k 元 de Bruijn 序列的反馈函数的一个升级算法

朱士信, 孙 琳
(合肥工业大学应用数学系, 安徽合肥 230009)

摘 要: 本文定义了 k 个从 k 元 n 级 de Bruijn-Good 图到 k 元 n - 1 级 de Bruijn-Good 图的满同态映射 D_a, 利用这些同态映射, 我们证明了 n 级非奇反馈函数 $f(x_1, x_2, \cdots, x_n)$ 与以 $D_a(G_f)$ 为状态图的 n - 1 级非奇反馈函数 $g(x_1, x_2, \cdots, x_{n-1})$ 的一个关系定理, 给出了 k 元 de Bruijn 序列的反馈函数的一个升级算法, 特别当 k = 2, a = 0 时, 利用映射 D 在 $\mathbf{Z}_2$ 上运算的简单性, 本文给出了一个从 2 元 n - 2^r 级 de Bruijn 序列反馈函数直接生成 2 元 n 级 de Bruijn 序列的反馈函数的有效算法.

关键词: de Bruijn-Good 图; de Bruijn 序列; 同态映射; 非奇反馈函数
中图分类号: TN911 文献标识码: A 文章编号: 0372-2112 (2006) 06-1066-03

An Algorithm for Generating Feedback Functions of *k*-ary De Bruijn Sequences by Raising Stage

ZHU Shi-xin, SUN Lin
(Department of Applied Mathematics, Hefei University of Technology, Hefei, Anhui 230009, China)

Abstract: k homomorphic mappings from k-ary n-stage de Bruijn-Good graph onto k-ary (n - 1)-stage de Bruijn-Good graph are defined. By using the homomorphic mappings, we prove a relational theorem between n-stage nonsingular feedback function $f(x_1, x_2, \cdots, x_n)$ and (n - 1)-stage nonsingular feedback function $g(x_1, x_2, \cdots, x_{n-1})$, whose state graph is $D_a(G_f)$, and give an algorithm for generating k-ary feedback functions of n-stage de Bruijn sequences from those of (n - 1)-stage de Bruijn sequences. In particular, when k = 2 and a = 0, by using the simplicity of mapping D over $\mathbf{Z}_2$, we give an effictive algorithm for generating n-stage feedback functions of de Bruijn sequences from (n - 2^r)-stage the feedback functions, where r is a nature number.

Key words: de Bruijn-Good praph; de Bruijn sequence; homomophic mapping; nonsingular feedback function

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 F_2 的运算的简单性, 目前已有大量产生二元 de-Bruijn 序列的生成算法, 如文献[1~3]. 但由于一般的有限域和环 $\mathbf{Z}_k$ 上运算的复杂性, 目前仅有为数不多的几个产生 k 元 de Bruijn 序列的生成算法[4~6]. 为了将产生二元 de Bruijn 序列的丰富算法应用于产生 k 元 de Bruijn 序列, 文献[7]给出了 de Bruijn 的升元算法. 由于文献[1~6]中所有算法都是直接产生 n 级 de Bruijn 序列, 即便是文献[7]中的升元算法, 也是从 n 级二元 de Bruijn 序列产生 n 级 k 元 de Bruijn 序列, 在 n 较大时, 上述所有算法的计算量仍十分巨大. 因此文献[8, 9]给出了二元 de Bruijn 序列的升级算法, 在已知一个级数较低的二元 de Bruijn 序列的反馈函数的条件下, 这两个算法都可较容易给出一个级数较高的二元 de Bruijn 序列的反馈函数, 因此这两个算法有实际应用价值.

本文定义了 k 个从 k 元 n 级 de Bruijn-Good 图到 k 元 n - 1 级 de Bruijn-Good 图的满同态映射, 利用这些映射, 我们给出了一个产生 k 元 de Bruijn 序列的升级算法, 该算法能从一个 n - 1 级 k 元 de Bruijn 序列的反馈函数直接生成 k 个 k 元 n 级 de Bruijn 序列的反馈函数; 进而给出了一个从 2 元 n - 2^r 级 de Bruijn 序列反馈函数直接生成 2 元 n 级 de Bruijn 序列的反馈函数的有效算法.

