1996

Coding theory and discrete transforms

Feng-Luan Hsu
Iowa State University

Follow this and additional works at: https://lib.dr.iastate.edu/rtd

Part of the Mathematics Commons

Recommended Citation
Hsu, Feng-Luan, "Coding theory and discrete transforms" (1996). Retrospective Theses and Dissertations. 11154.
https://lib.dr.iastate.edu/rtd/11154
INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6” x 9” black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
Coding theory and discrete transforms

by

Feng-Luan Hsu

A Dissertation Submitted to the
Graduate Faculty in Partial Fulfillment of the
Requirements for the Degree of
DOCTOR OF PHILOSOPHY
Department: Mathematics
Major: Mathematics

Approved:

Signature was redacted for privacy.
In Charge of Major Work
Signature was redacted for privacy.
For the Major Department
Signature was redacted for privacy.
For the Graduate College

Iowa State University
Ames, Iowa
1996

Copyright © Feng-Luan Hsu. 1996. All rights reserved.
# TABLE OF CONTENTS

ACKNOWLEDGMENTS .................................................. vi

CHAPTER 1. INTRODUCTION ........................................ 1
  Dissertation Organization ........................................ 4

CHAPTER 2. LOGARITHMS, SYNDROME FUNCTIONS, AND
THE INFORMATION RATES OF GREEDY LOOP TRANSVERSAL CODES ........................................ 5
  Abstract ......................................................... 5
  Introduction ...................................................... 6
  The greedy loop transversal algorithm ......................... 7
  Binary white-noise syndrome functions ......................... 10
  Dimensions of greedy LT codes ................................ 18
  References ....................................................... 24

CHAPTER 3. A DISCRETE Transform AND FUNCTION SPACES ON THE QUADRATIC CLOSURE OF GF(2) ....... 25
  Abstract ......................................................... 25
  Introduction ...................................................... 26
  Order and field structures on N ................................. 28
  Pascal’s Triangle and the Sierpiński triangle ................... 36
The transform and its inverse ........................................ 37
The top of the inverse matrix ........................................ 42
Function spaces ......................................................... 53
Small, coherent sequences ........................................... 62
References ............................................................... 70

CHAPTER 4.  EXPONENTIATION IN THE QUADRATIC CLO-
SURE OF GF(2) ......................................................... 73

CHAPTER 5.  CONCLUSION ........................................... 85

BIBLIOGRAPHY .......................................................... 92
LIST OF TABLES

Table 2.1: Efficiency of binary 2-, 3-, and 4-error greedy LT codes . . . 11
Table 2.2: Dimensions of binary greedy LT codes . . . . . . . . . . . 19
Table 2.3: Dimensions of binary greedy LT codes . . . . . . . . . . . 20
Table 2.4: Dimensions of binary greedy LT codes . . . . . . . . . . . 21
Table 2.5: Dimensions of binary greedy LT codes . . . . . . . . . . . 22
Table 2.6: Dimensions of ternary greedy LT 2-error codes . . . . . . 23
Table 3.1: The 16 × 16 transform matrix $f_4$ . . . . . . . . . . . . 71
Table 3.2: The first row of $f_4$ as Pascal’s Triangle modulo 2 . . . . . . 72
LIST OF FIGURES

Figure 2.1: Syndrome function for binary 2-error .................. 12
Figure 2.2: Syndrome function for binary 2-error .................. 13
Figure 2.3: Syndrome function for binary 3-error .................. 14
Figure 2.4: Syndrome function for binary 3-error .................. 15
Figure 2.5: Syndrome function for binary 4-error .................. 16
Figure 2.6: Syndrome function for binary 4-error .................. 17

Figure 5.1: Transformed syndrome function (n=32, t=1) .............. 87
Figure 5.2: Transformed syndrome function (n=32, t=2) .............. 88
Figure 5.3: Transformed syndrome function (n=32, t=3) .............. 89
Figure 5.4: Transformed syndrome function (n=32, t=4) .............. 90
Figure 5.5: Transformed syndrome function (n=256, t=2) .......... 91
ACKNOWLEDGMENTS

First of all, I would like to express my deepest gratitude to my major advisor, Professor Jonathan D. H. Smith, for suggesting me the problems and for his expert guidance throughout the preparation of this thesis. All through my graduate study at Iowa State University, he has been a constant resource of encouragements, inspiration, and tremendous ideas. Not only his way of problem-thinking and problem-solving that has benefited me most in research, but also his wisdom in life that has influenced me in every respect of life. It has been a great pleasure to work with such a scholar of knowledge, insight, and character.

I want to thank Professors Clifford Bergman, James Cornette, Herbert T. David, and Sung Yell Song for serving on my POS committee and giving their time and assistance during my studies at Iowa State University.

Special thanks are due to Professor Jack Lutz in the Department of Computer Science for sponsoring the use of the HP-UX machines in his department. It would have been difficult to obtain the graphical and tabular data presented here without the use of these machines.

I am also grateful to Ruth De Boer, Fran Hartman, Jan Nyhus, Ellen Olson, and Jim Lathrop for helping me in lots of different ways.

Most of all, I thank my parents, Jung-Hsin Hsu and A-Yen Tang Hsu, for their
never-ending love and support. Their encouragement and support make it possible for me to receive a higher education. I also thank my husband, Chih-Yao, for his patience, encouragement, assistance, and support; and my son Ian, for bringing me so much fun and joy. This dissertation is dedicated to them with my sincere appreciation.
CHAPTER 1. INTRODUCTION

The theory of error detecting and correcting codes is that branch of engineering and mathematics which deals with the reliable transmission and storage of data. The channels or the information media are not 100% reliable in practice, in the sense that noise (any form of interference) frequently causes data to be distorted.

To deal with this undesirable but inevitable situation, some form of redundancy is incorporated in the original data. With this redundancy, even if errors are introduced (up to some tolerance level), the original information can be recovered, or at least the presence of errors can be detected.

One of the problems to be resolved then is to determine how the channel encoder should add redundancy to the source encoder output. Another problem is to determine how the channel decoder should decide which sequence to decode to.

The design of error-correcting block codes has traditionally been influenced by two factors: an assumption of “white noise” (random noise) in the channel, and imposition of a severe limitation on the storage space available to the encoding and decoding algorithms. Under these influences, algebraic coding theory has been led to comprise an impressive directory of mathematically structured codes and their distance distributions. Nevertheless, in assessing the progress of the field a decade ago, Hamming [Ha, Chap 11.13] made the following comments:
In the year 1985, we are seeing a great decrease in the cost of storage, and hence there is a need to reconsider all the theory that we have developed in the past. Methods of design, encoding, and decoding which depend more on table look up and other forms of storage and less on computing need to be researched and developed. Again, you need to be warned that the theory is almost all designed to meet white noise, and in practice often the noise is not white and the theoretical benefits of a code may therefore not be realized in practice.

The general loop transversal approach to the construction of linear block codes, introduced in [Sm], ultimately relies more on the availability of cheap storage than on the use of exceptional mathematical structures. Rather than focusing on the code itself as the primary object of interest, the approach (see [Sm]) to the construction of linear block codes concentrates on the set of errors corrected by the code. These errors do not necessarily have to form a ball, as they would under the assumption of white noise, but might equally well form an asymmetric figure corresponding to bursts or some other distribution.

The basis for the loop transversal approach is the observation that the set $T$ of errors corrected by a linear code $C$ in a channel $V$ forms a loop transversal from $V$ to $C$. Recall that a transversal $T$ to a subgroup $C$ of a group $(V, +, 0)$ is a subset of $V$ with $V = \bigcup_{t \in T} (C + t)$. Thus each element $x$ of $V$ can be expressed uniquely as $x = x^c + x^e$, with $x^c \in C$ and $x^e \in T$. In the coding context, a received word $x$ is assumed to have resulted from exposure to the error $x^e$, and is thus decoded as $x^c$.

Define a binary operation $*$ on $T$ by $t * u = (t + u)^e$. Then for any $t, u$ in $T$, the equation $v * t = u$ has a unique solution $v$. If the equation $t * v = u$ also has a unique solution, then $T$ is a loop transversal. Equivalently, the algebra $(T, *, 0_e)$ is a loop.

If the channel $V$ is a vector space over a field $F$, and the code $C$ is a subspace of $V$, then is said to be a linear code. Define $\lambda \times t = (\lambda t)^e$ for $x$ in $F$ and $t$ in $T$. We
then have that \((T, *, F)\) is a vector space over \(F\), where \(T\) is the set of errors corrected by the code \(C\). Knowledge of the vector space \((T, *, F)\) is sufficient to determine the code \(C\) by local duality, which says that for \(t, u \in T\), \(t + u + t * u \in C\). Also, note that \((x + y)\varepsilon = x\varepsilon * y\varepsilon\) and \((\lambda x)\varepsilon = \lambda \times (x\varepsilon)\) for \(\lambda \) in \(F\) and \(x, y\) in \(V\). Thus the parity map \(\varepsilon : (V, +, F) \rightarrow (T, *, F)\) is a linear transformation. Since the code is the kernel of the parity map, the matrices of \(\varepsilon\) with respect to appropriate bases are parity-check matrices.

To get \((T, *, F)\), we use an isomorphism \(S : (T, *) \rightarrow (G, +)\), for example a monomorphism \(S : (T, *) \rightarrow (N, +_2)\) in binary case. Here \(+_2\) is the nim-addition. We call the monomorphism \(S : (T, *) \rightarrow (N, +_2)\) a syndrome function. The paper [HmS] gives more detail of the general loop transversal approach to the construction of linear codes, focusing especially on the greedy loop transversal algorithm in the binary case.

In the paper entitled “Logarithms, Syndrome Functions, and the Information Rates of Greedy Loop Transversal Codes” (Chapter 2), we use a greedy algorithm to construct syndrome functions of binary lexicodes up to high dimensionalities. The graphs of the syndrome functions turn out to have curious fractal properties. As part of an on-going program investigating these functions, we consider them as polynomials in subfields of the quadratic closure of GF(2). Passing from such a polynomial function to its coefficient sequence provides a linear transform, analogous to the discrete Fourier transform. Despite the exponentially increasing sizes of the transform matrices, they may be inverted explicitly. The inverse transform matrices have a fractal structure, including the Sierpiński triangle in their first row. The paper “A Discrete Transform and Function Spaces on the Quadratic Closure of GF(2)” (Chap-
ter 3) studies the transform, and uses the transform to analyze certain spaces of natural number functions that include the syndromes of the codes. Transforms of functions in these spaces exhibit a martingale property.

Finally, Theorem 4.6 in Chapter 4 represents a key result on exponentiation in the quadratic closure of GF(2). It was originally proved by H. W. Lenstra, Jr. in 1980 [Le2]. We will give an alternative, more elementary approach to the proof of this result in Chapter 4.

Dissertation Organization

This dissertation includes two papers, entitled "Logarithms, Syndrome Functions, and the Information Rates of Greedy Loop Transversal Codes" and "A Discrete Transform and Function Spaces on the Quadratic Closure of GF(2)," Chapters 2 and 3 respectively. In Chapter 4, we study some additional properties of the quadratic closure of GF(2). Chapter 5 comprises the general conclusions. In the Bibliography, we list all the references we used in the previous chapters.
CHAPTER 2. LOGARITHMS, SYNDROME FUNCTIONS, AND THE INFORMATION RATES OF GREEDY LOOP TRANSVERSAL CODES

A paper accepted by the Journal of Combinatorial Mathematics and Combinatorial Computing
Feng-Luan Hsu, Frank A. Hummer and Jonathan D. H. Smith

Abstract

The paper studies linear block codes and syndrome functions built by the greedy loop transversal algorithm. The syndrome functions in the binary white-noise case are generalizations of the logarithm, with curious fractal properties. The codes in the binary white-noise case coincide with lexicodes: their dimensions are listed for channel lengths up to the sixties, and up to the three hundreds for double errors. In the ternary double-error case, record-breaking codes of lengths 43 to 68 are constructed.

\(^1\)Graduate students and Professor, respectively, Department of Mathematics, Iowa State University.
Introduction

The general loop transversal approach to the construction of linear block codes was introduced in [Sm]. A companion paper [HmS] gives further details, concentrating on the greedy loop transversal algorithm in the binary case. In particular, it is shown there [HmS, Theorem 6.1] that the greedy loop transversal algorithm provides an alternative method for building binary lexicodes, especially suitable for good channels. The current paper has two aims. The first is to present data on the dimensions of the codes of various lengths constructed by the greedy loop transversal algorithm. (The phrase "loop transversal code" is abbreviated here to "LT code".) For binary channels, double, triple and quadruple white-noise error patterns are treated, corresponding to minimum distances 5, 6 (Table 2.2, 2.3, and 2.4) and 7–10 (Table 2.5) in metric language. The data may be read as giving the dimensions of lexicodes, for channel lengths beyond 300 in the double-error case. For ternary channels, greedy loop transversal codes and lexicodes differ, since the former are linear while the latter are not. Table 2.6 gives the dimensions of the ternary Hamming double-error correcting greedy loop transversal codes, for channel lengths up to 68. They include the perfect ternary Golay code, and new record-breaking codes for lengths above 42.

The second aim of the paper is to draw attention to the syndrome functions constructed by the greedy loop transversal algorithm for binary white-noise error patterns. For single errors, the syndrome (2.9) is essentially the logarithm function, so for other white-noise error patterns the syndromes may be considered as generalizations of the logarithm. Their graphs (Figures 2.1–2.6) display curious fractal properties that warrant further investigation. Another mysterious feature of the syndromes is the apparent convergence of the "efficiencies" defined below (2.11) and
recorded in Table 2.1.

The presentation of the graphical and tabular data in Sections 3 and 4 is prefaced by a description of the greedy loop transversal algorithm in Section 2, for arbitrary error patterns in channels over alphabets that are prime fields.

**The greedy loop transversal algorithm**

Fix a prime $p$. Each natural number $n$ (including 0) has a unique expansion

$$n = \sum_{i=0}^{\infty} n(i)p^i$$

with $0 \leq n(i) < p$ for each $i$. Moreover, $n(i) = 0$ for $i > \lfloor \log_p n \rfloor$. For $d > \lfloor \log_p n \rfloor$, the natural number $n$ may be identified with the vector $(n(d - 1), \ldots, n(1), n(0))$ in the $d$-dimensional vector space $V_d = GF(p)^d$ over the Galois field $GF(p)$ of order $p$.

Thus the set $\mathbb{N}$ of natural numbers is identified with the nested union $\bigcup_{d>0} V_d$ of vector spaces. The induced addition and subtraction operations on integers are written as $+_p$ and $-_p$ to avoid confusion with the usual addition and subtraction. For example, both $+2$ and $-2$ are the “nim sum” of [Co, p.51]. Besides the usual (well-)ordering $\leq$, the set of natural numbers carries a partial ordering $\subseteq_p$, known as the Hamming order, defined by

$$m \subseteq_p n \iff \exists F \subset \mathbb{N}. \quad m = n - \sum_{i \in F} n(i)p^i. \quad (2.2)$$

In other words, $m$ is bounded above by $n$ in the Hamming order if and only if the expansion (2.1) for $m$ is obtained from the expansion for $n$ by replacing certain digits $n(i)$ – namely those with $i$ in $F$ – by the digit 0. Note that 0 is the bottom element of $(\mathbb{N}, \subseteq_p)$, and that the Hamming distance between $m$ and $n$ is the rank of $m -_p n$ in the poset $(\mathbb{N}, \subseteq_p)$. 
A subset $X$ of a poset $(Y, \subseteq)$ is said to be self-subordinate if $y \subseteq x \in X$ implies $y \in X$. A self-subordinate subset $E$ of $(N, \subseteq_p)$ is called an error pattern if it contains the set $p^N = \{p^i | i \in N\}$. Error patterns model sets of errors to be corrected in the various channels $V_d$. For example, $\{\alpha p^i | \alpha \in GF(p); i \in N\}$ comprises the errors of Hamming weight at most 1. White noise double errors are modeled by $\{\alpha p^i +_p \beta p^j | \alpha, \beta \in GF(p); i, j \in N, |i-j| \leq 1\}$. Burst double errors are modeled by $\{\alpha p^i + p^j \beta p^j | \alpha, \beta \in GF(p); i, j \in N, |i-j| \leq 1\}$. Error patterns form partial algebras under the operations of the vector space $(N, +_p, GF(p))$. For example, the sum $p^i +_p p^j$ is defined in the burst double error pattern if and only if $|i-j| \leq 1$. Suppose that an error pattern $E$ is given. Then an $E$-syndrome, or just syndrome, is a partial function $s : E \to N$ which:

(a) injects;

(b) is a partial vector space homomorphism;

(c) has domain self-subordinate in $(E, \leq)$, and

(d) satisfies: $\forall n \in N, \exists r \in N. p^N \cap s(V_d \cap E) \text{ spans } V_r$.

