Volume II

Elements of Digital Satellite Communication

Channel Coding and Integrated Services Digital Satellite Networks

William W Wu

αA	βB	γC	δD	ξE
δC	ξD	αE	βA	γB
βE	γA	δB	ξC	αD
ξB	αC	βD	γE	δA
γD	δE	ξA	αB	βC

COMPUTER SCIENCE PRESS

Volume II

Elements of Digital Satellite Communication

Channel Coding and Integrated Services Digital Satellite Networks

William W Wu

International Telecommunications Satellite Organization (INTELSAT)

COMPUTER SCIENCE PRESS

Printed in the United States of America.

Computer Science Press
1803 Research Boulevard
Rockville, Maryland 20850
1 2 3 4 5 6 Printing Year 89 88 87 86 85

Library of Congress Cataloging in Publication Data

Wu, William W
Elements of digital satellite communications.

Bibliography: v. 1, p.: v. 2, p.,:
Includes index.
Contents: v. 1. System alternatives, analyses, and optimization—v. 2. Channel coding and integrated services digital satellite networks.
1. Artificial satellites in telecommunication.
2. Digital communications. I. Title.
TK5104.W8 1985 621.38′0422 85-5243
ISBN 0-91489-439-0 (v. 1)
ISBN 0-88175-000-X (v. 2)

Volume II

Elements of Digital Satellite Communication

Channel Coding and Integrated Services Digital Satellite Networks

ELECTRICAL ENGINEERING
COMMUNICATIONS AND SIGNAL PROCESSING

Raymond L. Pickholtz, Series Editor

Anton Meijer and Paul Peeters
Computer Network Architectures

Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt
Spread Spectrum Communications, Volume I

Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt
Spread Spectrum Communications, Volume II

Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt
Spread Spectrum Communications, Volume III

William W Wu
Elements of Digital Satellite Communication: System Alternatives, Analyses, and Optimization, Volume I

William W Wu
Elements of Digital Satellite Communication: Channel Coding and Integrated Services Digital Satellite Networks, Volume II

Also of interest:

Victor B. Lawrence, Joseph L. Lo Cicero, and Laurence B. Milstein, editors
IEEE Communication Society's Tutorials in Modern Communications

Wushow Chou, Editor-in-Chief
Journal of Telecommunication Networks

PREFACE

This is the second volume of the two-volume work *Elements of Digital Satellite Communication*. The chapters of each volume are listed below.

Volume I: SYSTEM ALTERNATIVES, ANALYSES, AND OPTIMIZATION

1. Overview
2. Transmission Link, Channel Characterization, and INTELSAT VI
3. Multiple Access
4. Digital Modems and Receivers
5. Synchronization
6. Satellite Switching and Onboard Processing
7. System Optimization

Volume II: CHANNEL CODING AND INTEGRATED SERVICES DIGITAL SATELLITE NETWORKS

1. Overview
2. Theoretical Foundations
3. Applications of Combinatorial Sets in Satellite Communication
4. Cryptology and Message Security
5. Channel Coding: Performance and Variations
6. Error Codec Implementation
7. Integrated Services Digital Satellite Networks and Protocols

Volume I of *Elements of Digital Satellite Communication* explores system alternatives including the techniques, analyses, and tradeoffs of multiple access, modulation, syncronization, satellite switching, and onboard processing. System modeling is presented in terms of satellite link channels in cascade. System optimization is addressed through a set of sample problems that can be solved not only by linear and nonlinear programming but by dynamic, integer, probabilistic, and/or combinatorial programming methods.

In Volume II we continue to identify, to explore, and to analyze selected subjects that are pertinent to either present or future digital satellite communication. The objectives of Volume II are the same as those of Volume I. The emphases on methodology, unified analyses, and the applications of alien theories that characterize Volume I are carried over to Volume II.

To cover any subject in depth, it must be at the expense of not covering other topics. Each chapter subject in this volume can be a book by itself. In fact, for error-correcting codes and cryptographic methods there are good books already written. What makes this book different is that it is written with satellite applications in mind. As elements of a system, the subjects can no longer be treated separately. In addition, it is not a simple task to ascertain the capabilities and limitations of each scheme when it is integrated into a particular system. However, such a task will be simpler if we know the fundamentals, alternatives, interface problems, and a satellite system environment. Chapters 4, 5, and 6 address this need.