2 同态及其性质

设 k 为大于 1 的自然数, 记 $\mathbf{Z}_k = \{0, 1, 2, \cdots, k-1\}$, $\mathbf{Z}_k^n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in \mathbf{Z}_k, i = 1, 2, \cdots, n\}$. 称由 k^n 个顶点 $(a_1, a_2, \cdots, a_n) \in \mathbf{Z}_k^n$ 及 k^{n+1} 条有向弧 $(a_1, a_2, \cdots, a_n) \rightarrow (a_2, a_3, \cdots, a_{n+1})$ 组成的有向图为 k 元 n 级 de Bruijn-Good 图, 记为 G_n. 并称 $(a_1, a_2, \cdots, a_n)$ 是 $(a_2, a_3, \cdots, a_{n+1})$ 的一个先导状态, $(a_2, a_3, \cdots, a_{n+1})$ 是 $(a_1, a_2, \cdots, a_n)$ 的一个后继状态, $(b_1, a_2, \cdots, a_n)$ 与 $(b_2, a_2, \cdots, a_n)$ 为共轭状态, 其中 $b_1 \neq b_2$. 如果从 G_n 到 G_{n-1} 的映射 f 满足:

收稿日期: 2004-09-28; 修回日期: 2005-12-01
基金项目: 安徽省自然科学基金项目(No. 03042203)

当 A 是B 在 G_n 中的后继状态时, f(A) 是 f(B) 在 G_{n-1} 中的后继状态,则称 f 是 G_n 到 G_{n-1} 的同态映射,简称同态.

对 $\forall(a_1, a_2, \cdots, a_n) \in \mathbf{Z}_k^n$, $\forall a \in \mathbf{Z}_k$, 定义 G_n 到 G_{n-1} 的映射 D_a 如下:

$$D_a(a_1, a_2, \cdots, a_n) = (a_2 - a_1 + a, a_3 - a_2 + a, \cdots, a_n - a_{r-1} + a)$$

由定义立即可得下述结论:

引理1　对 $\forall a \in \mathbf{Z}_k$, 映射 D_a 都是 G_n 到 G_{n-1} 的满同态;且对 $\forall B = (b_1, b_2, \cdots, b_n) \in G_{n-1}$, 则在 G_n 中恰好有 k 个状态 $A_j = (j, j + b_1 - a, j + b_1 + b_2 - 2a, \cdots, j + b_1 + b_2 + \cdots + b_{r-1} - (n-1)a)$ 满足 $D_a(A_j) = B$, $j = 0, 1, \cdots, k-1$.

称满足引理1中的同态映射为 $k-1$ 同态. 设 $C = a_1 a_2 \cdots a_t \cdots$ 为一个周期为 t 的n 级移位寄存器序列, 记它在 G_n 中对应的圈为 $C = [a_1, a_2, \cdots, a_t]$, 并称圈 C 上所含不同状态的个数t 为圈长. 称 $W(C) = a_1 + a_2 + \cdots + a_t \pmod k$ 为圈 $C = [a_1, a_2, \cdots, a_t]$ 的分类重量. 当 $k = 2$ 时, $W(C) = 0$ 或 1 分别是指圈 C 的 Hamming 重量为偶数和奇数.

引理2　设 $C_1 = [a_1 a_2 \cdots a_{k^{r-1}}]$ 是 G_{n-1} 中圈长为 k^{n-1} 的极大圈,则在 G_n 中恰好有 k 个长为 k^{n-1} 的两两无公共顶点的对偶圈

$$P_jC = [j, j + a_1 - a, j + a_1 + a_2 - 2a, \cdots, j + a_1 + a_2 + \cdots + a_{k^{n-1}-1} - (k^{r-1} - 1)a]$$

满足 $D_a(P_jC) = C_1$, $j = 0, 1, \cdots, k-1$.

