一种基于“编织法”的 de Bruijn 序列构造算法

高 杨,刘松华,王中孝
(洛阳外国语学院,河南洛阳 471003)

摘 要: 文章首先给出 n 级 de Bruijn 序列通过“编织法”所产生序列的周期,并证明其中所有 $2n$ 长状态两两不同. 之后,论证出平移等价意义下一条 n 级 de Bruijn 序列仅能编织出两条序列. 最后针对每一条序列,补全其缺失的四个 $2n$ 长状态即可构造出 $2n$ 级 de Bruijn 序列. 由于增添比特的方式有两种,因此由一条 n 级 de Bruijn 序列可构造出四条 $2n$ 级 de Bruijn 序列.

关键词: 序列密码; de Bruijn 序列; 编织法; 平移等价
中图分类号: TN918. 2 **文献标识码:** A **文章编号:** 0372-2112 (2018)01-0048-07
电子学报 URL: http://www. ejournal. org. cn **DOI:** 10. 3969/j. issn. 0372-2112. 2018. 01. 007

A de Bruijn Sequence Construction Algorithm Based on ‘Interleaving’ Construction Method

GAO Yang, LIU Song-hua, WANG Zhong-xiao
(*Luoyang University of Foreign Languages*, *Luoyang*, *Henan* 471003, *China*)

Abstract: Firstly, this paper determines the period of ‘Interleaving’ sequences from de Bruijn sequences of n-stage and proves all $2n$-tuple states are different from each other. Secondly, in the view of shift equivalence, the paper demonstrates that one can only construct two sequences from de Bruijn sequences of n-stage. For each one, the completion of its missing four $2n$-tuple states can construct de Bruijn sequences of $2n$-stage. Since there are two different ways to complete the missing bits, we can finally get four de Bruijn sequences of $2n$-stage from one de Bruijn sequence of n-stage.

Key words: stream cipher; de Bruijn sequence; interleaving method; shift equivalence

1 引言

序列密码因其高效、易于实现及成本低廉等特性在通信和密码领域有着广泛的应用. 线性反馈移位寄存器(Linear Feedback Shift Register, LFSR)序列因其良好的代数结构,其密码性质得到了人们持续的关注和清晰的刻画. 特别地,极大周期 LFSR 序列(亦称 m 序列)具有周期大,元素分布平衡以及良好的自相关性等密码性质. 因此早期的序列密码体制大多采用 m 序列作为驱动序列[1]. 然而近年来,随着相关攻击[2,3]和代数攻击[4,5]的不断发展,基于 LFSR 的密码体制面临越来越多的安全威胁,于是非线性反馈移位寄存器(Nonlinear Feedback Shift Register, NFSR)序列得到了越来越多的关注[6,7]. NFSR 序列因其天然的非线性结构使得代数攻击等传统手段难以奏效. 此外,由于非线性问题的困难性,NFSR 也常常在密码算法中与 LFSR 联合使用以提升整个系统的复杂度,例如 eSTREAM 计划中的 Grain 算法[8]. 在所有 NFSR 序列中,极大周期 NFSR 序列(亦称 M 序列或 de Bruijn 序列)是较为特殊的一类,其周期达到最大值 2^n 且全部 n 长状态出现且仅出现一次. 由于 de Bruijn 序列极好的伪随机性,因此针对该类序列的研究在当今序列密码领域中占有重要地位[9],而快速高效地构造大周期 de Bruijn 序列的意义也是不言而喻的.

利用较低级数 de Bruijn 序列构造高级数 de Bruijn 序列的递归思想在文献[10 ~ 12]中有所体现. 本文借鉴这种思想,首先引入 n 级 de Bruijn 序列的“编织

收稿日期:2016-07-13;修回日期:2017-01-08;责任编辑:李勇锋
基金项目:国家自然科学基金(No. 61502524)

法”[13],得到了周期为 $2^{2n}-4$ 的序列. 基于该序列的特殊性质,在特定位置上增添 4 个比特即可构造出 $2n$ 级 de Bruijn 序列. 此外,由于编织结果不唯一,施行一次算法可以得到多条互不平移等价的 de Bruijn 序列. 该算法不仅使 de Bruijn 序列级数成倍增长,还能由一条 de Bruijn 序列出发构造多条 de Bruijn 序列,实现 de Bruijn 序列构造规模的指数级扩张.

2　准备知识

2.1　周期序列及状态的位置

定义 1[14] 设无限序列 $\underline{a}=(a_0a_1a_2\cdots$, 如果存在一个正整数 l 满足

$$a_{l+k}=a_k,\ k=0,1,2\cdots \tag{1}$$

则称 $\underline{a}$ 是一个周期序列.

满足式(1)的全体 l 中的最小正整数称为 $\underline{a}$ 的周期,记作 $p(\underline{a})$. 此外, 若无特别说明, 本文所讨论的周期序列均用该序列的第一个周期表示.

定义 2　对于任意一条周期为 T 的序列 $\underline{b}$, 将其重复 n 次可以得到一条新的序列, 对序列 $\underline{b}$ 的这一操作称为 n 次复写, 并将 n 次复写的结果记作 $\underline{b}^n$.

本文规定, 序列 $\underline{b}^n$ 的周期为 nT. 对于一条周期为 T 的序列 $\underline{s}=(s_0s_1\cdots s_{T-1})$, r 长状态 $(x_0x_1\cdots x_{r-1})$ 在 $\underline{s}$ 中出现当且仅当存在 $p\in N$, 使得

$$s_{(p+i)\bmod T}=x_i,\ i=0,1,2,\cdots,r-1$$

均成立, 称该状态在 $\underline{s}$ 中的位置为 p. 特别的, 若某一状态在周期序列中多次出现, 规定其在该序列中的位置为所有位置中的最小值.

