第 36 卷 第 3 期 应 用 数 学 学 报 Vol. 36 No. 3
2013 年 5 月 ACTA MATHEMATICAE APPLICATAE SINICA May, 2013

具有 2^n 线性复杂度的 2^n 周期二元序列的 3 错线性复杂度 *

周建钦

(杭州电子科技大学通信工程学院，杭州 310018)

(安徽工业大学计算机学院，马鞍山 243002)

(E-mail: zhou9@yahoo.com)

摘　要　线性复杂度和 k 错线性复杂度是度量密钥流序列的密码强度的重要指标. 通过研究周期为 2^n 的二元序列线性复杂度，提出将 k 错线性复杂度的计算转化为求 Hamming 重量最小的错误序列. 基于 Games-Chan 算法，讨论了线性复杂度为 2^n 的 2^n 周期二元序列的 3 错线性复杂度分布情况；给出了对应 k 错线性复杂度序列的完整计数公式， k=3,4. 对于一般的线性复杂度为 2^n-m 的 2^n 周期二元序列，也可以使用该方法给出对应 k 错线性复杂度序列的计数公式.

关键词　周期序列；线性复杂度； k 错线性复杂度； k 错线性复杂度分布

MR(2000) 主题分类　94A55; 94A60; 11B50

中图分类　TN911; TN918.1

1　引言

线性复杂度是衡量密钥流序列随机性的一个重要指标，但高线性复杂度并不一定能保证序列是安全的. 有些序列的线性复杂度极不稳定，如果改变这些序列一个周期段中一个或几个元素，其线性复杂度发生很大的变化，则该序列仍然是密码学意义上的弱序列. 我国学者 Ding, Xiao 和 Shan[1] 最早注意到这个问题，因而率先创立了流密码的稳定性理论，并提出了重量复杂度，球体复杂度等流密码稳定性度量指标. 随后国外学者 Stamp 和 Martin[2] 也引入了类似 '球体复杂度' 的线性复杂度稳定性度量指标： k 错线性复杂度. 设 s 是周期为 N 的 q 元序列，当改变 s 的一个周期中至多 k $(0 \le k \le N)$ 位后，得到的所有序列的线性复杂度中最小的线性复杂度，称为 s 的 k 错线性复杂度，

本文 2011 年 5 月 13 日收到. 2011 年 9 月 7 日收到修改稿.

* 浙江省自然科学基金 (Y1100318), 安徽省自然科学基金 (1208085MF106) 资助项目.

记为 $L_k(s)$. Kurosawa 等 [3] 给出 2^n 周期二元序列 s 的 k 错线性复杂度严格小于线性复杂度 $L(s)$ 的最小值为: $k_{\min}=2^{W_H(2^n-L(s))}$, 其中 $W_H(b)$ 表示整数 b 在二进制表示下的 Hamming 重量.

Rueppel[4] 给出线性复杂度为 L 的 2^n 周期二元序列的具体个数. 当 $k=1,2$ 时, Meidl[5] 给出线性复杂度为 2^n 的 2^n 周期二元序列的 k 错线性复杂度分布情况. 当 $k=2,3$ 时, 朱凤翔和戚文峰 [6] 给出线性复杂度为 2^n-1 的 2^n 周期二元序列的 k 错线性复杂度分布情况. Fu, Niederreiter 和 Su[7] 给出所有 2^n 周期二元序列的 1 错线性复杂度分布情况. 本文通过研究周期为 2^n 的二元序列线性复杂度, 提出将 k 错线性复杂度的计算转化为求 Hamming 重量最小的错误序列. 基于 Games-Chan 算法, 讨论了线性复杂度为 2^n 的 2^n 周期二元序列的 3 错线性复杂度分布情况. 给出了对应 3,4 错线性复杂度序列的完整计数公式. 对于一般的线性复杂度为 2^n-m 的 2^n 周期二元序列, 也可以使用该方法给出对应 k 错线性复杂度序列的计数公式.

2 预备知识和引理

下文中所讨论的序列都是在 $GF(q)$ 域上. 设 $GF(q)$ 域上的两个向量 $x=(x_1,x_2,\cdots,x_n)$ 和 $y=(y_1,y_2,\cdots,y_n)$, 则定义 $x+y=(x_1+y_1,x_2+y_2,\cdots,x_n+y_n)$. 对于 $n=2m$, $\mathrm{Left}\,(x)$ 定义为 $(x_1,x_2,\cdots,x_m)$, 而 $\mathrm{Right}\,(x)$ 定义为 $(x_{m+1},x_{m+2},\cdots,x_n)$.

序列 $s=\{s_0,s_1,s_2,s_3,\cdots\}$ 的生成函数定义为

$$s(x)=s_0+s_1x+s_2x^2+s_3x^3+\cdots=\sum_{i=0}^{\infty}s_ix^i$$

有限序列 $s^N=\{s_0,s_1,s_2,\cdots,s_{N-1}\}$ 的生成函数定义为 $s^N(x)=s_0+s_1x+s_2x^2+\cdots+s_{N-1}x^{N-1}$. 如果 s 是周期序列, s^N 是它的第一周期, 则 $s(x)$ 可以表示成

$$\begin{aligned}s(x)=&s^N(x)(1+x^N+x^{2N}+\cdots)=\frac{s^N(x)}{1-x^N}\\=&\frac{s^N(x)/\gcd(s^N(x),1-x^N)}{(1-x^N)/\gcd(s^N(x),1-x^N)}=\frac{g(x)}{f_s(x)}.\end{aligned}$$

这里 $f_s(x)=(1-x^N)/\gcd(s^N(x),1-x^N)$, $g(x)=s^N(x)/\gcd(s^N(x),1-x^N)$.

显然, $\gcd(g(x),f_s(x))=1$, $\deg(g(x)<\deg(f_s(x)))$. $f_s(x)$ 是 s 的极小多项式, 且 $f_s(x)$ 的次数是序列 s 的线性复杂度, 记为 $L(s)$.

设 $N=2^n$, 则 $1-x^N=1-x^{2^n}=(1-x)^{2^n}=(1-x)^N$. 因而对于周期为 2^n 的二元序列, 求其线性复杂度, 可以转换为求 $s^N(x)$ 中因式 $(1-x)$ 的次数.

下面是两个众所周知的引理, 可以参见 [6].

引理 2.1 设周期为 $N=2^n$ 的二元序列 s, 其线性复杂度 $L(s)=2^n$, 当且仅当该序列的一个周期的 Hamming 重量为奇数.

因为 Hamming 重量为奇数的序列去掉一个 1 即变为 Hamming 重量为偶数的序列, 故下面主要考虑 Hamming 重量为偶数的序列.

引理 2.2 设周期为 $N=2^n$ 的二元序列 S_1 和 S_2. 如果 $L(s_1)\neq L(s_2)$, 则 $L(s_1+s_2)=\max\{L(s_1),L(s_2)\}$. 如果 $L(s_1)=L(s_2)$, 则 $L(s_1+s_2)<L(s_1)$.

如果最少改变二元序列 s 的 k 个元素，序列 s 的线性复杂度即可下降，根据引理 2.2, 则这 k 个位置为 1 的二元序列其线性复杂度也必为 $L(s)$. 因而 k 错线性复杂度的计算可以转化为求 Hamming 重量最小的二元序列，使得其线性复杂度也为 $L(s)$.