证明　由于 C_1 是 C_{n-1} 中圈长为 k^{n-1} 的极大圈, 故 $a_1 + a_2 + \cdots + a_{k^{n-1}} \equiv 0 \pmod k$, 即

$$a_{k^{n-1}} = -(a_1 + a_2 + \cdots + a_{k^{n-1}-1}) \pmod k$$

故 $D_a(P_jC) = [a_1, a_2, \cdots, a_{k^{r-1}}] = C_1$, 且容易证明 P_jC 都是 G_n 中长为 k^{r-1} 的圈, $j = 0, 1, \cdots, k-1$. 下面再证明 P_jC 与 $P_{j_1}C$ 没有公共顶点, $j \neq j_1$. 设

$$b = (a_1 + a_2 + \cdots + a_t + j - ta, a_1 + a_2 + \cdots + a_{t+1} + j - (t+1)a, \cdots, a_1 + a_2 + \cdots + a_{t+n-1} + j - (t+n-1)a) \in P_jC$$

$$c = (a_1 + a_2 + \cdots + a_s + j_1 - sa, a_1 + a_2 + \cdots + a_{s+1} + j_1 - (s+1)a, \cdots, a_1 + a_2 + \cdots + a_{s+n-1} + j_1 - (s+n-1)a) \in P_{j_1}C$$

如果 $s = t$, 则显然有 $b \neq c$. 假设 $b = c$, 则 $s \neq t$. 不妨设 $k^{n-1} \geqslant t > s \geqslant 1$, 则可得方程组

$$\begin{cases} a_{s+1} + \cdots + a_t + j - j_1 - (t-s)a = 0 \\ a_{s+2} + \cdots + a_{t+1} + j - j_1 - (t-s)a = 0 \\ \cdots\cdots \\ a_{s+n} + \cdots + a_{t+n-1} + j - j_1 - (t-s)a = 0 \end{cases}$$

解得 $a_{s+1} = a_{t+1}, \cdots, a_{s+2} = a_{t+2}, a_{s+n-1} = a_{t+n-1}$.

即 $(a_{s+1}, a_{s+2}, \cdots, a_{s+n-1}) = (a_{t+1}, a_{t+2}, \cdots, a_{t+n-1})$. 此与 C_1 是极大圈矛盾, 故 P_jC 与 $P_{j_1}C$ 没有公共顶点. 再根据 D_a 是 $k-1$ 同态知,在 G_n 中恰好有 k 个长为 k^{n-1} 的两两无公共顶点的对偶圈 P_jC 使 $D_a(P_jC) = C_1$, $j = 0, 1, \cdots, k-1$.

当 $k = 2$ 时, 由于 C_{r-1} 中圈长为 2^{r-1} 的极大圈 C_1 的 Hamming 重量为偶数, 故由文献[10]知, 在 G_n 中恰有 2 个圈长为 2^{r-1} 的两两无公共顶点的对偶圈 $P_j(C)$ 满足 $D_a(P_jC) = C_{1+j}$, $j = 0, 1$. 因此, 本引理是文献[10]的结论的推广.

引理3　设以 $f(x_1, x_2, \cdots, x_n)$ 为反馈函数的 n 级非奇移位寄存器的状态图为 G_f, 以 $D_a(G_f)$ 为状态图的 $n-1$ 级非奇移位寄存器的反馈函数为 $g(x_1, x_2, \cdots, x_{n-1})$, 则

$$f(x_1, x_2, \cdots, x_n) = g(a_2 - a_1 + a, a_3 - a_2 + a, \cdots, a_n - a_{n-1} + a) + a_n - a$$

证明　参考文献[10]中 140 页定理 2 的证明.

3　de Bruijn 序列的升级算法

对 $\forall x, y \in \mathbf{Z}_k$, 规定 $x^{(y)} = \begin{cases} 1, x = y \\ 0, x \neq y \end{cases}$, 则对 $\forall a_1, a_2, \cdots, a_n \in \mathbf{Z}_k$, 有 $x_1^{(a_1)} x_2^{(a_2)} \cdots x_n^{(a_n)} = 1$ 的充要条件是 $(x_1, x_2, \cdots, x_n) = (a_1, a_2, \cdots, a_n)$.

