扩展在上 $GF(3)$新型自缩序列模型及研究

王锦玲,陈亚华,兰娟丽
WANG Jin-ling,CHEN Ya-hua,LAN Juan-li

郑州大学 数学系,郑州 450001
Department of Mathematics,Zhengzhou University,Zhengzhou 450001,China
E-mail:wang63227@sohu.com

WANG Jin-ling,CHEN Ya-hua,LAN Juan-li.New model and studying of self-shrinking sequence developed on $GF(3)$. Computer Engineering and Applications,2009,45(35):114-119.

Abstract: Self-shrinking sequence is an important kind of pseudo-random sequences.Period and linear complexity are classic measures of pseudo-random sequences.So,it becomes an important issue to construct new models of self-shrinking sequence that could generate sequences with great period and high linear complexity.In view of this question,a new model of self-shrinking sequence over $GF(3)$ is constructed.After the study of the period and linear complexity of the generated sequence using the theory of finite fields,there are some main conclusions:The upper bound of the period is 3^n,the lower bound is $3^{2\lfloor n/3\rfloor}$;The upper bound of linear complexity is 3^n,the lower bound is $3^{2\lfloor n/3\rfloor-1}$.Moreover,the period and linear complexity of the generated sequence based on primitive trinomials and quarternomials of degree n over $GF(3)$ are discussed.

Key words: self-shrinking sequence;period;linear complexity;primitive trinomials;primitive quarternomials

摘 要:自收缩序列是一类重要的伪随机序列,而周期和线性复杂度是序列伪随机性的经典量度。如何构造自缩序列的新模型,使生成序列具有大的周期和高的线性复杂度是一个重要的问题。针对这一问题,构造了 $GF(3)$上一种新型的自缩序列模型,利用有限域理论,研究了生成序列的周期和线性复杂度,得到一些主要结论:周期上界 3^n,下界 $3^{2\lfloor n/3\rfloor}$;线性复杂度上界 3^n,下界 $3^{2\lfloor n/3\rfloor-1}$。进一步讨论了基于 $GF(3)$上本原三项式和四项式的自缩序列的周期和线性复杂度。

关键词:自缩序列;周期;线性复杂度;本原三项式;本原四项式
DOI:10.3778/j.issn.1002-8331.2009.35.035 **文章编号**:1002-8331(2009)35-0114-06 **文献标识码**:A **中图分类号**:TN918.4

1 引言

自收缩序列是 1994 年 Meier 和 Staffelbach 在文献[1]中提出,由于自缩序列生成方式结构简单,具有良好的伪随机性,成为序列密码研究的热点。在文献[1-2]中给出了自缩序列(记为 SS_2-序列)的周期下界 $2^{\lfloor n/2\rfloor}$,线性复杂度下界 $2^{\lfloor n/2\rfloor-1}$,上界 $2^{n-1}-(n-2)$;在文献[3]中,作者对基于 $GF(2)$上本原三项式和五项式的 LFSR 序列的 SS_2-序列,给出了更好的周期下界 $2^{\lfloor n/2\rfloor+1}$ 和线性复杂度下界 $2^{\lfloor n/2\rfloor}$;在文献[4-5]中,作者分别在 $GF(2)$和 $GF(3)$上构造了多位自缩序列(分别记为 MSS_2-序列和 MSS_3-序列),得到 MSS_2-序列的周期上界 2^{n-1},下界 $2^{\lfloor n/3\rfloor}$,线性复杂度下界 $2^{\lfloor n/3\rfloor-1}$;MSS_3-序列的周期下界 $3^{\lfloor n/3\rfloor}$,上界 $2\cdot3^{n-1}$;线性复杂度下界 $3^{\lfloor n/3\rfloor-1}$,上界 $2\cdot3^{n-1}$。在文献[5-6]中给出了基于 $GF(3)$上本原三项式和四项式的 LFSR 序列的 MSS_3-序列的周期下界 $2\cdot3^{\lfloor n/3\rfloor}$,线性复杂度下界 $3^{\lfloor n/3\rfloor}$。虽然多位自缩序列的周期和线性复杂度等安全性指标都有很好的改善,但多位自缩序列在输出比特为 0 时,收缩过快,以致于信息利用率降低,下面来看文献[5]中 MSS_3-序列的生成方式:

若 $a^\infty=(a_0,a_1,a_2\cdots)$是 $GF(3)$上一 n 级 m-序列,a^∞将的输出比特依次排列如下:

$a^\infty=(a_0,a_1,a_2)(a_3,a_4,a_5)\cdots(a_{3k},a_{3k+1},a_{3k+2})\cdots$若 $a_{3k}=0$,则不输出 a_{3k} 所在括号内序列 a^∞ 的比特;若 $a_{3k}=1$,则输出 a_{3k+1};若 $a_{3k}=2$,则输出 a_{3k+2};当序列 a^∞ 在 $a_{3k}=0$ 时,a^∞ 收缩过快过多,为了弥补 MSS_3-序列生成方式中的序列收缩过快过多,信息利用率降低的不足,在 $GF(3)$上重构自缩序列模型。进一步研究 $GF(3)$上新型自缩序列的周期和线性复杂度等伪随机性,与文献[4-7]相比有更好的周期和线性复杂度的界。

