

# 最佳信号设计的新进展

杨义先\*

(北京邮电大学信息工程系, 北京 100088)

**[摘要]** 随着当今信息社会的飞速发展,以各种光电信号为研究对象的一门综合性新学科——信号理论与设计,正在不断地发展和完善并受到国内外科技界越来越多的重视。作为这门新学科的一个重要分支,最佳信号设计的发展更为迅速。本文试图对最佳信号设计方面的部分新进展作一综述,并重点介绍作者近几年来在最佳序列和阵列设计方面的一些成果。

**[关键词]** 信号理论, 信号设计, 循环相关, 非循环相关, 汉明相关, 现代通信

## 1 引言

任何一个现代高科技系统都以先进的硬件设备为躯体,以优秀的软件为灵魂。高科技系统性能的提高既可采用硬件设备的更新换代,也可采用软件的改进和加强。在多数情况下,依靠软件的升级来提高系统性能更可以达到事半功倍之目的,甚至出现“四两拨千斤”之奇迹。本文将要介绍的最佳信号设计的本质思想就是要通过用更加先进合理的通信信号编码去代替过时的信号编码,其目的在于以最小的投入换取最大的效益。

以码分多址复用(CDMA)技术为基础的新一代移动通信系统将是下一世纪通信的主体。目前,以美国 Qualcomm 公司推出的 IS-95EIA/ITA 空中接口标准及其系统为代表的 CDMA 系统,在国际上掀起了一股研究应用 CDMA 多址方式的热潮,并迅速遍及世界各地。码型设计(即信号设计)是 CDMA 系统的一个关键。合适的码型能够极大地提高系统的性能,同时使系统易于实现。除了 CDMA 之外,最佳信号及其设计还在现代雷达、声纳、制导、空间测控及电子对抗等无线及有线系统的优化设计中扮演着越来越重要的角色。正是由于最佳信号设计的广泛性和重要性,过去几十年来世界各国的科学家和工程技术人员对此进行了长期不断的研究并取得了大批重要成果,目前仍在全面深入之中。需要指出的是,最佳信号本身并无严格的数学定义。在各种不同的工程领域中,由于实用背景的千差万别,对所用信号的需求标准也有差别。粗略地说,能满足某项工程的需要并使系统性能处于最优状态的信号就都统称为最佳信号,或者更准确地称为最佳离散信号。由此可见,某个信号是否最佳,仅是相对的而不是绝对的。其实,有时还会出现这种情况,对某类信号,当用一种工程标准去衡量时它可能是最佳的,但当改用另一种工程标准去衡量时,同一类信号可能就变成最差的了。我

---

青年科学基金资助项目。

本文于 1995 年 4 月 14 日收到。

\* 1994 年度“国家杰出青年科学基金”获得者。

们甚至可以断言：当前不存在，今后也不可能找到一类信号能同时满足所有工程标准的要求，因为有些工程要求之间本身就是互相抵触的。现今最主要的工程标准的要求是：循环相关，非循环相关和汉明相关等。下面我们将根据不同的工程标准来逐一介绍有关最佳信号设计方面的国际最新进展，以及作者自己的一些工作。

循环相关是目前应用最广泛、研究最深入的最佳信号准则，此方面的论文和专著已经不少而且也已经比较普及了，所以本文只是概括地作一些介绍。非循环相关的工程背景虽然很强，但其研究难度太大又缺乏必要的研究工具，正处于等待突破的阶段。由于扩频通信技术的军转民步伐加快，使得对各类跳频序列的需求矛盾越来越突出，由此促进了此方面的研究，本文也将对以汉明相关为标准的跳频序列设计新成果进行介绍。由于篇幅所限，本文不拟做全面详尽的介绍，最后列出的参考文献，希能有助于读者了解更多情况。

## 2 循环相关信号

在通信工程中碰到的许多问题都要求所处理的信号集至少具有如下两个条件或其中之一：(1) 信号集里的每一个信号都很容易与其自身的时延信号区分开来；(2) 信号集里的每一个信号都很容易与此信号集里的其它信号以及它们的时延信号区分开来。条件(1)对诸如遥测系统、雷达系统和扩频通信系统来说是十分重要的；而对同时遥测多个目标，多个终端系统识别和码分多址通信系统来说，条件(2)则更重要。在实用中，为了简化有关工程系统的具体实现过程，经常要求信号是周期性的。区分信号的一个最常用和最有用的测度是所谓的最小均方误差，即当两个信号之间的均方误差很大时，这两个信号就很容易彼此区分开来。人们已从理论上严格证明了：当信号的采样序列具有良好的循环相关特性时，信号与信号之间以及与其时延信号之间的均方误差就较大，从而可以利用带有相关接收器或匹配滤波器的导航和雷达系统等通信设备准确地提取出所需的信号或其时延。这便是循环相关为什么可以用作判别最佳信号的一个标准的工程背景。

