文章编号:0253-2778(2015)02-0107-05

三元 3^n 周期序列的 k 错线性复杂度的性质

唐 淼[1],开晓山[2]

(1. 安徽农业大学应用数学系,安徽合肥 230036;2. 合肥工业大学数学学院,安徽合肥 230009)

摘要:周期序列的线性复杂度和 k 错线性复杂度是衡量流密码系统的安全性能的两个重要指标.讨论了有限域 F_3 上的 3^n 周期序列的 k 错线性复杂度,得到了关于该类序列的 k 错线性复杂度和差错序列之间的一些性质.并且利用这些性质导出了一个结论,该结论显示了关于 3^n 周期序列 k 错线性复杂度的计算如何转化成关于 3^{n-1} 周期序列 k 错线性复杂度的计算,n 为任意的正整数.

关键词:流密码;周期序列;线性复杂度;k 错线性复杂度;差错序列

中图分类号:O236.2 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2015.02.003

AMS Subject Classification (2010): Primary 94A55; Secondary 94A60

引用格式: Tang Miao, Kai Xiaoshan. Some properties of the k-error linear complexity of ternary 3^n-periodic sequences[J]. Journal of University of Science and Technology of China, 2015,45(2):107-111,116.
唐淼,开晓山. 三元 3^n 周期序列的 k 错线性复杂度的性质[J]. 中国科学技术大学学报,2015,45(2):107-111,116.

Some properties of the k-error linear complexity of ternary 3^n-periodic sequences

TANG Miao[1], KAI Xiaoshan[2]

(1. *Department of Applied Mathematics, Anhui Agricultural University, Hefei* 230036, *China*;
2. *School of Mathematics, Hefei University of Technology, Hefei* 230009, *China*)

Abstract: Linear complexity and k-error linear complexity of periodic sequences are two important security indices of stream cipher systems. The k-error linear complexity of 3^n-periodic sequences over the finite field F_3 was discussed, and some of its properties and error sequences were obtained. By means of the properties, a result was presented, showing how the computation of the k-error linear complexity of a sequences with period 3^n can be reduced to the same computation for sequences with period 3^{n-1}, for any positive integer n.

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

收稿日期:2013-03-12;**修回日期**:2014-05-28

基金项目:安徽省自然科学基金(1208085MA14),安徽农业大学数学学科建设专项(2014XKJS-307)资助.

作者简介:唐淼,男,1981年生,硕士/讲师. 研究方向:编码与密码. E-mail: tangmiao@ahau.edu.cn

通讯作者:开晓山,博士/副教授. E-mail: kxs6@sina.com

0 引言

在流密码系统中,线性复杂度是一个重要的密码强度指标,为了抵抗 Berlekamp-Massey 算法的攻击,一个好的密钥序列必须具有大的线性复杂度.但是仅仅具有大的线性复杂度仍然是不够的,序列中改变几个比特就有可能导致其线性复杂度急剧下降,根据这一点,文献[1-2]中提出了序列的 k 错线性复杂度的概念(文献[1]中称之为球体复杂度).一个好的密钥序列必须不仅要具有大的线性复杂度,同时对较小的正整数 k 也要具有大的 k 错线性复杂度.

