伪随机序列技术

吴中一 编著

哈尔滨工业大学出版社

伪随机序列技术

吴中一 编著

哈尔滨工业大学出版社

内 容 简 介

本书介绍了伪随机序列的构造方法及其有关特性。着重讨论了序列的周期相关特性、非周期相关特性、奇相关特性和序列的最佳相位问题。对小互相关特性二元序列和非线性序列作了专门的讨论。其特点是利用微型机产生序列并分析序列特性，介绍了必要的程序供参考。

本书可供通信、雷达、测量、遥控、遥测和导航等专业的工程技术人员参考，对大专院校有关专业的师生也有参考价值。

伪随机序列技术

吴中一 编著

哈尔滨工业大学出版社出版
新华书店首都发行所发行
鸡西市印刷二厂排版
哈尔滨市外文印刷厂印装

开本 787×1092 1/32 印张9.125 字数204,000
1986年12月第1版 1986年12月第1次印刷
印数 1—2,500
书号 15341·27 定价 1.60元

前　言

伪随机序列或伪随机码的应用范围越来越广泛。在通信（包括扩频通信、卫星通信、保密通信和常规通信等）、雷达、导航、遥控、遥测、测量以及自控等领域都有着重要的应用。随着科学技术的发展，知识的更新，要求掌握和应用伪随机序列技术的人越来越多。为此，作者总结了多年的教学和科研实践，写出了这本书。

伪随机序列技术是一类编码技术，它既是数学问题，又是一种工程实用技术。本书力图避免繁琐、严谨的数学论证，而用通俗的语言说明数学问题。介绍了目前常用的伪随机序列的数学特征和构造方法；着重对伪随机序列的相关特性作了较深入的分析。

近年来，计算机尤其是微型机已成为广大科技工作者的工作手段。本书介绍了用微型机产生各类伪随机序列的技术，并相应地对其特性进行了一定的分析。这样便于读者在应用或进一步研究伪随机序列的性能时，使用计算机这一有力工具。

全书分五章。第一章介绍了移位寄存器序列，以使读者对伪随机序列有一概括的了解。第二章由伪随机序列的相关特性出发，对各类伪随机序列的数学特征作了扼要的说明，讨论了它们的一般特性及构造它们的算法，重点说明了 m 序列的构造算法。第三章是本书的重点，讨论了周期序列的相关特性，包括序列的周期相关特性、非周期相关特性、奇相

关特性和序列的最佳相位问题。第四章讨论了用于码分多址系统的小互相关二元序列的构造技术，重点讨论了戈尔德（*Gold*）序列。第五章是根据对保密技术的要求，扼要地介绍了非线性伪随机序列的构造技术。

本书由贾世楼同志审阅，刘明秋同志进行技术图表的处理。在编写本书过程中，参阅了一些同志的有关资料，并得到张乃通、许宗泽、周廷显等同志的支持与鼓励，在此谨表谢意。

由于作者学识浅薄，本书的错误和不妥之处在所难免，敬请批评指正。

作 者

1985年5月

目　　录

第一章　线性移位寄存器

伪随机序列又称伪噪声序列，它的应用十分广泛。例如，扩频通信、测距、导航、遥控、遥测、多址、保密编码和抗干扰等系统；自控系统中的系统辨识；测量系统中的噪声源；数字通信中的同步等等，都广泛应用了伪随机序列或其变形序列。本章从移位寄存器入门，由移位寄存器的适当反馈连接状态产生期望的序列，进而引出适当的理论，介绍产生线性序列的数学特征；阐明伪随机序列与移位寄存器之间的有机联系。本章主要讨论线性移位寄存器序列，而对非线性移位寄存器序列，则在第五章讨论。

1—1　移位寄存器序列

移位寄存器是由 n 级串接的存贮单元和一个时钟源组成。但是，这种静态移位寄存器作为序列产生器是没有意义的。因为这时不管移位寄存器的初始状态如何，当经过 n 个时钟周期后，各级最终都将处于恒定不变状态(全1或全0)。欲构成所谓动态移位寄存器，则在第一级上必须引入反馈。以后我们所提及的移位寄存器，都指动态移位寄存器。用移位寄存器作为序列产生器，其产生的0或1序列如图1—1所示，图中给出相应具有±1幅值的时间波形。

