

# 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

---

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

## 第十二讲 $m$ -序列的伪随机性

---

A vertical line with two white circles at different heights. The top circle is connected to a blue rectangular box containing the text '序列的伪随机性回顾'. The bottom circle is connected to a blue rectangular box containing the text '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  $\{a_i\} = (a_1 a_2 a_3 \cdots)$  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

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

当  $t=0$  时， $R(t)=T$ ；当  $t \neq 0$  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 $1/2^i$  ( $i=1, 2, \dots$ )，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

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

## 伪随机序列的定义

---

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

如果对于一切  $t \not\equiv 0 \pmod{p(\underline{a})}$ , 有

$$R(t) = -1$$

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

---



## 第十二讲 m-序列的伪随机性

---

A vertical line with two white circles. The top circle is connected to a blue bar containing the text '序列的伪随机性回顾'. The bottom circle is connected to a blue bar containing the text '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 $1 \leq i \leq n-2$ , 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

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

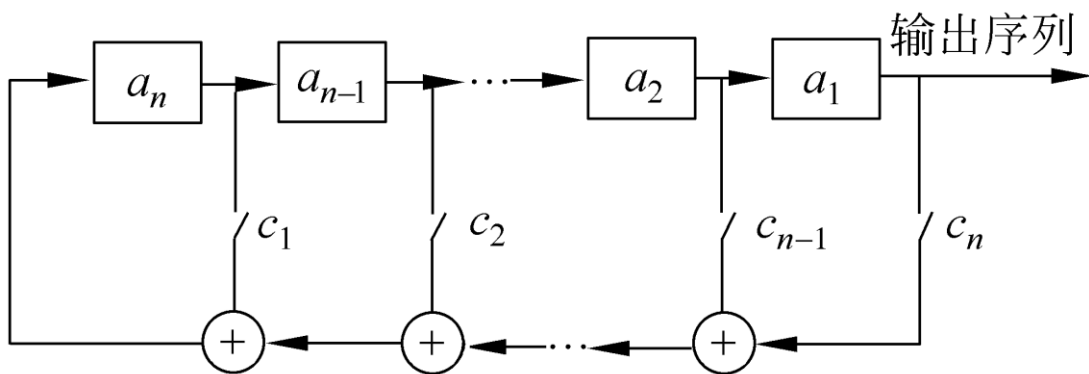
## 定理2.7的证明

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 $(**\cdots*1)$ 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 $(**\cdots*0)$ 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 $1 \leq i \leq n-2$ 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： $100\dots 01*\dots *$ ，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：

$$0 \quad \underbrace{11 \cdots 1}_{n \text{ 个 } 1} \quad 0$$

当这 $n+2$ 位通过移位寄存器时，便依次产生以下状态：

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

## 定理2.7的证明（续）

由于  $0 \underbrace{11 \dots 1}_{n-1 \text{ 个 } 1}$  ,  $\underbrace{11 \dots 1}_{n-1 \text{ 个 } 1} 0$  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：

**$1 \underbrace{00 \dots 0}_{n-1 \text{ 个 } 0} 1$**

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  $\{a_{i+t}\}$  对应位相同的位数。设序列  $\{a_i\}$  满足递推关系：

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

$$\text{故 } a_{h+n+t} = c_1 a_{h+n+t-1} \oplus c_2 a_{h+n+t-2} \oplus \cdots \oplus c_n a_{h+t}$$

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

$$\text{令 } b_j = a_j \oplus a_{j+t}, \text{ 序列 } \{b_j\} \text{ 满足: } b_{h+n} = c_1 b_{h+n-1} \oplus c_2 b_{h+n-2} \oplus \cdots \oplus c_n b_h$$

因为对应同样的特征多项式，所以  $\{b_i\}$  也是  $m$  序列。

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



感谢聆听!

xynie@uestc.edu.cn