Pure Mathematics 理论数学, 2025, 15(3), 136-143
Published Online March 2025 in Hans. https://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2025.153085

Hans汉斯

非线性反馈移位寄存器的互馈联结

王长存

青岛大学数学与统计学院，山东 青岛

收稿日期：2025年2月6日；录用日期：2025年3月5日；发布日期：2025年3月14日

摘　要

本文给出了定义在有限域$\mathbb{F}_2$上的任意多个非线性反馈移位寄存器的互馈联结的特征函数表达式。

关键词

非线性反馈移位寄存器，互馈联结，特征函数，星积

The Mutual Feedback Connection of Nonlinear Feedback Shift Registers

Changcun Wang

School of Mathematics and Statistics, Qingdao University, Qingdao Shandong

Received: Feb. 6th, 2025; accepted: Mar. 5th, 2025; published: Mar. 14th, 2025

Abstract

This paper presents the characteristic function expressions for the mutual feedback connections of an arbitrary number of nonlinear feedback shift registers defined over the finite field $\mathbb{F}_2$.

Keywords

Nonlinear Feedback Shift Register, Mutual Feedback Connection, Characteristic Function, *-Product

文章引用: 王长存. 非线性反馈移位寄存器的互馈联结[J]. 理论数学, 2025, 15(3): 136-143.
DOI: 10.12677/pm.2025.153085

1. 引言

移位寄存器是生成伪随机序列的重要模型，它在通信、编码、密码等领域有着广泛的应用。特别是在序列密码的设计中，人们主要使用移位寄存器作为序列源发生器，因此对移位寄存器的研究一直是序列密码设计与分析的重要内容。移位寄存器分为线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)和非线性反馈移位寄存器(Nonlinear Feedback Shift Register, NFSR)。如图 1 所示，每个 x_i 表示一个寄存器的状态，均取值于二元域，$(x_0, x_1, \cdots, x_{n-1})$ 称为该移位寄存器的状态向量，n 元布尔函数 f' 称为该移位寄存器的反馈函数。若反馈函数 f' 是线性布尔函数，则该移位寄存器称为 n 级 LFSR；若 f' 是非线性布尔函数，则为 n 级 NFSR。

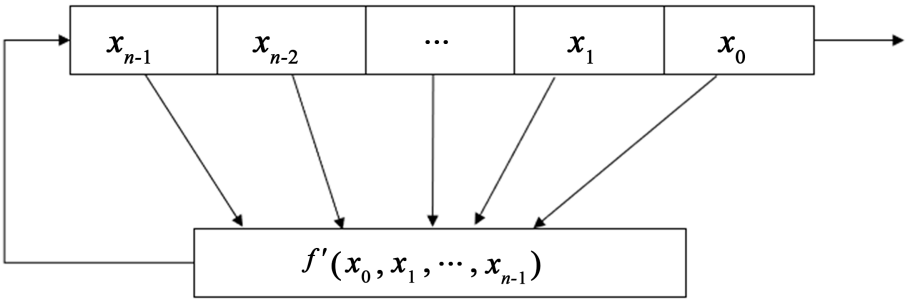

Figure 1. n-Shift register
图 1. n 级移位寄存器

上世纪中后期，密码设计者对 LFSR 所产生序列的密码学性质进行了深入与系统的研究，选用了具备极大周期的 m-序列作为序列密码的序列源，并对其进行非线性改造，从而得到非线性序列，以此应用于序列密码。但在本世纪初，针对基于 LFSR 设计的序列密码算法，人们提出了有效的相关攻击和代数攻击的思想与技术，这对基于 LFSR 设计的序列密码算法造成了极大的威胁。由此，以非线性序列作为序列密码的序列源成为了序列密码设计者的共识。由于 NFSR 可产生的 de Bruijn 序列具有最大周期、元素分布的平衡性等良好的密码学性质，又是非线性的生成方式，因此 NFSR 被认为是取代 LFSR 的一类理想的序列源发生器，逐渐在面向硬件实现的序列密码的设计中占据重要地位。

