第39卷第6期 中国科学技术大学学报 Vol. 39, No. 6
2009年6月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Jun. 2009

文章编号:0253-2778(2009)06-0594-05

环 F_2+uF_2 上 de Bruijn 序列的一个有效升级算法

张 霞[1],吴 波[2]

(1. 合肥学院数学系,安徽合肥 230022;2. 安徽大学数学与计算科学学院,安徽合肥 230039)

摘要:通过定义环 F_2+uF_2 上的 n 级 de Bruijn-Good 图到 $n-1$ 级 de Bruijn-Good 图的满同态映射 D,证明了一个由环 F_2+uF_2 上 $n-1$ 级 de Bruijn 序列的反馈函数产生 n 级 de Bruijn 序列的反馈函数的升级算法定理;进而利用 D 同态的计算公式给出由 m 级 de Bruijn 序列的反馈函数产生 n 级($m<n$)de Bruijn 序列的一个有效升级算法.

关键词:环 F_2+uF_2;de Bruijn 序列;D 同态;非奇反馈函数

中图分类号:O157.4 **文献标识码**:A

AMS Subject Classification (2000): 94B05

An efficient algorithm for generation of de Bruijn sequences over ring F_2+uF_2 by raising stage

ZHANG Xia[1], WU Bo[2]

(1. *Dept. of Mathematics, Hefei University, Hefei* 230022, *China*; 2. *Dept. of Mathematics, Anhui University, Hefei* 230039, *China*)

Abstract: A sur-homomorphism D from n-stage de Bruijn-Good graph to $(n-1)$-stage de Bruijn-Good graph over ring F_2+uF_2 was defined. It was proved an algorithm for generating n-stage de Bruijn sequences from a given feedback function of $(n-1)$-stage de Bruijn sequences. Furthermore, an efficient algorithm for generating n-stage de Bruijn sequences from a given feedback function of lower m-stage de Bruijn sequences by raising stage was given.

Key words: ring F_2+uF_2; de Bruijn sequences; D-homomorphism; nonsingular feedback function

0 引言

De Bruijn 序列(又称 M 序列)是一类最重要的密钥序列,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实际意义的研究问题.

由于二元数域 F_2 的运算的简单性,已有大量产生二元 de Bruijn 序列的生成算法.以往所有算法都是直接产生 n 级 de Bruijn 序列,文献[1,2]给出了二元 de Bruijn 序列的升级算法,在已知一个低级的二元 de Bruijn 序列的反馈函数的条件下,这两个算法都可较为容易地给出一个高级的二元 de Bruijn 序列的反馈函数,因此这两个算法有实际应用价值.但是由于一般的有限域,特别是环 Z_k 上运算的复杂性,目前仅有为数不多的几个产生的 k 元 de Bruijn 序列的生成算法[3~8].为了将产生二元 de Bruijn 序列的丰富算法应用于产生的 k 元 de Bruijn 序列,文献[6]给出了 de Bruijn 序列的升元算法.文献[8]给出 k 元 $n-1$ 级 de Bruijn 序列到 n 级 de Bruijn 序列的反馈函数的一个升级算法,但是由于

收稿日期:2007-04-15;**修回日期**:2008-03-26

基金项目:国家自然科学基金(60673074),教育部重点科研资助项目和安徽省教育厅自然科学重点项目(KJ2008A140)资助.

作者简介:张霞(通讯作者),女,1972年生,硕士/副教授. 研究方向:有限环上的纠错码理论和序列密码理论. E-mail: zhangxia@hfuu.edu.cn

一般的有限环 Z_k 上运算的复杂性,很难给出一个一般的由低级 de Bruijn 序列生成任意高级 de Bruijn 序列的高效升级算法.

文献[9,10]中引入一种介于环 Z_4 与域 F_4 之间的四元素环 $R=F_2+uF_2$. 关于环 R 本身的结构在文献[9,10]中均有详细描述,它是指剩余类环 $F_2[u]/(u^2)$,其元素分别记为$\{0,1,u,1+u\}$,若将 u 视为 Z_4 环上元素 2,$1+u$ 视为元素 3,则其乘法与 Z_4 环上乘法一致. 若将 u 视为域 $F_4=\{0,1,\beta,\beta^2\}$ 上元素 β,$1+u$ 视为 β^2,则其加法与域 F_4 上加法一致,因而它具有了环 Z_4 与域 F_4 的一些良好性质. 环 R 上的纠错码理论的研究已成为一个新热点.

