二元周期序列的 4-错线性复杂度

皮 飞[1],戚文峰[1,2]
(1.信息工程大学信息工程学院应用数学系,河南郑州 450002; 2.中国科学院信息安全国家重点实验室,北京 100190)

摘 要: k-错线性复杂度是衡量序列伪随机性的重要指标之一.对线性复杂度第一下降点为 4 的以 2 的方幂为周期的二元序列,本文通过分析 Games-Chan 算法,给出了其 4-错线性复杂度的所有可能取值形式以及具有给定 4-错线性复杂度的序列的计数.更进一步,给出了其 4-错线性复杂度的期望.结果表明,其 4-错线性复杂度的期望与线性复杂度相差不大.

关键词: 序列密码; 周期序列; 线性复杂度; k-错线性复杂度
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 12-2914-07

The 4-Error Linear Complexity of Binary Periodic Sequences

PI Fei[1], QI Wen-feng[1,2]
(1. *Department of Applied Mathematics, Information Engineering Institute, Information Engineering University, Zhengzhou, Henan* 450002, *China*;
2. *State Key Laboratory of Information Security, Chinese Academy of Sciences, Beijing* 100190, *China*)

Abstract: The k-error linear complexity is one of the important measures for assessing the pseudorandom properties of sequences. For binary sequences with period a power of 2, of which the first decreasing point of the linear complexity is 4, the possible values of the 4-error linear complexity and the number of sequences with given 4-error linear complexity are established based on the Games-Chan algorithm. Moreover, the expected value of the 4-error linear complexity is also provided. The results show that the 4-error linear complexity is close to the linear complexity.

Key words: stream cipher; periodic sequences; linear complexity; k-error linear complexity

1 引言

设 $\boldsymbol{S}=(s_0,s_1,\cdots)$是有限域 F_q 上的序列,N 为正整数,若对任意的 $i\geqslant 0$ 均有 $s_{i+N}=s_i$,则称序列 $\boldsymbol{S}$ 是 N-周期的,并记 $\boldsymbol{S}=(s_0,s_1,\cdots,s_{N-1})^\infty$.序列 $\boldsymbol{S}$ 的线性复杂度 $L(\boldsymbol{S})$是使得等式 $s_i+d_1s_{i-1}+\cdots+d_cs_{i-c}=0, i\geqslant c$ 成立的最小非负整数 c,其中 $d_1,d_2,\cdots,d_c\in F_q$.

线性复杂度是衡量序列伪随机性质的一个重要指标.但密码学意义上的强安全序列仅仅具有高的线性复杂度是不够的,我们希望在改变序列的少数比特时,其线性复杂度也不会急剧下降.这是为了避免攻击者以一条线性复杂度较低的序列来逼近密钥流序列.为此,文献[1]给出了序列 k-错线性复杂度的概念.

定义 1 设 $\boldsymbol{S}=(s_0,s_1,\cdots,s_{N-1})^\infty$是有限域 F_q 上的 N-周期序列,对任意非负整数 k,其 k-错线性复杂度 $L_{N,k}(\boldsymbol{S})$定义为

$$L_{N,k}(\boldsymbol{S})=\min_{W_N(\boldsymbol{E})\leqslant k}L(\boldsymbol{S}+\boldsymbol{E})$$

其中 $\boldsymbol{E}=(e_0,e_1,\cdots,e_{N-1})^\infty$跑遍 F_q 上所有 N-周期序列,$W_N(\boldsymbol{E})$表示序列 $\boldsymbol{E}$ 在一个 N-周期中非零元素的个数.

近年来,国内外学者对序列的 k-错线性复杂度进行了广泛的研究.设 $m(\boldsymbol{S})$为使得序列 $\boldsymbol{S}$ 的 k-错线性复杂度严格小于其线性复杂度的最小 k 值,本文中称其为线性复杂度的第一下降点.文献[2~4]研究了周期序列的 $m(\boldsymbol{S})$与其线性复杂度的关系.W.Meidl 等在文献[5]中给出了周期序列 k-错线性复杂度均值的下界,文献[6]利用离散傅里叶变换进一步研究了素数周期序列 k-错线性复杂度的均值,并给出了其更紧的下界.对 2^n-周期二元序列,文献[9]和[10]分别给出了其 1-错与 2-错线性复杂度的均值.

本文进一步研究了 2^n-周期二元序列 4-错线性复杂度的分布.对线性复杂度第一下降点 $m(\boldsymbol{S})=4$ 的序列,给出了其 4-错线性复杂度的所有可能取值形式以及具有给定 4-错线性复杂度的序列的计数.进一步,给出了其 4-错线性复杂度的期望.

收稿日期:2010-05-15;修回日期:2011-02-18
基金项目:国家自然科学基金(No.60833008,No.61070178)

2　预备知识

设 $\boldsymbol{S}=(s_0,s_1,\cdots,s_{N-1})^\infty$ 是有限域 F_q 上的 N-周期序列,定义其生成函数为 $S(x)=s_0+s_1x+\cdots$,设 $\boldsymbol{s}=(s_0,s_1,\cdots,s_{N-1})$ 是序列 $\boldsymbol{S}$ 的一个周期所对应的向量,定义其生成函数为 $s(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}$,则 $S(x)=s(x)/(1-x^N)$. 易知序列 $\boldsymbol{S}$ 的线性复杂度为(参见文献[11])

$$L(\boldsymbol{S})=N-\deg(\gcd(s(x),1-x^N)) \tag{1}$$

文献[2]给出了使得 2^n-周期二元序列 $\boldsymbol{S}$ 的 k-错线性复杂度严格小于其线性复杂度的最小 k 值,即

$$m(\boldsymbol{S})=2^{W_H(2^n-L(S))} \tag{2}$$

其中 $W_H(a)$ 表示整数 a 的二进制展开的汉明重量.

设 $\boldsymbol{s}^{(n)}=(s_0,s_1,\cdots,s_{2^n-1})$ 是 2^n-周期二元序列 $\boldsymbol{S}$ 的一个周期所对应的向量,定义序列 $\boldsymbol{S}$ 的重量为其一个周期中非零元素的个数,记为 $W(\boldsymbol{S})$,则有 $W(\boldsymbol{S})=W(\boldsymbol{s}^{(n)})$. 本文的证明充分运用了 Games-Chan(简记为 G-C)算法[12],下面介绍该算法的主要思想. 记 $f_L(\boldsymbol{a})$ 与 $f_R(\boldsymbol{a})$ 分别表示向量 $\boldsymbol{a}$ 的左右两半部分,则 $f_L(\boldsymbol{s}^{(n)})=(s_0,s_1,\cdots,s_{2^{n-1}-1})$, $f_R(\boldsymbol{s}^{(n)})=(s_{2^{n-1}},s_{2^{n-1}+1},\cdots,s_{2^n-1})$. 若 $f_L(\boldsymbol{s}^{(n)})=f_R(\boldsymbol{s}^{(n)})$,则 $L(\boldsymbol{S})=L(f_L(\boldsymbol{s}^{(n)}))$;否则 $L(\boldsymbol{S})=(2^{n-1}+L(\boldsymbol{B})$,其中 $\boldsymbol{B}$ 是以 $f_L(\boldsymbol{s}^{(n)})+f_R(\boldsymbol{s}^{(n)})$ 为一个周期的 2^{n-1}-周期序列. G-C 算法是一个递归过程,每一步将向量 $\boldsymbol{s}^{(m)}$, $1\leqslant m\leqslant n$ 分成 $f_L(\boldsymbol{s}^{(m)})$ 与 $f_R(\boldsymbol{s}^{(m)})$ 两部分,只有当 $f_L(\boldsymbol{s}^{(m)})\neq f_R(\boldsymbol{s}^{(m)})$ 时,线性复杂度才增加 2^{m-1}.

