文章编号: 1000- 2243(2006)03- 0339- 05

周期多序列的联合线性复杂度

陈智雄[1, 2], 谭示崇[1], 肖国镇[1]

(1. 西安电子科技大学 ISN 国家重点实验室, 陕西 西安 710071;
2. 莆田学院数学与应用数学系, 福建 莆田 351100)

摘要: 由有限域上周期多序列 S 与某扩域上的单序列 B 的对应关系, 通过适当选择该扩域, 使得 S 与 B 具有相同的极小多项式, 从而直接应用扩域上的单序列来刻画周期多序列的联合线性复杂度和联合 k- 错线性复杂度等问题, 把周期多序列的综合问题转化为扩域上单序列的综合问题.

关键词: 流密码; 周期多序列; 联合线性复杂度
中图分类号: TN918.4 文献标识码: A

Joint linear complexity of periodic multi- sequences

CHEN Zhi- xiong[1, 2], TAN Shi- chong[1], XIAO Guo- zhen[1]

(1. National Key Laboratory of ISN, Xidian University, Xi' an, Shaanxi 710071, China; 2. Department of Mathematics, Putian University, Putian, Fujian 351100, China)

Abstract: Complexity measures for sequences of elements of a finite field play an important role in cryptology. Recent developments in stream ciphers point towards an interest in word-based(or vectorized) stream ciphers, which require the study of the complexity of multi-sequences. A multi-sequence can be considered as a single sequence of elements of an extension field. We point out that a periodic multi-sequence has the same minimal polynomial, linear complexity and k- error linear complexity as its corresponding single sequence over an extension field which is chosen properly. The fact implies that in many cases the study on multi-sequences can be transferred into single-sequences.

Keywords: stream cipher; periodic multi-sequence; joint linear complexity;

1 引言与基本概念

在传统的流密码中, 加密是明文与密钥以比特为单位进行异或, 近年来以"字"(word)或"向量"(vector)为单位的流密码(下称多序列, multi-sequences)也受到重视, 这类序列在编码理论、密码学和数字信号处理等领域有重要的应用. 设 S 是一个字长为 t 的以"字"为单位的序列, 即 $S = (s_0, s_1, \cdots)$, 其中 $s_i = (a_{1i}, a_{2i}, \cdots, a_{ti})$, $a_{ji} \in GF(q)$, $1 \leqslant j \leqslant t$, $i = 0, 1, \cdots$, 称 S 为有限域 $GF(q)$ 上 t- 维多序列(t- dimensional multi-sequence). 当 $t = 1$ 时, 即为通常所指的序列, 此时也称为单序列. 由于多序列 S 可以写成矩阵的形式:

$$S = (s_0, s_1, \cdots) = \begin{pmatrix} a_{10} & a_{11} & a_{12} & \cdots \\ a_{20} & a_{21} & a_{22} & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{t0} & a_{t1} & a_{t2} & \cdots \end{pmatrix}$$

收稿日期: 2005- 11- 28
作者简介: 陈智雄(1972-), 男, 博士研究生, 讲师.
基金项目: 福建省自然科学基金资助项目(项目编号: A0540011); 福建省教育厅科研资助项目(项目编号: JA04264); 莆田市科技计划资助项目(项目编号: 2005S04)

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

其中第 i 列为 s_i. 用 A_j 表示上述矩阵的第 j 行, 即 $A_j = (a_{j0}, a_{j1}, a_{j2}, \cdots)$, $j = 1, 2, \cdots, t$, 那么 S 可以看作由 t 个"平行"序列构成的新序列, 并记 $S = (A_1, A_2, \cdots, A_t)$, 这也是多序列名称的由来.