本文通过定义环 F_2+uF_2 上的 n 级 de Bruijn-Good 图到 $n-1$ 级 de Bruijn-Good 图的满同态映射 D,证明了一个由环 F_2+uF_2 上 $n-1$ 级 de Bruijn 序列的反馈函数产生 n 级 de Bruijn 序列的反馈函数的升级算法定理;进而利用 D 同态的计算公式给出由 m 级 de Bruijn 序列的反馈函数产生 n 级 de Bruijn 序列的一个有效升级算法,这里 $m<n$.

1　环 F_2+uF_2 上的 D 同态及其性质

设 $R=F_2+uF_2=F_2[u]/(u^2)$.

$R^n=\{(a_1,a_2,\cdots,a_n)\mid a_i\in R,i=1,2,\cdots,n\}$.

称由 4^n 个顶点$(a_1,a_2,\cdots,a_n)\in R^n$ 及 4^{n+1}条有向弧 $(a_1,a_2,\cdots,a_n)\to(a_2,a_3,\cdots,a_{n+1})$组成的有向图为 R 上四元 n 级 de Bruijn-Good 图,记为 $G_n(R)$,简记为 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,称$(b_1,a_2,\cdots,a_n)$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: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.

特别说明,本文的运算都指的是环 R 上的运算.

由于环 R 的特征为 2,类似于二元数域 F_2[1]有

引理 1.1　设 k 是 2 的非负方幂,且 $k<n$,则

$$D^k(x_1,x_2,\cdots,x_n)=(x_1+x_{k+1},x_2+x_{k+2},\cdots,x_{n-k}+x_n).$$

由此引理立刻可得 D 同态的快速计算公式:

定理 1.2　令 $r=r_1+r_2+\cdots+r_s(r<n)$,其中 r_j 为 2 的非负方幂. 定义

$$E_i(x_{j_1}+x_{j_2}+\cdots)=x_{j_1}+x_{j_1+i}+x_{j_2}+x_{j_2+i}+\cdots.$$

则

$$D^r(x_1,x_2,\cdots,x_n)=D^{r_1}\cdots D^{r_s}(x_1,x_2,\cdots,x_n)=(E_{r_s}\cdots E_{r_1}(x_1),E_{r_s}\cdots E_{r_1}(x_2),\cdots,E_{r_s}\cdots E_{r_1}(x_{n-r})).$$

对 $\forall(a_1,a_2,\cdots,a_n)\in R^n$,定义 G_n 到 G_{n-1}的映射 D:

$$D((a_1,a_2,\cdots,a_n))=(a_1+a_2,a_2+a_3,\cdots,a_{n-1}+a_n).$$

由定义立即可得如下结论:

引理 1.3　映射 D 是 G_n 到 G_{n-1}的满同态;且对任意 $A=(a_1,a_2,\cdots,a_{n-1})\in G_{n-1}$,则在 G_n 中恰好有 4 个状态 $A_i=(i,i+a_1,i+a_1+a_2,\cdots,i+a_1+a_2+\cdots+a_{n-1})$满足:$D(A_i)=A$,$i=0,1,u,1+u$.

称引理 1.3 中的同态为 4-1 同态,或 D 同态.

定义 1.4　映射 $S:R^n\to R_n;(x_1,x_2,\cdots,x_n)\mapsto(x_2,x_3,\cdots,x_n,0)$;

映射 $P_i:R^n\to R;(x_1,x_2,\cdots,x_n)\mapsto x_i$.

