

Springer Series in Information Sciences 2

Editor: T.S. Huang



Springer Series in Information Sciences

Editors: King-sun Fu Thomas S. Huang Manfred R. Schroeder

- Volume 1 **Content-Addressable Memories**
By T. Kohonen
- Volume 2 **Fast Fourier Transform and Convolution Algorithms**
By H. J. Nussbaumer 2nd Edition
- Volume 3 **Pitch Determination of Speech Signals** Algorithms and Devices
By W. Hess
- Volume 4 **Pattern Analysis**
By H. Niemann
- Volume 5 **Image Sequence Analysis**
Editor: T. S. Huang
- Volume 6 **Picture Engineering**
Editors: King-sun Fu and T. L. Kunii
- Volume 7 **Number Theory in Science and Communication**
With Applications in Cryptography, Physics, Biology
and Digital Information
By M. R. Schroeder
- Volume 8 **Self-Organization and Associative Memory**
By T. Kohonen
- Volume 9 **An Introduction to Digital Picture Processing**
By L. P. Yaroslavsky
- Volume 10 **Probability, Statistical Optics, and Data Testing**
A Problem Solving Approach
By B. Roy Frieden
-

Henri J. Nussbaumer

Fast Fourier Transform and Convolution Algorithms

Second Corrected and Updated Edition

With 38 Figures

Springer-Verlag Berlin Heidelberg New York 1982

Professor Henri J. Nussbaumer

Department d'Electricité
Ecole Polytechnique Fédérale de Lausanne, 16, Chemin des Bellerive
CH-1007 Lausanne, Switzerland

Series Editors:

Professor King-sun Fu

School of Electrical Engineering, Purdue University
West Lafayette, IN 47907, USA

Professor Thomas S. Huang

Department of Electrical Engineering and Coordinated Science Laboratory,
University of Illinois, Urbana IL 61801, USA

Professor Dr. Manfred R. Schroeder

Drittes Physikalisches Institut, Universität Göttingen, Bürgerstraße 42-44,
D-3400 Göttingen, Fed. Rep. of Germany

ISBN-13:978-3-540-11825-1 e-ISBN-13:978-3-642-81897-4
DOI: 10.1007/978-3-642-81897-4

Library of Congress Cataloging in Publication Data. Nussbaumer, Henri J., 1931-. Fast Fourier transform and convolution algorithms. (Springer series in information sciences; 2) Bibliography: P. Includes index. 1. Fourier transformations - Data processing. 2. Convolutions (Mathematics) - Data processing. 3. Digital filters (Mathematics) I. Title. II. Series. QA403.5.N87 1982 515.723 82-10650

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, reuse of illustrations, broadcasting, reproduction by photocopying machine or similar means, and storage in data banks. Under § 54 of the German Copyright Law where copies are made for other than private use, a fee is payable to "Verwertungsgesellschaft Wort", Munich.

© by Springer-Verlag Berlin Heidelberg 1981 and 1982

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

2153/3130-543210

Preface to the Second Edition

In the first edition of this book, we covered in Chapter 6 and 7 the applications to multidimensional convolutions and DFT's of the transforms which we have introduced, back in 1977, and called polynomial transforms. Since the publication of the first edition of this book, several important new developments concerning the polynomial transforms have taken place, and we have included, in this edition, a discussion of the relationship between DFT and convolution polynomial transform algorithms. This material is covered in Appendix A, along with a presentation of new convolution polynomial transform algorithms and with the application of polynomial transforms to the computation of multidimensional cosine transforms.

We have found that the short convolution and polynomial product algorithms of Chap. 3 have been used extensively. This prompted us to include, in this edition, several new one-dimensional and two-dimensional polynomial product algorithms which are listed in Appendix B.

Since our book is being used as part of several graduate-level courses taught at various universities, we have added, to this edition, a set of problems which cover Chaps. 2 to 8. Some of these problems serve also to illustrate some research work on DFT and convolution algorithms.

I am indebted to Mrs A. Schlageter who prepared the manuscript of this second edition.

Lausanne
April 1982

HENRI J. NUSSBAUMER

Preface to the First Edition

This book presents in a unified way the various fast algorithms that are used for the implementation of digital filters and the evaluation of discrete Fourier transforms.

The book consists of eight chapters. The first two chapters are devoted to background information and to introductory material on number theory and polynomial algebra. This section is limited to the basic concepts as they apply to other parts of the book. Thus, we have restricted our discussion of number theory to congruences, primitive roots, quadratic residues, and to the properties of Mersenne and Fermat numbers. The section on polynomial algebra deals primarily with the divisibility and congruence properties of polynomials and with algebraic computational complexity.

The rest of the book is focused directly on fast digital filtering and discrete Fourier transform algorithms. We have attempted to present these techniques in a unified way by using polynomial algebra as extensively as possible. This objective has led us to reformulate many of the algorithms which are discussed in the book. It has been our experience that such a presentation serves to clarify the relationship between the algorithms and often provides clues to improved computation techniques.

