国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第15卷第4期 1993年12月 Vol. 15 No. 4

GF(q)上多元多项式与钟控序列*

李 超

(系统工程与数学系)

摘 要 本文讨论了有限域GF(q)($q=p^a$, $p\geqslant 2$ 为素数, $a\geqslant 1$ 为正整数)上多元多项式与钟控序列的周期和线性复杂度的关系。当前馈函数 $g(x_1,x_2,\cdots,x_n)\in GF(q)[x_1,x_2,\cdots x_n]$ 为一次多项式时, 我们给出了钟控序列到达最大周期与线性复杂度的充要条件。

关键词 有限域, 钟控序列, 多项式, 周期, 线性复杂度

分类号 TN911.21

在文献[1]中作者讨论了有限域GF(2)上LSRg[d,k]——互钟控序列的周期特性, 给出了LSRg[d,k]——互钟控序列到达最大周期与线性复杂度的充要条件, 特别当 $g(x_1,x_2,\cdots,x_n)\in GF(2)[x_1,x_2,\cdots,x_n]$只依赖于两个变元 x_i 和 $x_j(i\neq j)$时, 仅当 $g(x_1,x_2,\cdots,x_n)=1+x_i+x_j+x_ix_j$ 或 $x_i+x_j+x_ix_j$, LSRg[d,k]——互钟控序列不能到达周期与线性复杂度的最大值. 本文将文献[1]中结果推广到有限域GF(q)上, 给出GF(q)上LSRg[d_0,d_1,d_2]——互钟控序列模型, 当前馈函数 $g(x_1,x_2,\cdots,x_n)\in GF(q)[x_1,x_2,\cdots,x_n]$为一次多项式时, 我们给出了一系列充要条件, 使得LSRg[d_0,d_1,d_2]——互钟控序列到达周期与线性复杂度的最大值。

1 LSRg[d_0,d_1,d_2]——互钟控序列

为方便起见, 我们令 β 为有限域GF(q)的本原元, 即 $GF(q)=\{0,1,\beta,\beta^2,\cdots,\beta^{q-2}\}$。构作乘法群 $GF^*(q)=GF(q)-\{0\}$到二元群 $G=\{1,-1\}$ (G的群运算为普通数的乘法)的同态 $\chi:\chi(\beta^{2k})=1$, 而 $\chi(\beta^{2k+1})=-1$, $k=0,1,2,\cdots,\left[\frac{q-2}{2}\right]$。我们规定 $\chi(0)=0$.

利用群同态 χ, 构造GF(q)上一类互钟控序列如下:

定义 1.1 设 $\underline{a}=a_0a_1a_2\cdots$和$\underline{b}=b_0b_1b_2\cdots$为GF($q$)上 n 级 m 序列, $T_a=T_b=q^n-1$, d_0, d_1, d_2 为正整数, $d_i<q^n-1(i=0,1,2)$, $g(x_1,x_2,\cdots,x_n)\in GF(q)[x_1,x_2,\cdots,x_n]$。

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

其中 $s(0)=0$

* 1992年11月12日收稿

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

则称 q 元序列$\underline{u}=u_0u_1u_2\cdots=a_{s(0)}a_{s(1)}a_{s(2)}\cdots$为 GF($q$)上 LSRg$[d_0,d_1,d_2]$——互钟控序列。

例 1.1 设$\underline{a}=\underline{b}=010\beta0,\ \beta^2 11\beta1,\ \beta^2\beta\beta\beta^2\beta^2\cdots\cdots$为 GF($2^2$)上 2 级 m 序列，其中 β 为 GF(2)本原多项式 $f(x)=x^2+x+1$ 的零点，$g(x_1,x_2)=x_1+x_2$，$[d_0,d_1,d_2]=[1,2,3]$，则 $\underline{b}$关于 $g(x_1,x_2)$的前馈列为 $g(\underline{b})=11\beta\beta\beta^2,\beta0\beta^2\beta^2\beta,1010\beta^2,\cdots$，于是 LSRg[1,2,3]——互钟控序列$\underline{u}$为：

