$GF(q)$上广义自缩序列的线性复杂度

王慧娟,王锦玲
(郑州大学数学系,河南郑州 450001)

摘 要: 针对基于 $GF(q)$上 m-序列的广义自缩序列,本文利用一种新手段给出线性复杂度上界值.主要讨论素数 q 大于等于 3 时,$GF(q)$上广义自缩序列的线性复杂度.对于 $GF(3)$上广义自缩序列,把以往 $GF(3)$上广义自缩序列的线性复杂度的上界缩小得到一个更精确地上界值.拓展到大于 3 的素数,给出 $GF(q)$上广义自缩序列的线性复杂度精确上界值.

关键词: 线性复杂度; 广义自缩序列; m-序列; 特征多项式; 流密码
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 02-0414-05

The Linear Complexity of the Generalized Self-Shrinking Generator on $GF(q)$

WANG Hui-juan, WANG Jin-ling
(*Mathematics Department, Zhengzhou University, Zhengzhou, Henan* 450001, *China*)

Abstract: The purpose is to discuss the linear complexity of the generalized self-shrinking generator which is based on the m-sequences of $GF(q)$, and analyze the linear complexity on the condition when prime q greater than 3. Reach the upper bound of the generalized self-shrinking generator linear complexity on $GF(3)$, and diminish the linear complexity upper bound. The linear complexity upper bound on $GF(q)$ can have better accurate value.

Key words: linear complexity; m-sequences; generalized self-shrinking; characteristic polynomial; stream cipher

1 引言

以 m-序列作为驱动,通过处理获得良好的密钥序列是近几年的研究热点.其中线性复杂度是序列密码的一个重要指标.在以往的文献中只用了单一的手法来证明序列的线性复杂度的上界值.本文基于 $GF(q)(q\geqslant 3)$上 m-序列构造出的广义自缩序列,用另一手段给出广义自缩序列更为精确的线性复杂度上界值,这样对研究广义自缩序列具有深刻的密码学意义,并且能从广义自缩序列的整体层面上分析一类自缩序列的线性复杂度.广义自缩序列是从整体层面上来分析一类自缩序列的伪随机性问题,此类广义自缩序列更适合流密码的应用,所以研究广义自缩序列的线性复杂度具有深刻的密码学意义.

下面定义$GF(3)$和 $GF(q)$上的广义自缩序列:

定义 1 设 $a^{\infty}=a_0,a_1,a_2\cdots$是 $GF(3)$上的 n 级 m-序列,其中 $a_i\in GF(3)$, $G_1=(g_{10},g_{11},g_{12},\cdots g_{1n})$, $G_2=(g_{20},g_{21},g_{22},\cdots g_{2n})$,其中 $G_1,G_2\in GF(3)^n$,这时得到序列 $V_1^{\infty}=v_{10},v_{11},v_{12},\cdots,V_2^{\infty}=v_{20},v_{21},v_{22},\cdots$,其中 $v_{1k}=g_{10}a_k+g_{11}a_{k-1}+\cdots+g_{1n-1}a_{k-n+1}$, $v_{2k}=g_{20}a_k+g_{21}a_{k-1}+\cdots+g_{2n-1}a_{k-n+1}$, $k=0,1,2,\cdots$,若 $a_k=1$ 则输出 v_{1k};若 $a_k=2$ 则输出 v_{2k};否则放弃输出.我们把由这种输出模型输出的序列叫做 $GF(3)$上广义自缩序列,记为 $b^{\infty}=b_0,b_1,b_2\cdots$.

定义 2 设 $r^{\infty}=r_0,r_1,r_2\cdots$是 $GF(q)$上的 n 级 m-序列,其中 $r_i\in GF(q)$, $G_1=(g_{10},g_{11},g_{12},\cdots g_{1n})$, $G_2=(g_{20},g_{21},g_{22},\cdots g_{2n})$,其中 $G_1,G_2\in GF(q)^n$,这时得到序列 $V_1^{\infty}=v_{10},v_{11},v_{12},\cdots,V_2^{\infty}=v_{20},v_{21},v_{22},\cdots$,其中 $v_{1k}=g_{10}r_k+g_{11}r_{k-1}+\cdots+g_{1n-1}r_{k-n+1}$, $v_{2k}=g_{20}r_k+g_{21}r_{k-1}+\cdots+g_{2n-1}r_{k-n+1}$, $k=0,1,2,\cdots$,若 $r_k^{\frac{q-1}{2}}=1$ 则输出 v_{1k};若 $r_k^{\frac{q-1}{2}}=q-1$ 则输出 v_{2k};否则放弃输出.我们把由这种输出模型输出的序列叫做 $GF(q)$上广义自缩序列,记为 $s^{\infty}=s_0,s_1,s_2\cdots$.