对多序列的研究主要包括两方面. 一是多序列的分析, 文献[1]是介绍多序列联合线性复杂度(joint linear complexity)的综述文章; 文献[2]研究了周期多序列的联合线性复杂度的期望值; 文献[3]研究了一类特殊多序列的联合线性复杂度轮廓(joint linear complexity profile), 文献[4]、[5]利用代数曲线构造了具有几乎优的联合线性复杂度轮廓(almost perfect joint linear complexity profile)性质的多序列. 二是多序列的综合, 即求多序列的极小多项式与联合线性复杂度. 多序列的综合问题是多序列的一个极其重要的问题, 众所周知, 单序列的综合有 B-M 算法、连分式算法和欧几里德算法[6]等. 而在文献[7]、[8]中研究了多序列的综合及其在编码解码中的应用, Feng 等[9, 10]提出了广义欧几里德算法和迭代算法, 随后国内外许多学者也应用 Gröbner 基理论来处理这个问题[11, 12].

设 $GF(q)$ 是特征为 p 的有限域, q 是 p 的幂. t - 维多序列 $S = (s_0, s_1, s_2, \cdots) = (A_1, A_2, \cdots, A_t)$ 如果满足: $s_{i+N} = s_i$, $i \geqslant 0$, 则称正整数 N 是多序列 S 的周期, 其最小周期记为 $\mathrm{per}(S)$. 显然, $\mathrm{per}(S) = \mathrm{lcm}(\mathrm{per}(A_1), \mathrm{per}(A_2), \cdots, \mathrm{per}(A_t))$, 其中 $\mathrm{per}(A_j)$ 是 A_j, $1 \leqslant j \leqslant t$ 的最小周期.

周期为 N 的 t - 维多序列 $S = (A_1, A_2, \cdots, A_t)$ 的极小多项式 $F(x)$ 是指序列 $A_1, A_2, \cdots, A_t$ 的次数最低的共同的特征多项式, 易知 $F(x) = \mathrm{lcm}(f_1(x), f_2(x), \cdots, f_t(x))$, 其中 $f_j(x)$ 是 A_j, $1 \leqslant j \leqslant t$ 的极小多项式. 那么 $L(S) = \deg(F(x))$ 称为多序列 S 的联合线性复杂度.

设序列 A_j 的周期为 N, 记 $A_j^N(x)$ 为 A_j, $1 \leqslant j \leqslant t$ 的第一个周期所对应的多项式. 由于

$$f_j(x) = \frac{1 - x^N}{\gcd(1 - x^N, A_j^N(x))} \qquad (1 \leqslant j \leqslant t)$$

那么,

$$\begin{aligned} F(x) &= \mathrm{lcm}(f_1(x), f_2(x), \cdots, f_t(x)) \\ &= \mathrm{lcm}\left(\frac{1 - x^N}{\gcd(1 - x^N, A_1^N(x))}, \frac{1 - x^N}{\gcd(1 - x^N, A_2^N(x))}, \cdots, \frac{1 - x^N}{\gcd(1 - x^N, A_t^N(x))}\right) \\ &= \frac{1 - x^N}{\gcd(1 - x^N, A_1^N(x), A_2^N(x), \cdots, A_t^N(x))} \end{aligned} \tag{1}$$

虽然在上述文献中提出了许多多序列综合的算法, 但比单序列的综合要复杂的多. 本文旨在把多序列转化为一个单序列, 并从单序列来求多序列的综合问题, 进一步简化多序列的综合问题. 即对于 $GF(q)$ 上 t - 维多序列 S, 通过适当选择一个扩域 $GF(q^{t^*})$(其中整数 $t^* \geqslant t$), 使得 S 与该扩域上的一个单序列 B 对应, 证明了周期多序列 S 的极小多项式 $F(x) \in GF(q)[x]$ 与 $GF(q^{t^*})$ 上的单序列 B 的极小多项式 $g(x) \in GF(q^{t^*})[x]$ 相等, 并由此得出周期多序列的联合线性复杂度可由扩域上的一个单序列完全确定. 在第三节, 作为单序列 k - 错线性复杂度的概念的推广, 提出了联合 k - 错线性复杂度的概念, 并证明了多序列的联合 k - 错线性复杂度同样可由扩域上的一个单序列完全确定.