$\underline{u}=0001\beta^2,\ \beta01\beta\beta^2,\ \beta\beta^2\beta\beta^2\beta^2,\ 1\beta\beta^2\beta\beta,\ \beta^2 1001,\ 1\beta\beta\beta^2 0,\ 0011\beta,\ \beta^2 0\beta\beta^2 1,\ \beta^2\beta\beta^2 01,$
$\beta\beta^2 1\beta^2\beta^2,\ 0\beta01\beta,\ \beta\beta^2\beta^2 10,\ 01\beta\beta\beta^2,\ 10\beta^2 11,,\ \beta\beta^2 00\beta,\ \beta^2 11\beta0,\ 0\beta^2 1\beta\beta^2,\ \beta^2 01\beta0,$
$1\beta\beta^2\beta^2 1,\beta111\beta,\beta^2 100\beta^2,11\beta\beta^2 0,01\beta\beta^2\beta,00\beta\beta^2 1,\beta\beta^2\beta0\beta,\beta^2\beta1\beta\beta^2,1\beta011,1\beta\beta^2 10,$
$11\beta^2\beta\beta^2,\ 00\beta^2 1\beta,\ \beta^2\beta\beta^2 0\beta^2,\ 1\beta^2\beta\beta^2 0,\ \beta\beta^2 1\beta1,\ \beta\beta^2 0\beta1,\ \beta\beta\beta\beta^2 1,\ 0111\beta^2,\ \beta\beta^2 101,$
$11\beta^2 00,\ \beta^2 1\beta\beta^2\beta,\ \beta^2 00\beta^2\beta,\ \beta^2\beta^2\beta^2 1\beta,\ 1\beta1\beta\beta,\ \beta^2 1\beta11,\ \beta\beta^2 000,\ 11\beta^2\beta\beta^2,\ \cdots$

这时$\underline{u}$的周期 $p(\underline{u})=225=15^2$，$\underline{u}$的线性复杂度 $c(\underline{u})=30$（复杂度可由 Massey 算法[5]求出）

由上例可以看出，LSRg$[d_0,d_1,d_2]$——互钟控序列的周期 $p(\underline{u})$实际上为原驱动序列 $\underline{a}$的周期平方，本文将证明如下结果。

定理 1.1 当 $q=2^\alpha(\alpha\geqslant1)$，$g(x_1,x_2,\cdots,x_n)$为 GF($2^\alpha$)$[x_1,x_2,\cdots,x_n]$中一次多项式，则 (1) 当 $\chi(g(0,0,\cdots,0))=0$ 时，LSRg$[d_0,d_1,d_2]$——互钟控序列周期与线性复杂度到达最大值的充要条件为$((1-2^\alpha)d_0+2^{\alpha-1}d_1,+(2^{\alpha-1}-1)d_2,2^{mn}-1)=1$. (2)当 $\chi(g(0,0,\cdots,0))=1$ 时，LSRg$[d_0,d_1,d_2]$——互钟控序列周期与线性复杂度到达最大值的充要条件为$((d_0-d_2)+2^{\alpha-1}(d_2-d_1),\ 2^{mn}-1)=1$ (3) 当 $\chi(g(0,0,\cdots,0))=-1$ 时，LSRg$[d_0,d_1,d_2]$——互钟控序列周期与线性复杂度到达最大值的充要条件为$((d_0-d_2)+2^{\alpha-1}(d_1-d_2),\ 2^{mn}-1)=1$.

定理 1.2 当 $q=p^\alpha(p>3$ 为素数，$\alpha\geqslant1$ 或 $p=3,\alpha>1)$，$g(x_1,x_2,\cdots,x_n)\in$GF(p^α)$[x_1,x_2,\cdots,x_n]$为一次多项式，则

(1)当 $\chi(g(0,0,\cdots,0))=0$ 时，对任意正整数 $d_0,d_1,d_2,d_i\leqslant q^n-2(i=0,1,2)$，LSRg$[d_0,d_1,d_2]$——互钟控序列既不能到达周期最大值，也不能到达线性复杂度最大值。

(2) 当 $\chi(g(0,0,\cdots,0))=1$ 时，LSRg$[d_0,d_1,d_2]$——互钟控序列到达周期与线性复杂度最大值的充要条件为：$(d_0-\frac{q+1}{2}d_1+\frac{q-1}{2}d_2,\ q^n-1)=1$.

(3) 当 $\chi(g(0,0,\cdots,0))=-1$ 时，LSRg$[d_0,d_1,d_2]$——互钟控序列到达周期与线性复杂度最大值的充要条件为：$\left(d_0+\frac{q-1}{2}d_1-\frac{q+1}{2}d_2,\ q^n-1\right)=1$.