关于线性复杂度和 k 错线性复杂度的研究是流密码理论中的重要问题,国内外的学者均有大量的相关成果.其中,对于有限域 F_2 上的 2^n 周期序列,文献[3]中给出计算其线性复杂度的快速算法;而该算法在文献[1,4]中被推广到了更广泛的情形(有限域 $GF(p^m)$ 上的 p^n 周期序列).文献[2]中使用了 cost 序列作为辅助的记录工具,给出了计算有限域 F_2 上的 2^n 周期序列 k 错线性复杂度(对某个 k 值)的快速算法——Stamp-Martin 算法;而按类似的方式,有限域 $GF(p^m)$ 上的 p^n 周期序列的推广算法也被提出(见文献[1,5-6]).另外,在文献[2]的基础上,文献[7]中展示了计算有限域 F_2 上的 2^n 周期序列 k 错线性复杂度(对所有可能的 k 值而不是某一个 k 值)的算法——Lauder-Paterson 算法.文献[7]中的主要工作有:①对 Stamp-Martin 算法的步骤细节做了抽象的归纳定义,并给出了关于 k 错线性复杂度的一个结论及相应的严密证明;②以该结论为核心,设计给出了 Lauder-Paterson 算法.随后,文献[8]提出了有限域 $GF(p^m)$ 上的 p^n 周期序列的广义 Lauder-Paterson 算法.我们注意到,由于采用了不完全相同的途径,文献[8]仅推广了文献[7]中的第二部分而没有涉及第一部分.本文的目标是将文献[7]中第一部分的结论推广到更广泛的情形,并给出相应的归纳定义和结论的严密证明.有限域 F_2 上的 2^n 周期序列是有限域 $GF(p^m)$ 上的 p^n 周期序列的最特殊的情形($p=2,m=1$ 时),其他情形基本相似,且远比有限域 F_2 上的 2^n 周期序列的情形复杂.在推广的过程中,为了降低问题描述和理解的复杂程度,在本文中仅考虑其余情形中的一种——有限域 F_3 上的 3^n 周期序列,更广泛的情形与之类似.

本文讨论有限域 F_3 上的 3^n 周期序列的 k 错线性复杂度,通过引入伴随序列作为工具,得到了其 k 错线性复杂度和差错序列之间的一些性质,并利用这些性质得到一个结论,该结论展示了关于 3^n 周期序列的 k 错线性复杂度的计算如何转化为关于 3^{n-1} 周期序列的 k 错线性复杂度的计算.

1 预备知识

定义 1.1 设 s^∞ 是有限域 F_q 上的 N 周期序列,其中一个周期为 $s=(s_0,s_1,\cdots,s_{N-1})$.定义 s^∞ 的线性复杂度 $LC(s^\infty)$ 为使得 $s_i+d_1s_{i-1}+\cdots+d_ls_{i-l}=0,d_1,\cdots,d_l\in F_q$,对所有的 $i\geqslant l$ 均成立的最小的非负整数 l.特别的,$LC(s^\infty)=0$ 当且仅当 s^∞ 是零序列 $\mathbf{0}$.

定义 1.2 设 s^∞ 是有限域 F_q 上的 N 周期序列,其中一个周期为 $s=(s_0,s_1,\cdots,s_{N-1})$.定义 s^∞ 的 k 错线性复杂度 $LC_k(s^\infty)$ 为

$$\min\{LC((s+e)^\infty)\mid W_{\mathrm{H}}(e)\leqslant k\},$$

其中,$W_{\mathrm{H}}(e)$ 表示 e 的 Hamming 重量.

由于周期序列 s^∞ 可由一个周期 s 决定,为方便表示,在本文中 $s=(s_0,s_1,\cdots,s_{3^n-1})$ 既用来指代整个序列,也用来指代一个周期,将 $LC(s^\infty),LC_k(s^\infty)$ 分别简化表示 $LC(s),LC_k(s)$.另外,本文讨论的序列都是三元 3^n 周期序列 s,其元素 s_i 均属于有限域 $F_3=\{0,1,2\}$,其周期长度为 3^n,n 为任意的非负整数.

定义 1.3 设 s 是三元 3^n 周期序列,定义映射 $b^{(u)}(s)=(b^{(u)}(s)_0,\cdots,b^{(u)}(s)_{3^n-1})$,$u=0,1,2$,其中,$b^{(u)}(s)_i=\sum_{k=0}^{2-u}\binom{2-k}{u}s_{k3^{n-1}+i}$,$i=0,1,\cdots,3^{n-1}-1$.

下面的引理 1.1 展示了 3^n 周期序列 s 的线性复杂度与 3^{n-1} 周期序列 $b^{(u)}(s)$ 的线性复杂度之间的关系,$u=0,1,2$.文献[1,4]中所给出的计算 s 的线性复杂度的快速算法,其原理为递归地使用引理 1.1 直到 $n=0$.

