多位 Self—shrinking 序列模型及研究

王锦玲 孔佩娟
(郑州工业大学数力系) (宁波市工业机械学校,宁波,315010)

摘 要 给出了一种新的多位 Self—shrinking(自收缩)序列模型,且用一个 *LFSR* 装置就能实现该序列。利用有限域理论,解决了 Self—shrinking 最长序列周期下界、线性复杂度下界,并给出更一般多位 Self—shrinking 最长序列的周期下界、线性复杂度下界。

关键词 周期;线性复杂度;Self—shrinking 序列
中图分类号 O151

0 引 言

设 $a=(a_0,a_1,a_2,\cdots\cdots)$,$b=(b_0,b_1,b_2,\cdots\cdots)$是 F_2 上周期序列,将二序列按下列方式排列

$$a_0,a_1,a_2,\cdots\cdots$$
$$b_0,b_1,b_2,\cdots\cdots$$

如果 $b_i=1$,则选取 a_i,如果 $b_i=0$,则不取 a_i,这样得到的序列称为钟控序列,文献[2]中全面研究了钟控序列的特征,而本文将二条序列 a,b 改为仅用一条 m—序列实现自控的多位 Self—shrinking 序列,给出了多位 Self—shrinking 最长序列的周期下界、线性复杂度下界,具有更好的不可预测性,有较好的密码意义和数学意义。

1 理论基础

引理1:F_2 上周期序列 a,周期为 $p(a)=P$,则 $p(a^{(s)})=P/(s,p)$。

引理2:设 $a=(a_0,a_1,\cdots\cdots)$是 F_2 上 m—序列,将 a 的一个周期,$(a_0,a_1,\cdots,a_{2^n-2})$依次排列在一个圆周上,并使 a_{2^n-2}与 a_0 相邻,再设 $0<k\leqslant n$,那么 F_2 上任意一个 k 元素组$(b_1,b_2,\cdots,b_k)$在 a 的一个周期的上述圆周排列中出现的次数等于

$$\begin{cases} 2^{n-k} & \text{如果}(b_1,b_2,\cdots,b_k)\neq(0,0,\cdots,0) \\ 2^{n-k}-1 & \text{如果}(b_1,b_2,\cdots,b_k)=(0,0,\cdots 0) \end{cases} \qquad nd$$

引理3:设 a 是 F_2 上 m—序列,那么“1”在 a 的一个周期中恰出现 2^{n-1}次,而“0”在 a 的一个周期中恰出现 $2^{n-1}-1$ 次。

收稿日期:1997—10—30
第一作者 女 1963年2月生 硕士学位 讲师

2 多位Self－shrinking序列模型的构造

定义1：设 $a=(a_0,a_1,a_2,\cdots\cdots)$是 F_2 上 m－序列，将 $a=(a_0,a_1,a_2,\cdots\cdots)$按下列方式排列：

$$(a_0,a_1,a_2,),(a_3,a_4,a_5,),(a_6,a_7,a_8),\cdots\cdots,(a_{3k},a_{3k+1},a_{3k+2}),\cdots\cdots$$

如果 $a_{3k}=1$，则取 a_{3k+1}；如果 $a_{3k}=0$，则不取 a_{3k}所在的括号内 a 的分量，这样得到的序列称为 a 的多位Self－shrinking序列，记为 $C=(C_k)$，用下图表示 $C=(C_k)$的生成过程

$$\text{LFSR} \xrightarrow{a_k} \text{clock control} \longrightarrow C_k$$

例如：有序列 $a=(1,0,0,*,*,*,\cdots\cdots)$排成：

$$(1,0,0,),(*,*,*),\cdots,(*,*,*),\cdots$$

（“＊”指序列某分量，以后不再说明）

clock control 输出 C 的一个分量“0”，

例如有序列 $a=(1,1,0,*,*,*,\cdots\cdots)$排成：

$$(1,1,0),(*,*,*),\cdots,(*,*,*),\cdots$$

clock control 输出 C 的一个分量“1”，

例如有序列 $a=(0,1,0,*,*,*,\cdots\cdots)$排成：

$$(0,1,0),(*,*,*),\cdots,(*,*,*),\cdots$$

Clock control 不输出上式第一括号内的分量，看第二个括号内分量的情况，这样生成的多位Self－shrinking序列装置仅用一个LFSR实现，较简便。

