PM-1 3 1/2" x 4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT

PRECISIONSM RESOLUTION TARGETS

GRAPHICAL PROPERTIES OF QUASI-CYCLIC CODES

by

MORTEZA ESMAEILI

A thesis submitted to

the Faculty of Graduate Studies and Research

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics and Statistics

Carleton University

Ottawa, Canada

©1996

Morteza Esmacili

National Library
of Canada

Acquisitions and
Bibliographic Services Branch

395 Wellington Street
Ottawa Ontario
K1A 0N4

Bibliothèque nationale
du Canada

Direction des acquisitions et
des services bibliographiques

395, rue Wellington
Ottawa (Ontario)
K1A 0N4

Your file Votre référence

Our file Notre référence

The author has granted an irrevocable non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of his/her thesis by any means and in any form or format, making this thesis available to interested persons.

L'auteur a accordé une licence irrévocable et non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de sa thèse de quelque manière et sous quelque forme que ce soit pour mettre des exemplaires de cette thèse à la disposition des personnes intéressées.

The author retains ownership of the copyright in his/her thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without his/her permission.

L'auteur conserve la propriété du droit d'auteur qui protège sa thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

ISBN 0-612-19370-5

Canada

Name Morteza Esmaili

Dissertation Abstracts International is arranged by broad, general subject categories. Please select the one subject which most nearly describes the content of your dissertation. Enter the corresponding four-digit code in the spaces provided.

Area - the humanities

SUBJECT TERM

0405

U-M-I

SUBJECT CODE

Subject Categories

THE HUMANITIES AND SOCIAL SCIENCES

COMMUNICATIONS AND THE ARTS

Architecture 0729
Art History 0377
Cinema 0900
Dance 0378
Fine Arts 0357
Information Science 0723
Journalism 0391
Library Science 0399
Mass Communications 0708
Music 0413
Speech Communication 0459
Theater 0465

EDUCATION

General 0515
Administration 0514
Adult and Continuing 0516
Agricultural 0517
Art 0273
Bilingual and Multicultural 0282
Business 0688
Community College 0275
Curriculum and Instruction 0727
Early Childhood 0518
Elementary 0524
Finance 0277
Guidance and Counseling 0519
Health 0480
Higher 0745
History of 0520
Home Economics 0278
Industrial 0521
Language and Literature 0272
Mathematics 0280
Music 0522
Philosophy of 0998
Physical 0523

Psychology 0525
Reading 0535
Religious 0527
Sciences 0714
Secondary 0533
Social Sciences 0534
Sociology of 0340
Special 0529
Teacher Training 0530
Technology 0710
Tests and Measurements 0286
Vocational 0747

LANGUAGE, LITERATURE AND LINGUISTICS

Language 0679
General 0289
Ancient 0290
Linguistics 0291
Modern 0401
Literature 0294
Classical 0295
Comparative 0297
Medieval 0298
Modern 0316
African 0591
American 0305
Asian 0352
Canadian (English) 0355
Canadian (French) 0593
English 0311
Germanic 0312
Latin American 0315
Middle Eastern 0313
Romance 0314
Slavic and East European

PHILOSOPHY, RELIGION AND THEOLOGY

Philosophy 0422
Religion 0318
General 0321
Biblical Studies 0319
Clergy 0320
History of 0322
Philosophy of 0469
Theology

SOCIAL SCIENCES

American Studies 0323
Anthropology 0324
Archaeology 0326
Cultural 0327
Physical 0310
Business Administration 0272
General 0770
Accounting 0454
Banking 0338
Management 0385
Marketing 0501
Canadian Studies 0503
Economics 0505
General 0508
Agricultural 0509
Commerce-Business 0510
Finance 0511
History 0358
Labor 0366
Theory 0351
Folklore 0578
Geography 0578
Gerontology 0578
History 0578
General

Ancient 0579
Medieval 0581
Modern 0582
Black 0328
African 0331
Asia, Australia and Oceania 0332
Canadian 0334
European 0335
Latin American 0336
Middle Eastern 0333
United States 0337
History of Science 0585
Law 0398
Political Science 0615
General 0616
International Law and 0617
Relations 0617
Public Administration 0617
Recreation 0814
Social Work 0452
Sociology 0626
General 0627
Criminology and Penology 0938
Demography 0631
Ethnic and Racial Studies 0628
Individual and Family 0629
Studies 0630
Industrial and Labor 0700
Relations 0344
Public and Social Welfare 0709
Social Structure and 0999
Development 0453
Theory and Methods 0453
Transportation 0453
Urban and Regional Planning 0453
Women's Studies

THE SCIENCES AND ENGINEERING

BIOLOGICAL SCIENCES

Agriculture 0473
General 0285
Agronomy 0475
Animal Culture and 0476
Nutrition 0475
Animal Pathology 0476
Food Science and 0359
Technology 0478
Forestry and Wildlife 0479
Plant Culture 0480
Plant Pathology 0817
Plant Physiology 0777
Range Management 0746
Wood Technology

Biology 0306
General 0287
Anatomy 0308
Biostatistics 0309
Botany 0379
Cell 0329
Ecology 0353
Entomology 0369
Genetics 0793
Limnology 0410
Microbiology 0307
Molecular 0317
Neuroscience 0416
Oceanography 0433
Physiology 0821
Radiation 0778
Veterinary Science 0472
Zoology

Biophysics 0784
General 0760
Medical

EARTH SCIENCES

Biogeochemistry 0425
Geochemistry 0996

Geodesy 0370
Geology 0372
Geophysics 0373
Hydrology 0388
Mineralogy 0411
Paleobotany 0345
Paleocology 0426
Paleontology 0418
Paleozoology 0985
Palynology 0427
Physical Geography 0368
Physical Oceanography 0415

HEALTH AND ENVIRONMENTAL SCIENCES

Environmental Sciences 0768
Health Sciences 0566
General 0300
Audiology 0992
Chemotherapy 0567
Dentistry 0350
Education 0749
Hospital Management 0758
Human Development 0982
Immunology 0564
Medicine and Surgery 0347
Mental Health 0569
Nursing 0570
Nutrition 0380
Obstetrics and Gynecology 0354
Occupational Health and 0381
Therapy 0571
Ophthalmology 0419
Pathology 0572
Pharmacology 0382
Pharmacy 0573
Physical Therapy 0574
Public Health 0575
Radiology 0575
Recreation

Speech Pathology 0460
Toxicology 0383
Home Economics 0384

PHYSICAL SCIENCES

Pure Sciences 0485
Chemistry 0749
General 0486
Agricultural 0487
Analytical 0488
Biochemistry 0738
Inorganic 0490
Nuclear 0491
Organic 0494
Pharmaceutical 0495
Physical 0754
Polymer 0405
Radiation 0605
Mathematics 0986
Physics 0606
General 0608
Acoustics 0748
Astronomy and 0607
Astrophysics 0798
Atmospheric Science 0759
Atomic 0609
Electronics and Electricity 0610
Elementary Particles and 0752
High Energy 0756
Fluid and Plasma 0611
Molecular 0463
Nuclear 0346
Optics 0984
Radiation 0984
Solid State

Engineering 0537
General 0538
Aerospace 0539
Agricultural 0540
Automotive 0541
Biomedical 0542
Chemical 0543
Civil 0544
Electronics and Electrical 0348
Heat and Thermodynamics 0545
Hydraulic 0546
Industrial 0547
Marine 0794
Materials Science 0548
Mechanical 0743
Metallurgy 0551
Mining 0552
Nuclear 0549
Packaging 0765
Petroleum 0554
Sanitary and Municipal 0790
System Science 0428
Geotechnology 0796
Operations Research 0795
Plastics Technology 0994
Textile Technology

PSYCHOLOGY

General 0421
Behavioral 0384
Clinical 0622
Developmental 0620
Experimental 0623
Industrial 0624
Personality 0625
Physiological 0889
Psychobiology 0369
Psychometrics 0632
Social

The undersigned hereby recommend to
The Faculty of Graduate Studies and Research
acceptance of the thesis.

Graphical Properties of Quasi-Cyclic Codes

submitted by

Morteza Esmacili

in partial fulfilment of the requirements
for the degree of Doctor of Philosophy

Chairman, Department of Mathematics and Statistics

Thesis Supervisor

Thesis Supervisor

External Examiner

Carleton University

©M. Esmacili 1996

Abstract

The graphical properties of quasi-cyclic (QC) codes are investigated. As a first step, the trellis oriented generator matrix of a finitely generated vector space $\mathcal{V} = \mathcal{V}_1 \times \mathcal{V}_2 \times \cdots \times \mathcal{V}_n$ over a field F is introduced, where $\mathcal{V}_i$, $1 \leq i \leq n$, is a vector space over F . The smallest regular trellis diagram (SRTD) of a linear block code C is defined which is more applicable to soft decision decoding than the minimal trellis diagram (MTD). The SRTD of the class of cyclic-form codes, which includes cyclic codes as a subclass, along with a construction algorithm for this diagram is presented. Having introduced a canonical generator matrix M for QC-code C , both the MTD and SRTD of C are determined. This theory is used to find the 2^l -section MTD of the Reed-Muller code $\mathcal{R}(r, m)$, the 8-section SRTD of $\mathcal{R}(r, m)$, and the 2^l -section SRTD of $QC\mathcal{R}(r, m, l)$, which is the largest sub-code of $\mathcal{R}(r, m)$ invariant under a shift by 2^{m-l} positions.

Contents

1	INTRODUCTION AND PRELIMINARY RESULTS	1
1.1	Background	4
1.2	Branch Complexity	9
1.3	First Order Reed-Muller Codes	18
2	TRELLIS STRUCTURE OF LINEAR BLOCK CODES	22
2.1	Trellis Complexity of Generalized Linear Block Codes	23
2.2	Reed-Muller Codes	34
2.3	A Direct-sum Structure for Optimal $(4L,k,4)$ Linear Block Codes . . .	44
2.4	Summary	47
3	CANONICAL REPRESENTATION OF QUASI-CYCLIC CODES	49
3.1	Introduction	49
3.2	Canonical Generator Matrix	50
3.2.1	The Golay Code	55
3.2.2	Reed-Muller Codes	56
3.3	Quasi-Cyclic Codes in Cyclic Form	58
3.3.1	General Cyclic Codes	58
3.3.2	Cyclic Codes	59

3.4	1-Generator quasi-cyclic codes	61
3.5	Permutations and Quasi-Cyclic Codes	66
3.6	Summary	73
4	CYCLIC-FORM CODES AND THEIR SMALLEST REGULAR TRELLIS DIAGRAM	74
4.1	Introduction	74
4.2	Cyclic-Form Codes and Their SRTD	75
5	THE TRELLIS STRUCTURE OF QUASI-CYCLIC CODES	82
5.1	Introduction	82
5.2	Minimal Trellis Diagram	82
5.2.1	State and Branch Complexity	87
5.3	Smallest Regular Trellis Diagram	88
5.4	Applications	95
5.4.1	Reed-Muller Codes	95
5.4.2	Golay Code	96
5.4.3	Concatenated Codes	99
5.5	Summary	100
6	QUASI-CYCLIC STRUCTURE OF REED-MULLER CODES AND THEIR SMALLEST REGULAR TRELLIS DIAGRAM	101
6.1	Introduction	101
6.2	Quasi-Cyclic Structure of Reed-Muller Codes	102
6.3	Quasi-Cyclic Codes with Regular Minimal Trellis Diagrams Derived from Reed-Muller Codes	111
6.4	The Smallest Regular Trellis Diagram of Reed-Muller Codes	114
6.4.1	The Smallest Regular Trellis Diagram of $QCR(r, m, l)$	115
6.4.2	The 8-section Smallest Regular Trellis Diagram of $\mathcal{R}(r, m)$	116

6.5 Summary	120
7 CONCLUSIONS	121

Chapter 1

INTRODUCTION AND PRELIMINARY RESULTS

Introduction

In the application of error-correcting codes to communications systems, one of the most important problems is to develop and implement an efficient decoding algorithm for a given code. Ideally, one would also like the algorithm to be universal or applicable over a wide range of error-correcting codes. The Viterbi algorithm [27] provides such a solution for the decoding of convolutional codes through its use of the trellis diagram associated with the code. Bahl [23] and Wolf [24] demonstrated that one could also construct a trellis diagram for a block code and hence employ the Viterbi algorithm in its decoding. Wolf gave a simple algorithm for the construction of this trellis diagram and showed that for an (n, k) binary code, the trellis diagram has at most $2^{\min\{k, n-k\}}$ states. Forney [5] later gave a procedure for the construction of the *minimal* trellis diagrams¹ for the class of Reed-Muller codes and the (24,12) extended Golay code. In most instances, the code was found to have far fewer than 2^{n-k} states. That same year, Muder [18] rephrased Forney's work in graph theoretic terms. Since then, several authors [4, 9, 10, 11, 13] have studied the problem of

¹A *minimal* trellis diagram is the trellis having the least number of states among all trellis diagrams representing the code.

bounding the number of states in the minimal trellis diagram of an arbitrary block code, and finding minimal trellises for linear block codes. In particular, Kschischang and Sorokine [13] have studied the minimal trellis structure of a block code by making use of the shortest code words of the code called atomic code words.

A linear block code C of length n is called quasi-cyclic (QC) if it is invariant under a cyclic shift of m positions, i.e., T^m , where $m < n$. More precisely T is the cyclic shift operator which acts on the n -tuple $(c_1, c_2, \dots, c_n)$ as follows

$$T(c_1, c_2, \dots, c_n) = (c_n, c_1, c_2, \dots, c_{n-1}).$$

The analysis of the trellis structures of QC codes is the main goal of this dissertation.

In general, the minimal trellis diagram of a length n code is not regular, in the sense that the number of vertices in the diagram is not the same for all time indices i , $0 < i < n$. When the minimal trellis diagram is not regular a better (from an implementation point of view) non-minimal trellis may be found.

One of the most important factors in the evaluation of a trellis diagram is the number of identical non-communicating parallel sub-trellises in the trellis. The reason for this is that parallel sub-trellises allow for faster decoding.

In this work, the concept of a *smallest regular trellis diagram* (SRTD) is introduced. The term "smallest" is used to denote the fact that, in attempting to arrive at a regular trellis diagram, the resultant trellis is not necessarily minimal but it has the same state complexity (maximum number of states) as the minimal trellis. The SRTD has the maximum number of parallel sub-trellises, which is important in the decoding process. In those instances where the minimal trellis diagram has the same number of states at all time indices, except for the initial and final time indices, the SRTD is in fact the minimal trellis diagram.

The remainder of this Chapter presents the background for this thesis. The method used to derive the results is new and is mainly based on a trellis product

operation and the principle of induction. However, except for Theorem 1.2.3 there are no new results in this Chapter.

In Chapter 2, the work presented in [13] on the trellis structure of block codes has been extended to a Cartesian product of a finite set of vector spaces over the same field. This extension allows for a complete and extremely simple description of the 2^l -section minimal trellis diagrams of the Reed-Muller codes, compared to the complex presentation given by Kasami, *et al* [9]. As another application of this extension, a two-component direct-sum structure for optimal binary codes of length $4n$ and minimum distance 4 is introduced.

The theory developed in Chapter 2 is used to analyze QC codes. They have a module structure that can be considered an algebraic generalization of the ideal structure of cyclic codes. The ideal structure of a cyclic code determines a generator polynomial that can be used to construct a generator matrix that illustrates the cyclic structure of the code. In Chapter 3, a similar set of polynomial code words called *polynomial generator set* (PG-set) is introduced for QC codes that can be used to construct a *canonical generator matrix* (CG-matrix), illustrating the QC structure of the code. This presentation is illustrated by several examples including Reed-Muller codes and the (24, 12) extended Golay code.

The class of *cyclic-form* codes, including cyclic codes as a subclass, and their SRTD along with a construction algorithm are studied in Chapter 4. The SRTD of a QC codes can easily be derived using the structure of cyclic form codes.

Applying the canonical representation of QC codes and the graphical structure of cyclic-form codes presented in Chapters 3 and 4, respectively, the minimal trellis diagram and the smallest regular trellis diagram of QC codes is analyzed in Chapter 5. It is shown that the minimal trellis diagram of a QC code is symmetric about the center of the graph with a nondecreasing state space dimension on the left side. It is also proved that for a QC code C with canonical components $C_1, C_2, \dots$ and

C_i ,

$$t_{SR}(C) = \prod_{i=1}^p t_{SR}(C_i),$$

where $t_{SR}(C)$ is the number of identical parallel sub-trellises in the smallest regular trellis diagram of the code C . If C is not a QC code, then the above relation is not necessarily valid.

Forney [5] showed in 1988 that Reed-Muller codes have a relatively simple 4-section trellis structure. The underlying simplicity of this trellis structure stems from the quasi-cyclic structure of these codes as it is shown in Chapter 3. Further analysis of the QC structure of Reed-Muller codes is given in Chapter 6. In particular, $QC\mathcal{R}(r, m, l)$, the largest sub-code of the r -th order Reed-Muller code $\mathcal{R}(r, m)$ invariant under a shift of 2^{m-l} positions, and its smallest regular trellis diagram are presented in Chapter 6. The 8-section smallest regular trellis diagram of $\mathcal{R}(r, m)$ is also introduced in Chapter 6. In terms of VLSI implementation, a comparison of the 2^l section smallest regular trellis diagram of $QC\mathcal{R}(r, m, l)$ and the trellis diagram of $\mathcal{R}(r, m)$ shows that $QC\mathcal{R}(r, m, l)$ may be preferable to $\mathcal{R}(r, m)$.

1.1 Background

Let F be a field and let C be an (n, k) linear block code over F where n and k refer to the length and dimension of the code, respectively. For nonnegative integers i and j , the interval $[i, j]$ is said to be the span interval, or simply the span, of code word $c = (c_1, \dots, c_n) \in C$ if $c_i c_j \neq 0$, and $c_l = 0$ for $l < i$ and $j < l$. In this case the code word c is said to be *active* in the interval $[i, j-1]$, and has span length $j-i+1$. The *starting* and *ending* positions of c are defined to be i and j , respectively.

Definition 1.1.1 (Atomic Codeword) [13] A code word $c \in C$ is said to be an *atomic code word* if it cannot be expressed as a linear combination of code words of

C' with span lengths strictly smaller than that of c . The set of all atomic code words with the same span is called an atomic class.

Calling two code words of a linear block code C equivalent if they have the same span interval defines an equivalence relation on C . An equivalence class of the partition of C obtained by this relation consists of all code words having the same span interval. In this partition, any equivalence class containing an atomic code word is called an atomic class. This is due to the fact that if $a \in C$ is atomic and the span interval of $c \in C$ is the same as that of a , then c is also an atomic code word. An (n, k) linear block code has k distinct atomic classes² [13].

Linear block codes can be decoded using the Viterbi algorithm and a trellis. This idea was introduced by Bahl [23] and further investigated by Wolf [24]. For this purpose, a linear block code C can be represented by a minimal trellis diagram G in the sense that G has the minimum possible number of states at time index i , $0 \leq i \leq n$. In fact G is an edge labeled directed graph with unique initial and final vertices v_0 and v_n , such that

1. Each directed path connecting v_0 and v_n has length n (and is associated with one code word of C).
2. Two paths representing two different code words differ in at least one edge.
3. The number of vertices of G at distance i , $1 \leq i \leq n$, from v_0 is the minimum possible.

Using the terminology of dynamic systems [6], the vertices of G at distance i , $0 \leq i \leq n$, from v_0 are called the *states* at time index i .

Other than the concept of an atomic code word, all that is required is the graph multiplication operation in order to construct the minimal trellis diagram of a linear block code.

²This can be considered a consequence of Theorem 2.1.1.

Figure 1.1: (a) : G' ; (b) : G'' ; (c) : $G' \times G''$

Definition 1.1.2 (Trellis Product) [13] The product $G' \times G''$ of two length n trellises $G' = (V', E', A)$ and $G'' = (V'', E'', A)$, is defined by

$$G' \times G'' = \left(\bigcup_{i=0}^n V'_i \times V''_i, \bigcup_{i=1}^n E'_i \times E''_i, A \right)$$

with

$$(c', c'') = ((v'_1, a', v'_2), (v''_1, a'', v''_2)) := ((v'_1, v''_1), a' + a'', (v'_2, v''_2))$$

where

$$c' \in E', c'' \in E'', v' \in V', v'' \in V'', \text{ and } a', a'' \in A.$$

Note that V , E , and A in a trellis $G = (V, E, A)$ refer to the vertex, edge, and label sets, respectively. V_i refers to the set of vertices of G at time index i and E_i denotes the set of edges of G connecting the elements of V_{i-1} to the elements of V_i . A is a semi-group under the operation '+'. Definition 1.1.2 is illustrated in Fig. 1.1. The product of k trellises of the same length follows by induction on the definition. Note that the components of code word c are the labels of a path in the minimal trellis diagram of the code. In this work the labeling is ignored, as we are only concerned with the trellis structure.

For $0 \leq i \leq n-1$, let

$$i^- = \{0, 1, \dots, i\} \quad , \quad i^+ = \{i+1, i+2, \dots, n\} \quad (1.1)$$

and define $C_{i,-}$ and $C_{i,+}$ as

$$\begin{aligned} C_{i,-} &= \{c \in C : c_j = 0, \quad i+1 \leq j \leq n\} \\ C_{i,+} &= \{c \in C : c_j = 0, \quad 1 \leq j \leq i\} \end{aligned} \quad (1.2)$$

Figure 1.2: The minimal trellis diagram of the $(n, 1)$ linear block code C generated by code word c with span interval $[a, b]$.

In addition, define $C_{0+} = C_{n-} = C$.

Let Z be the set of integers and $\{G_i\}_{i \in Z}$ be a set of groups. The direct-sum group $G = \bigoplus_{i \in Z} G_i$ is called a group code [6].

Theorem 1.1.1 (State Space Theorem) [6] *The number of states at time index i in the minimal trellis diagram G of a group code C is equal to the cardinality of the quotient group $\frac{C}{C_{i-}C_{i+}}$.*

Fig. 1.2 is the minimal trellis diagram of the $(n, 1)$ linear code C generated by code word c with span interval $[a, b]$.

It is shown in [13] that if G_i , $1 \leq i \leq k$, is the minimal trellis diagram of atomic code word $a^{(i)}$, where the $a^{(i)}$ are from k distinct atomic classes of C , then $G = G_1 \times G_2 \times \dots \times G_k$ is the minimal trellis diagram of C . Therefore we have the following definition.

Definition 1.1.3 (Trellis Oriented Generator Matrix) *Let C be an (n, k) linear block code. Any $k \times n$ matrix in which each row is a representative of one of the k distinct atomic classes of C is called a trellis oriented generator matrix (TOGM) for C .*

Since all atomic code words in one atomic class, say A , have the same minimal trellis diagram, hereafter we will use the term "minimal trellis diagram of atomic class A ".

Figure 1.3: Minimal trellis diagrams for the code with generator matrix M in example 1.1.1.

Theorem 1.1.2 [13] *The generator matrix M of a linear block code C is a TOGM iff no two rows of M either start or end in the same position³.*

Example 1.1.1 The following generator matrix M representing a linear $(8,3)$ code is a TOGM

$$M = \begin{bmatrix} 1 & * & * & * & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & * & * & * & * & 1 \\ 0 & 0 & 0 & 1 & * & 1 & 0 & 0 \end{bmatrix}. \quad (1.3)$$

The minimal trellis diagrams corresponding to the rows of this matrix, denoted by G_1 , G_2 , and G_3 , and the minimal trellis diagram of the code are given in Fig 1.3. The entries in M denoted by $*$ have no effect on the structure of the trellis for C .

Define the set of all atomic classes of C by $\mathcal{A}(C)$, or simply $\mathcal{A}$. For $\hat{C}$ a linear sub-code of C , let $\mathcal{A}(\hat{C})$ denote the set of all atomic classes of C contained in $\hat{C}$. For $C_{i,-}$ and $C_{i,+}$, this is denoted by $\mathcal{A}([1, i])$ and $\mathcal{A}([i + 1, n])$, respectively. In general, $\mathcal{A}([i, j])$ denotes the set of all atomic classes of C with span in $[i, j]$. Let $\mathcal{E}([i, j])$ denote the set of atomic classes of C with span that ends in $[i, j]$, and $\mathcal{I}([i, j])$ denote

³Theorem 2.1.2 is a generalization of this theorem.

the set of all atomic classes of C with span that begins in $[i, j]$. Given that an atomic class with span $[a, b]$ is active in the interval $[a, b - 1]$, no element of either $A([1, i])$ or $A([i + 1, n])$ can be active at time i , and in fact atomic code word c is active at time i if and only if

$$c \notin A([1, i]) \cup A([i + 1, n]).$$

Therefore we have the following theorem.

Theorem 1.1.3 [6] $S_i(C) = k - |A([1, i]) \cup A([i + 1, n])|$, where $2^{S_i(C)}$ is the number of states at time index i in the minimal trellis diagram of C . $S_i(C)$, or simply S_i , is defined as the state space dimension at time index i .

Lemma 1.1.1

$$c \in C_{i-} \text{ (resp. } C_{i+}), \iff \text{span}(c) \subseteq [1, i] \text{ (resp. } \subseteq [i + 1, n]).$$

where $\text{span}(c)$ denotes the span interval of c .

The proof follows directly from (1.2) and so is omitted. Define $\mathcal{K}(C)$ to be the dimension of C .

Corollary 1.1.1

$$\begin{aligned} \mathcal{K}(C_{i-}) &= |A([1, i])|, \\ \mathcal{K}(C_{i+}) &= |A([i + 1, n])|, \end{aligned} \tag{1.4}$$

and $\mathcal{K}(C_{0-})$ and $\mathcal{K}(C_{n+})$ are defined to be zero. It follows that $\mathcal{K}(C_{0+}) = \mathcal{K}(C_{n-}) = n$.

As an example Table 1 presents the parameters of the linear (8,3) code C with TOGM M given by (1.3).

1.2 Branch Complexity

For simplicity, only binary linear codes are considered in this section. However, the results hold for q -ary linear codes if base 2 is replaced by q .

i	0	1	2	3	4	5	6	7	8
$ A([1, i]) $	0	0	0	0	0	1	2	2	3
$ A([i + 1, n]) $	3	2	2	1	0	0	0	0	0
$ A([1, i]) \cup A([i + 1, n]) $	3	2	2	1	0	1	2	2	3
S_i	0	1	1	2	3	2	1	1	0

Table 1.1: Parameters of the (8,3) binary linear code with generator matrix M given by (1.3).

Let V be the set of vertices of the minimal trellis diagram, G , of a linear (n, k) block code C , and let V_i be the set of vertices at time index i , $0 \leq i \leq n$. For $1 \leq i \leq n$, let $T_i(G) \equiv G - (V_i \cup V_{i-1})^c$ where B^c denotes the complement of the set B [7]. In other words, $T_i(G)$ is the subgraph of G consisting of vertices at time index i and $i - 1$ with edges connecting these two sets of vertices in G . Considering G as an oriented graph, denote the number of edges entering vertex $v \in V$ by $ed(v)$, and the number of edges leaving v by $ld(v)$.

Lemma 1.2.1 *In V_i , the set of vertices of the minimal trellis diagram G of C at time i , all vertices have the same entering and leaving degrees, i.e.,*

$$\begin{aligned} ed(v) &= ed(u) \\ ld(v) &= ld(u), \end{aligned} \tag{1.5}$$

for all $v, u \in V_i$. Moreover, for binary codes these degrees are either 1 or 2, except for the initial and final time indices 0 and n , respectively.⁴

Proof Let G_1 and G_2 be the minimal trellis diagrams of atomic classes A_1 and A_2 , respectively, such that A_1 vanishes at time i and A_2 emerges at time $i + 1$ (if these atomic classes exist). From the definition of graph multiplication, $G_1 \times G_2$

⁴Note that for q -ary codes, the degrees $ed(v)$ and $ld(v)$ are either 1 or q , except at the initial and final time indices, 0 and n .

has precisely one vertex at time i , and this unique vertex has entering and leaving degree 2, as shown in Fig. 1.4.

Figure 1.4: The trellis product, $G_1 \times G_2$, at time i .

Let G_3 be the minimal trellis diagram of atomic class A_3 active at time i (if such an atomic class exists). Then $G_1 \times G_2 \times G_3$ has 2 vertices at time i , both of which have entering and leaving degree 2. Now, considering $G_1 \times G_2$ and applying induction on m , the number of atomic classes active at time i , we see that

$$|V_i| = 2^m \quad (1.6)$$

and all vertices in V_i have leaving and entering degree 2. Note that non-active classes at time i do not affect the trellis G at time i .

This argument can also be applied in cases where just G_1 or G_2 exists, or neither exists. ♣

Corollary 1.2.1 $b(T_i(G))$, the number of edges of $T_i(G)$, satisfies

$$b(T_i(G)) = 2^{S_i} \text{ed}(v_i) = 2^{S_{i-1}} \text{ld}(v_{i-1}) \quad (1.7)$$

where v_i and v_{i-1} are arbitrary elements of V_i and V_{i-1} , respectively.

$T_i(G)$ is a bipartite graph. Let $t_i(G)$ denote the number of components in $T_i(G)$, and define this as the sub-trellis number of G at time i . For simplicity in Lemma 1.2.2, define

$$\begin{aligned} I &= \{i : \text{some atomic class starts at time } i, 1 \leq i \leq n\} \\ E &= \{i : \text{some atomic class ends at time } i, 1 \leq i \leq n\}. \end{aligned} \quad (1.8)$$

Figure 1.5: Form for the components of $T_i(G)$. (a): $i \in I, i \notin E$; (b): $i \in I \cap E$ and $A([i]) = \emptyset$; (c): $i \in I \cap E$ and $A([i]) \neq \emptyset$; (d): $i \notin I, i \in E$; (e): $i \notin I \cup E$.

In the following lemma $A([i])$ denotes the set of atomic classes with both starting and ending position i . This set has at most one element.

Lemma 1.2.2 *Let C be an (n, k) linear block code with minimal trellis diagram G . Then, for $1 \leq i \leq n$,*

$$t_i(G) = \begin{cases} 2^{S_i-1} & \text{if } i \in I \text{ and } i \notin E \\ 2^{S_i-1} & \text{if } i \in I \cap E \text{ and } A([i]) = \emptyset \\ 2^{S_i} & \text{otherwise.} \end{cases} \quad (1.9)$$

Moreover all components of $T_i(G)$ are identical, and have one of the forms given in Fig. 1.5.

