《通信原理》

（16b 伪随机序列）

蔡志岗

光学与光学工程系

中山大学物理学院

lasers@netease.com

13316105077

光信息实验室：84110909

第11章 正交编码、扩频通信与伪随机码

- 正交编码
- 伪随机序列
- 扩频通信

第11章 正交编码、扩频与伪随机序列

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11章 正交编码、扩频与伪随机序列

引言

- **扩展频谱通信**与光纤通信、卫星通信一同被誉为进入信息时代的三大高技术通信传输方式。。
- 扩频通信：一种信息传输方式，其信号所占有的频带宽度远大于所传信息必需的最小带宽；频带的扩展是通过一个独立的码序列（一般是伪随机码）来完成，用编码及调制的方法来实现的，与所传信息数据无关；在接收端则用同样的码进行相关同步接收、解扩及恢复所传信息数据。

第11章 正交编码与伪随机序列

- 11.3 伪随机序列
  - 11.3.1 基本概念
    - 什么是伪随机噪声？

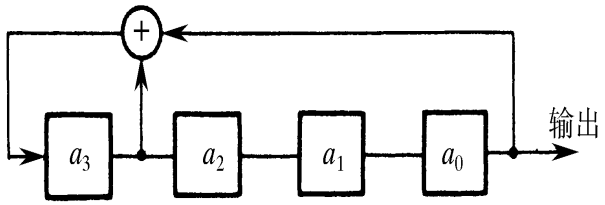
      具有类似于随机噪声的某些统计特性，同时又能够重复产生的波形。

      - 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。
  - 11.3.2 ***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。

m序列的产生

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”，即(0, 0, 0, 0)，则移位后得 到的仍为全“0”状态。

应该避免出现全“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11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。

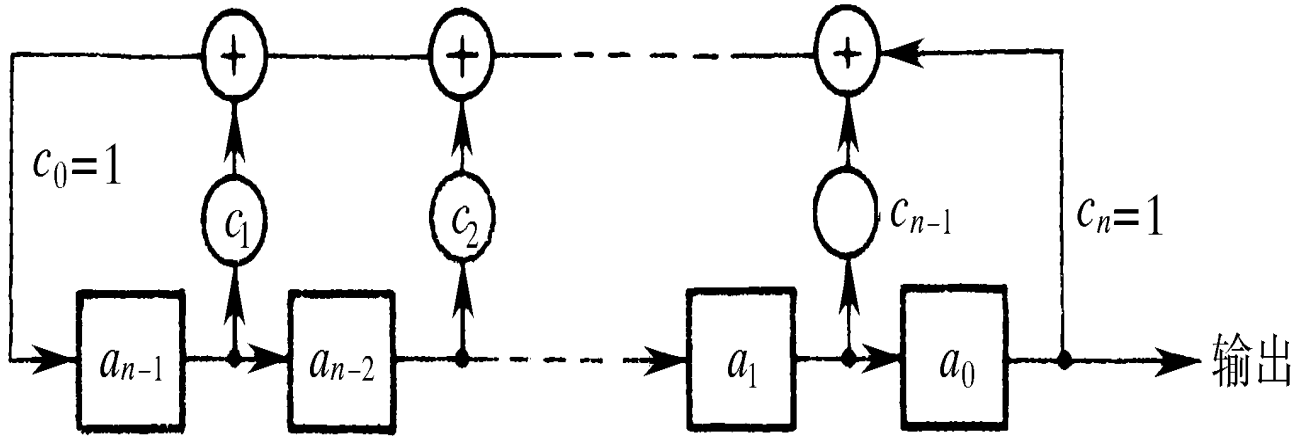
我们常常希望用尽可能少的级数产生尽可能长的序列。

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11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 = 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11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：$a_{-1}\ a_{-2}\cdots a_{-n}$，经过1次移位后，状态变为$a_0\ a_{-1}\cdots a_{-n+1}$。经过$n$次移位后，状态为$a_{n-1}\ a_{n-2}\cdots a_0$，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

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

因此，一般说来，对于任意一个输入a_k，有

$$a_k = \sum_{i=1}^{n} c_i a_{k-i}$$ – 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11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：

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = \sum_{i=0}^{n} c_i x^i \qquad \text{– 特征方程}$$

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前面例子（图）所示的。

第11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

$$G(x) = a_0 + a_1 x + a_2 x^2 + \cdots = \sum_{k=0}^{\infty} a_k x^k$$

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11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

