国防科技大学学报
JOURNAL OF ANTIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第12卷第4期　1990年12月　Vol.12 No.4

获得前馈序列最大周期的一般方法

肖　戎　唐朝京
（电子技术系）

摘　要　本文讨论了前馈序列的周期性问题，找到了使前馈序列获得最大周期的一般方法。

关键词　通信，密码学，序列/密码体制，流密码
分类号　TP918.1，TP918.2

在密码学中，如何度量一个给定的密码体制的安全性是非常重要的，这个问题至今尚未解决。人们试图得到一些能保证密码体制绝对安全的充分条件，但这种努力并不成功，只得到了一些必要条件。在流密码体制中，其安全性主要依赖于密码序列的安全性。一般认为，密码序列的安全性包括三个方面，其中之一是周期性，即密码序列的周期必须足够长。这样，如何保证密码序列具有足够长的周期就成了一个重要的问题。密码序列通常是由非线性生成器或前馈生成器产生的，本文讨论的是前馈生成器的周期性。不失一般性，本文中我们假设所有序列都是0、1二元序列。

1　前馈生成器和前馈序列周期

前馈生成器的工作原理如图1所示：其中$\{a_i\}$是一个移位寄存器序列，f是其反馈函数。T是F_2上的有s个变量的函数，称为前馈函数。序列$\{t_i\}=T(x_{i_1}, x_{i_2}, \cdots, x_{i_s})$称为前馈序列（$s\leqslant n$，$1\leqslant i_1<i_2<\cdots<i_s\leqslant n$）。当$f$给定以后，$\{t_i\}$的周期仅依赖于$T$，故称$T$的周期为$\{t_i\}$的周期。

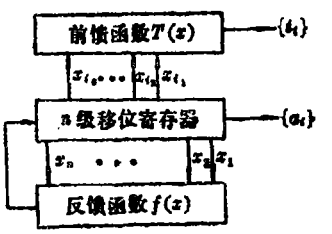

图　1

在移位寄存器序列中，m序列是一类最常用的序列。它不仅具有许多良好的性质，而且技术上非常易于实现。不失一般性，可假设前馈生成器中的移位寄存器序列为m序列，即f是线性函数，且$\{a_i\}$的特征多项式是一个本原多项式。$\{a_i\}$的周期$D=2^n-1$，显然，前馈序列$\{t_i\}$的周期l不大于$\{a_i\}$的周期D，即$l\leqslant D$．自然，希望前馈序列的周期l能与m序列的周期D相等（这也是前馈序列的最大周期）。然而，这一点并不是无条件成立的。实际上$l<D$的情况是存在的，下面的例子说明了这一点。

1990年1月4日收稿

例 设$n=4$，$f(x)=x^4+x+1$，$\{a_i\}=100011110101100$，$1000\cdots\cdots$

取$s=3$，且$(x_{i_1}, x_{i_2}, x_{i_3})=(x_1, x_2, x_3)$，

$$T(x_1,x_2,x_3)=x_1x_3+x_2x_3+x_1+x_2+x_3+1.$$

$T(x_1,x_2,x_3)$的真值表如表1：

表1 $T(x_1,x_2,x_3)$真值表

x_1	x_2	x_3	$T(x_1,x_2,x_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

则：$\{t_i\}=01000, 01000, 01000, \cdots\cdots$

$D=2^n-1=15$，$l=5$，

显然$l<D$.

这个例子说明了$l<D$存在的情形。更一般地，对于前馈序列小周期的分布规律有如下结论成立[1]：

设D为$\{a_i\}$的周期，l为$\{t_i\}$的周期，则$l<D$的概率为：

$$P(l<D)=1-\frac{d_D}{2^D}$$

其中$d_D=\sum_{r\mid D}\mu(r)\cdot 2^{\frac{D}{r}}$，$\mu(\cdot)$为Mobius函数。

此结论揭示了前馈序列出现小周期的概率。然而作为一个密码序列，必须能够确切地知道它的周期（或周期的下限），才能避免序列中出现太小的周期，因此仅仅知道前馈序列中出现小周期的概率是不够的，必须保证前馈序列能得到最大的周期。文献[2]中得到了在特定条件下获得前馈序列最大周期的充分条件，而本文将得到更一般的结果。

2 获得前馈序列最大周期的充分条件

定义 设$s\leqslant n$，称m序列n级状态$(x_1, x_2, \cdots, x_n)$中的任意s位$(x_{i_1}, x_{i_2}, \cdots, x_{i_s})$为一个$s$状态$(1\leqslant i_1<i_2<\cdots<i_s\leqslant n)$。若$x_{i_j}$全为$0(j=1,2,\cdots,s)$，则称其为全零$s$状态，否则称为非零$s$状态。

前馈函数T的一组输入即为$\{a_i\}$的一个s状态，显然，T的2^s种输入中全零s状态只有一种，而非零s状态有2^s-1种。

再设$T(0,0,\cdots,0)=e$（$e=0$或1），将T的真值表中元素e的个数记为N_e，而$\bar{e}$的个数记为$N_{\bar{e}}$，显然，$N_e+N_{\bar{e}}=2^s$.

