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

- 二元序列的相关概念
- 伪随机序列

二元序列的伪随机性

- GF（2）上的一个无限序列

$$\underset{\rightarrow}{a}=(a_1,a_2,...,a_n,...)$$

称为二元序列，若 $a_i \in GF(2)$。

- 周期：对于二元序列$\underset{\rightarrow}{a}$，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 $\underset{\rightarrow}{a}$ 是周期的。

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

周期的性质

- 设GF（2）上的一个无限序列 $\underset{\rightarrow}{a}=(a_1,a_2,\ldots,a_n,\ldots)$ 是周期为 $p(\underset{\rightarrow}{a})$ 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

$$p(\underset{\rightarrow}{a})\,|\,l$$

- 证明：

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

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

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

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

又由于 $0\le r<p(\underset{\rightarrow}{a})$，根据 $p(\underset{\rightarrow}{a})$ 的极小性可知 $r=0$，因此 $p(\underset{\rightarrow}{a})\,|\,l$ 。

游程的定义

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

$$(a_1, a_2, \ldots, a_{p(\underset{\rightarrow}{a})})$$

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

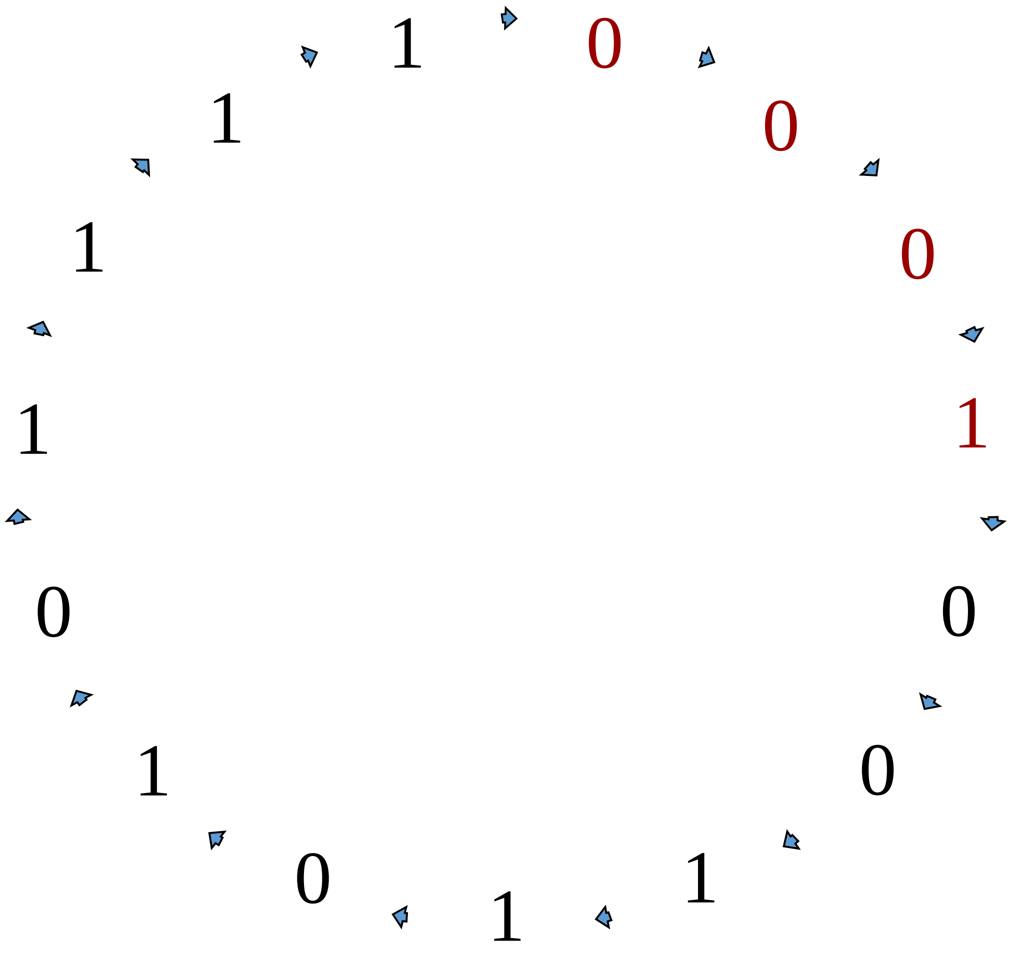
$$0\underbrace{11\cdots11}_{\text{都是1}}0 \text{ 或 } 1\underbrace{00\cdots00}_{\text{都是0}}1$$

的一连串两两相邻的项分别称为 $\underset{\rightarrow}{a}$ 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$\{a_i\}$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。

第九讲 二元序列的随机性

- 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$1/2^i$ $(i=1,2,\ldots)$，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 $t\not\equiv 0(\mathrm{mod}\ p(\underset{\rightarrow}{a}))$，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。

- 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。代数和编码（第三版）。高等教育出版社，2007.

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