关于映射 S,P_i 具有如下性质:设

$$X=(x_1,x_2,\cdots,x_n),Y=(y_1,y_2,\cdots,y_n)\in R^n,$$

① $S(X+Y)=S(X)+S(Y)$;

② $P_i(X+Y)=P_i(X)+P_i(Y)$;

③ $D\cdot S(X)=S\cdot D(X)+(0,0,\cdots,0,x_n)$;特别地有

$$P_i\cdot D\cdot S(X)=P_i\cdot S\cdot D(X),\ 1\leqslant i\leqslant n-2;$$

$$P_{n-1}\cdot D\cdot S(X)=-x_n;\ P_{n-1}\cdot S\cdot D(X)=0;$$

④ $P_i(X)=P_{i-1}\cdot S(X)$, $2\leqslant i\leqslant n$;

⑤ $P_i\cdot D(X)=P_{i+1}(X)-P_i(X)$, $1\leqslant i\leqslant n-1$;

这些性质可由定义直接验证.

设 $A_i=(a_1+i,a_2+i,\cdots,a_n+i)\in G_n$,$i=0,1,u,1+u$,由引理 1.1 知 $D(A_i)$相等,称它们为 G_n 的一组对偶顶点. 设 $C=[a_1,a_2,\cdots,a_p]$是 G_n 的一个周期为 p 的圈,记 C 在 D 同态下的像为 $D(C)$,则 $C_i=[a_1+i,a_2+i,\cdots,a_p+i](i=0,1,u,1+u)$是 G_n 的周期为 p 的圈. 如果对 $i=0,1,u,1+u$ 都有 $C_i=C$,称 C 为 G_n 的一个自对偶圈;如果 $C_i\neq C_j$,$i,j\in R$,称它们为一对相互对偶圈.

引理 1.5　设 $C=[a_1,a_2,\cdots,a_{4^{n-1}}]$是 G_{n-1}中圈长为 4^{n-1}的极长圈,则在 G_n 中恰好有 4 个长为 4^{n-1}的两两无公共顶点的一组相互对偶圈

$$C_j=[j,a_1+j,a_1+a_2+j,\cdots,a_1+a_2+\cdots+a_{4^{n-1}-1}+j]\ (j=0,1,u,1+u)$$

满足 $D(C_i)=C$.

引理 1.6　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 $D(G_f)$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

$$f(x_1,x_2,\cdots,x_n)=g(x_1+x_2,x_2+x_3,\cdots,x_{n-1}+x_n)+x_n.$$

对 $\forall x,y\in R$,规定 $x^{(y)}=\begin{cases}1, & x=y;\\ 0, & x\neq y;\end{cases}$ 则对 $\forall a_1,a_2,\cdots,a_n\in R$,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 1.7 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,σ_1,σ_2 分别是 G_f 中圈长为 l_1,l_2 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

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

是非奇异的,且 $g(x_1,x_2,\cdots,x_n)$将 A_1,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 中圈 σ_1,σ_2 合并成一个长为 $l=l_1+l_2$ 的圈,并保持其余圈不变.

证明 此证明同 Z_k 环上类似,可参阅文献[8]. □

2 环 F_2+uF_2 上 de Bruijn 序列的升级算法

下面给出 de Bruijn 序列的反馈函数的一个升级算法.

定理 2.1 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,则

$$\begin{aligned}f_n(x_1,x_2,\cdots,x_n)=&x_n+f_{n-1}(x_1+x_2,x_2+x_3,\cdots,x_{n-1}+x_n)+\\&(1+f_{n-1}(1,1,\cdots,1))(x_1^{(\alpha_1)}+x_1^{(t_1)})x_2^{(\alpha_2)}\cdots x_n^{(\alpha_n)}+\\&(1+f_{n-1}(1,1,\cdots,1))\cdot\\&(x_1^{(u+\alpha_1)}+x_1^{(u+t_1)})x_2^{(u+\alpha_2)}\cdots x_n^{(u+\alpha_n)}+\\&(u+f_{n-1}(u,u,\cdots,u))(x_1^{(\beta_1)}+x_1^{(t_u)})x_2^{(\beta_2)}\cdots x_n^{(\beta_n)}\end{aligned}\tag{1}$$

为一个 n 级 de Bruijn 序列的反馈函数. 其中,$\alpha_1=\beta_1=0$,$\alpha_{i+1}=1+\alpha_i$,$\beta_{i+1}=u+\beta_i$;t_1,t_u 分别满足:$f_{n-1}(1+t_1,1,\cdots,1)=1$,$f_{n-1}(u+t_u,u,\cdots,u)=u$.