定理 1.3 当 $q=3$ 时，$g(x_1,x_2,\cdots,x_n)$为 GF(3)上一次多项式，则当且仅当$(d_0+d_1+d_2,\ 3^n-1)=1$ 时，LSRg$[d_0,d_1,d_2]$——互钟控序列到达周期与线性复杂最大值。

2 结果的证明

我们令 $S=s(T_b)=s(q^m-1)$，其中 $s(t)$为定义 1.1 中下标函数，由 $s(t)$的定义易知，

对任意 $k\geqslant 0$，$0\leqslant t<T_b$，有 $s(kT_b+t)=kS+s(t)$于是仿文献[3]用母函数的方法可证如下引理：

引理 2.1 如果 $S\not\equiv 0(\bmod q^n-1)$，而 $f(x)$为$\underline{a}$的本原生成多项式，α^S 为 $f(x)$在其分裂域中一个根，$f^{(S)}(x)$表示 α^S 的极小多项式，则 LSRg$[d_0,d_1,d_2]$——互钟控序列的极小多项式 $f_{\underline{u}}(x)$满足：$f_{\underline{u}}(x)\mid f^{(S)}(x^{T_b})$。

引理 2.2 对任意多项式 $g(x_1,x_2,\cdots,x_n)$和正整数 d_0，d_1，d_2，LSRg$[d_0,d_1,d_2]$——互钟控序列周期与线性复杂度的最大值分别为$(q^n-1)^2$ 和 $n\cdot(q^n-1)$。

引理 2.3 LSRg$[d_0,d_1,d_2]$——互钟控序列到达周期与线性复杂度的最大值的充要条件为$(S,\ q^n-1)=1$.

证明 （充分性）

由于$(S,q^n-1)=1$. 所以 $f^{(S)}(x)$为 n 次本原多项式，由文献[4]中 Dickson 定理。

$f^{(S)}(x^{T_b})=f^{(S)}(x^{q^n-1})$为不可约多项式，而 $f_{\underline{u}}(x)\mid f^{(S)}(x^{T_b})$于是

$$f_{\underline{u}}(x)=1 \quad 或 \quad f_{\underline{u}}(x)=f^{(S)}(x^{T_b})$$

但 $\underline{u}^{(q^n-1)}=\underline{a}^{(S)}$不为全 0 序列，故 $f_{\underline{u}}(x)\neq 1$. 从而 $f_{\underline{u}}(x)=f^{(S)}(\chi^{T_b})$

则我们有：

$$p(\underline{u})=p(f_{\underline{u}}(x)=p(f^{(S)}(x^{T_b}))=(q^n-1)^2$$

$$c(\underline{u})=\deg(f_{\underline{u}}(x))=\deg(f^{(S)}(x^{T_b}))=n\cdot(q^n-1).$$

（必要性） 用反证法即可推出。

引理 2.4 设 $g(x_1,x_2,\cdots,x_n)=a_1x_1+a_2x_2+\cdots+a_nx_n$ $a_i\in GF(q)$不全为 0，则方程 $g(x_1,x_2,\cdots,x_n)=b$ 在 $GF^n(q)$中解数为 q^{n-1}. 这里 b 为 $GF(q)$中任意元。

证明 由于 a_i 不全为 0，不妨设 $a_1\neq 0$，则对于不定元 x_2，x_3，…，x_n 的任意取值，由方程 $a_1x_1+a_2x_2+\cdots+a_nx_n=b$ 可唯一决定 x_1 的取值，而$(x_2,x_3,\cdots,x_n)$共有 q^{n-1}中取法，故方程 $g(x_1,x_2,\cdots,x_n)=b$ 在 $GF^n(q)$中解数为 q^{n-1}.

由引理 2.3 可知，LSRg$[d_0,d_1,d_2]$——互钟控序列能否到达周期与线性复杂度最大值，取决于 $S=s(T_b)$，下面我们分析当 $g(x_1,x_2,\cdots,x_n)=a_1x_1+a_2x_2+\cdots+a_nx_n+a_{n+1}$，$(a_i\in GF(q)$，并且 a_i 不全为 0 $i=1,2,\cdots,n+1)$. S 的取值，分三种情况来讨论。

Casel. $q=2^a$ 的情形。

当 $q=2^a$ 时，$GF(2^a)$中满足 $\chi(a)=1$ 的元素 a 的个数为 2^{a-1}，而满足 $\chi(a)=-1$ 的元素个数为 $2^{a-1}-1$. 于是：

