第17卷 第6期　　电子科学学刊　　Vol. 17 No. 6
1995年11月　　JOURNAL OF ELECTRONICS　　Nov. 1995

一种快速生成 k 元 de Bruijn 序列的算法*

朱士信
（合肥工业大学应用数学系，合肥　230009）

摘要　De Bruijn 序列是一类最重要的非线性移位寄存器序列. 本文通过并置所有循环圈的周期约化，提出了一个新的生成 k 元 de Bruijn 序列的算法. 该算法每步运算可生成一列元素而不是一个元素，因此减少了运算次数，加快了生成速度.

关键词　移位寄存器，De Bruijn 序列，循环圈

1 引　言

De Bruijn 序列是一类最长的非线性移位寄存器序列，它在密码学及电讯学等领域中有广泛的应用，因而如何有效地构造 de Bruijn 序列是一个有意义的问题. 通常的构造方法是先由某一移位寄存器生成很多短圈，再将所有的短圈合并成全长圈，进而得到一个 de Bruijn 序列. 本文提出了一个完全不同的构造方法，该算法不仅具有文献[1—8]中算法所具有的容易实现的特点，而且每步运算可生成一列元素，而不象文献[1—8]中算法每次只生成一个元素. 因而减少了运算次数，加快了生成速度.

2 基本原理算法

对任意自然数 $k, k\geqslant 2$，令 $Z_k=\{0,1,\cdots,k-1\}$，$Z_k^n=\{A=a_1a_2\cdots a_n \mid a_i\in Z_k, i=1,2,\cdots,n\}$. 若 $A\in Z_k^n$，称 A 为一个 n 级状态. 若 $a_i>b_i$，称 $A=a_1a_2\cdots a_n> B=a_1\cdots a_{i-1}b_i\cdots b_n$. 若 A 是 B 的循环移动，则称 A 与 B 等价，并称任一状态所在的等价类为一个循环圈. 若状态 A 在循环圈 σ 所代表的等价类中，则称 A 在 σ 上，并用 σ 上的最小状态表示 σ，即状态 $A=a_1a_2\cdots a_n$ 代表其所在的循环圈，当且仅当

$$A\leqslant c_ja_{j+1}\cdots a_na_1a_2\cdots a_{j-1},\ j=1,2,\cdots,n.$$

定义 1　在状态 $A=a_1a_2\cdots a_n$ 中，如果 $a_j<a_{j+1}=a_{j+2}=\cdots=a_n=k-1$，则定义 $T(A)=[a_1\cdots a_{j-1}(a_j+1)]^r a_1a_2\cdots a_s$，其中 $n=rj+s$，r 和 s 都是非负整数，且 $0\leqslant s<j$，B^t 表示连续 t 段元素都是 B.

定义 2　设 $A=a_1a_2\cdots a_n$ 为一循环圈，令 $p=\mathrm{Min}\{r \mid A=(a_1a_2\cdots a_r)^{n/r}, r$ 为自然数$\}$，称 p 为圈 A 的长度，$a_1a_2\cdots a_r$ 为 A 的周期约化，记为 A'，即 $A'=a_1a_2\cdots a_r$.

1994-03-26 收到，1994-08-29 定稿
* 合肥工业大学科研基金资助项目

朱士信　男，1962年出生，副教授，现主要从事代数编码理论及移位寄存器序列理论的研究，特别是 de Bruijn 序列的构造方法及复杂性的研究.

如果 $p < n$，称 A 为可约循环圈；否则，称 A 为不可约循环圈。

引理 1　设 $A = a_1a_2\cdots a_n$ 为任一状态，则

(1) $A < T(A)$；

(2) 在 A 与 $T(A)$ 之间不存在循环圈；

(3) 若 A 为循环圈，且 $a_n \neq k-1$，则 $T^i(A) = a_1a_2\cdots a_{n-1}(a_n+i)$ 为不可约循环圈，$i = 1,2,\cdots,k-a_n-1$。

证明　(1) 由定义立即可得。

(2) 若 $a_n \neq k-1$，则 $T(A) = a_1a_2\cdots a_{n-1}(a_n+1)$，显然在 A 与 $T(A)$ 之间不存在循环圈；若 $a_j < a_{j+1} = a_{j+2} = \cdots = a_n = k-1$，假设存在循环圈 $B = b_1b_2\cdots b_n$ 使 $A < B \leqslant T(A)$，即 $a_1a_2\cdots a_n < b_1b_2\cdots b_n \leqslant [a_1\cdots a_{j-1}(a_j+1)]^r a_1\ a_2\cdots a_s$，其中 $n = rj+s$，$0 \leqslant s < j$，则 $b_i = a_i$，$i = 1,2,\cdots,j-1$，$b_j = a_j+1$。因为 B 是循环圈，故 $b_1b_2\cdots b_n \leqslant b_{j+1}\cdots b_nb_1b_2\cdots b_j$，则 $b_{j+1} \geqslant b_1 = a_1$；又 B 与 $A(T)$ 的前 j 个分量相同，它们的第 $j+1$ 个分量分别为 b_{j+1} 及 a_1，由 $B \leqslant T(A)$ 得，$b_{j+1} \leqslant a_1$。因此 $b_{j+1} = a_1$。同理可得，$b_{j_t+i} = a_i$，$i=1,2,\cdots,j-1$，$b_{j_t} = a_j+1$，即 $B = T(A)$。因此在 A 与 $T(A)$ 之间不存在循环圈。