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

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

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

移项整理后，得到 $\left(1+\sum_{i=1}^{n}c_i x^i\right)G(x)=\sum_{i=1}^{n}c_i x^i\left(a_{-i}x^{-i}+a_{-(i-1)}x^{-(i-1)}+\cdots+a_{-1}x^{-1}\right)$

第11章 正交编码与伪随机序列

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

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

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

式中

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

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

再将特征方程代入上式，最后得出

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

第11章 正交编码与伪随机序列

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

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≤$(n-1)$，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11章 正交编码与伪随机序列

【定理11.2】一个n级线性反馈移存器之相继状态具有周期性，周期为$p \le 2^n - 1$。

【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$p \le 2^n$。

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$p \le (2^n - 1)$。【证毕】

第11章 正交编码与伪随机序列

【定理11.3】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11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 $p_1 \le 2^{n_1} - 1$

$G_2(x)$的周期为 $p_2 \le 2^{n_2} - 1$

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

$$p = LCM[p_1, p_2] \le p_1 \cdot p_2 \le (2^{n_1} - 1) \cdot (2^{n_2} - 1)$$
$$= 2^n - 2^{n_1} - 2^{n_2} + 1 \le 2^n - 3 < 2^n - 1$$

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11章 正交编码与伪随机序列

【定理11.4】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

$$\frac{h(x)}{f(x)}=G(x)=\sum_{k=0}^{\infty}a_k x^k$$

$$=a_0+a_1x+a_2x^2+\cdots+a_{p-1}x^{p-1}+a_0x^p+a_1x^{p+1}+\cdots+a_{P-1}x^{2p-1}+\cdots$$

$$=(a_0+a_1x+a_2x^2+\cdots+a_{p-1}x^{p-1})+x^p(a_0+a_1x+\cdots+a_{P-1}x^{p-1})+$$

$$x^{2p}(a_0+a_1x+\cdots+a_{p-1}x^{p-1})+\cdots$$

$$=\left(1+x^p+x^{2p}+\cdots\right)(a_0+a_1x+\cdots+a_{p-1}x^{p-1})$$

$$=\left(\frac{1}{1+x^p}\right)(a_0+a_1x+\cdots+a_{p-1}x^{p-1})$$

上式移项整理后，变成 $\dfrac{h(x)\cdot(x^p+1)}{f(x)}=(a_0+a_1x+\cdots+a_{p-1}x^{p-1})$

第11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11.1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

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

可知，此时有$h(x)=1$。故有

第11章 正交编码与伪随机序列

$$G(x)=\frac{h(x)}{f(x)}=\frac{1}{f(x)}=\frac{b_0+b_1x+\cdots+b_{p-1}x^{p-1}}{x^p+1}$$
$$=\left(1+x^p+x^{2p}+\cdots\right)\left(b_0+b_1x+\cdots+b_{p-1}x^{p-1}\right)$$
$$=\left(b_0+b_1x+\cdots+b_{p-1}x^{p-1}\right)+x^p\left(b_0+b_1x+\cdots+b_{p-1}x^{p-1}\right)+\cdots$$

上式表明，序列A以ρ或ρ的某个因子为周期。

若A以ρ的某个因子ρ_1为周期，$\rho_1<\rho$，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$(x^{\rho_1}+1)$必能被$f(x)$整除。

所以，序列A之周期等于使$f(x)$能整除的$(x^{\rho}+1)$中最小正整数ρ。

【证毕】

第11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11.4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11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 $f(x)$:

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

  $f(x)$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

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

第11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：($x^4 + x + 1$)和($x^4 + x^3 + 1$)。由其中任何一个都可以产生*m*序列，用作为特征多项式构成的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11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11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11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
$c_5c_4c_3$	$c_2c_1c_0$

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

第11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*级移存器的一个状态，而且此移存器共有*m*个不同状态，所以可以把此移存器的这些相继状态列表，如下表所示。表中每一行为移存器的一个状态。*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11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11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$a_i \in (0, 1)$，$i = 0, 1, \cdots, (m - 1)$。所以表中每一位移存器状态可以看成是一个$m$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11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：

$$\overbrace{\cdots 1\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,0\,0}^{m\ =\ 15}\,1\,0\cdots$$

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；. . .。

严格讲，长度为k的游程数目占游程总数的2^{-k}，其中$1 \le k \le (n-1)$。而且在长度为k的游程中[其中$1 \le k \le (n-2)$]，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：

$$0\,1\underbrace{1\,1\cdots1}_{k\text{个}}0\underbrace{\times\times\cdots}_{(n-2-k)\text{个}} \quad (1\le k\le n-2)$$

