全国高技术重点图书 · 通信技术领域

最佳信号理论与设计

杨义先 著

人民邮电出版社

全国高技术重点图书·通信技术领域

最佳信号理论与设计

杨义先 著

人民邮电出版社

内 容 简 介

本书比较系统而全面地介绍了作者及国内外学术界近年来在最佳离散信号的码型设计和理论研究方面的最新成果，大部分内容在同类书籍中还是首次出现。

全书共分五章，分别重点介绍了最佳信号设计的基础理论、伪随机信号设计、循环相关信号设计、非循环相关信号设计和线性复杂度序列设计。书中介绍的大量最佳信号设计方法都可以直接用于工程设计。

本书可供通信与电子系统、信号与信息处理、信息科学、应用数学和计算机科学等领域的理论工作者、工程技术人员、研究生和高年级本科生作为专业课题研究的参考书。

全国高技术重点图书·通信技术领域

最佳信号理论与设计

杨义先 著

责任编辑 梁毅

人民邮电出版社出版发行

北京崇文区夕照寺街 14 号

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

*

开本：850×1168 1/32　　1996 年 12 月　　第 一 版

印张：9.625　　1996 年 12 月　北京第 1 次印刷

字数：249 千字　　印数：1—2 000 册

ISBN 7-115-06250-1/TN·1111

定价：20.00 元

《全国高技术重点图书》出版指导委员会

主　任： 朱丽兰

副主任： 刘　果　卢鸣谷

委　员： （以姓氏笔划为序）

王大中　王为珍　王守武　牛田佳　卢鸣谷
叶培大　刘　仁　刘　果　朱丽兰　孙宝寅
师昌绪　任新民　杨牧之　杨嘉墀　陈芳允
陈能宽　张钰珍　张效详　罗见龙　周炳琨
欧阳莲　赵忠贤　顾孝诚　谈德颜　龚　刚
梁祥丰

总干事： 罗见龙　梁祥丰

《全国高技术重点图书·通信技术领域》编审委员会

主　任： 叶培大

委　员： 陈俊亮　徐大雄　姚　彦
程时昕　陈芳烈　李树岭

前　言

最佳信号并无严格的数学定义。在现代雷达、通信、空间测控以及电子对抗等众多的工程领域中，不同的实用背景对所需信号提出了不同的要求。能很好地满足这些不同工程要求的信号都称为最佳信号（也有人称之为最佳离散信号）。所以对某个给定的信号，当用某种工程要求标准去衡量时它可能是最佳信号，但是改用另一种工程要求标准去评价时它或许就变成最差信号了。目前不存在（今后也几乎不可能找到）一种信号在所有工程要求标准之下都是最佳的，因为有些工程要求彼此之间本身就是相互抵触的。当前对于信号最普遍的工程要求大约可分为伪随机性、循环相关性、非循环相关性和线性复杂度等。

顾名思义，伪随机性就是假的随机性，它看起来像随机的，实际上并不是随机的。最经典的伪随机序列是最长线性反馈移位寄存器序列（简称 m－序列）和最长非线性反馈移位寄存器序列（简称 M－序列）。到目前为止，国内外已出版了众多著作专论伪随机序列。为了避免与现有书籍内容上的重复，本书在 1.2 节中简要综述了 m－序列和 M－序列的基本内容之后，在第二章重点介绍了一些著名的经典伪随机序列的推广和满足窗口特性的伪随机序列与阵列的设计。

循环相关性准则是一种使用相当广泛的工程准则。直观说来此准则要求信号的循环自相关函数尽量靠近一个脉冲函数，而不同信号之间的循环互相关函数尽量靠近零值。具有良好循环相关特性的信号在工程中的应用领域实在太广泛，很难逐一列出。最常见的应用领域包括诸如：系统同步、电子跟踪、跳频系统设计、信道分配等

等。本书第三章重点介绍了一些最新的循环相关信号以及一些新的有效的信号设计方法。除了介绍工程中常用的二元序列和四元序列之外，本章还介绍了一般的 p 元序列设计和阵列设计。

