



# 通信原理

## 第12章 正交编码与伪随机序列



# 第12章 正交编码与伪随机序列

## • 引言

正交编码与伪随机序列在数字通信技术中都是十分重要的。正交编码不仅可以用作纠错编码，还可以用来实现码分多址通信，目前已经广泛用于蜂窝网中。伪随机序列在误码率测量、时延测量、扩谱通信、密码及分离多径等方面都有着十分广泛的应用。因此，本章将在简要讨论正交编码概念之后，着重讨论伪随机序列及其应用。

# 第12章 正交编码与伪随机序列

## • 12.2 正交编码

### ■ 12.2.1 正交编码的基本概念

#### ◆ 正交性

- 若两个周期为 $T$ 的模拟信号 $s_1(t)$ 和 $s_2(t)$ 互相正交, 则有

$$\int_0^T s_1(t)s_2(t)dt = 0$$

同理, 若 $M$ 个周期为 $T$ 的模拟信号 $s_1(t), s_2(t), \dots, s_M(t)$ 构成一个正交信号集合, 则有

$$\int_0^T s_i(t)s_j(t)dt = 0 \quad i \neq j; \quad i, j = 1, 2, \dots, M$$

#### ◆ 互相关系数

- 对于二进制数字信号, 用一数字序列表示码组。这里, 我们只讨论二进制且码长相同的编码。这时, 两个码组的正交性可用如下形式的互相关系数来表述。



## 第12章 正交编码与伪随机序列

设长为 $n$ 的编码中码元只取值 $+1$ 和 $-1$ ，以及 $x$ 和 $y$ 是其中两个码组：

$$x = (x_1, x_2, x_3, \dots, x_n) \quad y = (y_1, y_2, y_3, \dots, y_n)$$

其中

$$x_i, y_i \in (+1, -1), \quad i = 1, 2, \dots, n$$

则 $x$ 和 $y$ 间的互相关系数定义为

$$\rho(x, y) = \frac{1}{n} \sum_{i=1}^n x_i y_i$$

若码组 $x$ 和 $y$ 正交，则必有 $\rho(x, y) = 0$ 。

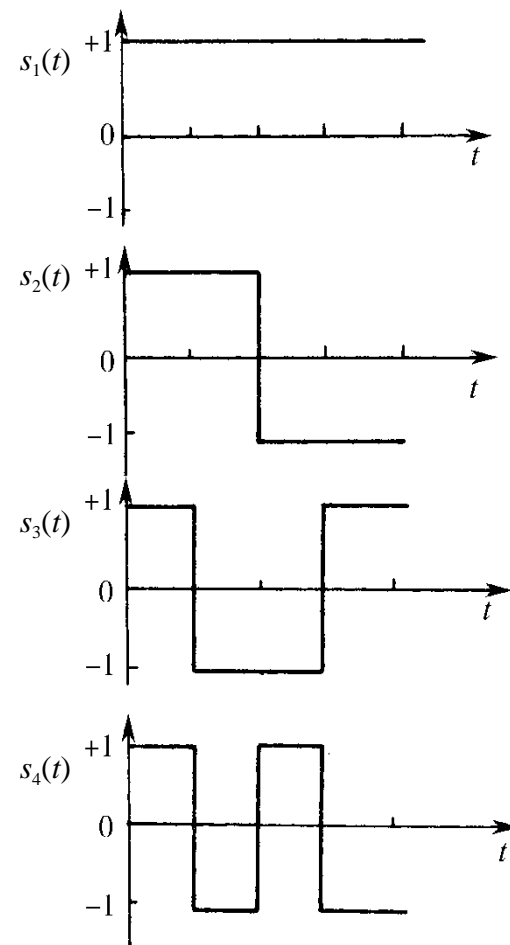
# 第12章 正交编码与伪随机序列

## ◆ 正交编码

例如，下图所示4个数字信号可以看作是如下4个码组：

$$\begin{cases} s_1(t) : (+1, +1, +1, +1) \\ s_2(t) : (+1, +1, -1, -1) \\ s_3(t) : (+1, -1, -1, +1) \\ s_4(t) : (+1, -1, +1, -1) \end{cases}$$

按照互相关系数定义式计算容易得知，这4个码组中任意两者之间的相关系数都为0，即这4个码组两两正交。我们把这种两两正交的编码称为正交编码。



# 第12章 正交编码与伪随机序列

## ◆ 自相关系数:

类似上述互相关系数的定义, 可以对于一个长为 $n$ 的码组 $x$ 定义其自相关系数为

$$\rho_x(j) = \frac{1}{n} \sum_{i=1}^n x_i x_{i+j}, \quad j = 0, 1, \dots, (n-1)$$

式中,  $x$ 的下标按模 $n$ 运算, 即有 $x_{n+k} \equiv x_k$ 。例如, 设

$$x = (x_1, x_2, x_3, x_4) = (+1, -1, -1, +1)$$

则有

$$\rho_x(0) = \frac{1}{4} \sum_{i=1}^4 x_i^2 = 1$$

$$\rho_x(1) = \frac{1}{4} \sum_{i=1}^4 x_i x_{i+1} = \frac{1}{4} (x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_1) = \frac{1}{4} (-1 + 1 - 1 + 1) = 0$$

$$\rho_x(2) = \frac{1}{4} \sum_{i=1}^4 x_i x_{i+2} = \frac{1}{4} (x_1 x_3 + x_2 x_4 + x_3 x_1 + x_4 x_2) = -1$$

$$\rho_x(3) = \frac{1}{4} \sum_{i=1}^4 x_i x_{i+3} = \frac{1}{4} (x_1 x_4 + x_2 x_1 + x_3 x_2 + x_4 x_3) = 0$$

## 第12章 正交编码与伪随机序列

### ◆ 用二进制数字表示互相关系数

- 在二进制编码理论中，常采用二进制数字“0”和“1”表示码元的可能取值。这时，若规定用二进制数字“0”代替上述码组中的“+1”，用二进制数字“1”代替“-1”，则上述互相关系数定义式将变为

$$\rho(x, y) = \frac{A - D}{A + D}$$

式中，A —  $x$ 和 $y$ 中对应码元相同的个数；

D —  $x$ 和 $y$ 中对应码元不同的个数。

- 例如，按照上式规定，上面例子可以改写成

$$\left\{ \begin{array}{l} s_1(t) : (0,0,0,0) \\ s_2(t) : (0,0,1,1) \\ s_3(t) : (0,1,1,0) \\ s_4(t) : (0,1,0,1) \end{array} \right.$$

## 第12章 正交编码与伪随机序列

- ◆ 用二进制数字表示自相关系数

- 上式中，若用 $x$ 的 $j$ 次循环移位代替 $y$ ，就得到 $x$ 的自相关系数 $\rho_x(j)$ 。具体地讲，令

$$x = (x_1, x_2, \dots, x_n)$$

$$y = (x_{1+j}, x_{2+j}, \dots, x_n, x_1, x_2, \dots, x_j)$$

代入定义式

$$\rho(x, y) = \frac{A - D}{A + D}$$

就得到自相关系数 $\rho_x(j)$ 。



# 第12章 正交编码与伪随机序列

## ◆ 超正交码和双正交码

▣ **超正交码**：相关系数 $\rho$ 的取值范围在 $\pm 1$ 之间，即有 $-1 \leq \rho \leq +1$ 。若两个码组间的相关系数 $\rho < 0$ ，则称这两个码组互相超正交。如果一种编码中任两码组间均超正交，则称这种编码为超正交码。

➤ 例如，在上例中，若仅取后3个码组，并且删去其第一位，构成如下新的编码：

$$\begin{cases} s_1'(t) : (0,1,1) \\ s_2'(t) : (1,1,0) \\ s_3'(t) : (1,0,1) \end{cases}$$

则不难验证，由这3个码组所构成的编码是超正交码。

# 第12章 正交编码与伪随机序列

## □ 双正交编码

➤ 由正交编码和其反码便可以构成双正交编码。

➤ 例： 上例中正交码为

$$\begin{cases} s_1(t) : (0,0,0,0) \\ s_2(t) : (0,0,1,1) \\ s_3(t) : (0,1,1,0) \\ s_4(t) : (0,1,0,1) \end{cases}$$

其反码为

$$\begin{cases} (1,1,1,1) \\ (1,1,0,0) \\ (1,0,0,1) \\ (1,0,1,0) \end{cases}$$

上两者的总体即构成如下双正交码：

(0,0,0,0) (1,1,1,1) (0,0,1,1) (1,1,0,0)

(0,1,1,0) (1,0,0,1) (0,1,0,1) (1,0,1,0)

此码共有8种码组，码长为4，任两码组间的相关系数为0或 - 1。

# 第12章 正交编码与伪随机序列

## 12.2.2 阿达玛矩阵

◆ 定义:

- 阿达玛矩阵简记为 **$H$ 矩阵**。它是一种方阵，仅由元素+1和 - 1构成，而且其各行（和列）是互相正交的。最低阶的 **$H$ 矩阵**是2阶的，即

$$\mathbf{H}_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}$$

下面为了简单，把上式中的 + 1和 - 1简写为 + 和 - ，这样上式变成

$$\mathbf{H}_2 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}$$

## 第12章 正交编码与伪随机序列

阶数为2的幂的高阶 $H$ 矩阵可以从下列递推关系得出

$$H_N = H_{N/2} \otimes H_2$$

式中,  $N = 2^m$ ;

$\otimes$  - 直积。

上式中直积是指将矩阵 $H_{N/2}$ 中的每一个元素用矩阵 $H_2$ 代替。  
例如：

$$H_4 = H_2 \otimes H_2 = \begin{bmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{bmatrix} = \begin{bmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{bmatrix}$$

## 第12章 正交编码与伪随机序列

$$H_8 = H_4 \otimes H_2 = \begin{bmatrix} H_4 & H_4 \\ H_4 & -H_4 \end{bmatrix} = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix}$$

- 上面给出几个 $H$ 矩阵的例子，都是对称矩阵，而且第一行和第一列的元素全为“+”。我们把这样的 $H$ 矩阵称为阿达玛矩阵的**正规形式**，或称为**正规阿达玛矩阵**。

# 第12章 正交编码与伪随机序列

## ◆ 性质

- 在 $H$ 矩阵中，交换任意两行，或交换任意两列，或改变任一行中每个元素的符号，或改变任一列中每个元素的符号，都不会影响矩阵的正交性质。因此，正规 $H$ 矩阵经过上述各种交换或改变后仍为 $H$ 矩阵，但不一定是正规的了。
- 按照递推关系式可以构造出所有 $2^k$ 阶的 $H$ 矩阵。可以证明，高于2阶的 $H$ 矩阵的阶数一定是4的倍数。不过，以4的倍数作为阶数是否一定存在 $H$ 矩阵，这一问题并未解决。
- $H$ 矩阵是正交方阵。若把其中每一行看作是一个码组，则这些码组也是互相正交的，而整个 $H$ 矩阵就是一种长为 $n$ 的正交编码，它包含 $n$ 个码组。因为长度为 $n$ 的编码共有 $2^n$ 个不同码组，现在若只将这 $n$ 个码组作为准用码组，其余 $(2^n - n)$ 个为禁用码组，则可以将其多余度用来纠错。这种编码在纠错编码理论中称为里德-缪勒(Reed-Muller)码。



# 第12章 正交编码与伪随机序列

## 12.2.3 沃尔什函数和沃尔什矩阵

### ◆ 沃尔什函数定义

$$wal(2j + p, \theta) = (-1)^{[j/2] + p} \left\{ wal[j, 2(\theta + 1/4)] + (-1)^{j+p} wal[j, 2(\theta - 1/4)] \right\}$$

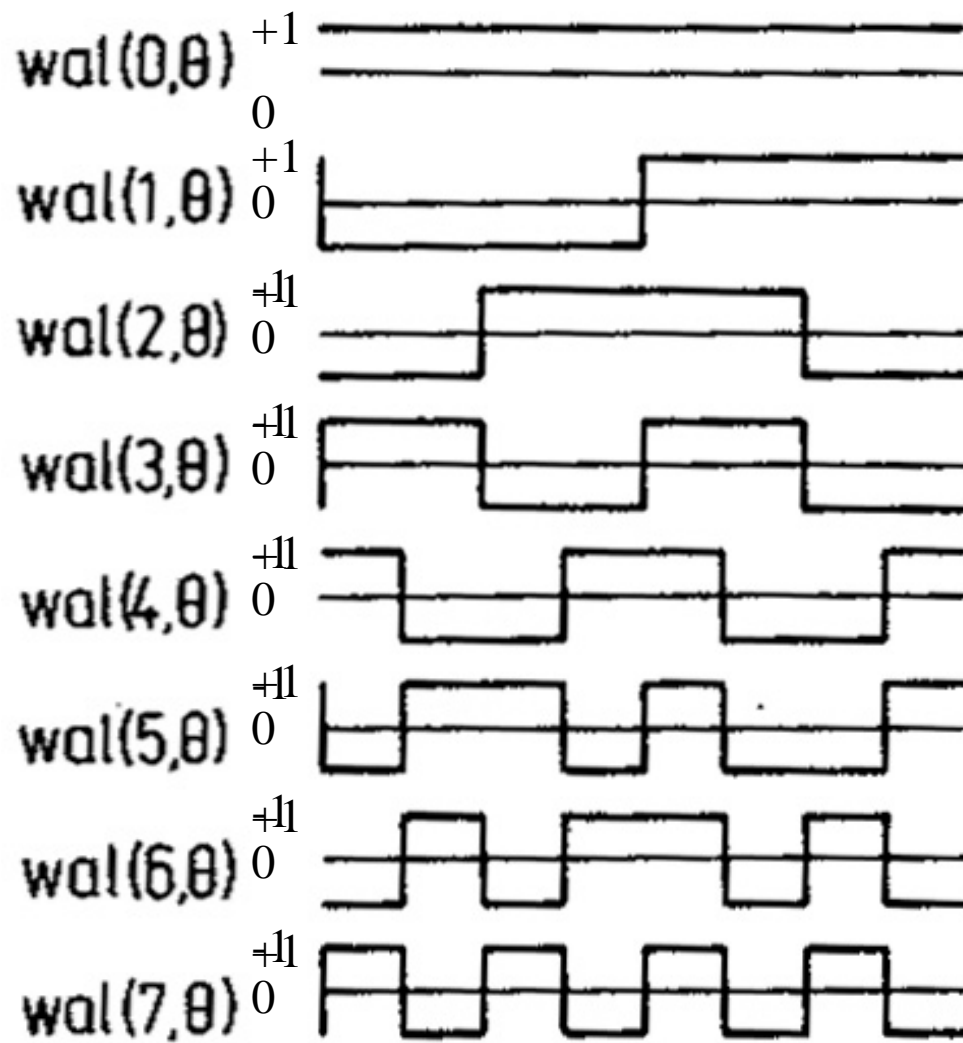
$$wal(0, \theta) = \begin{cases} 1 & -1/2 \leq \theta < 1/2 \\ 0 & \theta < -1/2, \theta \geq 1/2 \end{cases}$$

