第15卷 第5期 电 子 科 学 学 刊 Vol. 15, No. 5
1993 年 9 月 JOURNAL OF ELECTRONICS Sept., 1993

产生 k 元 M 序列的一种新算法*

朱 士 信
(合肥工业大学应用数学系,230009)

摘要 本文给出了生成 k 元 M 序列的一种新的算法. 该算法不再采用"主圈并一个圈"的经典并圈法,而是利用了"主圈并一组共轭圈"的新的并圈方法. 这样减少了选择桥状态的次数,进而加快了并圈速度.

关键词 M 序列;状态图;桥状态

1. 引言

M 序列是一类最长的非线性移位寄存器序列,其应用广泛. 2 元 M 序列的构造方法已得到较充分的研究. 文献[1—6]中分别给出了 k 元 M 序列的不同构造方法及原理. 本文通过利用纯轮换移位寄存器的状态图中圈的游程数的性质,给出了生成 k 元 M 序列的一种新的算法,并给出了能产生 M 序列的数目的计数公式.

2. 基本原理

对任意自然数 $k(\geqslant 2)$,令 $Z_k=\{0,1,\cdots,k-1\}$,记以 Z_k^n 到 Z_k 上的函数 $f(x_1,x_2,\cdots,x_n)=x_1$ 为反馈函数的 n 级纯轮换移位寄存器为 PCR_n,其状态图为 G_f,状态转移变换为 T_f,则 T_f 可逆. 并称 T_fA 为状态 $A=(a_1,a_2,\cdots,a_n)\in Z_k^n$ 的后继状态. 若圈 σ 在 G_f 中,状态 A 在圈 σ 上,则分别记为 $\sigma\in G_f$ 及 $A\in\sigma$.

引理 1 设有圈长分别为 $l_1,l_2,\cdots,l_r$ 的 r 个不同的圈 $\sigma_1,\sigma_2,\cdots,\sigma_r$, $A_b=(b,a_2,\cdots,a_n)\in\sigma_b$,若将 A_b 的后继状态 T_fA_b 变为 $T_fA_s(b)$,并保持 σ_b 上的其余状态的后继状态不变, $b=1,2,\cdots,r$,则 $\sigma_1,\sigma_2,\cdots,\sigma_r$ 便合并为一个圈长为 $\sum_{b=1}^{r}l_b$ 的圈. 其中 s 为 r 个文字 $1,2,\cdots,r$ 的任一 r 阶轮换,且不能分解为两个不相交的轮换的乘积.

定义 1 设 $A=(a_1,a_2,\cdots,a_n)\in Z_k^n$,若 $b_i=a_i, b_{n+1}=a_1$, $i=1,2,\cdots,n$, 则称 $B=(b_1,b_2,\cdots,b_{n+1})$ 为 A 的 $n+1$ 级扩张;设满足条件: $b_j\neq b_{j+1}$, $1\leqslant j\leqslant n$ 的 j 的个数为 d,则称 d 为状态 A 的游程数,记为 $D(A)$.

引理 2 在 G_f 中,同一圈 σ 上的所有状态的游程数必相等;并称该数值为 σ 的游程数,记为 $D(\sigma)$,则 $2\leqslant D(\sigma)\leqslant n$ 或 $D(\sigma)=0$.

为了能生成大量的 M 序列,在给出并圈规则之前,先定义一个 n 级状态的集合 V 如下:

1992.05.29 收到, 1992.09.12 定稿.
* 信息安全国家重点实验室基金及合肥工大科研基金资助项目.
朱士信 男, 1962 年生,讲师,现主要从事代数编码,特别是移位寄存器序列的研究.

任取自然数 $s:1\leqslant s\leqslant k^{(n-6)/2}$,令

$$V=\bigcup_{0\leqslant i<j<k-1}V_{ij},\quad V_{ij}=\{A_{ij}(t)\mid t=0,1,\cdots,s-1\}$$

设 $k^{l-1}<s\leqslant k^l$, l 为自然数,则 $A_{ij}(t)$ 的构造如下:

(1) $A_{ij}(t)$ 的前 4 个分量为 $(iji0)$;

(2) $A_{ij}(t)$ 的第 5 个到第 $l+4$ 个分量形成 t 的 k 进制表示;

(3) $A_{ij}(t)$ 的最后 $l+1$ 个分量都为 j,第 $n-l-1$ 个分量为 0;

(4) $A_{ij}(t)$ 的第 $r(l+1)+4$ 个分量为 0, 其中 $1\leqslant r\leqslant\lceil(n-7-2l)/(l+1)\rceil$, $\lceil x\rceil$表示大于等于 x 的最小整数.