2 周期多序列的联合线性复杂度

由于 $GF(q)$ 的线性空间 $(GF(q))^t$ 与 $GF(q^t)$ 是线性同构的, 于是 $GF(q)$ 上 t - 维多序列可视为 $GF(q^t)$ 上的一个单序列[6], 即任取 $u_1, u_2, \cdots, u_t \in GF(q^t)$ 中的一组基, 令

$$b_i = a_{1i}u_1 + a_{2i}u_2 + \cdots + a_{ti}u_t \in GF(q^t) \qquad (i = 0, 1, \cdots)$$

于是 $GF(q)$ 上的多序列 S 对应于 $GF(q^t)$ 上的一个单序列 $B = (b_0, b_1, \cdots)$. 那么研究多序列 S 的许多问题可以转化为对单序列 B 的研究.

设 $F(x) = c_0 + c_1x + \cdots + c_{L-1}x^{L-1} + x^L \in GF(q)[x]$ 是多序列 S 的极小多项式, 于是对所有的 $i \geqslant 0$,

$$a_{j,L+i} + c_{L-1}a_{j,L-1+i} + \cdots + c_1a_{j,1+i} + c_0a_{j,i} = 0 \qquad (j = 1, 2, \cdots, t)$$

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

当且仅当对所有的 $i \geqslant 0$,

$$\left(\sum_{k=0}^{L} c_k a_{1,\,k+i}\right) u_1 + \left(\sum_{k=0}^{L} c_k a_{2,\,k+i}\right) u_2 + \cdots + \left(\sum_{k=0}^{L} c_k a_{t,\,k+i}\right) u_t = 0,\quad c_L = 1$$

当且仅当对所有的 $i \geqslant 0$,

$$b_{L+i} + c_{L-1} b_{L-1+i} + \cdots + c_1 b_{1+i} + c_0 b_i = 0$$

从而 $F(x)$ 是单序列 B 的一个特征多项式, 但未必是极小多项式, 因为序列 B 的极小多项式 $g(x) \in GF(q^t)[x]$. 也即如下结论:

命题 **1**　如上述讨论, 单序列 B 的极小多项式是其所对应的多序列 S 的极小多项式的因式.

例 **1**[6]　设 u 为 $GF(2)$ 上多项式 $x^4 + x + 1 = 0$ 的根, 取 $GF(2^4) = GF(2)(u)$ 的一组基为 1, u, u^2, u^3. 那么 $GF(2)$ 上的多序列 S 与 $GF(2^4)$ 上的单序列 $B = (1\,u\,u^2\,u^3\,u^4\cdots)$ 相对应:

$$S = \begin{pmatrix} 1000100110101111\cdots \\ 0100110101111100\cdots \\ 0010011010111110\cdots \\ 0001001101011111\cdots \end{pmatrix}$$

易知 B 的极小多项式为 $g(x) = x + u \in GF(2^4)[x]$, 线性复杂度为 1, 而 4- 维多序列 S 的极小多项式为 $F(x) = x^4 + x + 1 \in GF(2)[x]$, 联合线性复杂度为 4.

正由于这一点区别, 对多序列的研究带来许多不便, 但我们将选择一个新的扩域 $GF(q^{t^*})$, 使得 S 与 B 具有相同的极小多项式.

引理 **1**　设 p 是有限域 $GF(q)$ 的特征, $(n, p) = 1$, q 在 Z_n^* 中的乘法阶为 l, t 为正整数. 若 $(l, t) = 1$, 则 $1 - x^n$ 在 $GF(q)$ 与 $GF(q^t)$ 中的既约分解式相同.

