LFSR 输出序列的特征向量表示法 [1]

王尚平 *** 王育民 *

*(西安电子科技大学 ISN 国家重点实验室 西安 710071)
**(西安理工大学 理学院 西安 710048)

摘 要 利用对线性反馈移位寄存器的输出序列的矩阵表示，通过对系数矩阵的特征向量分析，给出了输出结果的明确表达式，其中系数完全依赖于初始值及其极小多项式的互反多项式的根。该结果比以前的表达式更明确。

关键词 LFSR, 极小多项式, 流密码
中图号 TN918.1

1 引 言

在流密码系统中经常使用的密钥流生成器是所谓的非线性组合生成器 [1]。该生成器多由几个线性反馈移位寄存器 (LFSR) 和一个非线性组合函数组成，或由一个线性反馈移位寄存器和一个前馈逻辑组成。这些流密码的系统安全性分析都建立在对线性反馈移位寄存器的输出序列的精确表达式的基础上。LFSR 的输出的表达式已有深刻的结果 [1−5]，利用其极小多项式的根表示是这类结果的代表。但该表示式中对系数并未给出明确表达式。

本文利用反馈移位寄存器的矩阵表示，利用该矩阵的特征向量分析，给出了输出结果的明确表达式，其中系数完全依赖于初始值及其极小多项式的互反多项式的根。该结果比以前的表达式更明确，更有利于分析反馈移位寄存器的输出结果。

2 LFSR 输出序列的根表示法

LFSR 输出序列的根可表示如下 [1]:

引理 1 设 S^{∞} 是 GF(q) 上的周期序列，$f(x) \in \mathrm{GF}(q)[x]$ 是该序列的一个极小生成多项式. 设 $\alpha_1, \cdots, \alpha_n$ 是 $f(x)$ 的根，且重数分别为 $e_1, \cdots, e_m$. 以 GF(q^N) 表示 $f(x)$ 在 GF(q) 上的分裂域，则存在 $\beta_{ij} \in \mathrm{GF}(q^N)(i = 1, \cdots, m; j = 0, \cdots, e_i - 1)$，使对任意 n 有

$$s_n = \sum_{i=1}^{m} \sum_{j=0}^{e_i-1} (-1)^{j+1} \begin{bmatrix} n+j \\ j \end{bmatrix} \beta_{ij} \alpha_i^{-j-1-n} \tag{1}$$

引理 1 中 $f(x)$ 可能有重根，特别若假定 $f(x)$ 无重根，则有

引理 2 在引理 1 假设下，若进一步有 $f(x)$ 无重根，则

$$s_n = -\sum_{i=1}^{m} \beta_i \alpha_i^{-1-n} = -\sum_{i=1}^{m} \beta_i (\alpha_i^{-1})(\alpha_i^{-1})^n = -\sum_{i=1}^{m} \lambda_i (\alpha_i^{-1})^n \tag{2}$$

其中 $\lambda_i \doteq \beta_i \alpha_i^{-1}$，$\beta_i \in \mathrm{GF}(q^N)$.

[1] 2000-12-06 收到，2002-05-11 定稿
国家自然科学基金资助项目 (60073052)、陕西省教育厅自然科学研究计划资助项目 (00JK266)

3 LFSR 输出序列的特征向量表示法

设 LFSR 的极小多项式为

$$f(x)=1+c_1x+\cdots+c_mx^m\in \mathrm{GF}(q)[x] \tag{3}$$

以 $f(x)$ 为生成函数的 m 阶 LFSR 的输出序列记为 $S^{\infty}=(s_0,s_1,\cdots,s_n\cdots)$．下面用

$$\boldsymbol{S}_n=(s_n,s_{n+1},\cdots,s_{n+m-1}) \tag{4}$$

表示 LFSR 的第 n 个状态向量，则 $\boldsymbol{S}_{n+1}=(s_{n+1},s_{n+2},\cdots,s_{n+m-1},s_{n+m})$．其中

$$s_{n+m}=-(c_1s_{n+m-1}+\cdots+c_ms_n) \tag{5}$$

下面用

$$\boldsymbol{T}_f=\begin{bmatrix}0&0&0&\cdots&0&-c_m\\1&0&0&\cdots&0&-c_{m-1}\\0&1&0&\cdots&0&-c_{m-2}\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&\cdots&0&-c_2\\0&0&0&\cdots&1&-c_1\end{bmatrix} \tag{6}$$