由 G-C 算法的思想,可以定义一个有限域 F_2 上的 2^n 维向量集合 $F_2^{2^n}$ 到 2^{n-1} 维向量集合 $F_2^{2^{n-1}}$ 的映射 φ_n(参见文献[9]):

$$\varphi_n((s_0,s_1,\cdots,s_{2^n-1}))=(s_0+s_{2^{n-1}},s_1+s_{2^{n-1}+1},\cdots,s_{2^{n-1}-1}+s_{2^n-1})$$

则该映射有下面三个性质:

P1: $W(\varphi_n(\boldsymbol{s}^{(n)}))\leqslant W(\boldsymbol{s}^{(n)})$;

P2: $n\geqslant 1$ 时, $W(\varphi_n(\boldsymbol{s}^{(n)}))$ 与 $W(\boldsymbol{s}^{(n)})$ 同奇偶;

P3: $\boldsymbol{s}^{(n-1)}$ 的原像集合

$$\varphi_n^{-1}(\boldsymbol{s}^{(n-1)})=\{\boldsymbol{v}\in F_2^{2^n}\mid\varphi_n(\boldsymbol{v})=\boldsymbol{s}^{(n-1)}\}$$

中的元素个数为 $2^{2^{n-1}}$.

下面我们再介绍本文要用到的几个引理.

引理 1[8]　设 $0<c\leqslant 2^n$,则线性复杂度为 c 的 2^n-周期二元序列的条数为 2^{c-1}.

引理 2[9]　设 $\boldsymbol{S}$ 是 2^n-周期二元序列,则 $L(\boldsymbol{S})=2^n$ 当且仅当 $W(\boldsymbol{S})$ 为奇数.

引理 3[10]　设 $\boldsymbol{S}$ 是线性复杂度为 2^n-2^m, $0\leqslant m\leqslant n-1$ 的 2^n-周期二元序列, $N_2(L^*_{r,c})$ 表示 $L(\boldsymbol{S})=2^n-2^m$ 且 $L_{2^n,2}(\boldsymbol{S})=L^*_{r,c}$ 的序列 S 的条数,若整数 $L^*_{r,c}$ 满足

$$L^*_{r,c}=\begin{cases}2^n-2^m-2^{r+1}+c, & 1\leqslant r\leqslant m-1, \quad 1\leqslant c\leqslant 2^r-1\\ 2^n-2^{r+1}+c, & m+1\leqslant r\leqslant n-1, \quad 1\leqslant c\leqslant 2^r-1, \quad c\neq 2^r-2^m\end{cases}$$

则有

$$N_2(L^*_{r,c})=\begin{cases}2^{2^n-2^m-2^{r+1}+r+c}, & L^*_{r,c}=2^n-2^m-2^{r+1}+c, \quad 1\leqslant r\leqslant m-1, \quad 1\leqslant c\leqslant 2^r-1\\ 2^{2^n-2^{r+1}+2r-m+c-1}, & L^*_{r,c}=2^n-2^{r+1}+c, \quad m+1\leqslant r\leqslant n-1, \quad 1\leqslant c<2^r-2^m\\ 2^{2^n-2^{r+1}+2r-m+c-2}, & L^*_{r,c}=2^n-2^{r+1}+c, \quad m+1\leqslant r\leqslant n-1, \quad 2^r-2^m<c\leqslant 2^r-1\end{cases}$$

对不等于 $L^*_{r,c}$ 的正整数 C, $N_2(C)=0$.

3　主要结论

对线性复杂度第一下降点为 4 的 2^n-周期二元序列 $\boldsymbol{S}$,由式(2)知其线性复杂度 $L(\boldsymbol{S})=2^n-2^m-2^l$, $0\leqslant l<m\leqslant n-1$. 由引理 2 知 $W(\boldsymbol{S})$ 为偶数,故改变五个比特后序列 $\boldsymbol{S}$ 的线性复杂度变为 2^n,有 $L_{2^n,5}(\boldsymbol{S})=L_{2^n,4}(\boldsymbol{S})$,故下文只讨论其 4-错线性复杂度. 下面的定理给出了其 4-错线性复杂度的可能取值形式及具有给定 4-错线性复杂度的序列的计数.

定理 1　设 $\boldsymbol{S}$ 是线性复杂度为 $2^n-2^m-2^l$, $0\leqslant l<m\leqslant n-1$ 的 2^n-周期二元序列, $N_4(L_{r,c})$ 表示 $L(\boldsymbol{S})=2^n-2^m-2^l$ 且 $L_{2^n,4}(\boldsymbol{S})=L_{r,c}$ 的序列的条数. 若 $L_{r,c}$ 满足

$$L_{r,c}=\begin{cases}2^n-2^m-2^l-2^{r+1}+c, & 1\leqslant r\leqslant l-1, \quad 1\leqslant c\leqslant 2^r-1\\ 2^n-2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, \quad 1\leqslant c\leqslant 2^r-1, \quad c\neq 2^r-2^l\\ 2^n-2^{r+1}+c, & m+1\leqslant r\leqslant n-1, \quad 1\leqslant c\leqslant 2^r, \quad c\neq 2^r-\delta_1 2^m-\delta_2 2^l, \quad \delta_1,\delta_2\in\{0,1\}\end{cases}$$

则有

$$N_4(L_{r,c})=\begin{cases}2^{2^n-2^m-2^l-2^{r+1}+r+c}, & L_{r,c}=2^n-2^m-2^l-2^{r+1}+c, & 1\leqslant r\leqslant l-1, & 1\leqslant c\leqslant 2^r-1\\ 2^{2^n-2^m-2^{r+1}+2r-l+c-1}, & L_{r,c}=2^n-2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, & 1\leqslant c<2^r-2^l\\ 2^{2^n-2^m-2^{r+1}+2r-l+c-2}, & L_{r,c}=2^n-2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, & 2^r-2^l<c\leqslant 2^r-1\\ 2^{2^n-2^{r+1}+4r-2m-l+c-3}, & L_{r,c}=2^n-2^{r+1}+c, & m+1\leqslant r\leqslant n-1, & 1\leqslant c<2^r-2^m-2^l\\ 2^{2^n-2^{r+1}+4r-2m-l+c-4}, & L_{r,c}=2^n-2^{r+1}+c, & m+1\leqslant r\leqslant n-1, & 2^r-2^m-2^l<c<2^r-2^m\\ 2^{2^n-2^{r+1}+4r-2m-l+c-5}, & L_{r,c}=2^n-2^{r+1}+c, & m+1\leqslant r\leqslant n-1, & 2^r-2^m<c<2^r-2^l\\ 2^{2^n-2^{r+1}+4r-2m-l+c-6}, & L_{r,c}=2^n-2^{r+1}+c, & m+1\leqslant r\leqslant n-1, & 2^r-2^l<c\leqslant 2^r-1\end{cases}$$

且 $N_4(0)=2^{4n-2m-l-6}$. 对于不等于 $L_{r,c}$ 的正整数 C, $N_4(C)=0$.

