文章编号:1007－2985(2012)02－0028－07

2^n 周期平衡二元序列的 8 错线性复杂度*

周建钦[1,2],赵　起[1],崔洪成[1]

(1.安徽工业大学计算机学院,安徽 马鞍山　243002;2.杭州电子科技大学通信工程学院,浙江 杭州　310018)

摘　要:线性复杂度和 k 错线性复杂度分别是流密码密钥流序列强度和稳定性的重要度量指标.通过研究周期为 2^n 的二元序列线性复杂度,基于 *Games-Chan* 算法,讨论了线性复杂度小于 2^n 的 2^n -周期二元序列的 8 错线性复杂度的分布,给出其对应 8 错线性复杂度为 2^{n-2},2^{n-3},2^{n-4} 和 $2^{n-3}-2^{n-j}$ 的原始二元序列计数公式.

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

中图分类号:TN911;TN918.1　　**文献标志码**:A　　**DOI**:10.3969/j.issn.1007－2985.2012.02.008

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 1 个或几个元素,其线性复杂度发生很大的变化,那么该序列仍然是密码学意义上的弱序列.我国学者丁-肖-单[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 Martin 等[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 $k(0\leqslant k\leqslant N)$ 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.

苏明[3] 提出研究周期为 2^n 的二元序列的 $k=1,2$ 时 k -错线性复杂度;Rueppel R A[4] 给出线性复杂度为 L 的周期为 2^n 的二元序列的具体个数;Meidl W[5] 给出 $k=1,2$ 时线性复杂度为 2^n 的周期为 2^n 的二元序列的 k 错线性复杂度分布情况;朱凤翔等[6] 给出 $k=2,3$ 时线性复杂度为 2^n-1 的周期为 2^n 的二元序列的 k 错线性复杂度的分布;谭林等[7] 给出 $k=1,2$ 时 F_2 上 2^n -周期序列的 k -错误序列的计数,并给出了 F_2 上 2^n -周期序列的 $1-$ 错误序列个数的均值.

由于线性复杂度小于 2^n 的 2^n -周期二元序列具有偶数个非 0 元素,因而又称为平衡二元序列.笔者通过研究周期为 2^n 的二元序列线性复杂度,基于 Games-Chan 算法[8],讨论了线性复杂度小于 2^n 的 2^n -周期二元序列的 8 错线性复杂度的分布,给出其对应 8 错线性复杂度为 2^{n-2},2^{n-3},2^{n-4} 和 $2^{n-3}-2^{n-j}$ 的原始二元序列计数公式,并全部通过计算机编程进行了验证.

1　预备知识与引理

文中所涉及序列都是在 $GF(q)$ 域上,设 $GF(q)$ 域上的 2 个向量 $\boldsymbol{X}=(x_1\ \ x_2\ \ x_3\ \ \cdots\ \ x_{n-1}\ \ x_n)$ 和 $\boldsymbol{Y}=(y_1\ \ y_2\ \ y_3\ \ \cdots\ \ y_{n-1}\ \ y_n)$,则定义 $\boldsymbol{X}+\boldsymbol{Y}=(x_1+y_1\ \ x_2+y_2\ \ x_3+y_3\ \ \cdots\ \ x_{n-1}+y_{n-1}\ \ x_n+y_n)$.

* **收稿日期**:2011－10－22

基金项目:安徽省自然科学基金资助项目(1208085MF106)

作者简介:周建钦(1963－),男,山东巨野人,安徽工业大学计算机学院教授,硕士,主要从事通信、密码学与理论计算机科学研究.

对于序列 S,若存在正整数 T,使得 $s_{i+T}=s_i(i=0,1,2,3,\cdots)$ 成立,则称 S 为周期序列,最小正整数 T 称为序列 S 的最小周期.若序列 S 满足 $s_j+a_1s_{j-1}+a_2s_{j-2}+\cdots+a_Ls_{j-L}=0(j\geqslant L)$,其中 L 为正整数,$a_1,a_2,a_3,\cdots,a_L$ 是 $GF(q)$ 中的元素,则称序列 S 是一个 L 阶线性递归序列(也称差分方程),称最小的整数 L 为该递归序列的线性复杂度 $c(S)$.

