第 16 卷 第 2 期　　电子科学学刊　　Vol. 16, No. 2
1994 年 3 月　　JOURNAL OF ELECTRONICS　　Mar. 1994

GF(p^α) 上钟控序列*

李 超
(国防科技大学 7 系 长沙 410073)

摘要 本文利用有限域 GF(p^α) ($p>2$ 为素数，$\alpha \geqslant 1$ 为正整数) 上二次特征 η 建立了 GF(p^α) 上一类互钟控序列，即 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列. 讨论了当用作移位时钟控制的前馈函数 $g(x_1,x_2,\cdots x_n)$ 为二次型时，$\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列的周期和线性复杂度的特点.

关键词 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列，二次型，二次特征，周期，线性复杂度

1 引言

周期和线性复杂度是流密码体制的两类重要参数. 一般而言，周期和线性复杂度越大，流密码体制的安全性能越强. 钟控序列[1]相对于线性移存器序列和前馈序列而言，具有较大的周期和线性复杂度，从而倍受人们的重视[1-3]. 本文利用有限域 GF(p^α) ($p>2$ 为素数，$\alpha \geqslant 1$ 为正整数) 上二次特征 η，建立一类互钟控序列——$LSR_g[d_0,d_1,d_2]$-互钟控序列. 仿文献[2]用母函数方法，我们给出了这类互钟控序列的周期和线性复杂度上界. 证明了当 $g(x_1,x_2,\cdots,x_n)\in \mathrm{GF}(p^\alpha)[x_1,x_2,\cdots,x_n]$ 为二次型时，对任意正整数 d_0，d_1,d_2，$\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列均不能到达周期和线性复杂度上界，而当

$$g(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)+h(x_1,x_2,\cdots,x_n),$$

其中 $f(x_1,x_2,\cdots,x_n)$ 为 GF(p^α) 上退化二次型，$h(x_1,x_2,\cdots x_n)$ 为 GF(p^α) 上一次函数，并且 $h(0,0,\cdots,0)\neq 0$，则一定存在正整数 d_0,d_1,d_2，使得 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列到达周期和线性复杂度上界.

2 二次特征和 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列

为方便起见，令 $q=p^\alpha(p\geqslant 3.\ \alpha\geqslant 1)$，$\beta$ 为 GF(q) 上本原元，即 $\mathrm{GF}(q)=\{0,1,\beta,\beta^2\cdots,\beta^{q-2}\}$，用 $\underline{a},\underline{b},\cdots$ 表示 GF(q) 上 q 元序列，而 $p(\cdot),c(\cdot)$ 分别表示序列的周期和线性复杂度.

设 η 为 GF(q) 上二次特征，即当 α 为 $\mathrm{GF}^*(q)$ 中某个元素平方时，$\eta(\alpha)=1$，否则 $\eta(\alpha)=-1$. 我们规定 $\eta(0)=0$，易知 $\mathrm{GF}^*(q)$ 中恰好有 $(q-1)/2$ 个元素 α，使 $\eta(\alpha)=1$. 利用 η，我们建立钟控序列如下:

定义 1 设 $\underline{a}=a_0a_1a_2\cdots$ 和 $\underline{b}=b_0b_1b_2\cdots$ 分别为 q 元 n 级 m 序列，$p(\underline{a})=p(\underline{b})=q^n-1$，$d_0,d_1,d_2$ 为正整数，$d_i<q^n-1(i=0,1,2)$，$g(x_1,x_2,\cdots,x_n)\in\mathrm{GF}(p^\alpha)[x_1,x_2,\cdots,x_n]$，$\eta$ 为 GF(q) 上二次特征.

1992-11-09 收到，1993-09-28 定稿
* 国防科技大学校预研基金资助课题
李 超 男，1966 年生，硕士，讲师，现主要从事代数和密码学的教学和研究工作.