引理 1.1[1,4] 设 s 是三元 3^n 周期序列,

① 若 $b^{(0)}(s)\neq 0$,则

$$LC(s)=LC(b^{(0)}(s))+2\cdot 3^{n-1};$$

② 若 $b^{(0)}(s)=0$ 且 $b^{(1)}(s)\neq 0$,则

$$LC(s)=LC(b^{(1)}(s))+3^{n-1};$$

③ 若 $b^{(0)}(s)=b^{(1)}(s)=0$,则

$$LC(s)=LC(b^{(2)}(s)).$$

文献[2]中为了便于计算周期序列的 k 错线性复杂度,首次提出并使用了辅助的记录工具 cost 序列. 自此,cost 序列在 k 错线性复杂度的研究中被广泛使用(见文献[4-9]). 其中,文献[7]使用了辅助工具伴随序列(cost 序列的一种变形形式),讨论了二元 2^n 周期序列 k 错线性复杂度的性质. 下面将伴随序列的定义推广到三元 3^n 周期序列上.

定义 1.4　称三维向量 $S=(s,\sigma,3^n)$ 为三元 3^n 周期序列 s 的伴随序列. 其中,3^n 为序列 s 的周期长度,$\sigma=(\sigma_{ij})$ 为 $3^n\times 3$ 矩阵,非负整数 σ_{ij} 表示将序列 s 中元素 s_i 改变为 s_i+j 所需的最小代价($0\leqslant i\leqslant 3^n-1$, $j\in F_3$).

定义 1.5　设 $S=(s,\sigma,3^n)$,称任意的一个三元 3^n 周期序列 e 为 S 的一个差错序列. 定义映射

$$T(s\to s+e)=\sum_{e_i=j}\sigma_{ij},$$

并且定义 S 的 k 错线性复杂度为

$$LC_k(S)=\min\{LC(s+e)\mid T(s\to s+e)\leqslant k\}.$$

从定义可以看出,$T(s\to s+e)$ 的值表示的是将序列 s 改变为序列 $s+e$ 所需的最小总代价. 显然,若将矩阵 σ 的初始值设为 $\sigma_{ij}=\begin{cases}0, & j=0\\ 1, & j\neq 0\end{cases}$,则 S 的 k 错线性复杂度与序列 s 的 k 错线性复杂度是等价的.

2　主要结果

定义 2.1　设 $S=(s,\sigma,3^n)$,定义映射 $B^{(u)}(S)=(B^{(u)}(s),B^{(u)}(\sigma),3^{n-1})$, $u=0,1,2$, 有

① $B^{(0)}(s)=b^{(0)}(s)$;

$$B^{(0)}(\sigma)_{ij}=\min\{\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,d_k}\mid b^{(0)}(d_0,d_1,d_2)=j\};$$

② $B^{(1)}(s)=b^{(1)}(s+a^{(1)})$,其中,$a^{(1)}$ 是满足 $B^{(0)}(s+a)=0$ 的所有序列中使得 $T(s\to s+a)$ 达到最小值的序列;

$$B^{(1)}(\sigma)_{ij}=\min\left\{\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,d_k}\;\middle|\;\begin{matrix}b^{(0)}(d_0,d_1,d_2)=-b^{(0)}(s)_i\\ b^{(1)}(d_0,d_1,d_2)=b^{(1)}(a^{(1)})_i+j\end{matrix}\right\}-\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,a^{(1)}_{k3^{n-1}+i}};$$

③ $B^{(2)}(s)=b^{(2)}(s+a^{(2)})$,其中,$a^{(2)}$ 是满足 $B^{(0)}(s+a)=B^{(1)}(s+a)=0$ 的所有序列中使得 $T(s\to s+a)$ 达到最小值的序列;

$$B^{(2)}(\sigma)_{ij}=\min\left\{\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,d_k}\;\middle|\;\begin{matrix}b^{(0)}(d_0,d_1,d_2)=-b^{(0)}(s)_i\\ b^{(1)}(d_0,d_1,d_2)=-b^{(1)}(s)_i\\ b^{(2)}(d_0,d_1,d_2)=b^{(2)}(a^{(2)})_i+j\end{matrix}\right\}-\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,a^{(2)}_{k3^{n-1}+i}}.$$

显然,$B^{(0)}(s)=0$ 当且仅当 $b^{(0)}(s)=0$,此时由于零序列 0 是满足 $b^{(0)}(s+a)=0$ 的所有序列中使得 $T(s\to s+a)$ 达到最小值的序列,所以 $B^{(1)}(s)=b^{(1)}(s)$. 类似可得,$B^{(0)}(s)=B^{(1)}(s)=0$ 当且仅当 $b^{(0)}(s)=b^{(1)}(s)=0$,并且此时 s 满足 $B^{(2)}(s)=b^{(2)}(s)$.

