σ-LFSR 序列极小多项式性质研究

曾 光 杨 阳 韩文报 范淑琴
(解放军信息工程大学 郑州 450002)

摘 要：σ-线性反馈移位寄存器(σ-LFSR)是基于字设计的，在安全性和效率上达到较好折衷的一种反馈移位寄存器。σ-LFSR 输出序列的特征多项式为有限域上的矩阵多项式。该文利用有限域上矩阵多项式环的代数结构，给出了σ-LFSR 输出序列极小多项式唯一的充分必要条件。

关键词：流密码；σ-线性反馈移位寄存器；极小多项式；矩阵多项式
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2010)03-0737-05
DOI:10.3724/SP.J.1146.2009.00061

On the Properties of the Minimal Polynomial of σ-LFSR Sequence

Zeng Guang Yang Yang Han Wen-bao Fan Shu-qin
(*Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: σ-Linear Feedback Shift Register (σ-LFSR) is a word-oriented feedback shift register, which has a better tradeoff between the security and efficiency. The sequence generated by σ-LFSR is called the σ-linear recurrence sequence and its characteristic polynomial is the matrix polynomial over finite field. With analysis of the algebra structure of the matrix polynomial ring over finite field, the sufficient and necessary condition for the minimal polynomial of σ-linear recurrence sequence to be unique is given.

Key words: Stream cipher; σ-LFSR; Minimal polynomial; Matrix polynomial

1 引言

分组密码和流密码是两类重要的对称密码算法。在过去的几十年内，分组密码标准化进程极大地促进了分组密码的发展，DES和AES的征集、评估以及最终确立的过程使得分组密码成为研究和应用最为广泛的对称密码算法。然而多数实际应用的流密码算法却都被发现存在安全性问题，例如欧洲移动通信系统GSM采用的密码算法由流密码算法A5/1变为了分组密码算法A5/3，第3代移动通信系统采用了Kasumi分组算法，无线网络(Wi-Fi)由IEEE802.11a/b中采用的流密码算法RC4变为IEEE802.11i中的AES，蓝牙标准流密码算法E_0也被成功攻击等等。由于任何分组密码算法都可以利用OFB和CTR模式构造流密码算法，因此密码学界产生了是否还需要流密码的质疑。著名密码学家Shamir在“Stream Cipher: Dead or Alive” [1]中指出，流密码在两个应用领域依然具有优势。一是资源极端受限的硬件领域，二是需要极高加解密速度的软件领域。因此，对于一个优秀的流密码算法，它要么具有高的软件实现效率要么具有低的硬件资源开销。

近年来，涌现了许多适合软件快速实现的流密码算法，例如ABC[2]，CryptMT3[3]，Sober[4]，Sosemanuk[5]等等。可以发现上述流密码的设计方式较以往有着明显的不同，基于字设计和与CPU特点密切结合是两个突出的特点。传统流密码的设计是基于比特的，而现代流密码的设计是以字(如32 bit或64 bit)为基本操作，这种变化不仅使CPU的基本字指令得以充分发挥，重要的是其输出不再是一个比特而是一个字，从而增加了算法的吞吐率。

随着人们对适合软件快速实现密码算法追求的日益强烈，基于字的设计方式渐渐被流密码设计者广泛采纳。驱动部件是流密码算法的重要组成部分，它为流密码算法提供长周期和具有良好伪随机性的源序列。面向软件实现的流密码通常利用基于字的驱动部件，构造基于字的且适合软件实现的驱动部件是流密码设计中的重要课题。多年来，密码学家提出了一系列基于字的流密码驱动部件。例如，基于字的 LFSR，基于字的 NLFSR，T-函数[6]，基于字的置换表，TSR[7]和 SFMT[8]等等。

