非线性反馈移位寄存器串联分解唯一性探讨

王中孝* 戚文峰
(解放军信息工程大学数学工程与先进计算国家重点实验室 郑州 450002)

摘 要：非线性反馈移位寄存器(NFSR)是目前序列密码研究的热点问题之一。假定一个 NFSR 可以分解为更低级数 NFSR 的串联，该文讨论此分解是否唯一的问题。首先，对线性反馈移位寄存器(LFSR)而言，其串联分解等价于二元有限域 F_2 上单变元多项式的分解，因而是唯一的。其次，针对给定 NFSR 可以分解为更低级数 NFSR 到 LFSR 串联的情形，该文给出了此 NFSR 具有这样分解的一个充分必要条件，并据此指出所有这样分解中级数最大的 LFSR 是唯一的。该文的最后构造了一类反例，此类反例表明对一般情形而言，NFSR 的串联分解并不唯一。

关键词：流密码；非线性反馈移位寄存器；非线性反馈移位寄存器的串联；分解唯一性
中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2014)07-1656-05
DOI: 10.3724/SP.J.1146.2013.01062

On the Uniqueness of Decomposition of a NFSR into a Cascade Connection of Smaller NFSRs

Wang Zhong-xiao Qi Wen-feng
(*State Key Laboratory of Mathematical Engineering and Advanced Computing*, *PLA Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: The Nonlinear Feedback Shift Register (NFSR) is one of hot topics of stream cipher in recent studies. The uniqueness of a NFSR assuming to be decomposed into a cascade connection of smaller NFSRs is discussed in this paper. Firstly, the decomposition of Linear Feedback Shift Register (LFSR) is equivalent to the decomposition of univariate polynomials over the finite field of two elements F_2, thus it is unique. Secondly, for the case that a NFSR can be decomposed into a cascade connection of a NFSR into a LFSR, a necessary and sufficient condition is offered for a NFSR to have such a decomposition. Based on this condition, it is indicated that during all such decompositions, the largest LFSR is unique. However, the construction of counterexamples in a class shows that, for the general cases, the decomposition of a NFSR into a cascade connection of smaller NFSRs is not unique.

Key words: Stream cipher; Nonlinear Feedback Shift Register (NFSR); Cascade connection of NFSRs; Uniqueness of decomposition

1 引言

序列密码(也称流密码)因其高效、易于实现及成本低廉等特性在通信和密码领域有着广泛的应用。线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)序列因为具有良好的代数结构，其密码性质得到了持续的关注及清晰地刻画。特别地，极大周期 LFSR 序列即 m-序列，具有周期大、元素分布平衡以及良好的自相关性等密码性质，因此早期的序列密码体制大多采用 m-序列作为驱动序列。然而近年来，随着相关攻击[1−3]及代数攻击[4,5]的不断发展，基于 LFSR 的密码体制面临越来越多的安全威胁，于是非线性反馈移位寄存器(Nonlinear Feedback Shift Register, NFSR)序列得到了越来越多的关注[6−10]。虽然 NFSR 序列因其天然的非线性结构使得代数攻击等传统手段难以分析，然而由于非线性问题的困难性，NFSR 序列的周期等基本密码性质至今没有令人满意的结论，如欧洲序列密码计划中胜出的硬件算法 Trivium[10]输出序列的周期目前仍是一个公开问题。

基于利用较低级数 NFSR 来构造较高级数 NFSR 的思想，NFSR 的串联首先由文献[11]提出。欧洲序列密码计划中另一个胜出的硬件算法 Grain[12]即为一个 LFSR 到 NFSR 的串联。另一方面，对于用作非线性驱动的 NFSR(h)，假设其可以分解为 NFSR(f)到 NFSR(g)的串联。由文献[11]可知，如果 NFSR(f)含有全 0 的输出序列，那么

2013-07-19 收到，2014-04-03 改回
国家自然科学基金(61272042, 61100202, 61170235)资助课题
*通信作者：王中孝 zhongxiao_wang@126.com

