UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Trellis Decoding of Reed Solomon and Related Linear Block Codes

By

Werner Heinrich Büttner

A dissertation submitted in partial fulfillment of the requirements for the degree

Master of Engineering (Electronic)

in the

Department of Electrical and Electronic Engineering
in the
Faculty of Engineering

at the

UNIVERSITY OF PRETORIA

Advisor: Professor L.P. Linde

October 1999

Abstract

TRELLIS DECODING OF REED-SOLOMON AND RELATED LINEAR BLOCK CODES

by

Werner Heinrich Büttner

Advisor: Prof. L. P. Linde

Department of Electrical and Electronic Engineering

Master of Engineering (Electronics)

Reed-Solomon codes, a subset of multilevel non-binary cyclic codes with powerful burst error correcting capabilities, are known to be computationally efficient when algebraic decoding techniques are applied. They may however give weaker performance compared to convolutional coding techniques, at least at moderate bit error rates (around 10^{-5} to 10^{-6}) on the AWGN channel. This disadvantage mainly results from the lack of a general applicable method for soft-decision decoding. The aim is to construct a trellis from the generator matrix of a Reed-Solomon code and to show that apart from the historical Berlekamp Massey frequency domain techniques, other techniques usually reserved for convolutional code decoding, such as Maximum Likelihood (ML) and the Maximum A-Posteriori (MAP) techniques, can be successfully applied in the decoding process. Consequently, the main objective of this dissertation is to analyse, design and implement a soft-input, soft-output Reed-Solomon ML or MAP trellis decoding algorithm with performance and complexity comparable to conventional algebraic block decoding methods.

The main reason why trellis decoding is not often used for cyclic block codes, is the complexity of the decoder, especially in the case of long codes with high redundancy. In fact, it will be almost impossible to implement the Viterbi decoder for Reed-Solomon codes with moderate redundancy, considering the fact that the Viterbi decoder becomes computationally unfeasible and practically intractable for convolutional codes of constraint length greater than 10 to 12. Therefore, in order to reduce trellis complexity, a search for minimal block trellis decoding techniques is launched through:

- manipulation of the generator matrix with a view of obtaining minimal trellis structures, i.e., minimising the number of states in a specific block code trellis;

- devising methods to simplify trellis construction of large block codes (i.e., codes with large block size n and redundancy n-k);

- considering only a certain number of trellis paths which are most likely to be transmitted, in stead of all possible paths. This may for example be achieved through a expurgation process on the original trellis (i.e., eliminating paths not terminating in the zero state) or by applying maximum likelihood (ML) or maximum a-posteriori (MAP) decoding methods such as the Viterbi algorithm which results in significant computational savings through its 'survival path' mechanism. The expurgation process is block code specific, i.e., the existence of unterminated paths may differ for each code and is a function of each code's inherent algebraic structure.

The objective of this reduced search method is therefore to optimise the performance of the code while minimising trellis decoding complexity and the corresponding decoding delay.

In the process of constructing minimal trellis structures for cyclic block codes, a novel topological branch interconnecting (trellis branch indexing or labelling) scheme for block codes, and specifically Reed-Solomon codes, is proposed and developed. The technique identifies unique interconnecting patterns in the branch structures of sub-trellises, by which the remaining parts of the trellis may be uniquely defined without having to resort to complicated trellis branch calculations. It is shown that the complexity of the trellis construction process may be reduced by orders in magnitude (for relatively short block lengths), by exploiting the well defined cyclic trellis patterns inherent to the trellis structures of individual block codes.

After having established methods for efficient block trellis construction and the corresponding minimal trellis coder and decoder design, it is next shown how ML convolutional decoding techniques, such as the Viterbi decoding algorithm, can be successfully employed in the decoding process of block codes which could traditionally only be decoded by means of algebraic techniques. The study then investigates the error performance achievable using the trellis as a means of decoding. It is shown that the performance of ML (Viterbi) trellis block decoding with soft decisions matches the performance rendered by soft decision algebraic block decoding techniques in all respects.