由广义自缩序列的输出模型可以看出,$q=3$ 时,正是定义 1 的输出序列.并且只有当 $r_k=0(a_k=0)$时没有元素输出,所以$(q-1)q^{n-1}$是输出序列 s^{∞}的一个周期.那么输出序列 s^{∞}有特征多项式 $1-x^{(q-1)q^{n-1}}=(1-x^{\frac{(q-1)}{2}})^{q^{n-1}}$

收稿日期:2009-09-21;修回日期:2010-04-20
基金项目:河南省教育厅自然科学指导性计划项目(No.200510459003)

$(1+x^{\frac{(q-1)}{2}})^{q^{n-1}}$.输出序列 s^∞ 的线性复杂度是指序列 b^∞ 所满足的极小多项式的次数,笔者从 $(1-x^{\frac{(q-1)}{2}})^{q^{n-1}}$ 入手,来讨论满足序列 s^∞ 的特征多项式.

2　基础知识

在证明结论之前,先介绍几个引理.

引理 1　设 T 是 $GF(q^n)$ 到 $GF(q)$ 的任一线性投射,则存在 $c\in GF(q^n)$,有 $T(x)=Tr(cx)$,其中对任意的 x 属于 $GF(q^n)$,满足 $Tr(x)=\sum_{i=0}^{n-1}x^{q^i}$.

证明　参见文献[1].

定义 3　设 i 是任一正整数,$w_q(i)$表示 i 的 q 进制中的非零位的个数.

定义 4　设 R 表示次数小于 q^n 的多项式环,定义

$$P_q(k)=\Big\{\sum_{i=0}^{q^{n-1}}a_ix^i\in R\mid \text{当 } w_q(i)\geqslant k+1 \text{ 时},\alpha_i=0\Big\}$$

$$P_q^*(k)=\Big\{\sum_{i=0}^{q^{n-1}}a_ix^i\in R\mid \text{当 } w_q(i)\geqslant k+1 \text{ 时},\ \alpha_i=0 \text{ 且 } \alpha_0=0\Big\}.$$

从 $P_q(k)$的定义可以看出 $P_q(i)$属于 $P_q(j)$,其中 $i\leqslant j$.

引理 2　设 T 是 $GF(q^n)$到 $GF(q)$的一个线性投射,则 $T\in P_q(1)^*$.

证明　有引理 1 知 $\exists\, c\in GF(q^n)$有 $T(x)=Tr(cx)$ 且 $Tr(cx)=\sum_{j=0}^{n-1}c^jx^{q^j}$, $a_{q^j}=c^j$.所以只有当 $Tr(cx)$的系数是第 q^i 项时非零,即 $w_q(i)\geqslant 2$ 时 $a_i=0$ 且 $a_0=0$,所以 $T\in P_q^*(1)$.　　证毕.

引理 3　设 $f\in P_q(k_1)$, $g\in P_q(k_2)$,则 $fg\in P_q(k_1+k_2)$;如果 $f\in P_q^*(k_1)$, $g\in P_q(k_2)$,那么 $fg\in P_q^*(k_1+k_2)$.

证明　f,g 中 x 项的次数有以下情况:当 $i_1+i_2\leqslant q^n-1$ 时, $x^{i_1}x^{i_2}=x^{i_1+i_2}$;当 $i_1+i_2\geqslant q^n$ 时, $x^{i_1}x^{i_2}=x^{i_1+i_2-q^n+1}$,其中当 $i_1+i_2\leqslant q^n-1$ 时 $w_q(i_1+i_2)\leqslant w_q(i_1)+w_q(i_2)\leqslant k_1+k_2$,当 $i_1+i_2\geqslant q^n$ 时,$w_q(i_1+i_2-q^n+1)\leqslant w_q(i_1+i_2)-1+1\leqslant k_1+k_2$,得 $fg\in P_q(k_1+k_2)$;

当 $f\in P_q^*(k_1)$时,$f(0)=0$ 且 $fg(0)=f(0)g(0)=0$,所以 $fg\in P_q^*(k_1+k_2)$.　　证毕.

