周期序列球体复杂度的一个新算法

魏仕民[1,2], 陈 钟[2], 段云所[2]
(1. 淮北煤炭师范学院计算机科学技术系, 安徽淮北 235000; 2. 北京大学计算机科学与技术系, 北京 100871)

摘 要: 在分解周期序列极小多项式的基础上, 提出计算周期序列球体复杂度的一个新算法, 并给出该算法在特殊周期下的一个应用.

关键词: 流密码; 周期序列; 线性复杂度; 球体复杂度
中图分类号: TN918. 1 文献标识码: A 文章编号: 0372-2112 (2003) 08-1263-03

A New Algorithm for the Sphere Complexity of Periodic Sequence

WEI Shi-min[1,2], CHEN Zhong[2], DUAN Yun-suo[2]
(1. Department of Computer Science and Technique, Huaibe Coal Normal College, Huaibei, Anhui 235000, China;
2. Department of Computer Science and Technique, Peking University, Beijing 100871, China)

Abstract: Based on decomposition of the minimal polynomial of a periodic sequence, we propose a new algorithm for computing the sphere complexity of the sequence. The new algorithm is applied to the sequence with special period.

Key words: stream cipher; periodic sequence; linear complexity; sphere complexity

1 引言

密钥序列的线性复杂度是流密码强度的一个重要度量指标. 但有的序列的线性复杂度极不稳定, 当改变这些序列周期的一位或几位时, 其线性复杂度发生很大的变化. 我国学者早就注意到这个问题, 因而率先创立了流密码的稳定性理论[1~3], 并引入球体复杂度(又称 d-复杂度)、重量复杂度等流密码稳定性度量指标. 国外学者也引入类似球体复杂度的 k-错线性复杂度的概念[4], 并得到广泛的关注[4~7]. 本文在分解周期序列极小多项式的基础上, 提出计算周期序列球体复杂度的一个新算法, 并利用序列的迹表示, 给出该算法在特殊周期下的一个应用. 新算法的缺点是需要分解序列的极小多项式, 因而只能应用在极小多项式较为容易分解的周期序列上. 设 s 是周期为 N 的序列, 当改变 s 的一个周期中至多 k(1 ≤ k < N) 位、至少 1 位后, 得到的所有的序列线性复杂度中最小的那个称为 s 的 k-球复杂度, 记为 $sc_k(s)$. 设 e_m 是第一周期为 e_m^N(第 m+1 位是 1, 其余各位是 0) 的序列, 0 ≤ m ≤ N-1. 则可以表示为

$$sc_1(s) = \min_{\substack{0 \le m \le N-1 \\ a \in GF(q)^*}} \{c(s + ae_m)\},$$

这里 c(s) 表示 s 的线性复杂度, $GF(q)^*$ 表示 GF(q) 中所有非零元组成的集合. 我们已经发现一个新的算法用来计算 s 的 1-球复杂度, 下一节将给出这个算法. 整篇论文考虑的序列都是在特征为 p 的有限域 GF(q) 上.

2 计算 1-球复杂度新算法

设 s 是一个周期序列并且 s^N 是 s 的第一周期, 则

$$s(x) = \sum_{i=0}^{\infty} s_i x^i = \frac{s^N(x)}{1 - x^N} = \frac{r_s(x)}{f_s(x)}, \quad (1)$$

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

显然, $f_s(x)$ 是 s 的极小多项式, 且 $f_s(x)$ 的次数就是 s 的线性复杂度, 即 $\deg f_s(x) = c(s)$.