非循环相关性准则与循环相关性准则的唯一差别在于当计算相关函数值时用非循环移位去代替循环移位。上述定义上的唯一差别不但使非循环相关准则在工程背景方面与循环相关准则各不相同，而且使这两类最佳信号的设计截然不同。实际上，非循环相关信号的设计难度大多了，至今没有一种完美的研究方法。但是最近十年以来，国际上对非循环相关信号的研究相当活跃。本书第四章重点介绍了非循环相关序列、Costas 阵列、跳频码设计和同步阵列设计方面的一些最新的具体成果。

线性复杂度是序列密码中衡量一个密钥流的安全性的重要指标，它代表了用线性反馈移位寄存器去恢复密钥流序列的困难程度。过去人们所用的设计线性复杂度序列的常用方法是移位寄存器方法，此方面已有众多书籍作过详细介绍。本书第五章系统介绍了两种在以往同类书籍中很少出现过的新方法：Bent 函数方法和迹函数方法。这两种方法十分有效，目前已经用它们设计出了很多性能优良的线性复杂度序列，比如 Bent 序列、广义 Bent 序列、GMW 序列、NK 序列、级联 GMW 序列和复值 GMW 序列等。

本书所需的基础理论都集中在第一章。读者在阅读了第一章之后便可以独立地按任意顺序阅读其它各章。为突出重点，本书略去了一些繁琐的数学证明过程，同时注明了有关参考文献和出处，供有兴趣的读者查阅。本书不涉及高深的数学理论，一般工程技术人员都能阅读，书中所列出的许多现成的最佳信号甚至可以直接拿来用作有关工程实际问题所需的信号。

在本书的写作过程中作者得到了同事和家庭的多方支持与帮助。胡正名教授提出了许多有益建议，博士生许成谦和王端怡等为本书的整理作了不少工作。还要感谢我的爱人和父母亲对我工作的理解和支持。最后特别感谢国家教委跨世纪优秀人才专项基金和国

家杰出青年基金的资助。

由于本人水平有限，不足之处在所难免，欢迎读者批评指正。

作者

1995 年 1 月于北京

目　录

第一章　基础理论

本章是全书的基础，主要介绍与各种最佳信号设计有关的概念、实用背景和必要的数学基础。在1.1节归纳了以后各章所需的数学知识后，接着在1.2至1.5节分别介绍了最佳信号设计的移位寄存器理论、循环相关理论、非循环相关理论和线性复杂度理论。

1.1　数学基础

为保持全书的完整性，本节简要介绍了最佳信号设计所需要的数学知识，包括有限域理论和区组设计。本节力图简明扼要，不追求数学上的严格性，同时还略去了定理的证明过程。有兴趣更深了解这些数学知识的读者可查阅有关数学专著或教科书。

1.1.1　有限域理论[1~3]

域是一种特殊的带有运算的集合，比如大家熟悉的实数域或复数域就是两种最常见的含无穷多个元素的域。只包含有限(q)个元素的域就叫做有限域，记为 $GF(q)$。这里称 q 为有限域 $GF(q)$ 的阶。严格地说有：

定义 1.1.1.1　含 q 个元素的集合 M 称为有限域，如果该集合带有两种运算(分别称为加法和乘法)并且这两种运算满足如下定律：

1.自闭律：对任意两个元素 $a, b \in M$，存在唯一一对元素 $c, d \in M$ 使得 $ab = c$ 和 $a + b = d$。

2.结合律：对任意的 $a, b, c \in M$ 成立 $(a + b) + c = a + (b + c)$

和$(ab)c=a(bc)$。

3.交换律:对任意 $a,b\in M$ 成立$ab=ba$ 和$a+b=b+a$。

4.存在零元素和单位元素:在集合 M 中存在两个特殊的元素 0 和 1,它们满足 $0+a=a+0=a$ 和 $1\cdot a=a\cdot 1=a$,其

中 $a\in M$ 任取。

5.存在逆元素:对任意 $a\in M$,存在元素 $b\in M$ 满足$a+b=b+a=0$,特别当 $a\neq 0$ 时还存在 $c\in M$ 使得$ac=ca=1$。这时分别称 b 和 c 为 a 的负元和逆元。

