 2012.

[33] Ljung L, Söderström T. Theory and practice of recursive identification[M]. Cambridge: MIT Press, 1983.

[34] Horn R A, Johnson C R. Topics in matrix analysis[M]. Cambridge: Cambridge University Press, 1991.

[35] Cheng D Z, Qi H S, Li Z Q. Analysis and control of Boolean networks: A semi-tensor product approach[M]. London: Springer, 2011.

作者简介

王腾艺 (2001−), 女, 硕士生, 主要研究方向为逻辑动态系统, E-mail: wty202306@163.com;

刘新芸 (1989−), 女, 讲师, 博士, 主要研究方向为逻辑动态系统、博弈论, E-mail: liuxinyun1224@163.com;

邹云蕾 (1989−), 女, 副教授, 博士, 主要研究方向为非线性系统、逻辑动态系统, E-mail: ylzou@yzu.edu.cn.