第48卷第2期 中国科学技术大学学报 Vol.48,No.2
2018年2月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Feb. 2018

文章编号:0253-2778(2018)02-0105-06

一个计算指数周期序列的所有跃点的算法

唐 森[1],王菊香[2]

(1.安徽农业大学应用数学系,安徽合肥 230036;2.安徽建筑大学数理学院,安徽合肥 230601)

摘要:周期序列的 k 错线性复杂度是衡量流密码系统安全性能的一个重要指标,k 错线性复杂度的值随着 k 值的增加呈下降趋势,其中发生严格下降的点称为跃点.这里关注有限域 $GF(p^m)$ 上的 p^n 周期序列,p 是任意素数,讨论了该类序列的 k 错线性复杂度的性质,同时给出了一个算法:对于任意给定的序列,计算出其包含的所有跃点.

关键词:流密码;周期序列;k 错线性复杂度;跃点

中图分类号:O236.2;TN918.1 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2018.02.003

2010 Mathematics Subject Classification: Primary 94A55; Secondary 94A60

引用格式:唐森,王菊香. 一个计算指数周期序列的所有跃点的算法[J]. 中国科学技术大学学报,2018,48(2):105-110.

TANG Miao, WANG Juxiang. An algorithm for computing all the critical points of exponent periodic sequences[J]. Journal of University of Science and Technology of China, 2018,48(2):105-110.

An algorithm for computing all the critical points of exponent periodic sequences

TANG Miao[1], WANG Juxiang[2]

(1. *Department of Applied Mathematics, Anhui Agricultural University, Hefei* 230036, *China*;
2. *School of Mathematics and Physics, Anhui Jianzhu University, Hefei* 230601, *China*)

Abstract: The k-error linear complexity of periodic sequences is an important security indice of stream cipher systems. The k-error linear complexity decreases as the number of errors k increases, that the critical points are those where a decrease occurs in the k-error linear complexity. The p^n periodic sequences over the finite field $GF(p^m)$ were focused upon, where p is a prime. Some properties of the k-error linear complexity were discussed, and an algorithm was presented for computing all the critical points for a given sequence.

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

0 引言

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.特别地,$LC(s^\infty)=0$ 当且仅当 s^∞ 是零序列 0.

在流密码系统中,线性复杂度是一个重要的密

收稿日期:2016-08-24;**修回日期**:2017-11-22

基金项目:安徽省高校自然科学研究项目重点项目(KJ2017A136),安徽省高校优秀青年人才支持计划重点项目(gxyqZD2016032),安徽省教育厅自然科学基金一般项目(KJ2015JD18)资助.

作者简介:唐森(通讯作者),男,1981年生,硕士/副教授.研究方向:编码与密码.E-mail:tangmiao@ahau.edu.cn

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.关于计算线性复杂度的算法在国内外被广泛研究，其中，文献[1]给出计算有限域 F_2 上的 2^n 周期序列线性复杂度的快速算法(Games-Chan 算法).然而，文献[2,3]发现序列仅仅具有大的线性复杂度仍然是不够的，往往几个比特的改变就有可能导致其线性复杂度急剧下降.由此，序列的 k 错线性复杂度的概念被提出，一个好的密钥序列既要具有较高的线性复杂度，也要具有较高的 k 错线性复杂度(至少对较小的正整数 k).

文献[3]首次使用了辅助的记录工具 cost 序列，给出了计算有限域 F_2 上的 2^n 周期序列的 k 错线性复杂度的快速算法(Stamp-Martin 算法).此后，cost 序列作为工具在 k 错线性复杂度的研究中被广泛使用[4-15]，而文献[1,3]的算法也在文献[2,4]中被推广到了指数周期序列的情形，即有限域 $GF(p^m)$ 上的 p^n 周期序列.文献[5]使用了辅助工具——伴随序列(cost 序列的一种变形形式)，给出了计算有限域 F_2 上的 2^n 周期序列的所有跃点的算法(Lauder-Paterson 算法).对于有限域 $GF(p^m)$ 上的 p^n 周期序列，文献[6]推广了 Lauder-Paterson 算法，给出了计算序列所有跃点的一个算法.关于周期序列的 k 错线性复杂度、跃点等的研究还有很多[7-15]，其中，文献[15]讨论了有限域 $GF(p^m)$ 上的 p^n 周期序列(在 $p=3, m=1$ 的特殊情形下)的 k 错线性复杂度的性质.本文在文献[15]的基础上，将研究范围拓展到了有限域 $GF(p^m)$ 上的 p^n 周期序列的一般情形，给出了一个计算序列所有跃点的新算法，新算法使用了更接近 Lauder-Paterson 算法[5]的结构，比 Kaida 算法[6]具有更好的计算复杂度.