6.分配律:对任意 $a,b,c\in M$ 成立$a(b+c)=ab+ac$ 和$(b+c)a=ba+ca$。

例如:设 p 为一个素数,M 为整数集合$\{0,1,\cdots,p-1\}$,若将 M 中的加法运算和乘法运算分别定义为这些整数在模 $p(\mathrm{mod}p)$意义之下的加法和乘法,那么可以直接验证上述 6 条定律全都满足,所以 M 就是含 p 个元素的有限域,称之为素域 $GF(p)$。

设多项式 $A(x)=\sum_{i=0}^{n}a_ix^i$ 中每个系数 a_i 都是有限域$GF(p)$中的元素,那么称 $A(x)$为域 $GF(p)$上的多项式,并且将使得 $a_n\neq 0\mathrm{mod}p$ 的最大整数 n 称为该多项式的次数。称域 $GF(p)$上的多项式 $A(x)$和 $B(x)$ 关于多项式模 $F(x)$同余,如果存在另一个多项式 $K(x)$使得 $A(x)-B(x)=K(x)F(x)$。对给定的多项式 $f(x)$,如果存在两个次数大于 0 的多项式 $A(x)$和 $B(x)$使得 $f(x)=A(x)B(x)$,那么就称 $f(x)$可约,否则就称 $f(x)$是一个不可约多项式。

定理 1.1.1.2 设 $f(x)$是域 $GF(p)$中的一个 n 次不可约多项式,M 是$GF(p)$中次数小于 n 的所有多项式(共 p^n 个)所组成的集合,若将集合 M 中的加法和乘法分别定义为在模 $f(x)$意义下的加法和乘法,那么 M 就是一个有限域$GF(p^n)$,并称 M 为素域$GF(p)$的扩域。更进一步还可以证明任意一个有限域一定是某个素域的扩域。因此以下我们仅考虑含 $q=p^n$(p 为素数)个元素的有限域 GF

(q)，这里 p 称为该域的特征。

设 a 是有限域 $GF(q)$ 中的一个非零元素，由定义 1.1.1.1 中的自闭律和域的有限性，不难看出一定存在正整数 k 使得 $a^k = 1$（即 k 个 a 连乘等于 1），称使该等式成立的最小整数 k 为元素 a 的周期。

定理 1.1.1.3 设 $a \in GF(q)$，如果元素 a 的周期为 k，那么元素 a^m 的周期等于 $k/\gcd(k, m)$。此外 $GF(q)$ 中每个元素的周期显然不会超过 $q-1$，特别假如某个元素 α 的周期达到最大值 $q-1$，那么称 α 为该域的一个本原元素。此时有 $GF(q) = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}$，因此又可称 α 为 $GF(q)$ 的生成元素。本原元素的逆元也是本原元素，并且在 $GF(q)$ 中共有 $\varphi(q-1)$ 个本原元素。这里 $\varphi(n)$ 是欧拉函数，表示小于 n 并与 n 互素的正整数的个数。

定理 1.1.1.4 有限域 $GF(q)$ 中的任意元素 a 恒满足 $a^q = a$，因此整数 $q-1$ 是 $GF(q)$ 中一切非零元素的周期的倍数。

由以上定理可知域 $GF(q)$ 中的 q 次多项式 $x^q - x$ 在 $GF(q)$ 中共有 q 个根。若 $f(x)$ 是 $GF(q)$ 中的一个 k 次不可约多项式，那么 $f(x)$ 就在 $GF(q)$ 中没有根，但是可以证明此 $f(x)$ 在扩域 $GF(q^s)$（k 整除 s）中却刚好有 k 个根。更精确地说，有以下定理。