令 $u_0=a_0, u_t=a_{s(t)}, t\geqslant 1$,
其中

$$s(0)=0,\ s(t)=\begin{cases} s(t-1)+d_0, & \text{当 } \eta(g(b_{t-1},b_t,\cdots,b_{t+n-2}))=0; \\ s(t-1)+d_1, & \text{当 } \eta(g(b_{t-1},b_t,\cdots,b_{t+n-2}))=1; \\ s(t-1)+d_2, & \text{当 } \eta(g(b_{t-1},b_t,\cdots,b_{t+n-2}))=-1; \end{cases}$$

则称 q 元序列 $\underline{u}=u_0u_1u_2\cdots$ 为 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列.

例 1 设 $\underline{a}=\underline{b}=01021122,\ \cdots\cdots$ 为 GF (3) 上 2 级 m 序列, $g(x_1,x_2)=x_1^2$, $g'(x_1,x_2)=x_1^2+x_2+1$, 则 $\underline{b}$ 关于 $g(x_1,x_2)$ 和 $g'(x_1,x_2)$ 的前馈列分别为 $g(\underline{b})=01011111,\cdots,g'(\underline{b})=22000112,\cdots$,于是 $\mathrm{LSR}_g[1,2,3]$-互钟控序列 $\underline{u}=0121,2001,2210,1200,1120,0120,0212,0012,\cdots$, $p(\underline{u})=32$. $\mathrm{LSR}_{g'}[1,2,3]$-互钟控序列 $\underline{u}'=0222,0121,\cdots,p(\underline{u}')=8$,而 $\mathrm{LSR}_{g'}[3,1,2]$-互钟控序列 $\underline{u}''=0012,0122,1210,2220,0121,1201,2120,1010,1202,2102,1211,2021,2001,0211,2122,1112,\cdots,p(\underline{u})=64$.

3 周期特性

由于定义 1 中下标函数 $s(t)$ 满足 $s(kT_b+t)=ks(T_b)+s(t)$, 其中 $k\geqslant 0$, $T_b=p^n-1, 0\leqslant t<T_b$. 从而仿文献[2]用母函数方法易证如下引理.

引理 1 令 $S=s(T_b)=s(q^n-1)$, $S\not\equiv 0\ (\mathrm{mod}\, q^n-1)$, $f(x)$ 为 $\underline{a}$ 的本原生成多项式, α 为 $f(x)$ 在其分裂域中一个根, $f^{(S)}(x)$ 为 α^S 的极小多项式, 则有 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列 $\underline{u}$ 的极小多项式 $f_{\underline{u}}(x)\mid f^{(S)}(x^{T_b})$.

引理 2 $\mathrm{LSR}_g[d_0,\ d_1,\ d_2]$-互钟控序列周期和线性复杂度上界分别为 $(p^{\alpha n}-1)$ 和 $n\cdot(p^{\alpha n}-1)$.

引理 3 令 $S=s(T_b)=s(q^n-1)$, 则对于任意正整数 d_0, d_1, d_2 和任意前馈函数 $g(x_1,x_2,\cdots,x_n)$, $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列到达最大周期 $(p^{\alpha n}-1)^2$ 和最大线性复杂度 $n\cdot(p^{\alpha n}-1)$ 的充要条件为 $(S,q^n-1)=1$.

由引理 3, $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列能否到达最大周期和最大线性复杂度,关键在于 $S=s(T_b)$ 的值. 下面我们来分析 GF(q) 上二次型 $g(x_1,x_2,\cdots,x_n)$ 对应的 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列特点,主要结果如下:

定理 1 设 $g(x_1,x_2,\cdots,x_n)$ 为 GF(q) 上二次型,则对于任意正整数 d_0,d_1,d_2, $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列均不能到达周期和线性复杂度上界.

定理 2 设 $g(x_1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)+h(x_1,x_2,\cdots,x_n)$, 其中 $f(x_1,x_2,\cdots,x_n)$ 为退化二次型, 即 $f(x_1,x_2,\cdots,x_n)$ 等价于少于 n 个不定元的二次型, 而 $h(x_1,x_2,\cdots,x_n)$ 为一次函数,并且 $h(0,0,\cdots,0)\neq 0$, 则一定存在正整数 d_0,d_1,d_2, 使得 $\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列到达周期和线性复杂度上界.