设  $x = (x_0, x_1, \dots, x_{N-1})$  和  $y = (y_0, y_1, \dots, y_{N-1})$  是两个  $N$  长序列，对每个非负整数  $\tau$ ， $0 \leq \tau \leq N-1$  定义如下函数

$$R_{xy}(\tau) = \sum_{n=0}^{N-1} x_n y_{n+\tau}^*$$

为信号  $x$  和  $y$  之间的循环互相关函数，其中  $n+\tau$  理解为  $(n+\tau) \bmod N$ ，循环的含义就在于此。当  $x=y$  时，又称此函数为循环自相关函数。由此可见，两个信号之间的循环相关函数值实际上就是一个信号与另一个信号或其循环移位的复数共轭之间的内积。设计具有良好循环相关特性的信号集的任务就是要找出由若干个周期序列组成的信号集，使得它们满足以下两个条件之一或者同时满足：条件1，对集合中的每个序列  $x = \{x_n\}$ ，当  $1 \leq \tau \leq N-1$  时  $|R_{xx}(\tau)|$  要尽可能地小，即自相关函数要尽可能地接近于一个  $\delta$ -函数，或者说异相自相关函数值要尽可能地小；条件2，集合中两个不同信号之间的互相关函数的绝对值要尽可能地小，严格地说，对一切  $0 \leq \tau \leq N-1$ ， $x \neq y$  互相关值  $|R_{xy}(\tau)|$  要尽可能地小。在理论研究中，为了方便，人们常将“尽可能小”理解为零，但这种绝对理想的情形常常只是“一厢情愿”的，甚至是根本不可能的。在过去几十年中，国内外的专家学者们经过不断努力取得了不少突破性的成就，成功地设计出许多类同时具有良好循环自相关和互相关特性的序列和阵列集合，研究成果十

分丰富, 并已出版了数十部专著和众多的科技论文<sup>[1-12]</sup>。

按照信号元素的取值情况, 已有的循环相关离散信号可以分为两大类。第一大类是整值序列或阵列, 其特点是元素取值很简单, 比如: 只取+1或-1; 只取0或1; 只从某个有限域中取值(即多进制情形)等等。这一类序列或阵列的主要代表有: 平方剩余码, 辛格码, m-序列, 雅可比码, 霍尔码, 最佳二进阵列, Barker序列, Gold序列和移位寄存器序列等等。第二大类是复值或实值序列和阵列, 其特点是它的元素取自复数域或实数域中的任何一个部分。由于此类序列取值的复杂性, 它们更常用于模拟通信系统中。这类信号的主要代表有: FZC序列, Alltop序列, 三角序列和基于多项式的多相序列等等。

从设计方法来看, 目前所用的主要方法有: (1) 移位寄存器方法。这是工程中用得最多的方法, 它的优点是结构简单, 速度快, 成本低, 普适性强等。现在人们对移位寄存器特别是线性移位寄存器的研究已经比较成熟了。(2) 有限域方法。这是一种很先进的威力很大的方法, 其唯一的缺点是它需要有较深的数学基础, 一般的工程技术人员难以掌握和灵活使用。但随着有限域知识的逐步普及, 相信今后有限域方法将会发挥出越来越大的作用, 比如迹函数现在就已经比较广泛地用于循环相关信号的工程设计之中, 并已取得了不少有价值的成就。(3) 布尔函数方法。普通的工程技术人员几乎都或多或少地熟悉布尔函数, 所以这一方法的实用价值很大。目前采用布尔函数方法设计出的良好循环相关序列的代表是著名的 Bent序列。(4) 三角函数方法。只要用得巧我们完全可以用三角函数设计出一些性能良好的循环相关信号。比如<sup>[1,7]</sup>: 由如下 $(N-1)/2$ 个周期为 $N$ 的序列 $\{f_n = (f_n^{(0)}, f_n^{(1)}, \dots, f_n^{(N-1)}), 1 \leq n \leq (N-1)/2\}$ 组成的信号集就是一类同时具有良好循环自相关和互相关特性的实数序列, 其中对任意的 $1 \leq n \leq (N-1)/2$ 和 $0 \leq k \leq N-1$ ,  $f_n^{(k)}$ 由下面的三角函数所定义:  $f_n^{(k)} = \sqrt{2/N} \sin[(\pi/4) + 2\pi g(n)k/N]$ 。这里 $N$ 是一个奇数,  $g(n)$ 是 $\{1, 2, \dots, (N-1)/2\}$ 中的任意一个置换函数。(5) 多项式方法。人们最近发现利用多项式, 特别是一些低阶多项式, 可以设计出一批能使循环自相关和互相关同时达到理论最佳状态。比如<sup>[10]</sup>, 当取 $f(n)$ 是一个一阶多项式,  $g(n)$ 是一个二阶多项式时, 由公式:  $a_n^{(r)} = \alpha^{f(n)+rg(n)}, 0 \leq n \leq L-1$ 所定义的序列集 $A = \{a^{(r)} = (a_0^{(r)}, a_1^{(r)}, \dots, a_{L-1}^{(r)}); 1 \leq r \leq L-1\}$ 就是一类满足 Sarwate 上界的最佳循环相关信号。其中 $L$ 是一个大于3的素数,  $\alpha$ 是 $L$ 次单位复根。除以上几种主要方法之外, 常用的设计最佳循环相关信号的方法还有<sup>[1-5]</sup>: 数论方法; 矩阵方法, 这种方法在阵列设计等高维信号设计中尤为有用; 组合数学方法, 这主要是利用区组设计, 特别是循环差集设计, 来构造一些性能良好的信号。上述方法的技巧性要求较高。此外, 还有其它多种混合方法, 本文不再一一列举。

