第 17 卷 第 2 期　　电 子 科 学 学 刊　　Vol. 17 No. 2
1995 年 3 月　　JOURNAL OF ELECTRONICS　　Mar. 1995

一类可控序列的构造和分析

冯登国　　肖国镇
（西安电子科技大学信息保密所　西安　710071）

摘要　本文通过利用 GF(2^m) ($m\geqslant 2$) 上 L 级 m 序列来控制其上的 L 级 m 序列的方法，构造出了一类具有较高线性复杂度的周期序列. 这类序列的线性复杂度的下界为 $L((L+1)^m-L^m)$.

关键词　线性复杂度，可控序列，反馈多项式

1 引　　言

在密码学中，线性复杂度是度量密钥流序列安全性能的重要指标. 只有具有较高线性复杂度的密钥流序列才能提供强的安全性. 构造具有较高线性复杂度的序列是十分重要的. 本文利用 GF(2^m)($m\geqslant 2$) 上 L 级 m 序列来控制其上的 L 级 m 序列，可得出一类具有较高线性复杂度的周期序列. 本文限制在有限域 GF(2^m) ($m\geqslant 2$) 上讨论.

2 一类可控序列的构造

2.1 序列的根表示定理

引理 1　设 GF(2^m) 上的周期序列 $\{a_i\}$ 无重根，$\{d_i\in\overline{GF(2^m)}\backslash\{0\}\mid i=1,2,\cdots,n\}$ 是序列 $\{a_i\}$ 的根集，其中 $\overline{GF(2^m)}$ 表示 GF(2^m) 的代数闭域，则存在 $\lambda_i\neq 0$，$\lambda_i\in\overline{GF(2^m)}$，$i=1,2,\cdots,n$，使得

$$a_j=\sum_{i=1}^{n}\lambda_i\alpha_i^{-j},\quad j=0,1,2,\cdots. \tag{1}$$

反之，若 $\lambda_i,\alpha_i\in\overline{GF(2^m)}\backslash\{0\}$，$i=1,2,\cdots,n$，则当 $i\neq j$ 时，$\alpha_i\neq\alpha_j$，且对所有 $j=0,1,2,\cdots,\sum_{i=1}^{n}\lambda_i\alpha_i^{-j}\in GF(2^m)$. 令 $a_j=\sum_{i=1}^{n}\lambda_i\alpha_i^{-j}$，则 $\{a_i\}$ 的根集恰是 $\{\alpha_i\mid i=1,2,\cdots,n\}$，从而 $\{a_i\}$ 以

$$f(x)=\prod_{i=1}^{n}(x-\alpha_i) \tag{2}$$

1993-09-03 收到，1994-05-06 定稿
冯登国　男，1965 年生，博士生，研究兴趣为编码学、密码学、信息论和应用数学.
肖国镇　男，1934 年生，教授，博士导师，主要从事密码与编码的研究工作.

为极小反馈多项式，其线性复杂度为 n。

引理 2　设 $\{a_i\}$ 是 GF(2^m) 上 L 级 m 序列，其极小反馈多项式为 $f(x)$，易知

$$f(x)=\prod_{i=1}^{L}(x-\alpha^{2^{(i-1)}m}), \tag{3}$$

其中 α 是 GF(2^{mL}) 的一个本原元。适当选取 $\{a_i\}$ 的初态可使它具有形式

$$a_i=\sum_{j=0}^{L-1}\alpha^{-2^{mj}\cdot i},\quad i=0,1,2,\cdots. \tag{4}$$

引理 1 和引理 2 的证明与文献[1—3]中有关结果的证明类似。

2.2　一类可控序列的构造

设 $\{a_i\}$ 是 GF(2^m) ($m\geqslant 2$) 上的一个 L 级 m 序列，设 β 是 $\{a_i\}$ 的极小反馈多项式 $f(x)$ 的一个根，则 $\{a_i\}$ 可表示为

$$a_j=\sum_{i=0}^{L-1}\lambda_i\beta^{-2^{mi}\cdot j},\ j=0,1,2,\cdots;\ \lambda_i\neq 0, i=0,1,\cdots,L-1. \tag{5}$$