基金项目:河南省教育厅自然科学指导性项目(The Guidance Project of Natural Science of Henan Provincial Office of Education under Grant NO.200510459003)。

作者简介:王锦玲(1963-),女,副教授,主要研究方向:代数与密码;陈亚华(1982-),女,在读硕士研究生,主要研究方向:序列密码;兰娟丽(1983-),女,在读硕士研究生,主要研究方向:序列密码。

收稿日期:2008-07-09 **修回日期**:2008-10-23

2　理论基础

定义 1　若 a^∞ 是 $GF(q)$ 上的周期序列，设 $f(x)=x^n-c_{n-1}x^{n-1}-\cdots-c_1x-c_0$，$c_i\in GF(q)$。若 a_i 满足线性递归关系 $a_{n+k}=c_{n-1}a_{n+k-1}+\cdots+c_0a_k$，则称序列 a^∞ 是一个 LFSR 序列。

定义 2　称形式幂级数 $S^\infty(x)=\sum_{n=0}^{\infty}a_nx^n$ 为序列 a^∞ 的生成函数。当 $p(a^\infty)=N$ 时，$S^\infty(x)=S^N(x)\sum_{k=0}^{\infty}x^{kN}$，其中 $S^N(x)=\sum_{n=0}^{N-1}a_nx^n$。

引理 1[7]　设 a^∞ 是周期为 N（不一定是最小周期）的序列，则多项式

$$f(x)=\frac{1-x^N}{gcd(1-x^N,S^N(X))}$$

是序列 a^∞ 的极小多项式。

引理 2[7]　设 $a^\infty=(a_0,a_1,a_2\cdots)$ 是 $GF(3)$ 上一 n 级 m-序列，对于 $0<k\leqslant n$，$GF(3)$ 上任意 k 元组 $(b_1,b_2\cdots b_k)$ 在 a^∞ 的一个周期中出现的次数

$$\mathbb{N}(b_1,b_2\cdots b_k)=\begin{cases}3^{n-k} & 若(b_1,b_2\cdots b_k)\neq0\\ 3^{n-k}-1 & 若(b_1,b_2\cdots b_k)=0\end{cases}$$

引理 3[7]　设 $a^\infty=(a_0,a_1,a_2\cdots)$ 是 $GF(3)$ 上一 n 级 m-序列，则有：

(1)序列 a^∞ 的最小周期是 3^n-1。

(2)序列 a^∞ 是平衡的，即在 a^∞ 的一个周期内，1，2 各出现 3^{n-1} 次，0 出现 $3^{n-1}-1$ 次。

引理 4　设 $f(x)$ 是 $GF(3)$ 上的 n 次本原三项式，a^∞ 与 b^∞ 是由 $f(x)$ 生成的两条 n 级 m-序列，它们导出的序列 z_a^∞ 和 z_b^∞ 是平移等价的，从而 z_a^∞ 和 z_b^∞ 有相同的周期和线性复杂度。

证明　因为 a^∞ 和 b^∞ 是由同一个本原多项式 $f(x)$ 生成的两条 m-序列，所以 a^∞ 与 b^∞ 是平移等价的。即 $a^\infty=x^tb^\infty$，其中 t 表示左移算子。$0\leqslant t\leqslant T-1$，$T=3^n-1$。下面有：

当 $t=0\bmod3$ 时，令 $r=\sum_{i=0}^{t/3-1}a_{3i}$，则有 $z_a^\infty=x^rz_b^\infty$；

当 $t=1\bmod3$ 时，令 $r=\sum_{i=0}^{(t+T)/3-1}a_{3i}$，则有 $z_a^\infty=x^rz_b^\infty$；

当 $t=2\bmod3$ 时，令 $r=\sum_{i=0}^{(t+2T)/3-1}a_{3i}$，则有 $z_a^\infty=x^rz_b^\infty$；

∴结论成立。

3　$GF(3)$ 上新型自缩序列模型的构造

定义 3　设 $a^\infty=(a_0,a_1,a_2\cdots)$ 是 $GF(3)$ 上一 n 级 m-序列，将序列 a^∞ 输出比特依次分组如下：$a^\infty=(a_0,a_1,a_2)(a_3,a_4,a_5)\cdots(a_{3k},a_{3k+1},a_{3k+2})\cdots$ 若 $a_{3k}=0$，则不输出 a_{3k} 所在括号内 a^∞ 的比特；若 $a_{3k}=1$，则输出 a_{3k+1}；若 $a_{3k}=2$，则输出 a_{3k+1},a_{3k+2}；这样得到的序列称 z^∞ 为 $GF(3)$ 上 a^∞ 的自缩序列，记为 SS_3-序列。用图 1 表示序列 z^∞ 的生成过程：