Chapter 3 reviews the fast digital filtering algorithms, with emphasis on algebraic methods and on the evaluation of one-dimensional circular convolutions.

Chapters 4 and 5 present the fast Fourier transform and the Winograd Fourier transform algorithm.

We introduce in Chaps. 6 and 7 the concept polynomial transforms and we show that these transforms are an important tool for the understanding of the structure of multidimensional convolutions and discrete Fourier transforms and for the design of improved algorithms. In Chap. 8, we extend these concepts to the computation of one-dimensional convolutions by replacing finite fields of polynomials by finite fields of numbers. This facilitates introduction of number theoretic transforms which are useful for the fast computation of convolutions via modular arithmetic.

Convolutions and discrete Fourier transforms have many uses in physics and it is our hope that this book will prompt some additional research in these areas and will help potential users to evaluate and apply these techniques. We also feel that some of the methods presented here are quite general and might someday find new unexpected applications.

Part of the material presented here has evolved from a graduate-level course taught at the University of Nice, France. I would like to express my thanks to Dr. T.A. Kriz from IBM FSD for kindly reviewing the manuscript and for making many useful suggestions. I am grateful to Mr. P. Bellot, IBM, C.E.R., La Gaude, France, for his advice concerning the introductory chapter on number theory and polynomial algebra, and to Dr. J.W. Cooley, from IBM Research, Yorktown Heights, for his comments on some of the work which led to this book. Thanks are also due to Dr. P. Quandalle who worked with me on polynomial transforms while preparing his doctorate degree and with whom I had many fruitful discussions. I am indebted to Mrs. C. De Backer for her aid in improving the English and to Mrs. C. Chevalier who prepared the manuscript.

La Gaude
November 1980

HENRI J. NUSSBAUMER

Contents

Chapter 1 Introduction

1.1	Introductory Remarks	1
1.2	Notations	2
1.3	The Structure of the Book	3

Chapter 2 Elements of Number Theory and Polynomial Algebra

2.1	Elementary Number Theory	4
2.1.1	Divisibility of Integers	4
2.1.2	Congruences and Residues	7
2.1.3	Primitive Roots	11
2.1.4	Quadratic Residues	17
2.1.5	Mersenne and Fermat Numbers	19
2.2	Polynomial Algebra	22
2.2.1	Groups	23
2.2.2	Rings and Fields	24
2.2.3	Residue Polynomials	25
2.2.4	Convolution and Polynomial Product Algorithms in Polynomial Algebra	27

Chapter 3 Fast Convolution Algorithms

3.1	Digital Filtering Using Cyclic Convolutions	32
3.1.1	Overlap-Add Algorithm	33
3.1.2	Overlap-Save Algorithm	34
3.2	Computation of Short Convolutions and Polynomial Products	34
3.2.1	Computation of Short Convolutions by the Chinese Remainder Theorem	35
3.2.2	Multiplications Modulo Cyclotomic Polynomials	37
3.2.3	Matrix Exchange Algorithm	40
3.3	Computation of Large Convolutions by Nesting of Small Convolutions	43
3.3.1	The Agarwal-Cooley Algorithm	43
3.3.2	The Split Nesting Algorithm	47
3.3.3	Complex Convolutions	52
3.3.4	Optimum Block Length for Digital Filters	55
3.4	Digital Filtering by Multidimensional Techniques	56
3.5	Computation of Convolutions by Recursive Nesting of Polynomials	60
3.6	Distributed Arithmetic	64

3.7	Short Convolution and Polynomial Product Algorithms	66
3.7.1	Short Circular Convolution Algorithms	66
3.7.2	Short Polynomial Product Algorithms	73
3.7.3	Short Aperiodic Convolution Algorithms	78
Chapter 4 The Fast Fourier Transform		
4.1	The Discrete Fourier Transform	80
4.1.1	Properties of the DFT.	81
4.1.2	DFTs of Real Sequences.	83
4.1.3	DFTs of Odd and Even Sequences	84
4.2	The Fast Fourier Transform Algorithm	85
4.2.1	The Radix-2 FFT Algorithm	87
4.2.2	The Radix-4 FFT Algorithm	91
4.2.3	Implementation of FFT Algorithms	94
4.2.4	Quantization Effects in the FFT	96
4.3	The Rader-Brenner FFT.	99
4.4	Multidimensional FFTs	102
4.5	The Bruun Algorithm	104
4.6	FFT Computation of Convolutions	107
Chapter 5 Linear Filtering Computation of Discrete Fourier Transforms		
5.1	The Chirp z -Transform Algorithm.	112
5.1.1	Real Time Computation of Convolutions and DFTs Using the Chirp z -Transform.	113
5.1.2	Recursive Computation of the Chirp z -Transform.	114
5.1.3	Factorizations in the Chirp Filter	115
5.2	Rader's Algorithm	116
5.2.1	Composite Algorithms.	118
5.2.2	Polynomial Formulation of Rader's Algorithm	120
5.2.3	Short DFT Algorithms	123
5.3	The Prime Factor FFT	125
5.3.1	Multidimensional Mapping of One-Dimensional DFTs.	125
5.3.2	The Prime Factor Algorithm	127
5.3.3	The Split Prime Factor Algorithm.	129
5.4	The Winograd Fourier Transform Algorithm (WFTA).	133
5.4.1	Derivation of the Algorithm	133
5.4.2	Hybrid Algorithms	138
5.4.3	Split Nesting Algorithms.	139
5.4.4	Multidimensional DFTs	141
5.4.5	Programming and Quantization Noise Issues	142
5.5	Short DFT Algorithms	144
5.5.1	2-Point DFT	145
5.5.2	3-Point DFT	145