NFSR 的研究历史可以追溯到 19 世纪末数学家们研究的递归序列问题。但由于非线性问题的困难性以及没有涉及密码应用，关于 NFSR 密码学性质的研究工作并不多。Golomb 在[1]中系统整理了定义在二元域上的 LFSR 和 NFSR 的基本概念和上世纪获得的主要结果，奠定了此后关于 LFSR 和 NFSR 的研究基础。在上世纪，人们主要关注最大周期的 de Bruijn 序列的构造及其线性复杂度。然而，当前人们找到的 de Bruijn 序列的构造方式，与实际的序列密码应用偏离较大，这是至今没有一个成功的基于 de Bruijn 序列的序列密码算法的原因。近二十年，特别是 2004 年欧洲启动的 eSTREAM 序列密码项目最终推荐的基于 NFSR 设计的 Grain、Trivium 和 MICKEY [2]-[4]三个序列密码算法，突破了传统的基于 LFSR 的设计思想，均使用了定义在二元域上的 NFSR 作为序列源发生器，算法结构简洁，同时兼顾安全性、实现速率和灵活性。以上三个序列密码算法以及由此抽象出的三类模型，即 Grain 模型、Trivium 模型和 MICKEY 模型有力促进了围绕 NFSR 的实际应用的研究，其研究问题更加丰富与深刻，如线性子簇[5]-[8]，串联结构[9]-[11]，Galois NFSR 与 Fibonacci NFSR 的等价性[12]等问题。

在上述的三类序列密码模型的设计中，Trivium 型序列密码采用了 NFSR 的互馈联结模型。它是由若干多个 NFSR 相互驱动组成，其第 i 个 NFSR 的输出作为第 $i+1$ 个 NFSR 的输入，最后一个 NFSR 的输出作为第 1 个 NFSR 的输入。本文考察如下形式的 NFSR 的互馈联结。下面以两个移位寄存器的互馈联

结为例，如图 2 所示。它是由两个移位寄存器组合起来，右侧的第一个 n_1 级 NFSR 的输出是左侧第二个 n_2 级 NFSR 的输入，参与了第二个 NFSR 下一时刻的输出。记上述两个 NFSR 的反馈函数分别为 f_1' 和 f_2'，其特征函数为 f_1 和 f_2。我们将这种组合方式称为移位寄存器的互馈联结，记为 $(f_2 \mapsto f_1)$。移位寄存器的互馈联结的详细描述可参见[13]。

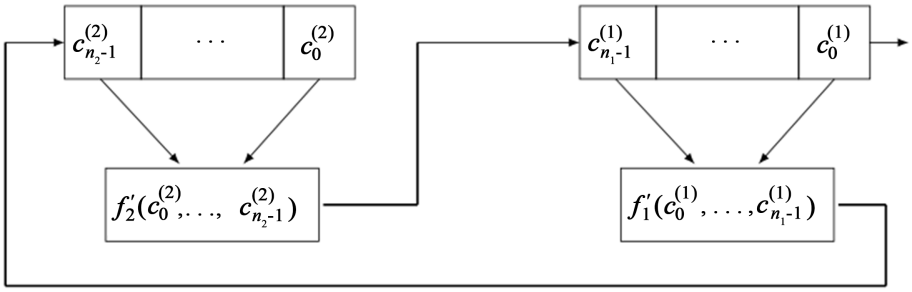

Figure 2. The mutual feedback connection of two NFSRs
图 2. 两个 NFSR 的互馈联结

易见，若图 2 中 f_1' 和 f_2' 均为非线性布尔函数，它们的互馈联结必与一个 n_1+n_2 级的 NFSR 等价，其反馈函数为非线性布尔函数，且由 f_1' 和 f_2' 唯一确定。事实上，任意有限多个 NFSR 的互馈联结本质上与一个级数更高的 NFSR 等价，因此确定多个 NFSR 的互馈联结的特征函数表达式是重要的基本问题。现设定义在二元域上的任意 k 个 NFSR(i)，设 n_i 级非线性反馈移位寄存器 NFSR(i)的反馈函数为 f_i'，其特征函数为 f_i，其中 $1\le i\le k$。以 $(f_k \mapsto f_{k-1} \mapsto \cdots \mapsto f_2 \mapsto f_1)$ 表示 NFSR(i) $(1\le i\le k)$ 的互馈联结。本文给出了互馈联结 $(f_k \mapsto f_{k-1} \mapsto \cdots \mapsto f_2 \mapsto f_1)$ 的特征函数的清晰表达式。