Proof

- 1- Suppose $i \in I$ and $i \notin E$. By Lemma 1.2.1 $ed(v) = 1$ for all $v \in V_i$, and $ld(v) = 2$ for all $v \in V_{i-1}$. Hence each vertex in V_{i-1} is linked with exactly 2 vertices of V_i . Corollary 1.2.1 now implies that $t_i(G) = 2^{S_i-1}$.
- 2- Suppose $i \in I \cap E$, and that A_1 and A_2 are distinct atomic classes which vanish and emerge at time i , respectively. Then $T_i(G_1 \times G_2)$, where G_1 and G_2 are the graphs corresponding to A_1 and A_2 , respectively, is a complete bipartite graph with 2 vertices in each part. Applying induction on S_i , the number of atomic classes active at time i , we see that the number of copies of $T_i(G_1 \times G_2)$ is 2^{S_i-1} . In fact, $T_i(G)$ is the union of these copies of $T_i(G_1 \times G_2)$.

- 3- If $i \in I \cap E$ and atomic code word c has both starting and ending position i , then no other atomic code word either start or end in position i . In this case $t_i(G) = 2^{S_i}$ and each component of $T_i(G)$ has the form given by Fig. 1.5.(c).

For the case $i \notin I$, corresponding to (d) and (e) in Fig. 1.5, the proof is similar and hence is omitted. ♣

Let $T_{ij}(G)$, $0 \leq i < j \leq n$, or simply T_{ij} , denote the bipartite graph with vertices V_i and V_j (the set of vertices of G at time i and j , respectively), and edges connecting vertex $v_i \in V_i$ to $v_j \in V_j$ iff these two vertices are connected in G . Then if there are d paths in G which connect v_i to v_j , they are connected by d edges in T_{ij} , meaning that T_{ij} is not necessarily a simple bipartite graph.

Theorem 1.2.1 *Let C be an (n, k) linear block code. The number of edges of T_{ij} entering vertex $v_j \in V_j$ is*

$$ed(v_j) = 2^{|E([i+1, j])|}. \quad (1.10)$$

It follows that the number of edges of T_{ij} , $|E(T_{ij})|$, is

$$|E(T_{ij})| = 2^{S_j + |E([i+1, j])|} \quad (1.11)$$

where S_j is the number of atomic classes active at time j .

Proof The proof is by induction on $|E([i+1, j])| \equiv e_{ij}(C)$. If $e_{ij}(C) = 0$, then the atomic class A_l , $1 \leq l \leq k$, has a minimal trellis graph G_l such that $T_{ij}(G_l)$ consists of either one path or 2 parallel paths. Therefore $T_{ij}(G) = T_{ij}(\prod_{l=1}^k G_l)$ consists of a number of parallel paths so that $ed(v_j) = 2^0 = 1$.

Let $e_{ij}(C) \geq 1$ and suppose that the theorem holds for any code C' with $e_{ij}(C') < e_{ij}(C)$. Let $G_1, G_2, \dots, G_k$ be the minimal trellis diagrams of atomic classes $A_1, A_2, \dots, A_k$, respectively, in C such that $A_1 \in E([i+1, j])$. The linear sub-code C' with atomic classes $A_2, A_3, \dots$, and A_k meets the induction hypothesis, and hence

$$ed(v'_j) = 2^{e_{ij}(C')} = 2^{e_{ij}(C)-1},$$

where $v'_j \in T_{ij}(G'') = T_{ij}(\prod_{l=2}^k G_l)$. The remainder of the proof follows from

$$G \approx G'' \times G_1 \quad \text{and} \quad T_{ij}(G) = T_{ij}(G'') \times T_{ij}(G_1).$$

In fact one copy of G'' is placed on each of the two paths of G_1 . Equivalently, since $A_1 \in E([i+1, j])$, one copy of $T_{ij}(G'')$ is placed on each path(edge) of $T_{ij}(G_1)$.

$T_{ij}(G_1)$ consists of two converging paths (edges), resulting in $ed(v_j) = 2 \times ed(v'_j) = 2^{o(C)}$. Equation (10) is simply the result of (9) and the fact that in the bipartite graph T_{ij} , $|V_j| = 2^S$. ♣

Remark The proof of Theorem (1.2.1) implies that

$$ld(v_i) = 2^{l([i+1, j])} \quad (1.12)$$

where $v_i \in V_i$ is a vertex of T_{ij} at time index i . This is in fact (1.10), with the direction of the directed graph G reversed.

From (1.11) and (1.12) we obtain

Corollary 1.2.2

$$S_j + |E([i+1, j])| = S_i + |l([i+1, j])|, \quad 0 \leq i < j \leq n. \square \quad (1.13)$$

Theorem 1.2.2 Let C be a linear (n, k) code with minimal trellis diagram G .

1. For $0 \leq i < j \leq n$, T_{ij} is a simple bipartite graph iff no atomic class has span $[a, b]$ contained in $[i+1, j]$; i.e., iff $A([i+1, j]) = \emptyset$. Each component of T_{ij} is a complete bipartite graph. Furthermore, the number of edges of T_{ij} connecting 2 adjacent vertices, $v_i \in V_i$ and $v_j \in V_j$, is

$$\alpha_{ij}(G) = 2^{|A([i+1, j])|}. \quad (1.14)$$

2. The number of components of T_{ij} [7], denoted by $t_{ij}(G)$, is

$$t_{ij}(G) = 2^{|l([1, i]) \cap E([i+1, n])|}, \quad (1.15)$$

and in terms of the graph structure, all of these components are identical.

Proof Consider the following partition of $E([i+1, j])$:

$$E([i+1, j]) = A([i+1, j]) \cup (E([i+1, j]) \cap I([1, i])).$$

Let $\hat{G}$ denote the graph obtained from the product of the graphs corresponding to the elements of $A([i+1, j])$. In $\hat{G}$, precisely $2^{|A([i+1, j])|}$ paths connect the unique vertex $\hat{v}_i \in \hat{V}_i$ to the unique vertex $\hat{v}_j \in \hat{V}_j$, where $\hat{V}_i$ and $\hat{V}_j$ are the singleton set of vertices of $\hat{G}$ at time indices i and j , respectively.

Now, take one element of $E([i+1, j]) \cap I([1, i])$, assuming one exists, and multiply its corresponding minimal graph by $\hat{G}$. The number of vertices of the resulting graph at time index i is doubled, and each is connected to the unique vertex at time j by $2^{|A([i+1, j])|}$ paths. Finally, the minimal trellis diagram $\hat{G}$ associated with $E([i+1, j])$ is obtained, in which any vertex at time index i is connected to the unique vertex at time index j by $2^{|A([i+1, j])|}$ paths (in fact this can be proved by induction on $m = |E([i+1, j]) \cap I([1, i])|$).

If $A_l \in I([i+1, j]) \cap E([j+1, n])$, then $\hat{G} \times G_l$ has two vertices at time index j , each of which is connected to each vertex at time i by $2^{|A([i+1, j])|}$ paths. This occurs because a copy of $\hat{G}$ is placed on each of the two paths in G_l . Inductively, by applying an element of $I([i+1, j]) \cap E([j+1, n])$, the number of vertices of the resulting graph at time index j is doubled while their entering degrees remains unchanged. Therefore, the graph G associated with

$$\mathcal{A}_1 = E([i+1, j]) \cup (I([i+1, j]) \cap E([j+1, n]))$$

has the following properties:

1. V_i , the set of vertices of G at time index i , has cardinality

$$|V_i| = 2^{|E([i+1, j]) \cap I([1, i])|}$$

2. V_j , the set of vertices of G at time index j , has cardinality

$$|V_j| = 2^{|I([i+1, j]) \cap E([j+1, n])|}$$

3. Any vertex in V_i is connected with any vertex in V_j by $2^{|A([i+1,j])|}$ paths.

The remaining atomic classes of C are precisely the elements of $\mathcal{A}_2 = I([1,i]) \cap E([j+1,n])$. Let G_0 be the minimal trellis diagram obtained from the product of the graphs of atomic classes in $\mathcal{A}_2$.

$T_{ij}(G_0)$ consists of $2^{|\mathcal{A}_2|}$ parallel paths by induction on $|\mathcal{A}_2|$. The fact that

$$G = G \times G_0,$$

implies that:

1. T_{ij} consists of $2^{|I([1,i]) \cap E([j+1,n])|}$ identical bipartite components.
2. The set of vertices of each component has properties 1, 2 and 3 stated above for G . ♣

In decoding C using the Viterbi algorithm, it may be advantageous to use a modified form of G called the L -section trellis instead of the n -section minimal trellis diagram of G .

Definition 1.2.1 (L-Section Trellis Diagram of a Linear Block Code) *Let C be a linear block code of length $n = Lm$. Consider the set of time indices $I = \{mk : 0 \leq k \leq L\}$. Suppose G is a minimal trellis diagram of C . Construct a new graph G in the following way:*

1. *Delete all the vertices and edges of G except those vertices that belong to V_{im} , for some $0 \leq i \leq L$.*
2. *For the remaining set of vertices connect $v \in V_{im}$ to $u \in V_{(i+1)m}$ by t edges iff v and u as two vertices of G are connected by t paths in G .*

The resultant graph is called the minimal L -section trellis diagram of C .

In fact this is a minimal diagram since the number of vertices of this graph at time index $i, 0 \leq i \leq L$ is the same as that of G at time im . An immediate consequence of Theorem 1.2.2 is the following.

Corollary 1.2.3 (Complexity of the Minimal L -Section Trellis Diagram)

Let C be a linear (n, k) block code with $n = Lm$, and let G be a minimal L -section trellis diagram for C . For $1 \leq i \leq L$, $T_i(G)$ has the following properties:

1. $T_i(G)$ is a simple bipartite graph iff no atomic class has span interval $[a, b]$ contained in $[im - m + 1, im]$. Furthermore, the number of edges of $T_i(G)$ connecting 2 adjacent vertices, $v_{i-1} \in V_{i-1}$ and $v_i \in V_i$, is $\alpha_i(G) = 2^{|A([im-m+1, im])|}$.
2. The number of components of $T_i(G)$ is $t_i(G) = 2^{|I([1, m-m]) \cap E([im+1, n])|}$, and all of these components are identical in terms of their graph structure.
3. Each of the components of $T_i(G)$ is a complete bipartite graph.

In terms of the Viterbi algorithm, it is desirable to obtain an L -section trellis graph which consists of several parallel sub-trellises. The following theorem determines the number of such identical components, in terms of the graph structure, in the L -section minimal trellis diagram of C .

Theorem 1.2.3 *Let C be an (n, k) linear block code with L -section minimal trellis diagram G , and $n = Lm$. Then G consists of 2^{k_t} identical (in terms of the graph structure) parallel sub-trellises, where*

$$k_t = |I([1, m]) \cap E([n - m + 1, n])|. \quad (1.16)$$

Proof Let $A_1 \in \mathcal{A}_1 \equiv I([1, m]) \cap E([n - m + 1, n])$ be an atomic class of C . In the L -section trellis diagram of C , this atomic class has the minimal trellis diagram shown in Fig. 1.6. Hence, induction on $|\mathcal{A}_1|$ shows that G , the graph corresponding to the set of atomic classes in $\mathcal{A}_1$, consists of 2^{k_t} paths connecting the unique vertex

Figure 1.6: Minimal L section trellis diagram of $A_1 \in I([1, m]) \cap E([n - m + 1, n])$

$v_0 \in V_0$ to the unique vertex $v_n \in V_n$ without any cross connections. On the other hand, if $A \notin \mathcal{A}_1$ then its L -section trellis diagram consists of 2 paths which share at least either the first or last edge. This implies that in the multiplication of the minimal L -section trellis diagrams of 2 elements of $\mathcal{A} - \mathcal{A}_1$, the resulting graph does not have any parallel sub-trellises where $\mathcal{A}$ denotes the set of atomic classes of C . Now induction on the cardinality of $\mathcal{A} - \mathcal{A}_1$ shows that $\hat{G}$, the minimal L -section trellis diagram corresponding to $\mathcal{A} - \mathcal{A}_1$, does not have any parallel sub-trellises. Since $G = G \times \hat{G}$, G is a graph with 2^k identical parallel sub-trellises, each of which is a copy of the graph $\hat{G}$. ♣

1.3 First Order Reed-Muller Codes

As an example, the trellis structure of the first order Reed-Muller codes is analyzed based on the TOGM.

Consider the first order Reed-Muller code $\mathcal{R}(1, m)$ with generator matrix

$$M = \begin{bmatrix} v_0 \\ v_m \\ v_{m-1} \\ \vdots \\ v_1 \end{bmatrix}.$$

v_0 has Hamming weight 2^m , and v_i , $1 \leq i \leq m$, is the concatenation of 2^{m-i} identical blocks of length 2^i , each of which is divided into 2 sub-blocks of length 2^{i-1} such that

the first sub-block is the string of all ones, and the second sub-block is the string of all zeros. By row operations M can be transformed into the following generator matrix

$$M' = \begin{bmatrix} v_m \\ v_m + v_{m-1} \\ v_m + v_0 \\ v_{m-2} \\ \vdots \\ v_1 \end{bmatrix}.$$

The first $n/4$ elements of the vectors $v_m + v_{m-1}$ and $v_m + v_0$ are all zeros. Denote the first $n/4$ elements of the vectors $v_m, v_1, v_2, \dots, v_{m-2}$ by $\hat{v}_m, \hat{v}_1, \hat{v}_2, \dots, \hat{v}_{m-2}$, respectively. Since the matrix

$$\hat{M} = \begin{bmatrix} \hat{v}_m \\ \hat{v}_{m-2} \\ \vdots \\ \hat{v}_1 \end{bmatrix}$$

is a generator matrix for $\mathcal{R}(1, m-2)$, the rows of $\hat{M}$ are linearly independent. Note that the independence of these vectors can be proved by induction on m . The 4-section minimal trellis diagram of $\mathcal{R}(1, m)$ is now introduced.

Theorem 1.3.1 *The first order Reed-Muller code $\mathcal{R}(1, m)$ has a minimal 4-section trellis diagram consisting of 2^{m-2} identical parallel sub-trellises. Moreover, each of these sub-trellises is a copy of the minimal 4-section trellis diagram of the sub-code $\hat{\mathcal{C}}$ generated by the 3 vectors v_0, v_m and v_{m-1} .*

Proof From the foregoing arguments and notation, there are $m-1$ rows in M' which do not have all zeros in the first $n/4$ elements. Since the first $n/4$ elements of these vectors (the rows of $\hat{M}$) are independent, with elementary row operations on the set $A = \{v_1, v_2, \dots, v_{m-2}, v_m\}$, none of the rows of M' can be transformed into a vector with all zeros in its first $n/4$ elements. Therefore, $m-1$ atomic classes are in

$I([1, 2^{m-2}])$, and the starting position of these atomic classes is determined only by elementary row operations on the set A . This also implies that the initial positions of $v_m + v_0$ and $v_m + v_{m-1}$ are in fact the starting positions of the 2 remaining atomic classes.

The transformation of M' into a row reduced matrix $\bar{M}$ can be done such that v_m , $v_m + v_{m-1}$ and $v_m + v_0$ remain as rows of $\bar{M}$. The set of nonzero vectors consisting of the last $n/4$ elements of the rows of M' is precisely the set of rows of $\bar{M}$. Therefore, in the row reduced matrix $\bar{M}$

$$\bar{M} = \begin{bmatrix} v_m \\ v_m + v_{m-1} \\ v_m + v_0 \\ u_{m-2} \\ \vdots \\ u_1 \end{bmatrix},$$

the set $B = \{\bar{v}_m + \bar{v}_0, \bar{u}_{m-2}, \dots, \bar{u}_1\}$ is independent, where $\bar{v}$ denotes the last $n/4$ elements of v . This implies that in the transformation of $\bar{M}$ into the trellis oriented generator matrix M_t , $m - 1$ atomic classes have their final nonzero digit in the interval $[3 \times 2^{m-2} + 1, 2^m]$, and these can be determined using only row operations on the vectors $u_1, \dots, u_{m-2}$ and $v_m + v_0$ such that $v_m + v_0$ remains unchanged. Note that the first $n/4$ elements of $v_m + v_0$ are all zero and hence by adding this vector to any row of $\bar{M}$ the new matrix is in reduced row echelon form.

In summary, v_m , $v_m + v_0$ and $v_m + v_{m-1}$ are atomic code words, and the rest of the atomic classes are in $I([1, 2^{m-2}]) \cap E([3 \times 2^{m-2} + 1, 2^m])$. This completes the proof based on Theorem 3. ♣

Remark The minimal 4-section trellis diagram of the code generated by the three vectors $v_m, v_m + v_0$ and $v_m + v_{m-1}$ is known. Therefore Theorem 1.3.1 provides sufficient information to determine the complexity of the minimal 4-section trellis diagram of $\mathcal{R}(1, m)$.

Figure 1.7: 4-section trellis diagram of the Reed-Muller code $\mathcal{R}(1,4)$.

Example 1.3.1 For $m = 4$, we have the following three matrices:

$$M = \begin{bmatrix} v_0 \\ v_4 \\ v_3 \\ v_2 \\ v_1 \end{bmatrix} = \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 1111 & 1111 & 0000 & 0000 \\ 1111 & 0000 & 1111 & 0000 \\ 1100 & 1100 & 1100 & 1100 \\ 1010 & 1010 & 1010 & 1010 \end{bmatrix},$$

$$M' = \begin{bmatrix} v_4 \\ v_4 + v_3 \\ v_4 + v_0 \\ v_2 \\ v_1 \end{bmatrix} = \begin{bmatrix} 1111 & 1111 & 0000 & 0000 \\ 0000 & 1111 & 1111 & 0000 \\ 0000 & 0000 & 1111 & 1111 \\ 1100 & 1100 & 1100 & 1100 \\ 1010 & 1010 & 1010 & 1010 \end{bmatrix},$$

and

$$M_t = \begin{bmatrix} v_4 \\ v_4 + v_3 \\ v_4 + v_0 \\ u_2 \\ u_1 \end{bmatrix} = \begin{bmatrix} 1111 & 1111 & 0000 & 0000 \\ 0000 & 1111 & 1111 & 0000 \\ 0000 & 0000 & 1111 & 1111 \\ 0101 & 0101 & 1010 & 1010 \\ 0011 & 0011 & 1100 & 1100 \end{bmatrix}.$$

M_t gives the minimal 4-section trellis diagram for $\mathcal{R}(1,4)$ which is shown in Fig. 1.7.

Chapter 2

TRELLIS STRUCTURE OF LINEAR BLOCK CODES

In the previous chapter, the minimal trellis structure of an (n, k) linear block code C over a field F was studied with C a k -dimensional subspace of an n -dimensional vector space $F^{(n)}$ over F . This chapter provides a generalization of this study. More precisely, the trellis complexity of a linear block code C over a field F is presented for C a subspace of the vector space $\mathcal{V} = \prod_{i=1}^n \mathcal{V}_i$ over F , and $\mathcal{V}_i$ ($1 \leq i \leq n$) a vector space over F . This is done by characterizing the trellis oriented generator matrix of the code. This provides an approach for an extremely simple and comprehensive analysis of the trellis structure of Reed-Muller codes. Specifically a generator matrix for the Reed-Muller codes is presented which is in trellis oriented form for the minimal 2^l -section trellis diagram. As another application of this theory, a decomposition is given for $(n, k, d) = (4L, k, 4)$ optimal linear block codes into two sub-codes such that the L -section minimal trellis diagram of the code is the product of those of the two sub-codes.

Note that in this chapter, an (n, k) linear block code C over F is considered as a subspace of $\mathcal{V} = \prod_{i=1}^n \mathcal{V}_i$, where $\mathcal{V}_i$ is a vector space over F . In this case, the i^{th} component of a code word in C is a vector in $\mathcal{V}_i$, so that C may not be a subspace of F^n (this is true only if $\mathcal{V}_i = F, 1 \leq i \leq n$). Although in the literature such a

code is known as a mixed code, in this thesis it is called a linear block code since the theory is used to study the trellis structure of linear block codes. The analysis of the L -section minimal trellis diagram of block codes may be considered as an application of this theory.

When studying the minimal L -section trellis diagram of a length n linear block code, where the length of some sections is greater than one, this technique allows one to consider all the bit positions in each section as a symbol. This in turn allows a theoretical analysis of the trellis oriented generator matrix for the L -section trellis diagram of a code without having to transfer the generator matrix of the code into a TOGM for the n -section minimal trellis diagram, in the sense of [13] (Theorem 1.1.2). This is indeed the key point when the 2^l -section trellis diagram of Reed-Muller codes is presented later in this Chapter.

In Section 2.2, a study of the minimal 2^l -section trellis diagrams of Reed-Muller codes is presented. In this regard there are two noteworthy points. The first is that Theorem 2.2.1 and Corollary 2.2.2 are new results and provide significant information about the structure of Reed-Muller codes. The second point is that the results, both new and previously known, are derived in an extremely simple and more intuitive way than in other presentations.

The decomposition of a $(4L, k, 4)$ binary linear block code C into two sub-codes C_1 and C_2 is given in Section 2.3. The code C is optimal iff C_1 and C_2 are optimal. In addition, the minimal trellis diagram of C is the product of that of C_1 and C_2 .

2.1 Trellis Complexity of Generalized Linear Block Codes

The dynamics of group codes [6] motivates the classification of this large class of codes and specifically a presentation of the trellis oriented generator matrix for

those subclasses that possess such a generator matrix. Let $\mathcal{V}_i$, $1 \leq i \leq n$, be a vector space over F and C (a linear block code) be a finitely generated subspace of the vector space $\mathcal{V} = \prod_{i=1}^n \mathcal{V}_i$. Then a trellis oriented generator matrix of C can be constructed for which the trellis complexity of C is completely determined. Forney [5] has mentioned that any generator matrix can be transformed into a trellis oriented form. In this Section we prove this statement and determine the atomic code words of C . Note that the definition of C is more general here than in the previous Chapter, where $\mathcal{V}_i = F$. In fact if $\mathcal{V}_i = F(q)$, $1 \leq i \leq n$, then C is a q -ary linear block code. As a special case, we determine the L -section trellis diagram of a q -ary linear block code when the sections are of arbitrary lengths.

A general definition of a row reduced generator matrix is used to define the trellis oriented generator matrix.

Let M be an $m \times n$ matrix in which the entries in the j^{th} column, $1 \leq j \leq n$, are in the vector space $\mathcal{V}_j$. M_j , $1 \leq j \leq n$, denotes the $m \times j$ matrix which is the same as M in its i^{th} column, $1 \leq i \leq j$.

Definition 2.1.1 (Row Reduced Matrix) *The matrix M is said to be in row reduced form if the nonzero rows of M_i , $1 \leq i \leq n$, are linearly independent.*

Any matrix M , with rows in $\prod_{i=1}^n \mathcal{V}_i$, can easily be transformed into an equivalent row reduced matrix. If p_i , $1 \leq i \leq n$, is the rank of M_i , then by elementary row operations M can be transformed into a matrix M^1 such that the nonzero entries in the first column are linearly independent and are located in the upper p_1 rows of the first column. Applying row operations on those rows of M^1 that are zero in the first column, we can transform M^1 into M^2 such that

1. M^1 and M^2 are the same in their first p_1 rows,
2. The nonzero entries of M^2 in the second column after the p_1^{th} row are linearly independent and located in the upper section below the p_1^{th} row.

The row reduced matrix $\bar{M}$ can be obtained in this manner with a finite number of row operations.

Example 2.1.1 Let $n = 4$, $F = GF(2)$, $\mathcal{V}_1 = F^3$, $\mathcal{V}_2 = F^5$, $\mathcal{V}_3 = F^2$, $\mathcal{V}_4 = F^6$, and let C be a subspace of $\mathcal{V} = \prod_{i=1}^4 \mathcal{V}_i$ with generator matrix

$$M = \begin{bmatrix} 111 & 10111 & 10 & 000000 \\ 100 & 01111 & 10 & 001111 \\ 100 & 00000 & 11 & 110111 \\ 100 & 00000 & 00 & 001111 \end{bmatrix}.$$

Note that C is a $(4, 4)$ linear block code, and M is a 4×4 matrix whose i^{th} column contains elements from $\mathcal{V}_i$. Adding the second row to the third and fourth rows results in the matrix

$$M^1 = \begin{bmatrix} 111 & 10111 & 10 & 000000 \\ 100 & 01111 & 10 & 001111 \\ 000 & 01111 & 01 & 111000 \\ 000 & 01111 & 10 & 000000 \end{bmatrix}.$$

Finally, by adding the third row to the fourth in M^1 , we obtain

$$M^2 = \begin{bmatrix} 111 & 10111 & 10 & 000000 \\ 100 & 01111 & 10 & 001111 \\ 000 & 01111 & 01 & 111000 \\ 000 & 00000 & 11 & 111000 \end{bmatrix},$$

which is, according to the definition, in row reduced form.

Definition 2.1.2 (Canonical Matrix) Let M be an $m \times n$ row reduced matrix whose entries in the j^{th} column are in the vector space $\mathcal{V}_j$ over F . Then M is said to be in canonical form if for each j , $1 \leq j \leq n$, the set of all nonzero entries in the j^{th} column such that each is the last nonzero entry of some row of M , is linearly independent.

A row reduced matrix M can be transformed into canonical form by elementary row operations. This can be done by adding scalar multiples of the lower rows to upper rows as required, beginning from the last column.

Example 2.1.2 Consider the last column of matrix M^2 above. Adding the last row to the third gives

$$M^3 = \begin{bmatrix} 111 & 10111 & 10 & 000000 \\ 100 & 01111 & 10 & 001111 \\ 000 & 01111 & 10 & 000000 \\ 000 & 00000 & 11 & 111000 \end{bmatrix}.$$

Clearly the remaining nonzero entries in the last column of M^3 are independent. The first and third rows of M^3 have their last nonzero entries in the third column, and these entries are dependent. Adding the third row in M^3 to the first one, we obtain the canonical matrix

$$M^4 = \begin{bmatrix} 111 & 11000 & 00 & 000000 \\ 100 & 01111 & 10 & 001111 \\ 000 & 01111 & 10 & 000000 \\ 000 & 00000 & 11 & 111000 \end{bmatrix}.$$

The atomic code words are characterized in Theorem 2.1.1. However, Theorem 1.1.2 determines the TOGM only for q -ary linear block codes, and is not valid for the class of codes considered in this section. Instead we have the following lemma.

Lemma 2.1.1 *Let C be a linear (n, k) block code over F , and M a generator matrix of C in canonical form. In addition, let A_{ij} denote the set of rows of M which have the same span interval $[i, j]$. Then any nonzero linear combination of the elements of A_{ij} is an atomic code word.*

Proof Let v be a nonzero linear combination of elements of A_{ij} . Assume that v is not atomic and

$$v = \sum_p u_p, \quad (2.1)$$

where each u_p is atomic with span length strictly smaller than that of v .

Let u_p be an arbitrary element in this expression of v . Since M is a generator matrix, u_p can be expressed uniquely as a linear combination of the rows of M . Suppose it has the following expression

$$u_p = \sum_{v_t \in M} \lambda_t v_t \quad (2.2)$$

where $v_t \in M$ means v_t is a row of matrix M . We show that $\lambda_t = 0$ in (2.2), for any $v_t \in M \cap A_{ij}$. Assume u_p has span interval $[s, e]$. Hence interval $[s, e]$ does not include interval $[i, j]$.

Let $e < j$. Define B_l , $j \leq l \leq n$, to be the set of rows of M with ending position l . The set of vectors consisting of the l -th components of the elements of B_l are linearly independent, according to the definition of canonical matrix. Hence in (2.2) all the coefficients corresponding to the elements of B_n are zero, otherwise u_p will have ending position $n > e$, which is a contradiction. Eliminating B_n , the same argument can be applied to show that in (2.2) all the coefficients corresponding to the elements of B_{n-1} are zero if $j \leq n-1$. Following this procedure, we see that in (2.2) the coefficients corresponding to the elements of B_j are zero. Therefore, with the assumption $e < j$, no element of A_{ij} , which is a subset of B_j , is involved in the expression of u_p given by (2.2).

Suppose $j \leq e$. Since the span of u_p is smaller than that of v , it follows from $j \leq e$ that $i < s$. Now define B'_l , $1 \leq l \leq i$, to be the set of rows of M with starting position l . An argument similar to the one given for the case $j < e$ shows that in (2.2) all the coefficients corresponding to the elements of B'_l , $l \leq i$, are zero. Therefore no element of A_{ij} is involved in the expression of u_p given by (2.2).

Now by replacing each u_p in (2.1) with its unique expression as a linear combination of the rows of M , we obtain an expression for v as a linear combination of rows of M without making use of the elements of A_{ij} . This says that vector v has at least two distinct representations as a linear combination of the rows of M , which

is a contradiction, since the rows of M are linearly independent. ♣

For the q -ary linear block codes defined in Section 2, if a is an atomic code word and the span of code word c is the same as that of a , then c is also an atomic code word. However, this is not true for the general class of linear block codes considered in this section. For example, in the canonical matrix M^4 , the code word corresponding to the sum of the first and fourth rows is not an atomic code word even though its span interval is the same as that of the atomic code word corresponding to the second row.

The following theorem characterizes the set of atomic code words of a general linear block code C .

Theorem 2.1.1 *With the assumptions of Lemma 2.1.1, let interval $[i, j]$ be the span-interval of code word $c \in C$ and*

$$c = \sum_{t=1}^k \lambda_t v_t \quad (2.3)$$

be c expressed as a linear combination of rows of M . Then c is an atomic code word iff at least one of the vectors in (2.3) with nonzero coefficients has span-interval $[i, j]$.

Proof From the structure of the canonical generator matrix M , the span-interval of all of the vectors (code words) with nonzero coefficients in (2.3) are subintervals of $[i, j]$. Equation (2.3) has the following unique form

$$c = \sum_{t=1}^k \lambda_t v_t = \sum_{v_t \in A_{i,j}} \lambda_t v_t + \sum_{v_t \notin A_{i,j}} \lambda_t v_t = c' + \sum_{v_t \notin A_{i,j}} \lambda_t v_t \quad (2.4)$$

with

$$c' = \sum_{v_t \in A_{i,j}} \lambda_t v_t.$$

If $c' \neq 0$, then according to Lemma 2.1.1 the code word c' is atomic with span-interval $[i, j]$. This along with (2.4) implies that c is also atomic.

On the other hand if $c' = 0$ then

$$c = \sum_{v_i \in A_{i,j}} \lambda_i v_i$$

meaning that c is not atomic. ♣

In terms of the canonical generator matrix M for a linear block code C , $c \in C_{i,+}$ iff c is a linear combination of those rows of M with zeros in their first i components. Similarly, $c \in C_{i,-}$ iff c is a linear combination of those rows of M with zeros in their last $n - i$ components. This leads to the following.

Lemma 2.1.2 *Let C be an (n, k) linear block code with canonical generator matrix M . From Definition 2.1.1, $C_{i,+}$ is an $(n, k - p_i)$ linear block code where p_0 is defined to be zero. The dimension of $C_{i,-}$ is equal to the number of rows of M that have a span-interval that is a subinterval of $[1, i]$.*

Lemma 2.1.2 and Theorem 1.1.1 provide the state space dimension of the minimal trellis diagram of C from the canonical generator matrix M .