Key Words: Trellis, Complexity Reduction, Bit Error Rate, Reed-Solomon, Topology.

Opsomming

TRELLIS DEKODEERING VAN REED-SOLOMON EN VERWANTE LINEÊRE BLOK KODES

deur

Werner Heinrich Büttner

Studieleier: Prof. L. P. Linde

Departement van Elektiese en Elektoniese Ingenieurswese

Meesters in Ingenieurswese (Elektronies)

Reed-Solomon kodes, 'n onderafdeling van multivlak nie-binêre sikliese kodes met kragtige foutkorreksie eienskappe, word geken as rekenkundig effektief wanneer algebraiese dekoderingstegnieke gebruik word. Hulle kan egter swakker vaar in vergelyking met konvolusie koderingstegnieke, minstens by gemiddelde bisfoutwaarskynlikhede (omtrent 10^{-5} tot 10^{-6}) in 'n AWGN kanaal. Hierdie nadeel spruit uit die afwesigheid van 'n algemene methode vir sagte-beslissing-dekodering. Die doel is die konstruksie van 'n trellis vanaf die generatormatriks van 'n Reed-Solomon kode en om aan te toon dat benewens die historiese Berlekamp Massey frekwensie tegniek, dit moontlik is om ander tegnieke wat normaalweg uitsluitlik vir die dekodering van konvolusie kodes dien, soos die "Maximum Likelihood" (ML) en die Maksimum A-Posteriori (MAP) tegnieke, suksesvol te benut in die dekoderingsproses. Gevolglik is die hoofdoelstelling van hierdie verhandeling die analise, ontwerp en implementering van 'n sagte-inset, sagte-uitset Reed-Solomon ML of MAP trellis dekoderingsalgoritme met foutkorreksie-eienskappe en kompleksiteit vergelykbaar met konvensionele algebraiese blokdekoderingstegnieke.

Die hoofrede hoekom trellis dekodering nie vrylik gebruik word vir sikliese blokkodes nie, is die kompleksiteit van die dekodeerder, veral in die geval van lang kodes met 'n hoë oortolligheid. Dit word amper 'n rekenkundige onmoontlikheid om 'n Vieterbi dekodeerder vir Reed-Solomon kodes met 'n gemiddelde oortolligheid te implementeer, siende dat dit rekenkundig en prakties onmoontlik is vir konvolusiekodes met 'n beperkings lengte groter as 10 tot 12. Ten einde trellis kompleksiteit te beperk, word

'n soektog na minimale blok trellise geloods deur:

- manipulasie van die generatormatriks met die doel om 'n minimale trellis struktuur te verkry, met ander woorde om die aantal toestande in 'n spesefieke blokkode trellis te minimiseer;

- ontwikkeling van metodes om trellis konstruksie vir groot blok kodes (kodes met groot bloklengte n en oortolligheid n-k) te vereenvoudig;

- om slegs 'n sekere aantal trellis paaie in berekening te bring as een van die mees waarskynlik gestuurde kode, in plaas daarvan om almal in berekening te bring. Hierdie kan byvoorbeeld bewerkstellig word deur 'n proses, waar sekere paaie wat nie in die nul toestand termineer nie, weg te laat. Dit kan vêrder ook gedoen word deur die ML of MAP dekoderingstegnieke soos die Viterbi algoritme te gebruik, wat 'n groot besparing in bewerkings teweegbring deur gebruikmaking van die oorblywende pad meganisme. The proses van uitlating van paaie verskil vir elke blokkode en is 'n funksie van elke kode se inherente algebraiese struktuur.

Die doel van hierde gereduseerde soektog metode is dus om die werkverrigting van die kode te optimiseer terwyl die dekoderingskompleksiteit en die saamhangende dekoderingsvertraging geminimiseer word.

