软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(4):952−961 [doi: 10.3724/SP.J.1001.2012.04006]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一类本原σ-LFSR 序列的构造与计数*

谭刚敏[1+], 曾 光[1,2], 韩文报[1], 刘向辉[1]

[1](解放军信息工程大学 信息工程学院,河南 郑州 450002)

[2](中国科学院 软件研究所 信息安全国家重点实验室,北京 100190)

Construction and Enumeration of a Class of Primitive σ-LFSR Sequences

TAN Gang-Min[1+], ZENG Guang[1,2], HAN Wen-Bao[1], LIU Xiang-Hui[1]

[1](Institute of Information Engineering, PLA Information Engineering University, Zhengzhou 450002, China)

[2](State Key Laboratory of Information Security, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: tgm157999@163.com

Tan GM, Zeng G, Han WB, Liu XH. Construction and enumeration of a class of primitive σ-LFSR sequences. *Journal of Software*, 2012,23(4):952−961. http://www.jos.org.cn/1000-9825/4006.htm

Abstract: The coordinate sequences of a primitive σ-LFSR sequence over GF(2^k) are *m*-sequences with the same minimal polynomial over GF(2), thus a primitive σ-LFSR sequence over GF(2^k) can be constructed by *m*-sequences over GF(2) if its interval vector is known. This paper studies the calculation of interval vectors of a class of primitive σ-LFSR sequences—Z primitive σ-LFSR sequences and presents an improved method to calculate the interval vectors of Z primitive σ-LFSR sequences in order *n* over GF(2^k), which uses the interval vectors of Z primitive σ-LFSR sequences of order 1 to calculate that of Z primitive σ-LFSR sequences in order *n* over GF(2^k). In addition, it is more effective than other existing methods. More importantly, the new method can also be applied to the calculation of interval vectors of *m*-sequences over GF(2^k). The enumeration formula of Z primitive σ-LFSR sequences of order *n* over GF(2^k) is also presented, which shows that the number of Z primitive σ-LFSR sequences of order *n* is much larger than the number of *m*-sequences of order *n* over GF(2^k).

Key words: stream cipher; primitive σ-LFSR; *m*-sequence; interval vector; linear complexity; enumeration

摘 要: 有限域 GF(2^k)上本原 σ-LFSR 序列的分量序列均是二元域上具有相同极小多项式的 *m*-序列,已知一条 GF(2^k)上本原 σ-LFSR 序列的距离向量,就可以用二元域上的 *m*-序列构造它.研究了一类本原 σ-LFSR 序列——Z 本原 σ-LFSR 序列距离向量的计算问题.给出了一种 GF(2^k)上 *n* 级 Z 本原 σ-LFSR 序列距离向量的计算方法,其主要思想是,利用 GF(2^k)上 1 级 Z 本原 σ-LFSR 序列的距离向量来计算 *n* 级 Z 本原 σ-LFSR 序列的距离向量.与其他现有方法相比,该方法的效率更高.更有价值的是,该方法也适用于 GF(2^k)上 *n* 级 *m*-序列距离向量的计算.最后给出了 GF(2^k)上 *n* 级 Z 本原 σ-LFSR 序列的计数公式,说明其个数比 GF(2^k)上 *n* 级 *m*-序列更多.

关键词: 流密码;本原 σ-LFSR;*m*-序列;距离向量;线性复杂度;计数

中图法分类号: TP309 **文献标识码**: A

* 基金项目: 国家自然科学基金(61003291); 国家高技术研究发展计划(863)(2009AA01Z417); 新世纪优秀人才计划(NCET-07-0384); 全国优秀博士学位论文作者专项基金(FANEDD-2007B74)

收稿时间: 2010-01-24; 修改时间: 2010-10-11; 定稿时间: 2011-03-07

在流密码算法的设计中,良好的初始源序列产生部件是算法安全性的一个重要保证.长期以来,由于能够产生大周期及伪随机性质良好的序列,基于线性反馈移位寄存器(linear feedback shift register,简称 LFSR)产生的*m*-序列一直是流密码中常用的初始源序列.但是随着现代信息技术的发展,传统的二元 *m*-序列已不能满足对流密码算法安全性和效率的要求.因此,对有限域 GF(2^k)上 LFSR、TSR、σ-LFSR、T 函数、多重序列等序列产生部件的研究引起了国内外学者的广泛兴趣.著名的流密码算法 SOSEMANUK[1],SNOW2.0[2],SOBER-t32[3]等,均是基于 GF(2^{32})上 *m*-序列设计的.

现代 CPU 的性能和速度已大为提升,如果能将 CPU 中常用运算与流密码算法设计结合在一起,那么算法实现将具有更高的效率.而且现代 CPU 都是基于字设计的,可以满足字流密码的发展趋势.σ-LFSR[4−10]便是在这种背景下提出的一类字移位寄存器模型,它不仅具有 LFSR 的优点,而且适合快速软件实现.有限域上 *m*-序列仅是本原σ-LFSR 序列的一种特殊形式.目前,关于σ-LFSR 已有不少研究成果:文献[5]研究了一类快速实现的三项式σ-LFSR,并给出一个本原σ-LFSR 的搜索算法;文献[6]给出了本原σ-LFSR 序列的迹表示及基判别定理;文献[7]讨论了基于 *m*-序列的本原σ-LFSR 序列构造;文献[8]研究了本原σ-LFSR 序列的线性复杂度;文献[9]研究了特殊情形下本原σ-LFSR 序列的计数问题.

最近几年,关于多重序列的研究也逐渐成为密码学者关注的热点之一.由于 GF(2^k)≅GF(2)^k,所以,任意 GF(2^k)上的序列均可看作 GF(2)上 *k* 重二元序列.即,任意 GF(2^k)上的序列均可通过 GF(2)上 *k* 条序列的并行实现来得到.当前,对多重序列的研究主要集中在序列复杂度方面的研究[11−14].

在实际应用中,为了达到良好的伪随机特性,多重序列的分量序列应选择具有良好统计特性的序列,*m*-序列是一个较好的选择.GF(2^k)上本原σ-LFSR 序列的分量序列都是 GF(2)上平移等价的 *m*-序列,故可将本原σ-LFSR 序列看成是一类特殊的多重序列,即各分量序列极小多项式相同的多重序列.此时,GF(2^k)上本原σ-LFSR 序列的产生可以通过 *k* 条 GF(2)上 *m*-序列的并行实现来完成.研究本原σ-LFSR 序列与已有经典 *m*-序列之间的固有关系、深入挖掘二者的性质、研究两个不同的生成方式是不是存在交集部分、并且如何用另外方式生成的问题具有重要意义.由于 *m*-序列的研究成果已十分丰富,因此,对 *m*-序列和本原σ-LFSR 序列关系的研究有助于研究本原σ-LFSR 序列的其他性质.文献[15]首次证明了 GF(2^k)上 *m*-序列的分量序列均是 GF(2)上极小多项式相同的 *m*-序列,提出用 GF(2)上 *m*-序列构造 GF(2^k)上 *m*-序列的思想,并给出一个 GF(2^k)上 *m*-序列距离向量应满足的条件.文献[4]证明了 GF(2^k)上本原σ-LFSR 序列的分量序列也为 GF(2)上 *m*-序列.文献[7]在文献[4]的基础上给出一个基于 *m*-序列构造本原σ-LFSR 序列的算法.对于 GF(2^k)上 *n* 级本原σ-LFSR 序列的构造,算法需判断 *kn*×*kn* 矩阵的可逆性,复杂性较高.本文给出一类本原σ-LFSR 序列——Z 本原σ-LFSR 序列的构造方法.指出 GF(2^k)上 *n* 级 Z 本原σ-LFSR 序列的距离向量可由 GF(2^k)上 1 级 Z 本原σ-LFSR 序列的距离向量来计算得到,且在计算的同时也确定了 *n* 级 Z 本原σ-LFSR 序列的极小多项式和线性复杂度.进一步证明了 GF(2^k)上 *n* 级 *m*-序列的距离向量也可由 GF(2^k)上 1 级 *m*-序列的距离向量来计算得到.最后,给出了 GF(2^k)上 *n* 级 Z 本原σ-LFSR 序列的计数公式,说明其选择空间比 *m*-序列更加广阔.