To construct a minimal trellis diagram, we must consider codes over a finite field. Hence for the remainder of this section, we assume that C is a linear block code over a finite field F . For each row of the canonical generator matrix M of C with span interval $[a, b]$, we associate a minimal trellis diagram G_{ab} as in Fig. 1.2, but with $q = |F|$ parallel paths connecting vertices $a - 1$ and b . One can easily check its minimality by comparing the number of states at time index i and the cardinality of the quotient group $\frac{D}{D_{i,-} D_{i,+}}$, where D is the one-dimensional code generated by the corresponding row of M . Now, the minimal trellis diagram of a linear block code can be introduced.

Theorem 2.1.2 *Let C be an (n, k) linear block code over the finite field $GF(q)$, and M a canonical generator matrix for C with rows denoted by $g_1, g_2, \dots, g_k$. Moreover,*

suppose that $G_i, 1 \leq i \leq k$, is a minimal trellis diagram of the one-dimensional code generated by g_i . Then, $G = \prod_{i=1}^k G_i$ is a minimal trellis diagram of C .

Proof The proof is by induction on k , the dimension of C . For codes of dimension 1, the proof is trivial as previously mentioned. Suppose that the statement holds for any linear block code of dimension not greater than $k-1$. Now, let $\bar{C}$ and $\hat{C}$ be two sub-codes of C of dimension $k-1$ and 1, respectively, such that $C = \bar{C}\hat{C}$ and $\hat{C}$ is generated by the code word corresponding to the last row of M . $\bar{C}$ is generated by the other $k-1$ rows of M . Suppose the generator of $\hat{C}$ (the last row vector of M) has span-interval $[j, l]$. Then according to the definition,

$$\hat{C}_{i-} = \begin{cases} 0 & \text{if } i \leq l-1 \\ \hat{C} & \text{if } l \leq i \end{cases} \quad \text{and} \quad \hat{C}_{i+} = \begin{cases} \hat{C} & \text{if } i \leq j-1 \\ 0 & \text{if } j \leq i \end{cases} \quad (2.5)$$

where $i \in [0, n]$. Since $C_{i-} = \bar{C}_{i-}\hat{C}_{i-}$ and $C_{i+} = \bar{C}_{i+}\hat{C}_{i+}$, it follows from (2.5) that

$$C_{i-} = \bar{C}_{i-}\hat{C}_{i-} = \begin{cases} \bar{C}_{i-} & \text{if } i < l \\ \bar{C}_{i-}\hat{C} & \text{if } l \leq i \end{cases} \quad (2.6)$$

and

$$C_{i+} = \bar{C}_{i+}\hat{C}_{i+} = \begin{cases} \bar{C}_{i+}\hat{C} & \text{if } i < j \\ \bar{C}_{i+} & \text{if } j \leq i. \end{cases} \quad (2.7)$$

For convenience let $|\frac{\bar{C}}{\bar{C}_{i-}\bar{C}_{i+}}|$ be denoted by s . If $i \in [j, l-1]$, then

$$|\frac{C}{C_{i-}C_{i+}}| = |\frac{\bar{C}\hat{C}}{\bar{C}_{i-}\hat{C}_{i-}\bar{C}_{i+}\hat{C}_{i+}}| = |\frac{\bar{C}\hat{C}}{\bar{C}_{i-}\bar{C}_{i+}}| = q|\frac{\bar{C}}{\bar{C}_{i-}\bar{C}_{i+}}| = qs. \quad (2.8)$$

By the induction hypothesis, the number of states of $\bar{G} = \prod_{i=1}^{k-1} G_i$ at time index i is s , therefore $G = \bar{G} \times G_k$ has qs states at time index $i, j \leq i \leq l-1$. Thus the number of states of G at time i is equal to the cardinality of $\frac{C}{C_{i-}C_{i+}}$, for $j \leq i \leq l-1$.

Now, suppose $i < j$, then

$$|\frac{C}{C_{i-}C_{i+}}| = |\frac{\bar{C}\hat{C}}{\bar{C}_{i-}\hat{C}_{i-}\bar{C}_{i+}\hat{C}_{i+}}| = \frac{|\bar{C}||\hat{C}|}{|\bar{C}_{i-}||\bar{C}_{i+}||\hat{C}|} = s. \quad (2.9)$$

Figure 2.1: The minimal trellis diagram of C with canonical generator matrix M^4 .

On the other hand for $i < j$, $G = G \times G_k$ and G have the same number of states at time index i . Hence for $i < j$, the number of states of G at time index i is equal to $|\frac{C}{C_{i-}C_{i+}}|$. The same argument can be applied for $i \leq j$, and the proof is complete by the principle of induction. ♣

Example 2.1.3 Using the canonical matrix M^4 and Theorem 2.1.2, the minimal trellis diagram for C is given in Fig. 2.1.

From Theorem 2.1.2, the canonical generator matrix M is a trellis oriented generator matrix for the linear code C . Let k, k_{i-} and k_{i+} be the dimensions of C, C_{i-} and C_{i+} , respectively. Then the number of states of G at time index i is $q^{k-k_{i-}-k_{i+}}$. In terms of the TOGM M , $k - k_{i-} - k_{i+}$ is the number of atomic classes of C active at time index i .

Remark If in the example M is considered as a generator matrix of a $(16, 4)$ linear code C' over F , then M^4 will not be a TOGM of C' since the first two rows have the same starting position. However, M^4 does correspond to a 4-section minimal trellis diagram for C' , with section lengths 3, 5, 2 and 6. In fact, as mentioned previously, an L -section minimal trellis diagram of a general linear block code can be obtained using the results of this section.

The theorems presented in Chapter 1 can be restated for the general linear block codes defined in this Chapter, and the proofs are essentially the same. For convenience, let $e(i)$ and $s(i)$ denote the number of atomic classes with ending and starting position i , respectively.

Theorem 2.1.3 *Under the assumptions of Theorem 2.1.2, let $0 \leq i \leq n$. Then*

1. *In V_i , the set of vertices of the minimal trellis diagram G of C at time index i , all vertices have the same entering and leaving degrees, i.e.,*

$$\epsilon d(v) = \epsilon d(u) = q^{e(i)} \quad (2.10)$$

and

$$ld(v) = ld(u) = q^{e(i+1)} \quad (2.11)$$

for all $v, u \in V_i$, except $ld(v_n) = \epsilon d(v_0) = 0$. In addition,

$$b(T_i(G)) = q^{s_{i-1} + e(i)} \quad (2.12)$$

where s_{i-1} is the number of atomic classes active at time $i - 1$.

2. *$t_i(C), 1 \leq i \leq n$, the number of components of $T_i(G)$, is*

$$t_i(C) = q^{a(i)} \quad (2.13)$$

where $a(i) = |I([1, i-1]) \cap E([i+1, n])|$. Moreover, each component is a complete bipartite graph with $q^{e(i)}$ vertices on one side and $q^{e(i)}$ vertices on the other. $t_0(C)$ is defined to be zero.

3. *G consists of $q^{|A_{1n}|}$ identical (in terms of the graph structure) parallel subtrellises, where A_{1n} is as in Lemma 2.1.1.*

Proof Let $a_1, a_2, \dots$, and a_k be atomic code words from distinct atomic classes $A_1, A_2, \dots$, and A_k of C with minimal trellis diagrams $G_1, G_2, \dots$, and G_k , respectively. Without loss of generality we may assume that the atomic code words $a_1, a_2, \dots$, and $a_{e(i)}$ end at position i . From the graph product operation it is clear that in $G = G_{e(i)+1} \times G_{e(i)+2} \times \dots \times G_{e(i)+k}$ every vertex of depth i is of entering degree 1. On the other hand, by induction on $e(i)$, it follows that in $\hat{G} = G_1 \times G_2 \times \dots \times G_{e(i)}$ every vertex at time i is of entering degree $q^{e(i)}$. Now

(2.10) follows from the fact that $\hat{G}$, the minimal trellis diagram of C is given by $\hat{G} = G \times \hat{G}$. The same argument is applied to (2.11).

To derive (2.12), it is enough to see that $b(T_i(G))$ is the product of the number of vertices at time $i - 1$, which is given by $|V_{i-1}| = q^{s(i-1)}$, and the leaving degree at that position, which is $q^{s(i)}$ according to (2.11).

Part 2 is an immediate result of the definition of the graph product operation, (2.10), and (2.11).

Suppose in the minimal trellis diagram G' of a length n code C' , for any $(c, c') \in T_1(G') \times T_n(G')$ there is a path (code word) containing c and c' as its first and last edges, respectively. Then, obviously G' has no parallel sub-trellises. Consider now G'' , the minimal trellis diagram of a length n linear block code C'' such that all the paths in G'' share in their last edges. It follows from the graph product operation that for any couple $(c, c') \in T_1(G' \times G'') \times T_n(G' \times G'')$ there is a path in $G' \times G''$ having c and c' as its initial and final edges, respectively. Hence $G = G' \times G''$ has no parallel sub-trellises.

Since all the paths of the minimal trellis diagram of each element of $S = \{a_1, a_2, \dots, a_k\} \setminus A_{1n}$ share either their last or first edges, the argument above along with applying induction on the cardinality of S shows that the product of the minimal trellis diagrams of the elements of S has no parallel sub-trellises. On the other hand, it is obvious that the product of the minimal trellis diagrams of the elements of A_{1n} consists of $q^{|A_{1n}|}$ parallel paths. This completes the proof of the third part of the theorem. ♣

Example 2.1.4 The parameters for code C , with TOGM M^4 , from Theorem 2.1.3 are given in Table 2.1 and are consistent with Fig. 2.1.

i	$e(i)$	$s(i)$	s_i	$b(T_i(G))$	$ed(v)$	$ld(v)$	$a(i)$	$t_i(C)$
0	0	0	0	0	0	4	0	0
1	0	2	2	4	1	2	0	1
2	1	1	2	8	2	2	1	2
3	1	1	2	8	2	1	1	2
4	2	0	0	4	4	0	0	1

Table 2.1: Relevant parameters for determining the complexity of the code C with TOGM M^4 .

2.2 Reed-Muller Codes

As an application of the theory developed in Section 2.1, the trellis structure of Reed-Muller codes is analyzed based on the TOGM.

Let $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$ be two n -tuples. The Boolean product of a and b is defined by $ab := (a_1b_1, a_2b_2, \dots, a_nb_n)$. The product of i n -tuples is called a Boolean product of degree i .

For a nonnegative integer m , consider the 2^m -tuples $v_0, v_1, \dots$, and v_m such that v_0 has Hamming weight 2^m , and v_i , $1 \leq i \leq m$, is the concatenation of 2^{m-i} identical blocks of length 2^i , each of which is divided into 2 sub-blocks of length 2^{i-1} such that the first sub-block is the string of all zeros, and the second sub-block is the string of all ones.

Definition 2.2.1 (Reed-Muller Codes) Let $0 \leq r \leq m$, and A be the set consisting of v_0 and all the Boolean products of the elements of $D = \{v_1, v_2, \dots, v_m\}$ up to degree r . The subspace of $GF(2)^{2^m}$ generated by A is defined as the r^{th} order Reed-Muller code of length 2^m , denoted $\mathcal{R}(r, m)$.

Since A is a linearly independent set of vectors, it follows from Definition 2.2.1 that $\mathcal{R}(r, m)$ has dimension

$$\sum_{i=0}^r \binom{m}{i},$$

and a generator matrix G_m^r whose rows are precisely the elements of A .

Example 2.2.1 $\mathcal{R}(2, 3)$ has the following generator matrix G_3^2

$$G_3^2 = \begin{bmatrix} v_0 \\ v_3 \\ v_2 \\ v_1 \\ v_2 v_3 \\ v_1 v_3 \\ v_1 v_2 \end{bmatrix} = \begin{bmatrix} 11 & 11 & 11 & 11 \\ 00 & 00 & 11 & 11 \\ 00 & 11 & 00 & 11 \\ 01 & 01 & 01 & 01 \\ 00 & 00 & 00 & 11 \\ 00 & 00 & 01 & 01 \\ 00 & 01 & 00 & 01 \end{bmatrix}. \quad (2.14)$$

The notation $M_1 \equiv M_2$, means that matrices M_1 and M_2 have the same row space, while $M_1 = M_2$, means that M_1 and M_2 have the same rows.

From the $(u, u + v)$ -construction of $\mathcal{R}(r, m)$ [19], it is known that G_m^r , the generator matrix of $\mathcal{R}(r, m)$, has the following form

$$G_m^r = \begin{bmatrix} G_{m-1}^r & G_{m-1}^r \\ \square & G_{m-1}^{r-1} \end{bmatrix}. \quad (2.15)$$

Therefore, we may express G_m^r in the following way

$$G_m^r = \begin{bmatrix} G_{m-2}^r & G_{m-2}^r & G_{m-2}^r & G_{m-2}^r \\ \square & G_{m-2}^{r-1} & \square & G_{m-2}^{r-1} \\ \square & \square & G_{m-2}^{r-1} & G_{m-2}^{r-1} \\ \square & \square & \square & G_{m-2}^{r-2} \end{bmatrix}. \quad (2.16)$$

Let B_m^i stand for the set of all Boolean products of degree precisely i , of the elements

of $D = \{v_1, v_2, \dots, v_m\}$. Then, for $0 \leq i \leq r \leq m$, G_m^r can be expressed in the form

$$G_m^r = \begin{bmatrix} B_m^r \\ B_m^{r-1} \\ \vdots \\ B_m^{i+1} \\ G_m^i \end{bmatrix}. \quad (2.17)$$

The case $i = N - 1$ in (2.17) is given by

$$G_m^r = \begin{bmatrix} B_m^r \\ G_m^{r-1} \end{bmatrix}. \quad (2.18)$$

The number of elements of B_m^r is given by

$$\binom{m}{r} = \begin{cases} \frac{m!}{r!(m-r)!} & 0 \leq r \leq m, \\ 0 & \text{otherwise.} \end{cases}$$

Combining (2.16) and (2.17) with $i = r - 2$ results in the following form for G_m^r

$$G_m^r = \begin{bmatrix} B_{m-2}^r & B_{m-2}^r & B_{m-2}^r & B_{m-2}^r \\ B_{m-2}^{r-1} & B_{m-2}^{r-1} & B_{m-2}^{r-1} & B_{m-2}^{r-1} \\ G_{m-2}^{r-2} & G_{m-2}^{r-2} & G_{m-2}^{r-2} & G_{m-2}^{r-2} \\ \square & B_{m-2}^{r-1} & \square & B_{m-2}^{r-1} \\ \square & G_{m-2}^{r-2} & \square & G_{m-2}^{r-2} \\ \square & \square & B_{m-2}^{r-1} & B_{m-2}^{r-1} \\ \square & \square & G_{m-2}^{r-2} & G_{m-2}^{r-2} \\ \square & \square & \square & G_{m-2}^{r-2} \end{bmatrix}. \quad (2.19)$$

Note that the arrangement of the elements of all identical blocks of G_m^r in equation (2.19) is the same. For example, an element of B_{m-2}^r is repeated 4 times, introducing one row of G_m^r .

If $\mathcal{R}(r, m)$ is considered as a subspace of $\prod_{i=1}^4 F^{2^{m-2}}$, then it is clear that G_m^r in (2.19) is in row reduced form according to Definition 2.1.1. This matrix is easily transformed into the matrix M given by (2.20) which is, according to Definition 2.1.2

and Theorem 2.1.2, a TOGM for the 4-section minimal trellis diagram of $\mathcal{R}(r, m)$. In the same way, the trellis oriented generator matrix M' , for the minimal 8-section trellis diagram of $\mathcal{R}(r, m)$ is given by (2.21).

$$M = \begin{bmatrix} B_{m-2}^r & B_{m-2}^r & B_{m-2}^r & B_{m-2}^r \\ B_{m-2}^{r-1} & B_{m-2}^{r-1} & \square & \square \\ \square & B_{m-2}^{r-1} & B_{m-2}^{r-1} & \square \\ \square & \square & B_{m-2}^{r-1} & B_{m-2}^{r-1} \\ G_{m-2}^{r-2} & \square & \square & \square \\ \square & G_{m-2}^{r-2} & \square & \square \\ \square & \square & G_{m-2}^{r-2} & \square \\ \square & \square & \square & G_{m-2}^{r-2} \end{bmatrix} \quad (2.20)$$

$$M' = \begin{bmatrix} B_{m-3}^r & B_{m-3}^r & B_{m-3}^r & B_{m-3}^r & B_{m-3}^r & B_{m-3}^r & B_{m-3}^r & B_{m-3}^r \\ G_{m-3}^{r-3} & \square & \square & \square & \square & \square & \square & \square \\ \square & G_{m-3}^{r-3} & \square & \square & \square & \square & \square & \square \\ \square & \square & G_{m-3}^{r-3} & \square & \square & \square & \square & \square \\ \square & \square & \square & G_{m-3}^{r-3} & \square & \square & \square & \square \\ \square & \square & \square & \square & G_{m-3}^{r-3} & \square & \square & \square \\ \square & \square & \square & \square & \square & G_{m-3}^{r-3} & \square & \square \\ \square & \square & \square & \square & \square & \square & G_{m-3}^{r-3} & \square \\ \square & \square & \square & \square & \square & \square & \square & G_{m-3}^{r-3} \\ B_{m-3}^{r-2} & B_{m-3}^{r-2} & \square & \square & \square & \square & \square & \square \\ \square & B_{m-3}^{r-2} & B_{m-3}^{r-2} & \square & \square & \square & \square & \square \\ \square & \square & B_{m-3}^{r-2} & \square & \square & \square & \square & \square \\ \square & \square & \square & B_{m-3}^{r-2} & \square & \square & \square & \square \\ \square & \square & \square & \square & B_{m-3}^{r-2} & \square & \square & \square \\ \square & \square & \square & \square & \square & B_{m-3}^{r-2} & \square & \square \\ \square & \square & \square & \square & \square & \square & B_{m-3}^{r-2} & \square \\ \square & \square & \square & \square & \square & \square & \square & B_{m-3}^{r-2} \\ B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & \square & \square & \square & \square \\ \square & \square & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & \square & \square \\ \square & \square & \square & \square & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} \\ \square & B_{m-3}^{r-1} & \square & B_{m-3}^{r-1} & B_{m-3}^{r-1} & \square & B_{m-3}^{r-1} & \square \end{bmatrix} \quad (2.21)$$

In the TOGM M' for the 8-section minimal trellis diagram of $\mathcal{R}(r, m)$, given by (2.21), the portion containing B_{m-3}^{r-1} is changed to the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \quad (2.22)$$

when B_{m-3}^{r-1} and $\square$ are replaced by 1 and 0, respectively. The latter matrix is G_3^1 , the generator matrix of the (8, 4, 4) Reed-Muller code $\mathcal{R}(1, 3)$. It is interesting that

in the same manner the portions of M' containing B_{m-3}^r , B_{m-3}^{r-1} , B_{m-3}^{r-2} , and G_{m-3}^{r-3} are changed into G_3^0 , G_3^1 , G_3^2 , and G_3^3 , respectively. This means that

$$M' = \oplus_{i=1}^{\binom{m-3}{r-3}} G_3^0 \oplus \oplus_{i=1}^{\binom{m-3}{r-2}} G_3^1 \oplus \oplus_{i=1}^{\binom{m-3}{r-1}} G_3^2 \oplus \oplus_{i=1}^{\sum_{j=0}^{r-3} \binom{m-3}{j}} G_3^3, \quad (2.23)$$

where for matrices $M1$ and $M2$ (with the same number of columns) the matrix $M1 \oplus M2$ is defined by

$$M1 \oplus M2 = \begin{bmatrix} M1 \\ M2 \end{bmatrix}$$

and $\oplus_{i=1}^n M$ stands for the n -fold direct-sum of M with itself.

Suppose G_3^i , $0 \leq i \leq 3$, is the TOGM of $\mathcal{R}(i, 3)$. For $0 \leq i \leq 2$, replace the 1's and 0's in G_3^i by B_{m-3}^{r-i} and a zero matrix of size B_{m-3}^{r-i} , respectively, and denote the resultant matrix by $\tilde{G}_3^i$. In the same manner, replace 1 and 0 in G_3^3 by $G_{m-3}^{r-3} = \bigcup_{i=0}^{r-3} B_{m-3}^i$ and a zero matrix of size G_3^3 , respectively, and denote the resulting matrix by $\tilde{G}_3^3$. With this notation, we obtain the expression

$$M' = \bigoplus_{i=0}^3 \tilde{G}_3^i. \quad (2.24)$$

A generalization of (2.24) is now presented. Before that we need a lemma. From (2.15) and (2.18), we obtain

$$G_m^r = \begin{bmatrix} G_{m-1}^r & G_{m-1}^r \\ \square & G_{m-1}^{r-1} \end{bmatrix} = \begin{bmatrix} B_{m-1}^r & B_{m-1}^r \\ G_{m-1}^{r-1} & G_{m-1}^{r-1} \\ \square & G_{m-1}^{r-1} \end{bmatrix} \equiv \begin{bmatrix} B_{m-1}^r & B_{m-1}^r \\ G_{m-1}^{r-1} & \square \\ \square & G_{m-1}^{r-1} \end{bmatrix} \quad (2.25)$$

Lemma 2.2.1 For integers r and m satisfying $0 \leq r \leq m-1$

$$B_m^r = \begin{bmatrix} B_{m-1}^r & B_{m-1}^r \\ \square & B_{m-1}^{r-1} \end{bmatrix} \quad (2.26)$$

Proof It follows from (2.15) and (2.18) that

$$G_m^r = \begin{bmatrix} B_m^r \\ G_{m-1}^{r-1} \end{bmatrix} = \begin{bmatrix} B_m^r \\ \frac{G_{m-1}^{r-1} \quad G_{m-1}^{r-1}}{\square \quad G_{m-1}^{r-2}} \end{bmatrix} \quad (2.27)$$

and

$$G_m^r = \begin{bmatrix} G_{m-1}^r & G_{m-1}^r \\ \square & G_{m-1}^{r-1} \end{bmatrix} = \begin{bmatrix} B_{m-1}^r & B_{m-1}^r \\ G_{m-1}^{r-1} & G_{m-1}^{r-1} \\ \square & B_{m-1}^{r-1} \\ \square & G_{m-1}^{r-2} \end{bmatrix} = \begin{bmatrix} B_{m-1}^r & B_{m-1}^r \\ \square & B_{m-1}^{r-1} \\ G_{m-1}^{r-1} & G_{m-1}^{r-1} \\ \square & G_{m-1}^{r-2} \end{bmatrix} \quad (2.28)$$

Now (2.26) follows from comparing (2.27) to (2.28). ♣

Define $\bar{G}_i^i$, $0 \leq i \leq l$, as was done previously for $l = 3$. This definition and Lemma 2.2.1 are what we need for the following theorem.

Theorem 2.2.1 For $l \geq 1$, the matrix

$$TM_l =: \bigoplus_{i=0}^l \bar{G}_i^i \quad (2.29)$$

is a TOGM for the 2^l -section minimal trellis diagram of $\mathcal{R}(r, m)$.

Proof The proof is by induction on l . The statement is true for $1 \leq l \leq 3$ according to (2.20), (2.21) and (2.25). Suppose it is true for integer $l \geq 3$, induction hypothesis. The following argument shows that it holds for $l + 1$.

For $0 \leq i \leq l - 1$, $\bar{G}_i^i$ is a matrix with 2^{m-l} columns and block elements B_{m-l}^{r-l} and matrices of zeros. Similarly, $\bar{G}_l^l$ is a matrix with 2^{m-l} columns, and block entries G_{m-l}^{r-l} and matrices of zeros. Applying (2.25) and (2.26), TM_l is transformed into a matrix M with 2^{m-l+1} block columns such that

1. The nonzero block entries of M are precisely the elements of the set $S = \{B_{m-l-1}^r, B_{m-l-1}^{r-1}, \dots, B_{m-l-1}^{r-l}, G_{m-l-1}^{r-l-1}\}$;
2. The nonzero block entries of each row of M are the same;
3. The size of zero blocks of each row is the same as that of its identical nonzero block entries.

By row operations M is transformed into a TOGM matrix TM for the 2^{l+1} -section minimal trellis diagram of $\mathcal{R}(r, m)$ such that TM meets the three properties stated for M .

Consider now the Reed-Muller codes $\mathcal{R}(0, l+1)$, $\mathcal{R}(1, l+1)$, $\dots$, $\mathcal{R}(l, l+1)$, and $\mathcal{R}(l+1, l+1)$. As special cases, for $0 \leq i \leq l+1$, TM is a TOGM for the 2^{l+1} -section minimal trellis diagram of $\mathcal{R}(i, l+1)$ if r and m are replaced by i and $l+1$, respectively. Since for $m = l+1$

$$B_{m-l-1}^j = B_0^j = \begin{cases} 1 & \text{if } j = 0, \\ 0 & \text{if } j \neq 0; \end{cases} \quad (2.30)$$

the TOGM of the 2^{l+1} -section minimal trellis diagram of $\mathcal{R}(i, l+1)$, $0 \leq i \leq l$, is obtained from TM if B_{m-l-1}^{r-i} is replaced by 1 and the rest by 0. In the same way, TM represents the TOGM of $\mathcal{R}(l+1, l+1)$ if G_{m-l-1}^{m-l-1} is replaced by 1 and the rest by zero. Therefore $TM = TM_{l+1}$. ♣

Example 2.2.2 For $l = 4$, the matrix TM_4 is given by (2.31) in which 0, 1, 2, 3, and 4 denote B_{m-4}^r , B_{m-4}^{r-1} , B_{m-4}^{r-2} , B_{m-4}^{r-3} , and G_{m-4}^{r-4} , respectively, and the dashes denote the blocks of zeros. This matrix is a TOGM for the 16-section minimal trellis diagram of $\mathcal{R}(r, m)$.

Note that the portion of TM_4 specified by i introduces a TOGM for the 16-section minimal trellis diagram of $\mathcal{R}(i, 4)$ if each block row of that portion is considered as just one row. It is also noteworthy that Theorem 2.2.1 includes the technique to derive TM_{l+1} from TM_l .

Theorem 2.2.1 provides the following two interesting corollaries.

Corollary 2.2.1 *The 2^l -section minimal trellis diagram of $\mathcal{R}(r, m)$ consists of $2^{\binom{m-l}{r-l}}$ structurally identical parallel sub-trellises.*

Proof Consider the following generator matrix of $\mathcal{R}(r, m)$

$$M = \begin{bmatrix} v_0 \\ B_m^1 \\ \vdots \\ B_m^r \end{bmatrix} \quad (2.32)$$

According to the definition of v_0 and B_m^i , $1 \leq i \leq r$, all the rows of M start with 0 and end with 1, except v_0 which starts and ends with 1. This along with Theorem 1.1.2 implies that the TOGM for the 2^m -section minimal trellis diagram of $\mathcal{R}(r, m)$, obtained from M via row operations, has one row which starts and ends with 1 iff $r = 0$. Therefore in TM_l , the TOGM for the 2^l -section minimal trellis diagram of $\mathcal{R}(r, m)$ given by Theorem 2.2.1, it is precisely $\bar{G}_l^0$ that starts and ends with nonzero block bits, namely B_{m-l}^r . Now, the result follows from Section 3 of Theorem 2.1.3. ♣

Corollary 2.2.2 *Let $TR_{r,m,l}$ denote the 2^l -section minimal trellis diagram of $\mathcal{R}(r, m)$. Then we have*

$$TR_{r,m,l} = TR_{0,l,l}^{\binom{m-l}{r-l}} \times TR_{1,l,l}^{\binom{m-l}{r-l}} \times \cdots \times TR_{l-1,l,l}^{\binom{m-l}{r-l}} \times TR_{l,l,l}^{\sum_{i=0}^{r-l} \binom{m-l}{i}}. \quad (2.33)$$

where for a given graph G , G^n stands for the n -fold product of G with itself.

While $2^{\binom{m-l}{r-l}}$ is the number of parallel sub-trellises of $TR_{r,m,l}$, the number of edges connecting two adjacent vertices of $TR_{r,m,l}$ is given by $2^{\sum_{i=0}^{r-l} \binom{m-l}{i}}$.

Let $0 \leq r, l \leq m$. Another result of Theorem 2.2.1 is the combinatorial equation

$$f(l) =: \sum_{i=0}^{l-1} \left\{ \binom{m-l}{r-i} \sum_{j=0}^i \binom{l}{j} \right\} + 2^l \sum_{i=0}^{r-l} \binom{m-l}{i} = \sum_{i=0}^r \binom{m}{i} \quad (2.34)$$

which gives the dimension of $\mathcal{R}(r, m)$ computed from TM_l and its components $\bar{G}_l^i$, $0 \leq i \leq l$.

Table 2.2: Complexity parameters of the 4-section minimal trellis diagram of Reed-Muller code $\mathcal{R}(r, m)$.

i	1	2	3	4
$\epsilon(i)$	$\sum_{j=0}^{r-2} \binom{m-2}{j}$	$\sum_{j=0}^{r-1} \binom{m-2}{j}$	$\sum_{j=0}^{r-1} \binom{m-2}{j}$	$\sum_{j=0}^r \binom{m-2}{j}$
$s(i)$	$\sum_{j=0}^r \binom{m-2}{j}$	$\sum_{j=0}^{r-1} \binom{m-2}{j}$	$\sum_{j=0}^{r-1} \binom{m-2}{j}$	$\sum_{j=0}^{r-2} \binom{m-2}{j}$
s_i	$\binom{m-2}{r} + \binom{m-2}{r-1}$	$\binom{m-2}{r} + \binom{m-2}{r-1}$	$\binom{m-2}{r} + \binom{m-2}{r-1}$	0
$\text{Log}_2(t_i)$	0	$\binom{m-2}{r}$	$\binom{m-2}{r}$	0

Table 2.3: Complexity parameters of the 8-section minimal trellis diagram of Reed-Muller code $\mathcal{R}(r, m)$.

i	$\epsilon(i)$	$s(i)$	s_i	$\text{Log}_2(t_i)$
1	$\sum_{j=0}^{r-3} \binom{m-3}{j}$	$\sum_{j=0}^r \binom{m-3}{j}$	$\sum_{j=0}^2 \binom{m-3}{r-j}$	0
2	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^{r-1} \binom{m-3}{j}$	$\binom{m-3}{r-1} + \sum_{j=0}^2 \binom{m-3}{r-j}$	$\binom{m-3}{r} + \binom{m-3}{r-1}$
3	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^{r-1} \binom{m-3}{j}$	$2\binom{m-3}{r-1} + \sum_{j=0}^2 \binom{m-3}{r-j}$	$\binom{m-3}{r} + 2\binom{m-3}{r-1}$
4	$\sum_{j=0}^{r-1} \binom{m-3}{j}$	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\binom{m-3}{r-1} + \sum_{j=0}^2 \binom{m-3}{r-j}$	$\binom{m-3}{r} + 2\binom{m-3}{r-1}$
5	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^{r-1} \binom{m-3}{j}$	$2\binom{m-3}{r-1} + \sum_{j=0}^2 \binom{m-3}{r-j}$	$\binom{m-3}{r} + 2\binom{m-3}{r-1}$
6	$\sum_{j=0}^{r-1} \binom{m-3}{j}$	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\binom{m-3}{r-1} + \sum_{j=0}^2 \binom{m-3}{r-j}$	$\binom{m-3}{r} + 2\binom{m-3}{r-1}$
7	$\sum_{j=0}^{r-1} \binom{m-3}{j}$	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^2 \binom{m-3}{r-j}$	$\binom{m-3}{r-1} + \binom{m-3}{r}$
8	$\sum_{j=0}^r \binom{m-3}{j}$	$\sum_{j=0}^{r-3} \binom{m-3}{j}$	0	0

From Theorem 2.1.3 and the TOGM's for the 4-section and 8-section minimal trellis diagrams of $\mathcal{R}(r, m)$, given by (2.20) and (2.21), respectively, the complexity parameters can be determined and are given in Tables 2.2 and 2.3.

