

## 摘要

本毕业设计主要介绍了两种常用的反馈移位寄存器序列 (m 序列和 Gold 序列) 的特性, 并对其进行仿真研究。

伪随机序列良好的随机性和接近于白噪声的相关函数, 使其易于从信号或干扰中分离出来。伪随机序列的可确定性和可重复性, 使其易于实现相关接收或匹配接收, 因此有良好的抗干扰性能。伪随机序列的这些特性使得它在伪码测距、导航、遥控遥测、扩频通信、多址通信、分离多径、数据加扰、信号同步、误码测试、线性系统、各种噪声源等方面得到了广泛的应用, 特别是作为扩频码在 CDMA 系统中的应用已成为其中的关键问题。

在本论文中首先简要阐述了伪随机序列的研究现状及其相关意义, 接着介绍了伪随机序列的发展历史, 研究方法和研究工具。然后分别对 m 序列和 Gold 序列这两种常用的伪随机序列的生成过程、随机特性以及相关特性进行了详细的研究, 并分析它们的优点以及存在的问题。最后在理论证明的基础上应用 MATLAB 仿真验证它们的随机特性, 并用仿真做出 m 序列和 Gold 序列相关特性图形并加以比较。

关键词: 伪随机序列; m 序列; Gold 序列; 相关;

## **ABSTRACT**

Matlab software has been used extensively in many engineering fields due to its strong operation function. To expanding or compressing the signal spectrum in spread spectrum system, the signal is generally multiplied by a spread Spectrum sequence.

The character of spread spectrum sequence significantly affects the communication quality. In all PN sequences, m-sequence and Gold-sequence are often used as spread spectrum sequence. In this paper, the brief introduction of the theory, property and constructing means of the two sequences are given first, and the generation and analysis of them by programming with M language in MATLAB are given later. The simulation results show the correctness and feasibility of this method. The simple and intuitive method is convenient for the engineering personnel.

**KEYWORDS:**PN sequence; Sequence; Spread spectrum sequence

# 目录

摘要 .....	1
ABSTRACT .....	2
第一章 前言 .....	4
1.1 研究课题的提出 .....	4
1.2 伪随机序列的应用及其意义 .....	4
1.3 伪随机序列研究现状 .....	4
1.4 研究内容 .....	5
第二章 伪随机序列与仿真工具的简介 .....	6
2.1 伪随机序列理论的发展历史 .....	6
2.2 伪随机序列的构造方法 .....	6
<b>2.3 MATLAB简介</b> .....	7
第三章 m序列 .....	9
3.1 m序列的定义 .....	9
3.2 m序列的产生 .....	9
3.3 m序列的性质 .....	12
3.4 m序列的计数 .....	15
第四章 Gold序列 .....	17
4.1 Gold序列的定义 .....	17
4.2 m序列优选对 .....	17
4.3 Gold序列的产生结构 .....	19
4.4 Gold码的性质 .....	20
4.5 平衡 Gold码 .....	23
第五章 序列的仿真及其仿真比较 .....	24
5.1 m序列的仿真 .....	24
5.2 Gold序列的仿真 .....	25
<b>5.3 MATLAB环境中伪随机序列相关函数的实现及特性</b> .....	27
5.4 两种相关函数间的相关特性比较 .....	27
参考文献: .....	29
致谢 .....	错误!未定义书签。
附录 MATLAB 程序 .....	错误!未定义书签。

# 第一章前言

## 1.1 研究课题的提出

伪随机序列具有良好的随机性和接近于白噪声的相关函数，并且有预先的可确定性和可重复性。这些特性使得伪随机序列得到了广泛的应用。

## 1.2 伪随机序列的应用及其意义

[1]在通信加密中的应用  $m$ 序列自相关性较好，容易产生和复制，而且具有伪随机性，利用 $m$ 序列加密数字信号使加密后的信号在携带原始信息的同时具有伪噪声的特点，以达到在信号传输的过程中隐藏信息的目的；在信号接收端，再次利用 $m$ 序列加以解密，恢复出原始信号。

[2]在雷达信号设计中的应用 近年兴起的扩展频谱雷达所采用的信号是已调制的具有类似噪声性质的伪随机序列，它具有很高的距离分辨力和速度分辨力。这种雷达的接收机采用相关解调的方式工作，能够在低信噪比的条件下工作，同时具有很强的抗干扰能力。该型雷达实质上是一种连续波雷达，具有低截获概率性，是一种体制新、性能高、适应现代高技术战争需要的雷达。采用伪随机序列作为发射信号的雷达系统具有许多突出的优点。首先，它是一种连续波雷达，可以较好地利用发射机的功率。其次，它在一定的信噪比时，能够达到很好的测量精度，保证测量的单值性，比单脉冲雷达具有更高的距离分辨力和速度分辨力。最后，它具有较强的抗干扰能力，敌方要干扰这种宽带雷达信号，将比干扰普通的雷达信号困难得多。