本文第二章介绍下文所需要的预备知识，第三章给出主要结果及其证明，第四章给出示例。

2. 预备知识

本文所研究的 NFSR 均定义在二元域 $\mathbb{F}_2=\{0,1\}$ 上。

二元域上具有两个代数运算，加法与乘法，定义如下[14]：

$$0+0=0,\ 0+1=1,\ 1+1=0.$$

$$0\cdot 0=0,\ 0\cdot 1=0,\ 1\cdot 1=1.$$

NFSR 的模型如图 1 所示，其中 $f'(x_0,x_1,\cdots,x_{n-1})$ 是 n 元布尔函数，称为该 NFSR 的反馈函数，并称

$$f(x_0,x_1,\cdots,x_n)=f'(x_0,x_1,\cdots,x_{n-1})+x_n$$

为该 NFSR 的特征函数。

记 NFSR(f)为以 f 为特征函数的 NFSR，其输出序列 $(a_0,a_1,a_2,\cdots)$ 称为 NFSR 序列，它满足递归关系

$$a_{n+k}=f'(a_k,a_{k+1},\cdots,a_{n+k-1}),\ k=0,1,2,\cdots$$

该 NFSR 的输出序列的全体记为 $G(f)$。

为了描述 NFSR 的互馈联结的特征函数，下面引入布尔函数的星积运算。

定义 1 [15] 设 n 和 m 是两个正整数，$f(x_0,x_1,\cdots,x_n)$ 和 $g(x_0,x_1,\cdots,x_m)$ 分别是 $n+1$ 元布尔函数和 $m+1$ 元布尔函数，则 $f(x_0,x_1,\cdots,x_n)$ 和 $g(x_0,x_1,\cdots,x_m)$ 的星积“$*$”定义为

$$f*g=f\left(g(x_0,x_1,\cdots,x_m),g(x_1,x_2,\cdots,x_{1+m}),\cdots,g(x_n,x_{n+1},\cdots,x_{n+m})\right).$$

若 g 是 h 的一个星积因子是指 g 和 h 满足 $h=f*g$。特别地，g 是 h 的一个线性星积因子是指 g 既

满足上述等式，又是一个线性布尔函数。

g 是 h 的非平凡星积因子是指 g 满足上述等式，又 $g \neq x_0$ 且 $g \neq h$。

星积有如下性质：

1) $f*g$ 不一定等于 $g*f$，即星积不具有交换性。但是，对于线性布尔函数而言，星积具有交换性，即对任意的线性布尔函数 l_1 和 l_2，满足

$$l_1 * l_2 = l_2 * l_1.$$

2) 星积具有左分配律，即对任意的布尔函数 f_1， f_2 和 g 都满足

$$(f_1 + f_2) * g = (f_1 * g) + (f_2 * g),$$

$$(f_1 \cdot f_2) * g = (f_1 * g) \cdot (f_2 * g).$$

3) 星积运算有结合律，即对任意的 n 元布尔函数 f_1， f_2 和 f_3 都有

$$(f_1 * f_2) * f_3 = f_1 * (f_2 * f_3).$$

4) 对任意的布尔函数 g，有

$$1 * g = 1.$$

3. 主要结果

在本节中，我们研究定义在二元域上的任意 k 个 NFSR 的互馈联结，如图 3 所示。其中 n_i 级非线性反馈移位移位寄存器 NFSR(i)的反馈函数为 f_i'，记 NFSR(i)的特征函数为 f_i，其中 $1 \le i \le k$。现将该 NFSR 的互馈联结记为 $(f_k \mapsto f_{k-1} \mapsto \cdots \mapsto f_2 \mapsto f_1)$。我们有如下结论。