证明 因为 $f_{n-1}(x_1,x_2,\cdots,x_{n-1})$是 $n-1$ 级 de Bruijn 序列的反馈函数,所以其状态图 $G_{f_{n-1}}$ 是 G_{n-1} 中的一个长为 4^{n-1} 的极大圈,记为 $C=[a_1,a_2,\cdots,a_{4^{n-1}}]$. 由引理 1.5 知,在 G_n 中恰有 4 个长为 4^{n-1} 的两两无公共顶点的一组相互对偶圈

$$C_j=[j,a_1+j,a_1+a_2+j,\cdots,a_1+a_2+\cdots a_{4^{n-1}-1}+j]\ (j=0,1,u,1+u)$$

满足 $D(C_i)=C$. 再由引理 1.6,以$\{C_0,C_1,C_u,C_{1+u}\}$为状态图的 n 级非奇移位寄存器的反馈函数为

$$g(x_1,x_2,\cdots,x_n)=x_n+f_{n-1}(x_1+x_2,x_2+x_3,\cdots,x_{n-1}+x_n).\tag{2}$$

记 $A_{j,n}=(j+\alpha_1,j+\alpha_2,\cdots,j+\alpha_n)\in G_n$,其中 $j\in R$,$\alpha_1=0$,$\alpha_{i+1}=1+\alpha_i$. 则 $A_{0,n},A_{1,n},A_{u,n},A_{1+u,n}$ 为一组对偶顶点,因此在 $G_g=\{C_0,C_1,C_u,C_{1+u}\}$中不同的圈上,不妨设 $A_{i,n}\in C_i$,$i\in R$. 设 $A_{1,n}^*=(t_1,\alpha_2,\alpha_3,\cdots,\alpha_n)$为 $A_{1,n}$ 在 C_1 上的先导状态,则 $A_{1+u,n}^*=(u+t_1,u+\alpha_2,u+\alpha_3,\cdots u+\alpha_n)$为 $A_{1+u,n}$ 在 C_{1+u}上的先导状态,且有 $1+\alpha_n=g(A_{1,n}^*)=\alpha_n+f_{n-1}(t_1+\alpha_2,\alpha_2+\alpha_3,\cdots,\alpha_{n-1}+\alpha_n)=\alpha_n+f_{n-1}(t_1+1,1,\cdots,1)$,即 t_1 满足 $f_{n-1}(1+t_1,1,\cdots,1)=1$. 则 $A_{i,n}$与 $A_{i+1,n}^*(i=0,u)$为共轭状态,由引理 1.7 依次交换 $A_{i,n}$与 $A_{i+1,n}^*(i=0,u)$的后继状态,并保持其他状态的后继状态不变,即将 G_g 中圈 C_0 和 C_1 并为一个圈 C_1,圈 C_u 和 C_{1+u}并为一个圈 C_2,对应的非奇反馈函数为

$$\begin{aligned}h(x_1,x_2,\cdots,x_n)=&g(x_1,x_2,\cdots,x_n)+\\&(g(A_1^*)+g(A_0))(x_1^{(\alpha_1)}+x_1^{(t_1)})x_2^{(\alpha_2)}\cdots x_n^{(\alpha_n)}+\\&(g(A_{1+u}^*)+g(A_u))\cdot\\&(x_1^{(u+\alpha_1)}+x_1^{(u+t_1)})x_2^{(u+\alpha_2)}\cdots x_n^{(u+\alpha_n)}.\end{aligned}\tag{3}$$

记 $B_j=(j+\beta_1,j+\beta_2,\cdots,j+\beta_n)$,其中 $j=0,u$,$\beta_1=0$,$\beta_{i+1}=u+\beta_i$. 显然 B_0 与 B_u 或者分别在圈 C_0,C_u 上,或者分别在圈 C_1,C_{1+u}上,从而 B_0 与 B_u 分别在圈 C_1 和 C_2 上. 设 B_u 的先导状态为 $B_u^*=(t_u,\beta_2,\cdots,\beta_n)$,则

$$\begin{aligned}u+\beta_n=h(B_u^*)=g(B_u^*)=&\\\beta_n+f_{n-1}(t_u+\beta_2,\beta_2+\beta_3,\cdots,\beta_{n-1}+\beta_n)=&\\\beta_n+f_{n-1}(t_u+u,u,\cdots,u),&\end{aligned}$$