本文第 1 节介绍σ-LFSR 相关知识.第 2 节研究 Z 本原σ-LFSR 序列的构造.第 3 节给出 Z 本原σ-LFSR 序列的计数公式.第 4 节给出一个构造 Z 本原σ-LFSR 序列的例子.第 5 节总结全文.

1 准备知识

1.1 σ-LFSR模型

σ-LFSR 的主要思想是引入循环移位操作,本节仅介绍它的一个等价模型.关于 σ-LFSR 的详细知识可参见文献[4,5,9].

定义 1. 设 *n* 是一个正整数,M_k(GF(2))表示 GF(2)上的 *k* 阶矩阵环,$C_0,C_1,\ldots,C_{n-1}$ 是 M_k(GF(2))上的元素.若 GF(2^k)上的序列 $\boldsymbol{S}=s_0,s_1,s_2,\ldots$满足关系

$$s_{i+n}=C_0s_i+C_1s_{i+1}+\ldots+C_{n-1}s_{i+n-1},i=0,1,2,\ldots,$$

则称 $\boldsymbol{S}$ 为 GF(2^k)上的 *n* 级 σ-LFSR 序列.多项式 $F(x)=x^n+C_{n-1}x^{n-1}+\ldots+C_1x+C_0$ 为它的 σ-特征多项式,生成 $\boldsymbol{S}$ 的次

数最低的 σ-特征多项式称为 σ-极小多项式.

定义 2. 如果 $\boldsymbol{S}$ 为 GF(2^k)上 n 级 σ-LFSR 序列且周期 T 为 $2^{kn}-1$,则称 $\boldsymbol{S}$ 为本原 σ-LFSR 序列.

显然,GF(2^k)上的 m-序列一定是本原 σ-LFSR 序列.因此,本原 σ-LFSR 序列的性质对 m-序列也成立.在实际应用中,本原 σ-LFSR 序列具有重要价值.

1.2 基本性质

定义 3. 设 $\boldsymbol{S}$ 是 GF(2^k)上的 σ-LFSR 序列,视 GF(2^k)为 GF(2)上的 k 维线性空间,$\{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\}$为其上一组基,则 $\boldsymbol{S}$ 可看作 GF(2)上的 k 维向量序列,它可写成

$$\boldsymbol{S}=S_0\lambda_0+S_1\lambda_1+\ldots+S_{k-1}\lambda_{k-1},$$

称 GF(2)上序列 S_i 为 $\boldsymbol{S}$ 的第 i 条分量序列,其中,$0\leqslant i\leqslant k-1$.

下文中,$\boldsymbol{S}=s_0,s_1,s_2,\ldots$表示 GF($2^k$)上序列,$S_i=s_{i,0},s_{i,1},s_{i,2},\ldots$表示序列 $\boldsymbol{S}$ 的第 i 条分量序列,其中 $0\leqslant i\leqslant k-1$.

引理 1[4]. 若 $\boldsymbol{S}$ 是 GF(2^k)上的 n 级本原 σ-LFSR 序列,其 σ-极小多项式为 $F(x)$,则它的 k 条分量序列都为 GF(2)上的 kn 级 m-序列且具有相同的极小多项式,即为 $F(x)$的行列式$|F(x)|$.

定义 4. 设 GF(2^k)在 GF(2)上的一组基为$\{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\}$,$\boldsymbol{S}$ 为 GF(2^k)上周期为 T 的序列.若 $\boldsymbol{S}$ 的分量序列都是 GF(2)上平移等价的 m-序列,则 $\boldsymbol{S}$ 可表示为

$$\boldsymbol{S}=L^{d_0}S_0\lambda_0+L^{d_1}S_0\lambda_1+\ldots+L^{d_{k-1}}S_0\lambda_{k-1},$$

其中,S_i 是 GF(2)上的 m-序列;L^tS_i 表示将 S_i 右移 t 位,t 为整数,$0\leqslant d_i\leqslant T-1$,$0\leqslant i\leqslant k-1$.称 $D_k=(d_0,d_1,\ldots,d_{k-1})$为序列 $\boldsymbol{S}$ 的距离向量.显然有 $d_0=0$.

由引理 1,显然可以定义本原 σ-LFSR 序列的距离向量.

对于 GF(2^k)上本原 σ-LFSR 序列,可以按照分量序列极小多项式对其进行分类:若 $f(x)$为 GF(2)上 kn 次本原多项式,则所有分量序列极小多项式为 $f(x)$的 n 级本原 σ-LFSR 序列为一类,称为 $f(x)$-类.对于同类中的本原 σ-LFSR 序列,一个距离向量对应唯一的本原 σ-LFSR 序列[7].因此,如果已知 GF(2^k)上 n 级 $f(x)$-类本原 σ-LFSR 序列的距离向量,就可以用 $f(x)$生成的 m-序列来构造它们.

下面给出本原 σ-LFSR 序列的基判别定理,它是基于 m-序列构造本原σ-LFSR 序列的基础.

引理 2[6,10]. 设 $\boldsymbol{S}$ 是 GF(2^k)上的序列,则 $\boldsymbol{S}$ 是 n 级本原σ-LFSR 序列当且仅当:

(I) $\boldsymbol{S}$ 的 k 条分量序列均为 GF(2)上极小多项式相同的 m-序列,且极小多项式为 GF(2)上 kn 次本原多项式;

(II) 设$\alpha\in$GF(2^k)为条件(I)中本原多项式的一个根,$D_k=(d_0,d_1,\ldots,d_{k-1})$为 $\boldsymbol{S}$ 的距离向量,则集合

$$A=\{\alpha^{d_0},\alpha^{d_0+1},\ldots,\alpha^{d_0+n-1},\alpha^{d_1},\alpha^{d_1+1},\ldots,\alpha^{d_1+n-1},\ldots,\alpha^{d_{k-1}},\alpha^{d_{k-1}+1},\ldots,\alpha^{d_{k-1}+n-1}\} \quad (1)$$

构成 GF(2^{kn})在 GF(2)上的一组基.

2 Z 本原σ-LFSR 序列的构造

距离向量是本原 σ-LFSR 序列的特征量.对于一般本原 σ-LFSR 序列,其距离向量的计算较为复杂.但是,对于一类本原 σ-LFSR 序列,其距离向量的分布却具有很强的规律性.

下面给出 Z 本原 σ-LFSR 序列的定义.为叙述方便,下文中若无特殊说明,$z=(2^{kn}-1)/(2^k-1)$.

