arXiv:2602.01134v1 [cs.IT] 1 Feb 2026

高非线性复杂度周期二元序列的结构与计数

Qin Yuan *、Chunlei Li †、Xiangyong Zeng*

摘要

非线性复杂度是衡量序列随机性的重要指标，其定义为能够生成给定序列的最短反馈移位寄存器的长度。本文刻画了非线性复杂度大于或等于 $\lfloor \frac{3n}{4} \rfloor$ 的 n-周期二元序列的结构。基于这些序列的结构，本文确定了此类周期序列数量的精确枚举公式。

关键词：周期序列，非线性复杂度，计数，随机性。

1 引言

伪随机序列在密码学、通信和测距中有广泛应用 [8, 33]。随机性或不可预测性的质量对伪随机序列至关重要。人们提出了各种复杂度度量来评估序列的随机性 [13, 24, 25, 32, 35, 40]。其中，线性复杂度已得到广泛研究 [5, 6, 15–17, 36]。序列的线性复杂度定义为能够生成该序列的最短线性反馈移位寄存器（LFSR）的长度 [23]。

*Q. Yuan 和 X. Zeng 任职于湖北大学智能感知系统与安全重点实验室（教育部）、湖北省应用数学重点实验室、湖北大学数学与统计学院，中国武汉，邮编 430062。电子邮箱：yuanqin2020@aliyun.com，xiangyongzeng@aliyun.com

†C. Li 任职于挪威卑尔根大学信息学系，挪威卑尔根，邮编 N-5020。电子邮箱：chunlei.li@uib.no

通过伯利坎普-梅西算法 [22], ，可以根据周期为 L 的序列的任意一个长度为 $2L$ 的子序列，唯一重构出该序列。为抵御这种攻击，密码系统中的序列应具有较高的线性复杂度。然而，高线性复杂度的序列也可能由短得多的、带有非线性函数的 FSR 生成，这种寄存器称为非线性反馈移位寄存器（NFSR）。与线性复杂度的定义类似，若允许 FSR 的反馈函数任意取值，也就是取消对线性反馈函数的限制，便得到非线性复杂度的概念 [12]。值得注意的是，NFSR 一直是流密码设计中的主要构建模块，例如 Trivium [1], 、Grain [9] 及其变体 Grain128-AEAD；后者进入了 NIST 轻量级密码标准化进程的最终阶段 [27]。另一方面，从理论角度对 NFSR 的认识仍很不充分 [10]。

关于序列非线性复杂度的现有研究包括：序列非线性复杂度的高效计算、最大/较大非线性复杂度序列的构造、具有给定非线性复杂度的序列的计数 [7,13,18,20, 26, 31, 34, 42],，以及非线性复杂度与相关性度量之间的关系 [3, 4, 11]。在非线性复杂度的计算方面，Jansen 和 Boekee [13] 最初将非线性复杂度与有向无环词图的最大深度联系起来，该深度可用于确定给定二元序列的非线性复杂度（剖面）。Rizomiliotis 等人利用相关线性方程的特殊结构，首次研究了二次复杂度 [32] ，随后将其方法扩展到一般的非线性复杂度 [31]。之后，Limniotis、Kolokotronis 和 Kalouptsidis 探讨了非线性复杂度与 Lempel-Ziv复杂度之间的关系，并提出了一种递归算法，用于生成给定序列的最小非线性反馈移位寄存器（NFSR） [20]。

高非线性复杂度序列的构造已得到研究 [18,30, 34, 37, 41, 42]。现有结果主要涉及任意正整数 $n \geq 3$的 n长二元序列和 n周期二元序列。对于 n长序列，Liang等人构造了非线性复杂度不小于 $n/2$ 的二元序列，并基于其结构确定了此类有限长度序列的精确数目 [18]。此外，函数域技术 [14, 38, 39] 已被用于构造具有高非线性复杂度的有限长度序列 [2, 21, 26]。对于具有最大非线性复杂度 $n-1$ 或接近最大非线性复杂度 $n-2$的n周期序列，其结构通过递归方法导出，并且

其精确枚举基于一般结构结果 [34,37]得以确定。最近，通过揭示有限长度序列与相应周期序列之间更为明确的关系，具有任意给定非线性复杂度的所有周期序列得到了深入研究 [42]。然而，对非线性复杂度小于 $n-2$ 的 n周期序列的认识仍然有限。

二元序列的非线性复杂度的计数与分布，为研究非线性复杂度的特性提供了重要的统计视角。Erdmann 和 Mur- phy 通过统计方法估算了各非线性复杂度类别中的序列数量，并提出了非线性复杂度的近似概率分布 [7]。对于周期序列，Petrides 和 Mykkeltveit [28,29] 引入了与非线性复杂度相关的递归结构以及递归上的复合运算，为按照非线性复杂度对周期二元序列进行分类提供了一种有趣的方法。然而，仍有若干情形尚未解决，且现有结果无法用于获得周期序列的精确数量。周期序列的非线性复杂度精确分布仍是一个悬而未决的问题。

对于 n-周期二元序列，目前仅研究了非线性复杂度为 $n-1$ 和 $n-2$ [34,37]的序列的结构与精确计数。根据我们近期在 [42], 中的工作，可以利用一组有限长度代表序列生成所有此类周期序列；然而， [42]并未研究周期序列的显式结构。因此，我们进一步研究具有高非线性复杂度的 n-周期二元序列的结构与计数。本文进一步证明，用于生成非线性复杂度大于或等于 $\lfloor \frac{3n}{4} \rfloor$ 的移位不等价 n-周期序列的有限长序列必定是唯一代表序列。基于这些唯一代表序列，我们推导出非线性复杂度大于或等于 $\lfloor \frac{3n}{4} \rfloor$ 的二元 n-周期序列的结构，并确定了此类序列的精确枚举公式。这些结果给出了此类周期序列的结构及其非线性复杂度的精确分布，并验证了 [7]中的近似统计结果。

本文其余部分的组织如下。第2 节介绍与非线性复杂度相关的基本记号、定义和引理。第3 节从两个不同的角度确定代表序列。第4节确定了 n-周期序列的结构，其中其非线性复杂度大于或等于 $\lfloor \frac{3n}{4} \rfloor$

这一结构。第5节推导出此类周期序列的精确枚举公式。最后，第6 节总结了本文的工作。此外，附录 A-C 给出了文中部分结果的技术性且冗长的证明，以提高可读性。

2 预备知识

本节将回顾由 Jansen 和 Boekee 引入的序列非线性复杂度的一些基础知识 [12,13], ，以及近期在 [42]中获得的关于高非线性复杂度二元周期序列的辅助结果。

定义 1. *([12, 13])* 字母表 $\mathcal{A}$上的序列 s 的非线性复杂度记为 $nlc(s)$，其定义为能够生成序列 s的最短反馈移位寄存器的长度。

对于序列 $\mathbf{s} = (s_0, s_1, \dots)$, 若干正整数 i和 k满足条件，则将项 s_{i+k}称为子序列 $\mathbf{s}_{[i:i+k]} = (s_i, \dots, s_{i+k-1})$ 的后继 。下面回顾序列非线性复杂度的一些性质。

引理 1. *([12, 13])* 序列 s 的非线性复杂度等于其最长相同子序列的长度加一，其中该相同子序列至少出现两次且具有不同的后继。

若一个序列 $(s_0, s_1, \cdots, s_{n-1})$ 由一个长度为 e的短序列重复多次构成，则称其为周期 有限长序列，其中 e 是 n的真因数；否则称其为非周期 有限长序列，或简称为非周期。下文中，$\mathbf{s}_n$ 表示一个非周期有限长序列，而$\mathbf{s}_n^\infty$表示无限长周期序列 $\underbrace{\mathbf{s}_n \cdots \mathbf{s}_n}_{\text{无限}}$.

我们将讨论范围限定为整数环 $\mathbb{Z}_2$ 上的二元序列。

引理 2. *([18])* 对于二元有限长序列 $(s_0, s_1, \dots, s_{n-1})$，若其非线性复杂度为 $c \geq \frac{n}{2}$，则在 $(s_0, s_1, \dots, s_{n-1})$ 中恰好存在一对长度为$c-1$ 且后继不同的相同子序列。

下面将回顾 [42], 中的若干定义和引理，这些内容为后续各节的讨论奠定了基础。

定义2。 对于 $c \geq \lfloor \frac{n}{2} \rfloor$ 和 $1 \leq d \leq$ 最小值$\{n-c, \lfloor \frac{n}{2} \rfloor\}$，我们用 $\mathcal{B}(n,c,d)$ 表示以$\boldsymbol{s}_{c+d}$开头的非周期二进制序列$\boldsymbol{s}_n$ 的集合，定义如下：

$$\mathcal{B}(n,c,d) = \{\, \boldsymbol{s}_n = \boldsymbol{s}_{c+d}\, \boldsymbol{s}_{[c+d:n]} = \underbrace{((s_0,\ldots,s_{d-1})^q\,(s_0,\ldots,s_{r-1},\overline{s}_r)}_{length=c+d}\, \boldsymbol{s}_{[c+d:n]})\,\} \qquad (1)$$

其中 $q = \lfloor \frac{c+d-1}{d} \rfloor$，$0 \leq r = (c+d-1) - qd < d$，$\boldsymbol{s}_d = (s_0,\ldots,s_{d-1})$ 是非周期的，q 重复 $(s_0,\ldots,s_{d-1})$ $\underline{\ }^q = \boldsymbol{s}_d \ldots \boldsymbol{s}_d$，$s_r = s_r \oplus 1$，且子序列 $\boldsymbol{s}_{[c+d:n]}$ 从 $\mathbb{Z}_2^{n-c-d}$中任意选取。参数 d 称为$\boldsymbol{s}_n$的间距。我们定义集合

$$\mathcal{B}(n,c) = \bigcup_{d=1}^{\min\{n-c,\lfloor \frac{n}{2} \rfloor\}} \mathcal{B}(n,c,d).$$

注意，由于 $c \geq \lfloor \frac{n}{2} \rfloor$，式（1）的结构保证序列 $\mathbf{s}_n$无论其子序列 $\mathbf{s}_{[c+d:n]} \in \mathbb{Z}_2^{n-c-d}$如何选择，都是非周期的。为确定具有 $\mathbf{s}_n^{\infty}$和 $\mathbf{s}_n \in \mathcal{B}$（$n$，$c$）的周期序列的非线性复杂度，$\mathbf{s}_n$ 的添加项在 [42]中被引入。

定义 3. 给定一个正整数 t，若序列 $\boldsymbol{s}_n$属于 $\mathcal{B}(n,c,d)$且满足

$$s_{n-1-i} = s_{(d-1-i) \bmod d} \ \ for\ 0 \leq i < t,\ \ and\ s_{n-1-t} \neq s_{(d-1-t) \bmod d},$$

则称 $s_{n-t},\ldots,s_{n-1}$为 $\boldsymbol{s}_n$ 的添加项，并将 $(\boldsymbol{s}_n)$ 记为 $\boldsymbol{s}_n$的添加项数。

定义左循环移位算子 $L^i(\mathbf{s}_n) = (s_i, s_{i+1},\ldots,s_{n-1}, s_0,\ldots,s_{i-1})$ 和右循环移位算子 $R^i(\mathbf{s}_n) = (s_{n-i},\ldots,s_{n-1}, s_0,\ldots,s_{n-i-1})$，其中 $i \geq 1$。引理 3 展示了 $nlc(\mathbf{s}_n)$ 和 $add(\mathbf{s}_n)$ 在循环移位算子作用下的变化规律。

引理 3. *([42])* (i) 对于 $\boldsymbol{s}_n \in \mathcal{B}(n,c,d)$ 以及正整数 $k < c$，其左移位序列$L^k(\boldsymbol{s}_n)$ 属于 $\mathcal{B}(n, c-t, d)$。特别地，当 $c-k \geq \lfloor \frac{n}{2} \rfloor$时，有

$$nlc(L^k(\boldsymbol{s}_n)) = nlc(\boldsymbol{s}_n) - k = c - k.$$

(ii) 对于$\boldsymbol{s}_n \in \mathcal{B}(n,c,d)$，若 $c \geq \lfloor \frac{n}{2} \rfloor$且 $add(\boldsymbol{s}_n) = t$，则有 $t < n-c$；而对于 $1 \leq k \leq \min\{t, n-c-d\}$，则有

$$R^k(\boldsymbol{s}_n) \in \mathcal{B}(n, c+k, d),\ \ nlc(R^k(\boldsymbol{s}_n)) = c+k,\ \ and\ \ \ add(R^k(\boldsymbol{s}_n)) = t-k.$$

定义 4. 设$\boldsymbol{s}_n$ 是 $\mathcal{B}(n, c)$ 中的一个序列，且 $E(\boldsymbol{s}_n) = \{R^k(\boldsymbol{s}_n) : 0 \le k < n\} \cap \mathcal{B}(n, c)$。满足以下条件的序列 $\widetilde{\boldsymbol{s}}_n \in E(\boldsymbol{s}_n)$

$$add(\widetilde{\boldsymbol{s}}_n) \ge add(\boldsymbol{a}_n), \forall\, \boldsymbol{a}_n \in E(\boldsymbol{s}_n)$$

称为$\boldsymbol{s}_n$的一个代表序列。此外，我们用 $\mathcal{R}(n, c)$ 表示 $\mathcal{B}(n, c)$中所有序列代表元的集合，即

$$\mathcal{R}(n, c) = \bigcup_{\boldsymbol{s}_n \in \mathcal{B}(n,c)} \left\{ \widetilde{\boldsymbol{s}}_n \in E(\boldsymbol{s}_n) : add(\widetilde{\boldsymbol{s}}_n) \ge add(\boldsymbol{a}_n), \forall\, \boldsymbol{a}_n \in E(\boldsymbol{s}_n) \right\}. \tag{2}$$

读者可参阅 [42, 例 1] 以更好地理解定义 2-4中的符号。

引理 4。 *([42])* 对于$\boldsymbol{s}_n \in \mathcal{R}(n, c)$ 且满足 $c \ge \lfloor \frac{n}{2} \rfloor$的情形，有 $nlc(\boldsymbol{s}_n^{\infty}) = nlc(\boldsymbol{s}_n) + add(\boldsymbol{s}_n)$。

引理 4 表明，若能确定 $\mathbf{s}_n$的一个序列代表元，则$nlc(\mathbf{s}_n^{\infty})$ 便可根据 $nlc(\mathbf{s}_n)$ 和 $add(\mathbf{s}_n)$直接计算得出。需要注意的是，刻画序列 $\mathbf{s}_n$ 的代表元并非易事，因为这需要了解 $E(\mathbf{s}_n)$中所有序列添加项的变化情况。中的一些工作 n使得我们能够生成所有非线性复杂度大于或等于 $\frac{n}{2}$ 的周期序列，如下所述。

引理 5。 *([42])* 设 n和 ω是两个正整数，且 $\omega \ge \frac{n}{2}$。设 $\mathcal{P}(n, \omega)$ 为周期为 n、非线性复杂度为 ω的二元序列集合，并将 $\mathcal{R}(n, \lceil \frac{n}{2} \rceil)$ 定义为(2)。那么，

$$\widetilde{\mathcal{P}}(n, \omega) = \left\{ (R^k(\boldsymbol{s}_n))^{\infty} : \boldsymbol{s}_n \in \mathcal{R}(n, \lceil \tfrac{n}{2} \rceil),\, add(\boldsymbol{s}_n) = \omega - \lceil \tfrac{n}{2} \rceil, 0 \le k < n \right\}.$$

尽管引理 5 提供了一种利用有限长度代表序列生成二元周期序列的方法，但它并未确定 $\mathcal{R}(n, \lceil \frac{n}{2} \rceil)$中相应代表序列的确切形式。为进一步刻画周期序列的精确结构，首先需要研究其性质以及

代表序列的构造。根据引理 3 (ii)，我们有

$$
\begin{aligned}
& \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \mathcal{R}(n, \lceil \tfrac{n}{2} \rceil),\, add(\mathbf{s}_n) = \omega - \lceil \tfrac{n}{2} \rceil, 0 \le k < n\} \\
= \; & \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \bigcup_{1 \le d \le n-\omega} \mathcal{R}(n, \lceil \tfrac{n}{2} \rceil, d),\, add(\mathbf{s}_n) = \omega - \lceil \tfrac{n}{2} \rceil, 0 \le k < n\} \bigcup \\
& \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \bigcup_{n-\omega < d \le \lfloor \frac{n}{2} \rfloor} \mathcal{R}(n, \lceil \tfrac{n}{2} \rceil, d),\, add(\mathbf{s}_n) = \omega - \lceil \tfrac{n}{2} \rceil, 0 \le k < n\} \\
= \; & \bigcup_{1 \le d < n-\omega} \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \mathcal{R}(n, \omega, d), add(\mathbf{s}_n) = 0, 0 \le k < n\} \\
& \bigcup \bigcup_{n-\omega \le d \le \lfloor \frac{n}{2} \rfloor} \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \mathcal{R}(n, n-d, d),\, add(\mathbf{s}_n) = \omega + d - n, 0 \le k < n\}.
\end{aligned} \tag{3}
$$

~因此，为了确定 $\mathcal{P}(n,\ \omega)$ 的结构及其数量，我们将首先分别在第 $\mathcal{R}(n,\ n-d,\ d)$ 中刻画具有最大间距的序列代表$\mathcal{R}(n,\ \omega,\ d)$ 中具有高非线性复杂度的代表序列 ω，详见第3节。

3 序列代表的刻画

本节从两个不同角度考察有限长序列成为代表序列的条件。通过分析，我们在第3.1小节中给出具有最大间距的代表序列的充要条件，并在第3.2小节中进一步提出一种基于非线性复杂度的判据，用于识别代表序列。

以下引理将在本节中用于确定序列代表 n.

