基于全体圈个数为 4 的 LFSR 构造 de Bruijn 序列的研究

周琮伟，胡斌，关杰
（信息工程大学密码工程学院，河南 郑州 450001）

摘 要：为了提高并圈法的构造效率，拓宽并圈法的应用深度，从圈结构中圈个数的角度，提出了基于全体圈个数为 4 的 LFSR 构造 de Bruijn 序列的方法。基于 LFSR 的级联特征，确定了一类级联型的反馈移位寄存器的圈结构，并据此给出了圈个数为 4 的 n 级 LFSR 的精确个数，以及基于全体圈个数为 4 的 n 级 LFSR 构造 n 级 de Bruijn 序列的全部数目。

关键词：线性反馈移位寄存器；de Bruijn 序列；级联；圈结构
中图分类号：TN918.6
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2022108

Construction de Bruijn sequence based on whole LFSR with 4 cycles

ZHOU Congwei, HU Bin, GUAN Jie
Department of Cryptogram Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: In order to improve the construction efficiency and widen the application depth of cycle-joining method, from the view of the number of cycles in the cycle structure, a method for constructing de Bruijn sequence based on whole LFSR with 4 cycles was proposed. Based on the characteristic of cascade connection of LFSR, the cycle structure of a class of cascaded feedback shift registers was determined. Accordingly, the exact number of whole n-order LFSR with 4 cycles was given, and the total number of n-order de Bruijn sequences constructed from whole n-order LFSR with 4 cycles as well.

Keywords: linear feedback shift register, de Bruijn sequence, cascade connection, cycle structure

0 引言

近几十年来，线性反馈移位寄存器（LFSR, linear feedback shift register）序列被广泛应用于通信编码和密码算法中，例如众所周知的 m 序列。然而由于 LFSR 固有的线性制约性及输入的多条乱源序列存在时间差，可以对其经过非线性改造产生的密钥流的序列周期与线性复杂度进行深刻的代数刻画[1]，并且在此基础上提出的相关攻击[2]、最佳仿射线性攻击[3]与代数攻击[4]等分析方法均有对应的算法攻击实例，因此逐渐将研究对象从 LFSR 转向非线性反馈移位寄存器序列。其中 n 级 de Bruijn 序列是一类重要的非线性反馈移位寄存器序列，其圈结构中圈长达到最大周期 2^n，同时其伪随机性质与线性复杂度[5]均优于 m 序列。此外，de Bruijn 序列在卫星通信[6]、电网技术[7]和基因测序[8]中均有广泛应用。

构造 de Bruijn 序列一直以来都是研究 de Bruijn 序列的核心问题，其构造思路主要是基于反馈移位寄存器圈结构中各圈的合并，其难点在于研究各圈上的共轭状态分布。在 20 世纪 70 年代至 90 年代，国际上掀起了研究构造 de Bruijn 序列的热潮，各种算法和结果层出不穷[9-17]，其中文献[12]比较全面地介绍了 de Bruijn 序列构造的经典算法。近期国内学者也给出了一些构造算法[18-19]，但快速构造密码学性质良好和实用性强的 de Bruijn 序列特征函数仍然是一个长期亟待解决的问题。

收稿日期：2022−01−20；**修回日期：**2022−04−15
基金项目：国家自然科学基金资助项目（No.61572516, No.61802437）
Foundation Item: The National Natural Science Foundation of China (No.61572516, No.61802437)

从 20 世纪 70 年代起，Lempel[20]引入 D-同态的概念，利用 n 级 de Bruijn 序列在 D-同态下的原像是 2 个 $n+1$ 级的等长圈，并结合 2 个等长圈上共轭状态的分布特点，给出了一个由 n 级到 $n+1$ 级 de Bruijn 序列特征函数的递归构造方法，且可以进一步拓展到 $n+2$ 级[21]。此类递归思路实际上可以看作产生 n 级 de Bruijn 序列的非线性反馈移位寄存器级联小级数的 LFSR，Chang 等[22]利用线性方程的方法给出了较为清晰的代数表达式。

另一方面，Li 等[23-25]、Li 等[26-27]和 Chang 等[28]研究了几类级联型 LFSR 的特征多项式，给出了其中几个 n 级 LFSR 圈结构的因子关联图，从而给出了其构造的算法和计数。特别地，Dong 等[29]还研究了利用仿射反馈移位寄存器构造 de Bruijn 序列的方法。以上方法均建立在小级数的 LFSR 级联特征多项式为本原多项式的 LFSR。同时，Dong 等[30-31]还研究了周期为 $\frac{2^n-1}{k}$ 的 n 次不可约多项式为特征多项式的 LFSR 圈结构的因子关联图，证明了其特征多项式的邻接矩阵（因子关联图的矩阵化）与本原多项式的 $k-$ 邻接矩阵相等，并利用雅可比和给出了 $k=3,5$ 时其对应的 $k-$ 邻接矩阵元素的具体表达式，即从理论上给出了这类 de Bruijn 序列的计数。从构造的实用性角度上分析，通过并圈方式直接构造的 de Bruijn 序列特征函数基于的 LFSR 圈结构中圈个数越少，效率一般越高。由于 LFSR 圈结构中圈个数一定为偶数[17]，且等于 2 的情形为 m 序列中添加一个零，因此本文进一步研究基于圈个数为 4 的 LFSR 构造 de Bruijn 序列的方法。同时，为了拓宽上述研究所基于的 LFSR 种类，增加构造的 de Bruijn 序列数目，给出更多清晰的 de Bruijn 序列特征函数形式，本文的工作延续和拓展了上述文献中的构造方法，并结合文献[31]的相关结论，提出了基于全体圈个数为 4 的 LFSR 构造 de Bruijn 序列的方法。

1　一类级联型的反馈移位寄存器的圈结构

令 $f(x_0,x_1,\cdots,x_n)=F(x_0,\cdots,x_{n-1})\oplus x_n$ 是 n 级反馈移位寄存器的特征函数，f 是 F_2 上任意的布尔函数。对于反馈移位寄存器，不同的初态 $(a_0,a_1,\cdots,a_{n-1})$ 产生不同的序列，记 2^n 个初态产生的序列集合为 $\Omega(f)$。当且仅当 $f(x_0,\cdots,x_{n-1},x_n)$ 是非奇异时[32]，$\Omega(f)$ 中的任意序列是周期的，即 f 可以写作

$$f(x_0,x_1,\cdots,x_{n-1})=x_0\oplus F_0(x_1,\cdots,x_{n-1})\oplus x_n \tag{1}$$