引理 4　设 α 是 $GF(q^n)$上的一个本原元,$f\in P_q^*(k)$,则存在一个 $g\in P_q(k)$,对所有的 $i=\{0,1,2\cdots q^n-2\}$,有 $g(\alpha^i)=\sum_{j=0}^{i}f(\alpha^j)$.

证明　若 $k\leqslant n-1$,设 $f=\sum_{r=1}^{q^n-2}a_rx^r(f\in P_q^*(k))$,

设 $g(x)=\Big(\sum_{r=1}^{q^n-2}a_r\frac{\alpha^r}{\alpha^r-1}x^r\Big)-\sum_{r=1}^{q^n-2}a_r\frac{1}{\alpha^r-1}$,

$$g(\alpha^i)=\Big(\sum_{r=1}^{q^n-2}a_r\frac{\alpha^r}{\alpha^r-1}\alpha^{ir}\Big)-\sum_{r=1}^{q^n-2}a_r\frac{1}{\alpha^r-1}$$

$$=\sum_{j=0}^{i}\Big(\sum_{r=1}^{q^n-2}a_r(\alpha^j)^r\Big)=\sum_{j=0}^{i}f(\alpha^j).$$　　证毕.

引理 5　设 $f\in P_q^*(k)$,$(k\leqslant n-1)$,则

$$\sum_{x\in GF(q^n)/\{0\}}f(x)=0.$$

证明　因为 $f\in P_q^*(k)$,所以 $f(0)=0$,设 $f=\sum_{r=1}^{q^n-2}a_rx^r$ ($a_0=0$, $a_{q^n-1}=0$), $\sum_{\alpha^k\in GF(q^n)}f(\alpha^k)=\sum_{r=1}^{q^n-2}a_r\Big(\frac{\alpha^r}{\alpha^r-1}\alpha^{(q^n-2)r}-\frac{1}{\alpha^r-1}\Big)=\sum_{r=1}^{q^n-2}a_r\Big(\frac{1}{\alpha^r-1}-\frac{1}{\alpha^r-1}\Big)=0$.

证毕.

引理 6　设 r^∞ 是 $GF(q)$上的 n 级 m – 序列,令 $d=\frac{q^n-1}{2}$,将 r^∞ 分成两部分 $r^\infty=(R_1,R_2)$,其中 $R_1=(r_0,r_1,\cdots r_{d-1})$, $R_2=(r_d,r_{d+1},\cdots r_{2d+1})$,则 $R_1=(q-1)R_2$.

证明　在 $GF(q)$上,设 n 级 m – 序列 r^∞的 k 个平移序列记为 r_j^∞, $j=0,1,\cdots k$,任取 k 个常数 l_j, $j=1,2,\cdots k$,则序列 $\sum_{j=0}^{k}l_jr_j^\infty$ 或为零序列,或为 r^∞的一个平移序列(见参考文献[7]),这时我们考虑序列 r^∞和 r_d^∞,有:$r^\infty=(R_1,R_2)$, $r_d^\infty=(R_2,R_1)$, $r^\infty+r_d^\infty=(R_1+R_2,R_2+R_1)$,可以看到 d 是序列 $r^\infty+r_d^\infty$ 的一个周期,所以 $r^\infty+r_d^\infty$ 不是 r^∞的一个平移序列,是一个零序列,既有 $R_1=(q-1)R_2$.　　证毕.

3　$GF(3)$上广义自缩序列的线性复杂度

根据定义 1,由输出模型可以看出,输出序列 b^∞的一个周期为 $2\cdot3^{n-1}$, $x^{2\cdot3^{n-1}}-1$ 是序列 b^∞的一个特征多项式,$x^{2\cdot3^{n-1}}-1=(x^2-1)^{3^{n-1}}=(x-1)^{3^{n-1}}(x-2)^{3^{n-1}}$.这里找到两组周期为 3^{n-1}的序列,设 $\xi_1,\xi_2,\cdots\xi_n$ 是 $GF(3^n)$上的一组基,取 $\xi_1=(0,0,\cdots0,1)$ $\xi_2=(0,0,\cdots1,0)\cdots\xi_n=(1,0,\cdots0,0)$. $GF(3^n)$上的任一元素都可以由 $\xi_1,\xi_2,\cdots\xi_n$ 线性表出,即 $\forall\, x\in GF(3^n)$,存在一组 $a_1,a_2,\cdots a_n\in GF(3)$有 $x=a_1\xi_1+a_2\xi_2+\cdots+a_n\xi_n$.