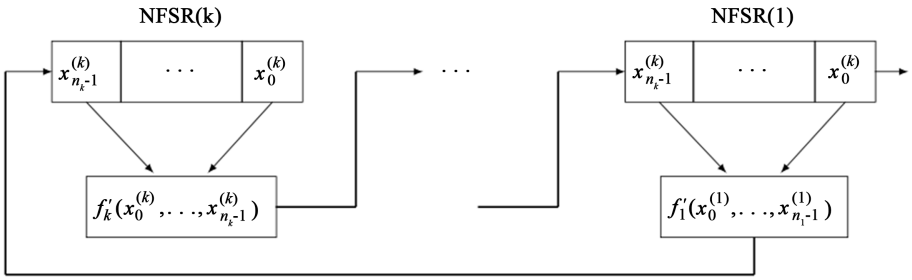

Figure 3. The mutual feedback connection of k NFSRs
图 3. k 个 NFSR 的互馈联结

定理 1 对于图 3 所示的 k 个 NFSR 的互馈联结，设每个反馈函数 f_i' 形如

$$f_i'\left(x_0^{(i)}, x_1^{(i)}, \cdots, x_{n_i-1}^{(i)}\right) = x_0^{(i)} + f_i''\left(x_1^{(i)}, \cdots, x_{n_i-1}^{(i)}\right),$$

则互馈联结 $(f_k \mapsto f_{k-1} \mapsto \cdots \mapsto f_2 \mapsto f_1)$ 的输出序列的全体为

$$G(f_k \mapsto f_{k-1} \mapsto \cdots \mapsto f_2 \mapsto f_1) = G\left(x_{n_1+n_2+\cdots+n_k} + f_2' * \left(f_3' * \left(f_4' * \cdots * \left(f_k' * f_1'\right)\right)\cdots\right)\right),$$

其中 x_i 表示该互馈联结的第 i 个输出。

证明 首先证明集合 $G(f_k \mapsto f_{k-1} \mapsto \cdots \mapsto f_2 \mapsto f_1)$ 包含于集合

$$G\left(x_{n_1+n_2+\cdots+n_k} + f_2' * \left(f_3' * \left(f_4' * \cdots * \left(f_k' * f_1'\right)\right)\cdots\right)\right).$$

记 NFSR(i)的特征函数为

$$f_i\left(x_0^{(i)},\cdots,x_{n_i-1}^{(i)},x_{n_i}^{(i)}\right)=f_i'\left(x_0^{(i)},\cdots,x_{n_i-1}^{(i)}\right)+x_{n_i}^{(i)},$$

设 NFSR(i)的初始状态为$\left(a_0^{(i)},a_1^{(i)},\cdots,a_{n_i-1}^{(i)}\right)$，$1\le i\le k$。

记 f_1' 的输出序列为 $\underline{a^{(k)}}=\left(a_{n_k}^{(k)},a_{n_k+1}^{(k)},\cdots\right)$，$f_i'$ 的输出序列为 $\underline{a^{(i-1)}}=\left(a_{n_{i-1}}^{(i-1)},a_{n_{i-1}+1}^{(i-1)},\cdots\right)$，$i=2,3,\cdots,k$。

由 NFSR(i)的反馈函数所定义的递归关系，可得如下等式

$$\begin{cases}a_{n_1+i}^{(1)}=f_2'\left(a_i^{(2)},a_{i+1}^{(2)},\cdots,a_{i+n_2-1}^{(2)}\right)\\ a_{n_2+i}^{(2)}=f_3'\left(a_i^{(3)},a_{i+1}^{(3)},\cdots,a_{i+n_3-1}^{(3)}\right)\\ \quad\vdots\\ a_{n_{k-1}+i}^{(k-1)}=f_k'\left(a_i^{(k)},a_{i+1}^{(k)},\cdots,a_{i+n_k-1}^{(k)}\right)\\ a_{n_k+i}^{(k)}=f_1'\left(a_i^{(1)},a_{i+1}^{(1)},\cdots,a_{i+n_1-1}^{(1)}\right)\end{cases}$$