例 1　给定序列 $\underline{s}=(00010111)$, $p(\underline{s})=8$. 其中 2 长状态 $\hat{w}=01$ 在 $\underline{s}$ 中的位置为 2, 而 4 长状态 $\hat{y}=1100$ 在 $\underline{s}$ 中的位置为 6.

2.2　周期序列的循环右移变换及平移等价

定义 3　将 F_2 上周期序列 $\underline{a}$ 循环右移一位的变换称为 $\underline{a}$ 的循环右移变换, 记为 R. 设 $\underline{a}=(a_0a_1a_2\cdots a_{n-1})$, 则 $\underline{a}$ 在循环右移变换 R 下的象为:

$$R\,\underline{a}=(a_{n-1}a_0a_1\cdots a_{n-2})$$

R^i 表示循环右移变换 R 的 i 次复合:

$$R^i\,\underline{a}=R(R^{i-1}\underline{a})=\cdots=(a_{n-i}a_{n-i+1}a_{n-i+2}\cdots a_{n-i-1})$$

此外, R 的逆变换 R^{-1} 表示循环左移变换, 即

$$R^{-1}\underline{a}=(a_1a_2a_3\cdots a_0).$$

定义 4　对于两条周期序列 $\underline{a}$ 和 $\underline{b}$, 若存在 $d\in Z$, 使得 $\underline{a}=R^d\underline{b}$, 称 $\underline{a}$ 和 $\underline{b}$ 平移等价, 记作 $\underline{a}\sim\underline{b}$; 反之, 则称 $\underline{a}$ 和 $\underline{b}$ 不平移等价, 记作 $\underline{a}\nsim\underline{b}$. 特别的, 当 $d=0$ 时, $\underline{a}=\underline{b}$.

性质 1[15] 对于两条周期均为 l 的序列 $\underline{a}$ 和 $\underline{b}$, 给定任意 m 长状态 $\hat{G}$, 其中 $m<l$. 若 $\hat{G}$ 在 $\underline{a}$ 和 $\underline{b}$ 中出现且仅出现一次, 则 $\underline{a}\sim\underline{b}$ 成立当且仅当 $\hat{G}$ 在 $\underline{a}$ 中的后一比特与 $\underline{b}$ 中的后一比特相同.

2.3　de Bruijn 序列及其变形

一个 n 级 NFSR 产生的序列最多可以包含 2^n 个不同的 n 长状态[16]. 若一条序列的周期为 2^n, 且 2^n 个不同的 n 长状态均出现且仅出现一次, 则称该序列为 n 级 de Bruijn 序列. 对于一条 n 级 de Bruijn 序列, “减变形”和“加变形”规定如下:

“减变形”: 将 de Bruijn 序列中 n 长全 0 状态替换为 $n-1$ 长全 0 状态, n 长全 1 状态替换为 $n-1$ 长全 1 状态, 得到一条周期为 2^n-2 的新序列.

“加变形”: 将 de Bruijn 序列中 n 长全 0 状态替换为 $n+1$ 长全 0 状态, n 长全 1 状态替换为 $n+1$ 长全 1 状态, 得到一条周期为 2^n+2 的新序列.

2.4　编织法

“编织法”(Interleaving Construction)是一种将两条序列合并为一条序列的方法[17],其描述如下[18]:给定两条周期均为 n 的序列 $\underline{s}=(s_0s_1s_2\cdots s_{n-1})$ 和 $\underline{t}=(t_0t_1t_2\cdots t_{n-1})$,可以得到一条周期为 $2n$ 的序列 $(s_0t_0s_1t_1s_2t_2\cdots s_{n-1}t_{n-1})$. 将该序列记作 $In(\underline{s},\underline{t})$,称为由 $\underline{s}$ 和 $\underline{t}$ 编织所得的序列,并将序列 $\underline{s},\underline{t}$ 称为 $In(\underline{s},\underline{t})$ 的基础序列.

特别地,对于一条 de Bruijn 序列,“编织法”指的是对其加、减变形且复写后的序列进行编织.

例 2　$\underline{s}=(00010111)$ 是一条 3 级 de Bruijn 序列, 对其进行“减变形”得到序列 $\underline{a}=(001011)$, 对其进行“加变形”得到序列 $\underline{b}=(0000101111)$. 易知

$$\mathrm{lcm}(p(\underline{a}),p(\underline{b}))=30$$

故我们可以得到如下编织序列:

$In(\underline{b}^{30/10},\underline{a}^{30/6})=In(\underline{b}^3,\underline{a}^5)=$(000001001101101011100101000011001111101001000101100011101111)

容易观察到该序列周期为 60,且其中每个 6 长状态仅出现一次.

3　主要结果

3.1　编织序列的性质

对于 n 级 de Bruijn 序列 $\underline{c}$ 的“编织法”,“减变形”序列 $\underline{a}$ 和“加变形”序列 $\underline{b}$ 的复写次数是确定的. 由 de Bruijn 序列性质知,$p(\underline{c})=2^n$. 进一步地,$p(\underline{a})=2^n-2$, $p(\underline{b})=2^n+2$. 易知,当 $n\geqslant 2$ 时,

$$\gcd(p(\underline{a}),p(\underline{b}))=2$$

故有

$$\mathrm{lcm}(p(\underline{a}),p(\underline{b}))=2^{2n-1}-2$$

因此在编织序列的一个周期中,序列 $\underline{a}$ 复写次数为

$$\mathrm{lcm}(p(\underline{a}),p(\underline{b}))(p(\underline{a})=2^{n-1}+1$$

序列 $\underline{b}$ 的复写次数为

$$\mathrm{lcm}(p(\underline{a}),p(\underline{b}))(p(\underline{b})=2^{n-1}-1$$

故 n 级 de Bruijn 序列产生的编织序列记作

$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$.