下面,我们给出 S,$B^{(0)}(S)$,$B^{(1)}(S)$,$B^{(2)}(S)$ 以及相应的差错序列之间满足的一些性质.

引理 2.1　设

$$S=(s,\sigma,3^n),T^{(1)}=T(s\to s+a^{(1)}).$$

对于 $B^{(1)}(S)$ 的任意一个差错序列 f,存在 S 的差错序列 e,使得

$$B^{(0)}(s+e)=0,B^{(1)}(s+e)=B^{(1)}(s)+f$$

并且

$$T(B^{(1)}(s)\to B^{(1)}(s)+f)+T^{(1)}=T(s\to s+e).$$

证明　设 $f=(f_0,f_1,\cdots,f_{3^{n-1}-1})$ 是 $B^{(1)}(S)=(B^{(1)}(s),B^{(1)}(\sigma),3^{n-1})$ 的任意一个差错序列. 对于任意的 $0\leqslant i\leqslant 3^{n-1}-1$,由于线性方程组

$$\begin{cases}\sum_{k=0}^{2}\binom{2-k}{0}(s_{k3^{n-1}+i}+e_{k3^{n-1}+i})=0\\ \sum_{k=0}^{1}\binom{2-k}{1}(-a^{(1)}_{k3^{n-1}+i}+e_{k3^{n-1}+i})=f_i\end{cases},$$

即

$$\begin{cases}e_i+e_{3^{n-1}+i}+e_{2\cdot 3^{n-1}+i}=-(s_i+s_{3^{n-1}+i}+s_{2\cdot 3^{n-1}+i})\\ 2e_i+e_{3^{n-1}+i}=f_i+(2a^{(1)}_i+a^{(1)}_{3^{n-1}+i})\end{cases}$$

有解,所以存在满足 $\begin{cases}b^{(0)}(s+e)=0\\ b^{(1)}(-a^{(1)}+e)=f\end{cases}$ 的差错序列 e. 令 $e=(e_0,e_1,\cdots,e_{3^n-1})$ 是所有这样的序列中使得 $T(s\to s+e)$ 达到最小值的序列,由于 $b^{(0)}(s+e)=0$,即 $B^{(0)}(s+e)=0$,则有

$$B^{(1)}(s+e)=b^{(1)}(s+e)=b^{(1)}(s+a^{(1)})+b^{(1)}(-a^{(1)}+e)=B^{(1)}(s)+f.$$

又由

$$T(B^{(1)}(s)\to B^{(1)}(s)+f)=\sum_{f_i=j}B^{(1)}(\sigma)_{ij}=$$

$$\sum_{i=0}^{3^{n-1}-1}\min\left\{\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,d_k}\left|\begin{array}{l}b^{(0)}(d_0,d_1,d_2)=-b^{(0)}(s)_i\\ b^{(1)}(d_0,d_1,d_2)=b^{(1)}(a^{(1)})_i+j\end{array}\right.\right\}-\sum_{i=0}^{3^{n-1}-1}\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,a^{(1)}_{k3^{n-1}+i}}=$$

$$\sum_{i=0}^{3^{n-1}-1}\min\left\{\sum_{k=0}^{2}\sigma_{k3^{n-1}+i,d_k}\left|\begin{array}{l}b^{(0)}(d_0,d_1,d_2)+b^{(0)}(s)_i=0\\ b^{(1)}(d_0,d_1,d_2)-b^{(1)}(a^{(1)})_i=f_i\end{array}\right.\right\}-T^{(1)}=$$

$$\min\left\{\sum_{i=0}^{3^n-1}\sigma_{ij}\left|\begin{array}{l}b^{(0)}(s+e)=0\\ b^{(1)}(-a^{(1)}+e)=f\end{array}\right.\right\}-T^{(1)}=T(s\to s+e)-T^{(1)},$$