2.3 A Direct-sum Structure for Optimal $(4L, k, 4)$ Linear Block Codes

Another application of the theory given in Section 2.1 is now presented. Let C be a $(4L, k, 4)$, $L \geq 1$, binary linear block code, i.e. C has length $4L$, dimension k , and minimum distance $d = 4$. Two sub-codes of C , say C_1 and C_2 , are introduced such that:

- 1- C is the direct-sum of C_1 and C_2 ;
- 2- The minimal trellis diagram of C is the product of the minimal trellis diagrams of C_1 and C_2 ;
- 3- C is optimal, i.e. C has maximum dimension, if and only if both C_1 and C_2 are optimal. This optimal code is denoted by $\mathcal{C}(4L, 4)$.

Let c_1 , c_2 , and c_3 be binary strings of weight 4 and length $4L$ such that

- 1- The first 4 bits of c_1 are nonzero, and in c_2 the nonzero bits are the first, second, fifth, and sixth bits;
- 2- The nonzero bits of c_3 are located in the first, third, fifth, and seventh positions.

$T^j(c)$ denotes a cyclic shift of c by j positions to the right. Consider the matrix $G_L(1, 2)$ consisting of the $4L$ -tuples $T^{4i}(c_1)$, $0 \leq i \leq L-1$, and $T^{4i}(c_j)$, $0 \leq i \leq L-2$, $j = 2$ and 3 .

Example 2.3.1 For $L = 3$ we have:

$$G_3(1, 2) = \begin{bmatrix} 1111 & 0000 & 0000 \\ 0000 & 1111 & 0000 \\ 0000 & 0000 & 1111 \\ 1100 & 1100 & 0000 \\ 0000 & 1100 & 1100 \\ 1010 & 1010 & 0000 \\ 0000 & 1010 & 1010 \end{bmatrix}. \quad (2.35)$$

The linear code associated with generator matrix $G_L(1, 2)$ is denoted by $\mathcal{R}_L(1, 2)$, because of the similarity between this code and the first order Reed-Muller codes.

Lemma 2.3.1 $\mathcal{R}_L(1, 2)$ is a $(4L, 3L - 2, 4)$ linear code.

Proof Consider $G_L(1, 2)$ as a $(3L - 2) \times L$ matrix with entries in $GF(2)^4$. For fixed i , $1 \leq i \leq L$, let B_i denote the set of nonzero entries that are in the i th column such that each is the first nonzero element of a row of $G_L(1, 2)$. B_i is the independent set $\{1111, 1100, 1010\}$ for $1 \leq i \leq L - 1$, and $B_L = \{1111\}$. Since $\sum_{i=1}^L |B_i| = 3L - 2$, the rows of $G_L(1, 2)$ are independent and hence $\mathcal{R}_L(1, 2)$ is of dimension $3L - 2$.

The row space of each column of $G_L(1, 2)$, viewed as a $(3L - 2) \times L$ matrix over $GF(2)^4$, is the set of all strings of weight 0, 2, and 4. Let c be a nonzero code word of $\mathcal{R}_L(1, 2)$, with c_i and c_j as the first and last nonzero components, each component of length 4, where $1 \leq i \leq j \leq L$. If $i \neq j$, then both c_i and c_j have weight at least two and hence c has weight at least four. Suppose $i = j$. This implies that all rows of $G_L(1, 2)$ involved in the formation of c have zero components except the j th one. This means that $c_j = 1111$, and c has weight four. Therefore, $\mathcal{R}_L(1, 2)$ has minimum distance four. ♣

Denote the $(L, k_{max}, 4)$, $L \geq 4$, binary linear block code of length L , minimum distance 4, and maximum dimension k_{max} by $C_{L,4}$. Let $\mathcal{C}_{L,4}$ stand for the $(4L, k_{max}, 4)$ code of length $4L$ obtained from $C_{L,4}$ by substituting every '0' bit with the 4-tuple '0000' and every '1' with the 4-tuple '1000'. Note that $\mathcal{R}_L(1, 2) \cap \mathcal{C}_{L,4} = \{0\}$, where '0' denotes the all zero code word.

Lemma 2.3.2 $\mathcal{R}_L(1, 2) \oplus \mathcal{C}_{L,4}$ has minimum distance four.

Proof Let c and c' be nonzero code words in $\mathcal{R}_L(1, 2)$ and $\mathcal{C}_{L,4}$, respectively. Denote the first four nonzero block components of c' by c'_1, c'_2, c'_3 , and c'_4 . Let c_i , $1 \leq i \leq 4$, be the block component of c corresponding to c'_i . Since c_i is in the row space of $\{1111, 1100, 1010\}$, it has even weight, implying that $c_i + c'_i$ has odd weight and therefore is a nonzero block. It follows that $c + c'$ has weight at least four. ♣

An immediate result of Lemma 2.3.2 is

$$k_{\max}(4L, 4) \geq 3L - 2 + k_{\max}(L, 4) \quad (2.36)$$

where $k_{\max}(n, d)$ is the maximum dimension of a code of length n and minimum distance d .

It is known that the extended Hamming codes are optimal $d = 4$ linear codes, and in the range between two successive extended Hamming codes, the shortened Hamming codes are also optimal and have the same redundancy. Specifically, for an optimal $(n, k, 4)$ linear code C , if $2^{m-1} < n \leq 2^m$, then $n - k = m + 1$. This implies that

$$k_{\max}(4L, 4) - k_{\max}(L, 4) = 3L - 2. \quad (2.37)$$

Lemma 2.3.2 along with (2.37) prove the first part of the following theorem.

Theorem 2.3.1 *Let m be a divisor of L and let G , G_1 , and G_2 be the L/m -section minimal trellis diagrams of $\mathcal{C}(4L, 4)$, $\mathcal{R}_L(1, 2)$, and $\mathcal{C}_{L,4}$, respectively. Then*

$$\mathcal{C}(4L, 4) = \mathcal{R}_L(1, 2) \oplus \mathcal{C}_{L,4} \quad (2.38)$$

and

$$G = G_1 \times G_2. \quad (2.39)$$

Proof Suppose M_1 and M_2 are the TOGMs for the L/m -section minimal trellis diagrams of $\mathcal{R}_L(1, 2)$ and $\mathcal{C}_{L,4}$, respectively. The nonzero entries of M_1 and M_2 are linearly independent when M_1 and M_2 are considered as matrices over $GF(2)^4$. Therefore, according to Theorem 2.1.2 the matrix M consisting of the rows of M_1 and M_2 is a TOGM for the L/m -section minimal trellis diagram of $\mathcal{C}(4L, 4)$, implying that $G = G_1 \times G_2$. ♣

Note that $G_L(1, 2)$ is a TOGM for the L/m -section minimal trellis diagram of $\mathcal{R}_L(1, 2)$.

Example 2.3.2 For $L = 7$, we have $k_{\max}(7, 4) = 3$. $\mathcal{C}_{7,4}$ has the following generator matrix

$$M_2 = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \quad (2.40)$$

Hence $\mathcal{C}(28, 22, 4)$ has TOGM

$$M = \begin{bmatrix} M_1 \\ M_2 \end{bmatrix} = \begin{bmatrix} \overbrace{\begin{matrix} & G_7(1, 2) & \end{matrix}} \\ 1000 & 1000 & 1000 & 1000 & 0000 & 0000 & 0000 \\ 0000 & 0000 & 1000 & 1000 & 1000 & 1000 & 0000 \\ 0000 & 1000 & 0000 & 1000 & 1000 & 0000 & 1000 \end{bmatrix} \quad (2.41)$$

It is easy to see that for $L \geq 3$, the number of parallel sub-trellises in the L -section minimal trellis diagram of $\mathcal{C}(4L, 4)$, denoted by $t(\mathcal{C}(4L, 4))$, is at most two and is equal to that of $\mathcal{C}(L, 4)$. Furthermore, if $t(\mathcal{C}(4L, 4)) = 2$ then $k_{\max}(L, 4) = 1 + k_{\max}(L - 2, 4)$, which is true if $L = 2^l + 1$. The state complexity of the L/m section minimal trellis diagram of $\mathcal{R}_L(1, 2)$ is 2, resulting in $S_{4L} = S_L + 2$, where S_{4L} and S_L are the state complexities of $\mathcal{C}(4L, 4)$ and $\mathcal{C}(L, 4)$, respectively.

2.4 Summary

The minimal trellis diagram of linear block codes has been analyzed. In particular, the trellis oriented generator matrix and the atomic code words of a length n block code C have been characterized when C is a subspace of the product vector space $\mathcal{V} = \mathcal{V}_1 \times \mathcal{V}_2 \times \cdots \times \mathcal{V}_n$ over $GF(q)$ and $\mathcal{V}_i$, $1 \leq i \leq n$, is a vector space over $GF(q)$. Using the trellis oriented generator matrix, the state and branch complexity of G , the minimal trellis diagram of C , as well as the number of identical parallel sub-trellises in G have been studied.

As an application of this theory, a comprehensive analysis of the minimal 2^l -section trellis diagram of Reed-Muller codes has been presented. Apart from the new results in this Chapter, primarily Theorem 2.2.1 and Corollary 2.2.2, previously

known results regarding Reed-Muller codes have been derived in an extremely simple way, and this confirms the high utility of this theory. As another application, an analysis of the trellis structure of the class of optimal $(4L, k, 4)$ linear block codes has been presented.

Chapter 3

CANONICAL REPRESENTATION OF QUASI-CYCLIC CODES

3.1 Introduction

A linear block code C of length n is called quasi-cyclic (QC) if it is invariant under a cyclic shift of m positions, i.e. T^m , where $m < n$. More precisely, T is the cyclic shift acting on the n -tuple $(c_1, c_2, \dots, c_n)$ so that

$$T(c_1, c_2, \dots, c_n) = (c_n, c_1, c_2, \dots, c_{n-1}).$$

The smallest such m is called the index of the code C . Cyclic codes are a subclass of QC codes. Seguin [21] has presented a module structure for QC codes which can be considered analogous to the ideal structure of cyclic codes. This chapter investigates the cyclic structure of QC codes.

Any cyclic code can be represented by a unique generator polynomial. In this chapter, we associate a polynomial generator set (PG-set) with QC code C that is a natural generalization of the generator polynomial of a cyclic code. When the PG-set is a singleton, the QC code is a cyclic code.

In this chapter, a canonical generator matrix (CG-matrix) of an (n, k) QC code C invariant under T^m is introduced. This matrix illustrates the symmetric structure of the minimal n/m section trellis diagram of C to be studied in Chapter 5.

Section II introduces the CG-matrix and PG-set of a QC code, and contains an analysis of the (24,12) Golay code and Reed-Muller codes. Some relations between QC codes and cyclic codes are given in Section III. The 1-generator QC codes are investigated in Section IV. Finally, in Section V the action of some permutation operations on QC codes is studied.

3.2 Canonical Generator Matrix

In this Section, C represents an (n, k) QC code where $n = Lm$ and C is invariant under the transformation T^m (cyclic shift by m positions). Denote T^m by Λ . Any code word $c = (c_1, c_2, \dots, c_n)$ of C can be expressed as $c = v_1 v_2 \dots v_L$ where $v_i = (c_{m(i-1)+1}, c_{m(i-1)+2}, \dots, c_{mi})$ is called the i^{th} block of c . For convenience, the symbol " $\square$ " is used to represent v_i if $v_i = (0, 0, \dots, 0)$.

Lemma 3.2.1 *In the QC code C , a code word $c = v_1 v_2 \dots v_t \square \dots \square$, with at least one $\square$ on the right, is an atomic code word iff $c' = \Lambda(c) = \square v_1 v_2 \dots v_t \square \dots \square$ is an atomic code word.*

Proof Suppose c' is not atomic. Then $c' = c'_1 + c'_2 + \dots + c'_r$ where the span of c'_i , $1 \leq i \leq r$, is contained in the span of c' . Without loss of generality we may assume the span of c'_j is strictly smaller than that of c' for some $1 \leq j \leq r$. Since C is a QC code invariant under Λ , we have

$$c = \Lambda^{-1}(c') = \Lambda^{-1}(c'_1 + c'_2 + \dots + c'_r) = \Lambda^{-1}(c'_1) + \Lambda^{-1}(c'_2) + \dots + \Lambda^{-1}(c'_r). \quad (3.1)$$

We also have

$$\begin{aligned} \text{span}(c'_i) &\subseteq \text{span}(c') \quad \text{iff} \quad \text{span}(\Lambda^{-1}(c'_i)) \subseteq \text{span}(\Lambda^{-1}(c')) = \text{span}(c), \\ \text{span}(c'_i) &\subset \text{span}(c') \quad \text{iff} \quad \text{span}(\Lambda^{-1}(c'_i)) \subset \text{span}(\Lambda^{-1}(c')) = \text{span}(c). \end{aligned} \quad (3.2)$$

It follows from (3.1) and (3.2) that c is not an atomic code word. The same argument shows that if c is not atomic then $T^m(c)$ is not atomic either. ♣

Let C be an (Lm, k) QC code with generator matrix M . Define the $k \times im$ matrices M_i , $1 \leq i \leq L$, such that the j^{th} column of M_i , $1 \leq j \leq im$, is the same as that of M . Denoting the i^{th} row of M_1 as the vector u_i , consider the vector space V (a subspace of F^m) generated by $B = \{u_1, u_2, \dots, u_k\}$, where F is the field on which the code has been defined. Assume that M is a TOGM for C and A is the set of all nonzero elements of B . Then, with the notation above, we have the following.

Theorem 3.2.1 *A is a basis of the vector space V .*

Proof Since any element of V is the first block of some code word in C , then A has to be a generator of V , so that A includes a basis of V , say $A' = \{u_1, u_2, \dots, u_p\}$. A cannot contain any other nonzero element, because any $p + 1$ nonzero vectors of V are linearly dependent and hence at least two of them have the same starting position, which is a contradiction. ♣

Definition 3.2.1 (Canonical Component) Let $c = v_1 \dots v_t \square \dots \square$, $1 \leq t \leq L$, be a code word of a QC code C of length $n = Lm$, where v_i and $\square$ have length m . The sub-code of C generated by the matrix $M(c)$

$$M(c) = \begin{bmatrix} c \\ \Lambda(c) \\ \vdots \\ \Lambda^{m-t}(c) \end{bmatrix} = \begin{bmatrix} v_1 & v_2 & \dots & v_t & \square & \dots & \square \\ \square & v_1 & v_2 & \dots & v_t & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \dots & \ddots & \square \\ \square & \dots & \square & v_1 & v_2 & \dots & v_t \end{bmatrix} \quad (3.3)$$

is denoted by $D(c)$ and is called the canonical component of C generated by c .

Note that according to Definition 1.1.3, any row in a TOGM of C can be replaced with another atomic code word from the same atomic class.

Let C be an (n, k) QC code with TOGM M and $n = Lm$. Assume that the $k \times m$ matrix M_1 , consisting of the first m columns of M , has rank p . According to Theorem 3.2.1, the number of nonzero rows of M_1 is p and these rows form a basis

for the row space of M_1 . Each of these p rows is the first block of one row in M . We denote the corresponding code words of C associated with these rows of M by $c^1, c^2, \dots, c^p$.

Theorem 3.2.2 (Canonical Representation Theorem) *Let C be an (n, k) QC code invariant under $\Lambda = T^m$, with $n = Lm$. Suppose that matrix M is a TOGM of C , and M_1 has rank p . $c^1, c^2, \dots, c^p$ are as defined above. Then*

$$C = D(c^1) \oplus D(c^2) \oplus \dots \oplus D(c^p) \quad (3.4)$$

and C has TOGM M'

$$M' = \begin{bmatrix} M(c^1) \\ M(c^2) \\ \vdots \\ M(c^p) \end{bmatrix} \quad (3.5)$$

where $M(c^i)$ is given by (3.3).

Proof Without loss of generality, let $c^1, c^2, \dots, c^p$ be the first p rows of M . Let $k > p$ and consider one of the remaining rows of M , say c^{p+1} . From Lemma 3.2.1, c^{p+1} has $t \geq 1$ zero blocks on the left before the first nonzero block. Denoting the backward shift (by m positions or one block) operator by Λ^{-1} , and applying Lemma 3.2.1, we see that $\tilde{c}^{p+1} = (\Lambda^{-1})^t(c^{p+1})$ is an atomic code word from precisely one of the p distinct atomic classes with representatives $c^1, c^2, \dots, c^p$. Without loss of generality, assume that $\tilde{c}^{p+1}$ and c^1 are two code words in the same atomic class. Then, within the generator matrix M , c^{p+1} can be replaced with $\Lambda^t(c^1)$.

Conversely, if $c^1 = v_1 v_2 \dots \square \dots \square$ has w zero blocks on the right side, after the last nonzero block, then $\Lambda^j(c^1)$, $1 \leq j \leq w$, is an atomic code word of C . Hence, there exists an atomic code word c'' , $1 \leq j \leq w$, in M such that $\Lambda^j(c^1)$ and c'' are in the same atomic class and c'' can be replaced with $\Lambda^j(c^1)$.

It follows that there is a one-to-one correspondence between the rows of M and the rows of M'

$$M' = \begin{bmatrix} M(c^1) \\ M(c^2) \\ \vdots \\ M(c^p) \end{bmatrix}$$

and this completes the proof. ♣

Based on Theorem 3.2.2, we give the following definition.

Definition 3.2.2 *The generator matrix M' in Theorem 3.2.2 is called the canonical generator matrix (CG-matrix) of C , while the set $\{g_1(x), g_2(x), \dots, g_p(x)\}$, consisting of the polynomials corresponding to the code words $\{c^1, c^2, \dots, c^p\}$, is called the polynomial generator set (PG-set) of C . The decomposition of C given by (3.4) is called the Canonical Decomposition of C , and the factors in this decomposition are termed the Canonical Components of C .*

Example 3.2.1 Consider the (18,6) QC code C , invariant under $\Lambda = T^3$, with generator matrix M

$$M = \begin{bmatrix} 111 & 110 & 111 & 001 & 000 & 000 \\ 111 & 001 & 000 & 000 & 111 & 110 \\ 000 & 111 & 110 & 111 & 001 & 000 \\ 110 & 111 & 001 & 000 & 000 & 111 \\ 000 & 000 & 111 & 110 & 111 & 001 \\ 001 & 000 & 000 & 111 & 110 & 111 \end{bmatrix}.$$

Using elementary row operations, we obtain the generator matrix $\hat{M}$

$$\hat{M} = \begin{bmatrix} 110 & 000 & 001 & 111 & 000 & 000 \\ 001 & 110 & 110 & 110 & 000 & 000 \\ 000 & 111 & 110 & 111 & 001 & 000 \\ 000 & 001 & 110 & 110 & 110 & 000 \\ 000 & 000 & 111 & 110 & 111 & 001 \\ 000 & 000 & 001 & 110 & 110 & 110 \end{bmatrix}.$$

$\hat{M}$ is a TOGM matrix for C .

Taking the two code words c^1 and c^2 corresponding to the first and second rows of $\hat{M}$, respectively, and applying Theorem 3.2.2, produces the CG-matrix M'

$$M' = \begin{bmatrix} M(c^1) \\ M(c^2) \end{bmatrix} = \begin{bmatrix} 110 & 000 & 001 & 111 & \square & \square \\ \square & 110 & 000 & 001 & 111 & \square \\ \square & \square & 110 & 000 & 001 & 111 \\ 001 & 110 & 110 & 110 & \square & \square \\ \square & 001 & 110 & 110 & 110 & \square \\ \square & \square & 001 & 110 & 110 & 110 \end{bmatrix}.$$

The PG-set of this code is

$$\{g_1(x), g_2(x)\} = \{1 + x + x^8 + x^9 + x^{10} + x^{11}, x^2 + x^3 + x^4 + x^6 + x^7 + x^9 + x^{10}\}.$$

Remark In the canonical decomposition of C , the canonical components $D(c^i)$, $1 \leq i \leq p$, have just one row iff the last block of c^i is a nonzero block.

Remark From the proof of Theorem 3.2.2, if atomic class A_i , which includes atomic code word c^i , $1 \leq i \leq p$, contains another atomic code word, say $\tilde{c}^i$, then in the TOGM M' , $M(c^i)$ can be replaced with $M(\tilde{c}^i)$. Note that this can occur iff for some i and j , $1 \leq i, j \leq p$, the span interval of atomic code word c^i lies inside the span of code word c^j .

In (3.4), the code word c^1 can be chosen such that $g_1(x)$ has minimum degree. Assume that $c^1, \dots, c^i$ have been found, where $1 \leq i \leq p-1$. Consider the linear code C'' such that $C = \bigoplus_{j=1}^i D(c^j) \oplus C''$. Now c^{i+1} is a code word of C'' which corresponds to a polynomial of minimum degree.

Remark Let $g(x)$ and $g'(x)$ be two polynomials corresponding to code words c and c' , respectively. Define $c < c'$ if $\deg(g(x)) < \deg(g'(x))$. Then, the foregoing argument shows that $0 < c^1 < c^2 < \dots < c^p$. Denoting the number of zero blocks on the extreme right of c^i by $m - m_i$, we have $m_1 \leq m_2 \leq \dots \leq m_p \leq m$. Therefore

$$\sum_{i=1}^p m_i = p(m+1) - k \quad (3.6)$$

which gives

$$p \leq m_i \quad (3.7)$$

for $1 \leq i \leq p$.

3.2.1 The Golay Code

The (24, 12, 8) extended binary Golay Code, denoted $\mathcal{G}_{24}$, is a well known QC code [15]. It has a double circulant generator matrix $M = [I|A]$, where I is the identity matrix of dimension 12, and A is a circulant matrix with leading row $c = 6750_8 = 110111101000$. The corresponding canonical generator matrix, invariant under T^2 , is

$$M = \begin{bmatrix} M(c^1) \\ M(c^2) \end{bmatrix} = \begin{bmatrix} M(11 & 00 & 11 & 11 & 00 & 11 & 00 & 00 & 00 & 00 & 00 & 00) \\ M(01 & 00 & 01 & 10 & 10 & 10 & 11 & 10 & 00 & 00 & 00 & 00) \end{bmatrix}$$

$$= \begin{bmatrix} 11001111 & 00110000 & 00000000 \\ 00110011 & 11001100 & 00000000 \\ 00001100 & 11110011 & 00000000 \\ 00000011 & 00111100 & 11000000 \\ 00000000 & 11001111 & 00110000 \\ 00000000 & 00110011 & 11001100 \\ 00000000 & 00001100 & 11110011 \\ \\ 01000110 & 10101110 & 00000000 \\ 00010001 & 10101011 & 10000000 \\ 00000100 & 01101010 & 11100000 \\ 00000001 & 00011010 & 10111000 \\ 00000000 & 01000110 & 10101110 \end{bmatrix}. \quad (3.8)$$

Another generator matrix for $\mathcal{G}_{24}$ [17] is

$$M' = \begin{bmatrix} 01111000 & 01111000 & 01111000 \\ 10011100 & 10011100 & 10011100 \\ 01010110 & 01010110 & 01010110 \\ 11110000 & 11110000 & 00000000 \\ 00000000 & 11110000 & 11110000 \\ 11001100 & 11001100 & 00000000 \\ 00000000 & 11001100 & 11001100 \\ 10101010 & 10101010 & 00000000 \\ 00000000 & 10101010 & 10101010 \\ 11111111 & 00000000 & 00000000 \\ 00000000 & 11111111 & 00000000 \\ 00000000 & 00000000 & 11111111 \end{bmatrix} = \begin{bmatrix} M'_1 \\ M'_2 \\ \vdots \\ M'_7 \end{bmatrix}. \quad (3.9)$$

This generator matrix is clearly in the form that represents a canonical representation of $\mathcal{G}_{24}$ under T^8 , with canonical components $C_1, C_2, \dots, C_7$ represented by generator matrices $M'_1, M'_2, \dots, M'_7$, respectively. Note that the row space of M' is not invariant under T^j , if $j < 8$. This is because neither $T^4(c)$ nor $T^6(c)$ is in the row space of M' , where c is the 6th row of M' . Therefore the QC code $\mathcal{G}_{24}$ represented by (3.9) has index 8, while the index for the representation given by (3.8) is 2.

3.2.2 Reed-Muller Codes

Reed-Muller codes and their minimal trellis diagram were studied in Chapter 2. According to (2.20) the Reed-Muller code $\mathcal{R}(r, m)$ is a QC-cyclic code invariant under $\Lambda = T^l$, where l is $1/4$ of the code length. This property is proved by another method in this Section. Note that the generator matrix of the Reed-Muller code $\mathcal{R}(r, m)$ given by (2.20) is a canonical representation of this code.

Lemma 3.2.2 $\mathcal{R}(1, m)$, the Reed-Muller code of length $n = 2^m$ and dimension $m + 1$, is a QC code invariant under $\Lambda = T^{2^{m-2}}$.

Proof Consider the following generator matrix G_m^1 of $\mathcal{R}(1, m)$

$$G_m^1 = \begin{bmatrix} v_0 \\ v_1 \\ \vdots \\ v_m \end{bmatrix} \quad (3.10)$$

It can be easily verified that C' , the subspace of F^{2^m} generated by the three vectors v_0 , v_{m-1} , and v_m , coincides with the subspace generated by the vectors v_m , $\Lambda(v_m)$, and $\Lambda^2(v_m)$. On the other hand $\Lambda(v_i) = v_i$, $1 \leq i \leq m-2$. Therefore $\mathcal{R}(1, m)$ is invariant under Λ . ♣

Corollary 3.2.1 *If $v \in F^{2^m}$, and $f(x)v = f(\Lambda)v$, then by Lemma 3.2.2, $\mathcal{R}(1, m)$ is a submodule of the $F[x]$ -module F^{2^m} , and has the following decomposition into cyclic submodules*

$$\mathcal{R}(1, m) = \left(\bigoplus_{i=1}^{m-2} \langle v_i \rangle \right) \oplus \langle v_m \rangle \quad (3.11)$$

in which as vector spaces $\langle v_m \rangle$ and $\langle v_i \rangle$, $1 \leq i \leq m-2$, are subspaces of F^{2^m} with dimensions 3 and 1, respectively.

Theorem 3.2.3 *$\mathcal{R}(r, m)$, the Reed-Muller code of length $n = 2^m$ consisting of the Boolean polynomials of degree at most r , is a QC code invariant under $\Lambda := T^{2^{m-1}}$.*

Proof (By induction on r .) From Lemma 3.2.2, the statement is true for $\mathcal{R}(1, m)$. Suppose it holds for $\mathcal{R}(r-1, m)$, $r \leq m$ (induction hypothesis).

Let t be a code word of $\mathcal{R}(r, m)$. Without loss of generality, we may assume that t is a Boolean monomial. If t has degree $r-1$, then $t \in \mathcal{R}(r-1, m)$ and hence $\Lambda(t) \in \mathcal{R}(r-1, m) \subset \mathcal{R}(r, m)$.

Suppose t has degree r , and $t = u_1 u_2 \cdots u_r$ where $u_i \in \{v_1, v_2, \dots, v_m\}$. Denote $u_1 u_2 \cdots u_{r-1}$ by t' . By the assumption $\Lambda(t')$ is in $\mathcal{R}(r-1, m)$.

Since $u_r \in \mathcal{R}(1, m)$, we have $\Lambda(u_r) \in \mathcal{R}(1, m)$, and hence it is a polynomial in m variables of degree 1, while $\Lambda(t')$ is a polynomial in m variables of degree at most

$r - 1$. Therefore $\Lambda(t')\Lambda(u_r)$ is a polynomial of degree at most r , implying that it is a code word in $\mathcal{R}(r, m)$. The proof follows from the fact that

$$\Lambda(t) = \Lambda(t'u_r) = \Lambda(t')\Lambda(u_r) , \quad (3.12)$$

and the principle of induction. ♣

3.3 Quasi-Cyclic Codes in Cyclic Form

3.3.1 General Cyclic Codes

We first consider the case $p = 1$ in Theorem 3.2.2 so that the nonzero blocks in all code words of C are scalar multiples, and there is just one canonical component. By replacing this unique nonzero block with a 1 and the zero block by a 0, the QC code C can be viewed as a cyclic code. From (3.6), we obtain the well known relation between the length and dimension of cyclic codes, $m_1 = m + 1 - k$. Therefore, if $p = 1$, the properties of C are well known. A QC code of this form will be referred to as a *general cyclic code*.

Example 3.3.1 In the binary $(8, 5)$ cyclic code generated by $a(x) = 1 + x^2 + x^3 + x^5$, the nonzero polynomial code word of least degree is $g(x) = 1 + x + x^2 + x^3$. It follows that the $(24, 5)$ QC code C invariant under T^3 with cyclic basis $c = v \square vv \square v \square \square$, where v is a nonzero 3-tuple and $\square$ denotes the 3-tuple 000 , has TOGM

$$M = \begin{bmatrix} v & v & v & v & \square & \square & \square & \square \\ \square & v & v & v & v & \square & \square & \square \\ \square & \square & v & v & v & v & \square & \square \\ \square & \square & \square & v & v & v & v & \square \\ \square & \square & \square & \square & v & v & v & v \end{bmatrix}. \quad (3.13)$$

An (n, k) QC code C with $n = Lm$, invariant under $\Lambda = T^m$, is called a 1-generator QC code if there is a code word $c \in C$ such that the set $\{c, \Lambda(c), \dots, \Lambda^{k-1}(c)\}$

is a basis for C' , as a vector space. The code word c will be called the cyclic basis of C' . In fact any 1-generator QC' code C' is a cyclic submodule of the $F[x]$ -module F^n with $f(x)c = f(\Lambda)c$, and vice versa [21, 22].

Any general cyclic code is a 1-generator QC' code. Note that a 1-generator QC' code C' is a general cyclic code iff $p = 1$. The following proposition can now be stated.

