第 22 卷 第 1 期
2000 年 1 月

电 子 科 学 学 刊
JOURNAL OF ELECTRONICS

Vol.22 No.1
Jan. 2000

De Bruijn 序列的升元算法 [1]

朱士信

(合肥工业大学应用数学系 合肥 230009)

摘 要 本文给出一种 de Bruijn 序列的升元算法. 该算法每步运算可生成一列元素而不是一个元素, 因而减少了运算次数, 加快了生成速度.

关键词 移位寄存器序列, de Bruijn 序列, 循环圈

中图号 TN911.22, O157.4

1 引 言

De Bruijn 序列是一类最重要的非线性移位寄存器序列. 它在密码、通信和天文测距等领域内有着非常广泛的应用, 因此如何有效地生成这类序列是一个有着实际意义的研究问题. 由于二元数域上运算的特殊性, 目前已经有大量产生二元 n 级 de Bruijn 序列的生成算法 [1−4] . 但由于一般的有限域上、特别是整环环 Z_k 上运算的复杂性, 上述生成二元 n 级 de Bruijn 序列的丰富算法几乎不能推广成产生 k 元 n 级 de Bruijn 序列的生成算法. 因此目前仅有为数不多的几个产生 k 元 n 级 de Bruijn 序列的生成算法 [5−7] . 为了能够将各种各样的产生二元 n 级 de Bruijn 序列的算法直接应用于多元 de Bruijn 序列的构造过程中, 本文首次提出 de Bruijn 序列的升元算法, 即从 m 元 n 级 de Bruijn 序列生成 $k(k > m \geq 2)$ 元 n 级 de Bruijn 序列的生成算法.

在本文中, 我们先定义一个算子, 并由该算子产生所有循环圈, 再并置这些循环圈的周期约化, 给出一个产生 k 元 n 级 de Bruijn 序列的生成算法, 进而给出一个从 m 元 n 级 de Bruijn 序列生成 k 元 n 级 de Bruijn 序列的升元算法. 该升元算法从一个给定的 m 元 n 级 de Bruijn 序列生成 $\prod_{i=m}^{k-1}[(i-1)!]^{t_i}$ 个 k 元 n 级 de Bruijn 序列, 其中 $t_i = \sum_{j=1}^{n} i^{n-j-1}$, $k > m \geq 2$. 该升元算法生成一个 k 元 n 级 de Bruijn 序列所占用的存储比特数约为 kn , 每步运算所用时间约为 $O(n)$ 单位; 而且该算法每步运算可产生一列元素, 而不象文献 [1—5] 中的算法每步运算都只产生一个元素, 因而该算法减少了运算次数, 加快了生成速度.

2 基本理论

记 $Z_k = \{0, 1, \cdots, k-1\}$, $Z_k^n = \{A = a_1a_2\cdots a_n | a_i \in Z_k,\ i = 1, 2, \cdots, n\}$, 并称 $A = a_1a_2\cdots a_n \in Z_k^n$ 为一个 n 级状态, 简称状态. 如果 $a_i > b_i$, 则称状态 $A = a_1a_2\cdots a_n$ 大于状态 $B = a_1a_2\cdots a_{i-1}b_i\cdots b_n$. 如果一个状态是另一个状态的循环移动, 则称它们相互等价, 如 $A_i = a_ia_{i+1}\cdots a_na_1a_2\cdots a_{i-1}$, $(i = 1, 2, \cdots, n)$ 是相互等价的, 并称任一状态所在的等价类为一个循环圈. 用每个等价类中的最大状态表示其所在的循环圈, 因此状态 $A = a_1a_2\cdots a_n$ 代表一个循环圈的充要条件为 $A \geq a_ja_{j+1}\cdots a_na_1a_2\cdots a_{j-1}$, $j = 1, 2, \cdots, n$. 设 $A = a_1a_2\cdots a_n$ 为一个循环圈, 令

$$p = \min\{r | A = (a_1a_2\cdots a_r)^{n/r},\ r\text{为自然数},\},$$

[1] 1998-04-21 收到, 1999-01-28 定稿
原机械部基金资助项目

其中 $(a_1a_2\cdots a_r)^{n/r}$ 表示 $a_1a_2\cdots a_r$ 重复 n/r 次，则称循环圈 A 的长度为 p，并称 $A'=a_1a_2\cdots a_r$ 为 A 的周期约化. 如果 $p<n$，则称 A 为可约循环圈；否则称 A 为不可约循环圈，如 $A=3332$ 是长度为 4 的不可约循环圈，$B=(31)^2=3131$ 是长度为 2 的可约循环圈，且 B 的周期约化为 $B'=31$.