定理 1 设序列$\underline{c}$是一条 n 级 de Bruijn 序列,对其进行“减变形”和“加变形”,分别得到两条序列$\underline{a}$和$\underline{b}$,则编织序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$的周期为 $2^{2n}-4$.

证明 易知,$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$由序列$\underline{b}^{2^{n-1}-1}$及序列$\underline{a}^{2^{n-1}+1}$编织而成,这两条序列周期均为

$$\mathrm{lcm}(p(\underline{a}),p(\underline{b}))=2^{2n-1}-2,$$

因此 $T|2^{2n}-4$. 另一方面,由于

$$p(\underline{a})=2^n-2,p(\underline{b})=2^n+2.$$

故对于序列$\underline{a}$,有 $a_i=a_{i+k_1(2^n-2)}$成立; 对序列$\underline{b}$,有 $b_j=b_{j+k_2(2^n+2)}$成立,其中 i ,j , k_1, $k_2\in N$.

设编织序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$的周期为 T,则该序列可表示为$(r_0r_1r_2\cdots r_{T-1})$,亦可表示为$(b_0a_0b_1a_1\cdots b_{T/2-1}a_{T/2-1})$,因此 T 必为偶数.

并有

$$r_s=r_{s+T},s\in N \tag{2}$$

成立.

由编织法的定义知,当 $s=2l$ 时,$r_s=b_l$,故式(2)等价于 $b_l=b_{(s+T)/2}=b_{l+T/2}$,应有 $p(\underline{b})\mid T/2$; 当 $s=2l+1$ 时,$r_s=a_l$,式(2)等价于 $a_l=a_{(s+T-1)/2}=a_{l+T/2}$,应有 $p(\underline{a})\mid T/2$. 因此,有 $2\cdot\mathrm{lcm}(p(\underline{a}),p(\underline{b}))\mid T$,即 $2^{2n}-4\mid T$.

综上所述,序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$的周期为 $2^{2n}-4$. #

易知基础序列$\underline{b}^{2^{n-1}-1}$与$\underline{a}^{2^{n-1}+1}$中分别出现许多重复状态. 故接下来需要考虑的问题是编织序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中特定长度状态的重复情况.

定理 2 序列$\underline{a}$与$\underline{b}$的定义沿用定理 1,则在编织序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中,每个 $2n$ 长状态仅出现一次.

证明 序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中每个 $2n$ 长状态均由$\underline{b}$中某个 n 长状态和$\underline{a}$中某个 n 长状态编织而成. 给定 $0\leqslant i<2^n-2$,记 $\hat{w}_i$ 是序列$\underline{a}$中出现在位置 i 的 n 长状态; 给定 $0\leqslant j<2^n+2$,记 $\hat{y}_j$ 是序列$\underline{b}$中出现在位置 j 的 n 长状态. 那么编织序列中全部 $2n$ 长状态均包含在下列四个集合中:

$$H_1=\{In(\hat{y}_{2i},\hat{w}_{2j})(0\leqslant i\leqslant 2^{n-1},0\leqslant j\leqslant 2^{n-1}-2\}$$
$$H_2=\{In(\hat{y}_{2i+1},\hat{w}_{2j+1})(0\leqslant i\leqslant 2^{n-1},0\leqslant j\leqslant 2^{n-1}-2\}$$
$$H_3=\{In(\hat{w}_{2i},\hat{y}_{2j+1})(0\leqslant i\leqslant 2^{n-1}-2,0\leqslant j\leqslant 2^{n-1}\}$$
$$H_4=\{In(\hat{w}_{2i+1},\hat{y}_{2j})(0\leqslant i\leqslant 2^{n-1}-2,0\leqslant j\leqslant 2^{n-1}\}$$

由于四个集合代表的四种情况在编织序列中的地位等价,因此只需针对其中一类情况展开分析. 我们不妨对 H_1 进行讨论. 若在序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中出现两次 $In(\hat{y}_{2i},\hat{w}_{2j})$,则由定理 1 知

$$2j+k\times(2^n+2)\equiv 2j \bmod 2^n-2$$

成立. 其中$\underline{b}$的复写次数 $k\in\{1,2,\cdots,2^{n-1}-2\}$. 上式等价于 $2^n-2\mid k\times(2^n+2)$. 该式成立当且仅当 k 为 $2^{n-1}-1$ 的倍数,结合 k 的取值范围导出矛盾. 因此,形如 $In(\hat{y}_{2i},\hat{w}_{2j})$的 $2n$ 长状态两两不同,即 H_1 中无重复元素,同理可知,H_2,H_3,H_4 中亦无重复元素.

下面说明,H_1 分别与 H_2,H_3,H_4 无重复元素. 由 de Bruijn 序列定义可知,n 长状态 $\hat{w}_{2i}$与 $\hat{w}_{2i+1}$不可能相同,即状态集

$$\{\hat{w}_{2i}\mid 0\leqslant i\leqslant 2^{n-1}-2\}\text{与}\{\hat{w}_{2i+1}\mid 0\leqslant i\leqslant 2^{n-1}-2\}$$

中无相同元素. 因此形如 $In(\hat{y}_{2i},\hat{w}_{2j})$的 $2n$ 长状态与形如 $In(\hat{y}_{2i+1},\hat{w}_{2j+1})$的 $2n$ 长状态不可能相同,即 H_1 与 H_2 中无相同元素.