序列 $S=(s_1,s_2,s_3,\cdots)$ 的生成函数定义为 $s(x)=s_0+s_1x+s_2x^2+\cdots=\sum_{i=0}^{\infty}s_ix^i$,有限序列 $s^{(n)}=(s_1,s_2,s_3,\cdots,s_{n-1})$ 的生成函数定义为 $s^{(n)}(x)=s_0+s_1x+s_2x^2+\cdots+s_{n-1}x^{n-1}$.若 S 是周期序列,$s^{(n)}$ 是它的第一周期,则 $s(x)$ 可以表示成

$$s(x)=s^n(x)(1+x^n+x^{2n}+x^{3n}+\cdots)=\frac{s^n(x)}{1-x^n}=\frac{s^n(x)/\gcd(s^n(x),1-x^n)}{(1-x^n)/\gcd(s^n(x),1-x^n)}=\frac{g(x)}{f_s(x)},$$

且 $f_s(x)=(1-x^n)/\gcd(s^n(x),1-x^n)$,$g(x)=s^n(x)/\gcd(s^n(x),1-x^n)$.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化为求 $s^N(x)$ 中因式 $(1-x)$ 的次数.

下面的 2 个引理是众所周知的结果,也可参见文献[5]:

引理 1　设周期为 $N=2^n$ 的二元序列 S,其线性复杂度 $L(S)=N$,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 1 个 1 即变为 Hamming 重量为偶数的序列,所以下面主要考虑 Hamming 重量为偶数的序列.

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

若最少改变二元序列 S 的 k 个元素,序列 S 的线性复杂度即可下降,根据引理 2,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 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$(0<i<N)$.若 $j-i=2^r(1+2a)$,$a>0$,$0\leqslant i<j<N$,$r\geqslant 0$,则 $L(E_i+E_j)=2^n-2^r$.

2　周期为 2^n 平衡二元序列的 8 错线性复杂度

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

引理 4[5]　定义 1 的映射 φ_n 满足以下性质:(ⅰ)$W(\varphi_n(s^{(n)}))\leqslant W(s^{(n)})$;(ⅱ)$W(\varphi_n(s^{(n)}))$,$W(s^{(n)})$ 奇偶性相同;(ⅲ)集合 $\varphi_{n+1}^{-1}(s^{(n)})=\{v\in F_2^{2^{n+1}}\mid\varphi_{n+1}(v)=s^{(n)}\}$ 的大小为 2^{2^n}.

引理 5[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

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

给出线性复杂度小于 2^n 的 2^n-周期二元序列的全部 8 错线性复杂度分布非常重要,但也相当困难,下面讨论几种特殊情况.

定理 1　设 $N_8(2^{n-2})$ 表示周期为 2^n,线性复杂度 $L(S)<2^n$,8 错线性复杂度为 2^{n-2} 的二元序列 S 的个数,$n>3$,则

$$N_8(2^{n-2})=[2^n(2^n-4)(2^n-8)(2^n-12)(2^n-16)(2^n-20)(2^n-24)(2^n-28)/8!\,]\,2^{2^{n-2}-1}.$$

证明　设序列 $s^{(n)}$ 线性复杂度为 2^{n-2} 的二元序列,则 $s^{(n)}$ 的个数为 $2^{2^{n-2}-1}$.

