现代密码学

第十二讲 m-序列的伪随机性

信息与软件工程学院

第十二讲 m-序列的伪随机性

- 序列的伪随机性回顾
- m-序列的伪随机性

随机序列的一般特性

游程：设$\{a_i\}=(a_1a_2a_3\cdots)$为二元序列，例如00110111，其前两个数字是00，称为0的2游程；接着是11，是1的2游程；再下来是0的1游程和1的3游程。

自相关函数：GF(2)上周期为T的序列$\{a_i\}$的自相关函数定义为

$$R(t)=\sum_{k=1}^{T}(-1)^{a_k}(-1)^{a_{k+t}},0\le t\le T-1$$

当t=0时，R(t)=T；当t≠0时，称R(t)为异相自相关函数。

Golomb伪随机公设

3个随机性公设：

① 在序列的一个周期内，0与1的个数相差至多为1。

- 说明$\{a_i\}$中0与1出现的概率基本上相同

② 在序列的一个周期内，长为i的游程占游程总数的$1/2^i$ (i=1,2,…)，且在等长的游程中0的游程个数和1的游程个数相等。

- 说明0与1在序列中每一位置上出现的概率相同

③ 异相自相关函数是一个常数。

- 意味着通过对序列与其平移后的序列做比较，不能给出其他任何信息

伪随机序列的定义

设 $\underset{\rightarrow}{a}=(a_1,a_2,\ldots,a_{p(\underset{\rightarrow}{a})},\ldots)$ 是 GF（2）上一个周期等于 $p(\underset{\rightarrow}{a})$ 的周期序列。

如果对于一切 $t\not\equiv 0(\bmod p(\underset{\rightarrow}{a}))$，有

$$R(t)=-1$$

则称序列 $\underset{\rightarrow}{a}=(a_1,a_2,\ldots,a_{p(\underset{\rightarrow}{a})},\ldots)$ 为伪随机序列。

第十二讲 m-序列的伪随机性

序列的伪随机性回顾

m-序列的伪随机性

m序列的随机性

m序列满足Golomb的3个随机性公设。

定理2.7 **GF(2)上的n长m序列$\{a_i\}$具有如下性质：**

① 在一个周期内，**0**、**1**出现的次数分别为$2^{n-1}-1$和2^{n-1}。

② 在一个周期内，总游程数为2^{n-1}；对$1 \le i \le n-2$，长为**i**的游程有2^{n-i-1}个，且**0**、**1**游程各半；长为**n-1**的**0**游程一个，长为**n**的**1**游程一个。