定义 5　$\forall\, x\in GF(3^n)$且 $x=a_1\xi_1+a_2\xi_2+\cdots+a_n\xi_n$, $a_1,a_2,\cdots a_n\in GF(3)$,设 T 是 $GF(q^n)$到 $GF(q)$的一个线性投射,有 $T(x)=a_1$.

找到满足 $T(x)=1$ 的元素,记为 e_i,那么 e_i 就表示 $GF(3^n)$中最后一位是 1 的 n 长向量,即 $e_i=(*,*\cdots*,1)$,其中 $*$ 表示 $GF(3)$上的任一元素.设序列 $E=$

$e_0e_1\cdots e_i\cdots$,是在 $GF(3^{n-1})$上的周期为 3^{n-1}的序列.同时,满足 $T(x)=2$ 的元素设为 e_i',组成序列 $E'=e_0'e_1'\cdots e_i'\cdots$,也是一个在 $GF(3^{n-1})$上周期为 3^{n-1}的序列,且满足 $E'=2E$.设 $(x-1)^t$ 的展开式为 $\sum_{i=0}^{t}c_ix^i$, $c_i\in GF(3)$,把序列 E、E'代入可得:

$$\begin{aligned}\sum_{i=0}^{t}c_ie_i+\sum_{i=0}^{t}c_ie_i'&=\sum_{t_i}e_{t_i}+\sum_{t_j}2e_{t_j}+\sum_{t_i}e_{t_i}'+\sum_{t_j}2e_{t_j}'\\&=\sum_{t_i}e_{t_i}+\sum_{t_j}e_{t_j}+2\Big(\sum_{t_i}e_{t_i}+\sum_{t_j}e_{t_j}\Big)\\&=\sum_{t_i}e_{t_i}+\sum_{t_j}e_{t_j}+\Big(\sum_{t_i}e_{t_i}'+\sum_{t_j}e_{t_j}'\Big)\\&=\sum_{i=0}^{t}c_i^2e_i+\sum_{i=0}^{t}c_i^2e_i'\end{aligned}$$

其中 $c_{t_i}=1$, $c_{t_j}=2$, $c_i^2=1$.

定理 1 设 e_i 是满足 $T(x)=1$ 的所有 $GF(3^n)$上的元素,则 $\sum_{i=0}^{u}c_i^2e_i=0$,其中 $u=3^{n-1}-\left\lfloor\frac{n-3}{4}-1\right\rfloor$.

证明 e_i 是被加数当且仅当 i 满足 $\binom{3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1}{i}\bmod 3\neq 0$,即当 $\left\lfloor\frac{n-3}{4}\right\rfloor$ 的 3 进制表示的第 k 位是2时,i 的第 k 为表示是0,且当 $\left\lfloor\frac{n-3}{4}\right\rfloor$ 的 3 进制表示的第 k 位是 1 时,i 的第 k 为表示是 1 或 0.

定义 σ 是 $GF(3^n)$到 $GF(3^n)$的一个映射,当 x 是被加数时 $\sigma(x)=x$,其它情况时 $\sigma(x)=0$,所以由 σ 得定可得, $\sum_i c_i^2e_i=\sum_{x\in GF(3^n)}\sigma(x)$,如果可以证明 $\sigma(x)\in P_3^*(n-1)$,有引理 5 我们可以得到 $\sum_{x\in GF(3^n)}\sigma(x)=0$,即 $\sum_{i=0}^{u}c_i^2e_i=0$,而 $u=3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1$.下面证明 $\sigma(x)\in P_3^*(n-1)$.