The syndrome is said to be proper if $s$ is a properly partial function. In view of (c), this is equivalent to finiteness of the domain of $s$. For a proper syndrome, the length is defined to be

$$n = \max\{1 + \lfloor \log p m \rfloor | m \in \text{dom } s\}.$$  \hspace{1cm} (2.4)

The redundancy is defined to be

$$r = \max\{1 + \lfloor \log p (ms) \rfloor | m \in \text{dom } s\}.$$  \hspace{1cm} (2.5)

A proper syndrome $s$ defines a parity map

$$\varepsilon_s : V_n \to V_r$$  \hspace{1cm} (2.6)
by linearity and $p^i \varepsilon_s = p^i s$ for $i < n$. By (c), these values $p^i s$ are defined. Condition (b) guarantees that $s$ agrees with $\varepsilon_s$ on $V_n \cap E$. Condition (d) yields that $\varepsilon_s$ surjects. Condition (a) guarantees that $\text{dom } s$ embeds into $V_r$ under $\varepsilon_s$. A code $C_n$ in the channel $V_n$ correcting the set $V_n \cap E$ of errors, and having dimension $n - r$, is then given as the kernel of $\varepsilon_s$.

The greedy loop transversal algorithm determines an $E$-syndrome $s$ by the partial linearity (2.3) (b) and the greedy choice of $p^n s$ given that $s : (V_n \cap E) \to \mathbb{N}$ has already been defined. In other words, $p^n s$ is the minimal element of the set of integers $m$ satisfying the requirement

$$\forall e \neq f \in V_{n+1} \cap E, \quad (2.7)$$

$$e(n)m +_p (e -_p (e(n)p^n))s \neq f(n)m +_p (f -_p (f(n)p^n))s.$$ 

Then for $e \in (V_{n+1} - (V_n \cup \{p^n\})) \cap E,$

$$es := e(n)(p^n s) +_p (e -_p (e(n)p^n))s. \quad (2.8)$$

In (2.7) and (2.8), juxtaposition of an element of $GF(p)$ and an integer denotes the scalar multiple of that integer by the element of $GF(p)$. Note that the partial linearity requirement (2.3) (b) initializes the algorithm with $0 = 0$. If $E$ is closed under scalar multiplication, then (2.7) may be simplified. The greedy algorithm picks $p^n s$ to be the least integer not in anathema, the set

$$\{es +_p fs \mid e, f \in V_n \cap E; p^n +_p e \in E\}$$

(cf. [Sm.(5.1)]).
Binary white-noise syndrome functions

If $E$ is the binary white-noise single error pattern $\{0\} \cup 2^N$, the greedy loop transversal algorithm builds the improper syndrome function $s_1$ with $0s_1 = 0$ and

$$s_1 : 2^N \rightarrow \mathbb{N}; \ x \mapsto 1 + \log_2 x. \quad (2.9)$$

In this sense, the syndrome function for single errors is essentially the logarithm function. One may then regard the syndrome function $s_t$ built by the greedy loop transversal algorithm for the binary white-noise $t$-error pattern $E_t$ as a generalization of the logarithm function. To facilitate comparison with the logarithm function, the syndrome function

$$s_t : E_t \rightarrow \mathbb{N}; \ x \mapsto y \quad (2.10)$$

is graphed with $\log_2 x$ on the ordinate and $y$ on the abscissa in Figures 2.1, 2.3, and 2.5, for 2-error, 3-error, and 4-error cases. With a similar convention, the graph of $s_1$ would appear as a straight line of slope 1. Figures 2.2, 2.4, and 2.6 "plot the graphs of Figures 2.1, 2.3, and 2.5 on logarithmic paper", i.e., they graph $s_t : x \mapsto y$ by plotting $\log_2 \log_2 x$ against $\log_2 y$. The fractal form of Figures 2.1–2.6 is very striking, and clearly warrants further investigation. As an initial step in such an investigation, define a nodal point of the syndrome function $s_t$ to be a point on its graph of the form $(2^n, 2^k)$ for integral $n, k$. (The analysis given in [HmS] shows that the graph includes such points.) The proper syndrome given by the restriction of $s_t$ to the channel $V_n$ then yields a $t$-error correcting code $C_n$ with redundancy $k + 1$. By the sphere-packing bound,

$$2^{k+1} \geq \left( \begin{array}{c} n \\ t \end{array} \right) + \left( \begin{array}{c} n \\ t - 1 \end{array} \right) + \cdots + \left( \begin{array}{c} n \\ 1 \end{array} \right) + \left( \begin{array}{c} n \\ 0 \end{array} \right). \quad (2.11)$$
The efficiency of the code $C_n$ of redundancy $k + 1$ is the ratio of $\log_2\left(\binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{k-1} + \binom{n}{k} + \binom{n}{n}\right)$ to $k + 1$, usually expressed as a percentage. Table 2.1 lists these efficiencies for $0 < k < 19$ and $1 < t < 5$. Their apparent convergence to about 80% is rather curious.

Table 2.1: Efficiency of binary 2-, 3-, and 4-error greedy LT codes

<table>
<thead>
<tr>
<th>$k + 1$</th>
<th>2-Error</th>
<th>3-Error</th>
<th>4-Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>79.61</td>
<td>79.67</td>
<td>79.76</td>
</tr>
<tr>
<td>18</td>
<td>79.73</td>
<td>82.44</td>
<td>79.71</td>
</tr>
<tr>
<td>17</td>
<td>79.99</td>
<td>78.74</td>
<td>78.90</td>
</tr>
<tr>
<td>16</td>
<td>80.31</td>
<td>77.64</td>
<td>80.51</td>
</tr>
<tr>
<td>15</td>
<td>80.63</td>
<td>78.98</td>
<td>79.89</td>
</tr>
<tr>
<td>14</td>
<td>80.57</td>
<td>82.34</td>
<td>80.70</td>
</tr>
<tr>
<td>13</td>
<td>80.64</td>
<td>87.37</td>
<td>84.02</td>
</tr>
<tr>
<td>12</td>
<td>80.08</td>
<td>93.19</td>
<td>84.12</td>
</tr>
<tr>
<td>11</td>
<td>80.58</td>
<td>85.86</td>
<td>87.57</td>
</tr>
<tr>
<td>10</td>
<td>79.89</td>
<td>82.24</td>
<td>91.34</td>
</tr>
<tr>
<td>9</td>
<td>82.51</td>
<td>82.88</td>
<td>95.47</td>
</tr>
<tr>
<td>8</td>
<td>78.80</td>
<td>87.78</td>
<td>91.86</td>
</tr>
<tr>
<td>7</td>
<td>78.91</td>
<td>93.42</td>
<td>94.71</td>
</tr>
<tr>
<td>6</td>
<td>80.97</td>
<td>89.87</td>
<td>97.21</td>
</tr>
<tr>
<td>5</td>
<td>89.19</td>
<td>94.01</td>
<td>99.08</td>
</tr>
<tr>
<td>4</td>
<td>86.49</td>
<td>97.67</td>
<td>100.00</td>
</tr>
<tr>
<td>3</td>
<td>93.58</td>
<td>100.00</td>
<td>100.00</td>
</tr>
<tr>
<td>2</td>
<td>100.00</td>
<td>100.00</td>
<td>100.00</td>
</tr>
</tbody>
</table>
Figure 2.1: Syndrome function for binary 2-error
Figure 2.2: Syndrome function for binary 2-error
Figure 2.3: Syndrome function for binary 3-error
Figure 2.4: Syndrome function for binary 3-error
Figure 2.5: Syndrome function for binary 4-error
Figure 2.6: Syndrome function for binary 4-error
Dimensions of greedy LT codes

The final three tables record the dimensions of the codes $C_n$ of length $n$ constructed by the greedy loop transversal algorithm. For each $n$, the second column of Table 2.2, 2.3, and 2.4 records the dimension of the greedy LT code correcting binary white-noise double errors, i.e. of minimum Hamming distance $d = 5$. The third column records the dimension of the corresponding codes of minimum Hamming distance $d = 6$ obtained by adjoining a parity check (thus increasing the length by 1). For lengths less than $2^7$, the entries in parentheses are the dimensions of the best known linear code of length $n$ and minimum distance $d$, as recorded in [Ve]. Table 2.5 records analogous data for binary white-noise triple and quadruple errors, i.e. minimum distances $d = 7, 8, 9, 10$. Since binary greedy LT codes are the same as lexicodes [Theorem 6.1], Tables 2.2, 2.3, 2.4, and 2.5 may also be read as giving the dimensions of lexicodes. Table 2.6 lists the dimensions of the ternary greedy LT codes correcting white-noise Hamming double errors, i.e. with minimum Hamming distance $d = 5$. It is interesting to note that the code of length 11 has dimension 6, so that it coincides with the perfect ternary Golay code. The numbers in parentheses list the dimensions of the best known ternary linear codes of minimum distance 5, as recorded in [KP]. The greedy LT codes of lengths 43 to 50 are better than the best known to Kschischang and Pasupathy. The data in [KP] stopped at length 50, but the greedy LT codes of lengths 51 onwards are also likely to be world records.
Table 2.2: Dimensions of binary greedy LT codes

<table>
<thead>
<tr>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>4(4)</td>
<td>4(4)</td>
<td>43</td>
<td>31(31)</td>
<td>30(30)</td>
<td>74</td>
<td>60(61)</td>
<td>59(60)</td>
</tr>
<tr>
<td>13</td>
<td>5(5)</td>
<td>4(4)</td>
<td>44</td>
<td>32(32)</td>
<td>31(31)</td>
<td>75</td>
<td>61(61)</td>
<td>60(61)</td>
</tr>
<tr>
<td>14</td>
<td>6(6)</td>
<td>5(5)</td>
<td>45</td>
<td>33(33)</td>
<td>32(32)</td>
<td>76</td>
<td>62(62)</td>
<td>61(61)</td>
</tr>
<tr>
<td>15</td>
<td>7(7)</td>
<td>6(6)</td>
<td>46</td>
<td>34(34)</td>
<td>33(33)</td>
<td>77</td>
<td>63(63)</td>
<td>62(62)</td>
</tr>
<tr>
<td>16</td>
<td>8(8)</td>
<td>7(7)</td>
<td>47</td>
<td>35(35)</td>
<td>34(34)</td>
<td>78</td>
<td>64(64)</td>
<td>63(63)</td>
</tr>
<tr>
<td>17</td>
<td>9(9)</td>
<td>8(8)</td>
<td>48</td>
<td>36(36)</td>
<td>35(35)</td>
<td>79</td>
<td>65(65)</td>
<td>64(64)</td>
</tr>
<tr>
<td>18</td>
<td>9(9)</td>
<td>9(9)</td>
<td>49</td>
<td>37(37)</td>
<td>36(36)</td>
<td>80</td>
<td>66(66)</td>
<td>65(65)</td>
</tr>
<tr>
<td>19</td>
<td>10(10)</td>
<td>9(9)</td>
<td>50</td>
<td>38(38)</td>
<td>37(37)</td>
<td>81</td>
<td>67(67)</td>
<td>66(66)</td>
</tr>
<tr>
<td>20</td>
<td>11(11)</td>
<td>10(10)</td>
<td>51</td>
<td>39(39)</td>
<td>38(38)</td>
<td>82</td>
<td>68(68)</td>
<td>67(67)</td>
</tr>
<tr>
<td>21</td>
<td>12(12)</td>
<td>11(11)</td>
<td>52</td>
<td>40(40)</td>
<td>39(39)</td>
<td>83</td>
<td>69(69)</td>
<td>68(68)</td>
</tr>
<tr>
<td>22</td>
<td>12(12)</td>
<td>12(12)</td>
<td>53</td>
<td>41(41)</td>
<td>40(40)</td>
<td>84</td>
<td>70(70)</td>
<td>69(69)</td>
</tr>
<tr>
<td>23</td>
<td>13(13)</td>
<td>12(13)</td>
<td>54</td>
<td>41(42)</td>
<td>41(41)</td>
<td>85</td>
<td>71(71)</td>
<td>70(70)</td>
</tr>
<tr>
<td>24</td>
<td>14(14)</td>
<td>13(14)</td>
<td>55</td>
<td>42(43)</td>
<td>41(42)</td>
<td>86</td>
<td>72(72)</td>
<td>71(71)</td>
</tr>
<tr>
<td>25</td>
<td>15(15)</td>
<td>14(14)</td>
<td>56</td>
<td>43(44)</td>
<td>42(43)</td>
<td>87</td>
<td>73(73)</td>
<td>72(72)</td>
</tr>
<tr>
<td>26</td>
<td>16(16)</td>
<td>15(15)</td>
<td>57</td>
<td>44(45)</td>
<td>43(44)</td>
<td>88</td>
<td>74(74)</td>
<td>73(73)</td>
</tr>
<tr>
<td>27</td>
<td>17(17)</td>
<td>16(16)</td>
<td>58</td>
<td>45(46)</td>
<td>44(45)</td>
<td>89</td>
<td>75(75)</td>
<td>74(74)</td>
</tr>
<tr>
<td>28</td>
<td>18(18)</td>
<td>17(17)</td>
<td>59</td>
<td>46(47)</td>
<td>45(46)</td>
<td>90</td>
<td>76(76)</td>
<td>75(75)</td>
</tr>
<tr>
<td>29</td>
<td>19(19)</td>
<td>18(18)</td>
<td>60</td>
<td>47(48)</td>
<td>46(47)</td>
<td>91</td>
<td>77(77)</td>
<td>76(76)</td>
</tr>
<tr>
<td>30</td>
<td>19(20)</td>
<td>19(19)</td>
<td>61</td>
<td>48(49)</td>
<td>47(48)</td>
<td>92</td>
<td>78(78)</td>
<td>77(77)</td>
</tr>
<tr>
<td>31</td>
<td>20(21)</td>
<td>19(20)</td>
<td>62</td>
<td>49(50)</td>
<td>48(49)</td>
<td>93</td>
<td>78(79)</td>
<td>78(78)</td>
</tr>
<tr>
<td>32</td>
<td>21(22)</td>
<td>20(21)</td>
<td>63</td>
<td>50(51)</td>
<td>49(50)</td>
<td>94</td>
<td>79(80)</td>
<td>79(79)</td>
</tr>
<tr>
<td>33</td>
<td>22(22)</td>
<td>21(22)</td>
<td>64</td>
<td>51(52)</td>
<td>50(51)</td>
<td>95</td>
<td>80(81)</td>
<td>80(80)</td>
</tr>
<tr>
<td>34</td>
<td>23(23)</td>
<td>22(22)</td>
<td>65</td>
<td>52(53)</td>
<td>51(52)</td>
<td>96</td>
<td>81(82)</td>
<td>81(81)</td>
</tr>
<tr>
<td>35</td>
<td>24(24)</td>
<td>23(23)</td>
<td>66</td>
<td>53(53)</td>
<td>52(53)</td>
<td>97</td>
<td>82(83)</td>
<td>82(82)</td>
</tr>
<tr>
<td>36</td>
<td>25(25)</td>
<td>24(24)</td>
<td>67</td>
<td>54(54)</td>
<td>53(53)</td>
<td>98</td>
<td>83(84)</td>
<td>83(83)</td>
</tr>
<tr>
<td>37</td>
<td>26(26)</td>
<td>25(25)</td>
<td>68</td>
<td>55(55)</td>
<td>54(54)</td>
<td>99</td>
<td>84(85)</td>
<td>84(84)</td>
</tr>
<tr>
<td>38</td>
<td>27(27)</td>
<td>26(26)</td>
<td>69</td>
<td>56(56)</td>
<td>55(55)</td>
<td>100</td>
<td>85(86)</td>
<td>85(85)</td>
</tr>
<tr>
<td>39</td>
<td>27(28)</td>
<td>27(27)</td>
<td>70</td>
<td>56(57)</td>
<td>56(56)</td>
<td>101</td>
<td>86(87)</td>
<td>86(86)</td>
</tr>
<tr>
<td>40</td>
<td>28(29)</td>
<td>27(28)</td>
<td>71</td>
<td>57(58)</td>
<td>56(57)</td>
<td>102</td>
<td>87(88)</td>
<td>87(87)</td>
</tr>
<tr>
<td>41</td>
<td>29(30)</td>
<td>28(29)</td>
<td>72</td>
<td>58(59)</td>
<td>57(58)</td>
<td>103</td>
<td>88(89)</td>
<td>88(88)</td>
</tr>
<tr>
<td>42</td>
<td>30(30)</td>
<td>29(30)</td>
<td>73</td>
<td>59(60)</td>
<td>58(59)</td>
<td>104</td>
<td>89(90)</td>
<td>89(89)</td>
</tr>
</tbody>
</table>