结合现代计算机指令结构和平台化设计思想，针对通用 CPU 的特点，笔者在文献[9,10]中提出了一类适合软硬件高速实现、基于字的流密码驱动部

2009-01-16 收到，2009-10-09 改回
国家 863 计划项目(2009AA01Z417)，国家 973 计划项目(2007CB807902)，新世纪优秀人才计划项目(NCET-07-0384)和全国优秀博士学位论文作者专项基金(FANEDD-2007B74)资助课题
通信作者：曾光 sunshine_zeng@sina.com

件——σ-线性反馈移位寄存器(σ-LFSR)。它以字结构作为基本运算单元，利用少量计算机基本指令即可构造出具有较好密码学性质的最大周期序列，并且具有结构简单、实现快速的特点。σ-LFSR 是字 LFSR 的推广，Sober 和 Sosemanuk 等上述提到的流密码算法中的字 LFSR 都可以看成是σ-LFSR 的特例。

有限域上的多项式理论是研究有限域上经典 LFSR 的重要工具。熟知有限域上的一元多项式环是一个主理想整环，从而线性递归序列的极小多项式唯一。但是有限域上σ-线性递归序列的特征多项式不是有限域上的多项式，而是有限域上的矩阵多项式。本文通过分析有限域上矩阵多项式环的代数结构，指出了有限域上σ-线性递归序列的极小多项式一般不唯一，并给出了唯一的充要条件。

2 基础知识

σ-LFSR 是一基于字的 LFSR 模型，它的设计充分利用了现代 CPU 的特点。本节简单介绍它的概念，具体可参见文献[9,10]。

符号“σ”表示循环移位算子，循环移位具有良好的密码学性质，并且易于软硬件实现。σ-LFSR 设计的主要思想是在字 LFSR 中添加σ算子，并把它与域上乘法算子结合在一起进行处理。

设 m 为一个正整数，下文用 $\mathbb{F}_{2^m}$ 表示 2^m 元有限域。

定义 1 设 $\alpha_1,\alpha_2,\cdots,\alpha_m$ 是线性空间 $\mathbb{F}_{2^m}/\mathbb{F}_2$ 的一组基，设 $\beta=k_1\alpha_1+k_2\alpha_2+\cdots+k_{m-1}\alpha_{m-1}\in\mathbb{F}_{2^m}$，其中 $k_1, k_2,\cdots k_{m-1}\in\mathbb{F}_2$，则 $\mathbb{F}_{2^m}$ 上的循环移位算子σ如下：

$$\sigma(\beta)\triangleq k_{m-1}\alpha_1+k_1\alpha_2+\cdots+k_{m-2}\alpha_{m-1}$$

在具体实现时，σ 就是一个循环右移操作。如果选取 $\mathbb{F}_{2^m}$ 在 $\mathbb{F}_2$ 上的基为一组正规基时，则σ就是 $\mathbb{F}_{2^m}$ 上的 Frobenius 自同构，即 $\sigma(\beta)=\beta^2$。容易验证，σ 为 $\mathbb{F}_{2^m}/\mathbb{F}_2$ 上的一个线性变换。同时任给 $c\in\mathbb{F}_{2^m}$，c 可诱导出线性空间 $\mathbb{F}_{2^m}/\mathbb{F}_2$ 上的一个线性变换 C：$\mathbb{F}_{2^m}\to\mathbb{F}_{2^m}$ $C(\alpha)=c\alpha$，其中 $\alpha\in\mathbb{F}_{2^m}$。可以证明 $\mathbb{F}_{2^m}[\sigma]$ 为 $\mathbb{F}_{2^m}/\mathbb{F}_2$ 上的所有线性变换构成的集合[9,10]。

记 $\mathbb{F}_2$ 上 $m\times m$ 阶矩阵环为 $\boldsymbol{M}_m(\mathbb{F}_2)$，如给定 $\mathbb{F}_{2^m}$ 在 $\mathbb{F}_2$ 上的一组基，由文献[9,10]的结论有

$$\mathbb{F}_{2^m}[\sigma]\cong\boldsymbol{M}_m(\mathbb{F}_2) \tag{1}$$

定义 2 设 $c_0(\sigma),c_1(\sigma),\cdots,c_{n-1}(\sigma)\in\mathbb{F}_{2^m}[\sigma]$，若 $\mathbb{F}_{2^m}$ 上的序列 $\underline{s}=s_0,s_1,s_2,\cdots$ 满足递归关系

$$s_{i+n}=c_0(\sigma)s_i+c_1(\sigma)s_{i+1}+\cdots+c_{n-1}(\sigma)s_{i+n-1} \tag{2}$$