引理6. 设 $c \ge \lfloor \frac{n}{2} \rfloor$ 且 $s_{\bar{n}} \in \mathcal{B}(n, c, d_1)$ 满足 $add(s_n) = t_1$。假设 s_n 具有一个移位等价序列 $R^h(s_n) \in \mathcal{B}(n, c, d_2)$，且 $add(R^h(s_n)) = t_2$。令 $b = (n - c - d_1) - h$。则 $t_1 \le b < d_1 + d_2 - t_2$。

引理6 的技术证明见附录 A。

3.1 具有最大间距的序列代表 g

设 $c \ge \lceil \frac{n}{2} \rceil$。为确定周期序列的结构，本小节将给出一个充要条件，用以判断 $\mathcal{B}(n, c, d)$ 中具有最大间距 $d = n - c$ 的序列 $\mathbf{s}_n$ 是否可以作为序列代表元。此外，其非线性

复杂度可以直接确定。下文将给出本小节的主要结果，随后介绍证明中用到的辅助结果。

命题1. 设 $c \geq \lceil \frac{2n-1}{3} \rceil$ 且$\boldsymbol{s}_n$ 为$\mathcal{B}(n, c, d)$ 中的一个序列，且 $d = n - c$。则$\boldsymbol{s}_n \in \mathcal{R}(n, c)$ 当且仅当$\boldsymbol{s}^{[d:n]}$ 不能表示为$\boldsymbol{s}^{[d:n]} = (s_0, s_1, \ldots, s_{b-1})^l$，对任意非周期子序列$(s_0, \ldots, s_{b-1})$，其中 $b > 1$ 为 c的真因数。

为证明命题1，我们首先刻画间距 d，即移位序列$\mathbf{s}_n$ 在具有更多添加项时的间距。

引理 7. 设 $c \geq \lceil \frac{n}{2} \rceil$ 且$\boldsymbol{s}_n$ 为 $\mathcal{B}(n, c, d_1)$ 中的一个序列，且 $d_1 = n - c$，$add(\boldsymbol{s}_n) = t_1$。假设对某个整数 $0 < b < n$，移位序列 $R^b(\boldsymbol{s}_n) \in \mathcal{B}(n, c, d_2)$ 满足$add(R^b(\boldsymbol{s}_n)) = t_2 \geq t_1$。若 $d_1 + d_2 \leq c + t_2 + t_1 + 1$，则 $b = d_2$。

引理7 的证明见附录B。引理 $d_1 + d_2 \leq c + t_2 + t_1 + 1$ 7中的条件可以转化为关于非线性复杂度的条件。

推论1。设 $c \geq \lceil \frac{2n-1}{3} \rceil$ 和一个序列$\boldsymbol{s}_n \in \mathcal{B}(n, c, d_1)$ 满足 $d_1 = n - c$ 且$add(\boldsymbol{s}_n) = t_1$。如果存在正整数 $0 < b < n$，使得 $R^b(\boldsymbol{s}_n) \in \mathcal{B}(n, c, d_2)$满足 $add(R^b(\boldsymbol{s}_n)) = t_2 \geq t_1$，那么 $b = d_2$。

证明。由于 $c \geq \lceil \frac{2n-1}{3} \rceil$，我们有 $d_1 + d_2 \leq 2(n - c) \leq c + 1 \leq c + t_2 + t_1 + 1$. 因此，结论可直接由引理7得出。 □

根据上述准备，下面证明命题 1 。

命题1的证明。根据定义 4，只需证明：当且仅当 $\mathbf{s}_n$ 可以表示为 $\mathbf{s}^{[d:n]} = (s_0, \ldots, s_{b-1})^l$，其中 $l \geq 2$ 且 $(s_0, \ldots, s_{b-1})$ 是非周期序列时，$\mathbf{s}_n$ 在 $\mathcal{B}(n, c)$ 中有一个移位等价序列 $R^b(\mathbf{s}_n)$，且满足 $add(R^b(\mathbf{s}_n)) > add(\mathbf{s}_n)$。

对于充分性，由于 $\mathbf{s}^{[d:n]} = (s_d, \ldots, s_{n-b}, \ldots, s_{n-1}) = (s_0, s_1, \ldots, s_{b-1})^l$ 满足 $b < n - d$，可以得到 $(s_{n-b}, \ldots, s_{n-1}) = (s_0, \ldots, s_{b-1})$。此外，根据 $\mathbf{s}_n \in \mathcal{B}(n, c, d)$，

$$\mathbf{s}_c = ((s_0, s_1, \ldots, s_{b-1})^{l-1}(s_0, s_1, \ldots, s_{b-1} \oplus 1)).$$

因此，移位等价序列 $R^b(\mathbf{s}_n)$ 可表示如下，

$$\begin{aligned} R^b(\mathbf{s}_n) &= ((s_{n-b}, \ldots, s_{n-1})(s_0, \ldots, s_{c-1})(s_c, \ldots, s_{n-b-1})) \\ &= ((s_0, \ldots, s_{b-1})(s_0, s_1, \ldots, s_{b-1})^{l-1}(s_0, s_1, \ldots, s_{b-1} \oplus 1)(s_c, \ldots, s_{n-b-1})) \\ &= ((s_0, s_1, \ldots, s_{b-1})^l(s_0, s_1, \ldots, s_{b-1} \oplus 1)(s_c, \ldots, s_{n-b-1})). \end{aligned}$$

由于 $(l-1)b+b=c$，显然 $R^b(\mathbf{s}_n)$ 属于集合 $\mathcal{B}(n,c,b)$，其中 $b<n-d=\min\{n-c,c\}$。接下来只需证明 $add(R^b(\mathbf{s}_n)) > add(\mathbf{s}_n)$。对于 $\mathbf{s}_n=(s_0,\ldots,s_{d-1})(s_0,s_1,\ldots,s_{b-1})^l$，令 $add(\mathbf{s}_n)=t_1$，由引理 3 (ii) 可得 $t_1 \le n-c-1 \le d$。根据定义 3 和 $t_1 \le d$，可得

$$\begin{cases} s_{(b-1-i) \bmod b} = s_{d-1-i},\ 0 \le i < t_1, \\ s_{(b-1-t_1) \bmod b} \neq s_{d-1-t_1}. \end{cases} \tag{4}$$

由于 $bl=n-d \ge d \ge t_1$，$\mathbf{s}_n$ 的添加项是在 $(s_0,\ s_1,\ \ldots\ldots,\ s_{b-1})^l$ 末尾长度为 t_1 的子序列。根据 $\mathbf{s}^{[d:n]}=(s_0,\ s_1,\ \ldots\ldots,\ s_{b-1})^l$，$R^b(\mathbf{s}_n)$ 也可以表示为以下形式，

$$\begin{aligned} R^b(\mathbf{s}_n) &= ((s_{n-b},\ldots,s_{n-1})(s_0,\ldots,s_{d-1})(s_d,\ldots,s_{n-b-1})) \\ &= ((s_0,\ldots,s_{b-1})(s_0,\ldots,s_{d-1})(s_0,\ldots,s_{b-1})^{l-1}). \end{aligned}$$

因此，由定义 3 和（4）可得

$$add(R^b(\mathbf{s}_n)) = (l-1)b + add(\mathbf{s}_n). \tag{5}$$

因此，根据 $l \ge 2$，$R^b(\mathbf{s}_n) \in \mathcal{B}(n,\ c,\ b)$ 且 $add(R^b(\mathbf{s}_n)) > add(\mathbf{s}_n)$。

对于必要性，由于 $\mathbf{s}_n$ 具有移位等价序列 $R^b(\mathbf{s}_n) \in \mathcal{B}(n,c)$，且 $add(R^b(\mathbf{s}_n)) > add(\mathbf{s}_n)$，根据 $c \ge \lceil \frac{2n-1}{3} \rceil$ 和推论1，可得 $R^b(\mathbf{s}_n) \in \mathcal{B}(n,c,b)$。令 $\mathbf{v}_n = R^b(\mathbf{s}_n)$，则 $s_i = v_{i+b}$ 和 $v_{i_1} = v_{i_1+b}$，其中 $0 \le i_1 \le c$。因此，$(v_0,v_1,\ldots,v_{b-1}) = (v_b,v_{b+1},\ldots,v_{2b-1}) = (s_0,s_1,\ldots,s_{b-1})$。这意味着 $(s_0,\ldots,s_{b-1})$ 是非周期的，并且

$$\mathbf{v}_{c+b} = (s_0,s_1,\ldots,s_{b-1})^q(s_0,\ldots,s_{r-1},\overline{s}_r). \tag{6}$$

由于$\mathbf{s}_n \in \mathcal{B}(n,c,d)$，我们有$(s_{c-b},\ldots,s_{c-2},s_{c-1}) = (s_{n-b},\ldots,s_{n-2},s_{n-1})$，也就是说，

$$(v_c,\ldots,v_{c+b-2},v_{c+b-1}) = (v_0,\ldots,v_{b-2},\overline{v}_{b-1}).$$

回顾一下，$(v_0,v_1,\ldots,v_{b-1}) = (s_0,s_1,\ldots,s_{b-1})$，因此显然

$$(v_c,\ldots,v_{c+b-2},v_{c+b-1}) = (s_0,s_1,\ldots,\overline{s}_{b-1}).$$

结合（6）可知，$(s_{r+1},\ldots,s_{b-1})(s_0,\ldots,s_{r-1},s_r) = (s_0,s_1,\ldots,s_{b-1})$，这意味着 $r=b-1$，因为非周期序列 $\mathbf{s}_b$ 的所有移位都彼此不同。因此，$\mathbf{v}_{c+b} = (s_0,s_1,\ldots,s_{b-1})^q(s_0,s_1,\ldots,s_{b-1})$。所以，$R^b(\mathbf{s}_n)$的前 c 项满足

$$(s_{n-b},\ldots,s_{n-1},s_0,\ldots,s_{c-b-1}) = (s_0,\ldots,s_{b-1})^l.$$

由 $s_i = s_{i+d}, 0 \le i \le c-2$ 可得

$$((s_0, s_1, \ldots, s_{c-b-1})(s_{n-b}, \ldots, s_{n-1})) = ((s_d, s_{d+1}, \ldots, s_{n-b-1})(s_{n-b}, \ldots, s_{n-1})) = \mathbf{s}_{[d:n]}.$$

结合上述两个方程可得$\mathbf{s}^{[d:n]} = (s_0, s_1, \ldots\ldots, s_{b-1})^l$，其中 $n-d = c = bl$。由此即可得出所需结论。□

按照命题 1中必要性部分的证明，我们立即得到以下推论。

推论 2。设 $c \ge \lceil \frac{n}{2} \rceil$ 且 $\boldsymbol{s}_n \in \mathcal{B}(n, c, d)$ 满足 $d = n - c$。若其移位序列$R^b(\boldsymbol{s}_n) \in \mathcal{B}(n, c, b)$，则

(i) 当 $add(R^b(\boldsymbol{s}_n)) \ge add(\boldsymbol{s}_n)$时，我们有 $\boldsymbol{s}^{[d:n]} = (s_0, s_1, \ldots\ldots, s_{b-1})^l$，其中 $(s_0, \ldots\ldots, s_{b-1})$ 是一个特定的非周期子序列，且整数 $l \ge 2$。

(ii) 当 $add(R^b(\boldsymbol{s}_n)) > add(\boldsymbol{s}_n)$时，我们有 $1 \le b < d, b \mid n-d$；若 $d \ne \frac{n}{2}$，则 $b \nmid d$。

证明。（i）由命题 1的必要性证明可得。

（ii）由（i）可知，$\mathbf{s}^{[d:n]} = (s_0, \ldots, s_{b-1})^l$，因此可得 $b \mid n-d$。由于 $R^b(\mathbf{s}_n) \in \mathcal{B}(n, c, b)$，我们得到 $1 \le b \le d = n - c$。当 $d \ne \frac{n}{2}$ 时，$\mathbf{s}^{[d:2d]}$ 是 $\mathbf{s}^{[d:n]} = (s_0, \ldots, s_{b-1})^l$ 的子序列。因此，如果 $b \mid d$，则 $\mathbf{s}_d = \mathbf{s}^{[d:2d]} = (s_0, \ldots, s_{b-1})^m$，且 $d = bm$。由（1）可知，$\mathbf{s}_d$ 是非周期序列，矛盾。因此，如果 $d \ne \frac{n}{2}$，则 $b \nmid d$ 和$b < d$。当 $d = \frac{n}{2}$ 时，如果 $b = d$，则显然有 $add(R^b(\mathbf{s}_n)) = add(\mathbf{s}_n)$，矛盾。因此，$b \ne d$。所以，$1 \le b < d$、$b \mid n-d$，并且当 $d \ne \frac{n}{2}$ 时，$b \nmid d$。 □

根据命题1，若存在整数 b 满足 $1 < b < c$ 使得$\mathbf{s}^{[d:n]} = (s_0, \ldots, s_{b-1})^l$对某个非周期子序列$(s_0, \ldots, s_{b-1})$成立，则这样的整数 b是唯一的，从而意味着序列 $R^b(\mathbf{s}_n)$ 也是唯一的。现在我们可以给出相应周期序列$\mathbf{s}_n^\infty$的非线性复杂度。

推论*3.* 设 $c \ge \lceil \frac{2n-1}{3} \rceil$。对于满足 $d = n-c$的$\boldsymbol{s}_n \in \mathcal{B}(n, c, d)$，若$\boldsymbol{s}^{[d:n]} = (s_0, s_1, \ldots, s_{b-1})^l$对某个非周期子序列$(s_0, s_1, \ldots, s_{b-1})$及整数 $l \ge 2$成立，则 $R^b(\boldsymbol{s}_n)$是序列代表元，且 $nlc(\boldsymbol{s}_n^\infty) = c+n-d-b+add(\boldsymbol{s}_n)$；否则，$\boldsymbol{s}_n$ 是序列代表元，且 $nlc(\boldsymbol{s}_n^\infty) = c + add(\boldsymbol{s}_n)$。

证明。根据命题1，满足 $d = n - c$ 的 $\mathbf{s}_n \in \mathcal{B}(n, c, d)$ 要么只有一个移位等价序列 $R^b(\mathbf{s}_n)$，满足 $add(R^b(\mathbf{s}_n)) > add(\mathbf{s}_n)$，要么不存在这样的移位等价序列。当存在一个整数 b 满足 $\mathbf{s}^{[d:n]} = (s_0, \ldots, s_{b-1})^l$ 时，$R^b(\mathbf{s}_n)$ 是

$ES(\mathbf{s}_n)$ 的序列代表元。由 (5) 可得 $add(R^b(\mathbf{s}_n)) = (l-1)b + add(\mathbf{s}_n) = n - d - b + add(\mathbf{s}_n)$。根据引理 4，可得 $nlc(\mathbf{s}_n^\infty) = c + add(R^b(\mathbf{s}_n)) = n + c - d - b + add(\mathbf{s}_n)$。当不存在正整数 b 满足 $\mathbf{s}^{[d:n]} = (s_0, \ldots, s_{b-1})^l$ 时，由命题1可知 $\mathbf{s}_n$ 是 $ES(\mathbf{s}_n)$ 的序列代表元，这意味着根据引理 4，$nlc(\mathbf{s}_n^\infty) = c + add(\mathbf{s}_n)$。证明完毕。

□

根据实验数据，我们观察到，推论1在对非线性复杂度施加较弱限制的条件下 c仍然成立。然而，无法使用相同的技术加以证明。下面给出一个猜想。注意，如果该猜想成立，那么命题1 和推论3 中的结论也可以类似地对序列$\mathbf{s}_n \in \mathcal{B}(n, c, n-c)$进行证明，其中 $c \geq \lceil \frac{n}{2} \rceil$。

猜想1。 对于 $c \geq \lceil \frac{n}{2} \rceil$ 以及$\boldsymbol{s}_n \in \mathcal{B}(n, c, n-c)$，如果存在一个整数 $0 < b < n$使得 $R^b(\boldsymbol{s}_n) \in \mathcal{B}(n, c, d_2)$ 满足 $add(R^b(\boldsymbol{s}_n)) > add(\boldsymbol{s}_n)$，则 $b = d_2$。

3.2 确定具有高非线性复杂度的序列代表元

对于 $\mathcal{B}(n, c)$ 中的$\mathbf{s}_n$，若 $c \geq \lfloor \frac{n}{2} \rfloor$，则集合 $E(\mathbf{s}_n) = \{L^k(\mathbf{s}_n) : 0 \leq k < n\} \cap \mathcal{B}(n, c)$ 可能包含多个序列。在本节中，我们将建立一个下界 c_0，使得具有非线性复杂度 $c \geq c_0$ 的序列$\mathbf{s}_n$ 是一个序列代表元，从而能够确定周期序列的结构，并直接将$\mathbf{s}_n^\infty$的非线性复杂度计算为 $nlc(\mathbf{s}_n^\infty) = nlc(\mathbf{s}_n) + add(\mathbf{s}_n)$。

定理1。 设 $n \geq 1$和 k为整数。对于序列 $\boldsymbol{s}_n \in \mathcal{B}(n, c)$，若 $c \geq c_0 = \lfloor \frac{3n}{4} \rfloor$，则 $\boldsymbol{s}_n \in \mathcal{R}(n, c)$，并且 $\boldsymbol{s}_n^\infty$的非线性复杂度满足 $nlc(\boldsymbol{s}_n^\infty) = nlc(\boldsymbol{s}_n) + add(\boldsymbol{s}_n)$。

此外，偶数 n 的紧界 c_0 为 $c_0 =$ $\begin{cases} \lfloor \frac{3n}{4} \rfloor - 1, & n = 8k, \ \forall k, \lfloor \frac{3n}{4} \rfloor \text{ 为奇数时；} \\ \lfloor \frac{3n}{4} \rfloor - 2, & n = 8k+2, 8k+6, \ \forall k, \\ & n = 8k+4 \ k \geq 2. \text{ 时；} \end{cases}$

证明。 我们首先将 $\mathcal{B}(n, c)$ 中的循环移位等价序列，在对序列参数施加某些限制的条件下，转换为 $\mathcal{B}(n, \lfloor \frac{n}{2} \rfloor)$ 中的移位等价序列。然后，我们将利用引理 6给出的 $\mathcal{B}(n, \lfloor \frac{n}{2} \rfloor)$中的移位等价序列的性质，证明 $\mathbf{s}_n \in \mathcal{R}(n, c)$ 中的第一条结论。

当 $c \geq \lfloor \frac{3n}{4} \rfloor$ 时，设在$\mathcal{B}(n,c)$中存在一对移位等价序列 $(\mathbf{s}'_n, \mathbf{v}'_n)$，满足 $0 \leq add(\mathbf{s}'_n) < add(\mathbf{v}'_n)$。令 $\mathbf{s}'_n \in \mathcal{B}(n,c,d_1)$ 和 $\mathbf{v}'_n \in \mathcal{B}(n,c,d_2)$。由于$c > \frac{n}{2}$，我们有 $d_1 \leq n-c$和 $d_2 \leq n-c$。如果 $d_1 = n-c$，则由 $c \geq \lfloor \frac{3n}{4} \rfloor \geq \lceil \frac{2n-1}{3} \rceil$和推论1可得 $b = d_2$。因此，根据推论 2 (ii)，我们知道 $d_2 = b < d_1 = n-c$。所以， $d_1 + d_2 < 2(n-c)$。

令 $m = \lfloor \frac{n}{2} \rfloor$。由引理 3 (i) 可知，$\mathbf{s}_n = L^{c-m}(\mathbf{s}'_n) \in \mathcal{B}(n,m,d_1)$，且 $\mathbf{v}_n = L^{c-m}(\mathbf{v}'_n) \in \mathcal{B}(n,m,d_2)$。因此，$(\mathbf{s}_n, \mathbf{v}_n)$ 是 $\mathcal{B}(n,m)$ 中的一对移位等价序列，并且 $t_1 = add(\mathbf{s}_n) = add(\mathbf{s}'_n) + (c-m) \geq c-m$，以及 $t_2 = add(\mathbf{v}_n) \geq t_1 + 1$。假设 $\mathbf{v}_n = R^{a+b}(\mathbf{s}_n)$ 且 $a = n-m-d_1$。根据引理 6，只需处理 $t_1 \leq b < d_1 + d_2 - t_2$ 的情形。回顾我们已经有

$$d_1 + d_2 < 2(n-c), \ t_1 \geq c-m, \ t_2 \geq t_1 + 1 \geq (c-m) + 1. \tag{7}$$

由于 $c \geq c_0 = \lfloor \frac{3n}{4} \rfloor$ 和 $m = \lfloor \frac{n}{2} \rfloor$，可推出 $d_1 + d_2 \leq 2\lceil \frac{n}{4} \rceil - 1 \leq 2\lfloor \frac{n}{4} \rfloor + 1 \leq t_1 + t_2$，这与 $t_1 < d_1 + d_2 - t_2$ 矛盾。因此，当 $c \geq \lfloor \frac{3n}{4} \rfloor$时，不存在满足 $add(\mathbf{s}'_n) < add(\mathbf{v}'_n)$ 的 $\mathcal{B}(n, c)$ 中的一对移位等价序列 $(\mathbf{s}'_n, \mathbf{v}'_n)$。也就是说，每个满足 $c \geq c_0 = \lfloor \frac{3n}{4} \rfloor$ 的序列 $\mathbf{s}_n \in \mathcal{B}(n,c)$ 都是一个序列代表元。第一条陈述得证。

