文章编号:1007－2985(2012)03－0032－04

# 周期二元序列的部分 4 -错误序列计数公式*

周建钦[1,2],刘　军[1]
(1.杭州电子科技大学通信工程学院,浙江 杭州　310018;2.安徽工业大学计算机学院,安徽 马鞍山　243032)

**摘　要**:$k$ -错线性复杂度是度量密钥流序列的密码强度的一个重要指标.为了更好地刻画和研究序列的随机性,研究了周期为 $2^n$ 的二元序列 $\underline{s}$ 的 $k$ -错线性复杂度($LC_k(\underline{s})$)的分布情况,讨论了满足 $LC_k(\underline{s})=LC(\underline{s}+\underline{e})$ 条件下的 $k$ -错误序列 $\underline{e}$ 的分布情况.基于 Games-Chan 算法,通过将 $k$ -错线性复杂度的计算转化为求 Hamming 重量最小的错误序列的方法,给出了线性复杂度小于 $2^n$ 的 $2^n$ 周期二元序列的部分 4 -错误序列的计数公式.

**关键词**:序列密码;线性复杂度;$k$ -错线性复杂度;$k$ -错误序列
**中图分类号**:TN918　　**文献标志码**:A　　**DOI**:10.3969/j.issn.1007－2985.2012.03.009

线性复杂度和 $k$ -错线性复杂度是密钥流序列的密码强度的重要指标.为了抵抗 B-M 算法的攻击,密钥流序列的线性复杂度应保证足够大,但仅考虑有较高线性复杂度是不够的,还希望当序列改变少量的比特时,其线性复杂度不会急剧下降.为此,Ding-Xiao-Shan[1]提出了序列的稳定性理论及序列的球形复杂度,随后国外学者 Stamp M 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.之后,Kurosawa K 等[3]提出了错误序列的概念.谭林等[4]在此基础上引出了 $k$ -错误序列,认为一条安全性强的序列不仅要有较高的线性复杂度和 $k$ -错线性复杂度,而且对数值较小的 $k$ 值,还要有较少的 $k$ -错误序列,并给出了相应的 $k$ -错误序列($k=1,2$)的计数公式.随后,李鹤龄[5]给出了有限域 $F_p$ 上 $p^n$ 周期序列的 1 -错误序列的个数,讨论了 2 -错误序列的个数.

笔者在文献[6]提出的将 $k$ -错线性复杂度的计算转化为求 Hamming 重量最小的错误序列的方法的基础上,对于 $k=4$,给出了线性复杂度小于 $2^n$ 的 $2^n$ -周期二元序列的部分 $k$ 错误序列的计数公式 $M_k(s)$.

## 1　预备知识

设 $s=(s_0,s_1,s_2,\cdots,s_{N-1})^\infty$ 是周期为 $N$ 的二元序列,序列 $s$ 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 $s^N=\{s_0,s_1,s_2,\cdots,s_N\}$ 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,那么 $s(x)$ 可以表示成

$$s(x)=s^N(x)(1+x^N+x^{2N}+\cdots)=\frac{s^N(x)}{1-x^N}=\frac{s^N(x)/\gcd(s^N(x),1-x^N)}{(1-x^N)/\gcd(s^N(x),1-x^N)}=\frac{g_s(x)}{f_s(x)}.$$

显然,$\gcd(g_s(x),f_s(x))=1$,$\deg(g_s(x))<\deg(f_s(x))$,$f_s(x)$ 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,记作 $LC(s)$.

---

* **收稿日期**:2011－12－19
**基金项目**:浙江省自然科学基金资助项目(Y1100318;R1090138)
**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.

**定义 1**[2]　设 $s=(s_0,s_1,\cdots,s_{N-1})^N$ 是 $N$ -周期序列,其 $k$ -错误线性复杂度 $LC(s)$ 定义为

$$LC_k(s)=\min_{W_H(e)\leqslant k} LC(s+e),$$

其中 $e=(e_0,e_1,\cdots,e_{N-1})^N$,$W_H(e)$ 表示序列 $e$ 在一个周期 $N$ 内的 Hamming 重量.随后,Kurosawa 等[3] 提出了错误序列的概念,谭林等[4] 认为错误序列的多少与密钥序列的安全强度有很大的关系,故在此基础上给出了 $k$ -错误序列的定义.