式中  $p = 0$  或  $1$ ,  $j = 0, 1, 2, \dots$ , 及指数中的  $[j/2]$  表示取  $j/2$  的整数部分。

- ◆ 正弦和余弦函数可以构成一个完备正交函数系。由于正弦和余弦函数具有完备和正交性，所以由其构成的无穷级数或积分（即傅里叶级数和傅里叶积分）可以表示任一波形。类似地，由取值 “+1” 和 “-1” 构成的沃尔什函数也具有完备正交性，也可以用其表示任一波形

# 第12章 正交编码与伪随机序列

- ◆ 前8个沃尔什函数的波形示于下图中





## 第12章 正交编码与伪随机序列

- ◆ 由于沃尔什函数的取值仅为 “+ 1”和 “- 1”，所以可以用其离散的抽样值表示成矩阵形式。例如，上图中的8个沃尔什函数可以写成如下沃尔什矩阵：

$$W = \begin{bmatrix} + & + & + & + & + & + & + & + \\ - & - & - & - & + & + & + & + \\ - & - & + & + & + & + & - & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ - & + & + & - & + & - & - & + \\ - & + & - & + & + & - & + & - \\ + & - & + & - & + & - & + & - \end{bmatrix}$$

由上图和矩阵可以看出，沃尔什矩阵是按照每一行中 “+ 1”和 “- 1”的交变次数由少到多排列的。

沃尔什函数（矩阵）天生具有数字信号的特性，所以它们在数字信号处理和编码理论中有不小应用前景。



# 第12章 正交编码与伪随机序列

## • 12.3 伪随机序列

### ■ 12.3.1 基本概念

#### ◆ 什么是伪随机噪声？

具有类似于随机噪声的某些统计特性，同时又能够重复产生的波形。

#### ◆ 优点：它具有随机噪声的优点，又避免了随机噪声的缺点，因此获得了日益广泛的实际应用。

#### ◆ 如何产生伪随机噪声？

目前广泛应用的伪随机噪声都是由周期性数字序列经过滤波等处理后得出的。在后面我们将这种周期性数字序列称为伪随机序列。它有时又称为伪随机信号和伪随机码。

### ■ 12.3.2 $m$ 序列

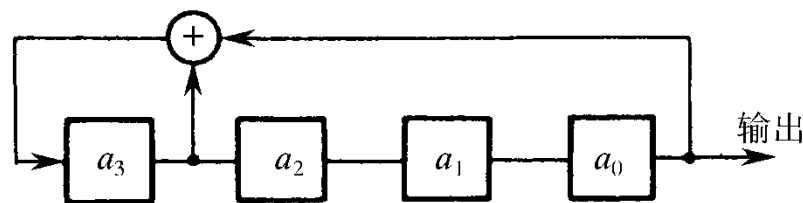
#### ◆ $m$ 序列的产生： $m$ 序列是最长线性反馈移位寄存器序列的简称。它是由带线性反馈的移存器产生的周期最长的一种序列。

# 第12章 正交编码与伪随机序列

例：下图中示出一个4级线性反馈移存器。

设其初始状态为 $(a_3, a_2, a_1, a_0) = (1, 0, 0, 0)$ ，则在移位1次时，由 $a_3$ 和 $a_0$ 模2相加产生新的输入 $a_4 = 1 \oplus 0 = 1$ ，新的状态变为 $(a_4, a_3, a_2, a_1) = (1, 1, 0, 0)$ 。这样移位15次后又回到初始状态 $(1, 0, 0, 0)$ 。

若初始状态为全“0”， $(0, 0, 0, 0)$ ，则移位后得到的仍为全“0”状态。应避免出现全“0”状态，否则移存器的状态将不会改变。



初始状态	1	0	0	0
	1	1	0	0
	1	1	1	0
	1	1	1	1
	0	1	1	1
	1	0	1	1
	0	1	0	1
	1	0	1	0
	1	1	0	1
	0	1	1	0
	0	0	1	1
	1	0	0	1
	0	1	0	0
	0	0	1	0
	0	0	0	1
	1	0	0	0

$2^4 - 1 = 15$  (个)



## 第12章 正交编码与伪随机序列

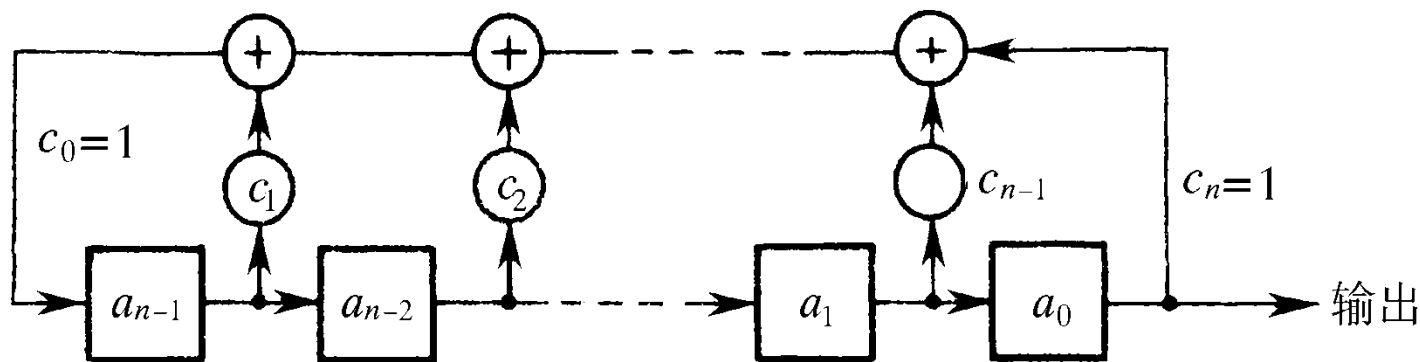
因为4级移存器共有 $2^4 = 16$ 种可能的状态。除全“0”状态外，只剩15种状态可用。这就是说，由任何4级反馈移存器产生的序列的周期最长为15。

我们常常希望用尽可能少的级数产生尽可能长的序列。由上例可见，一般来说，一个 $n$ 级线性反馈移存器可能产生的最长周期等于 $(2^n - 1)$ 。我们将这种最长的序列称为最长线性反馈移存器序列，简称 $m$ 序列。

反馈电路如何连接才能使移存器产生的序列最长，这就是本节将要讨论的主题。

# 第12章 正交编码与伪随机序列

## 一般的线性反馈移存器原理方框图



图中各级移存器的状态用 $a_i$ 表示,  $a_i = 0$ 或 $1$ ,  $i = \text{整数}$ 。

反馈线的连接状态用 $c_i$ 表示,  $c_i = 1$ 表示此线接通 (参加反馈);  $c_i = 0$ 表示此线断开。

反馈线的连接状态不同, 就可能改变此移存器输出序列的周期 $p$ 。

# 第12章 正交编码与伪随机序列

## □ 基本的关系式

### ➤ 递推方程

设一个 $n$ 级移存器的初始状态为： $a_{-1} a_{-2} \dots a_{-n}$ ，经过1次移位后，状态变为 $a_0 a_{-1} \dots a_{-n+1}$ 。经过 $n$ 次移位后，状态为 $a_{n-1} a_{n-2} \dots a_0$ ，上图所示就是这一状态。再移位1次时，移存器左端新得到的输入 $a_n$ ，按照图中线路连接关系，可以写为

$$a_n = c_1 a_{n-1} \oplus c_2 a_{n-2} \oplus \dots \oplus c_{n-1} a_1 \oplus c_n a_0 = \sum_{i=1}^n c_i a_{n-i} \quad (\text{模} 2)$$

因此，一般说来，对于任意一个输入 $a_k$ ，有

$$a_k = \sum_{i=1}^n c_i a_{k-i} \quad - \text{称为递推方程}$$

它给出移位输入 $a_k$ 与移位前各级状态的关系。按照递推方程计算，可以用软件产生 $m$ 序列，不必须用硬件电路实现。

# 第12章 正交编码与伪随机序列

## ➤ 特征方程 (特征多项式)

$c_i$ 的取值决定了移存器的反馈连接和序列的结构, 故 $c_i$ 是一个很重要的参量。现在将它用下列方程表示:

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n = \sum_{i=0}^n c_ix^i \quad - \text{特征方程}$$

式中 $x_i$ 仅指明其系数 (1或0) 代表 $c_i$ 的值,  $x$ 本身的取值并无实际意义, 也不需要去计算 $x$ 的值。例如, 若特征方程为

$$f(x) = 1 + x + x^4$$

则它仅表示 $x_0$ ,  $x_1$ 和 $x_4$ 的系数 $c_0 = c_1 = c_4 = 1$ , 其余的 $c_i$ 为0, 即 $c_2 = c_3 = 0$ 。按照这一特征方程构成的反馈移存器就是上图所示的。



# 第12章 正交编码与伪随机序列

## ➤ 母函数

我们也可以将反馈移存器的输出序列 $\{a_k\}$ 用代数方程表示为

$$G(x) = a_0 + a_1x + a_2x^2 + \cdots = \sum_{k=0}^{\infty} a_k x^k$$

上式称为母函数。

- 递推方程、特征方程和母函数就是我们要建立的3个基本关系式。下面的几个定理将给出它们与线性反馈移存器及其产生的序列之间的关系。



# 第12章 正交编码与伪随机序列

## □ 定理

**【定理12.1】**  $f(x) \cdot G(x) = h(x)$

式中,  $h(x)$ 为次数低于 $f(x)$ 的次数的多项式。

**【证】** 将递推方程代入母函数, 得到

$$\begin{aligned} G(x) &= \sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{\infty} \left( \sum_{i=1}^n c_i a_{k-i} \right) x^{k-i} \cdot x^i = \sum_{i=1}^n c_i x^i \left( \sum_{k=0}^{\infty} a_{k-i} x^{k-i} \right) \\ &= \sum_{i=1}^n c_i x^i \left( a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1} + \sum_{k=0}^{\infty} a_k x^k \right) \\ &= \sum_{i=1}^n c_i x^i (a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1}) + \sum_{i=1}^n c_i x^i \cdot G(x) \end{aligned}$$

移项整理后, 得到

$$\left( 1 + \sum_{i=1}^n c_i x^i \right) G(x) = \sum_{i=1}^n c_i x^i (a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1})$$

## 第12章 正交编码与伪随机序列

$$\left(1 + \sum_{i=1}^n c_i x^i\right) G(x) = \sum_{i=1}^n c_i x^i (a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1})$$

将上式右端用符号 $h(x)$ 表示, 并因 $c_0 \equiv 1$ , 故上式变成

式中 
$$\left(\sum_{i=0}^n c_i x^i\right) \cdot G(x) = h(x)$$

$$h(x) = \sum_{i=1}^n c_i x^i (a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1})$$

由此式可以看出, 当电路给定后,  $h(x)$ 仅决定于初始状态( $a_{-i} \dots a_{-1}$ )。

再将特征方程代入上式, 最后得出

$$f(x) \cdot G(x) = h(x)$$

## 第12章 正交编码与伪随机序列

在

$$h(x) = \sum_{i=1}^n c_i x^i (a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1})$$

中, 若 $a_{-1} = 1$ , 则 $h(x)$ 的最高次项为 $x^{n-1}$ ; 若 $a_{-1} = 0$ , 则最高项次数 $< (n-1)$ , 所以我们得知 $h(x)$ 的最高项次数 $\leq (n-1)$ , 而 $f(x)$ 的最高项次数 $= n$ , 因为已规定 $c_n = 1$ , 特征方程中最高项为 $x_n$ 。故 $h(x)$ 的次数必定低于 $f(x)$ 的次数。【证毕】



## 第12章 正交编码与伪随机序列

**【定理12.2】** 一个 $n$ 级线性反馈移存器之相继状态具有周期性，周期为 $p \leq 2^n - 1$ 。

**【证】** 线性反馈移存器的每一状态完全决定于前一状态。因此，一旦产生一状态 $R$ ，若它与以前的某一状态 $Q$ 相同，则状态 $R$ 后之相继状态必定和 $Q$ 之相继状态相同，这样就可以具有周期性。

在 $n$ 级移存器中，每级只能有两种状态：“1”或“0”。故 $n$ 级移存器最多仅可能有 $2^n$ 种不同状态。所以，在连续 $(2^n + 1)$ 个状态中必有重复。如上所述，一旦状态重复，就有周期性。这时周期 $p \leq 2^n$ 。

若一旦发生全“0”状态，则后继状态也为全“0”，这时的周期 $p = 1$ 。因此，在一个长的周期中不能包括全“0”状态。所以周期 $p \leq (2^n - 1)$ 。【证毕】