引理 2.3 设 E_i 是周期为 $N=2^n$ 的二元序列, 它的第一周期序列只在第 i 位置元素是 1, 其他位置元素全为 0, $0\leq i\leq N$. 若 $j-i=2^r(1+2a)$, $a\geq 0$, $0\leq i<j<2^n$, $r\geq 0$, 则 $L(E_i+E_j)=2^n-2^r$.

证　设 E_i+E_j 对应的多项式 $x^i+x^j=x^i(1+x^{j-i})=x^i(1-x^{j-i})=x^i(1-x^{2^r+2a2^r})$, 其中 a 为非负整数. 因为

$$1-x^{2^r+2a2^r}=(1-x^{2^r})(1+x^{2^r}+x^{2\cdot 2^r}+\cdots+x^{2a\cdot 2^r})=(1-x^{2^r})f(x)$$

且 $f(1)=1$, 所以 $\gcd((1-x)^{2^n},x^i(1-x^{j-i}))=\gcd((1-x)^{2^n},1-x^{2^r})=\gcd((1-x)^{2^n},(1-x)^{2^r})=(1-x)^{2^r}$, 即 $L(E_i+E_j)=2^n-2^r$. 证毕.

现在考虑只有 4 个位置非零周期 $N=2^n$ 的二元序列.

引理 2.4 设 s 为周期 $N=2^n$ 的二元序列，非零元素个数为 4, 则 s 可以分解为 2 个 E_{ij} 之和. 设第 1 个 E_{ij} 其非零元素位置为 $i,j,j-i=2^d(1+2u)$, 且第 2 个 E_{ij} 其非零元素位置为 k,l, $l-k=2^e(1+2v)$, 且 $i<k$, $k-i=2c+1$. 若 $d=e$, 则其线性复杂度为 $2^n-(2^d+1)$, 否则为 $2^n-2^{\min(d,e)}$.

证　若 $d\neq e$, 根据引理 2.2, $L(s)=2^n-2^{\min(d,e)}$.

若 $d=e$, E_i+E_j 对应的多项式为

$$x^i+x^j=x^i(1-x^{j-i})=x^i(1-x^{2^d(1+2u)})=x^i(1-x^{2^d})(1+x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d}).$$

E_k+E_l 对应的多项式为

$$x^k+x^l=x^k(1-x^{l-k})=x^k(1-x^{2^d(1+2v)})=x^k(1-x^{2^d})(1+x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d}).$$

$E_i+E_j+E_k+E_l$ 对应的多项式为

$$\begin{aligned}x^i+x^j+x^k+x^l=&x^i(1-x^{2^d})[(1+x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d})\\&+x^{k-i}(1+x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d})]\\=&x^i(1-x^{2^d})[1+x^{k-i}+(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d})\\&+x^{k-i}(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d})]\\=&x^i(1-x)^{2^d}[1+x^{2c+1}+(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2u\cdot 2^d})\\&+x^{k-i}(x^{2^d}+x^{2\cdot 2^d}+\cdots+x^{2v\cdot 2^d})]\\=&x^i(1-x)^{2^d+1}[(1+x+x^2+\cdots+x^{2c})\\&+(x^{2^d}+x^{3\cdot 2^d}+\cdots+x^{(2u-1)\cdot 2^d})(1+x)^{2^d-1}\\&+x^{k-i}(x^{2^d}+x^{3\cdot 2^d}+\cdots+x^{(2v-1)\cdot 2^d})(1+x)^{2^d-1}].\end{aligned}$$

由于 $(1+x+x^2+\cdots+x^{2c})$ 没有因式 $(1+x)$, 故 $\gcd((1-x)^{2^n},x^i+x^j+x^k+x^l)=(1-x)^{2^d+1}$, 所以 $L(s)=2^n-(2^d+1)$. 证毕.

3 线性复杂度为 2^n 二元序列的 3 错线性复杂度

定义 3.1[5] 设 $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 是二元序列 s 的第一周期, $n\geq 1$. 根据 Games-Chan 算法，定义映射 φ_n 从 $F_2^{2^n}$ 到 $F_2^{2^{n-1}}$,

$$\varphi_n(s^{(n)})=\varphi_n((s_0,s_1,s_2,\cdots,s_{2^n-1}))=(s_0+s_{2^{n-1}},s_1+s_{2^{n-1}+1},\cdots,s_{2^{n-1}-1}+s_{2^n-1}).$$

引理 3.1[5] 定义 3.1 的映射 φ_n 满足下面的性质,

1) $W(\varphi_n(s^{(n)}))\leq W(s^{(n)})$;

2) $W(\varphi_n(s^{(n)})),W(s^{(n)})$ 奇偶性相同;

3) 集合 $\varphi_{n+1}^{-1}(s^{(n)})=\left\{v\in F_2^{2^{n+1}}|\varphi_{n+1}(v)=s^{(n)}\right\}$ 的大小为 2^{2^n}.

引理 3.2[4] 设 $N(L)$ 表示周期为 2^n, 线性复杂度为 L 的二元序列个数，则

$$N(L)=\begin{cases}1, & L=0,\\ 2^{L-1}, & 1\leq L\leq 2^n.\end{cases}$$

引理 3.3 设 $s^{(n)},t^{(n)}$ 是 2 个不同的序列但线性复杂度均为 c, $1\leq c\leq 2^{n-1}-1$, $u^{(n)}$, $v^{(n)}$ 是 2 个不同的序列但线性复杂度均为 2^n, 且 $W(u^{(n)})=W(v^{(n)})=1$, 则 $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 不同.

证 欲证明 $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 不同，即证明 $s^{(n)}+u^{(n)}+v^{(n)}$ 与 $t^{(n)}$ 不同，即证明 $u^{(n)}+v^{(n)}$ 与 $s^{(n)}+t^{(n)}$ 不同. 因为 $s^{(n)},t^{(n)}$ 是 2 个不同的序列但线性复杂度均为 $c,1\leq c\leq 2^{n-1}-1$, 所以 $s^{(n)}+t^{(n)}$ 的线性复杂度小于 $2^{n-1}-1$, 且前 2^{n-1} 个元素与后 2^{n-1} 个元素相同.

假设 $u^{(n)}+v^{(n)}$ 与 $s^{(n)}+t^{(n)}$ 相同，则 $u^{(n)}+v^{(n)}$ 前 2^{n-1} 个元素与后 2^{n-1} 个元素相同，所以前 2^{n-1} 个元素中只有一个元素 1, 故 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-1}, 与 $s^{(n)}+t^{(n)}$ 的线性复杂度小于 $2^{n-1}-1$ 矛盾. 证毕.

引理 3.4 设序列 $s^{(n)}$ 线性复杂度为 c, $1\leq c\leq 2^{n-1}-1$, 序列 $u^{(n)}$ 线性复杂度为 2^n, 且 $u^{(n)}$ 中元素 1 的个数为 1, 则 $s^{(n)}+u^{(n)}$ 的 1 错线性复杂度为 c.

证 求 1 错线性复杂度，即叠加一个元素 1 的个数为 1 的序列，然后求最小的线性复杂度. 设 $v^{(n)}$ 是与 $u^{(n)}$ 不同的序列但线性复杂度为 2^n, 且 $v^{(n)}$ 中元素 1 的个数为 1.