在后续分析中，为了确定偶数 n 的紧界，根据 n 的形式，我们将讨论分为四种不同情形： $n = 8k+2$， $n = 8k+6$， $n = 8k+4$，以及 $n = 8k$。为了使证明更易读，我们先概述关键思路和主要步骤，然后再给出详细证明。

对于情形 (i) $n = 8k+2$ 和 (ii) $n = 8k+6$，已经得到了下界 $c_0 = \lfloor \frac{3n}{4} \rfloor$，并且已证明所有非线性复杂度不小于 c_0 的序列都是代表序列。要验证这个界的紧性，只需给出一个反例：一个非线性复杂度等于 $c_0 - 1$ 、但不是代表序列的序列。这便确认该界无法进一步改进。详细证明如下。

(i) 当 $n = 8k+2$ 时，假设一个序列具有以下形式

$$\mathbf{s}_n = (s_0, \ldots, s_{8k+1}) = ((\underline{\alpha\beta^{2k-1}}\, \alpha\beta^{2k-1}\, \alpha\beta^{2k-1}\, \beta)\alpha\beta^{2k}),$$

其中 $\beta = \bar{\alpha}$ 和 β^l 是由 l 次重复 β 得到的序列，其中 l为正整数。显然，$\mathbf{s}_n$ 属于 $\mathcal{B}(8k+2, 4k+1, 2k)$，且 $add(\mathbf{s}_n) = 2k-1$，其中 $\mathbf{s}_{2k}$ 是

带下划线的。考虑以下序列

$$\mathbf{u}_n = R^{2k-1}(\mathbf{s}_n) = ((\underline{\beta^{2k-1}\alpha}\,\beta^{2k-1}\alpha\,\beta^{2k-1}\alpha\,\beta^{2k-1}\beta)\alpha\beta),$$
$$\mathbf{v}_n = R^{6k}(\mathbf{s}_n) = ((\underline{\beta^{2k-2}\alpha\beta^2}\,\beta^{2k-2}\alpha\beta^2\,\beta^{2k-2}\alpha\beta^2\,\beta^{2k-3}\alpha)\beta).$$

显然，具有 $add(\mathbf{u}_n) = 0$的 $\mathbf{u}_n \in \mathcal{B}(8k+2, 6k, 2k)$，以及具有 $add(\mathbf{v}_n) = 1$的 $\mathbf{v}_n \in \mathcal{B}(8k+2, 6k, 2k+1)$。也就是说，对于 $\mathcal{B}(8k+2, 6k)$ 中的序列 $\mathbf{u}_n$，其循环移位序列 $\mathbf{v}_n = R^{4k+1}(\mathbf{u}_n)$ 属于具有 $add(\mathbf{v}_n) > add(\mathbf{u}_n)$ 的 $\mathcal{B}(8k+2, 6k)$。这表明，当 $n = 8k+2$ 时，下界 $c_0 = 6k+1 = \lfloor \frac{3n}{4} \rfloor$ 是一个紧界，使得任何具有 $c \geq c_0$ 的序列 $\mathbf{s}_n \in \mathcal{B}(n, c)$ 都是一个序列代表元。

(ii) 当 $n = 8k+6$ 时，只需在 $n = 8k+2$ 的证明中将 $2k$ 替换为 $2k+1$，即可直接得到证明。

对于情形 (iii) $n = 8k+4$ 和 (iv) $n = 8k$，我们重点讨论情形 $n = 8k+4$，因为情形 $n = 8k$ 可以用类似的方法处理。第一步，我们假设存在一个非线性复杂度至少为 $c_0 = \lfloor \frac{3n}{4} \rfloor - 2$ 、但不是代表序列的有限序列。根据各参数之间的关系，对所有可能的子情形进行分类和分析。在每种情形下，我们都推导出非周期子序列$\mathbf{s}^{d_1}$或$\mathbf{v}^{d_2}$ 的两种不同表示，并证明它们的汉明重量不同，由此得到矛盾。第二步，我们通过构造一个非线性复杂度恰好等于 $c_0 - 1$ 、但不是代表序列的序列，验证界 $c_0 = \lfloor \frac{3n}{4} \rfloor - 2$的紧性。完整证明见附录B。 —

□

注*1.* 定理*1*表明，如果 $c \geq c_0$，那么 $\mathbf{s}_n \in \mathcal{B}(n, c)$ 是一个序列代表元，即 $\mathbf{s}_n \in \mathcal{R}(n, c)$。如定理*1*所示，偶数 n 的紧下界已给出。事实上，对于奇数 n 的 $\mathcal{B}(n, c)$，非线性复杂度 c_0 的紧界与偶数 $n-1$ 和 $n+1$ 的紧界非常接近。并且，如果已知 $nlc(\mathbf{s}_n) = c$，那么可以在 $O(n)$ 时间内计算 $add(\mathbf{s}_n)$ 的值，因此可以直接通过 $c + add(\mathbf{s}_n)$ 确定 $nlc(\mathbf{s}_n^\infty)$。与直接计算周期序列的非线性复杂度相比，这种方法效率更高。当 n 为偶数时，紧下界给出了该周期序列非线性复杂度计算方法适用的精确范围。

此外，对于任意非线性复杂度为 $c \geq c_0$ 的序列 $\mathbf{a}_n$，根据引理 *2*，其中包含一对长度为 $(c-1)$、后继不同的相同子序列。这意味着对于某个 i，$L^i(\mathbf{a}_n) = \mathbf{s}_n \in \mathcal{B}(n, c)$。因此，对于每个非线性复杂度为 c 的有限长序列 $\mathbf{a}_n$，若 $c \geq c_0$，则可直接得到对应周期序列的非线性复杂度，即 $nlc(\mathbf{a}_n^\infty) = c + add(L^i(\mathbf{a}_n))$。

下面给出一个示例，以说明定理1的结果。

例1。以 s_{20} =(10001101000110100010) $\in$ $\mathcal{B}$(20,13, 7) 为例，其中$add(s_{20}) = 2$，s_d 带下划线，添加项用粗体表示。当 $n = 20$时，根据定理1可知，紧界 c_0 等于 13。由于 $nlc(s_{20}) = 13 = c_0$且 $add(s_{20}) = 2$，根据定理1，我们可以直接确定其对应周期序列的非线性复杂度：

$$nlc(s_{20}^{\infty}) = nlc(s_{20}) + add(s_{20}) = 13 + 2 = 15.$$

4 高非线性复杂度周期序列的结构

本节结合第3节的结果，证明当 $\omega \geq \lfloor \frac{3n}{4} \rfloor$时，每个序列$\mathbf{s}_n \in \mathcal{B}(n, \lceil \frac{n}{2} \rceil)$ 在 $add(\mathbf{s}_n) = \omega - \lceil \frac{n}{2} \rceil$ 下都是唯一的序列表示。进而，我们能够刻画 n-周期序列的结构，其中 $\omega \geq \lfloor \frac{3n}{4} \rfloor$。我们首先给出这类周期序列结构的主要结果。

定理 2。一个二元 n-周期序列的非线性复杂度为 $\omega \geq \lfloor \frac{3n}{4} \rfloor$，当且仅当它的一个非周期子序列（记为 $s_n = (s_0, s_1, \ldots, s_{n-1})$）可表示为以下两种形式之一：

(i) 当 $1 \leq d \leq n - \omega - 1$,

$$s_n = (\underbrace{(s_0, \ldots, s_{d-1})^q (s_0, \ldots, s_{r-1}, \overline{s}_r)}_{length=\omega+d} (s_{\omega+d}, \ldots, s_{n-2}) \overline{s}_{d-1}) \tag{8}$$

其中 $q = \lfloor \frac{\omega+d-1}{d} \rfloor$, $0 \leq r = (\omega + d - 1) - qd < d$, $s_d = (s_0, \ldots, s_{d-1})$ 是非周期的，而子序列 $(s_{\omega+d}, \ldots, s_{n-2})$ 是从 $\mathbb{Z}_2^{n-\omega-d-1}$ 中任意选取的。

(ii) 当 $n - \omega \leq d \leq \lfloor \frac{n}{2} \rfloor$, -

$$s_n = (s_0, s_1, \ldots, s_{n-1}) = (s_0, \ldots, s_{d-1})^{q'} (s_0, \ldots, s_{r'-1}, \overline{s}_{r'})$$

其中 $q' = \lfloor \frac{n-1}{d} \rfloor$, $0 \leq r' = (n - 1) - q'd < d$，且非周期子序列 $s_d = (s_0, s_1, \ldots, s_{d-1})$ 的选取使得若 $t = \omega + d - n = 0$，则 $s_{(n-1) \bmod d} = s_{d-1}$；若$t = \omega + d - n > 0$，则

$$\overline{s}_{(n-1) \bmod d} = s_{d-1}, s_{(n-i) \bmod d} = s_{(d-i) \bmod d}, \ 2 \leq i \leq t, s_{(n-t-1) \bmod d} = \overline{s}_{(d-t-1) \bmod d}.$$

定理2 的证明依赖于以下必要引理。首先，基于引理5，我们考虑如下集合

$$\mathcal{S}_\omega = \left\{ \mathbf{s}_n : \mathbf{s}_n \in \mathcal{B}\left(n, \left\lceil \frac{n}{2} \right\rceil\right), add(\mathbf{s}_n) = \omega - \left\lceil \frac{n}{2} \right\rceil \right\}. \tag{9}$$

首先，我们证明 $\mathcal{S}_\omega$ 中的每个序列都是引理 8所述的代表序列。然后，我们在引理 9 中证明， $\mathcal{S}_\omega$ 中的序列彼此移位不等价。

注意，根据（3）， $\mathcal{S}_\omega$ 中的所有序列及其移位版本可划分为以下两个不相交子集:

$$\begin{aligned} & \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \mathcal{B}(n, \lceil \tfrac{n}{2} \rceil),\ add(\mathbf{s}_n) = \omega - \lceil \tfrac{n}{2} \rceil, 0 \le k < n\} \\ = \ & \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \mathcal{S}_A, 0 \le k < n\} \cup \{R^k(\mathbf{s}_n) : \mathbf{s}_n \in \mathcal{S}_B, 0 \le k < n\}, \end{aligned} \tag{10}$$

其中

$$\begin{aligned} \mathcal{S}_A &= \bigcup_{1 \le d < n-\omega} \{\mathbf{s}_n : \mathbf{s}_n \in \mathcal{B}(n, \omega, d), add(\mathbf{s}_n) = 0\}, \\ \mathcal{S}_B &= \bigcup_{n-\omega \le d \le \lfloor \frac{n}{2} \rfloor} \{\mathbf{s}_n : \mathbf{s}_n \in \mathcal{B}(n, n-d, d),\ add(\mathbf{s}_n) = \omega + d - n\}. \end{aligned}$$

对于 $\mathbf{s}_n \in \mathcal{B}(n,\ c)$，回顾一下，其移位等价类 $E(\mathbf{s}_n)$ 在定义 4中定义为 $E(\mathbf{s}_n) = \{R^k(\mathbf{s}_n) :\ 0 \le k < n\} \cap \mathcal{B}(n,\ c)$。

引理 8。 设 $\omega \ge \lfloor \frac{3n}{4} \rfloor$。 若 $\boldsymbol{s}_n \in \mathcal{B}(n, \lceil \frac{n}{2} \rceil)$ 满足 $add(\boldsymbol{s}_n) = \omega - \lceil \frac{n}{2} \rceil$， 则 $\boldsymbol{s}_n$ 是其移位等价类 $E(\boldsymbol{s}_n)$ 的序列代表元。</*output*>

证明。 由（10），只需证明 $\mathcal{S}_A$ 和 $\mathcal{S}_B$ 中的序列都是代表序列。当 $1 \le d < n - \omega$时，由于 $\omega \ge \lfloor \frac{3n}{4} \rfloor$，根据定理 1 可知， $\mathcal{B}(n,\ \omega)$ 中的每个序列都是代表序列。因此， $\mathcal{S}_A$ 中的所有序列都是代表序列。

当 $n - \omega \le d \le \lfloor \frac{n}{2} \rfloor$时，序列属于集合 $\mathcal{S}_B$。假设 $\mathbf{s}_n \in \mathcal{S}_B$ 不是代表序列。那么，对于 $\mathbf{s}_n \in \mathcal{B}(n,\ c,\ d_1)$，其中 $c = n - d_1$ 且 $add(\mathbf{s}_n) = t_1 = \omega + d_1 - n$，存在一个移位序列，使得 $R^b(\mathbf{s}_n) \in \mathcal{B}(n,\ c,\ d_2)$ 满足$add(R^b(\mathbf{s}_n)) > t_1$。注意，

$$c + t_1 + t_2 + 1 \ge d_1 + 2\omega + 1 - n \ge d_1 + \left(2\left\lfloor \frac{3n}{4} \right\rfloor + 1 - n\right) \ge d_1 + \left\lfloor \frac{n}{2} \right\rfloor \ge d_1 + d_2.$$

因此，根据引理7 (i)，我们有 $b = d_2$。此外，根据推论 2，可得 $\mathbf{s}^{[d:n]} = (s_0,\ s_1,\ \ldots\ldots,\ s_{b-1})^l$，其中 $(s_0,\ \ldots\ldots,\ s_{b-1})$ 是某个非周期序列，并且

整数 $l \geq 2$。因此,

$$s_i = s_{i-d \,(\mathrm{mod}\ b)},\ \ d \leq i \leq n-1.$$

由于$\mathbf{s}_n \in \mathcal{B}(n,\ n-d,\ d)$, 我们有 $s_i = s_{i \bmod d},\ \ d \leq i \leq n-2$ 且 $s_{n-1} = s_{(n-1) \bmod d}$。由于$\mathbf{s}_d = \mathbf{s}^{[d:2d]}$ 包含于$\mathbf{s}^{[d:n]} = (s_0,\ s_1,\ \ldots,\ s_{b-1})^l$, 因此可得 $s_i = s_{i \bmod b},\ 0 \leq i < d$。于是, 我们得到

$$\begin{cases} s_{(n-1-d) \bmod b} = s_{n-1} = \overline{s}_{(n-1) \bmod d} = \overline{s}_{((n-1) \bmod d) \bmod b}, \\ s_{(n-2-d) \bmod b} = s_{n-2} = s_{(n-2) \bmod d} = s_{((n-2) \bmod d) \bmod b}, \\ \qquad \ldots \qquad = \qquad \ldots \\ s_{(d+1) \bmod b} = s_{2d+1} = s_1 = s_1, \\ s_{d \bmod b} = s_{2d} = s_0 = s_0, \end{cases} \tag{11}$$

其中, 对于（11）中的每一行, 第一个等式由 $s_i = s_{(i-d) \bmod b},\ \ d \leq i \leq n-1$ 得出, 第二个等式由 $s_i = s_{i \bmod d},\ \ d \leq i \leq n-2$ 和 $s_{n-1} = s_{(n-1) \bmod d}$ 得出, 第三个等式则由 $s_i = s_{i \bmod b},\ \ 0 \leq i < d$ 成立。

此外, 令 $t = add(\mathbf{s}_n) = \omega + d - n$, 则 $t < d$。因此, 根据定义 3, 由于$\mathbf{s}^{[d:n]} = (s_0,\ s_1,\ \ldots,\ s_{b-1})^l$ 且 $s_i = s_{i \bmod b},\ \ 0 \leq i < d$, 我们有

$$\begin{cases} s_{(d-1) \bmod b} = s_{d-1} = s_{n-1} = s_{b-1}, \\ s_{(d-2) \bmod b} = s_{d-2} = s_{n-2} = s_{b-2}, \\ \qquad \ldots \qquad = \qquad \ldots \\ s_{(d-t) \bmod b} = s_{d-t} = s_{n-t} = s_{(b-t) \bmod b}. \end{cases} \tag{12}$$

由于 $n - \omega \leq d \leq \lfloor \frac{n}{2} \rfloor$ 和 $\omega \geq \lfloor \frac{3n}{4} \rfloor$, 我们有 $b + d \leq \omega$。因此, 方程 (11) 和 (12) 的总数为 $(n-1-d) - (d-t) + 1 = \omega - d \geq b$。因此, $(s_{(n-1-d) \bmod b}, s_{(n-2-d) \bmod b}, \ldots, s_{(n-b-d) \bmod b})$ 作为 $\mathbf{s}_b = (s_0, \ldots, s_{b-1})$ 的移位版本, 其汉明重量为 $wt(\mathbf{s}_b)$。再次根据方程 (11) 和 (12), 可得

$$\begin{aligned} & \left(s_{(n-1-d) \bmod b}, s_{(n-2-d) \bmod b}, \ldots, s_{(n-b-d) \bmod b}\right) \\ = \ & \left(\overline{s}_{((n-1) \bmod d) \bmod b}, s_{((n-2) \bmod d) \bmod b}, \ldots, s_{((n-b) \bmod d) \bmod b}\right). \end{aligned}$$

这意味着 $(s_{((n-1) \bmod d) \bmod b},\ s_{((n-2) \bmod d) \bmod b},\ \ldots\ldots,\ s_{((n-b) \bmod d) \bmod b})$ 的汉明重量为 $wt(\mathbf{s}_b)$, 这与假设矛盾。因此, $\mathcal{S}_B$ 中的所有序列都是代表序列。证明完毕。

□

由引理 8，可得

$$\begin{aligned}\mathcal{S}_\omega &= \left\{\mathbf{s}_n : \mathbf{s}_n \in \mathcal{B}\left(n, \left\lceil \frac{n}{2} \right\rceil\right), add(\mathbf{s}_n) = \omega - \left\lceil \frac{n}{2} \right\rceil\right\} \\ &= \left\{\mathbf{s}_n : \mathbf{s}_n \in \mathcal{R}\left(n, \left\lceil \frac{n}{2} \right\rceil\right), add(\mathbf{s}_n) = \omega - \left\lceil \frac{n}{2} \right\rceil\right\}. \end{aligned} \tag{13}$$

现在证明 $\mathcal{S}_\omega$ 中的序列彼此移位不等价，这意味着每个代表序列都是唯一的。

引理 9. 设 $n \geq 3$ 和 $\omega \geq \lfloor \frac{3n}{4} \rfloor$。集合 $\{\boldsymbol{s}_n \in \mathcal{R}(n, \lceil \frac{n}{2} \rceil)\ add(\boldsymbol{s}_n) = \omega - \lceil \frac{n}{2} \rceil\}$ 中的所有代表序列彼此移位不等价。

证明。根据（13），只需证明

$$\left\{\mathbf{s}_n : \mathbf{s}_n \in \mathcal{B}\left(n, \left\lceil \frac{n}{2} \right\rceil\right),\ add(\mathbf{s}_n) = \omega - \left\lceil \frac{n}{2} \right\rceil\right\}$$

中的序列彼此移位不等价。根据（10），这等价于证明

$$\begin{cases} (1) \text{ sequences in the set } \mathcal{S}_A \text{ are shift inequivalent;} \\ (2) \text{ sequences in the set } \mathcal{S}_B \text{ are shift inequivalent;} \\ (3) \text{ sequences in } \mathcal{S}_A \text{ are shift inequivalent to those in } \mathcal{S}_B. \end{cases}$$