## 第12章 正交编码与伪随机序列

**【定理12.3】** 若序列 $A = \{ a_k \}$ 具有最长周期( $p = 2^n - 1$ ), 则其特征多项式 $f(x)$ 应为既约多项式。

**【证】** 所谓既约多项式是指不能分解因子的多项式。若一 $n$ 次多项式 $f(x)$ 能分解成两个不同因子, 则可令

$$f(x) = f_1(x) \cdot f_2(x)$$

这样, 式  $f(x) \cdot G(x) = h(x)$

可以写成如下部分分式之和:

$$G(x) = \frac{h(x)}{f(x)} = \frac{h_1(x)}{f_1(x)} + \frac{h_2(x)}{f_2(x)}$$

式中  $f_1(x)$  的次数为 $n_1$ ,  $n_1 > 0$ ,

$f_2(x)$  的次数为 $n_2$ ,  $n_2 > 0$ ,

且有

$$n_1 + n_2 = n$$

## 第12章 正交编码与伪随机序列

令  $G_1(x) = h_1(x) / f_1(x)$ ;  $G_2(x) = h_2(x) / f_2(x)$

则上式可以改写成  $G(x) = G_1(x) + G_2(x)$

上式表明, 输出序列 $G(x)$ 可以看成是两个序列 $G_1(x)$ 和 $G_2(x)$ 之和, 其中 $G_1(x)$ 是由特征多项式 $f_1(x)$ 产生的输出序列,  $G_2(x)$ 是由特征多项式 $f_2(x)$ 产生的输出序列。而且, 由定理12.2可知,

$G_1(x)$ 的周期为  $p_2 \leq 2^{n_2} - 1$

$G_2(x)$ 的周期为  $p_1 \leq 2^{n_1} - 1$

所以,  $G(x)$ 的周期 $p$ 应是 $p_1$ 和 $p_2$ 的最小公倍数 $\text{LCM}[p_1, p_2]$ , 即

$$p = \text{LCM}[p_1, p_2] \leq p_1 \cdot p_2 \leq (2^{n_1} - 1) \cdot (2^{n_2} - 1)$$

$$= 2^n - 2^{n_1} - 2^{n_2} + 1 \leq 2^n - 3 < 2^n - 1$$

上式表明,  $p$ 一定小于最长可能周期 $(2^n - 1)$ 。

若 $f(x)$ 可以分解成两个相同的因子, 即上面的 $f_1(x) = f_2(x)$ , 同样可以证明 $p < 2^n - 1$ 。

所以, 若 $f(x)$ 能分解因子, 必定有 $p < 2n - 1$ 。【证毕】

## 第12章 正交编码与伪随机序列

**【定理12.4】** 一个 $n$ 级移存器的特征多项式 $f(x)$ 若为既约的, 则由其产生的序列 $A = \{ a_k \}$ 的周期等于使 $f(x)$ 能整除的 $(x^p + 1)$ 中最小正整数 $p$ 。

**【证】** 若序列 $A$  具有周期 $p$ , 则有

$$\begin{aligned}\frac{h(x)}{f(x)} &= G(x) = \sum_{k=0}^{\infty} a_k x^k \\&= a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1} + a_0 x^p + a_1 x^{p+1} + \cdots + a_{p-1} x^{2p-1} + \cdots \\&= (a_0 + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1}) + x^p (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}) + \\&\quad x^{2p} (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}) + \cdots \\&= (1 + x^p + x^{2p} + \cdots)(a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}) \\&= \left( \frac{1}{1 + x^p} \right) (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1})\end{aligned}$$

上式移项整理后, 变成  $\frac{h(x) \cdot (x^p + 1)}{f(x)} = (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1})$

## 第12章 正交编码与伪随机序列

$$\frac{h(x) \cdot (x^p + 1)}{f(x)} = (a_0 + a_1x + \cdots + a_{p-1}x^{p-1})$$

由定理12.1可知,  $h(x)$ 的次数比 $f(x)$ 的低, 而且现已假定 $f(x)$ 为既约的, 所以上式表明 $(x^p + 1)$ 必定能被 $f(x)$ 整除。

应当注意, 此时序列A之周期 $p$ 与初始状态或者说与 $h(x)$ 无关。当然, 这里不考虑全“0”作为初始状态。

上面证明了若序列A具有周期 $p$ , 则 $(x^p + 1)$ 必能被 $f(x)$ 整除。另一方面, 若 $f(x)$ 能整除 $(x^p + 1)$ , 令其商为

$$b_0 + b_1x + \cdots + b_{p-1}x^{p-1}$$

又因为在 $f(x)$ 为既约的条件下, 周期 $p$ 与初始状态无关, 现在考虑初始状态 $a_{-1} = a_{-2} = \cdots = a_{-n+1} = 0, a_{-n} = 1$ , 由式

$$h(x) = \sum_{i=1}^n c_i x^i (a_{-i} x^{-i} + a_{-(i-1)} x^{-(i-1)} + \cdots + a_{-1} x^{-1})$$

可知, 此时有 $h(x) = 1$ 。故有



## 第12章 正交编码与伪随机序列

$$\begin{aligned} G(x) &= \frac{h(x)}{f(x)} = \frac{1}{f(x)} = \frac{b_0 + b_1x + \cdots + b_{p-1}x^{p-1}}{x^p + 1} \\ &= (1 + x^p + x^{2p} + \cdots)(b_0 + b_1x + \cdots + b_{p-1}x^{p-1}) \\ &= (b_0 + b_1x + \cdots + b_{p-1}x^{p-1}) + x^p(b_0 + b_1x + \cdots + b_{p-1}x^{p-1}) + \cdots \end{aligned}$$

上式表明，序列A以 $p$ 或 $p$ 的某个因子为周期。若A以 $p$ 的某个因子 $p_1$ 为周期， $p_1 < p$ ，则由式

$$\frac{h(x) \cdot (x^p + 1)}{f(x)} = (a_0 + a_1x + \cdots + a_{p-1}x^{p-1})$$

已经证明 $(x^{p_1} + 1)$ 必能被 $f(x)$ 整除。

所以，序列A之周期等于使 $f(x)$ 能整除的最最小正整数 $p$ 。

**【证毕】**

# 第12章 正交编码与伪随机序列

## □ 本原多项式

➤ 定义：若一个 $n$ 次多项式 $f(x)$ 满足下列条件：

$f(x)$ 为既约的；

$f(x)$ 可整除 $(x^m + 1)$ ,  $m = 2^n - 1$ ;

$f(x)$ 除不尽 $(x^q + 1)$ ,  $q < m$ ;

则称 $f(x)$ 为本原多项式。

➤ 由定理12.4可以简单写出一个线性反馈移存器能产生 $m$ 序列的充要条件为：反馈移存器的特征多项式为本原多项式。

## 第12章 正交编码与伪随机序列

- 【例】要求用一个4级反馈移存器产生 $m$ 序列，试求其特征多项式。

这时， $n = 4$ ，故此移存器产生的 $m$ 序列的长度为 $m = 2^n - 1 = 15$ 。由于其特征多项式 $f(x)$ 应可整除 $(x^m + 1) = (x^{15} + 1)$ ，或者说，应该是 $(x^{15} + 1)$ 的一个因子，故我们将 $(x^{15} + 1)$ 分解因子，从其因子中找 $f(x)$ ：

$$(x^{15} + 1) = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)$$

$f(x)$ 不仅应为 $(x^{15} + 1)$ 的一个因子，而且还应该是一个4次本原多项式。上式表明， $(x^{15} + 1)$ 可以分解为5个既约因子，其中3个是4次多项式。可以证明，这3个4次多项式中，前2个是本原多项式，第3个不是。因为

$$(x^4 + x^3 + x^2 + x + 1)(x + 1) = (x^5 + 1)$$



## 第12章 正交编码与伪随机序列

$$(x^4 + x^3 + x^2 + x + 1)(x + 1) = (x^5 + 1)$$

这就是说,  $(x^4 + x^3 + x^2 + x + 1)$  不仅可整除  $(x^{15} + 1)$ , 而且还可以整除  $(x^5 + 1)$ , 故它不是本原的。于是, 我们找到了两个4次本原多项式: 和。由其中任何一个都可以产生  $m$  序列, 用作特征多项式构成的4级反馈移存器就是上图中给出的。

### ➤ 本原多项式表

由上述可见, 只要找到了本原多项式, 我们就能由它构成  $m$  序列产生器。但是寻找本原多项式并不是很简单的。经过前人大量的计算, 已将常用本原多项式列成表备查。在下表中列出了部分已经找到的本原多项式。

# 第12章 正交编码与伪随机序列

$n$	本原多项式		$n$	本原多项式	
	代数式	8进制表示法		代数式	8进制表示法
2	$x^2 + x + 1$	7	14	$x^{14} + x^{10} + x^6 + x + 1$	42103
3	$x^3 + x + 1$	13	15	$x^{15} + x + 1$	100003
4	$x^4 + x + 1$	23	16	$x^{16} + x^{12} + x^3 + x + 1$	210013
5	$x^5 + x^2 + 1$	45	17	$x^{17} + x^3 + 1$	400011
6	$x^6 + x + 1$	103	18	$x^{18} + x^7 + 1$	1000201
7	$x^7 + x^3 + 1$	211	19	$x^{19} + x^5 + x^2 + x + 1$	2000047
8	$x^8 + x^4 + x^3 + x^2 + 1$	435	20	$x^{20} + x^3 + 1$	4000011
9	$x^9 + x^4 + 1$	1021	21	$x^{21} + x^2 + 1$	10000005
10	$x^{10} + x^3 + 1$	2011	22	$x^{22} + x + 1$	20000003
11	$x^{11} + x^2 + 1$	4005	23	$x^{23} + x^5 + 1$	40000041
12	$x^{12} + x^6 + x^4 + x + 1$	10123	24	$x^{24} + x^7 + x^2 + x + 1$	100000207
13	$x^{13} + x^4 + x^3 + x + 1$	20033	25	$x^{25} + x^3 + 1$	200000011



## 第12章 正交编码与伪随机序列

在制作 $m$ 序列产生器时，移存器反馈线（及模2加法电路）的数目直接决定于本原多项式的项数。为了使 $m$ 序列产生器的组成尽量简单，我们希望使用项数最少的那些本原多项式。

由表可见，本原多项式最少有3项（这时只需要用一个模2加法器）。对于某些 $n$ 值，由于不存在3项的本原多项式，我们只好列入较长的本原多项式。

由于本原多项式的逆多项式也是本原多项式，例如， $(x^{15} + 1)$ 的因子中的 $(x^4 + x + 1)$ 与 $(x^4 + x^3 + 1)$ 互为逆多项式，即10011与11001互为逆码，所以在表中每一本原多项式可以组成两种 $m$ 序列产生器。



## 第12章 正交编码与伪随机序列

在一些书刊中，有时将本原多项式用8进制数字表示。我们也将这种表示方法示于此表中右侧。例如，对于 $n = 4$ 表中给出“23”，它表示

2	3
0 1 0	0 1 1
$c_5 c_4 c_3$	$c_2 c_1 c_0$

即 $c_0 = c_1 = c_4 = 1$ ,  $c_2 = c_3 = c_5 = 0$ 。

# 第12章 正交编码与伪随机序列

## ◆ $m$ 序列的性质

### □ 均衡性

在 $m$ 序列的一个周期中，“1”和“0”的数目基本相等。准确地说，“1”的个数比“0”的个数多一个。

【证】设一个 $m$ 序列的周期为 $m = 2^n - 1$ ，则此序列可以表示为

$$a_0 a_1 a_2 \cdots a_{n-1} a_n a_{n+1} \cdots a_{m-1} a_0 a_1 \cdots$$

由于此序列中任何相继的 $n$ 位都是产生此序列的 $n$ 级移寄存器的一个状态，而且此移寄存器共有 $m$ 个不同状态，所以可以把此寄存器的这些相继状态列表，如下表所示。表中每一行为寄存器的一个状态。 $m$ 个相继的状态构成此 $m$ 序列的一个周期。由此表直接看出，最后一列的元素按自上而下排列次序就构成上式中的 $m$ 序列。自然，其他各列也构成同样的 $m$ 序列，只是初始相位不同。



# 第12章 正交编码与伪随机序列

$a_{n-1}$	$a_{n-2}$	...	$a_2$	$a_1$	$a_0$
$a_n$	$a_{n-1}$	...	$a_3$	$a_2$	$a_1$
...	...	...	...	...	...
$a_{n+i-1}$	$a_{n+i-2}$	...	$a_{i+2}$	$a_{i+1}$	$a_i$
...	...	...	...	...	...
$a_{n-2}$	$a_{n-3}$	...	$a_1$	$a_0$	$a_{n-1}$
$a_{n-1}$	$a_{n-2}$	...	$a_2$	$a_1$	$a_0$
...	...	...	...	...	...



## 第12章 正交编码与伪随机序列

因为此表中每一元素为一位2进制数字, 即 $a_i \in (0, 1)$ ,  $i = 0, 1, \dots, (m - 1)$ 。所以表中每一位移存器状态可以看成是一个 $n$ 位2进制数字。这 $m$ 个不同状态对应1至 $(2^n - 1)$ 间的 $m$ 个不同的2进制数字。由于1和 $m = (2^n - 1)$ 都是奇数, 故1至 $(2^n - 1)$ 间这 $m$ 个整数中奇数比偶数多1个。在2进制中, 奇数的末位必为“1”, 偶数的末位必为“0”, 而此末位数字就是表中最后一列。故表中最右列的相继 $m$ 个二进数字中“1”比“0”多一个。由于每列都构成一 $m$ 序列, 所以 $m$ 序列中“1”比“0”多一个。

【证毕】

## 第12章 正交编码与伪随机序列

### ▣ 游程分布

我们把一个序列中取值相同的那些相继的（连在一起的）元素合称为一个“**游程**”。在一个游程中元素的个数称为**游程长度**。例如，在前例中给出的 $m$ 序列可以重写如下：

$$\begin{array}{c} m = 15 \\ \cdots \overbrace{1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0} \cdots \end{array}$$

在其一个周期（ $m$ 个元素）中，共有8个游程，其中长度为4的游程有1个，即“1 1 1 1”，长度为3的游程有1个，即“0 0 0”，长度为2的游程有2个，即“1 1”和“0 0”，长度为1的游程有4个，即两个“1”和两个“0”。

一般说来，在 $m$ 序列中，长度为1的游程占游程总数的 $1/2$ ；长度为2的游程占游程总数的 $1/4$ ；长度为3的游程占 $1/8$ ；...

