系 统 科 学 与 数 学
J. Sys. Sci. & Math. Scis.
7 (4) (1987), 335—343

产生 M 序列的一个递推算法

章照止　罗乔林
(中国科学院系统科学研究所)

§1. 引　言

M 序列又称 de Bruijn 序列,是一类具有最长周期的非线性移位寄存器序列. 本文研究产生M序列的算法. 早在70年代万哲先等[1]对构造M序列的方法已有系统的研究. 此后有一系列的文章研究M序列的构造问题[2-7]. 最近 Fredricksen[8] 对这方面的工作给出了一个很好的综述. 产生M序列的一个常用方法是先由一个较简单的移位寄存器产生许多短圈,再用并圈法将这些短圈合并起来构成M序列. 如在[1,6]中就已给出过一些将n级纯轮换移位寄存器(简记为 PCR_n) 和n级补轮换移位寄存器(简记为 CCR_n) 产生的圈合并为M序列的方法. 与[1—7]不同, Fredricksen[8,9] 给出一个将 PCR_n 产生的圈合并为M序列的递推算法. 最近 Etzion 和 Lempel[10] 在 Fredricksen 算法的基础上,又提出一个将 PCR_n 产生的圈合并为M序列的递推算法. 此外他们在[10]中还提出一个将n级纯加移位寄存器(简记为 PSR_n) 产生的圈合并为M序列的递推算法. 这些递推算法的一个重要性质,是算法所能产生的M序列的数目与产生每个M序列所要占用的存储比特数(二进数字个数)成指数关系,以及每步递推(由前n个数推下一个数)所用的计算时间为 $O(n)$ 单位.

本文提出一个具有上述性质的将 CCR_n 产生的圈合并为M序列的递推算法. 具体地说,用本文给出的算法能产生 $2^{g(n)}$ 个M序列,其中

$$g(n)=\sum_{i=1}^{n-4}[g(n,i)+\log i], \tag{1}$$

$$g(n,i)=\begin{cases}(m-1)i, & 若\ n=m(i+2),\\ (m-1)i+r-2, & 若\ n=m(i+2)+r,\ 0<r<i+2.\end{cases} \tag{2}$$

(1)式中的对数取 2 为底. 产生每个M序列所要占用的存储比特数稍多于 $3n+g(n)$ 但不超过 $4n-4+g(n)$, 每步递推所用的计算时间为 $O(n)$ 单位. 如[10]文中指出的,具有上述性质的算法,对密码应用是有价值的.

§2. 圈的定义及并圈法

n 级移位寄存器的状态为长n的二元序列,记作 $s=(x_1,x_2,\cdots,x_n)$, 其中 $x_i\in B$

---

* 本工作得到中国科学院科学基金资助.

1986 年 9 月 22 日收到.

$=\{0,1\}$. 故总共有 2^n 个状态,记 B^n 为其状态集. 由一个 n 级移位寄存器的反馈函数 $f(x_1,x_2,\cdots,x_n)$ 可以导出一个从 B^n 到 B^n 的映射 T,

$$Ts=(x_2,\cdots,x_n,f(x_1,x_2,\cdots,x_n)),\quad s=(x_1,x_2,\cdots,x_n)\in B^n, \tag{3}$$

称为这个移位寄存器的状态转移变换.

$C=(s_0,s_1,\cdots,s_{N-1})$ 称为由一个 n 级移位寄存器产生的长 N 的圈,若状态 $s_0,s_1,\cdots,s_{N-1}$ 全不相同,且对这个移位寄存器的状态转移变换 T 有 $Ts_{N-1}=s_0$, $Ts_i=s_{i+1}$, $i=0,1,\cdots,N-2$. 由圈的定义易见,若定义 $T^0s=s$, $T^is=T(T^{i-1}s)$, $i>0$, 则圈 C 可以表示为

$$C=(T^0s,T^1s,\cdots,T^{N-1}s),\quad s\in C. \tag{4}$$

若 n 级移位寄存器是非奇异的,即其反馈函数 f 可表示为

$$f(x_1,x_2,\cdots,x_n)=x_1\oplus f_0(x_2,x_3,\cdots,x_n),$$

其中 f_0 为 $n-1$ 个变元的布尔函数, $\oplus$ 为模 2 加,则 B^n 中的每个状态一定在它所产生的某个圈上.换句话说,一个非奇异的 n 级移位寄存器可以产生 K(K 为某一正整数)个互不相交的圈,其圈长之和等于 2^n. 特别,若一个 n 级移位寄存器产生唯一的一个长 $N=2^n$ 的圈 C,则 C 称为一个全长圈. 众所周知,长 2^n 的全长圈与 n 级 M 序列是等价的.

