



# 现代密码学

## 第十一讲 $m$ -序列

信息与软件工程学院



# 第十一讲 m-序列



线性反馈移位寄存器的多项式表示

m-序列产生的条件

## 线性移位寄存器的一元多项式表示

定义2.1 设n级线性移位寄存器的输出序列满足递推关系

$$a_{n+k} = c_1 a_{n+k-1} \oplus c_2 a_{n+k-2} \oplus \dots \oplus c_n a_k \quad (*)$$

用延迟算子  $D$  ( $Da_k = a_{k-1}$ ) 作为未定元, 给出的反馈多项式为:

$$p(D) = 1 + c_1 D + \dots + c_{n-1} D^{n-1} + c_n D^n$$

这种递推关系可用一个一元高次多项式

$$p(x) = 1 + c_1 x + \dots + c_{n-1} x^{n-1} + c_n x^n$$

表示, 称这个多项式为LFSR的特征多项式。

# 关于特征多项式的解释

$$a_{n+k} = c_1 a_{n+k-1} \oplus c_2 a_{n+k-2} \oplus \cdots \oplus c_n a_k$$
$$\Leftrightarrow a_{n+k} \oplus c_1 a_{n+k-1} \oplus c_2 a_{n+k-2} \oplus \cdots \oplus c_n a_k = 0$$

$D(a_k) = a_{k-1}$ , 用  $p(D) = 1 + c_1 D + \cdots + c_n D^n$  作用于  $a_{n+k}$  后恰好就是上式的左边,

即

$$\begin{aligned} p(D)(a_{n+k}) &= (1 + c_1 D + \cdots + c_n D^n)(a_{n+k}) \\ &= a_{n+k} + c_1 D(a_{n+k}) + \cdots + c_n D^n(a_{n+k}) \\ &= a_{n+k} + c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_n a_k \end{aligned}$$

A decorative graphic consisting of several horizontal blue bars of varying lengths, stacked vertically, is positioned to the left of the title.

# 生成函数

---

定义2.2 给定序列  $\{a_i\}$ ，幂级数

$$A(x) = \sum_{i=1}^{\infty} a_i x^{i-1}$$

称为该序列的生成函数。

# 生成函数的性质

定理2.1 设  $\mathbf{p(x)=1+c_1x+...+c_{n-1}x^{n-1}+c_nx^n}$  是  $\mathbf{GF(2)}$  上的多项式，  $\mathbf{G(p(x))}$  中任一序列  $\{\mathbf{a_i}\}$  的生成函数  $\mathbf{A(x)}$  满足：

$$A(x) = \frac{\phi(x)}{p(x)}$$

其中

$$\phi(x) = \sum_{i=1}^n (c_{n-i} x^{n-i} \sum_{j=1}^i a_j x^{j-1})$$

## 定理2.1的证明

证明： 在等式

$$a_{n+1} = c_1 a_n \oplus c_2 a_{n-1} \oplus \dots \oplus c_n a_1$$

$$a_{n+2} = c_1 a_{n+1} \oplus c_2 a_n \oplus \dots \oplus c_n a_2$$

...

两边分别乘以  $x^n, x^{n+1}, \dots$ , 再求和, 可得

$$A(x) - (a_1 + a_2 x + \dots + a_n x^{n-1})$$

$$= c_1 x [A(x) - (a_1 + a_2 x + \dots + a_{n-1} x^{n-2})]$$

$$+ c_2 x^2 [A(x) - (a_1 + a_2 x + \dots + a_{n-2} x^{n-3})] + \dots + c_n x^n A(x)$$

移项  
整理

$$\begin{aligned} & (1 + c_1 x + \dots + c_{n-1} x^{n-1} + c_n x^n) A(x) \\ &= (a_1 + a_2 x + \dots + a_n x^{n-1}) + c_1 x (a_1 + a_2 x + \dots + a_{n-1} x^{n-2}) \\ &+ c_2 x^2 (a_1 + a_2 x + \dots + a_{n-2} x^{n-3}) + \dots + c_{n-1} x^{n-1} a_1 \end{aligned}$$

## 定理2.1 证明 (续)

移项  
整理

$$\begin{aligned} & (1+c_1x+\dots+c_{n-1}x^{n-1}+c_nx^n)A(x) \\ &= (a_1+a_2x+\dots+a_nx^{n-1})+c_1x(a_1+a_2x+\dots+a_{n-1}x^{n-2}) \\ &+ c_2x^2(a_1+a_2x+\dots+a_{n-2}x^{n-3})+\dots+c_{n-1}x^{n-1}a_1 \end{aligned}$$

$$p(x)A(x) = \sum_{i=1}^n (c_{n-i}x^{n-i} \sum_{j=1}^i a_jx^{j-1}) = \phi(x)$$

证毕。

注意： $A(x) = \frac{\phi(x)}{p(x)}$

$$\deg \phi(x) \leq n-1$$



## 一些定理和定义

根据初始状态的不同，由递推关系(\*)生成的非恒零的序列有 $2^n-1$ 个，记这 $2^n-1$ 个非零序列的全体为 $G(p(x))$ 。

**定理2.2**  $p(x)|q(x)$ 的充要条件是 $G(p(x)) \subset G(q(x))$ 。

——该定理说明：可用 $n$ 级LFSR产生的序列，也可用**级数更多**的LFSR来产生。

**定义2.3** 设 $p(x)$ 是 $GF(2)$ 上的多项式，使 $p(x)|(x^p-1)$ 成立的最小正整数 $p$ 称为 $p(x)$ **的周期或阶**。

**定理2.3** 若序列 $\{a_i\}$ 的特征多项式 $p(x)$ 定义在 $GF(2)$ 上， $p$ 是 $p(x)$ 的周期，则 $\{a_i\}$ 的周期 $r|p$ 。

——该定理说明： $n$ 级LFSR输出序列的周期 $r$ ，不依赖于初始条件，而依赖于特征多项式 $p(x)$ 。

A decorative graphic consisting of ten horizontal blue lines of varying lengths, stacked vertically, is positioned in the top left corner.