证明　设 α 是 $1 - x^n$ 的一个根, α 的乘法阶记为 $|\alpha|$, 则 $|\alpha|$ 整除 n, 那么在 $GF(q)$ 中以 α 为根的既约多项式的次数记为 m, m 是 q 模 $|\alpha|$ 的阶. 由于 $q^l \equiv 1 \bmod n$, 知 $q^l \equiv 1 \bmod |\alpha|$, 则 $m \mid l$, 从而 $(m, t) = 1$. 设在 $GF(q^t)$ 中以 α 为根的既约多项式的次数为 m_0, 则 $(q^t)^{m_0} \equiv q^{tm_0} \equiv 1 \bmod |\alpha|$, 得 $m \mid m_0$. 又 $(q^t)^m \equiv q^{tm} \equiv (q^m)^t \equiv 1 \bmod |\alpha|$, 得 $m_0 \mid m$, 故 $m = m_0$, 即在 $GF(q)$ 与 $GF(q^t)$ 中, 以 α 为根的既约多项式的次数相同, 它们显然是同一个多项式, 证毕.

定理 **1**　设 p 是有限域 $GF(q)$ 的特征, $N = p^v n$, $(n, p) = 1$, $GF(q)$ 上周期为 N 的 t- 维多序列 S 对应于 $GF(q^t)$ 上周期为 N 的单序列 B, q 在 Z_n^* 中的乘法阶为 l.

①如果 $(l, t) = 1$, 则 S 与 B 具有相同的极小多项式,

②如果 $(l, t) > 1$, S 适当增加若干行零序列后得到 t^* - 维多序列 $\overline{S}$ 且 $(l, t^*) = 1$, $\overline{S}$ 对应 $GF(q^{t^*})$ 上的单序列记为 $\overline{B}$, 则 S, $\overline{S}$ 与 $\overline{B}$ 具有相同的极小多项式.

证明　①B 的极小多项式 $g(x) = \dfrac{1 - x^N}{\gcd(1 - x^N, B^N(x))} = \dfrac{1 - x^N}{\gcd((1 - x^n)^{p^v}, B^N(x))}$, 由于 $1 - x^n$ 在有限域 $GF(q)$ 与 $GF(q^t)$ 中的既约分解式相同, 注意到

$$B^N(\alpha) = 0 \Leftrightarrow A_1^N(\alpha) = A_2^N(\alpha) = \cdots = A_t^N(\alpha) = 0$$

且 α 是 $B^N(x)$ 的 m 重根当且仅当 α 是 $A_1^N(x)$, $A_2^N(x)$, …, $A_t^N(x)$ 的 m 重根, 其中 α 是 $1 - x^n$ 的一个根. 故由 Eq(1), S 的极小多项式 $F(x) = g(x)$.

②由 $\overline{S}$ 的构造, 知 $\overline{S}$ 与 S 有相同的极小多项式, 再由 ①即得. 证毕.

根据上述定理, 求多序列的极小多项式和线性复杂度可以转化为求相应的单序列的极小多项式与线性复杂度.

例 **2**　条件同例 1. 因 S 的周期为 $N = 15$, 而 2mod15 的阶为 $l = 4$, 即 $(l, t) > 1$. 现 S 增加一行零序列, 即 $\overline{S}$ 为 5- 维多序列. 设 β 为 $x^5 + x^2 + 1 = 0$ 的一个根, 取 $GF(2^5) = GF(2)(\beta)$ 的一组基为 1, β, β^2, β^3, β^4. 则 $\overline{S}$ 所对应的单序列 $\overline{B} = (1\,\beta\,\beta^2\,\beta^3\,\beta^{18}\,\beta^{19}\,\beta^{20}\,\beta^{27}\,\beta^5\,\beta^6\,\beta^{11}\,\beta^{12}\,\beta^{23}\,\beta^8\,\beta^{29}\cdots)$, 易得 $\overline{B}$ 的极小多

©1994-2013 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

项式为 $x^4 + x + 1$, 即与多序列 S 的极小多项式相同.

最后, 如果周期序列 A_1, A_2, …, A_t 的极小多项式两两互素, 则周期多序列 $S = (A_1, A_2, \cdots, A_t)$ 的极小多项式与和序列 $A_1 + A_2 + \cdots + A_t$ 的极小多项式相同.

