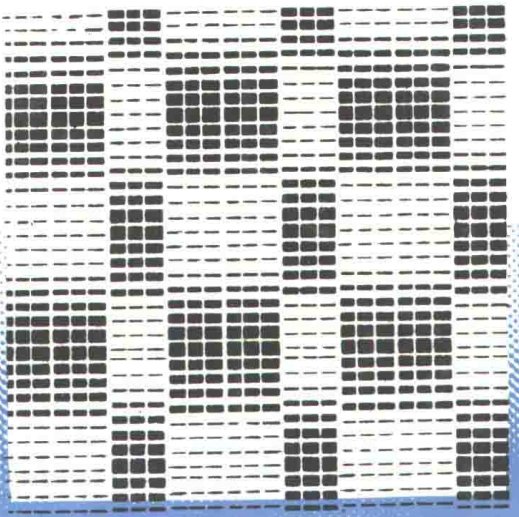

信息处理丛书·信息处理丛书

快速算法

蒋增荣 曾泳泓 余品能 编著

国防科技大学出版社

快速算法

蒋增荣　曾泳泓　余品能　编著

国防科技大学出版社

[湘] 新登字 009 号

内 容 简 介

快速算法是数字信号处理的支柱。本书是我国第一本综合论述数字信号处理中快速算法设计与分析的著作。它深入而系统地论述了卷积和离散富里叶变换的各种经典和现代的快速算法，Winograd 富里叶变换算法，多项式变换及其应用，离散余弦变换和 W 变换的快速算法，有关 Toeplitz 矩阵及 Toeplitz 系统的快速算法，格与树搜索的快速算法等。本书所论及的算法，大部分已在实际应用中起着非常重要的作用。

本书的宗旨是介绍数字信号处理中重要问题的最好快速算法，同时让读者懂得设计快速算法的一般技巧。本书可供无线电技术、电子工程、计算机与信息科学、计算数学以及相近专业的高年级学生、研究生、教师阅读，也可供广大科技工作者参考。

·信息处理丛书·

快 速 算 法

编　　著：蒋增荣　曾泳泓　余品能

责任编辑：胡见堂

责任校对：朱宝龙

*

国防科技大学出版社出版发行

新华书店总店科技发行所经销

国防科技大学印刷厂印装

*

开本：850×1168　1/32　印张：17.5　字数：439 千

1993 年 12 月第 1 版第 1 次印刷　　印数：2000 册

ISBN　7－81024－285－7

O·29　　定价：16.00 元

前　言

信号处理是一门内容非常广泛，界限又不十分明确的边缘学科，位于电子学、计算机科学、通信、数学等学科的结合部，已广泛应用于雷达、声纳、地震勘探、通信、医疗、气象、射电天文学等许多方面，具有非常广阔的应用前景，目前正呈蓬勃发展之势。微电子技术的发展是促使数字信号处理技术进一步飞速发展的重要因素，目前，各种数字信号处理器，即专用的信号处理计算机正在开发，有的已投放市场，用超大规模集成电路来制造数字信号处理器，已成为热门话题，所有这些，进一步促进了数字信号处理技术在更多领域中的广泛应用。除此之外，巧妙地设计算法可以满足更高的要求，因此，快速算法是数字信号处理技术的另一支柱，人们不会忘记，正是 Cooley－Tukey 的快速富里叶变换(FFT)将数字信号处理推向了一个新的高度，使数字信号处理技术走向实用。

数字信号处理就其理论来讲是一些算法的集合，因而有人将其列入计算数学的一个分支。国内外许多有成就的数学家正在从事这方面的研究。在这门学科中许多问题要研究其快速算法，否则便难以实现，例如离散富里叶变换(DFT)，卷积和相关，矩阵运算，滤波，编码与译码等无不如此。目前，这个领域发表的论文已浩如烟海，要全面地反映在一本书中是难以做到的。为此，本书着重讨论这些问题：卷积和 DFT 的快速算法，多项式变换，离散余弦(正弦)变换，W 变换(包括 Hartley 变换)以及广义富里叶变换的快速算法，Toeplitz 矩阵的快速算法，格和树搜索的快速算法。卷积和 DFT 是数字信号处理中最为重要的两个计算问题，而且两者关系