(3) 由于 A 为循环圈，且 $a_n \neq k-1$，则 $T^i(A) = a_1a_2\cdots a_{n-1}(a_n+i)$，显然，$T^i(A)$ 为循环圈；如果 $T^i(A)$ 可约，即 $T^i(A) = (a_1a_2\cdots a_r)^{n/r}$，$n/r > 1$，则 $a_r = a_n + i$，从而 $A = [a_1\cdots a_{r-1}(a_n+i)]^{n/r-1}a_1\cdots a_{r-1}a_n$，此与 A 是循环圈相矛盾；故 $T^i(A)$ 不可约。

易知，0^n 及 $(k-1)^n$ 都是循环圈。若 A 为任一循环圈，且 $0^n < A \leqslant (k-1)^n$，由引理 1 知，一定存在自然数 l 使得 $A = T^l(0^n)$。因此，可利用算子 T 列出介于 0^n 与 $(k-1)^n$ 之间的所有循环圈的一个单调上升的序列。

设 $S_1 = a_1a_2\cdots a_r$ 和 $S_2 = b_1b_2\cdots b_t$ 分别是长为 r 和 t 的两个序列，定义 S_1 与 S_2 的并置 S_1S_2 是一个长为 $r+t$ 的序列 $a_1a_2\cdots a_rb_1b_2\cdots b_t$。

算法 1　(1) 列一个循环圈序列，序列中第一个循环圈为 0^n；如果 A 是序列中的第 i 个循环圈，则第 $i+1$ 个循环圈为 $T^l(A)$，其中 l 是使得 $T^l(A)$ 为循环圈的最小自然数；序列中最后一个循环圈为 $(k-1)^n$；

(2) 按(1)中循环圈的顺序，并置所有循环圈的周期约化，形成一个 k 元序列。

例 1　在 $n=4, k=3$ 时，由算法1(1)可得循环圈的升列如下：

0000	0001	0002	0011	0012	0021	0022	0101
0102	0111	0112	0121	0122	0202	0211	0212
0221	0222	1111	1112	1122	1212	1222	2222

由算法1(2)得一个长为 3^4 的 3 元序列如下：

0|0001|0002|0011|0012|0021|0022|01|0102|0111|0112|

0121|0122|02|0211|0212|0221|0222|1|1112|1122|12|1222|2

其中每条竖线表示并置运算，可略去。显然，这是一个 3 元 4 级的 de Bruijn 序列。更一般地有：

定理 1　算法1(2)产生的序列为 k 元 n 级的 de Bruijn 序列。

证明　设 S 是算法1(2)产生的序列，下面分两步证明 S 是一个 k 元 n 级 de Bruijn

序列。

(1) 证明 S 的长度为 k^n. 记 k 元 n 级纯轮换移位寄存器的状态图为 G_n，易知，由算法1(1)产生的所有循环圈恰好是 G_n 中的所有圈. 由定义2知，每个循环圈的长度等于该循环圈上所含状态个数，而所有循环圈(即 G_n 中的所有圈)上所含状态的个数之和为 k^n. 又 S 是所有循环圈的周期约化的并置，故其长度为 k^n.

(2) 证明任一 n 级状态恰好在 S 中出现一次. 这等价于证明每一循环圈上的每一状态(共计 k^n 个)都在 S 中出现. 下面分四步证明.

(I) 若 $A=(a_1a_2\cdots a_p)^{n/p}$ 是循环圈，$a_j<a_{j+1}=a_{j+2}=\cdots=a_p=k-1$，则 $B=(a_1a_2\cdots a_p)^{n/p-1}a_1\cdots a_{j-1}(k-1)^{p-j+1}$ 也是循环圈. 而 A 的下一个循环圈 $T^l(A)$(以下简称为 A 的后继)是大于 A 的最小循环圈，即 $A<T^l(A)\leqslant B$，因此，$T^l(A)=(a_1a_2\cdots a_p)^{n/p-1}a_1\cdots a_{j-1}b_j\cdots b_p$.

