

线性变换移位寄存器序列

王明生^{1,2}, 唐再良¹

(1. 绵阳师范学院信息安全研究所, 四川 绵阳 621006;
2. 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100089)

摘要: 线性变换移位寄存器由 Tsaban 和 Vishne 提出, 是一个面向字的移位寄存器, 每次输出一个字节。研究了由 TSR 所生成的序列的基本性质, 并且给出了一个新的准则来判定一个线性变换移位寄存器系统的特征多项式是否不可约。利用这个准则, 不需要在扩域上做运算来判定一个线性变换移位寄存器系统的特征多项式是否不可约。

关键词: 密码学; 不可约特征多项式; 线性反馈移位寄存器; 线性变换移位寄存器

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00051

Linear transformation shift register sequences

WANG Ming-sheng^{1,2}, TANG Zai-liang¹

(1. Institute of Information Security, Mianyang Normal University, Mianyang 621006, China;
2. The State Key Lab of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100089, China)

Abstract: Linear transformation shift registers (TSR) were introduced by Tsaban and Vishne, which was a word-oriented shift register output a word per step. Some basic properties of sequences generated by the TSR were presented, and a new criterion for deciding if the characteristic polynomial of a TSR system is irreducible was given. This criterion avoids operations in extension fields.

Key words: cryptography, irreducible characteristic polynomials, linear feedback shift register, linear transformation shift register

1 引言

有限域中的序列被广泛应用于密码学和数字通信。这样的序列常通过线性反馈移位寄存器 (LFSR, linear feedback shifted register) 生成^[1-3]。

在工程实践中, 一个 LFSR 一次输出一个比特使其运算速度缓慢。在 1994 年的快速软件加密会议上, Preneel 提出了一个问题, 这个问题要求设计面向字的 LFSR^[4]。在文献[5]中, Tsaban 和

Vishne 提出一个面向字可以产生最大周期序列的 LFSR 的集合族, 这个集合族被称为线性变换移位寄存器 (TSR, linear transformation shift registers)。本文给出了一个新的充分必要条件, 来判定 TSR 的特征多项式是否不可约, 这个条件避免在扩域上做运算。

首先, 介绍一下序列的基本知识。设 F_q 是一个有限域, 其中, q 是一个素数的幂, 设 n 是一个正整数, $a_0, \dots, a_{n-1}$ 是 F_q 中给定的元素。如果对

收稿日期: 2016-04-03; 修回日期: 2016-05-04。通信作者: 王明生, wangmingsheng@iie.ac.cn

基金项目: 国家重点基础研究发展计划 (“973” 计划) 基金资助项目 (No.2013CB834203); 国家自然科学基金资助项目 (No.61379142)

Foundation Items: The National Basic Research Program of China (973 Program) (No.2013CB834203), The National Natural Science Foundation of China (No.61379142)

所有的 $k=0,1,2,\dots$, F_q 中元素组成的序列 $s_0, s_1, \dots$, 满足关系式(1)

$$s_{k+n} = a_{n-1}s_{k+n-1} + a_{n-2}s_{k+n-2} + \dots + a_0s_k \quad (1)$$

则称 $s_0, s_1, \dots$, 为 F_q 的 n 阶线性齐次循环序列。多项式 $f(x) = x^n - a_{n-1}x^{n-1} - a_{n-2}x^{n-2} - \dots - a_0 \in F_q[x]$ 称为线性递归序列的特征多项式。线性递归序列由 LFSR 生成。

设 m 是一个正整数, 在传统的应用中 $F_q = F_2$, m 表示处理器字节的比特数, 即 8、16、32、64。用 F_2^m 中的向量表示 m bit, 并且向量 $(v_0, \dots, v_{n-1})$ 被存储在 n 个处理器字节中。文献[5]引入了线性变换移位寄存器的定义, 具体如下。