为证明上述两定理,我们引进如下引理:

引理 4 设 f 为 GF(q) $(q=p^\alpha,\ p>2)$ 上非退化二次型, f 中不定元个数为 n, 则对任意 $b\in\mathrm{GF}(q)$, 方程 $f(x_1,x_2,\cdots,x_n)=b$ 在 $\mathrm{GF}^n(q)$ 中解数为

当 $2\mid n$ 时, $q^{n-1}+v(b)q^{(n-2)/2}\cdot\eta((-1)^{n/2}\Delta)$;

当 $2\nmid n$ 时, $q^{n-1}+q^{(n-1)/2}\cdot\eta((-1)^{(n-1)/2}b\Delta)$.

这里 η 为 GF(q) 上二次特征, $\Delta=\det(A_f)$, A_f 为 f 对应的对称矩阵.

$$v(b)=\begin{cases}q-1, & b=0;\\ -1, & \text{否则}\end{cases}$$

由引理 4 可以给出定理 1 证明如下：

(1) 当 $g(x_1,x_2,\cdots,x_n)$ 为非退化二次型时，如果 n 为偶数，则序列 $\underline{b}$ 关于 g 的前馈序列 $g(\underline{b})$ 中长 q^n-1 段内，0 的个数为 $q^{n-1}+(q-1)\cdot q^{(n-2)/2}-1$，$\beta^{2k}$ 和 β^{2k+1} $(k\geqslant 0)$ 的个数均为 $q^{n-1}-q^{(n-2)/2}$；或者 0 的个数为 $q^{n-1}-(q-1)\cdot q^{(n-2)/2}-1$；$\beta^{2k}$ 和 $\beta^{2k+1}(k\geqslant 0)$ 的个数为 $q^{n-1}+q^{(n-2)/2}$；于是

$S=s(T_b)=(q^{n-1}+(q-1)\cdot q^{(n-2)/2}-1)\cdot d_0+(q^{n-1}-q^{(n-2)/2})\cdot(q-1)/2\cdot d_1+(q^{n-1}-q^{(n-2)/2})\cdot(q-1)/2\cdot d_2$，或者

$S=s(T_b)=(q^{n-1}-(q-1)\cdot q^{(n-2)/2}-1)\cdot d_0+(q^{n-1}+q^{(n-2)/2})\cdot(q-1)/2\cdot d_1+(q^{n-1}+q^{(n-2)/2})\cdot(q-1)/2\cdot d_2$，即

当 $\eta((-1)^{n/2}\Delta)=1$ 时，$q^{n/2}-1|S$；当 $\eta((-1)^{n/2}\Delta)=-1$ 时，$q^{n/2}+1|S$． 总之 $(S,q^n-1)\neq 1$． 而当 n 为奇数时，同理可计算得：若 $\eta((-1)^{(n-1)/2}\cdot\Delta)=1$，则

$$S=s(T_b)=(q^{n-1}-1)d_0+(q^{n-1}+q^{(n-1)/2})\cdot(q-1)/2\cdot d_1+(q^{n-1}-q^{(n-1)/2})\cdot(q-1)/2\cdot d_2.$$

若 $\eta((-1)^{(n-1)/2}\cdot\Delta)=-1$，则

$$S=s(T_b)=(q^{n-1}-1)d_0+(q^{n-1}-q^{(n-1)/2})\cdot(q-1)/2\cdot d_1+(q^{n-1}+q^{(n-1)/2})\cdot(q-1)/2\cdot d_2.$$

由于 q 为奇数，并且 $q\geqslant 3$，故 $q-1|S$． 于是当 n 为奇数时，$(S,q^n-1)\neq 1$． 所以当 $g(x_1,x_2,\cdots,x_n)$ 为非退化二次型时，对任意正整数 d_0,d_1,d_2，$\mathrm{LSR}_g[d_0,d_1,d_2]$-互钟控序列不能到达周期和线性复杂度上界．

(2) 当 $g(x_1,x_2,\cdots x_n)$ 为退化二次型时，不妨设

$$g(x_1,x_2,\cdots,x_n)=a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2$$

$(k<n,a_i\neq 0,i=1,2,\cdots k)$（事实上，$g$ 经过非退化线性替换后可变为 $a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2$）．

如果 k 为偶数，则当 $\eta((-1)^{k/2}a_1a_2\cdots a_k)=1$ 时，

$S=[(q^{k-1}+(q-1)\cdot q^{(k-2)/2})\cdot q^{n-k}-1]\cdot d_0+(q^{k-1}-q^{(k-2)/2})\cdot q^{n-k}\cdot(q-1)/2\cdot d_1+(q^{k-1}-q^{(k-2)/2})\cdot q^{n-k}\cdot[(q-1)/2]\cdot d_2$.