表示 m 阶矩阵，则有

$$\boldsymbol{S}_{n+1}=\boldsymbol{S}_n\boldsymbol{T}_f=\boldsymbol{S}_{n-1}\boldsymbol{T}_f^2=\cdots=\boldsymbol{S}_0\boldsymbol{T}_f^{n+1} \tag{7}$$

由 (7) 式可知，LFSR 的第 n 个状态向量完全取决于初始状态向量 $\boldsymbol{S}_0$ 及 $\boldsymbol{T}_f^{n-1}$．故只要求得 $\boldsymbol{T}_f^{n-1}$ 的特征向量分解，即可获得 $\boldsymbol{S}_n$ 的精确表达式．下面先求 $\boldsymbol{T}_f$ 的特征向量分解．

定理 1　矩阵 $\boldsymbol{T}_f$ 的特征多项式为 $f(\lambda)$ 的互反多项式 $\tilde{f}(\lambda)=\lambda^m f(1/\lambda)$．

证明　$\boldsymbol{T}_f$ 的特征多项式为

$$\begin{aligned}|\lambda\boldsymbol{E}-\boldsymbol{T}_f|&=\begin{bmatrix}\lambda&0&0&\cdots&0&c_m\\-1&\lambda&0&\cdots&0&c_{m-1}\\0&-1&\lambda&\cdots&0&c_{m-2}\\\vdots&\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&0&\cdots&\lambda&c_2\\0&0&0&\cdots&-1&\lambda+c_1\end{bmatrix}\\&=\lambda^m+c_1\lambda^{m-1}+\cdots+c_{m-1}\lambda+c_m\\&=\lambda^m f(1/\lambda)\hat{=}\tilde{f}(\lambda)\end{aligned} \tag{8}$$

证毕

定理 2 设 $\gamma_1,\gamma_2,\cdots,\gamma_m$ 是 $f(x)$ 的根，则 $\alpha_i=\gamma_i^{-1}(i=1,\cdots,m)$ 是 $\boldsymbol{T}_f$ 的特征值，且特征根 α_i 对应的特征向量 $[x_{1,i},x_{2,i},\cdots,x_{m,i}]^T$ 为

$$\left.\begin{aligned}
x_{1,i}&=\alpha_i^{m-1}+c_1\alpha_i^{m-2}+\cdots+c_{m-2}\alpha_i+c_{m-1}\\
x_{2,i}&=\alpha_i^{m-2}+c_1\alpha_i^{m-3}+\cdots+c_{m-2}\\
&\vdots\\
x_{m-2,i}&=\alpha_i^2+c_1\alpha_i+c_2\\
x_{m-1,i}&=\alpha_i+c_1\\
x_{m,i}&=1
\end{aligned}\right\}\tag{9}$$

证明 由定理 1 显然 $\alpha_i(i=1,\cdots,m)$ 为 $\boldsymbol{T}_f$ 的特征根。设特征根 α_i 对应的特征向量为 $\boldsymbol{X}_i=[x_{1,i},x_{2,i},\cdots x_{m,i}]^T$，则有

$$(\alpha_i\boldsymbol{E}-\boldsymbol{T}_f)\boldsymbol{X}_i=0$$

其系数矩阵

$$\alpha_i\boldsymbol{E}-\boldsymbol{T}_f=\begin{bmatrix}
\alpha_i & 0 & 0 & \cdots & 0 & c_m\\
-1 & \alpha_i & 0 & \cdots & 0 & c_{m-1}\\
0 & -1 & \alpha_i & \cdots & 0 & c_{m-2}\\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\
0 & 0 & 0 & \cdots & \alpha_i & c_2\\
0 & 0 & 0 & \cdots & -1 & \alpha_i+c_1
\end{bmatrix}$$

$$\rightarrow\begin{bmatrix}
0 & 0 & 0 & \cdots & 0 & 0\\
-1 & 0 & 0 & \cdots & 0 & \alpha_i^{m-1}+c_1\alpha_i^{m-2}+\cdots c_{m-2}\alpha_i+c_{m-1}\\
0 & -1 & 0 & \cdots & 0 & \alpha_i^{m-2}+c_1\alpha_i^{m-3}+\cdots+c_{m-2}\\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\
0 & 0 & 0 & \cdots & 0 & \alpha_i^2+c_1\alpha_i+c_2\\
0 & 0 & 0 & \cdots & -1 & \alpha_i+c_1
\end{bmatrix}$$