状态 $s=(x_1,x_2,\cdots,x_n)$ 的共轭定义为 $s'=(x_1,x_2,\cdots,x_{n-1},x_n\oplus 1)$. 圈 C_1 称为与 C_2 相邻,若 C_1 与 C_2 不相交且存在状态 $s\in C_1$, 其共轭 $s'\in C_2$.

定理 1.[11] 若圈 $C_1=(s_0,\cdots,s_i,\cdots,s_{N_1-1})$ 与 $C_2=(t_0,\cdots,t_j,\cdots,t_{N_2-1})$ 相邻,其中 s_i 与 t_j 为一对共轭状态,则可通过互换 s_i 和 t_j 前的状态序列, 将 C_1 和 C_2 合并为一个圈 $C=(s_0,\cdots s_{i-1},t_j,\cdots,t_{N_2-1},t_0,\cdots,t_{j-1},s_i,\cdots,s_{N_1-1})$.

定理 1 给出一个将相邻的两个圈 C_1 和 C_2 合并为一个圈 C 的方法. 在定理 1 中, 状态 s_i 和 t_j 称为并圈所用的过渡状态. 根据定理 1, 分别在圈 C_1 和 C_2 上的任意一对共轭状态都可用作并圈的过渡状态. 显然用不同的过渡状态并出的圈也不同.

§3. CCR_n 圈的性质和分类

CCR_n 的反馈函数为 $f(x_1,x_2,\cdots,x_n)=\bar{x}_1=x_1\oplus 1$. 因此对 CCR_n 的状态转移变换 T, (3) 式化为

$$Ts=(x_2,\cdots,x_n,\bar{x}_1),\quad s=(x_1,x_2,\cdots x_n)\in B^n. \tag{5}$$

以后总设 T 为 CCR_n 的状态转移变换. 众所周知[11], CCR_n 产生的圈的长一定是 $2n$ 的正因数但又不是 n 的因数.

一个状态 $s=(x_1,x_2,\cdots,x_n)$ 所含游程数 $R(s)$ 定义为二元序列 $x_1x_2\cdots x_n$ (头尾不相接)中游程(包括 0 游程和 1 游程)的总个数. 例如, 状态 $s=(1,0,0,1,1,1)$ 所含游程数 $R(s)=3$.

定理 2. CCR_n 产生的圈 C 有如下性质:

1) 若 $s=(x_1,x_2,\cdots,x_n)\in C$, 则 $\bar{s}=(\bar{x}_1,\bar{x}_2,\cdots,\bar{x}_n)\in C$;

2) C 上一定存在 $R(s)$ 为奇数的状态 s;

3）存在某个正整数 k，$1 \leqslant k \leqslant K = \left[\frac{n+1}{2}\right]^-$，使

$$2k-1 \leqslant R(s) \leqslant 2k \tag{6}$$

对一切 $s \in C$ 成立，其中 $[u]^-$ 表示不超过 u 的最大整数。

证。1）由(5)式可见，若 $s \in C$，则 $\bar{s} = T^n s$，故 $\bar{s} \in C$。

2）任取 $s = (x_1, x_2, \cdots, x_n) \in C$。若 $R(s)$ 为偶数，则 $x_n = \bar{x}_1$。设 s 的第一个游程长为 l，即 $x_i = x_1$，$i = 1, 2, \cdots, l$，$x_{l+1} \neq x_1$。于是 $s' = T^l s = (x_{l+1}, \cdots, x_n, \bar{x}_1, \cdots, \bar{x}_l) \in C$，$R(s') = R(s) - 1$ 为奇数。

3）任取 $s \in C$，因 $1 \leqslant R(s) \leqslant n$，故存在某个正整数 k，$1 \leqslant k \leqslant K$，使(6)式成立。今对这个 k 证，若 $s = (x_1, x_2, \cdots, x_n) \in C$ 且 $R(s)$ 满足(6)，则 $R(Ts)$ 也满足(6)。分两种情况：a) $R(s) = 2k-1$，这时 $x_n \neq \bar{x}_1$，因此若 $x_1 \neq x_2$，则 $R(Ts) = 2k-1$，若 $x_1 = x_2$，则 $R(Ts) = 2k$；b) $R(s) = 2k$，这时 $x_n = \bar{x}_1$，因此若 $x_1 \neq x_2$，则 $R(Ts) = 2k-1$，若 $x_1 = x_2$，则 $R(Ts) = 2k$。根据这一事实及 C 的表示式(4)证得3)。