1°当 $\chi(g(0,0,\cdots,0))=0$，即 $g(0,0,\cdots,0)=0$ 时，序列$\underline{b}$关于 $g(x_1,x_2,\cdots,x_n)$的前馈序列中长 $q^n-1=2^{an}-1$ 段内，0 的个数为 $2^{a(n-1)}-1$. $\beta^{2k}(0\leqslant k\leqslant 2^{a-1}-1)$的个数为 $2^{a(n-1)}$. $\beta^{2k+1}(0\leqslant k\leqslant 2^{a-1}-2)$的个数为 $2^{a(n-1)}$. 从而

$$S=s(T_b)=(2^{a(n-1)}-1)d_0+2^{a(n-1)}\cdot\frac{2^a}{2}\cdot d_1$$

$$+2^{a(n-1)}\cdot\frac{2^a-2}{2}\cdot d_2=(2^{an}-1)d_0+2^{a(n-1)}\cdot$$

$$((1-2^a)d_0+2^{a-1}d_1+(2^{a-1}-1)d_2)$$

$(S,2^{an})=1$ 当且仅当$((1-2^a)d_0+2^{a-1}d_1+(2^{a-1}-1)d_2,2^{an}-1)=1$. 这就完成了定理 1.1

中(1)的证明。

2°当 $\chi(g(0,0,\cdots,0))=1$，即 $g(0,0,\cdots,0)=\beta^{2l}(l\in\{0,1,\cdots,2^{n-1}-1\})$，序列$\underline{b}$关于 $g(x_1,x_2,\cdots,x_n)$的前馈序列中长 $q^n-1=2^{\alpha n}-1$ 段内，0 的个数为 $2^{\alpha(n-1)}$，$\beta^{2k}(0\leqslant k\leqslant 2^{n-1}-1, k\neq l)$，的个数为 $2^{\alpha(n-1)}$，β^{2l}的个数为 $2^{\alpha(n-1)}-1$ 个，而 $\beta^{2k+1}(0\leqslant k\leqslant 2^{n-1}-2)$的个数为 $2^{\alpha(n-1)}$，

故
$$S=s(T_b)=2^{\alpha(n-1)}d_0+2^{\alpha(n-1)}\cdot\left(\frac{2^\alpha}{2}-1\right)\cdot d_1$$
$$+(2^{\alpha(n-1)}-1)d_1+2^{\alpha(n-1)}\cdot\frac{2^\alpha-2}{2}d_2$$
$$=(2^{\alpha n}-1)d_1+2^{\alpha(n-1)}((d_0-d_2)+2^{\alpha-1}(d_2-d_1))$$

于是$(S,2^{\alpha n}-1)=1$ 当且仅当
$$((d_0-d_2)+2^{\alpha-1}(d_2-d_1),\ 2^{\alpha n}-1)=1$$

这就完成了定理 1 中(2)的证明。

3°：类似 2°可证，这里从略。

至此，定理 1.1 得证。

Case2：$q=p^\alpha$（$P>3$ 为素数，$\alpha\geqslant 1$ 或 $p=3$，$\alpha>1$）情形。

当 $q=p^\alpha$ 时，GF(q)中满足 $\chi(a)=1$ 的元素 a 的个数等于满足 $\chi(a)=-1$ 的个数，均为$\frac{q-1}{2}$.

1°：当 $\chi(g(0,0,\cdots 0))=0$，即 $g(0,0,\cdots,0)=0$ 时序列$\underline{b}$关于 $g(x_1,x_2,\cdots,x_n)$的前馈序列中 0 的个数为 $q^{n-1}-1$，而 β^{2k}和 $\beta^{2k+1}\left(0\leqslant k\leqslant\frac{q-2}{2}\right)$的个数均为 q^{n-1}. 于是
$$S=s(T_b)=(q^{n-1}-1)d_0+q^{n-1}\cdot\frac{q-1}{2}\cdot d_1+q^{n-1}\cdot\frac{q-1}{2}\cdot d_2$$

因 $q=p^\alpha$ $(q>3)$。则$\frac{q-1}{2}>1$. $(S,\ q^n-1)$ 有大于 1 的因子$\frac{q-1}{2}$. 于是，LSRg$[d_0,d_1,d_2]$——互钟控序列一定不能到达周期与线性复杂度最大值，即定理 2.2 中(1)成立。