Note: numbers inside ( ) are data from Tom Verhoeoff in IEEE 1987
Table 2.3: Dimensions of binary greedy LT codes

<table>
<thead>
<tr>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>105</td>
<td>90(91)</td>
<td>89(90)</td>
<td>142</td>
<td>126</td>
<td>125</td>
<td>179</td>
<td>162</td>
<td>161</td>
</tr>
<tr>
<td>106</td>
<td>91(92)</td>
<td>90(91)</td>
<td>143</td>
<td>127</td>
<td>126</td>
<td>180</td>
<td>163</td>
<td>162</td>
</tr>
<tr>
<td>107</td>
<td>92(93)</td>
<td>91(92)</td>
<td>144</td>
<td>128</td>
<td>127</td>
<td>181</td>
<td>164</td>
<td>163</td>
</tr>
<tr>
<td>108</td>
<td>93(94)</td>
<td>92(93)</td>
<td>145</td>
<td>129</td>
<td>128</td>
<td>182</td>
<td>165</td>
<td>164</td>
</tr>
<tr>
<td>109</td>
<td>94(95)</td>
<td>93(94)</td>
<td>146</td>
<td>130</td>
<td>129</td>
<td>183</td>
<td>166</td>
<td>165</td>
</tr>
<tr>
<td>110</td>
<td>95(96)</td>
<td>94(95)</td>
<td>147</td>
<td>131</td>
<td>130</td>
<td>184</td>
<td>167</td>
<td>166</td>
</tr>
<tr>
<td>111</td>
<td>96(97)</td>
<td>95(96)</td>
<td>148</td>
<td>132</td>
<td>131</td>
<td>185</td>
<td>168</td>
<td>167</td>
</tr>
<tr>
<td>112</td>
<td>97(98)</td>
<td>96(97)</td>
<td>149</td>
<td>133</td>
<td>132</td>
<td>186</td>
<td>169</td>
<td>168</td>
</tr>
<tr>
<td>113</td>
<td>98(99)</td>
<td>97(98)</td>
<td>150</td>
<td>134</td>
<td>133</td>
<td>187</td>
<td>170</td>
<td>169</td>
</tr>
<tr>
<td>114</td>
<td>99(100)</td>
<td>98(99)</td>
<td>151</td>
<td>135</td>
<td>134</td>
<td>188</td>
<td>171</td>
<td>170</td>
</tr>
<tr>
<td>115</td>
<td>100(101)</td>
<td>99(100)</td>
<td>152</td>
<td>136</td>
<td>135</td>
<td>189</td>
<td>172</td>
<td>171</td>
</tr>
<tr>
<td>116</td>
<td>101(102)</td>
<td>100(101)</td>
<td>153</td>
<td>137</td>
<td>136</td>
<td>190</td>
<td>173</td>
<td>172</td>
</tr>
<tr>
<td>117</td>
<td>102(103)</td>
<td>101(102)</td>
<td>154</td>
<td>138</td>
<td>137</td>
<td>191</td>
<td>174</td>
<td>173</td>
</tr>
<tr>
<td>118</td>
<td>103(104)</td>
<td>102(103)</td>
<td>155</td>
<td>139</td>
<td>138</td>
<td>192</td>
<td>175</td>
<td>174</td>
</tr>
<tr>
<td>119</td>
<td>104(105)</td>
<td>103(104)</td>
<td>156</td>
<td>140</td>
<td>139</td>
<td>193</td>
<td>176</td>
<td>175</td>
</tr>
<tr>
<td>120</td>
<td>105(106)</td>
<td>104(105)</td>
<td>157</td>
<td>140</td>
<td>140</td>
<td>194</td>
<td>177</td>
<td>176</td>
</tr>
<tr>
<td>121</td>
<td>106(107)</td>
<td>105(106)</td>
<td>158</td>
<td>141</td>
<td>140</td>
<td>195</td>
<td>178</td>
<td>177</td>
</tr>
<tr>
<td>122</td>
<td>107(108)</td>
<td>106(107)</td>
<td>159</td>
<td>142</td>
<td>141</td>
<td>196</td>
<td>179</td>
<td>178</td>
</tr>
<tr>
<td>123</td>
<td>108(109)</td>
<td>107(108)</td>
<td>160</td>
<td>143</td>
<td>142</td>
<td>197</td>
<td>180</td>
<td>179</td>
</tr>
<tr>
<td>124</td>
<td>109(110)</td>
<td>108(109)</td>
<td>161</td>
<td>144</td>
<td>143</td>
<td>198</td>
<td>181</td>
<td>180</td>
</tr>
<tr>
<td>125</td>
<td>110(111)</td>
<td>109(110)</td>
<td>162</td>
<td>145</td>
<td>144</td>
<td>199</td>
<td>182</td>
<td>181</td>
</tr>
<tr>
<td>126</td>
<td>111(112)</td>
<td>110(111)</td>
<td>163</td>
<td>146</td>
<td>145</td>
<td>200</td>
<td>183</td>
<td>182</td>
</tr>
<tr>
<td>127</td>
<td>112(113)</td>
<td>111(112)</td>
<td>164</td>
<td>147</td>
<td>146</td>
<td>201</td>
<td>184</td>
<td>183</td>
</tr>
<tr>
<td>128</td>
<td>113</td>
<td>111</td>
<td>165</td>
<td>148</td>
<td>147</td>
<td>202</td>
<td>185</td>
<td>184</td>
</tr>
<tr>
<td>129</td>
<td>114</td>
<td>112</td>
<td>166</td>
<td>149</td>
<td>148</td>
<td>203</td>
<td>186</td>
<td>185</td>
</tr>
<tr>
<td>130</td>
<td>115</td>
<td>113</td>
<td>167</td>
<td>150</td>
<td>149</td>
<td>204</td>
<td>186</td>
<td>186</td>
</tr>
<tr>
<td>131</td>
<td>116</td>
<td>114</td>
<td>168</td>
<td>151</td>
<td>150</td>
<td>205</td>
<td>187</td>
<td>186</td>
</tr>
<tr>
<td>132</td>
<td>117</td>
<td>115</td>
<td>169</td>
<td>152</td>
<td>151</td>
<td>206</td>
<td>188</td>
<td>187</td>
</tr>
<tr>
<td>133</td>
<td>118</td>
<td>116</td>
<td>170</td>
<td>153</td>
<td>152</td>
<td>207</td>
<td>189</td>
<td>188</td>
</tr>
<tr>
<td>134</td>
<td>119</td>
<td>117</td>
<td>171</td>
<td>154</td>
<td>153</td>
<td>208</td>
<td>190</td>
<td>189</td>
</tr>
<tr>
<td>135</td>
<td>120</td>
<td>118</td>
<td>172</td>
<td>155</td>
<td>154</td>
<td>209</td>
<td>191</td>
<td>190</td>
</tr>
<tr>
<td>136</td>
<td>121</td>
<td>119</td>
<td>173</td>
<td>156</td>
<td>155</td>
<td>210</td>
<td>192</td>
<td>191</td>
</tr>
<tr>
<td>137</td>
<td>122</td>
<td>120</td>
<td>174</td>
<td>157</td>
<td>156</td>
<td>211</td>
<td>193</td>
<td>192</td>
</tr>
<tr>
<td>138</td>
<td>123</td>
<td>121</td>
<td>175</td>
<td>158</td>
<td>157</td>
<td>212</td>
<td>194</td>
<td>193</td>
</tr>
<tr>
<td>139</td>
<td>124</td>
<td>122</td>
<td>176</td>
<td>159</td>
<td>158</td>
<td>213</td>
<td>195</td>
<td>194</td>
</tr>
<tr>
<td>140</td>
<td>125</td>
<td>123</td>
<td>177</td>
<td>160</td>
<td>159</td>
<td>214</td>
<td>196</td>
<td>195</td>
</tr>
<tr>
<td>141</td>
<td>126</td>
<td>124</td>
<td>178</td>
<td>161</td>
<td>160</td>
<td>215</td>
<td>197</td>
<td>196</td>
</tr>
</tbody>
</table>
Table 2.4: Dimensions of binary greedy LT codes

<table>
<thead>
<tr>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
<th>n</th>
<th>d = 5</th>
<th>d = 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>216</td>
<td>198</td>
<td>197</td>
<td>253</td>
<td>235</td>
<td>234</td>
<td>290</td>
<td>271</td>
<td>270</td>
<td>327</td>
<td>308</td>
<td>307</td>
</tr>
<tr>
<td>217</td>
<td>199</td>
<td>198</td>
<td>254</td>
<td>236</td>
<td>235</td>
<td>291</td>
<td>272</td>
<td>271</td>
<td>328</td>
<td>309</td>
<td>308</td>
</tr>
<tr>
<td>218</td>
<td>200</td>
<td>199</td>
<td>255</td>
<td>237</td>
<td>236</td>
<td>292</td>
<td>273</td>
<td>272</td>
<td>329</td>
<td>310</td>
<td>309</td>
</tr>
<tr>
<td>219</td>
<td>201</td>
<td>200</td>
<td>256</td>
<td>238</td>
<td>237</td>
<td>293</td>
<td>274</td>
<td>273</td>
<td>330</td>
<td>311</td>
<td>310</td>
</tr>
<tr>
<td>220</td>
<td>202</td>
<td>201</td>
<td>257</td>
<td>239</td>
<td>238</td>
<td>294</td>
<td>275</td>
<td>274</td>
<td>331</td>
<td>312</td>
<td>311</td>
</tr>
<tr>
<td>221</td>
<td>203</td>
<td>202</td>
<td>258</td>
<td>240</td>
<td>239</td>
<td>295</td>
<td>276</td>
<td>275</td>
<td>332</td>
<td>313</td>
<td>312</td>
</tr>
<tr>
<td>222</td>
<td>204</td>
<td>203</td>
<td>259</td>
<td>241</td>
<td>240</td>
<td>296</td>
<td>277</td>
<td>276</td>
<td>333</td>
<td>314</td>
<td>313</td>
</tr>
<tr>
<td>223</td>
<td>205</td>
<td>204</td>
<td>260</td>
<td>242</td>
<td>241</td>
<td>297</td>
<td>278</td>
<td>277</td>
<td>334</td>
<td>315</td>
<td>314</td>
</tr>
<tr>
<td>224</td>
<td>206</td>
<td>205</td>
<td>261</td>
<td>243</td>
<td>242</td>
<td>298</td>
<td>279</td>
<td>278</td>
<td>335</td>
<td>316</td>
<td>315</td>
</tr>
<tr>
<td>225</td>
<td>207</td>
<td>206</td>
<td>262</td>
<td>244</td>
<td>243</td>
<td>299</td>
<td>280</td>
<td>279</td>
<td>336</td>
<td>317</td>
<td>316</td>
</tr>
<tr>
<td>226</td>
<td>208</td>
<td>207</td>
<td>263</td>
<td>245</td>
<td>244</td>
<td>300</td>
<td>281</td>
<td>280</td>
<td>337</td>
<td>318</td>
<td>317</td>
</tr>
<tr>
<td>227</td>
<td>209</td>
<td>208</td>
<td>264</td>
<td>246</td>
<td>245</td>
<td>301</td>
<td>282</td>
<td>281</td>
<td>338</td>
<td>319</td>
<td>318</td>
</tr>
<tr>
<td>228</td>
<td>210</td>
<td>209</td>
<td>265</td>
<td>247</td>
<td>246</td>
<td>302</td>
<td>283</td>
<td>282</td>
<td>339</td>
<td>320</td>
<td>319</td>
</tr>
<tr>
<td>229</td>
<td>211</td>
<td>210</td>
<td>266</td>
<td>248</td>
<td>247</td>
<td>303</td>
<td>284</td>
<td>283</td>
<td>340</td>
<td>321</td>
<td>320</td>
</tr>
<tr>
<td>230</td>
<td>212</td>
<td>211</td>
<td>267</td>
<td>249</td>
<td>248</td>
<td>304</td>
<td>285</td>
<td>284</td>
<td>341</td>
<td>322</td>
<td>321</td>
</tr>
<tr>
<td>231</td>
<td>213</td>
<td>212</td>
<td>268</td>
<td>249</td>
<td>249</td>
<td>305</td>
<td>286</td>
<td>285</td>
<td>342</td>
<td>323</td>
<td>322</td>
</tr>
<tr>
<td>232</td>
<td>214</td>
<td>213</td>
<td>269</td>
<td>250</td>
<td>249</td>
<td>306</td>
<td>287</td>
<td>286</td>
<td>343</td>
<td>323</td>
<td>323</td>
</tr>
<tr>
<td>233</td>
<td>215</td>
<td>214</td>
<td>270</td>
<td>251</td>
<td>250</td>
<td>307</td>
<td>288</td>
<td>287</td>
<td>344</td>
<td>324</td>
<td>323</td>
</tr>
<tr>
<td>234</td>
<td>216</td>
<td>215</td>
<td>271</td>
<td>252</td>
<td>251</td>
<td>308</td>
<td>289</td>
<td>288</td>
<td>345</td>
<td>325</td>
<td>324</td>
</tr>
<tr>
<td>235</td>
<td>217</td>
<td>216</td>
<td>272</td>
<td>253</td>
<td>252</td>
<td>309</td>
<td>290</td>
<td>289</td>
<td>346</td>
<td>326</td>
<td>325</td>
</tr>
<tr>
<td>236</td>
<td>218</td>
<td>217</td>
<td>273</td>
<td>254</td>
<td>253</td>
<td>310</td>
<td>291</td>
<td>290</td>
<td>347</td>
<td>327</td>
<td>326</td>
</tr>
<tr>
<td>237</td>
<td>219</td>
<td>218</td>
<td>274</td>
<td>255</td>
<td>254</td>
<td>311</td>
<td>292</td>
<td>291</td>
<td>348</td>
<td>328</td>
<td>327</td>
</tr>
<tr>
<td>238</td>
<td>220</td>
<td>219</td>
<td>275</td>
<td>256</td>
<td>255</td>
<td>312</td>
<td>293</td>
<td>292</td>
<td>349</td>
<td>329</td>
<td>328</td>
</tr>
<tr>
<td>239</td>
<td>221</td>
<td>220</td>
<td>276</td>
<td>257</td>
<td>256</td>
<td>313</td>
<td>294</td>
<td>293</td>
<td>350</td>
<td>330</td>
<td>329</td>
</tr>
<tr>
<td>240</td>
<td>222</td>
<td>221</td>
<td>277</td>
<td>258</td>
<td>257</td>
<td>314</td>
<td>295</td>
<td>294</td>
<td>351</td>
<td>331</td>
<td>330</td>
</tr>
<tr>
<td>241</td>
<td>223</td>
<td>222</td>
<td>278</td>
<td>259</td>
<td>258</td>
<td>315</td>
<td>296</td>
<td>295</td>
<td>352</td>
<td>332</td>
<td>331</td>
</tr>
<tr>
<td>242</td>
<td>224</td>
<td>223</td>
<td>279</td>
<td>260</td>
<td>259</td>
<td>316</td>
<td>297</td>
<td>296</td>
<td>353</td>
<td>333</td>
<td>332</td>
</tr>
<tr>
<td>243</td>
<td>225</td>
<td>224</td>
<td>280</td>
<td>261</td>
<td>260</td>
<td>317</td>
<td>298</td>
<td>297</td>
<td>354</td>
<td>334</td>
<td>333</td>
</tr>
<tr>
<td>244</td>
<td>226</td>
<td>225</td>
<td>281</td>
<td>262</td>
<td>261</td>
<td>318</td>
<td>299</td>
<td>298</td>
<td>355</td>
<td>335</td>
<td>334</td>
</tr>
<tr>
<td>245</td>
<td>227</td>
<td>226</td>
<td>282</td>
<td>263</td>
<td>262</td>
<td>319</td>
<td>300</td>
<td>299</td>
<td>356</td>
<td>336</td>
<td>335</td>
</tr>
<tr>
<td>246</td>
<td>228</td>
<td>227</td>
<td>283</td>
<td>264</td>
<td>263</td>
<td>320</td>
<td>301</td>
<td>300</td>
<td>357</td>
<td>337</td>
<td>336</td>
</tr>
<tr>
<td>247</td>
<td>229</td>
<td>228</td>
<td>284</td>
<td>265</td>
<td>264</td>
<td>321</td>
<td>302</td>
<td>301</td>
<td>358</td>
<td>338</td>
<td>337</td>
</tr>
<tr>
<td>248</td>
<td>230</td>
<td>229</td>
<td>285</td>
<td>266</td>
<td>265</td>
<td>322</td>
<td>303</td>
<td>302</td>
<td>359</td>
<td>339</td>
<td>338</td>
</tr>
<tr>
<td>249</td>
<td>231</td>
<td>230</td>
<td>286</td>
<td>267</td>
<td>266</td>
<td>323</td>
<td>304</td>
<td>303</td>
<td>360</td>
<td>340</td>
<td>339</td>
</tr>
<tr>
<td>250</td>
<td>232</td>
<td>231</td>
<td>287</td>
<td>268</td>
<td>267</td>
<td>324</td>
<td>305</td>
<td>304</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>251</td>
<td>233</td>
<td>232</td>
<td>288</td>
<td>269</td>
<td>268</td>
<td>325</td>
<td>306</td>
<td>305</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>252</td>
<td>234</td>
<td>233</td>
<td>289</td>
<td>270</td>
<td>269</td>
<td>326</td>
<td>307</td>
<td>306</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2.5: Dimensions of binary greedy LT codes