定理 1.1.1.5 设 $f(x)$ 是 $GF(q)$ 中的 k 次不可约多项式，a 是 $f(x)$ 在扩域 $GF(q^s)$ 中的一个根（$k \mid s$），并且 a 的周期 ε 满足 $(q^s)^k \equiv 1 \bmod \varepsilon$，那么 $GF(q^s)$ 中的元素 $a, a^q, \cdots, a^{**}(q^{k-1})$（其中 $a^{**}n$ 和 a^n 的含义一样，下同）便是 $f(x)$ 在 $GF(q^s)$ 中的全部根，因此

$$f(x) = \prod_{i=0}^{k-1} (x - a^{**}q^i)$$

称此式为域 $GF(q^s)$ 中元素 a 的极小多项式，而该多项式的次数称为元素 a 的次数。

上面域 $GF(q^s)$ 中的元素 $a, a^q, \cdots, a^{**}q^{k-1}$ 称为彼此共轭的。可以证明共轭元素有相同的极小多项式和相同的周期。另外，在域 $GF(q^s)$ 中根的周期同为 ε 的 k 次不可约多项式（若 $s=1$，则 $k \mid$

n，若 $s>1$，则 $k \mid s$，这里 $q=p^n$）共有 $\varphi(\varepsilon)/k$ 个。如果域 $GF(q)$ 上的 k 次不可约多项式 $f(x)$ 在扩域 $GF(q^s)$ 中的根 α 是 $GF(q^s)$ 的一个本原元素，那么就称 $f(x)$ 为一个本原多项式，于是 s 次本原多项式共有 $\varphi(q^s-1)/s$ 个。特别地，如果 $s=1$ 和 $q=p^n$，那么在域 $GF(q)$ 中 n 次本原多项式共有 $\varphi(q-1)/n$ 个。如果 α 是 $GF(q^s)$ 的一个本原元素，那么 s 次多项式 $f(x)=\prod_{i=0}^{s-1}(x-\alpha^{**q^i})$ 就一定是一个本原多项式。

域 $GF(q^s)$ 中的一个 s 维向量 $\Omega=(\omega_1,\omega_2,\cdots,\omega_s)$ 称为此域关于域 $GF(q)$ 的基底，如果 $GF(q^s)$ 中的每个元素都可以表示成 $a=x_1\omega_1+x_2\omega_2+\cdots+x_s\omega_s$，这里 $x_i\in GF(q)$，$i=1,2,\cdots,s$。如果 α 是 $GF(q)$ 上 s 次本原多项式的根（即 $GF(q^s)$ 的一个本原元素），那么向量 $\Omega=(\alpha^0,\alpha^1,\cdots,\alpha^{s-1})$ 也构成域 $GF(q^s)$ 的一组基底，称之为自然基底。如果 A 是 $GF(q^s)$ 中的一个 $s\times s$ 阶可逆矩阵，Ω 是 $GF(q^s)$ 的一组基底，那么乘积向量 ΩA 也是 $GF(q^s)$ 的一组基底。

迹函数是最佳信号设计中经常用到的函数，它实际上是从扩域 $GF(q^n)$ 到基础域 $GF(q)$ 的一种特殊线性变换。对任意 $\beta\in GF(q^n)$ 迹函数在 β 处的值定义为

$$\mathrm{Tr}(\beta)=\sum_{i=0}^{n-1}\beta^{**q^i}。$$

定理 1.1.1.6 上面所定义的迹函数 $\mathrm{Tr}(\beta)$ 满足如下性质：

(1) 对任意 $a,b\in GF(q)$ 和 $x,y\in GF(q^n)$ 成立

$\mathrm{Tr}(ax+by)=a\mathrm{Tr}(x)+b\mathrm{Tr}(y)$，即迹函数是线性函数。

(2) $\mathrm{Tr}(\beta^{**q^i})=[\mathrm{Tr}(\beta)]^{**q^i}$，$i=0,1,2,\cdots$。

(3) $\mathrm{Tr}_1^{mn}(\beta)=\mathrm{Tr}_1^{m}[\mathrm{Tr}_m^{mn}(\beta)]$，这里为避免混淆将从扩域 $GF(q^{kt})$ 到基础域 $GF(q^k)$ 的迹函数记为 $\mathrm{Tr}_k^{kt}(x)$。

(4) 对任意 $a\in GF(q)$，方程 $\mathrm{Tr}(x)=a$ 在域 $GF(q^n)$ 中刚好有 q^{n-1} 个解 x。

(5) 特别地，从 $GF(2^n)$ 到 $GF(2)$ 的迹函数满足 $\sum_{a\in GF(q)}(-1)^{*}$

$*\ \mathrm{Tr}(\beta\alpha)=0$，对任意 $\beta\in\{GF(2^n)\setminus 0\}$。其中 $q=2^n$。

1.1.2 区组设计理论[4,5]