首先定义函数 $\kappa_k(x)$:当 $x=e_i$, i 被 3^k 整除时 $\kappa_k(x)=1$,其他情况时 $\kappa_k(x)=0$,由数学归纳法来证明 $\kappa_k(x)\in P_3^*(3^k)$.可以发现 $\kappa_0(x)=T\in P_3^*(1)=P_3^*(3^0)$,假设 $\kappa_{k-1}(x)\in P_3^*(3^{k-1})$,命 $g_{k-1}(\alpha^i)=\sum_{j=0}^{i}\kappa_{k-1}(\alpha^j)$,有引理 4 可得 $g_{k-1}(x)\in P_3(3^{k-1})$,当 $\kappa_k(x)=1$ 时当且仅当 $\kappa_{k-1}(x)=1$ 且 $g(x)\neq 0$,所以 $\kappa_k(x)=\kappa_{k-1}(x)g^2(x)$,由引理 3 可得 $\kappa_k(x)\in P_3^*(3^k)$.

设 $\sigma_k(x)=1+g_k^2(x)$, $\sigma_k(x)\in P_3(2\cdot 3^{k-1})$, i 的第 k 位为 3 进制非零时 $\sigma_k(e_i)=1$,其他情况时 $\sigma_k(e_i)=0$, $h_{1k}=\sigma_{1k}$其中 $1k$ 表示 $\left\lfloor\frac{n-3}{4}\right\rfloor$ 的 3 进制表示的第 k 位是时的下标, $h_{2k}=\sigma_{2k}$其中 $\left\lfloor\frac{n-3}{4}\right\rfloor$ 的 3 进制表示的第 k 位是 2 时的下标,这时得到一个函数 $P=XT[\Pi(h_{2k}^4+1)\Pi(h_{1k}+1)^2]$,其中 X 是恒同映射, T 是定义 5 所定义的函数,又由于 $\Pi(h_{2k}^4+1)\Pi(h_{1k}+1)^2\in P_3^*(n-3)$,所以由引理 3 知 $P\in P_3^*(n-1)$. $P(x)=x$ 的充要条件是 $T(x)=1$ 且 $\Pi(h_{2k}^4+1)\Pi(h_{1k}+1)^2=1$,即 $T(x)=1$, $h_{2k}(x)=0$, $h_{1k}(x)\neq 2$.由此可以看出 $P(x)=\sigma(x)\in P_3^*(n-1)$由引理 5 得 $\sum_{x\in GF(3^n)}\sigma(x)=0$,即 $\sum_{i=0}^{u}c_i^2e_i=0$, $u=3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1$. 证毕.

定理 2 设 $GF(3)$上广义自缩序列的线性复杂度为 $LC(b^\infty)$,则 $LC(b^\infty)\leqslant 2\cdot 3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1$.

证明 从定理 1 的证明过程可以看出 $\sum_{i=0}^{u}c_i^2x^i$, $u=3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1$,是序列 E 的一个特征多项式,也是 E'的一个特征多项式.由广义自缩序列的输出模型和引理 6 可以得到, n 级 m – 序列 $a^\infty=a_0,a_1,a_2\cdots$ 控制输出的输出序列 $b^\infty=b_0,b_1,b_2\cdots$满足以下性质:

(1)输出序列 b^∞的一个周期为 $2\cdot 3^{n-1}$.

(2)输出序列 b^∞的一个 $2\cdot 3^{n-1}$周期中 $b_i=v_{1i}$与 $b_j=v_{2j}$的个数相同,都是 3^{n-1}个.

(3)当 $b_i=v_{1i}$时, $b_{i+3^{n-1}}=v_{2i}$, $b_i=v_{2i}$时 $b_{i+3^{n-1}}=v_{1i}$.

利用输出序列 $b^\infty=b_0,b_1,b_2\cdots$的以上性质,如果可以找到两个线性投射 $\Phi:\Phi(e_i)=v_{1k}$, $\Psi:\Psi(e_i')=v_{2k}$,那么就可以得到多项式 $\sum_{i=0}^{u}c_i(x^i+x^{i+3^{n-1}})$, $u=3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1$.将输出序列代入可得: $\sum_{i=0}^{u}c_i(b_i+b_{i+3^{n-1}})=\sum_{i=0}^{u}c_i^2v_{1i}+\sum_{i=0}^{u}c_i^2v_{2i}=\Phi\Big(\sum_{i=0}^{u}c_i^2e_i\Big)+\Psi\Big(\sum_{i=0}^{u}c_i^2e_i'\Big)=0$ 综上所述,可以得到 $GF(3)$上广义自缩序列的线性复杂度上界. 证毕.