3 周期多序列的联合 $k-$ 错线性复杂度

$k-$ 错线性复杂度是反映序列的线性复杂度的稳定性, 即改变序列的若干比特后, 线性复杂度的波动情况. 线性复杂度变化较大的序列是不能用来作为密钥序列的, 因此 $k-$ 错线性复杂度是序列的一个重要的度量指标. 有关单序列的 $k-$ 错线性复杂度得到广泛的研究[6, 13-15]. 下面定义周期多序列的联合 $k-$ 错线性复杂度的概念.

定义 设 S 与 E 是 $GF(q)$ 上周期为 N 的 $t-$ 维多序列, E^N 表示 E 的一个周期(为 $t \times N$ 矩阵), E^N 的非零列数用 $W(E^N)$ 表示, 那么 S 的联合 $k-$ 错线性复杂度(joint $k-$ error linear complexity) 定义为:

$$L_k(S) = \min_{0 \leqslant W(E^N) \leqslant k} L(S + E)$$

显然, 当 $t = 1$ 时即为通常定义的周期单序列的 $k-$ 错线性复杂度.

引理 **2** 设 $S = (A_1, A_2, \cdots, A_t)$ 与 $E = (E_1, E_2, \cdots, E_t)$ 是 $GF(q)$ 上周期为 N 的 $t-$ 维多序列. $\overline{S}$ 是 S 适当增加若干零序列后得 t^*- 维多序列, 即 $\overline{S} = (S, \underline{0}, \cdots, \underline{0})$. 对 $GF(q)$ 上任意的周期为 N 的 $(t^* - t)-$ 维多序列 $W = (W_1, W_2, \cdots, W_{t^*-t})$, 令 $\overline{E_1} = (E, \underline{0}, \cdots, \underline{0})$, $\overline{E_2} = (E, W)$ 是 t^*- 维多序列, 则 $L(\overline{S} + \overline{E_1}) \leqslant L(\overline{S} + \overline{E_2})$.

证明 由于多序列 $\overline{S} + \overline{E_1}$ 的极小多项式 $F_1(x)$ 是 $A_1 + E_1$, $A_2 + E_2$, …, $A_t + E_t$ 的极小多项式的最小公倍式, 而 $\overline{S} + \overline{E_2}$ 的极小多项式 $F_2(x)$ 是 $A_1 + E_1$, $A_2 + E_2$, …, $A_t + E_t$, W_1, W_2, …, W_{t^*-t} 的极小多项式的最小公倍式, 显然 $F_1(x)$ 整除 $F_2(x)$, 故 $L(\overline{S} + \overline{E_1}) \leqslant L(\overline{S} + \overline{E_2})$.

定理 **2** 设 $N = p^v n$, $(n, p) = 1$, $GF(q)$ 上周期为 N 的 $t-$ 维多序列 S 对应于 $GF(q^t)$ 上周期为 N 的单序列 B, q 在 Z_n^* 中的乘法阶为 l.

①如果 $(l, t) = 1$, $L_k(S) = L_k(B)$,

②如果 $(l, t) > 1$, 设 $\overline{S} = (S, \underline{0}, \cdots, \underline{0})$ 使得 $\overline{S}$ 为 t^*- 多序列且 $(l, t^*) = 1$, $\overline{S}$ 对应于 $GF(q^{t^*})$ 上的单序列记为 $\overline{B}$, 则 $L_k(S) = L_k(\overline{S}) = L_k(\overline{B})$.

证明 ①设 E 为 $GF(q)$ 上周期为 N 的 $t-$ 维多序列, 对应于 $GF(q^t)$ 上的单序列记为 E', 由定理 1 有:

$$L_k(S) = \min_{0 \leqslant W(E^N) \leqslant k} L(S + E) = \min_{0 \leqslant W(E'^N) \leqslant k} L(B + E') = L_k(B)$$

②符号同引理 2. 由定义及引理 2 有:

$$L_k(S) = \min_{0 \leqslant W(E^N) \leqslant k} L(S + E) = \min_{0 \leqslant W(\overline{E_1}^N) \leqslant k} L(\overline{S} + \overline{E_1}) = \min_{0 \leqslant W(\overline{E_2}^N) \leqslant k} L(\overline{S} + \overline{E_2}) = L_k(\overline{S})$$

再由 ①, $L_k(\overline{S}) = L_k(\overline{B})$. 证毕.