密切，也是目前研究最多、最为深刻、成果也最多的两个问题，本书理所当然地让它们占有较多的篇幅。现在已经有了许多快速计算卷积和 DFT 的方法，其中 Winograd 算法和多项式变换算法尤为重要，本书辟有专门的章节详细讨论这两种现代的方法，旨在进一步推广它们。离散余弦变换和 W 变换在某些应用领域已经证明比传统的 DFT 效果更为明显，特别可避免 DFT 不可避免的复数运算，近年来引起了人们普遍的关注，国外已有专著出版，但国内尚未在有关书籍中论及，本书对这两种变换的快速算法作了全面的论述。在平方滤波等方面，Toeplitz 矩阵起了关键作用，本书全面论述了关于 Toeplitz 矩阵以及 Toeplitz 系统的快速算法。格与树的搜索对于译码、神经网络等有重要的作用，本书介绍了最基本的搜索算法。

本书的宗旨是给读者介绍数字信号处理中重要问题的最好快速算法，同时让读者懂得设计快速算法的一般技巧。有鉴于此，本书特别重视算法设计原理的论述。对每一个算法，均详细地论述了它是如何构造出来的，并且分析了其时间复杂性，明确地给出了计算步骤，有的还给出了计算机上实现的方法。这是本书有别于其它同类书籍的地方。此外，本书所论及的算法，大部分已在实际应用中起着非常重要的作用。但是，对于这些算法的多方面实际应用，以及由此产生的有效字长，舍入误差以及最佳计算环境等，本书均未涉及，对这些领域作广泛的阐述，势必大大增加篇幅，也是作者力所不及的。作者认为，这样做反而失去了专论快速算法的清晰面目。对于工科学生以及一般的工程技术人员，要充分理解本书内容，还需要一些抽象代数、数论与多项式理论的知识。所有这些，希望读者参考其它有关文献。

作者多年来长期从事快速算法的教学与研究工作，对计算数学专业的研究生开设过多次“快速算法及其应用”的课程。同时结合银河—Ⅱ巨型计算机的软件研制及国防“八五”预研的科研项

目，对数字信号处理中的快速算法从理论到软件设计作过深入的研究，本书包含了作者的一些研究成果和实践经验，相信对读者有所裨益。本书写作过程中，参阅了国内外许多作者的论文及著作，特别是 H. J. Nussbaumer 和 R. E. Blahut 的专著，吸取了其中部分材料。在此深表谢意。

本书由蒋增荣、曾泳泓、余品能合作完成。第二、三、四章由蒋增荣撰写，第一、六章由曾泳泓撰写，第五章由蒋增荣与曾泳泓合写，第七章由余品能撰写。

限于水平，书中错误难免，恳请读者批评指正。

致谢　感谢何振亚先生、姚天任先生、胡光锐先生，他们对本书内容和结构提出了有益建议。

作　者
于国防科技大学
1993. 4

将增荣　1937年生，江苏宜兴人。1962[illegible]事工程学院，现任国防科技大学系统工程与数学系教授，特殊津贴获得者。出版过《数论变换》、《多项式变换及其应用》、《并行算法》等三部著作，其中《并行算法》获得1993年第七届“中国图书奖”，发表论文40余篇。主要从事快速算法、并行算法、数论与计算数论等方面的科研与教学工作。

曾泳泓　1962年生，湖南邵东人。1983年毕业于北京大学数学系，1986年在国防科技大学应用数学专业获硕士学位。现任国防科技大学七系副教授。曾获部委级科技进步二等奖2项。曾参与《多项式变换及其应用》的编撰工作。在国内外学术刊物发表论文20余篇。近年来主要从事信息处理的快速算法和并行算法、计算数论与计算机密码学的研究与教学。

余品能　1963年生，江苏宜兴人。1985年毕业于南京师范大学数学系，1988年获国防科技大学理学硕士学位，现任南京工程兵工程学院副教授。发表学术论文约20余篇。目前主要从事快速算法、算法复杂性理论、应用线性代数方面的教学和科研工作。