1 预备知识

设 α 是有限域 $GF(p^m)$ 的一个本原元，其中 p 是任意素数，则有限域 $GF(p^m)$ 可表示为

$$GF(p^m)=\{\alpha_0,\alpha_1,\cdots,\alpha_{p^m-1}\},$$

其中，$\alpha_0=0$，$\alpha_h=\alpha^{h-1}$，$1\leqslant h\leqslant p^m-1$.本文讨论的序列 s^∞ 中的元素 s_i 均属于 $GF(p^m)$，周期长度为 p^n，其中 m 为任意的正整数，n 为任意的非负整数.

定义 1.1 设 s^∞ 是有限域 $GF(p^m)$ 上的 p^n 周期序列，其中一个周期为 $s=(s_0,s_1,\cdots,s_{p^n-1})$.定义 s^∞ 的 k 错线性复杂度

$$LC_k(s^\infty)=\min\{LC((s+e)^\infty)\mid W_H(e)\leqslant k\},$$

其中，$W_H(e)$ 表示 e 的 Hamming 重量.

定义 1.2 设 s^∞ 是有限域 $GF(p^m)$ 上的 p^n 周期序列，其中一个周期为 $s=(s_0,s_1,\cdots,s_{p^n-1})$.对于任意的 $k\in[0,p^n]$，若 $LC_l(s^\infty)>LC_k(s^\infty)$ 对于所有的 $0\leqslant l<k$ 都成立，则称点对 $(k,LC_k(s^\infty))$ 为序列 s 的一个跃点.

由于周期序列 s^∞ 可由一个周期 s 决定，为了便于表述，在本文中 $s=(s_0,s_1,\cdots,s_{p^n-1})$ 既用来指代整个序列，同时也用来指代一个周期，将 $LC(s^\infty)$，$LC_k(s^\infty)$ 分别简化表示为 $LC(s)$，$LC_k(s)$.

引理 1.1[2,4] 设 s 是有限域 $GF(p^m)$ 上的 p^n 周期序列，定义映射 $b^{(u)}(s)=(b^{(u)}(s)_0,\cdots,b^{(u)}(s)_{p^{n-1}-1})$，$u=0,1,\cdots,p-1$，其中，

$$b^{(u)}(s)_i=\sum_{k=0}^{p-u-1}\binom{p-k-1}{u}s_{kp^{n-1}+i},$$

① 若 u 是使得 $b^{(u)}(s)\neq 0$ 成立的最小整数，$0\leqslant u\leqslant p-2$，则

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

② 若 $b^{(u)}(s)=0$ 对所有的整数 $0\leqslant u\leqslant p-2$ 成立，则 $LC(s)=LC(b^{(p-1)}(s))$.

引理 1.1 展示了 p^n 周期序列 s 的线性复杂度与 p^{n-1} 周期序列 $b^{(u)}(s)$ 的线性复杂度之间的关系，$u=0,1,\cdots,p-1$.文献[2,4]中采用递归的方式使用引理 1.1，给出了计算 s 的线性复杂度的快速算法.文献[5]对二元 2^n 周期序列定义了伴随序列，下面将该定义推广到有限域 $GF(p^m)$ 上的 p^n 周期序列上.

定义 1.3 称三维向量 $S=(s,\sigma,p^n)$ 为有限域 $GF(p^m)$ 上的 p^n 周期序列 s 的伴随序列.其中，p^n 为序列 s 的周期长度，$\sigma=(\sigma_{ij})$ 为 $p^n\times p^m$ 矩阵，非负整数 σ_{ij} 表示将序列 s 中元素 s_i 改变为 α_j 所需的最小代价($0\leqslant i\leqslant p^n-1$，$\alpha_j\in GF(p^m)$).