[3]在通信系统中的应用 伪随机序列是一种貌似随机，实际上是有规律的周期性二进制序列，具有类似噪声序列的性质，在CDMA中，地址码都是从伪随机序列中选取的，在CDMA中使用一种最易实现的伪随机序列： $m$ 序列，利用 $m$ 序列不同相位来区分不同用户；为了数据安全，在CDMA的寻呼信道和正向业务信道中使用了数据掩码(即数据扰乱)技术，其方法是用长度为2的42次方减1的 $m$ 序列用于对业务信道进行扰码(注意不是扩频)，它在分组交织器输出的调制字符上进行，通过交织器输出字符与长码PN码片的二进制模2相加而完成。

## 1.3 伪随机序列研究现状

迄今为止，人们获得的伪随机序列仍主要是PC (相控)序列，移位寄存器序列( $m$ 和 $M$ 序列), Gold序列, GMW序列, 级联GMW序列, Kasami序列, Bent序列, No序列。

其中 $m$ 序列是最有名和最简单的，也是研究的最透彻的序列。 $m$ 序列还是研究其它序列的基础。它序列平衡，有最好的自相关特性，但互相关满足一定条件的族序列数很少(对于本原多项式的阶数小于等于13的 $m$ 序列，互为优选对的序列数不多于6)，且线性复杂度很小。 $M$ 序列族序列数极其巨大(当寄存器级数等于6时，有226个序列)。但其生成困难，且其互相关特性目前知之甚少，一般很少用。Gold序列互相关函数为3值，序列部分平衡，有良好的相关特性，族序列数相对较大，但它有致命的弱点，线性复杂度很低，仅是相同长度的 $m$ 序列的两倍，这制约了Gold序列的广泛应用，特别在抗干扰及密码学中的应用。GMW序列具有序列平衡，线性复杂度大，自相关性能好(同 $m$ 序列)等优点。它是非线性序列，且数量比 $m$ 序列多。作为单个序列GMW序列有优势，但一族GMW序列满足

一定互相关条件的序列数很少。一般不用于多址通信作地址码。级联GMW序列平衡性和相关性同于GMW序列，族数比GMW序列多，一般情况下，线性复杂度比GMW序列大。Kasami序列分小集Kasami序列和大集Kasami序列。小集Kasami序列族序列数大，且互相关值达welch下界，大集Kasami序列族序列数非常大，互相关较小集Kasami序列为劣。它们都有共同的弱点，序列是不平衡的，线性复杂度不大(但比m,Gold序列稍大)。Bent序列是80年代初构造出来的，具有序列平衡，相关值达welch下界，族序列数多，线性复杂度大等优点。它在整个80年代，90年代大放光芒，也是目前综合性能最好的伪随机序列。但Bent序列构造较难，未有满足一定要求的快速算法。No序列是80年代末构造出来的一种新型伪随机序列，它的突出优点是线性复杂度很大，且相关值可达welch下界，族序列数多，但有序列不平衡的弱点。

## 1.4 研究内容

首先研究生成序列的反馈移位寄存器、反馈逻辑函数。主要研究它们的生成、随机特性以及相关特性，并分析它们的优缺点以及存在的问题。最后在理论证明的基础上应用 MATLAB 仿真验证它们的随机特性，并用仿真作出 m 序列和 Gold 序列相关特性图形并加以比较。

## 第二章伪随机序列与仿真工具的简介

通过抛硬币的方法可以得到一个随机序列，它具有两个方面的特点：一是预先不可确定、不可重复实现。即在实验前无法预知序列是怎样的，而且在所有的序列中不可能有两个是完全一致的。另一方面所有序列都具有某些共同的随机特性，对二元序列Golomb总结了三条随机性假设：

R1 若序列的周期 $L$ 为偶数，则0的个数与1的个数相等；若 $L$ 为奇数，则0的个数比1的个数多1或少1。

R2 长为1的游程占 $1/2$ ，且0游程和1游程的个数相等或至多差一个。

R3 序列的异相自相关函数为一个常数，即序列为二值自相关序列。

能否产生真正的随机序列一直都处在激烈的争论中，但可以肯定的是随机序列的产生、复制和控制在实际中都是难以实现的。如果一个序列，一方面它的结构是可以预先确定的，并且可以重复的产生和复制；另一方面又具有某种随机特性(R1--R3)，便称这种序列为伪随机序列。简单的讲，伪随机序列就是具有某种随机特性的确定序列。

### 2.1 伪随机序列理论的发展历史

伪随机序列的理论与应用研究大体上可以分成三个阶段：(1)纯粹理论研究阶段(1948年以前)；(2) $m$ 序列研究的黄金阶段(1948-1969)；(3)非线性生成器的研究阶段(1969-)。

1948年以前，学者们研究伪随机序列的理论仅仅是因为其优美的数学结构。最早的研究可以追溯到1894年，作为一个组合问题来研究所谓的De Bruijn序列；上世纪30年代，环上的线性递归序列则成为人们的研究重点。

1948年Shannon信息论诞生后，这种情况得到了改变。伪随机序列已经被广泛的应用在通信以及密码学等技术领域。Shannon证明了“一次一密”是无条件安全的，无条件保密的密码体制要求进行保密通信的密钥量至少与明文量一样大。因此在此后的一段时间内，学者们一直致力于研究具有足够长周期的伪随机序列。如何产生这样的序列是20世纪50年代早期的研究热点。线性反馈移位寄存器(LFSR)序列是这个时期研究最多的，因为一个 $n$ 级LFSR可以产生周期为