**定义 2**[4]　设 $N$ -周期序列 $s$ 的 $k$ -错线性复杂度为 $LC_k(s)$,若 $N$ -周期序列 $e$ 满足 $LC(s+e)=LC_k(s)$ 且 $1\leqslant W_H(e)\leqslant k$,则称 $e$ 为 $s$ 的 $k$ -错误序列.记序列 $s$ 的 $k$ 错误序列的总数为 $M_k(s)$.

以下将 $2^n$ 周期二元序列 $s$ 表示成 $s^{(n)}$.下面给出 3 个重要的引理,也可参考文献[6].

**引理 1**　设序列 $s^{(n)}$ 的线性复杂度 $LC(s^{(n)})=2^n$,当且仅当该序列的一个周期的 Hamming 重量为奇数.

**引理 2**　设 2 个不同的序列 ${s_1}^{(n)}$ 和 ${s_2}^{(n)}$,若 $LC({s_1}^{(n)})\neq LC({s_2}^{(n)})$,则 $L({s_1}^{(n)}+{s_2}^{(n)})=\max\{L({s_1}^{(n)}),L({s_2}^{(n)})\}$;若 $LC({s_1}^{(n)})=LC({s_2}^{(n)})$,则 $L({s_1}^{(n)}+{s_2}^{(n)})<L({s_1}^{(n)})$.

**引理 3**　设 $E_i$ 是周期为 $2^n$ 的二元序列,在其一个周期内,只有第 $i$ 位置元素是 $1,0\leqslant i<2^n$.若 $j-i=2^r(1+2a)$,$a\geqslant 0$,$0\leqslant i<j<2^n$,$r\geqslant 0$,则 $LC(E_i+E_j)=2^n-2^r$.

**引理 4**[3]　设 $s^{(n)}$ 是周期为 $2^n$ 的二元序列,则 $\mathrm{merr}(s^{(n)})=2^{W_H(2^n-LC(s^{(n)}))}$,其中 $\mathrm{merr}(s^{(n)})$ 为满足不等式 $LC_k(s^{(n)})<LC(s^{(n)})$ 的最小正整数 $k$,$W_H(a)$ 是整数 $a$ 的二进制表示下的 Hamming 重量.

## 2　$2^n$ -周期序列的 4 -错误序列

**定理 1**　设序列 $s^{(n)}$ 满足 $LC(s^{(n)})<2^n$,$LC_4(s^{(n)})=c$,$1\leqslant c\leqslant 2^{n-3}$,则 $M_4(s^{(n)})=1$.

**证明**　设 2 个不同的序列 $p^{(n)}$ 和 $q^{(n)}$,$LC(p^{(n)})=LC(q^{(n)})=c$,$1\leqslant c\leqslant 2^{n-3}$.另设 2 个不同的序列 $u^{(n)}$ 和 $v^{(n)}$,$W_H(u^{(n)})=2$ 或 4,$W_H(v^{(n)})=2$ 或 4.

假设 $p^{(n)}+u^{(n)}$ 和 $q^{(n)}+v^{(n)}$ 是相同的,也即 $p^{(n)}+q^{(n)}$ 与 $u^{(n)}+v^{(n)}$ 相同.根据引理 2,$LC(p^{(n)}+q^{(n)})<c\leqslant 2^{n-3}$,再根据 Games-Chan 算法,此时 $u^{(n)}+v^{(n)}$ 呈 8 等分分布,故只能取 $W_H(u^{(n)}+v^{(n)})=8$,$LC(u^{(n)}+v^{(n)})=2^{n-3}$.从而,$p^{(n)}+u^{(n)}\neq q^{(n)}+v^{(n)}$.

因此,序列 $s^{(n)}=p^{(n)}+u^{(n)}$ 的 4 -错误序列只有 $u^{(n)}$ 本身,即 $M_4(s^{(n)})=1$.证毕.

**例 1**　$n=5$,$LC_4(s^{(n)})=4$,令 $s^{(n)}=(10100001100110111011101110111011)$,经验证,其 4 -错误序列 $e^{(n)}=$(0001 1010 0010 0000 0000 0000 0000),即 $M_4(s^{(n)})=1$.

**定理 2**　设序列 $s^{(n)}$ 满足 $LC(s^{(n)})<2^n$,$LC_4(s^{(n)})=2^{n-2}-2^{n-m}$,$n\geqslant 4$,$4\leqslant m\leqslant n$,则 $M_4(s^{(n)})=1$ 或 2.