定义 1.4 设 e 是任意的一个有限域 $GF(p^m)$ 上的 p^n 周期序列，定义映射

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

并且定义 S 的 k 错线性复杂度为

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

定义 1.5 设 $S=(s,\sigma,p^n)$.对于任意的 $k\in[0,p^n]$，若 $LC_l(S)>LC_k(S)$ 对于所有的 $0\leqslant l<k$ 都成立，则称点对 $(k,LC_k(S))$ 为序列 S 的一个跃点.

在上述定义中，$T(s\to s+e)$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 $\sigma_{ij}=\begin{cases}0, s_i=\alpha_j;\\ 1, s_i\neq\alpha_j,\end{cases}$ 则伴随序列 S 的 k 错线性复杂度 $LC_k(S)$ 与序列 s 的 k 错线性复杂度 $LC_k(s)$ 是等价的，伴随序列 S 的跃点 $(k, LC_k(S))$ 与序列 s 的跃点 $(k, LC_k(s))$ 也是等价的.

文献[15]在 $p=3, m=1$ 的特殊情形下讨论了有限域 $GF(p^m)$ 上的 p^n 周期序列，对序列 S 的 k 错线性复杂度与序列 $b^{(u)}(S)$ 的 k 错线性复杂度之间的分解关系做了严谨的数学证明，$u=0,1,\cdots,p-1$.本文的目标是将该结论推广到有限域 $GF(p^m)$ 上的 p^n 周期序列的一般情形，用映射的方式刻画序列按周期长度由大到小迭代分解的过程，并表示出序列的跃点在两者之间的分解和对应的关系式；然后，借助该关系式和 Lauder-Paterson 算法[5]的结构，给出计算序列所有跃点的新算法.

2　主要结果

定义 2.1　设 $S=(s,\sigma,p^n)$，定义映射 $B^{(u)}(S)=(B^{(u)}(s),B^{(u)}(\sigma),p^{n-1})$，$u=0,1,\cdots,p-1$，其中各分量按下列规则计算：

① $B^{(0)}(s)=b^{(0)}(s)$，

$$B^{(0)}(\sigma)_{ij}=\min\left\{\sum_{k=0}^{p-1}\sigma_{kp^{n-1}+i,l}\ \middle|\ b^{(0)}(d_0,\cdots,d_{p-1})=\alpha_j,\ d_k=\alpha_l, k=0,\cdots,p-1\right\};$$

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

$$B^{(u)}(\sigma)_{ij}=\min\left\{\sum_{k=0}^{p-1}\sigma_{kp^{n-1}+i,l}\ \middle|\ \begin{array}{c}b^{(r)}(d_0,\cdots,d_{p-1})=0, r=0,\cdots,u-1,\\ b^{(u)}(d_0,\cdots,d_{p-1})=\alpha_j,\\ d_k=\alpha_l, k=0,\cdots,p-1\end{array}\right\}-\sum_{\substack{k=0,\\ tk\,p^{n-1}+i=\alpha_l}}^{p-1}\sigma_{kp^{n-1}+i,l}.$$

由文献[15，定理 2.1]的证明过程可看出，按相似的方式易将其推广到有限域 $GF(p^m)$ 上的 p^n 周期序列的一般情形，下面我们不加证明地给出该推广结论.

引理 2.1　设 $S=(s,\sigma,p^n)$ 为有限域 $GF(p^m)$ 上的 p^n 周期序列 s 的伴随序列，$T^{(u)}=T(s\to t^{(u)})$，$u=1,\cdots,p-1$，

① 若 $0\leqslant k<T^{(1)}$，则

$LC_k(S)=LC_k(B^{(0)}(S))+(p-1)p^{n-1}$；

②若 $T^{(u)}\leqslant k<T^{(u+1)}$，$u=1,\cdots,p-2$，则

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

③若 $T^{(p-1)}\leqslant k$，则

$LC_k(S)=LC_{k-T^{(p-1)}}(B^{(p-1)}(S))$.

由引理 2.1，序列 S 的跃点可由序列 $B^{(u)}(S)$ 的跃点表示，$u=0,1,\cdots,p-1$，而关于序列 S 的全体跃点的计算同样可以转化为关于序列 $B^{(u)}(S)$ 跃点的计算.