根据引理 2.3, $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^n-2^d, $d\geq 0$ 为整数. 即 $u^{(n)}+v^{(n)}$ 的线性复杂度最小为 $2^n-2^{n-1}=2^{n-1}$, $s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度最小为 2^{n-1}. 由于 $s^{(n)}+u^{(n)}+u^{(n)}$ 的线性复杂度为 c, $1\leq c\leq 2^{n-1}-1$, 故 $s^{(n)}+u^{(n)}$ 的 1 错线性复杂度为 c. 证毕.

下面的定理 3.1 是 [5] 中的定理 1. 本文给出新的证明方法.

定理 3.1 设 $L(r,c)=2^n-2^r+c$, $2\leq r\leq n$, $1\leq c\leq 2^{r-1}-1$, $N_1(L(r,c))$ 表示周

期为 2^n, 线性复杂度 $L(s)=2^n$, 1 错线性复杂度为 $L(r,c)$ 的二元序列个数，则

$$N_1(L)=\begin{cases}2^n, & L=0,\\ 2^{L+r-1}, & L=L(r,c),\\ 0, & \text{其他}.\end{cases}$$

证 设 s 是线性复杂度 $L(s)=2^n$ 的二元序列， $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 是序列 s 的第一周期. 根据 Games-Chan 算法， $\mathrm{Left}\,(s^{(t)})\neq \mathrm{Right}(s^{(t)}),1\le t\le n,L(s^{(0)})=1$, 其中 $s^{(t)}=\varphi_{t+1}\cdots\varphi_n(s^{(n)})$.

所以 $s^{(0)}=\{1\}$, 且 $s_0+s_1+\cdots+s_{2^t-1}=1,L(s^{(t)})=2^t,1\le t\le n$.

先考虑简单情形 $W(s^{(n)})=1$, 即 $s^{(n)}$ 中元素 1 的个数为 1. $\{s_0,s_1,\cdots,s_{2^n-1}\}$ 中只有一个元素 1, 所以这样 $s^{(n)}$ 的个数为 2^n, 即 $N_1(0)=2^n$.

考虑一般情况 $L(r,c)=2^n-2^r+c,\ 2\le r\le n,\ 1\le c\le 2^{r-1}-1$.

设 s 是线性复杂度 $L(s)=L(r,c)$ 的二元序列， $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 是序列 s 的第一周期. 因为 $L(r,c)=2^n-2^r+c=2^{n-1}+\cdots+2^r+c$, 所以 $\mathrm{Left}\,(s^{(r)})=\mathrm{Right}(s^{(r)})$, 且 $L(s^{(r)})=c$.

因为线性复杂度为 2^r 且 $W(t^{(r)})=1$ 的 $t^{(r)}$ 个数为 2^r, 根据引理 3.4, $s^{(r)}+t^{(r)}$ 的 1 错线性复杂度为 c.

根据引理 3.2 和引理 3.3, $s^{(r)}+t^{(r)}$ 的个数为 $2^{c-1}\times 2^r=2^{c+r-1}$. 根据引理 3.1, 生成每个 $s^{(r)}+t^{(r)}$ 的 $s^{(n)}+t^{(n)}$ 的个数 $2^{2^{n-1}+\cdots+2^r}=2^{2^n-2^r}$.

存在序列 $t^{(n)}$ 使得 $t^{(r)}=\varphi_{r+1}\cdots\varphi_n(t^{(n)}),\ L(t^{(n)})=2^n$ 且 $W(t^{(n)})=1$, 故 $s^{(n)}+t^{(n)}$ 的 1 错线性复杂度为 $2^{n-1}+\cdots+2^r+L_1(s^{(r)}+t^{(r)})=2^n-2^r+c=L(r,c)$.

所以 $N_1(L(r,c))=2^{2^n-2^r}\times 2^{c+r-1}=2^{L(r,c)+r-1}$

当 $L(r,c)$ 由小到大变化时，$N_1(L(r,c))$ 分别为 $r=n,\ 2^n,2^{n+1},\cdots,2^{2^{n-1}-1+n-1};\ r=n-1,\ 2^{2^{n-1}+1+(n-1)-1},2^{2^{n-1}+2+(n-1)-1},\cdots,2^{2^{n-1}+2^{n-2}-1+n-1};\cdots,r=2,\ 2^{2^n-2^2+1+2-1}$.

由于 $N_1(0)=2^n$, 再累加以上值, 得 1 错线性复杂度为 0 或 $L(r,c)$ 的二元序列个数为 2^{2^n-1}. 根据引理 3.2, 所有 $L(s)=2^n$ 的二元序列的个数为 2^{2^n-1}, 故不存在这样的序列, $L(s)=2^n$, 1 错线性复杂度不为 0 且不为 $L(r,c)=2^n-2^r+c,2\le r\le n,\ 1\le c\le 2^{r-1}-1$. 证毕.

引理 3.5 设 $s^{(n)},t^{(n)}$ 是 2 个不同的序列但线性复杂度均为 $c,\ 1\le c\le 2^{n-2},\ u^{(n)},v^{(n)}$ 是 2 个不同的序列但线性复杂度均为 2^n, 且 $u^{(n)},v^{(n)}$ 的非零元素个数分别为 1 或 3, 则 $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 不同.

证 欲证明 $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 不同，即证明 $s^{(n)}+u^{(n)}+v^{(n)}$ 与 $t^{(n)}$ 不同，即证明 $u^{(n)}+v^{(n)}$ 与 $s^{(n)}+t^{(n)}$ 不同.

因为 $s^{(n)},t^{(n)}$ 是 2 个不同的序列但线性复杂度均为 $c,\ 1\le c\le 2^{n-2}$, 所以 $s^{(n)}+t^{(n)}$ 的线性复杂度小于 2^{n-2}, 且 $s^{(n)}+t^{(n)}$ 的 2^n 个元素可以分成 4 个相同部分.

假设 $u^{(n)}+v^{(n)}$ 与 $s^{(n)}+t^{(n)}$ 相同，则 $u^{(n)}+v^{(n)}$ 的 2^n 个元素可以分成 4 个相同部分，故 $u^{(n)}+v^{(n)}$ 的非零元素个数只能为 4, $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-2}, 与 $s^{(n)}+t^{(n)}$ 的线性复杂度小于 2^{n-2} 矛盾. 证毕.

引理 3.6 设序列 $s^{(n)}$ 线性复杂度为 c, $1 \le c \le 2^{n-1}-3$, $c \ne 2^{n-1}-2^m$, $2 \le m < n-1$, 序列 $u^{(n)}$ 线性复杂度为 2^n, 且 $u^{(n)}$ 中元素 1 的个数为 1 或 3, 则 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度为 c. 设序列 $s^{(n)}$ 线性复杂度为 $c, c=2^{n-1}-2^m, 0 \le m < n-1$, 则存在 $u^{(n)}$, 使得 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度小于 c.

证 求 3 错线性复杂度，即叠加一个元素 1 的个数为 1 或 3 的序列，然后求最小的线性复杂度. 设 $v^{(n)}$ 是与 $u^{(n)}$ 不同的序列但线性复杂度为 2^n, 且 $v^{(n)}$ 中元素 1 的个数为 1 或 3.

若 $u^{(n)}+v^{(n)}$ 的线性复杂度最小为 2^{n-1}, 则 $s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度最小为 2^{n-1}. 由于 $s^{(n)}+u^{(n)}+u^{(n)}$ 的线性复杂度为 c, $1 \le c \le 2^{n-1}-1$, 故 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度为 c.