(II) 设循环圈 $A\neq(k-1)^n$，B 是 A 的后继，则 $A'B'=AC$，其中 A' 为 A 的周期约化，C 为一序列. 事实上，若 $A'=A$，结论显然；若 $A'\neq A$，设 $A=(a_1a_2\cdots a_p)^{n/p}$，$n/p>1$，$a_j<a_{j+1}=a_{j+2}=\cdots=a_p=k-1$，由(I)知，$B=T^l(A)=(a_1a_2\cdots a_p)^{n/p-1}a_1\cdots a_{j-1}b_j\cdots b_p$. 显然 B 不可约，即 $B'=B$，故 $A'B'=Aa_1\cdots a_{j-1}b_j\cdots b_p$.

(III) 如果 A 是可约循环圈，下面证明 A 上每个状态在 S 中出现. 设 $A=(a_1a_2\cdots a_p)^{n/p}$，$n/p>1$.

(a) 若 $p=1$，当 $a_1\neq k-1$ 时，A 的后继 $B=a_1^{n-1}(a_1+1)$，则 $A'B'=a_1^n(a_1+1)=A(a_1+1)$；当 $a_1=k-1$ 时，A 是循环圈 $C=(k-2)(k-1)^{n-1}$ 的后继，则 $C'A'=(k-2)(k-1)^n=(k-2)A$；即 $p=1$ 时，A 上的唯一一个状态 a_1^n 出现在 S 中.

(b) 若 $p>1$，设 $a_j<a_{j+1}=\cdots=a_p=k-1$，则 $j\geqslant 1$(否则 $A=(k-1)^n$，即 $p=1$)，由(I)知，A 的后继 $B=(a_1a_2\cdots a_p)^{n/p-1}a_1\cdots a_{j-1}b_j\cdots b_p$，且 B 不可约；由算法1(1)知，A 是 $C=a_1a_2\cdots a_{p-1}(a_p-1)(k-1)^{n-p}$ 的后继，显然，C 不可约. 因此 $C'A'B'$ 含有子序列 $(k-1)^{n-p}(a_1a_2\cdots a_p)^{n/p}a_1a_2\cdots a_{j-1}$，则 A 上的 p 个不同状态全部在该子序列中出现，因而也在 S 中出现.

(IV) 如果 A 是不可约循环圈，下面证明 A 上每个状态在 S 中出现. 设 $A=a_1a_2\cdots a_n$，若 $a_n\neq k-1$，由引理1(3)知，A 的后继 $B=a_1a_2\cdots a_{n-1}(a_n+1)$ 不可约，因此 $A'B'=a_1a_2\cdots a_na_1a_2\cdots a_{n-1}(a_n+1)$，此时 A 上每个状态在 $A'B'$ 中出现，因而在 S 中出现. 若 $a_j<a_{j+1}=a_{j+2}=\cdots=a_n=k-1$，由(I)得，$A$ 的后继 $B=a_1a_2\cdots a_{j-1}b_j\cdots b_n$. 下面分两步证明 $A=a_1a_2\cdots a_j(k-1)^{n-j}$ 上的每个状态在 S 中出现.

(a) 证明循环圈 A 上的状态 $A_i=a_ia_{i+1}\cdots a_na_1\cdots a_{i-1}$ 在 S 中出现，$i=1,2,\cdots,j$. 若 $B\neq(k-1)^n$，设 B 的后继为 C，由(II)知，$B'C'=BD$，D 为一序列. 显然 A_i 出现在 $A'B'C'=a_1a_2\cdots a_na_1\cdots a_{j-1}b_j\cdots b_nD$ 中，因而 A_i 出现在 S 中；若 $B=(k-1)^n$，则 $A=(k-2)(k-1)^{n-1}$，此时 $j=1$，$A_1=A=A'$，故结论也成立.

(b) 证明 A 上的状态 $B_i=(k-1)^{n-j-i}a_1a_2\cdots a_j(k-1)^i$ 出现在 S 中，$i=0,1,\cdots,j-1$. 设 r_1 是使得 $a_1a_2\cdots a_j(k-1)^i=(a_1a_2\cdots a_{r_1})^{t_1}a_1a_2\cdots a_{s_1}$ 成立的最小自然数，$0\leqslant t_1<r_1$. 当 $r_1=1$ 且 $a_1=0$ 时，$t_1=0$，因而 $i=0$，故 $a_1a_2\cdots a_j(k-1)^i=0^{i+j}=$