定义 1 设 T 是 F_q^m 中的线性变换, $S = \langle a_0, \dots, a_{n-1} \rangle \in F_q^n$ 。向量 $R = (v_0, \dots, v_{n-1}) \in M_{m \times n}(F_q)$ 的一个 TSR 步骤 (T, S) 是线性变换, 即 $\langle T, S \rangle(R) := (v_1, v_2, \dots, v_{n-1}, T(a_0v_0 + a_1v_1 + \dots + a_{n-1}v_{n-1}))$ (2)

则 $\langle T, S, R \rangle$ 系统称为一个 TSR。

当 T 是 F_q 中 $m \times m$ 的单位矩阵 I_m 时, TSR 系统是每一步输出一个字节的平凡 LFSR。

定义 2 设 $\{v_i\}_{i=0}^\infty$ 是 F_q^m 中的序列, 如果它可以由一个 TSR 系统生成, 则称它为一个 TSR 序列; 即存在 $T \in M_m(F_q)$ 和 $S = \langle a_0, \dots, a_{n-1} \rangle \in F_q^n$, 对所有的 $j = 0, 1, \dots$, 使

$$v_{j+n} = T(a_{n-1}v_{j+n-1} + \dots + a_1v_{j+1} + a_0v_j) \quad (3)$$

成立。当 $T = I_m$ 时, 称 $\{v_i\}$ 为 LFSR 序列。

文献[5]中关于 TSR 的一些基本结果如下。

命题 1 一个 TSR 步骤 $\langle T, S \rangle$ 的特征多项式是

$$f_{\langle T, S \rangle}(x) = f_S(x)^m \cdot f_T\left(\frac{x^n}{f_S(x)}\right) \quad (4)$$

其中, $f_S(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$, $f_T(x)$ 是矩阵 T 的特征多项式。

命题 2 设 F_{q^m} 是 $f_T(x)$ 的分裂域, α 是 $f_T(x)$ 在 F_{q^m} 中的根, 则 $f_{\langle T, S \rangle}(x)$ 在 F_q 中不可约, 当且仅当 $x^n - \alpha f_S(x)$ 在 F_{q^m} 中不可约。

寻找不可约特征多项式是寻找本原中最难的部分^[6,7]。

由命题 2 可知, 判定 $f_{\langle T, S \rangle}(x)$ 在 F_q 中是否可

约, 必须在 F_{q^m} 中检查 $x^n - \alpha f_S(x)$ 是否可约。因此, 这种方法的主要问题是需要在 F_q 的代数扩域中做运算。因此, 如果有一些合理的准则, 在判定 $f_{\langle T, S \rangle}(x)$ 在 F_q 中是否可约时, 可以避免在 F_q 的扩域中做运算, 这可能是有用的。

由于缺少适当的参考文献, 为了方便进一步研究, 在第 2 节和第 3 节证明了 TSR 序列的一些基本结果, 这些结果的推导过程和经典的 LFSR 序列类似。第 4 节给出了一个判断 TSR 系统的多项式是否不可约的新准则, 这个准则避免了在扩域上做运算。

2 TSR 序列的性质

首先, 本文符号定义如下。

令 F_q 表示含有 q 个元素的有限域, F_q^m 是 F_q 上 m 维向量空间, $F[x]^m$ 是多项式环 $F[x]$ 上秩为 m 的自由模, $F_q[[x]]^m$ 是形式幂级数环 $F_q[[x]]$ 上的秩为 m 的自由模。本文将 $F_q[x]^m$ 和 $F_q^m[x]$ 等同, $F_q[[x]]^m$ 和 $F_q^m[[x]]$ 等同。

对于 $h(x) = (h_1(x), \dots, h_m(x))' \in F_q[x]^m$, 定义 $\deg(h(x)) = \max_{i=1}^m(\deg h_i(x))$ 。

首先, 考虑 TSR 序列的生成函数。设 $\{v_i\}_{i=0}^\infty$ 是一个由 TSR 系统 $\langle T, S \rangle$ 生成的 F_q 上的 TSR 序列, 其中, $T \in M_m(F_q)$, 且 $S = \langle a_0, \dots, a_{n-1} \rangle \in F_q^n$ 。