若 $u^{(n)}+v^{(n)}$ 的线性复杂度小于 2^{n-1}, 则 $u^{(n)}+v^{(n)}$ 前 2^{n-1} 个元素与后 2^{n-1} 个元素相同，且前 2^{n-1} 个元素中元素 1 的个数为 2. 根据引理 2.3, $u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^m$, $0 \le m < n-1$. 所以， $L(s^{(n)}+u^{(n)}+v^{(n)}) \ge L(s^{(n)})$. 故 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度为 c.

设序列 $s^{(n)}$ 线性复杂度为 c, $c=2^{n-1}-2^m$, $0 \le m < n-1$, 则当 $u^{(n)}+v^{(n)}$ 的线性复杂度也为 c 时， $L(s^{(n)}+u^{(n)}+v^{(n)}) < c$, 即 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度小于 c. 证毕.

引理 3.7 设 $N_3(2^{n-2})$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 2^{n-2} 的二元序列 s 个数，则

$$N_3(2^{n-2}) = \left\{ \binom{2^n}{3} - \left[2^n + 2^{n-2}\binom{4}{2}(2^n-4) \right] \right\} 2^{2^{n-2}-1}.$$

证 设序列 $s^{(n)}$ 线性复杂度为 2^{n-2}, 则 $s^{(n)}$ 的个数为 $2^{2^{n-2}-1}$.

设序列 $u^{(n)}$ 线性复杂度 2^n 且 $W(u^{(n)})=1$, 易知存在序列 $v^{(n)}$ 且 $W(v^{(n)})=3$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-2}. 即 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中至少两个非零元素距离为 2^{n-2} 的倍数，易知恰好存在一个序列 $v^{(n)}$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-2}. 即 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 则 $u^{(n)}$ 的个数为 $\binom{2^n}{3}$.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中恰好两个非零元素距离为 2^{n-2} 的倍数，则 $u^{(n)}$ 的个数为 $2^{n-2}\binom{4}{2}(2^n-4)$.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中任意两个非零元素距离均为 2^{n-2} 的倍数，则 $u^{(n)}$ 的个数为 $2^{n-2}\binom{4}{3}=2^n$.

设序列 $s^{(n)}$ 线性复杂度为 2^{n-2}, 序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中不存在两个非零元素距离为 2^{n-2} 的倍数，类似于引理 3.6, 可知 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度为 2^{n-2}. 这样 $s^{(n)}+u^{(n)}$ 的个数为

$$\left\{ \binom{2^n}{3} - \left[2^n + 2^{n-2}\binom{4}{2}(2^n-4) \right] \right\} 2^{2^{n-2}-1}.$$

证毕.

例如，当 $n=3$ 时，

$$\binom{2^n}{3}-\left[2^n+2^{n-2}\binom{4}{2}(2^n-4)\right]=0,$$

即线性复杂度 $L(s)=2^3$, 3 错线性复杂度为 2 的二元序列 s 个数为 0.

当 $n=4$ 时，

$$\left\{\binom{2^n}{3}-\left[2^n+2^{n-2}\binom{4}{2}(2^n-4)\right]\right\}2^{2^{n-2}-1}=2048,$$

即线性复杂度 $L(s)=2^4$, 3 错线性复杂度为 4 的二元序列 s 个数为 2048.

引理 3.8 设 $N_3(2^{n-1}-2^{n-m}+x)$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 $2^{n-1}-2^{n-m}+x$ 的二元序列 s 个数， $n>3,\ 1<m<n-1,\ 0<x<2^{n-m-1}$, 则

$$\begin{aligned}&N_3(2^{n-1}-2^{n-m}+x)\\=&\left\{\binom{2^n}{3}-(2^{m-2}-1)\times 2^{n+1}-(2^{m-1}-1)\times\binom{2^{n-m}}{2}\times 2^{m+1}\right.\\&-3\times 2^{n-m-2}\left[\binom{2^m}{3}-4\binom{2^{m-1}}{2}\right]\\&\left.-\binom{2^{n-m}}{2}\times\left[\binom{2^m}{2}-2^{m-1}\right]\times 2^m\right\}2^{2^{n-1}-2^{n-m}+x-1}.\end{aligned}$$

证 设序列 $s^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-m}+x$, 则 $s^{(n)}$ 的个数为 $2^{2^{n-1}-2^{n-m}+x-1}$.

设序列 $s^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-m}+x$, 序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$ 或 3, 由引理 3.6, 可知 $s^{(n)}+u^{(n)}$ 的 3 错线性复杂度为 $2^{n-1}-2^{n-m}+x$. 序列 $u^{(n)}$ 的个数为 $\binom{2^n}{3}+2^n$.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$, 则恰好有 1 个 $v^{(n)}$ 使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-2}$, 恰好有 2 个不同 $v^{(n)}$ 使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-3}$,$\cdots$, 恰好有 2^{m-2} 个不同 $v^{(n)}$ 使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-m}$. 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-m}+x$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$, 此时， $s^{(n)}+u^{(n)}=t^{(n)}+v^{(n)}$. 因而不需要考虑这样 2^n 个 $u^{(n)}$ ，其中 $W(u^{(n)})=1$. 同时我们知道存在 $2^{m-1}-1$ 个不同的 $v^{(n)}$ 和 $t^{(n)}$ 使得 $s^{(n)}+u^{(n)}=t^{(n)}+v^{(n)}$.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中两个非零元素距离为 $2^{n-r}(1+2a)$, $1<r\le m$, $a\ge 0$, 易知存在一个序列 $v^{(n)}$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-r}$, $1<r\le m$. 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-m}+x$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$, 此时， $s^{(n)}+u^{(n)}=t^{(n)}+v^{(n)}$.

将 $u^{(n)}$ 分成 2^{n-m} 个子序列, 子序列中元素的距离为 2^{n-m}. 若 3 个非零元素均属于一个子序列，且 $u^{(n)}$ 中两个非零元素距离为 2^{n-1}, 则存在 $2^{m-1}-2$ 个不同的序列 $v^{(n)}$,

$W(v^{(n)})=3$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度分别为 $2^{n-1}-2^{n-r}, 1<r\le m$. 这样 $u^{(n)}$ 的个数为 $2^{n-m}\times 2\times\binom{2^{m-1}}{2}\times 2=C1$.