$2^n - 1$ 的最大长度序列，而且具有满足Golomb随机性假设的随机特性，通常称之为 $m$ 序列。这段时期的研究奠定了LFSR序列的基本理论和一些经典结论。

但是，在1969年Massey发表了“移位寄存器综合与BCH译码”一文，引发了序列研究方向的根本性变革，从此伪随机序列的研究进入了构造非线性序列生成器的阶段。Berlekamp-Massey算法(简称B-M算法)指出：如果序列的线性复杂度为 $n$ ，则只需要 $2n$ 个连续比特就可以恢复出全部的序列。从这个结论可以看出 $m$ 序列是一种“极差”的序列，它的线性复杂度太小，因而不能够直接用来做流密码系统的密钥流序列。从这里还可以看到仅仅靠Golomb的三个随机性假设来评测序列是不够的，还需要其它的一些指标。此后直到今天，密码学界的学者们一直在努力寻找构造“好”的伪随机序列的方法。

### 2.2 伪随机序列的构造方法

就现有的文献，可以把构造伪随机序列的方法分成两大类：一类是基于数学的理论构造伪随机序列；另一类是基于LFSR构造伪随机序列。两种构造方法各有



优缺点，前者在理论上容易分析序列的随机性质，但往往不容易实现或者实现的代价比较高；而后者则恰恰相反，在工程上很容易实现，成本较低，但有的情况下不容易分析其随机性质。

基于数学理论构造伪随机序列又可以分为两类：基于数论的构造和基于有限域的构造。前者利用的数学工具主要是二次剩余理论和割圆理论，像Legendre序列、Jacobi序列、m序列、差集序列和割圆序列等就属于此类构造；后者利用的数学工具主要是迹函数，像Bent序列、GMW序列和椭圆曲线序列等为该类构造的代表。

基于LFSR的伪随机序列生成器有很多，总体上可以分为两大类：一类是用一个n元布尔函数作用于n个输入比特，布尔函数的输出作为密钥流序列；另一类是用一个LFSR控制另一个LFSR。前者包含两种生成器，即熟知的非线性组合生成器和非线性滤波生成器。由于m序列的线性复杂度太小，不能直接用作密钥流序列，因此通常采用将m序列作驱动序列，然后用一个布尔函数作用于这些驱动序列的方法来提高序列的线性复杂度。非线性组合生成器由n个LFSR和一个非线性组合器组成；非线性滤波生成器由一个LFSR和一个前馈逻辑组成。第二类生成器也包含两种控制模型，钟控生成器和缩减生成器。这两种生成器的原理都是用一个控制序列对另一个基序列做不规则采样。钟控生成器是在基序列中插入新的符号，其输出序列指数幂的依赖于产生它的生成器的输入参数；而缩减生成器包括自缩减生成器则是在基序列中删除符号，这种构造结构简单易于用硬件实现。

## 2.3 MATLAB 简介

MATLAB是Math Works公司开发的一种跨平台的，用于矩阵数值计算的简单高效的数学语言，与其它计算机高级语言如C,C++,Fortran,Basic,Pascal等相比，MATLAB语言编程要简洁得多，编程语句更加接近数学描述，可读性好，其强大的图形功能和可视化数据处理能力也是其他高级语言望尘莫及的。对于具有任何一门高级语言基础的读者来说，学习MATLAB十分容易。但是，要用好MATLAB却不是短时间就可以达到的。这并不是因为MATLAB语言复杂难懂，而是实际问题的求解往往更多的是需要使用者具备数学知识和专业知识。MATLAB使得人们摆脱了常规计算机编程的繁琐，让人们能够将大部分精力投入到研究问题的数学建模上。可以说，应用MATLAB这个数学计算和系统方针的强大工具，可以使科学研究的效率得以成百倍的提高。

目前，MATLAB已经广泛用于理工科大学从高等数学到几乎各门专业课程之中，成为这些课程进行虚拟试验的有效工具。在科研部门，MATLAB更是极为广泛地得到应用，成为全球科学家和工程师进行学术交流首选的共同语言。在国内许多著名学术期刊上登载的论文，大部分的数值结果和图形都是借助MATLAB来完成的。

以其他高级语言相比较，MATLAB具有独特的优势：

(1) MATLAB是一种跨平台的数学语言。采用MATLAB编写的程序可以在目前所有的操作系统上运行(只要这些系统上安装了MATLAB平台)。MATLAB程序不依赖于计算机类型和操作系统类型。

(2) MATLAB是一种超高级语言。MATLAB平台本身是用C语言写成的，其中汇集了当前最新的数学算法库，是许多专业数学家和工程学者多年的劳动结晶。使用MATLAB意味着站在巨人的肩膀上观察和处理问题，所以在编程效率，程序

的可读性、可靠性和可以执行上远远超过了常规的高级语言。这使得MATLAB成为进行科学研究和数值计算的首选语言。

(3) MATLAB语法简单，编程风格接近数学语言描述，是数学算法开发和验证的最佳工具。MATLAB以复数矩阵运算为基础，其基本编程单位是矩阵，使得编程简单，而功能极为强大。对于常规语言中必须使用许多语句才能实现的功能，如矩阵分解、矩阵求逆、积分、快速傅里叶变换，甚至串口操作、声音的输入输出等，在MATLAB中用一两句指令即可实现。而且，MATLAB中的数值算法是经过千锤百炼的，比用户自己编程实现的算法的可信度和可靠性都大为提高。