故可解得特征向量 $\boldsymbol{X}_i$ 的分量

$$x_{t,i}=\sum_{k=0}^{m-t}c_k\alpha_i^{m-t-k},\qquad t=1,\cdots,m\tag{10}$$

其中 $c_0=1$，此即为 (9) 式。 证毕

利用定理 1 和定理 2 可求得 $\boldsymbol{T}_f$ 的特征值和特征向量。下面利用矩阵理论来求 $\boldsymbol{T}_f$ 的对角分解。

假设 LFSR 的生成函数 $f(x)$ 无重根，即 $\boldsymbol{T}_f$ 的特征值互异，则可知 $\boldsymbol{T}_f$ 的特征向量组 $\boldsymbol{X}_1,\cdots,\boldsymbol{X}_m$ 是线性无关的，且有

$$\boldsymbol{T}_f=\boldsymbol{P}\begin{bmatrix}
\alpha_1 & & & \\
& \alpha_2 & & \\
& & \ddots & \\
& & & \alpha_m
\end{bmatrix}\boldsymbol{P}^{-1}\tag{11}$$

其中

$$\boldsymbol{P}=[\boldsymbol{X}_1,\boldsymbol{X}_2,\cdots,\boldsymbol{X}_m]=(x_{t,i})_{m\times m} \tag{12}$$

其中 $x_{t,i}$ 如式 (10) 所示。

定理 3　假设 m 阶矩阵 $\boldsymbol{P}$ 如 (12) 式所示，则

$$(1)\ |\boldsymbol{P}|=\prod_{1\le i<j\le m}(\alpha_i-\alpha_j) \tag{13}$$

(2) $\boldsymbol{P}^{-1}\hat{=}(y_{ij})_{m\times m}$，其中

$$y_{i1}=\frac{(-1)^{m-i}}{\prod\limits_{\substack{s\ne i\\ 1\le s\le m}}(\alpha_s-\alpha_i)},\qquad i=1,\cdots,m \tag{14}$$

$$y_{ij}=y_{i1}\cdot\alpha_i^{j-1},\qquad j=1,\cdots,m \tag{15}$$

证明　(1) 求矩阵 $\boldsymbol{P}$ 的行列式 $|\boldsymbol{P}|$，并利用范德蒙行列式即可得结论。

(2) 因为 $\boldsymbol{P}^{-1}=\boldsymbol{P}^*/|\boldsymbol{P}|$，$|\boldsymbol{P}|$ 由式 (13) 给出，求 $\boldsymbol{P}$ 的伴随矩阵 $\boldsymbol{P}^*$ 可得结论。

证毕

利用 (11) 式，可知

$$\boldsymbol{T}_f^n=\boldsymbol{P}\begin{bmatrix}\alpha_1^n & & & \\ & \alpha_2^n & & \\ & & \ddots & \\ & & & \alpha_m^n\end{bmatrix}\boldsymbol{P}^{-1}$$

结合 (7) 式及定理 3

$$\begin{aligned}\boldsymbol{S}_n&=\boldsymbol{S}_0\boldsymbol{T}_f^n\\ &=\boldsymbol{S}_0[x_{ti}]_{m\times m}\cdot\begin{bmatrix}\alpha_1^n & & & \\ & \alpha_2^n & & \\ & & \ddots & \\ & & & \alpha_m^n\end{bmatrix}[y_{ij}]_{m\times m}\\ &=[s_0,s_1,\cdots,s_{m-1}]\cdot[x_{ti}]_{m\times m}\cdot[\alpha_i^n\cdot y_{ij}]_{m\times m}\\ &=[s_0,s_1,\cdots,s_{m-1}]\cdot\left[\sum_{i=1}^m x_{ti}\cdot\alpha_i^n\cdot y_{ij}\right]_{m\times m}\\ &=\left[\sum_{t=1}^m\sum_{i=1}^m s_{t-1}\cdot x_{ti}\cdot y_{ij}\cdot\alpha_i^n\right]_{1\times m}\\ &=\left[\sum_{i=1}^m\left(\sum_{t=1}^m s_{t-1}\cdot x_{ti}\cdot y_{ij}\right)\alpha_i^n\right]_{1\times m}\end{aligned} \tag{17}$$

