全国高技术重点图书 • 通信技术领域

并元理论及其应用

杨义先　许成谦　胡正名　著

人民邮电出版社

全国高技术重点图书·通信技术领域

并元理论及其应用

杨义先　许成谦　胡正名　著

人民邮电出版社

图书在版编目(CIP)数据

并元理论及其应用/杨义先,许成谦,胡正名著．北京:人民邮电出版社,2002.6

全国高技术重点图书·通信技术领域

ISBN 7-115-10211-2

Ⅰ.并 … Ⅱ.①杨 …②许 …③胡 … Ⅲ.密码－理论 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2002)第 013111 号

全国高技术重点图书·通信技术领域

并元理论及其应用

◆ 著　　杨义先　许成谦　胡正名

责任编辑　陈万寿

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号

邮编　100061　电子函件　315@ptpress.com.cn

网址　http://www.ptpress.com.cn

读者热线　010-67180876

北京汉魂图文设计有限公司制作

北京隆昌伟业印刷有限公司印刷

新华书店总店北京发行所经销

◆ 开本：850×1168　1/32

印张：8.75

字数：227 千字　　2002 年 6 月第 1 版

印数：1-3 000 册　　2002 年 6 月北京第 1 次印刷

ISBN 7-115-10211-2/TN·1860

定价：24.00 元

内容提要

本书是国内外第一本比较系统地介绍作者及国内外学术界在并元理论与应用方面的研究成果的学术专著。全书共分6章，分别介绍并元运算及并元群、并元区组设计、Walsh函数和Walsh变换、Hadamard矩阵、并元微积分、并元信号的分析和综合以及与并元码密切相关的Bent函数。

本书层次分明，内容取舍得当，广度与深度之间的关系处理得体，可以作为国内网络安全、信息安全、计算机安全等领域相关人员的技术培训教材，还可以作为通信与电子系统、信号与信息处理、密码学、信息科学、应用数学等专业的大学生和研究生的教学参考书。本书还可作为国内众多安全公司的技术人员提高理论水平的实用工具书。

作者简介

杨义先，1983 年 7 月毕业于成都电讯工程学院应用数学专业，1986 年 7 月获北京邮电学院应用数学专业硕士学位，1988 年 12 月获北京邮电大学电子与通信系统专业博士学位。1992 年 10 月至今任北京邮电大学教授。1993 年至今任北京邮电大学信号与信息处理专业博士生导师。从事信息安全、信号与信息处理、密码学专业的教学、科研和成果转化工作。已发表论文 300 余篇、出版著作 10 余部。杨教授与本书相关研究成果曾获 1992 年邮电部科技进步奖一等奖、1991 年国家教委科技进步奖二等奖、1997 年国家教委科技进步奖二等奖、1997 年军队科技进步奖二等奖、1997 年邮电部科技进步奖一等奖。

许成谦，1984 年 7 月毕业于东北师范大学数学专业，1994 年 4 月获北京邮电大学应用数学专业硕士学位，1997 年 4 月获北京邮电大学信号与信息处理专业博士学位。1997 年 5 月至今历任燕山大学副教授、教授、博士生导师。从事信号与信息处理、通信与电子系统专业的教学和科研。已经发表论文 50 余篇。

胡正名，北京邮电大学教授，博士生导师，全国政协常委。胡教授是我国最早从事并元理论研究的学者之一，已经在并元理论及其应用方面取得了一大批具有国际先进水平的科研成果。

序

并元理论起源于20世纪60年代末70年代初，当时，人们发现以Walsh-Hadamard变换为代表的非正弦正交变换在处理离散信号时的综合性能远远好于传统的傅里叶变换，而绝大部分非正弦正交变换都以并元理论为基础。于是，国内外众多学者开始从事并元理论的研究，并发表了数以千计的高水平学术论文。但是，由于其自身的理论难度以及缺乏系统的研究方法和体系，致使国内外至今仍然没有一本专著对并元理论进行过系统的阐述，这不能不说是此领域内的一件憾事。幸好，本书作者始终坚持不懈地从事并元理论及其应用方面的研究，并巧妙地抓住了并元运算“不进位”这个“纲”，从而将众多看似各不相关的结果有机地融为了一体，终于形成了国内外在此方面的第一本专著，填补了一个既有很高理论价值，又有丰富应用背景的空白。因此，《并元理论及其应用》是一本难得的好书，它结束了过去近30年来，国际上在此领域内“有论文，无专著”的历史。