(4)MATLAB计算精度很高，MATLAB中数据是一双精度存储的，一个实数采用8字节存储，而一个复数则采用16字节存储。通常矩阵运算精度高达 $10^{15}$ 以上，完全能够满足一般工程和科学计算的需要。与其它语言相比，MATLAB对计算机内存、硬盘空间的要求也是比较高的。

(5) MATLAB具有强大的绘图功能。利用MATLAB的绘图功能，可以轻易地获得高质量的曲线图。具有多种形式来表达二维、三维图形，并具有强大的动画功能，可以非常直观地表现抽象的数值结果。这也是MATLAB广为流行的重要原因之一。

(6) MATLAB具有串口操作、声音输入输出等硬件操控能力。随着版本的提高，这种能力还会不断加强，使得人们利用计算机和实际硬件相连接的半实物仿真的梦想得以轻易实现。

(7) MATLAB程序可以直接映射为DSP芯片可接受的代码，大大提高了现代电子通信设备的研发效率。

(8)MATLAB的程序执行效率比其他语言低。MATLAB程序通常是解释执行的，在执行效率和速度上低于其它高级语言，当然如果对执行效率有特别要求，可以采用C语言编制算法，然后通过MATLAB接口在MATLAB中执行。事实上，MATLAB自带的许多内部函数均是用C语言编写并编译的，因此利用MATLAB内部函数的程序部分运行速度并不比其他语言中相应函数低。



## 第三章 m序列

### 3.1 m序列的定义

m序列是最长线性反馈移存器序列的简称，它是由带线性反馈的移存器产生的周期最长的一种序列。

### 3.2 m序列的产生

扰码的目的是使短周期输入序列变为长周期的信道序列。从原则上看，就可以用将一个长周期序列叠加在输入序列上的方法来实现，并且叠加序列的周期越长越好。从理论上说，一个真正的随机(二进制)序列的“周期”是无限长的，但是，采用这种序列时在接收端将无法产生相同的序列与之同步。所以，人们就不得不企图用简单电路来产生尽量长的序列。同时随机噪声在通信技术中，首先是作为有损通信质量的因素受到人们重视的。信道中存在的随机噪声会使模拟信号产生失真，或使数字信号解调后出现误码；同时，它还是限制信道容量的一个重要因素。因此，最早人们是企图设计消除或减小通信系统的随机噪声，但是，有时人们也希望获得随机噪声。例如，在实验室中对通信设备或系统进行测试时，有时要故意加入一定的随机噪声，这时则需要产生它。

20世纪40年代末，随着通信理论的发展，仙农(Shannon)就曾指出，在某种情况下，为了实现最有效的通信，应采用具有白噪声的统计特性的信号。另外，为了实现高可靠的保密通信，也希望利用随机噪声。然而，利用随机噪声的最大困难是它难以产生和处理。直到60年代，伪随机噪声的出现才使上述困难的到解决。

伪随机噪声具有类是与随机噪声的一些统计特性，同时又便于重复产生和处理。由于它具有随机噪声的优点，又避免了它的缺点，因此获得了日益广泛的实际应用。目前广泛应用的伪随机噪声都是由数字电路产生的周期序列(即滤波等处理后)得到的。今后我们将这种周期序列称为伪随机序列。

通常产生伪随机序列的电路为一反馈移存器。他又可分为线性反馈移存器和非线性反馈移存器两类。由线性反馈移存器产生出的周期最长的二进制数字序列，称为最大长度线性反馈移存器序列，通常简称为m序列。由于它的理论比较成熟，实现比较简便，实际应用也比较广泛，故这里将重点讨论它。

m序列是最长线性反馈移存器序列的简称，它是由带线性反馈的移存器产生的周期最长的一种序列。图1就是一个这样的电路。图中示出了n级移位寄存器，其中有若干级经模2加法器反馈到第1级。不难看出，在任何一个时刻去观察移位寄存器的状态，必然是 $2^n$ 个状态之一，其中每一状态代表一个n位的二进制数字；但是，必须把全0排斥在外，因为如果一个进入全0，不论反馈线多少或在哪些级，这种状态就不会再改变。所以，寄存器的状态可以是非全0的 $2^n - 1$ 状态之一。这个电路的输出序列是从寄存器移出的，尽管移位寄存器的状态每一移位节拍改变一次，但无疑地是循环的。如果反馈线所分布的级次是恰当的，那么，移位寄存器的状态必然各态历经后才会循环。这里所谓“各态历经”就是所有 $2^n - 1$ 个状态都经过了。由此可见，应用n级移位寄存器所产生的序列

的周期最长是 $2^n - 1$ 。同时由于这种序列虽然是周期的，但当 $n$  足够大时周期可以很长，在一个周期内0和1的排列有很多不同方式，对每一位来说是0还是1，看来好像是随机的，所以又称为伪随机码；又因为它的某一些性质和随机噪声很相似，所以又称为伪噪声码（PN 码）。