根据定理2可以将 CCR_n 产生的圈分为 K 类，记 $\mathscr{C}_k (1 \leqslant k \leqslant K)$ 为圈上状态满足 $2k-1 \leqslant R(s) \leqslant 2k$ 的那些圈 C 构成的类。

记 $L(s)$ 为状态 s 所含最长游程的长。根据定理2的2)，一个 CCR_n 产生的圈 C 上一定有 $R(s)$ 为奇数的状态，显然 C 上 $R(s)$ 为奇数的那些状态 s 有相同的 $L(s)$ 值。定义 $L(C)$ 为这个 $L(s)$ 值。于是可以将 $\mathscr{C}_k (1 \leqslant k \leqslant K)$ 再分为若干子类，记 $\mathscr{C}_{kl}$ 为 $\mathscr{C}_k$ 中 $L(C) = l$ 的那些圈 C 构成的子类。

引理 1. 若 $\mathscr{C}_{k2}$，$k < K$ 非空，C 为其中任一圈，s 为 C 上 $R(s)$ 为奇数的任一状态，则 s 至少含两个长为2的游程。

证。因 $k \leqslant K-1$，故

$$R(s) = 2k - 1 \leqslant 2(K-1) - 1 = 2\left[\frac{n+1}{2}\right]^- - 3 \leqslant n - 2,$$

但 $L(s) = 2$，因此 s 至少含两个长为2的游程。

根据引理1，对 $\mathscr{C}_{k2} (k < K)$ 中的圈 C，C 上 $R(s)$ 为奇数的状态 s，可定义 $D(s)$ 为 s 所含长2的游程间的最短间隔。两个长2的游程间的间隔定义为它们中间所夹的0和1的个数。例如，状态 $s = (1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$ 的 $D(s) = 0$。状态 $s = (1, 1, 0, 1, 0, 0, 1, 0, 1, 1)$ 的 $D(s) = 2$。定义 $D(C) = \min D(s)$，其中极小是对 C 上 $R(s)$ 为奇数的一切状态 s 而取。于是可以将 $\mathscr{C}_{k2} (k < K)$ 再细分为若干子类，记 $\mathscr{C}_{k2d}$ 为 $\mathscr{C}_{k2}$ 中 $D(C) = d$ 的那些圈 C 构成的子类。

§4. 将 CCR_n 圈合并为全长圈

引理 2. 设 C 为 $\mathscr{C}_{kl}$，$k < K$，$l \geqslant 3$ 中的一个圈，则 C 上一定有 $2i = 2(l-2)$ 个状态 $s_1, s_2, \cdots, s_i, \bar{s}_1, \bar{s}_2, \cdots, \bar{s}_i$，它们的共轭 $s'_1, s'_2, \cdots, s'_i, \bar{s}'_1, \bar{s}'_2, \cdots, \bar{s}'_i$ 在 $\mathscr{C}_{k+1}$ 的某些圈上。

证. 根据 $\mathscr{C}_{kl}$ 的定义及定理 2 的 1), C 上一定存在 $R(s)=2k-1$ 且形如 $s=(0, x_2, \cdots, x_{n-l-1}, 1, 0^l)$ 的状态,其中 0^l 表示 l 个接连的零 $0, 0, \cdots, 0$. 因此 $s_j=T^{-j}s=(1^j, 0, x_2, \cdots, x_{n-l-1}, 1, 0^{l-j})$, $j=1, 2, \cdots, i=l-2$ 都在 C 上,且 $R(s_j)=2k$. 因 $l-j\geqslant 2$, 故 s_j 的共轭 s_j' 所含游程数 $R(s_j')=2k+1=2(k+1)-1$. 因此它们都在 $\mathscr{C}_{k+1}$ 的某些圈上. 根据定理 2 的 1) $\bar{s}_j, j=1, 2, \cdots, i$ 也在 C 上. 因 $\bar{s}_j$ 的共轭为 $\bar{s}_j'$, 于是由 $R(\bar{s}_j')=R(s_j')=2(k+1)-1$ 证得引理.

引理 3. 1) 若 $\mathscr{C}_{k2d}$, $k<K$, $d>0$ 非空,则 $\mathscr{C}_{k2d-1}$ 非空. 设 C 为 $\mathscr{C}_{k2d}$ 中的一个圈,则 C 上一定有两个状态 $s_1, \bar{s}_1$, 它们的共轭 $s_1', \bar{s}_1'$ 在 $\mathscr{C}_{k2d-1}$ 的某个圈上.