则称 $\underline{s}$ 为 $\mathbb{F}_{2^m}$ 上的 n 级σ-线性递归序列，并将该系统称为 n 级σ-线性反馈移位寄存器(σ-LFSR)，将多项式 $f(x)=x^n+c_{n-1}(\sigma)x^{n-1}+\cdots+c_1(\sigma)x+c_0(\sigma)$ 称为 n 次σ-多项式或者序列 $\underline{s}$ 的特征多项式。

由式(1)，σ-LFSR 可看作矩阵环 $\boldsymbol{M}_m(\mathbb{F}_2)$ 上的 LFSR，它是一种最广泛的线性变换寄存器模型。实际上 Twisted GFSR，TSR，MT 和 SFMT 都是σ-LFSR 的特例。在给定的 $\mathbb{F}_{2^m}$ 在 $\mathbb{F}_2$ 上的一组基下，$\mathbb{F}_{2^m}$ 中的元素与 m 维向量空间 $\mathbb{F}_2^m$ 同构，同时任意σ-多项式可转化为矩阵多项式，进一步它又可表示为如下的多项式矩阵形式。

$$\boldsymbol{F}(x)=\begin{pmatrix} f_{11}(x) & f_{12}(x) & \cdots & f_{1m}(x)\\ f_{21}(x) & f_{22}(x) & \cdots & f_{2m}(x)\\ \vdots & \vdots & \ddots & \vdots\\ f_{m1}(x) & f_{m2}(x) & \cdots & f_{mm}(x)\end{pmatrix}_{m\times m}$$

其中 $f_{ij}\in\mathbb{F}_2[x]$，$i,j=1,2,\cdots,m$。在此意义下，σ-LFSR 的定义可以改写如下：

定义 3 设 $C_0,C_1,\cdots,C_{n-1}\in\boldsymbol{M}_m(\mathbb{F}_2)$，若 $\mathbb{F}_{2^m}$ 上的序列 $\underline{s}=s_0,s_1,\cdots$ 满足递归关系

$$s_{i+n}=C_0s_i+C_1s_{i+1}+\cdots+C_{n-1}s_{i+n-1} \tag{3}$$

则将该系统称为 n 级σ-LFSR。

下文对σ-多项式和矩阵多项式不再区别，总把 $F(x)$ 记为σ-多项式 $f(x)$ 在给定基下对应的矩阵多项式。

3 主要结论

由定义 2 可知σ-线性递归序列的特征多项式不是有限域上多项式环 $\mathbb{F}_2[x]$ 中的多项式，而是 $\mathbb{F}_2$ 上的矩阵多项式，因此研究有限域上矩阵多项式环 $\boldsymbol{M}_m(\mathbb{F}_2)[x]$ 的代数结构至关重要。熟知 $\mathbb{F}_2[x]$ 是一个主理想整环，同时也是一个欧几里德环，存在对应的多项式欧几里德算法。对于 $\boldsymbol{M}_m(\mathbb{F}_2)[x]$，也存在单侧的欧几里德算法，那么很自然地考虑它是否为一个主理想环，对此有如下定理。