定义 5. 设 $\boldsymbol{S}$ 是 GF(2^k)上 n 级本原 σ-LFSR 序列,其距离向量 $D_k=(d_0,d_1,\ldots,d_{k-1})$.若 d_i 满足 $z|d_i$,则称 $\boldsymbol{S}$ 是 GF(2^k)上 n 级 Z 本原 σ-LFSR 序列,其中,$0\leqslant i\leqslant k-1$.

由定义 5 可知,Z 本原 σ-LFSR 序列只是本原 σ-LFSR 序列的一种特殊形式,GF(2^k)上 1 级本原 σ-LFSR 序列一定是 Z 本原 σ-LFSR 序列.文献[15]研究了 m-序列的分量序列和距离向量的若干性质,得到如下重要结论.

引理 3[15]. 设 $\boldsymbol{S}$ 是 GF(2^k)上的 n 级 m-序列,$\boldsymbol{S}$ 的距离向量为 $D_k=(d_0,d_1,\ldots,d_{k-1})$,则 $z|d_i$,其中,$0\leqslant i\leqslant k-1$.

引理 3 说明,GF(2^k)上的 m-序列一定是 Z 本原 σ-LFSR 序列.

由引理 1 可知,对于 GF(2)上任意 kn 次本原多项式 $f(x)$,可以用其生成的 m-序列来构造 GF(2^k)上 n 级 $f(x)$-类 Z 本原 σ-LFSR 序列.因此,有如下定义:

定义 6. 设 $f(x)$是 GF(2)上 kn 次本原多项式,$f(x)$的 Z 集合 $Z_{kn}^{(f)}$ 定义为

$$Z_{kn}^{(f)}=\{D_k=(d_0,d_1,\ldots,d_{k-1})|D_k \text{ 满足条件I}\},$$

其中,条件I为 $z|d_i,0\leqslant i\leqslant k-1$,且 GF($2^k$)上分量序列极小多项式为 $f(x)$,距离向量为 D_k 的序列是 n 级本原 σ-LFSR 序列.

由定义 6 可知, $Z_{kn}^{(f)}$ 即为 GF(2^k)上所有 n 级 $f(x)$-类 Z 本原 σ-LFSR 序列距离向量的集合.下文中将讨论如何快速计算 $Z_{kn}^{(f)}$.

2.1 Z本原σ-LFSR序列的距离向量

定理 1. 设 $f(x)$是 GF(2)上 kn 次本原多项式,α为 $f(x)$的一个根,则α^z 是 GF(2)上一个 k 次本原多项式 $g(x)$的一个根.定义对应关系φ为

$$\varphi:\begin{cases}Z_{kn}^{(f)}\to Z_{k\cdot 1}^{(g)}\\(d_0,d_1,...,d_{k-1})\to(d_0/z,d_1/z,...,d_{k-1}/z)\end{cases},$$

则φ是双射.

证明:若α为 GF(2^{kn})上本原元,则α^z 为 GF(2^k)上本原元.定理的第 1 部分成立.

若 $D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$,由引理 2 可知,集合 A 构成 GF(2^{kn})在 GF(2)上的一组基,其中,A 如公式(1)所示.设 L 为 GF(2)上添加 $\{\alpha^{d_0},\alpha^{d_1},...,\alpha^{d_{k-1}}\}$ 构成的线性空间,有[L:GF(2)]=k.因为α^z 为 GF(2^k)上的本原元且 $z|d_i,0\leqslant i\leqslant k-1$,所以 α^{d_i} 均为 GF(2^k)上的元素,即 $L\subseteq$GF(2^k).又因为[GF(2^k):GF(2)]=k,所以 L=GF(2^k), $\{\alpha^{d_0},\alpha^{d_1},...,\alpha^{d_{k-1}}\}$ 为 L 在 GF(2)上的一组基.设 $e_i=d_i/z$,则 $\{(\alpha^z)^{e_0},(\alpha^z)^{e_1},...,(\alpha^z)^{e_{k-1}}\}$ 构成 GF(2^k)在 GF(2)上的一组基.由引理 2 可知,GF(2^k)上以 $E_k=(e_0,e_1,\ldots,e_{k-1})$为距离向量,$g(x)$为分量序列极小多项式的序列是 1 级本原 σ-LFSR 序列.显然,此序列是 Z 本原 σ-LFSR 序列.进一步地有 $E_k\in Z_{k\cdot 1}^{(g)}$,$\varphi$是映射.

若 $E_k=(e_0,e_1,\ldots,e_{k-1})\in Z_{k\cdot 1}^{(g)}$, α^z 是 $g(x)$的一个根,则由引理 2, $\{(\alpha^z)^{e_0},(\alpha^z)^{e_1},...,(\alpha^z)^{e_{k-1}}\}$ 构成 GF(2^k)在 GF(2)上的一组基.因为α为 GF(2^{kn})上的本原元,所以$\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$构成 GF($2^{kn}$)在 GF($2^k$)上的一组基.因此,

$$\{\alpha^{e_0z},\alpha^{e_0z+1},...,\alpha^{e_0z+n-1},\alpha^{e_1z},\alpha^{e_1z+1},...,\alpha^{e_1z+n-1},...,\alpha^{e_{k-1}z},\alpha^{e_{k-1}z+1},...,\alpha^{e_{k-1}z+n-1}\}$$

构成 GF(2^{kn})在 GF(2)上的一组基.再利用引理 2,$(d_0,d_1,\ldots,d_{k-1})=(e_0z,e_1z,\ldots,e_{k-1}z)\in Z_{kn}^{(f)}$, φ是满射.

设$\beta=\alpha^z$,由前面的证明可知:$(e_0,e_1,\ldots,e_{k-1})\in Z_{k\cdot 1}^{(g)}$ 当且仅当 $\{\beta^{e_0},\beta^{e_1},...,\beta^{e_{k-1}}\}$ 构成 GF(2^k)在 GF(2)上的一组基,$(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$ 当且仅当集合A构成GF(2^{kn})在GF(2)上的一组基.因为$\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$构成GF($2^{kn}$)在GF($2^k$)上的一组基且 $\alpha^{d_i}\in$GF(2^k),所以 A 构成 GF(2^{kn})在 GF(2)上的一组基当且仅当 $\{\alpha^{d_0},\alpha^{d_1},...,\alpha^{d_{k-1}}\}$ 构成 GF(2^k)在GF(2)上的一组基.即, $\{\beta^{d_0/z},\beta^{d_1/z},...,\beta^{d_{k-1}/z}\}$ 构成 GF(2^{kn})在 GF(2)上的一组基.因此有 $|Z_{kn}^{(f)}|=|Z_{k\cdot 1}^{(g)}|$.

综上,φ是双射. □

定理 1 说明,计算任意 GF(2)上 kn 次本原多项式 $f(x)$的 Z 集合可以通过计算 GF(2)上 k 次本原多项式 $g(x)$的 Z 集合来得到.即,GF(2^k)上所有 n 级 $f(x)$-类 Z 本原 σ-LFSR 序列的距离向量集合可由 GF(2^k)上所有 1 级 $g(x)$-类 Z 本原 σ-LFSR 序列的距离向量集合计算得到.根据文献[7],求取 $g(x)$的 Z 集合仅需判断 $k\times k$ 矩阵的可逆性.