In die konstruksie proses van minimale trellis strukture vir sikliese blokkodes, word 'n nuwe topologiese tak interkonneksie (trellis tak indeksering) skema vir blok kodes, en meer spesifiek Reed-Solomon kodes, voorgestel en ontwikkel. Hierdie tegniek identifiseer unieke interkonneksiepatrone in die takstruktuur van sub-trellise, waarmee die res van die trellis uniek gedefinieer kan word sonder om ingewikkelde trellis takbewerkings te verrig. Daar word aangetoon dat die kompleksiteit van die trellis konstruksieproses ordes vereenvoudig kan word (vir relatiewe klein bloklengtes), deur die goed gedefinieerde sikliese trellispatrone inherent in die trellisstruktuur van individuele blokkodes te gebruik.

Nadat metodes vir effektiewe blok trelliskonstruksie en die minimale trellis kodeerder en dekodeerder bepaal is, word daar aangetoon hoe ML konvolusie dekoderingstegnieke soos die Viterbi algoritme suksesvol benut kan word in die dekoderingsproses van blok kodes, wat normaalweg slegs deur middel van algebraiese tegnieke dekodeer kon word.

Die studie ondersoek dan die foutkorreksieverrigting wat verkry word indien die trellis tegniek as dekoderingsproses benut word.

Daar word aangetoon dat die verrigting van ML (Viterbi) trellis blokdekodering met sagte beslissings in alle aspekte dieselfde is as die verrigting verkry deur sagte beslissing algebraïese tegnieke.

Sleutelwoorde: Trellis, Kompleksiteit Vermindering, Bisfoutwaarskynlikheid, Reed-Solomon, Topologie.

Dedication

This dissertation is dedicated to L. du Preez.

Your support and effort will forever be remembered.

Acknowledgments

The following persons have given invaluable input, without which this dissertation would not have reached the state which it is in now.

Firstly I would like to thank Professor L.P. Linde, who as my mentor and project leader has always been there when needed. Without his expertise and time, this project would not have become what it is today.

Secondly, I would like to thank L. Staphorst, who has sacrificed enormous amounts of time to assist with various parts of the project. His help is greatly appreciated.

Sincere thanks also goes out to D. J. van Wyk, who had the initial drive to start this project.

Several persons have sacrificed their time to proofread this dissertation. Again, thanks goes out to Professor L.P. Linde, who has on more than one occasion set aside time to read the dissertation. The other people who have contributed in this aspect are amongst other B.H. Waldeck and Y. Iglauer.

Thanks also goes out to S. Swanepoel, who was always available to listen to problems and provide solutions.

I would also like to take this opportunity to thank various other people, the list being to long to reproduce here, who have given their utmost to help make this project a success.

And, last but not least, thanks goes to my parents and my girlfriend L. du Preez who have helped and assisted me throughout the whole project.

List of Acronyms and Abbreviations

List of Acronyms

AWGN	Additive White Gaussian Noise
BCH	Bose-Chaudhuri-Hocquenghem
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CTD	Code Trellis Diagram
GF	Galois Field
HD	Hard-Decision
MAP	Maximum A-Posteriori Probability
ML	Maximum-Likelihood
MLD	Maximum-Likelihood Decoder
RS	Reed Solomon
SD	Soft-Decision
SDML	Soft-Decision-Maximum-Likelihood
SP	Trellis Sub-Part

List of Abbreviations

dB	Decibel
E_b	Energy per Bit
E_{bit}/N_0	Energy to Noise Ratio
G	Generator Matrix
H	Parity Check Matrix
h_x	Column x of Parity Matrix H
I	Unit Matrix
M	Encoder Memory Arrangement
N	Number of States
N_0	Single Sided Noise Power Spectral Density
P(x)	Probability
P_{Bit}	Bit Error Probability
P_{Block}	Block Error Probability