# 第十一讲 m-序列

---

A vertical line with two white circles is positioned on the left side of the slide. The top circle is connected to a blue rectangular box containing the text '线性反馈移位寄存器的多项式表示'. The bottom circle is connected to a blue rectangular box containing the text 'm-序列产生的条件'.

线性反馈移位寄存器的多项式表示

m-序列产生的条件

## 不可约多项式

定理2.4 设 $p(x)$ 是 $n$ 次不可约多项式，周期为 $m$ ，序列 $\{a_i\} \in G(p(x))$ ，则 $\{a_i\}$ 的周期为 $m$ 。

证明：设 $\{a_i\}$ 的周期为 $r$ ，由定理2.3有 $r|m$ ，所以 $r \leq m$ 。

设 $A(x)$ 为 $\{a_i\}$ 的生成函数， $A(x) = \phi(x)/p(x)$ ，即 $p(x)A(x) = \phi(x) \neq 0$ ， $\phi(x)$ 的次数不超过 $n-1$ 。而

$$\begin{aligned} A(x) &= \sum a_i x^{i-1} = a_1 + a_2 x + \dots + a_r x^{r-1} + x^r (a_1 + a_2 x + \dots + a_r x^{r-1}) \\ &\quad + (x^r)^2 (a_1 + a_2 x + \dots + a_r x^{r-1}) + \dots \\ &= a_1 + a_2 x + \dots + a_r x^{r-1} / (1 - x^r) \\ &= a_1 + a_2 x + \dots + a_r x^{r-1} / (x^r - 1) \end{aligned}$$



$$A(x) = \frac{a_1 + a_2x + \cdots + a_rx^{r-1}}{x^r - 1} = \frac{\phi(x)}{p(x)}$$

$$p(x)(a_1 + a_2x + \cdots + a_rx^{r-1}) = \phi(x)(x^r - 1)$$

$$p(x) \mid \phi(x)(x^r - 1)$$

$$\gcd(p(x), \phi(x)) = 1$$

$$p(x) \mid (x^r - 1), \text{ 因此 } m \leq r$$

$$\text{故 } m = r$$

## m-序列产生的必要条件

定理2.5  $n$ 级LFSR产生的序列有最大周期 $2^n-1$ 的必要条件是其特征多项式为不可约的。

证明：设 $n$ 级LFSR产生的序列周期达到最大 $2^n-1$ 。

反证法：设特征多项式为 $p(x)$ ，若 $p(x)$ 可约，可设为 $p(x)=g(x)h(x)$ ，其中 $g(x)$ 不可约，且次数 $k < n$ 。由于 $G(g(x)) \subset G(p(x))$ ，而 $G(g(x))$ 中序列的周期一方面不超过 $2^k-1$ ，另一方面又等于 $2^n-1$ ，这是矛盾的，所以 $p(x)$ 不可约。

该定理的逆不成立，即LFSR的特征多项式为不可约多项式时，其输出序列不一定是 $m$ 序列。

A decorative blue horizontal bar with a series of vertical lines is positioned to the left of the section header.

## 定理2.5 的反例

---

**例2.4**  $f(x)=x^4+x^3+x^2+x+1$ 为GF(2)上的不可约多项式，这可由 $x, x+1, x^2+x+1$ 都不能整除 $f(x)$ 得到。以 $f(x)$ 为特征多项式的LFSR的输出序列可由

$$a_k=a_{k-1}\oplus a_{k-2}\oplus a_{k-3}\oplus a_{k-4}(k\geq 4)$$

和给定的初始状态求出，设初始状态为**0001**，则输出序列为**000110001100011...**，周期为5，不是m序列。

## m-序列产生的充要条件

定义2.4 若 $n$ 次不可约多项式 $p(x)$ 的阶为 $2^n-1$ ，则称 $p(x)$ 是 $n$ 次本原多项式。

定理2.6 设 $\{a_i\} \in G(p(x))$ ， $\{a_i\}$ 为 $m$ 序列的充要条件是 $p(x)$ 为本原多项式。

证明：若 $p(x)$ 是本原多项式，则其阶为 $2^n-1$ ，得 $\{a_i\}$ 的周期等于 $2^n-1$ ，即 $\{a_i\}$ 为 $m$ 序列。

反之，若 $\{a_i\}$ 为 $m$ 序列，即其周期等于 $2^n-1$ ，由定理2.5知 $p(x)$ 是不可约的。由定理2.3知 $\{a_i\}$ 的周期 $2^n-1$ 整除 $p(x)$ 的阶，而 $p(x)$ 的阶不超过 $2^n-1$ ，所以 $p(x)$ 的阶为 $2^n-1$ ，即 $p(x)$ 是本原多项式。

对于任意的正整数 $n$ ，至少存在一个 $n$ 次本原多项式。所以对于任意的 $n$ 级LFSR，至少存在一种连接方式使其输出序列为 $m$ 序列

## m-序列举例

**例2.5** 设 $p(x)=x^4+x+1$ ，若LFSR以 $p(x)$ 为特征多项式，则输出序列的递推关系为

$$a_k = a_{k-1} \oplus a_{k-4} (k \geq 4)$$

若初始状态为1001，则输出为

100100011110101100100011110101...

周期为 $2^4-1=15$ 。

若初始状态为1000，则输出为

100011110101100100011110101...

100100011110101100100011110101...





---

感谢聆听!

[xynie@uestc.edu.cn](mailto:xynie@uestc.edu.cn)

---