设 $t = s + ae_m$, 为了使得我们的讨论有意义, 不妨假定 $f_s(x) \neq 1$, 则

$$t(x) = s(x) + ae_m(x) = \frac{s^N(x) + ae_m^N(x)}{1 - x^N} = \frac{s^N(x) + ex^m}{1 - x^N},$$

所以 $c(t) = N - \deg(\gcd(1 - x^N, s^N(x) + ax^m))$. 因此 s 的 1-球复杂度表示为

$$sc_1 = N - \max_{\substack{0 \le m \le N-1 \\ a \in GF(q)^*}} \{\deg(\gcd(1 - x^N, s^N(x) + ax^m))\}.$$

为讨论方便, 当 $sc_1(s) = N - \deg(\gcd(1 - x^N, s^N(x) + ax^m))$ 时, 我们分别称 m 和 a 是最佳错误位置和最佳错误值.

定理 1 设 s 是一个周期序列并且 s^N 是 s 的第一周期, 则 $\gcd(1 - x^N, s^N(x) + ax^{m-1})$ 整除 $f_s(x)$, 这里 $a \in GF(q)^*$.

证明 假设命题不成立, 则存在 $\gcd(1 - x^N, s^N(x) + ax^{m-1})$ 的一个不可约因式 $p(x)$ 使得 $(p(x))^n \mid \gcd(1 - x^N, s^N(x) + ax^{m-1})$ 且 $(p(x))^n$ 不能整除 $f_s(x)$, 因而 $p(x) \mid (1 -$

收稿日期: 2001-12-29; 修回日期: 2002-06-18
基金项目: 国家自然科学基金(No. 60172015, No. 60003015, No. 60073051); 安徽省自然科学基金(No. 03042204); 国家重点基础研究规划发展项目(No. G1999035804)

$x^N)/f_s(x)$. 由式(1)得 $s^N(x)=r_s(x)\#(1-x^N)/f_s(x)$, 所以 $p(x)|s^N(x)$. 显然 $p(x)|1-x^N$ 且 $p(x)|s^N(x)+ax^{m-1}$, 因而 $p(x)|1$. 这与 $p(x)$ 是 $f_s(x)$ 的一个不可约多项式矛盾.

由定理 1 可得, m 是最佳错误位置且 a 是最佳错误值当且仅当 $s^N(x)+ax^m$ 含有 $f_s(x)$ 的最高次数因式. 设 $f_s(x)$ 的不可约分解为 $f_s(x)=(f_1(x))^{k_1},\ ,\ ,(f_l(x))^{k_l}$. 则 $c(s)=\sum_{i=1}^{l}k_i\deg(f_i(x))$. 现在可以将 $f_s(x)$ 的因式按次数从大到小依次排列为 $d_1(x), d_2(x),\ ,\ , d_M(x)$. 则计算最佳错误位置和最佳逼近序列线性复杂度的算法如下.

算法 1 初始值: $i=1; j=0; k=1$;

(1) 如果 $d_i(x)|s^N(x)+kx^j$, 则 $sc_1(s)=N-\deg(d_i(x))$, $m=j, a=k$, 停止; 否则, 转向(2).

(2) 如果 $k<q-1$, 则 $k=k+1$, 转向(1); 否则, 转向(3).

(3) 如果 $j<N-1$, 则 $j=j+1$, 转向(1); 否则, $i=i+1$, 转向(1).

最终算法输出最佳错误位置 m、最佳错误值 a 和最佳逼近序列线性复杂度 $sc_1(s)$.

算法 1 的算法复杂度主要集中在判断 $d_i(x)|s^N(x)+kx^j$ 是否成立上. 因此, 如果要简化算法 1, 必须简化判断 $d_i(x)|s^N(x)+kx^j$ 的计算量. 最直观的一种方法就是在判断 $d_1(x)=f_s(x)$ 是否整除 $s^N(x)+kx^j$ 的过程中, 如果 $d_1(x)$ 不能整除 $s^N(x)+kx^j$, 则保留 $d_1(x)$ 除 $s^N(x)+kx^j$ 所得的余式. 其后, 判断 $d_i(x)|s^N(x)+kx^j$ 是否成立就变成判断 $d_i(x)$ 整除相应余式是否成立. 由于余式的次数小于 $d_1(x)$ 的次数, 当然也小于 $s^N(x)+kx^j$ 的次数, 因而算法得到了一定的简化. 可以采用类似的方法进一步处理以后的判断. 在本文中并不深入讨论算法的简化, 而是把注意力放在算法的应用上, 以说明我们提出的算法是有意义的.