NFSR(h)的输出序列集中将包含 NFSR(g)的全部输出序列。特别地，如果 NFSR(g)恰为一个 LFSR，那么 NFSR(h)的输出序列集中将包含一个 LFSR 的全部输出序列。这也意味着，对于错误的初态选取，NFSR(h)的输出序列将是完全的 LFSR 序列，这将给密码体制带来很大的安全隐患。因而对给定 NFSR，判定其是否可以分解为更低级数 NFSR 的串联是十分有意义的。文献[13]研究了将给定 NFSR 分解为更低级数 NFSR 到 LFSR 串联的问题，然而该文并未讨论此种分解是否唯一的问题，并且由于计算中存在系数膨胀等问题，极端情形下算法将因内存溢出而无法执行。本文探讨 NFSR 串联分解是否唯一的问题。首先，对于 LFSR 的串联而言，其串联分解等价于二元有限域 F_2 上单变元多项式的分解，因而是唯一的。其次，本文证明了给定 NFSR 可以分解为更低级数 NFSR 到 LFSR 串联的一个充要条件，并据此指出，所有这样的分解中级数最大的 LFSR 是唯一的。这一结论有助于改进文献[13]中的算法以提高其效率。本文的最后构造了一类反例，该反例表明对于一般的 NFSR 而言，其串联分解并不具有唯一性。

2　准备知识

在下文中，记号 F_2 表示二元有限域，F_2^n 表示 F_2 上的 n 维向量空间。符号“+”表示普通的加法，符号“⊕”表示模 2 加法。

本节给出布尔函数、非线性反馈移位寄存器(NFSR)及其串联的简单介绍。

2.1 布尔函数及星积运算

给定正整数 n, n 元布尔函数 f 是 F_2^n 到 F_2 的一个映射，记 n 元布尔函数的全体为 $\mathcal{B}_n$。一个 n 元布尔函数 f 可以由如式(1) n 元多项式唯一表示。

$$f(x_0,\cdots,x_{n-1})=\bigoplus_{\alpha=(\alpha_0,\cdots,\alpha_{n-1})\in\mathrm{F}_2^n} u_\alpha\cdot\left(\prod_{j=0}^{n-1}x_j^{\alpha_j}\right) \tag{1}$$

其中 $u_\alpha\in\mathrm{F}_2$，上述表达式称为布尔函数 f 的代数正规型，下文中出现的布尔函数皆用其代数正规型表示。如果 $f(0,\cdots,0)=0$，也即 f 不含有常数项 1，则称 f 是规范的。更进一步，如果 f 还满足其次数 $\deg(f)=1$，则称 f 是线性的。给定布尔函数 $f\in\mathcal{B}_{m+1}$ 以及 $g\in\mathcal{B}_{n+1}$，定义 f 到 g 的星积，记为 $f*g$。

$$f*g=f\big(g(x_0,\cdots,x_n),g(x_1,\cdots,x_{n+1}),\cdots,g(x_m,\cdots,x_{n+m})\big) \tag{2}$$

本文用符号“$*$”代替“$\cdot$”以区别于普通的乘法。需要注意的是，多数情况下星积运算不满足交换律，即 $f*g\neq g*f$。

2.2 NFSR 及其串联

对于正整数 n，以 $f_0(x_0,\cdots,x_{n-1})$ 为反馈函数的 n 级 NFSR 如图 1 所示。称布尔函数。

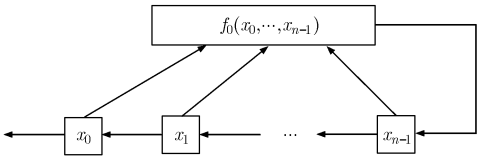

图 1 n 级 NFSR

$$f(x_0,\cdots,x_n)=f_0(x_0,\cdots,x_{n-1})\oplus x_n \tag{3}$$

为特征函数，记该 NFSR 为 NFSR(f)。特别地，当 $f(x_0,\cdots,x_n)$ 是线性函数时，NFSR(f)即为线性反馈移位寄存器(LFSR)。NFSR(f)的输出序列 $\underline{a}=(a_t)_{t\geq0}$ 是指满足如式(4)关系的一条二元序列：