本书是胡正名教授、杨义先教授、许成谦教授师徒三代历经20余年潜心研究的结晶，也是他们参加并完成的十余个国家级和省部级重大科研项目成果的精华之汇集。本书比较全面地总结了并元基础理论、典型的并元系统(Walsh函数与Hadamard变换)、并元微积分、并元信号设计与处理以及并元区组设计等方面的理论和应用成果，而且还详细介绍了并元理论在信号处理、纠错编码和保密通信等方面的众多应用。书中不少内容都是作者自己的研究成果。本书的理论水平很高，许多章节的内容都达到了国际先进水平。本书的应用价值也很大，它对密码理论与技术、离散信号和纠错编码等都有较好的指导意义。本书的特点主要体现在以下几个方面：

(1) 学术水平高,应用价值大;
(2) 内容丰富,层次分明;
(3) 文笔流畅,取舍恰当;
(4) 构思新颖。

希望本书的出版能够激发大量的理论与应用后继研究。

中国工程院院士

2001 年 10 月于北京邮电大学

前　言

并元理论是建立在并元运算基础上的一套应用数学理论。从1971年至今，并元理论正迅速走向成熟。特别是并元代数理论、并元分析理论、并元矩阵理论等分支已经比较完善。但是由于各种原因，并元理论的“知名度”目前还不够高，很多学者还不十分了解它。为此本书将对并元理论与应用做比较系统的介绍。

并元理论基本上就是以并元运算去代替常规的四则运算而产生的一种新理论。并元运算是一种不进位运算。并元运算，特别是并元加法有广泛的工程实用背景。比如，任何一个序列密码体制的加密其实就是密文序列与密钥序列之间的并元相加，而其脱密过程刚好是密文序列与密钥序列之间的并元相加；数字通信系统中，噪声对信道的干扰过程实际上就是噪声序列与信息序列之间的并元相加过程；逻辑电路中的异或运算也是一种典型的并元相加运算；因此布尔函数相加实际上就是它们的真值表之间的并元相加。在第一章我们首先介绍并元四则运算，然后介绍包含并元运算的并元群论、并元区组设计理论。

在经典的傅里叶分析中是以三角函数为完备正交系对信号进行逼近和分析。而在并元理论中是以Walsh函数为完备正交系对信号进行逼近和分析。在数字技术迅速发展的今天，由于Walsh函数和Walsh变换特别适合数字信息的处理，因此以Walsh函数和Walsh变换为重要内容的并元理论在电子和通信领域将有广泛的应用前景。在第二章我们首先由并元运算给出Walsh函数的定义，然后给出Walsh函数的一些等价定义和重要性质。最后介绍Walsh矩阵及其快速构造、Walsh变换及其快速算法、信号的Walsh频谱特性以及Walsh滤波。

沃尔什矩阵实质是 Hadamard 矩阵的特殊形式。由于 Hadamard 矩阵在电子和通信工程中的广泛应用,同时也为了拓展并元理论的研究范围,在第三章我们将介绍 Hadamard 矩阵的重要结果。特别是要介绍 Hadamard 矩阵的布尔函数研究方法。

并元四则运算是并元理论的基本运算。通过基本的并元运算我们可以定义出并元微分运算和并元积分运算。并元微积分不但可以作为一种处理方法用于信号分析之中,而且在数学分析领域内也具有特殊作用。在第四章我们介绍连续函数和离散函数的并元微分和并元积分运算、函数的并元微分与并元积分的关系、广义并元导数与广义 Walsh 变换的关系以及广义并元导数的应用。