Proposition 3.3.1 *The canonical components of a QC' code C' are precisely the invariant factors of the module C' iff each canonical component is a general cyclic code.*

The QC' codes represented by (2.20) and (3.9) are two examples of such codes.

3.3.2 Cyclic Codes

A subclass of (mk, k) cyclic codes have been viewed as QC' codes invariant under T^m [2]. More precisely, these codes are 1-generator QC' codes. The question arises as to when, in general, a cyclic code C' can be interpreted as a QC' code invariant under T^m , $m > 1$. In this case, the relationship between the TOGM of C' , viewed as a cyclic code, and the TOGM of C' , viewed as a QC' code, is of interest. The following proposition answers this question.

Proposition 3.3.2 *Let C' be an (n, k) cyclic code with generator polynomial $g(x)$. Suppose $m < k$ with $k-1 = tm+r$, $0 \leq r < m$. If $n = Lm$, then C' can be viewed as a QC' code invariant under T^m , with polynomial generator set $\{g(x), xg(x), \dots, x^{m-1}g(x)\}$. $r+1$ components of the QC' code C' have dimension $t+1$, and $m-r-1$ components have dimension t .*

Example 3.3.2 The $(15, 5)$ cyclic code C' with generator polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$ can be considered as a QC' code invariant under T^3 .

The polynomial generator set is $\{g(x), xg(x), x^2g(x)\}$, and the canonical generator matrix is

$$\begin{bmatrix} M(c^1) \\ M(c^2) \\ M(c^3) \end{bmatrix} = \begin{bmatrix} 111 & 011 & 001 & 010 & 000 \\ 000 & 111 & 011 & 001 & 010 \\ 011 & 101 & 100 & 101 & 000 \\ 000 & 011 & 101 & 100 & 101 \\ 001 & 110 & 110 & 010 & 100 \end{bmatrix}. \quad (3.14)$$

Example 3.3.3 Consider the (15, 9) cyclic code C with $g(x) = 1 + x + x^2 + x^3 + x^6$. Note that this code is not an (mk, k) code. In this case $k - 1 = 8$, and both 3 and 5 divide 15 and are smaller than 8. For $m = 3$ and $L = 5$, the PG-set is $\{g(x), xg(x), x^2g(x)\}$ and the canonical generator matrix is

$$\begin{bmatrix} M(c^1) \\ M(c^2) \\ M(c^3) \end{bmatrix} = \begin{bmatrix} 111 & 100 & 100 & 000 & 000 \\ 000 & 111 & 100 & 100 & 000 \\ 000 & 000 & 111 & 100 & 100 \\ 011 & 110 & 010 & 000 & 000 \\ 000 & 011 & 110 & 010 & 000 \\ 000 & 000 & 011 & 110 & 010 \\ 001 & 111 & 001 & 000 & 000 \\ 000 & 001 & 111 & 001 & 000 \\ 000 & 000 & 001 & 111 & 001 \end{bmatrix}. \quad (3.15)$$

For $m = 5$ and $L = 3$, the PG-set is $\{g(x), xg(x), \dots, x^4g(x)\}$, and the canonical generator matrix is

$$\begin{bmatrix} M(c^1) \\ M(c^2) \\ M(c^3) \\ M(c^4) \\ M(c^5) \end{bmatrix} = \begin{bmatrix} 11110 & 01000 & 00000 \\ 00000 & 11110 & 01000 \\ 01111 & 00100 & 00000 \\ 00000 & 01111 & 00100 \\ 00111 & 10010 & 00000 \\ 00000 & 00111 & 10010 \\ 00011 & 11001 & 00000 \\ 00000 & 00011 & 11001 \\ 00001 & 11100 & 10000 \end{bmatrix}. \quad (3.16)$$

Example 3.3.4 The (15, 7) primitive BCH code with generator polynomial $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ can be represented by the following generator matrices $M1$ and $M2$, viewed as QC codes under T^3 and T^5 , respectively.

$$M1 = \begin{bmatrix} 100 & 010 & 111 & 000 & 000 \\ 000 & 100 & 010 & 111 & 000 \\ 000 & 000 & 100 & 010 & 111 \\ 010 & 001 & 011 & 100 & 000 \\ 000 & 010 & 001 & 011 & 100 \\ 001 & 000 & 101 & 110 & 000 \\ 000 & 001 & 000 & 101 & 110 \end{bmatrix} \quad M2 = \begin{bmatrix} 10001 & 01110 & 00000 \\ 00000 & 10001 & 01110 \\ 01000 & 10111 & 00000 \\ 00000 & 01000 & 10111 \\ 00100 & 01011 & 10000 \\ 00010 & 00101 & 11000 \\ 00001 & 00010 & 11100 \end{bmatrix}$$

3.4 1-Generator quasi-cyclic codes

The definition of 1-generator QC codes was given in Section 3.3. Some properties of these codes are presented in this section. Consider a 1-generator (Lm, k) QC code C invariant under T^m with cyclic basis $u = (u_1, u_2, \dots, u_L)$ where each u_i is considered as one symbol. Define the *block-span length* of u to be the length of the smallest interval of block.. containing all nonzero symbols in u . If the nonzero symbols of the cyclic basis u are identical, then as in previous section, C can be viewed as a cyclic code. In this section, it is assumed that the non zero symbols u_i are not all the same, and therefore C has at least two canonical components.

As an application of Theorem 3.2.2, we have the following lemma.

Lemma 3.4.1 *Let $A = \{v_1, v_2\}$ be an independent subset of the vector space $GF(2)^m$ over $GF(2)$ and $v_3 = v_1 + v_2$. Consider a 1-generator QC code C of length Lm with cyclic basis $c = v_1 v_2 v_3 \square \dots \square$, where $\square$ denotes a block of m zeros. Then, C has dimension $k = L - 1$ and its canonical decomposition consists of two components, one of which has dimension 1.*

Proof Let $a(x) = a_0 + a_1x + \dots + a_{m-1}x^{m-1}$, $b(x) = b_0 + b_1x + \dots + b_{m-1}x^{m-1}$, and $d(x) = d_0 + d_1x + \dots + d_{m-1}x^{m-1}$ be the polynomial representations of v_1 , v_2 , and v_3

respectively, and define $t_i(x) = a_i + b_i x + d_i x^2$ for $0 \leq i \leq m-1$. It has been shown in [22] that if

$$h(x) = \frac{1 + x^L}{\gcd(t_0(x), t_1(x), \dots, t_{m-1}(x), 1 + x^L)} \quad (3.17)$$

then $k = \deg(h(x))$.

If $t_i(x) \neq 0$, then it has precisely two nonzero coefficients, implying that $t_i(x) = 1 + x$, or $1 + x^2$, or $x + x^2$. On the other hand, since $v_1 + v_2 = v_3 \neq 0$, at least for one index, say j , we have $t_j(x) = 1 + x^2$. Therefore

$$\gcd(t_0(x), t_1(x), \dots, t_{m-1}(x)) = 1 + x.$$

resulting in $k = L - 1$.

According to Theorem 3.2.2, the canonical decomposition of C consists of two components, and considering the dimension of C , each of these components has dimension at most $m - 2$. It follows that the atomic code word derived from c is of the form $c' = u_1 u_2 u_3 \square \dots \square$, where $u_i \in \{v_1, v_2, v_3\}$. ♣

For the remainder of the section suppose that the first symbol of u is nonzero. It may happen that in the 1-generator QC code C with cyclic basis u , one of the atomic code words is u itself. This is answered in the following theorem.

Theorem 3.4.1 *Let C be a 1-generator (Lm, k) QC code, invariant under T^m , with cyclic basis u in which the nonzero symbols are not identical. If there are enough zero blocks on the rightmost side of u , then u is an atomic code word of C . In addition, all atomic code words of the 1-generator $(mL + rL, k')$ QC code C' with cyclic basis u' , obtained from u by adding $r \geq 1$ zero blocks to the right side of u , can be read from the atomic code words of C' .*

Proof Let e denote the block-span length of u and e_0 be the number of zero symbols on the rightmost side of u , so that $e + e_0 = L$. A generator matrix for C is shown in Fig. 3.1. In this figure, the first row of section B is u , the cyclic basis of C . The vector containing the first e blocks of u has been denoted by v , so that the first and

Figure 3.1: Generator matrix of a 1-generator QC code C with cyclic basis u , where u is the first row of B .

last symbols of v are nonzero and the number of zero blocks on the right side of v is e_0 . The i th row of section A is the i th block shift of the last row of section B . A_2 , B_4 , and B_5 consist of zero blocks.

Consider the matrix M_1 consisting of A and the rows of B containing B_1 . Since we have assumed that C has at least two canonical components, the rows involved in transforming M , shown by Fig. 3.1, into a row reduced matrix are precisely those in M_1 . We now investigate this fact in more detail. In the row operations, v is preserved but added to the rows of A if necessary for the transformation. If there are exactly two canonical components, then the resulting row reduced matrix M' contains section B and a transformed A , say A' , in which the i th row has its first nonzero symbol in the i th block. If in the row reduced matrix M' , u is the vector of smallest block-span length, then it remains as an atomic code word. This will happen when $e_0 \geq 2e - 3$, since in this case all the rows of A' have block span length at least e .

To transform the row reduced matrix M' into a TOGM for C , only the rows of M' involving $B3$ and A' are needed and $B2$ has no role in obtaining this TOGM. In other words, the dimension of the canonical components of C distinct from B are obtained by row operations involving only A , $B1$, and $B3$. Note that if M does not have full rank, then $B2$ is involved in the row operations that transform the rows of A . To avoid $B2$ having such a role, we initially reduce the rows of A so that the resulting matrix is a generator matrix for C with full rank. With this matrix, adding i zero-blocks to the right side of u increases the dimension of the canonical component B , but does not change the dimension of the other components.

Now suppose that the number of rows located in $B2$, other than those that border $B1$ and $B3$, is at least c . Then the areas of $A2$ affected by the first and second steps of row operations, applying $B1$ and $B3$ respectively, are completely distinct. In this case, the middle portion of $A2$ remains zero during the transformation to a TOGM. Under this condition, if we add a zero block to the right side of u to obtain u' , the atomic code words of the QC code C' (with cyclic basis u') are u' and those of C , distinct from u , with one zero block added to the middle. ♣

Remark In the generator matrix M shown in Fig. 3.1, let p_i denote the dimension of the matrix M_i . $\{p_i\}_{i=1}$ is a nondecreasing sequence. Let w be the smallest integer satisfying $p_{w+1} = p_w + 1$. Then if $B1$ and $B3$ have dimension at least w , u is an atomic code word and the dimensions of the other canonical components of C remain unchanged for the QC code C' obtained from C by adding zero blocks on the right side of u . Moreover, if $c_0 \geq \epsilon + 2(w - 1)$, then the atomic code words of C' can be read from those of C .

Example 3.4.1 Consider the 1-generator QC code C invariant under T^2 with cyclic basis u

$$u = 11 \ 01 \ 11 \ 01 \ 00 \ 00 \ 00 \ 00 \ , \quad (3.18)$$

which has TOGM

$$\begin{bmatrix} M(c^1) \\ M(c^2) \end{bmatrix} = \begin{bmatrix} M(11 & 01 & 11 & 01 & 00 & 00 & 00 & 00) \\ M(01 & 00 & 00 & 00 & 00 & 10 & 10 & 10) \end{bmatrix}. \quad (3.19)$$

For this code, $p_1 = 2$ and $p_2 = 3$, so that $w = 1$ and we have $c + 2(w - 1) = 4 + 2(1 - 1) = 4$ zero blocks on the right of u . Note that this number of zero blocks may not be reduced since the QC code invariant under T^2 with cyclic basis $u' = 11011101000000$ has TOGM

$$\begin{bmatrix} M(c^1) \\ M(c^2) \end{bmatrix} = \begin{bmatrix} M(11 & 10 & 01 & 00 & 00 & 00 & 00) \\ M(01 & 00 & 00 & 00 & 00 & 11 & 10) \end{bmatrix}, \quad (3.20)$$

and u' is not an atomic code word of C' .

Although the above example shows that to have u as an atomic code word, the number of zero blocks on the rightmost side of u has to be at least $c + 2(w - 1)$, in most cases this number can be reduced substantially. This is illustrated by the following example.

Example 3.4.2 Consider the QC code $C1$, invariant under T^3 , with cyclic basis

$$u_1 = 110 \ 010 \ 011 \ 111 \ 000, \quad (3.21)$$

with $p_1 = 3$ and $p_2 = 4$. This implies that $w = 1$ and $c + 2(w - 1) = 4$, but $C1$ has TOGM

$$\begin{aligned} M1 &= \begin{bmatrix} M(c^1) \\ M(c^2) \\ M(c^3) \end{bmatrix} = \begin{bmatrix} M(110 & 010 & 011 & 111 & 000) \\ M(011 & 1 & 000 & 110 & 010) \\ M(001 & 100 & 111 & 110 & 100) \end{bmatrix} \\ &= \begin{bmatrix} 110 & 010 & 011 & 111 & 000 \\ 000 & 110 & 010 & 011 & 111 \\ 011 & 111 & 000 & 110 & 010 \\ 001 & 100 & 111 & 110 & 100 \end{bmatrix}. \end{aligned} \quad (3.22)$$

To illustrate Theorem 3.4.1, consider the QC codes $C2$ and $C3$, invariant under T^3 , with cyclic bases u_2 and u_3 , respectively, where

$$\begin{aligned} u_2 &= 110 \ 010 \ 011 \ 111 \ 000 \ 000, \\ u_3 &= 110 \ 010 \ 011 \ 111 \ 000 \ 000 \ 000. \end{aligned} \quad (3.23)$$

$C2$ and $C3$ have the following trellis oriented generator matrices, $M2$ and $M3$, respectively.

$$\begin{aligned} M2 &= \begin{bmatrix} M(110 \ 010 \ 011 \ 111 \ 000 \ 000) \\ M(011 \ 111 \ 000 \ 000 \ 110 \ 010) \\ M(001 \ 100 \ 111 \ 000 \ 110 \ 100) \end{bmatrix} \\ &= \begin{bmatrix} 110 & 010 & 011 & 111 & 000 & 000 \\ 000 & 110 & 010 & 011 & 111 & 000 \\ 000 & 000 & 110 & 010 & 011 & 111 \\ 011 & 111 & 000 & 000 & 110 & 010 \\ 001 & 100 & 111 & 000 & 110 & 100 \end{bmatrix} \end{aligned} \quad (3.24)$$

$$\begin{aligned} M3 &= \begin{bmatrix} M(110 \ 010 \ 011 \ 111 \ 000 \ 000 \ 000) \\ M(011 \ 111 \ 000 \ 000 \ 000 \ 110 \ 010) \\ M(001 \ 100 \ 111 \ 000 \ 000 \ 110 \ 100) \end{bmatrix} \\ &= \begin{bmatrix} 110 & 010 & 011 & 111 & 000 & 000 & 000 \\ 000 & 110 & 010 & 011 & 111 & 000 & 000 \\ 000 & 000 & 110 & 010 & 011 & 111 & 000 \\ 000 & 000 & 000 & 110 & 010 & 011 & 111 \\ 011 & 111 & 000 & 000 & 000 & 110 & 010 \\ 001 & 100 & 111 & 000 & 000 & 110 & 100 \end{bmatrix} \end{aligned} \quad (3.25)$$

As stated in Theorem 3.4.1, these generator matrices can be read directly from the TOGM of $C1$, given by (3.22).

3.5 Permutations and Quasi-Cyclic Codes

The trellis complexity of a linear block code may be decreased by properly permuting its bit positions. From this point of view, Vardy and Be'ery [1] have studied some sub-classes of BCH codes. In this section their work is extended to QC codes.

Let C be a QC code of length $n = Lm$, invariant under T^m . Denote a subset of $\{0, 1, \dots, n-1\}$ of the form $\bigcup_{j=1}^r \{i_j m, i_j m + 1, \dots, i_j m + m - 1\}$ by I_m , where $0 \leq i_1 \leq i_2 \leq \dots \leq i_r \leq L-1$. This notation is used so that C can be seen as a cyclic group code of length L in which each symbol is an m -tuple. For a nonnegative integer a , we define

$$am + I_m = \{(am + j) \bmod n : j \in I_m\}.$$

For a subset I of $\{0, 1, \dots, n-1\}$, $C[I]$ is defined as the sub-code of C consisting of all the code words that are zero in those positions not in I . $C(I)$ is the code obtained from $C[I]$ by deleting those positions not contained in I . For $c \in C[I]$ the code word of $C(I)$ corresponding to c is denoted by c_I . That is $C(I) = \{c_I : c \in C[I]\}$.

Proposition 3.5.1 *Let C be a QC code of length $n = Lm$, invariant under T^m , and I_m a subset of $\{0, 1, \dots, n-1\}$ such that $am + I_m = I_m$ for some smallest integer $a < L$. Then $C(I_m)$ is a QC code invariant under T^m .*

Proof Since $am + I_m = I_m$, we have $C[I_m] = C[am + I_m]$. If $c \in C[I_m]$ then $T^{am}(c) \in C[am + I_m] = C[I_m]$, implying that $T^{am}(c)_{I_m} \in C(I_m)$. From $am + I_m = I_m$ and $am < n$ it follows that a is a divisor of L , say $L = aL'$, and

$$I_m = \bigcup_{j=0}^{L'-1} \{(i_1 + ja)m, (i_1 + ja)m + 1, \dots, (i_1 + ja)m + m - 1\}. \quad (3.26)$$

This means that the distance between two successive block-bits of I_m is $(a-1)$ block-bits (that is $(a-1)m$ bits) and this is a constant. It follows that for $c \in C[I]$ we have $T^{am}(c)_{I_m} = T^m(c_{I_m})$. Therefore $T^m(c_{I_m}) \in C(I_m)$. ♣

Proposition 3.5.2 *Let C be a QC code of length $n = Lm$, invariant under T^m , and I_m a subset of $\{0, 1, \dots, n-1\}$. Then for nonnegative integer a we have $C(I_m) = C(am + I_m)$ up to a possible cyclic shift of columns of $C(I_m)$.*

Figure 3.2: The diagram illustrating Proposition (3.5.2).

Proof C is invariant under T^m and hence $c \in C[Im]$ iff $T^{am}(c) \in C[am + Im]$. Therefore $C[Im] = C[am + Im]$ when c and $T^{am}(c)$ are considered as identical elements. Hence $C(Im) = C(am + Im)$ when c_{Im} and $T^{am}(c)_{am+Im}$ are viewed as identical element. Let us look at this correspondence in more detail. Suppose $I = \{i_1, i_2, \dots, i_r\}$ and j is the largest number such that $(am + i_j m) \bmod n = am + i_j m$. This is equivalent to saying that $r - j$ block-bits of Im are shifted to the left under the operator T^{am} . It follows that $c \in C(Im)$ iff $T^{m(r-j)}(c) \in C(am + Im)$. ♣

This proposition is illustrated by Fig. 3.2.

From Propositions 3.5.1 and 3.5.2 it follows that $C(tm + Im)$ is a QC code, invariant under T^m , for any integer t if $am + Im = Im$ for some integer $a < L$. In fact we have $C(tm + Im) = C(Im)$. This results in the following condition. If $n = Lrb$ with $rm = |Im|$, then

$$C'' = C(Im) \oplus C(m + Im) \oplus \dots \oplus C(bm - m + Im)$$

is an $(n, k'b)$ QC code invariant under T^{rm} , where k' is the dimension of $C(Im)$ and $L = rb$.

Example 3.5.1 Consider the Golay code $\mathcal{G}_{24}$ with double circulant generator

matrix M given by (3.8). In this case $n = 24$, $m = 2$, and $L = 12$. Let $I_2 = \{0, 1, 6, 7, 12, 13, 18, 19\}$. Since $6 + I_2 = I_2$, $C(I_2)$ is a QC code under T^2 and $rm = |I_2|$ implies that $r = 4$. Consider the permutation π defined by $\pi(0, 1, \dots, 23) = (I_2, 2 + I_2, 4 + I_2)$. Under this permutation the generator matrix M is transformed into

$$\bar{M} = \begin{bmatrix} 11111111 & 00000000 & 00000000 \\ 01101010 & 10011010 & 00000000 \\ 00111100 & 11110000 & 00000000 \\ 00011000 & 01101100 & 00101000 \\ 00001111 & 00111100 & 00000000 \\ 00000110 & 01001101 & 01100000 \\ 00000011 & 01011010 & 11000000 \\ 00000000 & 11111111 & 00000000 \\ 00000000 & 01010110 & 01101010 \\ 00000000 & 00111100 & 11110000 \\ 00000000 & 00001111 & 00111100 \\ 00000000 & 00000000 & 11111111 \end{bmatrix}. \quad (3.27)$$

From this matrix we see that $C(I_2) = \{00000000, 11111111\}$ and

$$\begin{aligned} C'' &= C(I_2) \oplus C(2 + I_2) \oplus C(4 + I_2) \\ &= \begin{bmatrix} 11111111 & 00000000 & 00000000 \\ 00000000 & 11111111 & 00000000 \\ 00000000 & 00000000 & 11111111 \end{bmatrix}, \end{aligned} \quad (3.28)$$

which is obviously a $(24, 3)$ QC code invariant under T^8 . Note that $C(I_2)$ is a cyclic code.

Example 3.5.2 As another example, consider the double circulant $(48, 24, 12)$ code (which is equivalent to an extended quadratic residue code) with systematic generator matrix $M = [I_{24} \ A]$, where A is the circulant matrix with leading row $1772667_{\mathbf{a}}$. Let $I_2 = \{0, 1, 6, 7, 12, 13, 18, 19, 24, 25, 30, 31, 36, 37, 42, 43\}$. Under the permutation π defined by $\pi(0, 1, \dots, 47) = (I_2, 2 + I_2, 4 + I_2)$, the TOGM M , obtained from M , is changed to matrix $\hat{M}$ given by (3.29). The blank spaces of $\hat{M}$ is covered by 0s. Note that the code C presented by M , (3.29), has state complexity $S = 16$, while introducing C by $\hat{M}$, (3.29), results in $S = 14$.

[illegible]

One can easily check that although (00000000 01011001 01010110) is an element of the row space of M given by (3.27), (01010110 00000000 01011001) is not in this space. This shows that $\pi(C)$ need not be a QC code under T^{rm} where $n = rbm$ and π is the permutation operation on the n -tuple $(0, 1, \dots, n-1)$ by which the positions corresponding to $jm + Ia$, $0 \leq j \leq b-1$, are bunched together and form the $(j+1)$ -th section of the new n -tuple. The next two propositions determine the permutations π such that $\pi(C)$ is also a QC code.

Let C be a cyclic code of length $n = n_1 n_2$ and $I = \{i_1, i_2, \dots, i_{n_1}\}$ be a subset of $\{0, 1, \dots, n-1\}$. Assume $I_k = kn_1 + I$ such that $\{0, 1, \dots, n-1\} = \bigcup_{k=0}^{n_2-1} I_k$, and consider a permutation π on the set $\{0, 1, \dots, n-1\}$ by which the positions corresponding to I_k , $0 \leq k \leq n_2-1$, are placed in the $(k+1)$ -th part of the new n -tuple in increasing order.

Proposition 3.5.3 $\pi(C)$ is a QC code invariant under T^{m_1} .

Proof Let $c \in C$. For simplicity $c = (c_0, c_1, \dots, c_{n-1})$ is denoted by $(0, 1, \dots, n-1)$. According to the definition of π and $\lambda =: T^{m_1}$ we have

$$\begin{aligned}\pi(c) &= (I, n_1 + I, 2n_1 + I, \dots, (n_2 - 1)n_1 + I) \\ \lambda\pi(c) &= ((n_2 - 1)n_1 + I, I, n_1 + I, \dots, (n_2 - 2)n_1 + I).\end{aligned}\tag{3.30}$$

In addition

$$\begin{aligned}\lambda(c) &= (n - n_1, n - n_1 + 1, \dots, n - 1, 0, 1, \dots, n - n_1 - 1) \\ \pi\lambda(c) &= (I', n_1 + I', 2n_1 + I', \dots, (n_2 - 1)n_1 + I')\end{aligned}\tag{3.31}$$

where $I' = \{i'_1, i'_2, \dots, i'_{n_1}\}$ and $i'_j = (i_j + n - n_1) \bmod n$. That is $I' = n - n_1 + I \bmod n$. This implies that $\lambda\pi(c) = \pi\lambda(c)$. Therefore, from $\lambda(c) \in C$ we have that $\lambda\pi(c) \in \pi(C)$. ♣

This proposition is illustrated by Fig. 3.3 with $n_1 = m$.

Example 3.5.3 The (15, 7) BCH code has generator matrix M given by (3.32). Let $I = \{0, 4, 6, 7, 8\}$, $n_1 = 5$, and $n_2 = 3$, so that $I_0 = I$, $I_1 = 5 + I$, and $I_2 = 10 + I$. According to the definition of π we have

Figure 3.3: Illustration of Proposition 3.5.3.

$$\pi(0, 1, \dots, 14) = (I_0, I_1, I_2).$$

Under the permutation π , the generator matrix M is transformed into matrix M as shown below.

$$M = \begin{bmatrix} 100010111000000 \\ 010001011100000 \\ 001000101110000 \\ 000100010111000 \\ 000010001011100 \\ 000001000101110 \\ 0000001000101110 \\ 0000000100010111 \end{bmatrix} \quad M = \begin{bmatrix} 11111 & 00000 & 00000 \\ 00000 & 11111 & 00000 \\ 00000 & 00000 & 11111 \\ 01001 & 00110 & 10000 \\ 00100 & 11100 & 11000 \\ 00011 & 11000 & 00100 \\ 00001 & 10100 & 01010 \end{bmatrix} \quad (3.32)$$

The code considered with generator matrix M is a QC' code of index 5.

Proposition 3.5.4 is a generalization of Proposition 3.5.3 to QC' codes, and the proof is omitted since it is essentially the same as that for Proposition 3.5.3.

Proposition 3.5.4 *Let C be a QC' code of length $n=rbm$, invariant under T^m . Suppose that $I_m = \bigcup_{j=1}^r \{i_j m, i_j m + 1, \dots, i_j m + m - 1\}$, and $\bigcup_{t=0}^{b-1} rmt + I_m = \{0, 1, \dots, n-1\}$. Then $\pi(C)$ is a QC' code invariant under T^{rm} , where π is the permutation on the n -tuple $(0, 1, \dots, n-1)$ by which the positions corresponding to $rmt + I_m$, $0 \leq t \leq b-1$, form the $t+1$ -th part of the resulting n -tuple. ♣*

Example 3.5.4 Consider again the Golay code $\mathcal{G}_{24}$ with double circulant generator matrix M given by (3.8). Choose $I_2 = \{0, 1, 4, 5, 6, 7, 10, 11\}$, so that $r = 4$ and $b = 3$. With the permutation

$$\pi(0, 1, \dots, 23) = (I2, 8 + I2, 16 + I2)$$

we obtain the generator matrix $\hat{M}$

$$\hat{M} = \begin{bmatrix} 1111111 & 0000000 & 0000000 \\ 0000000 & 1111111 & 0000000 \\ 0000000 & 0000000 & 1111111 \\ 01011010 & 10111000 & 0000000 \\ 00110011 & 11001100 & 0000000 \\ 00011101 & 01011010 & 0000000 \\ 00001111 & 00110000 & 11000000 \\ 00000101 & 00101011 & 10100000 \\ 00000011 & 11110011 & 11110000 \\ 00000000 & 01011010 & 10111000 \\ 00000000 & 00110011 & 11001100 \\ 00000000 & 00011101 & 01011010 \end{bmatrix} \quad (3.33)$$

$\mathcal{G}_{24}$ with generator matrix $\hat{M}$ is a QC code of index eight.

3.6 Summary

The relationship between quasi-cyclic codes and cyclic codes has been investigated through their respective generator matrices and generator polynomials. The canonical generator matrix of a quasi-cyclic code provides a justification for the term "*quasi-cyclic*". This relationship has been illustrated by studying the (24, 12) Golay code and the Reed-Muller codes. In these cases, the canonical generator matrices show the decomposition of C , viewed as a module, into invariant factors. The canonical generator matrices of the 1-generator QC codes C and C' with cyclic bases u and u' , respectively, were compared for the case when u and u' have the same nonzero section. The action of two types of permutations on QC codes has been studied.

Chapter 4

CYCLIC-FORM CODES AND THEIR SMALLEST REGULAR TRELLIS DIAGRAM

4.1 Introduction

The minimal 4-section trellis diagram of the Reed-Muller code $\mathcal{R}(r, m)$, discussed in Chapter 2, is regular in the sense that $|V_i| = |V_j|$, $1 \leq i, j \leq 3$, where $|V_i|$ denotes the number of vertices in the trellis at depth i . The advantage of this trellis structure is that all circuits in a VLSI implementation are equally active at all time indices, which results in more efficient decoding. This suggests to have the following definition.

Definition 4.1.1 (Regular Trellis Diagram) *A trellis diagram of a linear (n, k) block code C is called regular if for all i and j , $1 \leq i, j \leq n - 1$, $|V_i| = |V_j|$, where $|V_i|$ denotes the number of vertices of the trellis at time index i .*

In general, the minimal trellis diagram of a linear block code is not necessarily a regular trellis, implying that this minimal diagram is not necessarily the best when considering a VLSI implementation of the decoder. From this point of view the *smallest regular trellis diagram* (SRTD) of a linear block code C , introduced by the

following definition, is preferred to the minimal trellis diagram of C .

Definition 4.1.2 (Smallest Regular Trellis Diagram) A trellis diagram G_{SR} representing a linear block code C is called the smallest regular trellis diagram (SRTD) of C if

1. G_{SR} is regular;
2. The state complexity of G_{SR} is the same as that of G , the minimal trellis diagram of C ;
3. $t_{SR}(C)$, the number of identical parallel sub-trellises in G_{SR} , is maximum among all trellises representing C which satisfy conditions 1 and 2.

As example, the minimal 8-section trellis diagram of $\mathcal{R}(3,6)$ has only 2 identical parallel sub-trellises, whereas the corresponding SRTD has 128 parallel sub-trellises.

The structure of QC codes suggests that a SRTD can be determined for a more general class of codes, called *cyclic-form codes*. Hence, this chapter considers cyclic-form codes and their smallest regular trellis diagrams.

4.2 Cyclic-Form Codes and Their SRTD

It is known that in terms of state complexity a cyclic code is the worst among linear block codes of the same length and dimension [11]. However, in this chapter it is shown that cyclic codes, and in general cyclic-form codes, are not so poor when the number of parallel sub-trellises and trellis partitioning are considered. These two factors play a major role in the implementation of a soft decision decoder for these codes using a trellis [11].

Definition 4.2.1 (Cyclic-Form Code) An (n, k) linear block code C is called a cyclic-form code if in M , the trellis oriented generator matrix of C , for any i , $1 \leq i \leq k$, precisely one row of M has span $[i, n - k + i]$.