情形（1）：假设 $\mathcal{S}_A$ 中存在移位等价的序列，即 $\mathbf{s}_n \in \mathcal{B}(n, \omega, d_1)$ 和 $R^h(\mathbf{s}_n) = \mathbf{v}_n \in \mathcal{B}(n, \omega, d_2)$，则有 $add(\mathbf{s}_n) = add(\mathbf{v}_n) = 0$, $1 \leq d_1, d_2 \leq n - \omega - 1 \leq \lceil \frac{n}{4} \rceil$。令 $\mathbf{s}'_n = L^{\omega - \lfloor \frac{n}{2} \rfloor}(\mathbf{s}_n)$ 和 $\mathbf{v}'_n = L^{\omega - \lfloor \frac{n}{2} \rfloor}(\mathbf{v}_n)$。因此可知

$$\begin{cases} & \mathbf{s}'_n \in \mathcal{B}(n, \lfloor \frac{n}{2} \rfloor, d_1), \quad add(\mathbf{s}'_n) = t_1 = \omega - \lfloor \frac{n}{2} \rfloor, \\ R^h(\mathbf{s}'_n) = & \mathbf{v}'_n \in \mathcal{B}(n, \lfloor \frac{n}{2} \rfloor, d_2), \quad add(\mathbf{v}'_n) = t_2 = \omega - \lfloor \frac{n}{2} \rfloor, \end{cases} \tag{14}$$

其中 $1 \leq d_1,\ d_2 \leq n - \omega - 1$。

根据引理 6，我们有

$$\left(n - \left\lfloor \frac{n}{2} \right\rfloor - d_1\right) + t_1 \leq h < \left(n - \left\lfloor \frac{n}{2} \right\rfloor - d_1\right) + (d_1 + d_2 - t_2). \tag{15}$$

因此 $n - h \leq \lfloor \frac{n}{2} \rfloor + d_1 - t_1 < \lfloor \frac{n}{2} \rfloor + d_1$。这意味着 $\mathbf{v}'_{[h-t_1:n]} = \mathbf{s}'_{[-t_1:n-h]}$ 包含在 $\mathbf{s}'_{[-t_1:\lfloor \frac{n}{2} \rfloor + d_1 - 1]}$ 中。根据 $\mathbf{s}'_n$ 的结构可知，$\mathbf{v}'_{[h-t_1:n]} = (v'_{h-t_1}, v'_{h-t_1+1}, \ldots, v'_{n-1})$ 中的每个长度为 d_1 的序列都是 $\mathbf{s}'_{d_1}$ 的一个移位版本。此外，由 (14) 和 (15) 可得

$$h - t_1 \leq n - \left\lfloor \frac{n}{2} \right\rfloor + d_2 - t_2 - 1 - t_1 \leq n - \left\lfloor \frac{n}{2} \right\rfloor + (n - \omega - 1) - 1 - \left(2\omega - 2\left\lfloor \frac{n}{2} \right\rfloor\right) \leq \left\lfloor \frac{n}{2} \right\rfloor - d_1.$$

因此 $(v'_{\lfloor \frac{n}{2} \rfloor - d_1}, \ v'_{\lfloor \frac{n}{2} \rfloor - d_1 + 1}, \ \cdots, \ v'_{\lfloor \frac{n}{2} \rfloor - 1})$和 $(v'_{\lfloor \frac{n}{2} \rfloor + d_2 - d_1}, \ v'_{\lfloor \frac{n}{2} \rfloor + d_2 - d_1 + 1}, \ \cdots, \ v'_{\lfloor \frac{n}{2} \rfloor + d_2 - 1})$ 都包含在 $\mathbf{v}'_{[h-t_1:n]}$中，这意味着它们都是$\mathbf{s}'_{d_1}$的移位序列。根据 $(\mathbf{v}'_n$ （1）的结构可知

$$(v'_{\lfloor \frac{n}{2} \rfloor - d_1}, v'_{\lfloor \frac{n}{2} \rfloor - d_1 + 1}, \ldots, v'_{\lfloor \frac{n}{2} \rfloor - 2}) = (v'_{\lfloor \frac{n}{2} \rfloor + d_2 - d_1}, v'_{\lfloor \frac{n}{2} \rfloor + d_2 - d_1 + 1}, \ldots, v'_{\lfloor \frac{n}{2} \rfloor + d_2 - 2})$$

且 $v'_{\lfloor \frac{n}{2} \rfloor - 1} \neq v'_{\lfloor \frac{n}{2} \rfloor + d_2 - 1}$，矛盾。因此， $\mathcal{S}_A$中的所有序列都不移位等价。

情形（2）：假设 $\mathcal{S}_B$ 中存在移位等价序列，则

$$\begin{cases} \mathbf{s}_n \in \mathcal{B}(n, n-d_1, d_1), & n-\omega \leq d_1 \leq \lfloor \frac{n}{2} \rfloor, \qquad add(\mathbf{s}_n) = \omega + d_1 - n, \\ \mathbf{v}'_n \in \mathcal{B}(n, n-d_2, d_2), & n-\omega \leq d_2 \leq d_1 \leq \lfloor \frac{n}{2} \rfloor, \quad add(\mathbf{v}'_n) = \omega + d_2 - n. \end{cases}$$

令 $c = n - d_1$， $\mathbf{v}_n = L^{n-d_2-c}(\mathbf{v}'_n)$，则

$$\begin{cases} \mathbf{s}_n \in \mathcal{B}(n, c, d_1), & n-\omega \leq d_1 \leq \lfloor \frac{n}{2} \rfloor, \qquad add(\mathbf{s}_n) = t_1 = \omega + d_1 - n, \\ \mathbf{v}_n \in \mathcal{B}(n, c, d_2), & n-\omega \leq d_2 \leq d_1 \leq \lfloor \frac{n}{2} \rfloor, \quad add(\mathbf{v}_n) = t_2 = \omega + d_1 - n. \end{cases}$$

由于$\mathbf{s}_n$ 与$\mathbf{v}_n$ 移位等价，令$\mathbf{v}_n = R^b(\mathbf{s}_n)$，其中 $0 < b < n$，则$\mathbf{s}_n = R^{n-b}(\mathbf{v}_n)$。注意

$$c + t_1 + t_2 + 1 = d_1 + 2\omega + 1 - n \geq d_1 + \left(2 \left\lfloor \frac{3n}{4} \right\rfloor + 1 - n \right) \geq d_1 + \left\lfloor \frac{n}{2} \right\rfloor \geq d_1 + d_2. \quad (16)$$

因此，一方面，对于序列对 $(\mathbf{s}_n, R^b(\mathbf{s}_n))$，由引理 7 和 (16) 可得 $b = d_2$；另一方面，对于 $(\mathbf{v}_n, R^{n-b}(\mathbf{v}_n))$，同样由引理 7 和 (16) 可得$n - b = d_1$。于是， $b = d_2 = n - d_1$。由 $d_1, d_2 \leq \lfloor \frac{n}{2} \rfloor$，可推出 $b = d_1 = d_2 = \frac{n}{2}$。这导致 $t_1 = t_2 = 0$，与

$$t_1 = t_2 = \omega + d_1 - n \geq \left\lfloor \frac{3n}{4} \right\rfloor - \frac{n}{2} \geq 1, \ (n \geq 3).$$

因此， $\mathcal{S}_B$ 中的序列是移位不等价的。

情形（3）：假设 $\mathcal{S}_A$ 中的某些序列与 $\mathcal{S}_B$中的序列移位等价：

$$\begin{cases} \mathbf{s}_n \in \mathcal{B}(n, n-d_1, d_1), & n-\omega \leq d_1 \leq \lfloor \frac{n}{2} \rfloor, \quad add(\mathbf{s}_n) = t = \omega + d_1 - n, \\ R^h(\mathbf{s}_n) = \mathbf{v}'_n \in \mathcal{B}(n, \omega, d_2), & 1 \leq d_2 < n - \omega, \qquad add(\mathbf{v}'_n) = 0. \end{cases}$$

令 $c = n - d_1$，且 $\mathbf{v}_n = L^t(\mathbf{v}'_n)$，则

$$\begin{cases} \mathbf{s}_n \in \mathcal{B}(n, c, d_1), & n-\omega \leq d_1 \leq \lfloor \frac{n}{2} \rfloor, \quad add(\mathbf{s}_n) = t_1 = \omega + d_1 - n, \\ R^{h-t}(\mathbf{s}_n) = \mathbf{v}_n \in \mathcal{B}(n, c, d_2), & 1 \leq d_2 < n - \omega, \qquad add(\mathbf{v}_n) = t_2 = \omega + d_1 - n. \end{cases}$$

由于

$$c+t_1+t_2+1=d_1+2\omega+1-n\geq d_1+\left(2\left\lfloor\frac{3n}{4}\right\rfloor+1-n\right)\geq d_1+\left\lfloor\frac{n}{2}\right\rfloor\geq d_1+d_2,$$

由引理 7 可知 $h-t=d_2$。

根据 $\mathbf{s}_n\in\mathcal{B}(n,\ n-d_1,\ d_1)$ 和 $add(\mathbf{s}_n)=t$，可得

$$s_{-t-1}=\overline{s}_{d_1-t-1},\ s_i=s_{i+d_1},\ \ i\in[-t,n-d_1-2]\ \text{ and }\ s_{n-d_1-1}=\overline{s}_{n-1}. \tag{17}$$

由于 $R^{d_2+t}(\mathbf{s}_n)=\mathbf{v}_n\in\mathcal{B}(n,\ \omega,\ d_2)$ 且 $add(R^{d_2+t}(\mathbf{s}_n))=0$，因此可得

$$\begin{aligned}&s_{-d_2-t-1}=\overline{s}_{-t-1},\ s_i=s_{i+d_2},\ \ i\in[-d_2-t,\omega-d_2-t-2],\\ &\text{and}\ \ s_{\omega-d_2-t-1}=\overline{s}_{\omega-t-1}=\overline{s}_{n-d_1-1},\end{aligned} \tag{18}$$

上述方程中的所有下标均以 n为模。

由（18）可知，任意连续的 d_2 项组成

$$(\overline{s}_{-d_2-t-1},s_{-d_2-t},s_{-d_2-t+1},\ldots,s_{\omega-t-2},\overline{s}_{\omega-t-1})$$

由 $\mathbf{v}^{d_2}$ 的一个移位序列构成。于是 $(s_{-d_2-t-1},\ s_{-d_2-t},\ s_{-d_2-t+1},\ \ldots\ldots,\ s_{-t-2})$ 是 $\mathbf{v}^{d_2}$ 的一个移位序列。由（17）和（18），可知

$$\begin{aligned}&(\overline{s}_{-d_2-t-1},s_{-d_2-t},s_{-d_2-t+1},\ldots,s_{-t-2})\\ =&(s_{-t-1},s_{-t},s_{-t+1},\ldots,s_{d_2-t-2})\\ =&(\overline{s}_{d_1-t-1},s_{d_1-t},s_{d_1-t+1},\ldots,s_{d_1+d_2-t-2}).\end{aligned}$$

因此，$(s_{d_1-t-1},\ s_{d_1-t},\ s_{d_1-t+1},\ \ldots\ldots,\ s_{d_1+d_2-t-2})$ 是$\mathbf{v}^{d_2}$ 的一个移位版本。考虑子序列 $(s_{d_1-t-1},\ s_{d_1-t},\ s_{d_1-t+1},\ \ldots\ldots,\ s_{d_1+d_2-t-2})$，由于其下标满足

$$-d_2-t\leq d_1-t-1,\ d_1-t,\ldots,d_1+d_2-t-2\leq\omega-t-2,$$

它也是$\mathbf{v}^{d_2}$ 的一个移位版本，这就产生了矛盾。因此，$\mathcal{S}_A$ 中的序列与 $\mathcal{S}_B$ 中的序列不移位等价。

综合以上三个子情形，以下各项中不存在移位等价的序列

$$\left\{\mathbf{s}_n:\mathbf{s}_n\in\mathcal{B}\left(n,\left\lceil\frac{n}{2}\right\rceil\right),\ add(\mathbf{s}_n)=\omega-\left\lceil\frac{n}{2}\right\rceil\right\}.$$

因此由（13），每个满足 $\mathbf{s}_n\in\mathcal{R}(n,\lceil\frac{n}{2}\rceil)$ 且 $add(\mathbf{s}_n)=\omega-\lceil\frac{n}{2}\rceil$ 都是唯一代表序列。

□

结合引理8 和9，我们立即得到以下命题。

命题 2。 每个序列 $s_n \in \mathcal{B}(n, \lceil \frac{n}{2} \rceil)$ 满足 $add(s_n) \geq \lfloor \frac{3n}{4} \rfloor - \lceil \frac{n}{2} \rceil$，都是 $E(s_n)$ 中的唯一代表序列。

基于命题 2，结合引理3 和定理 1，根据有限长度序列的非线性复杂度，我们可以得出 $\mathbf{s}_n$ 是唯一代表序列。

推论 4。 设整数 $k \geq 0$ 和 $c \geq \lfloor \frac{3n}{4} \rfloor$。对于 $s_n \in \mathcal{B}(n, c)$，有

(i)s_n 是唯一代表序列。

(ii) 当 $n = 4k + 2$时，不等式 $c \geq \lfloor \frac{3n}{4} \rfloor$ 给出了一个紧的下界，使得每个序列 $s_n \in \mathcal{B}(n, c)$ 都是唯一代表序列。

证明。 (i) 对于任意序列 $\mathbf{s}_n \in \bigcup \mathcal{B}(n, c, d)$，由引理 3 (i)可知$1 \leq d \leq n-c$ $L^{c-\lceil \frac{n}{2} \rceil}(\mathbf{s}_n) \in \mathcal{B}(n, \lceil \frac{n}{2} \rceil, d)$，且 $add(L^{c-\lceil \frac{n}{2} \rceil}(\mathbf{s}_n)) = add(\mathbf{s}_n) + (c - \lceil \frac{n}{2} \rceil) \geq \lfloor \frac{3n}{4} \rfloor - \lceil \frac{n}{2} \rceil$。因此，

$$\begin{aligned} &\left\{ \mathbf{s}_n^\infty : \mathbf{s}_n \in \bigcup_{1 \leq d \leq n-c} \mathcal{B}(n, c, d),\ c \geq \left\lfloor \frac{3n}{4} \right\rfloor \right\} \\ \subset &\left\{ \mathbf{s}_n^\infty : \mathbf{s}_n \in \bigcup_{1 \leq d \leq \lfloor \frac{n}{2} \rfloor} \mathcal{B}\left(n, \left\lceil \frac{n}{2} \right\rceil, d\right),\ add(\mathbf{s}_n) \geq \left\lfloor \frac{3n}{4} \right\rfloor - \left\lceil \frac{n}{2} \right\rceil \right\}. \end{aligned}$$

结合命题2，我们得出，当 $c \geq \lfloor \frac{3n}{4} \rfloor$时， $L^{c-\lceil \frac{n}{2} \rceil}(\mathbf{s}_n)$ 是其移位等价类的唯一代表序列

$$E(L^{c-\lceil \frac{n}{2} \rceil}(\mathbf{s}_n)) = \{R^k(\mathbf{s}_n) : 0 \leq k < n\} \cap \mathcal{B}(n, \lceil n/2 \rceil)$$

在 $\mathcal{B}\left(n, \lceil \frac{n}{2} \rceil\right)$ 内。因此，$\mathbf{s}_n$ 是其移位等价类 $E(\mathbf{s}_n) = \{R^k(\mathbf{s}_n)$ 中的唯一代表序列: $0 \leq k < n\} \cap \mathcal{B}(n, c)$ 在 $\mathcal{B}(n, c)$ 内。也就是说，$\mathbf{s}_n$ 是唯一代表序列。因此，第一个陈述得证。

(ii) 根据定理1，当 $n = 4k + 2$ 对任意整数 k时， $c \geq \lfloor \frac{3n}{4} \rfloor$ 表示确保$\mathbf{s}_n$ 为代表序列的紧下界。因此， $c \geq \lfloor \frac{3n}{4} \rfloor$ 也可作为确保$\mathbf{s}_n$ 为唯一代表序列的紧下界。 □

注2. 实验数据表明，当 $n = 4k+2$ 对任意整数 k成立时， $add(s_n) = t \geq \lfloor \frac{3n}{4} \rfloor - \lceil \frac{n}{2} \rceil$ 可作为紧下界，从而确保$s_n \in \mathcal{B}(n, \lceil \frac{n}{2} \rceil)$ 是唯一代表序列。对于 n的其他取值，当 $n \in \{7, 11, 13, 15, \ldots\}$时，界$add(s_n) \geq \lfloor \frac{3n}{4} \rfloor - \lceil \frac{n}{2} \rceil$ 在命题2中同样是紧下界。

基于上述准备，我们现在可以证明 n-周期序列在非线性复杂度为 $\geq \lfloor \frac{3n}{4} \rfloor$ 时于定理 2中的结构。定义 $\mathcal{P}(n,\omega)$ 为周期为 n 且非线性复杂度为 ω的二元移位不等价序列的集合。

定理 2 的证明。 对于 $\lfloor \frac{3n}{4} \rfloor \leq \omega \leq n-1$，根据引理 5 和命题 2，可得

$$\mathcal{P}(n,\omega) = \{\mathbf{s}_n^\infty : \mathbf{s}_n \in \mathcal{B}(n, \lceil \tfrac{n}{2} \rceil),\ add(\mathbf{s}_n) = \omega - \lceil \tfrac{n}{2} \rceil\}.$$

此外，由式（10）可得

$$\begin{aligned}\mathcal{P}(n,\omega) = & \sum_{1 \leq d < n-\omega} \{\mathbf{s}_n^\infty : \mathbf{s}_n \in \mathcal{B}(n,\omega,d),\ add(\mathbf{s}_n) = 0\} \\ & + \sum_{n-\omega \leq d \leq \lfloor \frac{n}{2} \rfloor} \{\mathbf{s}_n^\infty : \mathbf{s}_n \in \mathcal{B}(n, n-d, d),\ add(\mathbf{s}_n) = \omega + d - n\}.\end{aligned}$$

(i) 当 $1 \leq d \leq n-\omega-1$时，根据式（$\mathbf{s}_n \in \mathcal{B}(n,\omega,d)$（见式 1）给出的结构以及定义 $add(\mathbf{s}_n)$ 3中的定义可知，有 $s_{n-1} = s_{(n-1) \bmod d}$ 和 $s_{n-1} = s_{d-1}$，于是 $s_{(n-1) \bmod d} = s_{d-1}$，因此 $\mathbf{s}_n$ 具有式（8）所示的形式。

(ii) 当 $n-\omega \leq d \leq \lfloor \frac{n}{2} \rfloor$时，$\mathbf{s}_n \in \mathcal{B}(n, n-d, d)$ 的形式为

$$\mathbf{s}_n = (s_0, s_1, \ldots, s_{n-1}) = (s_0, \ldots, s_{d-1})^{q'} (s_0, \ldots, s_{r'-1}, \overline{s}_{r'})$$

其中 $q' = \lfloor \frac{n-1}{d} \rfloor$，$0 \leq r' = (n-1) - q'd < d$。此外，若 $add(\mathbf{s}_n) = 0$，则 $\mathbf{s}_n$ 满足 $s_{n-1} = \overline{s}_{d-1}$；若 $add(\mathbf{s}_n) = t = \omega + d - n > 0$，则根据 $\mathbf{s}_n$ 的结构和定义3， $\mathbf{s}_n$ 满足

$$\overline{s}_{(n-1) \bmod d} = s_{d-1}, s_{(n-i) \bmod d} = s_{(d-i) \bmod d},\ 2 \leq i \leq t, s_{(n-t-1) \bmod d} = \overline{s}_{(d-t-1) \bmod d}.$$