The subjects discussed in Chapters 3, 7, and parts of Chapter 2 have not previously appeared in any text or any other literature. To make the material more useful, particularly Chapter 3, Chapter 2 on theoretical foundations has been provided. Further, in addition to the theoretical derivations, useful source data are included in the appendices.

The level of treatment in this volume is more in depth than in Volume I. This depth is reflected in the mathematical maturity, as in Chapter 3, and in detail, as found in Chapter 7. If the reader is interested only in the mechanics of the procedures without requiring the knowledge of why and how they are formulated, step-by-step algorithms and examples are provided separately. Otherwise, the material in Chapter 2 and other derivations cannot be omitted. One exception is the TDMA network protocol presented in Chapter 7.

Some parts of Chapters 2, 3, 5, and 6 were written and copyrighted (U.S. Library of Congress Registration TXU 28-031) as lecture notes. Originally, Volume I was concerned with the overall system aspect of satellite communication and Volume II provided the details of the subsystem aspect. The end result is almost as planned, with the exception that in Chapter 7 of the present Volume II, the issues of Integrated Services Digital Satellite Networks (ISDSN) turn out to be more extensive than any element presented in Volume I.

It should be apparent that some unique characteristics of a satellite network in general cannot be found in any terrestrial cable network. These characteristics include:

- *Broadcasting Capability*
  With a satellite, a signal from one station can be received simultaneously at all stations in the coverage area of the satellite. Within a satellite coverage area, additional stations can be installed without affecting the satellite system.
- *Distance Capability*
  With a satellite, message transmission is independent of distance and terrain.
- *Processing Capability*
  With a satellite, onboard processing can provide signal enhancement, error rate reduction, efficiency improvement, and network switching flexibility.
- *Transmission Capability*
  Through multiple access techniques multi-destinational high-speed multi-way transmission is not only feasible but effective.
- *Implementation Advantage*
  It costs less and takes less time to launch a satellite, and to build a group of earth stations, than to utilize long-distance cables or fiber optics.

For the above reasons we can see that a mere extension of the terrestrial-based ISDN (Integrated Services Digital Network) experience limits the range and scope of a truly integrated services digital network. Therefore, we define and discuss in Chapter 7 the criteria and issues concerning ISDSN and suggest that ISDN be included for an effective digital communication network including satellites. In pursuit of this objective, we discuss the INTELSAT TDMA network as a possible connerstone for such an integrated network.

For comments and corrections on this second volume, I wish to thank Drs. Elwyn Berlekamp, Willis Gore, C. L. (David) Liu, and P. Tong for Chapters 2, 3, and 5; Dr. James Massey for Chapter 4; and Dr. Leonard S. Golding and Keiichiro Koga for Chapter 7. However, none of them has seen the final version. Thus any additional error, or omissions, are my responsibility.

In Chapter 4 on cryptology and message security, Sections 4.4.1, 4.4.3, 4.6.1–4.6.5, parts of 4.7 and 4.8 are the work of Dr. J. Massey. I have only added a few illustrations and a number of examples. Therefore, I am most grateful for Dr. Massey's generosity in permitting the use of his lecture notes, a fact which not only renders that chapter outstanding but has served to improve the overall quality of this book.

I have also benefited from the use of the original derivations or the answers of my questions about their previous work, and express my thanks to Drs. R. C. Bose, David Chase, David G. Leeper, James Morakis, Neil J. A. Sloane, and Andrew Viterbi.

The computer program of the INTELSAT TDMA Network has been jointly developed by KDD Laboratories and Mitsubishi Software Company. The competence and dedication of K. Koga, H. Shinonaga, and H. Maruo are reflected in the end results, as described in Chapter 7. I wish to thank for their support J. Dicks, G. Forcina, S. Kahng, J. Jankowski, G. Paine, E. Podraczky, and O. Shimbo from INTELSAT; H. Kaji and T. Muratani from KDD Laboratories.

I wish also to thank L. Blue, B. Brienza, A. Gorelick, S. Kaplan, B. Kogut, R. Liu, and R. Ramminger for their efforts on the second volume.