<table>
<thead>
<tr>
<th>n</th>
<th>$d = 7$</th>
<th>$d = 8$</th>
<th>$d = 9$</th>
<th>$d = 10$</th>
<th>n</th>
<th>$d = 7$</th>
<th>$d = 8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>2(2)</td>
<td>2(2)</td>
<td>1(1)</td>
<td>1(1)</td>
<td>41</td>
<td>24(25)</td>
<td>23(24)</td>
</tr>
<tr>
<td>13</td>
<td>3(3)</td>
<td>2(2)</td>
<td>1(1)</td>
<td>1(1)</td>
<td>42</td>
<td>25(26)</td>
<td>24(25)</td>
</tr>
<tr>
<td>14</td>
<td>4(4)</td>
<td>3(3)</td>
<td>2(2)</td>
<td>1(1)</td>
<td>43</td>
<td>26(27)</td>
<td>25(26)</td>
</tr>
<tr>
<td>15</td>
<td>5(5)</td>
<td>4(4)</td>
<td>2(2)</td>
<td>2(2)</td>
<td>44</td>
<td>27(28)</td>
<td>26(27)</td>
</tr>
<tr>
<td>16</td>
<td>5(5)</td>
<td>5(5)</td>
<td>2(2)</td>
<td>2(2)</td>
<td>45</td>
<td>28(29)</td>
<td>27(28)</td>
</tr>
<tr>
<td>17</td>
<td>6(6)</td>
<td>5(5)</td>
<td>3(3)</td>
<td>2(2)</td>
<td>46</td>
<td>29(30)</td>
<td>28(29)</td>
</tr>
<tr>
<td>18</td>
<td>7(7)</td>
<td>6(6)</td>
<td>3(3)</td>
<td>3(3)</td>
<td>47</td>
<td>30(31)</td>
<td>29(30)</td>
</tr>
<tr>
<td>19</td>
<td>8(8)</td>
<td>7(7)</td>
<td>4(4)</td>
<td>3(3)</td>
<td>48</td>
<td>31(31)</td>
<td>30(31)</td>
</tr>
<tr>
<td>20</td>
<td>9(9)</td>
<td>8(8)</td>
<td>5(5)</td>
<td>4(4)</td>
<td>49</td>
<td>32(32)</td>
<td>31(31)</td>
</tr>
<tr>
<td>21</td>
<td>10(10)</td>
<td>9(9)</td>
<td>5(5)</td>
<td>5(5)</td>
<td>50</td>
<td>33(33)</td>
<td>32(32)</td>
</tr>
<tr>
<td>22</td>
<td>11(11)</td>
<td>10(10)</td>
<td>6(6)</td>
<td>5(5)</td>
<td>51</td>
<td>34(34)</td>
<td>33(33)</td>
</tr>
<tr>
<td>23</td>
<td>12(12)</td>
<td>11(11)</td>
<td>6(7)</td>
<td>6(6)</td>
<td>52</td>
<td>35(35)</td>
<td>34(34)</td>
</tr>
<tr>
<td>24</td>
<td>12(12)</td>
<td>12(12)</td>
<td>7(7)</td>
<td>6(7)</td>
<td>53</td>
<td>36(36)</td>
<td>35(35)</td>
</tr>
<tr>
<td>25</td>
<td>12(12)</td>
<td>12(12)</td>
<td>8(8)</td>
<td>7(7)</td>
<td>54</td>
<td>37(37)</td>
<td>36(36)</td>
</tr>
<tr>
<td>26</td>
<td>12(12)</td>
<td>12(12)</td>
<td>9(9)</td>
<td>8(8)</td>
<td>55</td>
<td>38(38)</td>
<td>37(37)</td>
</tr>
<tr>
<td>27</td>
<td>13(14)</td>
<td>12(13)</td>
<td>9(10)</td>
<td>9(9)</td>
<td>56</td>
<td>38(39)</td>
<td>38(38)</td>
</tr>
<tr>
<td>28</td>
<td>13(14)</td>
<td>13(14)</td>
<td>10(10)</td>
<td>9(10)</td>
<td>57</td>
<td>39(40)</td>
<td>38(39)</td>
</tr>
<tr>
<td>29</td>
<td>14(15)</td>
<td>13(14)</td>
<td>11(11)</td>
<td>10(10)</td>
<td>58</td>
<td>40(41)</td>
<td>39(40)</td>
</tr>
<tr>
<td>30</td>
<td>15(16)</td>
<td>14(15)</td>
<td>12(12)</td>
<td>11(11)</td>
<td>59</td>
<td>41(42)</td>
<td>40(41)</td>
</tr>
<tr>
<td>31</td>
<td>16(17)</td>
<td>15(16)</td>
<td>12(12)</td>
<td>12(12)</td>
<td>60</td>
<td>41(43)</td>
<td>41(42)</td>
</tr>
<tr>
<td>32</td>
<td>16(17)</td>
<td>16(17)</td>
<td>13(13)</td>
<td>12(12)</td>
<td>61</td>
<td>42(44)</td>
<td>41(43)</td>
</tr>
<tr>
<td>33</td>
<td>17(18)</td>
<td>16(17)</td>
<td>14(14)</td>
<td>13(13)</td>
<td>62</td>
<td>43(45)</td>
<td>42(44)</td>
</tr>
<tr>
<td>34</td>
<td>18(19)</td>
<td>17(18)</td>
<td>14(14)</td>
<td>14(14)</td>
<td>63</td>
<td>44(46)</td>
<td>43(45)</td>
</tr>
<tr>
<td>35</td>
<td>19(20)</td>
<td>18(19)</td>
<td></td>
<td></td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>20(20)</td>
<td>19(20)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>21(21)</td>
<td>20(20)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>22(22)</td>
<td>21(21)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>23(23)</td>
<td>22(22)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>23(24)</td>
<td>23(24)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2.6: Dimensions of ternary greedy LT 2-error codes

<table>
<thead>
<tr>
<th>n</th>
<th>d = 5</th>
<th>n</th>
<th>d = 5</th>
<th>n</th>
<th>d = 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1(1)</td>
<td>27</td>
<td>18(19)</td>
<td>49</td>
<td>39(38)</td>
</tr>
<tr>
<td>6</td>
<td>1(1)</td>
<td>28</td>
<td>19(20)</td>
<td>50</td>
<td>40(39)</td>
</tr>
<tr>
<td>7</td>
<td>2(2)</td>
<td>29</td>
<td>20(21)</td>
<td>51</td>
<td>41</td>
</tr>
<tr>
<td>8</td>
<td>3(3)</td>
<td>30</td>
<td>21(22)</td>
<td>52</td>
<td>42</td>
</tr>
<tr>
<td>9</td>
<td>4(4)</td>
<td>31</td>
<td>22(23)</td>
<td>53</td>
<td>43</td>
</tr>
<tr>
<td>10</td>
<td>5(5)</td>
<td>32</td>
<td>23(24)</td>
<td>54</td>
<td>44</td>
</tr>
<tr>
<td>11</td>
<td>6(6)</td>
<td>33</td>
<td>24(25)</td>
<td>55</td>
<td>45</td>
</tr>
<tr>
<td>12</td>
<td>6(6)</td>
<td>34</td>
<td>25(26)</td>
<td>56</td>
<td>46</td>
</tr>
<tr>
<td>13</td>
<td>6(6)</td>
<td>35</td>
<td>26(27)</td>
<td>57</td>
<td>47</td>
</tr>
<tr>
<td>14</td>
<td>6(7)</td>
<td>36</td>
<td>27(28)</td>
<td>58</td>
<td>48</td>
</tr>
<tr>
<td>15</td>
<td>8(8)</td>
<td>37</td>
<td>28(29)</td>
<td>59</td>
<td>49</td>
</tr>
<tr>
<td>16</td>
<td>8(9)</td>
<td>38</td>
<td>29(30)</td>
<td>60</td>
<td>50</td>
</tr>
<tr>
<td>17</td>
<td>9(10)</td>
<td>39</td>
<td>30(31)</td>
<td>61</td>
<td>51</td>
</tr>
<tr>
<td>18</td>
<td>10(11)</td>
<td>40</td>
<td>31(32)</td>
<td>62</td>
<td>52</td>
</tr>
<tr>
<td>19</td>
<td>11(12)</td>
<td>41</td>
<td>32(33)</td>
<td>63</td>
<td>53</td>
</tr>
<tr>
<td>20</td>
<td>12(13)</td>
<td>42</td>
<td>33(33)</td>
<td>64</td>
<td>54</td>
</tr>
<tr>
<td>21</td>
<td>13(14)</td>
<td>43</td>
<td>34(33)</td>
<td>65</td>
<td>55</td>
</tr>
<tr>
<td>22</td>
<td>14(15)</td>
<td>44</td>
<td>35(33)</td>
<td>66</td>
<td>56</td>
</tr>
<tr>
<td>23</td>
<td>15(16)</td>
<td>45</td>
<td>36(34)</td>
<td>67</td>
<td>57</td>
</tr>
<tr>
<td>24</td>
<td>16(17)</td>
<td>46</td>
<td>37(35)</td>
<td>68</td>
<td>58</td>
</tr>
<tr>
<td>25</td>
<td>16(18)</td>
<td>47</td>
<td>37(36)</td>
<td>69</td>
<td>59</td>
</tr>
<tr>
<td>26</td>
<td>17(19)</td>
<td>48</td>
<td>38(37)</td>
<td>70</td>
<td>60</td>
</tr>
</tbody>
</table>

Note: numbers inside ( ) are data from Kschischang and Pasupathy in IEEE 1992
References


CHAPTER 3. A DISCRETE TRANSFORM AND FUNCTION 
SPACES ON THE QUADRATIC CLOSURE OF GF(2)

A paper submitted for publication 
to Discrete Mathematics Feng-Luan Hsu and Jonathan D. H. Smith

Abstract

The construction of syndrome functions for binary error-correcting codes using greedy algorithms yields sequences of linear endomorphisms of Galois fields that are successive quadratic extensions of the two-element field. As part of the analysis of such endomorphisms, this paper introduces and studies a linear transform of them, analogous to the discrete Fourier transform. Although the matrices of the transforms are non-sparse and increase in size exponentially, they can all be inverted explicitly. The inverse transform matrices have a fractal structure, including the Sierpiński triangle in their first row. The paper uses the transform to analyze certain spaces of natural number functions that include the syndromes of the codes. Transforms of functions in these spaces exhibit a martingale property.

\footnote{Graduate student and Professor, respectively, Department of Mathematics, Iowa State University.}
Introduction

A general "loop transversal" approach to the construction of linear block codes was introduced in [Sm]. A subsequent paper [HS] gives further details, concentrating on the greedy loop transversal algorithm in the binary case. The greedy algorithm was used in [HHS] to construct syndrome functions of binary lexicodes up to high dimensionalities. The graphs of the syndrome functions turn out to have curious fractal properties. As part of an on-going program investigating these functions, we consider them as polynomials in subfields of the quadratic closure of GF(2). Passing from such a polynomial function to its coefficient sequence provides a linear transform, analogous to the discrete Fourier transform. Despite the exponentially increasing sizes of the transform matrices, they may be inverted explicitly. The current paper is devoted to a detailed analysis of the transform.

It proves convenient to identify the quadratic closure of GF(2) with the (ordered) set N of natural numbers. Thus N becomes a subfield of the Field On$_2$ introduced by Conway [Co, Chapter 6] [Le], and the finite field GF(2$^n$) becomes \{n \in N | n < 2^n \}. Note that \{2^0, 2^1, \ldots, 2^{2n} \} is a basis of the GF(2)-space GF(2$^n$). Moreover, the GF(2)-endomorphisms $x \mapsto x^2$, $x \mapsto x^{2^1}$, \ldots, $x \mapsto x^{2^{2n-1}}$ are linearly independent in the GF(2$^n$)-space of functions GF(2$^n$) \rightarrow GF(2$^n$). Thus a GF(2)-linear function $h : GF(2^n) \rightarrow GF(2^n)$ can be written in the form

$$h(x) = a_{n,0}x^{2^0} + a_{n,1}x^{2^1} + a_{n,2}x^{2^2} + \ldots + a_{n,2n-1}x^{2^{2n-1}}$$

$$= (x^{2^0}, x^{2^1}, x^{2^2}, \ldots, x^{2^{2n-1}})(a_{n,0}, a_{n,1}, a_{n,2}, \ldots, a_{n,2n-1})^T.$$

To describe such a linear function $h(x)$, one only needs to look at the function values
\[ h(2^i), \text{ for } 0 \leq i \leq 2^n - 1. \] So we have

\[
\begin{bmatrix}
(2^0)^{2^0} & (2^0)^{2^1} & \ldots & (2^0)^{2^{2^n-1}} \\
(2^1)^{2^0} & (2^1)^{2^1} & \ldots & (2^1)^{2^{2^n-1}} \\
\vdots & \vdots & \ddots & \vdots \\
(2^{2^n-1})^{2^0} & (2^{2^n-1})^{2^1} & \ldots & (2^{2^n-1})^{2^{2^n-1}}
\end{bmatrix}
\begin{bmatrix}
an_{0,0} \\
an_{1,0} \\
an_{1,1} \\
an_{2^n-1,0}
\end{bmatrix}
= 
\begin{bmatrix}
h(2^0) \\
h(2^1) \\
h(2^2) \\
h(2^{2^n-1})
\end{bmatrix}.
\]

Now, multiplying both sides of the equation by the inverse \( f_n^{-1} \) of the \( 2^n \times 2^n \) matrix \( f_n \) on the left, one obtains the function values of a new linear function \( \tilde{h} : \)

\[ \begin{bmatrix}
\tilde{h}(2^0), \tilde{h}(2^1), \tilde{h}(2^2), \ldots, \tilde{h}(2^{2^n-1})
\end{bmatrix}^T = 
\begin{bmatrix}
a_{n,0}, a_{n,1}, a_{n,2}, \ldots, a_{n,2^n-1}
\end{bmatrix}^T.
\]

\[ = 
\begin{bmatrix}
(2^0)^{2^0} & (2^0)^{2^1} & (2^0)^{2^2} & \ldots & (2^0)^{2^{2^n-1}} \\
(2^1)^{2^0} & (2^1)^{2^1} & (2^1)^{2^2} & \ldots & (2^1)^{2^{2^n-1}} \\
(2^2)^{2^0} & (2^2)^{2^1} & (2^2)^{2^2} & \ldots & (2^2)^{2^{2^n-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
(2^{2^n-1})^{2^0} & (2^{2^n-1})^{2^1} & (2^{2^n-1})^{2^2} & \ldots & (2^{2^n-1})^{2^{2^n-1}}
\end{bmatrix}
\begin{bmatrix}
h(2^0) \\
h(2^1) \\
h(2^2) \\
h(2^{2^n-1})
\end{bmatrix}^{-1} = 
\begin{bmatrix}
h(2^0) \\
h(2^1) \\
h(2^2) \\
h(2^{2^n-1})
\end{bmatrix}.
\]

\[ = f_n^{-1}[h(2^0), h(2^1), h(2^2), \ldots, h(2^{2^n-1})]^T .
\]

Passing from the linear function \( h \) to the linear function \( \tilde{h} \) provides the \( 2^n \)-dimensional linear transform, an analogue of the discrete Fourier transform. For example, the field \( GF(2^{16}) \) becomes \( \{ n \in \mathbb{N} | n < 2^{16} \} \). Using hexadecimal notation for these numbers, Table 3.1 displays the \( 16 \times 16 \) transform matrix \( f_4 \). Note that the number in the \((i + 1, j)\)-entry is the square of the number in the \((i, j)\)-entry, for \( 1 \leq i \leq 15, 1 \leq j \leq 16 \). Here the square is taken in \( GF(2^{16}) \). So it will be enough to construct the whole matrix if we know the entries \((1, j)\), for \( 1 \leq j \leq 16 \), i.e. the first row of the matrix. In Table 3.2 , we transform the numbers in the first row of the matrix into
binary format, and transpose the row to a column. Observe that the numbers form a Sierpiński triangle, i.e. Pascal’s Triangle modulo 2. For any n, we have similar results. If we denote the rows of Pascal’s Triangle modulo 2, namely 1, 3, 5, F, 11, 33, 55, ... (in hexadecimal format), by $P_0 = 1$, $P_1 = 3$, $P_3 = 5$, ..., then we have $f^{-1}_n$ of the form

$$
\begin{bmatrix}
  P_{2^n-1} & P_{2^n-2} & P_{2^n-3} & \ldots & P_0 \\
  P_{2^n-1}\varphi & P_{2^n-2}\varphi & P_{2^n-3}\varphi & \ldots & P_0\varphi \\
  P_{2^n-1}\varphi^2 & P_{2^n-2}\varphi^2 & P_{2^n-3}\varphi^2 & \ldots & P_0\varphi^2 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  P_{2^n-1}\varphi^{2^n-1} & P_{2^n-2}\varphi^{2^n-1} & P_{2^n-3}\varphi^{2^n-1} & \ldots & P_0\varphi^{2^n-1}
\end{bmatrix},
$$

where $x\varphi^k = x^{2^k}$ for each $n > 0$.