若 3 个非零元素均属于一个子序列，且不存在 $u^{(n)}$ 中两个非零元素距离为 2^{n-1}, 则存在非零元素个数为 3 的 3 个序列 $v_1^{(n)}, v_2^{(n)}, v_3^{(n)}$, 使得 $u^{(n)}+v_1^{(n)}, u^{(n)}+v_2^{(n)}, u^{(n)}+v_3^{(n)}$ 互不相同，线性复杂度为 $2^{n-1}-2^{n-r}$, $1<r\le m$. 这样 $u^{(n)}$ 的个数为

$$2^{n-m}\left[\binom{2^m}{3}-2\times\binom{2^{m-1}}{2}\times 2\right]=C2.$$

若只有 2 个非零元素属于一个子序列，且 $u^{(n)}$ 中两个非零元素距离为 2^{n-1}. 则存在 $2^{m-1}-1$ 个不同的序列 $v^{(n)}$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度分别为 $2^{n-1}-2^{n-r}$, $1<r\le m$. 这样 $u^{(n)}$ 的个数为

$$2\binom{2^{n-m}}{2}\times 2^{m-1}\times 2^m=\binom{2^{n-m}}{2}\times 2^{2m}=C3.$$

若只有 2 个非零元素属于一个子序列，且不存在 $u^{(n)}$ 中两个非零元素距离为 2^{n-1}, 则恰好有一个 $v^{(n)}$ 使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-r}$, $1<r\le m$, 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-m}+x$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$, 此时, $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 相同. 这样 $u^{(n)}$ 的个数为

$$2\binom{2^{n-m}}{2}\times\left[\binom{2^m}{2}-2^{m-1}\right]\times 2^m=C4.$$

故 3 错线性复杂度为 $2^{n-1}-2^{n-m}+x$ 的二元序列 s 的个数为

$$\begin{aligned}
&N_3(2^{n-1}-2^{n-m}+x)\\
=&\left[\binom{2^n}{3}-\frac{2^{m-1}-2}{2^{m-1}-1}\times C1-\frac{2^{m-1}-1}{2^{m-1}}\times C3-\frac{3}{4}\times C2-\frac{1}{2}\times C4\right]2^{2^{n-1}-2^{n-m}+x-1}\\
=&\left\{\binom{2^n}{3}-\frac{2^{m-1}-2}{2^{m-1}-1}\times 2^{n-m+2}\binom{2^{m-1}}{2}-\frac{2^{m-1}-1}{2^{m-1}}\times\binom{2^{n-m}}{2}\times 2^{2m}\right.\\
&-\frac{3}{4}\times 2^{n-m}\left[\binom{2^m}{3}-4\binom{2^{m-1}}{2}\right]-\binom{2^{n-m}}{2}\\
&\left.\times\left[\binom{2^m}{2}-2^{m-1}\right]\times 2^m\right\}2^{2^{n-1}-2^{n-m}+x-1}\\
=&\left\{\binom{2^n}{3}-(2^{m-2}-1)\times 2^{n+1}-(2^{m-1}-1)\times\binom{2^{n-m}}{2}\times 2^{m+1}\right.\\
&-3\times 2^{n-m-2}\left[\binom{2^m}{3}-4\binom{2^{m-1}}{2}\right]-\binom{2^{n-m}}{2}\\
&\left.\times\left[\binom{2^m}{2}-2^{m-1}\right]\times 2^m\right\}2^{2^{n-1}-2^{n-m}+x-1}.
\end{aligned}$$

证毕.

推论 3.1 设 $N_3(2^{n-2}+1)$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 $2^{n-2}+1$ 的二元序列 s 个数， $n>3$, 则

$$N_3(2^{n-2}+1)=\left[\binom{2^n}{3}-2^{n-3}\binom{4}{2})(2^n-4)\right]2^{2^{n-2}}.$$

证 容易验证这是 $m=2$ 时引理 3.8 的特例．下面再直接证明这个推论，以便有助于引理 3.8 的理解.

设序列 $s^{(n)}$ 线性复杂度为 $2^{n-2}+1$, 则 $s^{(n)}$ 的个数为 $2^{2^{n-2}}$.

设序列 $s^{(n)}$ 线性复杂度为 $2^{n-2}+1$, 序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$ 或 3, 由引理 3.6, 可知 $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度为 $2^{n-2}+1$. 序列 $u^{(n)}$ 的个数为 $\binom{2^n}{3}+2^n$.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$, 则恰好有一个 $v^{(n)}$ 使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-2}, 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-2}+1$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$, 此时， $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 相同， $s^{(n)}+v^{(n)}$ 与 $t^{(n)}+u^{(n)}$ 相同.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中至少两个非零元素距离为 2^{n-2} 的倍数，易知恰好存在一个序列 $v^{(n)}$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-2}. 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-2}+1$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$, 此时， $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 相同， $s^{(n)}+v^{(n)}$ 与 $t^{(n)}+u^{(n)}$ 相同．由引理 3.7, 序列 $u^{(n)}$ 的个数为 $2^n+2^{n-2}\binom{4}{2}(2^n-4)$. 所以

$$\begin{aligned}N_3(2^{n-2}+1)&=\left\{\binom{2^n}{3}+2^n-\left[2^n+2^n+2^{n-2}\binom{4}{2}(2^n-4)\right]\Big/2\right\}2^{2^{n-2}}\\&=\left[\binom{2^n}{3}-2^{n-3}\binom{4}{2}(2^n-4)\right]2^{2^{n-2}}.\end{aligned}$$

证毕.

引理 3.9 设 $N_3(2^{n-2}+2^{n-3})$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 $2^{n-2}+2^{n-3}$ 的二元序列 s 个数， $n>3$, 则

$$N_3(2^{n-2}+2^{n-3})=\left[\binom{2^n}{3}-7\times 2^n-384\binom{2^{n-3}}{2}\right]2^{2^{n-2}+2^{n-3}-1}.$$

证 设序列 $s^{(n)}$ 线性复杂度为 $2^{n-2}+2^{n-3}$, 则 $s^{(n)}$ 的个数为 $2^{2^{n-2}+2^{n-3}-1}$.

由于 $2^{n-2}+2^{n-3}=2^{n-1}-(2^{n-2}-2^{n-3})=2^{n-1}-2^{n-3}$, 根据引理 3.6, 存在序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$ 或 3, $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度小于 $2^{n-1}-2^{n-3}$.

显然，对于所有序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$, $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度小于 $2^{n-1}-2^{n-3}$.

考虑线性复杂度为 2^n 的 $u^{(n)}$, $W(u^{(n)})=3$. 设 $u^{(n)}$ 中至少两个非零元素距离为 $2^{n-3}(2k+1)$ 或 2^{n-1}, k 为整数，易知存在一个序列 $v^{(n)}$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-3}$, 即 $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度小于 $2^{n-1}-2^{n-3}$.

将 $u^{(n)}$ 分成 2^{n-3} 个子序列，子序列中元素的距离为 2^{n-3}. 若 3 个非零元素均属于一个子序列，则 $u^{(n)}$ 中至少两个非零元素距离为 $2^{n-3}(2k+1)$ 或 2^{n-1}. 在子序列中，距

离均不为奇数的可能情况： 10101 或 1010001, 此时均存在距离 (在子序列中) 为 4 的情况.

若只有 2 个非零元素属于一个子序列，且不满足子序列中两个非零元素距离为 $2^{n-3}(2k+1)$ 或 2^{n-1}, 则子序列中两个非零元素距离为 2^{n-2} 或 $3\times 2^{n-2}$, 这样 $u^{(n)}$ 的个数为

$$2\binom{2^{n-3}}{2}\times(6+2)\times 8=128\binom{2^{n-3}}{2}.$$

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 且 $u^{(n)}$ 中至少两个非零元素距离为 2^{n-2} 或 $3\times 2^{n-2}$, 易知恰好存在一个序列 $v^{(n)}$, $W(v^{(n)})=3$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-2}. 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-3}$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$, 此时， $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 相同， $s^{(n)}+v^{(n)}$ 与 $t^{(n)}+u^{(n)}$ 相同.