由于非奇异反馈移位寄存器产生的输出序列都是周期的，因此可以在此基础上定义序列的左移变换为

$$L:Ls=L(s_0,s_1,\cdots,s_{N-1})=(s_1,s_2,\cdots,s_{N-1},s_0) \tag{2}$$

则集合

$$[s]:=\{s,Ls,\cdots,L^{N-1}s\} \tag{3}$$

为 $\Omega(f)$ 的一个平移等价类或者一个圈。若 $\Omega(f)$ 有 r 个圈，则 $\Omega(f)$ 或反馈移位寄存器的圈结构可以写作

$$\Omega(f)=[s_1]\bigcup[s_2]\bigcup\cdots\bigcup[s_r] \tag{4}$$

引理 1 表述了圈结构中非常重要的圈合并与圈分解的概念。

引理 1[32]　设 $\nu=(v_0,v_1,\cdots,v_{n-1})$ 在圈 $[s_i]$ 上，其共轭状态 $\hat{\nu}=(v_0\oplus 1,v_1,\cdots,v_{n-1})$ 在圈 $[s_j](j\neq i)$ 上，则可以通过交换 ν 和 $\hat{\nu}$ 这 2 个状态的后继使这 2 个圈合并为一个圈，其对应的圈合并后的特征函数为

$$f'=f(x_0,x_1,\cdots,x_n)\oplus x_1^{v_1}x_2^{v_2}\cdots x_{n-1}^{v_{n-1}} \tag{5}$$

同理，若 ν 和其共轭状态 $\hat{\nu}$ 都在圈 $[s_i]$ 上，则可以通过交换 ν 和 $\hat{\nu}$ 这 2 个状态的后继使这一个圈分解为 2 个圈，其对应的圈分解后的特征函数也如上。

级联或者称为反馈移位寄存器的串联始见于文献[33]，由定义 1 描述。

定义 1　设 n 级的反馈移位寄存器在初态 $(a_0,a_1,\cdots,a_{n-1})$ 下产生序列 $\boldsymbol{a}$ 且特征函数为 f，m 级的反馈移位寄存器初态为 $(b_0,b_1,\cdots,b_{m-1})$ 且特征函数为 g，则称特征函数为 $f*g$ 的反馈移位寄存器为级联型，其输出序列 $\boldsymbol{b}$ 满足

$$b_{i+m}=a_i\oplus g(b_i,b_{i+1},\cdots,b_{i+m-1}),i=0,1,2,\cdots \tag{6}$$

其中，若设

$$\begin{aligned}&f(x_0,x_1,\cdots,x_n)=F(x_0,x_1,\cdots,x_{n-1})\oplus x_n\\&g(x_0,x_1,\cdots,x_m)=G(x_0,x_1,\cdots,x_{m-1})\oplus x_m\end{aligned} \tag{7}$$

则特征函数 $f*g$ 可表示为

$$\begin{aligned}f*g=f(&g(x_0,x_1,\cdots,x_m),g(x_1,x_2,\cdots,x_{m+1}),\cdots,\\&g(x_n,x_{n+1},\cdots,x_{n+m}))\end{aligned} \tag{8}$$

特征函数 $f*g$ 对应的 $m+n$ 级的级联型反馈移位寄存器的结构框架如图 1 所示。

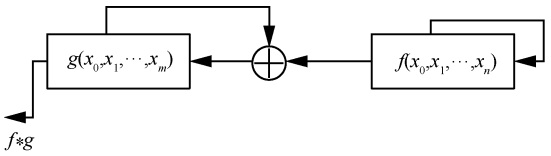

图 1 特征函数 $f*g$ 对应的 $m+n$ 级的级联型反馈移位寄存器的结构框架

为了研究基于 LFSR 的反馈移位寄存器的级联特征，本文首先给出 LFSR 特征多项式的相关概念。设全体 LFSR 的特征函数形如

$$c_0x_0 \oplus c_1x_1 \oplus \cdots \oplus c_{n-1}x_{n-1} \oplus x_n, c_i \in F_2 (0 \leqslant i \leqslant n-1) \tag{9}$$

则存在 F_2 上的一一映射

$$\psi : \psi(c_0x_0 \oplus c_1x_1 \oplus \cdots \oplus c_{n-1}x_{n-1} \oplus x_n) = c_0 \oplus c_1x \oplus \cdots \oplus c_{n-1}x^{n-1} \oplus x^n \tag{10}$$

此时，称 $\psi(x)$ 为该LFSR的特征多项式。文献[17]指出，若 $\psi(x)$ 为 F_2 上的 n 次不可约多项式，则该 LFSR 的圈结构 $\Omega(\psi(x))$ 可表示为

$$\Omega(\psi(x)) = 1[1] + \frac{2^n-1}{p(\psi(x))}[p(\psi(x))] \tag{11}$$

其中，$\bullet[*]$ 表示圈长为 $*$ 的圈有 $\bullet$ 个，$p(\psi(x))$ 表示 $\psi(x)$ 在 F_2 上的周期。因此，如果可以将 F_2 上的任一特征多项式分解为若干不可约多项式的乘积[17]，则可以确定 LFSR 的圈结构。文献[34]证明了包含 LFSR 的一类级联型反馈移位寄存器的输出序列的周期分布情况，即引理 2。

引理 2[34] 设 $g(x_0,x_1,\cdots,x_m)$ 是 LFSR 的特征函数，其特征多项式 $\psi(g)$ 为 F_2 上的 m 次不可约多项式，且设

$$\begin{cases} f = x_0 \oplus F_0(x_1,\cdots,x_{n-1}) \oplus x_n \\ \boldsymbol{a} = (a_0,a_1,\cdots,a_{n-1},\cdots) \in \Omega(f) \end{cases} \tag{12}$$

其中，序列 $\boldsymbol{a}$ 的周期表示为 $p(\boldsymbol{a})$。

1) 若 $p(\psi(g)) \nmid p(\boldsymbol{a})$，设在初态 $(a_0,a_1,\cdots,a_{n-1})$ 加载下，特征函数为 $f*g$ 的级联型的反馈移位寄存器生成的序列集合为 $\theta(g)^{-1}(\boldsymbol{a})$，则 $\theta(g)^{-1}(\boldsymbol{a})$ 包含一条周期长度为 $p(\boldsymbol{a})$ 的序列和 2^m-1 条周期长度为 $\mathrm{lcm}\{p(\boldsymbol{a}),p(\psi(g))\}$ 的序列，其中 $\mathrm{lcm}\{p(\boldsymbol{a}),p(\psi(g))\}$ 表示 $p(\psi(g)),p(\boldsymbol{a})$ 的最小公倍数。

2) 若 $p(\psi(g)) \mid p(\overline{a})$，对于任意一条序列 $\boldsymbol{x} \in \theta(f)^{-1}(\boldsymbol{a})$，有

$$p(x)\begin{cases} p(\boldsymbol{a}), & \psi(g) \mid \psi(\boldsymbol{a}(x)) \\ 2p(\boldsymbol{a}), & \psi(g) \nmid \psi(\boldsymbol{a}(x)) \end{cases} \tag{13}$$

