国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第15卷第2期 1993年6月 Vol. 15 No. 2

$GF(q)$上的$[d,k]$——自控序列*

李 超

(系统工程与应用数学系)

摘 要 本文将R. A. Rueppel文[1]中$GF(2)$上的$[d,k]$——自控序列模型推广到一般有限域$GF(q)$上。讨论了$GF(q)$上任意n级M序列或n级收缩M序列的$[d,k]$——自控序列的平移等价性和周期特点。

关键词 $[d,k]$——自控序列，平移等价，保留型，删去型

分类号 TN918.3，O157.4

在1987年欧洲密码会议上，Rueppel[1]首次提出自钟控概念，建立了如下所示$GF(2)$上$[d,k]$——自控序列模型：设d和k是互素的正整数，二元序列$\underline{a}=a_0a_1a_2\cdots(a_i\in GF(2))$的$[d,k]$——自控序列是指二元序列$\underline{u}=u_0u_1u_2\cdots$ 其中$u_0=a_0$ $u_i=a_{f(i)}$ $(i=1,2,\cdots)$ 这里

$$f(0)=0\quad,\qquad f(i)=\begin{cases}f(i-1)+d & ,\quad \text{当 } a_{f(i-1)}=0\\ f(i-1)+k & ,\quad \text{当 } a_{f(i-1)}=1\end{cases}$$

在文[1]中，Rueppel证明了当$\underline{a}$为n级m序列时，$\underline{a}$的$[1,2]$——自控序列的周期为$[\frac{2}{3}(2^n-1)]$，一个周期内含"1"的个数为$[\frac{1}{3}(2^n-1)]$，在文[2]中，Rueppel和Lai Xuejia用图论方法给出了$GF(2)$上一般$[d,k]$——自控序列周期上界为$[\frac{3}{4}(2^n-1)]$。本文将Rueppel的$GF(2)$上$[d,k]$——自控序列模型推广到$GF(q)$上，建立$GF(q)$上$[d,k]$——自控序列的概念，讨论了这类自控序列平移等价特性和周期特点，证明了当

$$n\geqslant M=\begin{cases}k & \text{当 } d=1,\ \underline{a}\text{为}n\text{级收缩}M\text{序列}\\ dk-2\min\{d,k\}+1. & \text{否则}\end{cases}$$

时，对任意n级M序列或n级收缩M序列$\underline{a}$，$\underline{a}$的所有平移等价的序列所产生的$[d,k]$——自控序列均彼此平移等价，从而它们具有相同的周期，此时周期上界为$\frac{q^n}{\min\{d,k\}}$.

1 $GF(q)$上$[d,k]$——自控序列模型

设$GF(q)=\{0,\alpha^0,\alpha^1,\cdots,\alpha^{q^n-2}\}$，其中$\alpha$为有限域$GF(q)$的生成元。由于本文不涉及

* 1992年5月18日收稿

$GF(q)$的代数结构。而只关系到$GF(q)$上M序列及收缩M序列的伪随机特性，不妨用0，1，2，…，q^n-1表示$GF(q)$中q^n个元，即用0表示零元0，i表示元素$\alpha^{i-1}(i=1,2,\cdots,q^n-1)$.

定义 1.1 $GF(q)$上n级反馈移位寄存器产生的周期为q^n的q元序列，称为$GF(q)$上n级M序列。

熟知n级M序列具有如下伪随机特性，即在n级M序列的一个周期内：

(1) 0，1，…，$q-1$各数字均出现q^{n-1}次。

(2) r长k游程个数$=\begin{cases}1,(r=n)\\ q-2,(r=n-1)\\ (q-1)^2\cdot q^{n-r-2},(1\leqslant r\leqslant n-2)\end{cases}$

其中$k=0,1,2,\cdots,q-1$，而全部游程总数为$q^{n-1}(q-1)$.