引理 3 V 中任何两个状态都不在 G_f 中的同一圈上.

设 $A=(a_1,a_2,\cdots,a_n)\in Z_k^n$, 令 $V(A)=\sum_{i=1}^{n}a_ik^{n-i}$. 若 $\sigma\in G_f$,则定义

$$V_{\max}(\sigma)=\max\{V(A)\mid A=(a_1,a_2,\cdots,a_n)\in\sigma\}$$
$$V_{\min}(\sigma)=\min\{V(A)\mid A=(a_1,a_2,\cdots,a_n)\in\sigma\}$$
$$V(\sigma)=\min\{V(A)\mid A=(a_1,a_2,\cdots,a_n)\in\sigma,\ 且\ a_1=a_3\neq a_2\}$$

当 σ 上不含形如 $(a_1,a_2,a_1\cdots)$ 的状态时,约定 $V(\sigma)=0$,其中 $a_1\neq a_2$.

下文中用"$A\to B$"表示在并圈过程中 B 是 A 的后继状态; 用 x^r 表示连续的 r 个分量为 x; S_{ij} 及 S_j 均为 $0,1,\cdots,k-1$ 的任一 k 阶不可分解的轮换, 且 S_{ij} 将 i 映到 j. 本文采用的并圈规则如下:

$R1$ $(i,j^{n-1})\to(j^{n-1},S_j(i)),i,j=0,1,\cdots,k-1$;

$R2$ 当 $0\leqslant i<j\leqslant k-1,t=1,2,\cdots,n-2$;且当 $j=1$ 时 $t\neq1$, 则 $(j^{n-t},i^t)\to(j^{n-t-1},i^{t+1}),(i,j^{n-t},i^{t-1})\to(j^{n-t},i^{t-1},j)$;

$R3$ 设 $A=(a_1^{t_1},a_2^{t_2},\cdots,a_r^{t_r})\in\sigma$, $r>2$, $t_i\geqslant2$, $a_i\neq a_{i+1}$, $x=a_1\neq a_r=y$, 若 $V(A)=V_{\max}(\sigma)$,则

$$(b,a_1^{t_1-1},a_2^{t_2},\cdots,a_r^{t_r})\to(a_1^{t_1-1},a_2^{t_2},\cdots,a_r^{t_r},S_{xy}(b)),\forall b\in Z_k;$$

$R4$ 若 $A_{ij}(t)\in V,(j^2,i,\cdots,0,j^{l+1})$ 为 $A_{ij}(t)$ 的共轭, 则 $A_{ij}(t)\to(j^2,i,\cdots,0,j^{l+1}),(j^2,i,\cdots,0,j^{l+1})\to T_fA_{ij}(t)$;

$R5$ 设 $A=(a_1,a_2^{t_2},\cdots,a_r^{t_r})\in\sigma$ 及 $B=(a_2^{t_2+1},a_3^{t_3},\cdots,a_r^{t_r})\in\sigma'$ 分别满足 $V(A)=V_{\max}(\sigma),V(B)\neq V_{\max}(\sigma')$, (其中 $r>2,a_2\neq a_r,a_i\neq a_{i+1},t_i\geqslant2$). 令 $t=\max\{a_2,\cdots,a_r\}$,则 $t<k-1$,于是

$$(i,a_2^{t_2},\cdots,a_r^{t_r})\to(a_2^{t_2},\cdots,a_r^{t_r},i+1),\ t+1\leqslant i\leqslant k-2$$
$$(k-1,a_2^{t_2},\cdots,a_r^{t_r})\to(a_2^{t_2},\cdots,a_{r-1}^{t_{r-1}},a_r^{t_r+1})$$
$$(a_r,a_2^{t_2},\cdots,a_r^{t_r})\to(a_2^{t_2},\cdots,a_r^{t_r},t+1);$$