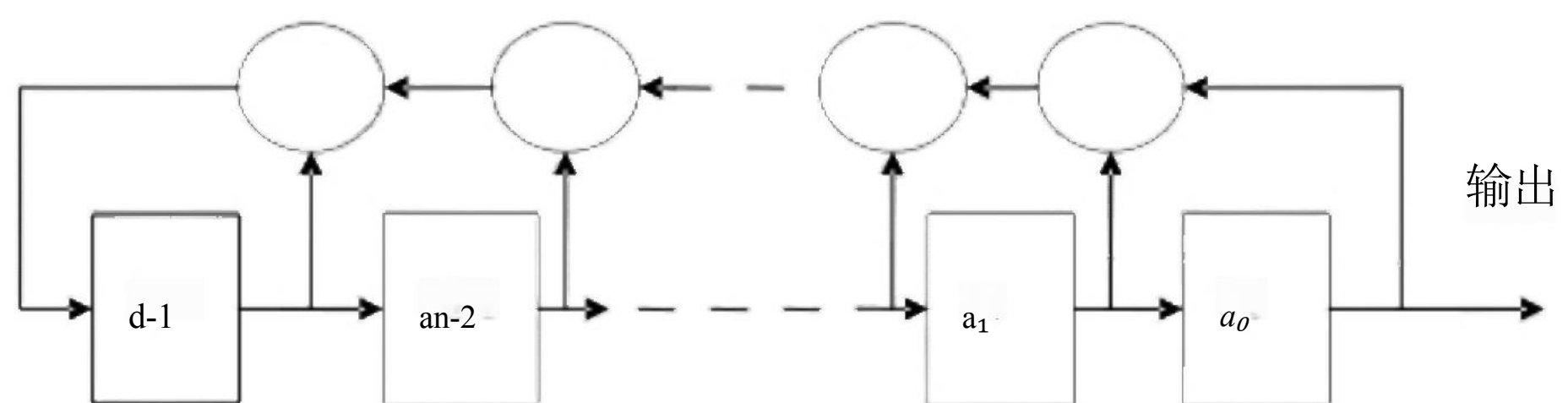


图3-1 最长线性移位寄存序列的产生

要用 $n$  级移位寄存器来产生 $m$ 序列，关键在于选择哪几级移位寄存器作为反馈，

这里扼要陈述选择的方法，但不予证明。将移位寄存器用一个 $n$  阶的多项式 $f(x)$

表示，这个多项式的0次幂系数或常数为1，其 $k$  次幂系数为1时代表第 $k$  级移位寄存器有反馈线；否则无反馈线。注意这里的系数只能取0或1， $x$  本生的取值并无实际意义，也不需要去计算  $x$  的值。称 $f(x)$  为特征多项式。例如特征多

项式 $f(x)=1+x+x^4$  对应于图2 所示的电路。理论分析证明：当特征多项式

$f(x)$  是本原多项式时，与它对应的移位寄存器电路就能产生  $m$  序列，如果加、

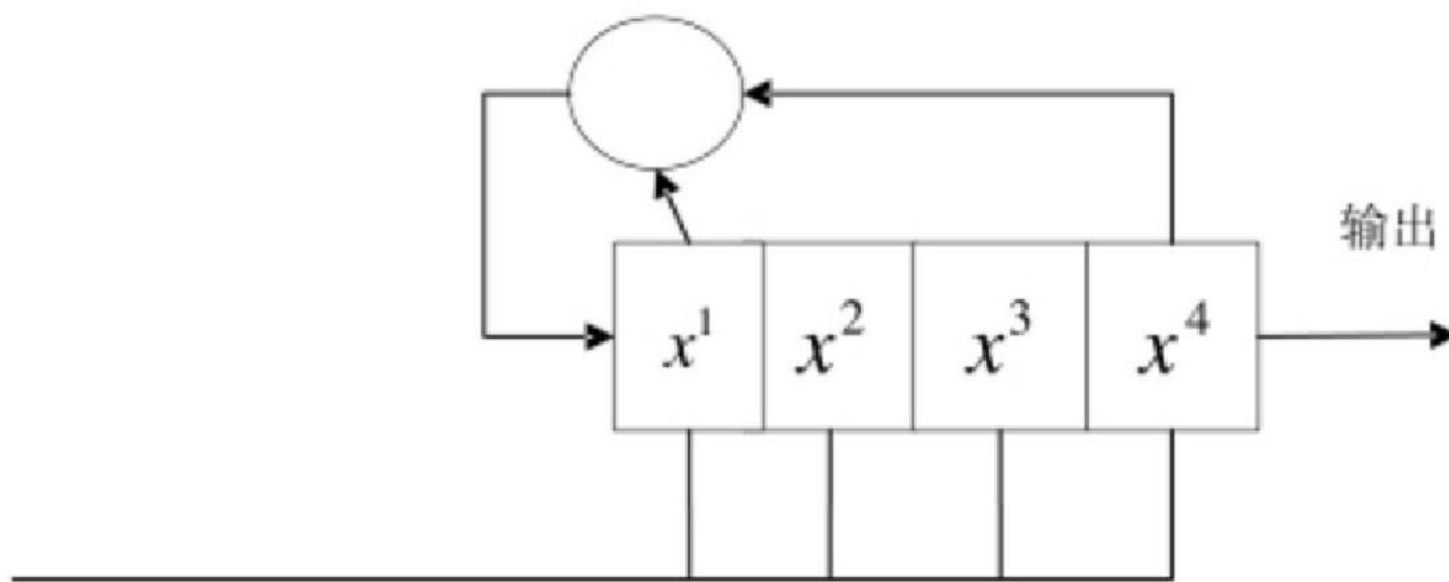
减法采用模2运算，那么的倒量  $g(x) = \frac{1}{f(x)}$  就代表所产生的 $m$ 序列，这个序列