设序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=3$, 则至少两个非零元素距离为 $2^{n-3}\times k$ 的个数为

$$2^{n-3}\binom{8}{3}+2\binom{2^{n-3}}{2}\binom{8}{2}8.$$

因而 3 错线性复杂度为 $2^{n-1}-2^{n-3}$ 的二元序列 s 的个数为

$$\begin{aligned}&N_3(2^{n-2}+2^{n-3})\\&=\left[\binom{2^n}{3}-2^{n-3}\binom{8}{3}-2\binom{2^{n-3}}{2}\binom{8}{2}8+64\binom{2^{n-3}}{2}\right]2^{2^{n-2}+2^{n-3}-1}\\&=\left[\binom{2^n}{3}-7\times 2^n-384\binom{2^{n-3}}{2}\right]2^{2^{n-2}+2^{n-3}-1}.\end{aligned}$$

证毕.

引理 3.10 设 $N_3(2^{n-1}-2^{n-m})$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 $2^{n-1}-2^{n-m}$ 的二元序列 s 个数， $n>3$, $1<m\le n$, 则

$$\begin{aligned}&N_3(2^{n-1}-2^{n-m})\\&=\left[\binom{2^n}{3}-2^{n-m}\binom{2^m}{2}-\binom{2^{n-m}}{2}\binom{2^m}{2}2^{m+1}+\binom{2^{n-m}}{2}\times 2^{2m}(2^{m-2}-1)\right.\\&\quad\left.+2^{n-m-1}\times\binom{2^{m-1}}{3}-2^{n-2}\times(2^{m-2}-1)\right]2^{2^{n-1}-2^{n-m}-1}.\end{aligned}$$

证 设序列 $s^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-m}$, 则 $s^{(n)}$ 的个数为 $2^{2^{n-1}-2^{n-m}-1}$.

根据引理 3.6, 存在序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$ 或 3, $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度小于 $2^{n-1}-2^{n-m}$. 显然，对于所有序列 $u^{(n)}$ 线性复杂度 2^n, $W(u^{(n)})=1$, $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度小于 $2^{n-1}-2^{n-m}$.

考虑线性复杂度为 2^n 的 $u^{(n)}$, $W(u^{(n)})=3$. 设 $u^{(n)}$ 中至少两个非零元素距离为 $2^{n-m}(2k+1)$ 或 2^{n-1}, k 为整数，易知存在一个序列 $v^{(n)}$, 使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-m}$. 即 $u^{(n)}+s^{(n)}$ 的 3 错线性复杂度小于 $2^{n-1}-2^{n-m}$.

将 $u^{(n)}$ 分成 2^{n-m} 个子序列，子序列中元素的距离为 2^{n-m}.

若只有 2 个非零元素属于一个子序列，这样 $u^{(n)}$ 的个数为 $2\binom{2^{n-m}}{2}\times\binom{2^m}{2}\times 2^m=C1$.

若只有 2 个非零元素属于一个子序列，且 $u^{(n)}$ 中两个非零元素距离不是 $2^{n-m}(2k+1)$，这样 $u^{(n)}$ 的个数为 $2\binom{2^{n-m}}{2}\times 2\times\binom{2^{m-1}}{2}\times 2^m$，其中距离为 2^{n-1} 的个数：$2\binom{2^{n-m}}{2}\times 2^{m-1}\times 2^m$.

因而，若只有 2 个非零元素属于一个子序列， $u^{(n)}$ 中不存在两个非零元素距离为 $2^{n-m}(2k+1)$ 或 2^{n-1} (子序列中距离为 2^{m-1})，这样 $u^{(n)}$ 的个数为

$$
\begin{aligned}
&2\binom{2^{n-m}}{2}\times 2\times\binom{2^{m-1}}{2}\times 2^m-2\binom{2^{n-m}}{2}\times 2^{m-1}\times 2^m\\
=&\binom{2^{n-m}}{2}\times 2^{2m}\times(2^{m-1}-2)=C2.
\end{aligned}
$$

对每个序列 $u^{(n)}$ 线性复杂度 2^n， $W(u^{(n)})=3$，且 $u^{(n)}$ 中两个非零元素距离为 $2^{n-m+1}\times k$，k 为整数，易知存在一个序列 $v^{(n)}$， $W(v^{(n)})=3$，使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-2^{n-2},2^{n-1}-2^{n-3},\cdots$，或 $2^{n-1}-2^{n-m+1}$. 故 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-1}-2^{n-m}$. 所以 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$，此时， $s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 相同， $s^{(n)}+v^{(n)}$ 与 $t^{(n)}+u^{(n)}$ 相同.

若 3 个非零元素均属于一个子序列，这样 $u^{(n)}$ 的个数为 $2^{n-m}\times\binom{2^m}{3}=C3$.

若 3 个非零元素均属于一个子序列，且 $u^{(n)}$ 中不存在两个非零元素距离为 $2^{n-m}(2k+1)$，这样 $u^{(n)}$ 的个数为 $2^{n-m+1}\times\binom{2^{m-1}}{3}$，其中存在两个非零元素距离为 2^{n-1} (子序列中距离为 2^{m-1}) 的个数： $2^{n-m+1}\times 2^{m-2}\times(2^{m-1}-2)=2^n\times(2^{m-2}-1)$.

因而，若 3 个非零元素均属于一个子序列， $u^{(n)}$ 中不存在两个非零元素距离为 $2^{n-m}(2k+1)$ 或 2^{n-1} (子序列中距离为 2^{m-1})，这样 $u^{(n)}$ 的个数为 $2^{n-m+1}\times\binom{2^{m-1}}{3}-2^n\times(2^{m-2}-1)=C4$.

对每个序列 $u^{(n)}$ 线性复杂度 2^n，$W(u^{(n)})=3$，任意两个非零元素距离为 $2^{n-m+1}\times k$，k 为整数，且不存在两个非零元素距离为 2^{n-1}，则存在线性复杂度 2^n，非零元素个数为 3 的 3 个序列 $v_1^{(n)},v_2^{(n)},v_3^{(n)}$，使得 $u^{(n)}+v_1^{(n)},u^{(n)}+v_2^{(n)},u^{(n)}+v_3^{(n)}$ 互不相同，线性复杂度为 $2^{n-1}-2^{n-2},\cdots$ 或 $2^{n-1}-2^{n-m+1}$.

因而 3 错线性复杂度为 $2^{n-1}-2^{n-m}$ 的二元序列 s 的个数为

$$
\begin{aligned}
&N_3(2^{n-1}-2^{n-m})\\
=&\left[\binom{2^n}{3}-C3-C1+C2/2+C4/4\right]2^{2^{n-1}-2^{n-m}-1}\\
=&\left[\binom{2^n}{3}-2^{n-m}\binom{2^m}{3}-\binom{2^{n-m}}{2}\binom{2^m}{2}2^{m+1}+\binom{2^{n-m}}{2}\times 2^{2m}(2^{m-2}-1)\right.\\
&\left.+2^{n-m-1}\times\binom{2^{m-1}}{3}-2^{n-2}\times(2^{m-2}-1)\right]2^{2^{n-1}-2^{n-m}-1}.
\end{aligned}
$$

证毕.

容易验证引理 3.7 是 $m=2$ 时引理 3.10 的特例；引理 3.9 是 $m=3$ 时引理 3.10 的特例.

若 $m=4$, 易得

$$N_3(2^{n-1}-2^{n-4})=\left[\binom{2^n}{3}-34\times 2^n-3072\binom{2^{n-4}}{2}\right]2^{2^{n-1}-2^{n-4}-1}.$$

证毕.