5.5.3	4-Point DFT	145
5.5.4	5-Point DFT	146
5.5.5	7-Point DFT	146
5.5.6	8-Point DFT	147
5.5.7	9-Point DFT	148
5.5.8	16-Point DFT	149
Chapter 6 Polynomial Transforms		
6.1	Introduction to Polynomial Transforms	151
6.2	General Definition of Polynomial Transforms	155
6.2.1	Polynomial Transforms with Roots in a Field of Polynomials	157
6.2.2	Polynomial Transforms with Composite Roots	161
6.3	Computation of Polynomial Transforms and Reductions	163
6.4	Two-Dimensional Filtering Using Polynomial Transforms	165
6.4.1	Two-Dimensional Convolutions Evaluated by Polynomial Transforms and Polynomial Product Algorithms	166
6.4.2	Example of a Two-Dimensional Convolution Computed by Polynomial Transforms	168
6.4.3	Nesting Algorithms	170
6.4.4	Comparison with Conventional Convolution Algorithms	172
6.5	Polynomial Transforms Defined in Modified Rings	173
6.6	Complex Convolutions	177
6.7	Multidimensional Polynomial Transforms	178
Chapter 7 Computation of Discrete Fourier Transforms by Polynomial Transforms		
7.1	Computation of Multidimensional DFTs by Polynomial Transforms	181
7.1.1	The Reduced DFT Algorithm	182
7.1.2	General Definition of the Algorithm.	186
7.1.3	Multidimensional DFTs	193
7.1.4	Nesting and Prime Factor Algorithms	194
7.1.5	DFT Computation Using Polynomial Transforms Defined in Modified Rings of Polynomials.	196
7.2	DFTs Evaluated by Multidimensional Correlations and Polynomial Transforms	201
7.2.1	Derivation of the Algorithm	201
7.2.2	Combination of the Two Polynomial Transform Methods	205
7.3	Comparison with the Conventional FFT	206
7.4	Odd DFT Algorithms	207
7.4.1	Reduced DFT Algorithm. $N=4$	209
7.4.2	Reduced DFT Algorithm. $N=8$	209
7.4.3	Reduced DFT Algorithm. $N=9$	209
7.4.4	Reduced DFT Algorithm. $N=16$	210

Chapter 8 Number Theoretic Transforms

8.1 Definition of the Number Theoretic Transforms 211
 8.1.1 General Properties of NTTs 213
 8.2 Mersenne Transforms 216
 8.2.1 Definition of Mersenne Transforms 216
 8.2.2 Arithmetic Modulo Mersenne Numbers 219
 8.2.3 Illustrative Example. 221
 8.3 Fermat Number Transforms 222
 8.3.1 Definition of Fermat Number Transforms 223
 8.3.2 Arithmetic Modulo Fermat Numbers 224
 8.3.3 Computation of Complex Convolutions by FNTs 227
 8.4 Word Length and Transform Length Limitations 228
 8.5 Pseudo Transforms 230
 8.5.1 Pseudo Mersenne Transforms 231
 8.5.2 Pseudo Fermat Number Transforms. 234
 8.6 Complex NTTs. 236
 8.7 Comparison with the FFT 239

Appendix A Relationship Between DFT and Conyolution Polynomial Transform Algorithms

A.1 Computation of Multidimensional DFT's by the Inverse Polynomial Transform Algorithm 241
 A.1.1 The Inverse Polynomial Transform Algorithm 241
 A.1.2 Complex Polynomial Transform Algorithms 244
 A.1.3 Round-off Error Analysis 246
 A.2 Computation of Multidimensional Convolutions by a Combination of the Direct and Inverse Polynomial Transform Methods 247
 A.2.1 Computation of Convolutions by DFT Polynomial Transform Algorithms 248
 A.2.2 Convolution Algorithms Based on Polynomial Transforms and Permutations. 249
 A.3 Computation of Multidimensional Discrete Cosine Transforms by Polynomial Transforms 251
 A.3.1 Computation of Direct Multidimensional DCT's 251
 A.3.2 Computation of Inverse Multidimensional DCT's 253

Appendix B Short Polynomial Product Algorithms 255

Problems 263
References 269
Subject Index 275