第15卷 第2期 电子科学学刊 Vol. 15, No. 2
1993年3月 JOURNAL OF ELECTRONICS Mar., 1993

De Bruijn 序列的 k 次齐次复杂度*

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. 本文定义并研究了 n 级 De Bruijn 序列的 k 次齐次复杂度 $C_k(s)$，给出了 $C_k(s)$ 的一个上界. $k=1$ 及 $k=2$ 时，$C_k(s)$ 分别为人们所熟知的线性复杂度及二次齐次复杂度.

关键词 De Bruijn 序列;齐次复杂度;矩阵;矩阵的秩

1. 引言

De Bruijn 序列是一类最重要的非线性移位寄存器序列，它在通信及密码等领域内有极广泛的应用. 复杂度是刻划这类序列特性的一个重要概念. 文献[1—4]对二元 De Bruijn 序列的线性复杂度作了全面的研究. 文献[5]对其二次齐次复杂度进行了初步讨论. 本文定义并研究二元 n 级 De Bruijn 序列的 k 次齐次复杂度，k 为自然数，且 $1\leqslant k\leqslant n$. $k=1$ 时，它即为线性复杂度，$k>1$ 时，它是一个非线性问题. 本文利用非线性问题线性化的方法，得到了 De Bruijn 序列 k 次齐次复杂度的一个上界，并指出某些序列的 k 次齐次复杂度能达到这一上界.

2. 基本概念

定义 1 如果 n 级反馈函数 $f(x_0,x_1,\cdots,x_{n-1})$ 能表成如下形式:

$$f(x_0,x_1,\cdots,x_{n-1})=\sum_{0\leqslant i_1\leqslant\cdots\leqslant i_{k-1}\leqslant n-1} a_{i_1\cdots i_k}x_{i_1}\cdots x_{i_k} \tag{1}$$

则称 $f(x_0,x_1,\cdots,x_{n-1})$ 为 n 级 k 次齐次函数。

由于在 $F_2=\{0,1\}$ 中 $x^2=x$，故当 $i_1=i_2=\cdots=i_r$ 时，简记 $a_{i_1\cdots i_k}x_{i_1}\cdots x_{i_k}$ 为 $a_{i_1 i_{r+1}\cdots i_k}x_{i_1}x_{i_{r+1}}\cdots x_{i_k}$，$r\leqslant k$. 因此，(1)式可表为

$$f(x_0,x_1,\cdots,x_{n-1})=\sum_{i=0}^{n-1}a_ix_i+\sum_{0\leqslant i_1<i_2\leqslant n-1}a_{i_1i_2}x_{i_1}x_{i_2}+\cdots+\sum_{0\leqslant i_1<\cdots<i_k\leqslant n-1}a_{i_1\cdots i_k}x_{i_1}\cdots x_{i_k}$$

当 $k=1$ 及 $k=2$ 时，$f(x_0,x_1,\cdots,x_{n-1})$ 分别为文献[1—5]中所讨论的情形.

两个序列的加法及乘法分别定义为同位分量相加及连乘. 设 $s=\{s_0,s_1,\cdots,s_{p-1},\cdots\}$ 是周期为 p 的序列，N 为一自然数，E 为序列的平移算子. 记 $s^N=\{s_0,s_1,\cdots,$

1991.10.07 收到，1992.03.09 定稿.
* 信息安全国家重点实验室基金和合肥工业大学科研基金资助项目.

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.

$s_{N-1}\}$，$E^i s=\{s_i, s_{i+1}, \cdots, s_{p-1}, s_0, \cdots, s_{i-1}, \cdots\}$，$(E^{i_1}\cdot E^{i_2}\cdot\cdots\cdot E^{i_k})s=E^{i_1}s\cdot E^{i_2}s\cdot\cdots\cdot E^{i_k}s$。注意：$(E^{i_1}\cdot E^{i_2})s\neq E^{i_1+i_2}s$。若 s 是由 k 次齐次函数 $f(s_0, s_1, \cdots, s_{n-1})$ 生成的，则 $s_{i+n}=f(s_i, s_{i+1}, \cdots, s_{i+n-1})$，$i=0,1,2,\cdots$ 可改写为

$$\sum_{i=0}^{n-1} a_i E^{i} + \sum_{0\leqslant i_1<i_2\leqslant n-1} a_{i_1i_2}(E^{i_1}\cdot E^{i_2})s+\cdots+\sum_{0\leqslant i_1<\cdots<i_k} \cdot a_{i_1i_2\cdots i_k}(E^{i_1}\cdot E^{i_2}\cdot\cdots\cdot E^{i_k})s=E^n s \qquad (2)$$