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“×”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11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$1 \le k \le (n-2)$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11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：

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

所以，长度为k的游程占游程总数的比例为

$$\frac{2^{n-k-1}}{2^{n-1}} = 2^{-k}, \qquad 1 \le k \le (n-2)$$

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

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

【证毕】

第11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

$$M_p \oplus M_r = M_s$$

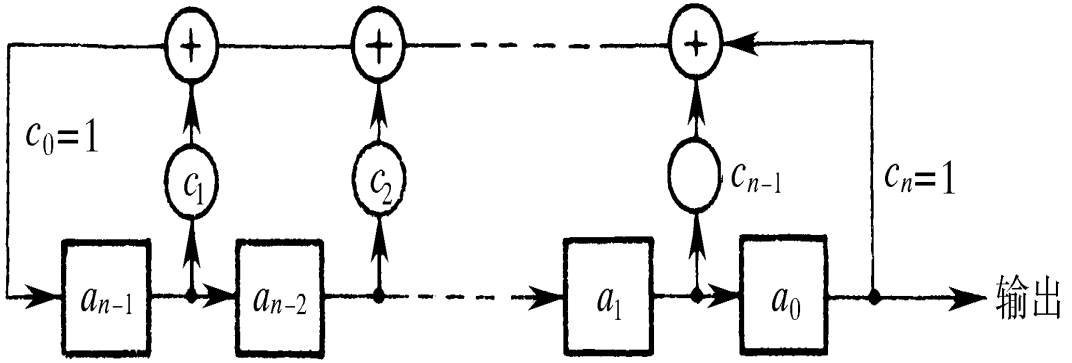
现在分析一个$m = 7$的m序列M_p作为例子。设M_p的一个周期为1110010。另一个序列M_r是M_p向右移位一次的结果，即M_r的一个相应周期为0121001。这两个序列的模2和为

$$1110010 \oplus 0111001 = 1001011$$

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11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。



这一初始状态也就是上表中第一行的$a_0a_1a_2\cdots a_{n-1}$。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

$$a_n = c_1a_{n-1} + c_2a_{n-2} + \cdots + c_na_0$$

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$a_r\ a_{r+1}\ a_{r+2}\cdots a_{n+r-1}$代入递推方程式，得到下一个输入：

$$a_{n+r} = c_1a_{n+r-1} + c_2a_{n+r-2} + \cdots + c_na_r$$

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

$$a_n + a_{n+r} = c_1a_{i+n-1} + c_2a_{i+n-2} + \cdots + c_na_i$$

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$c_1c_2\cdots c_n$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11章 正交编码与伪随机序列

- 自相关函数

现在我们讨论*m*序列的自相关系数。由11.2节互相关系数定义式得知，*m*序列的**自相关系数**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：

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

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

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

当$j = 0$时，显然$\rho(0) = 1$。所以，我们最后写成：

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

不难看出，由于m序列有周期性，故其自相关系数也有周期性，周期也是m，

即 $$\rho(j) = \rho(j - km), \qquad \text{当} \quad j \geq km, \qquad k = 1,\ 2, \cdots$$