The views and judgments expressed in this book are solely those of the author, and do not necessarily reflect the official policies of INTELSAT, an organization owned and participated in by 109 countries.

CONTENTS

Preface xi

1. Overview 1

2. Theoretical Foundations 4

2.1 Fundamentals 4
2.2 Number Systems 4
2.2.1 Prime Numbers 5
2.3 Congruences 6
2.3.1 First Order Congruences 7
2.3.2 Higher Order Congruences 8
2.4 Euler's Function 8
2.5 Fermat's Theorem 9
2.6 Irreducible Polynomials 10
2.7 Finite Field and Arithmetic Inverses 10
2.8 The Euclidean Algorithm 11
2.9 Information Measures 12
2.10 Combinatorial Sets 13
2.10.1 Difference Sets 13
2.11 Projective Geometry Sets 15
2.11.1 Geometries over Finite Fields 15
2.11.2 Planar Projective Geometry Sets $\{D_p\}$ 15
2.11.3 The Generation of Planar Projective Geometry Sets .. 19
2.11.4 Properties of Planar Projective Geometry Sets 22
2.12 Euclidean Geometry Sets 25
2.12.1 Euclidean Geometries 27
2.12.2 Linear Transformations of Vector Spaces over Finite Fields 28
2.12.3 Properties of Transformed Lines in a Finite Euclidean Plane 33
2.12.4 Euclidean Geometry Difference Sets 34
2.12.5 The Set-Generation Algorithm 36
2.12.6 Table of Primitive Polynomials over GF($p \neq 2$) 37
2.13 Latin Squares 38
2.14 Concluding Remarks 41
2.15 References 41
2.16 Problems 42

3. Applications of Combinatorial Sets in Satellite Communication **44**
3.1 The Power of Combinatorial Sets 44
3.2 Random Multiple Access Systems 45
3.3 The Algorithm for RMA Sequence Generation 47
3.4 Characteristics of the RMA Sequences 52
3.5 Performance Derivations of RMA Systems 57
3.5.1 System Access Probability 58
3.5.2 Error Probability Derivations 61
3.5.3 Channel Utilization Factor of RMA Systems 64
3.6 Antennas 66
3.6.1 Phase Array Antennas 67
3.6.2 Sidelobe Controls 72
3.6.3 Difference Set Arrays 76
3.7 Sidelobe Characteristics of Difference Set Arrays 78
3.7.1 Comparison of Random and Difference Set Arrays 84
3.8 Control of Aliasing in Signal Processing 86
3.9 Transponder Frequency Assignment 88
3.10 Collision Control in Packet Transmission 95
3.11 Minimization of Beam Interference 96
3.12 Generation of Error-Correcting Codes 96
3.13 Concluding Remarks 99
3.14 References 99
3.15 Problems 101

4. Cryptology and Message Security **102**
4.1 Message Security and Satellite Communication 102
4.2 Cryptology 104
4.2.1 Cryptographic Functions 104
4.2.2 Cryptographic Satellite Communication Systems 106
4.3 Secret Systems 107
4.3.1 Block Ciphering 107
4.3.2 Blockless Ciphering 109
4.3.3 Feedback Ciphering 110
4.3.4 Cascade Ciphering 111
4.3.5 Transmission Ciphering 111
4.4 Key Management 112
4.4.1 Key Generation 112
4.4.2 Key Distribution 113
4.4.3 Conditional Key Distribution 114
4.4.4 Key Recognition 115
4.5 Information-Theoretic Systems 115
4.5.1 Shannon's Model 116
4.5.2 Ideal Secrecy Systems 117
4.5.3 Practical Secrecy Systems 124