引理4　设 G_f 是非奇反馈函数 $f(x_1, x_2, \cdots, x_n)$ 的状态图, σ_1, σ_2 分别是 G_f 中圈长为 l_1, l_2 的两个不同的圈, 如果 $A_j = (b_j, a_2, \cdots, a_n) \in \sigma_j$, $j = 1, 2$, 其中 $b_1 \neq b_2$, 则

$$g(x_1, x_2, \cdots, x_n) = f(x_1, x_2, \cdots, x_n) + (f(A_2) - f(A_1)) \cdot (x_1^{(b_1)} - x_1^{(b_2)}) x_2^{(a_2)} \cdots x_n^{(a_n)}$$

是非奇异的,且 $g(x_1, x_2, \cdots, x_n)$ 将 A_1 与 A_2 在 G_f 中的后继状态互换,并保持其他所有状态的后继不变, 即 $g(x_1, x_2, \cdots, x_n)$ 将 G_f 中的圈 σ_1 与 σ_2 合并成了一个圈长为 $l = l_1 + l_2$ 的圈,并保持其余圈不变.

证明　对 $\forall A \in \mathbf{Z}_k^n$, 如果 $A \neq A_j$, $j = 1, 2$, 则 $(x_1^{(b_1)} - x_1^{(b_2)}) x_2^{(a_2)} \cdots x_n^{(a_n)} = 0$, 故 $g(A) = f(A)$; 又 $g(A_1) = f(A_1) + (f(A_2) - f(A_1)) \cdot 1 = f(A_2)$, 且 $g(A_2) = f(A_2) + (f(A_2) - f(A_1)) \cdot (-1) = f(A_1)$ 即 $g(x_1, x_2, \cdots, x_n)$ 将 A_1 与 A_2 在 G_f 中的后继状态互换, 且保持其他所有状态的后继状态不变, 从而得证引理. 证毕

定理1　设 $n \geqslant 3$, 设 $f_{n-1}(x_1, x_2, \cdots, x_{n-1})$ 是 $n-1$ 级 de Bruijn 序列的反馈函数, 对 $\forall a \in \mathbf{Z}_k$, 则 $f_n(x_1, x_2, \cdots, x_n) = f_{n-1}(x_2 - x_1 + a, x_3 - x_2 + a, \cdots, x_n - x_{r-1} + a) + x_n - a + \sum_{j=1}^{k-2} (f(j-1, j, \cdots, j+n-2) - f(b_j, j, \cdots, j+n-2)) (x_1^{b_j} - x_1^{(j-1)}) x_2^{(j)} x_3^{(j+1)} \cdots x_n^{(n+j-2)}$ 为一个n 级 de Bruijn 序列的反馈函数,

其中 b_1 满足 $f_{n-1}(a+1-b_1, a+1, \cdots, a+1) = a+1$, $b_j = b_1 + j + 1$, $j = 2, 3, \cdots, k-1$.

证明　由于 $f_{n-1}(x_1, x_2, \cdots, x_{n-1})$ 是 $n-1$ 级 de Bruijn 序列的反馈函数, 故其状态图 $G_{f_{r-1}}$ 是 G_{r-1} 中的一个极大圈, 设为 $C_1 = [a_1 a_2 \cdots a_{k^{n-1}}]$, 由引理 2 知, 在 G_n 中恰好有 k 个无公共顶点的长为 k^{n-1} 的对偶圈 $P_jC = [j, j + a_1 - a, j + a_1 + a_2 - 2a, \cdots, j + a_1 + a_2 + \cdots + a_{k^{n-1}-1} - (k^{n-1} - 1)a]$ 满足 $D_a(P_jC) = C_1$, $j = 0, 1, \cdots, k-1$, 则 k 个对偶状态 $A = P_0A = (0, 1, \cdots, n-1)$, $P_1A = (1, 2, \cdots, n)$, $\cdots$, $P_{k-1}A = (k-1, 0, \cdots, n-2)$, 恰好在这 k 个对偶圈上. 不妨设 $A \in P_0C = C$, 则 $P_jA \in P_jC$, $j = 0, 1, \cdots, k-1$.