其中，

$$\boldsymbol{a}(x) = a_{p(\boldsymbol{a})-1} \oplus a_{p(\boldsymbol{a})-2}x \oplus \cdots \oplus a_0x^{p(\boldsymbol{a})-1} \oplus x^{p(\boldsymbol{a})} \tag{14}$$

通常，基于级联型反馈移位寄存器构造 de Bruijn 序列的方法主要是将给定的特征函数依据引理2的1)中的限制条件代入级联型的递归式，并直接对集合 $\theta(g)^{-1}(\boldsymbol{a})$ 中的生成序列按平移等价进行分类，便可推导出其圈结构中的圈个数，即定理 1，从而进一步得到这类级联型反馈移位寄存器的圈结构 $\Omega(f*g)$。

定理 1 设 $g(x_0,x_1,\cdots,x_m)$ 是 LFSR 的特征函数，其特征多项式 $\psi(g)$ 为 F_2 上的 m 次不可约多项式，且设 $f = x_0 \oplus F_0(x_1,\cdots,x_{n-1}) \oplus x_n$，$\boldsymbol{a} = (a_0,a_1,\cdots,a_{n-1},\cdots) \in \Omega(f)$。若 $p(\psi(g)) \nmid p(\boldsymbol{a})$，则序列集合 $\theta(g)^{-1}(a)$ 的圈结构中共有 $1+\left(p(\psi(g)),p(\boldsymbol{a})\right)\dfrac{2^m-1}{p(\psi(g))}$ 个圈。其中，$\left(p(\psi(g)),p(\boldsymbol{a})\right)$ 表示 $p(\psi(g)),p(\boldsymbol{a})$ 的最大公约数。

证明 由引理 2 的 1)可知，在 2^m 个不同的周期序列中有且仅有一个序列周期为 $p(\boldsymbol{a})$，设它相应的初态为 $(b_0^*,b_1^*,\cdots,b_{m-1}^*)$，当所取的初态 $(b_0',b_1',\cdots,b_{m-1}')$ 不同于上述初态时，所得的序列 $B' = (b_0',b_1',\cdots,b_{m-1}',\cdots)$ 的周期为 $q = \mathrm{lcm}\{p(\boldsymbol{a}),p(\psi(g))\}$。现考察与 B' 平移等价的序列 $(b_m',b_{m+1}',b_{m+2}',\cdots)$ 的 $p(\boldsymbol{a})$ 采样的点

$$b_m',b_{m+p(\boldsymbol{a})}',\cdots,b_{m+(P-1)p(\boldsymbol{a})}',b_{m+Pp(\boldsymbol{a})}',\cdots \tag{15}$$

其中，$P = \dfrac{\mathrm{lcm}\{p(\boldsymbol{a}),p(\psi(g))\}}{p(\boldsymbol{a})} = \dfrac{q}{p(\boldsymbol{a})}$。因为这些点满足

$$\begin{aligned} &b_m' = a_0 \oplus g(b_0',b_1',\cdots,b_{m-1}') \\ &b_{m+p(\boldsymbol{a})}' = a_{p(\boldsymbol{a})} \oplus g(b_{p(\boldsymbol{a})}',b_{p(\boldsymbol{a})+1}',\cdots,b_{p(\boldsymbol{a})+m-1}'),\cdots \\ &b_{m+(P-1)p(\boldsymbol{a})}' = a_{(P-1)p(\boldsymbol{a})} \oplus g(b_{(P-1)p(\boldsymbol{a})}', \\ &b_{(P-1)p(\boldsymbol{a})+1}',\cdots,b_{(P-1)p(\boldsymbol{a})+m-1}') \\ &b_{m+Pp(\boldsymbol{a})}' = a_{Pp(\boldsymbol{a})} \oplus g(b_{Pp(\boldsymbol{a})}',b_{Pp(\boldsymbol{a})+1}',\cdots,b_{Pp(\boldsymbol{a})+m-1}'),\cdots \end{aligned} \tag{16}$$

而 $a_0 = a_{p(\boldsymbol{a})} = \cdots = a_{(P-1)p(\boldsymbol{a})} = a_{Pp(\boldsymbol{a})} = \cdots$，所以当

$$\begin{aligned} &(b_0',b_1',\cdots,b_{m-1}'),(b_{p(\boldsymbol{a})}',b_{p(\boldsymbol{a})+1}',\cdots,b_{p(\boldsymbol{a})+m-1}'), \\ &\cdots,(b_{(P-1)p(\boldsymbol{a})}',b_{(P-1)p(\boldsymbol{a})+1}',\cdots,b_{(P-1)p(\boldsymbol{a})+m-1}'), \\ &(b_{Pp(\boldsymbol{a})}',b_{Pp(\boldsymbol{a})+1}',\cdots,b_{Pp(\boldsymbol{a})+m-1}'),\cdots \end{aligned} \tag{17}$$

中的任一数组作为递推关系 $b_{m+i}=a_i\oplus g(b_i,b_{i+1},\cdots,b_{i+m-1}),i=0,1,2,\cdots$ 的初值时，所产生的序列

$$\begin{aligned}&(b_0',b_1',\cdots,b_{m-1}',b_m',\cdots),\\&(b_{p(\boldsymbol{a})}',b_{p(\boldsymbol{a})+1}',\cdots,b_{p(\boldsymbol{a})+m-1}',b_{m+p(\boldsymbol{a})}',\cdots),\cdots,\\&(b_{(P-1)p(\boldsymbol{a})}',b_{(P-1)p(\boldsymbol{a})+1}',\cdots,b_{(P-1)p(\boldsymbol{a})+m-1}',b_{m+(P-1)p(\boldsymbol{a})}',\cdots),\\&(b_{Pp(\boldsymbol{a})}',b_{Pp(\boldsymbol{a})+1}',\cdots,b_{Pp(\boldsymbol{a})+m-1}',b_{m+Pp(\boldsymbol{a})}',\cdots),\cdots\end{aligned}\tag{18}$$

均与 B' 平移等价，且仅限于取它们作为初态时所得序列。注意到， B' 的周期为 $q=Pp(\boldsymbol{a})$，因此

$$\begin{aligned}&(b_{0+jp(\boldsymbol{a})}',b_{1+jp(\boldsymbol{a})}',\cdots,b_{m-1+jp(\boldsymbol{a})}',b_{m+jp(\boldsymbol{a})}',\cdots)=\\&(b_{(P+j)p(\boldsymbol{a})}',b_{(P+j)p(\boldsymbol{a})+1}',\cdots,b_{(P+j)p(\boldsymbol{a})+m-1}',\\&b_{m+(P+j)p(\boldsymbol{a})}',\cdots),j\geqslant 0\end{aligned}\tag{19}$$