定理 1[11] 有限域上矩阵多项式环 $\boldsymbol{M}_m(\mathbb{F}_2)[x]$ 是一个单侧主理想环。

该定理为研究σ-线性递归序列的特征多项式奠定了基础，在给出唯一性定理之前首先给出一些定义。设 $V(\mathbb{F}_{2^m})$ 为 $\mathbb{F}_{2^m}$ 上无限序列的集合，在 $V(\mathbb{F}_{2^m})$ 上定义左移变换 L，即对任意的 $V(\mathbb{F}_{2^m})$ 中序列 $\underline{a}=a_0,a_1,a_2,\cdots$，定义 $L(\underline{a})=a_1,a_2,a_3,\cdots$。容易验证 L 是 $V(\mathbb{F}_{2^m})$ 上的一个线性变换。利用左移变换，式(2)可以写为

$$\begin{aligned}L^n\underline{a}&=c_0(\sigma)\underline{a}+c_1(\sigma)L\underline{a}+\cdots+c_{n-1}(\sigma)L^{n-1}\underline{a}\\&=\sum_{i=0}^{n-1}c_i(\sigma)L^i\underline{a}\end{aligned} \tag{4}$$

即 $\left(L^n+\sum_{i=0}^{n-1}c_i(\sigma)L^i\right)\underline{a}=0$，其中 L^0 是 $\mathbb{F}_{2^m}$ 上的单位变换。

定义 4　对 $\mathbb{F}_{2^m}$ 上的任意序列 $\underline{a}$，如存在多项式 $f(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$ 使得 $f(L)\underline{a}=\underline{0}$, 那么称 $f(x)$为序列 $\underline{a}$ 的零化多项式。如果序列 $\underline{a}$ 的零化多项式 $f(x)$首一，则称序列 $\underline{a}$ 为 $\mathbb{F}_{2^m}$ 上的σ-线性递归序列。

事实上，对任意$V(\mathbb{F}_{2^m})$中的周期序列，都存在一个首一零化多项式，因此它就是σ-线性递归序列。但是σ-线性递归序列的零化多项式不唯一，它们之间有如下联系。

引理 1　设 $\underline{a}$ 为 $\mathbb{F}_{2^m}$ 上的σ-线性递归序列，则存在唯一正次数非零矩阵多项式 $\boldsymbol{M}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$ 使得

(1)$\boldsymbol{M}(x)$是序列 $\underline{a}$ 的零化多项式，即 $\boldsymbol{M}(L)\underline{a}=0$；

(2)对任意 $\boldsymbol{F}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$，$F(L)\underline{a}=0$ 当且仅当 $\boldsymbol{M}(x)\,|_R\ \boldsymbol{F}(x)$，其中“$|_R$”表示右整除。

证明　构造零化矩阵多项式的集合如下：

$$Ann(\underline{a})=\{\boldsymbol{F}(x)\mid \boldsymbol{F}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]\ \text{且}\ F(L)\underline{a}=0\}$$

显然 $Ann(\underline{a})\subset \boldsymbol{M}_m(\mathbb{F}_2)[x]$，且 $Ann(\underline{a})$非零。如果 $\boldsymbol{F}(x)$, $\boldsymbol{G}(x)\in Ann(\underline{a})$，由于

$$[F(L)+G(L)]\ \underline{a}=F(L)\underline{a}+G(L)\underline{a}=0$$

那么有 $\boldsymbol{F}(x)+\boldsymbol{G}(x)\in Ann(\underline{a})$。另外，对于任意 $\boldsymbol{F}(x)\in Ann(\underline{a})$，$H(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$，因为

$$[H(x)\boldsymbol{F}(x)]\ \underline{a}=H(x)\boldsymbol{F}(x)\ \underline{a}=H(x)\ \underline{0}=\underline{0},$$

则有 $H(x)\boldsymbol{F}(x)\in Ann(\underline{a})$。这就证明了 $Ann(\underline{a})$是 $\boldsymbol{M}_m(\mathbb{F}_2)[x]$的一个非零左理想。由定理 1 知，存在 $Ann(\underline{a})$中的非零多项式 $\boldsymbol{M}(x)$使得 $Ann(\underline{a})=(\boldsymbol{M}(x))_l$，且 $\boldsymbol{M}(x)$是唯一确定的。这就证明了条件(1)成立，再根据左主理想环的性质可知条件(2)成立。　　证毕