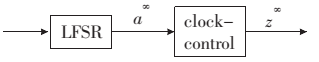

图 1　$GF(3)$ 上 a^∞ 的自缩序列 z^∞ 的生成过程图

下面来看 $GF(3)$ 上 SS_3-序列的一个实例：

例　设 $f(x)=x^2+2x+2=x^2-x-1$ 是 $GF(3)$ 上 2 次本原三项式，$a^\infty=10112022\cdots$ 是由 $f(x)$ 生成的 2 级 m-序列，由引理 3 得：序列 a^∞ 的最小周期为 3^2-1。将 a^∞ 在一个周期段内的输出比特依次分组如下：

$a^\infty=(101)(120)(221)(011)(202)(210)(112)(022)\cdots$ 这样得到 $z^\infty=022102101\cdots$。所以 z^∞ 的最小周期为 $9=3^2$。

下面给出 $GF(3)$ 上 SS_3-序列的周期和线性复杂度的下界，为方便起见，记序列的最小周期为 $p(\cdot)$，线性复杂度为 $L(\cdot)$。

4　周期和线性复杂度

4.1　周期

设 $a^\infty=(a_0,a_1,a_2\cdots)$ 是 $GF(3)$ 上一 n 级 m-序列，将序列 a^∞ 输出比特依次分组如下：

$$(a_0,a_1,a_2)\cdots(a_{3^n-3},a_{3^n-2},a_0)(a_1,a_2,a_3)\cdots(a_{3^n-5},a_{3^n-4},a_{3^n-3})$$
$$(a_{3^n-2},a_0,a_1)\cdots(a_{3^n-4},a_{3^n-3},a_{3^n-2})(a_0,a_1,a_2)$$

由此看到，把序列 a^∞ 的三个周期内输出比特依次分组排列后，(a_0,a_1,a_2) 重复出现。

∴ SS_3-序列 z^∞ 是周期的。

定理 1　设 $a^\infty=(a_0,a_1,a_2)$ 是 $GF(3)$ 上一 n 级 m-序列，z^∞ 为 a^∞ 导出的 SS_3-序列，则 $p(a^\infty)|3^n$。

证明　由引理 2 知：在序列 a^∞ 的一个周期内，每个三元组 $(b_1,b_2,b_3)\neq0$ 出现 3^{n-3} 次，$(b_1,b_2,b_3)=0$ 出现 $3^{n-3}-1$ 次。

∴$(1,*,*)$ 出现 $3\times3\times3^{n-3}=3^{n-1}$ 次，此时 z^∞ 输出 3^{n-1} 个比特。

∴$(2,*,*)$ 出现 $3\times3\times3^{n-3}=3^{n-1}$ 次，此时 z^∞ 输出 $2\cdot3^{n-1}$ 个比特。

∴$(0,*,*)$ 出现 $3\times3\times(3^{n-3}-1)=3^{n-1}-9$ 次，此时 z^∞ 输出 0 个比特。

∴$3^{n-1}+2\cdot3^{n-1}=3^n$ 是 z^∞ 的一个周期，设 z^∞ 的最小周期为 $p(z^\infty)$。

∴ $p(z^\infty)|3^n$，由前面的例子知道，周期上界是可以达到的。

定理 2　SS_3-序列的最小周期 $p(z^\infty)\geqslant3^{2\lfloor n/3\rfloor}$

证明　设 $m=3\lfloor n/3\rfloor$，当 $n=3k$ 时，$m=n$；当 $n=3k+1$ 时，$m=n-1$；当 $n=3k+2$ 时，$m=n-2$。

∵ $a^\infty=(a_0,a_1,a_2)$ 是 $GF(3)$ 上一 n 级 m-序列

∴ $a(3t)\triangleq(a_{3t},a_{3t+1},a_{3t+m-1})$　$t=0,1,2\cdots$ 跑遍了 $GF(3)^m$ 上的所有向量，特别跑遍了如下形式的向量：

(1)$(2,x_0,x_0')(2,x_1,x_1')\cdots(2,x_{m/3},x_{m/3}')$

(2)$(1,x_0,x_0')(1,x_1,x_1')\cdots(1,x_{m/3},x_{m/3}')$

在第一种情况下，$z\ (t)=(z_t,z_t',z_{t+1},z_{t+1}'\cdots z_{t+m/3-1},z_{t+m/3-1}')$，$t=0,1,2\cdots$ 跑遍了 $GF(3)^{2m/3}$ 上的所有向量

∴ $p(z^\infty)\geqslant3^{2\lfloor n/3\rfloor}$

在第二种情况下，$z(t)=(z_t,z_{t+1},\cdots,z_{t+m/3-1})$，$t=0,1,2\cdots$ 跑遍了 $GF(3)^{m/3}$ 上的所有向量