4 结语

1) 指出了任何周期多序列均与某扩域上的一个单序列一一对应关系, 证明了它们具有相同的极小多项式、线性复杂度和 $k-$ 错线性复杂度, 而且该性质与扩域上基的选取无关, 从而周期多序列的综合问题归结为单序列的综合问题, B-M 算法是一个有效的通用方法. 正由于多序列与单序列的这一联系, 为进一步研究周期多序列, 特别是在理论上讨论周期多序列的联合线性复杂度、联合线性复杂度轮廓、联合 $k-$ 错线性复杂度以及其他问题提供便利.

2) 类似于联合 $k-$ 错线性复杂度, 可以定义联合 $k-$ 错线性复杂度轮廓(joint $k-$ error linear complexity profile), 但本文的方法似乎不能直接用来讨论联合线性复杂度轮廓的相关问题.

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

参考文献：

[1] NIEDERREITER H. Linear complexity and related complexity measures for sequences[C]// JOHANSSON T, MAITRA S. INDOCRYPT 2003. Lecture Notes in Computer Science: Volume No2904. Berlin: Springer-Verlag, 2003: 1-17.

[2] MEIDL W, NIEDERREITER H. The expected value of the joint linear complexity of periodic multisequences[J]. J Complexity, 2003, 19(1): 61-72.

[3] MEIDL W, WINTERHOF A. On the joint linear complexity profile of explicit inversive multisequences[J]. J Complexity, 2005, 21(3): 324-336.

[4] XING C P, LAM K Y, WEI Z. A class of explicit perfect multisequences[C]// ASIACRYPT'99. Lecture Notes in Computer Science: Volume No1716. Berlin: Springer-Verlag, 1999: 299-305.

[5] XING C P. Multisequences with almost perfect linear complexity profile and function fields over finite fields[J]. J Complexity, 2000, 16(5): 661-675.

[6] DING C S, XIAO G Z, SHAN W J. The stable theory of stream ciphers[C]// Lecture Notes in Computer Science: Volume No561. Berlin: Springer-Verlag, 1991.

[7] ARMAND M A. Multisequence shift register synthesis over commutative rings with identity with applications to decoding cyclic codes over integer rings[J]. IEEE Trans I T, 2004, 50(1): 220-228.

[8] CHEN P H. Multisequence linear shift register synthesis and its application to BCH decoding[J]. IEEE Trans Communication, 1976, 22(4): 438-440.

[9] FENG G L, TSENG K K. A generalized euclidean algorithm for multisequence shift-register synthesis[J]. IEEE Trans I T, 1989, 35(3): 584-594.

[10] FENG G L, TSENG K K. A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes[J]. IEEE Trans I T, 1991, 37(5): 1 274-1 286.

[11] WANG P L, ZHU Y F. $F[x]$-lattice basis reduction algorithm and multisequences synthesis[J]. Science in China (Series F), 2001, 44(5): 321-328.

[12] ZHOU J J, QI W F, ZHOU Y J. A generalization of Gröbner bases and a synthesis algorithm ofmultisequences over $Z/(m)^*$[J]. Science in China (Series A), 1995, 38(5): 552-561.

[13] MEIDL W, NIEDERREITER H. Linear complexity, k-error linear complexity and the discrete Fourier transform[J]. J Complexity, 2002, 18(1): 87-103.

[14] NIEDERREITER H, SHPARLINSKI I E. Periodic sequences with maximal linear complexity and almostmaximal k-error linear complexity[C]// PETERSON K G. Cryptography and Coding 2003. Lecture Notes in Computer Science: Volume No2898. Berlin: Springer-Verlag, 2003: 183-189.

[15] 牛志华，董庆宽，肖国镇. p^n-周期二元序列的线性复杂度与 k-错线性复杂度[J]. 西安电子科技大学学报：自然科学版，2004，31(4)：622-625.

© 1994-2013 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net