4.5.4 The Results of Hellman and Lu 125
4.6 The Data Encryption Standard 126
4.6.1 Key Generation 126
4.6.2 The Transformation 134
4.7 Multiple Access Cryptosystems 138
4.7.1 One-Way Functions 139
4.7.2 The Diffie-Hellman System 139
4.7.3 Trapdoor One-Way Functions 142
4.7.4 Public Key Cryptosystems 143
4.7.5 The Pohlig-Hellman Scheme 144
4.7.6 General Multiple Access Cryptosystems 146
4.8 A Measure of Secrecy 147
4.9 The Rivest-Shamir-Adleman Algorithm 150
4.9.1 Analyses of the RSA Algorithm 152
4.10 McEliece's Public Key System 154
4.10.1 The Goppa Codes 155
4.11 Secret Sharing Systems 158
4.11.1 Shamir's Polynomial Method 159
4.11.2 The Method of Matrices by Karnin, Greene, and Hellman 160
4.11.3 The Modular Method of Asmuth and Bloom 161
4.12 The Unified Method for Construction of Secret Sharing Systems 163
4.12.1 Maximum Distance Codes and Reed-Solomon Codes 163
4.12.2 Latin Squares and Reed-Solomon Codes 163
4.12.3 Construction of Extended Reed-Solomon Codes from Mutually Orthogonal Latin Squares 165
4.12.4 The Construction of Mutually Orthogonal Latin Squares 168
4.12.5 Prime Powered Orthogonal Latin Squares 168
4.13 Concluding Remarks 171
4.14 References 172
4.15 Problems 174

5. Channel Coding: Performance and Variations 175
5.1 Introduction 175
5.2 Justification of Error Controls in Satellite Communication Links 177
5.2.1 Coding Gains and Losses 177
5.2.2 Performance Bounds 179
5.3 A Classification of Error Control Techniques 181
5.4 Error Detection and Retransmission with Correction 185
5.4.1 Types of ARQ 186
5.4.2 ARQ Tradeoffs 187
5.4.3 Hybrid ARQ-FEC 188

5.4.4 Efficiency Measures 189
5.4.5 Performance Measures 194
5.4.6 ARQ in Digital Communication Satellite Systems 197
5.5 Block Codes 205
5.5.1 The Bit Error Rate Calculation 205
5.5.2 Most Useful Block Codes 209
5.5.3 Block Code Performance 215
5.6 Convolutional Codes 218
5.6.1 Threshold Decoding 218
5.6.2 Viterbi Decoding 225
5.6.3 Sequential Decoding 234
5.6.4 Nonbinary Character Error-Correcting Convolutional Codes 245
5.7 Soft-Decision Decoding 245
5.7.1 Decoding with Channel Measurement Information for Block Codes 248
5.7.2 Optimal Bit-by-Bit and Maximum Radius Decoding 251
5.7.3 Soft-Decision Performance in Viterbi Decoding 252
5.7.4 Weighted Erasure Decoding 255
5.7.5 Generalized Minimum Distance Decoding 256
5.7.6 *A Posteriori* Probability Decoding 258
5.8 Code Concatenation in Multiple Message Transmission 261
5.8.1 Measured Results of Self-Orthogonal Codes for Concatenation 265
5.8.2 Viterbi/Reed-Solomon Code Concatenation 267
5.8.3 Multistage Concatenation 269
5.8.4 The CCSDS Recommendation 270
5.9 Concluding Remarks 273
5.10 References 273
5.11 Problems 276

6. Error Codec Implementation 279
6.1 Introduction 279
6.2 BCH Codes 280
6.2.1 BCH Encoding 282
6.2.2 BCH Decoding 283
6.3 Fast Polynomial Multiplication Circuits 301
6.4 Sequential Polynomial Multiplication Circuit 307
6.5 Maximum Length Sequence Polynomial Multiplication 308
6.6 BCH Codec Complexity 317
6.7 Coset Decoders 318
6.7.1 Coset Decoding of BCH Codes 321
6.7.2 The INTELSAT TDMA Error-Correcting Codec 322
6.8 The (1057, 813, 33) Difference-Set Codec Design 327
6.9 Convolutional Codes 337
6.9.1 Convolutional Code Encoder 337

6.9.2 Threshold Decoders 339
6.9.3 Sequential Decoders 345
6.9.4 The Viterbi Decoder 348
6.10 Nonbinary Character Error-Correcting Block Codes 357
6.10.1 Berlekamp's Reed-Solomon Code Encoding 357
6.10.2 Reed-Solomon Code Decoding 358
6.11 Concluding Remarks 370
6.12 References 370
6.13 Problems 373