只有前 P 个两两不同的数组作为初值产生的序列与 B' 平移等价。根据上面的讨论，所有平移等价的序列在同一个圈上，因此共有

$$\begin{aligned}&\frac{2^m-1}{P}=\frac{(2^m-1)p(\boldsymbol{a})}{q}=\frac{p(\boldsymbol{a})p(\psi(g))(2^m-1)}{qp(\psi(g))}=\\&\left(p(\psi(g)),p(\boldsymbol{a})\right)\frac{2^m-1}{p(\psi(g))}\end{aligned}\tag{20}$$

个周期为 q 的圈，加上一个周期为 $p(\boldsymbol{a})$ 的圈。证毕。

若 $\Omega(f)$ 中的每个圈圈长都不被 $p(\psi(g))$ 整除，将 $\Omega(f)$ 中所有平移不等价的序列代入定理 1，可以立即推出这类级联型反馈移位寄存器的圈结构，即推论 1。

推论 1　设 $g(x_0,x_1,\cdots,x_m)$ 是 LFSR 的特征函数，其特征多项式 $\psi(g)$ 为 F_2 上的 m 次不可约多项式，设

$$\begin{aligned}&\Omega(f)=n_1[p_1]+n_2[p_2]+\cdots+n_r[p_r]\\&p(\psi(g))\nmid p_j,j=1,2,\cdots,r\end{aligned}\tag{21}$$

则有

$$\begin{aligned}&\Omega(f*g)=n_1[p_1]+n_2[p_2]+\cdots+n_r[p_r]+\\&n_1\left(p(\psi(g)),p_1\right)\frac{2^m-1}{p(\psi(g))}\left[\mathrm{lcm}\left\{p(\psi(g)),p_1\right\}\right]+\\&n_2\left(p(\psi(g)),p_2\right)\frac{2^m-1}{p(\psi(g))}\left[\mathrm{lcm}\left\{p(\psi(g)),p_2\right\}\right]+\cdots+\\&n_r\left(p(\psi(g)),p_r\right)\frac{2^m-1}{p(\psi(g))}\left[\mathrm{lcm}\left\{p(\psi(g)),p_r\right\}\right]\end{aligned}\tag{22}$$

2　构造 de Bruijn 序列的方法

利用 $f*g$ 的特征函数结构，可以给出任意 n 级 LFSR 与级联型反馈移位寄存器之间的关系。

定理 2　任意 n 级 LFSR 等价于唯一确定的若干 LFSR 经过级联生成的级联型反馈移位寄存器。

证明　设 n 级 LFSR 的特征函数为

$$\begin{aligned}&f(x)=c_0x_0\oplus c_1x_1\oplus\cdots\oplus c_{n-1}x_{n-1}\oplus x_n,\\&c_i\in F_2(0\leqslant i\leqslant n-1)\end{aligned}\tag{23}$$

则其特征多项式为

$$\begin{aligned}&\psi\left(f(x)\right)=\psi(c_0x_0\oplus c_1x_1\oplus\cdots\oplus c_{n-1}x_{n-1}\oplus x_n)=\\&c_0\oplus c_1x\oplus\cdots\oplus c_{n-1}x^{n-1}\oplus x^n\end{aligned}\tag{24}$$

根据多项式的唯一分解定理，该特征多项式 $\psi\left(f(x)\right)$ 可以唯一分解成若干不可约多项式的乘积，此时不妨令 $\psi\left(f(x)\right)=\psi\left(h(x)\right)\psi\left(g(x)\right)$，其中 $\psi\left(h(x)\right)$ 和 $\psi\left(g(x)\right)$ 分别为 m 和 p 次不可约多项式，且满足 $m+p=n$。具体地，设

$$\begin{aligned}&\psi\left(h(x)\right)=a_0\oplus a_1x\oplus\cdots\oplus a_{m-1}x^{m-1}\oplus x^m,\\&a_i\in F_2(0\leqslant i\leqslant m-1)\end{aligned}\tag{25}$$

$$\begin{aligned}&\psi\left(g(x)\right)=b_0\oplus b_1x\oplus\cdots\oplus b_{p-1}x^{p-1}\oplus x^p,\\&b_i\in F_2(0\leqslant i\leqslant p-1)\end{aligned}\tag{26}$$

根据 $\psi(f(x))=\psi(h(x))\psi(g(x))$，可得

$$\sum_{j+k=i}a_jb_k=c_i,0\leqslant i\leqslant n-1\tag{27}$$

另一方面，设 $\psi\left(h(x)\right)$ 和 $\psi\left(g(x)\right)$ 对应的 LFSR 特征函数分别为

$$\begin{aligned}&h(x)=a_0x_0\oplus a_1x_1\oplus\cdots\oplus a_{m-1}x_{m-1}\oplus x_m\\&g(x)=b_0x_0\oplus b_1x_1\oplus\cdots\oplus b_{p-1}x_{p-1}\oplus x_p\end{aligned}\tag{28}$$

则有

$$\begin{aligned}&h(x)*g(x)=\\&h(g(x_0,x_1,\cdots,x_p),g(x_1,x_2,\cdots,x_{p+1}),\cdots,\\&g(x_m,x_{m+1},\cdots,x_{m+p}))\end{aligned}\tag{29}$$

又因为

$$\sum_{j+k=i}a_jb_k=c_i,0\leqslant i\leqslant n-1\tag{30}$$

代入式(29)可得 $h(x)*g(x)=f(x)$，即特征函数为 $h(x)$ 和 $g(x)$ 对应的 LFSR 级联生成的级联型反馈移位寄存器恰为特征函数为 $f(x)$ 对应的 LFSR。进一步地，对于 $\psi\left(f(x)\right)$ 分解为一般情况时，本文可以反复迭代上述过程，又根据多项式的唯一分解定

理，因此任意 LFSR 均等价于唯一确定的若干 LFSR 经过级联生成的级联型反馈移位寄存器，此时其特征多项式分解的若干不可约多项式恰为级联型反馈移位寄存器中各 LFSR 的特征多项式。证毕。

根据定理 2 以及推论 1，由于 LFSR 圈结构中圈个数至少为 2，则对于任意圈个数为 4 的 n 级 LFSR 等价的级联型反馈移位寄存器，级联的 LFSR 个数最多为 2，因此可得定理 3。

定理 3 圈个数为 4 的 $n(n\geqslant 3)$ 级 LFSR 个数为

$$\frac{1}{2}\sum_{m+p=n}\frac{\varphi(2^m-1)}{m}\frac{\varphi(2^p-1)}{p}+\frac{\varphi\left(\frac{2^n-1}{3}\right)}{n},(m,p)=1 \tag{31}$$

