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

$$a_{n+k}=c_1a_{n+k-1} \oplus c_2a_{n+k-2} \oplus \cdots \oplus c_na_k \qquad (*)$$

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：

$$p(D)=1+c_1D+\ldots+c_{n-1}D^{n-1}+c_nD^n$$

这种递推关系可用一个一元高次多项式

$$p(x)=1+c_1x+\ldots+c_{n-1}x^{n-1}+c_nx^n$$

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

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

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

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

其中

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

定理2.1的证明

证明： 在等式

$$a_{n+1}=c_1a_n \oplus c_2a_{n-1} \oplus \dots \oplus c_na_1$$

$$a_{n+2}=c_1a_{n+1} \oplus c_2a_n \oplus \dots \oplus c_na_2$$

$$\dots$$

两边分别乘以$x^n, x^{n+1}, \dots$，再求和，可得

$$A(x)-(a_1+a_2x+\dots+a_nx^{n-1})$$

$$=c_1x[A(x)-(a_1+a_2x+\dots+a_{n-1}x^{n-2})]$$

$$+c_2x^2[A(x)-(a_1+a_2x+\dots+a_{n-2}x^{n-3})]+\dots+c_nx^nA(x)$$

移项整理

$$(1+c_1x+\dots+c_{n-1}x^{n-1}+c_nx^n)A(x)$$

$$=(a_1+a_2x+\dots+a_nx^{n-1})+c_1x(a_1+a_2x+\dots+a_{n-1}x^{n-2})$$

$$+c_2x^2(a_1+a_2x+\dots+a_{n-2}x^{n-3})+\dots+c_{n-1}x^{n-1}a_1$$

定理2.1 证明（续）

移项整理

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

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

证毕。

注意：$A(x)=\dfrac{\phi(x)}{p(x)}$

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

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)。

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

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$r\le m$。

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

$$A(x)=\sum a_i x^{i-1}=a_1+a_2x+\ldots+a_rx^{r-1}+x^r(a_1+a_2x+\ldots+a_rx^{r-1})$$

$$+(x^r)^2(a_1+a_2x+\ldots+a_rx^{r-1})+\ldots$$

$$=a_1+a_2x+\ldots+a_rx^{r-1}/(1-x^r)$$

$$=a_1+a_2x+\ldots+a_rx^{r-1}/(x^r-1)$$

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

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

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

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

$$p(x)\mid(x^r-1),\text{因此}m\le r$$

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。

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

<u>100100011110101</u>100100011110101…

周期为$2^4-1=15$。

若初始状态为1000，则输出为

<u>100011110101100</u>100011110101…

<u>100100011110101</u>100100011110101…

感 谢 聆 听!

xynie@uestc.edu.cn