0^j,此时 $B_0=(k-1)^{n-j}0^j$,由于 S 的最后及最前 n 个分量分别为 $(k-1)^n$ 及 0^n,且 S 是周期序列，故 $B_0=(k-1)^{n-j}0^j$ 出现在 S 中．当 $r_1\neq 1$ 或 $a_1\neq 0$ 时，则 $a_{r_1}\neq 0$ (否则，$a_{r_1}a_1a_2\cdots a_{r_1-1}<a_1a_2\cdots a_{r_1}$，此与 A 是循环圈矛盾)．令 $N_1=a_1a_2\cdots a_{r_1-1}(a_{r_1}-1)(k-1)^{n-r_1}$,如果 N_1 不是循环圈，设 r_2 是使得 $N_1=(a_1a_2\cdots a_{r_2})^{t_2}a_1a_2\cdots a_{t_2}$ 成立的最小自然数，$t_2<r_2$,令 $N_2=a_1a_2\cdots a_{r_2-1}(a_{r_2}-1)(k-1)^{n-r_2}$,如果 N_2 不是循环圈,重复上述步骤，直到 $N_h=a_1a_2\cdots a_{r_h-1}(a_{r_h}-1)(k-1)^{n-r_h}$ 是循环圈．由于 $T(N_h)=N_{h-1},\cdots,\ T(N_2)=N_1,\ T(N_1)=(a_1a_2\cdots a_{r_1})^{t_1}a_1a_2\cdots a_tb_1b_2\cdots b_{n-j-i}$，其中 T 是定义 1 中的算子．设 P 是 N_h 的后继,则 $P>T(N_1)$,又 $a_1a_2\cdots a_j(k-1)^{n-j}$ 为循环圈,且比 P 小,故 $P=a_1a_2\cdots a_j(k-1)^ic_1c_2\cdots c_{n-j-i}$．设 P 的后继为 Q,由 (II) 知，$P'Q'=PR$，R 为一段序列．又 $r_h\leqslant r_{h-1}\leqslant\cdots\leqslant r_2\leqslant r_1\leqslant j+i$，故 $n-r_h\geqslant n-i-j$，而 $N'_hP'Q'$ 必含有 $(k-1)^{n-r_h}P$,从而必含有 $(k-1)^{n-i-j}a_1a_2\cdots a_j(k-1)^i$，即 B_i 出现在 $N'_hP'Q'$ 中,从而出现在 S 中．

综上所述,序列 S 为 k 元 n 级 de Bruijn 序列．

由算法 1 及定理 1 可立即得到一个生成 k 元 n 级 de Bruijn 序列的递归算法如下：

算法 2　取初值 0^n,在 0^n 的周期约化后并置 0^n 的后继 $0^{n-1}1$ 的周期约化;设已并置循环圈 $A=a_ia_{i+1}\cdots a_{i+n-1}$ 的周期约化 A',下一步递归并置运算如下：

(1) 若 $a_{i+n-1}=j\neq k-1$，则依次并置 $k-j-1$ 个不可约循环圈的周期约化 $a_ia_{i+1}\cdots a_{i+n-2}(j+1),\ a_ia_{i+1}\cdots a_{i+n-2}(j+2),\cdots,a_ia_{i+1}\cdots a_{i+n-2}(k-1)$；

(2) 若 $a_{i+n-1}=k-1$，如果 $A=(k-1)^n$，停止；否则，依次计算 $T(A)$，$T^2(A),\cdots$,直到 $T^l(A)$,其中 l 是使得 $T^l(A)$ 为循环圈的最小自然数，并置 $T(A)$ 的周期约化．

3 总　　结

我们通过定义循环圈和产生循环圈的算子 T，给出了产生 de Bruijn 序列的一个新的算法．该算法不仅同文献[1—8]中算法一样，具有产生一个 k 元 n 级 de Bruijn 序列所要占用的存储比特数小和每一步运算所要进行的时间少的特点，而且每步运算可产生一列元素，而文献[1—8]中算法每步运算仅产生一个元素，因而该算法减少了运算次数，加速了生成速度．因此该算法不仅具有一定的理论意义，更重要的是有较高的实用价值．

参　考　文　献

[1] Etzion T. J. Algorithms, 1986, 7(2): 331—340.
[2] Yan Junhui, Systems Science and Mathematical Science, 1991, 4(1): 32—40.
[3] Fredricksen H. SIAM Review, 1982, 24(2):195—221.
[4] 高鸿勋．应用数学学报，1979，2(4)：316—324．
[5] 章照止，罗乔林．系统科学与数学，1987，7：355—343．
[6] 熊荣华．中国科学，A 辑，1988，31(8)：877—886．
[7] 朱士信．电子科学学刊，1993，15(5)：523—526．
[8] 朱士信．高校应用数学学报，1993，8(3)：308—313．

A FAST ALGORITHM FOR THE GENERATION OF k-ARY DE BRUIJN SEQUENCES

Zhu Shixin

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

Abstract De Bruijn sequences are highly important nonlinear shift register sequences. This paper presents a new algorithm for the generation of k-ary de Bruijn sequences by juxtaposing the periodic reductions of the necklaces. Its each 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, De Bruijn sequence, Necklace