更进一步地,序列$\underline{b}$由序列$\underline{a}$增添两个 0 和两个 1 得到,因此据编织法可知

$$\{\hat{y}_{2i}\mid 0\leqslant i\leqslant 2^{n-1}\}=\{\hat{w}_{2i}\mid 0\leqslant i\leqslant 2^{n-1}-2\}\cup\{000\cdots0\}\cup\{111\cdots1\}$$
$$\{\hat{y}_{2i+1}\mid 0\leqslant i\leqslant 2^{n-1}\}=\{\hat{w}_{2i+1}\mid 0\leqslant i\leqslant 2^{n-1}-2\}\cup\{000\cdots0\}\cup\{111\cdots1\}$$

又因集合$\{\hat{w}_{2i+1}\mid 0\leqslant i\leqslant 2^{n-1}-2\}$中不存在 n 长全 0 状态和 n 长全 1 状态,且

$$\{\hat{w}_{2i}\mid 0\leqslant i\leqslant 2^{n-1}-2\}\cap\{\hat{w}_{2i+1}\mid 0\leqslant i\leqslant 2^{n-1}-2\}=\varnothing.$$

由此可知$\{\hat{y}_{2i}\mid 0\leqslant i\leqslant 2^{n-1}\}$与$\{\hat{w}_{2i+1}\mid 0\leqslant i\leqslant 2^{n-1}-2\}$中无相同 n 长状态,故 H_1 与 H_4 中无相同元素. 同理,H_1 与 H_3 中无相同元素.

采用相同方法分析可知,H_i 与 H_j 中均无相同元素,其中 i ,$j\in\{2,3,4\}$. 综上,结论成立. #

由定理 1 知,序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$的周期为 $2^{2n}-4$. 定理 2 又证明了该序列的每个 $2n$ 长状态在一个周期中仅出现一次. 故序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$的一个周期中出现了 $2^{2n}-4$ 个互不相同的 $2n$ 长状态. 这个特殊的性质使人联想到 $2n$ 级 de Bruijn 序列,而本文讨论的“编织法”本身正基于 n 级 de Bruijn 序列. 由此可以看出,“编织法”不失为一种由低级数 de Bruijn 序列出发构造更高级数 de Bruijn 序列的方法. 两者的关系将放在后文深入讨论.

3.2 所有编织情形的讨论

给定一条 n 级 de Bruijn 序列,对其进行“加变形”和“减变形”,会产生诸多平移等价类. 当这些平移等价类作为基础序列时,其编织所得结果相互之间却不一定保持平移等价的关系. 本节考虑在给定原始 de Bruijn 序列条件下基础序列的所有可能情况,并证明不同情况中编织序列的等价性,最后证明出所有情况下的编织序列均归结为两个平移等价类. 以下引理 1 和引理 2 是显然的.

引理 1　设$\underline{a}$是一条周期序列,则

$$R^p\,\underline{a}^i=(R^p\,\underline{a})^i,\text{其中 } p\in Z, i\in N_+.$$

引理 1 表明了序列平移与序列复写两种运算的可交换性. 在后文中,为了表示方便,当序列的平移变化与复写同时出现时,规定对其先进行复写操作再进行平移变换.

引理 2　序列$\underline{a}$与$\underline{b}$的定义沿用定理 1,则有

$$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})\sim In(\underline{a}^{2^{n-1}+1},R^{-1}\underline{b}^{2^{n-1}-1}).$$

上述引理表明,从平移等价的角度来看,任意两条序列编织产生的所有情况均可归结到固定一条序列为起始编织序列的情况. 为了讨论的方便,本文统一将$\underline{b}$作为起始编织序列. 由引理 2 可以直接得到如下推论:

推论　序列$\underline{a}$与$\underline{b}$的定义沿用定理 1,则有

$$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})\sim In(R\,\underline{b}^{2^{n-1}-1},R\,\underline{a}^{2^{n-1}+1}).$$

将$R\underline{b}$视为$\underline{b}$,将$R\underline{a}$视为$\underline{a}$代入推论,即得到:

$$\begin{aligned}&R^2In(R\underline{b}^{2^{n-1}-1},R\underline{a}^{2^{n-1}+1})\\&=R^4In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})\\&=In(R^2\,\underline{b}^{2^{n-1}-1},R^2\,\underline{a}^{2^{n-1}+1})\end{aligned}$$

递推可得:

$$R^{2s}In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})=In(R^s\underline{b}^{2^{n-1}-1},R^s\underline{a}^{2^{n-1}+1}),$$

依此关系可得下述引理.

引理 3　序列$\underline{a}$与$\underline{b}$的定义沿用定理 1,则有

$$In(R^s\underline{b}^{2^{n-1}-1},R^t\underline{a}^{2^{n-1}+1})\sim In(\underline{b}^{2^{n-1}-1},R^{t-s}\underline{a}^{2^{n-1}+1})$$

成立,

其中$s,t\in Z$且$s\leqslant t$.

证明　由上方推论知

$$\begin{aligned}&In(R^s\underline{b}^{2^{n-1}-1},R^t\underline{a}^{2^{n-1}+1})\\&=In(R^s\underline{b}^{2^{n-1}-1},R^s(R^{t-s}\underline{a})^{2^{n-1}+1})\\&=R^{2s}In(\underline{b}^{2^{n-1}-1},R^{t-s}\underline{a}^{2^{n-1}+1})\end{aligned}$$

因此立得结论. #

特别的,当$s>t$时,一定存在$u\in Z$,使得

$$s+u \bmod 2^n+2<t+u \bmod 2^n-2$$

成立,将$R^u\underline{a}$及$R^u\underline{b}$视为$\underline{b}$和$\underline{a}$代入引理 3 时,有

$$\begin{aligned}&In(R^s(R^u\underline{b})^{2^{n-1}-1},R^t(R^u\underline{a})^{2^{n-1}+1})\\&=In(R^{(s+u)\bmod 2^n+2}\underline{b}^{2^{n-1}-1},R^{(t+u)\bmod 2^n-2}\underline{a}^{2^{n-1}+1})\end{aligned}$$

此时满足引理 3 的条件.