定义 1　若 $a_i>a_{i+1}=a_{i+2}=\cdots=a_n=0$，则定义算子 T 的运算如下：

$$T(a_1a_2\cdots a_n)=[(a_1a_2\cdots a_{i-1}(a_i-1)]^r a_1a_2\cdots a_s,$$

其中 $n=ri+s$, r, s 为非负整数，且 $0\le s<i$.

引理 1[7]　设 $A=a_1a_2\cdots a_n$ 为任一 n 级状态，则 (1) $A>T(A)$. (2) 在 $T(A)$ 与 A 之间不存在循环圈.

设 A 是循环圈，B 是小于 A 的最大循环圈，则称 B 是 A 的后继，记为 $F(A)$，则 $F(A)=T^l(A)$，其中 l 是使得 $T^l(A)$ 为循环圈的最小自然数. 显然，$(k-1)^n$ 与 0^n 分别是 Z_k^n 上最大与最小的循环圈. 若 A 为 Z_k^n 上的任一循环圈，且 $0^n\le A\le(k-1)^n$，由引理 1 知，一定存在自然数 l 使得 $A=T^l(k-1)^n$. 因此可利用算子 T，从 $(k-1)^n$ 开始能够生成 Z_k^n 上所有循环圈.

设 $a=a_1a_2\cdots a_r$ 和 $b=b_1b_2\cdots b_s$ 分别是长为 r 和 s 的两个序列，定义 a 和 b 的并置 ab 是一个长为 $r+s$ 的序列 $a_1a_2\cdots a_rb_1b_2\cdots b_s$.

算法 1　取初始循环圈为 $(k-1)^n$，生成其周期约化 $k-1$；再并置 $(k-1)^n$ 的后继循环圈 $T(k-1)^n=(k-1)^{n-1}(k-2)$ 的周期约化 $(k-1)^{n-1}(k-2)$；假设已并置循环圈 A 的周期约化，下一步再并置 A 的后继 $T(A)$ 的周期约化，直到并置 0^n 的周期约化 0 为止.

引理 2[7]　算法 1 产生的序列是一个长为 k^n 的 k 元 n 级 de Bruijn 序列.

3　De Bruijn 序列的升元算法

本节将给出 de Bruijn 序列的升元算法. 先观察下面一个具体例子.

例 1　取 $k=n=4$，则由算子 T 生成 Z_4^4 上所有循环圈如下：

3333	3332	3331	3330	3322	3321	3320	3312	3311	3310
3302	3301	3300	3232	3231	3230	3222	3221	3220	3212
3211	3210	3202	3201	3200	3131	3130	3122	3121	3120
3112	3111	3110	3102	3101	3100	3030	3022	3021	3020
3012	3011	3010	3002	3001	3000	2222	2221	2220	2211
2210	2201	2200	2121	2120	2111	2110	2101	2100	2020
2011	2010	2001	2000	1111	1110	1100	1010	1000	0000

由算法 1 产生的 4 元 4 级 de Bruijn 序列为

3|3332|3331|3330|3322|3321|3320|3312|3311|3310|3302|
3301|3300|32|3231|3230|3222|3221|3220|3212|3211|3210|
3302|3301|3200|31|3130|3122|3121|3120|3112|3111|3110|
3102|3101|3100|30|3022|3021|3020|3012|3011|3010|3002|
3001|3000|2|2221|2220|2211|2210|2201|2200|21|2120|
2111|2110|2101|2100|20|2011|2010|2001|2000|1|1110|1100|10|1000|.

其中每条竖线表示并置符号.

在上例的 de Bruijn 序列中，若从循环圈 $1^4=1111$ 的周期约化 1 前截断，到循环圈 0^4 的周期约化 0 为止，则得到一个 2 元 4 级 de Bruijn 序列如下： 1111011001010000；若从循环圈 2^n 的周期约化前截断，到循环圈 0^4 的周期约化 0 为止，则得到一个 3 元 4 级 de Bruijn 序列如下：

22221222022112210220122002121202111211021012100202011201020012000111101100101000 0.