设 $f_S(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1} \in F_q[x]$ 是一个与 $S = (a_0, \dots, a_{n-1}) \in F_q^n$ 相关的多项式, 且 $f_{\langle T, S \rangle}(x) = \det(x^n I_m - f_S(x)T)$ 是 TSR 步骤 $\langle T, S \rangle$ 的特征多项式, $f_{\langle T, S \rangle}(x)$ 的互反多项式定义为

$$\begin{aligned} f_{\langle T, S \rangle}^*(x) &= x^{mn} f_{\langle T, S \rangle}(x^{-1}) \\ &= \det(I_m - (a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x)T) \end{aligned} \quad (5)$$

令

$$A = I_m - (a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x)T \in M_m(F_q[x]) \quad (6)$$

$$G(x) = \sum_{i=0}^\infty v_i x^i \in F_q^m[[x]] \quad (7)$$

是序列 $\{v_i\}_{i=0}^\infty$ 的生成函数, 其中, $F_q^m[[x]]$ 和 $F_q[[x]]^m$ 等同, 则得到命题 3。

命题 3 设 A 和 $G(x)$ 定义如式(6)、式(7)所示, 则存在一个向量 $(g_0, \dots, g_{m-1})' \in F_q[x]^m$, 满足

条件 $\max(\deg g_i(x)) < n$, 且使等式(8)成立

$$AG(x) = (g_0, \dots, g_{m-1})^t \quad (8)$$

另一方面, 给定一个式(6)定义的 A , 对任意的元素 $g = (g_0, \dots, g_{m-1})^t \in F_q[x]^m$ 满足 $\deg(g) < n$, 存在唯一的 TSR 序列 $\{v_i\}_{i=0}^\infty$ 使等式(8)成立。

证明 注意等式

$$\begin{aligned} AG(x) &= \sum_{i=0}^{\infty} (v_i - (a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x) T v_i) x^i \\ &= \sum_{j=0}^{n-1} (v_j - \sum_{l=0}^j a_{l+n-j} T v_l) x^j + \sum_{j=n}^{\infty} (v_j - \sum_{l=j-n}^j a_{l+n-j} T v_l) x^j \end{aligned} \quad (9)$$

其中, 令 $a_n = 0$ 。

当 $\{v_j\}_{j=0}^\infty$ 是一个 TSR 序列时, 对任意的 $j \geq n$, $v_j = T(a_0 v_{j-n} + a_1 v_{j-n+1} + \dots + a_{n-1} v_{j-1})$ 。所以

$$AG(x) = \sum_{j=0}^{n-1} (v_j - \sum_{l=0}^j a_{l+n-j} T v_l) x^j \in F_q^m[x] = F_q[x]^m \quad (10)$$

令

$$(g_0, \dots, g_{m-1})^t = \sum_{j=0}^{n-1} (v_j - \sum_{l=0}^j a_{l+n-j} T v_l) x^j \quad (11)$$

则 $AG(x) = g(x)$, 且 $\deg(g) < n$ 。

另一方面, 给定 $g = (g_0, \dots, g_{m-1})^t \in F_q[x]^m$ 满足 $\deg(g) < n$, 则由形式幂级数 $G(x) = A^{-1}g$ 确定的序列 $\{u_i\}_{i=0}^\infty$ 一定满足 $\deg AG(x) < n$ 。因此, 通过式(9)可知, 对所有的 $j \geq n$, $u_j - \sum_{l=j-n}^j a_{l+n-j} T u_l = 0$ 成立, 即 $\{u_i\}_{i=0}^\infty$ 是一个 TSR 序列。

为了陈述下面的推论, 引入一个新的集合 B , 定义如下

$$B = \{g = (g_0, \dots, g_{m-1})^t \in F_q[x]^m \mid \deg g < n\} \quad (12)$$

推论 1 给定如定义 1 中的 T 和 S , 则 F_q 上所有 TSR 序列组成的集合和集合 B 之间存在一个双射。

推论 2 使用和命题 3 相同的符号。设 r 是 $\{v_j\}_{j=0}^\infty$ 在 F_q^m 中的最小正周期, 可以得到

$$f_{\langle T, S \rangle}^*(x) G'(x) = (1 - x^r) h(x) \quad (13)$$

其中, $h(x) \in F_q[x]^m$ 且 $\deg h(x) < mn$, $G'(x) = v_0 + v_1 x + \dots + v_{r-1} x^{r-1} \in F_q[x]^m$ 。