设序列 $u^{(n)}$,$W(u^{(n)})=0$,易知存在一个序列 $W(v^{(n)})=4$,使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-2},即 $s^{(n)}$

$+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$,$W(u^{(n)})=2$,易知存在一个序列 $W(v^{(n)})=2,4$ 或 6,使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-2},即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$,$W(u^{(n)})=4$,易知存在一个序列 $W(v^{(n)})=0,2,4,6$ 或 8,使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-2},即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$,$W(u^{(n)})=6$,易知存在一个序列 $W(v^{(n)})=2,4,6,8$,使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-2},即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$,$W(u^{(n)})=8$,且 $u^{(n)}$ 中至少 2 个非 0 元素距离为 2^{n-2} 的倍数. 易知存在一个序列 $v^{(n)}$,$W(v^{(n)})=4,6$ 或 8,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-2},即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-2}.

设序列 $u^{(n)}$,$W(u^{(n)})=8$,且 $u^{(n)}$ 中不存在 2 个非 0 元素距离为 2^{n-2} 的倍数. 易知不存在序列 $v^{(n)}$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-2},即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度等于 2^{n-2}. 序列 $u^{(n)}$ 的个数为 $2^n(2^n-4)(2^n-8)(2^n-12)(2^n-16)(2^n-20)(2^n-24)(2^n-28)/8!$.

因而,8 错线性复杂度为 2^{n-2} 的二元序列 S 的个数为

$$N_8(2^{n-2})=[2^n(2^n-4)(2^n-8)(2^n-12)(2^n-16)(2^n-20)(2^n-24)(2^n-28)/8!\ ]\,2^{2^{n-2}-1}.$$

证毕.

例如,当 $n=4$ 时,

$[2^n(2^n-4)(2^n-8)(2^n-12)(2^n-16)(2^n-20)(2^n-24)(2^n-28)/8!\ ]\,2^{2^{n-2}-1}=0$,即线性复杂度小于 $L(S)<2^4$,8 错线性复杂度为 8 的二元序列 S 的个数为 0.

当 $n=5$ 时,

$[2^n(2^n-4)(2^n-8)(2^n-12)(2^n-16)(2^n-20)(2^n-24)(2^n-28)/8!\ ]\,2^{2^{n-2}-1}=(32\times28\times24\times20\times16\times12\times8\times4)\times2^7=8\ 388\ 608$,通过计算机验证,线性复杂度小于 $L(S)<2^5$,8 错线性复杂度为 8 的二元序列 S 的个数为 83 886 08.

定理 2　设 $N_8(2^{n-3})$ 表示周期为 $L(S)<2^n$,线性复杂度 2^n,8 错线性复杂度为 2^{n-3} 的二元序列 S 的个数,$n>4$,则

$$\begin{aligned}N_8(2^{n-3})=\{&2^n(2^n-8)(2^n-16)(2^n-24)/4!+2^n(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)/6!+\\&\binom{2^{n-3}}{3}\binom{8}{2}^3+\binom{2^{n-3}}{2}\binom{8}{2}\binom{8}{2}(2^n-16)(2^n-24)/2!+\binom{2^{n-3}}{1}\binom{8}{2}(2^n-8)(2^n-16)\cdot\\&(2^n-24)(2^n-32)/4!+2^n(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)\cdot\\&(2^n-48)(2^n-52)/8!+\binom{2^{n-3}}{4}\binom{8}{2}^4+\binom{2^{n-3}}{3}\binom{8}{2}^3(2^n-24)(2^n-32)/2!+\\&\binom{2^{n-3}}{2}\binom{8}{2}\binom{8}{2}(2^n-16)(2^n-24)(2^n-32)(2^n-40)/4!+\\&\binom{2^{n-3}}{1}\binom{8}{2}(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)(2^n-48)/6!+\\&\binom{2^{n-3}}{2}\binom{8}{3}\binom{8}{3}\left[\binom{2^{n-3}-2}{1}\binom{8}{2}+(2^n-16)(2^n-24)/2!\ \right]+\\&\binom{2^{n-3}}{1}\binom{8}{3}\left[\binom{2^{n-3}-1}{2}\binom{8}{2}\binom{8}{2}(2^n-24)+\binom{2^{n-3}-1}{1}\binom{8}{2}\right]\cdot\\&(2^n-16)(2^n-24)(2^n-32)/3!+(2^n-8)(2^n-16)\cdot\\&(2^n-24)(2^n-32)(2^n-40)/5!\ ]\}2^{2^{n-3}-1}.\end{aligned}$$

证明　设序列 $s^{(n)}$ 线性复杂度为 2^{n-3} 的二元序列,则 $s^{(n)}$ 的个数为 $2^{2^{n-3}-1}$.

