



# 现代密码学

## 第九讲 二元序列的伪随机性

信息与软件工程学院

## 第九讲 二元序列的伪随机性

---

A diagram consisting of two white circles connected by a vertical line. Each circle is partially enclosed by a blue rectangular bar. The top bar contains the text '二元序列的相关概念' and the bottom bar contains '伪随机序列'.

二元序列的相关概念

伪随机序列

## 二元序列的定义

- GF (2) 上的一个无限序列

$$\underline{a} = (a_1, a_2, \dots, a_n, \dots)$$

称为二元序列，其中  $a_i \in GF(2)$ 。

- 周期：对于二元序列  $\underline{a}$ ，如果存在正整数  $l$ ，使得对于一切正整数  $k$  都有

$$a_k = a_{k+l}$$

则称  $\underline{a}$  是周期的。

满足上述条件的最小正整数称为  $\underline{a}$  的周期，记为  $p(\underline{a})$

## 周期的性质

- 设GF (2) 上的一个无限序列  $\underline{a} = (a_1, a_2, \dots, a_n, \dots)$  是周期为  $p(\underline{a})$  的二元序列，并设正整数  $l$  对任何非负整数  $k$  都有  $a_k = a_{k+l}$ ，则一定有

$$p(\underline{a}) \mid l$$

- 证明：

设  $l = qp(\underline{a}) + r$ ，其中  $q, r$  为正整数，且  $0 \leq r < p(\underline{a})$ ，则有

$$a_k = a_{k+l}$$

$$\Rightarrow a_k = a_{qp(\underline{a})+r+k}$$

$$\Rightarrow a_k = a_{r+k}$$

又由于  $0 \leq r < p(\underline{a})$ ，根据  $p(\underline{a})$  的极小性可知  $r = 0$ ，因此  $p(\underline{a}) \mid l$ 。



## 游程的定义

设  $\underline{a}$  是 GF (2) 上周期为  $p(\underline{a})$  的周期序列。将  $\underline{a}$  的一个周期

$$(a_1, a_2, \dots, a_{p(\underline{a})})$$

依次排列在一个圆周上使  $a_{p(\underline{a})}$  与  $a_1$  相连, 把这个圆周上形如

$$\underbrace{011\dots110}_{\text{都是1}} \text{ 或 } \underbrace{100\dots001}_{\text{都是0}}$$

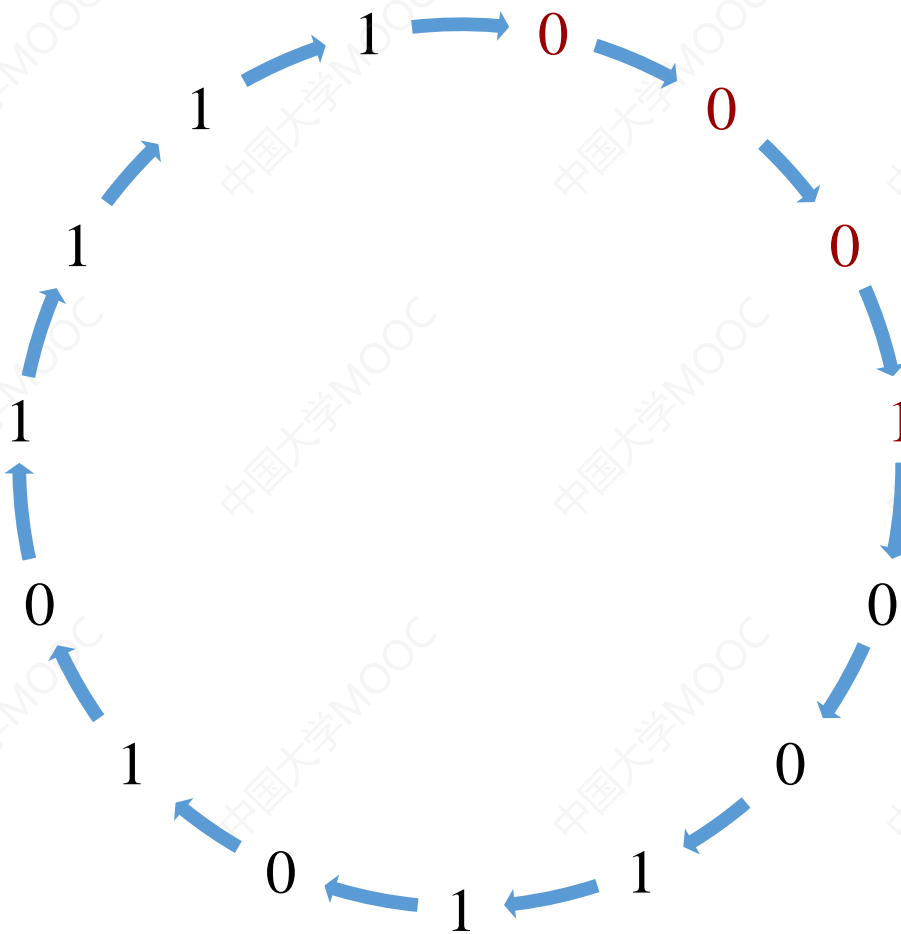
的一连串两两相邻的项分别称为  $\underline{a}$  的一个周期中一个 1 游程或一个 0 游程。而 1 游程中 1 的个数或 0 游程中 0 的个数称为游程的长度。