Example 4.2.1 The linear block code C with generator matrix

$$M = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

is a cyclic-form code. Note that this code is not a cyclic code, but all cyclic codes are cyclic-form codes.

Theorem 4.2.1 *The smallest regular trellis diagram G_{SR} of an (n, k) linear cyclic-form code C consists of $\max\{1, 2^{2s-k}\}$ structurally identical parallel sub-trellises, where s is the state complexity of the code.*

Proof Let G_{min} be the minimal trellis diagram of C . If $s = k$, then it is obvious that the graph formed by 2^k internally disjoint paths of length n , that share the same initial and final vertices, is the smallest regular trellis diagram of C . Now suppose $k - s > 0$. Consider the bipartite graph G with 2^s vertices on each side such that each vertex has degree 2, and the i -th pair of vertices, $1 \leq i \leq 2^{s-1}$, on the left side are adjacent to both the i -th and $(2^{s-1} + i)$ -th vertices on the right side. Pairs of vertices are determined beginning with the top two, and proceeding down the graph to the bottom two. The graph $2G$ is defined to be the graph obtained by concatenating two copies of G such that the right most vertices of the left copy are also the left most vertices of the right copy. This construction is illustrated in Fig. 4.1.

G consists of 2^{s-1} components, while the number of components in $2G$ is 2^{s-2} . Define $(m+1)G$ to be the graph obtained by concatenating mG with G , in the same manner that $2G$ was defined. It is easily checked that mG consists of 2^{s-m} components (induction on m). The central part of G_{min} is $(k-s)G$, and contains those time indices for which the number of vertices is 2^s . Hence, this part of G_{min} has 2^{2s-k} components. In fact, it can be shown that this part of G_{min} determines the structure of G_{SR} . This is shown by the following algorithm:

1. Delete the two sections of G_{min} that lie on the right and left sides of $(k-s)G$, except for the initial and final vertices v_0 and v_n .
2. Connect vertex v_0 (resp. v_n) to all vertices on the left (resp. right) side of $(k-s)G$ by 2^s internally disjoint paths.

The resultant trellis is regular and has state complexity s , satisfying the first two conditions of an SRTD. This trellis consists of 2^{2s-k} identical parallel sub-trellises and indeed it is G_{SR} , since an increase in the number of components of $(k-s)G$ causes either an increase in the state complexity or a loss of code linearity. ♣

Example 4.2.2 For the cyclic-form code C with trellis oriented generator matrix

$$M = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

the minimal trellis diagram G_{min} , the bipartite graph G and the central portion, $2G$, of G_{min} are shown in Fig. 4.1.

Corollary 4.2.1 *The smallest regular trellis diagram of an (n, k) linear cyclic block code C consists of*

$$t(C) = \begin{cases} 2^k & \text{if } 2k < n+1 \\ \max\{1, 2^{2n-3k}\} & \text{if } 2k \geq n+1 \end{cases} \quad (4.1)$$

identical parallel sub-trellises.

We now describe a method for constructing the smallest regular trellis diagram of an (n, k) linear cyclic-form block code C with trellis oriented generator matrix M .

If $s = k$, then the smallest regular trellis diagram, G_{SR} , consists of 2^k parallel paths of length n connecting the initial and final vertices. Suppose $k - s = m > 0$.

Figure 4.1: a) The minimal trellis diagram, G_{min} , of the linear block code C given in Example 1.2.2; b) the bipartite graph G ; c): $2G$, the central section of G_{min} .

Consider the $(n, 2m)$ linear block code C' with generator matrix M' whose first m and last m rows are precisely the first and last m rows of M . The state complexity of C' is $m = k - s$. Let G'_{min} denote the minimal trellis diagram of C' . The following steps can be used to obtain G'_{SR} , the smallest regular trellis diagram of C' :

1. Discard the portion of G'_{min} between the initial vertex and the vertices at time index m .
2. In the remaining graph, connect the initial vertex v_0 to all vertices at time index m with internally disjoint paths.
3. At time index j , $1 \leq j < m$, place one vertex on each path drawn in the previous step.
4. Repeat the above steps with time indices 0 and m replaced by time indices n and $n - m + 1$, respectively. The resulting graph is G'_{SR} .

With the rows of M' removed from M , the remaining matrix M'' represents an $(n, 2s - k)$ linear block code C'' with state complexity that is also $2s - k$. Hence G''_{SR} , the smallest regular trellis diagram of C'' , consists of 2^{2s-k} parallel paths connecting the initial and final vertices. The smallest regular trellis diagram G_{SR} of C is $G_{SR} = G'_{SR} \times G''_{SR}$.

This construction produces a sectionalized trellis diagram, even when $t(C) = 1$. The resulting trellis is a $(k - s + 2)$ -section trellis in which each edge in the first and last sections has a label of $(k - s + 2)/2$ bits and the other edges have a label of 1 bit.

Example 4.2.3 Consider the cyclic-form code C given in Example 4.2.2 with trellis oriented generator matrix M , and parameters $k = 6$ and $s = 4$. The matrices

M' and M'' are given by

$$M' = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \quad M'' = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

and the trellis diagrams G''_{mm} , G''_{SR} , G''_{SR} , and G_{SR} are shown in Fig. 4.2. G_{SR} is a 4-section trellis diagram. Each edge in the first and last section of G_{SR} has a label of 4 bits whereas the edges of the second and third sections have a label of one bit. Note that considering G''_{SR} and G_{SR} as 4-section trellises shows that these two trellises are indeed minimal trellis diagrams of C' and C with trellis oriented generator matrices M' and $\bar{M}$, respectively, where

$$M' = \begin{bmatrix} 1101 & 1 & 0 & 0000 \\ 0111 & 1 & 1 & 0000 \\ 0000 & 1 & 0 & 1110 \\ 0000 & 0 & 1 & 1101 \end{bmatrix} \quad \bar{M} = \begin{bmatrix} 1101 & 1 & 0 & 0000 \\ 0111 & 1 & 1 & 0000 \\ 0010 & 1 & 0 & 1000 \\ 0001 & 1 & 1 & 1100 \\ 0000 & 1 & 0 & 1110 \\ 0000 & 0 & 1 & 1101 \end{bmatrix}$$

These two matrices are sectionalized versions of M' and M , respectively.

This observation leads to a simpler algorithm for the construction of the SRTD of a cyclic-form code. For C an (n, k) cyclic-form code with state complexity s and TOGM M , this algorithm is given by the followings steps:

1. Consider the first and the last $(n - k + s)/2$ columns of M as two columns, so that M is now a $k \times (k - s + 2)$ matrix $\bar{M}$.
2. The minimal trellis diagram of the $(k, k - s + 2)$ code $\bar{C}$ with TOGM $\bar{M}$, in the sense of Theorem 2.1.2, is the SRTD of C .

Figure 4.2: Relating to Example 4.2.3: a) G'_{min} , the minimal trellis diagram of C'' ; b) G'_{SR} , the smallest regular trellis diagram of C'' ; c) G''_{SR} , the smallest regular trellis diagram of C''' ; d) G_{SR} , the smallest regular trellis diagram of C .

Chapter 5

THE TRELLIS STRUCTURE OF QUASI-CYCLIC CODES

5.1 Introduction

In Chapter 3 a canonical generator matrix was associated with a QC code. In this chapter the canonical generator matrix is employed to analyze both the minimal trellis diagram and SRTD of these codes. In particular, Theorems 5.2.1 and 5.3.1 show that QC codes have an interesting graphical structure. The symmetric structure of these two associated graphs is a result of the cyclic structure of QC codes.

The minimal trellis diagram and the smallest regular trellis diagram are investigated in Sections 2 and 3, respectively.

5.2 Minimal Trellis Diagram

In terms of trellis complexity, the canonical representation theorem describes the minimal L -section trellis diagram of a QC code. Consider a QC code C with a canonical decomposition and TOGM M' given by (3.4) and (3.5), respectively. If G_i , $1 \leq i \leq p$, is the minimal L -section trellis diagram of $D(c^i)$, then $G = \prod_{i=1}^p G_i$ is the minimal L -section trellis diagram of C . It is straightforward to show that G_i is a symmetric graph with nondecreasing state space dimension from vertex v_0 to the

center. This leads to the following theorem.

Theorem 5.2.1 *Let C be an (Lm, k) QC code invariant under $\Lambda = T^m$. Then the minimal L -section trellis diagram of C is a symmetric graph with nondecreasing state space dimension from vertex v_0 to the center of the graph. $\square$*

In the remainder of this section, we show that the trellis complexity of a QC code C with generator matrix M can be determined without transforming M into a TOGM. This complexity can be obtained from a row reduced generator matrix of C .

Lemma 5.2.1 *Suppose M is a generator matrix of an (Lm, k) QC code C invariant under T^m and M_i , $1 \leq i \leq L$, is the $k \times im$ matrix whose j^{th} column is the same as that of M , $1 \leq j \leq im$. Moreover, suppose that M' is a TOGM for C . Then the number of rows of M' with nonzero entries within the first im positions (or i leftmost blocks) is precisely p_i , the rank of M_i .*

Proof From the definition, M' is a row reduced matrix. Let r_i denote the number of atomic classes with starting position in the interval $[1, im]$. If u is one of the rows of M' with starting position in $[1, im]$, then the string of the first im components of u can be regarded as a vector, denoted by u .

Having M' as a TOGM implies that $\{u_1, u_2, \dots, u_{r_i}\}$ is an independent set. Since the remainder of the rows of M' are zero in their first i blocks, the set $\{u_1, u_2, \dots, u_{r_i}\}$ is a basis of V_i , the row space of M_i . Hence $r_i = p_i$. $\clubsuit$

The following theorem determines the effective length of the elements of the generator set of a QC code. For convenience define $p_0 = 0$.

Theorem 5.2.2 *Using the notation of Lemma 5.2.1,*

1. *The number of atomic classes of C with precisely $w - 1$ zero blocks on the leftmost side is $p_w - p_{w-1}$.*

2. The number of canonical components of C of dimension w , denoted by r_w , is $r_w = 2p_w - (p_{w-1} + p_{w+1})$.

Proof From Lemma 5.2.1, assume that M is a TOGM of C . The first statement is an immediate consequence of Lemma 5.2.1. For the second statement, according to Theorem 3.2.2, all atomic classes of C can be obtained from p_1 atomic classes whose support begins in the interval $[0, m]$. In fact, cyclic shifts of these p_1 code words produce all atomic classes. Suppose atomic class A has precisely $w - 1$ zero blocks on its leftmost side. From the first statement, the number of such atomic classes is $p_w - p_{w-1}$. If A has at least one zero block on its rightmost side, then $\Lambda(A)$ is also an atomic class that has precisely w zero blocks on its leftmost side. Hence, $\Lambda(A)$ is one of the $p_{w+1} - p_w$ atomic classes with w zero blocks on their leftmost side. Conversely, if A has no zero block on its rightmost side, then $(\Lambda^{-1})^{w-1}(A)$ is one of the p_1 atomic code words of M whose first block is nonzero.

Therefore $(p_w - p_{w-1}) - (p_{w+1} - p_w)$ is the number of atomic classes of effective block length $m - w + 1$, or equivalently, the number of canonical components of C of dimension w . ♣

Example 5.2.1 Consider the $(18, 6)$ QC code C with index 3 and generator matrix M

$$M = \begin{bmatrix} 111 & 011 & 101 & 110 & 101 & 000 \\ 000 & 111 & 011 & 101 & 110 & 101 \\ 101 & 000 & 111 & 011 & 101 & 110 \\ 110 & 101 & 000 & 111 & 011 & 101 \\ 101 & 110 & 101 & 000 & 111 & 011 \\ 011 & 101 & 110 & 101 & 000 & 111 \end{bmatrix} \quad (5.1)$$

For this code we have

$$M_1 = \begin{bmatrix} 111 \\ 000 \\ 101 \\ 110 \\ 101 \\ 011 \end{bmatrix} \quad M_2 = \begin{bmatrix} 111 & 011 \\ 000 & 111 \\ 101 & 000 \\ 110 & 101 \\ 101 & 110 \\ 011 & 101 \end{bmatrix} \quad M_3 = \begin{bmatrix} 111 & 011 & 101 \\ 000 & 111 & 011 \\ 101 & 000 & 111 \\ 110 & 101 & 000 \\ 101 & 110 & 101 \\ 011 & 101 & 110 \end{bmatrix}$$

Hence $p_1 = 3$, $p_2 = 5$, and $p_3 = 6$. It follows that

$$x_1 = 2p_1 - (p_0 + p_2) = 1$$

$$x_2 = 2p_2 - (p_1 + p_3) = 1$$

$$x_3 = 2p_3 - (p_2 + p_4) = 1.$$

Corollary 5.2.1 *From Theorem 5.2.2, the L-section minimal trellis diagram of C consists of $2^{2p_1-p_2}$ identical parallel sub-trellises.*

Corollary 5.2.2 *The graph structure of the minimal L-section trellis diagram of a QC code C is completely specified by a row reduced generator matrix for C (so there is no need to construct a trellis oriented generator matrix for C).*

Proof Let M and $\hat{M}$ be two generator matrices of C such that $\hat{M}$ is the row reduced matrix obtained from M . Moreover, suppose matrix M' is a TOGM of C derived from $\hat{M}$.

In the process of transforming $\hat{M}$ into M' , the number of zero blocks on the leftmost side of the rows of $\hat{M}$ remains unchanged. Hence, by Lemma 5.2.1, p_i is the number of rows of $\hat{M}$ for which all of the i leftmost blocks are nonzero. Therefore p_i is determined by $\hat{M}$. ♣

If the QC code C has dimension k , then $p_i < k, 1 \leq i \leq L$, and the necessary code information is obtained once $p_1, p_2, \dots$, and p_j have been computed where j is the smallest integer such that $p_j = k$. Let j be the smallest integer such that

$p_j = k$. Then Theorem 3.2.2 implies that $p_i - p_{i-1} \geq 1$ for $1 \leq i \leq j$ and $p_i = p_j$ for $i > j$. Further, we can show that computation of the p_i 's can be stopped when $p_i - p_{i-1} = 1$.

Theorem 5.2.3 *The necessary graph information for the minimal L -section trellis diagram of C , considered in Lemma 5.2.1, is obtained by computing $p_1, p_2, \dots$, and p_i where i is the smallest integer such that $p_i - p_{i-1} = 1$.*

Proof If $p_i - p_{i-1} = 1$, then there is just one atomic class A with $i - 1$ zero blocks on its leftmost side, and hence all the atomic classes with $j \geq i$ zero blocks on their leftmost side can be derived from A through cyclic shifts of A .

Let t be the smallest integer such that $p_t - p_{t-1} = 1$ and $t = k - p_{i-1}, t \geq 1$. Then $p_{i+t} = p_{i-1} + t + 1$ for $0 \leq t \leq t - 1$. Now, it is easy to see that there is one canonical component of dimension $i + t - 1$. It follows that we need just $p_1, p_2, \dots$, and p_i since the dimension of the remaining canonical components is not greater than $i - 1$. ♣

Corollary 5.2.3 *If C has dimension k , then the set $\{p_1, p_2, \dots, p_{\lfloor k/2 \rfloor}\}$ determines the L -section minimal trellis diagram of C .*

Example 5.2.2 Let $A = \{c_1, c_2, \dots, c_u\}$ be an independent set in the vector space $GF(2)^m$ over $GF(2)$. Consider the 1-generator QC code C with cyclic basis $c = c_1 c_2 \cdots c_u \square \cdots \square$ of length Lm , $L \geq u$, in which each $\square$ represents a string of zeros of length m . If $L = u$, then C has dimension w , and $p_1 = p_2$. This implies that a canonical decomposition of C consists of w components each of dimension one. Suppose $L > u$, and M is a generator matrix of C with rows $c, \Lambda(c) = I^m(c), \Lambda^2(c), \dots, \Lambda^{k-1}(c)$, where k is the dimension of C . Then the two sets $B_1 = \{c_1, c_2, \dots, c_u\}$ and $B_2 = \{c_1 c_2, c_2 c_3, \dots, c_u \square, \square c_1\}$ are the nonzero rows of M_1 and M_2 , respectively. Since these two sets are independent, we have $p_1 = w$ and $p_2 = w + 1$. It follows from Theorems 3.2.2 and 5.2.3 that the canonical

decomposition of C consists of w components, and $w - 1$ of these components are of dimension one. On the other hand, the constraints (3.7) and $k \leq L$ imply that the remaining canonical component of C has dimension $L - w + 1$.

5.2.1 State and Branch Complexity

Again let C be an (Lm, k) QC code invariant under T^m with an L -section minimal trellis diagram G in which all the sections have the same length.

It is clear from the structure of the TOGM M of C that, m_i , the number of rows of M which end in block i , $1 \leq i \leq L$, is

$$m_i = x_L + x_{L-1} + \cdots + x_{L-i+1}, \quad (5.2)$$

where x_j is the number of canonical components of C of dimension j . By induction it can be shown that

$$m_i = p_{L-i+1} - p_{L-i}, \quad 1 \leq i \leq L. \quad (5.3)$$

In fact the entering degree of each vertex at time index i is 2^{m_i} . The dimension of C_{i-} , given by k_{i-} , is

$$k_{i-} = \sum_{j=1}^i m_j = \sum_{j=1}^i (p_{L-j+1} - p_{L-j}) = p_L - p_{L-i} = k - p_{L-i}. \quad (5.4)$$

From the symmetry of the minimal trellis diagram G we have $k_{i+} = k_{(L-i)-} = k - p_i$. Therefore, by the state space theorem [5]

$$s_i = k - k_{i-} - k_{i+} = p_i + p_{L-i} - k, \quad (5.5)$$

where 2^{s_i} is the number of states of G at time index i . The number of edges of G connecting the vertices at times $i - 1$ and i is denoted by 2^{b_i} , and b_i is called the branch complexity of G at time i . From (5.3) and (5.5), we get

$$b_i = s_i + m_i = p_i + p_{L-i+1} - k. \quad (5.6)$$

The number of edges connecting any two adjacent vertices of G is 2^{m_1} while the number of vertices of G at time $i + 1$ adjacent to a fixed vertex at time i is $2^{m_1 - m_2}$. It follows that

$$l_i = s_i - m_i + m_1 = p_{i-1} + p_{L-i} - p_{L-1} \quad (5.7)$$

where 2^{l_i} is the number of identical parallel complete bipartite graphs forming G^i , the sub-trellis of G between time indices $i - 1$ and i .

5.3 Smallest Regular Trellis Diagram

In Chapter 4 a trellis diagram of a linear (n, k) block code C was defined to be regular if for all i and j , $1 \leq i, j \leq n - 1$, $|V_i| = |V_j|$, where $|V_i|$ denotes the number of vertices of the trellis at time index i . In general, the minimal trellis diagram of a linear block code is not necessarily a regular graph, which implies that this minimal diagram may be inefficient when trellis decoding is considered.

In this section, an L -section trellis diagram is determined for an (Lm, k) QC code C invariant under T^m which is regular and has state complexity equal to that of the minimal L -section trellis diagram. Furthermore, the number of identical parallel sub-trellises in the given diagram is the maximum possible. Such a trellis has been defined as the *Smallest Regular Trellis Diagram* (SRTD).

The canonical components $C_1, C_2, \dots, C_p$ of a QC code C are cyclic form codes when a block of length m is considered as a symbol. Theorem 5.3.1 is the main result of this section, as it establishes the relationship $t_{SR}(C) = \prod_{i=1}^p t_{SR}(C_i)$.

Let C be an (n, k) cyclic form code with TOGM M , minimal trellis diagram G , and state complexity s such that $2s \geq k \geq s$. The kernel of C , $\ker C$, is the sub-code of C with TOGM $\ker M$, the *kernel of M* , consisting of the first and last $k - s$ rows of M . The minimal trellis diagram corresponding to $\ker M$ is denoted as $\ker G$. If $2s \leq k$ and $k > s$ then we define $\ker C = C$. In C with $k = s$, any code word is considered as $\ker C$.

According to theorem 4.2.1, G_{SR} , the smallest regular trellis diagram of an (n, k) linear cyclic form block code C with minimal trellis diagram G and state complexity s , consists of $t_{SR}(C) = \max\{1, 2^{2s-k}\}$ structurally identical parallel sub-trellises, each a copy of the SRFD of $\ker C$ if $2s - k > 0$ and $k - s > 0$. The proof of Theorem 4.2.1 shows that $t_{SR}(C) > 1$ iff the center of G , $c(G)$, is a connected graph.

Lemma 5.3.1 *Let C be an (n, k) cyclic form code with FOGM M , minimal trellis diagram G , and state complexity s such that $2s - k > 0$ and $k - s > 0$. Then the i^{th} row of $\ker M$, $1 \leq i \leq k - s$, ends at time index $n - k + i$, which is when the $(k - s + i)^{th}$ row starts.*

Proof The first part of the statement is trivial. The $k - s + i$ th row of $\ker M$ ends at time index $n - (k - s - i)$, and hence it starts at time index $n - (k - s - i) - (n - k) = s + i = n - k + i$. $\clubsuit$

Under the assumptions of Lemma 5.3.1, we have

Corollary 5.3.1 *The number of states of $\ker G$ at time index i , denoted by $|A_i^G|$, is*

$$|A_i^G| = \begin{cases} 2^i & \text{if } 1 \leq i \leq k - s, \\ 2^{s-i} & \text{if } k - s + i \leq 2s, \\ 2^{n-i} & \text{if } 2s + i \leq n - 1. \end{cases} \quad (5.8)$$

The portion of the trellis $\ker G$ from time index $k - s$ to time index $2s + 1$ is called the center of $\ker G$ and denoted by $c(\ker G)$. The corresponding interval, $[k - s, 2s]$, is denoted by $c(\ker C)$.

Consider the portion of $c(\ker G)$ bounded by time indices $n - k$ and $n - s$. This is called the effective center of $\ker G$ and denoted by $ec(\ker G)$. This terminology is used because $ec(\ker G)$ is connected iff $c(\ker G)$ is connected. The interval $[n - k, n - s] \equiv [s, k]$ is denoted by $ec(\ker C)$ and it is not difficult to determine that $ec(\ker C) \subseteq c(\ker C)$.

2

OF/DE

2

PM-1 3½"x4" PHOTOGRAPHIC MICROCOPY TARGET
NBS 1010a ANSI/ISO #2 EQUIVALENT

PRECISIONSM RESOLUTION TARGETS

Figure 5.1: (a) $\ker G$, the minimal trellis diagram of code $\ker C'$ with generator matrix $\ker M$ given by (5.9), (b) $cc(\ker G)$, (c) $c(\ker G)$.

Example 5.3.1 Let C be the (15,9) cyclic code with generator matrix M and leading row

$$g = 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0$$

The state complexity of this code is 6 and $\ker C'$ has TOGM

$$\ker M = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & & & \\ & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & & \\ & & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & & & \\ & & & & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & & \\ & & & & & 1 & 1 & 0 & 0 & 1 & 0 & 1 & & \\ & & & & & & 1 & 1 & 0 & 0 & 1 & 0 & 1 & \end{bmatrix} \quad (5.9)$$

$\ker G$, $c(\ker G)$, and $cc(\ker G)$ are shown in Fig. 5.1. This shows that $cc(\ker C') = [6, 9]$ and $c(\ker C') = [3, 12]$.

Corollary 5.3.2 *Let C_1 be an (n, k_1) binary code that is a sub-code of the (n, k_2) binary code C_2 ($k_1 < k_2$) and let $k_i - s_i > 0$ and $2s_i - k_i > 0$, $i = 1, 2$. Then*

$$ec(ker C_1) \subset ec(ker C_2) \subset c(ker C_2) \subset c(ker C_1). \quad (5.10)$$

Proof $k_1 < k_2$ implies that $s_1 = n - k_1 > n - k_2 = s_2$. Hence $k_1 - s_1 < k_2 - s_2$, and therefore $[k_2 - s_2, 2s_2] \subset [k_1 - s_1, 2s_1]$. It is trivial to show that $[s_1, k_1] \subset [s_2, k_2]$. ♣

Let $n \geq 2$, and denote by $\mathcal{C}_n^-$ the set of cyclic form codes of length n such that $2s - k \leq 0$ where k and s are the dimension and state complexity of the code, respectively. The condition $2s - k \leq 0$ implies that $\frac{2}{3}n \leq k \leq n$ and therefore, there must exist a code C_1^- in $\mathcal{C}_n^-$ with minimum dimension $k_1^- \geq \frac{2}{3}n$ and minimal trellis diagram G_1^- . The center of G_1^- , denoted by $c(G_1^-)$, is defined to be the subgraph of G_1^- bounded by and including time indices $s_1^- = n - k_1^-$ and k_1^- . $c(G_1^-)$ is obviously a connected graph. All the elements of $\mathcal{C}_n^-$ of the same dimension will be considered identical since all have the same graphical structure. C_i^- denotes the element of $\mathcal{C}_n^-$ of dimension $k_i^- = k_1^- + i - 1$, if such a code exists in $\mathcal{C}_n^-$. It is easy to see that $s_i^- = s_1^- - i + 1$, where s_1^- is the state complexity of C_1^- . The effective center of the minimal trellis diagram of C_i^- , denoted $ec(G_i^-)$, is defined to be the subgraph of G_i^- bounded by, and including, time indices s_i^- and k_i^- . Using this notation

$$\begin{aligned} ec(C_i^-) &= [s_i^-, k_i^-], \\ c(C_i^-) &= [s_i^-, k_i^-] = [s_1^- - (i - 1), k_1^- + (i - 1)]. \end{aligned}$$

Lemma 5.3.2 *$ec(G_i^-)$ is a connected graph.*

Proof The statement is trivial for $i = 1$. Let $i \geq 2$. Consider the $(n - 2i + 2, k_1^- - 2i + 2)$ cyclic form code C_0 with generator matrix M_0 obtained from M_1^- , the TOGM of C_1^- , by deleting the first and last $i - 1$ rows and columns. It has state complexity s_0 equal to s_1^- , and center

$$c(C_0) = [s_0, k_1^- - 2i + 2] = [s_1^- - i + 1, k_1^- - i + 1]. \quad (5.11)$$

$c(G_0)$ is a connected graph since

$$2s_0 - (k_1^- - 2i + 2) = 2(s_1^- - i + 1) - (k_1^- + i - 1) + 2i - 2 = 2s_1^- - k_1^- - i + 1 \leq 2s_1^- - k_1^- - 1 < 0.$$

From (5.11) and the fact that time index t of G_0 corresponds to time index $t + i - 1$ of G_1^- , it follows that $c(G_0)$ is a subgraph of $cc(G_1^-)$, and hence $cc(G_1^-)$ is connected. ♣

Let $\mathcal{C}_n^+$ be the set of all cyclic form codes of length n such that $2s > k > s$, where all codes of the same dimension are considered identical.

Lemma 5.3.3 *Suppose $C \in \mathcal{C}_n^+$ and has maximum possible dimension k . Then*

$$cc(\ker C) \subset cc(C_1^-) \subset c(\ker C); \quad (5.12)$$

so that

$$[n - k, k] \subset [n - k_1^-, k_1^-] \subset [k - s, 2s].$$

Proof If $k = k_1^- + i$, then $s = s_1^- - i$ and

$$2s - k = 2(s_1^- - i) - k_1^- - i = 2s_1^- - k_1^- = 2s_1^- k_1^- - 3i < 0,$$

which is a contradiction. Therefore $k < k_1^-$. On the other hand, since $k - s = k_1^- - s_1^- - 2i > 0$, $k = k_1^- - 1$ is a necessary and sufficient condition for C to have maximum dimension k with $k > s$.

$k < k_1^-$ implies that $[n - k, k] \subset [n - k_1^-, k_1^-]$. If $2s < k_1^- = k + 1$, then $2s - k < 1$ which is a contradiction, hence $2s \geq k_1^-$. Relations $n - k_1^- \geq k - s$ and $2s \geq k_1^-$ are equivalent, therefore $[n - k_1^-, k_1^-] \subset [k - s, 2s]$. ♣

We define $\ker \mathcal{C}_n^+ = \{\ker C : C \in \mathcal{C}_n^+\}$, and $\mathcal{C}_n = \mathcal{C}_n^- \cup \ker \mathcal{C}_n^+$. For $C \in \mathcal{C}_n$, the common center of C , $cc(C)$, is defined to be the interval $[s_1^-, k_1^-]$. It follows from (5.10) and (5.12) that

$$cc(C) \subset cc(C) \subset c(C). \quad (5.13)$$

Theorem 5.3.1 *The L -section SRTD of an (Ln, k) QC code C invariant under $\Lambda = T^m$ with canonical components $C_1, C_2, \dots, C_p$ consists of $t_{SR}(C) = \prod_{i=1}^p t_{SR}(C_i)$ identical parallel sub-trellises.*

Proof The L -section SRTD of C and canonical component C_i are denoted by G_{SR} and $G_{SR,i}$, respectively, while their L -section minimal trellis diagrams are denoted by G and G_i . It follows from Theorem 3.2.2 that

$$s = \sum_{i=1}^p s_i, \quad \text{and} \quad G = \prod_{i=1}^p G_i, \quad (5.14)$$

where s and s_i are the state complexities of C and C_i , respectively.

In terms of the L -section trellis diagram, C_i is a cyclic form code. Therefore, G_i , $1 \leq i \leq p$, attains its maximum state complexity in the center of the graph. This along with (5.14) results in the regular graph $\prod_{i=1}^p G_{SR,i}$ having the same state complexity as G_{SR} . It then follows that

$$t_{SR}(C) \geq \prod_{i=1}^p t_{SR}(C_i).$$

Suppose that $C_1, C_2, \dots, C_q$, $q \leq p$, are the canonical components of C with $k_i > s_i$. The SRTD of C_j with $k_j = s_j$ consists of 2^{k_j} parallel paths connecting the initial and final vertices. For i , $1 \leq i \leq q$, define

$$C'_i = \begin{cases} C_i & \text{if } C_i \in \mathcal{C}_L^-, \\ \ker C_i & \text{if } C_i \in \mathcal{C}_L^+; \end{cases} \quad \text{and} \quad C'' = \bigoplus_{i=1}^q C'_i.$$

Denoting the L -section minimal trellis diagram of C'_i by G'_i , where G'_i is either G_i or $\ker G_i$, we define $G'' = \prod_{i=1}^q G'_i$. G'' is in fact the L -section minimal trellis diagram of C'' and is a symmetric graph with a nondecreasing number of states moving towards the center. The center of G'' , $c(G'')$, contains $cc(G'') = \prod_{i=1}^q cc(G'_i)$. $cc(G'')$ is connected since it is the product of connected graphs. Hence, the SRTD of C'' has precisely one component resulting in

$$t_{SR}(C) \leq \prod_{i=1}^p t_{SR}(C_i). \quad \clubsuit$$

Corollary 5.3.3 *From Theorem 5.3.1 it is apparent that*

$$G_{SR} = \prod_{i=1}^p G_{SR,i}. \quad (5.15)$$

Figure 5.2: 4-section SRTD of the QC code given by (5.17), which is invariant under T^2 .