引理 3.11 设 $n>2,\ L(r,c)=2^n-2^r+c,\ 3\le r\le n,\ 1\le c\le 2^{r-2}-1,\ N_3(L(r,c))$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 $L(r,c)$ 的二元序列个数，则

$$N_3(L)=\begin{cases}\dbinom{2^n}{3}+2^n, & L=0,\\ 2^{L-1}\dbinom{2^r}{3}+2^r, & L=L(r,c).\end{cases}$$

证 设 s 是线性复杂度 $L(s)=2^n$ 的二元序列， $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$, 是序列 s 的第一周期. 根据 Games-Chan 算法， Left $(s^{(t)})\neq \mathrm{Right}(s^{(t)}),\ 1\le t\le n,\ L(s^{(0)})=1$, 其中 $s^{(t)}=\varphi_{t+1}\cdots\varphi_n(s^{(n)})$.

所以 $s^{(0)}=\{1\}$, 且 $s_0+s_1+\cdots+s_{2^t-1}=1,\ L(s^{(t)})=2^t,\ 1\le t\le n$.

先考虑简单情形 $W(s^{(n)})=1$, 即 $s^{(n)}$ 中元素 1 的个数为 1. $\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 中只有一个元素 1, 所以这样 $s^{(n)}$ 的个数为 2^n.

考虑情形 $W(s^{(n)})=3$. $\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 中只有 3 个元素 1, 所以这样 $s^{(n)}$ 的个数为 $\binom{2^n}{3}$. 所以 $N_3(0)=\binom{2^n}{3}+2^n$.

考虑 $L(r,c)=2^n-2^r+c,\ \ r=n,\ c=1$. 设 s 是线性复杂度 $L(s)=L(r,c)=1$ 的二元序列，这样的序列只有一个. $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 是序列 s 的第一周期. 根据 Games-Chan 算法，设 r 是最大的整数，满足 Left $(s^{(r)}),\mathrm{Right}(s^{(r)})$ 相同. 因为 Left $(s^{(n)}),\mathrm{Right}(s^{(n)})$ 相同，故 $r=n$.

又因为线性复杂度 2^n 且 $W(t^{(n)})=1$ 或 3 的 $t^{(n)}$ 个数为 $\binom{2^n}{3}+2^n$, $s^{(n)}+t^{(n)}$ 的个数，即 $N_3(1)=\binom{2^n}{3}+2^n$.

考虑情况 $L(r,c)=2^n-2^r+c,\ \ 3\le r\le n,\ 1\le c\le 2^{r-2}-1$.

设 s 是线性复杂度 $L(s)=L(r,c)$ 的二元序列， $s^{(n)}=\{s_0,s_1,s_2,\cdots,s_{2^n-1}\}$ 是序列 s 的第一周期. 因为 $L(r,c)=2^n-2^r+c=2^{n-1}+\cdots+2^r+c$, 所以 Left $(s^{(r)}),\mathrm{Right}(s^{(r)})$ 相同，且 $s^{(r)}$ 的线性复杂度为 c.

因为线性复杂度为 2^r 且 $W(t^{(r)})=1$ 或 3 的 $t^{(r)}$ 个数为 $\binom{2^r}{3}+2^r$, 根据引理 3.6, $s^{(r)}+t^{(r)}$ 的 3 错线性复杂度为 c.

根据引理 3.5, $s^{(r)}+t^{(r)}$ 的个数为 $2^{c-1}\times\left[\binom{2^r}{3}+2^r\right]$.

根据引理 3.1, 生成每个 $s^{(r)}+t^{(r)}$ 的 $s^{(n)}+t^{(n)}$ 的个数 $2^{2^{n-1}+\cdots+2^r}=2^{2^n-2^r}$.

存在序列 $t^{(n)}$ 使得 $t^{(r)}=\varphi_{r+1}\cdots\varphi_n(t^{(n)}),\ \ L(t^{(n)})=2^n$ 且 $W(t^{(n)})=W(t^{(r)})$, 故 $s^{(n)}+t^{(n)}$ 的 3 错线性复杂度为 $2^{n-1}+\cdots+2^r+L_3(s^{(r)}+t^{(r)})=2^n-2^r+c=L(r,c)$. 所以

$$N_3(L(r,c))=2^{2^n-2^r}\times 2^{c-1}\times\left[\binom{2^r}{3}+2^r\right]=2^{L(r,c)-1}\left[\binom{2^r}{3}+2^r\right].$$

证毕.

定理 3.2 设 $n>2,\ L(r,c)=2^n-2^r+c$ 或 $2^n-2^3+1,\ 4\le r\le n,\ 1\le c\le 2^{r-1}-1$, $N_3(L(r,c))$ 表示周期为 2^n, 线性复杂度 $L(s)=2^n$, 3 错线性复杂度为 $L(r,c)$ 的二元序列个数. 令

$$\begin{aligned}f(n,m)=&\binom{2^n}{3}-(2^{m-2}-1)\times 2^{n+1}-(2^{m-1}-1)\times\binom{2^{n-m}}{2}\times 2^{m+1}\\&-3\times 2^{n-m-2}\left[\binom{2^m}{3}-4\binom{2^{m-1}}{2}\right]-\binom{2^{n-m}}{2}\times\left[\binom{2^m}{2}-2^{m-1}\right]\times 2^m\\g(n,m)=&\binom{2^n}{3}-2^{n-m}\binom{2^m}{3}-\binom{2^{n-m}}{2}\binom{2^m}{2}2^{m+1}\\&+\binom{2^{n-m}}{2}\times 2^{2m}(2^{m-2}-1)+2^{n-m-1}\times\binom{2^{m-1}}{3}-2^{n-2}\times(2^{m-2}-1),\end{aligned}$$

则

$$N_3(L)=\begin{cases}\binom{2^n}{3}+2^n, & L=0,\\ 2^{L(r,c)-1}\left[\binom{2^r}{3}+2^r\right], & L=L(r,c),\ 1\le c\le 2^{r-2}-1,\ r>2,\\ 2^{L(r,c)-1}g(r,m), & L=L(r,c),\quad c=2^{r-1}-2^{r-m},\quad 1<m\le r,\quad r>3,\\ 2^{L(r,c)-1}f(r,m), & L=L(r,c),\quad c=2^{r-1}-2^{r-m}+x,\\ & 1<m<r-1,\quad 0<x<2^{r-m-1},\quad r>3,\\ 0, & \text{其他}.\end{cases}$$

证　根据引理 3.11, 我们只需考虑 $4\le r\le n,\ 2^{r-2}\le c\le 2^{r-1}-1$.

若 $4\le r\le n,\ c=2^{r-1}-2^{r-m},\ 1<m\le r$, 根据引理 3.1 和引理 3.10, $N_3(L(r,c))=2^{L(r,c)-1}g(r,m)$.

若 $4\le r\le n,\ c=2^{r-1}-2^{r-m}+x,\ 1<m<r-1,\ 0<x<2^{r-m-1}$, 根据引理 3.1 和引理 3.8, $N_3(L(r,c))=2^{L(r,c)-1}f(r,m)$.

若 $n=3$, 周期为 2^n, 线性复杂度为 2^n 的二元序列个数是 $2^{2^3-1}=128$. 由引理 3.11, $N_3(0)=N_3(L(3,1))=\binom{2^n}{3}+2^n=64$, 因而其他情况二元序列个数是 0. 证毕.