2) 若 $\mathscr{C}_{k20}$, $k<K$ 非空,则 $\mathscr{C}_{k3}$ 非空. 设 C 为 $\mathscr{C}_{k20}$ 中的一个圈,则 C 上一定有两个状态 $s_1, \bar{s}_1$, 它们的共轭在 $\mathscr{C}_{k3}$ 的某个圈上.

证. 1) 根据 $\mathscr{C}_{k2d}$ 的定义及定理 2 的 1), C 上一定存在 $R(s)=2k-1$ 且形如 $s=(0, x_2, \cdots, x_{n-d-3}, x_{n-d-2}, x_{n-d-1}, \cdots, x_{n-3}, 1, 0, 0)$ 的状态,其中 $x_{n-d-3}=x_{n-d-2}=0$, 若 d 为奇数; $x_{n-d-3}=x_{n-d-2}=1$, 若 d 为偶数,且 $x_{i+1}\neq x_i$, $i=n-d-2, \cdots, n-4$. 因此 $s_1=T^{-1}s=(1, 0, x_2, \cdots, x_{n-d-3}, x_{n-d-2}, x_{n-d-1}, \cdots, x_{n-3}, 1, 0)$ 也在 C 上,且 $R(s_1)=2k$. 由此易见, s_1 的共轭 s_1' 有 $R(s_1')=2k-1$, $D(s_1')=d-1$, 且 s_1' 所在的圈 $C'=(T^0s_1', T^1s_1', \cdots, T^{N-1}s_1')$ 有 $L(C')=2$, $D(C')=d-1$. 按定义 C' 为 $\mathscr{C}_{k2d-1}$ 的圈. 再由定理 2 的 1) 及 $\bar{s}_1$ 的共轭为 $\bar{s}_1'$ 证得 1).

2) 的证明方法和 1) 完全一样,故略去.

由引理 2、引理 3 和定理 1 导出一个将 CCR_n 产生的圈合并为全长圈的简单方法. 在合并过程中的每一步,我们得到一个由一部分 CCR_n 圈合并起来的主圈和其它有待合并的 CCR_n 圈. 开始时,取 $\mathscr{C}_K\left(K=\left[\frac{n+1}{2}\right]^-\right)$ 中的唯一的一个圈作为主圈,下一步将 $\mathscr{C}_{K-1}$ 中的圈并入主圈,并入次序为先并 $\mathscr{C}_{K-1l}$, $l\geqslant 3$, 再并 $\mathscr{C}_{K-120}, \mathscr{C}_{K-121}, \cdots$ 直到将 $\mathscr{C}_{K-1}$ 中的圈全部并入主圈为止. 在合并上列各子类中的圈时,次序可以任意. 一般地在第 i 步将 $\mathscr{C}_{K-i}$ 中的圈并入主圈,并入次序仍为先并 $\mathscr{C}_{K-il}$, $l\geqslant 3$, 再并 $\mathscr{C}_{K-i20}$, $\mathscr{C}_{K-i21}, \cdots$ 直到将 $\mathscr{C}_{K-i}$ 中的圈全部并入主圈为止. 由引理 2 和引理 3 以及我们规定的将 CCR_n 圈并入主圈的次序,保证了这一合并过程的每一步都是可行的. 这一过程一直进行到将 CCR_n 产生的圈全部并入主圈时终止. 这时的主圈即为一个全长圈. 注意 $\mathscr{C}_{k1}$, $k<K$ 总是空集,故在合并过程中没有考虑.

5. 产生 M 序列的一个递推算法

现在我们将 § 4 中描述的构造全长圈的方法具体化为一个产生 M 序列的递推算法. § 2 中已提到一个二元 n 级 M 序列

$$a=(a_0, a_1, \cdots, a_{N-1}, \cdots), \quad N=2^n$$

与一个长 $N=2^n$ 的全长圈

$$C=(s_0, s_1, \cdots, s_{N-1}),$$

其中

$$s_j=(a_j,a_{j+1},\cdots,a_{j+n-1}),\quad j=0,1,\cdots,N-1$$

是等价(一一对应)的。从状态 s_j 转移到 s_{j+1} 有两种可能情况:

1) $a_{j+n}=\bar{a}_j$, 即 $(a_j,a_{j+1},\cdots,a_{j+n-1})\to(a_{j+1},\cdots,a_{j+n-1},\bar{a}_j)$;

2) $a_{j+n}=a_j$, 即 $(a_j,a_{j+1},\cdots,a_{j+n-1})\to(a_{j+1},\cdots,a_{j+n-1},a_j)$.