令

$$b_j=\sum_{i=0}^{L-1}\beta^{-2^{mi}\cdot j},\quad j=0,1,2,\cdots. \tag{6}$$

集合 A 和 B 满足条件：$A\cup B=\{0,1,2,\cdots,2^m-2\}$，$A\cap B=\phi$。取 GF($2^m$) 的一个生成元 α，则对任意的 $a\in$ GF(2^m)，$a\neq 0$，一定存在唯一的 $t\in\{0,1,2,\cdots,2^m-2\}$ 使 $a=\alpha^t$。再取 $U\in\{1,2,\cdots,2^{mL}-2\}$。令

$$x_n=\begin{cases}a_n, & b_n=0;\\ a_n, & b_n=\alpha^t,\ t\in A;\\ a_{n+u}, & b_n=\alpha^t,\ t\in B.\end{cases} \tag{7}$$

$\{x_n\}$ 即是所构造的序列，是通过 $\{b_n\}$ 控制 $\{a_n\}$ 构造出来的。

3　可控序列的分析

由 $\{x_n\}$ 的构造易知，当集合 B 很小时，$\{x_n\}$ 更象 $\{a_n\}$，因而在选取 A,B 时，应使 B 大些。本节主要来讨论这类序列的线性复杂度和周期。

3.1　映射的多项式表示

引理 3　设 σ 是 GF(2^m) 到 GF(2^n) ($n\leqslant m$) 的任一映射，则 σ 可表示为

$$\sigma(x)=\sigma(0)+\sum_{i=1}^{2^m-1}c_ix^i,$$

其中 $c_i=\sum_{a\in GF(2^m)\setminus\{0\}}[\sigma(0)-\sigma(a)]a^{-i}$。

令 σ_i:GF(2^m)$\to$GF(2)，($i=1,2$) 如下

$$\begin{cases}\sigma_1(0)=1;\\ \sigma_1(a)=\begin{cases}1, & a=\alpha^t,\ t\in A;\\ 0, & a=\alpha^t,\ t\in B.\end{cases}\end{cases}\qquad\begin{cases}\sigma_2(0)=0\\ \sigma_2(a)=\begin{cases}0, & a=\alpha^t,\ t\in A;\\ 1, & a=\alpha^t,\ t\in B.\end{cases}\end{cases} \tag{9}$$

显然 $\sigma_2(a)=1+\sigma_1(a)$.

由引理 3 知,

$$\sigma_1(x)=\sigma_1(0)+\sum_{i=1}^{2^m-1}c_ix^i=1+\sum_{i=1}^{2^m-1}c_ix^i, \tag{10}$$

其中

$$\begin{aligned}c_{2^m-1}&=\sum_{a\in GF(2^m)\setminus\{0\}}[\sigma_1(0)-\sigma_1(a)]a^{-(2^m-1)}=\sum_{a\in GF(2^m)\setminus\{0\}}[\sigma_1(0)-\sigma_1(a)]\\&=\sigma_1(0)+\sum_{a\in GF(2^m)\setminus\{0\}}\sigma_1(a)=(1+|A|)(\mathrm{mod}2).\end{aligned} \tag{11}$$

当 $1\leqslant i\leqslant 2^m-2$ 时,

$$c_i=\sum_{a\in GF(2^m)\setminus\{0\}}[\sigma_1(0)-\sigma_1(a)]a^{-i}=1+\sum_{t\in A}(\alpha^{-i})^t. \tag{12}$$

因为对任意的 $a\in GF(2^m)$, 有 $\sigma_2(a)=1+\sigma_1(a)$, 所以 σ_2 的多项式表示为

$$\sigma_2(x)=\sum_{i=1}^{2^m-1}c_ix^i. \tag{13}$$

这样

$$x_n=a_n\sigma_1(b_n)+a_{n+v}\sigma_2(b_n). \tag{14}$$

显然 $x_n\in GF(2^m)$,

$$x_n=a_n+(a_n+a_{n+v})\sigma_2(b_n). \tag{15}$$

$$\begin{aligned}\sigma_2(b_n)&=\sum_{i=1}^{2^m-1}c_i\left(\sum_{j=0}^{L-1}\beta^{-2^mi\cdot n}\right)^i\\&=\sum_{i=1}^{2^{i_s}-1}c_i\left(\sum_{j=0}^{L-1}\beta^{-2^mi\cdot n\cdot 2^{i_0}}\right)\cdots\left(\sum_{j=0}^{L-1}\beta^{-2^mi\cdot n\cdot 2^{i_s}}\right)\\&=\sum_{i=1}^{2^{i_s}-1}c_i\sum_{i_0i_1\cdots i_s=0}^{L-1}\beta^{-n(2^mi_0+i_0+\cdots+2^mi_s+i_s)},\end{aligned} \tag{16}$$