ISBN 7-81024-285-7

9 787810 242851 >

ISBN　7-81024-285-7
O·29　定价：16.00元

·目　　录·

第一章　卷积的快速算法

第四章　多项式变换及其应用

第五章　其它离散变换及其快速算法

第一章　卷积的快速算法

卷积（Convolution）是数字信号处理中最常见的计算问题，数字滤波、相关甚至离散 Fourier 变换（DFT）都可以变成卷积的计算。在数字信号处理之外的领域也经常遇到。对卷积的快速算法研究受快速富里叶变换（FFT）的刺激而得到了快速发展。FFT 算法可用于计算卷积，并使 N 点序列的卷积的运算量从 $O(N^2)$ 减少为 $O(N\log N)$ *，大大提高了卷积的计算速度。然而用 FFT 计算也有一些缺点，如复运算，不能精确计算，计算长度受限制等。尽管后来提出了另外一些变换，如数论变换、多项式变换等，亦可用于计算卷积，并克服了用 FFT 计算的一些缺点，但同时又增加了新的麻烦。大约在本世纪70年代中后期，以 Winograd 及 Agarwal－Cooley 等为代表的人物提出了计算卷积的另一种方法，这种方法是首先建立短卷积的乘法运算量最少的算法，即人们常说的 Winograd 短卷积算法，然后利用嵌套或迭代的技巧计算长卷积及多维卷积。同变换方法相比，这种算法的运算量很多情况下更少，并可克服变换方法的某些限制。当然，也由于算法结构相对变换方法复杂一些而增加了实现的难度。本章要介绍的就是这一类算法，并统一用多项式代数对算法进行描述。至于计算卷积的变换方法，本书的后续章节中将会讲到。

---

* 本章 log 若无特别说明，均指以2为底的对数

§1 卷积及其等价形式

在数字信号处理及其它学科中，由于用途不同，卷积有多种形式。常见的有循环卷积、斜循环卷积、线性卷积等，我们将不讨论这些卷积的实际背景及其用途，只讨论其形式定义及算法。上述卷积都可用多项式相乘表示，这样，就可统一地利用多项式代数来研究它们的快速算法。

尽管本章中大部分内容与卷积所在的数域没有关系，但也有些地方与数域有关。因此，下设 F 为一个数域，所讨论的是数域 F 中卷积。在实际应用中，F 通常为实数域、复数域或有限域。

[**定义1.1**] 设 a_n 和 $b_n(n=0,1,\cdots,N-1)$ 为 F 中二个长 N 的序列，称

$$c_k=\sum_{n=0}^{N-1}a_n\,b_{\langle k-n\rangle_N},\quad k=0,1,\cdots,N-1 \qquad (1.1.1)$$

为 a_n 和 b_n 的（一维）循环卷积（Cyclic Convolution）. 其中 $\langle k-n\rangle_N$ 表示 $k-n$ 关于模 N 的最小非负剩余；为书写方便起见，有时简记为 $\langle k-n\rangle$.

根据定义，也可以写成

$$c_k=\sum_{n=0}^{k}a_n\,b_{k-n}+\sum_{n=k+1}^{N-1}a_n\,b_{N+k-n},k=0,1,\cdots,N-1.$$

循环卷积又称圆卷积或周期卷积，是本章讨论的重点。

[**定义1.2**] 设 a_n 和 $b_n(n=0,1,\cdots,N-1)$ 为 F 中二个长 N 的序列，称

$$c_k=\sum_{n=0}^{k}a_n\,b_{k-n}-\sum_{n=k+1}^{N-1}a_n\,b_{N+k-n},k=0,1,\cdots,N-1. \qquad (1.1.2)$$

为 a_n 和 b_n 的（一维）斜循环卷积（Skew—Cyclic Convolution）.

[**定义1.3**] 设 $a_n(n=0,1,\cdots,N-1)$，$b_l(l=0,1,\cdots,L-1)$

为 F 中二个序列，并设 $a_n = 0$ ($n < 0$ 或 $n \geqslant N$)，$b_l = 0$ ($l < 0$ 或 $l \geqslant L$)，称

$$c_k = \sum_{n=0}^{N-1} a_n b_{k-n}, \quad k = 0, 1, \cdots, L + N - 2.$$

为 a_n 和 b_n 的线性卷积 (Linear Convolution).

上述三种卷积在数字信号处理中应用非常广泛，FIR 滤波就是线性卷积，相关可变成线性卷积或循环卷积，DFT 也可变成线性卷积。下面给出这些卷积的多项式表示形式。

由序列 a_n ($n=0, 1, \cdots, N-1$) 可构造一个次数不超过 $N-1$的多项式 $A(z)$，

$$A(z) = \sum_{n=0}^{N-1} a_n z^n.$$

称为 a_n 的生成多项式。显然，a_n 和 $A(z)$ 是一对一的关系。因此，求序列 a_n 的问题等价于求出 a_n 的生成多项式 $A(z)$. 这样，快速计算卷积的问题可利用多项式代数理论进行研究。