其中，φ 为欧拉函数，当 x 不为整数时，$\varphi(x)=0$。

证明 定理 2 中，对于任意 n 级 LFSR 的特征函数

$$\begin{aligned}&f(x)=c_0x_0\oplus c_1x_1\oplus\cdots\oplus c_{n-1}x_{n-1}\oplus x_n,\\&c_i\in F_2(0\leqslant i\leqslant n-1)\end{aligned} \tag{32}$$

本文要求其为非奇异，即 $c_0=1$。当 $n=1$ 时，$\psi(f(x))$ 只能取 $1\oplus x$，故其圈结构为

$$\Omega\left(\psi\left(f(x)\right)\right)=1[1]+1[1] \tag{33}$$

当 $n>1$ 时，由于 $\psi(f(x))$ 可以分解为若干不可约多项式的乘积，而这些不可约多项式恰好对应级联型反馈移位寄存器中各 LFSR 的特征多项式，当特征多项式为不可约多项式 $\psi(x)$ 时，其圈结构可表示为

$$\Omega\left(\psi(x)\right)=1[1]+\frac{2^n-1}{p\left(\psi(x)\right)}\left[p\left(\psi(x)\right)\right] \tag{34}$$

综上，当 n 为任意正整数时，其分解的不可约多项式对应的 LFSR 圈结构中圈个数至少为 2。根据推论 1，若分解的不可约多项式超过 2 个，则圈个数超过 4，故分解的不可约多项式至多为 2 个。

当 $\psi(f(x))$ 为不可约多项式时，可得

$$p\left[\psi\left(f(x)\right)\right]=\frac{2^n-1}{3} \tag{35}$$

根据文献[35]，F_2 上周期为 l 的 n 次不可约多项式的个数为 $\frac{\varphi(l)}{n}$，在此情形下，其圈个数为 4 的 LFSR 个数为

$$\frac{\varphi\left(\frac{2^n-1}{3}\right)}{n} \tag{36}$$

当 $\psi\left(f(x)\right)$ 分解为 2 个不可约多项式的乘积时，分别设这 2 个不可约多项式为

$$\psi\left(h(x)\right),\psi\left(g(x)\right) \tag{37}$$

且满足 $\psi\left(f(x)\right)=\psi\left(h(x)\right)\psi\left(g(x)\right)$，其级数为 m,p 且 $m+p=n$，根据推论 1，不可约多项式对应的 LFSR 圈结构中圈个数只能为 2，故此时这 2 个不可约多项式即本原多项式，又根据辗转相除法，当且仅当 $(m,p)=1$ 时，有

$$\begin{aligned}&\left(p\left[\psi\left(h(x)\right)\right],p\left[\psi\left(g(x)\right)\right]\right)=\\&(2^m-1,2^p-1)=2^{(m,p)}-1=1\end{aligned} \tag{38}$$

可得

$$\begin{aligned}&\Omega(h*g)=1[1]+1\left[p\left(\psi(h)\right)\right]+1\left[p\left(\psi(g)\right)\right]+\\&1\left[\mathrm{lcm}\left\{p\left(\psi(h)\right),p\left(\psi(g)\right)\right\}\right]\end{aligned} \tag{39}$$

此时，圈个数恰为 4。注意到，当 h 和 g 均为线性情形时，$\Omega(h*g)=\Omega(g*h)$，在此情形下，其圈个数为 4 的 LFSR 个数为

$$\frac{1}{2}\sum_{m+p=n}\frac{\varphi(2^m-1)}{m}\frac{\varphi(2^p-1)}{p},(m,p)=1 \tag{40}$$

综上，本文要求 $n\geqslant 3$ 是因为 m 和 p 不能同时为 1，当 $n=3$ 时，唯一一个圈个数为 4 的 LFSR 的特征函数为 $x_0\oplus x_3$。2 种情形的个数加之，定理 3 即证。证毕。

文献[31]证明了定理 3 中当 $\psi\left(f(x)\right)$ 为不可约多项式时，通过圈合并的方法可得到的 de Bruijn 序列个数为

$$N_n=3x_m^4+(-1)^m4x_m^3+x_m^2 \tag{41}$$

其中，$x_m=\frac{2^m-(-1)^m}{3},n=2m$。本文给出当分解的不可约多项式个数为 2 时，通过圈合并得到的 de Bruijn 序列个数，即定理 4。

定理 4 设任意 m 级和 p 级 LFSR 的特征函数分别为

$$\begin{aligned}&h(x_0,\cdots,x_m)=x_0\oplus h_1x_1\oplus\cdots\oplus h_{m-1}x_{m-1}\oplus x_m\\&g(x_0,\cdots,x_p)=x_0\oplus g_1x_1\oplus\cdots\oplus g_{p-1}x_{p-1}\oplus x_p\end{aligned} \tag{42}$$

其分别对应的 $\psi(h)$ 和 $\psi(g)$ 都是本原多项式，满足 $(m,p)=1$ 且 m 和 p 不同时为 1。令 h 产生的 m 序列为 $\boldsymbol{a}_1=(a_1^{(0)},a_1^{(1)},\cdots,a_1^{(2^m-2)})$，$g$ 产生的 m 序列为 $\boldsymbol{a}_2=(a_2^{(0)},a_2^{(1)},\cdots,a_2^{(2^p-2)})$。又令 $\boldsymbol{a}_1^{(k)}=\left(a_1^{(k)},\cdots,a_1^{(k+m+p-1)}\right),\boldsymbol{a}_2^{(l)}=\left(a_2^{(l)},\cdots,a_2^{(l+m+p-1)}\right)$，则 $\forall k,l$ 有 $\boldsymbol{a}_1^{(k)}\neq\boldsymbol{a}_2^{(l)}$，且只有唯一的一对 k_0,l_0 使 $\boldsymbol{a}_1^{(k_0)},\boldsymbol{a}_2^{(l_0)}$ 是一对共轭点。同时以特征函数为

$$\begin{cases} h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus \\ x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}} \\ h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus \\ x_1^{a_1^{(k_0+1)}}x_2^{a_1^{(k_0+2)}}\cdots x_{m+p-1}^{a_1^{(k_0+m+p-1)}}\oplus x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}} \\ h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus \\ x_1^{a_1^{(k_0+1)}}x_2^{a_1^{(k_0+2)}}\cdots x_{m+p-1}^{a_1^{(k_0+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}} \end{cases}$$

$$\left(0\leqslant k\leqslant 2^m-2,0\leqslant l\leqslant 2^p-2,(k,l)\neq(k_0,l_0)\right) \quad (43)$$

的级联型反馈移位寄存器产生 de Bruijn 序列。且产生周期为 2^{m+p} 的 de Bruijn 序列个数为

$$\sum_{(m,p)=1}^{m+p=n}(2^{n-1}-1)\frac{\varphi(2^m-1)}{m}\frac{\varphi(2^p-1)}{p},n\geqslant 4 \quad (44)$$