若 C 为由 CCR_n 产生的圈用§4中的方法合并而成的全长圈,则情况 1) 对应于一个 CCR_n 圈内的状态转移,即 s_j 和 s_{j+1} 属于同一个 CCR_n 圈;而情况 2) 对应于一个 CCR_n 圈到另一个 CCR_n 圈的状态转移,即 s_j 和 s_{j+1} 分别属于两个不同的 CCR_n 圈. 这时 s_{j+1} 为合并成 C 时所用的一个过渡状态(参看定理 1 及其后的说明). 从以上讨论知,若对任一 j, $0\leqslant j\leqslant N-1$, 我们能利用已知的状态 $s_j=(a_j,a_{j+1},\cdots,a_{j+n-1})$ 及预先选定的存储信息,通过计算判断出下一状态 $s_{j+1}=(a_{j+1},\cdots,a_{j+n-1},a_{j+n})$ 是否属于合并成 C 时所用的过渡状态,那么我们就能用递推算法产生 C 所对应的 M 序列 a.

今考虑一个有 $n-4$ 个状态构成的有序集 $V=\{V(i),\ i=1,2,\cdots,n-4\}$, 其中

$$V(i)=T^{-x(i)}(\overline{s(i)}),\quad 1\leqslant i\leqslant n-4. \tag{7}$$

这里,状态 $s(i)$ 构造如下:

1) 若 $n=m(i+2)$, 则 $s(i)$ 可分为 m 段,每段为一长 $i+2$ 的数列. 取 $s(i)$ 的最末一段为 $1\ 0\ 0^i$, 其它各段的前两个数为 1 0, 剩下的数任意取.

2) 若 $n=m(i+2)+1$, 则除了最头上一段长 $i+3$ 的数列外, $s(i)$ 的取法同 1). 取 $s(i)$ 的头一段的前 4 个数为 1 0 1 0, 其它数任意取.

3) 若 $n=m(i+2)+r$, $2\leqslant r\leqslant i+1$, 则 $s(i)$ 可分为 $m+1$ 段,除头一段长 r 外其它段都长 $i+2$. 取 $s(i)$ 的头一段的前两个数为 1 0, 其它数任意取. $s(i)$ 的后 m 段的取法同 1).

$x(i)$ 可在 $\{0,1,\cdots,i-1\}$ 中任意取. T 如前为 CCR_n 的状态转移变换.

例 1. $n=12$ 对应的 $s(i)$, $i=1,2,\cdots,8$ 如下:

$$\begin{array}{l}
1\ 0\ x_1(1)\ 1\ 0\ x_2(1)\ 1\ 0\ x_3(1)\ 1\ 0\ 0\\
1\ 0\ x_1(2)\ x_2(2)\ 1\ 0\ x_3(2)\ x_4(2)\ 1\ 0\ 0\ 0\\
1\ 0\ 1\ 0\ x_1(3)\ x_2(3)\ x_3(3)\ 1\ 0\ 0\ 0\ 0\\
1\ 0\ x_1(4)\ x_2(4)\ x_3(4)\ x_4(4)\ 1\ 0\ 0\ 0\ 0\ 0\\
1\ 0\ x_1(5)\ x_2(5)\ x_3(5)\ 1\ 0\ 0\ 0\ 0\ 0\ 0\\
1\ 0\ x_1(6)\ x_2(6)\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\\
1\ 0\ x_1(7)\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\\
1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0
\end{array}$$

其中 $x_j(i)$ 为自由参数.

引理 4. 集 V 中的 $n-4$ 个状态分别在 $n-4$ 个不同的 CCR_n 圈上,且这些状态都可用作并圈的过渡状态.

证. 由 $s(i)$ 的构造易见, $Ts(i)$ 的首尾都是 0, 且 $Ts(i)$ 尾上的一个长 $i+2$ 的 0 游程为 $Ts(i)$ 所含的最长游程. 于是有 $R(Ts(i))$ 为奇数, $L(Ts(i))=i+2$. 记 $C(i)$ 为 $s(i)$ 所在的 CCR_n 圈,则按定义有 $L(C(i))=i+2$, $i=1,2,\cdots,n-4$.

故它们是 $n-4$ 个不同的圈. 又根据定理 2 的 1), $V(i)$ 也在 $C(i)$ 上,证得引理的前一部分. 引理的后一部分由 $C(i)$ 属于某一 $\mathscr{C}_{kl}$, $k<K$, $l=i+2$ 及引理 2 证得.