因此，所需的结论 (i) 和 (ii) 随之成立。 □

定理 2 在本文中给出了 n-周期序列在非线性复杂度为 $\geq \lfloor \frac{3n}{4} \rfloor$ 时的结构。这进一步改进了 [42], 中的结果，其中提供了一种方法来生成集合 $\mathcal{P}(n,\omega)$，但并未揭示周期序列在 $\mathcal{P}(n,\omega)$ 中的内部结构。

5 具有高非线性复杂度的周期序列的计数

本节致力于确定 $|\mathcal{P}(n,\omega)|$ 对于 $\omega \geq \lfloor \frac{3n}{4} \rfloor$ 的精确值，其中 $|\mathcal{P}(n,\omega)|$ 表示 $\mathcal{P}(n,\omega)$ 的基数。

设 $A(d)$ 为所有长度为 d 的非周期序列 $\mathbf{s}_d$ 构成的集合。由于任意长度为 n 的序列都可视为周期整除 n 的周期序列，我们得到 $\sum |A(d)| = 2^n$。根据默¨比乌斯反演公式 [19],，我们有 $|A(d)| = \sum \mu(e) 2^{d/e}$，$d|n$ $e|d$其中默¨比乌斯函数定义为

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes}, \\ 0 & \text{if } n \text{ is divisible by the square of a prime.} \end{cases} \tag{19}$$

根据定理 $\mathcal{P}(n,\ \omega)$ 中给出的序列结构，定理 2表明，当 $1 \leq d < n - \omega$时，若已选定 $\mathbf{s}_d$，则 $(s_0,\ s_1,\ \ldots,\ s_{d+\omega-1})$ 和 s_{n-1} 均已确定，只有$(s_{d+\omega},\ s_{d+\omega+1},\ \ldots,\ s_{n-2})$ 可以在 $\mathbb{Z}_{2^{n-\omega-1-d}}$中任意选取。因此，序列的数量为

$$2^{n-\omega-1-d}|A(d)| = \sum_{e|d} \mu(e) 2^{n-\omega-1-d+d/e}.$$

当 $n - \omega \leq d \leq \lfloor \frac{n}{2} \rfloor$时，若 $t = \omega + d - n = 0$，则 $d = n - \omega$ 并记为

$$N(n, d, 0) = \{\mathbf{s}_d \in A(d) : s_{n-1 \,(\mathrm{mod}\ d)} = s_{d-1}\},$$

其中 $A(d)$ 是所有非周期 d 长度序列 $\mathbf{s}_d$ 的集合。若 $t = \omega + d - n > 0$，则记为

$$\begin{aligned} & N(n, d, t) \\ = \ & \{\mathbf{s}_d \in A(d) : \overline{s}_{(n-1) \bmod d} = s_{d-1}, s_{(n-i) \bmod d} = s_{(d-i) \bmod d},\ 2 \leq i \leq t, \\ & s_{(n-t-1) \bmod d} = \overline{s}_{(d-t-1) \bmod d}\}. \end{aligned} \tag{20}$$

Thus

$$|\mathcal{P}(n,\omega)| = \sum_{d=1}^{n-\omega-1} \sum_{e|d} \mu(e) 2^{n-\omega-1-d+d/e} + |N(n, n-\omega, 0)| + \sum_{n-\omega<d\leq\lfloor\frac{n}{2}\rfloor} |N(n, d, \omega + d - n)|.$$

接下来，我们将分别确定在 $t > 0$ 条件下 $N(n,\ d,\ 0)$ 和 $N(n,\ d,\ t)$ 的值。

引理 10. 设 $N(n, d, 0) = \{\mathbf{s}_d \in A(d) : s_{(n-1) \text{模 } d} = s_{d-1}\}$. 对于合数 d，有

$$|N(n, d, 0)| = \begin{cases} |A(d)| = \sum_{e|d} \mu(e) 2^{d/e}, & \text{if } d \mid n, \\ 2^{d-1} - 2 - \sum_{e|d, 1<e<d} |N(n, e, 0)|, & \text{if } d \nmid n. \end{cases}$$

此外，对于素数 d，有

$$|N(n,d,0)| = \begin{cases} |A(d)| = 2^d - 2, & if\ d \mid n, \\ 2^{d-1} - 2, & if\ d \nmid n. \end{cases}$$

证明。若 $d \mid n$，则 $|\{s_d \in A(d) : s_{(n-1) \bmod d} = s_{d-1}\}| = |\{s_d \in A(d)\}| = |A(d)|$。若 $d \nmid n$，则 $N(n,d,0) = \{s_d \in A(d) : s_{(n-1)} \text{模 } _d = s_{d-1}\}$。因此，为了确定 $N(n,d,0)$ 在 2^{d-1} 向量 $(s_0, \ldots, s_{d-2}) \in \mathbb{Z}_2^{d-1}$ 中的值，我们只需排除那些会导致 $s^{[0:d]} = (s_0, s_1, \ldots, s_{d-2}, s_{(n-1) \bmod d})$ 不是非周期有限长序列的序列。下面，我们将研究 $s^{[0:d]} = (s_0, s_1, \ldots, s_{d-1}) = (s_0, s_1, \ldots, s_{d-2}, s_{n-1 \,(\bmod d)})$ 是周期有限长序列的情形。

若 $(s_0, s_1, \ldots, s_{d-1})$ 是周期有限长序列，则它等于 $(s_e)^{d/e}$，其中 s_e 是非周期的，且 $e|d, 1 \le e < d$。因此，只需刻画使得 $(s_0, s_1, \ldots, s_{d-1})$ 为周期的 s_e。当 $e = 1$ 时，s_e 有两种选择，即 (0) 或 (1)，从而得到 $s^{[0:d]} = (0^d)$ 或 (1^d)。当 $e > 1$ 时，由于 $(s_0, s_1, \ldots, s_{d-1}) = (s_e)^{d/e}$，我们有 $s_{d-1} = s_{e-1}$ 以及 $s_{(n-1) \bmod d} = s_{(n-1)} \bmod e$。此外，由 $s_{(n-1) \bmod d} = s_{d-1}$ 可知，s_e 满足 $s_{(n-1) \bmod e} = s_{e-1}$。于是 s_e 的个数为 $|\{s_e \in A(e) : s_{(n-1)} \bmod e = s_{e-1}\}| = |N(n,e,0)|$，其中 $A(e)$ 是由所有长度为 e 的非周期有限长序列 s_e 构成的集合。因此可得$|N(n,d,0)| = 2^{d-1} - 2 - \sum_{e|d, 1<e<d} |N(n,e,0)|$。

因此，$|N(n, d, 0)|$的计算可简化为素数 e 时的 $|N(n, e, 0)|$。对于素数 d，当 $d \mid n$ 时，$|N(n, d, 0)| = |A(d)|$ 显然成立。当 $d \nmid n$ 时，由于素数 d 只有真因数 1，因此有 $|N(n, d, 0)| = 2^{d-1} - 2$。证毕。 □

注意，$N(n, d, 0)$ 的值由 d 和（$n \bmod d$）决定。当 $t > 0$ 时，方程

$$\overline{s}_{(n-1) \bmod d} = s_{d-1}, s_{(n-i) \bmod d} = s_{(d-i) \bmod d},\ 2 \le i \le t, s_{(n-t-1) \bmod d} = \overline{s}_{(d-t-1) \bmod d}$$

可以等价地视为一个二元线性方程组 $A \cdot \mathbf{x}^T = \mathbf{b}^T$，其中$_{t-1}\mathbf{x} = (s_0, s_1, \ldots, s_{d-1})$，$\mathbf{b} = (1, 0, \ldots 0, 1)$，且矩阵 $A = (a_{i,j})_{(t+1) \times d}$ 满足$a_{i,\ ((n-i) \text{模 } d)+1} = 1$，$a_{i,\ (d-i)+1} = 1$，$i, j \ge 1$，其余元素均为0。因此，(20)中定义的 $N(n,d,t)$也可以另一种方式表示为

$$N(n,d,t) = \{\mathbf{x} = (s_0, s_1, \ldots, s_{d-1}) \in A(d) :\ A \cdot \mathbf{x}^T = \mathbf{b}^T\}.$$

注意， A 的每一行都有两个1，其余为0，且$s_{(n-i)\text{模 }d}$与带有 $1 \le i \le t+1$ 的$s_{(d-i) \bmod d}$的下标之间的间距相同，等于$(n-d)$模 d。因此， A 的第 i行可由对 A的第一行进行左循环移位 i 比特得到。于是我们可以将 A 的间隔定义为 A第一行中两个1在循环意义下之间最少的0的个数，记为 $gap(A)$。事实上， $gap(A)$可以完全确定矩阵A。令 $l \equiv n$（模 d），则可以看出，若 $l \le \lceil \frac{d-1}{2} \rceil$，则 $gap(A) = l-1$，否则$gap(A) = d-1-l$。

—

根据以上讨论，我们将通过以下递归关系确定 $N(n,\ d,\ t)$。令 $B = (A,\ b^T)$ 表示增广矩阵， $rank(A)$ 表示矩阵 A 的秩。特别地，对于素数 d， $rank(A)$ 和 $rank(B)$ 可直接得到。

引理 11。 设 $N(n,\ d,\ t)$ 及 $t > 0$ 由 (20)定义。

(i) 对于合数 d，令 最大值$_{e|d,\ 1<e<d}\{e\} = \tilde{e}_d$。当 $t < \tilde{e}_d$ 时，有

$$|N(n,d,t)| = \begin{cases} 0, & if\ d \,|\, n, \\ 2^{d-t-1} - \sum\limits_{e|d, 1<e<d} |N(n,e,t)|, & if\ d \nmid n. \end{cases}$$

当 $t \ge \tilde{e}_d$ 时，我们得到

$$|N(n,d,t)| = \begin{cases} 0, & if\ d \,|\, n\ or\ if\ d \nmid n\ and\ rank(A) \ne rank(B), \\ 2^{d-rank(A)}, & if\ d \nmid n\ and\ rank(A) = rank(B). \end{cases}$$

(ii) 对于素数 d，可得

$$|N(n,d,t)| = \begin{cases} 0, & if\ d \,|\, n\ or\ if\ d \nmid n\ and\ t \ge d, \\ 2^{d-t-1}, & if\ d \nmid n\ and\ 1 \le t \le d-2, \\ 2, & if\ d \nmid n\ and\ t = d-1. \end{cases}$$

证明。 (i) 若 $d \,|\, n$，则（20）中第二个方程的条件可改写为$s_{n-1\,(\text{模 }d)} = s_{d-1} = s_{d-1}$，这与之矛盾。因此 $|N(n,\ d,\ t)| = 0$。

当 $t < \tilde{e}_d$时，令 $l = n(\text{模 } d)$，则 $0 \le l < d$。若 $d \nmid n$，则由 (20) 可得

$$\mathbf{s}_{[0:d]} = (s_0, s_1, \ldots, s_{d-1}) = (s_0, \ldots, s_{d-t-2})(\overline{s}_{l-t-1}, s_{l-t}, \ldots, s_{l-2}, \overline{s}_{l-1}), \tag{21}$$

其中，$\bar{s}_{l-t-1}$ 可由（$s_0, \ldots, s_{d-t-2}$）确定，s_{l-t} 也可由（$s_0, \ldots, s_{d-t-2}, s_{l-t-1}$）确定。这个过程继续进行，使我们能够推导出 $\mathbf{s}_d$ 完全由（$s_0, \ldots, s_{d-t-2}$）确定。因此，在 2^{d-t-1} 个序列（$s_0, \ldots, s_{d-t-2}$）中，只需减去不满足（21）中 $\mathbf{s}_d$ 为非周期的那些序列（$s_0, \ldots, s_{d-t-2}$）。也就是说，

$|N(n, d, t)| = 2^{d-t-1} - |\{(s_0, \ldots, s_{d-t-2})$: 式（21）中的序列是一个周期有限长序列$\}|$.

下面，我们研究哪些情形会使式（21）中的序列成为周期有限长序列，也就是说，$\mathbf{s}^{[0:d]} = (\mathbf{s}_e)^{d/e}$，其中 $\mathbf{s}_e$ 是具有 $e|d$、$1 \le e < d$ 的非周期序列。当 $e = 1$ 时，我们有 $\mathbf{s}^{[0:d]} = (0^d)$ 或 (1^d)，这与 $s_{(n-1) \bmod d} = s_{d-1}$ 矛盾。当 $e > 1$ 时，由 $\mathbf{s}^{[0:d]} = (\mathbf{s}_e)^{d/e}$ 可得

$$s_{(d-j) \bmod d} = s_{(d-j) \bmod e} = s_{(e-j) \bmod e} \quad \text{and} \quad s_{(n-j) \bmod d} = s_{(n-j) \bmod e}$$

对于 $1 \le j \le t+1$。由于条件 $s_{(n-1) \bmod d} = s_{d-1}$，$s_{(n-i) \bmod d} = s_{(d-i) \bmod d}$，其中 $2 \le i \le t$，且 $s_{(n-t-1) \bmod d} = s_{(d-t-1) \bmod d}$，根据 $\mathbf{s}^{[0:d]} = (\mathbf{s}_e)^{d/e}$，可知 $\mathbf{s}_e \in A(e)$ 满足

$$s_{(n-1) \bmod e} = s_{e-1}, s_{(n-i) \bmod e} = s_{(e-i) \bmod e} \quad \text{and} \quad s_{(n-t-1) \bmod e} = s_{(e-t-1) \bmod e},$$

其中 $A(e)$ 表示所有长度为 e 的非周期有限长序列 $\mathbf{s}_e$ 的集合。因此

$$\begin{aligned} & |\{(s_0, \ldots, s_{d-t-2}) : \text{the sequence in (21) is periodic}\}| \\ = & \sum_{e|d, 1<e<d} |\{\mathbf{s}_e \in A(e) : s_{(n-1) \bmod e} = s_{e-1}, s_{(n-i) \bmod e} = s_{(e-i) \bmod e},\ 2 \le i \le t, \\ & \text{and } s_{(n-t-1) \bmod e} = s_{(e-t-1) \bmod e}\}| \\ = & \sum_{e|d, 1<e<d} |N(n, e, t)|. \end{aligned}$$

因此，$|N(n, d, t)| = 2^{d-t-1} - \sum_{e|d, 1<e<d} |N(n, e, t)|$

当 $t > \tilde{e}_d$ 时，假设 $\mathbf{s}^{[0:d]}$ 是一个周期有限长序列，那么 $\mathbf{s}^{[0:d]} = (\mathbf{s}_e)^{d/e}$ 其中 $\mathbf{s}_e$ 是非周期的，且 $e|d, 1 \le e < d$。由于 $add(\mathbf{s}_n) = t$，我们有 $s_{(d-j) \bmod d} = s_{(d-j) \bmod e} = s_{(e-j) \bmod e}$，且 $s_{(n-j) \bmod d} = s_{(n-j) \bmod e}$，对于 $1 \le j \le t+1$。由（20）可得 $s_{(n-1) \bmod e} = s_{(n-1) \bmod d} = s_{d-1} = s_{e-1}$，并且

$$s_{(n-1) \bmod e} = s_{(n-e-1) \bmod e} = s_{(n-e-1) \bmod d} = s_{d-e-1} = s_{e-e-1} = s_{e-1},$$

这就产生了矛盾。因此，$\mathbf{s}_d$ 是非周期的。

当 $t=\tilde{e}_d$ 时，根据 d 与 $\tilde{e}_d$ 的因子之间的关系，我们将讨论分为两种情况。对于满足 $e_1<\tilde{e}_d$ 的 $e_1|d$，可以得到与 $t>\tilde{e}_d$ 情况类似的矛盾，这意味着$\mathbf{s}_d \neq (\mathbf{s}^{e_1})^{d/e_1}$。对于 $e_1=\tilde{e}_d$，由于 $\tilde{e}_d|d$，假设$\mathbf{s}_d=(\mathbf{s}^{\tilde{e}_d})^{d/\tilde{e}_d}$，则条件可化简为 $s_{(n-1) \bmod \tilde{e}_d}=s_{\tilde{e}_d-1}$ 和 $s_{(n-i) \bmod \tilde{e}_d}=s_{(\tilde{e}_d-i) \text{ 模 } \tilde{e}_d}, 2 \leq i \leq \tilde{e}_d$。因此，

$$
\begin{aligned}
&s_{(2n-1) \bmod \tilde{e}_d}=s_{(n-(\tilde{e}_d-n+1)) \bmod \tilde{e}_d}=s_{(\tilde{e}_d-(\tilde{e}_d-n+1)) \bmod \tilde{e}_d}=s_{(n-1) \bmod \tilde{e}_d},\\
&s_{(3n-1) \bmod \tilde{e}_d}=s_{(2n-(\tilde{e}_d-n+1)) \bmod \tilde{e}_d}=s_{(2n-1) \bmod \tilde{e}_d},\\
&\cdots \quad \cdots,\\
&s_{(\tilde{e}_d n-1) \bmod \tilde{e}_d}=s_{((\tilde{e}_d-1)n-1) \bmod \tilde{e}_d}
\end{aligned}
$$

这意味着

$$
s_{\tilde{e}_d-1}=s_{(\tilde{e}_d n-1) \bmod \tilde{e}_d}=s_{((\tilde{e}_d-1)n-1) \bmod \tilde{e}_d}=\cdots=s_{(2n-1) \bmod \tilde{e}_d}=s_{(n-1) \bmod \tilde{e}_d},
$$

这与条件 $s_{(n-1) \bmod \tilde{e}_d}=s_{\tilde{e}_d-1}$ 矛盾。因此，假设不成立。也就是说，$\mathbf{s}^{[0:d]}$ 始终是非周期的，可记为 $\mathbf{s}_d$。

因此，当 $t \geq \tilde{e}_d$ 和 $d \nmid n$时，我们有

$$
\begin{aligned}
&|N(n,d,t)|\\
=\ &\left|\left\{\mathbf{s}_d: \overline{s}_{(n-1) \bmod d}=s_{d-1}, s_{(n-i) \bmod d}=s_{(d-i) \bmod d}, s_{(n-t-1) \bmod d}=\overline{s}_{(d-t-1) \bmod d}\right\}\right|,
\end{aligned}
$$

这等于上文定义的方程在 $A \cdot \mathbf{x}^T=\mathbf{b}^T$且满足 $A, \mathbf{x}^T, \mathbf{b}^T$时的解的个数。因此，对于 $B=(A, \mathbf{b}^T)$，若 $rank(A)=rank(B)$，则 $|N(n,d,t)|=2^{d-rank(A)}$；若 $rank(A) \neq rank(B)$，则 $|N(n,d,t)|=0$。

(ii) 若 d是素数，当 $d \mid n$时，与 (i) 类似，可以证明 $|N(n,d,t)|=0$。当 $d \nmid n$时，由于 $A=(a_{i,j})_{(t+1)\times d}$且 $B=(A, b^T)$，我们知道 $rank(A) \leq rank(B) \leq 1+t$。假设 $rank(A)<1+t$。那么存在 $i_1, i_2, \ldots, i_k$，其对应的最小正整数 $2 \leq k \leq 1+t$ 满足

$$
L^{i_1}(\mathbf{s})+L^{i_2}(\mathbf{s})+\cdots+L^{i_{k-1}}(\mathbf{s})=L^{i_k}(\mathbf{s}), \tag{22}
$$