注：需要指出的是引理 1 中的 $\boldsymbol{M}(x)$不一定是首一的。

定义 5　设 $\underline{a}$ 为 $\mathbb{F}_{2^m}$ 上σ-线性递归序列，将次数最低的首一零化矩阵多项式 $\boldsymbol{M}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$称为序列 $\underline{a}$ 的极小多项式，并记为 $M_{\underline{a}}(x)$。

由引理 1 的证明可知，σ-线性递归序列的极小多项式可能不唯一，下面给出一个特例。

例 1　设 $\mathbb{F}_4$ 的生成多项式为 $p(x)=x^2+x+1\in \mathbb{F}_2[x]$，$\alpha$ 为 $p(x)$在 $\mathbb{F}_4$ 中的一个根，则$\{1,\ \alpha\}$构成 $\mathbb{F}_4$ 在上 $\mathbb{F}_2$ 的一组基。设序列 $\underline{a}=\alpha,\alpha,0,\alpha,\alpha,0,\cdots$ 是一个周期为 3 的 $\mathbb{F}_4$ 上序列，将其表成向量序列为

$$\begin{array}{cccccccccc}1&1&0&1&1&0&1&1&0&\cdots\\0&0&0&0&0&0&0&0&0&\cdots\end{array}$$

设 $\mathbb{F}_2$ 上的矩阵多项式为如下形式

$$x^2+\begin{pmatrix}1&a\\0&b\end{pmatrix}x+\begin{pmatrix}1&c\\0&d\end{pmatrix}\tag{5}$$

其中 $a,\ b,\ c,\ d$ 为 $\mathbb{F}_2$ 中的元素。容易验证形如式(5)的矩阵多项式都是 $\underline{a}$ 的极小多项式，由此可见序列 $\underline{a}$ 的极小多项式不唯一。设 $\boldsymbol{F}_1(x)$和 $\boldsymbol{F}_2(x)$是如下的矩阵多项式：

$$\boldsymbol{F}_1(x)=\begin{pmatrix}1&0\\0&1\end{pmatrix}x^2+\begin{pmatrix}1&0\\0&0\end{pmatrix}x+\begin{pmatrix}1&0\\0&0\end{pmatrix}$$

$$\boldsymbol{F}_2(x)=\begin{pmatrix}1&0\\0&1\end{pmatrix}x^2+\begin{pmatrix}1&0\\0&1\end{pmatrix}x+\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

由引理 1 的证明过程可知，存在 $\boldsymbol{M}(x)\in M_2(\mathbb{F}_2)[x]$ 使得 $\boldsymbol{M}(x)$右整除 $\boldsymbol{F}_1(x)$和 $\boldsymbol{F}_2(x)$同时成立。事实上，容易验证有

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

即 $Ann(\underline{a})=(\boldsymbol{M}(x))_l$，进一步有

$$\boldsymbol{F}_1(x)=\left(\begin{pmatrix}0&0\\0&1\end{pmatrix}x^2+\begin{pmatrix}1&0\\0&0\end{pmatrix}\right)\boldsymbol{M}(x)$$

$$\boldsymbol{F}_2(x)=\left(\begin{pmatrix}0&0\\0&1\end{pmatrix}x^2+\begin{pmatrix}0&0\\0&1\end{pmatrix}x+\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)\boldsymbol{M}(x)$$

由例 1 可见，一般情形下，σ-线性递归序列的极小多项式不唯一。

定义 6　设 $\boldsymbol{I}_m$ 为 m 级单位矩阵，$\boldsymbol{F}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$，如存在 $\boldsymbol{G}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$，使得 $\boldsymbol{G}(x)\boldsymbol{F}(x)=\boldsymbol{F}(x)\boldsymbol{G}(x)=\boldsymbol{I}_m$，则称 $\boldsymbol{F}(x)$是可逆的。