在最佳离散信号的设计过程中如何使信号的相关函数尽可能地逼近一个脉冲函数是一个十分重要的问题。从物理意义上讲,使相关函数逼近脉冲函数的主要目的是使我们能够很容易地将信号与它的移位信号区分开来。信号的移位是多种多样的。除了最常见的循环移位外还有诸如并元移位和 Walsh 移位等等。怎样设计离散信号才能使我们可以很容易地将信号与其并元移位信号区分开来呢? 也就是说怎样才能使信号的并元相关函数尽可能地逼近脉冲函数呢? 这就是第五章要介绍的问题。在第五章我们介绍并元相关函数的性质、并元码、并元码的并元矩阵研究方法、并元码的并元区组设计研究方法以及并元码的推广形式——并元互补序列族。

Bent 函数是一种特殊的布尔函数。利用 Bent 函数可以构造出一些循环相关性和线性复杂度都很好的最佳离散信号。最后介绍 Bent 函数的推广形式——Bent 互补函数族。

本书的部分内容取自作者的博士学位论文和已发表的论文。这些内容也是国家重点基础研究发展规划项目(编号:G1999035805)、国家杰出青年基金项目(批准号:69425001)、国家自然科学基金项目(批准号:69882002,60073049)、高校骨干教师资助计划项目和河北省自然科学基金资助项目(编号:699245)所进行的研究课题的一部分。

从本书可以看到,并元理论具有丰富的内容。但是还有很多问

题需要进一步研究。可以说并元理论是需要进一步完善的理论。我们将这本书奉献给读者，希望能给并元理论的进一步研究提供参考。但是由于我们水平有限，书中难免有不妥之处，恳请读者指正。

作者

目　录

第一章　并元理论基础

1.1　并元运算

实数的并元运算与实数的二进制表示密切相关。我们首先介绍实数的二进制表示。

设 a 是一个非负实数，如果

$$a = \sum_{j=-\infty}^{N-1} a_j 2^j \tag{1.1}$$

其中 $a_j = 0, 1, j = N-1, N-2, \cdots$，那么我们可以将 a 写为二进制表示

$$a = (a_{N-1}, a_{N-2}, \cdots, a_1, a_0; a_{-1}, a_{-2}, \cdots) \tag{1.2}$$

由式(1.1)可见，a_j 中带有非负下标的数字对应于 a 的整数部分，而带有负下标的数字对应于 a 的小数部分，两者之间用分号隔开。有时也把 a 简写为 $a = (a_j)$。

二进制数可分为二进制有理数与二进制无理数两类。对于一个实数，若它的二进制表示中从某位数字开始全是 0 或全是 1，则称其为二进制有理数。否则称其为二进制无理数。例如，$\frac{1}{2}$ 的二进制表示为(0;1000…)或(0;0111…)，$\frac{5}{8}$ 的二进制表示为(0;101000…)或(0;100111…)，因此 $\frac{1}{2}$、$\frac{5}{8}$ 都是二进制有理数。而 $\frac{1}{3}$ 的二进制表示为(0;010101…)，因此 $\frac{1}{3}$ 是二进制无理数。容易看出，若 a 是二进制无理数，它的二进制表示中一定出现无穷多个 0 与无穷多个 1。

对于一个二进制有理数，若它的二进制表示中从某位数字开始

全是0,则称此数的二进制表示为有尽表示。这时在记法上可以将这些0略去。例如,$\frac{1}{2}=(0;1)$,$\frac{5}{8}=(0;101)$。特别是对于非负整数,我们采用略掉";"号的有尽表示。例如,19=(10011)。