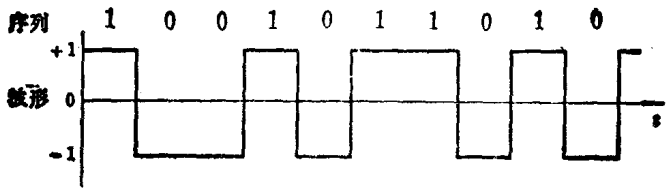


图 1—1　移位寄存器序列和波形

首先，考虑一个简单的移位寄存器，如图1—2。该移位寄存器由六级具有移位功能的存贮单元、一个模 2 加法器及

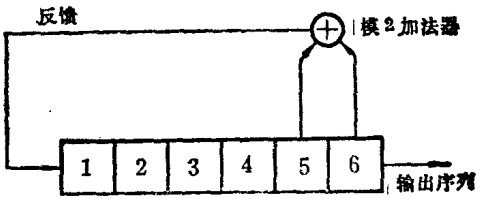


图 1—2　简单的移位寄存产生器

一条反馈线所组成。存贮单元的移位由时钟源驱动。模 2 加法器的逻辑功能表现为两个元素“0”和“1”的相加能力附合图1—3（a）所示规则，即除了1⊕1 = 0外，完全遵循着普通加法规律，其对应的波形相当于进行乘法运算，如图1—3（b）所示。

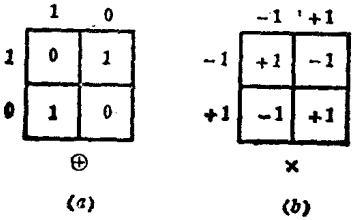


图 1—3　序列模 2 加与波形相乘规则

满足图1—3（a）所示的模2加要求，即可着手讨论图1—2的移位寄存器是如何工作了。存贮着1或0的各存贮单元所处的状态，分别用数字1到6来表示，存贮内容直至下一个时钟脉冲到达之后才能引起依次的顺序改变，1单元的内容变换到2单元，原来2单元的内容变换到3单元，…，最后5单元和6单元的内容经模2相加，其结果反馈到1单元。即一个移位寄存器是每作用一个移位脉冲后，存贮单元的内容右移一位，移位寄存器序列可由最后单元输出。

假定开始五个单元的内容为“0”，第6个单元为“1”，即寄存器初始状态为000001。第一个时钟脉冲到达后，整个状态右移一位，6单元中的“1”是移位寄存器序列的第一个数字，而反馈到1单元的“1”是5单元的“0”和6单元的“1”模2和的结果。依次类推，最后输出序列将为：

$$100000100001100010100111101000111001001011011101100110101011111$$

（1—1—1）

可见序列中共有63个元素。随着钟脉冲的加入，输出则是这63个元素的周期性重复。这种反馈信号都反馈到单一的输入端称为简单移位寄存产生器（$SSRG$）。另一类称为多往返移位寄存产生器（$MRSRG$），其模2加法器的输出可以反馈加至两个或更多个单元上，如图1—4所示。图1—2为

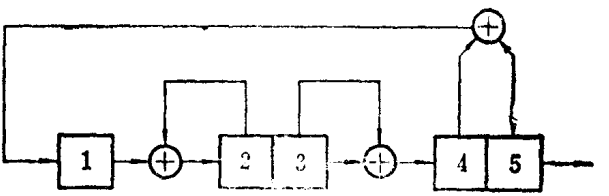


图1—4 MRSRG举例

一般形式，而图1—4则为标准形式，其每一存贮单元和它相邻单元之间放置一个模 2 加法器，从而构成标准组件。它可以减小反馈回路上的固有延迟，提高移位寄存器的工作速度，常称为组件移位寄存产生器（$MSRG$）。无论 $MRSRG$或 $MSRG$，若不考虑其暂态过程，总能与一个简单移位寄存产生器（$SSRG$）相等效。因此，后面总是以$SSRG$为代表来讨论。