成立。

对于任意的 $i\ge 0$，使用上述的等式，互馈联结 $\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right)$ 在 $n_1+n_2+\cdots+n_k+i$ 时刻的输出为

$$\begin{aligned}&a_{n_1+n_2+\cdots+n_k+i}^{(1)}=f_2'\left(a_{n_2+\cdots+n_k+i}^{(2)},a_{n_2+\cdots+n_k+i+1}^{(2)},\cdots,a_{n_2+\cdots+n_k+i+n_2-1}^{(2)}\right)\\&=f_2'\left(f_3'\left(a_{n_3+\cdots+n_k+i}^{(3)},\cdots,a_{n_3+\cdots+n_k+i+n_3-1}^{(3)}\right),\cdots,f_3'\left(a_{n_3+\cdots+n_k+i+n_2-1}^{(3)},\cdots,a_{n_3+\cdots+n_k+i+n_2+n_3-2}^{(3)}\right)\right)\\&=\cdots\\&=f_2'\left(f_3'\left(f_4'\left(\cdots\left(f_{k-1}'\left(f_k'\left(f_1'\left(a_i^{(1)},a_{i+1}^{(1)},\cdots,a_{i+n_1-1}^{(1)}\right),\cdots,f_1'\left(a_{i+n_k+n_{k-1}+\cdots+n_2-(k-1)}^{(1)},\cdots,a_{i+n_k+n_{k-1}+\cdots+n_1-k}^{(1)}\right)\cdots\right)\right)\right)\right)\right)\right)\end{aligned}$$

根据有限域 $\mathbb{F}_2$ 的运算规则，上述等式改写为

$$\begin{aligned}&a_{n_1+n_2+\cdots+n_k+i}^{(1)}\\&+f_2'\left(f_3'\left(f_4'\left(\cdots\left(f_{k-1}'\left(f_k'\left(f_1'\left(a_i^{(1)},a_{i+1}^{(1)},\cdots,a_{i+n_1-1}^{(1)}\right),\cdots,f_1'\left(a_{i+n_k+n_{k-1}+\cdots+n_2-(k-1)}^{(1)},\cdots,a_{i+n_k+n_{k-1}+\cdots+n_1-k}^{(1)}\right)\right)\cdots\right)\right)\right)\right)\right)\\&=0\end{aligned}$$

令

$$\begin{aligned}&F\left(x_0,x_1,\cdots,x_{n_1+n_2+\cdots+n_k}\right)\\&=x_{n_1+n_2+\cdots+n_k}\\&\quad+f_2'\left(f_3'\left(f_4'\left(\cdots\left(f_{k-1}'\left(f_k'\left(f_1'\left(a_i^{(1)},a_{i+1}^{(1)},\cdots,a_{i+n_1-1}^{(1)}\right),\cdots,f_1'\left(a_{i+n_k+n_{k-1}+\cdots+n_2-(k-1)}^{(1)},\cdots,a_{i+n_k+n_{k-1}+\cdots+n_1-k}^{(1)}\right)\right)\cdots\right)\right)\right)\right)\right)\\&=x_{n_1+n_2+\cdots+n_k}+f_2'*\left(f_3'*\left(f_4'*\cdots*\left(f_k'*f_1'\right)\right)\cdots\right)\end{aligned}$$

则有

$$F\left(x_0,x_1,\cdots,x_{n_1+n_2+\cdots+n_k}\right)\left(\underline{a^{(1)}}\right)=0,$$

即互馈联结 $\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right)$ 的输出序列 $\underline{a^{(1)}}$ 满足由布尔函数 $F\left(x_0,x_1,\cdots,x_{n_1+n_2+\cdots+n_k}\right)$ 所确定的递归关系，从而有

$$G\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right)\subseteq G\left(F\left(x_0,x_1,\cdots,x_{n_1+n_2+\cdots+n_k}\right)\right).$$

