有限域上定长序列的最短线性递归长度分布

尹 乾 罗运纶 胡小红 付新丽

(北京师范大学信息科学学院计算机系 北京 100875)

摘 要 研究有限域 $F(q)$上任意给定长度的序列的最短线性递归长度的分布. 对任意正整数 n 和 $0\leq l\leq n$,计算出了长度为 n、最短线性递归长度为 l 的序列个数,指出了对于固定长度为 n 的任意序列,其最短线性递归长度大部分情况下等于 $n/2$ 或 $n/2+1$,即其最短线性递归长度的分布一般都集中在长度的一半位置.

关键词 B-M 算法;最短线性递归长度;分布

中图法分类号 TP311

The Distributing Regulation of the Shortest Linear Recurring Length over the Finite Field

YIN Qian LUO Yun-Lun HU Xiao-Hong FU Xin-Li

(*Department of Computer, College of Information Science, Beijing Normal University, Beijing* 100875)

Abstract In this paper, when B-M algorithm is applied to search the shortest linear recurring length of single sequence over the finite field $F(q)$, the distribution of the shortest linear recurring sequence over the finite field $F(q)$ is studied. The amount of the sequences, whose length is n and shortest linear recurring length is l, has been calculated where $0\leq l\leq n$. It is found that the shortest linear recurring length l is always equal to $n/2$ or $n/2+1$ for any sequence of length n. In other words, it is always equal to the half of the length of the given sequence.

Keywords B-M algorithm; the shortest linear recursive length; distribution

1 引 言

流密码是密码学中一种重要的加密体制,其主要思想是采用伪随机序列进行加密. 目前使用最多的伪随机序列为移位寄存器序列,所以对移位寄存器序列的研究就成为了流密码体制中的一个重要问题. 而 20 世纪 60 年代末提出的线性反馈移位寄存器的 B-M 综合算法(全称为 Berlekam-Massey 算法),是第一个解决线性反馈移位寄存器综合问题的算法,从而使得序列的线性复杂度问题成为流密码的一个重要强度指标. 所谓的线性反馈移位寄存器综合问题指的是对已知的序列,求它的最短线性递归长度(也可以说是求序列的线性复杂度)和最小生成多项式组成的综合解. 使用该算法求出的为给定序列的最短线性移位寄存器的长度以及该序列的最小生成多项式,可以在域 $Z/(p)$上实现.

在参考文献[3]中给出了环上的两种单条序列最短线性移位寄存器综合算法之间的关系;在参考文献[2]中给出了多条序列最短线性移位寄存器综合问题的解决算法,是对 B-M 算法序列个数的扩展;在参考文献[4]中给出了利用 Gröbner 基理论求解环上多条序列的综合算法;但都没有给出利用这些算法求出的最短线性递归长度的分布. 本文在利用 B-M 算法求单条序列最短线性递归长度时,完整地求出了最短线性递归长度的分布.

收稿日期:2003-01-02;修改稿收到日期:2005-09-08.尹 乾,女,1975 年生,博士研究生,讲师,主要研究方向为计算机密码学、软件可靠性. E-mail:yinqian@bnu.edu.cn. 罗运纶,男,1948 年生,博士,副教授,主要研究方向为计算机密码学、计算代数. 胡小红,女,1976 年生,硕士,主要研究方向为计算机密码学. 付新丽,女,1976 年生,硕士,主要研究方向为计算机密码学.

2 定义几个记号

$$A_{l-1}=\begin{pmatrix} a_0 & a_1 & \cdots & a_{l-1} \\ a_1 & a_2 & \cdots & a_l \\ \vdots & \vdots & \vdots & \vdots \\ a_{l-1} & a_l & \cdots & a_{2l-2} \end{pmatrix},$$

$S_{l-1}=\{A_{l-1}\mid a_0,a_1,\cdots,a_{2l-2}\in F(q)\}$,

$T_n=\{a_0,a_1,\cdots,a_n\mid a_i\in F(q)\}$,

$F(q)$为 q 个元的有限域,其中 q 为素数幂.