$R6$ 设 $A_j=(a,b_j,a,a_4,\cdots,a_n)\in\sigma_j$,且 σ_j 上不含 V 中状态,$(b_j\neq a,j=1,\cdots,r,b_1<\cdots<b_r,r\geqslant1)$,若 $V(A_j)=V(\sigma_j)$,记 $A_0=(a^3,a_4,\cdots,a_n)\in\sigma_0$,当 $D(\sigma_j)>2$ 时, $T_fA_j\to T_f^2A_{j+1},T_fA_r\to T_f^2A_0(j=0,1,\cdots,r-1)$;

$R7$ 设 $A_j=b_j,a_1,\cdots,a_{n-1})\in\sigma_j$, σ_j 上无上述各类状态; 若 $V(T_fA_j)=V_{\min}(\sigma_j)$ $(j=1,\cdots,r,b_1<\cdots<b_r,r\geqslant1,a_1\neq a_{n-1})$, 记 $A_0=(a_1,a_1,a_2,\cdots,a_{n-1})\in\sigma_0$, 则

$A_r \to T_f A_0, A_j \to T_f A_{j+1}(j=0,1,\cdots,r-1)$;

$R8$　否则，$A \to T_f A$.

在上述并圈过程中，如果 $A \to B$，且 A 及 B 不在 G_f 中的同一个圈上，则称 A 为桥状态. 从上述并圈规则易知，任何一个状态至多被选作一次桥状态，且 G_f 中每个圈上至少有一个状态被选作桥状态.

定理 1　按上述并圈规则合并 G_f 中所有圈便得到一个最大圈.

证明　只需要证明 G_f 中所有非零圈均与全零圈(只有零状态组成的圈)被连为一个圈. 为此，对 $\forall \sigma \in G_f$，利用引理 1，引理 2 及并圈规则对 $D(\sigma)$ 进行数字归纳法，便可证明 σ 与全零圈被连为一个圈.

由并圈规则知，在并圈过程中，一旦某一个状态被选作桥状态，则它的全体共轭状态或部分共轭状态也被选作桥状态，从而减少了寻找及判断桥状态的次数，进而加快了并圈速度.

3.产生 M 序列的递归算法

算法 1　任取参数 $s, 1 \leqslant s \leqslant k^{(n-6)/2}$，选择并储存 $[ks(k-1)/2]$ 个状态组成集合 V，任意取定 k 个数字 $0,1,\cdots,k-1$ 的 k 阶不可分解的轮换 S_{ij} 及 S_i，$i,j=0,1,\cdots,k-1, i>j$，且 S_{ij} 将 i 映到 j (其它元素的对应只须保证 S_{ij} 及 S_i 为 k 阶不可分解的轮换即可). 任取初值 $A_0=(a_0,a_1,\cdots,a_{n-1})$，设已生成 $A_r=(a_r,a_{r+1},\cdots,a_{r+n-1})$，生成 $A_{r+1}=(a_{r+1},\cdots,a_{r+n})$ 中 a_{r+n} 如下：

(1) 若 $A_r=A_{ij}(t)\in V$；或 $A_r=(j^2,a_{r+2},\cdots,a_{r+n-1})$，且 $(i,j,a_{r+2},\cdots,a_{r+n-1})\in V$；或 $A_r=(j^{n-t},i^t)$ 或 $A_r=(i,j^{n-t},i^{t-1})$ $(0\leqslant i<j\leqslant k-1, t=1,2,\cdots,n-2$，且 $j=1$ 时 $t\neq 1)$，则转到(7)；若 $A_r=(i,j^{n-1})$，则 $a_{r+n}=S_j(i)$.

(2) 设 $\bar{A}_r$ 为 A_r 的某一共轭状态，如果 A_r 或 $\bar{A}_r=(b_1^{t_1},\cdots b_s^{t_s})\in\sigma$，且 $V(b_1^{t_1},\cdots,b_s^{t_s})=V_{\max}(\sigma)$，(其中，$b_i\neq b_{i+1}, b_j\geqslant 2, s>2$. 令 $i=b_1>j=b_s$)，则 $a_{r+n}=S_{ij}(a_r)$.