引理 2.2　设 $S=(s,\sigma,p^n)$，

$T^{(u)}=T(s\to t^{(u)})$，$u=1,\cdots,p-1$，

① 若 $LC_k(S)>(p-1)p^{n-1}$，则 $(k,LC_k(S))$ 是 S 的一个跃点当且仅当 $(k', LC_{k'}(B^{(0)}(S)))$ 是 $B^{(0)}(S)$ 的一个跃点，其中

$LC_k(S)=LC_{k'}(B^{(0)}(S))+(p-1)p^{n-1}, k=k'$；

②若

$(p-u-1)p^{n-1}<LC_k(S)\leqslant(p-u)p^{n-1}$，

则 $(k,LC_k(S))$ 是 S 的一个跃点当且仅当 $(k', LC_{k'}(B^{(u)}(S)))$ 是 $B^{(u)}(S)$ 的一个跃点，其中 $LC_k(S)=LC_{k'}(B^{(u)}(S))+(p-u-1)p^{n-1}, k=k'+T^{(u)}$，$u=1,\cdots,p-2$；

③若 $0\leqslant LC_k(S)\leqslant p^{n-1}$，则 $(k,LC_k(S))$ 是 $B^{(u)}(S)$ 的一个跃点当且仅当 $(k', LC_{k'}(B^{(p-1)}(S)))$ 是 $B^{(p-1)}(S)$ 的一个跃点，其中

$LC_k(S)=LC_{k'}(B^{(p-1)}(S))$，$k=k'+T^{(p-1)}$.

算法 2.1　计算序列 s 所有的跃点的算法

```
Input:S=(s,σ,p^n),lb,ub,LC
CPs(S,lb,ub,LC)
{if n>0 then
  calculated T^(u),u=1,…,p-1,
  let u1 be the least number such that T^(u)>0,
  if u1≤p-1 then
    CPs(B^(u1-1)(S),lb,min{ub,lb+T^(u1)-1},LC+(p-u1)p^(n-1))
    for u2=u1 to p-2 do
```

if $T^{(u_2)}<T^{(u_2+1)}$ and $lb+T^{(u_2)}\leqslant ub$ then

CPs($B^{(u_2)}$(S), $lb+T^{(u_2)}$, min{ub, $lb+T^{(u_2+1)}-1$}, $LC+(p-u_2-1)p^{n-1}$)

if $u_1=p-1$ then

CPs($B^{(p-2)}$(S), lb, min{ub, $lb+T^{(p-1)}-1$}, $LC+p^{n-1}$)

if $lb+T^{(p-1)}\leqslant ub$ then

CPs($B^{(p-1)}$(S), $lb+T^{(p-1)}$, ub, LC)

else * n=0 *\

if $s_0=0$ then Output(lb, LC)

if $s_0\neq 0$ and $\sigma_{00}>0$ then Output(lb, LC+1)

if $s_0\neq 0$ and $lb+\sigma_{00}\leqslant ub$ then Output($lb+\sigma_{00}$, LC)}

定理 2.1 设$(k, LC_k(S))$是序列 $S=(s,\sigma,p^n)$的满足 $k\in[0, ub-lb]$的任意一个跃点，$lb\leqslant ub$，则算法 2.1 中的程序 $CPs(S, lb, ub, LC)$会输出相应的点对$(lb+k, LC+LC_k(S))$.

证明 用数学归纳法证明.当 $n=0$ 时，显然序列 $s=s_0$，若 $s_0=0$，则 S 只有一个跃点(0,0)，而程序 CPs 输出(lb, LC)与之对应.若 $s_0\neq 0$ 且 $\sigma_{00}=0$，显然 $lb+\sigma_{00}\leqslant ub$，此时 S 同样只有一个跃点(0,0)，而程序 CPs 输出(lb, LC)与之对应.若 $s_0\neq 0$ 且 $\sigma_{00}>0$，则 S 有两个跃点(0,1)和$(\sigma_{00}, 0)$，显然 $0\in[0, ub-lb]$，程序 CPs 输出$(lb, LC+1)$与(0,1)对应；当 $\sigma_{00}\in[0, ub-lb]$时，即 $lb+\sigma_{00}\leqslant ub$ 时，程序 CPs 输出$(lb+\sigma_{00}, LC)$与$(\sigma_{00}, 0)$对应.