设序列 $u^{(n)}$,$W(u^{(n)})=0$,易知存在一个序列 $W(v^{(n)})=8$,使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3},即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-3}.

设序列 $u^{(n)}$,$W(u^{(n)})=2$,易知存在一个序列 $W(v^{(n)})=6$ 或 8,使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3},

即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-3}.

设序列 $u^{(n)}$，$W(u^{(n)})=4$，且 $u^{(n)}$ 中至少 2 个非 0 元素距离为 2^{n-3} 的倍数. 易知存在一个序列 $W(v^{(n)})=4,6$ 或 8，使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3}，即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-3}.

设序列 $u^{(n)}$，$W(u^{(n)})=4$，且 $u^{(n)}$ 中不存在 2 个非 0 元素距离为 2^{n-3} 的倍数. 易知不存在序列 $v^{(n)}$，使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3}，即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度等于 2^{n-3}. 这样序列 $u^{(n)}$ 个数为 $C1=2^n(2^n-8)(2^n-16)(2^n-24)/4!$.

设序列 $u^{(n)}$，$W(u^{(n)})=6$，且 $u^{(n)}$ 中至少 3 个非 0 元素距离为 2^{n-3} 的倍数. 易知存在一个序列 $W(v^{(n)})=2,4,6$ 或 8，使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3}，即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-3}.

设序列 $u^{(n)}$，$W(u^{(n)})=6$，且 $u^{(n)}$ 中不存在 3 个非 0 元素距离为 2^{n-3} 的倍数. 易知不存在序列 $v^{(n)}$，使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3}，即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度等于 2^{n-3}.

分成 2 种情况考虑：(ⅰ) 不存在 2 个非 0 元素距离为 2^{n-3} 倍数；(ⅱ) 只有 2 个非 0 元素距离为 2^{n-3} 的倍数.

得到序列 $u^{(n)}$ 个数为

$$C2=2^n(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)/6!+\binom{2^{n-3}}{3}\binom{8}{2}\binom{8}{2}\binom{8}{2}+\binom{2^{n-3}}{2}\binom{8}{2}\binom{8}{2}(2^n-16)(2^n-24)/2!+\binom{2^{n-3}}{1}\binom{8}{2}\cdot(2^n-8)(2^n-16)(2^n-24)(2^n-32)/4!.$$

设序列 $u^{(n)}$，$W(u^{(n)})=8$，且 $u^{(n)}$ 中至少 4 个非 0 元素距离为 2^{n-3} 的倍数. 易知存在一个序列 $W(v^{(n)})=0,2,4,6$ 或 8，使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3}，即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度小于 2^{n-3}.

设序列 $u^{(n)}$，$W(u^{(n)})=8$，且 $u^{(n)}$ 中不存在 4 个非 0 元素距离为 2^{n-3} 的倍数. 易知不存在序列 $v^{(n)}$，使得 $u^{(n)}+v^{(n)}$ 的线性复杂度为 2^{n-3}，即 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度等于 2^{n-3}.

同样可以分成 2 种情况考虑：(ⅰ) 不存在 3 个非 0 元素距离为 2^{n-3} 倍数；(ⅱ) 只有 3 个非 0 元素距离为 2^{n-3} 倍数.