可得 $T(B^{(1)}(s)\to B^{(1)}(s)+f)+T^{(1)}=T(s\to s+e)$. □

引理 2.2 设

$$S=(s,\sigma,3^n),T^{(1)}=T(s\to s+a^{(1)}).$$

对于 S 的任意一个满足 $B^{(0)}(s+e)=0$ 的差错序列 e,存在 $B^{(1)}(S)$ 的差错序列 f,使得 $B^{(1)}(s+e)=B^{(1)}(s)+f$ 并且

$$T(B^{(1)}(s)\to B^{(1)}(s)+f)+T^{(1)}\leqslant T(s\to s+e).$$

证明 设 $e=(e_0,e_1,\cdots,e_{3^n-1})$ 是 S 的任意一个满足 $B^{(0)}(s+e)=0$ 的差错序列,则 $b^{(0)}(s+e)=0$. 令 $f=b^{(1)}(-a^{(1)}+e)$,则有

$$B^{(1)}(s+e)=b^{(1)}(s+e)=$$

$$b^{(1)}(s+a^{(1)})+b^{(1)}(-a^{(1)}+e)=B^{(1)}(s)+f.$$

由引理 2.1 中证明可知,若 e 是所有满足 $\begin{cases}b^{(0)}(s+e)=0\\ b^{(1)}(-a^{(1)}+e)=f\end{cases}$ 的所有序列中使得 $T(s\to s+e)$ 达到最小值的序列,则有

$$T(s\to s+e)=T(B^{(1)}(s)\to B^{(1)}(s)+f)+T^{(1)};$$

但显然 e 不一定满足这一点,所以易得

$$T(s\to s+e)\geqslant T(B^{(1)}(s)\to B^{(1)}(s)+f)+T^{(1)}.$$ □

类似上述结论的推导过程,S 与 $B^{(0)}(S)$ 或 $B^{(2)}(S)$ 的情形可得.

引理 2.3 设 $S=(s,\sigma,3^n)$. 对于 $B^{(0)}(S)$ 的任意一个差错序列 f,存在 S 的差错序列 e,使得 $B^{(0)}(s+e)=B^{(0)}(s)+f$ 并且

$$T(B^{(0)}(s)\to B^{(0)}(s)+f)=T(s\to s+e).$$

引理 2.4 设 $S=(s,\sigma,3^n)$. 对于 S 的任意一个差错向量 e,存在 $B^{(0)}(S)$ 的差错向量 f,使得 $B^{(0)}(s+e)=B^{(0)}(s)+f$ 并且

$$T(B^{(0)}(s)\to B^{(0)}(s)+f)\leqslant T(s\to s+e).$$

引理 2.5 设

$$S=(s,\sigma,3^n),T^{(2)}=T(s\to s+a^{(2)}).$$

对于 $B^{(2)}(S)$ 的任意一个差错序列 f,存在 S 的差错序列 e,使得 $B^{(0)}(s+e)=B^{(1)}(s+e)=0$, $B^{(2)}(s+e)=B^{(2)}(s)+f$ 并且

$$T(B^{(2)}(s)\to B^{(2)}(s)+f)+T^{(2)}=T(s\to s+e).$$

引理 2.6 设

$$S=(s,\sigma,3^n),T^{(2)}=T(s\to s+a^{(2)}).$$

对于 S 的任意一个满足 $B^{(0)}(s+e)=B^{(1)}(s+e)=0$ 的差错序列 e,存在 $B^{(2)}(S)$ 的差错向量 f,使得 $B^{(2)}(s+e)=B^{(2)}(s)+f$,并且

$$T(B^{(2)}(s)\to B^{(2)}(s)+f)+T^{(2)}=T(s\to s+e).$$

注意,在引理 2.6 中,

$$T(B^{(2)}(s)\to B^{(2)}(s)+f)+T^{(2)}=T(s\to s+e)$$

是等式,而不是类似引理 2.2 及引理 2.4 中的不等式. 因为此时,对于任意的 $0\leqslant i\leqslant 3^{n-1}-1$,由于线性方程组