### 3 非循环相关信号

非循环相关准则与上述的循环相关准则的唯一区别在于此时信号已经不再是周期性的了, 相应地, 此时仅考虑非循环移位。换句话说, 在定义非循环相关函数时用非循环移位去代替循环相关中的循环移位。应该说, 非循环相关更加接近现实情形, 但因目前缺乏有效的研究工具, 使得非循环相关信号的设计难度很大。这里仅介绍一种具体的非循环相关最佳信号, 即 Costas 阵列。

设  $x = (x_0, x_1, \dots, x_{N-1})$  和  $y = (y_0, y_1, \dots, y_{N-1})$  是两个  $N$  长有限序列, 定义此

两个序列的非循环互相关函数为:  $\Theta_{xy}(\tau) = \sum_{n=0}^{N-1} x_n y_{n+\tau}^*$ ,  $0 \leq \tau \leq N-1$ 。需要指出的是, 当值  $n+\tau$  超过  $N$  时, 就将相应的  $y_{n+\tau}$  理解为零, 这就是与循环相关的主要区别。当  $x=y$  时, 就称之为非循环自相关函数。此定义当然可以直接推广到阵列信号的情形。下面将介绍的 Costas 阵列就是一个例子。首先介绍一下有关工程背景。

众所周知, 雷达和声纳信号常用于测试目标的距及其靠近或离开观察者的速度, 而距离既与信号时延时间成正比又与信号的频率移位成正比。在跳频雷达或声纳系统中, 从可能的频率集合  $\{f_1, f_2, \dots, f_m\}$  里选出一个或多个频率组成信号, 然后分别以时间间隔  $\{t_1, t_2, \dots, t_n\}$  发出这些信号。为方便计, 经常约定  $m=n$ 。于是可见此类信号可以用一个  $n$  阶置换矩阵  $A = |A_{ij}|$  来表示。这里  $n$  个行对应于  $n$  个频率  $\{f_i\}$ ,  $n$  个列代表  $n$  个时间间隔  $\{t_1, t_2, \dots, t_n\}$ ,  $A_{ij}=1$  的充要条件是在时间间隔  $t_j$  时发送频率  $f_i$ , 否则就取  $A_{ij}=0$ 。当这些发出的信号被目标反射回来时, 观察者只能收到原来信号在时间和频率上的延迟信号, 而且要根据这些延迟值确定出目标的距离和背向速度。为此, 观察者必须将收到的信号与已发出的信号备份进行比较。具体比较步骤是将备份信号的所有延迟重叠到收到的反射信号上, 再找出最一致的那个延迟信号, 而这里判定原信号与其延迟的“一致性”程度是由“1”被重叠的次数来确定的。用公式表示出来便是阵列  $A$  的二维非循环相关函数  $C_{\alpha\alpha} = \sum_{i,j=1}^n A_{ij} A_{(i+\tau)(j+\sigma)}$ 。在所有的  $n!$  个置换矩阵中, 并非每个都能用于上述的工程系统。最理想的情形是使此二维非循环相关函数的值始终不超过 1, 满足此条件的阵列就称为 Costas 阵列。目前有关此阵列的研究已经很丰富了, 此处仅介绍几种很有趣的构造方法:

构造法 1. 设  $p$  是一个素数,  $\alpha$  是  $GF(p)$  的本原元素, 对任意  $1 \leq i \leq p-1, 0 \leq j \leq p-2$ , 令  $A_{ij}=1$ , 当且仅当  $i=\alpha^j$ , 否则令  $A_{ij}=0$ , 那么  $A = [A_{ij}]$  就是一个  $(p-1)$  阶的 Costas 阵列。

构造法 2. 设  $\alpha$  是  $GF(q)$ ,  $q=p^m$  的一个本原元, 对任意  $1 \leq i, j \leq q-2$ , 令  $A_{ij}=1$ , 当且仅当  $\alpha^i + \alpha^j = 1$ , 否则令  $A_{ij}=0$ , 那么矩阵  $A = [A_{ij}]$  就是一个  $(q-2)$  阶的 Costas 阵列。

构造法 3. 设  $\alpha$  和  $\beta$  是  $GF(q)$  中的两个本原元, 对任意  $1 \leq i, j \leq q-2$ , 令  $A_{ij}=1$ , 当且仅当  $\alpha^i + \beta^j = 1$ , 否则令  $A_{ij}=0$ , 那么矩阵  $[A_{ij}]$  便是一个  $(q-2)$  阶的 Costas 阵列。

#### 4 汉明相关信号

在一个战术战场上, 分布着许多跳频电台, 由于各用户跳频起始相位的不同和传输时延的差异等原因, 在某一时隙可能有几个用户的信号载频跳到同一个频隙上造成频隙重合干扰, 使接收机的解调输出发生误差。频隙重合也称为击中或碰撞, 用公式表示便是汉明相关。设  $x = (x_0, x_1, \dots, x_{L-1})$  和  $y = (y_0, y_1, \dots, y_{L-1})$  是两个  $L$  长的跳频序列, 记  $h[x_j, y_{j+\tau}] = 1$ ,  $AHtx_j = x_{j+\tau}$ ,  $A7qTr = 0$ , 那么  $x$  与  $y$  之间的汉明互相关定义为:  $H_{xy}(\tau) = \sum_{j=0}^{L-1} h[x_j, y_{j+\tau}]$ ,  $0 \leq \tau \leq L-1$ , 这里  $j+\tau$  按  $(j+\tau) \bmod L$  理解。不难看出, 汉明相关值  $H_{xy}(\tau)$  表示两个跳频序列  $x$  和  $y$  在相对时延为  $\tau$  时, 在一个序列周期里发生频隙重合次数。显然  $H_{xy}(\tau)$  越小, 两个跳频序列之间的重合次数就越小, 也就是两个用户之间的相互干扰就越小, 这便是汉明相关的物理背景之一。当  $x=y$ , 即两个序列相同时, 称  $H_{xx}(\tau)$  为序列  $x$  的汉明自相关函数。

为了使跳频序列的性能最佳,通常要求尽可能地满足如下条件:(1) 每一个跳频序列都可以使用频隙集合中的所有频隙,以实现最大的处理增益;(2) 跳频序列集合中的任何两个跳频序列在所有相对时延下发生频隙重合次数尽可能小,也就是它们的汉明互相关的最大值要尽可能小;(3) 每个序列与其平移序列的频隙重合次数尽可能小,也就是说其汉明自相关的最大值尽可能小;(4) 为了向用户提供更多的选择,实现多址通信,要求跳频序列集合中的序列个数尽可能多;(5) 在某些工程中还要求跳频序列能控制实现宽间隔跳频,即要求在相邻的跳频时隙里发射的两个载波的频率间隔大于某个规定的值;(6) 为了使跳频系统具有良好的抗干扰性能,应使各频隙在一个序列周期中的出现次数基本相同,这称为均匀性;(7) 跳频序列应具有较好的随机性和较大的线性复杂度,使得敌人不能利用以前传输的频率信息来预测当前和以后的频率。在跳频通信地址编码研究方面的新成果主要体现在各种新的理论界限的发现和最佳跳频码的设计新方法这两个方面<sup>[6]</sup>。

现已新发现的比较有价值的跳频码理论界限主要有:

(1) 任何长度为  $L$  的  $q$  元跳频序列的异相汉明自相关最大值至少为

$$(L - L \bmod q)(L + L \bmod q - q) / [q(L - 1)];$$

(2) 在同步组网时,最多能构造出  $q^{k+1}$  个跳频序列,使得任意两个序列间的重合次数不大于  $k$ ;

(3) 如果信号集合中含有  $q^{k+1}$  个等长  $q$  跳频序列,那么序列的长度不会超过  $k(q^{k+1} - 1) / (q^k - 1)$ , 这里  $k$  表示集合中任意两个序列间的最大重合次数;

