

Fast Algorithms for Signal Processing

Richard E. Blahut

CAMBRIDGE

CAMBRIDGE

www.cambridge.org/9780521190497

This page intentionally left blank

Fast Algorithms for Signal Processing

Efficient algorithms for signal processing are critical to very large scale future applications such as video processing and four-dimensional medical imaging. Similarly, efficient algorithms are important for embedded and power-limited applications since, by reducing the number of computations, power consumption can be reduced considerably. This unique textbook presents a broad range of computationally-efficient algorithms, describes their structure and implementation, and compares their relative strengths. All the necessary background mathematics is presented, and theorems are rigorously proved. The book is suitable for researchers and practitioners in electrical engineering, applied mathematics, and computer science.

Richard E. Blahut is a Professor of Electrical and Computer Engineering at the University of Illinois, Urbana-Champaign. He is Life Fellow of the IEEE and the recipient of many awards including the IEEE Alexander Graham Bell Medal (1998) and Claude E. Shannon Award (2005), the Tau Beta Pi Daniel C. Drucker Eminent Faculty Award, and the IEEE Millennium Medal. He was named a Fellow of the IBM Corporation in 1980, where he worked for over 30 years, and was elected to the National Academy of Engineering in 1990.

Fast Algorithms for Signal Processing

Richard E. Blahut

Henry Magnuski Professor in Electrical and Computer Engineering,
University of Illinois, Urbana-Champaign



CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore,
São Paulo, Delhi, Dubai, Tokyo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org

Information on this title: www.cambridge.org/9780521190497

© Cambridge University Press 2010

This publication is in copyright. Subject to statutory exception and to the provision of relevant collective licensing agreements, no reproduction of any part may take place without the written permission of Cambridge University Press.

First published in print format 2010

ISBN-13 978-0-511-77637-3 eBook (NetLibrary)

ISBN-13 978-0-521-19049-7 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of urls for external or third-party internet websites referred to in this publication, and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

In loving memory of

Jeffrey Paul Blahut

May 2, 1968 – June 13, 2004

Many small make a great.

— **Chaucer**

Contents

<i>Preface</i>	xi
<i>Acknowledgments</i>	xiii

1	Introduction	1
1.1	Introduction to fast algorithms	1
1.2	Applications of fast algorithms	6
1.3	Number systems for computation	8
1.4	Digital signal processing	9
1.5	History of fast signal-processing algorithms	17

2	Introduction to abstract algebra	21
2.1	Groups	21
2.2	Rings	26
2.3	Fields	30
2.4	Vector space	34
2.5	Matrix algebra	37
2.6	The integer ring	44
2.7	Polynomial rings	48
2.8	The Chinese remainder theorem	58

3	Fast algorithms for the discrete Fourier transform	68
3.1	The Cooley–Tukey fast Fourier transform	68
3.2	Small-radix Cooley–Tukey algorithms	72
3.3	The Good–Thomas fast Fourier transform	80

3.4	The Goertzel algorithm	83
3.5	The discrete cosine transform	85
3.6	Fourier transforms computed by using convolutions	91
3.7	The Rader–Winograd algorithm	97
3.8	The Winograd small fast Fourier transform	102

4 Fast algorithms based on doubling strategies 115

4.1	Halving and doubling strategies	115
4.2	Data structures	119
4.3	Fast algorithms for sorting	120
4.4	Fast transposition	122
4.5	Matrix multiplication	124
4.6	Computation of trigonometric functions	127
4.7	An accelerated euclidean algorithm for polynomials	130
4.8	A recursive radix-two fast Fourier transform	139

5 Fast algorithms for short convolutions 145

5.1	Cyclic convolution and linear convolution	145
5.2	The Cook–Toom algorithm	148
5.3	Winograd short convolution algorithms	155
5.4	Design of short linear convolution algorithms	164
5.5	Polynomial products modulo a polynomial	168
5.6	Design of short cyclic convolution algorithms	171
5.7	Convolution in general fields and rings	176
5.8	Complexity of convolution algorithms	178

6 Architecture of filters and transforms 194

6.1	Convolution by sections	194
6.2	Algorithms for short filter sections	199
6.3	Iterated filter sections	202
6.4	Symmetric and skew-symmetric filters	207
6.5	Decimating and interpolating filters	213
6.6	Construction of transform computers	216
6.7	Limited-range Fourier transforms	221
6.8	Autocorrelation and crosscorrelation	222

7	Fast algorithms for solving Toeplitz systems	231
7.1	The Levinson and Durbin algorithms	231
7.2	The Trench algorithm	239
7.3	Methods based on the euclidean algorithm	245
7.4	The Berlekamp–Massey algorithm	249
7.5	An accelerated Berlekamp–Massey algorithm	255
8	Fast algorithms for trellis search	262
8.1	Trellis and tree searching	262
8.2	The Viterbi algorithm	267
8.3	Sequential algorithms	270
8.4	The Fano algorithm	274
8.5	The stack algorithm	278
8.6	The Bahl algorithm	280
9	Numbers and fields	286
9.1	Elementary number theory	286
9.2	Fields based on the integer ring	293
9.3	Fields based on polynomial rings	296
9.4	Minimal polynomials and conjugates	299
9.5	Cyclotomic polynomials	300
9.6	Primitive elements	304
9.7	Algebraic integers	306
10	Computation in finite fields and rings	311
10.1	Convolution in surrogate fields	311
10.2	Fermat number transforms	314
10.3	Mersenne number transforms	317
10.4	Arithmetic in a modular integer ring	320
10.5	Convolution algorithms in finite fields	324
10.6	Fourier transform algorithms in finite fields	328
10.7	Complex convolution in surrogate fields	331