## 第12章 正交编码与伪随机序列

严格讲，长度为 $k$ 的游程数目占游程总数的 $2^{-k}$ ，其中 $1 \leq k \leq (n-1)$ 。而且在长度为 $k$ 的游程中[其中 $1 \leq k \leq (n-2)$ ]，连“1”的游程和连“0”的游程各占一半。下面我们就来证明游程的这种分布规律。

【证】在上表中，每一行有 $n$ 个元素。我们考虑恰好含有连续 $k$ 个“1”的那些行，它们具有形状：

$$0 \underbrace{1 \ 1 \ 1 \ \dots \ 1}_{k \text{个}} 0 \underbrace{\times \ \times \ \dots \ \times}_{(n-2-k) \text{个}} \quad (1 \leq k \leq n-2)$$

其中左侧 $(k+2)$ 个元素中两端为“0”，中间全为“1”，这样就保证恰好含有连续 $k$ 个“1”，而右侧的 $(n-2-k)$ 个元素用“ $\times$ ”表示，它们可以任意取值“0”或“1”，不受限制。在上表的一个周期( $m = 2^n - 1$ 行)中，符合上式形式的行的数目，按排列组合理论可知，等于 $2^{n-2-k}$ 。

## 第12章 正交编码与伪随机序列

由反馈移存器产生 $m$ 序列的原理可知，形式如上式的一行中的 $k$ 个“1”，必定经过逐次位移最后输出，在输出序列中构成长度为 $k$ 的一个连“1”游程。反之，输出序列中任何一个长度为 $k$ 的连“1”游程，必然对应上表中这样的一行。所以，在 $m$ 序列一个周期中长度为 $k$ 的连“1”游程数目也等于 $2^{n-k-2}$ 。同理，长度为 $k$ 的连“0”游程数目也等于 $2^{n-k-2}$ 。所以长度为 $k$ 的游程总数（包括连“1”和连“0”的两种游程）等于

$$2^{n-k-2} + 2^{n-k-2} = 2^{n-k-1}$$

在序列的每一周期中，长度在 $1 \leq k \leq (n-2)$ 范围内的游程所包含的总码元数等于

$$\sum_{k=1}^{n-2} k \cdot 2^{n-k-1} = 1 \cdot 2^{n-2} + 2 \cdot 2^{n-3} + 3 \cdot 2^{n-4} + \cdots + (n-2) \cdot 2^1 = 2^n - 2n$$

上式求和计算中利用了下列算术几何级数公式：

$$\sum_{k=0}^{n-1} (a + kr)q^k = \frac{a - [a + (n-1)r]q^n}{1-q} + \frac{rq(1-q^{n-1})}{(1-q)^2}$$

## 第12章 正交编码与伪随机序列

因为序列的每一周期中共有 $(2^n - 1)$ 个码元，所以除上述码元外，尚余 $(2^n - 1) - (2^n - 2n) = (2n - 1)$ 个码元。这些码元中含有的游程长度，从上表观察分析可知，应该等于 $n$ 和 $(n - 1)$ ，即应有长为 $n$ 的连“1”游程一个，长为 $(n - 1)$ 的连“0”游程一个，这两个游程长度之和恰为 $(2n - 1)$ 。并且由此构成的序列一个周期中，“1”的个数恰好比“0”的个数多一个。

最后，我们得到，在每一周期中，游程总数为

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

计算上式求和时，利用了下列等比级数公式：

$$\sum_{k=1}^n aq^{k-1} = \frac{a(q^n - 1)}{q - 1}$$

所以，长度为 $k$ 的游程占游程总数的比例为

$$\frac{2^{n-k-1}}{2^{n-1}} = 2^{-k}, \quad 1 \leq k \leq (n - 2)$$



## 第12章 正交编码与伪随机序列

由于长度为 $k = (n - 1)$ 的游程只有一个，它在游程总数 $2^{n-1}$ 中占的比例为 $1 / 2^{n-1} = 2^{-(n-1)}$ ，所以上式仍然成立。因此，可将上式改写为

长度为 $k$ 的游程所占比例  $= 2^{-k}$ ,  $1 \leq k \leq (n - 1)$

【证毕】



## 第12章 正交编码与伪随机序列

### □ 移位相加特性

一个 $m$ 序列 $M_p$ 与其经过任意次延迟移位产生的另一个不同序列 $M_r$ 模2相加, 得到的仍是 $M_p$ 的某次延迟移位序列 $M_s$ , 即

$$M_p \oplus M_r = M_s$$

现在分析一个 $m = 7$ 的 $m$ 序列 $M_p$ 作为例子。设 $M_p$ 的一个周期为1110010。另一个序列 $M_r$ 是 $M_p$ 向右移位一次的结果, 即 $M_r$ 的一个相应周期为0121001。这两个序列的模2和为

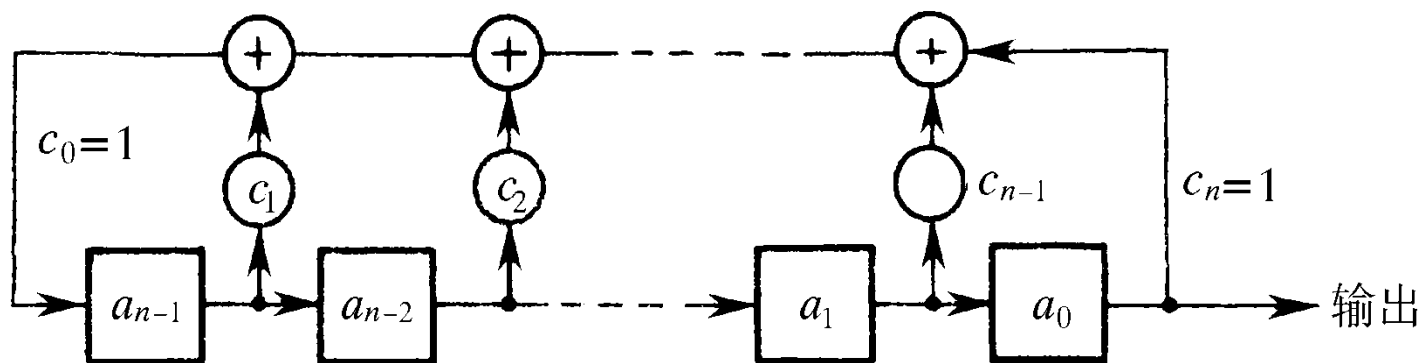
$$1110010 \oplus 0111001 = 1001011$$

上式得出的为 $M_s$ 的一个相应的周期, 它与 $M_p$ 向右移位5次的结果相同。下面我们对 $m$ 序列的这种移位相加特性作一般证明。



## 第12章 正交编码与伪随机序列

【证】设产生序列 $M_p$ 的 $n$ 级反馈移存器的初始状态如下图所示所



这一初始状态也就是上表中第一行的 $a_0 a_1 a_2 \dots a_{n-1}$ 。由这一初始状态代入递推方程式得到移存器下一个输入为

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_n a_0$$

若将序列 $M_p$ 的初始状态的 $r$ 次延迟移位作为序列 $M_r$ 的初始状态，则将 $M_r$ 的初始状态 $a_r a_{r+1} a_{r+2} \dots a_{n+r+1}$ 代入递推方程式，得到下一个输入： $a_{n+r} = c_1 a_{n+r-1} + c_2 a_{n+r-2} + \dots + c_n a_r$

## 第12章 正交编码与伪随机序列

将上两式相加 (模2) , 得到

$$a_n + a_{n+r} = c_1(a_{n-1} + a_{n+r-1}) + c_2(a_{n-2} + a_{n+r-2}) + \cdots + c_n(a_0 + a_r)$$

上式右端 $n$ 个括弧中两元素模2相加的结果一定是上表中另一行的元素。这是因为表中的各行包含了除全“0”外的全部 $n$ 位二进制数字。设相加结果为

$$a_{i+n-1} a_{i+n-2} \cdots a_{i+1} a_i$$

则上式可以改写为

$$a_n + a_{n+r} = c_1 a_{i+n-1} + c_2 a_{i+n-2} + \cdots + c_n a_i$$

上式表明 $(a_n + a_{n+r})$ 仍为原 $n$ 级反馈移存器按另一初始状态 $(a_{i+n-1} a_{i+n-2} \cdots a_{i+1} a_i)$ 产生的输入, 这是因为 $c_1 c_2 \cdots c_n$ 未改变, 移存器的反馈线接法也未改变。这个初始状态比 $M_p$ 的初始状态延迟了 $i$ 位。故序列 $M_p$ 和 $M_r$ 之和是 $M_p$ 经过延迟 $i$ 位的移位序列。【证毕】

# 第12章 正交编码与伪随机序列

## □ 自相关函数

现在我们讨论 $m$ 序列的自相关函数。由12.2节互相关系数定义式得知， $m$ 序列的自相关函数可以定义为：

$$\rho(j) = \frac{A - D}{A + D} = \frac{A - D}{m}$$

式中  $A$  -  $m$ 序列与其 $j$ 次移位序列一个周期中对应元素相同的数目；

$D$  -  $m$ 序列与其 $j$ 次移位序列一个周期中对应元素不同的数目；

$m$  -  $m$ 序列的周期。

上式还可以改写成如下形式：

$$\rho(j) = \frac{[a_i \oplus a_{i+j} = 0] \text{的数目} - [a_i \oplus a_{i+j} = 1] \text{的数目}}{m}$$

## 第12章 正交编码与伪随机序列

由 $m$ 序列的延迟相加特性可知，上式分子中的 $a_i \oplus a_{i+j}$ 仍为 $m$ 序列的一个元素。所以上式分子就等于 $m$ 序列一个周期中“0”的数目与“1”的数目之差。另外，由 $m$ 序列的均衡性可知， $m$ 序列一个周期中“0”的数目比“1”的数目少一个。所以上式分子等于 $-1$ 。这样，就有

$$\rho(j) = \frac{-1}{m}, \quad \text{当 } j = 1, 2, \dots, m-1$$

当 $j = 0$ 时，显然 $\rho(0) = 1$ 。所以，我们最后写成：

$$\rho(j) = \begin{cases} 1, & \text{当 } j = 0 \\ \frac{-1}{m}, & \text{当 } j = 1, 2, \dots, m-1 \end{cases}$$

不难看出，由于 $m$ 序列有周期性，故其自相关函数也有周期性，周期也是 $m$ ，即  $\rho(j) = \rho(j - km)$ ，当  $j \geq km$ ， $k = 1, 2, \dots$  而且 $\rho(j)$ 是偶函数，即有  $\rho(j) = \rho(-j)$ ， $j = \text{整数}$

## 第12章 正交编码与伪随机序列

上面数字序列的自相关函数 $\rho(j)$ 只定义在离散的点上 ( $j$ 只取整数)。但是, 若把 $m$ 序列当作周期性连续函数求其自相关函数, 则从周期函数的自相关函数的定义:

$$R(\tau) = \frac{1}{T_0} \int_{-T_0/2}^{T_0/2} s(t)s(t+\tau)dt$$

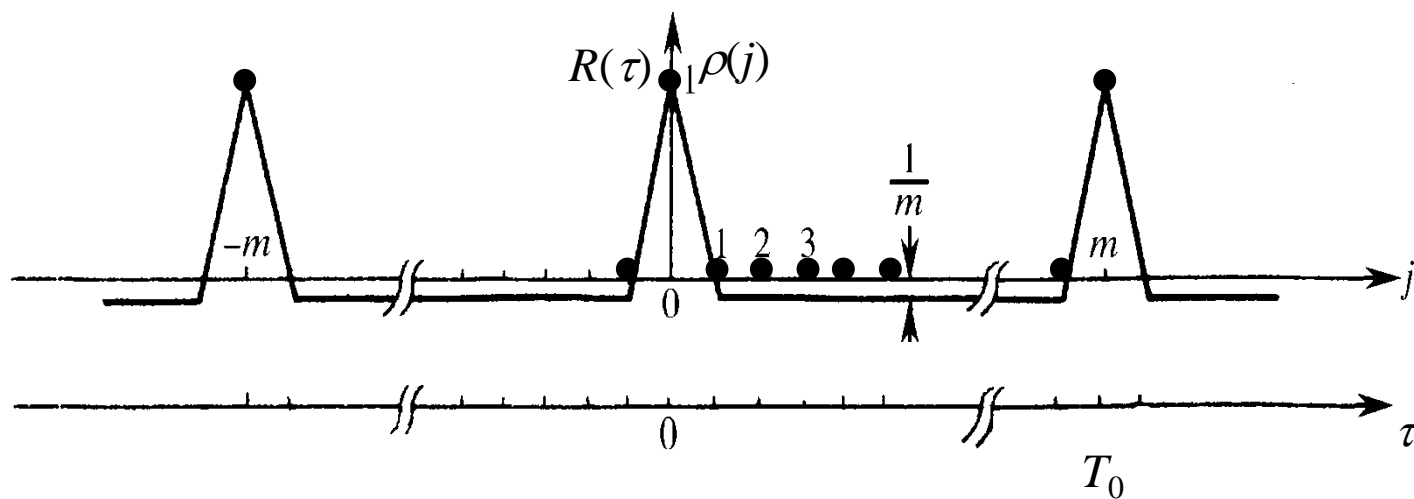
式中  $T_0$  -  $s(t)$ 的周期,

可以求出其自相关函数 $R(\tau)$ 的表示式为

$$R(\tau) = \begin{cases} 1 - \frac{m+1}{T_0} |\tau - iT_0|, & 0 \leq |\tau - iT_0| \leq \frac{T_0}{m}, & i = 0, 1, 2, \dots \\ -1/m, & \text{其他处} \end{cases}$$

## 第12章 正交编码与伪随机序列

按照上面的公式画出的 $\rho(j)$ 和 $R(\tau)$ 的曲线示于下图中。



图中的圆点表示 $j$ 取整数时的 $\rho(j)$ 取值，而折线是 $R(\tau)$ 的连续曲线。可以看出，两者是重合的。由图还可以看出，当周期 $T_0$ 非常长和码元宽度 $T_0/m$ 极小时， $R(\tau)$ 近似于冲激函数 $\delta(t)$ 的形状。