根据引理 4, 我们可任选一组参数 $x_j(i)$, $j=1,2,\cdots,g(n,i)$, 及 $z(i)$; $i=1,2,\cdots,n-4$, 其中 $g(n,i)$ 由 (2) 式给出. 将这组参数对应的集 V 中的状态及其共轭确定为它们所在圈并圈时所用的过渡状态. 下面还要确定其它 CCR_n 圈并圈时所用的过渡状态. 定义一个状态 $s=(x_1,x_2,\cdots,x_n)$ 的值为

$$|s|=x_1 2^{n-1}+x_2 2^{n-2}+\cdots+x_n. \tag{8}$$

引理 5. 若 s 为一 CCR_n 圈 C 上值最大的状态,则 s 具有如下性质:

1) s 头上一定是一个 1 游程,且为 s 所含的最长游程;

2) $R(s)$ 为奇数;

3) 若 $L(s)\geqslant 3$, 则 T^2s 可用作并圈的过渡状态.

证. 1) 由定理 2 的 1), C 上一定有含 1 游程的状态,故由 (8) 证得 1).

2) $R(s)$ 一定为奇数,否则 $|T^{-1}s|>|s|$, 与假设矛盾.

3) 由 2) 及 $L(s)\geqslant 3$ 知, $L(C)\geqslant 3$, 即 C 属于某一 $\mathscr{C}_{kl}$, $k<K$, $l\geqslant 3$. 故由引理 2 证得 3).

根据引理 5, 若 CCR_n 圈 $C\in\mathscr{C}_{kl}$, $k<K$, $l\geqslant 3$, 但不属于 V, 我们可确定 T^2s 及其共轭为 C 并圈时所用的过渡状态, 其中 s 为 C 上值最大的状态. 最后若 CCR_n 圈 $C\in\mathscr{C}_{k2d}$, $k<K$, $d\geqslant 0$, 我们可确定引理 3 中给出的状态 s_1 及其共轭为 C 并圈时所用的过渡状态. 若 C 上满足引理 3 中条件的状态 s_1 多于一个, 则取其中值最大的一个作为过渡状态. 至此,我们已经按照 § 4 中描述的构造全长圈的方法,具体地确定了一组可行的并圈所用的过渡状态. 下面给出产生 M 序列的具体算法.

算法 I. 选定并存储一组参数 $x_j(i)$, $j=1,2,\cdots,g(n,i)$, 及 $z(i)$; $i=1,2,\cdots,n-4$. 给定初始值 $\alpha_0=(0,0,\cdots,0)=(0^n)$. 由已知的 $\alpha_j=(a_j,a_{j+1},\cdots,a_{j+n-1})$ 计算 a_{j+n} 如下:

1) 若 $a_{j+1}=0$, 置 $\alpha_j^*=(a_{j+1},\cdots,a_{j+n-1},1)$. 算出 $i=L(C)-2$, 其中 C 为 α_j^* 所在的 CCR_n 圈. 若 $i=0$, 转到 5); 否则,若 $\alpha_j^*=V(i)=T^{-z(i)}\overline{(s(i))}$, 转到 4); 若 $\alpha_j^*\neq V(i)$, 转到 5).

2) 若 $a_{j+1}=1$, 置 $\alpha_j^*=(a_{j+1},\cdots,a_{j+n-1},0)$. 算出 α_j^* 尾上一个 0 游程的长 l. 若 $l>2$, 转到 5); 否则, 若 $l=1$, 转到 3); 若 $l=2$, 置 $\alpha=T^2s$, 其中 s 为 α_j^* 所在的 CCR_n 圈 C 上值最大的状态,若 $\alpha_j^*=\alpha$, 转到 4); 若 $\alpha_j^*\neq\alpha$, 转到 5).

3) 若 $L(\alpha_j^*)\neq 2$, 转到 5); 否则, 算出 α_j^* 头上一个 1 游程的长 l', 若 $l'=2$, 转到 5); 若 $l'=1$, 置 $\alpha=s_1$, 其中 s_1 为 α_j^* 所在的 CCR_n 圈 C 上满足下列条件的状态: a) s_1 头上为一个 1 游程 1; b) s_1 尾上为一个 0 游程 0; c) s_1 含一个长 2 的游程,它与 s_1 尾上的 0 游程之间的间隔等于 $D(C)$; d) s_1 为 C 上满足条件 a), b), c) 的状态中值最大的状态; 若 $\alpha_j^*=\alpha$, 转到 4); 若 $\alpha_j^*\neq\alpha$, 转到 5).

4) 置 $a_{j+n}=a_j$, 停.

5) 置 $a_{j+n}=a_j\oplus 1$.

定理 3. 1) 对于任意选定的一组参数,算法 I 产生一个 n 级 M 序列.