下面证明 $G\left(F\left(x_0,x_1,\cdots,x_{n_1+n_2+\cdots+n_k}\right)\right)\subseteq G\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right)$。

$\forall \underline{a}\in G(F)$，则有

$$x_{n_1+n_2+\cdots+n_k}+f_2'*\left(f_3'*\left(f_4'*\cdots*\left(f_k'*f_1'\right)\right)\cdots\right)\left(\underline{a}\right)=0$$

成立。对于任意的 $i\geq 0$，

$$\begin{aligned}&a_{n_1+n_2+\cdots+n_k+i}\\&=f_2'\left(f_3'\left(f_4'\left(\cdots\left(f_{k-1}'\left(f_k'\left(f_1'\left(a_i^{(1)},a_{i+1}^{(1)},\cdots,a_{i+n_1-1}^{(1)}\right),\cdots,f_1'\left(a_{i+n_k+n_{k-1}+\cdots+n_2-(k-1)}^{(1)},\cdots,a_{i+n_k+n_{k-1}+\cdots+n_1-k}^{(1)}\right)\right)\cdots\right)\right)\right)\right)\end{aligned}$$

现由给定序列 $\underline{a}\in G(F)$，求出 NFSR(i)的初始状态，$i=2,3,\cdots,k$。由于每个 NFSR(i)的反馈函数形如

$$f_i'\left(x_0^{(i)},x_1^{(i)},\cdots,x_{n_i-1}^{(i)}\right)=x_0^{(i)}+f_i''\left(x_1^{(i)},\cdots,x_{n_i-1}^{(i)}\right),$$

则

$$\begin{aligned}&a_{n_1+n_2+\cdots+n_i-1}^{(1)}=f_2'\left(a_{n_2+\cdots+n_i-1}^{(2)},a_{n_2+\cdots+n_i}^{(2)},\cdots,a_{n_2+\cdots+n_i+n_2-2}^{(2)}\right)\\&=f_2'\left(f_3'\left(a_{n_3+\cdots+n_i-1}^{(3)},\cdots,a_{n_3+\cdots+n_i+n_3-2}^{(3)}\right),\cdots,f_3'\left(a_{n_3+\cdots+n_i+n_2-2}^{(3)},\cdots,a_{n_3+\cdots+n_i+n_2+n_3-3}^{(3)}\right)\right)\\&=\cdots\\&=f_2'\left(f_3'\left(f_4'\left(\cdots\left(f_{i-1}'\left(f_i'\left(a_{n_i-1}^{(i)},\cdots,a_{2n_i-2}^{(i)}\right),\cdots,f_i'\left(a_{n_i+n_{i-1}+\cdots+n_2-(i-1)}^{(i)},\cdots,a_{n_i+n_i+n_{i-1}+\cdots+n_2-i}^{(i)}\right)\right)\cdots\right)\right)\right)\right)\\&=f_i'\left(a_{n_i-1}^{(i)},\cdots,a_{2n_i-2}^{(i)}\right)+f_2''\left(f_3''\left(f_4''\left(\cdots\left(f_{i-1}''\left(f_i'\left(a_{n_i}^{(i)},\cdots,a_{2n_i-1}^{(i)}\right),\cdots,f_i'\left(a_{n_i+n_{i-1}+\cdots+n_2-(i-1)}^{(i)},\cdots,a_{n_i+n_i+n_{i-1}+\cdots+n_2-i}^{(i)}\right)\right)\cdots\right)\right)\right)\right)\\&=a_{n_i-1}^{(i)}+f_i''\left(a_{n_i}^{(i)},\cdots,a_{2n_i-2}^{(i)}\right)\\&\quad+f_2''\left(f_3''\left(f_4''\left(\cdots\left(f_{i-1}''\left(f_i'\left(a_{n_i}^{(i)},\cdots,a_{2n_i-1}^{(i)}\right),\cdots,f_i'\left(a_{n_i+n_{i-1}+\cdots+n_2-(i-1)}^{(i)},\cdots,a_{n_i+n_i+n_{i-1}+\cdots+n_2-i}^{(i)}\right)\right)\cdots\right)\right)\right)\right)\end{aligned}$$