引理 3 说明了一个重要的事实,即当两条编织序列同时循环右移变换时,编织结果总可以归结为仅对一条序列循环右移变换的情形.

引理 4　序列$\underline{a}$与$\underline{b}$的定义沿用定理 1,则有

$$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})\nsim In(\underline{b}^{2^{n-1}-1},R\underline{a}^{2^{n-1}+1}).$$

证明　不妨设$\underline{a}$的第一个 n 长状态为 $000\cdots1$,$\underline{b}$的第一个 $n+1$ 长状态为 $000\cdots0$. 易知,在编织序列$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中,$2n$ 长状态 $\hat{G}=00\cdots01$ 的后一比特为 0. 因为序列$\underline{a}$中不存在 n 长全 0 和全 1 状态,因此当$\underline{a}$的前 $n-1$ 比特为 0 时,序列$\underline{a}$的最后一位为 1,换言之,$R\underline{a}^{2^{n-1}+1}$的第一个比特为 1. 另一方面,在 $In(\underline{b}^{2^{n-1}-1},R\underline{a}^{2^{n-1}+1})$中,$2n$ 长状态 $\hat{G}$ 的后一比特为 1.

根据定理 1,$2n$ 长状态 $\hat{G}$ 在序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$与 $In(\underline{b}^{2^{n-1}-1},R\underline{a}^{2^{n-1}+1})$中仅出现一次,且在两序列中,该状态之后的比特不同,故由性质 1 知结论成立. #

下面是本文的核心引理.

引理 5　序列$\underline{a}$与$\underline{b}$的定义沿用定理 1,则有

$$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})\sim In(\underline{b}^{2^{n-1}-1},R^2\,\underline{a}^{2^{n-1}+1}).$$

证明　由定理 1 知,序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中任一 $2n$ 长状态均包含在下列四个集合中:

$$H_1=\{In(\hat{y}_{2i},\hat{w}_{2j})(0\leqslant i\leqslant 2^{n-1},0\leqslant j\leqslant 2^{n-1}-2\}$$

$$H_2=\{In(\hat{y}_{2i+1},\hat{w}_{2j+1})(0\leqslant i\leqslant 2^{n-1},0\leqslant j\leqslant 2^{n-1}-2\}$$

$$H_3=\{In(\hat{w}_{2i},\hat{y}_{2j+1})(0\leqslant i\leqslant 2^{n-1}-2,0\leqslant j\leqslant 2^{n-1}\}$$

$$H_4=\{In(\hat{w}_{2i+1},\hat{y}_{2j})(0\leqslant i\leqslant 2^{n-1}-2,0\leqslant j\leqslant 2^{n-1}\}$$

不妨选取 $2n$ 长状态 $\hat{G}=In(\hat{y}_{2i_0},\hat{w}_{2j_0})$,易知有如下关系式成立:

$$2i_0+(2^n+2)\times v_b=2j_0+(2^n-2)\times v_a\qquad(3)$$

其中v_a,v_b分别为序列$In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$中出现状态$\hat{G}$时,$\underline{a}$和$\underline{b}$的复写次数.

$$v_a\in\{0,1,2,\cdots,2^{n-1}\},\ v_b\in\{0,1,2,\cdots,2^{n-1}-2\}$$

另一方面,由于序列$\underline{a}$进行了两次循环右移变换,故在序列 $In(\underline{b}^{2^{n-1}-1},R^2\,\underline{a}^{2^{n-1}+1})$中,状态 $\hat{G}$ 可表示为$In(\hat{y}_{2i_0},(R^2\hat{w})_{(2j_0-2)\bmod 2^n-2})$,形如$In(\hat{y}_{2i},R^2\hat{w}_{2j})$. 由定理 1 知,$\hat{G}$在$In(\underline{b}^{2^{n-1}-1},R^2\,\underline{a}^{2^{n-1}+1})$中仅出现一次. 因此,$\hat{G}$不可能具有$In(\hat{y}_{2i+1},R^2\hat{w}_{2j+1})$,$In(\hat{w}_{2i},R^2\hat{y}_{2j+1})$或$In(\hat{w}_{2i+1},R^2\hat{y}_{2j})$等形式,故必有如下等式成立.

$$2i_0+(2^n+2)\times v_b'=2j_0-2+(2^n-2)\times v_a'\qquad(4)$$

其中v_a',v_b'分别为序列$In(\underline{b}^{2^{n-1}-1},R^2\,\underline{a}^{2^{n-1}+1})$中出现状态$\hat{G}$时,$\underline{a}$和$\underline{b}$的复写次数.

$$v_a'\in\{0,1,2,\cdots,2^{n-1}\},\ v_b'\in\{0,1,2,\cdots,2^{n-1}-2\}$$

结合式(3)(4),有

$$\begin{aligned}2j_0-2i_0&=(2^n+2)\times v_b-(2^n-2)\times v_a\\&=(2^n+2)\times v_b'-(2^n-2)\times v_a'+2\end{aligned}$$

即 $(2^{n-1}+1)\times(v_b-v_b')+(2^{n-1}-1)\times(v_a'-v_a)=1$.

因为 $\gcd(2^{n-1}+1,2^{n-1}-1)=1$,根据欧几里得扩展算法,$(v_b-v_b')$与$(v_a'-v_a)$均有解,这也从另一个角度说明状态 $\hat{G}$ 在序列 $In(\underline{b}^{2^{n-1}-1},R^2\,\underline{a}^{2^{n-1}+1})$中一定存在.