其中 $i=2^{i_0}+2^{i_1}+\cdots+2^{i_s}$, 即 i 的二进制表示。

$$\begin{aligned}x_n&=\sum_{j=0}^{L-1}\lambda_j\beta^{-2^mj\cdot n}+\sum_{j=0}^{L-1}\lambda_j\beta^{-2^mj\cdot n}(1+\beta^{-2^mj\cdot v})\sigma_2(b_n)\\&=\sum_{j=0}^{L-1}\lambda_j\beta^{-2^mj\cdot n}+\sum_{i=1}^{2^{n_s}-1}\sum_{ii_0\cdots i_s=0}^{L-1}c_i\lambda_j(1+\beta^{-2^mj\cdot v})\beta^{-n(2^mj+2^mj_0+i_0+\cdots+2^mi_s+i_s)}.\end{aligned} \tag{17}$$

3.2 可控序列的周期和线性复杂度

令

$$T_1=\{\beta^{2^mj}\mid j=0,1,\cdots,L-1\}, \tag{18}$$

$$T_2=\{\beta^{2^mj+2^mj_0+i_0+\cdots+2^mi_s+i_s}\mid_{\substack{j,j_0,\cdots,j_s=0,1,\cdots,L-1\\ i=1,2,\cdots,2^m-1}}\}. \tag{19}$$

引理 4 (1) $T_1\subset T_2$; (2) T_2 中元素两两不同,且 $|T_2|=L((L+1)^m-1)$.

引理 4 的证明参见文献[4].

由(17)式 x_n 可写为

$$x_n=\sum_{j=0}^{L-1}\lambda_j\beta^{-2^mj\cdot n}+\sum_{j=0}^{L-1}c_{2^m-1}\lambda_j(1+\beta^{-2^mj\cdot v})\beta^{-n\cdot 2^m(j+t)}$$

$$+\sum_{i=1}^{2^m-2}\sum_{j_0\cdots j_s=0}^{L-1} c_i\lambda_j(1+\beta^{-2^{mj}\cdot\nu})\beta^{-n(2^{mj}+2^{mj_0}+i_0+\cdots+2^{mj_s}+i_s)}$$

$$+c_{2^m-1}\sum_{\substack{j i_0\cdots i_{m-1}=0\\ j,i_0,\cdots,i_{m-1}\text{不全相等}}}^{L-1}\lambda_j(1+\beta^{-2^{mj}\cdot\nu})\beta^{-n(2^{mj}+2^{mj_0}+2^{mj_1}+\cdots+2^{mj_{m-1}}+m-1)} \tag{20}$$

当$|A|$为奇数时，$(1+|A|)\bmod 2=0$，即 $c_{2^m-1}=0$。因此当选择A使 $\sum_{i\in A}(\alpha^{-i})^t\neq 1$ $(i\in\{1,2,\cdots,2^m-2\})$ 时，序列 $\{x_n\}$ 的线性复杂度为：$L((L+1)^m-1)+L-L^{m+1}=L((L+1)^m-L^m)$。

当$|A|$为偶数时，$(1+|A|)\bmod 2=1$，即 $c_{2^m-1}=1$。当选择A使 $\sum_{i\in A}(\alpha^{-i})^t\neq 1$ $(i\in\{1,2,\cdots,2^m-2\})$ 时，序列 $\{x_n\}$ 的线性复杂度至少为 $L((L+1)^m-1)-L=L((L+1)^m-2)$。如果还满足条件：

$$\left.\begin{aligned}
&\lambda_0+\lambda_{L-1}(1+\beta^{-2^{m(L-1)}\cdot\nu})\neq 0,\\
&\lambda_1+\lambda_0(1+\beta^{-\nu})\neq 0,\\
&\lambda_2+\lambda_1(1+\beta^{-2^m\cdot\nu})\neq 0,\\
&\quad\vdots\\
&\lambda_j+\lambda_{j-1}(1+\beta^{-2^{m(j-1)}\cdot\nu})\neq 0,\\
&\quad\vdots\\
&\lambda_{L-1}+\lambda_{L-2}(1+\beta^{-2^{m(L-1)}\cdot\nu})\neq 0,
\end{aligned}\right\} \tag{21}$$