其实如果 v_{ik}给定的话, Φ 和 Ψ 很容易找到的.如当 $v_{1k}=a_{k+1}$, $v_{2k}=a_{k+1}+a_{k-1}$,这时正是 $GF(3)$上第四类广义自缩序列(见文献[13]),可设

$\Phi(x)=Tr((c\,\alpha^{3^{n-1}})x)$, $\Psi(x)=Tr((c\,\alpha^{3^{n-1}})x)+Tr((c\,\alpha^{3^{n-1}})x+c\,\alpha^{3^{n-1}}\cdot\alpha^{-1})$,

其中 $c\in GF(3)$, α 是 $GF(3^n)$的本原元

4 $GF(q)$上广义自缩序列的线性复杂度

从 $GF(3)$上广义自缩序列的线性复杂度的证明得

到启发,首先在 $GF(q^n)$ 上找到两组周期为 q^{n-1} 的序列,设 $\xi_1,\xi_2,\cdots\xi_n$ 是 $GF(q^n)$ 上的一组基,取 $\xi_1=(0,0,\cdots0,1),\xi_2=(0,0,\cdots1,0)\cdots\xi_n=(1,0,\cdots0,0)$. $GF(q^n)$ 上的任一元素都可以由 $\xi_1,\xi_2,\cdots\xi_n$ 线性表出,即 $\forall x\in GF(q^n)$,存在一组 $a_1,a_2,\cdots a_n\in GF(q)$ 有 $x=a_1\xi_1+a_2\xi_2+\cdots+a_n\xi_n$. 作投射 $Y:GF(q^n)\to GF(q)$, $Y(x)=a_1^{\frac{q-1}{2}}$,可以看出,即可以得到 $Y(x)\in P_q^*\left(\frac{q-1}{2}\right)$.

定理 3　设 e_i 是满足 $Y(x)=a_1^{\frac{q-1}{2}}=1$ 的所有 $GF(q^n)$ 上的元素,则 $\sum_{i=0}^{u}c_i^{q-1}e_{\frac{q-1}{2}\cdot i}=0$,其中 $u=q^{n-1}-\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor-1,2n\geqslant q+3$.

证明　由数论知识可得,e_i 是被加数 i 当且仅当满足 $\begin{pmatrix}q^{n-1}-\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor-1\\ i\end{pmatrix}\bmod q\neq 0$,即当 $\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor$ 的 q 进制表示的第 k 位是 t_1 时,i 的第 k 为表示是 t_2, t_1、t_2 满足 $q-1-t_1\geqslant t_2$.

定义映射 σ 是 $GF(q^n)$ 到 $GF(q^n)$ 得映射,当 x 是被加数时 $\sigma(x)=x$,其他情况时 $\sigma(x)=0$,所以由 σ 得定义可得, $\sum_i c_i^{q-1}e_{\frac{q-1}{2}\cdot i}=\sum_{x\in GF(q^n)}\sigma(x)$,下面证明 $\sigma(x)\in P_q^*(n-1)$. 设 $\kappa_k(x)$:当 $x=e_i$,i 被 q^k 整除时 $\kappa_k(x)=1$,其他情况时 $\kappa_k(x)=0$,类同定理 1 的证明可得 $\kappa_k(x)\in P_q^*(q^k)$. 设 $\sigma_k(x)=1+(q-1)g_k^{q-1}(x)$,其中 $g_{k-1}(\alpha^i)=\sum_{j=0}^{i}\kappa_{k-1}(\alpha^j)$, $\sigma_k(x)\in P_q((q-1)\cdot q^{k-1})$,且 i 的第 k 位为 q 进制表示非零时 $\sigma_k(e_i)=1$,其他情况时 $\sigma_k(e_i)=0$, $h_{ik}=\sigma_{ik}$其中 ik 表示 $\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor$ 的 q 进制表示的第 k 位是时 i 的下标,这时得到以下映射 $P=XY\prod_k\left\{\prod_{t=1}^{q-1}\left[\prod_{j=1}^{t}(h_{tk}+j)^{q-1}\right]\right\}$, X 是 $GF(q^n)$ 上的 $\frac{q-1}{2}$ 位平移. 通过验证可得 $P(x)=\sigma(x)\in P_q^*(n-1)$. 由引理 5 可得 $\sum_i c_i^{q-1}e_{\frac{q-1}{2}\cdot i}=\sum_{x\in GF(q^n)}\sigma(x)=0$ 其中 $u=q^{n-1}-\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor-1$.　　证毕.