由上述可知， $m$ 序列的自相关函数只有两种取值：0和 $(1/m)$ 。有时把这类序列称为**双值自相关**序列。

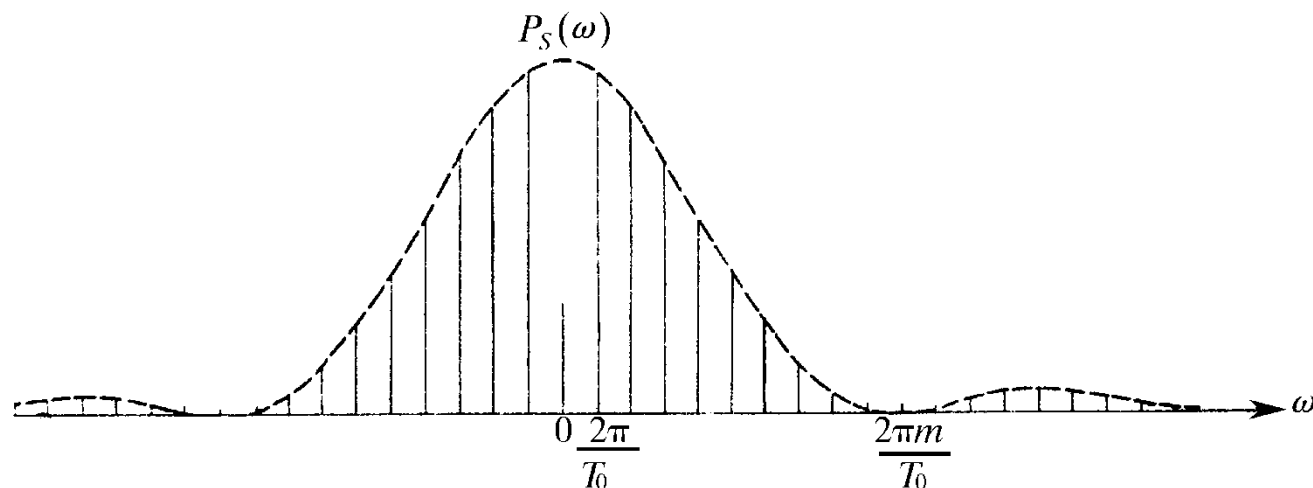
# 第12章 正交编码与伪随机序列

## 功率谱密度

信号的自相关函数与功率谱密度构成一对傅里叶变换。因此，很容易对 $m$ 序列的自相关函数式作傅里叶变换，求出其功率谱密度

$$P_s(\omega) = \frac{m+1}{m^2} \left[ \frac{\sin(\omega T_0 / 2m)}{(\omega T_0 / 2m)} \right]^2 \sum_{\substack{n=-\infty \\ n \neq 0}}^{\infty} \delta\left(\omega - \frac{2\pi n}{T_0}\right) + \frac{1}{m^2} \delta(\omega)$$

按照上式画出的曲线示于下图中。由此图可见，在 $T_0 \rightarrow \infty$ 和 $m/T_0 \rightarrow \infty$ 时， $P_s(\omega)$ 的特性趋于白噪声的功率谱密度特性。



## 第12章 正交编码与伪随机序列

### □ 伪噪声特性

我们对一正态分布白噪声取样，若取样值为正，则记为“+”；若取样值为负，则记为“-”。将每次取样所得极性排成序列，例如

...+-++---+-++--...

这是一个随机序列，它具有如下3个基本性质：

- 序列中“+”和“-”的出现概率相等。
- 序列中长度为1的游程约占1/2；长度为2的游程约占1/4；长度为3的游程约占1/8；...。一般说来，长度为 $k$ 的游程约占 $1/2^k$ 。而且在长度为 $k$ 的游程中，“+”游程和“-”游程约各占一半。
- 由于白噪声的功率谱密度为常数，功率谱密度的逆傅里叶变换，即自相关函数，为一冲激函数 $\delta(\tau)$ 。当 $\tau \neq 0$ 时， $\delta(\tau) = 0$ 。仅当 $\tau = 0$ 时， $\delta(\tau)$ 是个面积为1的脉冲。





## 第12章 正交编码与伪随机序列

由于 $m$ 序列的均衡性、游程分布和自相关特性与上述随机序列的基本性质极相似，所以通常将 $m$ 序列称为伪噪声(PN)序列，或称为伪随机序列。

但是，具有或部分具有上述基本性质的PN序列不仅只有 $m$ 序列一种。 $m$ 序列只是其中最常见的一种。除 $m$ 序列外， $M$ 序列、二次剩余序列（或称为Legendre序列）、霍尔(Hall)序列和双素数序列等都是PN序列。



# 第12章 正交编码与伪随机序列

---



# 第12章 正交编码与伪随机序列

## 12.3.3 其他伪随机序列简介

### ◆ $M$ 序列

- 定义：由非线性反馈移存器产生的周期最长的序列称为  $M$  序列。

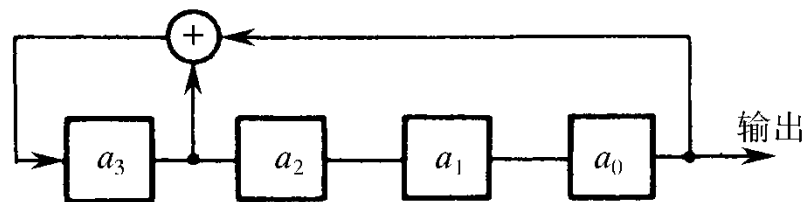
由上节对  $m$  序列产生器的分析可知，一个  $n$  级  $m$  序列产生器只可能有  $(2^n - 1)$  种不同的状态。但是  $n$  级移存器最多可有  $2^n$  种状态，在  $m$  序列中不能出现的是全 “0” 状态。在线性反馈条件下，全 “0” 状态出现后，产生器的状态将不会再改变；但是在非线性反馈条件下，却不一定如此。因此，非线性反馈移存器的最长周期可达  $2^n$ ，我们称这种周期长达  $2^n$  的序列为  $M$  序列。

# 第12章 正交编码与伪随机序列

## □ $M$ 序列的产生方法

目前，如何产生 $M$ 序列的问题，尚未从理论上完全解决，人们只找到很少几种构造它的方法。下面仅简单介绍利用 $m$ 序列产生器构成 $M$ 序列产生器的方法。

首先观察右图中的例子。它是一个 $n = 4$ 级的 $m$ 序列产生器。图中给出了它的15种状态。若使它增加一个“000”状态，就可变成 $M$ 序列产生器了。



初始状态	1	0	0	0
	1	1	0	0
	1	1	1	0
	1	1	1	1
	0	1	1	1
	1	0	1	1
	0	1	0	1
	1	0	1	0
	1	1	0	1
	0	1	1	0
	0	0	1	1
	1	0	0	1
	0	1	0	0
	0	0	1	0
	0	0	0	1
	1	0	0	0

$2^4 - 1 = 15$  (个)

## 第12章 正交编码与伪随机序列

因为移存器中后级状态必须是由其前级状态移入而得，故此“0000”状态必须处于初始状态“1000”之前和“0001”状态之后。这就是说，我们需要将其递推方程修改为非线性方程，使“0001”状态代入新的递推方程后，产生状态“0000”（而不是“1000”），并且在“0000”状态代入后产生状态“1000”（而不是保持“0000”不变）。

修改前的递推方程为

$$a_k = \sum_{i=1}^n c_i a_{k-i} = a_{k-1} \oplus a_{k-4}$$

为满足上述要求，修改后的递推方程应为

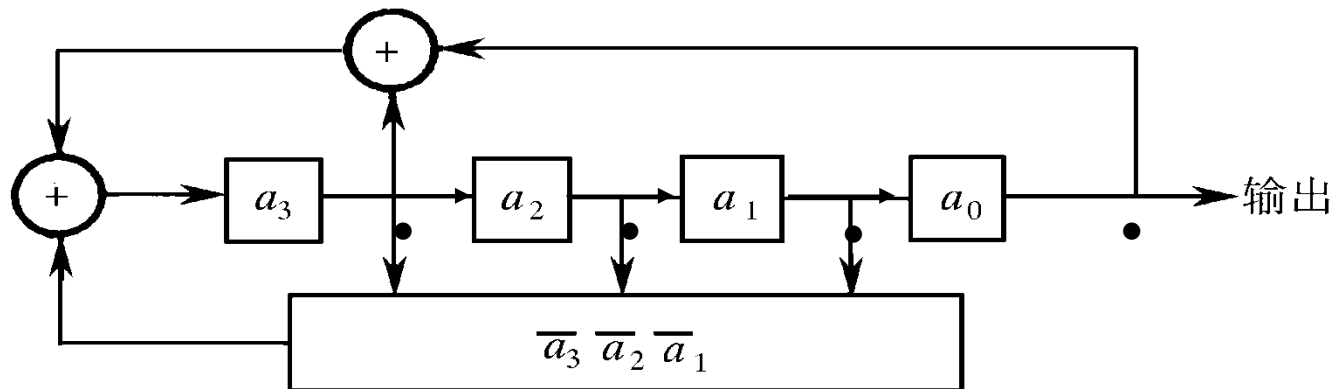
$$\begin{aligned} a_k &= a_{k-1} \oplus a_{k-4} \oplus \bar{a}_{k-1} \bar{a}_{k-2} \bar{a}_{k-3} a_{k-4} \oplus \bar{a}_{k-1} \bar{a}_{k-2} \bar{a}_{k-3} \bar{a}_{k-4} \\ &= a_{k-1} \oplus a_{k-4} \oplus \bar{a}_{k-1} \bar{a}_{k-2} \bar{a}_{k-3} = \sum_{i=1}^4 c_i a_{k-i} \oplus \bar{a}_{k-1} \bar{a}_{k-2} \bar{a}_{k-3} \end{aligned}$$

## 第12章 正交编码与伪随机序列

对于 $n$ 级 $m$ 序列产生器也一样。为使 $n$ 级 $m$ 序列产生器变成 $M$ 序列产生器，也只需使其递推方程改为

$$a_k = \sum_{i=1}^4 c_i a_{k-i} \oplus \bar{a}_{k-1} \bar{a}_{k-2} \cdots \bar{a}_{k-n+1} = \sum_{i=1}^n c_i a_{k-i} \oplus \prod_{j=1}^{n-1} \bar{a}_{k-i}$$

有了递推方程，就不难构造出此 $M$ 序列产生器。例如用这种方法得到的一个4级 $M$ 序列产生器如下图所示。





# 第12章 正交编码与伪随机序列

## □ $M$ 序列的性质

$M$ 序列与 $m$ 序列类似，也在一定程度上具有噪声特性。它满足 $m$ 序列的前两个性质，即：

- 在 $M$ 序列的一个周期中，出现“0”与“1”的数目相等。
- 在 $n$ 级 $M$ 序列的一个周期中，游程共有 $2^{n-1}$ 个，其中长度为 $k$ 的游程占 $1/2^k$ ， $1 \leq k \leq n-2$ ；长为 $n$ 的游程有两个，没有长为 $(n-1)$ 的游程。在同长的游程中，“0”游程和“1”游程各占一半。这两个性质的证明方法与 $m$ 序列的一样。

但是， $M$ 序列不再具有 $m$ 序列的移位相加特性及双值自相关特性。

## 第12章 正交编码与伪随机序列

### □ $M$ 序列的优点

$M$ 序列与 $m$ 序列相比，最主要的优点是数量大，即同样级数 $n$ 的移存器能够产生的平移不等价 $M$ 序列总数比 $m$ 序列的大得多，且随 $n$ 的增大迅速增加。在下表中给出了级数 $n$ 与可能产生的两种序列数目的比较。

$n$	1	2	3	4	5	6	7	8	9	10
$m$ 序列数目	1	1	2	2	6	6	18	16	48	60
$M$ 序列数目	1	1	2	16	2048	6.71088 $\times 10^7$	1.44115 $\times 10^{17}$	1.32922 $\times 10^{36}$	2.26156 $\times 10^{74}$	1.30935 $\times 10^{151}$

$M$ 序列的数量虽然相当大，但是目前能够实际产生出来的 $M$ 序列数目却还不很多。这还有待于今后继续研究。



# 第12章 正交编码与伪随机序列

## ◆ 二次剩余序列

- 定义：二次剩余又称平方剩余数，例如， $3^2 = 9$ ；9被7除得到的余数是2，即有

$$3^2 = 9 \equiv 2 \pmod{7}$$

则称2为模7的平方剩余数。

一般说来，如果能找到一个整数 $x$ ，它使

$$x^2 \equiv i \pmod{p}$$

若此方程成立，我们就认为这个方程有解。满足此方程的 $i$ 就是模 $p$ 的二次剩余；否则， $i$ 就是模 $p$ 的二次非剩余。当规定 $a_0 = -1$ ，且

$$a_i = \begin{cases} 1, & \text{若 } i \text{ 是模 } p \text{ 的二次剩余} \\ -1, & \text{若 } i \text{ 是模 } p \text{ 的非二次剩余} \end{cases}$$