List of Figures

Figure 1	Example of a Convolutional Encoder with R=2/3 and M=1	14
Figure 2	Trellis Diagram of Convolutional Code as per Figure 1	18
Figure 3	Structure of a Digital Transmission System	20
Figure 4	System Model for the Derivation of Decoding Strategy	23
Figure 5	Probability Density Functions	24
Figure 6	Schematic Representation of the Viterbi Algorithm	28
Figure 7	Untrue Trellis Diagram A for the (3,2)-Parity-Check-Code	30
Figure 8	Untrue Trellis Diagram B for the (3,2)-Parity-Check-Code	31
Figure 9	True Trellis Diagram A for the (3,2)-Parity-Check-Code	31
Figure 10	True Trellis Diagram B for the (3,2)-Parity-Check-Code	32
Figure 11	True Trellis Diagram C for the (3,2)-Parity-Check-Code	32
Figure 12	Full Syndrome Trellis Diagram for the (7,4)-Hamming-Code	36
Figure 13	Expurgated Trellis Diagram for the (7,4)-Hamming-Code	37
Figure 14	Syndrome Trellis Diagram A for the (5,3)-Code	38
Figure 15	Syndrome Trellis Diagram B for the (5,3)-Code	39
Figure 16	Comparison between Different HD Methods	45
Figure 17	Comparison between Different SD Methods	46
Figure 18	Bit Error Rate of the (7,4)- Hamming-Code	47
Figure 19	Block Error Rate of the (7,4)-Hamming-Code	48
Figure 20	Bit Error Rate of the (16,11)-Reed-Muller-Code	49
Figure 21	Bit Error Rate of the (31,21)-BCH-Code	50
Figure 22	Bit Error Rate of the (15,7)-BCH-Code	51
Figure 23	Comparison of BCH-Codes with (7,4)-Hamming Code	52
Figure 24	Bit Error Rate of the (16,5)-Reed-Muller-Code R(1,4)	53
Figure 25	Bit Error Rate of the (16,11)-Reed-Muller-Code R(2,4)	54
Figure 26	Bit Error Rate of the (32,16)-Reed-Muller-Code R(2,5)	55
Figure 27	Bit Error Rate of the (32,26)-Reed-Muller-Code R(3,5)	56
Figure 28	Bit Error Rate of the (32,31)-Reed-Muller-Code R(4,5)	57
Figure 29	Comparison of Reed-Muller-Codes for Different Parameters	58
Figure 30	Branch Structure of Reed Solomon Trellis in Galois Field GF(4)	71
Figure 31	Section 1 of the (7,5)-Reed-Solomon Trellis in GF(4)	84
Figure 32	Section 2 of the (7,5)-Reed-Solomon Trellis in GF(4)	85

Figure 33	Section 3 of the (7,5)-Reed-Solomon Trellis in GF(4)	86
Figure 34	Section 4 of the (7,5)-Reed-Solomon Trellis in GF(4)	87
Figure 35	Section 5 of the (7,5)-Reed-Solomon Trellis in GF(4)	88
Figure 36	Section 6 of the (7,5)-Reed-Solomon Trellis in GF(4)	89
Figure 37	Section 7 of the (7,5)-Reed-Solomon Trellis in GF(4)	90
Figure 38	Flow Diagram of the Topological Trellis Design Algorithm	96
Figure 39	Symbol Error Rate of (7,5)-Reed-Solomon Code	97
Figure 40	(5,3)-Code Trellis Diagram1	107
Figure 41	(5,3)-Code Trellis Diagram 2	107
Figure 42	Trellis Simulation Software for Parity Check Matrix H_1	110
Figure 43	Trellis Simulation Software for Parity Check Matrix H_2	111
Figure 44	Comparison of Reduced and Original Block Error Rates	118
Figure 45	Graphical Representation of N_Σ and $\rho(C)$ for (15,7)-BCH	124
Figure 46	Single Code Trellis for Codeword 1	146
Figure 47	Single Code Trellis for Codeword 2	146
Figure 48	Single Code Trellis for Codeword 3	147
Figure 49	Single Code Trellis for Codeword 4	147
Figure 50	Single Code Trellis for Codeword 5	148
Figure 51	Single Code Trellis for Codeword 6	148
Figure 52	Single Code Trellis for Codeword 7	149
Figure 53	Single Code Trellis for Codeword 8	149
Figure 54	Combined Single Code Trellis Diagram	150
Figure 55	Final Syndrome Trellis Diagram	150
Figure 56	Trellis Diagram for Code C_1	164
Figure 57	Trellis Diagram for Code C_2	164
Figure 58	Combined Shannon Product Trellis Diagram	165
Figure 59	State Profile for C_1	167
Figure 60	State Profile for C_2	168
Figure 61	State Profile for C_3	168
Figure 62	State Profile for C_4	168
Figure 63	State Profile for C_5	169
Figure 64	Syndrome Trellis Diagram for the (7,5,3)-RS-Code	170