证明 由命题 3 可知, 存在一个 $g = (g_0, \dots, g_{m-1})^t$, 满足 $\deg(g) < n$, 且使 $AG(x) = (g_0, \dots, g_{m-1})^t$ 成立。故 $f_{\langle T, S \rangle}^*(x) G(x) = A^* AG(x) = A^*(g_0, \dots, g_{m-1})^t$,

其中, A^* 是 A 的伴随矩阵, 即 $A^* A = A A^* = f_{\langle T, S \rangle}^*(x) I_m$ 。

设 $A^*(g_0, \dots, g_{m-1}) = (h_0, \dots, h_{m-1})$, 由 A^* 定义可知, A^* 中每一个元素的度最多为 $n(m-1)$ 。因此, 每一个 $h_i(x)$ 的度最多为 $n(m-1) + n - 1 = nm - 1$ 。

因为 r 是 $\{v_i\}_{i=0}^\infty$ 的一个周期, 所以 $G(x) = \frac{G'(x)}{1 - x^r}$, 其中, $G'(x) = v_0 + v_1 x + \dots + v_{r-1} x^{r-1} \in F_q[x]^m$, 且 $F_q^m[x]$ 与 $F_q[x]^m$ 等同。因此, 推论 2 成立。

由推论 2 的证明过程可以得到推论 3。

推论 3 设 $v_0, v_1, \dots$ 是 F_q^m 中的 TSR 序列, $G(x) \in F_q[[x]]^m$ 是它的生成函数, 那么

$$G(x) = \frac{h(x)}{f_{\langle T, S \rangle}^*(x)} \quad (14)$$

其中, $h(x) \in F_q[x]^m$ 且 $\deg h(x) < mn$ 。

当 $T = I_m$ 时, 由推论 2 的证明过程可以得到推论 4。

推论 4 设 $v_0, v_1, \dots$ 是一个 F_q^m 上的 LFSR 序列, $G(x) \in F_q[[x]]^m$ 是它的生成函数, 那么

$$G(x) = \frac{h(x)}{f^*(x)} \quad (15)$$

其中, $f^*(x) = 1 - a_{n-1}x - \dots - a_0x^n$, $h(x) \in F_q[x]^m$ 且 $\deg h(x) < n$ 。

备注 推论 3 说明, 任何一个特征多项式为 $f_{\langle T, S \rangle}(x)$ 的 TSR 序列可以由一个特征多项式为 $f_{\langle T, S \rangle}(x)$ 的、长度为 mn 的 LFSR 通过每一步输出大小为 m 的字节生成。

3 TSR 序列的周期

在这一节中, 通过前面的结果来研究 TSR 的周期。

设 $\langle T, S \rangle$ 是一个 TSR 系统, $\{v_i\}_{i=0}^\infty$ 是一个 TSR 序列。设

$$[\langle T, S \rangle] = \begin{pmatrix} 0 & I & 0 & \dots & 0 \\ 0 & 0 & I & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & I \\ a_0 T & a_1 T & \dots & a_{n-2} T & a_{n-1} T \end{pmatrix} \quad (16)$$

$s_k = (v_k, v_{k+1}, \dots, v_{k+n-1})^t (k = 0, 1, \dots)$, 则 $s_{k+1} =$

$[\langle T, S \rangle]_{s_k} (k=0,1,\dots)$, 所以, $s_k = [\langle T, S \rangle]^k s_0$ 。

首先, 给出2个简单的引理。

引理1 设 $\{v_j\}_{j=0}^\infty$ 是定义1中的 $\langle T, S \rangle$ 系统生成的一个 TSR 序列, 其中, $a_0 \neq 0$ 且 $\det T \neq 0$, 那么该序列的最小正周期整除矩阵 $[\langle T, S \rangle]$ 在一般线性群 $GL(mn, F_q)$ 中的阶。