即 t_u 满足 $f_{n-1}(u+t_u,u,\cdots,u)$,且 B_0 与 B_u^* 互为共轭. 再由引理 1.7,交换 B_0 与 B_u^* 的后继状态,并保持其他状态的后继状态不变,可将圈 C_1 和 C_2 合并得到长为 4^n 的极大圈,对应的 n 级 de Bruijn 序列的反馈函数 $f_n(x_1,x_2,\cdots,x_n)$为

$$f_n(x_1,x_2,\cdots,x_n)=h(x_1,x_2,\cdots,x_n)+(h(B_u^*)+h(B_0))(x_1^{(\beta_1)}+x_1^{(t_u)})x_2^{(\beta_2)}\cdots x_n^{(\beta_n)}.$$

由式(2),(3)得

$$\begin{aligned}f_n(x_1,x_2,\cdots,x_n)=&g(x_1,x_2,\cdots,x_n)+\\&(g(A_1^*)+g(A_0))(x_1^{(\alpha_1)}+x_1^{(t_1)})x_2^{(\alpha_2)}\cdots x_n^{(\alpha_n)}+\\&(g(A_{1+u}^*)+g(A_u))\cdot\\&(x_1^{(u+\alpha_1)}+x_1^{(u+t_1)})x_2^{(u+\alpha_2)}\cdots x_n^{(u+\alpha_n)}+\end{aligned}$$

$$(g(B_u^*)+g(B_0))(x_1^{(\beta_1)}+x_1^{(t_u)})x_2^{(\beta_2)}\cdots x_n^{(\beta_n)}=$$
$$x_n+f_{n-1}(x_1+x_2,x_2+x_3,\cdots,x_{n-1}+x_n)+$$
$$(1+f_{n-1}(1,1,\cdots,1))(x_1^{(\alpha_1)}+x_1^{(t_1)})x_2^{(\alpha_2)}\cdots x_n^{(\alpha_n)}+$$
$$(1+f_{n-1}(1,1,\cdots,1))\cdot$$
$$(x_1^{(u+\alpha_1)}+x_1^{(u+t_1)})x_2^{(u+\alpha_2)}\cdots x_n^{(u+\alpha_n)}+$$
$$(u+f_{n-1}(u,u,\cdots,u))(x_1^{(\beta_1)}+x_1^{(t_u)})x_2^{(\beta_2)}\cdots x_n^{(\beta_n)}.$$

证毕. □

定理 2.1 给出 de Bruijn 序列的反馈函数的一个升级算法,如果直接用递推的方式由一个给定的低级 de Bruijn 序列的反馈函数产生 n 级 de Bruijn 序列,当 n 很大时,计算量则十分巨大,为此我们利用 D 同态的性质,给出一个可以由一个低级的 de Bruijn 序列的反馈函数产生一个任意高级 de Bruijn 序列的有效升级算法.

引理 2.2 记 $X_i=(x_{1,i},x_{2,i},\cdots,x_{i,i})\in R^i$, $i=n,n-1,\cdots,1$,其中,对 $2\leqslant i\leqslant n-1$ 及 $1\leqslant j\leqslant i$, $x_{j,i}=x_{j,i+1}+x_{j+1,i+1}$,有

$$P_{n-i}\cdot D^i\cdot S(X_n)=x_{n,n}+x_{n-1,n-1}+\cdots+x_{n-i+1,n-i+1}.$$

证明 类似于文献[1]中定理 3 由归纳法可证. □

对 $j\in R$, $i\leqslant n$,记 $A_{0,i}=(\alpha_1,\alpha_2,\cdots,\alpha_i)$, $A_{j,i}=(j+\alpha_1,j+\alpha_2,\cdots,j+\alpha_i)\in R^i$; $B_{0,i}=(\beta_1,\beta_2,\cdots,\beta_i)$, $B_{u,i}=(u+\beta_1,u+\beta_2,\cdots,u+\beta_i)\in R^i$,其中,$\alpha_1=\beta_1=0$, $\alpha_{i+1}=1+\alpha_i$, $\beta_{i+1}=u+\beta_i$. 记 $X_i=(x_{1,i},x_{2,i},\cdots,x_{n,i})\in R^i$,其中,对 $2\leqslant i\leqslant n-1$ 及 $1\leqslant j\leqslant i$, $x_{j,i}=x_{j,i+1}+x_{j+1,i+1}$. 则定理 2.1 中的式(1)可改写为