3 应用

本节介绍新算法在特殊周期序列上的一个应用. 设 s 是周期为 q^n-1 的序列, s 的极小多项式 $f_s(x)$ 的不可约分解为 $f_s(x)=f_0(x)f_1(x)\ ,\ f_{l-1}(x)$. 记 $n_k=\deg(f_k(x))$, $k=0,1,\ ,\ ,l-1$, 则 $n_k|n$ 且 $c(s)=n_0+n_1+\ ,\ n_{l-1}$. 设 A 是 $GF(q^n)$ 的一个本原元, 则存在一个最小的正整数 l_k 使得 $A^{l_k}\in GF(q^{n_k})$ 是 $f_k(x)$ 的一个根. 取 l_k 为模 $N=q^n-1$ 的分圆陪集 $L_k=\{l_k, ql_k,\ ,\ ,q^{n_k-1}l_k\}$ 的陪集首. 序列 s 可以表示为

$$s=s_{[0]}+s_{[1]}+\ ,\ +s_{[l-1]},$$

这里 $s_{[k]}=(s_{k0}, s_{k1},\ ,\ )$ 是以 $f_k(x)$ 为极小多项式的周期序列. 由于序列 $s_{[k]}$ 的迹可表示为

$$s_{ki}=T_{n_k}(B_kA^{-l_ki}),$$

这里 $B_k\in GF(q^{n_k})$; $T_{n_k}: GF(q^{n_k})\to GF(q)$ 是迹映射. 因而序列 s 可以表示为

$$s_i=\sum_{k=0}^{l-1}T_{n_k}(B_kA^{-l_ki}).$$

由有限序列 s^N 的形式幂级数表示 $s^N(x)$ 知 s^N 的离散 Fourier 变换(DFT)为

$$S_j=\sum_{i=0}^{N-1}s_iA^{ij}=s^N(A^j).$$

这里 A 的幂次对 N 取模. 将迹表示代入得

$$S_j=\sum_{k=0}^{l-1}\sum_{u=0}^{n_k-1}B_k^u\sum_{i=0}^{N-1}A^{(j-q^ul_k)i}=\begin{cases}-B_k^u & \text{如果存在 } u \text{ 和 } k \text{ 使得 } j-q^ul_k\equiv 0\ (\mathrm{mod}N)\\ 0 & \text{否则}\end{cases}$$

这是因为若 $j-q^ul_k\equiv 0\ (\mathrm{mod}N)$ 不成立, 则有 $\sum_{i=0}^{N-1}A^{(j-q^ul_k)i}=0$. 显然, 如果 j 在 L_k 中, 则存在 $u\in[0, n_k-1]$ 和 $k\in[0, l-1]$ 使方程 $j-q^ul_k\equiv 0\ (\mathrm{mod}N)$ 成立.

设 C 是模 N 分圆陪集首集合, 并且假设 $l_0, l_1,\ ,\ ,l_{t-1}$ 是 C 的开始的 t 个陪集首, 记 $r=|C|$. 设 $a=a^{w_a}$, 则容易看出错误序列 ae_m 表示为

$$ae_{m,i}=\sum_{k=0}^{r-1}T_{n_k}(-A^{w_a+l_k(m-i)}).$$

设 $B_k=A^{v_k}$, 则 $s_i=\sum_{k=0}^{l-1}T_{n_k}(A^{v_k-l_ki})$. 记 $t=s+ae_m$, 则

$$t_i=\sum_{k=0}^{l-1}Tr^{n_k}((A^{v_k-w_a+l_km})A^{-l_ki})+\sum_{k=t}^{r-1}Tr^{n_k}(-A^{w_a+l_k(m-i)}),$$