证明 由于 $\det[\langle T, S \rangle] \neq 0$, 所以 $[\langle T, S \rangle]$ 是 $GL(mn, F_q)$ 中的元素。设 l 是 $[\langle T, S \rangle]$ 的阶, 那么, 对所有的 $k=0,1,\dots$, $s_{k+l} = [\langle T, S \rangle]^{k+l} s_0 = [\langle T, S \rangle]^k s_0 = s_k$ 成立, l 是向量序列的一个周期, 因此, 序列的最小正周期是 l 的因子。

引理2 设 $f_{\langle T, S \rangle}(x)$ 是一个不可约多项式, 则 $\text{ord}(f_{\langle T, S \rangle})$ 和矩阵 $[\langle T, S \rangle]$ 在一般线性群 $GL(mn, F_q)$ 中的阶相等。

证明 因为 $f_{\langle T, S \rangle}(x)$ 是 $[\langle T, S \rangle]$ 的特征多项式且不可约, 所以, 它也是 $[\langle T, S \rangle]$ 的极小多项式。因此, $[\langle T, S \rangle]^e = I_{mn}$ 当且仅当 $f_{\langle T, S \rangle}(x) | (x^e - 1)$ 。由 $f_{\langle T, S \rangle}$ 和矩阵 $[\langle T, S \rangle]$ 各自阶的定义可得引理2成立。

由上面的讨论, 可以得到本文的主要结果。

定理1 设 $v_0, v_1, \dots$, 是最小正周期为 r 的 TSR 序列, 如果它的特征多项式 $f_{\langle T, S \rangle}(x)$ 是 $F_q[x]$ 中的不可约多项式, 那么, $f_{\langle T, S \rangle}(x)$ 的阶为 r 。

证明 由引理1和引理2可知, $r | \text{ord}(f_{\langle T, S \rangle}(x))$ 成立, 由推论2可得 $f_{\langle T, S \rangle}^*(x)G'(x) = (1-x^r)h(x)$ 。由于每个多项式 $h(x)$ 的度至多为 $mn-1$, 所以 $f_{\langle T, S \rangle}^*(x) | (1-x^r)$, 因此 $\text{ord}(f_{\langle T, S \rangle}^*(x)) \leq r$ 。又因为 $\text{ord}(f_{\langle T, S \rangle}(x)) = \text{ord}(f_{\langle T, S \rangle}^*(x))$, 所以 $\text{ord}(f_{\langle T, S \rangle}(x)) = r$ 。

备注 由定理1可知, 当特征多项式 $f_{\langle T, S \rangle}(x)$ 是 F_q 上的本原多项式时, 任意非零的 TSR 序列有一个周期是 $q^{mn}-1$ 。

4 $f_{\langle R, S \rangle}(x)$ 不可约的一个新准则

文献[5]提出了一个在 F_q 的扩域中检查 $f_{\langle T, S \rangle}(x)$ 不可约性的准则, 但是在域 F_q 中检查不可约多项式 $f_{\langle T, S \rangle}(x)$ 有时是比较方便的。本节提出一个新的准则, 通过这个准则在 F_q 上做运算就

可以检查 $f_{\langle T, S \rangle}(x)$ 是否可约。

和文献[5]一样, 考虑一般的情况: 设 $p(x), f(x), g(x) \in F_q[x]$, $Q(x) := g(x)^{\deg p(x)} p(\frac{f(x)}{g(x)}) \in F_q[x]$ 。

定义3^[5] 如果 $Q(x)$ 满足2个条件: 1) $f(x)$ 和 $g(x)$ 互素; 2) $p(x)$ 首一的不可约多项式, 则称 $Q(x)$ 是一个候选。

定理2 设 $Q(x)$ 是一个候选, $\deg p(x) = m$, $\deg f(x) = n > \deg g(x)$ 且 $f(0) = 0$, 那么 $Q(x)$ 是不可约的当且仅当 $Q(x)$ 没有重根, 且

$$f(y) + (-1)^n g(0)^{-1} g(y) N_{F_{q^{mn}}/F_{q^m}}(x) - \prod_{k=0}^{n-1} (y - x^{q^{mk}}) \in Q(x) F_q[x, y] \quad (17)$$