引理 2　非零σ-线性递归序列 $\underline{a}$ 的零化多项式一定不是可逆多项式矩阵。

证明　设 $\boldsymbol{F}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$ 可逆且逆矩阵为 $\boldsymbol{G}(x)$，则有 $G(L)F(L)\underline{a}=\boldsymbol{I}_m\underline{a}=\underline{a}$。由 $G(L)F(L)\underline{a}=G(L)\underline{0}=\underline{0}$，可知 $\underline{a}$ 为零序列，与已知矛盾。证毕

定义 7　设 $\boldsymbol{F}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$ 且 $\deg(|\boldsymbol{F}(x)|)\geqslant 1$。若对于任给矩阵多项式 $\boldsymbol{P}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$ 和 $\boldsymbol{Q}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$，由 $\boldsymbol{F}(x)=\boldsymbol{P}(x)\boldsymbol{Q}(x)$可推出 $\boldsymbol{P}(x)$可逆或者 $\boldsymbol{Q}(x)$可逆，则称 $\boldsymbol{F}(x)$为不可约矩阵多项式。

引理3　设 $\boldsymbol{F}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$为首一不可约矩阵多项式。如果$\sigma$-线性递归序列 $\underline{a}$ 以 $\boldsymbol{F}(x)$为特征多项式，则序列 $\underline{a}$ 有唯一的极小多项式 $\boldsymbol{F}(x)$。

证明　设 $Ann(\underline{a})=(\boldsymbol{M}(x))_l$，于是存在 $\boldsymbol{G}(x)\in \boldsymbol{M}_m(\mathbb{F}_2)[x]$ 使得 $\boldsymbol{F}(x)=\boldsymbol{G}(x)\boldsymbol{M}(x)$。由 $\boldsymbol{F}(x)$不可约则有要么 $\boldsymbol{G}(x)$可逆，要么 $\boldsymbol{M}(x)$可逆。再有引理 2 知必有 $\boldsymbol{G}(x)$可逆。于是 $\boldsymbol{F}(x)$和 $\boldsymbol{M}(x)$互为右相伴，故 $Ann(\underline{a})=(\boldsymbol{F}(x))_l$，因此 $\boldsymbol{F}(x)$为序列 $\underline{a}$ 的唯一极

小多项式。 证毕

为了给出 σ -线性递归序列的极小多项式唯一的充分必要条件，需要介绍块 Hankel 矩阵。设 $\boldsymbol{X}_i\in\mathbb{F}_2^m$ 为列向量，定义块 Hankel 为

$$\boldsymbol{D}_n^{(r,s)}=\begin{pmatrix} X_n & X_{n+1} & \cdots & X_{n+s-2} & X_{n+s-1} \\ X_{n+1} & X_{n+2} & \cdots & X_{n+s-1} & X_{n+s} \\ \vdots & & \ddots & \vdots & \vdots \\ X_{n+r-1} & X_{n+r} & \cdots & \cdots & X_{n+r+s-2} \end{pmatrix}_{mr\times s} \tag{6}$$

有限域中的元素在给定一组基的条件下与向量空间同构，故可设 $\underline{a}=X_0,X_1,X_2,\cdots$ 是 σ -线性递归序列的向量表示，其中 $\boldsymbol{X}_i\in\mathbb{F}_2^m$ 为列向量，则对 $t\in\mathbb{N}$ 有

$$\boldsymbol{D}_t^{(n,n)}=\begin{pmatrix} X_t & X_{t+1} & \cdots & X_{t+n-2} & X_{t+n-1} \\ X_{t+1} & X_{t+2} & \cdots & X_{t+n-1} & X_{t+n} \\ \vdots & & \ddots & \vdots & \vdots \\ X_{t+n-1} & X_{t+n} & \cdots & \cdots & X_{t+2n-2} \end{pmatrix}_{mn\times n} \tag{7}$$