In Section 2, we describe the order and field structure on $\mathbb{N}$. In Section 3, we discuss relevant properties of Pascal’s Triangle modulo 2. The structure of the inverse transform matrix is determined in Section 4 and Section 5. In Section 6, we examine subspaces of the GF(2)-space $\prod_{i=0}^{\infty} \text{End GF}(2^{2^n})$ defined by certain properties of their elements, namely coherence, smallness, the nesting property and the martingale property. These properties are displayed by the syndrome functions of binary lexicodes. We show that the martingale property is equivalent to coherence, and that the smallness, coherence and nesting properties are independent of each other. The final section completes the investigation of the relationship between these properties.

**Order and field structures on $\mathbb{N}$**

For $k \in \mathbb{N}$, write $k = \sum_{i=0}^{\infty} k_i 2^i$ with $k_i \in \{0, 1\}$. Then we have a bijection $\mathbb{N} \rightarrow \prod_{i=0}^{\infty} \text{GF}(2); k \mapsto \sum_{i=0}^{\infty} k_i$. Using this bijection, we can make $\mathbb{N}$ a GF(2)-space.
The induced addition on \( \mathbb{N} \) is called *nim addition* (to contrast with the usual addition on \( \mathbb{N} \)), because of its role in the analysis of the game of Nim [Co, Chapter 11]. In this paper, we will use \( \sum \) and \(+\) for nim addition and use \(-\) for ordinary subtraction. Note that the ordinary addition can always be written in terms of subtraction. For example, the ordinary sum of \( a \) and \( b \) will be represented by \( a - (-b) \).

Let \( (\mathbb{N}, \leq) \) be the usual linear order on the natural numbers. For \( a, b \in \mathbb{N} \), we then use the following “interval” notations: “open” \( (a, b) := \{n \in \mathbb{N} | a < n < b \} \), “closed above” \( [a, b] := \{n \in \mathbb{N} | a < n \leq b \} \), “closed below” \( [a, b) := \{n \in \mathbb{N} | a < n < b \} \), “closed” \( [a, b] := \{n \in \mathbb{N} | a \leq n \leq b \} \). Occasionally, it is convenient to identify \( b \) with \( (0, b) \), e.g. writing \( GF(2) = 0, 1 \) simply as 2.

The essential property of nim addition which we need is that for any three natural numbers \( a, \beta, \gamma \), with \( \gamma < a + \beta \), there exists \( \alpha' < a \) with \( \alpha' + \beta = \gamma \) or \( \beta' < \beta \) with \( \alpha + \beta' = \gamma \). Since for \( \alpha' \neq \alpha \), \( \beta' \neq \beta \), we have \( \alpha' + \beta \neq \alpha + \beta \neq \alpha + \beta' \), it follows that

\[
\alpha + \beta \text{ is the smallest natural number different from all natural numbers } \alpha' + \beta \text{ with } \alpha' < \alpha \text{ and from all } \alpha + \beta' \text{ with } \beta' < \beta. \tag{3.1}
\]

It was noticed by Conway that this property may in fact be taken as a recursive definition of nim addition. As Conway remarks, nim addition is in a sense the “simplest” addition making the natural numbers into a group. The same thing happens for the binary operation \(*\) known as *nim multiplication*. The basic inequality to be used here expresses the absence of zero-divisors, i.e. \( (a + a')*(\beta + \beta') \neq 0 \), for \( a \neq a', \beta \neq \beta' \). So \( a * \beta \neq a' * \beta + a * \beta' + a' * \beta' \). This leads to the following definition of nim
multiplication, due to Conway:

\[ \alpha \ast \beta \text{ is the smallest natural number different from all natural numbers} \]

\[ (\alpha' \ast \beta) + (\alpha \ast \beta') + (\alpha' \ast \beta') \text{ with } \alpha' < \alpha, \text{ and } \beta' < \beta. \quad (3.2) \]

Efficient algorithms to aid in the computation of the nim sum \( x + y \) and the nim product \( x \ast y \) of two natural numbers \( x, y \) are as follows:

if \( x = y \) then \( x + y = 0 \) else

if \( \exists n \in \mathbb{N}. \ y < x = 2^n \) then

\( x + y \) is the ordinary sum of \( x \) and \( y \).

if \( \exists n \in \mathbb{N}. \ x = 2^n \) then

if \( x = y \) then \( x \ast y \) is the ordinary product of \( x \) and \( x \)
else if \( y < x \) then \( x \ast y \) is the ordinary product of \( x \) and \( x \).

The algorithms are complemented by the distributive laws. As an example of the use of the algorithms, one obtains \( 2^{2n+k} = 2^{2n} \ast 2^k \) for \( k < 2^n \).

Theorem 3.1 [Co. Theorem 49] The set \( \mathbb{N} \) of natural numbers, with nim addition and nim multiplication, is a quadratically closed field of characteristic 2, the quadratic closure of \( GF(2) \).

In this paper, we will write \( \prod_{i=0}^{r} a_i \) for the iterated nim product \( a_0 \ast a_1 \ast \ldots \ast a_r \).
We also set \( \alpha_n = 2^{2^n} \) and \( \beta_n = \prod_{i=1}^{n-1} \alpha_i \). Note \( GF(\alpha_0) < GF(\alpha_1) < GF(\alpha_2) < \ldots \), and \( \mathbb{N} = \bigcup_{i \geq 0} GF(\alpha_i) \). Also, \( \alpha_i \) satisfies the equation

\[ x_i^2 + x_i + \prod_{j < i} \alpha_j = x_i^2 + x_i + \beta_{i-1} = 0. \quad (3.5) \]
so that \( GF(\alpha_i) \) is the quadratic extension \( GF(\alpha_{i-1})[\alpha_i] \).
Proposition 3.2 The map \( \varphi : (\mathbb{N}, +, \ast) \rightarrow (\mathbb{N}, +, \ast); \ a \mapsto a^2 \) is an automorphism of the field \( \mathbb{N} \).

PROOF. Let \( a \) and \( b \) be natural numbers. Then :

1. \((a + b)\varphi = (a + b)^2 = a^2 + a \ast b + a \ast b + b^2 = a^2 + b^2 = a \varphi + b \varphi; \)

2. \((a \ast b)\varphi = (a \ast b)^2 = (a \ast b) \ast (a \ast b) = (a \ast a) \ast (b \ast b) = a^2 \ast b^2 = a \varphi \ast b \varphi; \)

3. If \( a^2 = b^2 \), then \( a^2 + b^2 = 0 \Rightarrow (a + b)^2 = 0 \Rightarrow a + b = 0 \Rightarrow a = b, \varphi \) injects;

4. For any subfield \( \text{GF}(\alpha_n) \), consider \( \varphi_n : (\text{GF}(\alpha_n), +, \ast) \rightarrow (\text{GF}(\alpha_n), +, \ast); a \mapsto a^2 \). The cardinality of the domain and codomain is \(|\text{GF}(\alpha_n)| = 2^{2n} < \infty \). Since \( \varphi_n \) injects, it also surjects. Thus \( \varphi \) surjects.\( \square \)

The automorphism \( \varphi \) of \( \mathbb{N} \) is called the Frobenius automorphism.

Let \( K \) be a field, and let \( A \) be a finite-dimensional algebra over \( K \). Let \( t \) be an element of \( A \) with characteristic polynomial \( p(x) \). The trace \( \text{Tr}_K(t) \) of \( t \) over \( K \) is the negative of the coefficient of \( x^{(\deg p) - 1} \) in \( p(x) \). Now, let \( K = \text{GF}(\alpha_{n-1}) \) and \( A = \text{GF}(\alpha_n) \). For \( a \in \text{GF}(\alpha_n) \), we can write \( a = a_1 \ast \alpha_{n-1} + a_2 \) with \( a_i \in [0, \alpha_{n-1}) \). Now \( a^2 = (a_1 \ast \alpha_{n-1} + a_2)^2 = a_1^2 \ast \alpha_{n-1}^2 + a_2^2 = a_1^2 \ast (\alpha_{n-1} + \beta_{n-1}) + a_2^2 = a_1 \ast (a_1 \ast \alpha_{n-1}) + a_1^2 \ast \beta_{n-1} + a_2^2 = a_1 \ast \alpha_{n-1} + a_1 \ast \alpha_{n-1} \ast a_2 + a_1 \ast \beta_{n-1} + a_2^2 = a_1 \ast \alpha_{n-1} + a_1 \ast a_2 + a_1 \ast \beta_{n-1} + a_2^2, \) so the characteristic polynomial of \( a \in \text{GF}(\alpha_n) \) is \( x^2 + a_1 \ast x + a_1 \ast a_2 + a_1 \ast \beta_{n-1} + a_2^2 \).

The coefficient of \( x \) here, viz. \( \text{Tr}_{\alpha_{n-1}}(a) \), is \( a_1 \). Summarizing,

Lemma 3.3 [Le2] If \( a \in \text{GF}(\alpha_n) \), and we write \( a = a_1 \ast \alpha_{n-1} + a_2 \), for \( 0 \leq a_1, a_2 < \alpha_{n-1} \), then \( \text{Tr}_{\alpha_{n-1}}(a) = a_1.\square \)

Lemma 3.4 If \( x < \alpha_n \), then \( x \varphi^2 = x^{\alpha_n} = x. \)
PROOF. If \( x < \alpha_n \), then \( x \in GF(\alpha_n) \). Certainly, \( 0 \varphi^{2^n} = 0^{\alpha_n} = 0 \). Otherwise, \( x \) is an element of the cyclic group \( (GF(\alpha_n)^*, *, 1) \) of order \( \alpha_n - 1 \). So \( x \varphi^{2^n} = x^{\alpha_n} = x \), as required. □

Lemma 3.5 \( \beta_n = 2^{2^n-1} \).

PROOF. One has \( \beta_n = \prod_{i=0}^{2^n-1} \alpha_i = 2^{2^0} \cdot 2^{2^1} \cdot \ldots \cdot 2^{2^{n-1}} = 2^{2^0 + 2^1 + \ldots + 2^{n-1}} = 2^{\frac{2^n - 1}{2 - 1}} = 2^{2^n - 1} \). □

Lemma 3.6 \( \beta_n = \beta_{n-1} \cdot \alpha_{n-1} \).

PROOF. \( \beta_n = 2^{2^n-1} = 2^{2^{n-1} - (-2^{n-1}) - 1} = 2^{2^{n-1} + (2^{n-1} - 1)} = 2^{2^{n-1} - 2^{n-1} - 1} = \alpha_{n-1} \cdot \beta_{n-1} \). □

Lemma 3.7

\[
\alpha_n \varphi^k = \alpha_n + \sum_{i=0}^{k-1} \beta_n \varphi^i
\]  \hspace{1cm} (3.6)

for \( n \geq 0 \) and \( k \geq 1 \).

PROOF. By induction on \( k \). For \( k = 1 \), (3.6) reduces to \( \alpha_n \varphi = \alpha_n + \beta_n \), which holds by (3.5). Now assume (3.6) is true for \( m < k \). Then \( \alpha_n \varphi^k = (\alpha_n + \beta_n) \varphi^{k-1} = \alpha_n \varphi^{k-1} + \beta_n \varphi^{k-1} = (\alpha_n + \sum_{i=0}^{k-2} \beta_n \varphi^i) + \beta_n \varphi^{k-1} = \alpha_n + \sum_{i=0}^{k-1} \beta_n \varphi^i \), as required. □

Lemma 3.8 (Cf. [Co2, p.234]).

\[
\alpha_n^{2^n} = \alpha_n \varphi^{2^n} = \alpha_n + 1.
\]  \hspace{1cm} (3.7)
PROOF. By induction on $n$. If $n = 0$, then $\alpha_0 = 2^0 = 2$, whence $\alpha_0^\alpha = 2^2 = 3 = 2+1 = \alpha_0 + 1$, and (3.7) holds. Now assume that $\alpha_k^\alpha = \alpha_k \varphi^{2^k} = \alpha_k + 1$, for $k < n$. We want to show that $\alpha_n^\alpha = \alpha_n \varphi^{2^n} = \alpha_n + 1$. Note that $\alpha_n^\alpha = \alpha_n \varphi^{2^n} = \alpha_n + \sum_{i=0}^{2^n-1} \beta_n \varphi^i$, by Lemma 3.7.

Now, we need to show that $\sum_{i=0}^{2^n-1} \beta_n \varphi^i = 1$. Actually, we are going to prove

$$\sum_{i=0}^{2^n-1} \beta_n \varphi^i = 1 \quad (3.8)$$

for $m \leq n$, by induction on $m$. If $m = 0$, then (3.8) reduces to $2^{2^0-1} = 2^0 = 1$. Assume (3.8) is true for $m < n$. Then by Lemma 3.6, $\sum_{i=0}^{2^n-1} \beta_n \varphi^i = \sum_{i=0}^{2^n-1} (\alpha_n^{-1} \beta_n^{-1} \varphi^i)$

$$= \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i + \sum_{i=2^n-1}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i$$

$$= \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i + \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^{i+2^n-1} \beta_n^{-1} \varphi^{i+2^n-1}$$

$$= \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i + \sum_{i=0}^{2^n-1} (\alpha_n^{-1} \varphi^{2^n-1}) \beta_n^{-1} \varphi^{2^n-1} \varphi^i$$

$$= \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i + \sum_{i=0}^{2^n-1} (\alpha_n^{-1} + 1) \varphi^i \beta_n^{-1} \varphi^i$$

$$= \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i + \sum_{i=0}^{2^n-1} \alpha_n^{-1} \varphi^i \beta_n^{-1} \varphi^i$$

$$+ \sum_{i=0}^{2^n-1} 1 \varphi^i \beta_n^{-1} \varphi^i$$

$$= \sum_{i=0}^{2^n-1} \beta_n^{-1} \varphi^i = 1$$

the third from last equality holding by Lemma 3.4.

So we have proved $\sum_{i=0}^{2^n-1} \beta_n \varphi^i = 1$, and therefore the Lemma. □

Lemma 3.9 Define $A_n : GF(\alpha_n) \to GF(\alpha_n)$; $x \mapsto \sum_{i=0}^{2^n-1} x \varphi^i$. Then for $0 \leq x < \beta_n$.

$$A_n(x) = 0. \quad (3.9)$$
Moreover, $A_n(x) = \prod_{0 \leq i < \beta_n} (x + i)$.

PROOF. First, note that $A_n$ is linear, because of the linearity of $\varphi$. The result will be proved by induction on $n$. If $n = 0$, we have $A_0(x) = x = 0$, so 0 is the only root and (3.9) is true for $n = 0$. Assume $A_k(x) = \sum_{i=0}^{2^k-1} x \varphi^i = 0$, for $0 \leq x < \beta_k$, and $0 \leq k < n$.