由引理 3 知, 以 $C, P_1C, \cdots, P_{k-1}C$ 为状态图的非奇反馈

函数为$h(x_1, x_2, \cdots, x_n) = f_{n-1}(x_2 - x_1 + a, x_3 - x_2 + a, \cdots, x_n - x_{n-1} + a) + x_n - a$. 设在圈 P_jC 上$P_jA = (j, j+1, \cdots, j+n-1)$的先导状态为 $A_j = (b_j, j, j+1, \cdots, j+n-2)$, 即 $h(b_j, j, j+1, \cdots, j+n-2) = j+n-1$, 则 $h(b_j, j, j+1, \cdots, j+n-2) = f_{n-1}(j-b_j+a, a+1, a+1, \cdots, a+1) + j+n-2-a = j+n-1$. 从而, $f_{n-1}(j-b_j+a, a+1, a+1, \cdots, a+1) = a+1$. 由于$f_{n-1}(x_1, x_2, \cdots, x_{n-1})$是非奇的, 故$j-b_j+a = j+1-b_{j+1}+a$, 则 $b_j = b_{j+1}-1$, $j = 2, 3, \cdots, k-1$. 其中 $f_{n-1}(a+1-b_1, a+1, a+1, \cdots, a+1) = a+1$.

由于圈 $P_{j-1}C$ 上状态$P_{j-1}A$ 与圈P_jC 上状态A_j 为共轭状态, 故交换 $P_{j-1}A$ 与A_j 的后继, 并保持其他状态后继不变, $j = 1, 2, \cdots, k-1$, 由引理 4 知, 则将圈合 $P_0C, P_1C, \cdots, P_{k-1}C$ 合并成了 G_n 中一个圈长为$k \cdot k^{n-1} = k^n$ 的极大圈, 从而以此圈为状态图的反馈函数 $f_n(x_1, x_2, \cdots, x_n)$产生级 de Bruijn 序列. 且 $f_n(x_1, x_2, \cdots, x_n) = f_{n-1}(x_2 - x_1 + a, x_3 - x_2 + a, \cdots, x_n - x_{n-1} + a) + x_n - a + \sum_{j=1}^{k-2} (f(j-1, j, \cdots, j+n-2) - f(b_j, j, \cdots, j+n-2))(x_1^{b_j} - x_1^{(j-1)}) x_2^{(j)} x_3^{(j+1)} \cdots x_n^{(n+j-2)}$

如果已知一个 $n-1$ 级 de Bruijn 序列的反馈函数 $f_{n-1}(x_1, x_2, \cdots, x_{n-1})$, 对$\forall a \in \mathbf{Z}_k$, 由定理 1 知, 只要由 $f_{n-1}(a+1-b_1, a+1, a+1, \cdots, a+1) = a+1$ 求出b_1, 则可直接写出一个 n 级 de Bruijn 序列的反馈函数. 由于$b_1 \in \mathbf{Z}_k$, 则最多计算 k 次函数值$f_{n-1}(a+1-b_1, a+1, a+1, \cdots, a+1)$便可求出$b_1$. 因此利用定理 1 由一个 $n-1$ 级 de Bruijn 序列的反馈函数, 最多只要 k 次计算便可求出一个n 级 de Bruijn 序列的反馈函数, 因此该算法快速有效. 由于 a 有k 种不同的取值, 故由定理 1 可产生 k 个n 级 de Bruijn 序列的反馈函数. 在 $k=2$, $a=0$ 时, 由于映射 D 的运算的简单性, 下面给出一个 2 元 de Bruijn 序列一个有效的升级算法. 该算法从一个 2 元 $n-2^r$ 级 de Bruijn 序列反馈函数直接生成 2 元 n 级 de Bruijn 序列的反馈函数.

定理 2 设 r 是非负整数, $2^r < n$, 记 $D^i(x_1, x_2, \cdots, x_n) = (t_{i_1}, i_{t_2}, \cdots, i_{t_{i+1}}, i = 0, 1, \cdots, 2^r-1, e_2 \in \mathbf{Z}_2, e_{j+1} = e_j + 1, j = 2, 3, \cdots n-1$. $f_{n-2^r}(x_1, x_2, \cdots, x_{n-2^r})$是 2 元 $n-2^r$ 级 de Bruijn 序列的反馈函数, 则 $f_n(x_1, x_2, \cdots, x_n) = f_{n-2^r}(x_1 + x_{2^r+1}, x_2 + x_{2^r+2}, \cdots, x_{n-2^r} + x_n) + x_{n-2^{r+1}} + \sum_{i=0}^{2^r-1} t_{i_2}^{e_2} t_{i_3}^{e_3} \cdots t_{i_{n-1}}^{e_{n-1}}$ 是 2 元 n 级 de Bruijn 序列反馈函数.