其中 $p$ 为奇数，则称 $\{a_i\}$ 为二次剩余序列， $i = 0, 1, 2, \dots$ ，其周期为 $p$ 。

## 第12章 正交编码与伪随机序列

□ 例：设 $p = 19$ ，容易算出

$$12 \equiv 1 \pmod{19},$$

$$32 \equiv 9 \pmod{19},$$

$$52 \equiv 6 \pmod{19},$$

$$72 \equiv 11 \pmod{19},$$

$$92 \equiv 5 \pmod{19},$$

$$112 \equiv 7 \pmod{19},$$

$$132 \equiv 17 \pmod{19},$$

$$152 \equiv 16 \pmod{19},$$

$$172 \equiv 4 \pmod{19},$$

$$22 \equiv 4 \pmod{19},$$

$$42 \equiv 16 \pmod{19},$$

$$62 \equiv 17 \pmod{19},$$

$$82 \equiv 7 \pmod{19},$$

$$102 \equiv 5 \pmod{19},$$

$$122 \equiv 11 \pmod{19},$$

$$142 \equiv 6 \pmod{19},$$

$$162 \equiv 9 \pmod{19},$$

$$182 \equiv 1 \pmod{19}.$$

因此，1、4、5、6、7、9、11、16、17是模19的二次剩余；  
而2、3、8、10、12、13、14、15、18是模19的非二次剩余。



## 第12章 正交编码与伪随机序列

这样，得到周期 $p = 19$ 的二次剩余序列为：

- + — — + + + - + - + — — — — + + -

式中  $+ \equiv +1$ ;  $- \equiv -1$ 。

这种序列具有随机序列基本性质的第1)条性质，但一般不具备第2)条性质。当 $p = 4t - 1$ 时 ( $t =$  正整数)，它是双值自相关序列，即具有近于随机序列基本性质第3)条的性质；当 $p = 4t + 1$ 时，它不是双值自相关序列。但是若 $p$ 很大，它仍具有近于第3)条的性质。一般认为它也属于伪随机序列。

# 第12章 正交编码与伪随机序列

## ◆ 双素数序列

- 上述二次剩余序列的周期 $p$ 为素数。在双素数序列中，周期 $p$ 是两个素数 $p_1$ 和 $p_2$ 的乘积，而且 $p_2 = p_1 + 2$ ，即有

$$p = p_1 \cdot p_2 = p_1(p_1 + 2)$$

- 定义：双素数序列 $\{a_i\}$ 的定义为：

$$a_i = \begin{cases} \left(\frac{i}{p_1}\right)\left(\frac{i}{p_2}\right), & \text{当}(i, p) = 1 \\ 1, & \text{当} i \equiv 0 \pmod{p_2} \\ -1, & \text{当} i \text{为其他值} \end{cases}$$

式中

$$\left(\frac{i}{p_j}\right) = \begin{cases} 1, & \text{若} i \text{是模} p_j \text{的二次剩余} \\ -1, & \text{若} i \text{是模} p_j \text{的非二次剩余} \end{cases} \quad (j=1,2)$$

$(i, p) = 1$ 表示 $i$ 和 $p$ 互为素数（最大公因子为1）。

## 第12章 正交编码与伪随机序列

- 例：设 $p_1=3$ ,  $p_2=5$ ,  $p=3 \cdot 5=15$ 。这时在一个周期中满足 $(i, p)=1$ 条件的 $i$ , 即小于15且与15互素的正整数有：1、2、4、7、8、11、13、14。对于这些 $i$ 值, 可以计算出：

$$\left(\frac{i}{p_1}\right): \quad \left(\frac{1}{3}\right) = \left(\frac{4}{3}\right) = \left(\frac{7}{3}\right) = \left(\frac{13}{3}\right) = 1$$

$$\left(\frac{2}{3}\right) = \left(\frac{8}{3}\right) = \left(\frac{11}{3}\right) = \left(\frac{14}{3}\right) = -1$$

$$\left(\frac{i}{p_2}\right): \quad \left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{11}{5}\right) = \left(\frac{14}{5}\right) = 1,$$

$$\left(\frac{2}{5}\right) = \left(\frac{7}{5}\right) = \left(\frac{8}{5}\right) = \left(\frac{13}{5}\right) = -1,$$

## 第12章 正交编码与伪随机序列

对这些 $i$ 值作 $(i/p_1)(i/p_2)$ 的运算后, 得出 $a_1 = a_2 = a_4 = a_8 = 1$ 以及 $a_7 = a_{11} = a_{13} = a_{14} = -1$ 。又因 $i = 0 \equiv 5 = 10 \pmod{5}$ , 故 $a_0 = a_5 = a_{10} = 1$ 。对于其余的 $i$ , 有 $a_3 = a_6 = a_9 = a_{12} = -1$ 。所以此双素数序列为:

+ + + - + + — — + - + — — — —

式中  $+ \equiv +1$ ;

$- \equiv -1$ 。

可以验证, 双素数序列也基本满足随机序列的基本性质, 所以也属于PN序列。



# 第12章 正交编码与伪随机序列

## • 12.4 扩展频谱通信

### ■ 分类：

- ◆ 直接序列(DS)扩谱：它通常用一段伪随机序列（又称为伪码）表示一个信息码元，对载波进行调制。伪码的一个单元称为一个**码片**。由于码片的速率远高于信息码元的速率，所以已调信号的频谱得到扩展。
- ◆ 跳频(FH)扩谱：它使发射机的载频在一个信息码元的时间内，按照预定的规律，离散地快速跳变，从而达到扩谱的目的。载频跳变的规律一般也是由伪码控制的。
- ◆ **线性调频**：载频在一个信息码元时间内在一个宽的频段中线性地变化，从而使信号带宽得到扩展。由于此线性调频信号若工作在低频范围，则它听起来像鸟声，故又称“鸟声”调制。



# 第12章 正交编码与伪随机序列

## 目的

- 提高抗窄带干扰的能力，特别是提高抗有意干扰的能力。由于这类干扰的带宽窄，所以对于宽带扩谱信号的影响不大。
- 防止窃听。扩谱信号的发射功率谱密度可以很小，小到低于噪声的功率谱密度，将发射信号隐藏在背景噪声中，使侦听者很难发现。此外，由于采用了伪码，窃听者不能方便地听懂发送的消息。
- 提高抗多径传输效应的能力。由于扩谱调制采用了扩谱伪码，它可以用来分离多径信号，所以有可能提高其抗多径的能力。
- 多个用户可以共用同一频带。在同一扩谱频带内，不同用户采用互相正交的不同扩谱码，就可以区分各个用户的信号，从而按照码分多址的原理工作。
- 提供测距能力。通过测量扩谱信号的自相关特性的峰值出现时刻，可以从信号传输时间的大小计算出传输距离

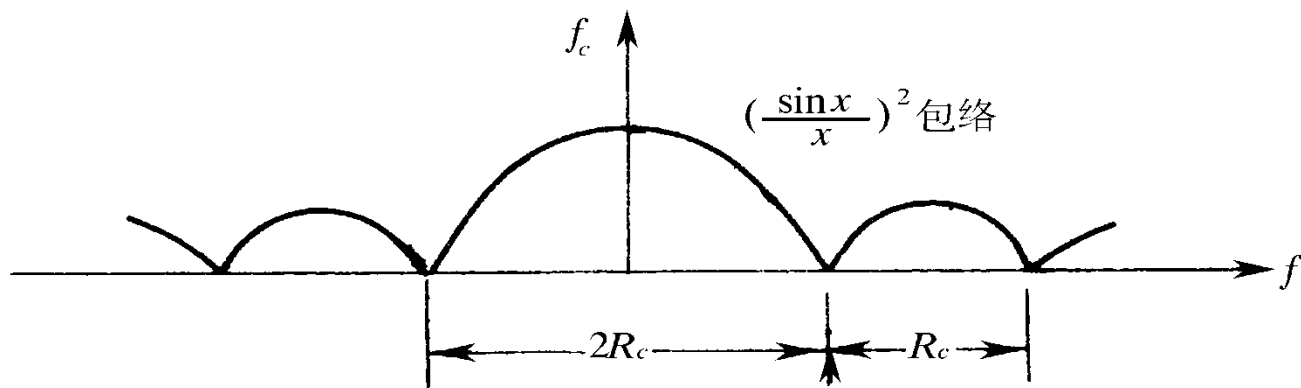


# 第12章 正交编码与伪随机序列

## 直接序列扩谱系统

### ◆ 原理

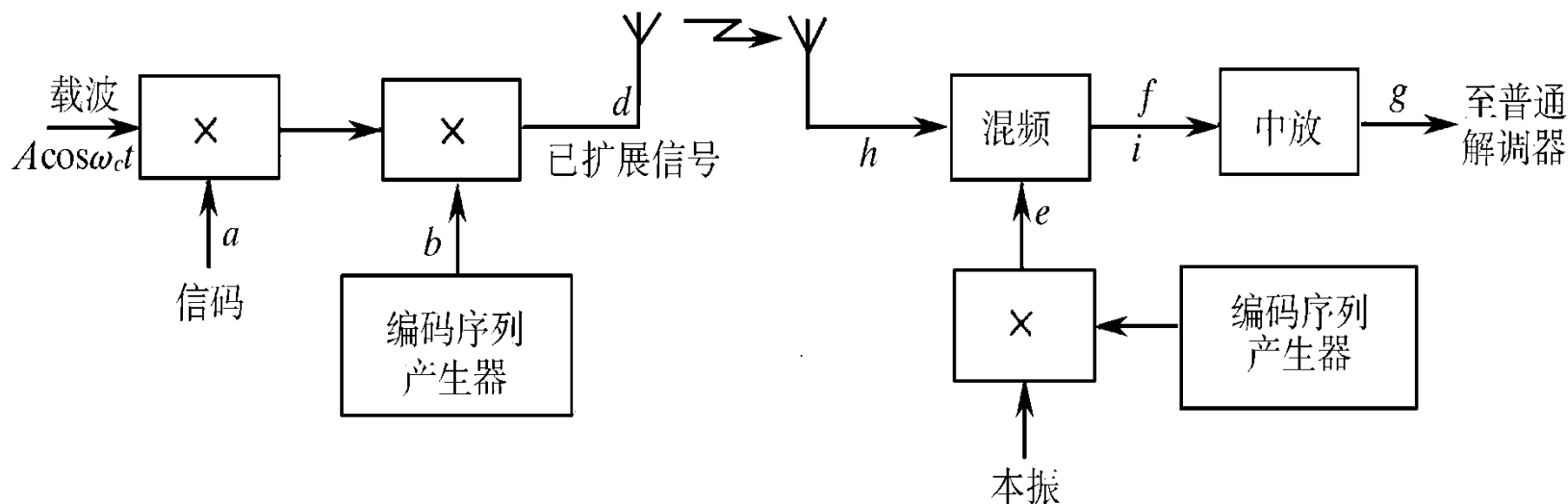
- 用一组伪码代表信息码元去调制载波。最常用的是2PSK。这种信号的典型功率谱密度曲线示于下图中。



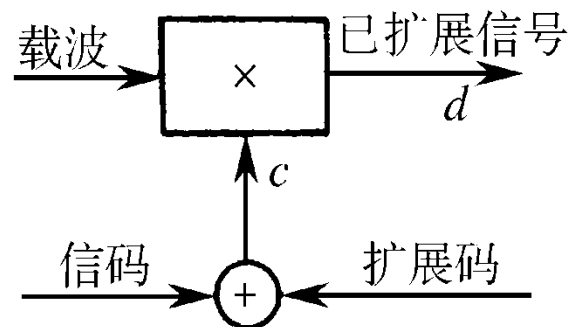
图中所示主瓣带宽（零点至零点）是伪码时钟速率 $R_c$ 的两倍。每个旁瓣的带宽等于 $R_c$ 。例如，若所用码片的速率为5 Mb/s，则主瓣带宽将为10 MHz，每个旁瓣宽为5 MHz。