证明 设 $\boldsymbol{s}^{(n)}=(s_0,s_1,\cdots,s_{2^n-1})$ 是序列 $\boldsymbol{S}$ 的一个 2^n 周期所对应的向量, $\boldsymbol{s}^{(t)}=\varphi_{t+1}\cdots\varphi_n(\boldsymbol{s}^{(n)})=(s_0^{(t)},s_1^{(t)},\cdots,s_{2^t-1}^{(t)})$, $m\leqslant t\leqslant n-1$. 由 G-C 算法知序列 $\boldsymbol{S}$ 满足 $f_L(\boldsymbol{s}^{(t)})\neq f_R(\boldsymbol{s}^{(t)})$, $m+2\leqslant t\leqslant n$, $f_L(\boldsymbol{s}^{(m+1)})=f_R(\boldsymbol{s}^{(m+1)})$ 且 $L(f_L(\boldsymbol{s}^{(m+1)}))=2^m-2^l$. 设 $\boldsymbol{b}^{(m)}=f_L(\boldsymbol{s}^{(m+1)})$, 类似 $\boldsymbol{s}^{(t)}$ 定义 $\boldsymbol{b}^{(k)}$, $l\leqslant k\leqslant m-1$, 则 $f_L(\boldsymbol{b}^{(k)})\neq f_R(\boldsymbol{b}^{(k)})$, $l+2\leqslant k\leqslant m$, $f_L(\boldsymbol{b}^{(l+1)})=f_R(\boldsymbol{b}^{(l+1)})$ 且 $L(f_L(\boldsymbol{b}^{(l+1)}))=2^l$. 由 $\boldsymbol{s}^{(m)}=\boldsymbol{0}$ 及 $\boldsymbol{b}^{(l)}=\boldsymbol{0}$ 可知

$$\sum_{i=0}^{2^{n-m}-1}s_{j+i\cdot 2^m}=0,0\leqslant j\leqslant 2^m-1 \tag{3}$$

及

$$\sum_{i=0}^{2^{m-l}-1}b_{j+i\cdot 2^l}=0,0\leqslant j\leqslant 2^l-1 \tag{4}$$

由引理 2 及 φ_n 的性质 P2 知 $W(\boldsymbol{s}^{(t)})$ 为偶数且 $W(\boldsymbol{s}^{(t)})\leqslant W(\boldsymbol{s}^{(n)})$, $m\leqslant t\leqslant n$. 由 $m(\boldsymbol{S})=4$ 知 $W(\boldsymbol{s}^{(n)})\geqslant 4$ 且 $W(\boldsymbol{s}^{(m+1)}\geqslant 4$, 下面根据 $\boldsymbol{s}^{(n)}$ 与 $\boldsymbol{s}^{(m+1)}$ 的汉明重量分情形讨论.

情形 1 $W(\boldsymbol{s}^{(n)})=4$.

显然 $L_{2^n,4}(\boldsymbol{S})=0$, 且 $W(f_L(\boldsymbol{b}^{(l+1)}))=1$, $W(\boldsymbol{b}^{(m)})=W(f_L(\boldsymbol{s}^{(m+1)}))=2$. 由式(4)及 $f_L(\boldsymbol{b}^{(l+2)})\neq f_R(\boldsymbol{b}^{(l+2)})$ 知必存在某个 j, $0\leqslant j\leqslant 2^l-1$, 使得 $\boldsymbol{b}^{(m)}$ 中的两个非零元素分别属于集合 $\{b_j,b_{j+2^{l+1}},\cdots,b_{j+2^m-2^{l+1}}\}$ 和 $\{b_{j+2^l},b_{j+2^l+2^{l+1}},\cdots,b_{j+2^m-2^l}\}$. 故这样的 $\boldsymbol{b}^{(m)}$ 共有 $2^l\cdot(2^{m-l-1})^2$ 种可能. 对给定的某个 $\boldsymbol{b}^{(m)}$, 不妨设 $b_{j_1}=b_{j_2}=1$, 再由 $\boldsymbol{s}^{(m)}=\boldsymbol{0}$ 知

$$s_{j_1}^{(m+1)}=s_{j_2}^{(m+1)}=s_{j_1+2^m}^{(m+1)}=s_{j_2+2^m}^{(m+1)}=1 \tag{5}$$

则满足式(5)且 $W(\boldsymbol{s}^{(n)})=4$ 的序列 $\boldsymbol{S}$ 共有 $(2^{n-m-1})^4$ 种可能. 故

$$N_4(0)=2^l\cdot(2^{m-l-1})^2\cdot(2^{n-m-1})^4=2^{4n-2m-l-6}$$

情形 2 $W(\boldsymbol{s}^{(n)})>4$ 且 $W(\boldsymbol{s}^{(m+1)})>4$.

当 $j>m$ 时, $W(f_L(\boldsymbol{s}^{(j+1)})+f_R(\boldsymbol{s}^{(j+1)}))=W(\boldsymbol{s}^{(j)})>4$, 故 $f_L(\boldsymbol{s}^{(j+1)})$ 与 $f_R(\boldsymbol{s}^{(j+1)})$ 至少有五比特不相同, 所以改变 $\boldsymbol{s}^{(n)}$ 中四个比特后 $f_L(\boldsymbol{s}^{(j+1)})$ 与 $f_R(\boldsymbol{s}^{(j+1)})$ 也不相同, 从而

$$L_{2^n,4}(\boldsymbol{S})=2^{n-1}+2^{n-2}+\cdots+2^{m+1}+c_1$$

由 $f_L(\boldsymbol{s}^{(m+1)})=f_R(\boldsymbol{s}^{(m+1)})$ 且 $L(f_L(\boldsymbol{s}^{(m+1)}))=2^m-2^l$ 知 $c_1\leqslant 2^m-2^l$. 因为要使 $f_L(\boldsymbol{s}^{(m+1)})$ 中一比特发生改变, 需要至少改变 $\boldsymbol{s}^{(n)}$ 中的两个比特, 因此 $c_1=L_{2^m,2}(f_L(\boldsymbol{s}^{(m+1)}))$. 由引理 3 知

$$c_1=\begin{cases}2^m-2^l-2^{r+1}+c, & 1\leqslant r\leqslant l-1, & 1\leqslant c\leqslant 2^r-1\\ 2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, & 1\leqslant c\leqslant 2^r-1, \quad c\neq 2^r-2^l\end{cases}$$