∴ $p(z^\infty)\geqslant3^{\lfloor n/3\rfloor}$

综合两种情况可得:$p(z^\infty)\geqslant 3^{2\lfloor n/3\rfloor}$

由定理 1 和定理 2 知:$3^{2\lfloor n/3\rfloor}\leqslant p(z^\infty)\leqslant 3^n$,$p(z^\infty)$是 3 的幂,且周期上界可以达到。

4.2 SS_3–序列的线性复杂度

定理 3 设 a^∞ 是 $GF(3)$上一 n 级 m–序列,z^∞ 为 a^∞ 导出的 SS_3–序列,则 $3^{2\lfloor n/3\rfloor-1}<L(z^\infty)\leqslant 3^n$。

证明 由定理 1 知:$p(z^\infty)|3^n$,$\therefore f(x)=1-x^{3^n}$是 z^∞ 的一个特征多项式,$\therefore L(z^\infty)\leqslant 3^n$。$\because GF(3)$的特征是 3,$\therefore f(x)=1-x^{3^n}=(1-x)^{3^n}$。

设 $f_z(x)$是 z^∞ 的极小多项式,则 $f_z(x)|f(x)$

$\therefore f_z(x)$可以写成 $(1-x)^t$ 的形式,$t\leqslant 3^n$。

由序列的有理分式表示知:

$$f_z(x)=\frac{1-x^{3^n}}{gcd(1-x^{3^n},S^{3^n}(x))}$$

(1)当 $S^{3^n}(1)\neq 0$ 时,$gcd(1-x^{3^n},S^{3^n}(x))=1$

$\therefore f_z(x)=1-x^{3^n}$

$\therefore L(z^\infty)=3^n$,线性复杂度上界达到。

(2)当 $S^{3^n}(1)=0$ 时,$\gcd(1-x^{3^n},S^{3^n}(x))=(1-x)^a$,$a\geqslant 1$

$\therefore f_z(x)=1-x^{3^n-a}$

$\therefore L(z^\infty)\leqslant 3^n-1$

下证 $L(z^\infty)>3^{2\lfloor n/3\rfloor-1}$

假设 $L(z^\infty)\leqslant 3^{2\lfloor n/3\rfloor-1}$,则 $t\leqslant 3^{2\lfloor n/3\rfloor-1}$

又 $\because (1-x)^{3^{2\lfloor n/3\rfloor-1}}=1-x^{3^{2\lfloor n/3\rfloor-1}}$

$\therefore f_z(x)|1-x^{3^{2\lfloor n/3\rfloor-1}}$

$\therefore p(z^\infty)\leqslant 3^{2\lfloor n/3\rfloor-1}$,这与 $p(z^\infty)\geqslant 3^{2\lfloor n/3\rfloor}$ 矛盾

$\therefore L(z^\infty)>3^{2\lfloor n/3\rfloor-1}$

$\therefore 3^{2\lfloor n/3\rfloor-1}<L(z^\infty)\leqslant 3^n$

由以上结果可以看出:SS_3–序列 z^∞ 的周期和线性复杂度的界是以 3 的指数倍增加,相比文献[5],SS_3–序列具有更高的周期和线性复杂度。而与文献[4–5]的多位自缩序列的模型本质上不同的是,从 a^∞ 的输出比特依次分组 $a^\infty=(a_0,a_1,a_2)(a_3,a_4,a_5)\cdots(a_{3k},a_{3k+1},a_{3k+2})\cdots$中可以看出:每个括号收缩的比特个数与相应括号内的取值是对应相等的,因此该模型也可称为对应自缩序列生成器。在 $a_{3k}=2$ 时,对应括号内输出两个比特,弥补了 $a_{3k}=0$ 时 a^∞ 收缩过快过多的不足,更好地利用了原有的信息率。SS_3–序列 z^∞ 由序列 a^∞ 输出的过程中伴随着收缩,输出和自扩,而整体上是收缩的。SS_3–序列 z^∞ 由序列 a^∞ 来产生,当生成 a^∞ 的级数 n 充分大时,整体收缩比例约为 2/3。事实上,考虑 a^∞ 的 3 个周期,共 $3(3^n-1)$个比特,(0,*,*)出现 $3^{n-1}-1$ 次,收缩了 $3(3^{n-1})=3^n-3$ 个比特;(1,*,*)出现 3^{n-1} 次,收缩了 $2\cdot 3^{n-1}$ 个比特;(2,*,*)出现 3^{n-1} 次,收缩了 3^{n-1} 个比特。所以收缩比例为

$$\frac{3^n-3+2\cdot 3^{n-1}+3^{n-1}}{3^{n+1}-3}=\frac{2\cdot 3^n-3}{3\cdot 3^n-3}\approx\frac{2}{3}$$(n 充分大)。