又

$$\because\boldsymbol{S}_n=(s_n,\cdots,s_{n+m-1})$$

$$\therefore s_n=\sum_{i=1}^m\left(\sum_{t=1}^m s_{t-1}\cdot x_{ti}\cdot y_{i1}\right)\alpha_i^n \tag{18}$$

$$s_{n+j-1}=\sum_{i=1}^m\left(\sum_{t=1}^m s_{t-1}\cdot x_{ti}\cdot y_{ij}\right)\alpha_i^n,\qquad j=2,\cdots,m \tag{19}$$

又由 (18) 式可得

$$s_{n+j-1}=\sum_{i=1}^{m}\left(\sum_{t=1}^{m}s_{t-1}\cdot x_{ti}\cdot y_{i1}\right)\alpha_i^{n+j-1},\qquad j=2,\cdots,m \tag{20}$$

由 (19) 式及 (20) 式，又可得到 $y_{ij}=y_{i1}\cdot\alpha_i^{j-1}(j=2,\cdots,m)$，即 (15) 式. 上述结果，可总结为以下结论.

定理 4 假如 LFSR 输出序列 S^{∞} 的极小多项式 $f(x)$ 无重根，则该 LFSR 在 n 时刻的状态 $\boldsymbol{S}_n=[\sum_{i=1}^{m}(\sum_{t=1}^{m}s_{t-1}\cdot x_{ti}\cdot y_{ij})\alpha_i^n]_{1\times n}$，且输出为 $s_n=\sum_{i=1}^{m}(\sum_{t=1}^{m}s_{t-1}\cdot x_{ti}\cdot y_{i1})\alpha_i^n$，即 (18) 式. 其中 $[s_0,s_1,\cdots,s_{m-1}]$ 是 S^{∞} 的初始状态. 且有 $x_{t,i}=\sum_{k=0}^{m-t}c_k\alpha_i^{m-t-k},(t=1,\cdots,m;i=1,\cdots,m)$，即 (10) 式；$y_{i1}=\dfrac{(-1)^{m-i}}{\prod\limits_{\substack{j\neq i\\1\le j\le m}}(\alpha_j-\alpha_i)}$，$(i=1,\cdots,m)$，即 (14) 式；$y_{ij}=y_{i1}\cdot\alpha_i^{j-1}(j=1,\cdots,m)$，即 (15) 式.

定理 4 中假定了 $f(x)$ 无重根，假如 $f(x)$ 有重根，不妨设 $\gamma_1,\cdots,\gamma_l$ 是 $f(x)$ 的根，且重数分别为 $e_1,\cdots,e_l$，则 $f(x)$ 的互反多项式根为 $\alpha=\gamma_1^{-1},\cdots,\alpha=\gamma_l^{-1}$，且重数亦分别为 $e_1,\cdots,e_l$，则由矩阵理论：

$$\boldsymbol{T}_f=\boldsymbol{P}\begin{bmatrix}\boldsymbol{J}_1 & & & \\ & \boldsymbol{J}_2 & & \\ & & \ddots & \\ & & & \boldsymbol{J}_l\end{bmatrix}\boldsymbol{P}^{-1} \tag{21}$$

其中

$$\boldsymbol{J}_h=\begin{bmatrix}\alpha_h & 0 & 0 & \cdots & 0\\ 1 & \alpha_h & 0 & \cdots & 0\\ 0 & 1 & \alpha_h & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & \alpha_h\end{bmatrix}_{e_h\times e_h},\qquad h=1,\cdots,l \tag{22}$$