故序列 $\boldsymbol{S}$ 的 4-错线性复杂度为

$$L_{r,c}=\begin{cases}2^n-2^m-2^l-2^{r+1}+c, & 1\leqslant r\leqslant l-1, & 1\leqslant c\leqslant 2^r-1\\ 2^n-2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, & 1\leqslant c\leqslant 2^r-1, \quad c\neq 2^r-2^l\end{cases}$$

由引理 3 和映射 φ_n 的性质 P3 容易计算其相应的序列条数为

$$N_4(L_{r,c})=\begin{cases}2^{2^n-2^m-2^l-2^{r+1}+r+c}, & L_{r,c}=2^n-2^m-2^l-2^{r+1}+c, & 1\leqslant r\leqslant l-1, & 1\leqslant c\leqslant 2^r-1\\ 2^{2^n-2^m-2^{r+1}+2r-l+c-1}, & L_{r,c}=2^n-2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, & 1\leqslant c<2^r-2^l\\ 2^{2^n-2^m-2^{r+1}+2r-l+c-2}, & L_{r,c}=2^n-2^m-2^{r+1}+c, & l+1\leqslant r\leqslant m-1, & 2^r-2^l<c\leqslant 2^r-1\end{cases}$$

情形 3　$W(\boldsymbol{s}^{(n)})>4$ 且 $W(\boldsymbol{s}^{(m+1)})=4$.

由 $\boldsymbol{s}^{(t)}=\varphi_{t+1}\cdots\varphi_n(\boldsymbol{s}^{(n)}),2\leqslant t\leqslant n-1$ 知,改变 $\boldsymbol{s}^{(n)}$ 中的四个比特至多会导致 $\boldsymbol{s}^{(t)}$中四个比特的改变(为叙述方便,下文直接说改变 $\boldsymbol{s}^{(t)}$中的比特).设 $\boldsymbol{a}^{(n)}$是由 $\boldsymbol{s}^{(n)}$改变四个比特后所得的向量,类似 $\boldsymbol{s}^{(t)}$定义 $\boldsymbol{a}^{(t)}$,易知 $\boldsymbol{a}^{(t)}$和 $\boldsymbol{s}^{(t)}$至多有四个比特不相同.

设 $r,m+1\leqslant r\leqslant n-1$ 是满足 $W(\boldsymbol{s}^{(r)})=4$ 的最大整数,由 $W(\boldsymbol{s}^{(m+1)})=4$ 知这样的 r 是存在的.对于任意整数 $j,r<j<n$,有 $W(f_L(\boldsymbol{s}^{(j+1)})+f_R(\boldsymbol{s}^{(j+1)}))=W(\boldsymbol{s}^{(j)})>4$,故改变四个比特后 $f_L(\boldsymbol{s}^{(j+1)})$与 $f_R(\boldsymbol{s}^{(j+1)})$也不相同.从而我们可以适当地改变 $\boldsymbol{s}^{(n)}$中的四个比特使得 $\boldsymbol{s}^{(r)}$变为 $\boldsymbol{a}^{(r)}=0$,则有

$$L_{2^n,4}(\boldsymbol{S})=2^{n-1}+2^{n-2}+\cdots+2^{r+1}+c\ ,\ 1\leqslant c\leqslant 2^r$$

由定义 1 知 c 是改变$\boldsymbol{s}^{(r+1)}$中四个比特后所得向量 $\boldsymbol{a}^{(r+1)}$的线性复杂度的最小值.不妨设 $\boldsymbol{a}^{(n)}$就是达到此最小值时 $\boldsymbol{s}^{(n)}$所变成的向量.下面我们来证明 $c\neq 2^r-\sigma_1 2^m-\sigma_2 2^l,\sigma_1,\sigma_2\in\{0,1\}$.

设 $\boldsymbol{s}^{(r)}=(0,0,\cdots,\underset{u}{\overset{\uparrow}{1}},\cdots,\underset{v}{\overset{\uparrow}{1}},\cdots,\underset{\alpha}{\overset{\uparrow}{1}},\cdots,\underset{\beta}{\overset{\uparrow}{1}},\cdots,0)$,则 $\boldsymbol{s}^{(r+1)}=(s_0^{(r+1)},s_1^{(r+1)},\cdots,s_{2^{r+1}-1}^{(r+1)})$满足

$$s_i^{(r+1)}+s_{i+2^r}^{(r+1)}=1\ ,\ i\in\{u,v,\alpha,\beta\}\qquad(6)$$

且 $s_j^{(r+1)}+s_{j+2^r}^{(r+1)}=s_j^{(r)}=0,0\leqslant j\leqslant 2^r-1,j\neq u,v,\alpha,\beta$.于是我们可以适当地改变$(s_u^{(r+1)},s_{u+2^r}^{(r+1)})$,$(s_v^{(r+1)},s_{v+2^r}^{(r+1)})$,$(s_\alpha^{(r+1)},s_{\alpha+2^r}^{(r+1)})$和$(s_\beta^{(r+1)},s_{\beta+2^r}^{(r+1)})$中各一个比特,从而使得 $\boldsymbol{s}^{(r)}$变为 $\boldsymbol{a}^{(r)}=\boldsymbol{0}$且 $W(f_L(\boldsymbol{a}^{(r+1)}))$为偶数.由引理 2 知 $c\neq 2^r$.