下面部分研究基于 $GF(3)$上本原三项式的 LFSR 序列 a^∞ 导出的对应自缩序列 z^∞ 的周期和线性复杂度。

5 基于 $GF(3)$上本原三项式的 SS_3–序列的周期和线性复杂度

定理 4 设 $f(x)$是 $GF(3)$上的 n 次本原三项式,a^∞ 是由 $f(x)$生成的 m–序列,又若在 a^∞ 导出的序列 z^∞ 中,至少出现长为 $2\lfloor n/3\rfloor+1$ 的 1–游程(或 2–游程,或 0–游程),则 $p(z^\infty)\geqslant 3^{2\lfloor n/3\rfloor+1}$。

证明 设 $m=2\lfloor n/3\rfloor$,由定理 2 知:$p(z^\infty)\geqslant 3^{2\lfloor n/3\rfloor}$。即 z^∞ 中长为 m 的所有状态都出现。又若在 z^∞ 中出现连续 $m+1$ 个 1(或 0 或 2),则 m 元状态全 1(或 0 或 2)在序列 a^∞ 的一个周期内至少出现了两次

$\therefore p(z^\infty)\geqslant 3^m+1$

由定理 1 知:$p(z^\infty)|3^n$

$\therefore p(z^\infty)\geqslant 3^m+1=3^{2\lfloor n/3\rfloor+1}$

定理 5 基于 $GF(3)$上本原三项式 $f(x)=x^n+c_1x^k+c_0$ 的 LFSR 序列 a^∞ 导出的 SS_3–序列,则在下列情形下 z^∞ 的周期 $p(z^\infty)\geqslant 3^{2\lfloor n/3\rfloor+1}$,且线性复杂度 $L(z^\infty)\geqslant 3^{2\lfloor n/3\rfloor}$。

证明 以下设 $d=2\lfloor n/3\rfloor$

情形 1 $n=3r$

(1)c_0,c_1 都是 2 且 $k=3s+1$ 时

即 $f(x)=x^n+2x^k+2=x^n-x^k-1$,由引理 4:设 a^∞ 的 n 元初态为 $(\underbrace{200200\cdots200}_{n\text{个}})$,则 $a^\infty=(\underbrace{200200\cdots200}_{n\text{个}}20*\cdots)$,从而 $z^\infty=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^\infty)\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2)c_0,c_1 中有一个为 2

(2.1)$k=3s+1$

(2.1.1)$c_1=2$

即 $f(x)=x^n+2x^k+1=x^n-x^k-2$,由引理 4:设 a^∞ 的 n 元初态为 $(\underbrace{200200\cdots200}_{n\text{个}})$,则 $a^\infty=(\underbrace{200200\cdots200}_{n\text{个}}10*\cdots)$,从而 $z^\infty=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^\infty)\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.1.2)$c_0=2$

即 $f(x)=x^n+x^k+2=x^n-2x^k-1$,由引理 4:设 a^∞ 的 n 元初态为 $(\underbrace{200200\cdots200}_{n\text{个}})$,则 $a^\infty=(\underbrace{200200\cdots200}_{n\text{个}}20*\cdots)$,从而 $z^\infty=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^\infty)\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2)$k=3s+2$ 且 $c_1=2$

即 $f(x)=x^n+2x^k+1=x^n-x^k-2$,由引理 4:设 a^∞ 的 n 元初态

为$(\underbrace{122122\cdots122}_{\lfloor n/3\rfloor\text{个“122”}})$,则 $a^{\infty}=(\underbrace{122\cdots122}_{\lfloor n/3\rfloor\text{个“122”}}\ \underbrace{120\cdots120}_{\lfloor n/3\rfloor\text{个“120”}}\ 221\cdots)$,从而 $z^{\infty}=(\underbrace{2222\cdots222}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

情形 2　$n=3r+1$ 且 c_0,c_1 中有一个为 2

(1)$k=3s$ 且 $c_1=2$

即 $f(x)=x^n+2x^k+1=x^n-x^k-2$,由引理 4:设 a^{∞} 的 n 元初态为$(\underbrace{200200\cdots2002}_{n\text{个}})$,则 $a^{\infty}=(\underbrace{200200\cdots200}_{n\text{个}}\ 20*\cdots)$,从而 $z^{\infty}=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2)$k=3s+1$ 且 $c_0=2$

即 $f(x)=x^n+x^k+2=x^n-2x^k-1$,由引理 4:设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots2112}_{n\text{个}})$,$a^{\infty}=(\underbrace{211211\cdots211}_{n\text{个}}\ 21*\cdots)$,从而 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(3)且 $k=3s+2$ 且 $c_0=2$

即 $f(x)=x^n+x^k+2=x^n-2x^k-1$,由引理 4:设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots2112}_{n\text{个}})$,则 $a^{\infty}=(\underbrace{211211\cdots211}_{n\text{个}}\ 21*\cdots)$,从而 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