证明　根据定理 3 可知，当 $(m,p)=1$ 时，$\Omega(h*g)$ 中的圈个数为 4，故可设对应的圈为 $\{\boldsymbol{0},\boldsymbol{b}_1,\boldsymbol{b}_2,\boldsymbol{b}_1+\boldsymbol{b}_2\}$。由于 $\boldsymbol{a}_1,\boldsymbol{a}_2$ 是 m 序列，故圈 $\boldsymbol{b}_1,\boldsymbol{b}_2$ 上的状态均不可能是共轭的。下证圈 $\boldsymbol{b}_1,\boldsymbol{b}_2$ 之间只有一对共轭状态，设 $(x_0,x_1,\cdots,x_{m+p-1})$ 在 $\boldsymbol{b}_1$ 上，$(x_0\oplus 1,x_1,\cdots,x_{m+p-1})$ 在 $\boldsymbol{b}_2$ 上，则满足

$$\begin{cases} x_0\oplus h_1x_1\oplus h_2x_2\oplus\cdots\oplus h_{m-1}x_{m-1}\oplus x_m=0 \\ x_1\oplus h_1x_2\oplus h_2x_3\oplus\cdots\oplus h_{m-1}x_m\oplus x_{m+1}=0 \\ \vdots \\ x_{p-1}\oplus h_1x_p\oplus\cdots\oplus h_{m-1}x_{m+p-2}\oplus x_{m+p-1}=0 \\ x_0\oplus g_1x_1\oplus g_2x_2\oplus\cdots\oplus g_{p-1}x_{p-1}\oplus x_p=1 \\ x_1\oplus g_1x_2\oplus g_2x_3\oplus\cdots\oplus g_{p-1}x_p\oplus x_{p+1}=0 \\ \vdots \\ x_{m-1}\oplus g_1x_m\oplus\cdots\oplus g_{p-1}x_{m+p-2}\oplus x_{m+p-1}=0 \end{cases} \quad (45)$$

由式(45)的相关结论可证系数行列式 $|R|\neq 0$，故此线性方程只有唯一解，即只有唯一的一对 k_0,l_0 使 $\boldsymbol{a}_1^{(k_0)},\boldsymbol{a}_2^{(l_0)}$ 是一对共轭点。同理可得，$\forall k,l$ 有 $\boldsymbol{a}_1^{(k)}\neq\boldsymbol{a}_2^{(l)}$。易证全零状态的共轭状态在圈 $\boldsymbol{b}_1+\boldsymbol{b}_2$ 上，此时 4 个圈之间的共轭状态分布如图 2 所示，箭头上的数字表示共轭状态对的个数。

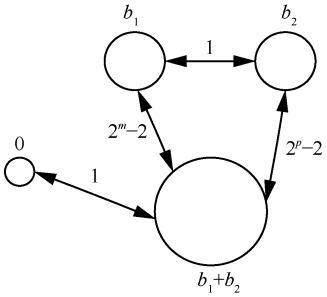

图 2　4 个圈之间的共轭状态分布

使这 4 个圈合并的方式共有 2 种。

1) 先合并圈 $\boldsymbol{b}_2,\boldsymbol{b}_1+\boldsymbol{b}_2$，然后合并 $\boldsymbol{b}_1$，最后合并 $\boldsymbol{0}$。

2) 先合并圈 $\boldsymbol{b}_1,\boldsymbol{b}_2$，然后合并 $\boldsymbol{b}_1+\boldsymbol{b}_2$，最后合并 $\boldsymbol{0}$。

这 2 种方式产生 de Bruijn 序列的特征函数分别为

$$\begin{cases} h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus \\ x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}} \\ h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus \\ x_1^{a_1^{(k_0+1)}}x_2^{a_1^{(k_0+2)}}\cdots x_{m+p-1}^{a_1^{(k_0+m+p-1)}}\oplus x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}} \\ h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus \\ x_1^{a_1^{(k_0+1)}}x_2^{a_1^{(k_0+2)}}\cdots x_{m+p-1}^{a_1^{(k_0+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}} \end{cases}$$

$$\left(0\leqslant k\leqslant 2^m-2,0\leqslant l\leqslant 2^p-2,(k,l)\neq(k_0,l_0)\right) \quad (46)$$

接下来固定 h,g，判定这 2 种方式产生 de Bruijn 序列的个数。

针对方式 1)，本文假设存在一组 (k',l')，满足 $(k',l')\neq(k_0,l_0),(k,l)\neq(k_0,l_0)$，则可得判定式

$$x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}}= x_1^{a_1^{(k'+1)}}x_2^{a_1^{(k'+2)}}\cdots x_{m+p-1}^{a_1^{(k'+m+p-1)}}\oplus x_1^{a_2^{(l'+1)}}x_2^{a_2^{(l'+2)}}\cdots x_{m+p-1}^{a_2^{(l'+m+p-1)}} \quad (47)$$

因为 $(k,l)\neq(k_0,l_0)$，所以

$$\left(a_1^{(k+1)},a_1^{(k+2)},\cdots,a_1^{(k+m+p-1)}\right)\neq \left(a_2^{(l+1)},a_2^{(l+2)},\cdots,a_2^{(l+m+p-1)}\right) \quad (48)$$

将

$$(x_1,x_2,\cdots,x_{m+n-1})=\left(a_1^{(k+1)},a_1^{(k+2)},\cdots,a_1^{(k+m+p-1)}\right) \quad (49)$$

代入判定式，若

$$\begin{aligned} x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}&=x_1^{a_2^{(l'+1)}}x_2^{a_2^{(l'+2)}}\cdots x_{m+p-1}^{a_2^{(l'+m+p-1)}} \\ x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}}&=x_1^{a_1^{(k'+1)}}x_2^{a_1^{(k'+2)}}\cdots x_{m+p-1}^{a_1^{(k'+m+p-1)}} \end{aligned} \quad (50)$$

则 $(k,l')=(k_0,l_0),(k',l)=(k_0,l_0)$，即 $k=k'$。故此方式产生的 de Bruijn 序列个数为

$$(2^m-1)(2^p-1)-1 \quad (51)$$

同理，针对方式 2)，由于只有唯一的小项需要比较，故此方式产生的 de Bruijn 序列个数为

$$(2^m-1)+(2^p-1) \quad (52)$$

综上，固定 h,g 之后，这 4 个圈合并产生 de Bruijn 序列的个数为 $2^{m+p}-2$。下证当 h,g 变化时，只针对方式 1)判定是否有重复的特征函数，而方式 2)显然没有。