假设结论在 $n-1$ 时成立，现在我们来讨论 n 时的情形.显然 $0\leqslant T^{(1)}\leqslant\cdots\leqslant T^{(p-1)}$，不妨设 u_1 是使得 $T^{(u)}>0$ 成立的最小值，若 u_1 存在则有 $1\leqslant u_1\leqslant p-1$，若 u_1 不存在则 $T^{(p-1)}=0$，则有 $lb+T^{(p-1)}\leqslant ub$，因此，程序 $CPs(S, lb, ub, LC)$必有子程序可以运行.下面讨论子程序的情况：

若 $1\leqslant u_1\leqslant p-2$，由归纳假设可知，子程序

$$CPs(B^{(u_1-1)}(S), lb, \min\{ub, lb+T^{(u_1)}-1\}, LC+(p-u_1)p^{n-1})$$

输出对应的所有跃点$(lb+k', LC+(p-u_1)p^{n-1}+LC_{k'}(B^{(u_1-1)}(S)))$，其中$(k', LC_{k'}(B^{(u_1-1)}(S)))$是 $B^{(u_1-1)}(S))$的任一满足 $k'\in[0, \min\{ub-lb, T^{(u_1)}-1\}]$的跃点.由引理 2.2，该子程序输出的点可对应到所有 S 的满足 $k=k'\in[0, \min\{ub-lb, T^{(u_1)}-1\}]$跃点$(k, LC_k(S))$.对每一个满足 $T^{(u_2)}<T^{(u_2+1)}$ 和 $lb+T^{(u_2)}\leqslant ub$ 的 $u_2, u_1\leqslant u_2\leqslant p-2$，由归纳假设可知，子程序

$$CPs(B^{(u_2)}(S), lb+T^{(u_2)}, \min\{ub, lb+T^{(u_2+1)}-1\}, LC+(p-u_2-1)p^{n-1})$$

输出对应的所有跃点

$$(lb+T^{(u_2)}+k', LC+(p-u_2-1)p^{n-1}+LC_{k'}(B^{(u_2)}(S))),$$

其中$(k', LC_{k'}(B^{(u_2-1)}(S)))$是 $B^{(u_2-1)}(S))$的任一满足 $k'\in[0, \min\{ub-(lb+T^{(u_2)}), T^{(u_2+1)}-T^{(u_2)}-1\}]$的跃点.由引理 2.2，该子程序输出的点可对应到所有 S 的满足

$$k=k'+T^{(u_2)}\in[T^{(u_2)}, \min\{ub-lb, T^{(u_2+1)}-1\}]$$

的跃点$(k, LC_k(S))$，$u_1\leqslant u_2\leqslant p-2$.

若 $u_1=p-1$，由归纳假设可知，子程序

$$CPs(B^{(p-2)}(S), lb, \min\{ub, lb+T^{(p-1)}-1\}, LC+p^{n-1})$$

输出对应的所有跃点$(lb+k', LC+p^{n-1}+LC_{k'}(B^{(p-2)}(S)))$，其中$(k', LC_{k'}(B^{(p-2)}(S)))$是 $B^{(p-2)}(S))$的任一满足 $k'\in[0, \min\{ub-lb, T^{(p-1)}-1\}]$的跃点.由引理 2.2，该子程序输出的点可对应到所有 S 的满足 $k=k'\in[0, \min\{ub-lb, T^{(p-1)}-1\}]$跃点$(k, LC_k(S))$.

若 $lb+T^{(p-1)}\leqslant ub$，由归纳假设可知，子程序

$$CPs(B^{(p-1)}(S), lb+T^{(p-1)}, ub, LC)$$

输出对应的所有跃点$(lb+T^{(p-1)}+k', LC+LC_{k'}(B^{(p-1)}(S)))$，其中$(k', LC_{k'}(B^{(p-1)}(S)))$是 $B^{(p-1)}(S))$的任一满足 $k'\in[0, ub-(lb+T^{(p-1)})]$的跃点.由引理 2.2，该子程序输出的点可对应到所有 S 的满足 $k=k'+T^{(p-1)}\in[T^{(p-1)}, ub-lb]$跃点$(k, LC_k(S))$.