**证明**　假设 $s^{(n)}=p^{(n)}+u^{(n)}$,其中 $LC(p^{(n)})=2^{n-2}-2^{n-m}$,$4\leqslant m\leqslant n$.根据引理 4,$\mathrm{merr}(p^{(n)})=8$.若要 $LC_4(s^{(n)})=2^{n-2}-2^{n-m}$,对所有 $W_H(u^{(n)})=0$ 或 2 的 $u^{(n)}$,$s^{(n)}$ 的 4 -错误序列即为 $u^{(n)}$,故 $M_4(s^{(n)})=1$.

假设序列 $u^{(n)}$ 满足 $W_H(u^{(n)})=4$.此外,令序列 $w^{(n)}$ 满足 $W_H(w^{(n)})=8$,$LC(w^{(n)})=2^{n-2}-2^{n-r}$,$2<r<m$,以及由 4 个非 0 比特分布构成的集合 $A_1=\{i,i+2^{n-2},i+2^{n-1},i+2^{n-1}+2^{n-2}\mid 0\leqslant i<2^{n-2}\}$.

(1) 若 $u^{(n)}$ 的 4 个非 0 元素属于 $w^{(n)}$ 的 8 个非 0 比特组合,但不属于 $A_1$,则存在 1 个序列 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})=2^{n-2}-2^{n-r}$,$2<r<m$,故 $M_4(s^{(n)})=2$.

(2) 若 $u^{(n)}$ 的 4 个非 0 元素不属于 $w^{(n)}$ 的 8 个非 0 比特组合,也不属于线性复杂度为 $2^{n-2}-2^{n-m}$ 的 8 个非 0 比特组合,此时不存在不同于 $u^{(n)}$ 的 $v^{(n)}$,$W_H(v^{(n)})=2$ 或 4,使得 $LC(u^{(n)}+v^{(n)})<2^{n-2}-2^{n-m}$,则保证 $LC_4(s^{(n)})=2^{n-2}-2^{n-m}$ 的 $s^{(n)}$ 的 4 -错误序列即为 $u^{(n)}$,故 $M_4(s^{(n)})=1$.证毕.

**例 2**　$m=n=5$,对情形(ⅰ),令 $s^{(n)}=(10110010101110101011101000111010)$,经验证,$e^{(n)}=$(1000 1000 1000 0000 1000 0000 0000 0000),(0000 0000 0000 1000 0000 1000 1000 1000).

**定理 3**　设 $s^{(n)}$ 满足 $LC(s^{(n)})<2^n$,$LC_4(s^{(n)})=2^{n-2}-2^{n-m}+x$,$n\geqslant 5$,$2<m<n-1$,$0<x<2^{n-m-1}$,则 $M_4(s^{(n)})=1$,2 或 $2^{m-2}$.

**证明** 令 $s^{(n)}=p^{(n)}+u^{(n)}$,其中 $LC(p^{(n)})=2^{n-2}-2^{n-m}+x$.根据引理4,merr$(p^{(n)})\geqslant 16$.故对任意 $u^{(n)}$,$W_H(u^{(n)})=0,2$ 或 $4$,$LC_4(s^{(n)})=2^{n-2}-2^{n-m}+x$.

(1) 假设 $u^{(n)}$ 满足 $W_H(u^{(n)})=2$,则 $s^{(n)}$ 的 4-错误序列即为 $u^{(n)}$,故 $M_4(s^{(n)})=1$.

(2) 假设 $u^{(n)}$ 满足 $W_H(u^{(n)})=4$,此外,令序列 $w^{(n)}$ 满足 $W_H(w^{(n)})=8$,$LC(w^{(n)})=2^{n-2}-2^{n-r}$,$2<r\leqslant m$,以及由4个非0比特分布构成的集合 $A_2=\{i,i+2^{n-2},i+2^{n-1},i+2^{n-1}+2^{n-2}\mid 0\leqslant i<2^{n-2}\}$.

(ⅰ) 若 $u^{(n)}$ 的4个非0元素属于集合 $A_2$,则存在 $\dfrac{2^{n-2}}{2^{n-m}}-1=2^{m-2}-1$ 个不同的 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})=2^{n-2}-2^{n-r}$,$2<r\leqslant m$;或取 $v^{(n)}=u^{(n)}$.故 $M_4(s^{(n)})=2^{m-2}$.