利用式(7)可知，矩阵多项式 $\boldsymbol{A}(x)=A_{n-1}x^{n-1}+\cdots+A_1x+A_0\in\boldsymbol{M}_m(\mathbb{F}_2)[x]$ 为序列 $\underline{a}$ 的零化多项式的充分必要条件是

$$(A_0,A_1,\cdots,A_{n-1})\boldsymbol{D}_t^{(n,n)}=(0,0,\cdots,0) \tag{8}$$

对 $t\in\mathbb{N}$ 成立。如果 $\underline{a}$ 是一个 n 阶 σ -线性递归序列，则式(8)等价于$(A_0,A_1,\cdots,A_{n-1})$是式(9)矩阵方程的一个解

$$(A_0,A_1,\cdots,A_{n-1})\boldsymbol{D}_0^{(n,n)}=(0,0,\cdots,0) \tag{9}$$

不仅如此，我们还有矩阵多项式

$$\boldsymbol{F}(x)=x^n+C_{n-1}x^{n-1}+\cdots+C_1x+C_0\in\boldsymbol{M}_m(\mathbb{F}_2)[x]$$

是序列 $\underline{a}$ 的特征多项式当且仅当$(C_0,C_1,\cdots,C_{n-1})$是式(10)矩阵多项式的一个解

$$(C_0,C_1,\cdots,C_{n-1})\boldsymbol{D}_0^{(n,n)}=(X_n,X_{n+1},\cdots,X_{2n-2}) \tag{10}$$

定理 2 设 $\boldsymbol{F}(x)=x^n+C_{n-1}x^{n-1}+\cdots+C_1x+C_0\in\boldsymbol{M}_m(\mathbb{F}_2)[x]$ 是一个首一矩阵多项式，$\underline{a}$ 是一个 n 阶 σ -线性递归序列，则下列条件等价：

(1)序列 $\underline{a}$ 以 $\boldsymbol{F}(x)$为唯一的极小多项式；

(2)$Ann(\underline{a})=(\boldsymbol{F}(x))_l$；

(3) $\boldsymbol{D}_0^{(n,n)}$ 的 mn 个行向量在 $\mathbb{F}_2$ 上线性无关且$(C_0,C_1,\cdots,C_{n-1})$是式(10)的一个解。

证明 采用(1)和(2)等价，(1)和(3)等价的证明方式。

(1)→(2) 反证法。如 $Ann(\underline{a})=(\boldsymbol{M}(x))_l$且 $\boldsymbol{M}(x)\neq\boldsymbol{F}(x)$，则存在 $\boldsymbol{G}(x\in\boldsymbol{M}_m(\mathbb{F}_2)[x]$使得 $\boldsymbol{F}(x)=\boldsymbol{G}(x)\cdot\boldsymbol{M}(x)$。令 $\deg(\boldsymbol{F}(x))=n$，断言在$(\boldsymbol{M}(x))_l$中一定存在一个次数$<n$ 的多项式。任取 $\boldsymbol{H}(x)\in(\boldsymbol{M}(x))_l$ 且 $\deg(\boldsymbol{H}(x))\geqslant n$，已知 $\boldsymbol{F}(x)$首一，由定理 1 可知存在 $\boldsymbol{Q}(x),\boldsymbol{R}(x)\in\boldsymbol{M}_m(\mathbb{F}_2)[x]$使得 $\boldsymbol{H}(x)=\boldsymbol{Q}(x)\boldsymbol{F}(x)+\boldsymbol{R}(x)$且 $\deg(\boldsymbol{R}(x))<\deg(\boldsymbol{F}(x))$。故设 $\boldsymbol{R}(x)\in(\boldsymbol{M}(x))_l$且满足 $\deg(\boldsymbol{R}(x))<n$，则 $\boldsymbol{F}(x)+\boldsymbol{R}(x)\in(\boldsymbol{M}(x))_l$。注意到 $\boldsymbol{F}(x)+\boldsymbol{R}(x)$也是一个首一的零化多项式，这与 $\boldsymbol{F}(x)$为唯一的极小多项式矛盾。