因而 $sc_1(s)=N-\max_{0\le m\le N-1}\sum_{k=0}^{l-1}z_{m,k,a}n_k$, 这里

$$z_{m,k,a}=\begin{cases}1 & \text{如果 } v_k\equiv w_a+ml_k\ (\mathrm{mod}N)\\ 0 & \text{否则}\end{cases}$$

$a\in GF(q)^*$

从上面的讨论可以将算法 1 中, 寻找 m 和 a 使得 $s^N(x)+ax^m$ 含有 $f_s(x)$ 的最高次数因式, 转化为寻找 m 和 a 使得 $N-\sum_{k=0}^{l-1}z_{m,k,a}n_k$ 的值达到最小.

算法 2 初始值: $i=0$; 对 $0\le u\le N$ 和 $1\le v\le q-1$, $c_{uv}=N$, $sc_1(s)=N$.

(1) 如果 $i<N$, 则 $j=1$, 转向(2); 否则, 停止.

(2) 如果 $j<q$, 则 $k=0$, 转向(3); 否则, $i=i+1$, 转向(1).

(3) 如果 $k<l$, 则 $y=v_j-w_k-il_k\ (\mathrm{mod}N)$, 转向(4); 否则, 转向(5).

(4) 如果 $y=0$, 则 $c_{ij}=c_{ij}-n_k$, $k=k+1$, 转向(3); 否则, 转向(3).

(5) 如果 $c_{ij}<sc_1(s)$, 则 $sc_1(s)=c_{ij}$, $m=i, a=j, j=j+1$, 转向(2); 否则, $j=j+1$, 转向(2).

最终算法输出最佳错误位置 m、最佳错误值 a 和最佳逼近序列线性复杂度 $sc_1(s)$.

4 结论

本文提出计算一般周期序列 12球复杂度的一个新算法, 我们也给出此算法在计算周期为 q^n-1 序列的 12球复杂度的一个应用. 新算法的缺点是需要分解序列的极小多项式, 因而只能应用在不需要花太大的代价分解极小多项式的周期序列

上. 研究这个算法的进一步改进和应用是有意义的.

参考文献:

[1] Ding C, Xiao G, Shan W. The Stability Theory of Stream Ciphers [M]. Berlin Heidelberg: Spinger2Verlag, 1991. 48- 153.

[2] 陈克非. 序列的d2复杂度 [J]. 电子学报, 1989, 17(1): 112- 113.

[3] 冯登国, 肖国镇. 序列周期稳定性新度量指标 [J]. 电子学报, 1994, 22(1): 86- 90.

[4] Stamp M, Martin C F. An algorithm for k2error linear complexity of bi2nary sequences with period 2^n [J]. IEEE Trans Inform. Theory, 1993, 39(4): 1398- 1401.

[5] Kaida T, Uehara S, Imamura K. An algorithm for the k2error linear complexity of sequences over GF(pm) with period pn, p a prime [J]. Information and Computation, 1999, 151(1): 134- 147.

[6] Wei S, Chen Z, Xiao G. A fast algorithm for k2 error linear complexity of a binary sequence [A]. 2001 International Conferences on Info2tech and Info2net Proceedings [C]. IEEE Press, 2001, No Conferences E, 152- 157.

[7] Wei S, Xiao G, Chen Z. An efficient algorithm for k2error linear com2plexity [J]. Chinese Journal of Electronics, 2002, 11(2): 265- 267.

作者简介:

魏仕民　男, 1962 年生于安徽省巢湖市, 博士, 淮北煤炭师范学院教授、北京大学博士后, 主要从事应用数学、密码学、网络与信息安全等领域的教学和科研工作.

陈　钟　男, 1963 年生于江苏省徐州市, 博士, 北京大学教授, 博士生导师, 主要从事软件工程、网络与信息安全等领域的教学和研究工作.