3 两个引理

引理 1. 若某个固定的$\{a_0,a_1,\cdots,a_n\}$有长度为 l 的最短线性递归且满足条件 $2l\leq n+1$,则 A_{l-1} 可逆,且线性递归系数唯一.

证明. 使用归纳法证明.

情形 $1(l=1)$. 全零序列的最短线性递归长度为 0,因此若 $l=1$,则 $a_0\neq 0$,故 A_{l-1} 可逆且线性递归系数唯一.

情形 $2(l>1$且$2l\leq n+1)$. 使用反证法证明如下:$\{a_0,a_1,\cdots,a_n\}$有最短线性递归 l,而 A_{l-1} 不可逆,则存在最小的 $m(m\leq l-1)$,使得矩阵

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_m \\ a_1 & a_2 & \cdots & a_{m+1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{l-1} & a_l & \cdots & a_{m+l-1} \end{pmatrix}$$

降秩(秩小于 $m+1$). 因为 m 是最小的,易见$\{a_0,a_1,\cdots,a_{m+l-1}\}$有长度为 m 的最短线性递归. 又 $m+l>m+l-1\geq 2m$ 成立,由归纳法的假设可知 A_{m-1} 可逆. 令 k 最大,使得$\{a_0,a_1,\cdots,a_k\}$有长度为 m 的最短线性递归,则 $m+l-1\leq k<n$ 成立. 故应该有$\{a_0,a_1,\cdots,a_{k+1}\}$的最短线性递归长度不长于$\{a_0,a_1,\cdots,a_n\}$的最短线性递归长度. 考虑方程组

$$\begin{pmatrix} a_0 & \cdots & a_{k-m} & a_{k-m+1} \\ \vdots & \vdots & \vdots & \vdots \\ a_m & \cdots & a_k & a_{k+1} \end{pmatrix}\begin{pmatrix} x_0 \\ \vdots \\ x_{k-m} \\ -1 \end{pmatrix}=0,$$

其系数矩阵的秩小于增广矩阵的秩,故方程组无解,从而得到:$\{a_0,a_1,\cdots,a_{k+1}\}$的最短线性递归长度$>k-m+1\geq l$,矛盾.

引理 1 得证. 证毕.

引理 2. S_{l-1}中可逆矩阵的个数为$(q-1)q^{2l-2}$.

证明. 使用归纳法证明如下:

情形 $1(l=1)$. 此时,$A_{l-1}=(a_0)$显然. A_{l-1} 可逆$\Leftrightarrow a_0\neq 0$,因此$S_0$中有 $q-1$ 个可逆矩阵,结论正确.

情形 $2(l>1)$. 令 k 最小,使得

$$rank\begin{pmatrix} a_0 & \cdots & a_{l-2} \\ \vdots & \vdots & \vdots \\ a_k & \cdots & a_{k+l-2} \end{pmatrix}=k$$

成立,则 $k\leq l-1$,即 $2k\leq k+l-1$. 若 $k>0$,因为$\{a_0,a_1,\cdots,a_{k+l-2}\}$的最短线性递归长度为 k,因此由引理 1 可知 A_{k-1} 可逆,由归纳假设可知这样的 A_{k-1}有$(q-1)q^{2k-2}$个. 取定其中的一个,a_{2k-1} 可以任意取值. 由 A_{l-1}可逆,知

$$rank\begin{pmatrix} a_0 & \cdots & a_{l-2} & a_{l-1} \\ \vdots & \vdots & \vdots & \vdots \\ a_k & \cdots & a_{k+l-2} & a_{k+l-1} \end{pmatrix}=k+1,$$

因此 a_{k+l-1}有 $q-1$ 种选择. 取定其中一种,记

$$c_0a_{k-i}+\cdots+c_{k-1}a_{i-1}+a_i=0,\ i=k,\cdots,k+l-2,$$

则 A_{l-1}可经矩阵的初等变换化为

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 1 & 0 & \cdots & \cdots & 0 \\ c_0 & \cdots & c_{k-1} & 1 & 0 & \cdots & 0 \\ 0 & c_0 & \cdots & c_{k-1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & c_0 & \cdots & c_{k-1} & 1 \end{pmatrix}A_{l-1}=$$

$$\begin{pmatrix} a_0 & \cdots & \cdots & a_{l-2} & a_{l-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{k-1} & \cdots & \cdots & a_{k+l-3} & a_{k+l-2} \\ 0 & \cdots & \cdots & 0 & c \\ \vdots & \vdots & \vdots & \iddots & * \\ 0 & \cdots & c & * & * \end{pmatrix},$$

其中 $c\neq 0$,“$*$”代表计算得到的任意数值,也就是说,$a_{k+l},\cdots,a_{2l-2}$可以任意取值.