当 $\eta((-1)^{k/2}a_1a_2\cdots a_k)=-1$ 时，

$S=[(q^{k-1}-(q-1)\cdot q^{(k-2)/2})\cdot q^{n-k}-1]\cdot d_0+(q^{k-1}+q^{(k-2)/2})\cdot q^{n-k}\cdot(q-1)/2\cdot d_1+(q^{k-1}+q^{(k-2)/2})\cdot q^{n-k}\cdot[(q-1)/2]\cdot d_2$ 易知 $q-1|S$.

如果 k 为奇数，同理可计算得 $q-1|S$.

故当 $g(x_1,x_2,\cdots,x_n)$ 为退化二次型时，结论也成立，从而定理 1 得证．

下面给出定理 2 的证明．不妨设 $f(x_1,x_2,\cdots,x_n)=a_1x_1^2+a_2x_2^2+\cdots+a_kx_k^2(k<n,\ a_i\neq 0)$，而 $h(x_1,x_2,\cdots,x_n)=b_1x_1+b_2x_2+\cdots+b_nx_n+b(b\neq 0$，而 b_i 不全为 0)．由于对任意 $c\in\mathrm{GF}(q)$．方程 $a_1x_1^2+\cdots+a_kx_k^2+b_1x_1+\cdots+b_nx_n+b=c$ 在 $\mathrm{GF}^n(q)$ 中解数为 q^{n-1}，于是 $\underline{b}$ 关于前馈函数 $g(x_1,x_2,\cdots,x_n)=f+h$ 的前馈序列中长 q^n-1 段内 0 的个数为 q^{n-1}． 又设前馈列中使得 $\eta(\alpha)=1$ 的 α 个数为 N_1，使

$\eta(\alpha) = -1$ 的 α 个数为 N_2，则对任意 $d < q^n - 1$，$(d, q^n - 1) = 1$ 方程 $q^{n-1} \cdot d_0 + N_1 \cdot d_1 + N_2 \cdot d_2 \equiv d(\bmod q^n - 1)$ 一定有正整数解 d_0, d_1, d_2。而对这组解，

$$S = s(T_b) \equiv d(\bmod q^n - 1).$$

故 $(S, q^n - 1) = 1$。故定理 2 成立。

参 考 文 献

[1] Beth T, Piper F C. The Stop-and-Go Generator. Advances in Cryptology-Proceeding of EUROCRYPT'84. Springer Lecture Notes in Computer Science, Vol. 209, 88—92.

[2] Smeets B. A Note on Sequences Generated by Clock Controlled Shift Register. EUROCRYPT'85. Spring-Verlag, 1986, 142—148.

[3] 李 超. LSR$_g$[d,k]-互钟控序列. 通信学报，1992，13(3): 71—73.

[4] Lidl R, Niederreiter H. Finite Field. London: Addsion-Wesley. Publishing Company, 1983. 282—283.

CLOCK CONTROLLED SEQUENCES OVER GF(p^a)

Li Chao

(National University of Defense Technology, Changsha 410073)

Abstract A class of clock-cross-controlled sequences over GF(p^α) ($p > 2$ is a prime number, $\alpha \geqslant 1$ is a positive number) using the quadratic character of GF(p^α), i.e., LSR$_g$[d_0, d_1, d_2]-clock-cross-controlled sequences is introduced. When the feed-forward function $g(x_1, x_2, \cdots, x_n)$, which is used as the controlling shift clock, is a quadratic form of GF(p^α), the properties of the period and the linear complexity of this sequences are discussed.

Key words LSR$_g$[d_0, d_1, d_2]-clock-cross-controlled sequences, Quadratic form, Quadratic character, Period, Linear complexity