记 $\boldsymbol{b}'^{(r)}=f_L(\boldsymbol{a}^{(r+1)})$,类似 $\boldsymbol{s}^{(t)}$定义 $\boldsymbol{b}'^{(k)},0\leqslant k\leqslant r-1$.若 $c(L(\boldsymbol{b}'^{(r)})=2^r-2^m$,则 $f_L(\boldsymbol{b}'^{(t)})\neq f_R(\boldsymbol{b}'^{(t)})$,$m+2\leqslant t\leqslant r-1$,$f_L(\boldsymbol{b}'^{(m+1)})=f_R(\boldsymbol{b}'^{(m+1)})$且 $L(f_L(\boldsymbol{b}'^{(m+1)}))=2^m$.因为 $\boldsymbol{s}^{(m)}=\boldsymbol{0}$且 $f_L(\boldsymbol{s}^{(m+2)})\neq f_R(\boldsymbol{s}^{(m+2)})$,我们不妨设 $\alpha\equiv u+2^m \bmod (2^{m+1})$,$\beta\equiv v+2^m \bmod (2^{m+1})$,即 $\alpha=u+w_1 2^m,\beta=v+w_2 2^m$,其中 w_1,w_2 均为奇数.故可设 $b'^{(m+1)}_{u \bmod 2^{m+1}}$,$b'^{(m+1)}_{v \bmod 2^{m+1}}$属于 $f_L(\boldsymbol{b}'^{(m+1)})$,$b'^{(m+1)}_{\alpha \bmod 2^{m+1}}$,$b'^{(m+1)}_{\beta \bmod 2^{m+1}}$属于 $f_R(\boldsymbol{b}'^{(m+1)})$.由于 $\boldsymbol{b}'^{(r)}$是由 $f_L(\boldsymbol{s}^{(r+1)})$适当改变位置 u,v,α,β 所得,并对应地改变 $f_R(\boldsymbol{s}^{(r+1)})$使得 $\boldsymbol{s}^{(r)}$变为 $\boldsymbol{a}^{(r)}=\boldsymbol{0}$,于是可以适当改变 $b'^{(m+1)}_{u \bmod 2^{m+1}}$,$b'^{(m+1)}_{v \bmod 2^{m+1}}$,$b'^{(m+1)}_{\alpha \bmod 2^{m+1}}$ 和 $b'^{(m+1)}_{\beta \bmod 2^{m+1}}$,从而使得 $f_L(\boldsymbol{b}'^{(m+1)})=f_R(\boldsymbol{b}'^{(m+1)})$且 $W(f_L(\boldsymbol{b}'^{(m+1)}))$为偶数,由引理 2 知 $L(f_L(\boldsymbol{b}'^{(m+1)}))<2^m$,这与 $L(f_L(\boldsymbol{b}'^{(m+1)}))=2^m$ 矛盾.

设 $\boldsymbol{b}^{(m)}=(0,0,\cdots,\underset{u'}{\overset{\uparrow}{1}},\cdots,\underset{v'}{\overset{\uparrow}{1}},\cdots,0)$,其中 $u'=u \pmod{2^m}$,$v'=v \pmod{2^m}$.若 $c(L(\boldsymbol{b}'^{(r)})=2^r-2^l$,则 $f_L(\boldsymbol{b}'^{(t)})\neq f_R(\boldsymbol{b}'^{(t)})$,$l+2\leqslant t\leqslant r-1$,$f_L(\boldsymbol{b}'^{(l+1)})=f_R(\boldsymbol{b}'^{(l+1)})$且 $L(f_L(\boldsymbol{b}'^{(l+1)}))=2^l$.由 $\boldsymbol{b}^{(l)}=\boldsymbol{0}$及 $\boldsymbol{b}^{(l+1)}\neq\boldsymbol{0}$知 $v'\equiv u'+2^l \pmod{2^{l+1}}$,故 $b'^{(l+1)}_{u' \bmod 2^{l+1}}$和 $b'^{(l+1)}_{v' \bmod 2^{l+1}}$分别属于 $f_L(\boldsymbol{b}'^{(l+1)})$和 $f_R(\boldsymbol{b}'^{(l+1)})$,与上面的分析类似,可适当改变 $b'^{(l+1)}_{u' \bmod 2^{l+1}}$和 $b'^{(l+1)}_{v' \bmod 2^{l+1}}$ 使得 $f_L(\boldsymbol{b}'^{(l+1)})=f_R(\boldsymbol{b}'^{(l+1)})$且 $W(f_L(\boldsymbol{b}'^{(l+1)}))$为偶数,由引理 2 知 $L(f_L(\boldsymbol{b}'^{(l+1)}))<2^l$,矛盾.

同理可以证明 $c\neq 2^r-2^m-2^l$.下面讨论 $L(\boldsymbol{S})=2^n-2^m-2^l$,$L_{2^n,4}(\boldsymbol{S})$为上述情况时序列 $\boldsymbol{S}$ 的条数.

由 $L(f_L(\boldsymbol{a}^{(r+1)}))=c$ 及式(1)可知 $f_L(\boldsymbol{a}^{(r+1)})$所对应的生成函数为

$$\begin{aligned}A(x)&=a_0^{(r+1)}+a_1^{(r+1)}x+\cdots+a_{2^r-1}^{(r+1)}x^{2^r-1}\\&=(1+x)^{2^r-c}a(x)\end{aligned}$$

其中 $a(1)\neq 0$.由 $v'\equiv u'+2^l \pmod{2^{l+1}}$知 $v'=u'+w_3 2^l$,其中 w_3 为奇数,于是有 $v=u+w_4 2^l$,其中 w_4 为奇数.则

$$\begin{aligned}&A(x)+x^u+x^v+x^\alpha+x^\beta\\&=(1+x)^{2r-c}a(x)+x^u(1+x^{w_1})^{2^m}+x^{u+w_4 2^l}(1+x^{w_2})^{2^m}\\&=(1+x)^{2r-c}a(x)+x^u(1+x^{w_2})^{2^m}(1+x^{w_4})^{2^l}\\&\quad+x^u x^{w_2 2^m}(x^{(w_1-w_2)2^m}-1)\end{aligned}$$

由 w_1,w_2,w_4 均为奇数知$(1+x)^{2^m+2^l}\parallel(1+x^{w_2})^{2^m}(1+x^{w_4})^{2^l}$,$(1+x)^{2^{m+1}}\parallel(x^{(w_1-w_2)2^m}-1)$,其中$(1+x)^n\parallel a(x)$表示$(1+x)^n\mid a(x)$但$(1+x)^{n+1}\nmid a(x)$.因为 $2^{m+1}>2^m+2^l$,则

$$A(x)=(1+x)^{2r-c}a(x)+(1+x)^{2^m+2^l}a_1(x)$$

其中 $a(1)\neq 0,a_1(1)\neq 0$.

由引理 1 知满足 $L(f_L(\boldsymbol{a}^{(r+1)}))=c$ 且$f_L(\boldsymbol{a}^{(r+1)})=f_R(\boldsymbol{a}^{(r+1)})$的向量 $\boldsymbol{a}^{(r+1)}$有 2^{c-1}种取法,下面对 c 的取值分情况讨论.

(1)当 $c<2^r-2^m-2^l$ 时,$(1+x)^{2^m+2^l}\parallel A(x)+x^u+x^v+x^\alpha+x^\beta$,则不存在两个具有相同线性复杂度 c 且仅在位置 u,v,α,β 不同的 2^r 维向量.从而对给定的 $\boldsymbol{s}^{(r)}$和 c,满足改变后的 $\boldsymbol{s}^{(r+1)}$线性复杂度为 c 且 $\boldsymbol{s}^{(r)}=\varphi_{r+1}(\boldsymbol{s}^{(r+1)})$的情况共有 $2^4\cdot 2^{c-1}$种.与情形 1 的讨论类似,$\boldsymbol{s}^{(r)}$共有 $2^{4r-2m-l-6}$种可能.递归运用 φ_n 的性质 P3 知此种情况下序列 $\boldsymbol{S}$ 的条数为

$$\begin{aligned}K&=2^{2^{n-1}}\cdot 2^{2^{n-2}}\cdots 2^{2^{r+1}}\cdot 2^{4r-2m-l-6}\cdot 2^{c-1}\cdot 2^4\\&=2^{2^n-2^{r+1}+4r-2m-l+c-3}\end{aligned}$$

(2)当 $2^r-2^m-2^l<c$ 时,$(1+x)^{2^r-c}\parallel A(x)+x^u+x^v+x^\alpha+x^\beta$,即存在两个具有相同线性复杂度且仅在位置 u,v,α,β 不同的 2^r 维向量.