综上可得，程序 $CPs(S, lb, ub, LC)$输出的点对$(lb+k, LC+LC_k(S))$可对应到所有 S 的满足 $k\in[0, ub-lb]$的跃点$(k, LC_k(S))$.

定理 2.2 设 s 是有限域 $GF(p^m)$上的 p^n 周期序列.在算法 2.1 中输入 $S=(s,\sigma,p^n)$，$lb=0$，$ub=p^n$，$LC=0$，则程序 $CPs(S, 0, p^n, 0)$会输出序列 s 的所有的跃点，其中 $\sigma_{ij}=\begin{cases}0, s_i=\alpha_j;\\ 1, s_i\neq\alpha_j;\end{cases}0\leqslant i\leqslant p^n-1$，$0\leqslant j\leqslant p^m-1$.

证明 将矩阵 σ 的初始值设为 $\sigma_{ij}=\begin{cases}0, s_i=\alpha_j;\\ 1, s_i\neq\alpha_j;\end{cases}$ $0\leqslant i\leqslant p^n-1$，$0\leqslant j\leqslant p^m-1$，则伴随序列 S 的跃点

$(k,LC_k(S))$与序列 s 的跃点$(k,LC_k(s))$是等价的.由定理 2.1,$CPs(S,0,p^n,0)$可输出序列 s 的满足$k\in[0,p^n]$所有的跃点,也就是序列 s 包含的所有跃点.

3　复杂度分析与算法实例

Kaida 讨论了算法的计算复杂度[6],现在我们做一个类似的讨论,从计算复杂度的角度比较新算法与 Kaida 算法.考虑算法运行过程中某一级子程序 $CPs(S,lb,ub,LC)$的执行过程,此时 $S=(s,\sigma,p^{l+1})$是长为 p^{l+1}的序列,$l=p-1,\cdots,0$,我们需要计算 $p-1$ 个 $T^{(u)}$ 和不超过 p 个 $B^{(u)}(S)=(B^{(u)}(s),B^{(u)}(\sigma),L)$,$L=p^l$.其中,每一个 $T^{(u)}$,$u=1,\cdots,p-1$,需要 $L\cdot p^{m(p-u)}\cdot p$ 次 $GF(p^m)$上的加法运算,计算 $p-1$ 个 $T^{(u)}$共需要

$$\sum_{u=1}^{p-1}L\cdot p^{m(p-u)}\cdot p=L\cdot p\cdot\frac{p^m-p^{pm}}{1-p^m}\approx Lp^{(p-1)m+1}$$

次加法运算;每一个 $B^{(u)}(s)$需要 $L\cdot p$ 次加法运算,而每一个 $B^{(u)}(\sigma)=(\sigma_{ij})_{L\times p^m}$ 需要 $L\cdot p^m\cdot p$ 次加法运算,计算 $B^{(u)}(S)$共需要不超过 $p(Lp+Lp^{m+1})$次加法运算.因此,该子程序向下执行一级约需要 $Lp^{m(p-1)+1}$ 次 $GF(p^m)$上的加法运算,而 Kaida 算法执行类似的部分约需要 $Lp^{m(p+1)+2}$ 次 $GF(p^m)$上的加法运算,新算法比 Kaida 算法具有更好的计算复杂度.

下面,用一个具体的例子展示算法 2.1 的执行过程.为了降低该执行过程描述和理解的复杂程度,例中使用的有限域 $GF(p^m)$上的 p^n 周期序列是 $p=3,m=1$ 时的情形.

例 3.1　设序列 $s=(200110120)^\infty$,计算序列 s 所有的跃点.

解　在算法 2.1 中输入 $S=(s,\sigma,9)$,$lb=0$,$ub=9$,$LC=0$,其中 $s=(200110120)$,而

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

则程序的执行过程如下,按标号由小到大的顺序执行,其中上标 T 表示矩阵的转置.

$n=2$:

① $CPs(S,0,9,0)$

$T^{(1)}=1,T^{(2)}=3,u_1=1,$

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

$$B^{(1)}(S)=((210),\begin{bmatrix}0&2&0\\0&0&2\\0&2&2\end{bmatrix}^{\mathrm{T}},3),$$

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

$n=1$:

②$CPs(B^{(0)}(S),0,0,6)$

$T^{(1)}=1,T^{(2)}=1,u_1=1,$

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

④ $CPs(B^{(1)}(S),1,2,3)$

$T^{(1)}=0,T^{(2)}=2,u_1=2,$

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

⑥ $CPs(B^{(2)}(S),3,9,0)$

$T^{(1)}=0,T^{(2)}=2,u_1=2,$

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

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

$n=0$:

③$CPs(B^{(0)}(S),0,0,8)$　Output(0,9).