We want to show (3.9) is true for $k = n$. Since $[0, \beta_n) = [0, \alpha_{n-1}) \cup [\alpha_{n-1}, \beta_n)$, we have the following 2 cases:

Case(1) : $x \in GF(\alpha_{n-1})$. Here $A_n(x) = \sum_{i=0}^{2^n-1} x \varphi^i = \sum_{i=0}^{2^n-1} x \varphi^i + \sum_{i=2^n-1}^{2^{n-1}-1} x \varphi^i = \sum_{i=0}^{2^{n-1}-1} x \varphi^i + \sum_{i=0}^{2^{n-1}-1} x \varphi^{i+2^n-1} = \sum_{i=0}^{2^{n-1}-1} x \varphi^i + \sum_{i=0}^{2^{n-1}-1} (x \varphi^{2^n-1}) \varphi^i = \sum_{i=0}^{2^{n-1}-1} x \varphi^i + \sum_{i=0}^{2^{n-1}-1} x \varphi^i = 0$, as required.

Case(2) : $x \in GF(\alpha_n) \setminus GF(\alpha_{n-1})$, and $x < \beta_n$. Note that $x$ can be written as $x = x_1 \ast \alpha_{n-1} + x_2$, where $x_2 \in GF(\alpha_{n-1})$ and $1 \leq x_1 < \beta_{n-1}$. So $A_n(x) = A_n(x_1 \ast \alpha_{n-1} + x_2) = A_n(x_1 \ast \alpha_{n-1}) + A_n(x_2) = A_n(x_1 \ast \alpha_{n-1})$.

$$= \sum_{i=0}^{2^n-1} (x_1 \ast \alpha_{n-1}) \varphi^i$$

$$= \sum_{i=0}^{2^n-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=2^n-1}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i$$

$$= \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^{i+2^n-1}$$

$$= \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=0}^{2^{n-1}-1} ((x_1 \ast \alpha_{n-1}) \varphi^{2^n-1}) \varphi^i$$

$$= \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 \varphi^{2^n-1} \ast \alpha_{n-1} \varphi^{2^n-1}) \varphi^i$$

$$= \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 \ast (\alpha_{n-1} + 1)) \varphi^i$$

$$= \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=0}^{2^{n-1}-1} (x_1 \ast \alpha_{n-1}) \varphi^i + \sum_{i=0}^{2^{n-1}-1} x_1 \varphi^i$$
\[ 35 \]

Finally, since \( \text{deg}(A_n(x)) = \beta_n \) and \( A_n(x) = 0 \) for \( 0 \leq x < \beta_n \), the interval \([0, \beta_n)\) is a full set of roots of \( A_n(x) \), i.e. \( A_n(x) = \prod_{0 \leq i < \beta_n} (x + i) \). □

**Lemma 3.10** For \( \beta_n \leq x < \alpha_n \), \( A_n(x) = 1 \). Moreover, \( A_n(x) = 1 + \prod_{\beta_n \leq i < \alpha_n} (x + i) \).

**PROOF.** First, observe that \( A_n(x) \) is invariant under \( \varphi \) over \( \text{GF}(\alpha_n) \), i.e. \( A_n(x)\varphi = A_n(x)^2 = A_n(x) \). So \( A_n(x) = 1 \) or \( 0 \), for \( x \in \text{GF}(\alpha_n) \). Now by Lemma 3.9, we have \( A_n(x) = 0 \), for \( 0 \leq x < \beta_n \). So for \( x \in [0, \alpha_n) - [0, \beta_n) \), i.e. for \( \beta_n \leq x < \alpha_n \), we have \( A_n(x) = 1 \). Similarly, since \( \text{deg}(A_n(x)) = \beta_n \), we have found all the roots of \( A_n(x) = 1 \), i.e. \( A_n(x) + 1 = \prod_{\beta_n \leq i < \alpha_n} (x + i) \). Thus \( A_n(x) = 1 + \prod_{\beta_n \leq i < \alpha_n} (x + i) \), as required. □

**Corollary 3.11** \( \prod_{1 \leq i < \beta_n} i = 1 \), \( \prod_{\beta_n \leq i < \alpha_n} i = 1 \), and \( \prod_{1 \leq i < \alpha_n} i = 1 \).

**PROOF.** By Lemma 3.9, note that \( x(x + 1)(x + 2)...(x + \beta_n - 1) = \sum_{i=0}^{2^n-1} x^i = \sum_{i=0}^{2^n-1} x^{2i} = x + x^2 + x^4 + ... + x^{\beta_n} = x(1 + x + x^2 + ... + x^{\beta_n - 1}) \). So \( (x + 1)(x + 2)...(x + \beta_n - 1) = 1 + x + x^3 + ... + x^{\beta_n - 1} \). Since the leading coefficient on both sides is equal to 1, the product of all the roots on each side is equal to the constant term. Hence we have \( \prod_{1 \leq i < \beta_n} i = 1 \). Now by Lemma 3.10, note that \( (x + \beta_n)(x + \beta_n + 1)(x + \beta_n + 2)...(x + \alpha_n - 1) = 1 + \sum_{i=0}^{2^n-1} x^i = 1 + \sum_{i=0}^{2^n-1} x^{2i} = 1 + x + x^2 + x^4 + ... + x^{\beta_n} \). So \( (x + \beta_n)(x + \beta_n + 1)(x + \beta_n + 2)...(x + \alpha_n - 1) = 1 + x + x^2 + x^4 + ... + x^{\beta_n} \). Since the leading coefficient on both sides is equal to 1, the product of all the roots on each side is equal to the constant term. Hence we have \( \prod_{\beta_n \leq i < \alpha_n} i = 1 \). The final equation \( \prod_{1 \leq i < \alpha_n} i = 1 \) follows from the previous 2 equations. □
Pascal’s Triangle and the Sierpiński triangle

Table 3.2 displays the first few rows of Pascal’s Triangle modulo 2, a pattern also known as the Sierpiński triangle. Reading the rows of the triangle as binary representations of positive integers, denote them by $P_0 = 1$, $P_1 = 3$, $P_3 = 5$, etc.

**Lemma 3.12** $P_{2^n} = 2^{2^n} + 1$, while $P_{2^n+i} = P_i \cdot P_{2^n}$ for $1 \leq i < 2^n$.

**Proof.** Note that the $k$th row of Pascal’s Triangle modulo 2 is determined by the coefficients of $(x + 1)^k$, i.e. if we denote the coefficient of $x^n$ in $(x + 1)^k$ by $k_n$, then $P_k = \sum_{i=0}^{k} k_i \cdot 2^i$. So to compute $P_{2^n}$, we expand $(x + 1)^{2^n}$, which is equal to $x^{2^n} + 1$. Thus $P_{2^n} = 2^{2^n} + 1$. Now to compute $P_{2^n+i}$ for $1 \leq i < 2^n$, we expand $(x + 1)^{2^n+i}$ which is equal to $(x + 1)^{2^n} \cdot (x + 1)^i = (x^{2^n} + 1) \cdot (x + 1)^i = (x + 1)^i \cdot x^{2^n} + (x + 1)^i$.

So $P_{2^n+i} = P_i \cdot 2^{2^n} + P_i = (2^n + 1) \cdot P_i = P_{2^n} \cdot P_i$. □

**Corollary 3.13** For $1 \leq i < 2^{n-1}$,

$$P_{2^n-i} = P_{2^{n-1-i}} \cdot \alpha_{n-1} + P_{2^n-1-i}.$$  \hspace{1cm} (3.10)

**Proof.**

$P_{2^n-i} = P_{(2^{n-1}-(2^{n-1}-i))}-i = P_{2^{n-1}+(2^{n-1}-i)} = P_{2^n-1} \cdot P_{2^n-1-i}$

$= P_{2^n-1-i} \cdot \alpha_{n-1} + P_{2^n-1-i}$. □

**Corollary 3.14** For $1 \leq i < 2^{n-1}$,

$$P_{2^n-i} \varphi^j = P_{2^n-1-i} \varphi^j \cdot \alpha_{n-1} + P_{2^n-1-i} \sum_{k=0}^{j-1} \beta_{n-1} \varphi^k + P_{2^n-1-i} \varphi^j.$$  \hspace{1cm} (3.12)

**Proof.**

$P_{2^n-i} \varphi^j = (P_{2^n-1-i} \cdot \alpha_{n-1} + P_{2^n-1-i}) \varphi^j = P_{2^n-1-i} \varphi^j \cdot \alpha_{n-1} \varphi^j + P_{2^n-1-i} \varphi^j$

$= P_{2^n-1-i} \varphi^j + (P_{2^n-1-i} + \sum_{k=0}^{j-1} \beta_{n-1} \varphi^k) + P_{2^n-1-i} \varphi^j = P_{2^n-1-i} \varphi^j \cdot \alpha_{n-1} + P_{2^n-1-i} \beta_{n-1} \varphi^j + P_{2^n-1-i} \varphi^j$. The penultimate equality here follows by Lemma 3.7. □
Corollary 3.15 For $0 < k < 2^n$, if we write $k = \sum_{i=0}^{\infty} k_i \cdot 2^i$, with $k_i \in \{0,1\}$, then $P_k = \prod\{P_{2^i}|k_i = 1\}$.

**Proof.** Since $0 < k < 2^n$, there exists $m \leq n$ such that $2^{m-1} \leq k < 2^m$. We now prove the corollary by induction on $m$. If $m = 1$, then $k = 1$. So $k_0 = 1$, and $k_i = 0$ for $i \neq 0$. Then $\prod\{P_{2^i}|k_i = 1\} = P_2 = P$, so the equality holds for $m = 1$.

Now assume the equality for $2^{m-1} \leq k < 2^m$. We want to show that it holds for $2^m \leq k < 2^{m+1}$ too. If $2^m \leq k < 2^{m+1}$, then we can write $k = 2^m + a$, for some $a < 2^m$. Now we write $a = \sum_{i=0}^{\infty} a_i \cdot 2^i$, where $a_i \in \{0,1\}$ for $i \leq m-1$, and $a_i = 0$ for $i > m$. So $k = \sum_{i=0}^{\infty} k_i \cdot 2^i$ with $k_i = a_i$ for $0 \leq i \leq m-1, k_m = 1$, and $k_i = 0$ for $i > m$. By the induction hypothesis, we then have $P_a = \prod\{P_{2^i}|a_i = 1\}$, so $P_k = P_{2^m+a} = P_{2^m} \cdot P_a = P_{2^m} \cdot \prod\{P_{2^i}|a_i = 1\} = \prod\{P_{2^i}|k_i = 1\}$, as required. \(\square\)

**The transform and its inverse**

In this section and the next, we show the general method for constructing the inverse $f_n^{-1}$ of the transform matrix $f_n$ defined in (3.11). In this section, we will show that the $(i+1,j)$-th entry in $f_n^{-1}$ is the square of the $(i,j)$-th entry in $f_n^{-1}$, for $1 \leq i < 2^n, 1 \leq j < 2^n$. Thus, for the construction of $f_n^{-1}$, it suffices to determine the numbers in the first row of $f_n^{-1}$. In the next section, we show that the numbers in the first row of $f_n^{-1}$ turn out to be the rows of Pascal's Triangle modulo 2 (Theorem 3.34).

Let $f_n = f_n(1,2,\ldots,2^{2^n-1})$ be the $2^n \times 2^n$ matrix with entries given by

$$[f_n]_{i,j} = 2^{i-1} \varphi^{j-1}. \quad (3.11)$$
It is convenient to set up special notation for some other matrices. Let $A_n$ be the $(2^n - 1) \times (2^n - 1)$ matrix with entries given by

$$[A_n]_{i,j} = 2^{i-1} \varphi^j. \quad (3.12)$$

Let $B_n$ be the $(2^n - 1) \times 1$ matrix with entries given by

$$[B_n]_{i,1} = 2^{2^n - 1} \varphi^i. \quad (3.13)$$

Let $X_n$ be the $(2^n - 1) \times 1$ matrix with entries given by

$$[X_n]_{i,1} = P_{2^n-i}. \quad (3.14)$$

Let $C_n$ be the $(2^n - 1) \times 1$ matrix with entries given by

$$[C_n]_{i,1} = 2^{i-1}. \quad (3.15)$$

Let $d_{(a,b,n)}$ be the $(b - (a - 1)) \times 1$ matrix with entries given by

$$[d_{(a,b,n)}]_{i,1} = \alpha_n \varphi^{a-(-i)-1}. \quad (3.16)$$

Let $D_{(a,b,n)}$ be the $(b - (a - 1)) \times (b - (a - 1))$ matrix with entries given by

$$[D_{(a,b,n)}]_{i,j} = [d_{(a,b,n)}]_{i,1} = \alpha_n \varphi^{a-(-i)-1}. \quad (3.17)$$

Let $\tilde{f}_{i,j} = [f_n]_{(2^n - (i)) \times (2^n - (j))}$ be the $(2^n - 1) \times (2^n - 1)$ matrix formed by dropping the $i$-th row and the $j$-th column from $f_n$, i.e.

$$\tilde{f}_{a,b} = \begin{cases} 
2^{i-1} \varphi^{j-1}, & \text{if } 1 \leq i < a, 1 \leq j < b; \\
2^i \varphi^{j-1}, & \text{if } a \leq i < 2^n, 1 \leq j < b; \\
2^{i-1} \varphi^j, & \text{if } 1 \leq i < a, b \leq j < 2^n; \\
2^i \varphi^j, & \text{if } a \leq i < 2^n, b \leq j < 2^n.
\end{cases} \quad (3.18)$$
Let $R_a$ be the $(2^n - 1) \times 1$ matrix with entries given by

$$[R_a]_{i,1} = a \varphi^i. \quad (3.19)$$

Let $e_i$ be the $(2^n - 1) \times 1$ column vector with entries given by

$$[e_i]_j = \begin{cases} 1, & \text{if } j = i; \\ 0, & \text{otherwise}. \end{cases} \quad (3.20)$$

Let $Q_{n,k}$ be the $(2^n - 1) \times (2^n - 1)$ matrix with the $i$-th column given by

$$Q_{n,k} = \begin{cases} e_i, & \text{if } 1 \leq i < k; \\ e_{i+1}, & \text{if } k \leq i < 2^n - 1; \\ e_k, & \text{if } i = 2^n - 1. \end{cases} \quad (3.21)$$

**Lemma 3.16** Let $H_k(x_0, x_1, \ldots, x_{k-1})$

$$= \begin{bmatrix} x_0 & x_1 & \cdots & x_0 \varphi^{k-1} \\
 x_1 & x_1 & \cdots & x_1 \varphi^{k-1} \\
 \vdots & \vdots & \ddots & \vdots \\
 x_{k-1} & x_{k-1} & \cdots & x_{k-1} \varphi^{k-1} \end{bmatrix}_{k \times k}$$

$$= \begin{bmatrix} x_0 & x_1^2 & \cdots & x_0^{2^{k-1}} \\
 x_1 & x_1^2 & \cdots & x_1^{2^{k-1}} \\
 \vdots & \vdots & \ddots & \vdots \\
 x_{k-1} & x_{k-1}^2 & \cdots & x_{k-1}^{2^{k-1}} \end{bmatrix}_{k \times k}.$$ 

Then we have

$$\det(H_k) = \prod_{\varphi \not\in \{0,1,2,\ldots,k-1\}} \sum_{i \in I} x_i. \quad (3.22)$$
PROOF. First note that \( \det(H_k) = \sum_j (-1)^{\sigma(j)}(x_0\varphi_{j_0})(x_1\varphi_{j_1})\ldots(x_{k-1}\varphi_{j_{k-1}}) \), where \( \sigma(j) \) is the number of inversions in the permutation \( j = (j_0, j_1, \ldots, j_n) \) and \( j \) varies over all \( k! \) permutations of \( \{0, 1, 2, \ldots, k-1\} \). So the determinant is a homogeneous polynomial with total degree

\[
1 - (-2) - (-2^2) - \ldots - (-2^{k-1}) = \frac{2^k - 1}{2 - 1} = 2^k - 1 \tag{3.23}
\]

in the variables \( x_0, x_1, \ldots, x_{k-1} \). On the other hand, consider \( V = \{0, 1, \ldots, k-1\} \).

Then for a non-empty subset \( I \) of \( V \), \( \sum_{i \in I} x_i \) is a factor of \( \det(H_k) \). This is because, for \( j \in V \), \( \sum_{i \in I} x_i\varphi^j = (\sum_{i \in I} x_i)\varphi^j \), so if we add all the rows indexed in \( I \) together, we get a new row which has \( (\sum_{i \in I} x_i)\varphi^j \) in the \( j \)-th entry. So these entries have the common factor \( \sum_{i \in I} x_i \). And this common factor is also a factor of \( \det(H_k) \).