[引理1.1] 设 c_k, a_n, b_n 为 F 中长 N 的序列，其生成多项式分别为 $C(z), A(z), B(z)$，则

(1) c_k 为 a_n 和 b_n 的循环卷积的充要条件是

$$C(z) \equiv A(z)B(z) \bmod (z^N - 1) \qquad (1.1.4)$$

(2) c_k 为 a_n 和 b_n 的斜循环卷积的充要条件是

$$C(z) \equiv A(z)B(z) \bmod (z^N + 1) \qquad (1.1.5)$$

记号 $P(z) \bmod Q(z)$ 表示多项式 $P(z)$ 除以多项式 $Q(z)$ 所得的剩余多项式。因此，$P(z) \bmod (z^N - 1)$ 只要把 $P(z)$ 中 z^N 用1代替即可。例如，$4z^3 + 3z^2 + 2z + 1 \bmod (z^2 - 1) = 4z + 3 + 2z + 1 = 6z + 4$. 同样，$P(z) \bmod (z^N + 1)$ 只要把 z^N 用 -1代替即可。

通过简单的计算不难验证引理的正确性。

[引理1.2] 设 a_n ($n=0, 1, \cdots, N-1$)，b_l ($l=0, 1, \cdots, L-1$) 为 F 中二个序列，则 c_k ($k=0, 1, \cdots, L+N-2$) 为 a_n 和

b_i 的线性卷积的充要条件是

$$C(z) = A(z)B(z) \qquad (1.1.6)$$

其中 $C(z)$, $A(z)$ 和 $B(z)$ 分别为 c_k, a_n, b_l 的生成多项式。

上述引理也可通过简单计算证明，请读者自己完成。

这样，循环卷积、斜循环卷积和线性卷积可分别用多项式形式（1.1.4），（1.1.5）及（1.1.6）表示，这种形式在以后的讨论中将经常用到。

[定义1.4] 设 $a_{n_1,n_2,\cdots,n_r}$, $b_{n_1,n_2,\cdots,n_r}$ ($n_i=0,1,\cdots,N_i-1$; $i=1,2,\cdots,r$) 为F中二个 r 维序列，称

$$c_{k_1,k_2,\cdots,k_r} = \sum_{n_1=0}^{N_1-1}\cdots\sum_{n_r=0}^{N_r-1} a_{n_1,n_2,\cdots,n_r}\, b_{(k_1-n_1),\cdots,(k_r-n_r)_{N_r}},$$

$$k_i = 0,1,\cdots,N_i-1;\ i=1,2,\cdots,r \qquad (1.1.7)$$

为序列 $a_{n_1,n_2,\cdots,n_r}$ 及 $b_{n_1,\cdots,n_r}$ 的 r 维循环卷积，特别地，当 $r=2$ 时，为二维循环卷积。

序列 $a_{n_1,\cdots,n_r}$ 对应一个 r 元多项式

$$A(z_1,\cdots,z_r) = \sum_{n_1=0}^{N_1-1}\cdots\sum_{n_r=0}^{N_r-1} a_{n_1,\cdots,n_r} z_1^{n_1}\cdots z_r^{n_r},$$

称为 $a_{n_1,\cdots,n_r}$ 的生成多项式。$a_{n_1,\cdots,n_r}$ 和其生成多项式是一对一的。同样，若令 $b_{n_1,\cdots,n_r}$ 和 $c_{k_1,\cdots,k_r}$ 的生成多项式分别为 $B(z_1,\cdots,z_r)$ 和 $C(z_1,\cdots,z_r)$，则容易证明。

[引理1.3] $c_{k_1,\cdots,k_r}$ 为 $a_{n_1,\cdots,n_r}$ 和 $b_{n_1,\cdots,n_r}$ 的 r 维循环卷积的充要条件为

$$C(z_1,\cdots,z_r) \equiv A(z_1,\cdots,z_r)B(z_1,\cdots,z_r) \bmod (z_1^{N_1}-1),\cdots,(z_r^{N_r}-1), \qquad (1.1.8)$$

同样地，序列 $a_{n_1,\cdots,n_r}$ 也可用其生成多项式序列来表示，设

$$A_{n_1}(z_2,\cdots,z_r) = \sum_{n_2=0}^{N_2-1}\cdots\sum_{n_r=0}^{N_r-1} a_{n_1,\cdots,n_r} z_2^{n_2}\cdots z_r^{n_r},$$