设$\psi(h')$和$\psi(g')$分别是m'和p'次本原多项式，且有$m+p=n=m'+p'$，设针对方式 1)产生 de Bruijn 序列的特征函数为

$$h'*g'\oplus x_1^0x_2^0\cdots x_{m'+p'-1}^0\oplus x_1^{a_3^{(k'+1)}}x_2^{a_3^{(k'+2)}}\cdots x_{m'+p'-1}^{a_3^{(k'+m'+p'-1)}}\oplus x_1^{a_4^{(l'+1)}}x_2^{a_4^{(l'+2)}}\cdots x_{m'+p'-1}^{a_4^{(l'+m'+p'-1)}}$$
$$\left((m',p')=1,0\leqslant k'\leqslant 2^{m'}-2,0\leqslant l'\leqslant 2^{p'}-2,(k',l')\neq(k_0',l_0')\right)\tag{53}$$

假设$h*g\neq h'*g'$，则必有$m+n=p\geqslant 4$（一次和二次的本原多项式只有一个），则可得判定式

$$h*g\oplus x_1^0x_2^0\cdots x_{m+p-1}^0\oplus x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}}=$$
$$h'*g'\oplus x_1^0x_2^0\cdots x_{m'+p'-1}^0\oplus x_1^{a_3^{(k'+1)}}x_2^{a_3^{(k'+2)}}\cdots x_{m'+p'-1}^{a_3^{(k'+m'+p'-1)}}\oplus x_1^{a_4^{(l'+1)}}x_2^{a_4^{(l'+2)}}\cdots x_{m'+p'-1}^{a_4^{(l'+m'+p'-1)}}\tag{54}$$

即

$$h*g\oplus h'*g'=x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}}\oplus x_1^{a_3^{(k'+1)}}x_2^{a_3^{(k'+2)}}\cdots x_{m'+p'-1}^{a_3^{(k'+m'+p'-1)}}\oplus x_1^{a_4^{(l'+1)}}x_2^{a_4^{(l'+2)}}\cdots x_{m'+p'-1}^{a_4^{(l'+m'+p'-1)}}\tag{55}$$

因为h,g,h',g'都有x_0,x_{m+p}项，故式(55)左端方程可改写为

$$x_{i_1}\oplus x_{i_2}\oplus\cdots\oplus x_{i_t}\quad(1\leqslant i_1<i_2<\cdots<i_t\leqslant m+p-1,1\leqslant t\leqslant m+p-1)\tag{56}$$

又$\sum_{j=1}^{t}x_{i_j}=1$的解的个数为$2^{t-1}2^{m+p-1-t}=2^{m+p-2}$。而式(55)右端方程为

$$x_1^{a_1^{(k+1)}}x_2^{a_1^{(k+2)}}\cdots x_{m+p-1}^{a_1^{(k+m+p-1)}}\oplus x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}\cdots x_{m+p-1}^{a_2^{(l+m+p-1)}}\oplus x_1^{a_3^{(k'+1)}}x_2^{a_3^{(k'+2)}}\cdots x_{m'+p'-1}^{a_3^{(k'+m'+p'-1)}}\oplus x_1^{a_4^{(l'+1)}}x_2^{a_4^{(l'+2)}}\cdots x_{m'+p'-1}^{a_4^{(l'+m'+p'-1)}}=1\tag{57}$$

的解最多只有 4 个，即当$m+p=n\geqslant 5$时，得出矛盾。当$m+p=n=4$时，可设

$$h=1\oplus x,g=1\oplus x\oplus x^3$$
$$h'=1\oplus x,g'=1\oplus x^2\oplus x^3\tag{58}$$

此时，式(55)右端方程为

$$x_1^{a_2^{(l+1)}}x_2^{a_2^{(l+2)}}x_3^{a_2^{(l+3)}}\oplus x_1^{a_4^{(l'+1)}}x_2^{a_4^{(l'+2)}}x_3^{a_4^{(l'+3)}}=1\tag{59}$$

的解最多只有 2 个，同理得出矛盾。故$h*g=h'*g'$经适当排列可知$h=h',g=g'$。根据定理 3，方式 1)产生的 de Bruijn 序列个数为

$$\frac{1}{2}\sum_{m+p=n}\frac{\varphi(2^m-1)}{m}\frac{\varphi(2^p-1)}{p},(m,p)=1,n\geqslant 4\tag{60}$$

综上，结合这 4 个圈合并产生 de Bruijn 序列的个数为$2^{m+p}-2$可知，由定理 4 描述的特征函数产生 de Bruijn 序列的个数为

$$(2^{m+p}-2)\left[\frac{1}{2}\sum_{(m,p)=1}^{m+p=n}\frac{\varphi(2^m-1)}{m}\frac{\varphi(2^p-1)}{p}\right]=\sum_{(m,p)=1}^{m+p=n}(2^{n-1}-1)\frac{\varphi(2^m-1)}{m}\frac{\varphi(2^p-1)}{p},n\geqslant 4\tag{61}$$

证毕。

由定理 4 可知，当圈个数为 4 的 LFSR 的特征多项式分解为 2 个不可约多项式的情形时，只能通过定理中描述的这几种并圈方式构造 de Bruijn 序列的特征函数。结合定理 3 与文献[31]的相关结论，本文证明了基于全体圈个数为 4 的n级 LFSR 构造n级 de Bruijn 序列的全部数目。定理 4 证明过程中，只要求解出n元线性方程组的解，通过任意 2 个互素的$m,p(m+p=n)$级本原多项式，就可以直接得到定理 4 中没有重复的且数量庞大的n级 de Bruijn 序列特征函数。

3 结束语

本文从圈个数的角度，基于 LFSR 的反馈移位寄存器的级联特征和线性方程的思想，给出了圈个数为 4 的 LFSR 的具体数目，从而给出了基于全体圈个数为 4 的n级 LFSR 构造n级 de Bruijn 序列的并圈方法，并且得到了其全部数目。该方法可以通过任意 2 个级数互素的本原多项式直接构造大级数的 de Bruijn 序列特征函数，同时其分析思路也可以进一步丰富和促进 LFSR 构造 de Bruijn 序列的理论结果。但该方法仍然需要求解一个n元线性方程组，因此在该方法上是否有更具体的 de Bruijn 序列特征函数形式，以及在圈个数上是否可以进一步推广将是笔者下一步研究的内容。

参考文献：

[1] 丁存生, 肖国镇. 流密码学及其应用[M]. 北京: 国防工业出版社, 1994.
DING C S, XIAO G Z. Stream cipher and its applications[M]. Beijing: National Defense Industry Press, 1994.

[2] SIEGENTHALER T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 2006, 34(1): 81-85.

[3] RUEPPEL R A. Analysis and design of stream ciphers[M]. Berlin: Springer, 1986.

[4] COURTOIS N T, MEIER W. Algebraic attacks on stream ciphers with linear feedback[C]//2003 International Workshop on the Theory and

Application of Cryptographic Techniques (EUROCRYPT). Berlin: Springer, 2003: 345-359.