其中 $a_{n_i}^{(i)},\cdots,a_{n_i+n_i+n_{i-1}+\cdots+n_2-i}^{(i)}$ 都由 $\underline{a}$ 的相应位置唯一确定。

依次考察 a_t，$n_1+n_2+\cdots+n_{i-1}\leq t\leq n_1+n_2+\cdots+n_i-1$，则由上述等式可唯一确定 $a_r^{(i)}$ 的值，其中 $0\leq r\leq n_i-1$，故 $\underline{a^{(i)}}$ 的值都由 $\underline{a^{(1)}}$ 的相应位置的值确定，从而可确定所有寄存器的初始状态。

此时，$\underline{a^{(1)}}$ 可由 $\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right)$ 生成，故有

$$G(F)\subseteq G\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right).$$

综上，$G(F)=G\left(f_k\mapsto f_{k-1}\mapsto\cdots\mapsto f_2\mapsto f_1\right)$。证毕。

注记 上述定理利用布尔函数的星积运算，给出了任意有限多个 NFSR 的互馈联结的特征函数的清晰表达式，同时也得到了其反馈函数的表达式，这为研究多个 NFSR 的互馈联结以及特殊形式的 NFSR 的互馈联结形式的分解提供了基本依据。

4. 示例

本节给出两个 NFSR 互馈联结的例子，以此说明定理 1 的结论。

设定义在二元域上的6级互馈联结如图4所示，其中右侧的NFSR的反馈函数为 $f_1'\left(x_0,x_1,x_2\right)=x_0+x_1x_2$，左侧的 NFSR 的反馈函数为 $f_2'\left(x_3,x_4,x_5\right)=x_3+x_4x_5$。

设在 t 时刻，该互馈联结的状态向量为 $\left(t_0,t_1,t_2,t_3,t_4,t_5\right)$，记 $t+1$ 时刻的状态向量为 $\left(t_0',t_1',t_2',t_3',t_4',t_5'\right)$，则上述状态满足如下关系：

$$t_0'=t_1,t_1'=t_2,t_2'=t_3+t_4t_5,t_3'=t_4,t_4'=t_5,t_5'=t_0+t_1t_2.$$

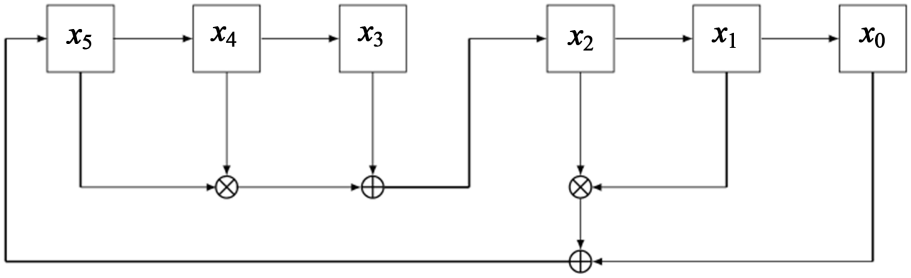

Figure 4. The mutual feedback connection between 3-NFSR and 3-NFSR
图 4. 3 级 NFSR 与 3 级 NFSR 的互馈联结

设该互馈联结的初态为(100000)，则其状态转移过程为：

$$(100001)\to(000011)\to(001110)\to(011100)\to(111001)\to(110010)\to(100101)$$
$$(001011)\to(011110)\to(111101)\to(111010)\to(110100)\to(101001)\to(010011)$$
$$\to(101110)\to(011101)\to(111011)\to(111110)\to(111100)\to(111000)$$
$$\to(110000)\to(100001).$$