(ⅱ) 若 $u^{(n)}$ 的4个非0元素属于 $w^{(n)}$ 的8个非0比特组合,但不属于 $A_2$,则存在1个序列 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})=2^{n-2}-2^{n-r}$,$2<r\leqslant m$;或取 $v^{(n)}=u^{(n)}$.故 $M_4(s^{(n)})=2$.

(ⅲ) 若 $u^{(n)}$ 的4个非0元素不属于 $w^{(n)}$ 的8个非0比特组合,则不存在不同于 $u^{(n)}$ 的 $v^{(n)}$,$W_H(v^{(n)})=2$ 或 $4$,使得 $LC(u^{(n)}+v^{(n)})<2^{n-2}-2^{n-m}+x$,则 $s^{(n)}$ 的 4-错误序列即为 $u^{(n)}$.故 $M_4(s^{(n)})=1$.证毕.

**例3** $n=5$,$m=3$,对定理3证明中情形(2ⅱ),令 $s^{(n)}=(10110110101101101011011010110110)$,经验证,$e^{(n)}=(00100000\ 00100000\ 00100000\ 00100000)$,$(00000010\ 00000010\ 00000010\ 00000010)$.

**定理4** 设 $s^{(n)}$ 满足 $LC(s^{(n)})<2^n$,$LC_4(s^{(n)})=2^{n-1}-2^{n-m}$,$2\leqslant m\leqslant n$,则 $M_4(s^{(n)})=1,2,4$ 或 $8$.

**证明** 令 $s^{(n)}=p^{(n)}+u^{(n)}$,其中 $LC(p^{(n)})=2^{n-1}-2^{n-m}$.

对所有满足 $W_H(u^{(n)})=0$ 或 $2$ 的序列 $u^{(n)}$,存在满足 $W_H(v^{(n)})=2$ 或 $4$ 的 $v^{(n)}$,使得 $LC(u^{(n)}+v^{(n)})=2^{n-1}-2^{n-m}$,则 $LC_4(s^{(n)})<2^{n-1}-2^{n-m}$.故 $s^{(n)}$ 不存在 $W_H(s^{(n)})=2$ 的 4-错误序列.

设序列 $u^{(n)}$ 满足 $W_H(u^{(n)})=4$.先将序列分成 $2^{n-m+1}$ 个子序列,子序列中的每个元素之间的位置满足 $\{i,i+2^{n-m+1},\cdots,i+(2^{m-1}-2)\cdot 2^{n-m+1},i+(2^{m-1}-1)\cdot 2^{n-m+1}\mid 0\leqslant i\leqslant 2^{n-m+1}-1\}$.

(1) 若 $u^{(n)}$ 中有2个非0元素属于同一子序列,另外2个非0元素另属于一个子序列,但不存在2个非0元素之间的距离 $2^{n-m}(1+2a)$,$a\geqslant 0$ 或 $2^{n-1}$,则存在3个不同的序列 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})<2^{n-1}-2^{n-m}$;或取 $v^{(n)}=u^{(n)}$.故 $M_4(s^{(n)})=4$.

(2) 若 $u^{(n)}$ 中有2个非0元素属于同一子序列,另外2个非0元素另属于2个不同的子序列,且不存在2个非0元素之间的距离为 $2^{n-m}(1+2a)$,$a\geqslant 0$ 或 $2^{n-1}$,则存在1个序列 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})<2^{n-1}-2^{n-m}$;或取 $v^{(n)}=u^{(n)}$.故 $M_4(s^{(n)})=2$.

(3) 若 $u^{(n)}$ 中只有3个非0元素属于同一子序列,但不存在2个非0元素之间的距离为 $2^{n-m}(1+2a)$,$a\geqslant 0$ 或 $2^{n-1}$,则存在3个不同的序列 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})<2^{n-1}-2^{n-m}$;或取 $v^{(n)}=u^{(n)}$.故 $M_4(s^{(n)})=4$.