区组设计的内容十分丰富，历史也相当久远，这里仅简单地介绍一些最基本的概念和本书中将要用到的结论。

设 $S=\{s_1,s_2,\cdots,s_v\}$ 是一个 v 元集合，如果 S 上的一个 $v\times v$ 阶方阵 $A=(a_{ij})$ 满足条件：(1)矩阵 A 的每一行是 S 的一个无重全排列，(2)矩阵 A 的每一列也是 S 的一个无重全排列，那么就称矩阵 A 是 S 上的一个拉丁方。设 $B=(b_{ij})$ 是 S 上的另一个 $v\times v$ 阶拉丁方，如果元素组 (a_{ij},b_{ij})，$1\leqslant i,j\leqslant v$，跑遍集合 $S\times S$ 中的所有元素，那么就称拉丁方 A 和 B 是集合 S 上的一对 $v\times v$ 阶正交拉丁方，或说 A 和 B 正交。

设 S 是一个有限集合，$B_1,B_2,\cdots,B_b$ 是它的 b 个子集或 b 个无重排列。由这些子集组成的族 $B=\{B_1,B_2,\cdots,B_b\}$ 就叫做集合 S 上的一个区组设计，S 叫做该设计的基集，各 $B_i(1\leqslant i\leqslant b)$，叫做该设计的区组。$S$ 的诸元素的一种确定的安排就叫做 S 上的组合设计。需要强调的是每一个区组都是一个子集，或都是一个无重排列，其中无重复的元素，而区组族 B 则可以有重复的区组。此外区组设计的概念十分广泛，对区组、区组族和诸元素的安排方式几乎无限制。要使研究的问题对理论和实际有意义和作用，往往需要对它们加上适当的限制条件。下面就介绍一些满足不同限制条件的特殊区组设计。

设 B 是基集 S 上的一个区组设计。如果 B 有分解式

$$B=B_1\cup B_2\cup\cdots\cup B_r$$

使得对任意元 $s\in S$ 和任意足标 $j\in[1,r]$，s 恰在 B_j 的一个区组中出现，则这样的区组设计叫做一个可分解区组设计，简称为可分解设计。每一个 B_i 叫做一个平行联组或简称为联组，又叫做一个平行区组族或简称为平行族。

有限集合 S 的一个完全区组设计定义为 S 的满足一定条件的

若干个无重复排列的全体，其中每一个全排列叫做一个区组。例如考虑一个 $v\times v$ 阶拉丁方 A，它的每一行(或每一列)都可视为集 S 的一个全排列。因此一个拉丁方是一个完全区组设计。假如在完全区组设计中的所有全排列都是随机选取的，这时就称此完全区组设计为随机完全区组设计。下面重点讨论不完全的区组设计。

定义 1.1.2.1 设 $S=\{s_1, s_2, \cdots, s_v\}$ 是一个 v 元集。设 $B=\{B_1, B_2, \cdots, B_b\}$ 是 S 上的一个区组设计。如果 B 满足以下条件：

(1) 每个 $B_j(1\leqslant j\leqslant b)$ 中所含元素个数为常数 k，称之为区组的容量；

(2) 对 S 中的任意元 s，含 s 的 B 中子集的个数是一个常数 r，称之为 S 中元素在区组中的出现次数；

(3) 对 S 中的任意二元子集 $\{s_i, s_j\}$，包含该子集的 B 中子集的个数也是一个常数 λ，称之为 S 中二相异元的相遇次数；则称 B 是集合 S 上的一个平衡不完全的区组设计，或者更精确地称作一个 (b, v, r, k, λ)－平衡不完全区组设计，简称为 (b, v, r, k, λ)－设计。这里 b, v, r, k, λ 叫做设计参数。

所有区组的容量相同，以及 S 中任意元出现的次数相同且任一对相异元的相遇次数也相同，这就是设计的平衡性含义。平衡不完全区组设计又记为 *BIBD* 或 *BIB* 设计，这是由其英文名词第一个字母所组成的缩写形式。需要指出的是在定义 1.1.2.1 中条件(2)实际上可由条件(1)和(3)推出，因而可以略去。这里列出条件(2)是为了强调这一条件同时也是组合学文献的习惯。