证明 易证得: $D^{2^r}(x_1, x_2, \cdots, x_n) = (x_1 + x_{2^r+1}, x_2 + x_{2^r+2}, \cdots, x_{n-2^r} + x_n)$, 根据定理 1, 用归纳法立即得证定理 2.

根据定理 2, 若 $f_m(x_1, x_2, \cdots, x_n)$是 2 元 m 级 de Bruijn 序列反馈函数, 要构造 2 元 $n = m + 2^r$ 级 de Bruijn 序列反馈函数, 只要计算出 $D^i(x_1, x_2, \cdots, x_n)$, $i = 0, 1, \cdots, 2^r$, 则可直接写出 n 级 de Bruijn 序列反馈函数, 而 $D^i(x_1, x_2, \cdots, x_n)$ 的计算非常简单. 因此, 定理 2 是 2 元 de Bruijn 序列反馈函数的一个有数的升级算法, 最后给一个具体例子: 取 2 元 2 级 de Bruijn 序列反馈函数 $f_2(x_1, x_2) = x_1 + 1$, 取 $r=1$, 由于

$D(x_1, x_2, x_3, x_4) = (x_1 + x_2, x_2 + x_3, x_3 + x_4)$,

$D^2(x_1, x_2, x_3, x_4) = (x_3 + x_1, x_4 + x_2)$,

取 $e_2 = 1$, 则由定理 2 得 4 级 2 元 de Bruijn 序列反馈函数为

$$f_4(x_1, x_2, x_3, x_4) = f_2(x_3 + x_1, x_4 + x_2) + x_3 + x_2\overline{x_3}x_4 + (x_2 + x_3)(\overline{x_3 + x_4}) = \overline{x_1} + x_2 + x_3 + \overline{x_2}x_3\overline{x_4}$$

参考文献:

[1] LEMPEL A. On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers[J]. IEEE Trans Comput, 1970, 19(12): 1204-1209.

[2] FREDRICLSON H. A survey of full cycle algorithms[J]. SIAM Rev, 1982, 24(4): 195-221.

[3] 章照止, 罗乔林. 产生 M 序列的一个递推算法[J]. 系统科学与数学学报, 1987, 7(4): 335-343.
ZHANG Zhao-zhi, LUO Qiao-lin. A recursive algorithm for the generation of de Bruijn sequences[J]. J Sys Sci & Math Scis, 1987, 7(4): 335-343. (in Chinese)

[4] YAN Junhui. Constructing the hamilton cycle on n-ary de bruijn sequences[J]. Sys Sci & Math Scis, 1991, 4(1): 32-40.

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

[6] 朱士信. 一种快速生成k 元 de Bruijn 序列的算法[J]. 电子科学学刊, 1995, 17(6): 618-622.
ZHU Shi-xin. A fast algorithm for the generation of -ary de Bruijn sequences[J]. J Electronics, 1995, 17(6): 618-622. (in Chinese)

[7] 朱士信. de Bruijn 序列的升元算法[J]. 电子科学学刊, 2000, 22(1): 68-72.
ZHU Shi-xin. An algorithm for generating of de Bruijn sequences by raising elements[J]. J Electronics, 2000, 22(1): 68-72. (in Chinese)

[8] ANNEXSTEIN F S. Generating de bruijn sequences: An efficient implementation[J]. IEEE Trans Comput, 1997, 46(2): 198-200.

[9] CHANG T, PARK B, et al. An efficient implementation of the D-homomorphism for generation of de Bruijn sequences[J]. IEEE Trans Inform Th, 1999, 45(4): 1280-1283.

[10] 万哲先, 代宗铎, 等. 非线性移位寄存器序列[M]. 北京: 科学出版社, 1978. 138-139.

作者简介:

朱士信 男, 1962 年 7 月生于安徽省枞阳县. 博士, 教授, 研究方向为代数编码理论和序列密码理论, 发表学术论文 40 多篇.

E-mail: sxinzhu@tom.com