各位的取值按 $g(x)$  自低至高的幂次的系数。所谓“本原多项式”，即 $f(x)$  必须满

足以下条件：

满足以下条件：

- (1)  $f(x)$  为既约的，即不能被1或它本身以外的其他多项式除尽；
- (2) 当 $q=2^n-1$  时，则 $f(x)$  能除尽 $1+x^n$ ；
- (3) 当 $q < 2^n-1$  时， $f(x)$  不能除尽 $1+x^n$ 。



移位

图3-2 m 序列的产生

由上述可见，只要找到了本原多项式，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，如在表3.1中列出了一部分。

n	本原多项式		n	本原多项式	
	代数式	八进制数字表示法		代数式	八进制数字表示法
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	$x^2+x+1$	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

### 3.3 m序列的性质

(1) 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。

(2) 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。

一般来说，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的占1/8...严格地讲，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，连“1”的游程和连“0”的游程各占一半。

(3) 移位相加特性

m序列和它的位移序列模二相加后所得序列仍是该m序列的某个位移序列。设 $M_r$ 是周期为p的m序列M。r次延迟移位后的序列，那么  $M_r \oplus M_s = M_t$

其中 $M_t$ 为 $M_r$ 某次延迟移位后的序列。例如，

$M_0 = 00011110101100$        $1 \cdots M_r$  延迟两位后得 $M_2$ ，再模二相加

$M_2 = 010 \quad 001111010110, \dots$

$M_3 = M_0 + M_2 = 010110010001111, \dots$

可见， $M_3 = M_0 + M_2$  为 $M_0$ 延迟8位后的序列。

(4) 自相关特性

m序列具有非常重要的自相关特性。在m序列中，常常用+1代表0，用-1

代表1。此时定义：设长为p的m序列，记作  $a_1, a_2, a_3, \dots, a_p$  ( $p=2^n-1$ )。经

过j次移位后，m序列为  $a_{j+1}, a_{j+2}, \dots, a_{j+p}$ ，其中  $a_{j+p} = a_j$  (以p为周期)

以上两序列的对应项相乘然后相加，利用所得的总和

$$a_1 \cdot a_{j+1} + a_2 \cdot a_{j+2} + a_3 \cdot a_{j+3} \cdots + a_p \cdot a_{j+p} = \sum_{i=1}^p a_i a_{j+i} \quad (3-1)$$

来衡量一个m序列与它的j次移位序列之间的相关程度，并把它叫做m序列

$(a_1, a_2, a_3 \cdots a_p)$  的自相关函数。记作

$$R(j) = \sum_{i=1}^p a_i a_{j+i}$$

(3-2)



当采用二进制数字0 和 1 代表码元的可能取值时

$$R(j) = \frac{A-D}{A+D} = \frac{A-D}{p} \quad (3-3)$$

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

(3-4)

由移位相加特性可知， $a_i$  和  $a_{i+j}$  仍是  $m$  序列中的元素，所以上式分子就等于  $m$  序列中一个周期中  $\begin{cases} 1 & j=0 \\ -1/p & j=\pm 1, \pm 2, \dots, \pm(p-1) \end{cases}$  的数目与 1 的数目之差。另外由  $m$  序列的均衡性可知，在一个周期中 0 比 1 的个数少一个，故得  $A-D=-1$  ( $j$  为非零整数时) 或  $p$  ( $j$  为零时)。因此得

(3)

-5)