且

$$\boldsymbol{T}_f^n=\boldsymbol{P}\begin{bmatrix}\boldsymbol{J}_1^n & & & \\ & \boldsymbol{J}_2^n & & \\ & & \ddots & \\ & & & \boldsymbol{J}_l^n\end{bmatrix}\boldsymbol{P}^{-1} \tag{23}$$

其中

$$\boldsymbol{J}_h^n=\begin{bmatrix}\alpha_h^n & 0 & 0 & \cdots & 0\\ \binom{n}{1}\alpha_h^{n-1} & \alpha_h^n & 0 & \cdots & 0\\ \binom{n}{2}\alpha_h^{n-2} & \binom{n}{1}\alpha_h^{n-1} & \alpha_h^n & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ \binom{n}{e_h-1}\alpha_h^{n-e_h+1} & \binom{n}{e_h-2}\alpha_h^{n-e_h+2} & \binom{n}{e_h-3}\alpha_h^{n-e_h+3} & \cdots & \alpha_h^n\end{bmatrix}$$

$(h=1,\cdots,l)$ 由此可知

$$\begin{aligned}\boldsymbol{S}_n &= \boldsymbol{S}_0 T_f^n \\ &= [s_0, s_1, \cdots, s_{m-1}]\boldsymbol{P}_{m\times m}\begin{bmatrix}\boldsymbol{J}_1^n & & & \\ & \boldsymbol{J}_2^n & & \\ & & \ddots & \\ & & & \boldsymbol{J}_l^n\end{bmatrix}\boldsymbol{P}_{m\times m}^{-1}\end{aligned} \tag{24}$$

在此一般情况下，求 $\boldsymbol{P}_{m\times m}$ 及 $\boldsymbol{P}_{m\times m}^{-1}$ 则是表达式的关键所在。上述所得的结果与引理 1，2 的结论形式上是一致的。但引理 1，2 的结论表示式中对系数并未给出明确表达式。定理 4 利用反馈移位寄存器的矩阵表示，通过对系数矩阵的特征向量分析，给出了输出结果的明确表达式，其中系数完全依赖于初始值及其极小多项式的互反多项式的根。该结果比以前的表达式更明确。

4 小　结

采用矩阵的特征向量表示法，本文求出了当 LFSR 的生成函数无重根是其输出序列的精确表达式，该表示法较以前的 LFSR 输出序列的根表示法更明确。但是特征向量表示法在 LFSR 生成函数有重根时，其特征向量矩阵的逆矩阵计算则有待进一步研究。

参　考　文　献

[1] 丁存生，肖国镇，流密码学极其应用，北京，国防工业出版社，1994, 39–78.

[2] R. A. Rueppel, Analysis and Design of Stream Cipher[M], Berlin, Springer-Verlag, 1986, 33–67.

[3] R. A. Rueppel, O. J. Staffelbach, Product of linear recurring sequences with maximum complexity, IEEE Trans. on IT, 1987, 33(1), 121–134.

[4] M. J. B. Robshaw, On evaluating the linear complexity of a sequence of least period 2^n, Design Codes and Cryptography, 1994, 4, 263–269.

[5] 王育民，刘建伟. 通信网的安全——理论与技术，西安，西安电子科技大学出版社，1999, 230–281.

THE EIGENVECTOR REPRESENTATION OF LFSR'S OUTPUT SEQUENCE

Wang Shangping* **　　Wang Yumin*

*(*National Key Lab. on ISN, Xidian University, Xi'an* 710071, *China*)

**(*Xi'an University of Technology, Xi'an* 710048, *China*)

Abstract　By using coefficient matrix representation of LFSR's output sequences and analyzing the eigenvector representation of the coefficient matrix, the output sequences of LFSR is expressed, where the coefficients completely rely on the initial input values of the LFSR and the roots of the reciprocal polynomial of LFSR's minimum polynomial. The result is more explicit than the former result.

Key words　LFSR, Minimum polynomial, Stream ciphers

王尚平：　男，1963 年生，教授，博士生，密码学专业，研究方向为信息保密理论与电子商务的安全性.

王育民：　男，1936 年生，教授，博士生导师，长期从事信息论、信道编码、密码学以及通信网的安全性等方面的研究.