$$f_n(X_n)=x_{n,n}+f_{n-1}(D(X_n))+$$
$$(1+f_{n-1}(1,1,\cdots,1))\cdot$$
$$(x_{1,n}^{(\alpha_1)}+x_{1,n}^{(t_{1,n})})x_{2,n}^{(\alpha_2)}\cdots x_{n,n}^{(\alpha_n)}+$$
$$(1+f_{n-1}(1,1,\cdots,1))\cdot$$
$$(x_{1,n}^{(u+\alpha_1)}+x_{1,n}^{(u+t_{1,n})})x_{2,n}^{(u+\alpha_2)}\cdots x_{n,n}^{(u+\alpha_n)}+$$
$$(u+f_{n-1}(u,u,\cdots,u))\cdot$$
$$(x_{1,n}^{(\beta_1)}+x_{1,n}^{(u+t_{u,n})})x_{2,n}^{(\beta_2)}\cdots x_{n,n}^{(\beta_n)}.$$

反复运用定理 2.1 可得

$$f_{n-1}(D(X_n))=x_{n-1,n-1}+f_{n-2}(D^2(X_n))+$$
$$(1+f_{n-2}(1,1,\cdots,1)\cdot$$
$$(x_{1,n-1}^{(\alpha_1)}+x_{1,n-1}^{(t_{1,n-1})})x_{2,n-1}^{(\alpha_2)}\cdots x_{n-1,n-1}^{(\alpha_{n-1})}+$$
$$(1+f_{n-2}(1,1,\cdots,1))\cdot$$
$$(x_{1,n-1}^{(u+\alpha_1)}+x_{1,n-1}^{(u+t_{1,n-1})})x_{2,n-1}^{(u+\alpha_2)}\cdots x_{n-1,n-1}^{(u+\alpha_{n-1})}+$$
$$(u+f_{n-2}(u,u,\cdots,u))\cdot$$
$$(x_{1,n-1}^{(\beta_1)}+x_{1,n-1}^{(t_{u,n-1})})x_{2,n-1}^{(\beta_2)}\cdots x_{n-1,n-1}^{(\beta_{n-1})},$$

$$f_{n-2}(D^2(X_n))=x_{n-2,n-2}+f_{n-3}(D^3(X_n))+$$
$$(1+f_{n-3}(1,1,\cdots,1)\cdot$$
$$(x_{1,n-2}^{(\alpha_1)}+x_{1,n-2}^{(t_{1,n-2})})x_{2,n-2}^{(\alpha_2)}\cdots x_{n-2,n-2}^{(\alpha_{n-2})}+$$
$$(1+f_{n-3}(1,1,\cdots,1))\cdot$$
$$(x_{1,n-2}^{(u+\alpha_1)}+x_{1,n-2}^{(u+t_{1,n-2})})x_{2,n-2}^{(u+\alpha_2)}\cdots x_{n-2,n-2}^{(u+\alpha_{n-2})}+$$
$$(u+f_{n-3}(u,u,\cdots,u))\cdot$$
$$(x_{1,n-2}^{(\beta_1)}+x_{1,n-2}^{(t_{u,n-2})})x_{2,n-2}^{(\beta_2)}\cdots x_{n-2,n-2}^{(\beta_{n-2})},$$