2°：当 $\chi(g(0,0,\cdots,0))=1$，即存在 $l\left(0\leqslant l\leqslant\frac{q-2}{2}\right)$使得 $g(0,0,\cdots,0)=\beta^{2l}$时，序列$\underline{b}$关于 $g(x_1,x_2,\cdots,x_n)$的前馈列中 0 的个数为 q^{n-1}，$\beta^{2k}\left(0\leqslant k\leqslant\frac{q-2}{2},\ k\neq l\right)$的个数为 q^{n-1}，β^{2l}的个数为 $q^{n-1}-1$. 而 $\beta^{2k+1}\left(0\leqslant k\leqslant\frac{q-2}{2}\right)$的个数为 q^{n-1}.

故
$$S=s(T_b)=q^{n-1}\cdot d_0+q^{n-1}\left(\frac{q-1}{2}-1\right)d_1+(q^{n-1}-1)d_1$$
$$+q^{n-1}\left(\frac{q-1}{2}\right)d_2=(q^n-1)d_1+q^{n-1}\left(d_0-\frac{q+1}{2}d_1+\frac{q-1}{2}d_2\right)$$

则$(S,\ q^n-1)=1$ 当且仅当$\left(d_0-\frac{q+1}{2}d_1+\frac{q-1}{2}d_2,\ q^n-1\right)=1$. 即定理 2.2 中(2)成立。

3°：当 $\chi(g(0,0,\cdots,0))=-1$ 时，类似可计算
$$S=(q^n-1)d_2+q^{n-1}\left(d_0+\frac{q-1}{2}d_1-\frac{q+1}{2}d_2\right)$$

于是$(S,\ q^n-1)=1$ 当且仅当

$$\left(d_0+\frac{q-1}{2}d_1-\frac{q+1}{2}d_2,\quad q^n-1\right)=1$$

至此定理 2.2 得证。

Case3：$q=3$ 的情形。

当 $q=3$ 时，$GF(q)=\{0,1,2\}$. 而且 $\chi(0)=0$，$\chi(1)=1$，$\chi(2)=-1$.

对 GF(3)上任意一次多项式 $g(x_1,x_2,\cdots,x_n)$，当 $\chi(g(0,0,\cdots,0))$分别为 0，1，-1 时，S 的取值分别为：$(q^{n-1}-1)d_0+q^{n-1}d_1+q^{n-1}d_2$，$q^{n-1}d_0+(q^{n-1}-1)d_1+q^{n-1}d_2$，$q^{n-1}d_0+q^{n-1}d_1+(q^{n-1}-1)d_2$. 这时$(S,q^n-1)=1$ 当且仅当$(d_0+d_1+d_2,q^n-1)=1$. 于是定理 1.3 得证。

3 结 语

本文在一般有限域 GF(q)上，讨论了当前馈函数 $q(x_1,x_2,\cdots,x_n)$为一次多项式时，LSRg$[d_0,d_1,d_2]$——互钟控序列到达周期与线性复杂度最大值的充要条件，当 $g(x_1,x_2,\cdots,x_n)$为二次多项式时，利用 GF(q)上二次型理论同样可分析相应互钟控序列的特性，这些结果有待发表。

参 考 文 献

1 李超. LSRg$[d,k]$——互钟控序列. 通信学报，1992，(5)

2 李超. 关于钟控序列的一点注记. 通信保密，1992，(3)

3 B Smeets. A Note on Sequences Generatrd by Clock Controlled Shift Registers. Eurocrypt' 85，142－148

4 R Lidl and H Niederreiter. Finite Field. Addsion Wesley Publishing Company，1983

Polynomial in Several Elements and Clock Controlled Sequences over GF(q)

Li Chao

(Department of System Engineering and Mathematics)

Abstract

In this paper, the relation among the polynomial in several elements and the period and linear complexity of the clock controlled sequences over the finite field GF(q)($q=p^\alpha$, $p\geqslant 2$ is a prime number, $\alpha\geqslant 1$ is a positive integer number)is discussed. When the n-pry polynomial $g(x_1,x_2,\cdots,x_n)\in GF(q)[x_1,x_2,\cdots,x_n]$is a polynomial of degree 1, we give the necessary and sufficient condition that the clock controlled sequences get to the maximum period and the maximum linear complexity.

Key words polynomial, period, finite field, clock controlled sequences, linear complexity.