定义 1.2 设$\underline{a}$为$GF(q)$上n级M序列，若将$\underline{a}$的一个周期内全0状态0^n去掉一个0，得到$GF(q)$上新序列，称为$GF(q)$上n级收缩M序列。易知$GF(q)$上n级m序列为$GF(q)$上n级收缩M序列。

定义 1.3 设$\underline{a}$为$GF(q)$上n级M序列或n级收缩M序列，$d,k\geqslant 1$为互素的正整数，定义

$$u_0=a_0,u_i=a_{f(i)}\quad i=1,2,\cdots$$

式中

$$f(0)=0,\quad f(i)=\begin{cases}f(i-1)+d,\text{当 } a_{f(i-1)}=0\\ f(i-1)+k,\text{当 } a_{f(i-1)}\neq 0\end{cases}$$

则称q元序列$\underline{u}=u_0u_1\cdots$为$\underline{a}$的$[d,k]$——自控序列。

注：(1)由$[d,k]$——自控序列的定义易知，$[d,k]$——自控序列一定为殆周期序列(即去掉前面若干项后为周期序列)。我们把序列$\underline{a}$中那些在$\underline{u}$中被保留的数字叫做保留数字，否则称为删除数字。

(2) 当$q=2$时，即为Rueppel[1]中$[d,k]$——自控序列。

例 1.1 取$q=3,n=3$则$GF(3)$上3级M序列$\underline{a}=000100212101102012022111222$，…的$[1,2]$——自控序列为$\underline{u}=00010220102102112,\cdots$ 周期$p(\underline{u})=17$. 而由$\underline{a}$产生的3级收缩M序列$\underline{a}'=001002121011020120222111222$，…的$[1,2]$——自控序列$\underline{u}'=0010220102102112,\cdots p|\underline{u})=16$.

下面我们来讨论$GF(q)$上$[d,k]$——自控序列平移等价特性。

2 平移特价性

对于$GF(q)$上任意n级M序列或收缩M序列a，其$[d,k]$——自控序列一定为殆周期序列，但是同一个序列$\underline{a}$，如果从不同的初态出发，即选取不同u_0，所产生的$[d,k]$——自控序列未必相同，即平移等价的序列所产生的$[d,k]$——自控序列未必平移等价。如：$GF(3)$上2级M序列$\underline{a}=001021122,\cdots$的$[4,5]$——自控序列为$\underline{u}=02,\cdots$，而与$\underline{a}$平移等价序列$\underline{a}'=010211220,\cdots$，产生的$[4,5]$——自控序列为$\underline{u}'=01,\cdots$，显然$\underline{u}$与$\underline{u}'$不平移等价。但我们可以证明：$GF(q)$上任意$n$级$M$序列或$n$级收缩$M$序列的$[1,2]$——自

控序列与初态选取无关，并具有良好的统计特性（另文表述）。本文证明对一般正整数 d，k，只要选取适当的 n，则产生的 $[d,k]$ ——自控序列与初态选取无关。即有如下定理：

定理 2.1 设 $\underline{a}$ 为 $GF(q)$ 上 n 级 M 序列或 n 级收缩 M 序列，$d,k\geqslant 1$ 为互素的正整数，则当 $n\geqslant M(d,k)=\begin{cases}k-1 & \text{当 } d=1 \text{ 并且 } \underline{a} \text{ 为收缩 } M \text{ 序列}\\ dk-2\min\{d,k\}+1. & \text{否则}\end{cases}$

则 $\underline{a}$ 的所有平移等价的序列产生的$[d,k]$——自控序列均彼此平移等价。

为证明定理 2. 1，我们引入两个基本概念：

定义 2.1 q 元有限序列 $c_1c_2\cdots c_\lambda(c_i\in GF(q))$叫做 $GF(q)$ 上$[d,k]$——保留型(删去型)，是指对任意 q 元序列 $\underline{a}=a_0a_1a_2\cdots$，如果 $\underline{a}$ 中有一段 $a_ia_{i+1}\cdots a_{i+\lambda-1}$. 只要 $a_ia_{i+1}\cdots a_{i+\lambda-1}=c_1c_2\cdots c_\lambda$ 则 $a_{i+\lambda}$必在 $\underline{a}$ 的$[d,k]$——自控序列中保留(删除)。

例 2.1 设 $\underline{a}$ 为 $GF(3)$ 上任意 n 级 M 序列，$[d,k]=[2,3]$，则 020 * (其中 * 可取 $GF(3)$中任意元)为$[2,3]$——保留型，这是因为假设 a 中有一段为 $a_ia_{i+1}a_{i+2}a_{i+3}=020*$，以 $\underline{u}=u_0u_1\cdots$表示 $\underline{a}$ 的$[2,3]$——自控序列，由于 $\max\{2,3\}=3$，可知 a_i,a_{i+1},a_{i+2}中必有一个数字在 $\underline{u}$ 中保留。若 $u_j=a_i=0$，则 $u_{j+1}=a_{i+2}=0$，于是 $u_{j+2}=a_{i+4}$，若 $u_j=a_{i+1}=2$，则 $u_{j+1}=a_{i+4}$.