由广义自缩序列的输出模型和引理 6 可以得到,$GF(q^n)$ 上的 m – 序列 $a^\infty=a_0,a_1,a_2\cdots$ 控制输出的输出序列 $b^\infty=b_0,b_1,b_2\cdots$ 满足以下性质:

(1) 输出序列 b^∞ 的一个周期为 $(q-1)\cdot q^{n-1}$.

(2)输出序列 b^∞ 的一个 $(q-1)\cdot q^{n-1}$ 周期中 $b_i=v_{1i}$ 与 $b_j=v_{2j}$ 的个数相同,都是 $\frac{(q-1)}{2}q^{n-1}$ 个.

(3) $b_i=v_{1i}$ 时 $b_{i+\frac{(q-1)}{2}q^{n-1}}=v_{2i}$, $b_i=v_{2i}$ 时 $b_{i+\frac{(q-1)}{2}q^{n-1}}=v_{1i}$.

定理 4　设 $GF(q)$ 上的广义自缩输出序列 b^∞ 的线性复杂度为 $LC(b^\infty)$,满足 $LC(b^\infty)\leqslant(q-1)q^{n-1}-\left(\frac{q-1}{2}\right)\left(\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor+1\right),2n\geqslant q+3$.

证明　根据广义自缩输出序列定义的不同,可以找到两个线性投射, $T':GF(q^n)\to GF(q)$ $T'(e_i)=v_{1k}$, $T'':GF(q^n)\to GF(q)$ $T''(e_i')=v_{2k}$,其中 e_i' 满足 $Y(e_i')=q-1$,其中 $Y(x)=x^{\frac{q-1}{2}}$. 这时可以得到一个线性递归方程 $\sum_{i=0}^{u}c_i(x^{i\cdot\frac{q-1}{2}}+x^{\frac{q-1}{2}(i+q^{n-1})})$,其中 $u=q^{n-1}-\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor-1$. 把输出序列 b^∞ 代入可得, $\sum_{i=0}^{u}c_i\left(b_{i\cdot\frac{q-1}{2}}+b_{\frac{q-1}{2}(i+q^{n-1})}\right)=\sum_{i=0}^{u}c_i^{q-1}v_{1i\cdot\frac{q-1}{2}}+\sum_{i=0}^{u}c_i^{q-1}v_{2i\cdot\frac{q-1}{2}}=T'\left(\sum_{i=0}^{u}c_i^{q-1}e_i\right)+T''\left(\sum_{i=0}^{u}c_i^{q-1}e_i'\right)=0$.

即输出序列 b^∞ 满足线性递归方程 $\sum_{i=0}^{u}c_i(x^{i\cdot\frac{q-1}{2}}+x^{\frac{q-1}{2}(i+q^{n-1})})$,其中 $u=q^{n-1}-\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor-1$. 所以, $LC(b^\infty)\leqslant(q-1)q^{n-1}-\left(\frac{q-1}{2}\right)\left(\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor+1\right)$.　　证毕.

我们知道序列的线性复杂度是该序列极小多项式的次数,由 $GF(q^n)$ 上广义自缩序列的定义可知, $(1-x^{\frac{(q-1)}{2}})^{q^{n-1}}(1+x^{\frac{(q-1)}{2}})^{q^{n-1}}$ 是序列的一个特征多项式,且序列的极小多项式应整除该多项式, $\sum_{i=0}^{u}c_i(x^{i\cdot\frac{q-1}{2}}+x^{\frac{q-1}{2}(i+q^{n-1})})=\sum_{i=0}^{u}c_ix^{i\cdot\frac{q-1}{2}}(1+x^{\frac{q-1}{2}})^{q^{n-1}}=(1-x^{\frac{q-1}{2}})^u(1+x^{\frac{q-1}{2}})^{q^{n-1}}$,所以由以上的定义和证明可以得到 $GF(q)$ 上广义自缩序列的一个特征多项式.

定理 5　$GF(q)$ 上的多项式

$$\sum_{i=0}^{u}c_i(x^{i\cdot\frac{q-1}{2}}+x^{\frac{q-1}{2}(i+q^{n-1})}),$$

其中 $u=q^{n-1}-\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor-1$,则该多项式是 $GF(q)$ 上广义自缩序列的一个特征多项式.