# 第12章 正交编码与伪随机序列

## ◆ 原理方框图



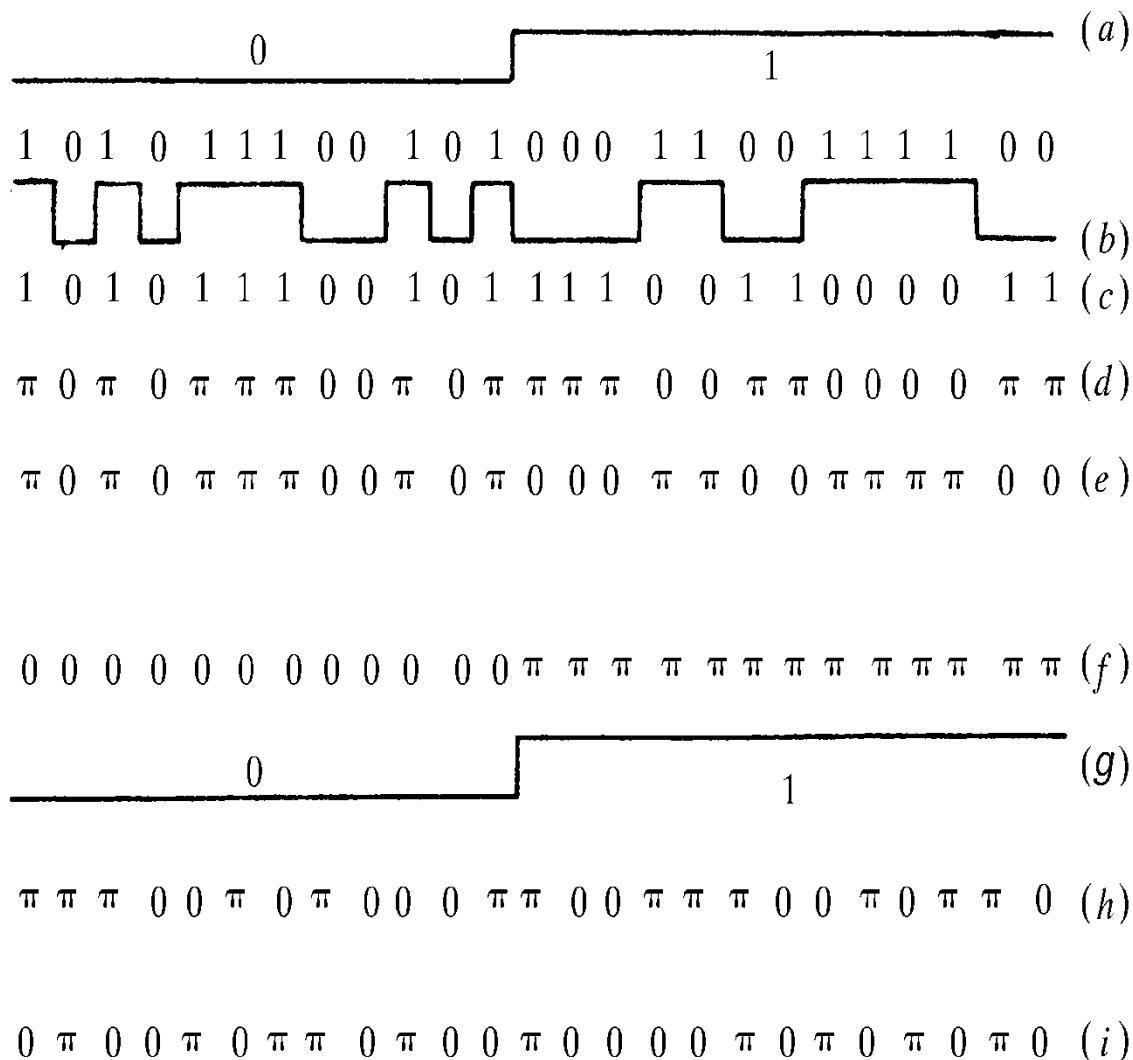
- ◆ 调制器简化方框图：先将两路编码序列模2相加，然后再去进行反相键控。



# 第12章 正交编码与伪随机序列

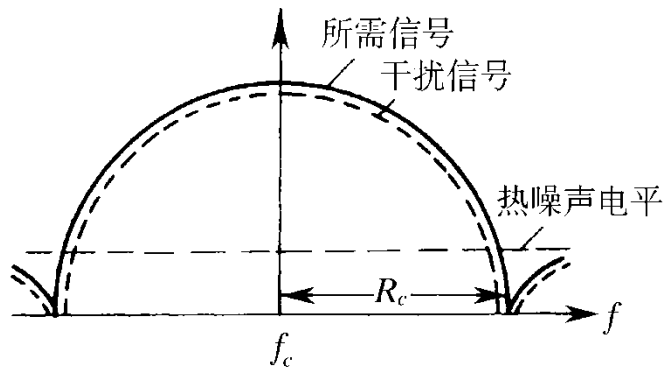
## ◆ 接收过程图解

- (a) 信码;
- (b) 伪码序列;
- (c) 发送序列;
- (d) 发送载波相位;
- (e) 混频用本振相位;
- (f) 中频相位;
- (g) 解调信号;
- (h) 干扰信号相位;
- (i) 混频后干扰信号相位。

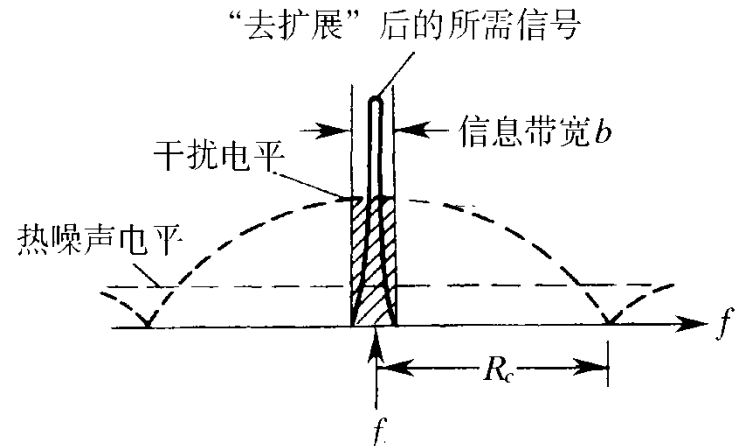


# 第12章 正交编码与伪随机序列

## ◆ 信号和干扰信号在频域中的变化



(a) 在接收机输入端



(b) 在接收机中放输出端

# 第12章 正交编码与伪随机序列

## 12.5 伪随机序列的其他应用

### ■ 分离多径技术

- ◆ 目的：多径衰落的原因在于每条路径的接收信号的相位不同。分离多径技术能够在接收端将多径信号的各条路径分离开，并分别校正每条路径接收信号的相位，使之按同相相加，从而克服衰落现象。

### ◆ 原理

- 考察发射的一个数字信号码元。设这个码元是用 $m$ 序列的一个周期去调制的余弦载波

$$M(t) \cos(\omega t + \theta)$$

其中 $M(t)$ 为一取值 $\pm 1$ 的 $m$ 序列。假设经过多径传输后，在接收机中频部分得到的输出信号为

$$\sum_{j=0}^{n-1} A_j M(t - j\Delta) \cos[\omega_i(t - j\Delta) + \varphi_j]$$



## 第12章 正交编码与伪随机序列

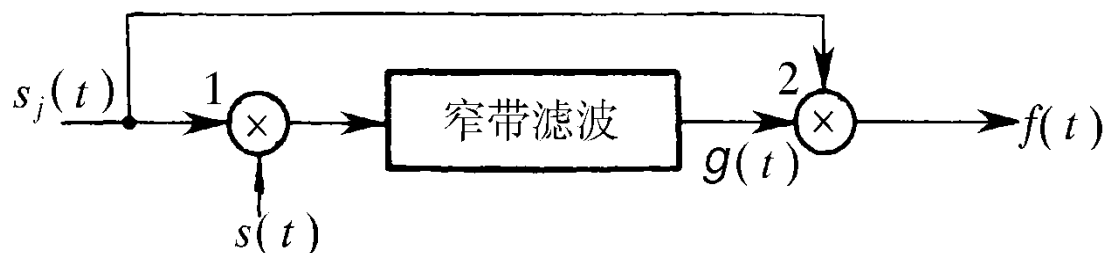
$$\sum_{j=0}^{n-1} A_j M(t - j\Delta) \cos[\omega_i(t - j\Delta) + \varphi_j]$$

其中共有 $n$ 条路径的信号。第 $j$ 条路径信号的振幅为 $A_j$ ，延迟时间为 $j\Delta$ ，载波附加的随机相位为 $\varphi_j$ ，中频角频率为 $\omega_i$ 。在此式中，忽略了各条路径共同的延迟，并且认为相邻路径的延迟时间差相等，均等于 $\Delta$ 秒。在设计中我们选用此 $\Delta$ 值作为 $m$ 序列的一个码元宽度。

为了消除各条射线随机相位 $\varphi_j$ 的影响，可以采用自适应校相滤波器。

# 第12章 正交编码与伪随机序列

## □ 自适应校相滤波器



设 $s_j(t)$ 是的第 $j$ 条射线

$$s_j(t) = A_j M(t - j\Delta) \cdot \cos[\omega_i(t - j\Delta) + \varphi_j]$$

它加于上图中电路的输入端。此电路由两个相乘器和一个窄带滤波器组成。在第1个相乘器中， $s_j(t)$ 与本地振荡电压 $s(t) = \cos(\omega_0 t + \varphi)$ 相乘。相乘结果通过窄带滤波器，后者的中心角频率为 $(\omega_i - \omega_0)$ ，其通带极窄，只能通过 $(\omega_i - \omega_0)$ 分量而不能通过各边带分量。故滤波输出 $g(t)$ 在忽略一常数因子后可以表示为

$$g(t) = A_j \cos[(\omega_i - \omega_0)t - j\Delta\omega_i t + \varphi_j - \varphi]$$



## 第12章 正交编码与伪随机序列

在第2个相乘器中,  $s_j(t)$ 与 $g(t)$ 相乘, 取出乘积中差频项 $f(t)$ , 仍忽略常数因子, 可将 $f(t)$ 表示为

$$f(t) = A_j^2 M(t - j\Delta) \cos(\omega_0 t + \varphi)$$

在上图中省略了上述分离出差频项 $f(t)$ 的带通滤波器。

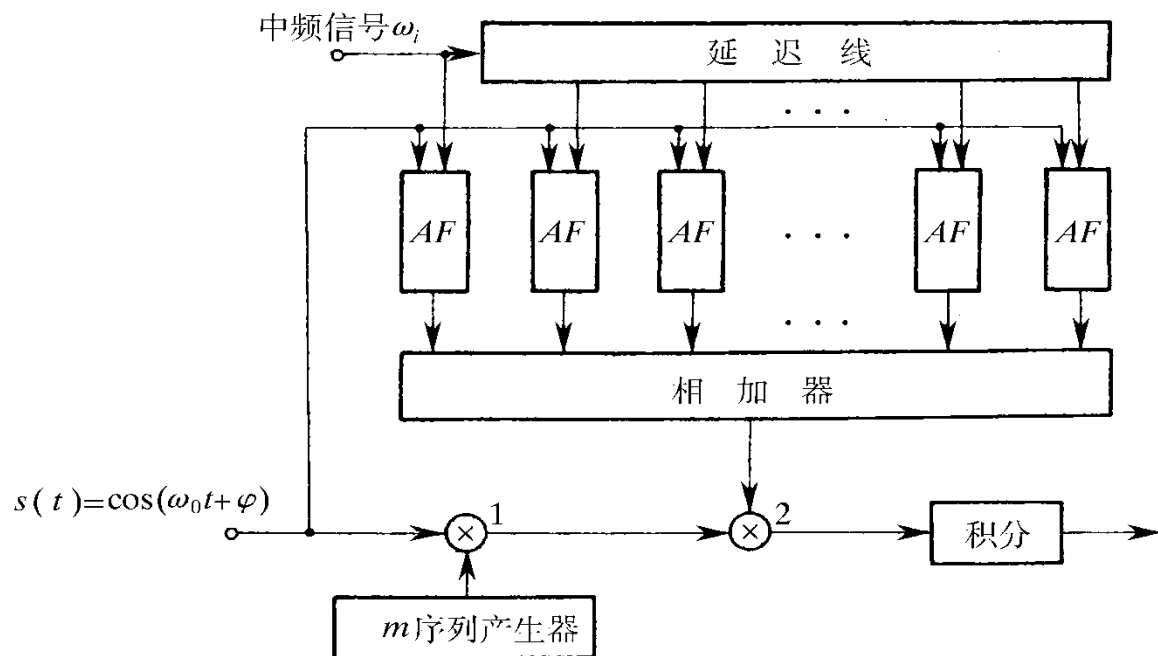
由上式可见, 经过自适应校相滤波器后, 接收信号中的随机相位可以消除。上面只分析了一条路径接收信号的情况。当多径信号输入此滤波器时, 每条路径信号都同样受到相位校正, 故使各路径信号具有相同的相位。这时的输出 $f(t)$ 变为

$$f(t) = \sum_{j=0}^{n-1} A_j^2 M(t - j\Delta) \cos(\omega_0 t + \varphi)$$

此式中各路径信号的载波得到了校正, 但是包络 $M(t - j\Delta)$ 仍然有差别。为了校正各路径包络的相对延迟, 可以采用下图所示的办法。



# 第12章 正交编码与伪随机序列



此图中AF为自适应校相滤波器，抽头延迟线的抽头间隔时间为 $\Delta$ 。设现在共有4条路径的信号， $n=4$ ，抽头延迟线共有3段，每段延迟时间为 $\Delta$ ，则相加器的输入信号包络为

$$\left. \begin{aligned}
 &\text{未经延迟的:} && A_0^2 M(t) + A_1^2 M(t-\Delta) + A_2^2 M(t-2\Delta) + A_3^2 M(t-3\Delta) \\
 &\text{经延迟}\Delta\text{的:} && A_0^2 M(t-\Delta) + A_1^2 M(t-2\Delta) + A_2^2 M(t-3\Delta) + A_3^2 M(t-4\Delta) \\
 &\text{经延迟}2\Delta\text{的:} && A_0^2 M(t-2\Delta) + A_1^2 M(t-3\Delta) + A_2^2 M(t-4\Delta) + A_3^2 M(t-5\Delta) \\
 &\text{经延迟}3\Delta\text{的:} && A_0^2 M(t-3\Delta) + A_1^2 M(t-4\Delta) + A_2^2 M(t-5\Delta) + A_3^2 M(t-6\Delta)
 \end{aligned} \right\}$$



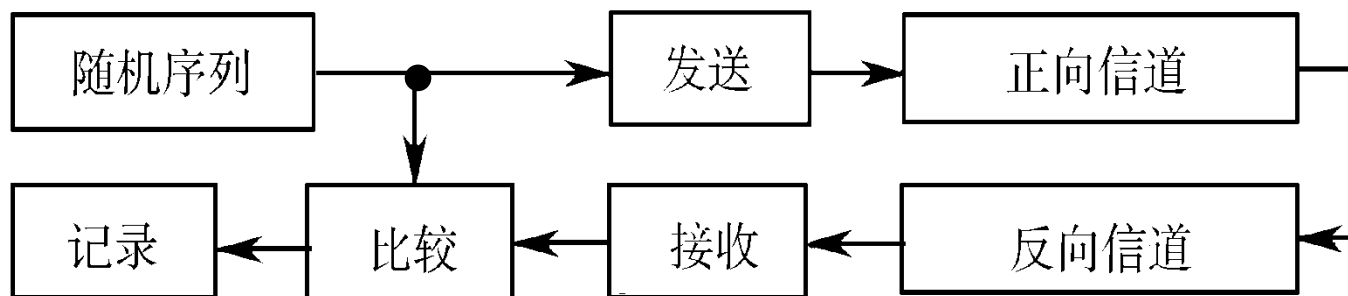
## 第12章 正交编码与伪随机序列

相加器输出信号的载波仍为 $\cos(\omega_0 t + \varphi)$ ，包络则为上式中各项之和。若上图中本地 $m$ 序列产生器的输出为 $M(t - 3\Delta)$ ，则在相乘器2中与接收的多径信号相乘并经积分后，就能分离出包络为 $(A_0^2 + A_1^2 + A_2^2 + A_3^2)M(t - 3\Delta)$ 的分量，即上式中右上至左下对角线上各项。或者说，相当于将4条路径的信号包络的相对延迟校正后相加了起来，而抑止掉了其余各项。在数字通信系统中，为了传输不同的符号，可以采用不同的 $m$ 序列。在接收端自然也需要有几个相应的 $m$ 序列分别与之作相关检测。