情形 3　$n=3r+2$

对小于 n 的任意正整数 k,由引理 4 知:设 a^{∞} 的 n 元初态为$(\underbrace{222222\cdots22222}_{n\text{个}})$,则 $a^{\infty}=(\underbrace{222222\cdots222}_{}\ 22*\cdots)$,从而 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$。

由定理 4 知:$p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$。

由上可以看出,对于 $GF(3)$上的任意 n 次本原三项式,除了

(1)$n=3r$,$c_0=2$ 且 $k=3s+2$

(2)$n=3r+1$,$c_0=2$,$c_1=2$

(3)$n=3r+1$,$c_0=2$,$c_1=1$ 且 $k=3s$

(4)$n=3r+1$,$c_0=1$,$c_1=2$ 且 $k=3s+1$ 或 $k=3s+2$

这 4 种情况下,总可以找到 a^{∞} 的适当的 n 元初态使得 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$。

∴对于任意的 n 次本原三项式生成的 LFSR 序列 a^{∞} 所导出的对应自缩序列 z^{∞},易得 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$ 的概率大于 7/9。且易得当 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$ 时,$L(z^{\infty})>3^{2\lfloor n/3\rfloor}$。

6　基于 $GF(3)$上本原四项式的 SS_3–序列的周期和线性复杂度分析

定理 6　设 $f(x)=x^n+c_2x^m+c_1x^l+c_0(n>m>l)$是 $GF(3)$上的本原四项式,r 是正整数,a^{∞} 是由 $f(x)$生成的 m–序列,z^{∞} 是由 a^{∞} 导出的 SS_3–序列,则在下列情形下 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$,$d=2\lfloor n/3\rfloor$。

证明　情形 1:$n=3r$

(1)$n=3r$,c_0,c_1,c_2 全部为 1 或全部为 2

(1.1)当 $m=3s$

(1.1.1)$l=3h+1$,c_0,c_1,c_2 全部为 1 或全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{200200\cdots200}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.1.2)$l=3h+2$,c_0,c_1,c_2 全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots211}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.2)当 $m=3s+1$

(1.2.1)$l=3h$,c_0,c_1,c_2 全部为 1 或全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{200200\cdots200}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.2.2)$l=3h+1$,c_0,c_1,c_2 全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{200200\cdots200}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.2.3)$l=3h+2$,c_0,c_1,c_2 全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots211}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.3)当 $m=3s+2$

(1.3.1)$l=3h$,c_0,c_1,c_2 全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots211}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.3.2)$l=3h+1$,c_0,c_1,c_2 全部为 2

设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots211}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.3.3)$l=3h+2$,c_0,c_1,c_2 全部为 1

设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots211}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2)$n=3r$,c_0,c_1,c_2 中有两个为 1,一个为 2

(2.1)当 $m=3s$

(2.1.1)$l=3h+1$,$c_1=2$ 或 $c_2=2$

设 a^{∞} 的 n 元初态为$(\underbrace{200200\cdots200}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{0000\cdots000}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.1.2)$l=3h+2$,$c_0=2$ 或 $c_2=2$

设 a^{∞} 的 n 元初态为$(\underbrace{211211\cdots211}_{n\text{个}})$,可得 $z^{\infty}=(\underbrace{1111\cdots111}_{d+1\text{个}}*\cdots)$

∴ $p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2)当 $m=3s+1$

(2.2.1)$l=3h$,$c_2=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots200}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2.2)$l=3h+1$,$c_0=2$ 或 $c_1=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots200}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2.3)$l=3h+2$,$c_2=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots211}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.3)当 $m=3s+2$

(2.3.1)$l=3h$,$c_0=2$ 或 $c_1=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots211}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.3.2)$l=3h+1$,$c_1=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots211}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.3.3)$l=3h+2$,$c_0=2$ 或 $c_1=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots200}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

情形 2 $n=3r+1$

(1)$n=3r+1$,c_0,c_1,c_2 全部为 1 或全部为 2

(1.1)当 $m=3s$

(1.1.1)$l=3h+1$,c_0,c_1,c_2 全部为 1

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.1.2)$l=3h+2$,c_0,c_1,c_2 全部为 1

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.2)当 $m=3s+1$

(1.2.1)$l=3h$,c_0,c_1,c_2 全部为 1

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.2.2)$l=3h+1$,c_0,c_1,c_2 全部为 2

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.2.3)$l=3h+2$,c_0,c_1,c_2 全部为 2

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.3)当 $m=3s+2$

(1.3.1)$l=3h$,c_0,c_1,c_2 全部为 1

设a^{∞}的n元初态为$\underbrace{211211\cdots211}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.3.2)$l=3h+1$,c_0,c_1,c_2 全部为 2

设a^{∞}的n元初态为$\underbrace{211211\cdots211}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(1.3.3)$l=3h+2$,c_0,c_1,c_2 全部为 2

设a^{∞}的n元初态为$\underbrace{211211\cdots211}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2)$n=3r+1$,c_0,c_1,c_2 中有两个为 1,一个为 2