$$f(a_t,\cdots,a_{t+n})=0,\ t=0,1,2,\cdots \tag{4}$$

其所有输出序列的集合记为 $G(f)$，对应不同的初态 $(a_0,\cdots,a_{n-1})$ 选取，不难发现 $|G(f)|=2^n$。由文献[14]可知，NFSR(f)中所有序列都是周期的当且仅当 f 是非奇异的，即 f 可以写成式(15)的形式。

$$f(x_0,\cdots,x_n)=x_0\oplus f_1(x_1,\cdots,x_{n-1})\oplus x_n \tag{5}$$

其中 f_1 为 $n-1$ 元布尔函数。本文仅讨论非奇异的特征函数，因此下文中出现的特征函数均是非奇异的。

NFSR(f)到 NFSR(g)的串联如图 2 所示，其中 $f=f_0(y_0,\cdots,y_{m-1})\oplus x_m, g=g_0(x_0,\cdots,x_{n-1})\oplus x_n$，其输出序列的集合记为 $G(f,g)$。如果 f 是规范的，那么当 NFSR(f)输出全 0 序列时，串联寄存器的输出序列即为 NFSR(g)的输出序列，因此容易知道 $G(g)\subset G(f,g)$。由文献[11], NFSR(f)到 NFSR(g)串联有如下基本性质。

定理 1[11]：如果 f 和 g 为特征函数，那么 $G(f,g)=G(f*g)$。

定理 1 表明对 NFSR(h)进行串联分解等价于寻找特征函数 f 和 g 使得 $h=f*g$，也即在星积运算下对特征函数 h 进行分解，以下简称为 h 的星积分解。

3　主要结果

本节讨论星积分解是否唯一的问题，首先给出相关定义并排除一些平凡的情况。

定义 1　如果 $h=f*g$，则称 f 是 h 的左星积因子，称 g 是 h 的右星积因子。

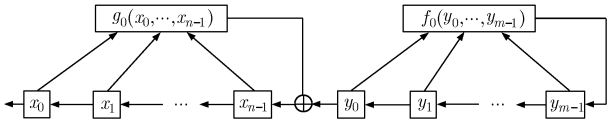

图 2　NFSR(f)到 NFSR(g)的串联

注意到对任意的布尔函数 h，始终有 $h = x_0 * h = h * x_0$ 成立，称上述分解为平凡的分解，称 h 和 x_0 为 h 平凡的星积因子。如果 h 除去平凡的星积因子外没有其它的(左或者右)星积因子，则称 h 是星积不可约的。除特殊声明外，所有星积分解都指非平凡的分解。

给定布尔函数 $f(x_0,\cdots,x_n)$，称 $D(f) = f(x_0 \oplus 1, \cdots, x_n \oplus 1)$ 为 f 的对偶多项式。由星积的定义，下述性质显然成立：

(1)设若 $h = f * g$，那么 $h \oplus 1 = (f \oplus 1) * g$。

(2)设 f 和 g 为布尔函数，则 $f * g = D(f) * (g \oplus 1)$。

(3)设 l_1 和 l_2 为线性函数，则 $l_1 * l_2 = l_2 * l_1$。

(4)设 f 和 g 为布尔函数，则 $D(f * g) = f * D(g)$。

由性质(1)可知，函数 h 和 $h \oplus 1$ 具有相同的星积分解性质。因此对星积分解而言，仅需考虑 h 是规范的情形。此外由性质(2)，如果 $h = f * g$ 且 $g(0,\cdots,0) = 1$，那么存在分解 $h = D(f) * (g \oplus 1)$ 使得 $(g \oplus 1)$ 是规范的。综上讨论，下文总是假定如果 $h = f * g$，那么 h, f 和 g 都是规范的。虽然对于一般情形星积运算不具有交换性质，然而性质(3)却表明，当 f 和 g 皆为线性函数时星积运算是可交换的。基于上述分析，定义 2 给出了星积分解唯一的定义。