(4) 同步组网时最多能构造出  $q(q-1)(q-2)\cdots(q-k)$  个  $q$  元非重复跳频序列,使得其中任意两个序列间的重合次数不大于  $k$ ;

(5) 在异步组网时,最多能构造出  $q(q-1)(q-2)\cdots(q-k)/L$  个  $L$  长的  $q$  元跳频非重复序列,使得任意两个序列间的汉明互相关值不超过  $k$ 。

当前新构造出的性能良好的跳频序列类就更多了,其中最具代表性的是:基于同余式的跳频序列;基于置换多项式的跳频序列;基于  $M$ - 和  $m$ - 序列的跳频序列;基于  $R$ - $S$  码的跳频序列;基于布尔函数的跳频序列和其它若干种宽间隔跳频序列等<sup>[6,15-17,1]</sup>。

## 5 结束语

作者于1991年获得国家自然科学基金青年基金资助,首次承担了有关最佳信号研究与设计的科技攻关任务,并已提前超额完成。该项目的主体是关于现代密码和编码的研究,本文所介绍的最佳信号设计也是其中的一个重要部分。文献 [18, 20] 报道了该项目有关并元相关最佳信号的研究和设计的内容。该项目结题后,获1993年邮电部科技进步一等奖。

## 参 考 文 献

- [1] 杨义先,林须端. 编码密码学. 北京:人民邮电出版社,1992.
- [2] 杨义先. 最佳信号理论与设计. 北京:人民邮电出版社,1995.
- [3] 钟义信. 伪噪声编码. 北京:人民邮电出版社,1979.
- [4] 肖国镇等. 伪随机序列及其应用. 北京:国防工业出版社,1985.
- [5] 斯维尔德利克 M B 著,郭桂蓉译,最佳离散信号. 北京:国防工业出版社,1984.

- [6] 梅文华, 杨义先. 跳频通信地址编码理论. 北京: 国防工业出版社, 1995.
- [7] Yang Yixian. Real Sequences with Good Autocorrelation and Cross-correlation. *J. of Electronics*, 1991, **8** (1): 68-76.
- [8] Yang Yixian. Generalized Legendre Sequences with Perfect Periodic Autocorrelation. *Shanghai Conference on Design, Codes and Finite Geometries*, 1993: 23-25.
- [9] 杨义先. 准最佳二进制阵列. *电子学报*, 1992, **20** (4): 37-44.
- [10] Yang Yixian. On Perfect Binary Arrays. *J. of Electronics*, 1990, **7** (2): 175-181.
- [11] Yang Yixian. On Pseudorandom Sequence (II) — Spectrum Properties. *Selected Papers for the Journal of BUPT*, 1991, **2** (1): 31-39.
- [12] Yang Yixian. Optical Orthogonal Codes. *Chinese J. of Electronics* 1991, **1** (1), 72-78.
- [13] Yang Yixian. On Costas Arrays. *J. of Electronics*, 1992, **9** (1): 17-25.
- [14] Golomb S, Taylor H. Algebraic Constructions for Costas Arrays. *J. of Comb. Theory, Ser. A*, 1984; **37** (1): 13-21.
- [15] Yang Yixian. A New Method for Designing Full Frequency Hop Codes. *J. of Electronics*, 1993, **10** (2): 132-138.
- [16] 杨义先. 跳频码设计新方法. *电子科学学刊*, 1992, **14** (6): 588-595.
- [17] 杨义先. 具有良好汉明相关特性的新序列. *通信学报*, 1995, **16** (1): 68-71.
- [18] 杨义先, 胡正名. 单值并元相关函数码. *电子学报*, 1988, **16** (6): 50-55.
- [19] 胡正名, 杨义先. 并元码的进一步研究. *通信学报*, 1989, **10** (5): 42-46.
- [20] 胡正名, 杨义先. 并元码的并元互相关特性. *通信学报*, 1993, **14** (1): 15-21.

## PROGRESSES IN PERFECT SIGNAL DESIGN

Yang Yixian

*(Department of Information Engineering, Beijing University of Posts and Telecommunications, Beijing 100088)*

**Abstract** With the rapid development of our modern information society, a new project, the theory and design of signals (TDS), is becoming more and more important. TDS concentrates on various optical and electronical signals used in different areas. Perfect signal design is one of the best finished branches of TDS. The aim of this paper is to review some new progresses in perfect signals design, including those made by the author himself.

**Key words** signal theory, signal design, cyclic correlation non-cyclic correlation, Hamming correlation, modern communications