(3) 设 $A_r=(b_1,b_2^{t_2},\cdots,b_s^{t_s})$ (其中 $b_2\neq b_3, b_i\neq b_{i+1}, t_i\geqslant 2, s>2$)，如果 $B_1=(m-1,b_2^{t_2},\cdots,b_s^{t_s})\in\sigma_1$，$B_2=(b_2^{t_2+1},b_3^{t_3},\cdots,b_s^{t_s})\in\sigma_2$ 分别满足 $V(B_1)=V_{\max}(\sigma_1)$，$V(B_2)\neq V_{\max}(\sigma_2)$，令 $t=\max\{b_2,\cdots,b_r\}$，则当 $a_r=a_{r+n-1}$ 时，$a_{r+n}=t+1$；当 $a_r=k-1$ 时，$a_{r+n}=a_{r+n-1}$；当 $t+1\leqslant a_r\leqslant k-2$ 时，$a_{r+n}=a_r+1$.

(4) 设 $a_{r+1}=a_{r+n-1}$，如果存在 $b_1,\cdots,b_t$ 使 $B_j=(b_j,a_{r+1},\cdots,a_{r+n-1})\in\sigma_j$ 满足 $V(T_f^{-1}B_j)=V(\sigma_j)$，且 σ_j 上不含 V 中状态 $(j=1,\cdots,s,s\geqslant 1$，不妨设 $b_1<\cdots<b_s)$，则当 $a_r=a_{r+1}$ 时，$a_{r+n}=b_1$；当 $a_r=b_j$ 时，$a_{r+n}=b_{j+1}(j=1,\cdots,s-1)$；当 $a_r=b_s$ 时，$a_{r+n}=a_{r+1}$.

(5) 设 $a_{r+1}\neq a_{r+n-1}$，如果存在 $B_j=(b_j,a_{r+1},\cdots,a_{r+n-1})$ 满足 $V(T_fB_j)=V_{\min}(\sigma_j)$，且 σ_j 不含上述任何桥状态 $(j=1,\cdots,s,s\geqslant 1$，且设 $b_1<\cdots<b_s)$，则当 $a_r=a_{r+1}$ 时，$a_{r+n}=b_1$；当 $a_r=b_j$ 时，$a_{r+n}=b_{j+1}$ $(j=1,\cdots,s-1)$；当 $a_r=b_s$ 时，$a_{r+n}=a_{r+1}$.

(6) $a_{r+n}=a_r$，停.

(7) 当 $a_r=i$ 时，$a_{r+n}=j$；当 $a_r=j$ 时，$a_{r+n}=i$.

定理 2　(1) 算法 1 产生的序列为 M 序列；(2) 若参数 s 为 $k^{l-1}<s\leqslant k^l$，$0\leqslant$

$l \leqslant [(n-6)/2]$，则算法 1 能产生 $[(k-1)!]^k[(k-2)!]^{k(k-1)/2}k^{[k(k-1)s\cdot N(n,s)/2]}$ 个平移不等价的 k 元 M 序列，其中 $N(n,s) = n - 6 - 2l - \lceil (n-2l-7)/(l+1) \rceil$。

注 平移不等价的 k 元 n 级 M 序列的个数为 $[(k-1)!]^{k^{n-1}}k^{k^{n-1}-n}$，本文的算法只能产生其中一部分。

参 考 文 献

[1] H Fredrickson, J. Maiorana, *Discrete Math.*, 23(1978)1, 207—210.
[2] T. Etzion, *J. Algorithms*, 7(1986)2, 331—340.
[3] A. Ralston, *J. Algorithms*, 2(1981)1, 50—62.
[4] Yan Junhui, *Systems Science and Mathematical Sciences*, 4(1991), 32—40.
[5] 朱士信，高校应用数学学报，6(1991)2，236—240.
[6] 熊荣华，中国科学，A 辑，1988 年，第 8 期，第 877—886 页.

A NEW ALGORITHM FOR GENERATING k-ARY M SEQUENCES

Zhu Shixin

(Hefei University of Technology, Hefei 230009)

Abstract A new algorithm for generating k-ary M sequences is given. Not the classical method that the main cycle is extended by joining to it one cycle but a new method that the main cycle is exended by joining to it a subset of cycles is used in the algorithm. The algorithm reduces the time of choosing bridging states, and accelerates the speed of joining cycles.

Key words M sequences; State graph; Bridging state