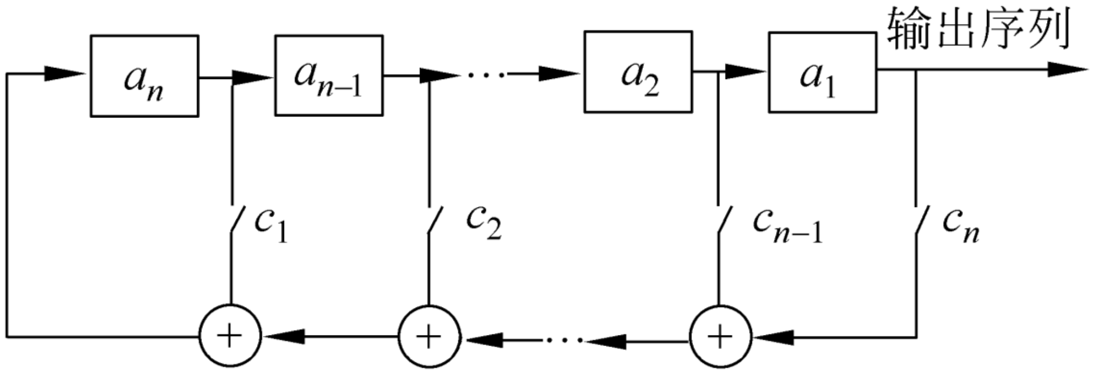
③ $\{a_i\}$的自相关函数为

$$R(t)=\begin{cases}2^n-1, & t=0\\ -1, & 0<t\le 2^n-2\end{cases}$$

定理2.7的证明

证明： ① 在n长m序列的一个周期内，除了全0状态外，每个n长状态（共2^n-1个）都恰好出现一次。

LFSR的输出为每个状态的a_1 ，因此输出为1的状态必然是（**⋯*1）的形式，



而m序列这类状态共有2^{n-1}个，所以输出中1的个数为2^{n-1}个。

输出为0的状态必然是（**⋯*0）的形式，

而m序列这类状态共有$2^{n-1}-1$个（因为不能有全零状态），所以输出中0的个数为$2^{n-1}-1$个。

定理2.7的证明（续）

证明：

② 对n=1,2，易证结论成立。

对n>2，当$1\leqslant i\leqslant n-2$时，n长m序列的一个周期内，长为i的0游程数目等于序列中如下形式的状态数目： 100…01*… … *，其中n-i-2个*可任取0或1。这种状态共有2^{n-i-2}个。同理可得长为i的1游程数目也等于 2^{n-i-2}，所以长为i的游程总数为2^{n-i-1}。

定理2.7的证明（续）

由于寄存器中不会出现全0状态，所以不会出现0的n游程，但必有一个1的n游程，而且1的游程不会更大，因为若出现1的n+1游程，就必然有两个相邻的全1状态，但这是不可能的。这就证明了1的n游程必然出现在如下的串中：

$$0\ \underbrace{11\cdots1}_{n个1}\ 0$$

当这n+2位通过移位寄存器时，便依次产生以下状态：

$$0\ \underbrace{11\cdots1}_{n-1个1}\quad \underbrace{11\cdots1}_{n个1}\ \underbrace{11\cdots1}_{n-1个1}\ 0$$

定理2.7的证明（续）

由于 $0\underbrace{11\cdots1}_{n-1个1}$，$\underbrace{11\cdots1}_{n-1个1}0$ 这两个状态只能各出现一次，所以不会再有1的n-1游程。

0的n-1游程只有一个:

$$1\underbrace{00\cdots0}_{n-1个0}1$$

于是在一个周期内，总游程数为

$$1+1+\sum_{i=1}^{n-2}2^{n-i-1}=2^{n-1}$$

定理2.7的证明（续）

③ $\{a_i\}$是周期为2^n-1的m序列，对于任一正整数$t(0<t<2^n-1)$，$\{a_i\}+\{a_{i+t}\}$在一个周期内为0的位数正好是序列$\{a_i\}$和$\{a_{i+\tau}\}$对应位相同的位数。设序列$\{a_i\}$满足递推关系：

$$a_{h+n}=c_1a_{h+n-1}\oplus c_2a_{h+n-2}\oplus\cdots\oplus c_na_h$$

故$a_{h+n+t}=c_1a_{h+n+t-1}\oplus c_2a_{h+n+t-2}\oplus\cdots\oplus c_na_{h+\tau}$

$$a_{h+n}\oplus a_{h+n+t}=c_1(a_{h+n-1}\oplus a_{h+n+t-1})\oplus c_2(a_{h+n-2}\oplus a_{h+n+t-2})\oplus\cdots\oplus c_n(a_h\oplus a_{h+t})$$

令$b_j=a_j\oplus a_{j+t}$,序列$\{b_j\}$满足：$b_{h+n}=c_1b_{h+n-1}\oplus c_2b_{h+n-2}\oplus\cdots\oplus c_nb_h$

因为对应同样的特征多项式，所以$\{b_i\}$也是m序列。

所以 $R(t)=\sum_{k=1}^{T}(-1)^{a_k}(-1)^{a_{k+t}}=\sum_{k=1}^{T}(-1)^{b_k}=2^{n-1}-1-2^{n-1}=-1$

感 谢 聆 听！

xynie@uestc.edu.cn