B-M 算 法

根据密码学的需要，对线性反馈移位寄存器(LFSR)主要考虑下面两个问题：

（1）如何利用级数尽可能短的LFSR产生周期大、随机性能良好的序列，即固定级数时，什么样的移存器序列周期最长。这是从密钥生成角度考虑，用最小的代价产生尽可能好的、参与密码变换的序列。

（2）当已知一个长为N序列$\underline{a}$时，如何构造一个级数尽可能小的LFSR来产生它。这是从密码分析角度来考虑，要想用线性方法重构密钥序列所必须付出的最小代价。这个问题可通过B-M算法来解决。

1、概念简介

设 $\underline{a}=(a_0,a_1,\cdots,a_{N-1})$ 是 F_2 上的长度为N的序列，而

$f(x)=c_0+c_1x+c_2x^2+\cdots+c_lx^l$ 是 F_2 上的多项式，c_0=1.

如果序列中的元素满足递推关系：

$$a_k=c_1a_{k-1}+c_2a_{k-2}+\cdots+c_la_{k-l},\ k=l,l+1,\cdots,N-1 \qquad (2)$$

则称$\langle f(x),l\rangle$产生二元序列$\underline{a}$。其中$\langle f(x),l\rangle$表示以$f(x)$为反馈多项式的l级线性移位寄存器。

如果$f(x)$是一个能产生$\underline{a}$并且级数最小的线性移位寄存器的反馈多项式，l是该移存器的级数，则称$\langle f(x),l\rangle$为**序列$\underline{a}$的线性综合解**。

线性移位寄存器的综合问题可表述为：给定一个N长二元序列$\underline{a}$，如何求出产生这一序列的最小级数的线性移位寄存器，即最短的线性移存器？

几点说明：

1、反馈多项式$f(x)$的次数$\leq l$。因为产生$\underline{a}$且级数最小的线性移位寄存器可能是退化的，在这种情况下 $f(x)$的次数$<l$；并且此时 $f(x)$中的$c_l=0$，因此在反馈多项式$f(x)$中$c_0=1$，但不要求$c_l=1$。

2、规定：0级线性移位寄存器是以$f(x)=1$为反馈多项式的线性移位寄存器，且n长$(n=1, 2, \ldots, N)$全零序列，仅由0级线性移位寄存器产生。事实上，以$f(x)=1$为反馈多项式的递归关系式是：$a_k=0$，$k=0, 1, \ldots, n-1$.因此，这一规定是合理的。

3、给定一个N长二元序列$\underline{a}$，求能产生$\underline{a}$并且级数最小的线性移位寄存器，就是求$\underline{a}$的线性综合解。利用B-M算法可以有效的求出。

2、B-M算法要点

用归纳法求出一系列线性移位寄存器：

$\langle f_n(x), l_n \rangle$ $\partial^0 f_n(x) \le l_n, \quad n = 1,2,\cdots,N$

每一个$\langle f_n(x), l_n \rangle$都是产生序列$\underline{a}$的前$n$项的最短线性移位寄存器，在$\langle f_n(x), l_n \rangle$的基础上构造相应的 ，使得$\langle f_{n+1}(x), l_{n+1} \rangle$ 是产生$\langle f_{n+1}(x), l_{n+1} \rangle$前n+1项的最短移存器，则最后得到的 就是产生$\langle f_N(x), l_N \rangle$二元序列$\underline{a}$的最短的线性移位寄存器。

3、B-M算法

任意给定一个N长序列$\underline{a}=(a_0,a_1,\cdots,a_{N-1})$，按$n$归纳定义

$\langle f_n(x),l_n\rangle$　　$n=0,\ 1,\ 2,\cdots,N-1$

1、取初始值：$f_0(x)=1,\quad l_0=0$

2、设$\langle f_0(x),l_0\rangle,\langle f_1(x),l_1\rangle,\cdots,\langle f_n(x),l_n\rangle$ $(0\le n<N)$

均已求得，且$l_0\le l_1\le\cdots\le l_n$

记：$f_n(x)=c_0^{(n)}+c_1^{(n)}x+\cdots c_{l_n}^{(n)}x^{l_n},c_0^{(n)}=1,$ 再计算：

$$d_n=c_0^{(n)}a_n+c_1^{(n)}a_{n-1}+\cdots+c_{l_n}^{(n)}a_{n-l_n}$$

称d_n为第n步差值。然后分两种情形讨论：

（ⅰ） 若d_n=0，则令：

$$f_{n+1}(x)=f_n(x),\quad l_{n+1}=l_n。$$

（ⅱ） 若d_n=1，则需区分以下两种情形：

① 当：$l_0=l_1=\cdots=l_n=0$时，

取：$f_{n+1}(x)=1+x^{n+1},l_{n+1}=n+1。$

② 当有m（$0\le m<n$），使：$l_m<l_{m+1}=l_{m+2}=\cdots=l_n。$

设：$f_{n+1}(x)=f_n(x)+x^{n-m}f_m(x),l_{n+1}=\max\{l_n,n+1-l_n\}$

最后得到的$\langle f_N(x),l_N\rangle$便是产生序列$\underline{a}$的最短线性移位寄存器。

4、实例

例2、求产生周期为7的m序列一个周期：0011101的最短线性移位寄存器。

解：设 $a_0a_1a_2a_3a_4a_5a_6=0011101$，首先取初值 $f_0(x)=1, l_0=0$，则由$a_0=0$得$d_0=1\cdot a_0=0$从而 $f_1(x)=1, l_1=0$；同理由$a_1=0$得$d_1=1\cdot a_1=0$从而 $f_2(x)=1, l_2=0$。

由$a_2=1$得$d_2=1\cdot a_2=1$，从而根据$l_0=l_1=l_2=0$ 知

$$f_3(x)=1+x^{2+1}=1+x^3,\ l_3=3$$

第1步，计算d_3：$d_3=1\cdot a_3+0\cdot a_2+0\cdot a_1+1\cdot a_0=1$

因为$l_2<l_3$，故$m=2$，由此

$$f_4(x)=f_3(x)+x^{3-2}f_2(x)=1+x+x^3$$
$$l_4=\max\{3,3+1-3\}=\max\{3,1\}=3$$

第2步，计算d_4：$d_4=1\cdot a_4+1\cdot a_3+0\cdot a_2+1\cdot a_1=0$，从而

$$f_5(x)=f_4(x)=1+x+x^3$$
$$l_5=l_4=3$$

第3步，计算d_5：$d_5=1\cdot a_5+1\cdot a_4+0\cdot a_3+1\cdot a_2=0$，从而

$$f_6(x)=f_5(x)=1+x+x^3$$
$$l_6=l_5=3$$

第4步，计算d_6：$d_6=1\cdot a_6+1\cdot a_5+0\cdot a_4+1\cdot a_3=0$，从而

$$f_7(x)=f_6(x)=1+x+x^3$$
$$l_7=l_6=3$$

这表明，$\langle 1+x+x^3,3\rangle$即为产生所给序列一个周期的最短线性移位寄存器。