得到序列 $u^{(n)}$ 个数为

$$\begin{aligned}C3=&2^n(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)(2^n-48)(2^n-52)/8!+\\&\binom{2^{n-3}}{4}\binom{8}{2}\binom{8}{2}\binom{8}{2}\binom{8}{2}+\binom{2^{n-3}}{3}\binom{8}{2}\binom{8}{2}\binom{8}{2}(2^n-24)(2^n-32)/2!+\\&\binom{2^{n-3}}{2}\binom{8}{2}\binom{8}{2}(2^n-16)(2^n-24)(2^n-32)(2^n-40)/4!+\\&\binom{2^{n-3}}{1}\binom{8}{2}(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)(2^n-48)/6!+\\&\binom{2^{n-3}}{2}\binom{8}{3}\binom{8}{3}\left[\binom{2^{n-3}-2}{1}\binom{8}{2}+(2^n-16)(2^n-24)/2!\right]+\\&\binom{2^{n-3}}{1}\binom{8}{3}\left[\binom{2^{n-3}-1}{2}\binom{8}{2}\binom{8}{2}(2^n-24)+\right.\\&\left.\binom{2^{n-3}-1}{1}\binom{8}{2}(2^n-16)(2^n-24)(2^n-32)/3!+\right.\\&(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)/5!.\end{aligned}$$

综上所述，序列 $u^{(n)}$ 个数为

$$\begin{aligned}C4=C1+C2+C3=&2^n(2^n-8)(2^n-16)(2^n-24)/4!+2^n(2^n-8)(2^n-16)(2^n-24)(2^n-32)\cdot\\&(2^n-40)/6!+\binom{2^{n-3}}{3}\binom{8}{2}^3+\binom{2^{n-3}}{2}\binom{8}{2}\binom{8}{2}(2^n-16)(2^n-24)/2!+\\&\binom{2^{n-3}}{1}\binom{8}{2}(2^n-8)(2^n-16)(2^n-24)(2^n-32)/4!+\end{aligned}$$

$$2^n(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)(2^n-48)(2^n-52)/8!+\binom{2^{n-3}}{4}\binom{8}{2}^4+$$
$$\binom{2^{n-3}}{3}\binom{8}{2}^3(2^n-24)(2^n-32)/2!+\binom{2^{n-3}}{2}\binom{8}{2}\binom{8}{2}(2^n-16)(2^n-24)(2^n-32)\cdot$$
$$(2^n-40)/4!+\binom{2^{n-3}}{1}\binom{8}{2}(2^n-8)(2^n-16)(2^n-24)(2^n-32)(2^n-40)\cdot$$
$$(2^n-48)/6!+\binom{2^{n-3}}{2}\binom{8}{3}\binom{8}{3}\left[\binom{2^{n-3}-2}{1}\binom{8}{2}+(2^n-16)(2^n-24)/2!\right]+$$
$$\binom{2^{n-3}}{1}\binom{8}{3}\left[\binom{2^{n-3}-1}{2}\binom{8}{2}\binom{8}{2}(2^n-24)+\binom{2^{n-3}-1}{1}\binom{8}{2}(2^n-16)(2^n-24)\cdot\right.$$
$$\left.(2^n-32)/3!+(2^n-8)(2^n-16)\cdot(2^n-24)(2^n-32)(2^n-40)/5!\right].$$

因而,8 错线性复杂度为 2^{n-2} 的二元序列 S 的个数为 $N_8(2^{n-3})=C4\cdot 2^{2^{n-3}-1}$.

证毕.

例如,当 $n=5$ 时,$N_8(2^{n-3})=7\ 480\ 320\times 8=59\ 842\ 560$,通过计算机验证,线性复杂度小于 $L(S)<2^5$,8 错线性复杂度为 4 的二元序列 S 的个数为 59 842 560.