$$\begin{cases}\sum_{k=0}^{2}\binom{2-k}{0}(s_{k3^{n-1}+i}+e_{k3^{n-1}+i})=0\\ \sum_{k=0}^{1}\binom{2-k}{1}(s_{k3^{n-1}+i}+e_{k3^{n-1}+i})=0\\ \sum_{k=0}^{0}\binom{2-k}{2}(-a^{(2)}_{k3^{n-1}+i}+e_{k3^{n-1}+i})=f_i\end{cases},$$

即

$$\begin{cases}e_i+e_{3^{n-1}+i}+e_{2\cdot 3^{n-1}+i}=-(s_i+s_{3^{n-1}+i}+s_{2\cdot 3^{n-1}+i})\\ 2e_i+e_{3^{n-1}+i}=-(2s_i+s_{3^{n-1}+i})\\ e_i=f_i+a^{(2)}_i\end{cases}$$

有且仅有唯一解,所以满足

$$\begin{cases}b^{(0)}(s+e)=0\\ b^{(1)}(s+e)=0\\ b^{(2)}(-a^{(2)}+e)=f\end{cases}$$

的差错序列 e 是存在并且唯一的.

利用上述性质,我们可以得到一个与引理 1.1 形似的结论,该结论展示了关于 3^n 周期序列的 k 错线性复杂度的计算如何转化成关于 3^{n-1} 周期序列的

k 错线性复杂度的计算，$n\geqslant 1$.

定理 2.1　设 $S=(s,\sigma,3^n)$ 为三元 3^n 周期序列 s 的伴随序列，

$$T^{(1)}=T(s\to s+a^{(1)}),$$
$$T^{(2)}=T(s\to s+a^{(2)}),k\geqslant 0,$$

① 若 $0\leqslant k<T^{(1)}$，则

$$LC_k(S)=LC_k(B^{(0)}(S))+2\cdot 3^{n-1};$$

② 若 $T^{(1)}\leqslant k<T^{(2)}$，则

$$LC_k(S)=LC_{k-T^{(1)}}(B^{(1)}(S))+3^{n-1};$$

③ 若 $T^{(2)}\leqslant k$，则 $LC_k(S)=LC_{k-T^{(2)}}(B^{(2)}(S))$.

证明　②先证

$$LC_k(S)\leqslant LC_{k-T^{(1)}}(B^{(1)}(S))+3^{n-1}.$$

设 f 是 $B^{(1)}(S)=(B^{(1)}(s),B^{(1)}(\sigma),3^{n-1})$ 的满足 $LC(B^{(1)}(s)+f)=LC_{k-T^{(1)}}(B^{(1)}(S))$ 和 $T(B^{(1)}(s)\to B^{(1)}(s)+f)\leqslant k-T^{(1)}$ 的一个差错向量. 由引理 2.1 可知存在 S 的差错向量 e，满足 $B^{(0)}(s+e)=0$，$B^{(1)}(s+e)=B^{(1)}(s)+f$ 和

$$T(s\to s+e)=T(B^{(1)}(s)\to B^{(1)}(s)+f)+T^{(1)}\leqslant (k-T^{(1)})+T^{(1)}=k.$$

又由引理 1.1 可得，

$$LC(s+e)=LC(b^{(1)}(s+e))+3^{n-1}=LC(B^{(1)}(s+e))+3^{n-1}=LC(B^{(1)}(s)+f)+3^{n-1}=LC_k(B^{(1)}(S))+3^{n-1},$$

所以 $LC_k(S)\leqslant LC_{k-T^{(1)}}(B^{(1)}(S))+3^{n-1}$.