如果在简单移位寄存产生器中，每一级存贮单元的内容用 x_i 来表示，i 为级的序号，而反馈函数能用一个模 2 和来表示，则我们称该种移位寄存产生器是线性的，如图1—5所示。这里用$f(x_1,x_2,\cdots,x_n)$表示反馈布尔函数，它有几个二元输入变量和一个二元输出变量。

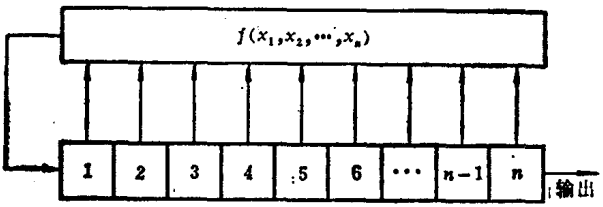


图 1—5　线性移位寄存产生器

由于移位寄存器是线性的，因此 $f(x_1,x_2\cdots,x_n)$ 可以表示为具有反馈连接系数 $C_i=1$ 或 0 的各级内容的模 2 和，即

$$f(x_1,x_2,\cdots,x_n)=C_1x_1\oplus C_2x_2\oplus\cdots\oplus C_nx_n \qquad (1—1—2)$$

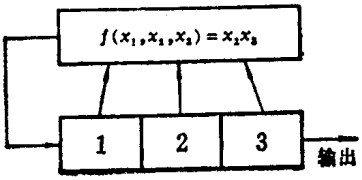
本章中，所有移位寄存产生器，除了作特殊说明外，都是指线性移位寄存产生器。

图1—6给出了一个非线性反馈移位寄存器的例子。其中

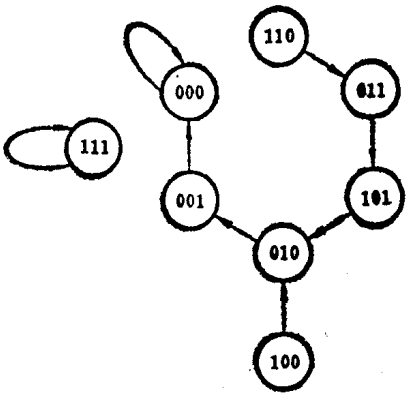
图（a）部分是移位寄存产生器，图（b）是它的状态图。反馈函数为

$$f(x_1,x_2,x_3)=x_2x_3 \qquad (1—1—3)$$

可见它是非线性的。若初始状态为110，即第一级内容为“1”，第二级为“1”和第三级为“0”。由反馈函数可见，



(a)



(b)

图1—6 非线性反馈移位寄存产生器

（a）原理图 （b）状态图

$x_2x_3=1\cdot0=0$，所以新的状态变为011。这一过程继续下去一直到达000状态，并将永远保持这种000状态。而当寄存器初始状态为111时，则$x_2x_3=1\cdot1=1$，新态还是111，随后每个时钟到来后，寄存器还始终保持111状态。再进一步

观察可知，状态010能由两个不同的先行状态获得，即101和100。而对于线性移位寄存器的每一状态只有一个先行状态。可见非线性反馈移位寄存产生器的构造机理要比线性的复杂得多。

还有一类非线性移位寄存器称为非线性前馈移位寄存器。它是在线性移位寄存产生器的基础上，序列再通过非线性前馈函数输出的一种移位寄存产生器。如图1—7所示。图

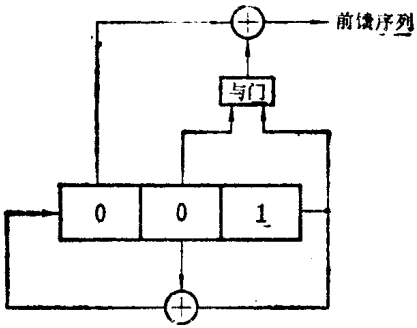


图1—7　非线性前馈移位寄存器

中假设初始状态为001，则输出序列为0101101。前馈函数 $f(x_1,x_2,x_3)=x_1\oplus x_2x_3$。显然，这类序列与线性移位寄存器序列不同，但较非线性反馈移位寄存器序列易于构造，故有其独特的用途（见第五章）。