①当 $2^r-2^m-2^l<c<2^r-2^m$ 时,$2^r-c>2^m$,与(1)

中讨论类似可知不存在仅在 u,v,α,β 中任意两个位置不同而具有相同线性复杂度的 2^r 维向量.即对给定的 c,若 $L(f_L(\boldsymbol{a}^{(r+1)}))=c$,则 $L(f_L(\boldsymbol{a}^{(r+1)})+\boldsymbol{e})=c$,其中 $\boldsymbol{e}$ 为仅在 u,v,α,β 四个位置为 1,其余位置为 0 的 2^r 维向量.且对给定的 $\boldsymbol{s}^{(r)}$,由 $f_L(\boldsymbol{a}^{(r+1)})$ 与 $f_L(\boldsymbol{a}^{(r+1)})+\boldsymbol{e}$ 所确定的 $\boldsymbol{s}^{(r+1)}$ 是相同的.从而对给定的 $\boldsymbol{s}^{(r)}$ 和 c,满足改变后的 $\boldsymbol{s}^{(r+1)}$ 线性复杂度为 c 且 $\boldsymbol{s}^{(r)}=\varphi_{r+1}(\boldsymbol{s}^{(r+1)})$ 的情况共有 $2^3\cdot 2^{c-1}$ 种.则此种情况下序列 $\boldsymbol{S}$ 的条数为

$$K/2=2^{2^n-2^{r+1}+4r-2m-l+c-4}$$

②当 $2^r-2^m<c<2^r-2^l$ 时,$2^l<2^r-c<2^m$,存在两个具有相同线性复杂度且仅在位置 u,α 或 v,β 不同的 2^r 维向量.即对给定的 c,若 $L(f_L(\boldsymbol{a}^{(r+1)}))=c$,则 $L(f_L(\boldsymbol{a}^{(r+1)})+\boldsymbol{e})=c$,其中 $\boldsymbol{e}$ 为仅在 u,v,α,β 四个位置为 1 或仅在位置 u,α 为 1 或仅在位置 v,β 为 1,而在其余位置为 0 的 2^r 维向量.且对给定的 $\boldsymbol{s}^{(r)}$,由 $f_L(\boldsymbol{a}^{(r+1)})$ 与 $f_L(\boldsymbol{a}^{(r+1)})+\boldsymbol{e}$ 所确定的 $\boldsymbol{s}^{(r+1)}$ 是相同的.从而对给定的 $\boldsymbol{s}^{(r)}$ 和 c,满足条件的 $\boldsymbol{s}^{(r+1)}$ 共有 $2^2\cdot 2^{c-1}$ 种取法.则此种情况下序列 $\boldsymbol{S}$ 的条数为

$$K/4=2^{2^n-2^{r+1}+4r-2m-l+c-5}$$

③当 $2^r-2^l<c<2^r$ 时,$2^r-c<2^l$,存在两个具有相同线性复杂度且仅在 u,v,α,β 中偶数个位置不同的 2^r 维向量.即对给定的 c,若 $L(f_L(\boldsymbol{a}^{(r+1)}))=c$,则 $L(f_L(\boldsymbol{a}^{(r+1)})+\boldsymbol{e})=c$,其中 $\boldsymbol{e}$ 为在 u,v,α,β 中偶数个位置为 1,其余位置为 0 的 2^r 维向量.且对给定的 $\boldsymbol{s}^{(r)}$,由 $f_L(\boldsymbol{a}^{(r+1)})$ 与 $f_L(\boldsymbol{a}^{(r+1)})+\boldsymbol{e}$ 所确定的 $\boldsymbol{s}^{(r+1)}$ 是相同的.从而对给定的 $\boldsymbol{s}^{(r)}$ 和 c,满足条件的 $\boldsymbol{s}^{(r+1)}$ 共有 $2\cdot 2^{c-1}$ 种取法.则此种情况下序列 $\boldsymbol{S}$ 的条数为

$$K/8=2^{2^n-2^{r+1}+4r-2m-l+c-6}$$

这样我们就完全证明了定理 1. 证毕

由定理 1 我们可以计算线性复杂度为 $2^n-2^m-2^l$ 的 2^n-周期二元序列 4-错线性复杂度的均值.

定理 2 设 $E_{4|L=2^n-2^m-2^l}$ 表示线性复杂度为 $2^n-2^m-2^l$,$0\leqslant l<m\leqslant n-1$ 的 2^n-周期二元序列 4-错线性复杂度的均值,则

$$E_{4|L=2^n-2^m-2^l}=\begin{cases}2^n-2^m-2^l-3+2^{-2^n+4n+2^m-2m+2^l-l-5}-\sum\limits_{r=1}^{l-1}2^{-2^r+r+1}-(2^{2^l-1}+1)\cdot\sum\limits_{r=l+1}^{m-1}2^{-2^r+2r-l}\\ \qquad -(2^{2^m+2^l-3}+2^{2^m-2}+2^{2^l-1}+1)\sum\limits_{r=m+1}^{n-1}2^{-2^r+4r-2m-l-2}, & l>0\\ 2^n-2^m-3+2^{-2^n+4n+2^m-2m-4}-\sum\limits_{r=1}^{m-1}2^{-2^r+2r+1}-(2^{2^m-1}+2)\sum\limits_{r=m+1}^{n-1}2^{-2^r+4r-2m-2}, & l=0\end{cases}$$

证明 由引理 1 知线性复杂度为 $2^n-2^m-2^l$ 的序列有 $2^{2^n-2^m-2^l-1}$ 条.当 $l>0$ 时,由定理 1 有

$$E_{4|L=2^n-2^m-2^l}=2^{-2^n+2^m+2^l+1}\sum_{r=1}^{n-1}\sum_{c=1}^{2^r-1}N_4(L_{r,c})\cdot L_{r,c}=\sum_{i=1}^{7}E_i$$