再证 $LC_k(S)\geqslant LC_{k-T^{(1)}}(B^{(1)}(S))+3^{n-1}$. 设 e 是 $S=(s,\sigma,3^n)$ 的差错向量且满足

$$LC(s+e)=LC_k(S),\ T(s\to s+e)\leqslant k.$$

假设 $B^{(0)}(s+e)\neq 0$，则 $b^{(0)}(s+e)\neq 0$，则由引理 1.1 可知 $LC(s+e)>2\cdot 3^{n-1}$；但是注意到向量 $a^{(1)}$ 满足 $B^{(0)}(s+a^{(1)})=0$，则 $b^{(0)}(s+a^{(1)})=0$，由引理 1.1 可知 $LC(s+a^{(1)})\leqslant 2\cdot 3^{n-1}$；又由于 $T(s\to s+a^{(1)})=T^{(1)}\leqslant k$，可得 $LC(s+e)\leqslant 2\cdot 3^{n-1}$. 两者矛盾，假设不成立，所以向量 e 必然满足 $B^{(0)}(s+e)=0$.

由引理 2.2 可知存在 $B^{(1)}(S)$ 的差错向量 f，满足 $B^{(1)}(s+e)=B^{(1)}(s)+f$ 和

$$T(B^{(1)}(s)\to B^{(1)}(s)+f)\leqslant T(s\to s+e)-T^{(1)}\leqslant k-T^{(1)}.$$

又由引理 1.1 可得，

$$LC(B^{(1)}(s)+f)=LC(B^{(1)}(s+e))=LC(b^{(1)}(s+e))=LC(s+e)-3^{n-1}=LC_k(S)-3^{n-1},$$

即 $LC_k(S)=LC(B^{(1)}(s)+f)+3^{n-1}$，所以

$$LC_k(S)\geqslant LC_{k-T^{(1)}}(B^{(1)}(S))+3^{n-1}.$$

综上可得，$LC_k(S)=LC_{k-T^{(1)}}(B^{(1)}(S))+3^{n-1}$.

定理中的另外两个结论①，③同理可证(由引理 2.3～2.6 和引理 1.1). □

下面，用一个例子来演示定理 2.1 的应用.

例 2.1　设 $S=(s,\sigma,9)$，其中，$s=(200110120)$，

$$\sigma=\begin{bmatrix}0&0&0&0&0&0&0&0&0\\1&1&1&1&1&1&1&1&1\\1&1&1&1&1&1&1&1&1\end{bmatrix}^{\mathrm{T}}.$$

当 $k=4$ 时，用定理 2.1 来计算 S 的 k 错线性复杂度.

解　对于 S，有

$$a^{(1)}=(200000000),T^{(1)}=1;$$
$$a^{(2)}=(200020010),T^{(2)}=3.$$

由 $4>T^{(2)}$ 可得

$$LC_4(S)=LC_1(B^{(2)}(S)),$$

其中，$B^{(2)}(S)=((100),\begin{bmatrix}0&0&0\\1&0&3\\2&0&3\end{bmatrix}^{\mathrm{T}},3)$.

对于 $\underline{S}=B^{(2)}(S)$，有

$$a^{(1)}=(020),T^{(1)}=0;$$
$$a^{(2)}=(200),T^{(2)}=2.$$

由 $T^{(1)}<1<T^{(2)}$ 可得

$$LC_1(\underline{S})=LC_1(B^{(1)}(\underline{S}))+3^{1-1}=LC_1(B^{(1)}(\underline{S}))+1,$$

其中，$B^{(1)}(\underline{S})=((1),\begin{bmatrix}0\\1\\2\end{bmatrix}^{\mathrm{T}},1)$.

对于 $\underline{S}=B^{(1)}(\underline{S})$，将 $\underline{s}_0=1$ 转化为 0 最少需要的 bit 数为 $\underline{e}_{0,2}=2>1$，则 $LC_1(\underline{S})=1$；所以，$LC_4(S)=2$. □

参考文献(References)

[1] Ding C S, Xiao G Z, Shan W J. The Stability Theory of Stream Ciphers [M]. Berlin: Springer-Verlag, 1991: Chapter 5.

[2] Stamp M, Martin C F. An algorithm for the k-error linear complexity of binary sequences with period 2^n [J]. IEEE Transactions on Information Theory, 1993, 39(4): 1 398-1 401.

(下转第 116 页)