对给定的周期为 N 的序列 $s=\{s_0, s_1, \cdots, s_{N-1}, \cdots\}$ 构造一个 $(N-n)\times(C_n^1+C_n^2+\cdots+C_n^k)$ 矩阵 $M_k(N,n)$ 为：$M_k(N,n)$ 的第一列到第 n 列分别为 s^{N-n}，$(Es)^{N-n},\cdots,(E^{n-1}s)^{N-n}$；第 $n+1$ 列到第 $C_n^1+C_n^2$ 列为 $[(E^{i_1}\cdot E^{i_2})s]^{N-n}$，$0\leqslant i_1<i_2\leqslant n-1$，且当 $(i_1,i_2)<(j_1,j_2)$（按字典排列法比较）时 $[(E^{i_1}\cdot E^{i_2})s]^{N-n}$ 在 $[(E^{j_1}\cdot E^{j_2})s]^{N-n}$ 之前；…；第 $(C_n^1+C_n^2+\cdots+C_n^{k-1})+1$ 列到第 $(C_n^1+C_n^2+\cdots+C_n^k)$ 列为 $[(E^{i_1}\cdot E^{i_2}\cdot\cdots\cdot E^{i_k})s]^{N-n}$，$0\leqslant i_1<i_2<\cdots<i_k\leqslant n-1$，顺序与上相同。

再构造一个 $(C_n^1+C_n^2+\cdots+C_n^k)$ 维的列向量 $A(k,n)$，其转置 $A'(k,n)=(a_0, a_1,\cdots,a_{n-1},a_{01},a_{02},\cdots a_{0(n-1)},a_{12},a_{13},\cdots,a_{1(n-1)},\cdots,a_{(n-2)(n-1)},\cdots,a_{12\cdots k},\cdots,a_{1\cdots k-1,k+1},\cdots,a_{1\cdots k-1,n-1},\cdots,a_{n-k,n-k+1,\cdots,n-1}$

例 1 设 $s=\{s_0,s_1,\cdots,s_7\}$，$n=k=3$，则

$$M_3(8,3)=\begin{pmatrix} s_0 & s_1 & s_2 & s_0s_1 & s_0s_2 & s_1s_2 & s_0s_1s_2\\ s_1 & s_2 & s_3 & s_1s_2 & s_1s_3 & s_2s_3 & s_1s_2s_3\\ s_2 & s_3 & s_4 & s_2s_3 & s_2s_4 & s_3s_4 & s_2s_3s_4\\ s_3 & s_4 & s_5 & s_3s_4 & s_3s_5 & s_4s_5 & s_3s_4s_5\\ s_4 & s_5 & s_6 & s_4s_5 & s_4s_6 & s_5s_6 & s_4s_5s_6 \end{pmatrix}$$

$$A'(3,3)=(a_0,a_1,a_2,a_{01},a_{02},a_{12},a_{012})$$

引理 1 给定 $s=\{s_0,s_1,\cdots,s_{N-1}\}$，则存在 n 级 k 次齐次函数生成 s 的充要条件是存在 $A(k,n)$ 使得 $M_k(N,n)A(k,n)=(E^ns)^{N-n}$ 成立。

证明 存在 $A(k,n)$ 使得 $M_k(N,n)A(k,n)=(E^ns)^{N-n}$ 成立，等价于 $A(k,n)$ 满足(2)式，从而等价于存在 n 级 k 次齐次函数生成 s。

定义 2 称所有能生成序列 $s=\{s_0,s_1,\cdots,s_{N-1}\}$ 的 k 次齐次函数中最小的级数 n 为序列 s 的 k 次齐次复杂度，记为 $C_k(s)$。

显然，若存在 $(C_n^1+C_n^2+\cdots+C_n^k)$ 维列向量 $A(k,n)$ 使得 $M_k(N,n)A(k,n)=(E^ns)^{N-n}$ 成立，则 $C_k(s)\leqslant n$。

由于 $k=1$ 的情形在文献[1—4]中已经得到广泛的研究，故本文设 $k>1$。

3. De Bruijn 序列的 k 次齐次复杂度

设 s 是 n 级 De Bruijn 序列，$M_k(2^n+l,l)$ 为与 s 相应的 $[2^n\times(C_l^1+C_l^2+\cdots+C_l^k)]$ 矩阵，因此，$M_k(2^n+l,l)$ 中每个线性列 E^is 是 s 的一个周期，$i=0,1,\cdots,l-1$。易知，$C_k(s)=\min\{l|(E^ls)^{2^n}$ 是 $M_k(2^n+l,l)$ 中所有列的线性组合$\}$

引理 2 设 s 是 n 级 De Bruijn 序列，则 $M_k(2^n+n,n)$ 中的所有列向量线性无关，即 $M_k(2^n+n,n)$ 的秩 $R(M_k(2^n+n,n))=C_n^1+C_n^2+\cdots+C_n^k$，$2\leqslant k\leqslant n$。