2) 过渡状态集 V 共有 $2^{g(n)}$ 个不同选法，其中 $g(n)$ 由式 (1) 和 (2) 给出. 因此算法 I 能用来产生 $2^{g(n)}$ 个 n 级 M 序列.

3) 算法 I 产生一个 n 级 M 序列占用的存储比特数为 $3n + g_1(n)$，其中

$$g_1(n) = \sum_{i=1}^{n-4} \{g(n, i) + [\log i]^+\}, \tag{9}$$

这里，$g(n, i)$ 由 (2) 式给出，$[u]^+$ 表示不小于 u 的最小整数. 每步递推所用的计算主要是 $2n$ 次补轮换以及大约相同数量的长 n 数列的比较.

证. 按照本节开头的讨论，算法 I 中的 1), 2), 3) 检查了 α_j 的下一个状态 α_{j+1} 是否属于我们所确定的过渡状态，并根据所得结论分别由 4) 和 5) 算出 a_{j+n}. 因此它产生一个 n 级 M 序列.

2) 因参数组有 $2^{g(n)}$ 个不同选法，不同参数组对应不同的 V. 故 V 也有 $2^{g(n)}$ 个不同选法. 又因属于 V 的过渡状态以 0 开头，不属于 V 的过渡状态以 1 开头. 故同一个状态不可能在这组参数是属于 V 的过渡状态而换一组参数又是不属于 V 的过渡状态. 因此不同 V 产生不同的 n 级 M 序列.

3) 可从算法 I 直接看出.

§6. 算法的推广

上节中考虑的过渡状态集 V 可以扩大使它包含更多的过渡状态. 选定 $n-4$ 个常数 h_i, $1 \leqslant h_i \leqslant 2^{g(n,i)}$, $i = 1, 2, \cdots, n-4$. 考虑一个有 $n-4$ 个状态集组成的有序集族 $V = \{V_i, i = 1, 2, \cdots, n-4\}$，其中 $V_i = \{V(i, 1), V(i, 2), \cdots, V(i, h_i)\}$ 为有 h_i 个状态的集合. V_i 中的状态可表示为

$$V(i, l) = T^{-z(i,l)}[\overline{s(i, l)}], \quad 1 \leqslant l \leqslant h_i, \quad 1 \leqslant i \leqslant n-4, \tag{10}$$

状态 $s(i, l)$ 的构造与 (7) 式中 $s(i)$ 的构造完全一样，其中的自由参数 $\{x_j(i, l), j = 1, 2, \cdots, g(n, i)\}$, $l = 1, 2, \cdots, h_i$ 为任选的 h_i 组不同的参数组. $z(i, l)$ 如前可在 $\{0, 1, \cdots, l-1\}$ 中任意取.

以下约定所有 V_i, $i = 1, 2, \cdots, n-4$ 中的状态都称为 V 中的状态，故 V 中共有 $h = \sum_{i=1}^{n-4} h_i$ 个状态.

引理 6. V 中的 h 个状态分别在 h 个不同的 CCR_n 圈上，且这些状态都可用作并圈的过渡状态.

证. 由引理 4 得集 V_i 中的状态所在的 CCR_n 圈与集 V_j 中的状态所在的 CCR_n 圈一定不相同，若 $i \neq j$. 另一方面，因状态 $Ts(i, l)$ 尾上的一个长 $i+2$ 的 0 游程为 $Ts(i, l)$ 所含的唯一的最长游程，因此不同参数组 $\{x_j(i, k), j = 1, 2, \cdots, g(n, i)\}$ 和 $\{x_j(i, l), j = 1, 2, \cdots, g(n, i)\}$ 对应的状态 $s(i, k)$ 和 $s(i, l)$ 也不可能在同一个 CCR_n 圈上. 这就证得引理的前一部分. 引理后一部分仍由引理 4 证得.

根据引理 6，我们可任意选定一组常数 h_i, $1 \leqslant h_i \leqslant 2^{g(n,i)}$, $1 \leqslant i \leqslant n-4$; 对每一 i, 选定 h_i 组不同的参数组 $\{x_j(i, l), j = 1, 2, \cdots, g(n, i)\}$, $l = 1, 2, \cdots, h_i$ 及一组

$x(i, l)$, $l=1, 2, \cdots, h_i$, $i=1, 2, \cdots, n-4$. 将这些参数组对应的V中的状态及其共轭确定为它们所在圈并圈时所用的过渡状态. V以外的过渡状态不变仍用上节所确定的. 这样我们又得到一组可行的并圈所用的过渡状态. 容易看出只要将算法 I 稍作修改,就可适用于这里的情况.