那么,对这样的 A_{l-1}和 k,可逆矩阵的数目为

$$(q-1)q^{2k-2}q(q-1)q^{l-k-1}=(q-1)^2q^{l+k-2},$$
$$k=1,2,\cdots,l-2.$$

若 $k=0$,则 $a_{l-1}\neq 0,a_l,\cdots,a_{2l-2}$可以任意取值,这样的矩阵共有$(q-1)q^{l-1}$个.

因此,S_{l-1}中可逆矩阵的数目为

$$(q-1)q^{l-1}+\Big(\sum_{k=1}^{l-1}q^{k-1}\Big)q^{l-1}(q-1)^2=$$

$$(q-1)q^{l-1}+(q-1)^2\frac{q^{l-1}-1}{q-1}q^{l-1}=(q-1)q^{2l-2}.$$

引理 2 得证. 证毕.

4　最短线性递归长度的分布

定理 1.　当 $2l\leq n+1$ 时，T_n 中最短线性递归长度为 l 的序列的个数为 $(q-1)q^{2l-1}$ 个.

证明.　由引理 1 可知：若 $2l\leq n+1$ 且 $\{a_0,a_1,\cdots,a_n\}$ 的最短线性递归长度为 l，则 A_{l-1} 可逆，递归系数唯一. 由引理 2 可知：可逆的 A_{l-1} 有 $(q-1)q^{2l-2}$ 种，a_{2l-1} 可以任意取，有 q 种. 取定一种则递归系数随之确定. 又 $a_0,a_1,\cdots,a_n$ 由 $a_0,a_1,\cdots,a_{2l-1}$ 及递归系数确定，所以定理 1 得证.　　证毕.

引理 3.　序列 $\{a_0,a_1,\cdots,a_n\}$ 的最短线性递归长度为 l，且满足

$$2l>n+1(l\leq n)\Leftrightarrow\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l+1}&\cdots&a_n\end{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{l-2}\\ -1\end{pmatrix}=0$$

无解且

$$\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l}&\cdots&a_{n-1}\end{pmatrix}$$

满秩，即秩等于 $n-l+1$.

证明.　分别证明充分性和必要性.

充分性. 由 $2l>n+1$，可知 $\{a_0,a_1,\cdots,a_n\}$ 的长为 l 的线性递归可以递归扩展到 a_{2l-1}，利用引理 1 可知：A_{l-1} 可逆，则其行向量组线性无关. 充分性得证.

必要性. 因为矩阵

$$\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l}&\cdots&a_{n-1}\end{pmatrix}$$

满秩，所以方程组

$$\begin{pmatrix}a_0&\cdots&a_{l-1}&a_l\\ \vdots&\vdots&\vdots&\vdots\\ a_{n-l}&\cdots&a_{n-1}&a_n\end{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{l-1}\\ -1\end{pmatrix}=0$$

有解，即 $\{a_0,a_1,\cdots,a_n\}$ 有长为 l 的线性递归. 又因为

$$\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l+1}&\cdots&a_n\end{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{l-2}\\ -1\end{pmatrix}=0$$

无解，所以 $\{a_0,a_1,\cdots,a_n\}$ 有长为 l 的最短线性递归. 必要性得证.　　证毕.

定理 2.　当 $2l>n+1$ 时，T_n 中最短线性递归长度为 l 的序列的个数为 $(q-1)q^{2(n-l+1)}$ 个.