$m$  序列的自相关函数只有两种取值 (1 和  $-1/p$ )。  $R(j)$  是一个周期函数，即

$R(j)=R(j+kp)$ , 式中,  $k=1,2,\dots,p=(2n-1)$  为周期。而且  $R(j)$  是偶函数，即

$R(j)=R(-j)$   $j=$  整数

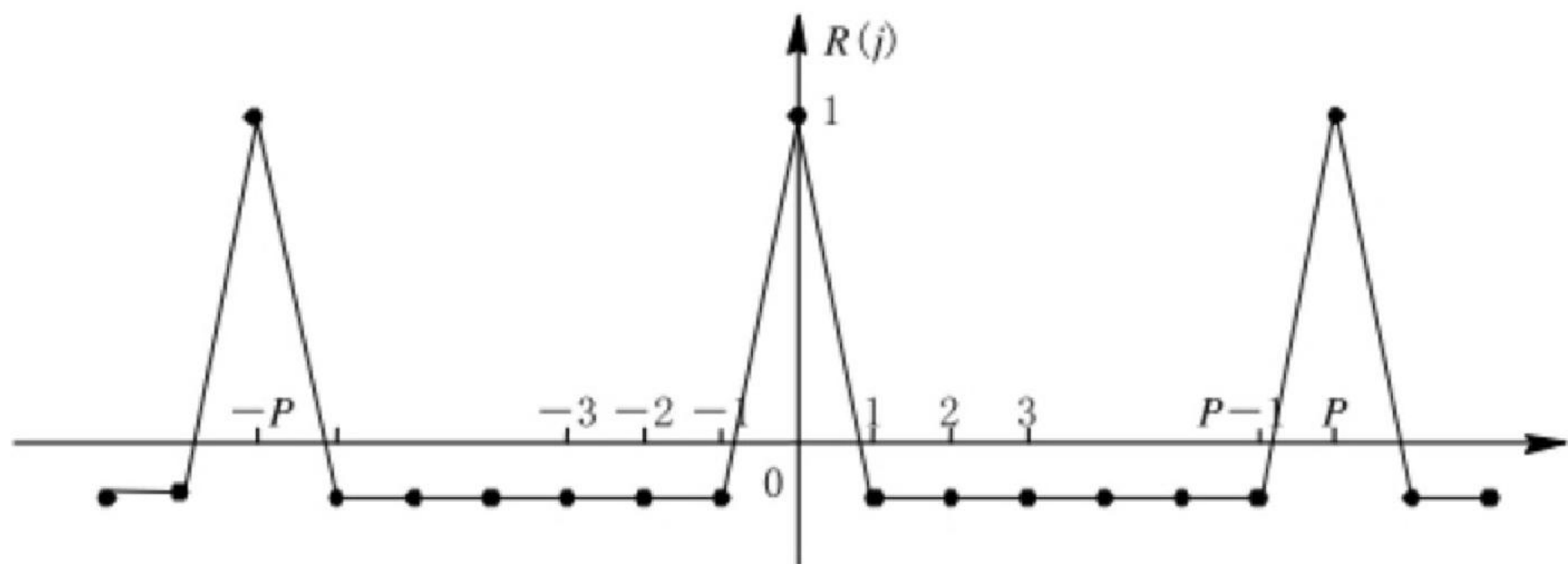


图3-3  $m$  序列的自相关函数

(5) 功率谱密度

令  $m$  序列长度为  $N$ , 周期  $T=NT$ ,  $T$  为码片宽。相应的双极性波形为

$c(t) = \sum_{n=-\infty}^{\infty} a(t-nT)$ ，其中： $a(t) \in (-1, 1)$ ，为  $m$  序列的一个周期

$c(t)$  的归一化自相关函数为： $r(\tau) = \frac{1}{T} \int_0^T c(\tau) \cdot c(t-\tau) dt$

(3-7)

$$r_T(\tau) = \begin{cases} \left(\frac{N+1}{N}\right) \left[1 - \frac{|\tau|}{T_c}\right], & |\tau| < T_c \\ 0, & \text{其他 } \tau \end{cases}$$

令:

$$\text{则 } r(\tau) = \sum_{n=-\infty}^{\infty} r_T(\tau - nT) - \frac{1}{N} = r_1(\tau) - \frac{1}{N} \quad \text{其中: } r_1(\tau) = \sum_{n=-\infty}^{\infty} r_T(\tau - nT)$$

c(1)的功率谱密度G(ω)→r(r) 互为付利叶变换

$$G(\omega) = F[r(\tau)] = F[r_1(\tau)] - F\left(\frac{1}{N}\right) \quad F_n = \frac{1}{T} \int_{-T/2}^{T/2} r_1(\tau) \cdot e^{-jn\omega_0\tau} d\tau$$

(3-8)

周期性函数r(r) 可以展为付利叶级数:

其中:

$$= \frac{1}{T} \int_{-\infty}^{\infty} r_T(\tau) \cdot e^{-jn\omega_0\tau} d\tau = \frac{1}{T} F[r_T(\tau)]_{\omega=n\omega_0}$$

(3-9)

$$F[r_1(\tau)] = 2\pi \sum_{n=-\infty}^{\infty} F_n \delta(\omega - n\omega_0) = \frac{2\pi}{T} \sum_{n=-\infty}^{\infty} F[r_T(\tau)] \delta(\omega - n\omega_0)$$

$$= \frac{2\pi}{T} \sum_{n=-\infty}^{\infty} \left(\frac{N+1}{N}\right) T_c Sa^2(\omega T_c / 2) \delta(\omega - n\omega_0)$$

(3-10)

$$F\left(\frac{1}{N}\right) = \frac{2\pi}{N} \delta(\omega)$$

(3-11)

$$G(\omega) = F[r_1(\tau)] - F\left(\frac{1}{N}\right) = \frac{2\pi T_c}{T} \left(\frac{N+1}{N}\right) \sum_{n=-\infty}^{\infty} Sa^2(\omega T_c / 2) \delta(\omega - n\omega_0) - \frac{2\pi}{N} \delta(\omega)$$

$$= 2\pi \left(\frac{N+1}{N^2}\right) \sum_{n=-\infty}^{\infty} Sa^2(\omega T_c / 2) \delta(\omega - n\omega_0) - \frac{2\pi}{N} \delta(\omega)$$

$$= 2\pi \left[ \sum_{n=-\infty}^{\infty} \text{Sa}^2(\omega T_c / 2) \delta(\omega - n\omega_0) + \frac{1}{N^2} \delta(\omega) \right]$$

(3-12)

双极性m序列码波形功率谱密度的特点:

- 1) 为离散谱, 间隔为 $\omega_0 = 2\pi / T = 2\pi / NT$ 。

- 2) 带宽近似为  $\Delta\omega=2\pi/T=N\omega_0$  ( $\Delta f=1/T$ 。)
- 3) 谱线的包络以  $\text{Sa}^2(\omega T/2)$  规律变化。
- 4) 支流分量  $\frac{1}{N^2}\delta(\omega)$  的强度与码长的平方  $N^2$  成反比。

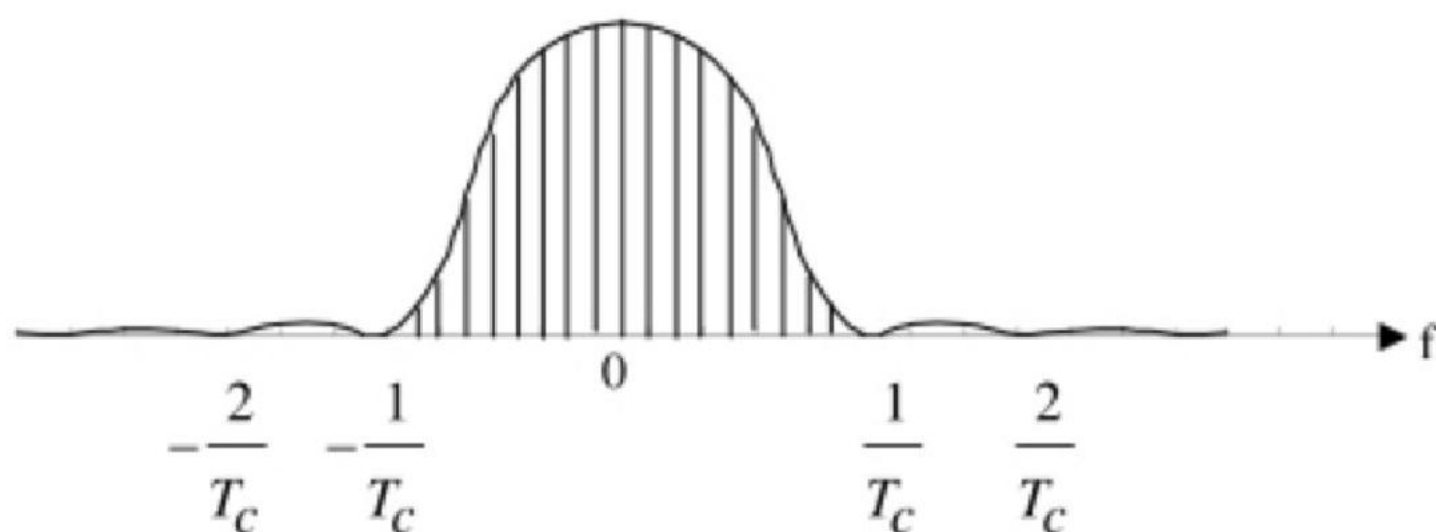


图3-4 m序列功率谱密度

#### (6) 伪噪声特性

如果我们取一正态分布白噪声取样，若取样值为正，记为“+”；若取样值为负，记为“-”，则将每次取样所得极性排成序列，可以写成

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

这是一个随机序列，它具有如下基本性质：

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……一般来说，长度为k的游程约占1/2<sup>k</sup>，而且在长度为k的游程中，“+”游程和“-”游程约占个一半。

由于白噪声的功率谱为常数，功率谱的逆傅里叶变换，即自相关函数为一冲激函数  $\delta(t)$ 。当  $t \neq 0$  时， $\delta(t)=0$ ；仅当  $t=0$  时， $\delta(t)$  是个面积为1的脉冲。

由于m序列的均衡性、游程分布、自相关特性和功率谱与上述随机序列的基本性质很相似，所以通常认为m序列属于伪噪声序列或伪随机序列。

### 3.4 m序列的计数

同长度不同反馈逻辑的m序列的数目等于同幂次的本原多项式的数目。可以

证明：n幂次本原多项式的数目为：
$$N_n = \frac{\Phi(2^n - 1)}{n}$$

其中： $\Phi(x)$  为欧拉函数，它等于：小于x的并与x互质的数的个数(包括1在

内)。例如， $x=2^4-1=15$ ，则小于15并与15互质的数为：1, 2, 4, 7, 8, 11,

13, 14, 共8个，则  $\Phi(15)=8$ ； $N_4=8/4=2$ 。



表3.2 列出了不同长度 $m$ 序列的数目和 $m$ 序列的计数

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----

$2^m - 1$	3	7	$\frac{m}{2}$	3	6	12	25	51	102	204	409	819	1638	3276
			$\frac{m}{2}$	1	3	7	5	1	3	7	6	1	8	7
$N_m$	1	2	2	6	6	18	16	48	60	176	144	630	576	1800

由表3.2可见，当m序列的长度(周期)不很大时，同长度的不同m序列的数目不大。例如长度为127的m序列仅有18种；长度为511的也仅有48种。多址系统中当地址数很大时，m序列作地址码就不够用了。因此人们又寻找出数量多同时又具有类似于m序列性质的伪随机码；例如：**Gold码**；

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：  
<https://d.book118.com/068036104072006063>