算法 II. 选定一组常数 h_i, $1 \leqslant h_i \leqslant 2^{g(n,i)}$, $i=1, 2, \cdots, n-4$, 选定一个V并存储V中状态的所有参数组. 给定初始值 $\alpha_0=(0, 0, \cdots, 0)=(0^n)$. 由已知的 $\alpha_j=(a_j, a_{j+1}, \cdots, a_{j+n-1})$ 计算 a_{j+n} 如下:

1) 若 $a_{j+1}=0$, 置 $\alpha_j^*=(a_{j+1}, \cdots, a_{i+n-1}, 1)$. 算出 $i=L(C)-2$, 其中C为 α_j^* 所在的 CCR_n 圈. 若 $i=0$, 转到5); 否则,若 $\alpha_j^* \in V_i$, 转到 4); 若 $\alpha_j^* \notin V_i$, 转到 5).

2), 3), 4) 5) 同算法 I.

定理 4. 1) 对任意选定的一组常数及 V, 算法II产生一个 n 级M序列.

2) 对选定的一组常数 $h_i, i=1,2,\cdots n\text{-}4, V$ 有

$$G(n)=\prod_{i=1}^{n-4} i\binom{2^{g(n,i)}}{h_i} \tag{11}$$

个不同选法,故算法 II 可用来产生 $G(n)$ 个不同的 n 级M序列.

3) 对不同的常数组选定的V一定不同,故产生的 n 级M序列也不同.

4) 算法 II 产生一个 n 级M序列占用的存储比特数为 $3n+g_2(n)$, 其中

$$g_2(n)=\sum_{i=1}^{n-4} h_i\{g(n,i)+[\log i]^+\}. \tag{12}$$

每步递推所用的计算主要是 $2n$ 次补轮换以及大约 $2n+h_{\max}n$ 次长 n 数列的比较, 其中

$$h_{\max}=\max_{1\leqslant i\leqslant n-4} h_i.$$

证. 与定理 3 的证法相同.

显然算法 I 是算法 II 的特殊情形,即当常数组取为 $h_i=1$, $i=1, 2, \cdots, n-4$ 时算法 II 化为算法 I. 比较定理 3 和定理 4 可见, 算法 II 能产生更多的M序列, 但它的性能 (算法能产生的M序列的个数的对数与产生一个M序列占用的存储比特数之比以及每步递推所用的计算时间)较算法 I 有所降低. 但当 h_i 取得很小时,性能降低是不多的.

此外V还可能有其它形式的扩大,这里就不多讨论了.

参 考 文 献

[1] 万哲先,戴宗铎,刘木兰,冯绪宁,非线性移位寄存器,科学出版社, 1978.
[2] 高鸿勋,求全部n级M序列及其反馈函数的一个方法与证明,应用数学学报, 2:4(1979), 316—324.
[3] 冯克勤,纯轮换与补轮换因子关联图的特性,应用数学学报, 5:1(1982), 1—14.
[4] 康庆德, $GF(2)$ 上M序列的构造方法,通信学报, 4:4(1983), 2—10.
[5] 康庆德, CCR_n 及 PCR_n 因子关联图中的重边,应用数学学报, 9:3(1986), 352—369.
[6] 熊荣华,M序列反馈函数的构造方法 I, 应用数学学报, 9:2(1986), 227—236.
[7] 熊荣华, M序列反馈函数的构造方法 II, 应用数学学报, 9:3(1986), 339—351.
[8] Fredricksen, H., A survey of full length non-linear shift register cycle algorithms, *SIAM Review*, **24**: 2 (1982), 195—221.
[9] Fredricksen, H., A class of non-linear de Bruijn cycles, *J. Comb. Theory, Ser. A*, **19**: 2 (1975), 192—199.

[10] Etzion, T., Lempel, A., Algorithms for the generation of full-length shift-register sequences, *IEEE Trans. Information Theory*, IT-**30**, 3 (1984), 480—484.
[11] Golomb, S. W., Shift Register Sequences, San Francisco: Holden-Day, 1967.

A RECURSIVE ALGORITHM FOR THE GENERATION OF DE BRUIJN SEQUENCES

ZHANG ZHAO-ZHI LUO QIAO-LIN
(Institute of Systems Science, Academia Sinica)

ABSTRACT

A recursive algorithm is presented for the generation of de Bruijn sequences. The algorithm is based on a method of joining the CCR_n cycles together to form a full cycle. It generates $2^{g(n)}$de Bruijin sequences of span n, using about $3n+g(n)$ bits of strorage for each sequence. The time required for producing the next bit from the last n bits is close to $2n$ units.