证明.　由引理 3 可知

$$\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l}&\cdots&a_{n-1}\end{pmatrix}$$

满秩. 因为 l 是最短线性递归的长度，故

$$\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l}&\cdots&a_{n-1}\\ a_{n-l+1}&\cdots&a_n\end{pmatrix}\begin{pmatrix}x_0\\ \vdots\\ x_{l-2}\\ -1\end{pmatrix}=0$$

无解. 由此可知系数矩阵的秩必小于增广矩阵的秩，即增广矩阵的末行不能表示为前 $n-l+1$ 行的线性组合. 由 $2l>n+1$，可知 $n-l+2\leq l$，因此可得

$$rank\begin{pmatrix}a_0&\cdots&a_{l-1}\\ \vdots&\vdots&\vdots\\ a_{n-l+1}&\cdots&a_n\end{pmatrix}=n-l+2,$$

而

$$rank\begin{pmatrix}a_0&\cdots&a_{l-2}\\ \vdots&\vdots&\vdots\\ a_{n-l+1}&\cdots&a_{n-1}\end{pmatrix}=n-l+1$$

取 k 最小，使得

$$rank\begin{pmatrix}a_0&\cdots&a_{l-2}\\ \vdots&\vdots&\vdots\\ a_k&\cdots&a_{k+l-2}\end{pmatrix}\text{降秩}=k.$$

若 $k=0$，则 $a_0=\cdots=a_{l-2}=0,a_{l-1}\neq 0$，有 $q-1$ 种取法. 又有 $a_l,\cdots,a_n$ 可以任意取，可知这样的序列有 $(q-1)q^{n-l+1}$ 种. 若 $0<k\leq n-l+1$，则矩阵

$$\begin{pmatrix}a_0&\cdots&a_{l-2}\\ \vdots&\vdots&\vdots\\ a_{k-1}&\cdots&a_{k+l-3}\\ a_k&\cdots&a_{k+l-2}\end{pmatrix}$$

的前 k 个行向量线性无关，最末行的行向量可以表示为前 k 个行向量的线性组合，因此得 $a_0,a_1,\cdots,a_{k+l-2}$ 有长为 k 的最短线性递归. 而由 $2k\leq k+n-l+1<k+l$，根据引理 1 和定理 1 可知：A_{k-1} 可逆，且 $a_0,a_1,\cdots,a_{k+l-2}$ 这样的序列有 $(q-1)q^{2k-1}$ 种. 但矩阵

$$\begin{pmatrix}a_0&\cdots&a_{l-2}&a_{l-1}\\ \vdots&\vdots&\vdots&\vdots\\ a_k&\cdots&a_{k+l-2}&a_{k+l-1}\end{pmatrix}$$

满秩，因此当 $a_0,a_1,\cdots,a_{k+l-2}$ 取定时，a_{k+l-1} 允许有 $q-1$ 种选择. 取定其中一种，记 $c_0a_{k-i}+\cdots+c_{k-1}a_{i-1}+a_i=0(i=k,\cdots,k+l-2)$，令

$$\boldsymbol{A}=\begin{pmatrix} a_0 & \cdots & a_{l-1} \\ \cdots & \cdots & \cdots \\ a_{k-1} & \cdots & a_{l+k-2} \\ a_k & \cdots & a_{l+k-1} \\ \cdots & \cdots & \cdots \\ a_{n-l+1} & \cdots & a_n \end{pmatrix},$$

则矩阵 $\boldsymbol{A}$ 经过初等变换可以变为

$$\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ddots & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & \cdots & 1 & 0 & \cdots & \cdots & 0 \\ c_0 & \cdots & c_{k-1} & 1 & 0 & \cdots & 0 \\ 0 & c_0 & \cdots & c_{k-1} & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & c_0 & \cdots & c_{k-1} & 1 \end{pmatrix} \boldsymbol{A}=$$

$$\begin{pmatrix} a_0 & \cdots & a_{k-1} & \cdots & a_{l-1} \\ \cdots & \cdots & \cdots & \cdots & \vdots \\ a_{k-1} & \cdots & a_{2k-2} & \cdots & a_{l+k-2} \\ 0 & \cdots & \cdots & 0 & c \\ \vdots & \vdots & \vdots & \iddots & * \\ 0 & \cdots & c & * & * \end{pmatrix},$$