……

$$f_{m+1}(D^{n-m-1}(X_n))=x_{m+1,m+1}+f_m(D^{n-m}(X_n))+$$
$$(1+f_m(1,1,\cdots,1)\cdot$$
$$(x_{1,m+1}^{(\alpha_1)}+x_{1,m+1}^{(t_{1,m+1})})x_{2,m+1}^{(\alpha_2)}\cdots x_{m+1,m+1}^{(\alpha_{m+1})}+$$
$$(1+f_m(1,1,\cdots,1))\cdot$$
$$(x_{1,m+1}^{(u+\alpha_1)}+x_{1,m+1}^{(u+t_{1,m+1})})x_{2,m+1}^{(u+\alpha_2)}\cdots x_{m+1,m+1}^{(u+\alpha_{m+1})}+$$
$$(u+f_m(u,u,\cdots,u))\cdot$$
$$(x_{1,m+1}^{(\beta_1)}+x_{1,m+1}^{(t_{u,m+1})})x_{2,m+1}^{(\beta_2)}\cdots x_{m+1,m+1}^{(\beta_{m+1})}.$$

其中,$t_{1,i}$, $t_{u,i}$分别满足: $f_{n-i}(1+t_{1,i},1,\cdots,1)=1$, $f_{n-i}(u+t_{u,i},u,\cdots,u)=u$, $i=n,n-1,\cdots,m+1$.

首先,对于 $i>m+1$,由定理 2.1,有

$$1=f_{n-i}(1+t_{1,i},1,\cdots,1)=$$
$$1+f_{n-i-1}(t_{1,i},0,\cdots,0)=$$
$$1+f_{n-i-2}(t_{1,i},0,\cdots,0)=\cdots=$$
$$1+f_m(t_{1,i},0,\cdots,0),$$
$$u=f_{n-i}(u+t_{u,i},u,\cdots,u)=$$
$$u+f_{n-i-1}(t_{u,i},0,\cdots,0)=\cdots=$$
$$u+f_m(t_{u,i},0,\cdots,0).$$

于是此时所有的 $t_{1,i}$, $t_{u,i}$满足 $f_m(t_{1,i},0,\cdots,0)$及 $f_m(t_{u,i},0,\cdots,0)=0$,从而当 $i,j>m+1$ 时 $t_{1,i}=t_{u,j}$,设为 t,满足 $f_m(t,0,\cdots,0)=0$,这里 $t\neq 0$.

其次,再由定理 2.1,有

$$a+f_{n-j}(a,a,\cdots,a)=f_{n-j-1}(0,\cdots,0)=$$
$$\cdots=f_m(0,\cdots,0)$$

式中,$a=1,u$, $j=1,2,\cdots,n-m-1$.

因此我们证明了下面的定理成立:

定理 2.3 设 f_m 是 m 级 de Bruijn 序列的反馈函数,则对 $\forall X_n\in R^n$,

$$f_n(X_n)=P_{n-m}\cdot D^m\cdot S(X_n)+$$
$$f_m(D^{n-m}(X_n))+f_m(0,0,\cdots,0)\cdot$$
$$\Big(\sum_{j\in\{0,u\}}\sum_{i=m+2}(x_{1,i}^{(j+\alpha_1)}+x_{1,i}^{(j+t)})x_{2,i}^{(j+\alpha_2)}\cdots x_{i,i}^{(j+\alpha_1)}+$$
$$\sum_{i=m+2}^{n}(x_{1,i}^{(\beta_1)}+x_{1,i}^{(t)})x_{2,i}^{(\beta_2)}\cdots x_{i,i}^{(\beta_i)}\Big)+$$
$$(1+f_m(1,1,\cdots,1))\cdot$$
$$(x_{1,m+1}^{(\alpha_1)}+x_{1,m+1}^{(t_{1,m+1})})x_{2,m+1}^{(\alpha_2)}\cdots x_{m+1,m+1}^{(\alpha_{m+1})}+$$

$$(1+f_m(1,1,\cdots,1))\cdot$$
$$(x_{1,m+1}^{(u+\alpha_1)}+x_{1,m+1}^{(u+t_{1,m+1})})x_{2,m+1}^{(u+\alpha_2)}\cdots x_{m+1,m+1}^{(u+\alpha_{m+1})}+$$
$$(u+f_m(u,u,\cdots,u))\cdot$$
$$(x_{1,m+1}^{(\beta_1)}+x_{1,m+1}^{(t_{u,m+1})})x_{2,m+1}^{(\beta_2)}\cdots x_{m+1,m+1}^{(\beta_{m+1})}.$$

$f_n(X_n)$是 n 级 de Bruijn 序列的反馈函数. 其中,t 满足 $f_m(t,0,\cdots,0)=0$;$t_{1,m+1}$,$t_{u,m+1}$分别满足

$$f_{m+1}(1+t_{1,m+1},1,\cdots,1)=1,$$
$$f_{m+1}(u+t_{u,m+1},u,\cdots,u)=u;$$

$\alpha_1=\beta_1=0$,$\alpha_{i+1}=1+\alpha_i$,$\beta_{i+1}=u+\beta_i$.