其中, $N_{F_{q^{mn}}/F_{q^m}}(x) = x x^{q^m} \cdots x^{q^{m(n-1)}}$ 。

证明

必要性。假设 $Q(x)$ 是不可约的, 则存在 $\xi \in F_{q^m}$ 和 $\theta \in F_{q^{mn}}$ 使

$$p(x) = \prod_{i=0}^{m-1} (x - \xi^{q^i}), \quad Q(x) = \prod_{i=0}^{mn-1} (x - \theta^{q^i}) \quad (18)$$

由于

$$\begin{aligned} Q(x) &= g(x)^m p\left(\frac{f(x)}{g(x)}\right) \\ &= g(x)^m \prod_{i=0}^{m-1} \left(\frac{f(x)}{g(x)} - \xi^{q^i}\right) \\ &= \prod_{i=0}^{m-1} (f(x) - g(x) \xi^{q^i}) \end{aligned} \quad (19)$$

因此, 对一些 i , $f(\theta) - g(\theta) \xi^{q^i} = 0$ 成立。

注意 θ 在 F_{q^m} 上的度为 n , 所以 $f(x) - g(x) \xi^{q^i}$ 是 θ 在 F_{q^m} 上的最小多项式。因此 $f(x) - g(x) \xi^{q^i} = \prod_{k=0}^{n-1} (x - \theta^{q^{mk}})$, 从而 $\xi^{q^i} = -(-1)^n g(0)^{-1} N_{F_{q^{mn}}/F_{q^m}}(\theta)$ 。

继而可得 $f(x) + g(x)(-1)^n g(0)^{-1} N_{F_{q^{mn}}/F_{q^m}}(\theta) = \prod_{k=0}^{n-1} (x - \theta^{q^{mk}})$, 即 $f(y) + g(y)(-1)^n g(0)^{-1} \cdot N_{F_{q^{mn}}/F_{q^m}}(\theta) - \prod_{k=0}^{n-1} (y - \theta^{q^{mk}}) = 0$ 。因此, $f(y) + g(y)(-1)^n g(0)^{-1} N_{F_{q^{mn}}/F_{q^m}}(x) - \prod_{k=0}^{n-1} (y - x^{q^{mk}}) \in F_q[x][y]$ 的系数属于 $F_q[y]$ 且 θ 是一个根。

因此, $f(y) + g(y)(-1)^n g(0)^{-1} N_{F_{q^{mn}}/F_{q^m}}(x) - \prod_{k=0}^{n-1} (y - x^{q^{mk}}) \in Q(x) F_q[x, y]$ 。

充分性。设 η 是 $Q(x)$ 在 F_{q^m} 中的一个根, 令 $b = (-1)^n g(0)^{-1} N_{F_{q^m}/F_{q^m}}(\eta)$, 则 $f(y) - bg(y) = \prod_{k=0}^{n-1} (y - \eta^{q^{mk}})$ 。所以, 对任意的 j

$$f(x) - b^{q^j} g(x) = \prod_{k=0}^{n-1} (x - b^{q^{j+mk}})$$

由 $f(\eta) - bg(\eta) = 0$, 以及 $f(x)$ 和 $g(x)$ 互素, 可得 $g(\eta) \neq 0$ 。因此, $b = \frac{f(\eta)}{g(\eta)}$ 。由 $Q(x)$ 的定义可知 b 是 $p(x)$ 的一个根, 又因为 $p(x)$ 是一个度为 m 的不可约多项式, 所以 $p(x) = \prod_{i=0}^{m-1} (x - b^{q^i})$ 。

因此

$$\begin{aligned} Q(x) &= g(x)^m \prod_{i=0}^{m-1} \left(\frac{f(x)}{g(x)} - b^{q^i} \right) \\ &= \prod_{i=0}^{m-1} (f(x) - g(x)b^{q^i}) \\ &= \prod_{i=0}^{m-1} \prod_{k=0}^{n-1} (x - \eta^{q^{i+mk}}) \\ &= \prod_{l=0}^{mn-1} (x - \eta^{q^l}) \end{aligned}$$