其中，$\mathbf{s}$ 是与矩阵 A 第一行对应的 d 维向量。因此，$L^{i_1}(\mathbf{s})+L^{i_2}(\mathbf{s})+\cdots+L^{i_{k-1}}(\mathbf{s})+L^{i_k}(\mathbf{s})=0$。根据矩阵 A 的定义，不失一般性，设

$$
L^{i_1}(\mathbf{s})=(\overbrace{0 \ldots 0}^{l-1} 1\, 0 \ldots\ldots 0\, \overbrace{0 \ldots 0}^{l-1} 1)=(0^{l-1} 1\, 0 \ldots\ldots 0\, 0^{l-1} 1),
$$

其中， $L^{i_1}(\mathbf{s})$ 中有两个 1，其余均为 0。因此， $gap(A) = l-1$ 且 $l \geq 1$。我们将 $L^{i_1}(\mathbf{s})$ 记为 $(\delta\, 0 \ldots\ldots 0\, \delta)$，其中 $\delta = (0^{l-1}1)$，其余均为 0。回顾一下， $L^{i_j}(\mathbf{s})$、$2 \leq j \leq k$ 是 $L^{i_1}(\mathbf{s})$ 的循环移位序列。于是，由于 $L^{i_1}(\mathbf{s}) + L^{i_2}(\mathbf{s}) + \cdots + L^{i_{k-1}}(\mathbf{s}) + L^{i_k}(\mathbf{s}) = 0$, 可得

$$\begin{pmatrix} L^{i_1}(\mathbf{s}) \\ L^{i_2}(\mathbf{s}) \\ L^{i_3}(\mathbf{s}) \\ \cdots \\ L^{i_k}(\mathbf{s}) \end{pmatrix} = \begin{pmatrix} \delta 0 \cdots\cdots\cdots 0\delta \\ \delta\delta 0 \cdots\cdots\cdots 0 \\ \cdot 0\delta\delta 0 \cdots\cdots\cdots \cdot 0 \\ \cdots\cdots\cdots\cdots \\ 0 \cdots\cdots\cdots 0\delta\delta \end{pmatrix},$$

其中， i_j， $2 \leq j \leq k$ 的阶可适当选取。结合向量 $\mathbf{s}$ 的向量长度为 d这一事实，可得 $kl = d.$

当 $t = 1, 2, \ldots\ldots, d-2,$ 时，由于 $kl = d$且 $k \leq 1+t \leq d-1,$ 我们有 $l > 1,$ 这与 d 为素数相矛盾。因此， $rank(A) = 1+t,$ 于是 $1+t = rank(A) \leq rank(B) \leq 1+t,$ 这意味着 $rank(A) = rank(B) = 1+t$。因此，$|N(n,\ d,\ t)| = 2^{d-rank(A)} = 2^{d-t-1}$。

当 $t = d-1$时，由 $kl = d$及 $2 \leq k \leq 1+t = d$可得 $l = 1$和 $k = d$。根据 (22), 有 $\mathbf{s} + L(\mathbf{s}) + L^2(\mathbf{s}) + \cdots + L^{d-1}(\mathbf{s}) = 0$。可见 $rank(A) = d-1 = t.$$_{t-1}$由于向量 $\mathbf{b} = (b_0, b_1, \ldots, b_t) = (1, 0, \ldots 0, 1)$ 满足 $b_0 \oplus b_1 \oplus \cdots \oplus b_t = 0,$ 其中$\oplus$ 表示异或运算, 因此有 $rank(B) = t$。于是 $rank(A) = rank(B) = t,$ 这意味着 $|N(n,d,t)| = 2^{d-rank(A)} = 2$。

当 $t \geq d$ 时，若 $t = d,$ 则与 $t = d-1$ 的证明类似，可得$rank(A) = d-1 = t-1$ 且 $rank(B) = t,$ 这意味着 $rank(A) \neq rank(B)$。因此$N(n,d,t) = 0$。若 $t > d,$ 则由 $add(\mathbf{s}_n) = t$ 可知

$$\overline{s}_{(n-1) \bmod d} = s_{d-1},\ s_{(n-i) \bmod d} = s_{(d-i) \bmod d},\ 2 \leq i \leq t,\ s_{(n-t-1) \bmod d} = \overline{s}_{(d-t-1) \bmod d},$$

我们看到 $s_{(\overline{n}-1) \bmod d} = s_{d-1}$ 且 $s_{(n-(d+1)) \bmod d} = s_{(d-(d+1)) \text{模}\ d,}$，这就产生了矛盾。因此 $|N(n,d,t)| = 0$。 □

注 3. 根据引理 11，对于素数 $d,$ $N(n,d,t)$ 的值由 $rank(A)$ 决定，而 $rank(A)$ 完全由 $gap(A)$ 决定。当 $n \pmod d = l > \lceil \frac{d-1}{2} \rceil$ 时，可得 $gap(A) = (d-l) - 1$。于是，$|N(n,d,t)| = |N(n',d,t)|$，其中 $n' \pmod d = l' = d-l \leq \lceil \frac{d-1}{2} \rceil$。因此，我们只需计算 $N(n,d,t)$，其中 $n \pmod d = l \leq \lceil \frac{d-1}{2} \rceil$。

根据上述分析，$|\mathcal{P}(n,\omega)|$ 的值可立即由下文得出。

定理 3. 对于正整数 $n \geq 3$ 和 $\omega \geq \lfloor \frac{3n}{4} \rfloor$，令 $\mathcal{P}(n,\omega)$ 表示周期为 n 且非线性复杂度为 ω 的二元移位不等价序列集合。则有

$$|\mathcal{P}(n,\omega)| = \sum_{d=1}^{n-\omega-1} \sum_{e|d} \mu(e) 2^{n-\omega-1-d+d/e} + \sum_{d=n-\omega}^{\lfloor \frac{n}{2} \rfloor} |N(n,d,\omega+d-n)|,$$

其中 $\mu(e)$ 是 ö在 (19) 中的莫比乌斯函数，$|N(n,n-\omega,0)|$ 和 $|N(n,d,\omega+d-n)|$ 与 $d > n-\omega$ 分别可由引理 *10* 和 *11* 确定。

例 2. 以 $n = 16$ 和 $\omega = 12 \geq \lfloor \frac{3n}{4} \rfloor$ 为例，

$$\begin{aligned} & |\mathcal{P}(n,\omega)| \\ = & \sum_{d=1}^{n-\omega-1} \sum_{e|d} \mu(e) 2^{n-\omega-1-d+d/e} + \sum_{d=n-\omega}^{\lfloor \frac{n}{2} \rfloor} |N(n,d,\omega+d-n)| \\ = & \sum_{d=1}^{3} \sum_{e|d} \mu(e) 2^{3-d+d/e} + |N(16,4,0)| + |N(16,5,1)| \\ & + |N(16,6,2)| + |N(16,7,3)| + |N(16,8,4)|. \end{aligned}$$

当 $d = 4$ 时，由引理 *10* 和 $4 \mid 16$ 可得 $|N(16,4,0)| = |A(4)| = 12$。当 $d \in \{5,6,7,8\}$ 时，根据引理 *11*，对于素数 d 和 $d \nmid n$，有 $|N(16,5,1)| = 2^{5-1-1} = 8$ 和 $|N(16,7,3)| = 2^{7-3-1} = 8$；对于合数 d，我们发现

$$|N(16,6,2)| = 2^{6-2-1} - |N(16,2,2)| - |N(16,3,2)| = 8 - 0 - 2 = 6,$$

以及 $|N(16,8,4)| = 0$ 由 $8 \mid 16$ 得出。因此得到 $|\mathcal{P}(n,\omega)| = 18 + 12 + 8 + 6 + 8 + 0 = 52$。该结果与 *[12, 表3.2]* 中给出的穷举搜索一致。

注 *4.* 根据本文的定理 *3*，利用引理 *10* 和引理 *11* 中的公式，可以直接计算 $|\mathcal{P}(n,\omega)|$，$\omega \geq \lfloor \frac{3n}{4} \rfloor$ 的精确值。*Sun* 等人 *[34]* 和 *Xiao* 等人 *[37]* 给出了 $|\mathcal{P}(n,n-1)|$ 和 $|\mathcal{P}(n,n-2)|$，这些值也可以用我们的方法计算。此外，根据定理 *3*，可以确定一个随机的 n-周期二元序列具有非线性复杂度 $\omega \geq \lfloor \frac{3n}{4} \rfloor$ 的精确概率：

$$\frac{n|\mathcal{P}(n,\omega)|}{|A(n)|} = \frac{n|\mathcal{P}(n,\omega)|}{\sum_{e|n} \mu(e) 2^{n/e}}$$

Erdmann 和 *Murphy* 在 *[7]* 中推导了非线性复杂度的近似概率分布；通过与我们的结果比较，可以评估该近似概率的准确性。

需要指出的是，本文提出的方法不适用于 $\lceil \frac{n}{2} \rceil \leq \omega < \lfloor \frac{3n}{4} \rfloor$这种情况。主要原因是，用于生成周期序列的某些有限长序列可能并非代表序列，因此难以识别这些代表序列。此外，某些代表序列彼此移位等价，因而并不唯一。这些因素共同阻碍了对相应周期序列的结构和计数进行准确刻画。

6 结论

本文证明，生成非线性复杂度大于或等于 $\lfloor \frac{3n}{4} \rfloor$ 的移位不等价 n-周期序列的有限长序列，正是唯一代表序列。这使我们能够确定此类周期序列的结构及其精确枚举。未来将研究这些周期序列的更多随机性性质，例如Golomb三随机性公设（平衡性、游程性、自相关性质）、 k错误非线性复杂度以及 k阶相关性度量。

参考文献

[1] C. Canni`ere 和 B. Preneel。Trivium。载于《新型流密码设计：*eSTREAM* 入围方案》（计算机科学讲义），4986：244–266。Springer Berlin Heidelberg，2008年。

[2] A. S. Castellanos、L. Quoos 和 G. Tizziotti。基于 Hermitian函数域的推广构造高非线性复杂度序列。*J. AlgebraAppl.*，23(2)：2450037，2024年2月。

[3] Z. Chen, Z. Chen, J. Obrovsky 和 A. Winterhof. 最大阶复杂度与2进复杂度。*IEEE* 信息论汇刊，70(8)：6060–6067，2024年8月。

[4] Z. Chen, A. I. Gómez, D. Gómez-Pérez 和 A. Tirkel. 二元序列族的相关性度量、线性复杂度与最大阶复杂度。有限域应用，78(101977)：1–11，2022年2月。[5] C. Ding. 某些广义分圆序列的线性复杂度。国际代数与计算杂志，8(4)：431–442，1998年8月。[6] C. Ding, T. Hesseseth 和 W. Shan. 关于勒让德序列的线性复杂度。*IEEE* 信息论汇刊，44(3)：1276–1278，1998年5月。[7] D. Erdmann 和 S. Murphy. 最大阶复杂度的近似分布。设计、码与密码学，10(3)：325–339，1997年3月。[8] S. W. Golomb. 移位寄存器序列：安全和受限访问码生成器、效率码生成器、指定性质生成器、数学模型，第*3*版。新加坡世界科学出版社，2017年。[9] M. Hell, T. Johansson, A. Maximov 和 W. Meier. Grain流密码系列。载于《新型流密码设计：*eSTREAM*决赛入围者》（计算机科学讲义），4986：179–190。Springer Berlin Heidelberg，2008年。[10] T. Helleseth. 非线性移位寄存器——综述与挑战。载于《代数曲线与有限域：密码学及其他应用》，121–144。柏林德古意特，2014年。[11] L. Işık 和 A. Winterhof. 最大阶复杂度与相关性度量。密码学，1(1)：1–7，2017年5月。[12] J. A. Jansen. 非线性流密码系统研究：构造与评估方法。博士论文，代尔夫特理工大学，荷兰代尔夫特，1989年。[13] J. A. Jansen 和 D. Boekee. 能够生成给定序列的最短反馈移位寄存器。载于《密码学进展——*CRYPTO 1989*》，90–99。施普林格纽约，1989年。[14] L. Jin, L. Ma, C. Xing 和 R. Zhu. 一种通过椭圆曲线构造的低相关性新型二元序列族。*IEEE* 信息论汇刊，数字对象标识符：10.1109/TIT.2025.3573103。

[15] P. Ke、Y. Jiang 和 Z. Chen. 关于具有最优自相关的偶长度两类四元序列的线性复杂度。高级数学通信，12(3)：525–539，2018年7月。[16] P. Ke、J. Zhang 和 S. Zhang. 关于长度为 $2p^m$的广义分圆二元序列的线性复杂度与自相关。设计、码与密码学，67(3)：325–339，2013年6月。[17] N. Li 和 X. Tang. 关于具有最优自相关值/幅度的周期为 $4N$ 的二元序列的线性复杂度。*IEEE* 信息论汇刊，57(11)：7597–7604，2011年11月。[18] S. Liang、X. Zeng、Z. Xiao 和 Z. Sun. 长度为 n且非线性复杂度不小于 $n/2$的二元序列。*IEEE* 信息论汇刊，69(12)：8116–8125，2023年12月。[19] R. Lidl 和 H. Niederreiter. 有限域。载于《数学及其应用百科全书》，第*2*版。剑桥大学出版社，英国，1996年。[20] K. Limniotis、N. Kolokotronis 和 N. Kalouptsidis. 关于有限长度序列的非线性复杂度和 Lempel-Ziv复杂度。*IEEE* 信息论汇刊，53(11)：4293–4302，2007年11月。[21] Y. Luo、C. Xing 和 L. You. 从函数域构造高非线性复杂度序列。*IEEE* 信息论汇刊，63(12)：7646–7650，2017年12月。[22] J. Massey. 移位寄存器综合与 BCH译码。*IEEE* 信息论汇刊，15(1)：122–127，1969年1月。[23] J. L. Massey 和 S. Serconek. 周期序列的线性复杂度：一般理论。载于密码学进展——*CRYPTO 1996*，358–371。Springer Berlin Heidelberg，1996年。[24] H. Niederreiter. 二元序列的一些可计算复杂度度量。载于序列及其应用 *1999*，67–78。施普林格伦敦，1999年。[25] H. Niederreiter. 序列的线性复杂度及相关复杂度度量。载于密码学进展——*INDOCRYPT 2003*，1–17。Springer Berlin Heidelberg，2003年。

[26] H. Niederreiter 和 C. Xing. 高非线性复杂度序列。*IEEE* 信息论汇刊，60(10)：6696–6701，2014年10月。[27]计算机安全资源中心（NIST）。轻量级密码学。*https://csrc.nist.gov/projects/lightweight-cryptography.html*，2020年。[28] G. Petrides 和 J. Mykkeltveit. 周期二元序列的非线性复杂度分类。载于序列及其应用——*SETA 2006*。209–222。Springer Berlin，2006年。[29] G. Petrides 和 J. Mykkeltveit. 递归的复合与周期二元序列的非线性复杂度。设计、码与密码学，49(1-3)：251–264，2008年3月。[30] P. Rizomiliotis. 构造具有最大非线性跨度的周期二元序列。*IEEE* 信息论汇刊，52(9)：4257–4261，2006年9月。[31] P. Rizomiliotis 和 N. Kalouptsidis. 关于二元序列非线性跨度的结果。*IEEE* 信息论汇刊，51(4)：1555–1563，2005年4月。[32] P. Rizomiliotis、N. Kolokotronis 和 N. Kalouptsidis. 关于二元序列的二次跨度。*IEEE* 信息论汇刊，51(5)：1840–1848，2005年5月。[33] R. A. Rueppel. 流密码的分析与设计。Springer Berlin，1986年。[34] Z. Sun、X. Zeng、C. Li 和 T. Helleseth. 关于最大非线性复杂度周期序列的研究。*IEEE* 信息论汇刊，63(10)：6188–6198，2017年10月。[35] Z. Sun、X. Zeng、C. Li、Y. Zhang 和 L. Yi. 有限域上最终周期序列的扩展复杂度。*IEEE* 信息论汇刊，67(11)：7550–7560，2021年11月。[36] X. Tang、P. Udaya 和 P. Fan. 一类具有三级相关特性和大线性跨度的新型非二进制序列。*IEEE* 信息论汇刊，51(8)：2906–2914，2005年8月。[37] Z. Xiao、X. Zeng、C. Li 和 Y. Jiang. 周期为 N 且非线性复杂度为 $N-2$的二元序列。密码学与通信，11(4)：735–757，2019年7月。

[38] C. Xing、P. V. Kumar和C. Ding。来自函数域的低相关大线性跨度序列。*IEEE* 信息论汇刊，49(6)：1439–1446，2003年6月。[39] C. Xing和K. Y. Lam。具有近乎完美线性复杂度谱的序列与有限域上的曲线。*IEEE* 信息论汇刊，45(5)：1267–1270，1999年5月。[40] F. Yan、P. Ke和Z. Chang。由Legendre序列对构造的Tang-Gong交错序列的对称2进复杂度。密码学与通信，17(1)：167– 179，2025年2月。[41] L. Yi、X. Zeng和Z. Sun。剩余类环上具有大非线性复杂度的有限长度非二元序列 $\mathbb{Z}_m$。高级数学通信，15(4)：701–720，2021年11月。[42] Q. Yuan、C. Li、X. Zeng、T. Helleseth和D. He。周期二元序列非线性复杂度的进一步研究。*IEEE* 信息论汇刊，70(7)：5376–5391，2024年7月。

附录 A：引理 6的证明

证明。设 $a = n - c - d_1$，则 $h = a + b$。因此，$\mathbf{v}_n = R^h(\mathbf{s}_n) = R^{a+b}(\mathbf{s}_n)$。由 [42]，中引理 8 证明的第一段可知，当 n 为偶数时，$0 < b \le c + d_2 - 1$。当 $c = \lfloor \frac{n}{2} \rfloor$ 且 n 为奇数时，我们断言 $0 \le b < c + d_2$。

设 $n = 2k+1$，则 $c = k$。由 $\mathbf{s}_{2k+1} \in \mathcal{B}(2k+1, k, d_1)$ 可知，$(s_0, s_1, \ldots, s_{k-2})$ 和 $(s_{d_1}, s_{d_1+1}, \ldots, s_{d_1+k-2})$ 是一对长度为 $k-1$ 且后继不同的相同子序列。令 $\mathbf{v}_n = R^h(\mathbf{s}_n)$，则设 $h \le n - c - d_1 - 1 = k - d_1$。由于 $\mathbf{v}_{2k+1} \in \mathcal{B}(2k+1, k, d_2)$ 满足 $d_2 \le k$，我们有 $\mathbf{v}_{2k} \in \mathcal{B}(2k, k, d_2)$。因此，$\mathbf{v}_{2k} \in \mathcal{B}(2k, k, d_2)$ 有一对相同的序列 $(v_0, v_1, \ldots, v_{k-2})$ 和 $(v_{d_2}, v_{d_2+1}, \ldots, v_{d_2+k-2})$，其长度为 $k-1$，开头处的后继不同，并且还有另一对

$$\begin{cases} (s_0, s_1, \ldots, s_{k-2}) & = (v_h, v_{h+1}, \ldots, v_{h+k-2}), \\ (s_{d_1}, s_{d_1+1}, \ldots, s_{d_1+k-2}) & = (v_{h+d_1}, v_{h+d_1+1}, \ldots, v_{h+d_1+k-2}). \end{cases}$$