更一般地，若从循环圈的 $(m-1)^n$ 的周期约化 $m-1$ 前截断，到循环圈 0^n 的周期约化 0 为止，则得到一个 m 元 n 级的 de Bruijn 序列，其中， $m=2,3,\cdots,k$. 反之，利用算法 1 可给出一个产生 de Bruijn 序列的升元算法。

为了从一个给定的 m 元 n 级 de Bruijn 序列可产生大量的 k 元 n 级 de Bruijn 序列，我们先给出如下引理.

引理 3 对给定的 $a_1a_2\cdots a_{n-1}$，设 $i=\max\{j|a_1a_2\cdots a_{n-1}j$ 为不可约循环圈 $\}$，若 $i\neq 0$, 则

(1) $a_1a_2\cdots a_{n-1}(i-1), a_1a_2\cdots a_{n-1}(i-2),\cdots, a_1a_2\cdots a_{n-1}0$ 都是不可约循环圈;

(2) 两个序列： $S=s_1a_1a_2\cdots, a_{n-1}ia_1a_2\cdots a_{n-1}(i-1)\cdots a_1a_2a_n\cdots a_{n-1}0s_2$ 和 $S=s_1a_1a_2\cdots a_{n-1}r_1a_1a_2\cdots a_{n-1}r_2\cdots a_1a_2\cdots a_{n-1}r_ia_1a_2\cdots a_{n-1}0s_2$ 含有完全相同的 n 级状态，其中 $(r_1,r_2,\cdots,r_i)$ 是 $1,2,\cdots,i$ 的任一排列， s_1 和 s_2 为任意序列.

证明 (1) 由于 $A=a_1a_2\cdots a_{n-1}i$ 是循环圈， $i\neq 0$，根据循环圈的定义知， $T^j(A)=a_1a_2\cdots a_{n-1}(i-j)$ 是循环圈，下面证明它们都是不可约的， $j=1,2,\cdots,i$.

假设 $T^j(A)=a_1a_2\cdots a_{n-1}(i-j)$ 是可约循环圈，即 $T^j(A)=a_1a_2\cdots a_{n-1}(i-j)=(a_1a_2\cdots a_r)^{n/r}$, 且 $n/r>1$，则 $A=a_1a_2\cdots a_{n-1}i=(a_1a_2\cdots a_r)^{n/r-1}a_1a_2\cdots a_{r-1}(a_r+j)$，显然 $a_1a_2\cdots a_{r-1}(a_r+j)(a_1a_2\cdots a_r)^{n/r-1}>(a_1a_2\cdots a_r)^{n/r-1}a_1a_2\cdots a_{r-1}(a_r+j)=A$，此与 A 是循环圈矛盾，因而 $a_1a_2\cdots a_{n-1}(i-j)$ 是不可约循环圈， $j=1,2,\cdots,i$.

(2) 显然两个序列 S 和 S' 所含的 n 级状态是完全相同的.

综合上述讨论，下面给出 de Bruijn 序列的升元算法.

算法 2 设 $(m-1)^ns_1s_2\cdots s_{m^n-2n}0^n$ 是一个 m 元 n 级的 de Bruijn 序列， $k>m$. 在序列后并置循环圈 $(k-1)^n$ 的周期约化 $k-1$；假设 A 是已被并置其周期约化的循环圈中的最小者，且 $(k-1)^n\geq A>(m-1)^n$ ，下步算法如下：

(1) 若 $A=(m0^{n-1})$ ，则停止。

(2) 计算 $T(A),T^2(A),\cdots$, 直到 $T^l(A)$ 是循环圈，即 l 是使 $T^l(A)=b_1b_2\cdots b_n$ 为循环圈的最小自然数，若 $T^l(A)$ 可约，或 $b_n=0$ ，则并置 $T^l(A)$ 的周期约化.

(3) 记 $b_n=i\neq 0$ ，任取 $1,2,\cdots,i$ 的一个排列 $(r_1,r_2,\cdots,r_i)$ ，并置 $b_1b_2\cdots b_{n-1}r_1b_1b_2\cdots b_{n-1}r_2\cdots b_1b_2\cdots b_{n-1}r_ib_1b_2\cdots b_{n-1}0$.