定义 2 设若 $h = f_1 * f_2 * \cdots * f_t = g_1 * g_2 * \cdots * g_s$，其中所有的 $f_u, g_v, 1 \le u \le t, 1 \le v \le s$ 是规范的且星积不可约的。如果或者经过适当排序后总是有 $t = s$ 且 $f_i = g_i, i = 1,2,\cdots,t$，则称 h 是星积分解唯一的。

3.1 LFSR 的串联分解

本节考虑线性反馈移位寄存器(LFSR)的串联。由星积定义可知，下述结论是显然的。

定理 2 设若线性函数 $l = f * g$，则 f 和 g 都是线性函数。

定理 2 表明 LFSR 仅可能由 LFSR 串联而成。对于线性函数 $l = c_0 x_0 \oplus c_1 x_1 \oplus \cdots \oplus c_m x_m$ 定义如下映射：

$$\varphi(l) = c_0 + c_1 x + \cdots \oplus c_m x^m \tag{6}$$

可以看到，映射 φ 将线性函数一一对应到二元有限域 F_2 上的单变元多项式。在此定义下，容易看到 $\varphi(l_1 * l_2) = \varphi(l_1) \cdot \varphi(l_2)$。这意味着对于线性函数而言，其星积分解本质上就是单变元多项式的分解。由有限域 F_2 上单变元多项式分解的唯一性可知，对 LFSR 而言，其串联分解是唯一的。

3.2 NFSR 到 LFSR 串联的情形

本小节研究文献[13]所讨论的情形，即 NFSR(h) 可以分解为 NFSR(f)到 LFSR(l)串联的情形。布尔函数 $f(x_0,\cdots,x_n)$ 对序列 $\underline{a} = (a_t)_{t \ge 0}$ 的作用，记为 $f \circ \underline{a}$，定义如下：

$$f \circ \underline{a} = \left(f(a_0,\cdots,a_n), f(a_1,\cdots,a_{n+1}),\cdots\right) \tag{7}$$

此记号下，序列 $\underline{a} \in G(f)$ 当且仅当 $f \circ \underline{a} = \underline{0}$。另外，不难发现 $(f * g) \circ \underline{a} = f \circ (g \circ \underline{a})$。给定序列集 $G(h)$ 和 $G(l)$，记 $G(h) \oplus G(l) = \{\underline{a} \oplus \underline{b} \mid \underline{a} \in G(h), \underline{b} \in G(l)\}$。若 l 是线性函数，引理 1 给出了一个 $h = f * l$ 的充分必要条件。

引理 1 设 h 和 l 皆为特征函数，那么存在特征函数 f 使得 $h = f * l$ 当且仅当 $G(h) = G(h) \oplus G(l)$。

证明 必要性：如果 $h = f * l$，那么对于任意的 $\underline{a} \in G(h)$ 及 $\underline{e} \in G(l)$，

$$\begin{aligned} h \circ (\underline{a} \oplus \underline{e}) &= (f * l) \circ (\underline{a} \oplus \underline{e}) = f \circ \left(l \circ (\underline{a} \oplus \underline{e})\right) \\ &= f \circ (l \circ \underline{a}) = h \circ \underline{a} = 0 \end{aligned} \tag{8}$$

换言之 $\underline{a} \oplus \underline{e} \in G(h)$，也即 $G(h) = G(h) \oplus G(l)$。

充分性：不妨设 h 及 l 分别为 $m+n$ 及 n 级 NFSR 的特征多项式，为

$$\left.\begin{aligned} h(x_0,\cdots,x_{m+n}) &= x_0 \oplus h_0(x_1,\cdots,x_{m+n-1}) \oplus x_{m+n} \\ l(x_0,\cdots,x_n) &= x_0 \oplus l_0(x_1,\cdots,x_{n-1}) \oplus x_n \end{aligned}\right\} \tag{9}$$