List of Tables

Table 1	Tabulation of Results	59
Table 2	Nodes for State 1 of (7,5) RS-Code in GF(4)	76
Table 3	Nodes for State 2 of (7,5) RS-Code in GF(4)	77
Table 4	Nodes for State 3 of (7,5) RS-Code in GF(4)	78
Table 5	Nodes for State 4 of (7,5) RS-Code in GF(4)	79
Table 6	Nodes for State 5 of (7,5) RS-Code in GF(4)	80
Table 7	Nodes for State 6 of (7,5) RS-Code in GF(4)	81
Table 8	Nodes for State 7 of (7,5) RS-Code in GF(4)	82
Table 9	Original (5,3) Code.bcc File	112
Table 10	Original (5,3) Code Trellis.btf File	113
Table 11	Reduced (5,3) Code.bcc File	114
Table 12	Reduced (5,3) Code Trellis.btf File	115
Table 13	Original Results.res File	116
Table 14	Reduced Results.res File	117
Table 15	Codewords of the (7,4)-Hamming Code in GF(2)	120
Table 16	Partial Code Words $T_J(C)$ with J = {1, 3, 6}	121
Table 17	Sub-Codes C_J with J = {1, 3, 6}	121
Table 18	Results for (15,7)-BCH Code after 2^{32} Permutations	123
Table 19	Comparison of N_Σ and $\rho(C)$ for (11,7)-Hamming Code	127
Table 20	Comparison of N_Σ and $\rho(C)$ for (15,5)-BCH Code	128
Table 21	Comparison of N_Σ and $\rho(C)$ for (11,7)-Hamming Code obtained with the Optimised Search Algorithm	129
Table 22	Comparison of N_Σ and $\rho(C)$ for (15,5)-BCH Code obtained with the Optimised Search Algorithm	130
Table 23	Galois Symbol Representation in Different Forms	173

Table of Contents

Chapter 1 **1**
Introduction **1**
1.1 Historical Overview 1
1.2 Goals and Objectives 3
1.3 Outline of Dissertation 4
1.4 Major Contributions 6

Chapter 2 **7**
Foundations of Channel Coding **7**
2.1 Introduction 7
2.2 Block Codes 7
2.2.1 Linear Block Code, Generator Matrix and Parity Check Matrix 8
2.2.2 Equivalent Codes and Systematic Codes 9
2.2.3 Cyclic Codes - Generator and Parity Check Polynomials 11
2.2.4 Syndrome 12
2.3 Convolutional Codes 13
2.3.1 Convolutional Encoder 13
2.3.2 Matrix Representation of Convolutional Codes 15
2.3.3 Trellis Diagram Representation 17
2.4 On the Decoding of Block and Convolutional Codes 19
2.4.1 General Decoding Principles 19
2.4.2 Decoding of Block Codes 26
2.4.3 Decoding of Convolutional Codes 27

Chapter 3 **29**
Decoding of Block Codes **29**
3.1 Introduction 29
3.2 Block Codes 29
3.3 Syndrome Trellis 33
3.4 Calculation of the Parity Check Matrix 40
3.5 Decoding in the Syndrome Trellis Diagram 42