证明 将 $M_k(2^n+n,n)$ 分成分块矩阵 $(M_1,M_2,\cdots,M_k)$，其中 M_i 是 $M_k(2^n+$

n,n）中的 i 次齐次（$E^{i_1}\cdot E^{i_2}\cdot\cdots\cdot E^{i_i}$）$s$ 组成的 $2^n\times C_n^i$ 子矩阵，由于 s 是 n 级 De Bruijn 序列,因此可对 $M_k(2^n+n,n)$ 进行适当的初等行对换，可将它等价地变为如下形式:

$$\begin{pmatrix} E_{n\times n} & & & & \\ * & E_{C_n^2\times C_n^2} & & & \\ * & * & E_{C_n^3\times C_n^3} & & \\ \cdots & \cdots & \cdots & \ddots & \\ * & * & * & \cdots & D_{C_n^k\times C_n^k} \\ * & * & * & \cdots & * \end{pmatrix}$$

其中 $E_{C_n^i\times C_n^i}$ 是 C_n^i 阶单位方阵，$i=1,\cdots,k$，$E_{C_n^i\times C_n^i}$ 的上方全为 0,故

$$R(M_k(2^n+n,n))=C_n^1+C_n^2+\cdots+C_n^k$$

引理 3 设 $n\geqslant 3$，若 $f(x_0,x_1,\cdots,x_{n-1})=x_0+f_0(x_1,\cdots,x_{n-1})$ 产生 n 级 De Bruijn 序,则 $x_1x_2\cdots x_{n-1}$ 在 $f_0(x_1,\cdots,x_{n-1})$ 中一定出现。

证明 参见文献[6]中74页定理 1。

引理 4 设 s 是 n 级 De Bruijn 序列，$2\leqslant k\leqslant n-2$，则

$$R[M_k(2^n+n+1,n+1)]\geqslant C_n^1+C_n^2+\cdots+C_n^k+2,\quad n\geqslant 3.$$

证明 由于 $M_k(2^n+n,n)$ 中的 $C_n^1+C_n^2+\cdots+C_n^k$ 个列向量全是 $M_k(2^n+n+1,n+1)$ 中的列向量,下面只须证明这些列向量与 E^ns 及（$E^0\cdot E^n$）s 构成（$C_n^1+C_n^2+\cdots+C_n^k+2$ 个线性无关向量。否则，存在一组不全为 0 的数 $a_{i_1i_2\cdots i_k}\in F_2$ 使下式成立:

$$\sum_{i=0}^{n}a_iE^is+\sum_{0\leqslant i_1<i_2\leqslant n-1}a_{i_1i_2}(E^{i_1}\cdot E^{i_2})s+\cdots+\sum_{0\leqslant i_1<i_2<\cdots<i_k\leqslant n-1}a_{i_1i_2\cdots i_k}\cdot(E^{i_1}\cdot E^{i_2}\cdot\cdots\cdot E^{i_k})s+a_{0n}(E^0\cdot E^n)s=0 \tag{3}$$

由于 $n+1$ 维向量$(0,\cdots,0,1)$及$(1,0,\cdots,0)$分别满足(3)式。分别将它们代入(3)式，可得 $a_0=a_n=0$。又由于 $M_k(2^n+n,n)$ 中的列向量组线性无关，故 $a_{0n}\neq 0$，即 $a_{0n}=1$。设 s 是 n 级反馈函数(不一定是齐次的) $f(x_0,x_1,\cdots,x_{n-1})=x_0+f_0(x_1,\cdots,x_{n-1})$ 生成的，故对任意 $(x_1,x_2,\cdots,x_{n-1})\in F_2^{n-1}$，$(1,x_1,x_2,\cdots,x_{n-1},x_n)$ 必满足(3)式。其中 $x_n=1+f_0(x_1,\cdots,x_{n-1})$，代入(3)式,即可得

$$f_0(x_1,\cdots,x_{n-1})=1+\sum_{i=1}^{n-1}a_ix_i+\cdots+\sum_{0\leqslant i_1<\cdots<i_k\leqslant n-1}a_{i_1\cdots i_k}x_{i_1}\cdots x_{i_k}$$

当 $i_1=0$ 时，$x_{i_1}=x_0=1$。由于 $k\leqslant n-2$，故在 $f_0(x_1,\cdots,x_{n-1})$ 中 $x_1x_2\cdots x_{n-1}$ 这一项一定不出现,从而与引理 3 矛盾。故得证。

注 引理 4 对 $k=n$ 时,结论不成立;对 $k=n-1$，结论是否成立,将有待于研究。

定理 1 设 $n\geqslant 3$，s 是 n 级 De Bruijn 序列,则

(1) 当 $2\leqslant k\leqslant n-2$ 时，$C_k(s)\leqslant 2^n-(C_n^2+C_n^3+\cdots+C_n^k)-1$;