推论 1. 设 $f(x),h(x)$是 GF(2)上 kn 次本原多项式,α,β分别是 $f(x),h(x)$的根.若α^z,β^z 在 GF(2)上的极小多项式相同,则 $Z_{kn}^{(f)}=Z_{kn}^{(h)}$.

证明:设α^z 在 GF(2)上极小多项式为 $g(x)$,定义

$$\varphi_1:\begin{cases}Z_{kn}^{(f)}\to Z_{k\cdot 1}^{(g)}\\(d_0,d_1,...,d_{k-1})\to(d_0/z,d_1/z,...,d_{k-1}/z)\end{cases},$$

$$\varphi_2:\begin{cases}Z_{kn}^{(h)}\to Z_{k\cdot 1}^{(g)}\\(d_0,d_1,...,d_{k-1})\to(d_0/z,d_1/z,....,d_{k-1}/z)\end{cases}.$$

由定理 1 可知,φ_1,φ_2 均为双射,且 $Z_{kn}^{(f)}=Z_{kn}^{(h)}$. □

由推论 1 可知,可以根据 Z 集合将 GF(2)上 $\frac{\phi(2^{kn}-1)}{kn}$ 个 kn 次本原多项式分为 $\frac{\phi(2^k-1)}{k}$ 类($\phi(x)$为欧拉函数),

每一类中本原多项式的Z集合相同.在构造GF(2^k)上所有n级Z本原σ-LFSR序列时,只需计算GF(2)上$\frac{\phi(2^k-1)}{k}$个k次本原多项式的Z集合,就可得到GF(2)上所有kn次本原多项式的Z集合.

事实上,如果知道了GF(2)上一个kn次本原多项式的Z集合,就可以计算出GF(2)上所有kn次本原多项式的Z集合.

定理 2. 设$f(x),h(x)$是GF(2)上两个kn次本原多项式,α,β分别是$f(x),h(x)$的根,则必存在整数$l,(l,T)=1$,使得$\beta=\alpha^l$.此时有$Z_{kn}^{(h)}=\{D_k=(l^{-1}d_0(\mathrm{mod}T),l^{-1}d_1(\mathrm{mod}T),\ldots,l^{-1}d_{k-1}(\mathrm{mod}T))|(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}\}$,其中,$T=2^{kn}-1$.

证明:设$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$,由引理2可知,集合$A$构成GF($2^{kn}$)在GF(2)上的一组基,其中,$A$如公式(1)所示.由定理1的证明可知,$\{\alpha^{d_0},\alpha^{d_1},\ldots,\alpha^{d_{k-1}}\}$构成GF($2^k$)在GF(2)上的一组基,即$\{\beta^{l^{-1}d_0},\beta^{l^{-1}d_1},\ldots,\beta^{l^{-1}d_{k-1}}\}$构成GF($2^k$)在GF(2)上的一组基.又$\beta$为GF($2^{kn}$)上本原元,所以$\{1,\beta,\ldots,\beta^{n-1}\}$构成GF($2^{kn}$)在GF($2^k$)上的一组基.从而,

$$\{\beta^{l^{-1}d_0},\beta^{l^{-1}d_0+1},\ldots,\beta^{l^{-1}d_0+n-1},\beta^{l^{-1}d_1},\beta^{l^{-1}d_1+1},\ldots,\beta^{l^{-1}d_1+n-1},\ldots,\beta^{l^{-1}d_{k-1}},\beta^{l^{-1}d_{k-1}+1},\ldots,\beta^{l^{-1}d_{k-1}+n-1}\}$$

也构成GF(2^{kn})在GF(2)上的一组基.由引理2,$(l^{-1}d_0(\mathrm{mod}T),l^{-1}d_1(\mathrm{mod}T),\ldots,l^{-1}d_{k-1}(\mathrm{mod}T))\in Z_{kn}^{(h)}$,且$|Z_{kn}^{(h)}|\geqslant|Z_{kn}^{(f)}|$.

同理,有$|Z_{kn}^{(f)}|\geqslant|Z_{kn}^{(h)}|$,从而有$|Z_{kn}^{(h)}|=|Z_{kn}^{(f)}|$.

综上,$Z_{kn}^{(h)}=\{D_k=(l^{-1}d_0(\mathrm{mod}T),l^{-1}d_1(\mathrm{mod}T),\ldots,l^{-1}d_{k-1}(\mathrm{mod}T))|(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}\}$. □

2.2 Z本原σ-LFSR序列的线性复杂度

对于σ-LFSR序列,其线性复杂度分为GF(2^k)上的线性复杂度和GF(2)上的线性复杂度.本文中,σ-LFSR序列的线性复杂度均表示GF(2^k)上的线性复杂度.

本节说明GF(2^k)上n级Z本原σ-LFSR序列的极小多项式和线性复杂度可分别由1级Z本原σ-LFSR序列的极小多项式和线性复杂度计算得到.首先给出本原σ-LFSR序列的迹表示[6].

设GF(2^k)上n级本原σ-LFSR序列$\boldsymbol{S}$的k条分量序列为$S_0,S_1,\ldots,S_{k-1}$,$Tr_1^{kn}(x)$表示GF(2^{kn})到GF(2)上的迹函数.由引理1可知,S_i为GF(2)上kn级m-序列,其中,$0\leqslant i\leqslant k-1$.设$S_i$的极小多项式为$f(x)$,$\alpha$为$f(x)$的一个根.由$m$-序列的迹表示,存在$\beta_i\in$GF($2^{kn}$),使得

$$s_{i,t}=Tr_1^{kn}(\beta_i\alpha^t) \tag{2}$$

又$f(x)$为GF(2)上kn次本原多项式,则$f(x)$可分解为$f(x)=f_0(x)f_1(x)\ldots f_{k-1}(x)$,其中,$f_i(x)$为GF($2^k$)上$n$次本原多项式.不妨设$\alpha^{2^i}$为$f_i(x)$的根.设$S_{f_i}$表示GF($2^k$)上由$f_i(x)$生成的序列($S_{f_i}$可以为全0序列),由序列的分解可知$\boldsymbol{S}=\sum_{i=0}^{k-1}S_{f_i}$.存在$\theta_i\in$GF($2^{kn}$),使得

$$s_{f_i,t}=Tr_1^{kn}(\theta_i\alpha^{2^i t}) \tag{3}$$

此时,若$\theta_0,\theta_1,\ldots,\theta_{k-1}$中有$u(1\leqslant u\leqslant k)$个数不为0,不妨设$\theta_0,\theta_1,\ldots,\theta_{u-1}$不为0,$\theta_u,\theta_{u+1},\ldots,\theta_{k-1}$均为0,则$\boldsymbol{S}$的极小多项式为$f_0(x)f_1(x)\ldots f_{u-1}(x)$,线性复杂度为$un$.

为方便起见,下文中$\beta_0,\beta_1,\ldots,\beta_{k-1}$如公式(2)所示,$\theta_0,\theta_1,\ldots,\theta_{k-1}$如公式(3)所示.

文献[8]研究了本原σ-LFSR序列的线性复杂度,得到如下结论.