Moreover, since \( V \) has \( 2^{k-1} \) nonempty subsets, we already have \( 2^{k-1} \) factors of \( \det(H_k) \), and hence all the factors of \( \det(H_k) \) by (3.23). This completes the proof of the lemma. \( \square \)

**Lemma 3.17** \( \det(H_k(2^0, 2^1, \ldots, 2^{k-1})) = \prod_{1 \leq i < 2^k} i \).

**PROOF.** By Lemma 3.16, \( \det(H_k(2^0, 2^1, \ldots, 2^{k-1})) = \prod_{\emptyset \neq I \subseteq \{0, 1, 2, \ldots, k-1\}} \sum_{i \in I} 2^i = \prod_{1 \leq i < 2^k} i \). \( \square \)

**Lemma 3.18** For all \( n \geq 0 \), \( \det(f_n) = 1 \).

**PROOF.** We have \( \det(f_n) = \det(H_{2n}(2^0, 2^1, \ldots, 2^{k-1}) = \prod_{1 \leq i < 2^{2n}} i = 1 \). The last equality here holds by Corollary 3.11. \( \square \)

**Lemma 3.19** \( [f_n^{-1}]_{i,j} = \det(\hat{f}_{i,j}) \).
PROOF. We have \([f_n^{-1}]_{i,j} = \det^{-1}(f_n) \ast \det([f_n](2^n_{-j}) \times (2^n_{-i})) = 1^*
\det([f_n](2^n_{-j}) \times (2^n_{-i})) = \det([f_n](2^n_{-j}) \times (2^n_{-i})) = \det(\hat{f}_{j,i})\) The second equality holds by Lemma 3.18, and the last by (3.18). □

**Theorem 3.20** For \(1 \leq a, b \leq 2^n\),

\[
[f_n^{-1}]_{b,a} = [f_n^{-1}]_{1,a} \varphi^{b-1}.
\] (3.24)

PROOF. First, by Lemma 3.19, we have \([f_n^{-1}]_{1,a} = \det(\hat{f}_{a,1}), [f_n^{-1}]_{1,a} \varphi^{b-1} = \det(\hat{f}_{a,1} \varphi^{b-1})\), and \([f_n^{-1}]_{b,a} = \det(\hat{f}_{a,b})\). Now

\[
\hat{f}_{a,1} = \begin{cases} 
2^{i-1} \varphi^j, & \text{if } 1 \leq i < a, 1 \leq j < 2^n; \\
2^i \varphi^j, & \text{if } a \leq i < 2^n, 1 \leq j < 2^n;
\end{cases}
\]

and by Lemma 3.4,

\[
\hat{f}_{a,1} \varphi^{b-1} = \begin{cases} 
2^{i-1} \varphi^{j-(b)-1}, & \text{if } 1 \leq i < a, 1 \leq j < 2^n; \\
2^i \varphi^{j-(b)-1}, & \text{if } a \leq i < 2^n, 1 \leq j < 2^n; \\
2^{i-1} \varphi^{j-(b)-1}, & \text{if } 1 \leq i < a, 1 \leq j < 2^n - b - (-1); \\
2^i \varphi^{j-(b)-1-2^n}, & \text{if } 1 \leq i < a, 2^n - b - (-1) \leq j < 2^n; \\
2^i \varphi^{j-(b)-1}, & \text{if } a \leq i < 2^n, 1 \leq j < 2^n - b - (-1); \\
2^i \varphi^{j-(b)-1-2^n}, & \text{if } a \leq i < 2^n, 2^n - b - (-1) \leq j < 2^n.
\end{cases}
\]

Now we move the first \(2^n - b\) columns to the end to form a new matrix, with the same determinant. (Recall that we are working over characteristic 2.) The new matrix \(\hat{f}_{a,b}\) now has the following entries:
\[
\begin{cases}
2^{i-1}\varphi^j, & \text{if } 1 \leq i < a, \ b \leq j < 2^n; \\
2^{i-1}\varphi^{j-1}, & \text{if } 1 \leq i < a, \ 1 \leq j < b; \\
2^i\varphi^j, & \text{if } a \leq i < 2^n, \ b \leq j < 2^n; \\
2^i\varphi^{j-1}, & \text{if } a \leq i < 2^n, \ 1 \leq j < b.
\end{cases}
\]

Thus we have \([f_{-1}]_{1,a}\varphi^{b-1} = \det(\hat{f}_{a,1}\varphi^{b-1}) = \det(\hat{f}_{a,b}) = [f_{-1}]_{h,a}\), completing the proof of the theorem.  \(\square\)

### The top of the inverse matrix

Theorem 3.20 shows that, in order to construct the inverse matrix \(f_n^{-1}\) of \(f_n\), it remains to determine the first row. The goal of the current section, Theorem 3.34 below, identifies the first row of \(f_n^{-1}\) as \((P_{2^n-1}, \ldots, P_1, P_0)\). The proof of Theorem 3.34 requires a chain of auxiliary Lemmas, formulated using the notation (3.12)-(3.21).

**Lemma 3.21** \(\det(\hat{f}_{2^n,1}) = 1\).

**Proof.** By (3.18), we have \([\hat{f}_{2^n,1}]_{i,j} = 2^{i-1}\varphi^j\), for \(1 \leq i, j < 2^n\). So \(\hat{f}_{2^n,1} = H_{2^n-1}(2^0\varphi, 2^1\varphi, \ldots, 2^{2^n-2}\varphi)\). Hence \(\det(\hat{f}_{2^n,1}) = \det(H_{2^n-1}(2^0, 2^1, \ldots, 2^{2^n-2}))\varphi = (\prod_{1 \leq i < 2^n} i)\varphi = 1\varphi = 1\). The penultimate equality holds by Lemma 3.17, and the last by Corollary 3.11.  \(\square\)

**Lemma 3.22** \(\det(A_n) = 1\).

**Proof.** By (3.12), we have that \(A_n^t\) is the \((2^n - 1) \times (2^n - 1)\) matrix with \([A_n^t]_{i,j} = 2^{i-1}\varphi^j\), and hence is equal to \(\hat{f}_{2^n,1}\) by (3.18). So by Lemma 3.21, \(\det(A_n) = \det(A_n^t) = \det(\hat{f}_{2^n,1}) = 1\).  \(\square\)
Lemma 3.23

Let \( M_n = \begin{bmatrix} C_n^t & 2^{2^n-1} \\ A_n & B_n \end{bmatrix}_{2^n \times 2^n} \). Then \( \det M_n = 1 \).

PROOF. Note \( M_n \) is the \( 2^n \times 2^n \) matrix with \( [M_n]_{i,j} = 2^{j-1} \varphi^{i-1} \). So by (3.11) and Lemma 3.18, we have \( \det M_n = \det(f_n^t) = \det(f_n) = 1. \square \)

Denote the Hadamard product of two \( k \times l \) matrices \( E, F \) by \( E \circ F \). Thus \( [E \circ F]_{i,j} = [E_{i,j}F_{i,j}], \) for \( 1 \leq i \leq k, 1 \leq j \leq l \).

Lemma 3.24

\[
A_{n+1} = \begin{bmatrix} A_n & B_n & A_n \circ D_{(1,2^n-1,n)} \\ C_n^t & \beta_n & (\alpha_n + 1) \ast C_n^t \\ A_n & B_n & A_n \circ D_{(2^{n+1},2^{n+1}-1,n)} \end{bmatrix}_{(2^{n+1}-1) \times (2^{n+1}-1)}
\]

PROOF. By (3.13), \( A_{n+1} \) is the \( (2^{n+1} - 1) \times (2^{n+1} - 1) \) matrix with \( [A_{n+1}]_{i,j} = 2^{j-1} \varphi^{i} \). We need to verify the following 9 equations:

\[
A_1 \equiv [A_{n+1}]_{(1,2^n-1) \times (1,2^n-1)} = A_n. \tag{3.25}
\]

\[
A_2 \equiv [A_{n+1}]_{(1,2^n-1) \times (2^n)} = B_n. \tag{3.26}
\]

\[
A_3 \equiv [A_{n+1}]_{(1,2^n-1) \times (2^{n+1},2^{n+1}-1)} = A_n \circ D_{(1,2^n-1,n)}. \tag{3.27}
\]

\[
A_4 \equiv [A_{n+1}]_{(2^n) \times (1,2^n-1)} = C_n^t. \tag{3.28}
\]
\[ \mathbf{A}_5 \equiv [A_{n+1}]_{[2^n] \times \{2^n\}} = \beta_n. \quad (3.29) \]

\[ \mathbf{A}_6 \equiv [A_{n+1}]_{[2^n] \times (2^{n+1},2^{n+1}-1)} = (\alpha_n + 1) \cdot C_n^k. \quad (3.30) \]

\[ \mathbf{A}_7 \equiv [A_{n+1}]_{(2^{n+1},2^{n+1}-1) \times \{1,2^n-1\}} = A_n. \quad (3.31) \]

\[ \mathbf{A}_8 \equiv [A_{n+1}]_{(2^{n+1},2^{n+1}-1) \times \{2^n\}} = B_n. \quad (3.32) \]

\[ \mathbf{A}_9 \equiv [A_{n+1}]_{(2^{n+1},2^{n+1}-1) \times (2^{n+1},2^{n+1}-1)} = A_n \circ D_{(2^{n+1},2^{n+1}-1,n)}. \quad (3.33) \]

Verification of (3.25):
By definition, \( A_1 \) is the \((2^n - 1) \times (2^n - 1)\) matrix with
\[ (A_1)_{i,j} = 2^{i-1} \varphi^i, \quad 1 \leq i, j \leq 2^n - 1. \] But this is just the matrix \( A_n \).

Verification of (3.26):
By definition, \( A_2 \) is the \((2^n - 1) \times 1\) matrix with
\[ (A_2)_{i,1} = 2^{2^n-1} \varphi^i, \quad 1 \leq i \leq 2^n - 1. \] But this is just the matrix \( B_n \).

Verification of (3.27):
By definition, \( A_3 \) has coefficients as follows, for \( 1 \leq i, j \leq 2^n - 1 \):
\[ (A_3)_{i,j} = 2^{(2^n+j-1)} \varphi = 2^{2^n+j-1} \varphi^i = (2^{2^n} \cdot 2^{j-1}) \varphi^i = 2^{2^n} \varphi^i \cdot 2^{j-1} \varphi^i = \alpha_n \varphi^i \cdot (A_n)_{i,j} = [D_{1,2^n-1,n}]_{i,j} \cdot (A_n)_{i,j} = [D_{1,2^n-1,n}]_{i,j} \cdot [A_n]_{i,j} = [A_n \circ D_{(1,2^n-1,n)}]_{i,j}. \] The prepenultimate equation holds by (3.17) with \( a = 1, \ b = 2^n - 1 \).

Verification of (3.28):
By definition, \( A_4 \) has coefficients as follows, for \( 1 \leq j \leq 2^n - 1 \):
\[ (A_4)_{1,j} = 2^{j-1} \varphi = 2^{j-1} = [C_n]_{j,1}. \] So \( A_4 = C_n^k \).

Verification of (3.29):
By definition, $A_5$ is the $1 \times 1$ matrix with $[A_5]_{1,1} = 2^{2n-1} \varphi^{2n} = 2^{2n-1}$.

Verification of (3.30):

By definition, $A_6$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$$[A_6]_{i,j} = 2^{(2^n+j-1)} \varphi^{2^n} = 2^{2^n+(j-1)} \varphi^{2^n} = (2^{2^n} * 2^{j-1}) \varphi^{2^n} = 2^{2^n} \varphi^{2^n} * 2^{j-1} \varphi^{2^n} = (\alpha_n + 1) * 2^{j-1} = (\alpha_n + 1) * [C_n]_{i,j} \text{ So } A_6 = (\alpha_n + 1) * C_n.$$  

Verification of (3.31):

By definition, $A_7$ has coefficients as follows, for $1 \leq i, j \leq 2^n - 1$:

$$[A_7]_{i,j} = 2^{j-1} \varphi^{2^{n+(i-j)}} = (2^{j-1} \varphi^{2^n}) \varphi^i = 2^{j-1} \varphi^i = [A_n]_{i,j}.$$

Verification of (3.32):

By definition, $A_8$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$$[A_8]_{i,1} = 2^{2^n-1} \varphi^{2^{n+(i-1)}} = (2^{2^n-1} \varphi^{2^n}) \varphi^i = 2^{2^n-1} \varphi^i = [B_n]_{i,1}.$$

Verification of (3.33):

By definition, $A_9$ has coefficients as follows, for $1 \leq i, j \leq 2^n - 1$:

$$[A_9]_{i,j} = 2^{2^n+(j-1)} \varphi^{2^n+i}, \quad 1 \leq i, j \leq 2^n - 1.$$

$$= 2^{2^n+(j-1)} \varphi^{2^n+i} = (2^{2^n} * 2^{j-1}) \varphi^{2^n+i} = 2^{2^n} \varphi^{2^n+i} * 2^{j-1} \varphi^{2^n+i}$$

$$= \alpha_n \varphi^{2^n+i} * (2^{j-1} \varphi^{2^n}) \varphi^i$$

$$= \alpha_n \varphi^{2^n+i} * 2^{j-1} \varphi^i = [D_{2^n-1,2n+1-1,n}]_{i,j} * [A_n]_{i,j}$$

$$= [A_n]_{i,j} * [D_{2^n-1,2n+1-1,n}]_{i,j}$$

$$= [A_n \circ D_{2^n-1,2n+1-1,n}]_{i,j}. \text{ The prepenultimate equation holds by (3.17) with } a = 1, \ b = 2^n - 1 \text{ and (3.12).} \quad \Box$$

**Lemma 3.25**

$$X_{n+1} = \begin{bmatrix} X_n * (2^n + 1) \\ 2^n + 1 \\ X_n \end{bmatrix}_{(2^{n+1}-1) \times 1}.$$
PROOF. By (3.14), $X_{n+1}$ is the $(2^{n+1} - 1) \times 1$ matrix with $[X_{n+1}]_{i,1} = P_{2^{n+1} - 1}$.

We need to verify the following 3 equations:

$$X_1 \equiv [X_{n+1}]_{(1,2^{n-1})x1} = X_n * (2^{2^n} + 1). \quad (3.34)$$

$$X_2 \equiv [X_{n+1}]_{(2^n)x1} = 2^{2^n} + 1. \quad (3.35)$$

$$X_3 \equiv [X_{n+1}]_{(2^{n+1},2^{n+1} - 1)x1} = X_n. \quad (3.36)$$

Verification of (3.34):

By definition, $X_1$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$$[X_1]_{i,1} = P_{2^{n+1} - i} = P_{(2^n-(2^n))} = P_{2^{n+1}-(2^n)} = P_{2^n} * P_{2^n - i} = (2^{2^n} + 1) * [X_n]_{i,1} = (2^{2^n} + 1). \quad (2^{2^n} + 1). \quad (2^{2^n} + 1).$$

So $X_1 = X_n * (2^{2^n} + 1)$.

Verification of (3.35):

By definition, $X_2$ is the $1 \times 1$ matrix with $[X_2]_{1,1} = P_{2^{n+1} - 2^n} = P_{(2^n-(2^n))} = P_{2^n} = 2^{2^n} + 1$. Verification of (3.36):

By definition, $X_3$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$$[X_3]_{i,1} = P_{2^{n+1}-(i+2^n)} = P_{(2^n-(2^n))} = P_{2^n - i} = [X_n]_{i,1}. \quad \Box$$

Lemma 3.26 If $A_n * X_n = B_n$, then

$$(A_n \circ D_{(a,(2^n-2)-(-a),n)}) * X_n = B_n \circ d_{(a,(2^n-2)-(-a),n)}.$$  

PROOF. $(A_n \circ D_{(a,(2^n-2)-(-a),n)}) * X_n$ has coefficients as follows, for $1 \leq i \leq 2^n - 1$:

$$[(A_n \circ D_{(a,(2^n-2)-(-a),n)}) * X_n]_{i,1}$$

$$= \sum_{1 \leq j \leq 2^n - 1} [A_n \circ D_{(a,(2^n-2)-(-a),n)}]_{i,j} * [X_n]_{j,1}$$
Lemma 3.27 If $A_n \ast X_n = B_n$, then $C_n^t \ast X_n = 2^{2n-1} + 1$.