例如，若 $n=4$, 则周期为 2^n, 线性复杂度为 2^n 的二元序列个数是 $\text{count}=2^{2^4-1}=2^{15}$.

由引理 3.11, $N_3(L(3,1))=2^8\left[\binom{2^3}{3}+2^3\right]=2^{14}=\text{count}/2$.

$N_3(0)=N_3(L(4,1))=\binom{2^4}{3}+2^4=2^6\times 9=\text{count}\times\frac{9}{512}$.

$N_3(L(4,2))=2\times\text{count}\times\frac{9}{512}=\text{count}\times\frac{9}{256}$.

$N_3(L(4,3))=4\times\text{count}\times\frac{9}{512}=\text{count}\times\frac{9}{128}$.

由引理 3.7, $N_3(L(4,4))=\left\{\binom{2^n}{3}-\left[2^n+2^{n-2}\binom{4}{2}(2^n-4)\right]\right\}2^{2^{n-2}-1}=\frac{\text{count}}{16}$.

由引理 3.8 或推论 3.1, $N_3(L(4,5))=\left[\binom{2^n}{3}-2^{n-3}\binom{4}{2}(2^n-4)\right]2^{2^{n-2}}=\text{count}\times\frac{13}{64}$.

由引理 3.9, $N_3(L(4,6)) = \left[\binom{2^n}{3} - 7\times 2^n - 384\binom{2^{n-3}}{2}\right] 2^{2^{n-2}+2^{n-3}-1} = \frac{\text{count}}{16}$.

由引理 3.10, $N_3(L(4,7)) = \left[\binom{2^n}{3} - 34\times 2^n - 3072\binom{2^{n-4}}{2}\right] 2^{2^{n-1}-2^{n-4}-1} = \frac{\text{count}}{32}$.

上述这些情况总和为 $\text{count} = 2^{15}$, 故其他情况二元序列个数是 0. 证毕.

4 结论

通过研究周期为 2^n 的二元序列线性复杂度，提出将 k 错线性复杂度的计算转化为求 Hamming 重量最小的错误序列. 基于 Games-Chan 算法，讨论了线性复杂度为 2^n 的 2^n 周期二元序列的 3 错线性复杂度分布情况. 给出了对应 3 错线性复杂度序列的完整计数公式. 根据引理 2.1, 3 错线性复杂度等于 4 错线性复杂度. 对于一般的线性复杂度为 $2^n - m$ 的 2^n 周期二元序列，也可以使用该方法给出对应 k 错线性复杂度序列的计数公式.

Kavuluru[8] 给出所有 2^n 周期二元序列的 2 错和 3 错线性复杂度分布情况. 基于本文结果，可以得到所有 2^n 周期二元序列的 3 错线性复杂度分布情况，并证明 Kavuluru 的 3 错线性复杂度分布公式是错误的，这些结果将另文给出.

致谢. 谨以此文纪念作者的母亲周马氏，她老人家于 2010 年 12 月 31 日下午去世. 正是由于母亲的激励，才使得作者完成了这些研究工作.

参 考 文 献

[1] Ding C S, Xiao G Z, Shan W J. The Stability Theory of Stream Ciphers. Lecture Notes in Computer Science, Vol.561, Berlin, Heidelberg: Springer-Verlag, 1991, 85–88

[2] Stamp M, Martin C F. An Algorithm for the k-error Linear Complexity of Binary Sequences with Period 2^n. *IEEE Transactions on Information Theory*, 1993, 39(4): 1398–1401

[3] Kurosawa K, Sato F, Sakata T, Kishimoto W. A Relationship Between Linear Complexity and k-Error Linear Complexity. *IEEE Transactions on Information Theory*, 2000, 46(2): 694–698

[4] Rueppel R A. Analysis and Design of Stream Ciphers. Berlin: Springer-Verlag, 1986, Chapter 4.

[5] Meidl W. On the Stablity of 2^n-periodic Binary Sequences. *IEEE Transactions on Information Theory*, 2005, 51(3): 1151–1155

[6] Zhu F X, Qi W F. The 2-error Linear Complexity of 2^n-periodic Binary Sequences with Linear Complexity 2^n–1. *Journal of Electronics*, 2007, 24(3): 390–395 (in Chinese)

[7] Fu F, Niederreiter H, Su M. The Characterization of 2^n-periodic Binary Sequences with Fixed 1-error Linear Complexity. In: Gong G., Helleseth T., Song H.-Y., Yang K. (eds.), SETA 2006, LNCS, Vol. 4086, 88–103, Springer-Verlag, 2006

[8] Kavuluru R. Characterization of 2^n-periodic Binary Sequences with Fixed 2-error or 3-error Linear Complexity. *Des. Codes Cryptogr.*, 2009, 53: 75–97

[9] Etzion T, Kalouptsidis N, Kolokotronis N, Limniotis K, Paterson K G. Properties of the Error Linear

Complexity Spectrum. *IEEE Transactions on Information Theory*, 2009, 55(10): 4681–4686

[10] Games R A, Chan A H. A Fast Algorithm for Determining the Complexity of a Binary Sequence with Period 2^n. *IEEE Transactions on Information Theory*, 1983, 29(1): 144–146

[11] Han Y K, Chung J H, Yang K. On the k-error Linear Complexity of p^m-periodic Binary Sequences. *IEEE Transactions on Information Theory*, 2007, 53(6): 2297–2304

[12] Lauder A, Paterson K. Computing the Error Linear Complexity Spectrum of a Binary Sequence of Period 2^n. *IEEE Transactions on Information Theory*, 2003, 49(1): 273–280

[13] Meidl W. How Many Bits have to be Changed to Decrease the Linear Complexity? *Des. Codes Cryptogr.*, 2004, 33: 109–122

[14] Wei S M, Xiao G Z, Chen Z. A Fast Algorithm for Determining the Minimal Polynomial of a Sequence with Period $2p^n$ over $GF(q)$. *IEEE Transactions on Information Theory*, 2002, 48(10): 2754–2758

[15] Zhou J Q. On the k-error Linear Complexity of Sequences with Period $2p^n$ over $GF(q)$. *Des. Codes Cryptogr.*, 2011, 58(3): 279–296

On the 3-Error Linear Complexity of 2^n-Periodic Binary Sequences with Linear Complexity 2^n

ZHOU Jianqin

(*Telecommunication School, Hangzhou Dianzi University, Hangzhou* 310018)

(*Computer Science School, Anhui University of Technology, Ma'anshan* 243002)

(*E-mail: zhou9@yahoo.com*)

Abstract The linear complexity and the k-error linear complexity of a sequence have been used as important measures of keystream sequence strength. By studying linear complexity of binary sequences with period 2^n, it is proposed that the computing of k-error linear complexity should be converted to finding error sequences with minimal Hamming weight. Based on Games-Chan algorithm, 3-error linear complexity distribution of 2^n-periodic binary sequences with linear complexity 2^n is discussed. For $k = 3, 4$, the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with linear complexity 2^n are derived. Based on those results, the counting functions for the number of all 2^n-periodic binary sequences with given 3-error linear complexity can be obtained. Generally, the complete counting functions on the k-error linear complexity of 2^n-periodic binary sequences with linear complexity $2^n - m$ can be obtained using a similar approach.

Key words periodic sequence; linear complexity; k-error linear complexity; k-error linear complexity distribution.

MR(2000) Subject Classification 94A55; 94A60; 11B50

Chinese Library Classification TN911; TN918.1