定理 3　设 $N_8(2^{n-4})$ 表示周期为 2^n,线性复杂度 $L(S)<2^n$,8 错线性复杂度为 2^{n-4} 的二元序列 S 的个数,则

$$N_8(2^{n-4})=\left(1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-2^{n-4}\binom{16}{8}\right)2^{2^{n-4}-1}.$$

证明　设序列 $s^{(n)}$ 线性复杂度为 2^{n-4} 的二元序列,则 $s^{(n)}$ 的个数为 $2^{2^{n-4}-1}$.

设序列 $u^{(n)}$,$W(u^{(n)})=0,2,4,6$,易知不存在 $v^{(n)}$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-(2^{n-2}+2^{n-3}+2^{n-4})=2^{n-4}$,即 $u^{(n)}+s^{(n)}$ 的 8 错线性复杂度等于 2^{n-4}.

易知存在序列 $u^{(n)}$,$v^{(n)}$,$W(u^{(n)})=W(v^{(n)})=8$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-(2^{n-2}+2^{n-3}+2^{n-4})=2^{n-4}$,即 $u^{(n)}+s^{(n)}$ 的 8 错线性复杂度小于 2^{n-4}.

设序列 $u^{(n)}$ 且 $W(u^{(n)})=8$,则 $u^{(n)}$ 的个数为 $\binom{2^n}{8}$.

假设序列 $u^{(n)}$,$v^{(n)}$,$W(u^{(n)})=W(v^{(n)})=8$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 2^{n-4}. 这样 16 个非 0 元素的组合个数为 2^{n-4}.

设序列 $u^{(n)}$,$W(u^{(n)})=8$,且 $u^{(n)}$ 中 8 个非 0 元素属于这样 16 个非 0 元素的组合,则 $u^{(n)}$ 的个数为 $2^{n-4}\binom{16}{8}$.

设序列 $s^{(n)}$ 线性复杂度为 2^{n-4} 的二元序列,序列 $u^{(n)}$,$W(u^{(n)})=0,2,4,6$ 或 8,且 $u^{(n)}$ 中 8 个非 0 元素不属于这样 16 个非 0 元素的组合,可知 $s^{(n)}+u^{(n)}$ 的 8 错线性复杂度为 2^{n-4}. 这样 $s^{(n)}+u^{(n)}$ 的个数为

$$\left(1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-2^{n-4}\binom{16}{8}\right)2^{2^{n-4}-1}.$$

证毕.

例如,当 $n=4$ 时,$(1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-2^{n-4}\binom{16}{8})2^{2^{n-4}-1}=(1+120+\binom{16}{4}+\binom{16}{6}+\binom{16}{8}-\binom{16}{8})2=9\ 949$,通过计算机验证,线性复杂度 $L(S)<2^4$,8 错线性复杂度为 1 的二元序列 S 的个数为 9 949.

当 $n=5$ 时,$(1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-2^{n-4}\binom{16}{8})2^{2^{n-4}-1}=(1+496+\binom{32}{4}+\binom{32}{6}+\binom{32}{8}-2\binom{32}{8})=22\ 870\ 418$,通过计算机验证,线性复杂度 $L(S)<2^5$,8 错线性复杂度为 2 的二元序列 S 的个数

为 22 870 418.

定理 4　设 $N_8(2^{n-3}-2^{n-j})$ 表示周期为 2^n,线性复杂度 $L(S)<2^n$,8 错线性复杂度为 $2^{n-3}-2^{n-j}$ 的二元序列 S 的个数,$n>3$,$3<j\leqslant n$,则

$$N_8(2^{n-3}-2^{n-j})=[1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-2^{n-8+j}(\binom{16}{8}-2)-2^{n-3}-(2^{n-9+j}-2^{n-5})(\binom{16}{8}-2)]2^{2^{n-3}-2^{n-j}-1}.$$

证明　设序列 $s^{(n)}$ 线性复杂度为 $2^{n-3}-2^{n-j}$ 的二元序列,$3<j\leqslant n$,则 $s^{(n)}$ 的个数为 $2^{2^{n-3}-2^{n-j}-1}$.