若 $u_j=a_{i+2}=0$，则 $u_{j+1}=a_{i+4}$，这表明 a_{i+4}在 $\underline{u}$ 中必被保留，从而 020 * 为$[2,3]$——保留型，类似可知 002 * 为$[2,3]$——删除型。

引理 2.1 如果 q 元序列 $\underline{a}$ 的一个周期内存在$[d,k]$——保留型，则 $\underline{a}$ 的所有平移等价的序列所产生的$[d,k]$——自控序列必殆平移等价(即去掉前面若干项后平移等价)。

证明 设 $\underline{a}=a_0a_1a_2\cdots$，$c_1c_2\cdots c_\lambda$ 为 $GF(q)$上$[d,k]$——保留型，由题设在 $\underline{a}$ 中存在一段 $a_ia_{i+1}\cdots a_{i+\lambda-1}$，使得 $a_ia_{i+1}\cdots a_{i+\lambda-1}=c_1c_2\cdots c_\lambda$. 由保留型定义可知 $a_{i+\lambda}$为保留数字，于是不管从何初态出发，所得$[d,k]$——自控序列均保留数字 $a_{i+\lambda}$，从而$[d,k]$——自控序列均彼此殆平移等价。

引理 2.2[4] 设$(d,k)=1,d>0,k>0$，则凡大于 $dk-d-k$ 的数均可表成 $dx+ky(x\geqslant 0,y\geqslant 0)$之形，但 $dk-d-k$ 不能表成此形。

引理 2.3 设 $\underline{a}$ 为 n 级 M 序列或 n 级收缩 M 序列，$(d,k)=1$，则当 $n\geqslant M(d,k)$时，在 $\underline{a}$ 的一个周期内必有$[d,k]$——保留型 $c_1c_2\cdots c_M*_1\cdots*_{m-1}c$，其中 $M=M(d,k)$. $m=\min\{d,k\}$，$*_1,\cdots*_{m-1}$为 $GF(q)$中任意元。

证明 (构造性证明)。

不妨设 $d<k$　　即　$m=\min\{d,k\}=d$.

当 $d=1$ 时　　O^{k-1}为$[1,k]$——保留型，从而当

$$n\geqslant M(1,k)=\begin{cases}k-1,\text{当 } \underline{a} \text{ 为 } n \text{ 级 } M \text{ 序列}\\ k,\text{当 } \underline{a} \text{ 为 } n \text{ 级收缩 } M \text{ 序列}\end{cases}$$

时，$\underline{a}$ 的一个周期内必存在保留型 o^{k-1}.

当 $d\neq 1$ 时，考虑集合 $\Omega=\{\alpha d+\beta k\mid\alpha,\beta$ 为非负整数，但 α,β 不同时为 $0\}$。由于自然数集为可列集，故 Ω 也为可列集，将 Ω 中元素按由小到大顺序排列为 $d,\cdots,\alpha d+\beta k\cdots$，由引理 2.2，由于$(d,k)=1$，故 $dk-d-k\notin\Omega$，而 $dk-d-k+i\in\Omega$，$i=1,2,3,\cdots$，令 $u=dk-d-k+1$，则 u 在 Ω 的排列中出现，并且其后为 $u+1$，$u+2$，$\cdots$. 我们构作长为 $u+k$

$-1=dk-d$ 的 q 元序列如下：$a_{dk-d}a_{dk-d-1}\cdots a_d a_{d-1}\cdots a_1$.

凡是下标 i 可表为 $\alpha d(\alpha\geqslant 1)$的 a_i 取为 0.

凡是下标 i 可表为 $\beta k(\beta\geqslant 1)$的 a_i 取非 0 元。

其余任取 $GF(q)$中元。

由于$(d,k)=1$.且 $dk-d<dk$,所以若下标 i 可表为 $\alpha d(\alpha\geqslant 1)$. 则 i 一定不能表为 βk $(\beta\geqslant 1)$,反之也对。

当 $n\geqslant dk-d-(d-1)=dk-2d+1$ 时,n 级 M 序列或 n 级收缩 M 序列 $\underline{a}$ 中必有一段为"$a_{dk-d}\cdots a_d$".