引理 4[8]. 设GF(2^k)在GF(2)上一组基为$\{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\}$,$\boldsymbol{S}$为GF($2^k$)上分量序列极小多项式为$f(x)$的$n$级本原$\sigma$-LFSR序列,$\alpha$为$f(x)$的一个根,则序列$\boldsymbol{S}$的线性复杂度为$un$当且仅当$\theta_0,\theta_1,\ldots,\theta_{k-1}$这$k$个数中有且仅有$u$个不为0且

$$\left.\begin{aligned}&\theta_0=\beta_0\lambda_0+\ldots+\beta_{k-1}\lambda_{k-1}\\&\theta_1=\beta_0^2\lambda_0+\ldots+\beta_{k-1}^2\lambda_{k-1}\\&\ldots\\&\theta_{k-1}=\beta_0^{2^{(k-1)}}\lambda_0+\ldots+\beta_{k-1}^{2^{(k-1)}}\lambda_{k-1}\end{aligned}\right\} \tag{4}$$

引理 5. 设GF(2^k)在GF(2)上的一组基为$\{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\}$,$\boldsymbol{S}$为GF($2^k$)上分量序列极小多项式为$f(x)$的$n$级本

原σ-LFSR序列,α为$f(x)$的一个根,$\boldsymbol{S}$的距离向量$D_k=(d_0,d_1,\ldots,d_{k-1})$,则$\boldsymbol{S}$的线性复杂度为$un$当且仅当$\eta_0,\eta_1,\ldots,\eta_{k-1}$这$k$个数中有且仅有$u$个不为0,其中,

$$\left.\begin{aligned}&\eta_0=\lambda_0+\alpha^{d_1}\lambda_1+\ldots+\alpha^{d_{k-1}}\lambda_{k-1}\\&\eta_1=\lambda_0+\alpha^{2d_1}\lambda_1+\ldots+\alpha^{2d_{k-1}}\lambda_{k-1}\\&\ldots\\&\eta_{k-1}=\lambda_0+\alpha^{2^{k-1}d_1}\lambda_1+\ldots+\alpha^{2^{k-1}d_{k-1}}\lambda_{k-1}\end{aligned}\right\}\tag{5}$$

证明:由引理4,$\boldsymbol{S}$的线性复杂度为un当且仅当$\theta_0,\theta_1,\ldots,\theta_{k-1}$这$k$个数中有且仅有$u$个不为0且公式(4)成立.

因为α为GF(2^{kn})上的本原元,所以存在整数l,使得$\beta_0=\alpha^l$.由距离向量的定义可知,$\beta_i=\alpha^{l+d_i}$,其中,$0\leqslant i\leqslant k-1$.令$\eta_i=(\beta_0^{2^i})^{-1}\theta_i$,则公式(5)成立.显然,$\theta_i=0$当且仅当$\eta_i=0$.因此,序列$\boldsymbol{S}$的线性复杂度为$un$当且仅当$\eta_0,\eta_1,\ldots,\eta_{k-1}$这$k$个数中有且仅有$u$个不为0. □

根据定理2,GF(2^k)上n级Z本原σ-LFSR序列距离向量可由1级Z本原σ-LFSR序列距离向量计算得到.事实上,此时也确定了n级Z本原σ-LFSR序列的线性复杂度.

定理3. 设GF(2^k)在GF(2)上的一组基为$\{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\}$,$f(x)$是GF(2)上$kn$次本原多项式,$\alpha$为$f(x)$的一个根,$\alpha^z$是GF(2)上$k$次本原多项式$g(x)$的一个根,$\varphi$的定义如定理1,则对任意$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$,距离向量为$D_k$的$n$级$f(x)$-类Z本原σ-LFSR序列线性复杂度为$un$当且仅当距离向量为$\varphi(D_k)$的1级$g(x)$-类Z本原σ-LFSR序列线性复杂度为$u$.

证明:设$f(x)$在GF(2^k)上可分解为$f(x)=f_0(x)f_1(x)\ldots f_{k-1}(x)$,其中,$f_i(x)$为GF($2^k$)上的$n$次本原多项式.不妨设$\alpha^{2^i}$为$f_i(x)$的根,其中,$0\leqslant i\leqslant k-1$.若距离向量为$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$的$n$级$f(x)$-类Z本原σ-LFSR序列线性复杂度$un$,由引理5可知,$\eta_0,\eta_1,\ldots,\eta_{k-1}$这$k$个数中有且仅有$u$个不为0,其中,$\eta_0,\eta_1,\ldots,\eta_{k-1}$如公式(5)所示.

设$E_k=(e_0,e_1,\ldots,e_{k-1})=\varphi(D_k)\in Z_{k-1}^{(g)}$,其中,$e_i=d_i/z$,$0\leqslant i\leqslant k-1$.由引理5可知,距离向量为$E_k$的1级$g(x)$-类Z本原σ-LFSR序列线性复杂度为$u$当且仅当$\delta_0,\delta_1,\ldots,\delta_{k-1}$这$k$个数中有且仅有$u$个不为0,其中,

$$\left.\begin{aligned}&\delta_0=\lambda_0+(\alpha^z)^{e_1}\lambda_1+\ldots+(\alpha^z)^{e_{k-1}}\lambda_{k-1}\\&\delta_1=\lambda_0+(\alpha^z)^{2e_1}\lambda_1+\ldots+(\alpha^z)^{2e_{k-1}}\lambda_{k-1}\\&\ldots\\&\delta_{k-1}=\lambda_0+(\alpha^z)^{2^{k-1}e_1}\lambda_1+\ldots+(\alpha^z)^{2^{k-1}e_{k-1}}\lambda_{k-1}\end{aligned}\right\}\tag{6}$$

显然,$\eta_i=\delta_i$.因此,距离向量为D_k的n级$f(x)$-类Z本原σ-LFSR序列线性复杂度为un当且仅当距离向量为$\varphi(D_k)$的1级$g(x)$-类Z本原σ-LFSR序列线性复杂度为u. □

定理4. 设$f(x),h(x)$是GF(2)上两个kn次本原多项式,α,β分别是$f(x),h(x)$的根,且$\beta=\alpha^l$.由定理2,任意$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$,有$E_k=(l^{-1}d_0(\mathrm{mod}T),l^{-1}d_1(\mathrm{mod}T),\ldots,l^{-1}d_{k-1}(\mathrm{mod}T)\in Z_{kn}^{(h)}$..进一步,若距离向量为$D_k$的$n$级$f(x)$-类Z本原σ-LFSR序列线性复杂度为$un$,则距离向量为$E_k$的$n$级$h(x)$-类Z本原σ-LFSR序列线性复杂度也为$un$.

证明:设GF(2^k)在GF(2)上的一组基为$\{\lambda_0,\lambda_1,\ldots,\lambda_{k-1}\}$,$f(x)$在GF($2^k$)上可分解为$f(x)=f_0(x)f_1(x)\ldots f_{k-1}(x)$,其中,$f_i(x)$为GF($2^k$)上的$n$次本原多项式.不妨设$\alpha^{2^i}$为$f_i(x)$的根,其中,$0\leqslant i\leqslant k-1$.若$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$,距离向量为$D_k$的$n$级$f(x)$-类Z本原σ-LFSR线性复杂度为$un$,由引理5可知,$\eta_0,\eta_1,\ldots,\eta_{k-1}$这$k$个数中有且仅有$u$个不为0,其中,$\eta_0,\eta_1,\ldots,\eta_{k-1}$如公式(5)所示.不妨设$\eta_0,\eta_1,\ldots,\eta_{u-1}$这$u$个数不为0,$\eta_u,\eta_{u+1},\ldots,\eta_{k-1}$这$k-u$个数为0.