7. Integrated Services Digital Satellite Networks and Protocols .. 375
7.1 Integrated Services Digital Satellite Network (ISDSN) 375
7.2 Integrated Service Digital Network (ISDN) 378
7.2.1 CCITT and CCIR 380
7.2.2 Transmission Characteristics 383
7.2.3 Network Performance 389
7.2.4 ISO's OSI Protocols 396
7.2.5 Protocal Reference Model—The Applications of OSI to ISDN 399
7.3 The INTELSAT TDMA Network and Protocol 408
7.3.1 Network Elements 409
7.3.2 Network Connections 410
7.3.3 Network Timing 416
7.3.4 Network Coordination 417
7.4 TDMA Condensed Time Plan Transmission Protocols 451
7.4.1 Circuit Establishment 455
7.4.2 Link Establishment 455
7.4.3 Data Transfer 456
7.4.4 Link and Circuit Disestablishment 456
7.5 Network Control Protocols 457
7.5.1 Terminal Acquisition Support 457
7.5.2 Sequential Terminal Acquisition Support (TAS) 457
7.5.3 Parallel Terminal Acquisition Support 462
7.5.4 Terminal Synchronization Support (TSS) 465
7.6 Protocols for Acquisition and Synchronization 466
7.6.1 Acquisition and Steady State Reception (ASSR) 469
7.6.2 Receive Frame Synchronization (RFS) Procedure 475
7.6.3 Transmit Frame Acquisition and Synchronization (TFAS) 476
7.7 TNS Computer Program Structure 478
7.7.1 Event Controller 478
7.7.2 Satellite Model 480
7.7.3 The Station Models 482
7.7.4 Burst Reception Model 482
7.7.5 Burst Transmission Model 482
7.7.6 External Event Model 485

7.8 Modular Operations 490
7.8.1 Acquisition and Synchronization Module (ASM) 490
7.8.2 Data Management Modules 509
7.9 Program Designations 513
7.9.1 Program Parameters 516
7.9.2 Network Operations 521
7.10 Theoretical Basis of Protocol Information 538
7.10.1 The Rate Distortion Theory 540
7.10.2 A Transmitter Model 542
7.10.3 Network with Delays 543
7.11 Queueing Networks 544
7.11.1 Opened and Closed Networks 545
7.12 Message Congestion 547
7.12.1 Congestion Process as Information Source 548
7.12.2 Congestion Control 549
7.13 Concluding Remarks 550
7.14 References 551
7.15 Problems 553

Afterword 556

Appendix 1: Tables of Primitive Polynomials over GF(p) for $p \neq 2$ and Even Powers of p 557

Appendix 2: Table of Difference Sets 563

Appendix 3: $n=4$ Random Multiple Access Sequences 568

Appendix 4: Codes for Error Controls 578

Appendix 5: Consultative Committee for Space Data Systems Recommendation for Telemetry Channel Coding 594

Appendix 6: Network Operation Parameters for Examples 7.10, 7.11 605

Appendix References 612

Glossary of Acronyms 613

Author Index 618

Subject Index 621

Volume I Author Index 631

Volume I Subject Index 636

Chapter 1

OVERVIEW

In the first volume of this two-volume set on elements of digital satellite communication, we discussed essential elements such as satellite transmission links, channel characterization, multiple access schemes with queues, and digital modulations including amplitude, frequency, phase, and their combinations. Some modulation performance analyses included the effects of interferences, nonlinearities, and additive white Gaussian noise. Channel equalization and interference cancellation techniques were presented. As a practical maximum likelihood sequence detector, the results of combining equalization and sequence estimation were illustrated in terms of complexity and performance.

In Volume I we considered almost all the relevant subjects related to frame synchronization in digital satellite communication from theory to practice, and included useful results and guidelines, from the past to the most recent; we provided construction procedures for synchronization sequence generation and gave actual sync sequences with their characteristics for a number of satellite systems. We know the tradeoffs of onboard processing along with onboard switching, computational complexity, and traffic algorithms. Through mathematical programming methods, the last chapter of Volume I demonstrates the usefulness and the power of optimization in a variety of problems within the sphere of satellite communication.

In this second volume we continue to identify, to explore, and to analyze essential elements in digital satellite communication. We begin by presenting in Chapter 2 the theoretical foundations to be used in the later chapters. These theoretical foundations include number systems, congruences, finite field theory, and combinatorial sets. The reason we include this material is not merely for the sake of convenience, but we feel it is absolutely essential to the full appreciation of Chapters 3 through 6. Furthermore, the presentation on the combinatorial Euclidean sets is not available elsewhere.