(2)→(1)利用左理想的定义即得。

(1)↔(3)序列 $\underline{a}$ 以 $\boldsymbol{F}(x)$为唯一的极小多项式，可知$(C_0,C_1,\cdots,C_{n-1})$是式(10)的一个解。同时由于极小多项式的唯一性，则式(10)有唯一解。将式(10)视为 m 个 mn 元线性方程构成的方程组，可看出这些方程组有唯一解的充分必要条件是 $\boldsymbol{D}_0^{(n,n)}$ 的 mn 个行向量在 $\mathbb{F}_2$ 上线性无关。反之，若$(C_0,C_1,\cdots,C_{n-1})$是式(10)的一个解，则有 $\boldsymbol{F}(x)$是序列 $\underline{a}$ 的特征多项式。同时 $\boldsymbol{D}_0^{(n,n)}$ 的 mn 个行向量在 $\mathbb{F}_2$ 上线性无关，说明式(10)只有一个解，因此 $\boldsymbol{F}(x)$为其唯一的极小多项式。

证毕

4 结束语

为了追求软件实现效率，采用字设计和与 CPU 特点密切结合的设计已成为近年来流密码设计的主流思想，其驱动部分的设计也是如此。密码学性质和效率是衡量流密码算法的优劣的标准，也更是衡量一个驱动部件好坏的根本标准。σ -LFSR 能够将软件实现效率和字 LFSR 的密码学性质两方面的优势相结合，利用少数 CPU 的快速指令(包括逻辑运算和小规模查表操作)即可容易地构造出密码学性质和效率兼顾的且达到最大周期的 σ -LFSR。本文通过分析有限域上矩阵多项式环的代数结构，给出了 σ -线性递归序列极小多项式唯一的充要条件。

参 考 文 献

[1] Shamir A. Stream cipher, dead or alive? Proc. Asiacrypt'04, Berlin: Springer-Verlag, 2004: 78.

[2] Anashin V, Bogdanov A, Kizhvatov I, and Kumar S. ABC-a new fast flexible stream cipher specification. version 3. http://www.ecrypt.eu.org/stream/, 2007-08-01.

[3] Matsumoto M, Saito M, and Nishimura T, *et al*.. CryptMT3 Stream Cipher. New Stream Cipher Designs, Berlin: Springer-Verlag, 2008: 7-19.

[4] Hawkes P and Rose G. Primitive specification and supportion documentation for SOBER-t16 submission to NESSIE. https://www.cosic.esat.kuleuven.be/nessie/, 2007-08-01.

[5] Berbain C, Billet O, and Canteaut A, *et al*.. Sosemanuk, a Fast Software-Oriented Stream Cipher. New Stream Cipher Designs, Berlin: Springer-Verlag, 2008: 98-118.

[6] Klimov A and Shamir A. Cryptographic applications of T-functions. Proc. SAC'03, Berlin: Springer-Verlag, 2004, 3006: 248-261.

[7] Tsaban B and Vishne U. Efficient linear feedback shift registers with maximal period. *Finite Fields and Their Applications*, 2002, 8(2): 256–267.

[8] Saito M and Matsumoto M. SIMD-oriented fast mersenne twister: A 128-bit pseudorandom number generator. Proc. Monte Carlo and Quasi-Monte Carlo Methods'06, Berlin: Springer-Verlag, 2008: 607–622.

[9] Zeng G, He K C, and Han W B. A trinomial type of σ-LFSR oriented toward software implementation. *Science in China Series F-Information Sciences*, 2007, 50(3): 359–372.

[10] Zeng G, Han W B, and He K C. High efficiency feedback shift register: σ -LFSR. Cryptology ePrint Archive, Report 2007/114. http://eprint.iacr.org/2007/114.pdf, 2007–08–01.

[11] Liang Z A and Ye Q K. The discussion on algebraic properties of polynomial matrices. *Applied Mathematics and Mechanics*, 1998, 19(10): 951–956.

曾　光：　男，1980 年生，讲师，研究方向为序列密码.

杨　阳：　女，1980 年生，讲师，研究方向为密码学及其应用.

韩文报：　男，1963 年生，教授，博士生导师，研究领域为信息安全.

范淑琴：　女，1978 年生，教授，硕士生导师，研究方向为密码算法分析.