Corollary 5.3.4 *The L -section SRTD of an (Lm, k) QC code C invariant under $\Lambda = T^m$, consists of $2\sum_{i=1}^{p_1} a_i$ structurally identical parallel sub-trellises, with*

$$a_i = \begin{cases} L - L_i + 1 & \text{if } L_i \geq \left\lfloor \frac{L+1}{2} \right\rfloor, \\ \max\{0, 3(L_i - 1) - L\} & \text{if } L_i < \left\lfloor \frac{L+1}{2} \right\rfloor; \end{cases} \quad (5.16)$$

where p_1 is the number of canonical components of C , and L_i is the effective length of the i -th component, $1 \leq i \leq p_1$.

Example 5.3.2 Consider the $(8,5)$ QC code C invariant under T^2 with generator matrix

$$M = \begin{bmatrix} 11 & 11 & 00 & 00 \\ 00 & 11 & 11 & 00 \\ 00 & 00 & 11 & 11 \\ 10 & 00 & 10 & 00 \\ 00 & 10 & 00 & 10 \end{bmatrix}. \quad (5.17)$$

For this code we have $p_1 = 2$, $m = 4$, $m_1 = 2$, $m_2 = 3$. Therefore $a_1 = 0$ and $a_2 = 2$, implying that the SRTD of C consists of 4 identical parallel sub-trellises, as shown in Fig. 5.2. Note that the 4-section minimal trellis diagram of this code has no parallel sub-trellises.

Figure 5.3: Minimal 4-section sub-trellis diagram of $\mathcal{R}(1, m)$.

5.4 Applications

5.4.1 Reed-Muller Codes

As an application of the preceding theory, some of the results of Chapter 2 are derived here using the QC structure of Reed-Muller codes. It was shown in Chapter 3 that Reed-Muller codes are QC codes invariant under $\Lambda = T^l$, where l is $1/4$ of the block length.

Theorem 5.4.1 *Let G be the minimal 4-section trellis diagram of the Reed-Muller code $\mathcal{R}(r, m)$. Then*

1. *G consists of*

$$2^{\binom{m-2}{r-1}}$$

structurally identical parallel sub-trellises.

2. *Any two adjacent vertices of G are connected by*

$$\sum_{i=0}^{r-2} \binom{m-2}{i}$$

edges.

3. *Considering the set of edges connecting two adjacent vertices of G as one edge, each sub-trellis of G is the product of $\binom{m-2}{r-1}$ copies of the graph shown in Fig. 5.3.*

Proof Consider the following generator matrix of $\mathcal{R}(r, m)$

$$G_{m,r} = \begin{bmatrix} G_{m-2}^{r-2} & G_{m-2}^{r-2} & G_{m-2}^{r-2} & G_{m-2}^{r-2} \\ \square & G_{m-2}^{r-1} & \square & G_{m-2}^{r-1} \\ \square & \square & G_{m-2}^{r-1} & G_{m-2}^{r-1} \\ \square & \square & \square & G_{m-2}^{r-2} \end{bmatrix}. \quad (5.18)$$

From (5.18), p_1 , p_2 , and p_3 can easily be determined:

$$\begin{aligned} p_1 &= \sum_{i=0}^r \binom{m-2}{i}, \\ p_2 &= \sum_{i=0}^{r-1} \binom{m-2}{i} + p_1, \\ p_3 &= \sum_{i=0}^{r-1} \binom{m-2}{i} + p_2. \end{aligned} \quad (5.19)$$

It follows from Theorem 5.2.2 that the number of canonical components of $\mathcal{R}(r, m)$ of dimension i , $1 \leq i \leq 4$, is given by

$$\begin{aligned} x_1 &= 2p_1 - (p_0 + p_2) = \binom{m-2}{r}, \\ x_2 &= 2p_2 - (p_1 + p_3) = 0, \\ x_3 &= 2p_3 - (p_2 + p_4) = \binom{m-2}{r-1}, \\ x_4 &= 2p_4 - (p_3 + p_5) = \sum_{i=0}^{r-2} \binom{m-2}{i}. \end{aligned} \quad (5.20)$$

The statements given in Theorem 5.4.1 follow from the values of x_1 , x_4 and x_2 , respectively. ♣

5.4.2 Golay Code

The matrices M and M' , given by (3.8) and (3.9), represent the $(24, 12, 8)$ extended binary Golay code $\mathcal{G}_{24}$ as QC code of indices 2 and 8, respectively.

To find the 3-section trellis diagram of this code, consider the following generator matrix

$$M = \begin{bmatrix} 1101111 & 00110000 & 00000000 \\ 00110011 & 11001100 & 00000000 \\ 00001100 & 11110011 & 00000000 \\ 00000011 & 00111100 & 11000000 \\ 00000000 & 11001111 & 00110000 \\ 00000000 & 00110011 & 11001100 \\ 00000000 & 00001100 & 11110011 \\ 01000110 & 10101110 & 00000000 \\ 00010001 & 10101011 & 10000000 \\ 00000100 & 01101010 & 11100000 \\ 00000001 & 00011010 & 10111000 \\ 00000000 & 01000110 & 10101110 \\ 01000110 & 10101110 & 00000000 \\ 00010001 & 10101011 & 10000000 \\ 00000100 & 01101010 & 11100000 \\ 00000001 & 00011010 & 10111000 \\ 00000000 & 01000110 & 10101110 \end{bmatrix} = \begin{bmatrix} 11001111 & 00110000 & 00000000 \\ 00110011 & 11001100 & 00000000 \\ 00001100 & 11110011 & 00000000 \\ 00000000 & 11001111 & 00110000 \\ 00000000 & 00110011 & 11001100 \\ 00000000 & 00001100 & 11110011 \\ 01000110 & 10101110 & 00000000 \\ 00000000 & 01000110 & 10101110 \\ 00000001 & 00111100 & 11000000 \\ 00010001 & 10101011 & 10000000 \\ 00000100 & 01101010 & 11100000 \\ 00000001 & 00011010 & 10111000 \end{bmatrix}. \quad (5.21)$$

The last four rows of the right matrix given by (5.21) are active at time indices 1 and 2, while among the first eight rows, four rows are active just in time index 1 and 4, and remaining are active in time index 2. Hence the 3-section minimal trellis diagram of $\mathcal{G}_{24}$ consists of 16 identical parallel sub-trellises, each a copy of the minimal 3-section trellis diagram of the $(24, 8, 8)$ sub-code with generator matrix formed by the first eight rows of the right matrix in (5.21). This trellis is shown in Fig. 5.4(a). Note that in terms of the 3-section trellis, the minimal trellis diagram and smallest regular trellis diagram of $\mathcal{G}_{24}$ are identical.

The 4-section smallest regular trellis diagram of $\mathcal{G}_{24}$ can be found from the following generator matrix

$$\begin{bmatrix} 110011 & 110011 & 000000 & 000000 \\ 001100 & 111100 & 110000 & 000000 \\ 000011 & 001111 & 001100 & 000000 \\ 000000 & 110011 & 110011 & 000000 \\ 000000 & 001100 & 111100 & 110000 \\ 000000 & 000011 & 001111 & 001100 \\ 000000 & 000000 & 110011 & 110011 \\ 010001 & 101010 & 111000 & 000000 \\ 000100 & 011010 & 101110 & 000000 \\ 000001 & 000110 & 101011 & 100000 \\ 000000 & 010001 & 101010 & 111000 \\ 000000 & 000100 & 011010 & 101110 \end{bmatrix} = \begin{bmatrix} 110011 & 110011 & 000000 & 000000 \\ 000000 & 110011 & 110011 & 000000 \\ 000000 & 000000 & 110011 & 110011 \\ 001100 & 111100 & 110000 & 000000 \\ 000000 & 001100 & 111100 & 110000 \\ 000011 & 001111 & 001100 & 000000 \\ 000000 & 000011 & 001111 & 001100 \\ 010001 & 101010 & 111000 & 000000 \\ 000000 & 010001 & 101010 & 111000 \\ 000100 & 011010 & 101110 & 000000 \\ 000000 & 000100 & 011010 & 101110 \\ 000001 & 000110 & 101011 & 100000 \end{bmatrix} = \begin{bmatrix} M_1 \\ M_2 \\ M_3 \\ M_4 \\ M_5 \\ M_6 \end{bmatrix}. \quad (5.22)$$

The SRTD corresponding to M_1 is shown in Fig. 5.4(b). Since the state complexity

Figure 5.4: (a), resp. (b), One of the 16, resp. 2^9 , identical parallel sub-trellises of the 3-section, resp. 4-section, SRTD of the (24, 12, 8) Golay code with generator matrix given by (5.21), resp. (5.22).

of the cyclic form sub-code C_i , $2 \leq i \leq 6$, is equal to its dimension, the 4 section SRTD of $\mathcal{G}_{24}$ consists of 2^9 identical parallel sub-trellises, each a copy of Fig. 5.4(b).

With $\mathcal{G}_{24}$ represented by M' (3.9), this code is no longer invariant under T^2 , and has index 8, with canonical components $C_1, C_2, \dots, C_7$ given by generator matrices $M'_1, M'_2, \dots, M'_7$, respectively. The 3-section minimal trellis diagram of $\mathcal{G}_{24}$ obtained from M' consists of 8 parallel identical sub-trellises each an 8 state regular trellis in which any two adjacent vertices are joined by two edges (See Fig. 5.5). Forney [5] has given the same 3-section 2^6 -state trellis diagram for $\mathcal{G}_{24}$ using the cubing construction.

Figure 5.5: One of the eight identical parallel sub-trellises of both the 3-section MTD and SRTD of the (24, 12, 8) Golay code with generator matrices given by (3.9) and (3.33). Note that each edge represents two parallel edges.

5.4.3 Concatenated Codes

The construction of multilevel concatenated codes was introduced by Zinoviev [25]. An m -level concatenated code is constructed from a set of m inner codes of the same length, say n_1 , and a set of m outer codes of the same length, say n_2 . Let $B_i, 1 \leq i \leq m$, be the i th outer code of an m -level concatenated code C , where B_i has length n_2 . It has been shown [12] that the n_2 -section minimal trellis diagram of C is the product of the minimal trellis diagrams of the outer codes.

For instance, consider a two-level concatenated code with outer codes B_1 and B_2 of length 1. If G_1 and G_2 , as shown in Fig. 5.6a and Fig. 5.6b, are the minimal trellis diagrams of B_1 and B_2 , respectively, then $G_1 \times G_2$, as shown in Fig. 5.6c, is the minimal trellis diagram of C . The SRTDs of B_1, B_2 and C , obtained from G_1, G_2 and $G_1 \times G_2$, consist of 1, 4 and 1 parallel sub-trellises, respectively. This means that

$$t_{SR}(C) < \prod_{i=1}^2 t_{SR}(B_i).$$

However, if the outer codes of C are QC codes, or in general, cyclic form codes, then it follows from Corollary 5.3.3 that the SRTD of C is the product of the SRTDs of the outer codes.

Figure 5.6: (a) : G_1 ; (b) : G_2 ; (c) : $G_1 + G_2$.

5.5 Summary

The trellis complexity of a QC code C of length $n = Lm$, invariant under T^m , has been determined via its associated canonical generator matrix. It has been shown that the minimal L -section trellis diagram of C is symmetric with a nondecreasing number of states moving towards the center. The smallest regular trellis diagram of a QC code typically consists of a large number of identical parallel sub trellises, which can be a key factor in the implementation of soft decision decoding using a trellis.

Chapter 6

QUASI-CYCLIC STRUCTURE OF REED-MULLER CODES AND THEIR SMALLEST REGULAR TRELLIS DIAGRAM

6.1 Introduction

The largest quasi-cyclic sub-code of the Reed-Muller code $\mathcal{R}(r, m)$, invariant under the shift $T^{2^{m-l}}$ is determined in this chapter. This code, denoted $QCR(r, m, l)$, is presented through its module decomposition into cyclic submodules. Using the cyclic form structure of $QCR(r, m, l)$, the 2^l -section smallest regular trellis diagram (SRTD) of this code is determined. The 8 -section SRTD is given for the Reed-Muller codes, $\mathcal{R}(r, m)$. The quasi-cyclic sub-codes of $\mathcal{R}(r, m)$ with regular 2^l -section minimal trellis diagrams are presented.

Forney [5] demonstrated that the Reed-Muller codes have a relatively simple 1-section trellis structure. In this chapter, it is shown that the quasi-cyclic (QC) structure of these codes is the reason behind this simple trellis. This motivates our investigation of the QC-structure of Reed-Muller codes and their associated trellis diagrams. The largest sub-code of the r th order Reed-Muller code $\mathcal{R}(r, m)$,

invariant under a shift by 2^{m-l} positions, denoted by $\text{QCR}(r, m, l)$, is determined for $1 \leq l \leq m$. For example, it is shown that

$$\text{QCR}(r, m, 1) \subset \text{QCR}(r, m, 2) \subset \mathcal{R}(r, m) \subset \text{QCR}(r, m, 3)$$

In addition,

$$k_{r,m,l} = \sum_{i=1}^l (2^i - 1) \binom{m-l}{r-i+1} + \sum_{i=0}^{l-1} \binom{m-l}{r-i}$$

where $k_{r,m,l}$ is the dimension of $\text{QCR}(r, m, l)$.

Based on the similarity between cyclic form codes and $\text{QCR}(r, m, l)$, the smallest regular trellis diagram of $\text{QCR}(r, m, l)$ is derived.

The QC-structure of Reed-Muller codes is presented in Section 2. In Section 3, the largest QC-sub-code of $\mathcal{R}(r, m)$ with a regular minimal trellis diagram is found. The structure of the 2^l -section SRFD of $\text{QCR}(r, m, l)$ is determined in the first part of Section 4. The 8-section SRFD of $\mathcal{R}(r, m)$ is given in the second part of Section 4.

6.2 Quasi-Cyclic Structure of Reed-Muller Codes

Reed-Muller codes are closely related to QC codes. It was previously shown that the r th order Reed-Muller code $\mathcal{R}(r, m)$ is invariant under $T^{2^{m-l}}$, a shift by 2^{m-l} positions. Although $\mathcal{R}(r, m)$ is not invariant under $T^{2^{m-1}}$, it is shown in this section that one of its subspaces of dimension $\sum_{i=0}^l \binom{m}{i} - \binom{m-l}{i}$ is invariant under $T^{2^{m-1}}$. In fact, based on Theorem 6.2.1 (which is the main result of this section), $\text{QCR}(r, m, l)$, the largest sub-code of $\mathcal{R}(r, m)$ invariant under $T^{2^{m-l}}$, $1 \leq l \leq m$, is determined. A generator matrix for $\text{QCR}(r, m, l)$ is given which represents a complete decomposition of this code into QC-sub-codes. $\text{QCR}(r, m, 3)$ and $\text{QCR}(r, m, 1)$ are given as examples.

In the remainder of this chapter, the notation $M_1 \sim M_2$ means that matrices M_1 and M_2 have the same row space, while $M_1 \approx M_2$ means that M_1 and M_2 have

the same set of rows.

As was shown in Chapter 2, the following matrix is the trellis oriented generator matrix of the minimal 8-section trellis diagram of $\mathcal{R}(r, m)$

$$G_m^r \equiv \begin{bmatrix} 1 & 1 & 1 & 1 & - & - & - & - \\ - & - & 1 & 1 & 1 & 1 & - & - \\ - & - & - & - & 1 & 1 & 1 & 1 \\ - & 1 & - & 1 & 1 & - & 1 & - \\ 2 & 2 & - & - & - & - & - & - \\ - & 2 & 2 & - & - & - & - & - \\ - & - & 2 & 2 & - & - & - & - \\ - & - & - & 2 & 2 & - & - & - \\ - & - & - & - & 2 & 2 & - & - \\ - & - & - & - & - & 2 & 2 & - \\ - & - & - & - & - & - & 2 & 2 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & - & - & - & - & - & - & - \\ - & 3 & - & - & - & - & - & - \\ - & - & 3 & - & - & - & - & - \\ - & - & - & 3 & - & - & - & - \\ - & - & - & - & 3 & - & - & - \\ - & - & - & - & - & 3 & - & - \\ - & - & - & - & - & - & 3 & - \\ - & - & - & - & - & - & - & 3 \end{bmatrix} \quad (6.1)$$

where 0, 1, 2 and 3 denote B_{m-3}^r , B_{m-3}^{r-1} , B_{m-3}^{r-2} , and G_{m-3}^{r-3} , respectively, and the dashes represent all zero matrices. Note that all matrices in a given row have the same size, and all non-zero matrices in a given row are identical.

It can easily be shown that the four rows in (6.1) containing the term B_{m-3}^{r-1} are not closed under the operator $T^{2^{m-3}}$. For instance, if $b_{m-3}^{r-1} \in B_{m-3}^{r-1}$ and $\square$ is a string of zeros of length 2^{m-3} , then

$$\square b_{m-3}^{r-1} b_{m-3}^{r-1} b_{m-3}^{r-1} b_{m-3}^{r-1} \square \square \square \notin \mathcal{R}(r, m).$$

Hence, $\mathcal{R}(r, m)$ is not invariant under $T^{2^{m-3}}$.

The largest sub-code of $\mathcal{R}(r, m)$ invariant under $T^{2^{m-3}}$ can easily be determined by inspection of the generator matrix (6.1). However, for the general case $T^{2^{m-l}}$, $l \geq 3$, finding the largest invariant sub-code is much more difficult, and requires the following lemmas.

Using (6.1) as a reference, for $l \geq 3$ it is possible to define matrices $M_{0,l}$, $M_{l-1,l}$, and $M_{l,l}$ as follows

$$M_{0,l} := \begin{bmatrix} B_{m-l}^r & B_{m-l}^{r-1} & \cdots & B_{m-l}^{r-l} \end{bmatrix}, \quad (6.2)$$

$$M_{l-1,l} := \begin{bmatrix} B_{m-l}^{r-l+1} & B_{m-l}^{r-l+1} & \square & \square & \dots & \square \\ \square & B_{m-l}^{r-l+1} & B_{m-l}^{r-l+1} & \square & \dots & \square \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \square & \dots & \square & B_{m-l}^{r-l+1} & B_{m-l}^{r-l+1} & \square \\ \square & \dots & \square & \square & B_{m-l}^{r-l+1} & B_{m-l}^{r-l+1} \end{bmatrix}, \quad (6.3)$$

$$M_{l,l} := \begin{bmatrix} G_{m-l}^{r-l} & \square & \square & \dots & \square \\ \square & G_{m-l}^{r-l} & \square & \dots & \square \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \square & \dots & \square & G_{m-l}^{r-l} & \square \\ \square & \dots & \square & \square & G_{m-l}^{r-l} \end{bmatrix}. \quad (6.4)$$

These three matrices have 2^l columns considering B_{m-l}^r , B_{m-l}^{r-l+1} , and G_{m-l}^{r-l} as individual entries. It is clear that $M_{0,l}$, $M_{l-1,l}$, and $M_{l,l}$ generate quasi-cyclic codes invariant under $T^{2^{m-l}}$. Denote these quasi-cyclic codes by $C_{0,l}$, $C_{l-1,l}$, and $C_{l,l}$, respectively. The remainder of the generator matrix G_m^r can be further subdivided into matrices containing terms of the form B_{m-l}^{r-i} for $1 \leq i \leq l-2$. Considering each of these sub-matrices as the generator matrix of a sub-code, we must determine the largest sub-code that is invariant under $T^{2^{m-l}}$. To achieve this, it is more convenient to first work with binary matrices first and find the cyclic sub-matrices. Then, we can substitute B_{m-l}^{r-i} for the 1s and replace the 0s by matrices of all zeros.

Let v_1 be a binary sequence of length 2^μ whose first 4 components are ones and the remaining components are all zero. Let u_1 be a second binary sequence of length 2^μ whose components are all zero except for the second and fourth components which are one. For $1 \leq i \leq 2^{\mu-1}$ define $v_i = T^{2^{i-2}}(v_1)$ and $u_i = T^{2^{i-2}}(u_1)$. $v_{2^{\mu-1}}$ is defined to be the binary sequence of length 2^μ such that only the last 2 components are nonzero.

We define the $(2^\mu - 1) \times 2^\mu$ matrices $M(2^\mu)$ and $M_c(2^\mu)$ as follows:

$$M(2^\mu) = \begin{bmatrix} v_1 \\ u_1 \\ \vdots \\ v_{2^{\mu-1}-1} \\ u_{2^{\mu-1}-1} \\ v_{2^{\mu-1}} \end{bmatrix} \quad M_c(2^\mu) = \begin{bmatrix} w \\ T(w) \\ \vdots \\ T^{2^{\mu-2}}(w) \end{bmatrix} \quad (6.5)$$

where $w = T^2(v_{2^{\mu-1}})$.

Example 6.2.1 For $\mu = 3$ we have

$$M(2^3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad M_c(2^3) = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (6.6)$$

Lemma 6.2.1 *With the foregoing notation, $M(2^\mu)$ is a row reduced generator matrix of a cyclic code, and its equivalent trellis oriented generator matrix is $M_c(2^\mu)$.*

Proof The proof is by induction on μ , and is omitted. ♣

Next, define

$$t_i = \begin{cases} v_i + v_{2^{\mu-2}+i}, & 1 \leq i \leq 2^{\mu-2} - 1 \\ \sum_{j=2^{\mu-2}}^{2^{\mu-1}-1} v_j, & i = 2^{\mu-2} \end{cases} \quad (6.7)$$

and

$$w_i = u_i + u_{2^{\mu-2}+i}, \quad \text{for } 1 \leq i \leq 2^{\mu-2} - 1. \quad (6.8)$$

For convenience, let pM denote the matrix obtained by concatenating p copies of a given matrix M . Now, define the row reduced matrices $M(2^{\mu-1} - 1, 2^{\mu-2} - 1)$

and $2M(2^{\mu-1})$ as

$$M(2^{\mu-1} - 1, 2^{\mu-2} - 1) := \begin{bmatrix} v_1 \\ w_1 \\ \vdots \\ v_{2^{\mu-2}-1} \\ w_{2^{\mu-2}-1} \\ v_{2^{\mu-2}} \\ \vdots \\ v_{2^{\mu-1}-1} \end{bmatrix} \quad 2M(2^{\mu-1}) := \begin{bmatrix} t_1 \\ w_1 \\ \vdots \\ t_{2^{\mu-2}-1} \\ w_{2^{\mu-2}-1} \\ t_{2^{\mu-2}} \end{bmatrix} \quad (6.9)$$

Example 6.2.2 For $\mu = 4$ we have

$$M(7, 3) = \begin{bmatrix} v_1 \\ w_1 \\ v_2 \\ w_2 \\ v_3 \\ w_3 \\ v_4 \\ v_5 \\ v_6 \\ v_7 \end{bmatrix} = \begin{bmatrix} 11110000 & 00000000 \\ 01010000 & 01010000 \\ 00111100 & 00000000 \\ 00010100 & 00010100 \\ 00001111 & 00000000 \\ 00000101 & 00000101 \\ 00000011 & 11000000 \\ 00000000 & 11110000 \\ 00000000 & 00111100 \\ 00000000 & 00001111 \end{bmatrix} \quad (6.10)$$

$$2M(2^3) = \begin{bmatrix} t_1 \\ w_1 \\ t_2 \\ w_2 \\ t_3 \\ w_3 \\ t_4 \end{bmatrix} = \begin{bmatrix} 11110000 & 11110000 \\ 01010000 & 01010000 \\ 00111100 & 00111100 \\ 00010100 & 00010100 \\ 00001111 & 00001111 \\ 00000101 & 00000101 \\ 00000011 & 00000011 \end{bmatrix} \quad 2M_c(2^3) = \begin{bmatrix} 11000000 & 11000000 \\ 01100000 & 01100000 \\ 00110000 & 00110000 \\ 00011000 & 00011000 \\ 00001100 & 00001100 \\ 00000110 & 00000110 \\ 00000011 & 00000011 \end{bmatrix} \quad (6.11)$$

Note that $2M_c(2^3)$ represents a $(16, 7)$ cyclic code. It is because a right shift of the last row of this matrix is equal to the sum of all rows of the matrix. In addition, two right shifts of the last row gives the first row. In general, if M represents a (n, k) cyclic code then pM is the generator matrix of a (pn, k) cyclic code.

Lemma 6.2.2 *With the foregoing notation, let C be a $(2^\mu, 3 \times 2^{\mu-2} - 2)$ linear block code with generator matrix $M(2^{\mu-1} - 1, 2^{\mu-2} - 1)$. Then the largest cyclic sub-code of C has generator matrix $2M_c(2^{\mu-1})$.*

Proof From the structure of $M(2^{\mu-1} - 1, 2^{\mu-2} - 1)$, it can be seen that in the row space of this matrix there is no vector whose first nonzero component is in the $2^{\mu-1}$ -th column. In other words, the binary linear block code C with generator matrix $M(2^{\mu-1} - 1, 2^{\mu-2} - 1)$ has no code word starting at time index $2^{\mu-1}$. This shows that the row space of this matrix, considered as a linear block code, does not contain a cyclic sub-code of dimension $\geq 2^{\mu-1}$.

It is obvious that the row space of $2M(2^{\mu-1})$ is a subspace of the row space of the matrix $M(2^{\mu-1} - 1, 2^{\mu-2} - 1)$. From Lemma 6.2.1, the trellis oriented generator matrix obtained from $2M(2^{\mu-1})$ is $2M_c(2^{\mu-1})$ represents a cyclic code, as mentioned previously. Therefore the row space of $M(2^{\mu-1} - 1, 2^{\mu-2} - 1)$ contains a cyclic code of dimension $2^{\mu-1} - 1$ with generator matrix $2M_c(2^{\mu-1})$. This is the largest cyclic sub-code of C , since C does not contain a cyclic sub-code of dimension $\geq 2^{\mu-1}$. ♣

Now the largest quasi-cyclic sub-code of the Reed-Muller code $\mathcal{R}(r, m)$ can be defined. First, consider the set of matrices $2^{l-i-1}M_c(2^{i+1})$ for $1 \leq i \leq l-2$. Then, for each matrix, replace the 1s by the matrix B_{m-i}^{r-i} , and the 0s by the matrix of all zeros, denoted by $\square$, with the same dimension as B_{m-i}^{r-i} . Denote the resulting matrix by $M_{i,l}$.

Lemma 6.2.3 *The matrix $M_{i,l}$, $1 \leq i \leq l-2$, is a generator matrix for a quasi-cyclic code $C_{i,l}$ of length 2^m and dimension $(2^{i+1} - 1) \times \binom{m-l}{r-i}$, which is invariant under $T^{2^{m-1}}$. Considering also the codes $C_{0,l}$, $C_{l-1,l}$ and $C_{l,l}$ defined earlier, for $0 \leq i \neq j \leq l$*

$$C_{i,l} \cap C_{j,l} = \emptyset. \quad (6.12)$$

Proof The first statement follows from the cyclic structure of $2^{l-i+1}M_c(2^{i-1})$ and the substitution of 1 and 0 with B_{m-i}^{r-i} and $\square$, respectively. For the second part, it

is sufficient to state that

$$\begin{aligned} B_{m-l}^{r-i} \cap B_{m-l}^{r-j} &= \emptyset \quad \text{if } 0 \leq i \neq j \leq l-1, \\ G_{m-l}^{r-l} \cap B_{m-l}^{r-i} &= \emptyset \quad \text{if } 0 \leq i \leq l-1. \quad \clubsuit \end{aligned} \quad (6.13)$$

Theorem 6.2.1 *The quasi-cyclic code*

$$QCR(r, m, l) = \bigoplus_{i=0}^l C_{i,l} \quad (6.14)$$

is the largest sub-code of $\mathcal{R}(r, m)$ invariant under $T^{2^{m-l}}$.

Proof The proof is by induction on l . According to Lemma 6.2.3, $QCR(r, m, l)$ is a QC code of length 2^m , which is invariant under $T^{2^{m-l}}$. Hence we need only show that this code is the largest sub-code of $\mathcal{R}(r, m)$ invariant under $T^{2^{m-l}}$. For $l = 1$ and 2, the statement follows from (2.25) and (2.19), respectively. Suppose it holds for a fixed $l \geq 2$ (induction hypothesis). Now we must show that $QCR(r, m, l+1)$ is the largest sub-code of $QCR(r, m, l)$ invariant under $T^{2^{m-l-1}}$ (note that $QCR(r, m, l+1)$ is a subspace of $QCR(r, m, l)$).

We can rewrite (2.26) in the form

$$B_{m-l}^{r-i} = \begin{bmatrix} B_{m-l-1}^{r-i} & B_{m-l-1}^{r-i} \\ \square & B_{m-l-1}^{r-i-1} \end{bmatrix}. \quad (6.15)$$

Then the matrices $M_{i,l}$ that generate the codes $C_{i,l}$, $0 \leq i \leq l-1$, can be expanded and partitioned into two sub matrices. The first sub-matrix consists of those rows which contain the blocks B_{m-l-1}^{r-i} and $\square$, and the second sub-matrix consists of those rows which contain the blocks B_{m-l-1}^{r-i-1} and $\square$. Applying (2.25) in a similar manner, $M_{l,l}$ can be partitioned into two sub-matrices with the first containing rows with entries B_{m-l-1}^{r-l} and $\square$, and the second consisting of rows with entries G_{m-l-1}^{r-l-1} and $\square$. From these $l+1$ matrices, like terms can be collected to form a new set of $l+2$ matrices, i.e., the rows of $M_{i,l}$ containing B_{m-l-1}^{r-i} are grouped with those rows of $M_{i-1,l}$ containing the same term to form a new matrix. What needs to be shown is that the matrix containing the terms B_{m-l-1}^{r-i} has $M_{i,l+1}$ as a sub-matrix and $M_{i,l+1}$

is the largest sub-matrix invariant under $T^{2^{m-l-1}}$. The matrices $M_{0,l+1}$ and $M_{l+1,l+1}$, containing the terms B_{m-l-1}^r and G_{m-l-1}^{r-l-1} respectively, are left behind in the process of collecting terms. Also, by collecting the rows containing the terms B_{m-l-1}^{r-l} in the expansion of $M_{l-1,l}$ and $M_{l,l}$, it is easy to see that we obtain $M_{l,l+1}$.