记

$$f_n(X_n)=P_{n-m}\cdot D^m\cdot S(X_n)+f_m(D^{n-m}(X_n))+\Delta_m.$$

下面我们考虑 Δ_m 的计算.

对于每一个 $X_n\in R^n$,Δ_m 的值依赖于 X_n,$D(X_n)$,$D^2(X_n)$,$\cdots$,$D^{n-m}(X_n)$中是否能取到某个 $A_{i,j}$,$A_{i+1,j}^*$,$B_{0,j}$或 $B_{u,j}^*$,其中 $i\in\{0,u\}$,$j\in\{m+1,m+2,\cdots,n\}$. 由于 $D(A_{i,j})=(a,a,\cdots,a)$,$D^2(A_{i,j})=(0,0,\cdots,0)$;$D(A_{i,j}^*)=(-t,1,\cdots,1)$,$D^2(A_{i,j}^*)=(1+t_j,0,\cdots,0)$(其中 $t_j\neq-1$),因此求和式 Δ_m 中的各项中至多一项不为零,只需对 X_n,$D(X_n)$,$D^2(X_n)$,$\cdots$,$D^{n-m}(X_n)$进行判断就可以了,而由 D 同态的计算公式,这种判断的计算复杂性较小.

因此由定理 2.3,在已知一个低级的 de Bruijn 序列反馈函数的情况下,可以不通过完全求出反馈函数,直接得出高级 de Bruijn 序列的下一状态. 因此定理 2.3 给出了一个有效升级算法.

3 结论

本文将 F_2 域上 de Bruijn 序列的升级算法推广到 F_2+uF_2 环上,给出了 F_2+uF_2 环上一个从 m 级 de Bruijn 序列直接生成 n 级($m<n$) de Bruijn 序列的一个有效升级算法. 该算法具有运算简单及所需存储空间小等特点,减少了运算次数,加快了生成速度,因此该算法不仅具有一定的理论意义而且有较高的实用价值.

参考文献(References)

[1] Chang T, Park B, Kim Y H, et al. An efficient implementation of the D-homomorphism for generation of de Bruijn sequences[J]. IEEE Trans Inform, 1999, 45(4):1 280-1 283.

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

[3] Yan Jun-hui. Constructing the Hamilton cycle on n-ary de Bruijn sequences [J]. Systems Sciences and Mathematical Sciences, 1991, 4(1):32-40.

[4] 熊荣华. 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.

[5] 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.

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

[7] Zhu Shi-xin, Wu bo. A recursive algorithm for generating k-ary de Bruijn sequences[J]. Journal of Hefei University of Technology (Natural Science), 2005, 8(9): 1 210-1 212.
朱士信, 吴波. 产生 k 元 de Bruijn 序列的一个递归算法[J]. 合肥工业大学学报,2005, 8(9): 1 210-1 212.

[8] Zhu Shi-xin, Sun Ling. An algorithm for generating feedback functions of k-ary de Bruijn sequences by raising stage[J]. Acta Electronica Sinica, 2006,34(6): 1 066-1 068.
朱士信, 孙琳. k 元 de Bruijn 序列的反馈函数的一个升级算法[J]. 电子学报, 2006,34(6): 1 066-1 068.

[9] Bonnecaze A, Udaya P. Cyclic codes and self-dual codes over F_2+uF_2[J]. IEEE Trans Inform Theory, 1999,45(4):1 250-1 255.

[10] Udaya P, Bonnecaze A. Decoding of cyclic codes over F_2+uF_2[J]. IEEE Trans Inform Theory, 1999, 45(6):2 148-2 157.

[11] 万哲先, 代宗铎, 刘木兰, 等. 非线性移位寄存器[M]. 北京:科学出版社, 1978.