其中 h_0 及 l_0 分别为 $(m+n-1)$ 和 $(n-1)$ 元布尔函数。记

$$\left.\begin{aligned} A_h &= \left\{\boldsymbol{a}_{(m+n)} = (a_0, a_1, \cdots, a_{m+n}) \,\middle|\, h(a_0,\cdots,a_{m+n}) = 0\right\} \\ B_l &= \left\{\boldsymbol{e}_{(m+n)} = (e_0, e_1, \cdots, e_{m+n}) \,\middle|\, l(e_i,\cdots,e_{i+n}) = 0, i = 0,1,\cdots,m\right\} \end{aligned}\right\} \tag{10}$$

由 h 和 l 定义集合

$$\begin{aligned} C_f = \{\boldsymbol{c}_m = &\left(l(a_0,\cdots,a_n),\cdots,l(a_m,\cdots,a_{m+n})\right) \,\big|\, \\ &h(a_0,\cdots,a_{m+n}) = 0\} \end{aligned} \tag{11}$$

并构造如下 $m+1$ 元布尔函数

$$f(c_0, c_1, \cdots, c_m) = 0 \text{当且仅当} (c_0, c_1, \cdots, c_m) \in C_f \tag{12}$$

下面证明这样得到的 f 为特征函数，也即 f 具有式(13)的形式

$$f(x_0,\cdots,x_m) = x_0 \oplus f_1(x_1,\cdots,x_{m-1}) \oplus x_m \tag{13}$$

首先证明：如果 $(c_0, c_1, \cdots, c_m) \in C_f$，那么 $(\bar{c}_0, c_1, \cdots, c_m) \notin C_f$，其中 $\bar{c}_0 = c_0 \oplus 1$ 为 c_0 的取反。如若不然，则存在 $\boldsymbol{a}_{(m+n)} = (a_0, a_1, \cdots, a_{m+n}) \in A_h, \boldsymbol{b}_{(m+n)} = (b_0, b_1, \cdots, b_{m+n}) \in A_h$ 满足 $c_0 = l(a_0,\cdots,a_n) = l(b_0,\cdots,b_n) \oplus 1$ 及 $c_i = l(a_i,\cdots,a_{i+n}) = l(b_i,\cdots,b_{i+n}), i = 1,2,\cdots,m$。由 $G(h) = G(h) \oplus G(l)$ 知，存在 $\boldsymbol{e}_{(m+n)} = (\bar{a}_0 \oplus b_0, a_1 \oplus b_1, \cdots, a_{n-1} \oplus b_{n-1}, e_n', \cdots, e_{m+n}') \in B_l$ 使得

$$\boldsymbol{e}_{(m+n)} \oplus \boldsymbol{b}_{(m+n)} = \left(\bar{a}_0, a_1, \cdots, a_{n-1}, b_n', \cdots, b_{m+n}'\right) \in A_h \tag{14}$$

其中 $b_{n+i}' = b_{n+i} \oplus e_{n+i}', i = 0,1,\cdots,m$。注意到 $\boldsymbol{b}_{(m+n)}$ 及 $\boldsymbol{e}_{(m+n)} \oplus \boldsymbol{b}_{(m+n)}$ 对应于 C_f 中同一个元素，因此

$$c_0 = a_0 \oplus l_0(a_1,\cdots,a_{n-1}) \oplus a_n = \overline{a}_0 \oplus l_0(a_1,\cdots,a_{n-1}) \oplus b_n' \oplus 1 \tag{15}$$

得到 $a_n = b_n'$。类次地由 c_i 可以得到 $a_{n+i} = b_{n+i}'$，i=1, 2,$\cdots,m$ 。也即

$$\boldsymbol{e}_{(m+n)} \oplus \boldsymbol{b}_{(m+n)} = (\overline{a}_0, a_1,\cdots,a_{n-1},a_n,\cdots,a_{m+n}) \in A_h \tag{16}$$