则序列 $\{x_n\}$ 的线性复杂度为 $L((L+1)^m-1)$，周期为 $2^{mL}-1$。

注意：在上面的讨论中反复应用了引理 1。

综上所述，可得下述定理。

定理　若选择A使 $\sum_{i\in A}(\alpha^{-i})^t\neq 1$ $(i\in\{1,2,\cdots,2^m-2\})$，当$|A|$为奇数时，序列 $\{x_n\}$ 的线性复杂度为 $L((L+1)^m-L^m)$，周期为 $2^{mL}-1$。当$|A|$为偶数时，序列 $\{x_n\}$ 的线性复杂度至少为 $L((L+1)^m-2)$。如果还满足条件(21)式，则序列$\{x_n\}$的线性复杂度为 $L((L+1)^m-1)$，周期为 $2^{mL}-1$。

在实际应用中，一般选择的 A，使 $\sum_{i\in A}(\alpha^{-i})^t$ 容易计算。

4 结　束　语

本文构造出了一类具有较高线性复杂度的周期序列，不难验证文献[4]中构造出的两种序列是本文的特例。文中讨论的控制序列和被控序列的根相同，是否可以用任一个L级m序列去控制另一个任意L级m序列来获得具有较高线性复杂度的周期序列，这个问题还有待于进一步研究。

参　考　文　献

[1] 肖国镇，梁传甲，王育民，伪随机序列及其应用，北京：国防工业出版社，1985，第二章。
[2] 万哲先. 代数和编码. 北京：科学出版社，1980，第三章.

[3] Lennart Brynielsson, On the Linear Complexity of Combined Shift Register Sequences, Advances in Cryptology-EUROCRYPTO'85, Springer-verlag, 1985, 156—160.
[4] 孙登峰. 密码与信息,1991,(3): 1—18.

CONSTRUCTING AND ANALYSING A CLASS OF CONTROLLABLE SEQUENCES

Feng Dengguo Xiao Guozhen
(Institute of Information Security, Xidian University, Xi'an 710071)

Abstract Using m-sequence over the finite field GF(2^m) of degree L to controll m-sequence over GF(2^m) of degree L, a class of periodic sequences with large linear complexity is constructed. The lower bounds of the linear complexity of the sequences are $L((L+1)^m - L^m)$.

Key words Linear complexity, Controllable sequence, Feedback polynomial

国际神经网络与信号处理学术大会征文通知

由中国南京东南大学和加拿大蒙特利尔康科迪亚大学联合组织，中国电子学会电路与系统学会、IEEE 上海分会及 IEEE 蒙特利尔分会共同发起，IEEE 电路与系统学会和 IEEE 信号处理学会合办，国家科学技术委员会、国家教育委员会、国家自然科学基金委员会及香港王宽诚教育基金会赞助的 1995 年国际神经网络与信号处理学术大会将于 1995 年 12 月 10 日至 12 月 13 日在中国南京东南大学举行。

征文范围

- 人工神经网络理论
- 神经网络人工智能
- 联想记忆
- 神经计算机
- 神经系统优化
- 模式识别
- 语音识别
- 自适应共振理论
- 有监督和无监督学习
- 模糊神经系统
- 神经认知科学
- 系统辨识和谱估计
- 非线性滤波和信号处理
- 自适应信号处理
- 生物医学信号处理
- 雷达和声纳信号处理
- 振动信号处理
- 多维信号处理
- 数字图象处理和分析
- 视频信号处理
- 高清晰度电视中的信号处理
- 其它应用

截止日期： 1995 年 4 月 30 日前，请寄 2000 字详细摘要
录用通知： 1995 年 6 月 30 日前发出
印刷全文： 1995 年 8 月 30 日前寄来
稿件请寄： 210096 南京市东南大学无线电系邹采荣博士收