⑤ $CPs(B^{(1)}(S),1,2,4)$　Output(1,5).

⑦$CPs(B^{(1)}(S),3,4,1)$　Output(3,2).

⑧$CPs(B^{(2)}(S),5,9,0)$　Output(5,0).

算法 2.1 输出了序列 s 所有的跃点(0,9),(1,5),(3,2),(5,0).同时,也可得序列 s 的所有 k 值与相应的 k 错线性复杂度分别为(0,9),(1,5),(2,5),(3,2),(4,2),(5,0),(6,0),(7,0),(8,0),(9,0).

4　结论

本文关注有限域 $GF(p^m)$上的 p^n 周期序列的一般情形,用映射的方式刻画了序列的跃点在不同周期长度序列之间的分解和对应的关系式,并借助该关系式和 Lauder-Paterson 算法的结构,给出计算序列所有跃点的一个新算法.相比于 Kaida 算法,新算法具有更好的计算复杂度.当然,新算法的计算量还是比较大,能进一步降低计算复杂度的改进算

法仍是值得探讨的.

参考文献(References)

[1] GAMES R A, CHAN A H. A fast algorithm for determining the linear complexity of a binary sequence with period 2^n[J]. IEEE Transactions on Information Theory, 1983, 29(1): 144-146.

[2] DING C S, XIAO G Z, SHANW J. The Stability Theory of Stream Ciphers [M]. Berlin: Springer-Verlag, 1991: Chapter 5.

[3] 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): 1398-1401.

[4] KAIDA T, UEHARA S, IMAMURA K. An algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n, p a prime[J]. Information and Computation, 1999, 151(2): 134-147.

[5] LAUDER A G B, PATERSON K G. Computing the error linear complexity spectrum of a binary sequence of period 2^n [J]. IEEE Transactions on Information Theory, 2003, 49(1): 273-280.

[6] KAIDA T. On the generalized Lauder-Paterson algorithm and profiles of the k-error linear complexity for exponent periodic sequences[C]// Sequences and Their Applications - SETA 2004. Heidelberg: Springer, 2005, LNCS 3486: 166-178.

[7] KURSOSAWA 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.

[8] 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 Yaodong, QI Wenfeng. On the k-error linear complexity of binary period sequences [J]. Acta Electronica Sinica, 2005, 33(1): 12-16.

[9] MEIDL W, NIEDERREITER H. On the expected value of the linear complexity and k-error linear complexity of periodic sequences [J]. IEEE Transactions on Information Theory, 2002, 48(11): 2817-2825.

[10] MEIDL W, VENKATESWARLU A. Remarks on the k-error linear complexity of p^n-periodic sequences[J]. Designs, Codes and Cryptography, 2007, 42(2): 181-193.

[11] 朱凤翔, 戚文峰.F_p上 p^n-周期序列的 1-错线性复杂度[J]. 电子与信息学报, 2007, 29(9): 2222-2225.
ZHU Fengxiang, QI Wenfeng. 1-error linear complexity of p^n-periodic sequences over F_p [J]. Journal of Electronics & Information Technology, 2007, 29(9): 2222-2225.

[12] 李鹤龄, 戚文峰.F_p上 p^n-周期序列的 k-错线性复杂度[J]. 通信学报, 2010, 31(6): 19-24.
LI Heling, QI Wenfeng. k-error sequences of p^n-periodic sequences over F_p [J]. Journal on Communications, 2010, 31(6): 19-24.

[13] CHANG Z L, KE P H. On the error linear complexity spectrum of binary sequences with period of power of two[J]. Chinese Journal of Electronics, 2015, 24(2): 366-372.

[14] TANG Miao. An algorithm for computing the error sequence of p^n-periodic binary sequences [J]. Applicable Algebra in Engineering, Communication and Computing, 2014, 25(3): 197-212.

[15] 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.
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.