引理 在$\{a_i\}$的一个周期内，每一个非零s状态出现2^{n-s}次，而全零s状态出现$2^{n-s}-1$次。

证明 设$\{a_i\}$的n级状态为：

x_1	x_2	x_3	$\cdots\cdots$	x_n

而其中的s状态为：

$\cdots$	x_{i_1}	$\cdots$	x_{i_2}	$\cdots\cdots$	x_{i_s}	$\cdots$

$(1\leqslant i_1<i_2<\cdots<i_s\leqslant n)$

当非全0的s状态$(x_{i_1}, x_{i_2}, \cdots, x_{i_s})$确定后，$n$级状态中的其余$n-s$位可以任选，共有$2^{n-s}$种选择，或者说共有$2^{n-s}$个$n$级状态中包含此$s$状态，即在$m$序列$\{a_i\}$的一个周期

中，每一个非全0的 s 状态均出现了 2^{n-s} 次。

当出现全0的 s 状态，即 $x_{i_1}=x_{i_2}=\cdots=x_{i_s}=0$ 时，由于 m 序列不能包含全0状态，故此时 $\{a_i\}$ 的 n 级状态中的其余 $n-s$ 位不能同时为0，而其它任何状态均为允许状态，因此在 $\{a_i\}$ 的一个周期中，全0的 s 状态出现次数要比非全0情况时少一次，即全0的 s 状态出现了 $2^{n-s}-1$ 次。　　（证毕）

定理　设 T 为前馈函数，$T(0,0,\cdots,0)=e$（$e=0$ 或 1），m 序列 $\{a_i\}$ 的周期为 $D=2^n-1$，若 $(N_{\bar{e}}, D)=1$，则前馈序列 $\{t_i\}$ 的周期 l 就等于 D.

证明　显然，$l \mid D$，若记 $\frac{D}{l}=r$，则 $r\geqslant 1$. $D=2^n-1$ 为奇数，则 r 也为奇数，故

$$(r, 2^{n-s})=1 \tag{1}$$

由于 $(N_{\bar{e}}, D)=1$，$r \mid D$，则

$$(r, N_{\bar{e}})=1 \tag{2}$$

由引理知，在 $\{a_i\}$ 的一个周期长度内，$\{t_i\}$ 中出现 $\bar{e}$ 的次数为 $N_{\bar{e}}\cdot 2^{n-s}$. 由于在 $\{t_i\}$ 的每个周期中 $\bar{e}$ 的个数是一个常数，不妨记作 h，则

$$h\cdot r=N_{\bar{e}}\cdot 2^{n-s},\ r \mid N_{\bar{e}}\cdot 2^{n-s} \tag{3}$$

由(1)、(2)式知：$(r, 2^{n-s})=1$，$(r, N_{\bar{e}})=1$. 又由(3)式知：$r \mid N_{\bar{e}}\cdot 2^{n-s}$，故 $r=1$. 这说明 $l=D$，即 $\{t_i\}$ 的周期等于 $\{a_i\}$ 的周期 2^n-1.　　（证毕）

定理说明：只要 $(N_{\bar{e}}, D)=1$，则前馈序列 $\{t_i\}$ 即能获得最大周期 2^n-1. 这一条件是非常容易满足的。例如，当 $n=10$，$D=2^n-1=1023$，若取 $s=5$，可以很容易地构造一个 $N_{\bar{e}}=17$ 的真值表，此时便有 $(N_{\bar{e}}, D)=(17, 1023)=1$. 以这个真值表作为前馈函数的真值表，即能使前馈序列获得最大周期1023.

当 n、s 取定以后，满足定理条件的前馈函数共有 $2\cdot\sum_{(N,D)=1}\binom{2^s}{N}$ 个，即至少有 $2\cdot\sum_{(N,D)=1}\binom{2^s}{N}$ 个前馈序列可得到最大周期 2^n-1，这一数量是非常大的。

推论　若前馈函数 T 的真值表中0、1个数相等，则前馈序列可得到最大周期。

证明　此时有 $N_{\bar{e}}=N_e=2^{s-1}$，显然 $(N_{\bar{e}}, D)=(2^{s-1}, 2^n-1)=1$，由定理立即得：$l=D$.　　（证毕）

这正是文[2]所得到的结果。此推论的条件也很容易满足，而且从密码学角度看，这一条件在许多情况下是必须满足的。因此这一结论具有重要的应用价值。

至此，本文已圆满解决了前馈序列的周期性问题。本文得到国防科技大学电子技术系青年教师研究基金资助。

参 考 文 献

[1] 肖戎.前馈序列的周期性研究.西安:第三届全国密码学会议，1988

[2] 唐朝京.一种获得前馈序列最大周期的方法.现代通信技术，1989，(2)

Method to Get the Longest Period of Feedforward Sequences

Xiao Rong Tang Chaojing
(Department of Electronic Technology)

Abstract

This paper discusses the periodicity of feedforward sequences. A general method to get the longest period of feedforward sequences is put forward.

Key words communication, cryptography, sequence / cipher system, stream cipher

(上接第130页)

A Microcomputer Interface with Multiple Functions

Zhang Wenming Lü Rui Chen Huihuang
(Department of Electronic Technology)

Abstract

A microcomputer inferface with multiple functions is presented. It is a kind of test and control means with strong function and can be applicated in the fields of microcomputer control, signal test, circuit self-test, fault diagnosis and digital signal generation with much practical value.

Key words: microcomputer, interface equipment, signal measurement/ circuit self-test, serial commuication