然而由 $\boldsymbol{a}_{(m+n)} = (a_0,a_1,\cdots,a_{m+n}) \in A_h$ 知道

$$a_0 \oplus h_0(a_1,\cdots,a_{m+n-1}) \oplus a_{m+n} = 0 \tag{17}$$

这与 $(\overline{a}_0,a_1,\cdots,a_{n-1},a_n,\cdots,a_{m+n}) \in A_h$ 矛盾。故而如果 $(c_0,c_1,\cdots,c_m) \in C_f$，那么 $(\overline{c}_0,c_1,\cdots,c_m) \notin C_f$。由 f 的定义知

$$f(x_0,\cdots,x_m) = x_0 \oplus f_0(x_1,\cdots,x_m) \tag{18}$$

另一方面，类似上述讨论可知：如果 $(c_0,c_1,\cdots,c_m) \in C_f$，那么 $(c_0,c_1,\cdots,\overline{c}_m) \notin C_f$。因此函数 f 又满足

$$f(x_0,\cdots,x_m) = x_m \oplus f_m(x_0,\cdots,x_{m-1}) \tag{19}$$

综上可知存在 $m-1$ 元布尔函数 $f_1(x_1,\cdots,x_{m-1})$ 使得

$$f(x_0,\cdots,x_m) = x_0 \oplus f_1(x_1,\cdots,x_{m-1}) \oplus x_m \tag{20}$$

容易验证，特征函数 f 满足 $h = f * l$。　　证毕

设若 $h = f * l$，由于前文假定 f 是规范的，因而 $G(l) \subset G(h)$。然而，通常情形下 $G(l) \subset G(h)$ 并不能保证 $G(h) = G(h) \oplus G(l)$。因此当 $h = f * l$ 时，引理 1 事实上对 $G(h)$ 和 $G(l)$间的序列关系给出了更深刻的刻画。由引理 1，下述定理是容易得到的。

定理 3 设 h 和 $f_i,l_i,i=1,2$ 皆为特征函数且 $\gcd(\varphi(l_1),\varphi(l_2)) = 1$。如果 $h = f_1 * l_1 = f_2 * l_2$，那么存在特征函数 f 使得 $h = f * l_1 * l_2$。

证明　由引理 1，因为 $h = f_1 * l_1$，所以

$$G(h) = G(h) \oplus G(l_1) \tag{21}$$

又因为 $h = f_2 * l_2$，所以又有

$$G(h) = G(h) \oplus G(l_2) = G(l_1) \oplus G(l_2) \tag{22}$$

注意到 $\gcd(\varphi(l_1),\varphi(l_2)) = 1$，由 LFSR 相关理论知道

$$G(l_1) \oplus G(l_2) = G(l_1 * l_2) \tag{23}$$

因而 $G(h) = G(h) \oplus G(l_1 * l_2)$，再由引理 1 可知存在特征函数 f 使得 $h = f * l_1 * l_2$。　　证毕

对于线性函数 l_1 和 l_2，如果线性函数 l 满足 $\varphi(l) = \mathrm{lcm}(\varphi(l_1),\varphi(l_2))$，则称 l 是函数 l_1 和 l_2 的最小公倍式。定理 3 表明若 $h = f_1 * l_1 = f_2 * l_2$，那么 l_1 和 l_2 的最小公倍式 l 也是 h 的右星积因子。因此，设若 NFSR(h)可以分解为 NFSR(f)到 LFSR(l)的串联，那么所有这样的分解中级数最大的 LFSR 是唯一的。文献[13]的基本内容为：设若 $h = f * l$，那么可以由 h 推导得出一个 l 的(线性)倍式。分解此倍式(对应于单变元多项式的分解)，将分解所得的因子逐一试错便可得到 h 所有的线性右星积因子，其中试错过程是算法复杂度的主要方面。定理 3 则表明，可以将所得的因子依照级数从大到小的次序进行试错，那么第 1 个正确的因子 l 是极大的，因而也是唯一的，余下的正确因子必定皆为 l 的因子故而无需再试，这样可以有效减少试错的次数进而提高算法的效率。