## 游程的例子

周期为15的二元序列  
**100010011010111**

**011110**为1的4游程  
**10001**为0的3游程



## 自相关函数

**GF(2)**上周期为**T**的序列**{a<sub>i</sub>}**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≠0**时，称**R(t)**为**异相自相关函数**。

# 第九讲 二元序列的随机性

---

A diagram consisting of two white circles connected by a vertical line. Each circle is partially overlapped by a blue rectangular box containing text. The top circle is connected to the top box, and the bottom circle is connected to the bottom box.

二元序列的相关概念

伪随机序列

---



# 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

## 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。

- 可以证明上述定义满足Golomb三个伪随机公设, 详情参考
- 万哲先著。代数 and 编码 (第三版)。高等教育出版社, 2007.



# 伪随机序列的例子

周期为15的二元序列

**100010011010111**

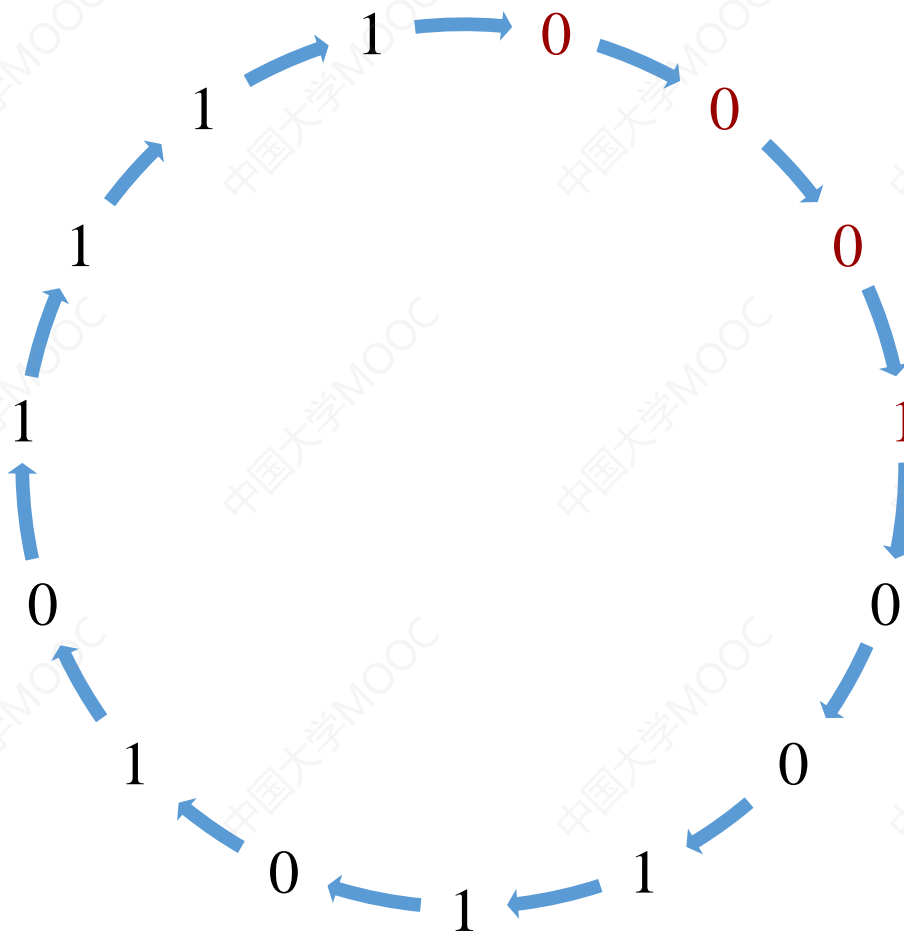
(1) **0**的个数为7

**1**的个数为8

(2) **0**的游程个数为4

**1**的游程个数为4

(3) 异相自相关函数等于  
**-1**



## 伪随机序列还应满足的条件

- C1. 周期 $p$ 要足够大，如大于 $10^{50}$ ；
- C2. 序列 $\{a_i\}_{i \geq 1}$ 产生易于高速生成；
- C3. 当序列 $\{a_i\}_{i \geq 1}$ 的任何部分暴露时，要分析整个序列，提取产生它的电路结构信息，在计算上是不可行的，称此为不可预测性。

C3决定了密码的强度，是流密码理论的核心。它包含了流密码要研究的许多主要问题，如线性复杂度、相关免疫性、不可预测性等等。



---

感谢聆听!

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

---