所以, $Q(x)$ 是 $F_q[x]$ 中一个不可约多项式的幂, 故当 $Q(x)$ 没有重根时, $Q(x)$ 是一个不可约多项式。

备注 当 $g(x)$ 中 x^{n-1} 的系数是 0 时, 定理 2 中的条件 “ $Q(x)$ 没有重根” 可以省略。

事实上, 只需要证明 $Q(x)$ 只有单根。

设 a_1 是 y^{n-1} 在 $f(y)$ 中的系数, a_2 是 y^{n-1} 在 $g(y)$ 中的系数。因为 $a_2 = 0$, $c(x) = a_1 + \sum_{i=0}^{n-1} x^{q^{mi}}$, 所以

$$Q(x) | c(x) = a_1 + (-1)^n g(0)^{-1} a_2 N_{F_{q^m}/F_{q^m}}(x) + \sum_{i=0}^{n-1} x^{q^{mi}}$$

由于 $c(x)^{q^m} - c(x) = (x^{q^{mn}} - x)$, 且 $F_{q^{mn}}$ 中所有的元素都是它的根。所以 $c(x)^{q^m} - c(x)$ 没有重根。因此, $Q(x)$ 只有单根。

由定理 2 可得推论 5。

推论 5 $f_{(T,S)}(x)$ 是 F_2 上的不可约多项式当且仅当

$$y^n + f_S(y) N_{F_{2^m}/F_{2^m}}(x) + \prod_{k=0}^{n-1} (y + x^{2^{mk}}) \in f_{(T,S)}(x) F_2[x, y]$$

且 $f_{(T,S)}(x)$ 没有重根。

推论 5 给出了检查 F_2 上的多项式 $f_{(T,S)}(x)$ 是

否不可约的另外一种准则, 这种准则不需要在 F_2 的扩域上进行运算。

5 结束语

传统的线性移位寄存器是流密码算法中的主要部件之一, 它每次产生一个新的比特。现代的硬件处理器以字节为单位, 因此, 有必要研究以字节为单元来移动的新型移位寄存器, 线性变换移位寄存器就是这样的一个模型。为了达到极大周期, 需要它的特征多项式是本原多项式。其中, 验证是否不可约是最花费计算量的部分, 本文给出了一种验证不可约的新方式。是否还有其他更为简单且同时能达到最大周期的移位寄存器模型是值得思考和研究的问题。另外, 在公开的文献中, 还没有基于 TSR 设计的流密码算法, 如何以此为基础部件, 设计新型的流密码算法也是值得进一步研究的问题。

参考文献:

- [1] BERLEKAMP E R. Algebraic coding theory—revised edition[M]. World Scientific Publishing Company, 2015.
- [2] GOLOMB S W. Shift register sequences[M]. Laguna Hills: Aegean Park Press, 1981.
- [3] LIDL R, NIEDERREITER H. Finite fields[M]. Cambridge: Cambridge University Press, 1983.
- [4] PRENEEL B. Fast software encryption[M]. Lecture Notes in Computer Science, Berlin: Springer, 1995: 1-5.
- [5] TSABAN B, VISHE U. Efficient linear feedback shift registers with maximal period[J]. Finite Fields Applications, 2002, 8(2): 256-267.
- [6] DEWAR M, PANARIO D. Linear transformation shift registers[J]. IEEE Transactions on Information Theory, 2003, 49(8):2047-2052.
- [7] DEWAR M, PANARIO D. Mutual irreducibility of certain polynomials[C]//The 7th International Conference on Finite Fields and Applications. c2003:59-68.

作者简介:



王明生 (1967-), 男, 四川射洪人, 博士, 中国科学院信息工程研究所研究员、博士生导师, 主要研究方向为密码学、隐私保护、信息安全的数学。

唐再良 (1958-), 男, 四川安岳人, 绵阳师范学院教授, 主要研究方向为符号计算与应用、信息安全。