3.3 一类反例

仍然是基于引理 1，下述定理构造了一类反例，此类反例表明对于一般情形的星积分解，确实存在分解不唯一的情形。

定理 4　如果特征函数 f 满足 $D(f) = f \oplus 1$，那么存在特征函数 g 使得

$$(x_0 \oplus x_1) * f = g * (x_0 \oplus x_1) \tag{24}$$

证明　设 h=$(x_0 \oplus x_1) * f$，由星积定义容易知道

$$h = (x_0 \oplus x_1) * f = (x_0 \oplus x_1) * (f \oplus 1) \tag{25}$$

因而 $G(f) \subset G(h), G(f \oplus 1) \subset G(h)$。注意到

$$\left.\begin{aligned} G(f) \cap G(f \oplus 1) &= \varnothing \\ |G(h)| &= |G(f)| + |G(f \oplus 1)| \end{aligned}\right\} \tag{26}$$

所以 $G(h) = G(f) \cup G(f \oplus 1) = G(f) \cup G(D(f))$。

又注意到 $G(x_0 \oplus x_1) = \{\underline{0}, \underline{1}\}$ 及 $G(D(f)) = G(f) \oplus \{\underline{1}\}$，因此

$$G(h) = G(h) \oplus G(x_0 \oplus x_1) \tag{27}$$

由引理 1 知，存在特征函数 g 满足 $h = g * (x_0 \oplus x_1)$ 也即

$$(x_0 \oplus x_1) * f = g * (x_0 \oplus x_1) \tag{28}$$

简单计数可知，所有 n 级 NFSR 特征函数的个数为 $2^{2^{n-1}}$，其中满足 $D(f) = f \oplus 1$ 的 f 的个数为 $2^{2^{n-2}}$，因此反例的数量是十分庞大的。需要说明的是，上述反例是非平凡的，即 f 不可能分解出 $(x_0 \oplus x_1)$作为其右星积因子，否则由性质(4)可知

$$D(f) = f_0 * D(x_0 \oplus x_1) = f_0 * (x_0 \oplus x_1) = f \tag{29}$$

与 $D(f) = f \oplus 1$ 矛盾。

本文构造了如下一个简单例子，令

$$f = x_0 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_4 \tag{30}$$

可以验证 f 满足 $D(f) = f \oplus 1$ 且星积不可约，由定理 4 计算得

$$g = x_0 \oplus x_3 \oplus x_1x_2 \oplus x_2x_3 \oplus x_4 \tag{31}$$

满足 $(x_0 \oplus x_1) * f = g * (x_0 \oplus x_1)$。　　证毕

可以验证 g 亦是星积不可约的。此例表明对于一般的星积分解而言，其分解并不具有唯一性。也即对一般情形的 NFSR 串联分解，其分解并不唯一。

最后，给定两个 n 级 NFSR 的特征函数 g_1 及 g_2，设若存在特征函数 f_1 及 f_2 使得

$$h = f_1 * f_2 = g_1 * g_2 \tag{32}$$

由前假定 f_1 和 f_2 是规范的，所以 $G(g_1)\subset G(h)$ 且 $G(g_2)\subset G(h)$，也即 $(G(g_1)\cup G(g_2))\subset G(h)$。极端情况下，满足此性质的 NFSR($h$)的级数至少为 2^n-1，如：令 g_1 为任一个 n 级 m-序列的特征多项式，令特征函数 $g_2=g_1\oplus(x_1\oplus 1)\cdots(x_{n-1}\oplus 1)$。这一现象表明，给定特征函数 g_1 及 g_2，即便存在 h 使得 $h=f_1*f_2=g_1*g_2$，由于 NFSR(h)的级数可能是指数级的，计算上求取 h 也是不可行的。实验也表明，对小级数的 NFSR 而言，其串联分解几乎是全部唯一的。从这个角度来看，构造更具一般性的反例是困难的。