其中

$$\begin{aligned}E_1&=2^{-2^n+2^m+2^l+1}\sum_{r=1}^{l-1}\sum_{c=1}^{2^r-1}2^{2^n-2^m-2^l-2^{r+1}+r+c}\cdot(2^n-2^m-2^l-2^{r+1}+c)\\&=2[\sum_{r=1}^{l-1}(2^n-2^m-2^l)\cdot 2^{-2^{r+1}+r}\sum_{c=1}^{2^r-1}2^c-\sum_{r=1}^{l-1}2^{-2^{r+1}+2r+1}\sum_{c=1}^{2^r-1}2^c+\sum_{r=1}^{l-1}2^{-2^{r+1}+r}\sum_{c=1}^{2^r-1}c2^c]\\&=2[(2^n-2^m-2^l)(2^{-1}-2^{-2^l+l})-\sum_{r=1}^{l-1}2^{-2^r+2r}+2^{-2^l+2l}-1+\sum_{r=1}^{l-1}2^{-2^r+2r}-\sum_{r=1}^{l-1}2^{-2^r+r}-2^{-1}+2^{-2^l+l}]\\&=2^n-2^m-2^l-2^{-2^l+l+n+1}+2^{-2^l+l+m+1}+2^{-2^l+l+1}+2^{-2^l+2l+2}-3-\sum_{r=1}^{l-1}2^{-2^r+r+1}\end{aligned}$$

$$\begin{aligned}E_2+E_3&=2^{-2^n+2^m+2^l+1}\sum_{r=l+1}^{m-1}\sum_{c=1}^{2^r-2^l-1}2^{2^n-2^m-2^{r+1}+2r-l+c-1}\cdot(2^n-2^m-2^{r+1}+c)\\&\quad+2^{-2^n+2^m+2^l+1}\sum_{r=l+1}^{m-1}\sum_{c=2^r-2^l+1}^{2^r-1}2^{2^n-2^m-2^{r+1}+2r-l+c-2}\cdot(2^n-2^m-2^{r+1}+c)\\&=2^{2^l-l}\sum_{r=l+1}^{m-1}[\sum_{c=1}^{2^r-2^l-1}2^{-2^{r+1}+2r+c}(2^n-2^m-2^{r+1}+c)+\sum_{c=2^r-2^l+1}^{2^r-1}2^{-2^{r+1}+2r+c-1}(2^n-2^m-2^{r+1}+c)]\\&=2^{2^l-l}\sum_{r=l+1}^{m-1}[2^{n-2^{r+1}+2r}(\sum_{c=1}^{2^r-2^l-1}2^c+\sum_{c=2^r-2^l+1}^{2^r-1}2^{c-1})-2^{m-2^{r+1}+2r}(\sum_{c=1}^{2^r-2^l-1}2^c+\sum_{c=2^r-2^l+1}^{2^r-1}2^{c-1})\\&\quad-2^{-2^{r+1}+3r+1}(\sum_{c=1}^{2^r-2^l-1}2^c+\sum_{c=2^r-2^l+1}^{2^r-1}2^{c-1})+2^{-2^{r+1}+2r}(\sum_{c=1}^{2^r-2^l-1}c\cdot 2^c+\sum_{c=2^r-2^l+1}^{2^r-1}c\cdot 2^{c-1})]\end{aligned}$$

$$
\begin{aligned}
&= 2^{2^l-l}\Big[2^n\sum_{r=l+1}^{m-1}2^{-2^{r+1}+2r}(2^{2^r}-1-2)-2^m\sum_{r=l+1}^{m-1}2^{-2^{r+1}+2r}(2^{2^r}-1-2)\\
&\quad-\sum_{r=l+1}^{m-1}2^{-2^{r+1}+3r+1}(2^{2^r}-1-2)+\sum_{r=l+1}^{m-1}2^{-2^{r+1}+2r}(2^{2^r+r-1}-2^{2^r}-2^{2^r-2^l}+2)\Big]\\
&= 2^{-2^l+l+n+1}-2^{n-2^m+2m+2^l-l-1}-2^{-2^l+l+m+1}+2^{-2^m+3m+2^l-l}-2^{-2^l+2l+2}\\
&\quad+2^{-2^m+2m+2^l-l-1}-2^{-2^l+l+1}-\sum_{r=l+1}^{m-1}2^{-2^r+2r-l}-\sum_{r=l+1}^{m-1}2^{-2^r+2r+2^l-l-1}\\
\sum_{i=4}^{7}E_i &= 2^{-2^n+2^m+2^l+1}\sum_{r=m+1}^{n-1}\sum_{c=1}^{2^r-2^m-2^l-1}2^{2^n-2^{r+1}+4r-2m-l+c-3}\cdot(2^n-2^{r+1}+c)\\
&\quad+2^{-2^n+2^m+2^l+1}\sum_{r=m+1}^{n-1}\sum_{c=2^r-2^m-2^l+1}^{2^r-2^m-1}2^{2^n-2^{r+1}+4r-2m-l+c-4}\cdot(2^n-2^{r+1}+c)\\
&\quad+2^{-2^n+2^m+2^l+1}\sum_{r=m+1}^{n-1}\sum_{c=2^r-2^m+1}^{2^r-2^l-1}2^{2^n-2^{r+1}+4r-2m-l+c-5}\cdot(2^n-2^{r+1}+c)\\
&\quad+2^{-2^n+2^m+2^l+1}\sum_{r=m+1}^{n-1}\sum_{c=2^r-2^l+1}^{2^r-1}2^{2^n-2^{r+1}+4r-2m-l+c-6}\cdot(2^n-2^{r+1}+c)\\
&= 2^{2^m-2m+2^l-l+1}\sum_{r=m+1}^{n-1}\Big[\sum_{c=1}^{2^r-2^m-2^l-1}(2^n-2^{r+1}+c)2^{-2^{r+1}+4r+c-3}+\sum_{c=2^r-2^m-2^l+1}^{2^r-2^m-1}(2^n-2^{r+1}+c)2^{-2^{r+1}+4r+c-4}\\
&\quad+\sum_{c=2^r-2^m+1}^{2^r-2^l-1}(2^n-2^{r+1}+c)2^{-2^{r+1}+4r+c-5}+\sum_{c=2^r-2^l+1}^{2^r-1}(2^n-2^{r+1}+c)2^{-2^{r+1}+4r+c-6}\Big]\\
&= 2^{2^m-2m+2^l-l+1}\Big[\sum_{r=m+1}^{n-1}2^{n-2^{r+1}+4r}(2^{2^r-6}-2^{-2})-\sum_{r=m+1}^{n-1}2^{-2^{r+1}+5r}(2^{2^r-5}-2^{-1})\\
&\quad+\sum_{r=m+1}^{n-1}2^{-2^{r+1}+4r}(2^{-2}-2^{2^r-2^m-2^l-3}-2^{2^r-2^m-4}-2^{2^r-2^l-5}+2^{2^r+r-6}-2^{2^r-5})\Big]\\
&= 2^{-2^m+2m+2^l-l+n-1}-2^{-2^m+3m+2^l-l}-\sum_{r=m+1}^{n-1}2^{-2^r+4r-2m-l-2}-\sum_{r=m+1}^{n-1}2^{-2^r+4r-2m+2^l-l-3}\\
&\quad-\sum_{r=m+1}^{n-1}2^{-2^r+4r+2^m-2m-l-4}-\sum_{r=m+1}^{n-1}2^{-2^r+4r+2^m-2m+2^l-l-5}+2^{-2^n+4n+2^m-2m+2^l-l-5}-2^{-2^m+2m+2^l-l-1}
\end{aligned}
$$