[5] CHAN A H, GAMES R A, KEY E L. On the complexities of de Bruijn sequences[J]. Journal of Combinatorial Theory, Series A, 1982, 33(3): 233-246.

[6] 姜春晓, 王佳蔚. 高动态卫星 DSSS 信号 Turbo 迭代捕获算法[J]. 通信学报, 2021, 42(8): 15-24.
JIANG C X, WANG J W. Turbo iterative acquisition algorithm for satellite high-mobility DSSS signal[J]. Journal on Communications, 2021, 42(8): 15-24.

[7] 许饶琪, 彭晓涛, 秦世耀, 等. 基于 M 序列的双馈风机变流器参数辨识方法研究[J]. 电网技术, 2022, 46(2): 578-586.
XU R Q, PENG X T, QIN S Y, et al. Parameter identification of doubly-fed induction generator converter based on M-sequence[J]. Power System Technology, 2022, 46(2): 578-586.

[8] 曾理, 成杰峰, 孟金涛, 等. 使用分布式 de Bruijn 图遍历基因拼接并行构建和化简[J]. 软件学报, 2013, 24(S2): 140-149.
CENG L, CHENG J F, MENG J T, et al. Parallelized de Bruijn graph construction and simplification for genome assembly[J]. Journal of Software, 2013, 24(S2): 140-149.

[9] FREDRICKSEN H. A class of nonlinear de Bruijn cycles[J]. Journal of Combinatorial Theory, Series A, 1975, 19(2): 192-199.

[10] ETZION T, LEMPEL A. Algorithms for the generation of full-length shift- register sequences[J]. IEEE Transactions on Information Theory, 1984, 30(3): 480-484.

[11] ANNEXSTEIN F S. Generating de Bruijn sequences: an efficient implementation[J]. IEEE Transactions on Computers, 1997, 46(2): 198-200.

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

[13] JANSEN C J A, FRANX W G, BOEKEE D E. An efficient algorithm for the generation of de Bruijn cycles[J]. IEEE Transactions on Information Theory, 1991, 37(5): 1475-1478.

[14] YANG J H, DAI Z D. Construction of m-ary de Bruijn sequences[C]//1992 International Workshop on the Theory and Application of Cryptographic Techniques (EUROCRYPT). Berlin: Springer, 1992: 357-363.

[15] HAUGE E R, MYKKELTVEIT J. On the classification of de Bruijn sequences[J]. Discrete Mathematics, 1996, 148(1/2/3): 65-83.

[16] MYKKELTVEIT J, SZMIDT J. On cross joining de Bruijn sequences[J]. Contemporary Mathematics, 2015, 632: 333-344。

[17] GOLOMB W. Shift register sequences[M]. Los Angeles: Aegean Park Press, 1981.

[18] 关杰, 周琮伟. M 序列反馈函数多项式表示的快速构造方法[J]. 通信学报, 2018, 39(4): 84-90.
GUAN J, ZHOU C W. Method of fast construction of M-sequence feedback functions with polynomial representation[J]. Journal on Communications, 2018, 39(4): 84-90.

[19] 高杨, 刘松华, 王中孝. 一种基于“编织法”的 de Bruijn 序列构造算法[J]. 电子学报, 2018, 46(1): 48-54.
GAO Y, LIU S H, WANG Z X. A de Bruijn sequence construction algorithm based on ‘interleaving’ construction method[J]. Acta Electronica Sinica, 2018, 46(1): 48-54.

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

[21] SIU M K, TONG P. Generation of some de Bruijn sequences[J]. Discrete Mathematics, 1980, 31(1): 97-100.

[22] CHANG Z L, GONG G, WANG Q. Cycle structures of a class of cascaded FSRs[J]. IEEE Transactions on Information Theory, 2020, 66(6): 3766-3774.

[23] LI C Y, ZENG X Y, HELLESETH T, et al. The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs[J]. IEEE Transactions on Information Theory, 2014, 60(5): 3052-3061.

[24] LI C Y, ZENG X Y, LI C L, et al. A class of de Bruijn sequences[J]. IEEE Transactions on Information Theory, 2014, 60(12): 7955-7969.

[25] LI C Y, ZENG X Y, LI C L, et al. Construction of de Bruijn sequences from LFSRs with reducible characteristic polynomials[J]. IEEE Transactions on Information Theory, 2016, 62(1): 610-624.

[26] LI M, JIANG Y P, LIN D D. The adjacency graphs of some feedback shift registers[J]. Designs, Codes and Cryptography, 2017, 82(3): 695-713.

[27] LI M, LIN D D. The adjacency graphs of LFSRs with primitive-like characteristic polynomials[J]. IEEE Transactions on Information Theory, 2017, 63(2): 1325-1335.

[28] CHANG Z L, EZERMAN M F, LING S, et al. Construction of de Bruijn sequences from product of two irreducible polynomials[J]. Cryptography and Communications, 2018, 10(2): 251-275.

[29] DONG Y J, TIAN T, QI W F, et al. The adjacency graphs of FSRs with a class of affine characteristic functions[J]. Finite Fields and Their Applications, 2018, 53: 21-35.

[30] DONG J W, PEI D Y. Construction for de Bruijn sequences with large stage[J]. Designs, Codes and Cryptography, 2017, 85(2): 343-358.

[31] 董军武, 裴定一. 一类不可约多项式的邻接矩阵[J]. 数学学报(中文版), 2018, 61(5): 843-856.
DONG J W, PEI D Y. The adjacency matrix of some class of irreducible polynomials[J]. Acta Mathematica Sinica (Chinese Series), 2018, 61(5): 843-856.

[32] 万哲先, 代宗铎, 刘木兰, 等. 非线性反馈移位寄存器[M]. 北京: 科学出版社, 1978.
WAN Z X, DAI Z D, LIU M L, et al. Non-linear feedback shift register[M]. Beijing: Science Press, 1978.

[33] ZIERLER N. Linear recurring sequences[J]. Journal of the Society for Industrial and Applied Mathematics, 1959, 7(1): 31-48.

[34] MYKKELTVEIT J, SIU M K, TONG P. On the cycle structure of some nonlinear shift register sequences[J]. Information and Control, 1979, 43(2): 202-215.

[35] LIDL R, NIEDERREITER H. Finite fields: encyclopedia of mathematics and its applications[J]. Computers & Mathematics with Applications, 1997, 7: 136.

[作者简介]

周琮伟（1994– ），男，四川眉山人，信息工程大学博士生，主要研究方向为移位寄存器中的数学理论。

胡斌（1972– ），男，河南信阳人，博士，信息工程大学教授、博士生导师，主要研究方向为密码设计与分析。

关杰（1974– ），女，河南郑州人，博士，信息工程大学教授、博士生导师，主要研究方向为密码设计与分析。