4 结束语

本文探讨了非线性反馈移位寄存器(NFSR)的串联分解是否唯一的问题。首先，对于线性反馈移位寄存器(LFSR)而言，其串联分解等价于二元有限域 F_2 上的单变元多项式分解因而是唯一的。其次，本文给出了给定 NFSR 可以分解为更低级数的 NFSR 到 LFSR 串联的一个充分必要条件。据此可以证明，所有这样分解中级数最大的 LFSR 是唯一的，该结论可以有效地改进文献[13]中的算法以提高其效率。最后，本文构造了一类反例表明对于一般的情形，该分解并不具有唯一性。由于非线性问题的困难性，目前仅能对较小级数和一些特殊的 NFSR 进行串联分解，因此构造更具一般性的反例是困难的。事实上，正是由于计算上的困难性，关于 NFSR 的串联分解仍然有很多问题尚不明了。特别地，NFSR 的串联分解完全不同于整数分解或者其它整环上的分解，因此对 NFSR 的串联分解而言，考虑到其结构的特殊性，是否存在更加合理的分解唯一的定义并对其进行进一步的论证是极有意义的。

参 考 文 献

[1] Meier W and Staffelbach O. Fast correlation attacks on certain stream ciphers[J]. *Journal of Cryptology*, 1989, 1(3): 159–176.

[2] Canteaut A and Trabbia M. Improved fast correlation attacks using parity-check equations of weight 4 and 5[C]. Advances in Cryptology-EUROCRYPT 2000, Bruges, Belgium, 2000: 573–588.

[3] 薛帅, 戚文峰. 模 2^n 加法最佳线性逼近研究[J]. 电子与信息学报, 2012, 34(9): 2156–2160.
Xue Shuai and Qi Wen-feng. Research on the best linear approximation of addition modulo 2^n[J]. *Journal of Electronics & Information Technology*, 2012, 34(9): 2156–2160.

[4] Courtois N and Meier W. Algebraic attacks on stream ciphers with linear feedback[C]. Advances in Cryptology-EUROCRYPT 2003, Warsaw, Poland, 2003: 346–359.

[5] Courtois N. Fast algebraic attacks on stream ciphers with linear feedback[C]. Advances in Cryptology-CRYPTO 2003, Santa Barbara, USA, 2003: 176–194.

[6] Dubrova E. Synthesis of binary machines[J]. *IEEE Transactions on Information Theory*, 2011, 57(10): 6890–6893.

[7] Dubrova E. A scalable method for constructing Galois NLFSRs with period 2^n–1 using cross-joint pairs[J]. *IEEE Transactions on Information Theory*, 2013, 59(1): 703–709.

[8] Hu Hong-gang and Gong Guang. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions[J]. *International Journal of Foundations of Computer Science*, 2011, 22(6): 1317–1329.

[9] Turan M S. On the nonlinearity of maximum-length NFSR feedbacks[J]. *Cryptography and Communications*, 2012, 4(3/4): 233–243.

[10] Chrisophe D C and Bart P. New Stream Cipher Designs: The eSTREAM Finalists[M]. Berlin: Springer, 2008: 244–266.

[11] Green D K and Dimond K R. Nonlinear product-feedback shift registers[J]. *Proceedings of the IEE*, 1970, 117(4): 681–686.

[12] Martin H, Thomas J, and Willi M. New Stream Cipher Designs: The eSTREAM Finalists[M]. Berlin: Springer, 2008: 179–190.

[13] Ma Zhen, Qi Wenfeng, and Tian Tian. On the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR[J]. *Journal of Complexity*, 2013, 29(2): 173–181.

[14] Golomb S W. Shift Register Sequences[M]. San Francisco: Aegean Park Press, 1967, Chapter VI.

王中孝： 男，1985 年生，博士生，研究方向为序列密码.

戚文峰： 男，1963 年生，教授，博士生导师，研究方向为密码学与信息安全.