下面说明状态 $\hat{G}$ 在序列 $In(\underline{b}^{2^{n-1}-1},\underline{a}^{2^{n-1}+1})$与

$In(\underline{b}^{2^{n-1}-1}, R^2\ \underline{a}^{2^{n-1}+1})$中位置差为一固定值. 通过欧几里得扩展算法可知

$$\begin{aligned}1 &= 2^{n-1}-1-2\times(2^{n-2}-1)\\ &= 2^{n-1}-1-[2^{n-1}+1-(2^{n-1}+1)]\times(2^{n-2}-1)\\ &= (1-2^{n-2})\times(2^{n-1}+1)+2^{n-2}\times(2^{n-1}-1)\end{aligned}$$

由于$\underline{b}$在两编织序列中均复写$2^{n-1}-1$次,因此有

$$v_b - v_b^{'} = 1-2^{n-2} \bmod 2^{n-1}-1$$

可见当n取定时,$v_b - v_b^{'}$为一定值,记为$g(n)$. 根据编织法的规则,形如$In(\hat{y}_{2i}, \hat{w}_{2j})$的$2n$长状态$\hat{G}$在序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$中的位置应为$2\cdot(2i+(2^n+2)v_b$,在序列$In(\underline{b}^{2^{n-1}-1}, R^2\ \underline{a}^{2^{n-1}+1})$中位置应为$2\cdot(2i+(2^n+2)v_b^{'})$,故两者位置差可表示为$2\cdot(2^n+2)\cdot g(n)$. 当$n$取定时,该数随之确定. 同理证得形如$In(\hat{y}_{2i+1}, \hat{w}_{2j+1})$,$In(\hat{w}_{2i}, \hat{y}_{2j+1})$,$In(\hat{w}_{2i+1}, \hat{y}_{2j})$的$2n$长状态在两序列中的位置差也为$2\cdot(2^n+2)\cdot g(n)$. 由此可知编织序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$与$In(\underline{b}^{2^{n-1}-1}, R^2\ \underline{a}^{2^{n-1}+1})$中任意两相同$2n$长状态的位置差为一定值$g(n)$. 即

$$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1}) = R^{g(n)} In(\underline{b}^{2^{n-1}-1}, R^2\ \underline{a}^{2^{n-1}+1})$$

因此序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$与$In(\underline{b}^{2^{n-1}-1}, R^2\ \underline{a}^{2^{n-1}+1})$平移等价. #

例 3 给定一条 de Bruijn 序列(00010111),其中$n=3$. 对其进行“加变形”和“减变形”,得到两条序列$\underline{a}=(001011)$,$\underline{b}=(0000101111)$.

$In(\underline{b}^3, \underline{a}^5)=(00000100110110101110010100001100111110100100011011000111011)$

$In(\underline{b}^3, R^2\ \underline{a}^5)=(01010000110011111010010001011000111011110000010011011010111 0)$

易知,有$In(\underline{b}^3, \underline{a}^5)=R^{20}In(\underline{b}^3, R^2\ \underline{a}^5)$或

$$In(\underline{b}^3, R^2\ \underline{a}^5)=R^{40}In(\underline{b}^3, \underline{a}^5)$$成立.

另一方面,根据上方结论,有:

$$v_b - v_b^{'}(=1-2^{3-2} \equiv -1 \bmod 2^{3-1}-1, g(n)=2$$

因此任意 6 长状态在序列$In(\underline{b}^3, \underline{a}^5)$中的位置与在序列$In(\underline{b}^3, R^2\ \underline{a}^5)$中的位置差为$2\cdot(2^n+2)\cdot g(n)=40$.

引理 2 和引理 3 说明了无论编织顺序如何,由序列$R^p\underline{a}^{2^{n-1}+1}, p\in Z$与$R^q\underline{b}^{2^{n-1}-1}, q\in Z$编织所得的全部序列都等价于如下形式

$$In(\underline{b}^{2^{n-1}-1}, R^m\ \underline{a}^{2^{n-1}+1}), m\in Z$$

再结合引理 4 和引理 5 可知,所有形如$In(\underline{b}^{2^{n-1}-1}, R^m\underline{a}^{2^{n-1}+1})$的序列仅包含两个平移等价类,其中一个平移等价类为:

$$\{In(\underline{b}^{2^{n-1}-1}, R^{2k}\underline{a}^{2^{n-1}+1})(k\in N, k<2^{n-1}-1\},$$

另一个为:

$$\{In(\underline{b}^{2^{n-1}-1}, R^{2k+1}\underline{a}^{2^{n-1}+1})(k\in N, k<2^{n-1}-1\}.$$

因此,当n级 de Bruijn 序列c确定后,无论对基础序列$\underline{a}^{2^{n-1}+1}$、$\underline{b}^{2^{n-1}-1}$施行何种循环右移变换,其复写后编织形成的序列有且仅有两个平移等价类. 表述为如下定理.

定理 3 对于任意一条n级 de Bruijn 序列$\underline{c}$,对其进行“减变形”和“加变形”,分别得到两条序列$\underline{a}$和$\underline{b}$. 则所有形如$In(R^{l_1}\underline{b}^{2^{n-1}-1}, R^{l_2}\underline{a}^{2^{n-1}+1})$及$In(R^{l_1}\underline{a}^{2^{n-1}+1}, R^{l_2}\underline{b}^{2^{n-1}-1})$的序列包含在两个平移等价类中,其中$l_1, l_2\in Z$.

3.3 基于“编织法”构造 de Bruijn 序列

接下来,研究“编织法”与 de Bruijn 序列的关系.