x	Contents	
	10.8 Integer ring transforms	336
	10.9 Chevillat number transforms	339
	10.10 The Preparata–Sarwate algorithm	339
11	Fast algorithms and multidimensional convolutions	345
	11.1 Nested convolution algorithms	345
	11.2 The Agarwal–Cooley convolution algorithm	350
	11.3 Splitting algorithms	357
	11.4 Iterated algorithms	362
	11.5 Polynomial representation of extension fields	368
	11.6 Convolution with polynomial transforms	371
	11.7 The Nussbaumer polynomial transforms	372
	11.8 Fast convolution of polynomials	376
12	Fast algorithms and multidimensional transforms	384
	12.1 Small-radix Cooley–Tukey algorithms	384
	12.2 The two-dimensional discrete cosine transform	389
	12.3 Nested transform algorithms	391
	12.4 The Winograd large fast Fourier transform	395
	12.5 The Johnson–Burrus fast Fourier transform	399
	12.6 Splitting algorithms	403
	12.7 An improved Winograd fast Fourier transform	410
	12.8 The Nussbaumer–Quandalle permutation algorithm	411
A	A collection of cyclic convolution algorithms	427
B	A collection of Winograd small FFT algorithms	435
	<i>Bibliography</i>	442
	<i>Index</i>	449

Preface

A quarter of a century has passed since the previous version¹ of this book was published, and signal processing continues to be a very important part of electrical engineering. It forms an essential part of systems for telecommunications, radar and sonar, image formation systems such as medical imaging, and other large computational problems, such as in electromagnetics or fluid dynamics, geophysical exploration, and so on. Fast computational algorithms are necessary in large problems of signal processing, and the study of such algorithms is the subject of this book. Over those several decades, however, the nature of the need for fast algorithms has shifted both to much larger systems on the one hand and to embedded power-limited applications on the other.

Because many processors and many problems are much larger now than they were when the original version of this book was written, and the relative cost of addition and multiplication now may appear to be less dramatic, some of the topics of twenty years ago may be seen by some to be of less importance today. I take exactly the opposite point of view for several reasons. Very large three-dimensional or four-dimensional problems now under consideration require massive amounts of computation and this computation can be reduced by orders of magnitude in many cases by the choice of algorithm. Indeed, these very large problems can be especially suitable for the benefits of fast algorithms. At the same time, smaller signal processing problems now appear frequently in handheld or remote applications where power may be scarce or nonrenewable. The designer's care in treating an embedded application, such as a digital television, can repay itself many times by significantly reducing the power expenditure. Moreover, the unfamiliar algorithms of this book now can often be handled automatically by computerized design tools, and in embedded applications where power dissipation must be minimized, a search for the algorithm with the fewest operations may be essential.

Because the book has changed in its details and the title has been slightly modernized, it is more than a second edition, although most of the topics of the original book have been retained in nearly the same form, but usually with the presentation rewritten. Possibly, in time, some of these topics will re-emerge in a new form, but that time

¹ *Fast Algorithms for Digital Signal Processing*, Addison-Wesley, Reading, MA, 1985.

is not now. A newly written book might look different in its choice of topics and its balance between topics than does this one. To accommodate this consideration here, the chapters have been rearranged and revised, even those whose content has not changed substantially. Some new sections have been added, and all of the book has been polished, revised, and re-edited. Most of the touch and feel of the original book is still evident in this new version.

The heart of the book is in the Fourier transform algorithms of Chapters 3 and 12 and the convolution algorithms of Chapters 5 and 11. Chapters 12 and 11 are the multi-dimensional continuations of Chapters 3 and 4, respectively, and can be partially read immediately thereafter if desired. The study of one-dimensional convolution algorithms and Fourier transform algorithms is only completed in the context of the multidimensional problems. Chapters 2 and 9 are mathematical interludes; some readers may prefer to treat them as appendices, consulting them only as needed. The remainder, Chapters 4, 7, and 8, are in large part independent of the rest of the book. Each can be read independently with little difficulty.

This book uses branches of mathematics that the typical reader with an engineering education will not know. Therefore these topics are developed in Chapters 2 and 9, and all theorems are rigorously proved. I believe that if the subject is to continue to mature and stand on its own, the necessary mathematics must be a part of such a book; appeal to a distant authority will not do. Engineers cannot confidently advance through the subject if they are frequently asked to accept an assertion or to visit their mathematics library.

Acknowledgments

My major debt in writing this book is to Shmuel Winograd. Without his many contributions to the subject, the book would be shapeless and much shorter. He was also generous with his time in clarifying many points to me, and in reviewing early drafts of the original book. The papers of Winograd and also the book of Nussbaumer were a source for much of the material discussed in this book.

The original version of this book could not have reached maturity without being tested, critiqued, and rewritten repeatedly. I remain indebted to Professor B. W. Dickinson, Professor Toby Berger, Professor C. S. Burrus, Professor J. Gibson, Professor J. G. Proakis, Professor T. W. Parks, Dr B. Rice, Professor Y. Sugiyama, Dr W. Vanderkulk, and Professor G. Verghese for their gracious criticisms of the original 1985 manuscript. That book could not have been written without the support that was given by the International Business Machines Corporation. I am deeply grateful to IBM for this support and also to Cornell University for giving me the opportunity to teach several times from the preliminary manuscript of the earlier book. The revised book was written in the wonderful collaborative environment of the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory of the University of Illinois. The quality of the book has much to do with the composition skills of Mrs Francie Bridges and the editing skills of Mrs Helen Metzinger. And, as always, Barbara made it possible.