(2.1)当 $m=3s$

(2.1.1)$l=3h+1$,$c_0=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots2002}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.1.2)$l=3h+2$,$c_0=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots2002}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2)当 $m=3s+1$

(2.2.1)$l=3h$,$c_0=2$ 或 $c_1=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots2002}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2.2)$l=3h+1$,$c_1=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.2.3)$l=3h+2$,$c_1=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.3)当 $m=3s+2$

(2.3.1)$l=3h$,$c_0=2$ 或 $c_1=2$

设a^{∞}的n元初态为$\underbrace{200200\cdots2002}_{n个}$,可得$z^{\infty}=\underbrace{0000\cdots000}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.3.2)$l=3h+1$,$c_1=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

(2.3.3)$l=3h+2$,$c_1=2$ 或 $c_2=2$

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

情形 3 $n=3r+2$

设a^{∞}的n元初态为$\underbrace{211211\cdots2112}_{n个}$,可得$z^{\infty}=\underbrace{1111\cdots111}_{d+1个}*\cdots)$

$\therefore\ p(z^{\infty})\geqslant 3^{d+1}=3^{2\lfloor n/3\rfloor+1}$

从以上分析可以得出:对于情形 1 和情形 2,由任意的 n 次本原四项式生成的 LFSR 序列 a^{∞} 所导出的对应自缩序列 z^{∞} 的周期 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$ 的概率约为 1/2,而对于情形 3,$p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$ 的概率为 1,所以对于任意的 n 次本原四项式生成的 LFSR 序列 a^{∞} 所导出的对应自缩序列 z^{∞} 的周期 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$ 的概率约为 $1\times\frac{1}{3}+\frac{1}{2}\times\frac{1}{3}+\frac{1}{2}\times\frac{1}{3}=\frac{2}{3}$,且易得当 $p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$ 时,$L(z^{\infty})>3^{2\lfloor n/3\rfloor}$。

7　结束语

周期和线性复杂度是度量序列安全性的两个最重要的指标,由上结论可以看出:SS_3-序列比 MSS_3-序列的周期和线性复杂度下界更好;基于 $GF(3)$上本原三项式和四项式的 LFSR 序列 a^{∞} 导出的 SS_3-序列 z^{∞} 的周期和线性复杂度的下界是 $GF(3)$上由一般的本原多项式生成的 SS_3-序列 z^{∞} 的周期和线性复杂度的 3 倍的概率分别大于 7/9,2/3。而生成 SS_3-序列在模型构造上克服了多位自缩生成器生成序列过多过快的不足,所以扩展在 $GF(3)$上的新型自缩序列是适合流密码应用的伪随机序列。下面列表将 MSS_3-序列的周期和线性复杂度与 SS_3-序列进行详细比较。

表 1　MSS_3-序列与 SS_3-序列的周期和线性复杂度比较表

序列	生成多项式	周期	线性复杂度
MSS_3-序列	n 次本原多项式	$3^{\lfloor n/3\rfloor}\leqslant p(z^{\infty})\leqslant 2\times 3^{n-1}$	$3^{\lfloor n/3\rfloor-1}<L(z^{\infty})\leqslant 2\times 3^{n-1}$
	n 次本原三,四项式	$p(z^{\infty})\geqslant 2\times 3^{\lfloor n/3\rfloor}$	$L(z^{\infty})>3^{\lfloor n/3\rfloor}$
SS_3-序列	n 次本原多项式	$3^{2\lfloor n/3\rfloor}\leqslant p(z^{\infty})\leqslant 3^{n}$	$3^{2\lfloor n/3\rfloor-1}<L(z^{\infty})\leqslant 3^{n}$
	多于 7/9 的 n 次本原三项式	$p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$	$L(z^{\infty})>3^{2\lfloor n/3\rfloor}$
	多于 2/3 的 n 次本原四项式	$p(z^{\infty})\geqslant 3^{2\lfloor n/3\rfloor+1}$	$L(z^{\infty})>3^{2\lfloor n/3\rfloor}$

最后给出进一步值得研究的问题:

(1)基于一般本原多项式的周期和线性复杂度有待进一步研究。

(2)新的研究基于 n 次本原三项式和四项式的 SS_3-序列的周期和线性复杂度的方法。

参考文献:

[1] Meier W,Staffelbach O.The self-shrinking generator[C]//LNCS 950:Advances in Cryptology Eurocrypt'94.Berlin:Spring-verlag,1995:205-214.

[2] Blackburn S R.The linear complexity of the self-shrinking generator[J].IEEE Transactions of Information Theory,1999,45(6):2073-2077.

[3] 张楠,戚文峰.基于三项和五项本原多项式的 Self-shrinking 序列[J].信息工程大学学报,2004,5(2):4-8.

[4] 王锦玲.多位 Self-shrinking 序列模型与研究[J].郑州大学学报,1998,19(2):119-122.