为了画算法 2 的算法框图方便起见，给出如下约定：设 A 是引理 3 中的不可约循环圈，即 $A=a_1a_2\cdots a_{n-1}i$ ，对给定的 $1,2,\cdots,r$ 的任一排列 $(r_1,r_2,\cdots,r_i)$ ，称引理 3(2) 中子序列 $a_1a_2\cdots a_{n-1}r_1a_1a_2\cdots a_{n-1}r_2\cdots a_1a_2\cdots a_{n-1}r_ia_1a_2\cdots a_{n-1}0$ 为 A 的一个完全子序列，显然 A 有 $i!$ 个不同的完全子序列. 图 1 是算法 2 的算法框图.

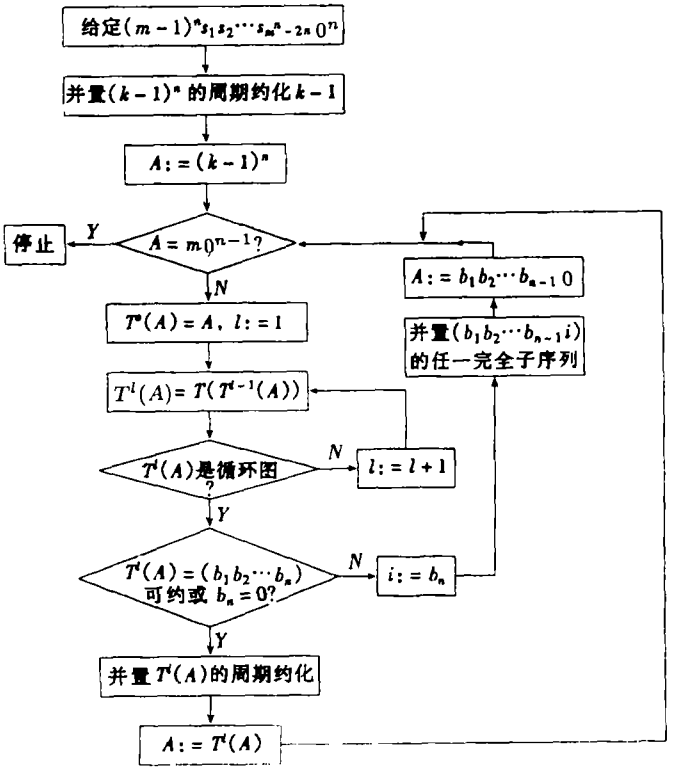

图 1

定理 1　算法 2 从一个给定的 m 元 n 级 de Bruijn 序列至少可产生 $\prod_{i=m}^{k-1}[(i-1)!]^{t_i}$ 个 k 元 n 级 de Bruijn 序列，其中 $t_i=\sum_{j=1}^{n} i^{n-j-1}$.

证明　(1) 对任意 n 级状态 $A=(a_1,a_2,\cdots,a_n)$，令 $a=\max\{a_1,a_2,\cdots,a_n\}$. 当 $m\le a\le k-1$ 时，由引理 2 知，状态 A 在算法 2 所生成的那段序列中出现且仅出现一次；当 $0\le a\le m-1$ 时，由于 $(m-1)^n s_1 s_2\cdots s_{m^n-2n}0^n$ 是 m 元 n 级 de Bruijn 序列，因此 A 在其中出现仅出现一次. 因此算法 2 产生的序列为 k 元 n 级 de Bruijn 序列.