由定理 1 和定理 2 知,$p(In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1}))=2^{2n}-4$,一个周期中全部$2n$长状态共$2^{2n}-4$个. 而对于一条$2n$级 de Bruijn 序列,在其一个周期中,全部2^{2n}个$2n$长状态均出现. 经对比,序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$所缺失的四个$2n$长状态为:

$$\hat{A}_1 = 0000\cdots00$$
$$\hat{A}_2 = 1111\cdots11$$
$$\hat{A}_3 = 1010\cdots10$$
$$\hat{A}_4 = 0101\cdots01$$

序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$无法形成以上四个状态的原因在于序列$a$中不存在$n$长片段(000…0)和(111…1). 因此,在序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$适当位置上添加比特使其出现上述四个$2n$长状态,即可实现由编织序列$In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1})$向$2n$级 de Bruijn 序列的转化.

下面给出由n级 de Bruijn 序列构造$2n$级 de Bruijn 序列的“In算法”.

Step1:给定n级 de Bruijn 序列$\underline{c}$,分别对其进行“加变形”和“减变形”得到序列$\underline{b}$和序列$\underline{a}$.

Step2:将序列$\underline{b}$复写$2^{n-1}-1$遍,将序列$\underline{a}$复写$2^{n-1}+1$遍,分别得到$\underline{b}^{2^{n-1}-1}$和$\underline{a}^{2^{n-1}+1}$.

Step3:对$\underline{b}^{2^{n-1}-1}$和$\underline{a}^{2^{n-1}+1}$进行编织,并记

$$I_1 = In(\underline{b}^{2^{n-1}-1}, \underline{a}^{2^{n-1}+1}), I_2 = In(\underline{b}^{2^{n-1}-1}, R\ \underline{a}^{2^{n-1}+1})$$

Step4:对于序列I_1,在连续$2n-1$个 0 后增添 0;在连续$2n-1$个 1 后增添 1,得到$2^{2n}-2$长序列$I_1^{'}$;对于序列I_2,在连续$2n-1$个 0 后增添 0;在连续$2n-1$个 1 后增添 1,得到$2^{2n}-2$长序列$I_2^{'}$.

Step5:在序列$I_1^{'}$中找到$2n-1$长状态 01010…010,在其后增添 10,得到2^{2n}长序列M_1. 在序列$I_1^{'}$中找到$2n-1$长状态 10101…101,在其后增添 01,得到2^{2n}长序列M_2;在序列$I_2^{'}$中找到$2n-1$长状态 01010…010,在其后

增添 10,得到 2^{2n} 长序列 $\underline{M}_3$. 在序列 $\underline{I}_2'$ 中找到 $2n-1$ 长状态 10101…101,在其后增添 01,得到 2^{2n} 长序列 $\underline{M}_4$.

下面以 $\underline{M}_1$ 为例说明,序列 $\underline{M}_2$,$\underline{M}_3$,$\underline{M}_4$ 按相同方法讨论即可.

记 $2n-1$ 长全 0 状态为状态 $\hat{S}$,则序列 $\underline{I}_1$ 中必存在 $2n+1$ 长状态 $1\hat{S}1$,那么 I_1 中 $2n$ 长状态转移部分图示为:

$$\cdots\rightarrow 1\hat{S}\rightarrow\hat{S}1\rightarrow\cdots$$

在 Step4 中,$2n+1$ 长状态 $1\hat{S}1$ 扩展为 $2n+2$ 长状态 $10\hat{S}1$,亦即 $1\hat{S}01$. 结合扩展后状态的两种表示可知,I_1(中 $2n$ 长状态转移图示部分为:

$$\cdots\rightarrow 1\hat{S}\rightarrow\hat{S}0(0\hat{S})\rightarrow\hat{S}1\rightarrow\cdots$$

故在序列 $\underline{I}_1$ 中添加 0 后,除新增 $2n$ 长状态 $\hat{S}0$ 外,原序列诸 $2n$ 长状态转移情况不发生改变. 而 $\hat{S}0$ 即为四个缺失状态之一的 $\hat{A}_1$. 同理在序列 $\underline{I}_1$ 中添加 1 可使 $\hat{A}_2$ 出现,同时不改变原序列诸 $2n$ 长状态转移情况.

下面考虑 Step5. 记 $2n-1$ 长状态 0101…010 为状态 $\hat{u}$,则序列 I_1'(中必存在 $2n+1$ 长状态 $0\hat{u}0$,那么 I'_1 中 $2n$ 长状态转移图示部分为:

$$\cdots\rightarrow 0\hat{u}\rightarrow\hat{u}0\rightarrow\cdots$$

易知 Step5 将 $2n+1$ 长状态 $0\hat{u}0$ 扩展为 $2n+3$ 长状态 $001\hat{u}0$,亦即 $0\hat{u}100$. 结合扩展后状态的两种表示可知,I_1' 中 $2n$ 长状态转移图示部分为:

$$\cdots\rightarrow 0\hat{u}\rightarrow\hat{u}1\rightarrow 1\hat{u}\rightarrow\hat{u}0\rightarrow\cdots$$

故在序列 I_1' 中添加两比特后,除新增 $2n$ 长状态 $\hat{u}1$ 和 $1\hat{u}$ 外,原序列诸 $2n$ 长状态转移情况不发生改变. 而 $\hat{u}1$ 和 $1\hat{u}$ 分别为四个缺失状态中的 $\hat{A}_3$ 和 $\hat{A}_4$.

序列 $\underline{M}_1$ 在 $\underline{I}_1$ 基础上增添了状态 $\hat{A}_1$,$\hat{A}_2$,$\hat{A}_3$,$\hat{A}_4$,同时不改变 $\underline{I}_1$ 原有 $2^{2n}-4$ 个 $2n$ 长状态转移情况. 故序列 $\underline{M}_1$ 是一条 de Bruijn 序列. 同理,$\underline{M}_2$,$\underline{M}_3$,$\underline{M}_4$ 均为 de Bruijn 序列.