Building on the results of Chapter 2, Chapter 3 demonstrates the usefulness of these combinatorial sets in satellite communication for a wide variety of areas. These areas include the generation of signature sequences for random multiple access systems with prescribed characteristics, sidelobe control in phase array antennas, control aliasing in signal processing, determination of transponder frequency assignment, collision control in satellite packet transmission, minimization of beam interference, and the generation of error-correcting codes for either error detection, retransmission, or forward error correction. In all cases the sets provide the optimal solutions. Once the reader is familiar with the basic properties of sets, a single set can often serve for a large number of unrelated applications in satellite communication, as we shall demonstrate in this chapter.

The advantage of the multidestination transmission capability of a satellite system can turn into a disadvantage if sensitive information is received by the wrong people. Information transmitted through a satellite is also vulnerable to message tampering and identity falsification. As the nature of the information transmitted through a satellite network becomes increasingly complex, message security is no longer limited to the domain of military, diplomatic, or governmental operations. Chapter 4 relates cryptology to digital satellite communication. The needs, justifications, and examples of cryptosystems using satellites are brought forth. The characteristic distinctions between communication systems with and without encryption/decryption are observed. Cryptology is concerned with the degree of unrecognizability of a message; cryptosystems make transmitted messages unrecognizable to all but the intended receivers. All significant cryptographic algorithms and cryptosystems are discussed in this chapter.

The problems of studying cryptology are also mentioned. These problems include the difficulty of evaluating a cryptosystem in terms of its cryptographic strength, and the unavailability of some of the ''secrets'' on a cryptographic algorithm for nontechnical reasons. Because of the importance of secret sharing systems to satellite communication, we devote one section of Chapter 4 to the first published survey of all the work done in this area, and another section to presenting—also for the first time—a unified construction method for secret sharing systems.

Chapter 5 provides the justifications, variations, classifications, performance measures, and limitations of basic error coding applications for satellite communication channels. Justifications are discussed through tradeoffs of power, bandwidth, and efficiency. Variations are illustrated by the diversity of applicable codes and decoding techniques. Such diversity can be unified into a simple classification. For practical purposes, critical distinctions and applicabilities among the codes are examined. Potentially useful codes and coding techniques are suggested, and their coding gain expressions are provided. Code performance measures are compared on a sample of applicable codes for channels under consideration.

Code and decoding selection criteria are put forward for the satellite transmission environment. A number of implementable codes are listed in the Appendix.

Coding limitations are sized up through performance bounds. New formulations are derived for forward error correction, error detection, and their combination. We also include both analytical and experimental results of soft decision and code concatenations.

Because encryption and decryption devices are in general simpler to implement than error-correcting codecs, we discuss the theoretical foundations of the cryptological algorithms in Chapter 4 without considering implementation. In Chapter 6 we are concerned with the complexity and design of error-correcting codecs, whose performance is described in Chapter 5. The designs for some decoders are illustrated at the element logical level in Chapter 6.

In Chapter 7, we embark on a number of topics that relate to networks, satellites, and protocols. When we consider issues related to integrated digital satellite network services, these issues are no longer elements of satellite communication, but, instead, satellite communication becomes an element of such network services. We are interested in this area because it is important and it is challenging. In this chapter, some criteria have been outlined toward the establishment of such a global service network. The international organization responsible for the development and standardization of such a task is introduced. In some areas its work is criticized, while in other areas its work is highly praised.

A large portion of Chapter 7 is devoted to the INTELSAT TDMA network protocol operation, which includes network architecture, network elements, and detailed protocol procedures. The objectives are twofold: the first is to reveal the inner workings of this first international high-speed commercial digital satellite network and the second is to explore some of its merits, which may be introduced as international standards.

Among its theoretical aspects, Chapter 7 includes the connection between network protocol information and rate-distortion theory, and the equivalence between an open network of series queues (as in a satellite link) and a closed network with feedback queues. Since the main purpose of satellite communication is to transmit and receive messages, or to carry traffic, and as the volume of traffic increases congestion will result, Chapter 7 concludes with a brief discussion on congestion control.