而且$\rho(j)$是偶函数，即有 $$\rho(j) = \rho(-j), \qquad j = \text{整数}$$

第11章 正交编码与伪随机序列

上面数字序列的自相关系数$\rho(j)$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：

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

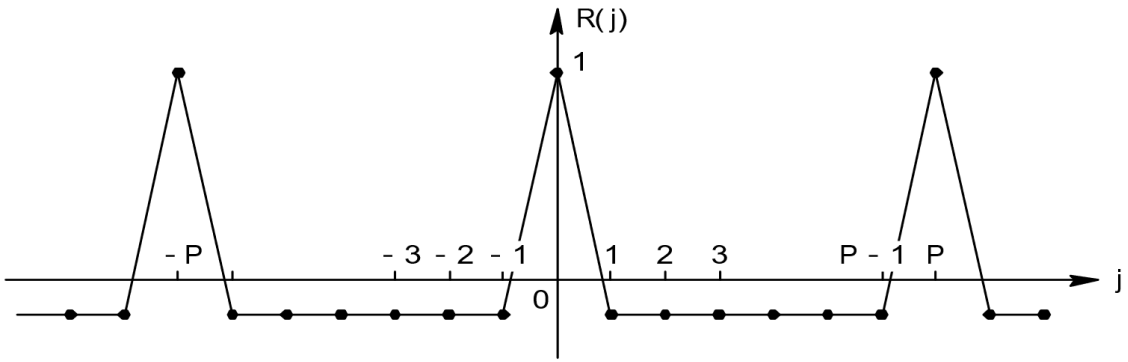
式中 T_0 – $s(t)$的周期，

可以求出其自相关函数$R(\tau)$的表示式为

$$R(\tau)=\begin{cases}1-\dfrac{m+1}{T_0}\left|\tau-iT_0\right|, & 0\le\left|\tau-iT_0\right|\le\dfrac{T_0}{m}, \quad i=0,1,2,\cdots\\ -1/m, & \text{其他处}\end{cases}$$

第11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序列的自相关系数只有两种取值：1和$(-1/m)$。有时把这类序列称为**双值自相关**序列。

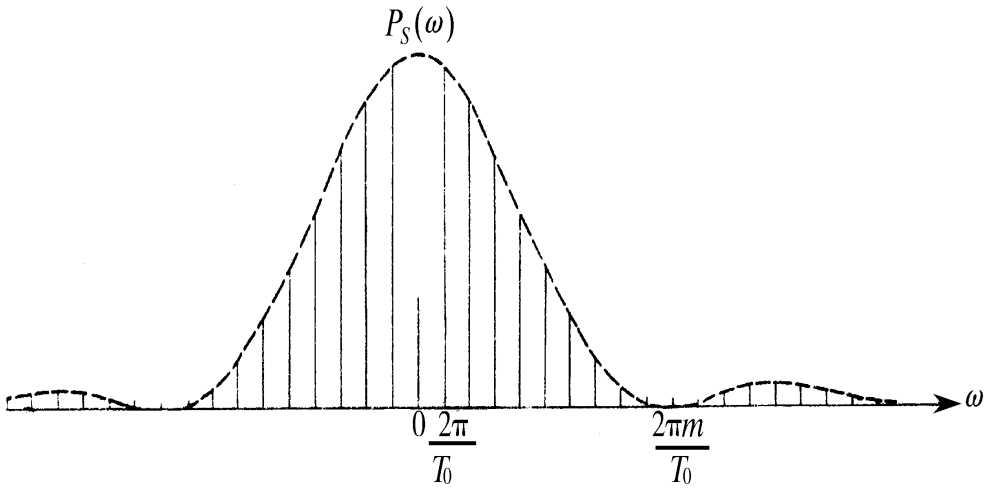
第11章 正交编码与伪随机序列

- 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$T_0\to\infty$和$m/T_0\to\infty$时，$P_S(\omega)$的特性趋于白噪声的功率谱密度特性。



第11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11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。

在课程中，伪随机序列用于：

- **FSK实验**：信息码
  - 产生；误码率测量；位同步提取
- **DPSK实验**：信息码
  - 产生；误码率测量；载波提取
- **扩频通信设计实验**：
  - 信息码（低速），扩频序列（高速）
  - 产生；直接扩频；解扩频
  - VHDL编程，CPLD芯片

小复习

- m序列的产生
  - 线性反馈移位寄存器
  - 递推方程
  - 特征方程(特征多项式)
  - 母函数
- 本源多项式（表）
  - 二进制；八进制

- m序列的性质
  - 均衡性
  - 游程分布
  - 移位相加特性
  - 自相关函数
  - 功率谱密度
  - 伪随机特征

还有，几个定理要了解

伪随机序列的应用

- 误码率测量
- 扩频通信
- 分离多径技术
- 延时测量
- 噪声产生器
- 加密通信

第11章 正交编码与伪随机序列

- 其它伪随机序列:
  - M序列
  - 二次剩余序列
  - 双素数序列

第11章 正交编码与伪随机序列

- 11.3.3 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。

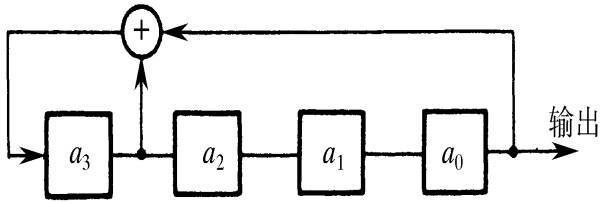
      由上节对*m*序列产生器的分析可知，一个*n*级*m*序列产生器只可能有$(2^n - 1)$种不同的状态。但是*n*级移存器最多可有2^n种状态，在*m*序列中不能出现的是全“0”状态。在线性反馈条件下，全“0”状态出现后，产生器的状态将不会再改变；但是在非线性反馈条件下，却不一定如此。因此，非线性反馈移存器的最长周期可达2^n，我们称这种周期长达2^n的序列为***M*序列**。