定义2：设 $a=(a_0,a_1,a_2,\cdots)$则称 $a^{(s)}=(a_0,a_s,a_{2s},\cdots)$为 a 的 s 采样序列。

定义3：设 L 是序列的平移变换，即设 $a=(a_0,a_1,a_2,\cdots\cdots)$，则称 $L(a)=(a_1,a_2,\cdots\cdots)$，$L^k(a)=(a_k,a_{k+1},\cdots\cdots)$。

性质1：$a=(a_0、a_1,\cdots\cdots)$是 F_2 上序列，则 $C=(C_k)$序列就是 $a^{(3)}$来控制 $L(a^{(3)})$实现的。

性质2：$P(a^{(3)})=P(L(a^{(3)})=P/(3,p)$，

其中，$P=P(a)=2^n-1$。

3 多位Self－shrinking最长序列的周期下界和线性复杂度下界

$C=(C_k)$序列由 m－序列 a 自控而得，虽然浪费一些信息量，但利用提高序列的周期，线性复杂度来得到很好补偿，以确保安全可靠性。

定理1：设 $a=(a_0,a_1,a_2,\cdots\cdots)$是级数为 n，由LFSR生成的 m－序列，而 $C=(C_k)$是由 a 生成的多位Self－shrinking序列，则 C 的周期 $P(C)|2^{n-1}$。

证明：将 a 序列第一个周期内分量排成：

$$(a_0,a_1,a_2,),(a_3,a_4,a_5),\cdots,(a_{2^n-4},a_{2^n-3},a_{2^n-2})$$

由引理2每个$(b_1,b_2,b_3)\neq(0,0,0)$，出现 2^{n-3}次所有的 $b_1\neq0$ 的$(b_1,b_2,b_3)\neq(0,0,0)$共出现 $2^{n-3}\times4=2^{n-1}$次，$\therefore P(c)|2^{n-1}$。

定理 2：条件同定理 1，则多位 Self－shrinking 最长序列 $C=(C_k)$周期 $P(c)\geqslant 2^{[n/3]-1}$。

证明：第一种情况，设 n 是 3 的倍数，即 $n=3k$，a 的 n－比特序列有这种情况：

$$(1, x_1, *, x_2, *, \cdots, 1, x_{k-1}, *)$$

由定义 1 多位 Self－Shrinking 最长序列 $C=(C_k)=(x_1, x_2, \cdots, x_{k-1})$　　$\therefore P(C)\geqslant 2^{k-1}$；

第二种情况：$n=3k+1$，或 $n=3k+2$

例如：a 的 n－比特序列有这样情况：

$$(1, x_1, *, 1, x_2, *, \cdots, 1, x_{k-1}, *, 1), n=3k+1$$

输出得 $C=(x_1, x_2, \cdots, x_{k-1}, 1)$，$P(c)\geqslant 2^{k-1}$；

例如 a 的 n－比特序列有这样情况：

$$(1, x_1, *, 1, x_2, *, \cdots, 1, x_{k-1}, *, 1, x_k), n=3k+2$$

输出得 $C=(x_1, x_2, \cdots, x_{k-1}, x_k)$　　$\therefore P(c)\geqslant 2^k > 2^{k-1}$