1—2　移位寄存器序列的性质

一个移位寄存器所产生的序列的形式取决于寄存器的级数、反馈抽头的连接和初始条件。通常输出序列分为两类：最大长度序列（m序列）和非最大长度序列。当移位寄存产

生器具有 n 级，若序列长度为 2^n-1，则为最大长度序列，而序列长度小于 2^n-1，则为非最大长度序列。图1—2所示的简单移位寄存产生器产生的序列，因其序列长度为 $2^6-1=63$，所以它是最大长度序列。在该序列中，包含着除六个“0”之外的所有六态数字。

对于一个给定级数的移位寄存器，其反馈连接情况就决定该序列的长度是否为最大长度。对于非最大长度序列，初始条件决定了所产生的是哪一种序列。即对非最大长度序列来说，不同的初始条件可能产生不同的序列；而对于最大长度序列，若不计及暂态过程，则与初始条件无关（全“0”态除外）。下面讨论实现最大长度序列的重要定理。

定理1 具有奇数个抽头的简单移位寄存产生器，不可能产生一个最大长度序列。

证明：假定移位寄存器全部载荷着“1”，于是很清楚，寄存器将保持着全“1”状态。由于总共具有 2^n 个状态，而全“0”状态的周期为1，全“1”状态的周期也为1。所以具有奇数个抽头的移位寄存产生器，所能产生序列的最大长度是 2^n-2，要比最大长度序列的长度小1，所以它不是最大长度序列。事实上，所产生的序列长度可能比 2^n-2 还要短得多。

如果现在的目标是寻求最大长度序列，就应废弃采用奇数个反馈抽头的产生器。

现在考虑产生一个规定序列的反序列方法。一般情况下，若原始序列为…，a_k，a_{k+1}，a_{k+2}…，于是其反序列为…，a_{k+2}，a_{k+1}，a_k，…。当它是最大长度序列时，寻求互反的移位寄存器方法是很易得到的。例如一个 n 级简单移位寄存产生器，在 n，k，m，…等级上有反馈抽头，这样互

反序列产生器将在 n，$n-k$，$n-m$，…等级上具有反馈抽头（$n>k>m\cdots$）。

例如在图 1—8 中，给出了 $n=5$ 的移位寄存产生器。图（a）在第 5 级和第 2 级上抽头反馈，得原序列周期 $N=31$ 位；图（b）则在第 5 级和 $5-2=3$ 的第 3 级上抽头反馈，得周期也是 31 位的互反序列。若初始状态都为00001，原序列和互反序列为

原序列：1000010101110110001111100110101

互反序列：1000010010110011111000110111010

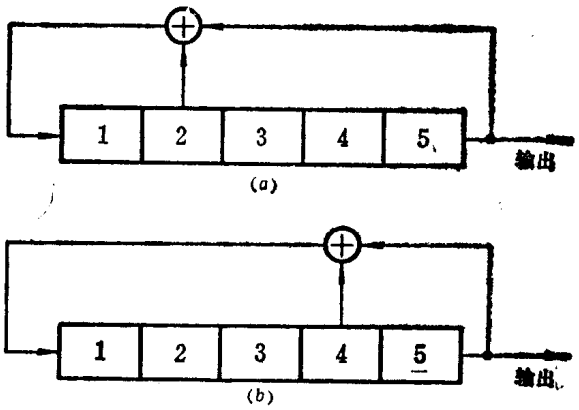


图 1—8　最大长度序列产生器　（a）原序列　（b）互反序列

若在举例中使用的是一个非最大长度产生器，则上述方法就不适用，我们将发现互反产生器所产生的序列是与其它产生器产生的序列互反。

可以指出，对于一个 n 级的简单移位寄存产生器，只要