5　结论

本文 $GF(q)$ 上的广义自缩序列是从整体上研究一类自缩序列的线性复杂度,能为在流密码系统的提供多样性和灵活性的应用. 在文献[2]中讨论的 $GF(2)$ 上

的自缩序列是 $GF(2)$上广义自缩序列的特例,若将 $q=2$ 代入$(q-1)q^{n-1}-\left(\frac{q-1}{2}\right)\left(\left\lfloor\frac{2n-q-3}{2(q-1)^2}\right\rfloor+1\right)$(*)中,得到结果不超过文献[2]中,讨论的 $GF(2)$上的自缩序列线性复杂度的上界 $2^{n-1}-(n-2)$,将 $q=3$ 代入(*)式,与 $GF(3)$上的广义自缩序列的线性复杂度的上界 $2\cdot3^{n-1}-\left\lfloor\frac{n-3}{4}\right\rfloor-1$ 相一致.所以广义自缩序列线性复杂度的上界值为广义自缩序列的伪随机性提供良好的理论依据.

这里进行两点猜想:

(1)由于在 $GF(2)$上广义自缩序列线性复杂度的上界没有达到, $GF(q)$上的广义自缩序列的线性复杂度是否还有更小的界值.

(2)根据界值的表达式,是否能断定 $GF(q)$上的广义自缩序列线性复杂度的上界,随着 q 的增大而趋近于广义自缩序列的周期.

参考文献:

[1] Lidl R Niederiter H. Finite Field[M]. US : Addision-wesly Publishing Company, 1983. 47 – 131.

[2] Simon R Blackburn. The linear complexity of the self-shrinking generator[J]. IEEE Transactions on Information Theory, 1991, 45(06): 2073 – 2077.

[3] Hu Yupu, Xiao Guozhen. Generalized-slef shrinking generator [J]. IEEE, Trans on Inform Theory, 2004, 150(04): 714 – 719.

[4] Hu Yupu, Bai Gouqiang, Xiao Guozhen. Generalized-slef shrinking generator on GF(q) [J]. Journal of Xi'an University, 2001. 28(01): 5 – 7.

[5] Hu Yupu, Xiao Guozhen. The minimum period of a new generalized-slef shrinking generator [J]. Journal on Communication, 2003, 24(06): 169 – 176.

[6] 万哲先. 代数和编码[M]. 北京: 高等教育出版社. 2007. 183 – 238.

[7] Hu Yupu, Zhang Yuqing, Xiao Guozhen. Symmetric Key Cryptography [M]. Beijin: China Machine Press, 2002. 119 – 125.

[8] W Meier, O Stafflebach. The self-shrinking Generator [A]. Advanced in Cryptology-Eurocrypt'94[C]. LNCS . Berlin: Springer-verlag, 1995. 205 – 214 .

[9] Dong Lihua, Hu Yupu, Shun Hongbou. The linear complexity of the generalized-self shrinking generator [J]. Chinese Journal of Electronics, 2008, 36(07): 1373 – 1377.

[10] Hu Yupu, Wei Shimin, Xiao Guozhen. The linear complexity of the generalized legendary shrinking and generalized jacobi shrinking [J]. Chinese Journal of Electronics, 2000, 28(02): 113 – 117.

[11] Xi Zejun, Cheng Jiaxing, Liu Zhihua. A new design method for families of sequences with large linear span [J]. Chinese Journal of Electronics, 2008, 36(10): 1961 – 1965.

[12] Wang Jinling, Wang Juanli. A new generalized-slef shrinking generator on GF(q) [J]. Journal of Shandong University, (Natural Science), 2009, 44 (10): 91 – 96.

[13] Wang Huijuan, Wang Jinling, Gong Lvle. The fourth class of generalized self-shrinking sequences on GF(3) [A]. Advances in Cryptology-China Crypt'2009 Proceedings of 2009 Annual Conference of the Chinese Association for Cryptologic Research[C]. Beijing: Science Press, 2009. 58 – 63.

作者简介:

王慧娟 女,汉族,1985 年生,郑州大学数学系硕士研究生,主要研究方向:对称密码学.
E-mail: whj409@163.com

王锦玲 女,汉族,1964 年生,郑州大学数学系硕士研究生导师,副教授,主要从事对称密码学和代数学的研究.
E-mail: wang63227@163.com