其后具有不同的后继，其中 $h + d_1 + k - 2 \le (k - d_1) + d_1 + k - 2 = 2k - 2$。这与引理 2 中的事实相矛盾。因此我们有 $h \ge n - c - d_1$。对于 $\mathbf{v}_n = R^h(\mathbf{s}_n) \in \mathcal{B}(n, c, d_2)$ 和 $R^{h'}(\mathbf{v}_n) \in \mathcal{B}(n, c, d_1)$，我们看到 $h' = n - h \ge n - c - d_2$，即 $h \le c + d_2$。

因此我们得到 $n-c-d_1 \le h = (n-c-d_1) + b \le c+d_2$。由 $n-c-d_1 \ge 1$ 可知 $0 \le b < c+d_2$。因此，所述结论成立。

因此，当 n 为偶数时，我们有 $0 < b \le c+d_2-1$；当 n 为奇数时，我们有 $0 \le b \le c+d_2-1$。于是，只需考察满足 $0 \le b \le c+d_2-1$的$\mathbf{v}_n = R^{a+b}(\mathbf{s}_n)$，其中当$b=0$时，$-c = \lfloor \frac{n}{2} \rfloor$为奇数 n。注意，$\mathbf{v}_n = R^{a+b}(\mathbf{s}_n)$具有以下形式，

$$\begin{aligned} \mathbf{v}_n &= (\overbrace{(v_0,\ \ldots,\ v_{c+d_2-1})}^{c+d_2}(v_{c+d_2},\ \ldots,\ v_{n-t_2-1})\overbrace{(v_{n-t_2},\ \ldots,\ v_{n-1})}^{t_2}) \\ = R^{a+b}(\mathbf{s}_n) &= (\underbrace{(v_0,\ \ldots,\ v_{b-2},\ v_{b-1})}_{b}(v_b,\ \ldots,\ v_{b+a-t_1-1})\underbrace{(v_{b+a-t_1},\ \ldots,\ v_{n-1})}_{t_1+c+d_1-b}). \end{aligned} \tag{23}$$

由于满足 add的$\mathbf{v}_n \in \mathcal{B}(n,\ c,\ d_2) = t_2(\mathbf{v}_n)$，可得

$$v_i = v_{i+d_2} \text{ for } i \in [-t_2, c-2] \text{ and } v_{c-1} = \overline{v}_{c+d_2-1}. \tag{24}$$

此外，由于满足 add的$\mathbf{s}_n \in \mathcal{B}(n,\ c,\ d_1) = t_1(\mathbf{s}_n)$，因此有

$$s_i = s_{i+d_1} \text{ for } i \in [-t_1, c-2] \text{ and } s_{c-1} = \overline{s}_{c+d_1-1}.$$

由于 $v_{i+a+b} = s_i$，我们有

$$v_i = v_{i+d_1} \text{ for } i \in [b+a-t_1, b+n-d_1-2] \text{ and } v_{b+n-d_1-1} = \overline{v}_{b+n-1}, \tag{25}$$

其中，上述等式中的下标均按 n 取模。因此，$(v_{b+a-t_1}, \ldots, v_{n-1}, v_n, \ldots, v_{b+n-2}, v_{b+n-1})$中任意连续 d_1 项所组成的子序列，都是 $\mathbf{s}_{d_1}$ 的一个移位版本。根据 (23) 中 $\mathbf{v}_n = R^{a+b}(\mathbf{s}_n)$ 的形式，我们将利用 (24) 和 (25) 证明，$\mathbf{s}_n$ 的子序列 $\mathbf{s}_{d_1}$ 有两种汉明重量不同的表示，这显然构成矛盾。下文中，我们针对 $0 \le b \le c+d_2-1$ 时 b 的不同取值分两种情形讨论。

$$\begin{aligned} \mathbf{v}_n &= (\overbrace{v_0, v_1, \ldots, v_i, v_{i+1}, \ldots, v_{c+d_2-2}, v_{c+d_2-1}}^{c+d_2}, \ldots, v_{n-t_2}, \ldots, v_{n-1}) \\ = R^{a+b}(\mathbf{s}_n) &= (\underbrace{v_0, \ldots, v_{b-1}, v_b,\ \ldots,\ v_{b+a-t_1}}_{b+(a-t_1)+d_1+d_2}, \ldots, v_{b+a-t_1+d_1+d_2-1}, \ldots,\ v_{n-1}). \end{aligned}$$

$\overleftarrow{\quad}$ $-d_2$　　$\overleftrightarrow{\quad}$ d_1-length

图1：情形（1）的可视化描述

情形（1）：若 $0 \le b < t_1$，则 $b + a - t_1 \le c - d_1$。考虑 d_1 元组子序列$\mathbf{v}_{[c+d_2-d_1:c+d_2]}$，由 (24) 可得

$$\mathbf{v}_{[c+d_2-d_1:c+d_2]} = (v_{c+d_2-d_1}, \ldots, v_{c+d_2-2}, v_{c+d_2-1}) = (v_{c-d_1}, \ldots, v_{c-2}, \overline{v}_{c-1}).$$

回想一下，任意连续的 d_1 项（v_{b+a-t_1}，……，v_{n-1}，v_n，……，v_{b+n-2}，v_{b+n-1}）都由$\mathbf{s}_{d_1}$ 的一个移位版本组成。由于 $b + a - t_1 \le c - d_1$ 和 $c + d_2 \le n + b - 1$，因此 $\mathbf{v}_{[c-d_1:c]}$ 和$\mathbf{v}_{[c+d_2-d_1:\ c+d_2]}$ 都是$\mathbf{s}_{d_1}$的移位版本。综合这些结果，它们的汉明重量满足

$$wt(\mathbf{s}_{d_1}) = wt(\mathbf{v}_{[c-d_1:c]}) = wt(\mathbf{v}_{[c+d_2-d_1:c+d_2]}) = wt((v_{c-d_1}, \ldots, v_{c-2}, \overline{v}_{c-1})),$$

矛盾。

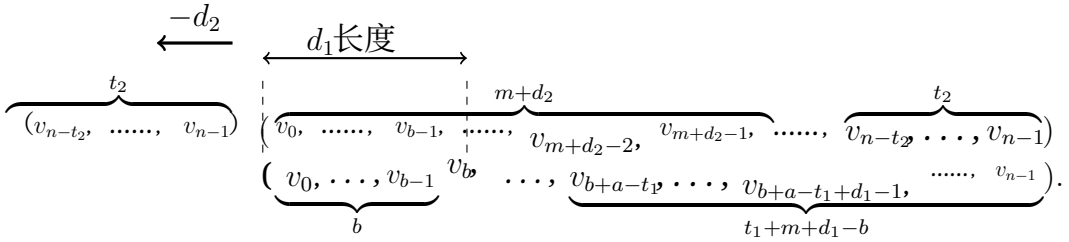

图2：情形（2）的可视化描述

情形（2）：如果 $d_1 + d_2 \le b + t_2$ 且 $b < c + d_2$，那么 $d_1 + d_2 - t_2 \le b < c + d_2$。考虑 d_1元组子序列 $\mathbf{v}_{[b-d_1-d_2:\ b-d_2]}$，由于 $-t_2 \le b - d_1 - d_2$ 且 $b - d_2 < c$，由（24）可得

$$\mathbf{v}_{[b-d_1-d_2:b-d_2]} = (v_{b-d_1-d_2}, \ldots, v_{b-d_2-2}, v_{b-d_2-1}) = (v_{b-d_1}, \ldots, v_{b-2}, v_{b-1}) = \mathbf{v}_{[b-d_1:b]}.$$

回顾一下，（v_{b+a-t_1-n}，……，v_{-1}，v_0，……，v_{b-2}，v_{b-1}）中的任意连续 d_1 项都由$\mathbf{s}_{d_1}$ 的一个移位版本组成。由于 $b - d_1 - d_2 \ge b + a - t_1 - n$ 和 $b - d_2 < b$，我们得到$\mathbf{v}_{[b-d_1-d_2:\ b-d_2]}$ 以及（v_{b-d_1}，……，v_{b-2}，v_{b-1}）都是$\mathbf{s}_{d_1}$的移位版本。结合上述等式可得

$$wt(\mathbf{s}_{d_1}) = wt(v_{b-d_1}, \ldots, v_{b-2}, \overline{v}_{b-1}) = wt(\mathbf{v}_{[b-d_1-d_2:b-d_2]}) = wt(\mathbf{v}_{[b-d_1:b]}),$$

这与矛盾相矛盾。

因此，只有 $t_1 \le b < d_1 + d_2 - t_2$ 才有可能。 □

附录B：引理7的证明

证明。根据引理6，对于 $R^b(\mathbf{s}_n) \in \mathcal{B}(n, c, d_2)$，只需考虑 $t_1 \le b < d_1 + d_2 - t_2$。令 $R^b(\mathbf{s}_n) = \mathbf{v}_n$。那么 $v_{i+b} = s_i$，其中下标均取模 n。假设 $b \neq d_2$，那么我们将推出矛盾：同一子序列 $\mathbf{v}_{d_2}$(或 $\mathbf{s}_{d_1}$) 的两个移位版本具有不同的汉明重量。由于 $\mathbf{v}_n \in \mathcal{B}(n, c, d_2)$ 且 $add(\mathbf{v}_n) = t_2$，可得

$$v_{-t_2-1} = \overline{v}_{d_2-t_2-1},\ v_i = v_{i+d_2} \text{ for } i \in [-t_2, c-2] \text{ and } v_{c-1} = \overline{v}_{c+d_2-1}. \tag{26}$$

此外，由于$\mathbf{s}_n \in \mathcal{B}(n, c, d_1)$ 满足 $add(\mathbf{s}_n) = t_1$，因此有

$$s_{-t_1-1} = \overline{s}_{d_1-t_1-1},\ s_i = s_{i+d_1} \text{ for } i \in [-t_1, c-2] \text{ and } s_{c-1} = \overline{s}_{c+d_1-1}.$$

由 $s_i = v_{i+b}$，可得

$$v_{b-t_1-1} = \overline{v}_{b+d_1-t_1-1},\ v_i = v_{i+d_1} \text{ for } i \in [b-t_1, b+c-2] \text{ and } v_{b+c-1} = \overline{v}_{b+c+d_1-1}. \tag{27}$$

根据 (26)，$(v_{-t_2-1}, v_{-t_2}, v_{-t_2+1}, \ldots, v_{c+d_2-2}, v_{c+d_2-1})$ 中任意连续的 d_2 项所组成的子序列，是 $\mathbf{v}_{d_2} = (v_0, \overline{v}_1, \ldots, v_{d_2-1})$ 的一个移位版本。同理，根据 (27)，$(v_{b-t_1-1}, v_{b-t_1}, v_{b-t_1+1}, \ldots, v_{b+c+d_1-2}, v_{b+c+d_1-1})$ 中任意连续的 d_1 项所组成的子序列，是 $\mathbf{s}_{d_1} = (s_0, s_1, \ldots, s_{d_1-1})$ 的一个移位版本。接下来，我们将研究 $\mathbf{v}_{d_2}$ 和 $\mathbf{s}_{d_1}$ 的移位序列的不同表示形式。注意，$d_2 \le d_1 \le c$ 和 $t_2 \ge t_1 \ge 0$。根据 b 的取值，我们将讨论分为四种情况。

情形（1）： $d_2 + 1 \le b \le c + t_1$。容易验证，$(v_c, v_{c+1}, \ldots\ldots, v_{c+d_2-1})$ 是$\mathbf{v}_{d_2}$的移位版本。由于 $d_2 + 1 \le b \le c + t_1$，上述下标满足 $b - t_1 \le c, c+1, \ldots\ldots, c + d_2 - 1 \le b + c - 2$。由式（27）可从 $c + d_1 = n$ 推出

$$(v_c, v_{c+1}, \ldots, \overline{v}_{c+d_2-1}) = (v_{c+d_1}, v_{c+d_1+1}, \ldots, \overline{v}_{c+d_1+d_2-1}) = (v_0, v_1, \ldots, \overline{v}_{d_2-1}).$$

因此，$(v_0, v_1, \ldots\ldots, v_{d_2-1})$ 是$\mathbf{v}_{d_2} = (v_0, v_1, \ldots\ldots, v_{d_2-1})$ 的移位序列，这就产生了矛盾。

情形（2）： $c + t_1 + 1 \le b < d_1 + d_2 - t_2$。由于 $d_1 + d_2 < c + t_2 + t_1$，这种情形不可能发生。

情形（3）： $d_2 - t_2 \le b < d_2$。由于 $-t_2 \le c+b-d_2, c+b-d_2+1, \ldots\ldots, c+b-1 \le c+d_2-2$，显然 $(v_{c+b-d_2}, v_{c+b-d_2+1}, \ldots\ldots, v_{c+b-1})$ 是$\mathbf{v}_{d_2}$（26）中的一个移位序列。根据

$d_2 \le c$和（27），下标满足 $b-t_1 \le c+b-d_2$，$c+b-d_2+1$，……，$c+b-2 \le c+b-2$，且 $v_{c+b-1} = \overline{v}_{c+b-1+d_1}$。于是我们有

$$\begin{aligned} & (v_{c+b-d_2}, v_{c+b-d_2+1}, \ldots, v_{c+b-2}, v_{c+b-1}) \\ = \ & (v_{c+b+d_1-d_2}, v_{c+b+d_1-d_2+1}, \ldots, v_{c+b+d_1-2}, \overline{v}_{c+b+d_1-1}) \\ = \ & (v_{b-d_2}, v_{b-d_2+1}, \ldots, v_{b-2}, \overline{v}_{b-1}), \end{aligned}$$

这意味着（v_{b-d_2}，v_{b-d_2+1}，……，v_{b-2}，$\overline{v}_{b-1}$）是$\mathbf{v}^{d_2}$的移位序列。事实上，根据 $-t_2 \le b-d_2$，$b-d_2+1$，……，$b-1 \le c+d_2-2$和（26），我们有$\mathbf{v}_{[b-d_2:\ d]} =$（$v_{b-d_2}$，$v_{b-d_2+1}$，……，$v_{b-2}$，$v_{b-1}$）是$\mathbf{v}^{d_2}$的移位序列，矛盾。

情形（4）：$t_1 \le b \le d_2-t_2-1$。考虑序列（$v_{c+d_2-d_1}$，$v_{c+d_2-d_1+1}$，……，v_{c+d_2-1}）。根据（27），由于 $b-t_1 \le c+d_2-d_1$，$c+d_2-d_1+1$，……，$c+d_2-1 \le b+n-2$，我们可以看出（$v_{c+d_2-d_1}$，$v_{c+d_2-d_1+1}$，……，v_{c+d_2-1}）是$\mathbf{s}^{d_1}$的移位序列。由（26）可得

$$(v_{c+d_2-d_1}, v_{c+d_2-d_1+1}, \ldots, v_{c+d_2-1}) = (v_{c-d_1}, v_{c-d_1+1}, \ldots, v_{c-2}, \overline{v}_{c-1}).$$

因此，$(v_{c-d_1}$，v_{c-d_1+1}，……，$\overline{v}_{c-2}$，$v_{c-1})$是$\mathbf{s}^{d_1}$的移位序列。此外，由于 $d_1+d_2 < c+t_2+t_1$，我们有 $b-t_1 \le c-d_1$。因此，由式 (27)可知，$(v_{c-d_1}$，v_{c-d_1+1}，……，v_{c-2}，$v_{c-1})$是$\mathbf{s}^{d_1}$的移位序列，这就产生了矛盾。

最后，综合上述四种情况并应用条件 $t_1 \le b < d_1+d_2-t_2$，我们得出结论：$b = d_2$。

□

附录 C：定理1中紧界的证明

Pr（iii）$n = 8k+4$ 和（iv）$n = 8k$情形下紧界的证明：

（iii）当 $n = 8k+4$ 时，令 $c \ge c_0 = 6k+1$ 和 $m = \lfloor \frac{n}{2} \rfloor = 4k+2$。假设存在一对满足 $0 \le add(\mathbf{s}'_n) < add(\mathbf{v}'_n)$ 的移位等价序列 $(\mathbf{s}'_n, \mathbf{v}'_n)$，则根据引理 3，我们有 $\mathbf{s}_n = L^{c-m}(\mathbf{s}'_n) \in \mathcal{B}(n, m, d_1)$ 且 $\mathbf{v}_n = L^{c-m}(\mathbf{v}'_n) \in \mathcal{B}(n, m, d_2)$。此外，根据式 (7)，一些参数满足

$$\begin{cases} d_1 + d_2 < 2(n-c) \le 4k+6, \quad k \ge 2 \\ add(\mathbf{s}_n) = t_1 \ge c-m \ge 2k-1, \quad add(\mathbf{v}_n) = t_2 \ge t_1+1 \ge 2k. \end{cases} \tag{28}$$

令 $\mathbf{v}_n = R^{a+b}(\mathbf{s}_n)$，$a = n-m-d_1$。因此，根据引理 6，只需研究 $t_1 < b < d_1+d_2-t_2$ 的情形，也就是 $2k \le b \le 2k+4$。

由于 $b < d_1 + d_2 - t_2$，我们有 $n - t_2 - 1 > b + a - t_1$。由 $d_1 \le t_1 + t_2$可得 $b < d_1 + d_2 - t_2 \le d_2 + t_1$，这意味着 $b + (a - t_1) + d_1 < m + d_2$。因此，$\mathbf{v}_n = R^{a+b}(\mathbf{s}_n)$ 具有如下形式:

$$\begin{array}{rl} \mathbf{v}_n & = (\overbrace{v_0,\, v_1,\, \ldots, v_i,\, v_{i+1}, \ldots,\, v_{m+d_2-2},\, v_{m+d_2-1}}^{m+d_2}, \ldots, \overbrace{v_{n-t_2}, \ldots, v_{n-1}}^{t_2}) \\ = R^{a+b}(\mathbf{s}_n) & = (\underbrace{v_0,\, \ldots,\, v_{b-1}}_{b},\, v_b,\, \ldots,\, \underbrace{v_{b+a-t_1},\, \ldots,\, v_{b+a-t_1+d_1-1},\, \ldots,\, v_{n-1}}_{t_1+m+d_1-b}). \end{array} \tag{29}$$

回顾一下，我们有

$$v_{-t_2-1} = \overline{v}_{d_2-t_2-1},\ v_i = v_{i+d_2} \text{ for } i \in [-t_2, m-2] \text{ and } v_{m-1} = \overline{v}_{m+d_2-1}. \tag{30}$$

and

$$v_{b+a-t_1-1} = \overline{v}_{d_1+b+a-t_1-1},\ v_i = v_{i+d_1} \text{ for } i \in [b+a-t_1, b+n-d_1-2] \text{ and } v_{b+n-d_1-1} = \overline{v}_{b+n-1}. \tag{31}$$

根据（29）和（31），序列组 $\mathcal{A}$ 和 $\mathcal{B}$ 中的每个序列都是$\mathbf{s}^{d_1}$的移位等价序列。

$$\mathcal{A} = \begin{cases} (\overline{v}_{b+a-t_1-1}, v_{b+a-t_1}, \ldots, v_{b+a-t_1+d_1-2}), \\ (v_{b+a-t_1}, \ldots, v_{b+a-t_1+d_1-1}), \\ \quad \ldots \qquad \ldots \\ (v_{m+d_2-d_1}, \ldots, v_{m+d_2-1}), \end{cases} \tag{32}$$

$$\mathcal{B} = \begin{cases} (v_{-t_2-1}, \ldots, v_{-t_2+d_1-2}), \\ (v_{-t_2}, \ldots, v_{-t_2+d_1-1}), \\ \quad \ldots \qquad \ldots \\ (v_{b-d_1-1}, \ldots, v_{b-2}), \\ (v_{b-d_1}, \ldots, v_{b-2}, \overline{v}_{b-1}), \end{cases} \tag{33}$$