[5] 王锦玲,王娟,陈忠宝.上多位自收缩序列的模型与研究[C]//密码学进展——China Crypt'2007.成都:西南交通大学出版社,2007:299-300.

[6] 王娟.$GF(3)$上多位自收缩序列的模型与研究[D].郑州:郑州大学,2008.

[7] 胡予濮,张玉清,肖国镇.对称密码学[M].北京:机械工业出版社,2002:64-76.

[8] Coppersmith D,Krawczyk H.Mansour Y.The shrinking generator[C]//LNCS 1773:Advance in Cryptology Eurocrypt'93.Berlin:Spring-Verlag,1993:22-39.

[9] 白恩健,董庆宽,肖国镇.自缩控生成器[J].西安电子科技大学学报:自然科学版,2004,31(2):264-268.

[10] Lidl R,Niederretier H.Finite fields[M].[S.l.]:Addison-Wesley Publishing Company,1983.

(上接 100 页)

$r_i u^2)\boldsymbol{g}_i+\sum_{j=k_1+1}^{k_1+k_2}(\lambda_j+\mu_j u)\boldsymbol{g}_j+\sum_{l=k_1+k_2+1}^{k}\lambda_l\boldsymbol{g}_l\}=0$,又因为 ϕ 为单射,故有

$$\sum_{i=1}^{k_1}(\lambda_i+\mu_i u+r_i u^2)\boldsymbol{g}_i+\sum_{j=k_1+1}^{k_1+k_2}(\lambda_j+\mu_j u)\boldsymbol{g}_j+\sum_{l=k_1+k_2+1}^{k}\lambda_l\boldsymbol{g}_l=0$$

由此得 $\lambda_i=0,\mu_j=0,r_l=0,i=1,2,\cdots,k;j=1,2,\cdots,k_1+k_2;l=1,2,\cdots,k_1$。

(2)设 $\phi(C)$的对偶码为 $\phi(C)^{\perp}$,则由引理 2(2)知,$\phi(C^{\perp})\subseteq\phi(C)^{\perp}$,又 ϕ 为单射且 $\dim(\phi(C))=3k_1+2k_2+k_3$,所以$|\phi(C^{\perp})|=|C^{\perp}|=2^{3(n-k)+2k_3+k_2}=2^{3n-(3k_1+2k_2+k_3)}=|\phi(C)^{\perp}|$,因此,$\phi(C^{\perp})=\phi(C)^{\perp}$。

4　环 R 和 R_1 上线性码间的关系

下面两个定理将环 R_1 上的线性码与环 R 上的一类线性码对应起来,证明较为简单,这里将其省略。

定理 4　设 $\varnothing\neq C\subseteq R_1^n$,则 C 为环 R_1 上线性码当仅当 $f(C)$为环 R 上的线性码。

定理 5　设 C 为 R_1 上长为 n 的线性码,则

$$\boldsymbol{G}'=\begin{pmatrix}\boldsymbol{I}_{t_1} & \boldsymbol{B} & \boldsymbol{B}_{11}+u\boldsymbol{B}_{12}\\ 0 & u\boldsymbol{I}_{t_2} & u\boldsymbol{D}\end{pmatrix}$$

为码 C 的生成矩阵当且仅当

$$f\boldsymbol{G}'=\begin{pmatrix}u\boldsymbol{I}_{t_1} & u\boldsymbol{B} & u\boldsymbol{B}_{11}+u^2\boldsymbol{B}_{12}\\ 0 & u^2\boldsymbol{I}_{t_2} & u^2\boldsymbol{D}\end{pmatrix}$$

为环 R 上的线性码 $f(C)$的生成矩阵,其中 $\boldsymbol{B},\boldsymbol{D},\boldsymbol{B}_{11},\boldsymbol{B}_{12}$ 为域 F_2 上矩阵。

5　结束语

环 $F_2+uF_2+u^2F_2$ 上的线性码的研究,为构造出参数好的域上的码提供了一种可能,也有助于进一步去研究环 $F_2+uF_2+\cdots+u^kF_2$ 上的线性码。

参考文献:

[1] Hammons R,Kumar P V,Calderbank A R,et al.The Z_4-linearity of kerdock,preparata,goethals,related codes[J].IEEE Trans Inform Theory,1994,40(2):301-319.

[2] Bonnecaze A,Udaya P.Cyclic codes and self-dual codes over F_2+uF_2[J].IEEE Trans Inform Theory,1999,45(4):1250-1255.

[3] 余海峰,朱士信.环 F_2+uF_2 上线性码及其对偶码的二元象[J].电子与信息学报,2006,28(11):2121-2123.

[4] 耿普,李超.环 F_2+uF_2 上线性码的结构特征[J].电子与信息学报,2007,29(12):2912-2914.

[5] 陈鲁生.沈世镒.编码理论基础[M].北京:高等教育出版社,2005:106-109.