(2) 任取 $i, i=m,m+1,\cdots,k-1$，当 $a_1,a_2,\cdots,a_{n-j-1}$ 取小于 i 的任何值时，$i^j a_1 a_2\cdots a_{n-j-1}(1)$ 是不可约循环圈，因此共有 i^{n-j-1} 个形如 $i^j a_1 a_2\cdots a_{n-j-1}(i-1)$ 的不可约循环圈，其中 $j=1,2,\cdots,n-1$. 故共有 $t_i=\sum_{j=1}^{n} i^{n-j-1}$ 个形如上述形式的不可约循环圈. 由算法 2 知，由于 $i^j a_1 a_2\cdots a_{n-j-1}(i-1)$ 是不可约循环圈，因此，不可约循环圈 $i^j a_1 a_2\cdots a_{n-j-1}(i-1)$，$i^j a_1 a_2\cdots a_{n-j-1}(i-2)$，$\cdots$，$i^j a_1 a_2\cdots a_{n-j-1}1$ 之间的顺序可任意排列，又由于根据不同排列顺序所产生的 de Bruijn 序列不等价，因此，对每一个形如 $i^j a_1 a_2\cdots a_{n-j-1}(i-1)$ 的不可约循环圈，算法 2 可产生 $(i-1)!$ 个不等价的 de Bruijn 序列. 故根据 t_i 个形如 $i^j a_1 a_2\cdots a_{n-j-1}(i-1)$ 的不可约循环圈，算法 2 可产生 $\prod_{i=m}^{k-1}[(i-1)!]^{t_i}$ 个不等价的 k 元 n 级 de Bruijn 序列. 由于存在不同于 $i^j a_1 a_2\cdots a_{n-j-1}(i-1)$ 的不可约循环圈 (如 303002)，因此，算法 2 至少可产生 $\prod_{i=m}^{k-1}[(i-1)!]^{t_i}$ 个不等价的 k 元 n 级 de Bruijn 序列.

例 2　设 $S=2^4 a_1 a_2\cdots a_{3^4-8}0^4$ 是任一给定的 3 元 4 级 de Bruijn 序列，则由算法 2 可生

成 $\prod_{i=3}^{3}[(i-1)!]^{t_i}=(2!)^{3^2+3+1}=2^{13}$ 个平移不等价的 4 元 4 级 de Bruijn 序列如下：

$$2222a_1a_2\cdots a_{73}0000|3|\underline{3332|3331}|3330|\underline{3322|3321}|3320|\underline{3312|3311}|$$
$$3310|\underline{3302|3301}|3300|32|3231|3230|\underline{3222|3221}|3220|\underline{3212|3211}|3210|$$
$$\underline{3202|3201}|3200|31|3130|\underline{3122|3121}|3120|\underline{3112|3111}|3110|\underline{3102|3101}|$$
$$3100|30|\underline{3022|3021}|3020|\underline{3012|3011}|3010|\underline{3002|3001}|3000.$$

其中两相邻的不可约循环圈下方的横线表示这两个循环圈可交换顺序。因为有 13 对不可约循环圈可交换顺序，故共可产生 2^{13} 个 4 元 4 级 de Bruijn 序列。

4 结 论

算法 2 不仅具备运算简单以及所需存储空间小等优点，而且每步运算可产生一列元素，其中最多时一步可产生 $[(k-1)n]$ 个元素，且仅有 k 步产生一个元素，因而减少了运算次数，加快了生成速度。

参 考 文 献

[1] Fredricksen H. A survey of full length nonlinear shift-register cycle algorithms. SIAM Review, 1982, 24(2): 195-221.

[2] Yan Junhui. Constructing the Hamilton cycle on r-ary de Bruijn sequences. Systems Science and Mathematical Sciences, 1991, 4(1): 32-40.

[3] 章照业，罗乔林. 产生 M 序列的一个递推算法. 系统科学与数学， 1987, 7(4): 335-343.

[4] 朱士信. 产生二元 de Bruijn 序列的一个新算法. 高校应用数学学报， 1993, 8(3): 308-313.

[5] 熊荣华. 生成 Q 元 M 序列的理论和算法. 中国科学， A 辑， 1988, 31(8): 877-886.

[6] 朱士信. 产生 k 元 M 序列的一种新算法. 电子科学学刊， 1993, 15(5): 523-526.

[7] 朱士信. 一种快速生成 k 元 de Bruijn 序列的算法. 电子科学学刊， 1995, 17(6): 618-622.

AN ALGORITHM FOR GENERATING DE BRUIJN SEQUENCES BY RAISING ELEMENTS

Zhu Shixin

(*Department of Applied Mathematics, Hefei University of Technology, Hefei* 230009)

Abstract An algorithm for generating k-ary de Bruijn sequences from m-ary de Bruijn sequences is given in this paper. Its each operational step produces a string of elements instead of one element. Hence the algorithm reduces the time of operation, and accelerates the speed of generation.

Key words Shift register sequence, De Bruijn sequence, Cycle

朱士信： 男， 1962 年生，教授，从事代数编码、密码以及代数学等相关领域的教学和科研工作.