Now, consider the binary matrices $2^{l-i-1}M_c(2^{i+1})$ that were used to define $M_{i,l}$, for $1 \leq i \leq l-2$. In the above expansions of $M_{i,l}$ and $M_{i+1,l}$ using (6.15), the new matrix obtained by collecting the rows containing the terms B_{m-l-1}^{r-l-1} has an equivalent form as a binary matrix. Take the binary matrix $2^{l-i-1}M_c(2^{i+1})$ and replace the 1s with [01] and the 0s by [00], then take the matrix $2^{l-i-2}M_c(2^i)$ and replace the 1s by [11] and the 0s by [00]. The direct sum of these two binary matrices is a matrix with 2^{i+1} columns and $3 \times 2^{i+1} - 2$ rows. Since

$$\begin{bmatrix} 2^{l-i-1}M_c(2^{i+1}) \\ 2^{l-i-2}M_c(2^i) \end{bmatrix} = 2^{l-i-1} \begin{bmatrix} M_c(2^{i+1}) \\ 2M_c(2^i) \end{bmatrix},$$

it is not difficult to see that the above substitutions and direct sum yield the matrix $2^{l-i-1}M(2^{i+1} - 1, 2^i - 1)$. It follows from Lemma 6.2.2 that $2^{l-i-1}M(2^{i+1} - 1, 2^i - 1)$ includes a unique largest cyclic sub-code with generator matrix $2^{l-i-1}M_c(2^i)$. If the 1s and 0s in this latter matrix are replaced with B_{m-l-1}^{r-l} and $\square$, respectively, we obtain $M_{i,l+1}$, the generator matrix for $C_{i,l+1}$. ♣

Remark The dimension of $QCR(r, m, l)$ is

$$k_{r,m,l} = \sum_{i=0}^{l-1} (2^{i+1} - 1) \binom{m-l}{r-i} + 2^l \sum_{i=0}^{r-l} \binom{m-l}{i}. \quad (6.16)$$

In addition, the generator matrix

$$G_{r,m,l} = \begin{bmatrix} M_{0,l} \\ M_{1,l} \\ \vdots \\ M_{l-1,l} \\ M_{l,l} \end{bmatrix}, \quad (6.17)$$

for the QC code $QCR(r, m, l)$ is a trellis oriented generator matrix.

Example 6.2.3 For $l = 3$, $G_{r,m,3}$, the generator matrix of $QCR(r, m, 3)$, is given by

$$G_{r,m,3} \equiv \begin{bmatrix} 1 & 1 & - & - & 1 & 1 & - & - \\ - & 1 & 1 & - & - & 1 & 1 & - \\ - & - & 1 & 1 & - & - & 1 & 1 \\ 2 & 2 & - & - & - & - & - & - \\ - & 2 & 2 & - & - & - & - & - \\ - & - & 2 & 2 & - & - & - & - \\ - & - & - & 2 & 2 & - & - & - \\ - & - & - & - & 2 & 2 & - & - \\ - & - & - & - & - & 2 & 2 & - \\ - & - & - & - & - & - & 2 & 2 \end{bmatrix} \oplus \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & - & - & - & - & - & - & - \\ - & 3 & - & - & - & - & - & - \\ - & - & 3 & - & - & - & - & - \\ - & - & - & 3 & - & - & - & - \\ - & - & - & - & 3 & - & - & - \\ - & - & - & - & - & 3 & - & - \\ - & - & - & - & - & - & 3 & - \\ - & - & - & - & - & - & - & 3 \end{bmatrix} \quad (6.18)$$

where 0, 1, 2 and 3 stand for B_{m-3}^r , B_{m-3}^{r-1} , B_{m-3}^{r-2} and G_{m-3}^{r-3} , respectively, and a dash represents an all zeros matrix.

For $l = 4$, the generator matrix of $QCR(r, m, 4)$ is given by

$$G_{r,m,4} \equiv \begin{bmatrix} 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 11 & -- & 11 & -- & 11 & -- & 11 & -- \\ -1 & 1- & -1 & 1- & -1 & 1- & -1 & 1- \\ -- & 11 & -- & 11 & -- & 11 & -- & 11 \\ 22 & -- & -- & -- & 22 & -- & -- & -- \\ -2 & 2- & -- & -- & -2 & 2- & -- & -- \\ -- & 22 & -- & -- & -- & 22 & -- & -- \\ -- & -2 & 2- & -- & -- & -2 & 2- & -- \\ -- & -- & 22 & -- & -- & -- & 22 & -- \\ -- & -- & -2 & 2- & -- & -- & -2 & 2- \\ -- & -- & -- & 22 & -- & -- & -- & 22 \end{bmatrix} \oplus \begin{bmatrix} 33 & -- & -- & -- & -- & -- & -- & -- \\ -3 & 3- & -- & -- & -- & -- & -- & -- \\ -- & 33 & -- & -- & -- & -- & - & -- \\ -- & -3 & 3- & -- & -- & -- & -- & -- \\ -- & -- & 33 & -- & -- & -- & -- & -- \\ -- & -- & -3 & 3- & -- & -- & -- & -- \\ -- & -- & -- & 33 & -- & -- & -- & -- \\ -- & -- & -- & -3 & 3- & -- & -- & -- \\ -- & -- & -- & -- & 33 & -- & -- & -- \\ -- & -- & -- & -3 & 3- & -- & -- & -- \\ -- & -- & -- & -- & -- & 33 & -- & -- \\ -- & -- & -- & -- & -- & -3 & 3- & -- \\ -- & -- & -- & -- & -- & -- & 33 & -- \\ -- & -- & -- & -- & -- & -- & -3 & 3- \\ -- & -- & -- & -- & -- & -- & -- & 33 \end{bmatrix} \oplus$$

$$\begin{bmatrix}
 4- & -- & -- & -- & -- & -- & -- & -- \\
 -4 & -- & -- & -- & -- & -- & -- & -- \\
 -- & 4- & -- & -- & -- & -- & -- & -- \\
 -- & -4 & -- & -- & -- & -- & -- & -- \\
 -- & -- & 4- & -- & -- & -- & -- & -- \\
 -- & -- & -4 & -- & -- & -- & -- & -- \\
 -- & -- & -- & 4- & -- & -- & -- & -- \\
 -- & -- & -- & -4 & -- & -- & -- & -- \\
 -- & -- & -- & -- & 4- & -- & -- & -- \\
 -- & -- & -- & -- & -4 & -- & -- & -- \\
 -- & -- & -- & -- & -- & 4- & -- & -- \\
 -- & -- & -- & -- & -- & -4 & -- & -- \\
 -- & -- & -- & -- & -- & -- & 4- & -- \\
 -- & -- & -- & -- & -- & -- & -4 & -- \\
 -- & -- & -- & -- & -- & -- & -- & 4- \\
 -- & -- & -- & -- & -- & -- & -- & -4
 \end{bmatrix} \quad (6.19)$$

where for $0 \leq i \leq 3$ the number i represents the matrix B_{m-4}^{r-i} , 4 represents G_{m-4}^{r-4} , and a dash represents an all zeros matrix.

6.3 Quasi-Cyclic Codes with Regular Minimal Trellis Diagrams Derived from Reed-Muller Codes

In this section, QC'-sub-codes of $\mathcal{R}(r, m)$ invariant under $T^{2^{m-l}}$ are introduced which have a 2^l -section minimal trellis diagram with the same number of states at all time indices, $1 \leq i \leq 2^l - 1$. The advantage of this trellis structure is that all circuits in a VLSI implementation are equally active at all time indices, which typically results in more efficient decoding.

The largest quasi-cyclic sub-code of $\mathcal{R}(r, m)$ invariant under $T^{2^{m-l}}$ with a regular 2^l -section minimal trellis diagram is denoted by $\mathcal{RQCR}(r, m, l)$. From the trellis oriented generator matrix of $\mathcal{QCR}(r, m, l)$, the trellis oriented generator matrix of

$\mathcal{RQCR}(r, m, l)$ is given by

$$G_{r,m,l}^R = \begin{bmatrix} M_{0,l} \\ R_{1,l} \\ \vdots \\ R_{l-2,l} \\ M_{l-1,l} \\ M_{l,l} \end{bmatrix} \quad (6.20)$$

where $R_{i,l}$, $1 \leq i \leq l-2$, denotes the $\binom{m-l}{r-i} \times 2^m$ matrix obtained by concatenating 2^l copies of B_{m-i}^{r-i} in one row, and $M_{0,l}$, $M_{l-1,l}$, and $M_{l,l}$ are again given by (6.2), (6.3), and (6.4), respectively.

Example 6.3.1 The trellis oriented generator matrix of $\mathcal{RQCR}(r, m, 4)$, denoted by $G_{r,m,4}^R$, can be obtained from (6.19) and is given below

$$\begin{bmatrix} 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 11 & 11 & 11 & 11 & 11 & 11 & 11 & 11 \\ 22 & 22 & 22 & 22 & 22 & 22 & 22 & 22 \\ 33 & -- & -- & -- & -- & -- & -- & -- \\ -3 & 3- & -- & -- & -- & -- & -- & -- \\ -- & 33 & -- & -- & -- & -- & -- & -- \\ -- & -3 & 3- & -- & -- & -- & -- & -- \\ -- & -- & 33 & -- & -- & -- & -- & -- \\ -- & -- & -3 & 3- & -- & -- & -- & -- \\ -- & -- & -- & 33 & -- & -- & -- & -- \\ -- & -- & -- & -3 & 3- & -- & -- & -- \\ -- & -- & -- & -- & 33 & -- & -- & -- \\ -- & -- & -- & -- & -3 & 3- & -- & -- \\ -- & -- & -- & -- & -- & 33 & -- & -- \\ -- & -- & -- & -- & -- & -3 & 3- & -- \\ -- & -- & -- & -- & -- & -- & 33 & -- \end{bmatrix} \oplus \begin{bmatrix} 4- & -- & -- & -- & -- & -- & -- & -- \\ -4 & -- & -- & -- & -- & -- & -- & -- \\ -- & 4- & -- & -- & -- & -- & -- & -- \\ -- & -4 & -- & -- & -- & -- & -- & -- \\ -- & -- & 4- & -- & -- & -- & -- & -- \\ -- & -- & -4 & -- & -- & -- & -- & -- \\ -- & -- & -- & 4- & -- & -- & -- & -- \\ -- & -- & -- & -4 & -- & -- & -- & -- \\ -- & -- & -- & -- & 4- & -- & -- & -- \\ -- & -- & -- & -- & -4 & -- & -- & -- \\ -- & -- & -- & -- & -- & 4 & -- & -- \\ -- & -- & -- & -- & -- & -4 & -- & -- \\ -- & -- & -- & -- & -- & -- & 4 & -- \\ -- & -- & -- & -- & -- & -- & -- & 4 \\ -- & -- & -- & -- & -- & -- & -- & -4 \end{bmatrix} \quad (6.21)$$

The complexity parameters of $\mathcal{RQCR}(r, m, 3)$ and $\mathcal{RQCR}(r, m, 4)$ are given in Tables 6.1 and 6.2, respectively. These parameters are given in Table 6.3 for $\mathcal{RQCR}(r, m, 3)$ with $r = 3$ and $m = 6$.

Table 6.1: Complexity Parameters of the 8-Section Minimal Trellis Diagram of $\mathcal{RQCR}(r, m, 3)$.

i	$\epsilon(i)$	$s(i)$	s_i	$\log_2(t_i)$
1	$\sum_{j=0}^{r-3} \binom{m-3}{j}$	$\sum_{j=0}^r \binom{m-3}{j}$	$\sum_{j=0}^2 \binom{m-3}{r-j}$	0
2	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^2 \binom{m-3}{r-j}$	$\sum_{j=0}^1 \binom{m-3}{r-j}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
7	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^{r-2} \binom{m-3}{j}$	$\sum_{j=0}^2 \binom{m-3}{r-j}$	$\sum_{j=0}^1 \binom{m-3}{r-j}$
8	$\sum_{j=0}^r \binom{m-3}{j}$	$\sum_{j=0}^{r-3} \binom{m-3}{j}$	0	0

Table 6.2: Complexity Parameters of the 16-Section Minimal Trellis Diagram of $\mathcal{RQCR}(r, m, 4)$.

i	$\epsilon(i)$	$s(i)$	s_i	$\log_2(t_i)$
1	$\sum_{j=0}^{r-4} \binom{m-4}{j}$	$\sum_{j=0}^r \binom{m-4}{j}$	$\sum_{j=0}^3 \binom{m-4}{r-j}$	0
2	$\sum_{j=0}^{r-3} \binom{m-4}{j}$	$\sum_{j=0}^{r-3} \binom{m-4}{j}$	$\sum_{j=0}^3 \binom{m-4}{r-j}$	$\sum_{j=0}^2 \binom{m-4}{r-j}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
15	$\sum_{j=0}^{r-3} \binom{m-4}{j}$	$\sum_{j=0}^{r-3} \binom{m-4}{j}$	$\sum_{j=0}^3 \binom{m-4}{r-j}$	$\sum_{j=0}^2 \binom{m-4}{r-j}$
16	$\sum_{j=0}^r \binom{m-4}{j}$	$\sum_{j=0}^{r-4} \binom{m-4}{j}$	0	0

Table 6.3: Complexity Parameters of the 8-Section Minimal Trellis Diagram of $\mathcal{RQCR}(3, 6, 3)$.

i	1	2	$\dots$	7	8
$\epsilon(i)$	1	4	$\dots$	4	8
$s(i)$	8	4	$\dots$	4	1
s_i	7	7	$\dots$	7	0
$\log_2(t_i)$	0	4	$\dots$	4	0

Let $k_{r,m}$ and $k_{r,m,l}^R$ denote the dimensions of $\mathcal{R}(r,m)$ and $\mathcal{RQCR}(r,m,l)$, respectively. Then for $l = 3$ and 4 the dimensions are

$$\begin{aligned} k_{r,m} &= k_{r,m,3}^R + 3 \binom{m-3}{r-1}, \\ \text{and} \\ k_{r,m} &= k_{r,m,4}^R + 4 \binom{m-4}{r-1} + 10 \binom{m-4}{r-2}, \end{aligned} \tag{6.22}$$

respectively. Define

$$\begin{aligned} 2^{S_{r,m}} &= \max\{|V_i| : 0 \leq i \leq 2^l\} \\ \text{and} \\ 2^{S_{r,m,l}^R} &= \max\{|U_i| : 0 \leq i \leq 2^l\} \end{aligned}$$

where V_i and U_i are the set of vertices of the 2^l -section minimal trellis diagram of $\mathcal{R}(r,m)$ and $\mathcal{RQCR}(r,m,l)$ at time index i , respectively. $S_{r,m}$ and $S_{r,m,l}^R$ are defined to be the state complexities of these two codes. Comparing $S_{r,m,3}^R$ and $S_{r,m,4}^R$ (obtained from matrices $G_{r,m,3}^R$ and $G_{r,m,4}^R$, respectively) with $S_{r,m}$ (obtained from G_m^r , given by (6.1)) we obtain

$$\begin{aligned} S_{r,m} &= S_{r,m,3}^R + 3 \binom{m-3}{r-1}, \\ S_{r,m} &= S_{r,m,4}^R + 3 \binom{m-4}{r-1} + 3 \binom{m-4}{r-2}. \end{aligned} \tag{6.23}$$

This together with (6.22) shows that $\mathcal{R}(r,m)$ and $\mathcal{RQCR}(r,m,3)$ are comparable in terms of dimension. However, considering also the regularity of the codes, $\mathcal{RQCR}(r,m,3)$ may be preferred for trellis decoding. The minimum Hamming distance of these two codes is identical.

6.4 The Smallest Regular Trellis Diagram of Reed-Muller Codes

The 2^l -section SRTD of $\mathcal{QCR}(r,m,l)$ and the 8-section SRTD of $\mathcal{R}(r,m)$ are given in the first and second parts of this section, respectively. The QC-structure of

$QCR(r, m, l)$ produces a simple trellis structure. All internal sections (between time indices 1 and $2^l - 1$) of the parallel sub-trellises in the SRFD of $QCR(r, m, l)$ are identical. This property is illustrated in Fig. 6.1. However, this is not the case for the 8 section SRFD of $R(r, m)$ as seen in Fig. 6.4. The results of this section suggest that in terms of the 2^l section trellis diagram and VLSI implementation, $QCR(r, m, l)$ may be preferable to $R(r, m)$.

6.4.1 The Smallest Regular Trellis Diagram of $QCR(r, m, l)$

Let G_{l-1} denote the 2^l -section minimal trellis diagram of the quasi-cyclic code $C_{l-1,l}$ invariant under $T^{2^{m-l}}$. $T_l(G_{l-1})$ is a complete bipartite graph with $2^l \binom{m-l}{r-l+1}$ vertices on each side for $2 \leq l \leq 2^l - 1$. Denote the 2^l -section, smallest regular trellis diagram of $QCR(r, m, l)$ by $T_{r,m,l}$.

Theorem 6.4.1 $T_{r,m,l}$ consists of

$$2^{\sum_{i=0}^{l-2} (2^{i+1}-1) \binom{m-l}{r-l+1}}$$

identical parallel sub-trellises, each of which is a copy of G_{l-1} .

Proof According to Theorem 6.2.1, $QCR(r, m, l)$ is the direct sum of $C_{i,l}$, $0 \leq i \leq l$, and from (6.17), the 2^l -section minimal trellis diagram of this code is the product of the 2^l section minimal trellis diagrams of its components. All rows of $M_{i,l}$, $0 \leq i \leq l-2$, are active at time index 2^{l-1} , so for these components the state complexity is equal to the dimension. Hence, in the smallest regular trellis diagram of the sub-code $\bigoplus_{i=0}^{l-2} C_{i,l}$, the distinct paths representing any two code words have no connection except at the initial and final vertices, meaning that this graph consists of

$$2^{\sum_{i=0}^{l-2} (2^{i+1}-1) \binom{m-l}{r-l+1}}$$

parallel paths connecting the initial and final vertices. The minimal trellis for $C_{l,l}$ consists of one state, and its product with the trellis of the sub-code $\bigoplus_{i=0}^{l-2} C_{i,l}$ does

Figure 6.1: One of the 8 parallel sub trellises of $T_{3,5,3}$.

not alter the state complexity although it does increase the number of edges connecting two vertices. By Corollary 4.2.1, the 2^l -section minimal trellis diagram and 2^l -section smallest regular trellis diagram of $C_{l-1,l}$ are identical and have one component. ♣

Note that in $T_{r,m,l}$, the number of edges connecting two adjacent vertices is $2^{k_{r-l,m-l}}$, which is the number of code words in $\mathcal{R}(r-l, m-l)$.

Example 6.4.1 For the (32,25,4) quasi-cyclic code $\text{QCR}(3,5,3)$, the smallest regular trellis diagram, $T_{3,5,3}$, consists of 8 structurally identical parallel sub trellises, one of which is shown in Fig. 6.1.

6.4.2 The 8-section Smallest Regular Trellis Diagram of $\mathcal{R}(r, m)$

The 8-section minimal trellis diagram of $\mathcal{R}(r, m)$ is determined by its trellis oriented generator matrix G_m^r , given by (6.1). G_m^r consists of four parts, three of which are cyclic codes (in terms of the 8-section minimal trellis diagram). Therefore, determining the 8-section SRTD of $\mathcal{R}(r, m)$ is largely based on the 8-section SRTD of the code with trellis oriented generator matrix

$$M = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix} \quad (6.24)$$

Figure 6.2: The minimal trellis diagram for the trellis oriented generator matrix given by (6.24).

Figure 6.3: The smallest regular trellis diagram for the trellis oriented generator matrix given by (6.24).

Note that (6.24) is a generator matrix for the $(8,4,4)$ binary code, which is also a Reed-Muller code. The state complexity of the corresponding code is 3, and the minimal trellis diagram and smallest regular trellis diagram are given in Figs. 6.2 and 6.3, respectively. Note that Fig. 6.3 consists of four parallel sub-trellises, while there are no parallel sub-trellises in the minimal trellis diagram.

It follows that the 8-section SRTD of the sub-code of $\mathcal{R}(r, m)$ with trellis oriented

generator matrix

$$M' = \begin{bmatrix} B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & \square & \square & \square & \square \\ \square & \square & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & \square & \square \\ \square & \square & \square & \square & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} & B_{m-3}^{r-1} \\ \square & B_{m-3}^{r-1} & \square & B_{m-3}^{r-1} & B_{m-3}^{r-1} & \square & B_{m-3}^{r-1} & \square \end{bmatrix} \quad (6.25)$$

is the $\binom{m-3}{r-1}$ -fold product of the trellis in Fig.6.3 with itself. Given that the original graph has identical parallel subgraphs, induction on n shows that the n -fold product of this graph with itself yields a graph with 2^{2n} identical parallel sub-graphs. From Corollary 4.2.1, the SRTD of the sub-code of $\mathcal{R}(r, m)$ with trellis oriented generator matrix $G_m^r - M'$ consists of $2^{\binom{m-3}{r-1}}$ identical parallel sub-trellises. Hence, the following theorem has been proven.

Theorem 6.4.2 *The 8-section smallest regular trellis diagram of $\mathcal{R}(r, m)$ consists of*

$$2^{\binom{m-3}{r-1} + 2\binom{m-3}{r-1}}$$

identical parallel sub-trellises. ♣

Let G denote the 3-section minimal trellis diagram of the code given by the trellis-oriented generator matrix

$$\begin{bmatrix} B_{m-3}^{r-2} & B_{m-3}^{r-2} & \square \\ \square & B_{m-3}^{r-2} & B_{m-3}^{r-2} \end{bmatrix}.$$

The section of G between time indices 1 and 2, denoted by $T_2(G)$, is a complete bipartite graph with $2^{\binom{m-3}{r-2}}$ vertices on each side. Let T_1 denote the bipartite graph with two vertices on each side. Induction on n shows that $T^n = T_1^n \times T_2(G)$ is a complete bipartite graph with $2^{n + \binom{m-3}{r-2}}$ vertices on each side, where T_1^n denotes the n -fold product of T_1 with itself. Therefore, $T_1^{\binom{m-3}{r-1}} \times T_2(G)$ is a complete bipartite graph with $2^{\binom{m-3}{r-1} + \binom{m-3}{r-2}}$ vertices on each side. It follows that the number of components

Figure 6.4: One of the 4 parallel sub-trellises of the 8-section smallest regular trellis diagram of $\mathcal{R}(3,5)$.

in the 8-section SRTD of $\mathcal{R}(r,m)$ is

$$t_i(G_{SR}) = \begin{cases} 2^{\binom{m-3}{r} + 2\binom{m-3}{r-1}} & i = 5, \\ 2^{\binom{m-3}{r} - 3\binom{m-3}{r-1}} & i = 2, 3, 4, 6, 7, \\ 1 & i = 1, 8; \end{cases}$$

where for $i = 5$ each component is a copy of T' , and for $i = 2, 3, 4, 6$, and 7 each component is a copy of $T_2(G)$.

Example 6.4.2 One of the four identical parallel sub-trellises of the 8-section smallest regular trellis diagram of $\mathcal{R}(3,5)$ is given in Fig. 6.4.

Comparing Figs. 6.1 and 6.4, it would appear that a decoder for the 8-section SRTD of $QCR(3,5,3)$ would be simpler than a decoder for the SRTD of the Reed-Muller code $\mathcal{R}(3,5)$. The former requires 8 parallel processors, while the latter requires only 4. However, each processor in the decoder for $QCR(3,5,3)$ has 4 states, whereas there are 8 states in the processors for $\mathcal{R}(3,5)$. The tradeoff for this simplified decoder structure is a small decrease in the code dimension: $QCR(3,5,3)$ is a $(32,25,4)$ code while $\mathcal{R}(3,5)$ is a $(32,26,4)$ code. As another example, consider the 8-section SRTD of $\mathcal{R}(3,6)$, which is a $(64,42)$ code. This trellis has 128 parallel

sub-trellises, each of which has 64 states. The 8-section SRTD of $QCR(3, 6, 3)$ has 1024 parallel sub-trellises, each of which has only 8 states. The penalty for this highly parallel structure is a loss in dimension of 3. In general, when $l > 3$, a decoder for the 2^l -section SRTD of $QCR(r, m, l)$ is likely to be less complex than a decoder for the Reed-Muller code $\mathcal{R}(r, m)$.

6.5 Summary

The quasi-cyclic structure of Reed-Muller codes has been analyzed. Specifically, $QCR(r, m, l)$, the largest quasi-cyclic sub-code of $\mathcal{R}(r, m)$ invariant under T^{2^m-l} , has been determined. As a sub-code of $QCR(r, m, l)$, $RQCR(r, m, l)$, the largest regular quasi-cyclic sub-code of $\mathcal{R}(r, m)$ invariant under T^{2^m-l} has also been introduced.

The smallest regular trellis diagram of $QCR(r, m, l)$ was introduced. In addition, an algorithm was developed for constructing the trellis of these codes. It was shown that in terms of the 4-section trellis diagram, the smallest regular trellis diagram of $RQCR(r, m, l)$ is identical to the minimal trellis diagram of $\mathcal{R}(r, m)$.

For i and j , $1 < i, j < n$, each component of the bipartite graph T_i , the sub-graph of $T_{r,m,l}$ between time indices $i-1$ and i , is the same as any component of T_j . A similar property holds for the SRTD of $QCR(r, m, l)$. This is equivalent to the existence of many parallel identical sub-trellises in the trellis diagram, which is desirable when decoding using a trellis.

In terms of VLSI implementation, a comparison of the 2^l -section smallest regular trellis diagram of $QCR(r, m, l)$ and the trellis diagram of $\mathcal{R}(r, m)$ shows that $QCR(r, m, l)$ may be preferable to $\mathcal{R}(r, m)$.

Chapter 7

CONCLUSIONS

The trellis structure of quasi-cyclic codes has been studied. This analysis of the trellis diagrams of quasi-cyclic codes covers both the minimal trellis diagrams and the smallest regular trellis diagrams. The smallest regular trellis diagram has been introduced. It was shown that from the decoding complexity point of view it is preferable to the minimal trellis diagram.

It has been shown, using a canonical representation, that in general quasi-cyclic codes have compact trellis diagrams. The canonical representation of a quasi-cyclic code is a generalization of the representation of a cyclic code via its minimal generator polynomial code word.

The quasi-cyclic structure of Reed-Muller codes has been analyzed. The largest quasi-cyclic sub-code of $\mathcal{R}(r, m)$, invariant under a shift by 2^{m-l} bits, denoted $QCR(r, m, l)$, has been determined. It was shown that the quasi-cyclic structure of Reed-Muller codes and the (24, 12) extended Golay code is the main reason for the simple trellis diagrams of these codes.

The existence of a relationship between the module structure and the canonical representation of a quasi-cyclic code is left as an open problem. More precisely, for a quasi-cyclic code C , under what conditions can a generator matrix M representing both the canonical form and the module decomposition of C be constructed?

Bibliography

- [1] A. Vardy and Y. Be'ery, "Maximum-Likelihood Soft Decision Decoding of BCH Codes", *IEEE Trans. Inform. Theory*, vol. 40, No. 2, pp. 546-554, March 1994.
- [2] V. K. Bhargava, G. E. Seguin and J. M. Stein, "Some (mk, k) cyclic codes in quasi-cyclic form." *IEEE Trans. Inform. Theory*, vol. 24, pp. 630-632, Sept. 1978.
- [3] C. L. Chen, W. W. Peterson and E. J. Weldon, Jr., "Some results on quasi-cyclic codes," *Inform. and Contr.*, vol. 15, pp. 407-423, Nov. 1969.
- [4] Y. Berger and Y. Be'ery, "Bounds on the trellis size of linear block codes", *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 203-209, January 1993.
- [5] G. D. Forney, Jr., "Coset codes-Part II, Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 1152-1187, Sept. 1988.
- [6] G. D. Forney, Jr. and M. D. Trott, "The dynamics of group codes: state spaces, trellis diagrams and canonical encoders," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1491-1513, Sept. 1993.
- [7] F. Harary, *Graph Theory*, Addison-Wesley:New York, 1972.
- [8] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate $1/2$," *IEEE Trans. Inform. Theory*, vol. 20, p. 679, Sept. 1974.

- [9] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On structural complexity of the l-section minimal trellis diagrams for binary linear block codes", *IEICE Trans. Fundamentals Electron. Commun., Comput. Sci.*, 1992.
- [10] T. Kasami, T. Takata, T. Fujiwara, and S. Lin, "On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes", *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 242-245, January 1993.
- [11] T. Kasami, T. Takata, T. Fujiwara, and S. Lin. "On complexity of trellis structure of linear block codes," *IEICE Trans.*, vol. 39, no. 3, May 1993, pp. 1057-1064.
- [12] T. Kasami, T. Fujiwara, Y. Deskai, and S. Lin, "On structural complexity of the l-section minimal trellis diagram for binary linear block codes," *IEICE Trans.*, vol. E76-A, pp. 1411-1421, Sept. 1993.
- [13] F. R. Kschischang and V. Sorokine, "On the trellis structure of block codes," *IEEE Trans. Infor. Theory*, vol. IT-41, Nov. 1995, pp. 1924-1937.
- [14] F.R. Kschischang, "Applications of nonminimal trellis diagrams," *Proc. 4th Canadian Workshop on Infor. Theory*, Quebec City, Canada, May 1995.
- [15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, New York: North-Holland, 1977.
- [16] A. Poli and L. Huguet, *Error Correcting Codes, Theory and Application*, Masson and Prentice Hall:UK, 1992.
- [17] M. Ran and J. Snyders, "Constrained designs for maximum likelihood soft decoding of RM(2,m) and the extended Golay codes," *IEEE Trans. Commun.*, vol. 43, pp. 812-820, February/March/April 1995.

- [18] D. Muder, "Minimal trellises for block codes," *IEEE Trans. Infor. Theory*, vol. IT-34, no. 5, pp. 1049-1053, Sept. 1988.
- [19] S. Roman, *Coding and Information Theory*, Graduate Texts in Mathematics, vol. 134, Springer-Verlag: New York, 1992.
- [20] J. L. Massey, "Foundation and methods of channel encoding," *Proc. Int. Conf. on Inform. Theory and Systems*, vol. 65, Berlin, Sept. 1978.
- [21] G. E. Seguin and H. I. Huynh, *Quasi-Cyclic Codes: A Study*, Technical Report, Universite Laval, Quebec, Canada, 1985.
- [22] G. E. Seguin and G. Drolet, "The theory of one generator quasi-cyclic codes", unpublished manuscript, Royal Military College of Canada, Kingston, Ontario, 1990.
- [23] L.R. Bahl, J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding of linear codes for minimizing symbol error rate," *IEEE Trans. Infor. Theory*, vol. IT-20, Mar. 1974, pp. 284-287.
- [24] J.K. Wolf, "Maximum likelihood decoding of linear block codes using a trellis," *IEEE Trans. Infor. Theory*, vol. 24, pp. 76-80, Jan. 1978.
- [25] V.A. Zinoviev, "Generalized concatenated codes," *Problemy Peredachi Informatsii*, vol. 12, no. 1, pp. 5-15, 1976.
- [26] S. Lin and D. J. Costello, Jr., "Error Control Coding-Fundamentals and Applications," *Prentice-Hall, Englewood Cliffs, N.J* 07632, 1983.
- [27] G. D. Forney Jr., "The Viterbi algorithm", *Proc. IEEE*, vol. 61, pp. 268-278, 1973.

END

1 3 0 6 9 7

FIN