因为$h(x)$是GF(2)上kn次本原多项式,所以$h(x)$在GF(2^k)上可分解为$h(x)=h_0(x)h_1(x)\ldots h_{k-1}(x)$,其中,$h_i(x)$为GF($2^k$)上$n$次本原多项式,不妨设$\beta^{2^i}$为$h_i(x)$的根.令

$$\left.\begin{aligned}&\omega_0=\lambda_0+\beta^{l^{-1}d_1}\lambda_1+\ldots+\beta^{l^{-1}d_{k-1}}\lambda_{k-1}\\&\omega_1=\lambda_0+\beta^{2l^{-1}d_1}\lambda_1+\ldots+\beta^{2l^{-1}d_{k-1}}\lambda_{k-1}\\&\ldots\\&\omega_{k-1}=\lambda_0+\beta^{2^{k-1}l^{-1}d_1}\lambda_1+\ldots+\beta^{2^{k-1}l^{-1}d_{k-1}}\lambda_{k-1}\end{aligned}\right\}\tag{7}$$

则$\eta_i=\omega_i$,即$\omega_0,\omega_1,\ldots,\omega_{u-1}$这$u$个数不为0,$\omega_u,\omega_{u+1},\ldots,\omega_{k-1}$这$k-u$个数为0.由引理5可知,距离向量为$E_k$的$n$级$h(x)$-类Z本原$\sigma$-LFSR序列的极小多项式为$h_0(x)h_1(x)\ldots h_{u-1}(x)$,线性复杂度为$un$. □

2.3 GF(2^k)上m-序列的构造

本节指出,GF(2^k)上n级m-序列的距离向量也可由1级m-序列距离向量计算得到.

有限域上m-序列一定是Z本原σ-LFSR序列,下面的引理从线性复杂度的角度来判断Z本原σ-LFSR序列是否为m-序列.

引理6[8]. GF(2^k)上n级本原σ-LFSR序列的线性复杂度为n当且仅当它是GF(2^k)上n级m-序列.

对于任意GF(2)上kn级m-序列,可用其构造GF(2^k)上n级m-序列[15].进一步地,若GF(2)上kn级m-序列极小多项式为$f(x)$,设$f(x)=f_0(x)f_1(x)\ldots f_{k-1}(x)$,其中,$f_i(x)$为GF($2^k$)上$n$次本原多项式,则该序列构造的$m$条GF($2^k$)上$n$级$m$-序列极小多项式分别为$f_0(x),f_1(x),\ldots,f_{k-1}(x)$.

定义7. 设$f(x)$是GF(2)上kn次本原多项式,$f(x)$的M集合$M_{kn}^{(f)}$定义为

$$M_{kn}^{(f)}=\{D_k=(d_0,d_1,\ldots,d_{k-1})|D_k\text{满足条件II}\},$$

其中,条件II为:GF(2^k)上分量序列极小多项式为$f(x)$,距离向量为D_k的序列是n级m-序列.

由定义可知,$|M_{kn}^{(f)}|=k$且$M_{kn}^{(f)}\subseteq Z_{kn}^{(f)}$.

定理5. 设$f(x)$是GF(2)上kn次本原多项式,α为$f(x)$的一个根,则α^z是GF(2)上k次本原多项式$g(x)$的一个根.定义对应关系ψ为

$$\psi:\begin{cases}M_{kn}^{(f)}\to M_{k\cdot 1}^{(g)}\\(d_0,d_1,\ldots,d_{k-1})\to(d_0/z,d_1/z,\ldots,d_{k-1}/z)\end{cases},$$

则ψ是双射.

证明:若$f(x)$是GF(2)上kn次本原多项式,则对任意$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$,$D_k\in M_{kn}^{(f)}$当且仅当距离向量为$D_k$的$f(x)$-类Z本原$\sigma$-LFSR序列是GF($2^k$)上$n$级$m$-序列.由引理6可知,只需证明$D_k=(d_0,d_1,\ldots,d_{k-1})\in Z_{kn}^{(f)}$且距离向量为$D_k$的$n$级$f(x)$-类Z本原$\sigma$-LFSR序列线性复杂度为$n$当且仅当$E_k=(e_0,e_1,\ldots,e_{k-1})\in Z_{k\cdot 1}^{(g)}$且距离向量为$E_k$的1级$g(x)$-类Z本原$\sigma$-LFSR序列线性复杂度为1,其中,$e_i=d_i/z$.由定理1可知,$D_k\in Z_{kn}^{(f)}$当且仅当$E_k\in Z_{m\cdot 1}^{(g)}$.由定理3可知,距离向量为$D_k$的$n$级$f(x)$-类本原$\sigma$-LFSR序列线性复杂度为$n$当且仅当距离向量为$E_k$的1级$g(x)$-类Z本原$\sigma$-LFSR序列线性复杂度为1. □

由定理2和定理4可知,下面的推论是显然的.

推论2. 设$f(x),h(x)$是GF(2)上两个kn次本原多项式,α,β分别是$f(x),h(x)$的根,则必存在整数$l,(l,T)=1$,使得$\beta=\alpha^l$.此时,有$M_{kn}^{(h)}=\{D_k=(l^{-1}d_0(\mathrm{mod}T),l^{-1}d_1(\mathrm{mod}T),\ldots,l^{-1}d_{k-1}(\mathrm{mod}T))|(d_0,d_1,\ldots,d_{k-1})\in M_{kn}^{(f)}\}$,其中,$T=2^{kn}-1$.

由定理5可知,对于GF(2)上kn次本原多项式$f(x),f(x)$的M集合可由GF(2)上一个k次本原多项式的M集合计算得到.由推论2可知,如果知道了GF(2)上1个kn次本原多项式的M集合,就可以计算出GF(2)上所有kn次本原多项式的M集合.

3 Z本原σ-LFSR序列的计数

本原σ-LFSR序列的计数问题是一个公开问题,目前这个问题尚未得到解决,仅有一个猜想[4,9].本节给出Z本原σ-LFSR序列的计数公式.

关于GF(2)上可逆矩阵的计数,有下面的引理.

引理7[9]. GF(2)上k阶可逆方阵的个数$|GL_k(\mathrm{GF}(2))|=\prod_{i=0}^{k-1}(2^k-2^i)$.

定理6. GF(2^k)上n级Z本原σ-LFSR序列的个数为

$$\frac{\phi(2^{kn}-1)}{kn}\cdot 2^{k-1}\cdot|GL_{k-1}(\mathrm{GF}(2))|,$$

其中,$|GL_{k-1}(\mathrm{GF}(2))|=\prod_{i=0}^{k-2}(2^{k-1}-2^i)$, $\phi(x)$为欧拉函数.