其中 $c\neq 0$，“$*$”代表计算得到的任意数值，也就是说，$a_{k+l},\cdots,a_n$ 可取任意值，所以此种序列 $a_0,a_1,\cdots,a_n$ 共有 $(q-1)q^{2k-1}(q-1)q^{n+1-k-l}=(q-1)^2q^{n+k-l}$ 种. 因此，T_n 中最短线性递归长度为 l 且 $2l>n+1$ 的序列共有

$$(q-1)q^{n-l+1}+\Big(\sum_{k=1}^{n-l+1}q^{k-1}\Big)q^{n-l+1}(q-1)^2=$$

$(q-1)q^{2(n-l+1)}$ 种.

定理 2 得证. 证毕.

从定理 1 和定理 2 可以看出，当序列长度 $n+1$ 为偶数时，l 为 $(n+1)/2$ 的概率最大，为 $(q-1)/q$；而序列长度 $n+1$ 为奇数时，l 为 $(n+1)/2+1$ 的概率最大，也为 $(q-1)/q$.

参 考 文 献

1 Reeds J. A., Sloane N. J. A.. Shift-register synthesis (modulo m). Siam Titles on Computing, 1985, 14(3): 505～513

2 Feng Gui-Liang, Zeng Kai-Ming. An iterative algorithm for multi-sequence shift-register synthesis. Science in China, 1985, 15(8): 740～748(in Chinese)
(冯贵良，曾开明. 多个序列最短线性移位寄存器综合的迭代算法. 中国科学, 1985, 15(8): 740～748)

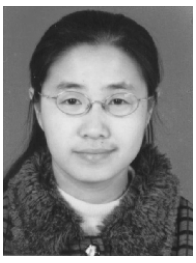
3 Zhou Yu-Jie, Zhou Jin-Jun. The relationship between two kinds of sequences syntheses algorithm over ring $Z/(m)$. In: Proceedings of the 5th Chinese Cryptology Academic Conference Collection, Chengdu, 1998, 24～29(in Chinese)
(周玉洁，周锦君. 环 $Z/(m)$ 上两种序列综合算法之间的关系. 见：第 5 届中国密码学学术会议论文集，成都, 1998, 24～29)

4 Zhou Jin-Jun, Qi Wen-Feng, Zhou Yu-Jie. Gröbner base extension and multi-sequences comprehensive algorithm over $Z/(m)$. Science in China, 1995, 25(2): 113～120(in Chinese)
(周锦君，戚文峰，周玉洁. Gröbner 基推广及 $Z/(m)$ 上多条序列综合算法. 中国科学, 1995, 25(2): 113～120)

5 Ye Ding-Feng, Dai Zong-Duo. Periodic sequence linear order of complexity under two marks replacing. In: Proceedings of the 4th Chinese Cryptology Academic Conference Collection, Zhengzhou, 1996, 7～9(in Chinese)
(叶顶锋，戴宗铎. 两个符号替换下周期序列的线性复杂度. 见：第 4 届中国密码学学术会议论文集，郑州, 1996, 7～9)

6 Feng Gui-Liang, Tzeng K. K.. A generalized Euclidean algorithm for multisequence shift-register synthesis. IEEE Transactions on Information Theory, 1989, 35(3): 584～594

7 Feng Gui-Liang, Tzeng K. K.. A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes. IEEE Transactions on Information Theory, 1991, 37(5): 1274～1287



YIN Qian, born in 1975, lecturer and Ph. D. candidate. Her major research interests include computer cryptology, software reliability.

LUO Yun-Lun, born in 1948, Ph. D., associate professor. His major research interest is computer cryptology.

HU Xiao-Hong, born in 1976, M. S.. Her major research interest is computer cryptology.

FU Xin-Li, born in 1976, M. S.. Her major research interest is computer cryptology.

Background

The major research interests of this group are computer cryptology. This paper is supported by the National Natural Science Foundation of China (Project No. 60275002) and the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CUHK4182/03E).

There is no clear description about the distribution of the length of shortest linear recurrence in other research works. In this paper, the distribution of the shortest linear recurrent length (SLRL) is completely obtained.