(2) $C_{n-1}(s)\leqslant 2^n-(C_n^2+C_n^3+\cdots+C_n^{n-1})=n+2$

(3) $C_n(s)=n+1$

证明　显然，$C_k(s) \geqslant n+1$，$k=2,3,\cdots,n$。

(1) 由于 $C_k(s) \geqslant n+1$，故 $M_k(2^n+n+1, n+1)$ 中所有列向量全是 $B = M_k(2^n + C_k(s), C_k(s))$ 中的列向量，根据引理 4，可设 $\alpha_1,\alpha_2,\cdots,\alpha_t$ 是 $M_k(2^n+n+1,n+1)$ 中的 t 个线性无关的列向量，其中 $t = C_n^1 + C_n^2 + \cdots + C_n^k + 2$，记 B 中的线性列向量 $E^i s$ 为 α_{t+i-n}，$i=n+1,n+2,\cdots,C_k(s)-1$。下面证明 $\alpha_1,\alpha_2,\cdots,\alpha_{t+C_k(s)-n-1}$ 线性无关。否则，令

$$t_0 = \max\{i \mid \alpha_{t+i-n} \text{ 能表为 } \alpha_1,\alpha_2,\cdots,\alpha_{t+i-n-1} \text{ 的线性组合}, i=n+1,n+2,\cdots, C_k(s)-1\}$$

则 $E^{t_0}s$ 能表为 $M_k(2^n+C_k(s), C_k(s))$ 中某些列向量的线性组合，故 s 的 k 次齐次复杂度最多为 t_0，与 s 的 k 次齐次复杂度为 $C_k(s)$ 矛盾。故 $\alpha_1,\alpha_2,\cdots,\alpha_{t+C_k(s)-n-1}$ 线性无关。又 B 的行数为 2^n，故

$$2^n \geqslant R(B) \geqslant t + C_k(s) - n - 1 = C_n^1 + C_n^2 + \cdots + C_n^k + C_k(s) - n + 1$$

即 $C_k(s) \leqslant 2^n - (C_n^2 + C_n^3 + \cdots + C_n^k) - 1$。

(2) 完全类似于(1)中证明可证：$M_k(2^n+n,n)$ 中的所有列向量与 $M_k(2^n+C_k(s), C_k(s))$ 中的线性列向量 $E^n s, E^{n+1}s,\cdots,E^{C_k(s)-1}s$ 构成线性无关向量组，故 $C_k(s) \leqslant 2^n - (C_n^2+\cdots+C_n^k)$，$1 \leqslant k \leqslant n$，从而 $C_{n-1}(s) \leqslant n+2$。

(3) 由于 $C_k(s) \leqslant 2^n - (C_n^2 + \cdots + C_n^k)$ 及 $C_n(s) \geqslant n+1$，故 $C_n(s) = n+1$。证毕。

显然，定理 1 中的(1)对 $k=1$ 时也成立，即文献[1]中的结论在本文中得到了进一步推广；而文献[5]中的结论是本文的特例。但本文给出的 $C_k(s)$ 的上界是否都是可达到的，有待于进一步研究；目前，我们只能对一些简单情形验证它们是可达的。如 $s=0000111101011001$ 时，$C_2(s)=9$。

参　考　文　献

[1] A. H. Chan et al., *J. Combin Theory*, Series A, **33**(1982)3, 233—246.

[2] L. E. Key, *IEEE Trans. on IT*, **IT-22**(1976)6, 732—736.

[3] A. H. Chan et al., *IEEE Trans. on IT*, **IT-36**(1990)3, 640—644.

[4] T. Etzion et al., *IEEE Trans. on IT*, **IT-30**(1984)5, 705—709.

[5] A. H. Chan et al., *IEEE Trans. on IT*, **IT-36**(1990)4, 822—829.

[6] 万哲先，刘木兰，代宗铎，冯绪宁，非线性移位寄存器，科学出版社，北京，1978 年，第 73—77 页。

THE HOMOGENEOUS COMPLEXITY OF DEGREE k OF DE BRUIJN SEQUENCES

Zhu Shixin

(Hefei University of Technology, Hefei　230009)

Abstract　De Bruijn sequences are highly important nonlinear shift register sequences. The homogeneous complexity $C_k(\varepsilon)$ of degree K of a De Bruijn sequence ε is defined and discussed. Its upper bound is given. The linear complexity and the quadratic complexity are special cases of $C_k(\varepsilon)$ for $k=1$ and $k=2$ respectively.

Key words　De Bruijn sequences; Homogeneous complexity of degree k; Matrix; Rank of matrix