例 4　给定 3 级 de Bruijn 序列 $\underline{c}$ = (00010111),则有 b = (0000101111),a = (001011). 最终得到四条 6 级 de Bruijn 序列,如下所示:

$\underline{M}_1$ = (0000001001101101011100101010000110011111101001000101100011101111)

$\underline{M}_2$ = (0000001001101101010111001010000110011111101001000101100011101111)

$\underline{M}_3$ = (0100000011001111010110001010100100110111111100001000111001011011)

$\underline{M}_4$ = (0100000011001111010111000101001001101111110000100011100101110 11)

4　结束语

本文介绍并重新研究了 de Bruijn 序列的“编织法”,结合序列密码应用背景,将该方法加以改进和推广,证明出基础序列发生平移变换的编织序列只包含两个平移等价类. 在此理论基础上给出了一种构造更高级数 de Bruijn 序列的“*In* 算法”,使 de Bruijn 序列的级数得以完成从 n 到 $2n$ 的跃升. 施行一次“编织法”可使一条 n 级 de Bruijn 序列扩展为四条 $2n$ 级 de Bruijn 序列,反复运用此方法可生成大量大级数 de Bruijn 序列,该构造思想在 de Bruijn 序列研究领域上有较为重要的启发意义. 另一方面,“*In* 算法”的简便性和高效性为其带来了广阔的应用前景. 下一步将重点研究“*In* 算法”与拆并圈理论的结合,并试图通过代数学理论深入探讨“*In* 算法”与 de Bruijn 序列特征多项式之间的联系. 此外,仿照两条序列的“编织法”,是否存在对 k 条序列编织形成 kn 级 de Bruijn 序列的算法也是值得深入研究的.

参考文献

[1] 王中孝,戚文峰. 非线性反馈移位寄存器串联分解唯一性探讨[J]. 电子与信息学报,2014,36(7):1656 – 1660.
Wang Zhong-xiao, Qi Wen-feng. On the uniqueness of decomposition of a NFSR into a cascade connection of smaller NFSRs[J]. Journal of Electronics & Information Technology, 2014, 36(7): 1656 – 1660. (in Chinese)

[2] Meier W, Staffelbach O. Fast correlation attacks on certain stream ciphers[J]. Journal of Cryptology, 1989, 1(3): 159 – 176.

[3] Courtois N T. Higher order correlation attacks, XL algorithm and cryptanalysis of toyocrypt[A]. Proceedings of Information Security and Cryptology-ICISC 2002, Lecture Notes in Computer Science 2587[C]. Berlin: Springer-Verlag, 2003. 182 – 199.

[4] Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback[A]. Advances in Cryptology EUROCRYPT 2003[C]. Warsaw, Poland, 2003. 346 – 359.

[5] Meier W, Pasalic E, Carlet C. Algebraic attacks and decomposition of boolean functions[A]. Proceedings of Advances in Cryptology EUROCRYPT 2004, Lecture Notes in Computer Science 3027[C]. Berlin: Springer – Verlag, 2004. 474 – 491.

[6] Turan M S. On the nonlinearity of maximum – length NFSR feedbacks[J]. Cryptography and Communications, 2012, 4(3/4): 233 – 243.

[7] Zhong J, Lin D. Driven stability of nonlinear feedback shift registers with inputs[J]. IEEE Transactions on Communications, 2016, 64(6): 2274 – 2284.

[8] Martin H, Thomas J, Willi M. New Stream Cipher Designs: The eSTREAM Finalists[M]. Berlin: Springer, 2008. 179 – 190.

[9] 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):1066 – 1068.
ZHU Shi-xin, SUN Lin. An algorithm for generating feedback functions of k-ary de Bruijn sequences by raising stage [J]. Acta Electronica Sinica, 2006, 34(6): 1066 – 1068. (in Chinese)

[10] Lempel A. On a homomorphism of the de Brujin graph and its application to design of feedback shift registers [J]. IEEE Transactions on Computers, 1970, 19(12): 1204 – 1209.

[11] Mandal K, Gong G. Crytographically strong de Bruijn sequences with large periods[A]. Proceedings of Selected Area in Crytography, Lecture Notes in Computer Science 7707[C]. Berlin: Springer-Verlag, 2013. 104 – 118.

[12] Abbas A, Mufutau A. A recursive construction of nonbinary de Bruijn sequences[J]. Designs Codes and Cryptography, 2011, 60(2): 155 – 169.

[13] Mitchell C J, Etzion T, Paterson K G. A method for constructing decodable de Brujin sequences[J]. IEEE Transactions on Information Theory, 1996, 42(5): 1472 – 1478.

[14] 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.

[15] Golomb S W. Shift Register Sequences[M]. San Francisco: Aegean Park Press, 1967.

[16] Dubrova E. Generation of full cycles by a composition of NLFSRs[J]. Designs, Codes and Cryptography, 2014, 73(2): 469 – 486.

[17] Gong G. Theory and applications of q-ary interleaved sequences[J]. IEEE Transactions on Information Theory, 1995, 41(2): 400 – 411.

[18] Li N, Tang X, Helleseth T. New M-ary sequences with low autocorrelation from interleaved technique[J]. Designs Codes and Cryptography, 2014, 73(1): 237 – 249.

作者简介

高 杨(通信作者) 男,1994 年生于河南洛阳,现为洛阳外国语学院研究生,主要研究方向为密码学.
E – mail: gaoyang_1279@126.com

刘松华 男,1979 年生于吉林安图,现为洛阳外国语学院研究生,主要研究方向为密码学.
E – mail: liusonghua0519@163.com