(4) 若 $u^{(n)}$ 中的4个非0元素均属于同一个子序列,但不存在2个非0元素之间的距离为 $2^{n-1}$,则存在 $\binom{4}{2}+1=7$ 个不同的 $v^{(n)}$,$W_H(v^{(n)})=4$,使得 $LC(u^{(n)}+v^{(n)})<2^{n-1}-2^{n-m}$;或取 $v^{(n)}=u^{(n)}$.故 $M_4(s^{(n)})=8$.

(5) 若 $u^{(n)}$ 中的4个非0元素属于4个不同的子序列,且不存在2个非0元素之间的距离为 $2^m(1+2a)$,$a\geqslant 0$,则不存在不同于 $u^{(n)}$ 的 $v^{(n)}$,$W_H(v^{(n)})=2$ 或 $4$,使得 $LC(u^{(n)}+v^{(n)})<2^{n-1}-2^{n-m}$,从而 $s^{(n)}$ 的 4-错误序列只能是 $u^{(n)}$.故 $M_4(s^{(n)})=1$.证毕.

**例4** $n=5$,$m=4$,对定理4证明中情形(3),令 $s^{(n)}=(10110000101101101000001010010110)$,经计算机验证,$M_4(s^{(n)})=4$;对定理4证明中情形(4),再令 $s^{(n)}=(10110000111000001001001011000010)$,经验证,$M_4(s^{(n)})=8$.

## 3 结语

讨论了线性复杂度小于 $2^n$ 的序列的4-错线性复杂度分布情况,对4-错线性复杂度对应的4-错误序列依次进行分析,确定了 $2^n$-周期序列 $s^{(n)}$ 的4-错线性复杂度分别为小于等于 $2^{n-3}$,$2^{n-2}-2^{n-m}$,$2^{n-2}-2^{n-m}+x$,$2^{n-1}-2^{n-m}$ 时所对应的错误序列的计数公式 $M_4(s^{(n)})$.

文献[7] 研究了关于对随机周期序列的线性复杂度和 $k$ -错线性复杂度统计性质(期望、方差的界) 的一些估计. 文献[4] 给出了 $2^n$ 周期序列的 1 -错误序列个数的期望值. 关于这方面的讨论，也可以研究线性复杂度无限制条件下 $2^n$ -周期二元序列的 $k$ -错误序列个数的统计特性.

**参考文献：**


[1] DING Cun-sheng, XIAO Guo-zhen, SHAN Wen-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 the $k$-Eerror Linear Complexity of Binary Sequences with Period $2^n$ [J]. IEEE Transactions on Information Theory, 1993, 39(4): 1 398 - 1 401.

[3] KUROSAWA K, SATO F, SAKATA T, et al. A Relationship Between Linear Complexity and $k$-Error Linear Complexity [J]. IEEE Transactions on Information Theory, 2000, 46(2): 694 - 698.

[4] 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.

[5] 李鹤龄，戚文峰. $F_p$ 上 $p^n$ -周期序列的 $k$ -错误序列 [J]. 通信学报, 2010, 31(6): 19 - 24.

[6] 周建钦. 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 [J]. 应用数学学报, 2012, 35(3).

[7] FU Fang-wei, NIEDERREITER H, SU Ming. The Characterization of $2^n$-Periodic Binary Sequences with Fixed 1-Error Linear Complexity [C]// GONG G, HELLESETH T, SONG H-Y, et al. SETA 2006, LNCS, Vol. 4 086, Springer, 2006: 88 - 103.


# On the 4-Error Sequence Distribution of $2^n$-Periodic Binary Sequences


ZHOU Jian-qin[1,2], LIU Jun[1]

(1. Telecommunication School, Hangzhou Dianzi University, Hangzhou 310018, China; 2. Computer Science School, Anhui University of Technology, Ma'anshan 243032, Anhui China)



**Abstract**: The $k$-error linear complexity of a sequence has been used as one of the important measure of keystream strength. In order to better depict and study randomicity of sequences, the $k$-error sequences ($\underline{e}$) distribution that corresponds with $LC_k(\underline{s})=LC(\underline{s}+\underline{e})$ is discussed by studying the distribution of $k$-error linear complexity of binary sequences ($\underline{s}$) with period $2^n$. Based on Games-Chan algorithm, it is proposed that the computation of $k$-error linear complexity should be converted to finding error sequences with minimal Hamming weight. For $k=4$, some the counting functions on the $k$-error sequences of $2^n$-periodic binary sequences with linear complexity less than $2^n$ are derived.



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


（责任编辑　向阳洁）