证明:设 $f(x)$是 GF(2)上任意 kn 次本原多项式,α为 $f(x)$的一个根.对任意距离向量 $D_k=(d_0,d_1,d_2,\ldots,d_{k-1}),z|d_i$, $0\leqslant i\leqslant k-1$.设 $\boldsymbol{S}$ 是 GF(2^k)上分量序列极小多项式为 $f(x)$,距离向量为 D_k 的序列.由引理 2 可知,$\boldsymbol{S}$ 是 GF(2^k)上 n 级 Z 本原 σ-LFSR 序列当且仅当集合 A 构成 GF(2^{kn})在 GF(2)上的一组基,其中,A 如公式(1)所示.由定理 1 的证明可知,A 构成 GF(2^{kn})在 GF(2)上的一组基当且仅当 $(\alpha^{d_0},\alpha^{d_1},\ldots,\alpha^{d_{k-1}})$ 构成 GF(2^k)在 GF(2)上的一组基.显然,有 $d_0=0$.因此, GF(2^k)上 n 级 Z 本原 σ-LFSR 序列的个数即为集合 $X=\{(1,\beta^{x_1},\beta^{x_2},\ldots,\beta^{x_{k-1}})\,|\,x_j\in[1,2^k-1],1\leqslant j\leqslant k-1\}$ 中能够构成 GF(2^k)在 GF(2)上基的元素个数,其中,$\beta=\alpha^z$.

若 $Y=(1,\beta^{y_1},\beta^{y_2},\ldots,\beta^{y_{k-1}})\in X$ 是 GF(2^k)在 GF(2)的一组基,则集合 X 中其他任意一组基都可以由 Y 经过一个可逆线性变换得到.令矩阵

$$V_k=\begin{pmatrix}1 & v_{12} & \cdots & v_{1k}\\ 0 & v_{22} & \cdots & v_{2k}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & v_{k2} & \cdots & v_{kk}\end{pmatrix}=\begin{pmatrix}1 & \theta\\ 0 & V_{k-1}\end{pmatrix}$$

表示可逆变换所对应的矩阵,其中,θ为 $k-1$ 维向量,V_{k-1} 为 $k-1$ 阶方阵,则每一组基对应一个可逆方阵 V_k,X 中能够构成 GF(2^k)在 GF(2)上基的元素个数等价于 V_k 可逆的个数.显然,V_k 可逆当且仅当 V_{k-1} 可逆.由引理 7 可知,GF(2)上 $k-1$ 阶可逆方阵的个数为 $|GL_{k-1}(\mathrm{GF}(2))|=\prod_{i=0}^{k-2}(2^{k-1}-2^i)$.对于每一个可逆方阵 V_{k-1},θ的取法有 2^{k-1} 种,则 V_k 可逆的取法共有 $2^{k-1}\cdot GL_{k-1}|(\mathrm{GF}(2))|$种.因此,GF($2^k$)上分量序列极小多项式为 $f(x)$的 n 级 Z 本原 σ-LFSR 序列的个数为 $2^{k-1}\cdot GL_{k-1}|(\mathrm{GF}(2))|$.又因为 GF(2)上 kn 次本原多项式的个数为 $\frac{\phi(2^{kn}-1)}{kn}$, 所以,GF($2^k$)上 n 级 Z 本原 σ-LFSR 序列的个数为 $\frac{\phi(2^{kn}-1)}{kn}\cdot 2^{k-1}\cdot|GL_{k-1}(\mathrm{GF}(2))|$. □

定理 6 说明,GF(2^k)上 n 级 Z 本原 σ-LFSR 序列的个数比 n 级 m-序列的个数要多,后者的个数为 $\frac{\phi(2^{kn}-1)}{n}$.

4 例 子

本节给出一个例子来说明 Z 本原 σ-LFSR 序列的构造方法.以 GF(2^3)上 Z 本原 σ-LFSR 序列的构造为例,取 GF(2^3)在 GF(2)上的一组基为$\{1,\lambda,\lambda^2\}$,其中,λ为 GF(2)上 3 次本原多项式 $p(x)$的一个根,$p(x)=x^3+x+1$.

由于 GF(2)上共有 2 个 3 次本原多项式,故所有 $3n$ 次本原多项式按照 Z 集合可分为 2 类.要构造 GF(2^3)上所有 n 级 Z 本原 σ-LFSR 序列,必须计算 2 个 3 次本原多项式的 Z 集合.由定理 2 可知,仅需计算 1 个 3 次本原多项式的 Z 集合即可.表 1 给出了 GF(2)上所有 3 次本原多项式的 Z 集合,表中线性复杂度表示 Z 集合中元素对应本原 σ-LFSR 序列的线性复杂度.如,距离向量为(0,1,4),分量序列极小多项式为 $g_1(x)$的 Z 本原 σ-LFSR 序列线性复杂度为 1.

Table 1 Z sets of all primitive polynomials of degree 3 over GF(2)

表 1 GF(2)上所有 3 次本原多项式的 Z 集合

类别	本原多项式	Z 集合	线性复杂度
1	$g_1(x)=x^3+x+1$	(0,1,4) (0,2,1) (0,4,2)	1
		(0,1,2) (0,1,5) (0,1,6) (0,2,3) (0,2,4) (0,2,5) (0,3,2) (0,3,4) (0,3,5) (0,3,6) (0,4,1) (0,4,3) (0,4,6) (0,5,1) (0,5,2) (0,5,3) (0,5,6) (0,6,1) (0,6,3) (0,6,4) (0,6,5)	3
2	$g_2(x)=x^3+x^2+1$	(0,3,5) (0,6,3) (0,5,6)	1
		(0,1,2) (0,1,3) (0,1,4) (0,1,6) (0,2,1) (0,2,4) (0,2,5) (0,2,6) (0,3,1) (0,3,4) (0,3,6) (0,4,1) (0,4,2) (0,4,3) (0,4,5) (0,5,2) (0,5,3) (0,5,4) (0,6,1) (0,6,2) (0,6,5)	3

下面我们利用表 1 来构造 GF(2^3)上所有 2 级 Z 本原 σ-LFSR 序列.由第 3 节的分析可知,此时只需计算 GF(2)上所有 6 次本原多项式的 Z 集合即可.而由定理 1 可知,GF(2)上 6 次本原多项式的 Z 集合可通过 GF(2)上 3 次本原多项式的 Z 集合计算得到.

以 GF(2)上 6 次本原多项式 $f_1(x)=x^6+x^5+1$ 为例.设 α 为 $f_1(x)$的一个根,则 α^z 是表 1 中 $g_1(x)$的一个根,这里,$z=9$.根据定理 1,$f_1(x)$的 Z 集合可通过 $g_1(x)$的 Z 集合中各个元素的分量乘以 z 来得到.由定理 3 可知,此时,$f_1(x)$的 Z 集合中元素对应 Z 本原 σ-LFSR 序列的线性复杂度也是确定的.根据定理 2 和定理 4,可以计算出 GF(2)上所有 6 次本原多项式的 Z 集合和 Z 集合中元素对应 Z 本原 σ-LFSR 序列的线性复杂度,计算结果见表 2.