注意，总存在一个正整数 i，使得 $m - t_1 \le d_2 i < m + d_2 - t_1$。下面，根据序列组 $\mathcal{A}$ 与 $\mathcal{B}$ 之间的序列关系，我们将给出 $\mathbf{s}^{d_1}$ 的两种不同表示，然后证明这两种表示具有不同的汉明重量，从而导致矛盾。我们根据 $d_2 i$ 与 $m + d_2 - b$ 的关系，将讨论分为三种情形。

情形（1）：若 $m - t_1 \le d_2 i < m + d_2 - b$，则考虑 $(v_{b+d_2 i-d_1},\ \ldots,\ v_{b+d_2 i-1})$，其中$b + a - t_1 \le b + d_2 i - d_1 < m + d_2 - d_1$。因此，从序列组 $\mathcal{A}$ （32），

$(v_{b+d_2i-d_1}, \ldots, v_{b+d_2i-1})$ 是 $\mathbf{s}^{d_1}$ 的移位版本。由 $d_1 \le t_1+t_2$ 和 $b > t_1$可知 $b-d_1 \ge -t_2$。此外 $-t_2 < b+a-t_1 \le b+d_2i-d_1 < m+d_2-d_1$。因此，（30）中的关系意味着

$$(v_{b+d_2i-d_1}, \ldots, v_{b+d_2i-1}) = (v_{b-d_1}, \ldots, v_{b-1})$$

也是$\mathbf{s}^{d_1}$的移位等价序列，这与$(v_{b-d_1}, \ldots, v_{b-2}, v_{b-1})$是$\mathbf{s}^{d_1}$的移位版本相矛盾，其中序列组 $\mathcal{B}$ 见（33）。

情形（2）：如果 $m+d_2-b < d_2i < m+d_2-t_1$，则考虑子序列（$v_{m+d_2-d_2i-d_1}, \ldots, v_{m+d_2-d_2i-1}$）。由 $d_1 \le t_1+t_2$，可得

$$-t_2 \le t_1-d_1 < m+d_2-d_2i-d_1 < b-d_1 < m+d_2-d_1.$$

因此，由序列组 $\mathcal{B}$见（33），$(v_{m+d_2-d_2i-d_1}, \ldots, v_{m+d_2-d_2i-1})$是$\mathbf{s}^{d_1}$的移位等价序列。回顾一下，$-t_2 < m+d_2-d_2i-d_1 < m+d_2-d_1$，那么由（30）可得

$$(v_{m+d_2-d_2i-d_1}, \ldots, v_{m+d_2-d_2i-1}) = (v_{m+d_2-d_1}, \ldots, \overline{v}_{m+d_2-1}),$$

也是$\mathbf{s}^{d_1}$的移位版本，这与$(v_{m+d_2-d_1}, \ldots, v_{m+d_2-1})$是$\mathbf{s}^{d_1}$ 依据序列组 $\mathcal{A}$ 见（32）的移位版本相矛盾。

情形（3）：若 $d_2i = m+d_2-b$，则令 $(-t_2-1)+(m+d_2-b) = g$。由 $t_1 < b < d_1+d_2-t_2$ 可知，g 和 $b+a-t_1-1$ 属于同一区间 $(m-d_1-1, m+d_2-t_1-t_2-1)$。由于我们无法确定哪一个更大，因此需要考虑三种可能的情形。

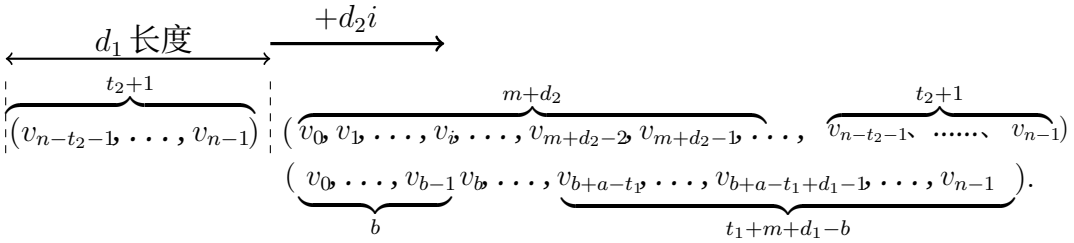

图 3：子情形 (3.1) 的可视化描述

子情形（3.1）：$b+a-t_1-1 < g$.由于 $b > t_1 > d_1-t_2-1$由 $d_1 \le t_1+t_2$，可得 $g < m+d_2-d_1$。因此 $b+a-t_1-1 < g < m+d_2-d_1$，这意味着 $(v_g, \ldots\ldots, v_{g+d_1-1})$

是$\mathbf{s}^{d_1}$根据 $\mathcal{A}$在（32）得到的移位版本。对于（v_{-t_2-1}，……， $v_{-t_2+d_1-2}$）作为$\mathbf{s}^{d_1}$的移位等价序列，由于 $g=\ (-t_2-1)\ +d_2 i<m+d_2-d_1$，由（30）可得

$$(v_{-t_2-1},\ldots,v_{-t_2+d_1-2})=(\overline{v}_g,\ldots,v_{g+d_1-1}),$$

这与（v_g，……， v_{g+d_1-1}）是$\mathbf{s}^{d_1}$的移位版本相矛盾。

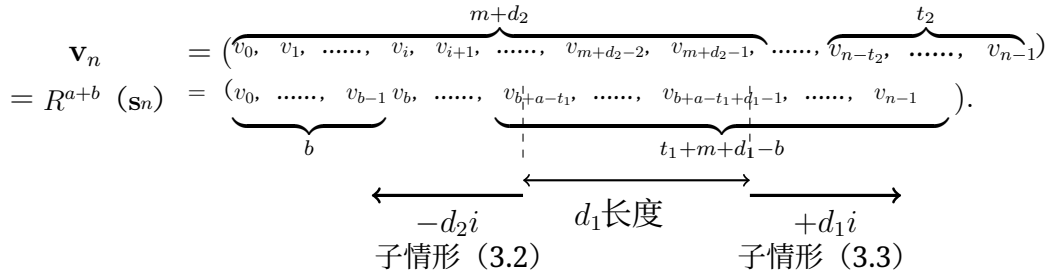

图4：子情形（3.2）和子情形（3.3）的可视化描述

子情形（3.2）： $b+a-t_1-1>g$. 那么 $2b+t_2>d_1+d_2+t_1$。考虑子序列 $(v_{b+a-t_1-1},\overline{v}_{b+a-t_1},\ldots,v_{b+a-t_1+d_1-2})$ 它是 $\mathbf{s}^{d_1}$ 的移位版本。令$h=b+a-t_1-1-d_2 i$。由于 $b+a-t_1-1-(m+d_2-b)\ =2b-d_1-d_2-t_1-1$以及 $2b+t_2>d_1+d_2+t_1$，可以得到 $h\geq -t_2$。回顾 $b+a-t_1-1<m+d_2-d_1$，根据（30）可得

$$(\overline{v}_{b+a-t_1-1},v_{b+a-t_1},\ldots,v_{b+a-t_1+d_1-2})=(\overline{v}_h,\ldots,v_{h+d_1-1}). \tag{34}$$

此外，显然 $h<b-d_1$ 由 $b<d_1+d_2-t_2\leq d_2+t_1$可知。因此 $-t_2\leq h<b-d_1$意味着（v_h，……， v_{h+d_1-1}）是$\mathbf{s}^{d_1}$ 在 $\mathcal{B}$中定义的移位等价序列（33），这与（34）矛盾。

子情形（3.3）： $b+a-t_1-1=g$，这意味着 $2b=d_1+d_2+t_1-t_2$。因此我们知道

$$(v_{b+a-t_1},v_{b+a-t_1+1},\ldots,v_{b+a-t_1+d_1-1})=(v_{-t_2},\ldots,v_{-t_2+d_1-1}). \tag{35}$$

当且仅当 35) 中的方程成立，其中 $d_1\,|(m+b-d_2)$ 因为 35) 中的两个子序列是非周期的，其中 $m+b-d_2=(n-t_2)\ -(b+a-t_1)$。现在这些参数满足

$$\begin{cases} t_1<b<d_1+d_2-t_2,\ \text{i.e. } 2k\leq b\leq 2k+4,\\ d_2\,|\,m+d_2-b,\\ 2b=d_1+d_2+t_1-t_2,\\ d_1\,|\,m+b-d_2. \end{cases} \tag{36}$$

接下来，我们将利用（36）和序列的结构推出矛盾。由于 $m+b \geq (4k+2)+2k > 4k+5 \geq d_1+d_2$ 由（28）得出，因此有 $m+b-d_2 > d_1$。此外，$d_1 \mid m+b-d_2$，由此可得 $2d_1 \leq m+b-d_2$。因此，根据 $b < d_1+d_2-t_2$，有 $2d_1 \leq m+b-d_2 < m+d_1-t_2$，这意味着 $d_1 \leq m-t_2-1$。同理，由于$d_2 \mid m+d_2-b$ 且 $m-b \geq (4k+2)-(2k+4) = 2k-2 > 0$ 由 $k \geq 2$ 得出，我们从（36）得知 $d_2 \leq m-b \leq m-t_1-1$。

因此，$2b = d_1+d_2+t_1-t_2 \leq (m-t_2-1)+(m-t_1-1)+t_1-t_2 = 2(m-t_2-1)$，也就是说，$t_1+1 \leq b \leq m-t_2-1 \leq m-t_1-2$，这意味着 $t_1 \leq \frac{m-3}{2} = 2k-\frac{1}{2}$。由 $t_1 \geq 2k-1$ 在(28)中，我们可以看出 $t_1 = 2k-1$，由此可得 $2k \leq b \leq 2k+1$。综上，我们得到 $t_1 = 2k-1$，$t_2 \geq 2k$，$2k \leq b \leq 2k+1$，$d_1 \leq m-t_2-1 \leq 2k+1$以及 $d_2 \leq m-t_1-1 \leq 2k+2$。最后，根据 b的取值，我们分为两种情况。

$b = 2k+1$。由 $2b = d_1+d_2+t_1-t_2$和 $t_1 = 2k-1$可得 $d_1+d_2-t_2 = 2k+3$。由于 $d_2 \leq 2k+2$，我们有 $d_1-t_2 \geq 1$。此外 $d_1-t_2 \leq (2k+1)-2k = 1$，因此 $d_1-t_2 = 1$，这意味着 $d_2 = 2k+2$。这与 $d_2 \mid m-b$且 $m-b = (4k+2)-(2k+1) = 2k+1$矛盾。

$b = 2k$。由 $2b = d_1+d_2+t_1-t_2$和 $t_1 = 2k-1$可得 $d_1+d_2-t_2 = 2k+1$。由于 $d_1 \leq 2k+1$和 $d_2 \leq 2k+2$，我们有 $d_2-t_2 \geq 0$和 $d_1-t_2 \geq -1$，这表明 $2k \leq t_2 \leq d_2 \leq 2k+2$和 $2k-1 \leq t_2-1 \leq d_1 \leq 2k+1$。因为 $d_2 \mid m-b$且 $m-b = 2k+2$，显然 $d_2 = 2k+2$。因此 $m+b-d_2 = 2k$。由$d_1 \mid m+b-d_2$可得 $d_1 = 2k$。所以，我们有 $a+b = (n-m-d_1)+b = 4k+2$和

$$\begin{cases} \mathbf{s}_n & \in \mathcal{B}(8k+4, 4k+2, 2k) \text{ with } add(\mathbf{s}_n) = t_1 = 2k-1 \\ R^{4k+2}(\mathbf{s}_n) = \mathbf{v}_n & \in \mathcal{B}(8k+4, 4k+2, 2k+2) \text{ with } add(\mathbf{s}_n) = t_2 = 2k+1 \end{cases}$$

根据$\mathbf{s}_n$的结构，我们知道$s_{-2k} = s_0$，$s_i = s_{i \bmod 2k}$，$-(2k-1) = -t_1 \leq i \leq m+d_1-2 = 6k$和 $s_{6k+1} = \overline{s_1}$。因此

$$\mathbf{v}_{d_2} = (s_{4k+2}, \ldots, s_{6k-1}, s_{6k}, s_{6k+1}, s_{6k+2}, s_{6k+3}) = (s_2, \ldots, s_{2k-1}, s_0, \overline{s}_1, s_{6k+2}, s_{6k+3}).$$

此外，我们有

$$\begin{aligned} \mathbf{v}_{d_2} &= (s_{6k+4}, \ldots, s_{8k+3}, s_0, s_1) \\ &= (s_{-2k}, s_{-2k+1}, \ldots, s_{-2}, s_{-1}, s_0, s_1) = (\overline{s}_0, s_1, \ldots, s_{2k-3}, s_{2k-2}, s_{2k-1}, s_0, s_1). \end{aligned}$$

结合$\mathbf{v}_{d_2}$的两种表示，可得 $s_0 = s_2 = s_4 = \cdots = s_{2k-2} = \overline{s}_0$和 $s_1 = s_3 = s_5 = \cdots = s_{2k-1} = s_1$，这与矛盾相悖。

因此，当 $n = 8k + 4$ 和 $c \geq 6k + 1$时，在 $\mathcal{B}(n, c)$中不存在一对满足 $add(\mathbf{s}'_n) < add(\mathbf{v}'_n)$的移位等价序列$(\mathbf{s}'_n, \mathbf{v}'_n)$。

另一方面，假设一个序列具有以下形式

$$\mathbf{s}_n = (s_0, \ldots, s_{8k+3}) = ((\underline{\alpha\beta\alpha^{2k-2}}\,\alpha\beta\alpha^{2k-2}\,\alpha\beta\alpha^{2k-2}\,\alpha^2)\alpha\beta\alpha^{2k}),$$

其中 $\beta = \bar{\alpha}$和 β^l 是由 l 个 β重复构成的序列。显然，$\mathbf{s}_n$ 属于 $\mathcal{B}(8k + 4,\ 4k + 2,\ 2k)$，且 $add(\mathbf{s}_n) = 2k - 2$，其中 $\mathbf{s}_d = \mathbf{s}_{2k}$ 带有下划线。考虑序列

$$\begin{aligned}\mathbf{u}_n &= R^{2k-2}(\mathbf{s}_n) = ((\underline{\alpha^{2k-1}\beta}\,\alpha^{2k-1}\beta\,\alpha^{2k-1}\beta\,\alpha^{2k})\alpha\beta\alpha^2),\\ \mathbf{v}_n &= R^{6k}(\mathbf{s}_n) = ((\underline{\alpha^{2k-3}\beta\alpha^4}\,\alpha^{2k-3}\beta\alpha^4\,\alpha^{2k-3}\beta\alpha^4\,\alpha^{2k-5}\beta)\alpha^2).\end{aligned}$$

显然，$\mathbf{u}_n \in \mathcal{B}(8k+4, 6k, 2k)$ 满足 $add(\mathbf{u}_n) = 0$，而 $\mathbf{v}_n \in \mathcal{B}(8k+4, 6k, 2k+2)$ 满足 $add(\mathbf{v}_n) = 2$。也就是说，对于 $\mathcal{B}(8k + 4, 6k)$ 中的序列 $\mathbf{u}_n$，其循环移位序列 $\mathbf{v}_n = R^{4k+2}(\mathbf{u}_n)$ 属于 $\mathcal{B}(8k + 4, 6k)$，且 $add(\mathbf{v}_n)$ 更大。这表明下界 $c_0 = 6k + 1$ 是一个紧界，使得任意满足 $c \geq c_0$ 的序列 $\mathbf{s}_n \in \mathcal{B}(n, c)$ 都是一个序列代表元。

(iv) 当 $n = 8k$ 时，剩下的情况是 $t_1 < b < d_1 + d_2 - t_2$，即$2k - 1 < b < (m - t_1) + (m - t_1 - 1) - (t_1 + 1) < 2k + 1$，这意味着 $b = 2k$。此情形 $n = 8k$ 的证明与 $n = 8k+4$ 的证明相似。具体而言，**子情形（3.3）**可化简为“$4k = 2b = d_1+d_2+t_1-t_2$ 意味着 $d_1 = 2k+1$、$d_2 = 2k$ 和 $t_2 = 2k$，这与 $d_1 \,|\, (m+b-d_2)$ 矛盾。”因此，当 $n = 8k$ 且 $c \geq 6k-1$ 时，在 $\mathcal{B}(n, c)$ 中不存在一对满足 $add(\mathbf{s}'_n) < add(\mathbf{v}'_n)$ 的移位等价序列 $(\mathbf{s}'_n, \mathbf{v}'_n)$。

另一方面，假设某个序列具有以下形式

$$\mathbf{s}_n = (s_0, \ldots, s_{8k-1}) = ((\underline{\alpha(\alpha\beta)^{k-1}}\,\alpha(\alpha\beta)^{k-1}\,\alpha(\alpha\beta)^{k-1}\,\alpha\beta)\,\alpha(\alpha\beta)^k),$$

其中 $\beta = \bar{\alpha}$且 $(\alpha\beta)^l$ 是由 l 个 $\alpha\beta$ 重复组成的序列，即 $\alpha\beta\alpha\beta\alpha\beta\ldots\alpha\beta$。显然，$\mathbf{s}_n$ 属于 $\mathcal{B}(8k,\ 4k,\ 2k-1)$，且 $add(\mathbf{s}_n) = 2k - 2$，其中 $\mathbf{s}_d = \mathbf{s}_{2k-1}$ 带有下划线。考虑以下序列

$$\begin{aligned}\mathbf{u}_n &= R^{2k-2}(\mathbf{s}_n) = (((\underline{(\alpha\beta)^{k-1}\alpha}\,(\alpha\beta)^{k-1}\alpha\,(\alpha\beta)^{k-1}\alpha\,(\alpha\beta)^{k-1}\alpha\,\beta)\alpha\alpha\beta),\\ \mathbf{v}_n &= R^{6k-2}(\mathbf{s}_n) = (((\underline{(\alpha\beta)^{k-2}\alpha(\alpha\beta)^2}\,(\alpha\beta)^{k-2}\alpha(\alpha\beta)^2\,(\alpha\beta)^{k-2}\alpha(\alpha\beta)^2\,(\alpha\beta)^{k-3}\alpha\alpha)\beta).\end{aligned}$$

显然，$\mathbf{u}_n \in \mathcal{B}(8k,\ 6k-2,\ 2k-1)$ 满足 $add(\mathbf{u}_n) = 0$，并且 $\mathbf{v}_n \in \mathcal{B}(8k,\ 6k-2,\ 2k+1)$ 满足 $add(\mathbf{v}_n) = 2$。也就是说，对于 $\mathcal{B}(8k,\ 6k-2)$ 中的序列 $\mathbf{u}_n$，其循环

移位序列 $\mathbf{v}_n = R^{4k}(\mathbf{u}_n)$ 属于 $\mathcal{B}(8k,\ 6k-2)$，且具有更大的 $add(\mathbf{v}_n)$。这表明，下界 $c_0 = 6k-1$ 是一个紧界，使得任何满足 $c \geq c_0$ 的序列 $\mathbf{s}_n \in \mathcal{B}(n,\ c)$ 都是一个序列代表元。□