设 $B=\{B_1, B_2, \cdots, B_b\}$ 是 v 元集 S 的一个 (b, v, r, k, λ)－设计，定义 B 的关联矩阵是一个 $b\times v$ 阶 0，1 矩阵 $A=(a_{ij}), 1\leqslant i\leqslant b, 1\leqslant j\leqslant v$。这里当 $s_j\in B_i$ 时，$a_{ij}=1$；当 $s_j\overline{\in} B_i$ 时，$a_{ij}=0$。利用关联矩阵可得如下一些基本结论。

定理 1.1.2.2 (b, v, r, k, λ)－设计中各参数之间必定满足恒等式 $bk=vr$ 和 $\lambda(v-1)=r(k-1)$。

此定理给出了平衡不完全区组设计存在的一个必要但非充分的

条件。为方便计，今后约定 J_v 表示元素全为 1 的 $v\times v$ 阶矩阵，I_v 表示 $v\times v$ 阶单位矩阵，W_v 表示元素全为 1 的 $v\times 1$ 阶矩阵。

定理 1.1.2.3 设 A 是一个 $b\times v$ 阶 0,1 矩阵。那么 A 是某个 (b,v,r,k,λ) - 设计的关联矩阵的充要条件是矩阵 A 同时满足关系式 $A^TA=(r-\lambda)I_v+\lambda J_v$ 和 $AW_v=kW_b$。

定理 1.1.2.4 (b,v,r,k,λ) - 设计中各参数满足以下不等式：$b\geqslant v$；$r\geqslant k$ 和 $(b+\lambda)/2\geqslant r\geqslant \max\{k,\sqrt{\lambda b},\lambda v/k\}$。

定理 1.1.2.5 设 A 是一个 (b,v,r,k,λ) - 设计的关联矩阵，则矩阵 $A^*=J_{b\times v}-A$，即矩阵 A 之补，是一个 $(b,v,b-r,v-k,b-2r+\lambda)$ - 设计的关联矩阵。称此两个设计为互补的设计。

由此定理可知在互补的一对设计中，总有一个的区组容量不超过 $v/2$，所以在构造 (b,v,r,k,λ) - 设计时，只需考虑 $k\leqslant v/2$ 的情形就够了。平衡不完全区组设计的构造方法千变万化而且一般来说技巧性都很强。目前人们已经找出了很多类不同的设计，已经知道具有如下参数的 (b,v,r,k,λ) - 设计都是存在的：

(1) $b=(3t+1)(2t+1)$，$v=6t+3$，$r=3t+1$，$k=3$，$\lambda=1$；

(2) $b=6t(t+1)$，$v=6t+1$，$r=3t$，$k=3$，$\lambda=1$，这里 $6t+1$ 是某个素数的幂次；

(3) $b=t(12t+1)$，$v=12t+1$，$r=4t$，$k=4$，$\lambda=1$，这里 $12t+1$ 是素数 p 的幂次并且有 $GF(v)$ 的一个原根 x 满足 $x^{4t}-1=x^q$，q 为奇数；

(4) $b=(3t+1)(4t+1)$，$v=12t+4$，$r=4t+1$，$k=4$，$\lambda=1$，这里 $4t+1$ 是某个素数的幂次；

(5) $b=2(t+1)(6t+5)$，$v=6t+6$，$r=6t+5$，$k=3$，$\lambda=2$；

(6) $b=2(2t+1)(3t+2)$，$v=6t+4$，$r=6t+3$，$k=3$，$\lambda=2$；

(7) $b=t(20t+1)$，$v=20t+1$，$r=5t$，$k=5$，$\lambda=1$，这里 $20t+1$ 是素数 p 的幂次并且有 $GF(v)$ 的一个原根 x 满足 $x^{4t}-1=x^q$，q 为奇数；

(8) $b=(5t+1)(4t+1)$，$v=20t+5$，$r=5t+1$，$k=5$，$\lambda=1$，这