Chapter 4 **41**

Performance Issues of Various Block Codes **41**

4.1 Introduction 41

4.2 Simulation Results 41

4.2.1 Bit Error Rate Performance of the (7,4)- Hamming-Code 47

4.2.2 Block Error Rate Performance of the (7,4)-Hamming-Code 48

4.2.3 Bit Error Rate Performance of the (16,11)-Reed-Muller-Code 49

4.2.4 Bit Error Rate Performance of the (31,21)-BCH-Code 50

4.2.5 Bit Error Rate Performance of the (15,7)-BCH-Code 51

4.2.6 Comparison of BCH-Codes with (7,4)-Hamming Code 52

4.2.7 Bit Error Rate of the (16,5)-Reed-Muller-Code R(1,4) 53

4.2.8 Bit Error Rate of the (16,11)-Reed-Muller-Code R(2,4) 54

4.2.9 Bit Error Rate of the (32,16)-Reed-Muller-Code R(2,5) 55

4.2.10 Bit Error Rate of the (32,26)-Reed-Muller-Code R(3,5) 56

4.2.11 Bit Error Rate of the (32,31)-Reed-Muller-Code R(4,5) 57

4.2.12 Comparison of Reed-Muller-Codes for Different Parameters 58

4.2.13 Tabulation of Results 59

4.2.14 General Discussion of Results 59

Chapter 5 **60**

Trellis Construction and Decoding of Non-Binary Reed-Solomon Codes **60**

5.1 Introduction to Reed-Solomon Codes 60

5.2 Algebraic Reed-Solomon Code Construction 60

5.3 Conventional Decoding methods for Reed-Solomon Codes 62

5.4 Error Correcting Characteristics of Reed-Solomon Codes 64

5.5 Various Trellis Construction Techniques 65

5.5.1 Syndrome Trellis Design for Reed-Solomon Codes 65

5.5.2 Coset Trellis Design for Reed-Solomon Codes 68

5.5.3 Modified Trellis Design Procedure for Reed-Solomon Codes 69

5.6 Topological Analysis of a Reed-Solomon Trellis 91

5.7 Symbol Error Rate of Reed-Solomon Codes 97

5.8 General Discussion on Reed-Solomon Performance 98

Chapter 6 **100**

Introduction to Trellis Complexity and Trellis Complexity Reduction **100**

6.1 Introduction 100

6.2 State Complexity 100
6.3 Branch Complexity 103
6.4 Overall Complexity 103
6.5 Generator Matrix Permutations 103
6.6 Decoding in the Trellis Diagrams 108
6.7 Bit Error Rate Calculations 112
6.8 Algorithms for Determining Minimal Trellis Diagram Representations 118
6.8.1 Terminated Brute Force Search Algorithm 119
6.8.2 Systematic Search Algorithm 126
6.8.3 Optimised Systematic Search Algorithm 128

Chapter 7 **131**
Conclusion **131**
7.1 Conclusion 131

References **133**

Appendix A **137**
Another Syndrome Trellis Construction Technique **137**
A.1 Introduction 137
A.2 Generation of the Code Book 137
A.3 Calculation of the Syndromes 139
A.4 Constructing the Syndrome Trellis Diagram 145

Appendix B **151**
Computation of the Parity Check Matrix from the Generator Matrix **151**
B.1 Introduction 151
B.2 Explanation by Example 151

Appendix C **155**
Generator Matrixes of Simulated Codes **155**
C.1 Introduction 155
C.2 Generator Matrixes of given BCH-Codes 155
C.3 Generator Matrixes of given Reed-Muller Codes 157

Appendix D **161**

Shannon Product of Trellises **161**

D.1 Introduction 161

D.2 Analytical Approach to the Shannon Trellis Product 161

D.3 Shannon Product of Trellises by Example 163

Appendix E **166**

Coset and Syndrome Trellises by Example **166**

E.1 Introduction 166

E.2 Syndrome Construction 166

E.3 Coset Construction 170

Appendix F **172**

Galois Field Arithmetic **172**

F.1 Introduction 172

F.2 Fields 172

Appendix G **175**

Simulation Code **175**

G.1 Introduction 175

G.2 Simulation Code 175