易知存在序列 $u^{(n)},v^{(n)},W(u^{(n)})=W(v^{(n)})=8$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-1}-(2^{n-2}+2^{n-3}+2^{n-j})=2^{n-3}-2^{n-j}$,即 $u^{(n)}+s^{(n)}$ 的 8 错线性复杂度小于 $2^{n-3}-2^{n-j}$.

设序列 $u^{(n)}$ 且 $W(u^{(n)})=8$,则 $u^{(n)}$ 的个数为 $\binom{2^n}{8}$.

假设序列 $u^{(n)},v^{(n)},W(u^{(n)})=W(v^{(n)})=8$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-3}-2^{n-j}$. 这样 16 个非 0 比特组合的个数为 $\dfrac{2^{2(n-3)}}{4\times 2^{n-j}}=2^{n-8+j}$,且每个组合都与另外 2 个组合有包含 8 个非 0 比特的交集. 这样 8 个非 0 比特等距离分布,构成集合 $A1$,$A1$ 的个数为 2^{n-3}. 例如,其 8 个位置可以为 $\{i,i+2^{n-3},i+2^{n-2},i+2^{n-2}+2^{n-3},i+2^{n-1},i+2^{n-1}+2^{n-3},i+2^{n-1}+2^{n-2},i+2^{n-1}+2^{n-2}+2^{n-3}\}$.

设序列 $u^{(n)},W(u^{(n)})=8$,且 $u^{(n)}$ 中 8 个非 0 元素属于这样 16 个非 0 元素的组合或者 $A1$,则 $u^{(n)}$ 的个数为 $C1=2^{n-8+j}(\binom{16}{8}-2)+2^{n-3}$.

假设序列 $u^{(n)},v^{(n)},W(u^{(n)})=W(v^{(n)})=8$,使得 $u^{(n)}+v^{(n)}$ 线性复杂度为 $2^{n-3}-2^{n-m}$,$3<m<j$. 这样 16 个非 0 元素的组合构成集合 $A2$,$A2$ 的个数为 2^{n-8+m}. $A2$ 的每个元素包含 $A1$ 的 2 个元素.

设序列 $u^{(n)},W(u^{(n)})=8$,且 $u^{(n)}$ 中 8 个非 0 元素属于这样 16 个非 0 元素的组合且不属于 $A1$,则 $u^{(n)}$ 的个数为 $2^{n-8+m}(\binom{16}{8}-2)$.

由于 $t^{(n)}=s^{(n)}+u^{(n)}+v^{(n)}$ 的线性复杂度为 $2^{n-3}-2^{n-j}$,因此 $s^{(n)}+t^{(n)}=u^{(n)}+v^{(n)}$. 此时,$s^{(n)}+u^{(n)}$ 与 $t^{(n)}+v^{(n)}$ 相同.

对于 $3<m<j$,所有这样 $u^{(n)}$ 的个数为 $C2=\sum_{m=4}^{j-1}2^{n-8+m}(\binom{16}{8}-2)=(2^{n-8+j}-2^{n-4})(\binom{16}{8}-2)$.

因而 8,错线性复杂度为 $2^{n-3}-2^{n-j}$ 的二元序列 S 的个数为

$$N_8(2^{n-3}-2^{n-j})=(1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-C1-C2/2)2^{2^{n-3}-2^{n-j}-1}=$$
$$[1+\binom{2^n}{2}+\binom{2^n}{4}+\binom{2^n}{6}+\binom{2^n}{8}-2^{n-8+j}(\binom{16}{8}-2)-2^{n-3}-$$
$$(2^{n-9+j}-2^{n-5})(\binom{16}{8}-2)]2^{2^{n-3}-2^{n-j}-1}.$$

证毕.

容易验证定理 3 是 $j=4$ 时定理 4 的特例.