## 第12章 正交编码与伪随机序列

### ■ 误码率测量

- ◆ 在实际测量数字通信系统的误码率时，测量结果与信源送出信号的统计特性有关。通常认为二进制信号中“0”和“1”是以等概率随机出现的。所以测量误码率时最理想的信源应是随机序列产生器。这样测量的结果，是符合实际运用时的情况。
- ◆ 用真正的随机序列产生器进行测量时，只适于闭环线路的测试，如下图所示：

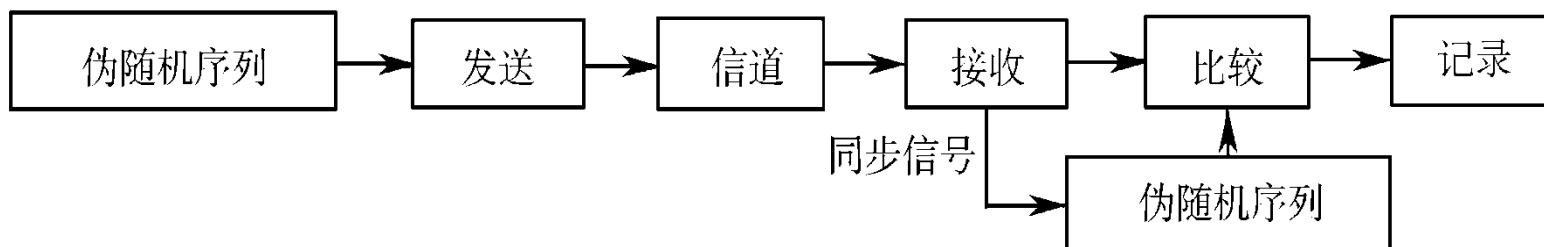


闭环测试法所用的信道不符合实际情况。

# 第12章 正交编码与伪随机序列

## ◆ 单程测试法

- 在测量单程数字通信的误码率时，不能利用随机序列，只能用伪随机序列代替它。如下图所示：



- 由于发送端用的是伪随机序列，而且通常是 $m$ 序列，接收端可以用同样的 $m$ 序列产生器，由同步信号控制，产生出相同的本地序列。本地序列和接收序列相比较，就可以检测误码。
- ITU建议用于数据传输设备测量误码的 $m$ 序列周期是511，其特征多项式建议采用 $x^9 + x^5 + 1$ ；以及建议用于数字传输系统(1544/2048和6312/8448 kb/s)测量的 $m$ 序列周期是 $2^{15} - 1 = 32767$ ，其特征多项式建议采用 $x^{15} + x^{14} + 1$ 。

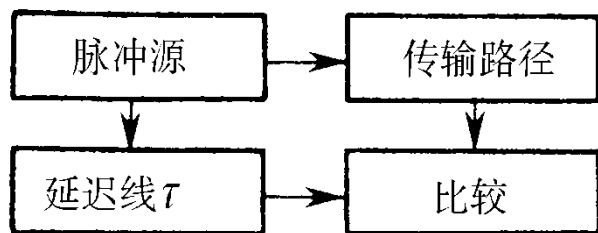
# 第12章 正交编码与伪随机序列

## 时延测量

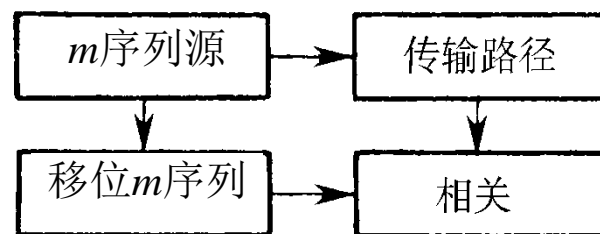
### ◆ 目的:

- 测量信号传输的时间延迟。
- 测量信号传播距离，即利用无线电信号测距。

### ◆ 原理



(a)



(b)

- 图(a): 测量的最大延迟 (距离) 受脉冲重复频率限制, 测量的精确度也受脉冲宽度 (或上升时间) 及标准延迟线的精确度限制。
- 图(b): 用 $m$ 序列代替周期性窄脉冲, 用相关器代替比较器, 可以改善测量延迟的性能。测量精确度决定于所用 $m$ 序列的一个码片的宽度。



# 第12章 正交编码与伪随机序列

## ■ 噪声产生器

### ◆ 用途：

- 测量通信系统在不同信噪比条件下的性能。

### ◆ 要求：

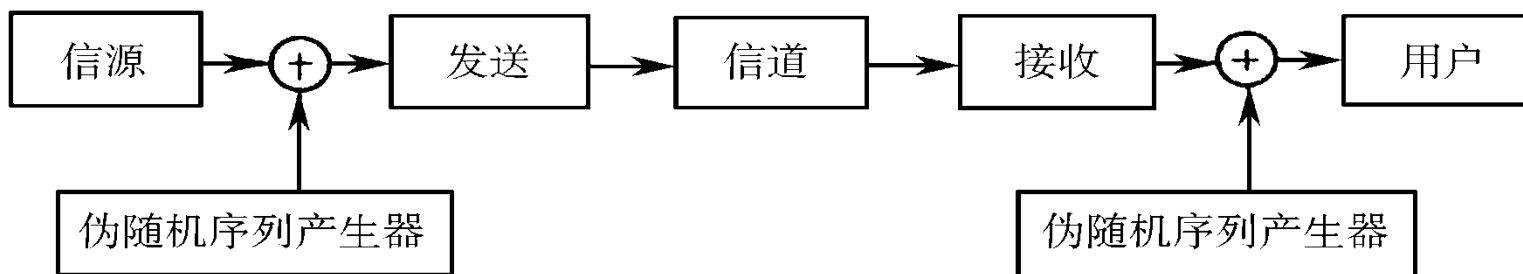
- 能产生带限白高斯噪声。

- ◆ 噪声二极管做成的噪声产生器，在测量数字通信系统的性能时不很适用。因为它在一段观察时间内产生的噪声的统计特性，不一定和同样长的另一段观察时间内的统计特性相同。测量得到的误码率常常很难重复得到。
- ◆  $m$ 序列的功率谱密度的包络是 $(\sin x / x)^2$ 形的。设 $m$ 序列的码元宽度为 $T_1$ 秒，则大约在0至 $(1 / T_1) \times 45\%$  Hz的频率范围内，可以认为它具有均匀的功率谱密度。所以，可以用 $m$ 序列的这一部分频谱作为噪声产生器的噪声输出。虽然是伪噪声，但有可重复性。

# 第12章 正交编码与伪随机序列

## ■ 通信加密

- ◆ 数字通信的优点：容易作到高度保密性的加密。
- ◆ 数字信号加密的基本原理：

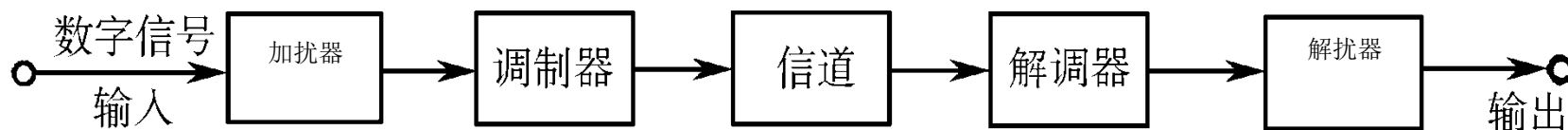


在保密通信应用中， $M$ 序列比 $m$ 序列优越得多，因为前者的数目比后者的大很多。数目越多，为解密所需要的搜索时间就越长。例如，在 $n = 10$ 时， $m$ 序列只有60个，而 $M$ 序列的数目约达 $1.3 \times 10^{151}$ 个。假定解密者用计算机搜索时，试探一种 $M$ 序列平均需要1 ns，则平均约需 $(1.3 \times 10^{151}) / 2(365 \times 24 \times 60 \times 60 \times 10^9) = 2 \times 10^{134}$ 年才能破译这个密码！

# 第12章 正交编码与伪随机序列

## ■ 数据序列的扰乱与解扰

- ◆ 目的：使所传输的数字信号具有接近随机的统计特性
- ◆ 加扰技术：不用增加多余度而扰乱信号，改变数字信号统计特性，使其近似于白噪声统计特性的一种技术。
- ◆ 采用加扰技术的通信系统

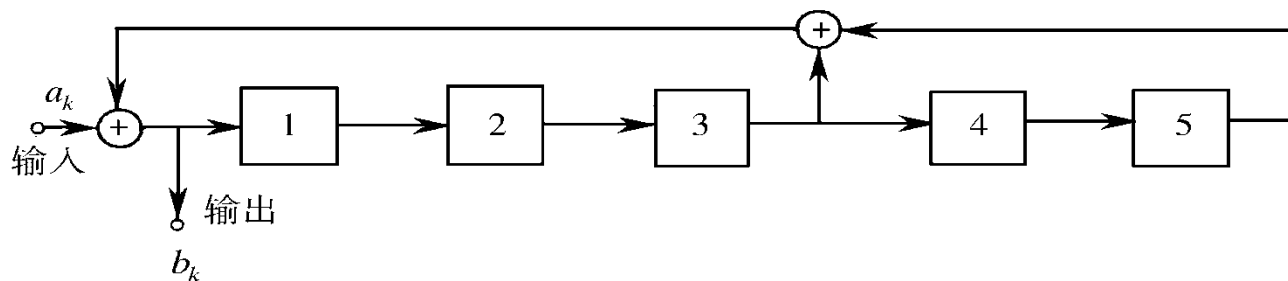




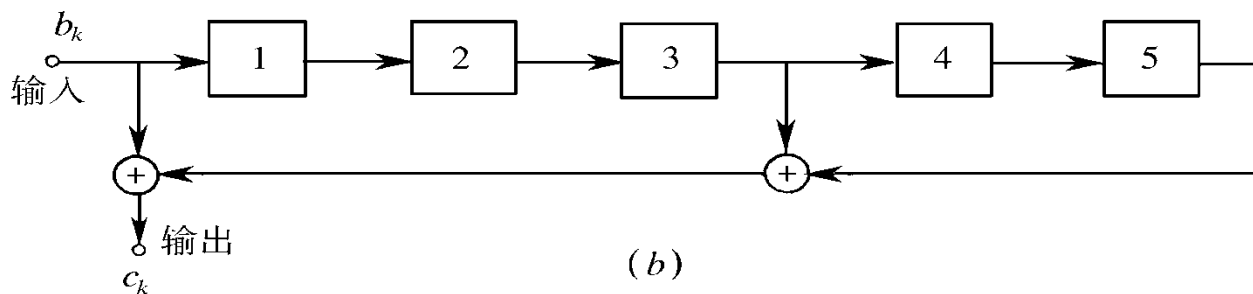
# 第12章 正交编码与伪随机序列

## ◆ 自同步加扰器和解扰器的原理

- 原理方框图：在下图中给出一种由5级移存器组成的自同步加扰器和解扰器。



(a)



(b)

(a) 加扰器

(b) 解扰器

## 第12章 正交编码与伪随机序列

### □ 工作原理

设加扰器的输入数字序列为 $\{a_k\}$ ，输出序列为 $\{b_k\}$ ；解扰器的输入序列为 $\{b_k\}$ ，输出序列为 $\{c_k\}$ 。在这里，符号 $\{a_k\}$ 表示二进制数字序列 $a_0a_1a_2 \dots a_k a_{k+1} \dots$ 。符号 $\{b_k\}$ 和 $\{c_k\}$ 均与此相仿。这样，由上图不难看出，加扰器的输出为

$$b_k = a_k \oplus b_{k-3} \oplus b_{k-5}$$

而解扰器的输出为

$$c_k = b_k \oplus b_{k-3} \oplus b_{k-5} = a_k$$

以上两式表明，解扰后的序列与加扰前的序列相同。



# 第12章 正交编码与伪随机序列

## □ 性能:

- 这种解扰器是自同步的，因为若信道干扰造成错码，它的影响至多持续移存器内的一段时间（连续5个输出码元）。
- 如果我们断开输入端，加扰器就变成一个反馈移存器序列产生器，其输出为一周期性序列。一般都适当设计反馈抽头的位置，使其构成为 $m$ 序列产生器。因为它能最有效地将输入序列扰乱，使输出数字码元之间相关性最小。
- 加扰器的作用可以看作是使输出码元成为输入序列许多码元的模2和。因此可以把它当作是一种线性序列滤波器；同理，解扰器也可看作是一个线性序列滤波器。
- 加扰技术在某种程度上也可以达到通信加密的目的。



# 第12章 正交编码与伪随机序列

## • 12.6 小结

正交编码与伪随机序列在数字通信技术中都有十分重要的作用，它们广泛应用于码分多址通信、误码率测量、扩展频谱通信、密码、纠错编码和分离多径等领域中。

正交编码是由一组离散的正交函数构成的。正交编码中各个码组的相关系数均等于0。阿达玛矩阵和沃尔什矩阵在正交编码中有着重要地位。

伪随机噪声可以具有类似于随机噪声的某些统计特性，同时又便于重复产生和处理。由于它具有随机噪声的优点，又避免了随机噪声的缺点，因此获得了日益广泛的实际应用。伪随机噪声都是由周期性伪随机序列经过滤波等处理后得出的。伪随机序列有时又称为伪随机信号或伪随机码。

m序列是线性反馈最长移存器序列。由于m序列的均衡性、游程分布和自相关特性与随机序列的这些性质极相似，所以通常将m序列称为伪噪声(PN)序列或伪随机序列。m序列是最主要的一种伪随机序列。递推方程、特征方程和母函数是设计和分析m序列产生器的三个基本关系式。一个线性反馈移存器能产生m序列的充要条件为：反馈移存器的特征方程为本原多项式。



## 第12章 正交编码与伪随机序列

在伪随机序列中M序列也有着重要的地位，它是一种非线性反馈移存器序列。

扩展频谱调制是一类宽带调制技术，其中包括DSSS、FHSS和线性调频。但是前两种是最常用的体制。扩频调制有许多优点，最主要的是抗干扰能力强和信号频蔽。目前，其应用日益广泛。

多径分离技术是专门适用于扩频信号的抗多径干扰。它可以将接收信号中有害的从多径来的信号分量变成有用的多径信号分量，从而增强接收信噪比。