负数的二进制表示为它的绝对值的二进制表示添上负号。

有了实数的二进制表示下面我们可以定义实数的并元运算[1,2]。

定义 1.1 两个用二进制表示的非负实数 $a=(a_j)$,$b=(b_j)$的并元加法(并元和)仍然是一个非负实数,其值定义为$((a_j+b_j)\mod 2)$,记为 $a\oplus b$,即

$$a\oplus b=((a_j+b_j)\mod 2) \tag{1.3}$$

由定义1.1可知,两个实数 a 与 b 的并元和是这样的一个实数,它的二进制表示的第 j 位数字是 a 与 b 的二进制表示的相应(第 j 位)数字的模2加。通常我们先求出 $a\oplus b$ 的二进制表示,然后再转换成十进制数。例如

$$5\oplus 3=(101)\oplus(011)=(110)=6$$

$$9\oplus 4=(1001)\oplus(0100)=(1101)=13$$

$$12.5\oplus 5.25=(1100;1)\oplus(101;01)=(0101;11)=5.75$$

注意,任意两个数的并元加法与平常的模2加法意义不同。例如,依模2加法,$5+7=0(\mod 2)$,而 $5\oplus 7=2$。但是限制在基本集$\{0,1\}$中时,两者结果是相同的。

并元加法满足如下性质:

性质 1.1 交换律 $a\oplus b=b\oplus a$。

性质 1.2 结合律$(a\oplus b)\oplus c=a\oplus(b\oplus c)$。

性质 1.3 $a\oplus b\leqslant\max\{a,b\}$。此性质表明并元加法是不进位的。

定义 1.2 两个用二进制表示的非负实数 $a=(a_j)$,$b=(b_j)$的并元减法(并元差)用 $a\ominus b$ 表示,其值定义为

$$a\ominus b=((a_j-b_j)\mod 2) \tag{1.4}$$

因为对于二进制表示的非负实数 $a=(a_j)$和 $b=(b_j)$,a_j-

$b_j \bmod 2 = a_j + b_j \bmod 2$，所以在二进制表示中 $a \oplus b = a \ominus b$。

定义 1.3 如果两个非负实数 a, b 的二进制表示分别为

$$a = (a_r \cdots a_1 a_0 ; a_{-1} a_{-2} \cdots)$$

$$b = (b_s \cdots b_1 b_0 ; b_{-1} b_{-2} \cdots)$$

那么 a 与 b 的并元乘法(并元积)用 $a \odot b$ 表示，其值定义为

$$a \odot b = \bigoplus \sum_{k=-s}^{r+1} a_{k-1} b_{-k} \tag{1.5}$$

其中 $\bigoplus \sum$ 表示相加的和按模 2 计算结果。

定义 1.3 中定义的两个非负实数的并元积可以这样直观理解：如果 a 和 b 的二进制表示分别为

$$a = (a_r \cdots a_1 a_0 ; a_{-1} a_{-2} \cdots)$$

$$b = (b_s \cdots b_1 b_0 ; b_{-1} b_{-2} \cdots) \tag{1.6}$$

将 a 的二进制表示按原来次序写出。而将 b 的二进制表示按原来相反方向次序写出，两者小数点(;)对齐成下列格式

$$a_r \quad \cdots \quad a_1 \quad a_0 \; ; \; a_{-1} \, a_{-2} \cdots \, a_{-s-1}$$

$$b_{-r-1} \cdots \, b_{-2} \, b_{-1} ; \; b_0 \quad b_1 \quad \cdots \, b_s$$

将上下对应数字相乘，然后再并元相加，所得到的结果就是 $a \odot b$。例如：设 $a = 7.25, b = 4.875$，则 $a = 7.25 = (111;01)$，$b = 4.875 = (100;111)$，$a \odot b = (1 \times 1) \oplus (1 \times 1) \oplus (1 \times 1) \oplus (0 \times 0) \oplus (1 \times 0) \oplus (0 \times 1) = 1$。

并元乘法具有下列性质。

性质 1.4 并元乘法满足交换律，即 $a \odot b = b \odot a$。

证明

$$\begin{aligned} & a \odot b \\ = \; & a_{-s-1} b_s + \cdots + a_{-2} b_1 + a_{-1} b_0 + a_0 b_{-1} \\ & + a_1 b_{-2} + \cdots + a_r b_{-r-1} \\ = \; & a_r b_{-r-1} + \cdots + a_1 b_{-2} + a_0 b_{-1} + a_{-1} b_0 \\ & + a_{-2} b_1 + \cdots + a_{-s-1} b_s \end{aligned}$$