该互馈联结生成的序列为：10000011001011010011011000 01…，且是以 26 为周期的周期序列。易知 f_1'， f_2' 满足定理 1 的条件，根据有限域 $\mathbb{F}_2$ 中的运算，则该互馈联结的特征函数为

$$x_{6+i}+f_2'*f_1'=x_{6+i}+x_i+x_{2+i}x_{3+i}+x_{1+i}x_{3+i}x_{4+i}+x_{2+i}x_{3+i}x_{4+i},$$

其中 x_i 为第 i 个时刻的输出。

5. 结论

本文考察了定义在有限域 $\mathbb{F}_2$ 上任意有限多个非线性反馈移位寄存器互馈联结，基于布尔函数的星积运算给出了该互馈联结的特征函数的清晰表达式，为研究多个 NFSR 的互馈联结以及特殊形式的 NFSR 的互馈联结形式的分解提供了基本依据。

参考文献

[1] Golomb, S.W. (2017) Shift Register Sequences: Secure and Limited-Access Code Generators, Efficiency Code Generators, Prescribed Property Generators, Mathematical Models. World Scientific Publishing.

[2] Hell, M., Johansson, T., Maximov, A. and Meier, W. (2008) The Grain Family of Stream Ciphers. In: Robshaw, M. and Billet, O., Eds., *Lecture Notes in Computer Science*, Springer, 179-190. https://doi.org/10.1007/978-3-540-68351-3_14

[3] De Cannière, C. and Preneel, B. (2008) Trivium. In: Robshaw, M. and Billet, O., Eds., *Lecture Notes in Computer Science*, Springer, 244-266. https://doi.org/10.1007/978-3-540-68351-3_18

[4] Babbage, S. and Dodd, M. (2008) The MICKEY Stream Ciphers. In: Robshaw, M. and Billet, O., Eds., *Lecture Notes in Computer Science*, Springer, 191-209. https://doi.org/10.1007/978-3-540-68351-3_15

[5] Tian, T. and Qi, W.-F. (2014) On the Largest Affine Sub-Families of a Family of NFSR Sequences. *Designs, Codes and Cryptography*, 71, 163-181. https://doi.org/10.1007/s10623-012-9723-1

[6] Mykkeltveit, J., Siu, M. and Tong, P. (1979) On the Cycle Structure of Some Nonlinear Shift Register Sequences. *Information and Control*, **43**, 202-215. https://doi.org/10.1016/s0019-9958(79)90708-3

[7] 田甜, 戚文峰. 非线性反馈移位寄存器序列子簇的研究进展[J]. 密码学报, 2014, 1(1): 72-82.

[8] 马蓁. 非线性反馈移位寄存器序列仿射子簇的研究[D]: [硕士学位论文]. 解放军信息工程大学, 2014.

[9] Tian, T. and Qi, W.F. (2014) On Decomposition of an NFSR into a Cascade Connection of Two Smaller NFSRs. *Applicable Algebra in Engineering, Communication and Computing*.

[10] 王中孝, 戚文峰. 非线性反馈移位寄存器串联分解唯一性探讨[J]. 电子与信息学报, 2014(7): 1656-1660.

[11] 章佳敏, 戚文峰. NFSR 串联分解唯一性的研究[J]. 信息工程大学学报, 2017, 18(1): 78-81, 110.

[12] Zhao, X., Qi, W. and Zhang, J. (2019) Further Results on the Equivalence between Galois NFSRs and Fibonacci NFSRs. *Designs*, *Codes and Cryptography*, **88**, 153-171. https://doi.org/10.1007/s10623-019-00677-y

[13] Scholefield, P.H.R. (1960) Shift Registers Generating Maximum-Length Sequences. *Electronic Technology*, **37**, 389-394.

[14] Lidl, R. and Niederreiter, H. (1983) Finite Fields. Addison-Wesley.

[15] Green, D.H. and Dimond, K.R. (1970) Nonlinear Product-Feedback Shift Registers. *Proceedings of the Institution of Electrical Engineers*, **117**, 681. https://doi.org/10.1049/piee.1970.0134