综上可得

$$
\begin{aligned}
&E_{4|L=2^n-2^m-2^l}=\\
&2^n-2^m-2^l-3+2^{-2^n+4n+2^m-2m+2^l-l-5}\\
&-\sum_{r=1}^{l-1}2^{-2^r+r+1}-(2^{2^l-1}+1)\sum_{r=l+1}^{m-1}2^{-2^r+2r-l}\\
&-(2^{2^m+2^l-3}+2^{2^m-2}+2^{2^l-1}+1)\sum_{r=m+1}^{n-1}2^{-2^r+4r-2m-l-2}
\end{aligned}
$$

注意到计算 E_1 时用到的和式 $-2\sum_{r=1}^{l-1}2^{-2^{r+1}+2r+1}\sum_{c=1}^{2^r-1}2^c$,当 $l>0$ 时有

$$
-2\sum_{r=1}^{l-1}2^{-2^{r+1}+2r+1}\sum_{c=1}^{2^r-1}2^c=-\sum_{r=1}^{l-1}2^{-2^r+2r+1}+2^{-2^l+2l+1}-2
$$

而当 $l=0$ 时,上式左边等于 0,右边等于 -1.故计算时将 $l>0$ 与 $l=0$ 分别考虑,利用同样的方法可以算得当 $l=0$ 时,

$$
\begin{aligned}
&E_{4|L=2^n-2^m-2^l}=2^n-2^m-3+2^{-2^n+4n+2^m-2m-4}\\
&-\sum_{r=1}^{m-1}2^{-2^r+2r+1}-(2^{2^m-1}+2)\sum_{r=m+1}^{n-1}2^{-2^r+4r-2m-2}
\end{aligned}
$$

证毕

另外要说明的是:当 $l=0$, $m\geqslant 3$ 时, $E_{4|L=2^n-2^m-2^l}$ 中和式 $\sum_{r=3}^{m-1}2^{-2^r+2r+1}+(2^{2^m-1}+2)\sum_{r=m+1}^{n-1}2^{-2^r+4r-2m-2}$ 的值接近 0.508.当 $l\geqslant 3$ 时, $E_{4|L=2^n-2^m-2^l}$ 中和式

$$
\begin{aligned}
&\sum_{r=3}^{l-1}2^{-2^r+r+1}+(2^{2^l-1}+1)\sum_{r=l+1}^{m-1}2^{-2^r+2r-l}\\
&+(2^{2^m+2^l-3}+2^{2^m-2}+2^{2^l-1}+1)\sum_{r=m+1}^{n-1}2^{-2^r+4r-2m-l-2}
\end{aligned}
$$

的值接近 0.063.这些和式的值相对于 $E_{4|LC=2^n-2^m-2^l}$ 来说都是较小的.

4　结束语

本文充分运用 G-C 算法,对线性复杂度形为 $2^n-2^m-2^l$, $0\leqslant l<m\leqslant n-1$ 的 2^n-周期二元序列 $\boldsymbol{S}$,研究了其 4-错线性复杂度的所有可能取值及具有给定 4-错线性复杂度的序列的计数,进一步给出了其 4-错线性复杂度的期望.结果表明,其 4-错线性复杂度的期望与其线性复杂度相差不大,即从整体上来看,改变序列 $\boldsymbol{S}$ 至多四个比特不会引起其线性复杂度急剧地下降.本文

的研究结果对此类序列能否作为序列密码体制的源序列具有一定的指导意义.

参考文献

[1] Stamp M, Martin C F. An algorithm for the *k*-error linear complexity of binary sequences with period 2^n[J]. IEEE Trans Inform Theory, 1993, 39(4): 1398 – 1401.

[2] Kurosawa K, Sato F, et al. A relationship between linear complexity and *k*-error linear complexity[J]. IEEE Trans Inform Theory, 2000, 46(2): 694 – 698.

[3] Meidl W. How many bits have to be changed to decrease the linear complexity? [J]. Design Codes and Cryptography, 2004, 33(2): 109 – 122.

[4] Niu Z H, Xiao G Z. Analysis of the linear complexity and its stability for $2p^n$ – periodic binary sequences[J]. IEICE Trans Fundamentals, 2005, E88-A(9): 2412 – 2418.

[5] Meidl W, Niederreiter H. On the expected value of the linear complexity and the *k*-error linear complexity of periodic sequences[J]. IEEE Trans Inform Theory, 2002, 48(11): 2817 – 2825.

[6] Meidl W, Niederreiter H. Linear complexity, *k*-error linear complexity, and the discrete fourier transform[J]. Journal of Complexity, 2002, 18(1): 87 – 103.

[7] 魏仕民. 确定周期序列 k 错线性复杂度的一个快速算法[J]. 电子学报, 2004, 32(5): 705 – 708.
WEI Shi-min. An efficient algorithm for determining the *k*-Error linear complexity of periodic sequences[J]. Acta Electronica Sinica, 2004, 32(5): 705 – 708. (in Chinese)

[8] Rueppel R A. Analysis and Design of Stream Ciphers[M]. Berlin: Springer-Verlag, 1986.

[9] Meidl W. On the stability of 2^n – periodic binary sequences [J]. IEEE Trans Inform Theory, 2005, 51(5): 1151 – 1155.

[10] Zhu F X, Qi W F. The 2-error linear complexity of 2^n – periodic binary sequences[J]. Chinese Journal of Electronics, 2008, 17(2): 356 – 360.

[11] Ding C, Xiao G, Shan W. The Stability Theory of Stream Ciphers[M]. Berlin: Springer-Verlag, 1991. 85 – 88.

[12] Games R A, Chan A H. A fast algorithm for determining the complexity of a binary sequence with period 2^n[J]. IEEE Trans Inform Theory, 1983, 29(1): 144 – 146.

[13] 赵耀东, 戚文峰. 二元周期序列的 k 错误线性复杂度[J]. 电子学报, 2005, 33(1): 12 – 16.
ZHAO Yao-dong, QI Wen-feng. On the *k*-error linear complexity of binary periodic sequences[J]. Acta Electronica Sinica, 2005, 33(1): 12 – 16. (in Chinese)

[14] Etzion T, Kalouptsidis N, et al. Properties of the error linear complexity spectrum[J]. IEEE Trans Inform Theory, 2009, 55(10): 4681 – 4686.

作者简介

皮 飞 男, 1986 年生于湖南常德, 硕士生, 研究方向为密码学.
E-mail: hcnui@163.com

戚文峰 男, 1963 年生于浙江宁波, 教授, 博士生导师, 研究领域包括密码学与信息安全.
E-mail: wenfeng.qi@263.net