例如,当 $n=4$,$j=4$ 时,

$$[1+\binom{2^4}{2}+\binom{2^4}{4}+\binom{2^4}{6}+\binom{2^4}{8}-2^{4-8+4}(\binom{16}{8}-2)-2^{4-3}-(2^{4-8+4}-2^{4-4})(\binom{16}{8}-2)/2]=9\ 949,$$

即线性复杂度 $L(S)<2^4$,8 错线性复杂度为 1 的二元序列 S 的个数为 9 949,与定理 3 的 $n=4$ 时结果相同.

当 $n=5$,$j=4$ 时,

$$[1+\binom{2^5}{2}+\binom{2^5}{4}+\binom{2^5}{6}+\binom{2^5}{8}-2^{5-8+4}(\binom{16}{8}-2)-2^{5-3}-(2^{5-9+4}-2^{5-5})(\binom{16}{8}-2)]2^1=22\ 870\ 418,$$

即线性复杂度 $L(S)<2^5$,8 错线性复杂度为 2 的二元序列 S 的个数为 22 870 418. 与定理 3 的 $n=5$ 时结果相同.

当 $n=5, j=5$ 时,

$$[1+\binom{2^5}{2}+\binom{2^5}{4}+\binom{2^5}{6}+\binom{2^5}{8}-2^{5-8+5}(\binom{16}{8}-2)-2^{5-3}-(2^{5-9+5}-2^{5-5})(\binom{16}{8}-2)]2^2=45\ 586\ 420,$$

通过计算机验证,线性复杂度 $L(S)<2^5$,8 错线性复杂度为 3 的二元序列 S 的个数为 45 586 420.

参考文献:

[1] DING Cun-sheng, XIAO Guo-zhen, SHAN Wei-juan. The Stability Theory of Stream Ciphers [M]. LNCS 561. Berlin: Springer-Verlag, 1991: 85 - 88.

[2] STAMP M, MARTIN C F. An Algorithm for Thek-Error Linear Complexity of Binary Sequences with Period 2^n [J]. IEEE Transactions on Information Theory, 1993, 39(4): 1 389 - 1 401.

[3] 苏 明. 周期序列复杂度的分布 [D]. 天津: 南开大学博士论文, 2004.

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

[5] MEIDL W. On the Stability of 2^n-Periodic Binary Sequences [J]. IEEE Transactions on Information Theory, 2005, 51(3): 1 151 - 1 155.

[6] ZHU Feng-xiang, QI Wen-feng. The 2-Error Linear Complexity of 2^n-Periodic Binary Sequences with Linear Complexity 2^n-1 [J]. Journal of Electronics (China), 2007, 24(3): 390 - 395.

[7] 谭 林, 戚文峰. F_2 上 2^n 周期序列的 k 错误序列 [J]. 电子与信息学报, 2008, 30(11): 2 592 - 2 595.

[8] GAMES R A, CHAN A H. A Fast Algorithm for Determining the Complexity of a Binary Sequence with Period 2^n [J]. IEEE Transactions on Information Theory, 1983, 29(1): 144 - 146.

8-Error Linear Complexity of 2^n-Periodic Balanced Binary Sequences

ZHOU Jian-qin[1,2], ZHAO Qi[1], CUI Hong-cheng[1]

(1. Computer Science School, Anhui University of Technology, Ma'anshan 243002, Anhui China;
2. Telecommunication School, Hangzhou Dianzi University, Hangzhou 310018, China)

Abstract: The linear complexity and the k-error linear complexity of a sequence have been used as the important measurement of keystream sequence strength. By studying linear complexity of binary sequences with period 2^n, based on Games-Chan algorithm, 8-error linear complexity distribution of 2^n-periodic binary sequences with linear complexity less than 2^n is discussed. The complete counting functions on 2^n-periodic balanced binary sequences with 8-error linear complexity 2^{n-2}, 2^{n-3}, 2^{n-4} and $2^{n-3}-2^{n-j}$ are derived respectively.

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

(责任编辑 陈炳权)