Table 2 Z sets of all primitive polynomials of degree 6 over GF(2)

表 2 GF(2)上所有 6 次本原多项式的 Z 集合

类别	本原多项式	Z 集合	线性复杂度
1	$f_1(x)=x^6+x^5+1$ $f_2(x)=x^6+x^4+x^3+x+1$ $f_3(x)=x^6+x^5+x^2+x+1$	(0,9,36) (0,18,9) (0,36,18)	2
		(0,9,18) (0,9,45) (0,9,54) (0,18,27) (0,18,36) (0,18,45) (0,27,18) (0,27,36) (0,27,45) (0,27,54) (0,36,9) (0,36,27) (0,36,54) (0,45,9) (0,45,18) (0,45,27) (0,45,54) (0,54,9) (0,54,27) (0,54,36) (0,54,45)	6
2	$f_4(x)=x^6+x+1$ $f_5(x)=x^6+x^5+x^3+x^2+1$ $f_6(x)=x^6+x^5+x^4+x+1$	(0,27,45) (0,54,27) (0,45,54)	2
		(0,9,18) (0,9,27) (0,9,36) (0,9,54) (0,18,9) (0,18,36) (0,18,45) (0,18,54) (0,27,9) (0,27,36) (0,27,54) (0,36,9) (0,36,18) (0,36,27) (0,36,45) (0,45,18) (0,45,27) (0,45,36) (0,54,9) (0,54,18) (0,54,45)	6

利用类似的方法,由表 1 可以构造出 GF(2^3)上所有 n 级 Z 本原 σ-LFSR 序列.同理,利用表 1 也可以构造出 GF(2^3)上所有 n 级 m-序列.

5 结论和下一步工作

研究距离向量的计算对基于 m-序列构造本原 σ-LFSR 序列具有重要意义.本文给出了一种用 GF(2^k)上 1 级 Z 本原 σ-LFSR 序列的距离向量计算 n 级 Z 本原 σ-LFSR 序列距离向量的方法,该方法也适用于 GF(2^k)上 m-序列距离向量的计算.在用 GF(2)上 m-序列构造 GF(2^k)上 n 级 Z 本原 σ-LFSR 序列(m-序列)时,利用本文中的方法只需计算 GF(2^k)上 1 级 Z 本原 σ-LFSR 序列(m-序列)的距离向量,当 n 较大时,复杂度显著降低.

距离向量是本原 σ-LFSR 序列的重要参数.大量实验表明,距离向量和本原 σ-LFSR 序列的其他性质(如本原 σ-LFSR 序列的采样性质)存在一定关系,但目前这种关系尚不清楚,也很少有这方面的文献.因此,对本原 σ-LFSR 序列距离向量的进一步研究将是很有意义的工作.

致谢 在此,我们向对本文提出建设性意见的审稿人表示衷心的感谢.

References:

[1] Berbain C, Billet O, Canteaut A, Courtois N, Gilbert H, Goubin L, Gouget A, Granboulan L, Lauradoux C, Minier M, Pornin T, Sibert H. SOSEMANUK, a fast software-oriented stream cipher. In: Robshaw M, Billet O, eds. Proc. of the New Stream Cipher Designs. LNCS 4986, Berlin, Heidelberg: Springer-Verlag, 2008. 98−118. [doi: 10.1007/978-3-540- 68351-3_9]

[2] Ekdahl P, Johansson T. A new version of the stream cipher SNOW. In: Nyberg K, Heys H, eds. Proc. of the SAC 2002. LNCS 2595, Berlin, Heidelberg: Springer-Verlag, 2002. 47−61. [doi: 10.1007/3-540-36492-7_5]

[3] Hawkes P, Rose G. Primitive specification and supporting documentation for SOBER-t32 submission to NESSIE. In: Proc. of the 1st NESSIE Workshop. Heverlee, 2000. https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions.html

[4] Zeng G, Han WB, He KC. High efficiency feedback shift register: σ-LFSR. Technical Report, 2007/114, Cryptology ePrint Archive, 2007. http://eprint.iacr.org/2007/114

[5] Zeng G, He KC, Han WB. A trinomial type of σ-LFSR oriented toward software implementation. Science in China (Series F: Information Sciences), 2007,50(3):359−372. [doi: 10.1007/s11432-008-0036-y]

[6] Zhang M, Zeng G, Han WB, He KC. Trace representation of primitive σ-LFSR sequences and its application. Journal of Electronics & Information Technology, 2009,31(4):942−945 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2008.00028]

[7] Liu XH, Han WB, Zeng G. Construction of primitive σ-LFSR sequences from *m*-sequences. Journal of Sichuan University (Natural Science Edition), 2009,46(6):1645−1649 (in Chinese with English abstract). [doi: 103969/j.issn.0490-6756.2009.06.015]

[8] Liu XH, Zeng G, Han WB. Research on linear complexity of primitive σ-LFSR sequences. Journal of Electronics & Information Technology, 2009,31(12):2897−2900 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2008.01701]

[9] Chorpade SR, Hasan SU, Lumari M. Primitive polynomials, singer cycles, and word-oriented linear feedback shift registers. Designs, Codes and Cryptography, 2011,58(2):123−134. [doi: 10.1007/s10623-010-9387-7]

[10] Niederreiter H. The multiple-recursive matrix method for pseudorandom number generation. Finite Fields and Their Application, 1995,1(1):3−30. [doi: 10.1006/ffta.1995.1002]

[11] Hu HG, Hu L, Feng DG. On the expected value of the joint 2-adic complexity of periodic binary multisequences. In: Gong G, Helleseth H, Song HY, Yang K, eds. Proc. of the Sequences and Their Applications (SETA 2006). LNCS 4086, Berlin, Heidelberg: Springer-Verlag, 2006. 199−208. [doi: 10.1007/11863854_17]

[12] Meidl W, Niederreiter H, Venkateswarlu A. Error linear complexity measures for multisequences. Journal of Complexity, 2007, 23(2):169−192. [doi: 10.1016/j.jco.2006.10.005]

[13] Fu FW, Niederreiter H, Özbudak F. Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences. Finite Fields and Their Application, 2009,15(4):475−496. [doi: 10.1016/j.ffa.2009.03.001]

[14] Dong LH, Hu YP, Zeng Y. Joint *k*-error 2-adic complexity for binary periodic multi-sequences. Chinese Journal of Computers, 2009,32(6):1134−1139 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2009.01134]

[15] Park WJ Jr, Komo JJ. Relationships between *m*-sequences over GF(q) and GF(q^m). IEEE Trans. on Information Theory, 1989,35(1): 183−186.

附中文参考文献:

[6] 张猛,曾光,韩文报,何开成.本原 σ-LFSR 序列的迹表示及其应用.电子与信息学报,2009,31(4):942−945. [doi: 10.3724/SP.J.1146.2008.00028]

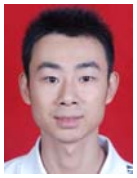
[7] 刘向辉,韩文报,曾光.基于 *m*-序列的本原 σ-LFSR 序列构造.四川大学学报(自然科学版),2009,46(6):1645−1649. [doi: 103969/j.issn.0490-6756.2009.06.015]

[8] 刘向辉,曾光,韩文报.本原 σ-LFSR 序列的线性复杂度研究.电子与信息学报,2009,31(12):2897−2900. [doi: 10.3724/SP.J.1146.2008.01701]

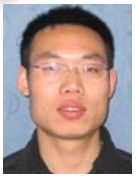
[14] 董丽华,胡予濮,曾勇.多重周期二元序列的联合 *k* 错 2-adic 复杂度.计算机学报,2009,32(6):1134−1139. [doi: 10.3724/SP.J.1016.2009.01134]

谭刚敏(1986－),男,陕西武功人,硕士生,主要研究领域为流密码设计与分析.

韩文报(1963－),男,教授,博士生导师,主要研究领域为密码学,信息安全.



曾光(1980－),男,博士,讲师,CCF 会员,主要研究领域为密码学.



刘向辉(1984－),男,博士生,主要研究领域为密码学.