第11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	$2^4-1=15$(个)
	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	

第11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

$$a_k = a_{k-1} \oplus a_{k-4} \oplus \bar{a}_{k-1}\bar{a}_{k-2}\bar{a}_{k-3}a_{k-4} \oplus \bar{a}_{k-1}\bar{a}_{k-2}\bar{a}_{k-3}\bar{a}_{k-4}$$

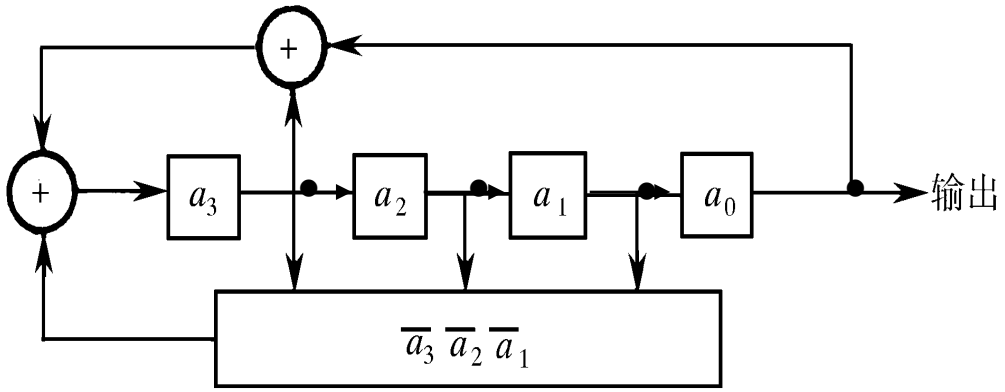
$$= a_{k-1} \oplus a_{k-4} \oplus \bar{a}_{k-1}\bar{a}_{k-2}\bar{a}_{k-3} = \sum_{i=1}^{4} c_i a_{k-i} \oplus \bar{a}_{k-1}\bar{a}_{k-2}\bar{a}_{k-3}$$

第11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11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$1/2^k$，$1 \le k \le n-2$；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11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	6.71088×10^{7}	1.44115×10^{17}	1.32922×10^{36}	2.26156×10^{74}	1.30935×10^{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11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，$i = 0, 1, 2, \ldots$，其周期为p。

第11章 正交编码与伪随机序列

- 例：设$p = 19$，容易算出

$12 \equiv 1 \pmod{19}$，　　$22 \equiv 4 \pmod{19}$，

$32 \equiv 9 \pmod{19}$，　　$42 \equiv 16 \pmod{19}$，

$52 \equiv 6 \pmod{19}$，　　$62 \equiv 17 \pmod{19}$，

$72 \equiv 11 \pmod{19}$，　　$82 \equiv 7 \pmod{19}$，

$92 \equiv 5 \pmod{19}$，　　$102 \equiv 5 \pmod{19}$，

$112 \equiv 7 \pmod{19}$，　　$122 \equiv 11 \pmod{19}$，

$132 \equiv 17 \pmod{19}$，　　$142 \equiv 6 \pmod{19}$，

$152 \equiv 16 \pmod{19}$，　　$162 \equiv 9 \pmod{19}$，

$172 \equiv 4 \pmod{19}$，　　$182 \equiv 1 \pmod{19}$。

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11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：

$$- \; + \; \underline{\quad} \; + \; + \; + \; - \; + \; - \; + \; \underline{\quad\quad\quad\quad} \; + \; + \; -$$

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11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

$(i,\ p) = 1$表示i和p互为素数（最大公因子为1）。

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

第11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11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 ＋ ≡ ＋1；

－ ≡ －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。

小复习

- m序列的产生
  - 线性反馈移位寄存器
  - 递推方程
  - 特征方程(特征多项式)
  - 母函数
- 本源多项式（表）
  - 二进制；八进制

- m序列的性质
  - 均衡性
  - 游程分布
  - 移位相加特性
  - 自相关函数
  - 功率谱密度
  - 伪随机特征

还有，几个定理要了解

伪随机序列的应用

- 误码率测量
- 扩频通信
- 分离多径技术
- 延时测量
- 噪声产生器
- 加密通信