综上可得 Self－shrinking 最长序列 c 的周期下界

$$P(c)\geqslant 2^{[n/3]-1}$$

定理 3：条件同定理 1，设 L 是多位 Self－shrinking 最长序列 C 的线性复杂度，则 $L>2^{[n/3]-2}$。

证明：由定理 1　$P(c)/2^{n-1}$，$\therefore p(c)=2^a$，由定理 2，$a\geqslant[n/3]-1$

在 F_2 上，$x^{p(c)}-1=(x-1)^{2^n}$

设 $f(x)$是 C 的极小多项式

$$\therefore f(x)/x^{p(c)}-1 \qquad \therefore f(x)=(x-1)^L$$

$\because L$ 是 C 的线性复杂度，$\therefore L>2^{a-1}$

如果上式不等式不成立，假设 $L\leqslant 2^{a-1}$，

则　$f(x)=(x-1)^L|(x-1)^{2^{a-1}}$

而　$(x-1)^{2^{a-1}}=(x^{2^{a-1}}-1)$

$\therefore x^{2^{a-1}}-1$ 是 c 的特征多项式，与 C 的周期假设 $P(C)=2^a$ 矛盾

$\therefore L>2^{a-1}$，即 $L>2^{[n/3]-2}$

由上结果得到 Self－shrinking 最长序列 c 的线性复杂度下界，是 2 的指数倍增大，按照定义 1，c 序列其实是由 a 的每相邻三个分量，至少收缩 2 位分量而得，所以称为多位 Self－shrinking 序列，下面将多位 Self－shrinking 推广到将 a 序列至少收缩 $N(\geqslant 2)$分量而得 Self－shrinking 序列情况。

4　多位 Self－shrinking 序列模型推广

定义 4：设 a 是 F_2 上的 m－序列，将 $a=(a_0, a_1, \cdots)$按下列方式排列：

$$(a_0, a_1, \cdots, a_{l-1}), (a_l, a_{l+1}, \cdots, a_{2l-1}), \cdots, \cdots$$

如果 $a_{lk}=1$，则取 a_{lk+1}；如果 $a_{lk}=0$，则不取 a_{lk}所在的括号内 a 的分量，这样得到的序列称为 a 的一般多位 Self－shrinking 序列，记为 $b=(b_k)$，也仅用一个 LFSR 来实现。

定理 4：设 $a=(a_0, a_1, \cdots)$是级数为 n 的 LFSR 生成的 m－序列，而 $b=(b_k)$是由 a 生

成的一般多位Self－shrinking序列，则 $P(b)|2^n-1$。

证明：将 a 序列第一个周期内分量排成：

$$(a_0, a_1, \cdots, a_{l-1}), (a_l, a_{l+1}, \cdots, a_{2l-1}), \cdots$$

由引理2，每个 $(b_0, b_1, \cdots, b_{l-1}) \neq (0,0,\cdots 0)$，出现 2^{n-l} 次，所有 $b_0 \neq 0$ 的 $(b_0, b_1, \cdots, b_{l-1}) \neq (0,0,\cdots,0)$ 共出现 $2^{n-l} \times 2^{l-1} = 2^{n-1}$ 次，$\therefore P(b)|2^{n-1}$。

定理5：条件同定理4，则一般多位Self－shrinking最长序列 $b=(b_k)$，周期 $P(b) \geqslant 2^{[n/l]-l+2}$。

证明：证明类似定理2，略。

定理6：条件同定理4，设 L 是一般多位Self－shrinking最长序列 b 的线性复杂度，则

$$L > 2^{[n/l]-l+1}$$

由以上结果看到，生成序列 a 的级数 n 较大时，我们可以多收缩几位 a 的分量，线性复杂度还是按照2的指数倍增大，结果很理想，而生成序列 a 的级数 n 较小时，我们不能将 a 的分量收缩过多，少收缩几位，以免影响所得Self－shrinking序列较好的线性复杂度。

本文是文献[4]结果更一般推广，给出序列 a 的分量无论收缩几位，Self－shrinking最长序列的周期下界，线性复杂度下界，但对推广的Self－shrinking最长序列的线性复杂度下界，能够达到序列个数，待进一步验证和论证。

参考文献

1 万哲先.代数和编码，北京：科学出版社，1980.218～260

2 王锦玲.控制序列的构造与分析.信息工程学院学报，1993.(2)：32～38

3 *Lidl, R, Niedereiter, H, Finite Field*.394～464

4 *Willi Meier Othmar Staffelbach. The Self－shrinking Generator*, 201～210, *Eurocrypt* '94

Study on Multi－self－shrinking Sequences Model

Wang Jinling
(*Zhengzhou University of Technology*)
Kong Peijuan
(*Ningbo Industry Machinery College*)

Abstract In this paper, we give a new kind of multi－self－shrinking sequences by using one LFSR. By applying the theory of finite field, we obtain the lower bound of period and linear complexity about the self－shrinking maximal length sequences, and describ the lower bound of period and linear complexity of general multi－self－shrinking maximal length sequences.

Keywords period; complexity; self－shrinking sequence