下证 "$a_{dk-d}a_{dk-d-1}\cdots a_d * _1\cdots * _{d-1}c$ 必为$[d,k]$——保留型。

因为"$a_{dk-d}\cdots a_d$"前面 k 项下标均可以表为 $\alpha d+\beta k(\alpha\geqslant 0,\beta\geqslant 0)$之形,由$[d,k]$——自控序列特点,前面连续 k 项至少有一项被保留。设这一项下标为 i.

若 $i=\alpha d(\alpha\geqslant 1)$. 则由以上 q 元序列的构成特点，$[d,k]$——自控序列必保留 $a_{(\alpha-1)d}$, $a_{(\alpha-2)d}\cdots a_d$,从而必保留 c.

若 $i=\beta k(\beta\geqslant 1)$,则由构成特点,$[d,k]$——自控序列必保留 $a_{(\beta-1)k},a_{(\beta-2)k}\cdots a_k$,从而必保留 c.

若 $i=\alpha d+\beta k,(\alpha\geqslant 1,\beta\geqslant k)$. 则$[d,k]$——自控序列必保留 a_d 或 a_k,从而必保留 c.

故当 $n\geqslant M(d,k)=dk-2d+1$ 时,n 级 M 序列或 n 级收缩 M 序列 $\underline{a}$ 中必有$[d,k]$——保留型。

至此，引理 2.3 得证。

由引理 2.1 和引理 2.3 可知定理 2.1 成立。

3 周期上界

由前面讨论当 $n\geqslant M(d,k)$时,同一个 n 级 M 序列或 n 级收缩 M 序列 $\underline{a}$,从不同的初态出发所产生的$[d,k]$——自控序列必殆平移等价，从而具有相同的周期，下面我们给出周期一个上界。

定理 3.1 设 $\underline{a}$ 为 n 级 M 序列或 n 级收缩 M 序列，d，$k\geqslant 1$，$(d,k)=1$.则当 $n\geqslant M(d,k)$时,$[d,k]$——自控序列周期上界为$\dfrac{q^n}{\min\{d,k\}}$.

证明 设 $\underline{a}$ 为 n 级 M 序列，当 $n\geqslant M(d,k)$时,$\underline{a}$ 的一个周期内必有$[d,k]$——保留型，不防设 a_i 被保留. 从而 a_i+q^n 也被保留，设 w 为 $\underline{a}$ 的一个周期内保留数字的个数，易知$[d,k]$——自控序列周期 $p(\underline{u})\mid w$. 且 w 必为集合$\{x_l+y_l\mid x_l\geqslant 0,y_l\geqslant 0,dx_l+ky_l=q^n\}$中某一个数。从而 $w\leqslant\dfrac{q^n}{\min\{d,k\}}$. 于是

$$p(\underline{u})\leqslant\frac{q^n}{\min\{d,k\}}.$$

当 $\underline{a}$ 为 n 级收缩 M 序列时，类似可证

$$p(\underline{u})\leqslant\frac{q^n-1}{\min\{d,k\}}\leqslant\frac{q^n}{\min\{d,k\}}$$

定理 3.2 设 $d,k\geqslant 0$ 为正整数,$(d,k)=1$,则当 $n\geqslant M(d,k)$时,若 d,k 均为奇数,则$[d,$

k]——自控序列必为奇数。

定理 3.3 设 d 为奇数，k 为偶数，则当 $n \geqslant m(d,k)$ 时，$[d,k]$——自控序列中必含奇数个 0.

定理 3.2 和 3.3 可由定理 3.1 推出，这里从略。

参 考 文 献

1 Rueppel R A. When Shift Reqisters Clock Themselves. Euvocrypt'87: 13－15

2 Rueppel, Lai Xucjia. [d,k]－Self－Decimated sequences. preprint

3 万哲先. 代数和编码. 科学出版社, 1976

4 华罗庚. 数论导引. 科学出版社, 1979

5 万哲先等. 非线性移位寄存器. 科学出版社, 1976

6 李超. LSRg [d, k] ——自控序列. 通信保密, 1991, (2)

$[d,k]$—— Self－Controlled－Sequences on $GF(q)$

Li Chao

(Department of System Engineering and Applied Mathematics.)

Abstract

In this paper, the model of [d,k]—— self－Controlled－Sequences on GF(2) presented by R. A Rueppel in paper[1] is developed on GF(q). For M－sequences of order n and abbreviating M－sequences of order arbitary n. We discuss the translative equivalent properties and periodic properties of this sequences.

Key words [d,k]－Self－Controlled－Sequence, translative equivalence, remained form, deleted form