PROOF. Recall the matrix $M_n$ of Lemma 3.18. By elementary column operations, when we add the elements of the first $2^n - 1$ columns of $M_n$ multiplied by $X_n$ to the last column of $M_n$, we have a new matrix with the same determinant. Thus we have

$$1 = \det \begin{bmatrix}
C_n^t & 2^{2n-1} + C_n^t \ast X_n \\
A_n & B_n + A_n \ast X_n
\end{bmatrix}_{2^n \times 2^n}$$

$$= \det \begin{bmatrix}
C_n^t & 2^{2n-1} + C_n^t \ast X_n \\
A_n & B_n
\end{bmatrix}_{2^n \times 2^n}$$

$$= \det \begin{bmatrix}
C_n^t & 2^{2n-1} + C_n^t \ast X_n \\
A_n & 0_{(2^n-1) \times 1}
\end{bmatrix}_{2^n \times 2^n}.$$ 

Now expanding the determinant of the matrix by the last column, we get

$$1 = (2^{2n-1} + C_n^t \ast X_n) \ast \det(A_n).$$

By Lemma 3.22, we thus have $2^{2n-1} + C_n^t \ast X_n = 1$, i.e. $C_n^t \ast X_n = 2^{2n-1} + 1$. □
Lemma 3.28 If $A_n \ast X_n = B_n$, then

$$A_{n+1} \ast X_{n+1} = \begin{bmatrix} B_n \circ d_{(1,2^n-1,n)} \\ (\alpha_n + 1) \ast 2^{2^n-1} \\ B_n \circ d_{(2^n+1,2^{n+1}-1,n)} \end{bmatrix}_{(2^{n+1}-1) \times 1}.$$

**Proof.** By Lemma 3.24 and Lemma 3.25, we have $A_{n+1} \ast X_{n+1}$

$$= \begin{bmatrix} A_n \ast X_n \ast (2^{2^n} + 1) \ast B_n \ast (2^{2^n} + 1) \ast (A_n \circ D_{(1,2^n-1,n)} \ast X_n) \\ C_n \ast X_n \ast (2^{2^n} + 1) \ast 2^{2^n-1} \ast (2^{2^n} + 1) \ast \alpha_n \ast C_n \ast X_n \\ A_n \ast X_n \ast (2^{2^n} + 1) \ast B_n \ast (2^{2^n} + 1) \ast (A_n \circ D_{(2^n+1,2^{n+1}-1,n)}) \ast X_n \end{bmatrix}.$$

To prove the lemma, we need to verify the following 3 equations:

1. $A_n \ast X_n \ast (2^{2^n} + 1) \ast B_n \ast (2^{2^n} + 1) \ast (A_n \circ D_{(1,2^n-1,n)} \ast X_n)$
   $$= B_n \circ d_{(1,2^n-1,n)};$$
   (3.37)

2. $C_n \ast X_n \ast (2^{2^n} + 1) \ast 2^{2^n-1} \ast (2^{2^n} + 1) \ast \alpha_n \ast C_n \ast X_n$
   $$= (\alpha_n + 1) \ast 2^{2^n-1};$$
   (3.38)

3. $A_n \ast X_n \ast (2^{2^n} + 1) \ast B_n \ast (2^{2^n} + 1) \ast (A_n \circ D_{(2^n+1,2^{n+1}-1,n)}) \ast X_n$
   $$= B_n \circ d_{(2^n+1,2^{n+1}-1,n)}.$$
   (3.39)

**Verification of 3.37:**

$$A_n \ast X_n \ast (2^{2^n} + 1) \ast B_n \ast (2^{2^n} + 1) \ast (A_n \circ D_{(1,2^n-1,n)}) \ast X_n$$

$$= (A_n \ast X_n + B_n) \ast (2^{2^n} + 1) \ast (A_n \circ D_{(1,2^n-1,n)}) \ast X_n$$
(by combining the first 2 terms)
\[ = (A_n \circ D_{(1,2^n-1,n)}) \ast X_n \quad \text{(by hypothesis)} \]
\[ = B_n \circ d_{(1,2^n-1,n)} \quad \text{(by Lemma 3.26 with } a = 1). \]

Verification of 3.38:
\[ C'_n \ast X_n \ast (2^{2n} + 1) + 2^{2n-1} \ast (2^{2n} + 1) + \alpha_n \ast C'_n \ast X_n \]
\[ = (2^{2n-1} + 1) \ast (2^{2n} + 1) + 2^{2n-1} \ast (2^{2n} + 1) + \alpha_n \ast (2^{2n-1} + 1) \]
(by Lemma 3.27)
\[ = (2^{2n} + 1) + \alpha_n \ast (2^{2n-1} + 1) \quad \text{(by combining the first 2 terms)} \]
\[ = \alpha_n + 1 + \alpha_n \ast (2^{2n-1} + 1) \]
\[ = \alpha_n + 1 + (\alpha_n + 1) \ast (2^{2n-1} + 1) \quad \text{(by Lemma 3.8)} \]
\[ = (\alpha_n + 1) \ast 2^{2n-1}. \]

Verification of 3.39:
\[ A_n \ast X_n \ast (2^{2n} + 1) + B_n \ast (2^{2n} + 1) + (A_n \circ D_{(2^n+1,2^{n+1}+1,n)} \ast X_n \]
\[ = (A_n \ast X_n + B_n) \ast (2^{2n} + 1) + (A_n \circ D_{(2^n+1,2^{n+1}+1,n)} \ast X_n \]
(by combining the first 2 terms)
\[ = (A_n \circ D_{(2^n+1,2^{n+1}+1,n)} \ast X_n \quad \text{(by hypothesis)} \]
\[ = B_n \circ d_{(2^n+1,2^{n+1}+1,n)} \ast X_n \quad \text{(by Lemma 3.26).} \]

Lemma 3.29
\[ B_{n+1} = \begin{bmatrix}
B_n \circ d_{(1,2^n-1,n)} \\
(\alpha_n + 1) \ast 2^{2^n-1} \\
B_n \circ d_{(2^n+1,2^{n+1}+1,n)}
\end{bmatrix}^{(2^n-1) \times 1} \]
PROOF. By (3.13), \( B_{n+1} \) is the \((2^{n+1} - 1) \times 1\) matrix with 
\[ [B_{n+1}]_{i,1} = 2^{n+1} - 1 \varphi^i. \]
We need to verify the following 3 equations:

\[
B_1 \equiv [B_{n+1}](1, 2^n - 1)_{x1} = B_n \circ d_{(1, 2^n - 1, n)}. 
\] (3.40)

\[
B_2 \equiv [B_{n+1}](2^n)_{x1} = (\alpha_n + 1) \ast 2^{2^n - 1}. 
\] (3.41)

\[
B_3 \equiv [B_{n+1}](2^{n+1, 2^n+1} - 1)_{x1} = B_n \circ d_{(2^n+1, 2^n+1-1, n)}. 
\] (3.42)

Verification of (3.40):

By definition, \( B_1 \) has coefficients as follows, for \( 1 \leq i \leq 2^n - 1 \):
\[
[B_1]_{i,1} = 2^{2^n+1-1} \varphi^i = 2^{(2^n - (-2^n)) - 1} \varphi^i = 2^{2^n + (2^n - 1)} \varphi^i = (2^{2^n} \ast 2^{2^n - 1} \varphi^i = 2^{2^n} \varphi^i \ast 2^{2^n} \varphi^i = (\alpha_n \varphi^i \ast [B_n]_{i,1} = [d_{(1, 2^n - 1, n)}]_{i,1} \ast [B_n]_{i,1} = [B_n]_{i,1} = [B_n]_{i,1} \circ d_{(1, 2^n - 1, n)}]_{i,1} = [B_n]_{i,1}. \] The prepenultimate equation holds by (3.16) with \( a = 1, b = 2^n - 1 \).

Verification of (3.41):

By definition, \( B_2 \) is the \(1 \times 1\) matrix with
\[
[B_2]_{1,1} = 2^{2^n+1-1} \varphi^2 = 2^{(2^n - (-2^n)) - 1} \varphi^2 = 2^{2^n + (2^n - 1)} \varphi^2 = (2^{2^n} \ast 2^{2^n - 1} \varphi^2 = 2^{2^n} \varphi^2 \ast 2^{2^n} \varphi^2 = (\alpha_n + 1) \ast 2^{2^n - 1}. 
\] Verification of (3.42):

By definition, \( B_3 \) has coefficients as follows, for \( 1 \leq i \leq 2^n - 1 \):
\[
[B_3]_{i,1} = 2^{2^n+1-1} \varphi^{2^n+i} = 2^{(2^n - (-2^n)) - 1} \varphi^{2^n+i} = 2^{2^n + (2^n - 1)} \varphi^{2^n+i} = (2^{2^n} \ast 2^{2^n - 1} \varphi^{2^n+i} = 2^{2^n} \varphi^{2^n+i} \ast 2^{2^n - 1} \varphi^i = \alpha_n \varphi^{2^n+i} \ast (2^{2^n - 1} \varphi^i = (2^{2^n - 1} \varphi^i = \alpha_n \varphi^{2^n+i} \ast 2^{2^n - 1} \varphi^i = \alpha_n \varphi^{2^n+i} \ast [B_n]_{i,1} = [d_{(2^n+1, 2^n+1-1, n)}]_{i,1} \ast [B_n]_{i,1} = [B_n]_{i,1} \circ d_{(2^n+1, 2^n+1-1, n)}]_{i,1} = [B_n]_{i,1}. \] The prepenultimate equation holds by (3.16) with \( a = 2^n + 1, b = 2^{n+1} - 1 \). □

Lemma 3.30 \( A_n \ast X_n = B_n \).
PROOF. By induction on \( n \). If \( n = 1 \), we have \( A_1 \ast X_1 = [1][P_1] = 1 \times 3 = 2^2 = B_1 \).

Assume \( A_k \ast X_k = B_k \). We want to show \( A_{k+1} \ast X_{k+1} = B_{k+1} \). By the induction hypothesis, Lemma 3.28 and Lemma 3.29, we have

\[
A_{k+1} \ast X_{k+1} = \begin{bmatrix}
B_k \circ d_{(1,2^k-1,k)} \\
(\alpha_k + 1) \ast 2^{2^k-1} \\
B_k \circ d_{(2^k+1,2^{k+1}-1,k)}
\end{bmatrix}_{(2^{n+1}-1) \times 1} = B_{k+1}.
\]

This completes the proof of the lemma. \( \square \)

**Lemma 3.31** \( (A_n Q_{n,k}) \ast (Q_{n,k}^t X_n) = B_n \).

**Proof.** \( (A_n Q_{n,k}) \ast (Q_{n,k}^t X_n) \) has coefficients as follows, for \( 1 \leq i \leq 2^n - 1 \):

\[
[(A_n Q_{n,k}) \ast (Q_{n,k}^t X_n)]_{i,1} = \sum_{j=1}^{2^n-1} [A_n Q_{n,k}]_{i,j} \ast [Q_{n,k}^t X_n]_{j,1}
\]

\[
= \sum_{j=1}^{k-1} [A_n Q_{n,k}]_{i,j} \ast [Q_{n,k}^t X_n]_{j,1} + \sum_{j=k}^{2^n-2} [A_n Q_{n,k}]_{i,j} \ast [Q_{n,k}^t X_n]_{j,1} + [A_n Q_{n,k}]_{i,2^n-1} \ast [Q_{n,k}^t X_n]_{2^n-1,1}
\]

\[
= \sum_{j=1}^{k-1} [A_n]_{i,j} \ast [X_n]_{j,1} + \sum_{j=k}^{2^n-2} [A_n]_{i,j} \ast [X_n]_{j+1,1} + [A_n]_{i,k} \ast [X_n]_{k,1}
\]

\[
= \sum_{j=1}^{k-1} [A_n]_{i,j} \ast [X_n]_{j,1} + \sum_{j=k}^{2^n-1} [A_n]_{i,j} \ast [X_n]_{j,1} + [A_n]_{i,k} \ast [X_n]_{k,1}
\]

\[
= \sum_{j=1}^{2^n-1} [A_n]_{i,j} \ast [X_n]_{j,1} = [A_n \ast X_n]_{i,1} = [B_n]_{i,1}.
\]

Thus \( (A_n Q_{n,k}) \ast (Q_{n,k}^t X_n) = B_n \). \( \square \)

**Lemma 3.32** Let \( E \) be the \( (2^n - 1) \times (2^n - 1) \) matrix with \( e_i \) as its \( i \)-th column, for \( 1 \leq i < 2^n - 1 \), and \( Q_{n,k}^t X_n \) as its last column. We then have \( (A_n Q_{n,k}) \ast E = \hat{f}_{k,1}^t \).
\begin{proof}
Note that $\hat{T}_{k,1}$ is the \((2^n - 1) \times (2^n - 1)\) matrix whose \(i\)-th column is
\[
\begin{cases}
R_{2i-1}, & 1 \leq i < k; \\
R_{2i}, & k \leq i < 2^n - 1.
\end{cases}
\]

\(A_{n,k}\) is the \((2^n - 1) \times (2^n - 1)\) matrix whose \(i\)-th column is
\[
\begin{cases}
R_{2i-1}, & 1 \leq i < k; \\
R_{2i}, & k \leq i < 2^n - 1; \\
R_{2k-1}, & i = 2^n - 1.
\end{cases}
\]

So the first \(2^n - 2\) columns of \(A_{n,k}\) and $\hat{T}_{k,1}$ agree. Hence for \(1 \leq i < 2^n - 1\),
\((A_{n,k}) \ast e_i\) is equal to the \(i\)-th column of \(A_{n,k}\), which is equal to the \(i\)-th column
of $\hat{T}_{k,1}$. We also have \((A_{n,k}) \ast (Q_{n,k}^t X_n) = B_n\) by Lemma 3.31. Since \(B_n = R_{2^{n-1}}\)
by (3.13) and (3.19), \((A_{n,k}) \ast E = \hat{T}_{k,1}\). □

\textbf{Lemma 3.33} \textit{Let \(E\) be defined as in Lemma 3.32. Then \(\det(E) = P_{2^n-i}\).}

\begin{proof}
Since the \(i\)-th column of the matrix \(E\) is \(e_i\), for \(1 \leq i < 2^n - 1\),
\(\det(E) = [Q_{n,k}^t X_n]_{2^n-1,1} = P_{2^n-i}\). □
\end{proof}

\textbf{Theorem 3.34} \textit{Let \(f_n\) be defined as in (3.11). Then the first row of \(f_n^{-1}\) is}

\( (P_{2^n-1}, ..., P_1, P_0) \).

\begin{proof}
We want to show that \([f_n^{-1}]_{1,i} = P_{2^n-i}\), for \(1 \leq i \leq 2^n\). But \([f_n^{-1}]_{1,i} = \det(\hat{f}_{i,1}) = \det(\hat{T}_{i,1}) = \det((A_{n,k}) \ast E) = \det(A_{n,k}) \ast \det(E) = \det(A_n) \ast \det(E) = 1 \ast P_{2^n-i} = P_{2^n-i}\), as required. □
\end{proof}
Corollary 3.35 \[ f^{-1}_{ij} \mid ij = p_{2n-j}p^{i-1}, \text{ for } 1 \leq i,j \leq 2^n. \]

**Proof.** By Theorem 3.20 and Theorem 3.34. \( \Box \)

**Function spaces**

This section studies relationships between certain subspaces of the GF(2)-space \( \prod_{n=0}^{\infty} \text{End } \text{GF}(\alpha_n) \). The subspaces are of interest in coding theory, since they contain the syndromes of binary lexicodes.

**Definition 3.36** A sequence of GF(2)-linear functions \( \{h_n : \text{GF}(\alpha_n) \to \text{GF}(\alpha_n)\} \) is said to be coherent if there exists a GF(2)-linear function \( f : \text{N} \to \text{N} \) such that \( \exists n. \forall m \geq n, h_m = f|_{\text{GF}(\alpha_m)} \). Let \( C \) denote the subset of \( \prod_{n=0}^{\infty} \text{End } \text{GF}(\alpha_n) \) consisting of coherent sequences.

**Proposition 3.37** The set \( C \) of coherent sequences forms a subspace of \( \prod_{n=0}^{\infty} \text{End } \text{GF}(\alpha_n) \).

**Proof.** First, note that the sequence of zero functions is coherent. Now let \( \{h_n : \text{GF}(\alpha_n) \to \text{GF}(\alpha_n)\} \) and \( \{k_n : \text{GF}(\alpha_n) \to \text{GF}(\alpha_n)\} \) be coherent sequences. To prove \( C \) is a subspace, we need to show that \( \{l_n = h_n + k_n : \text{GF}(\alpha_n) \to \text{GF}(\alpha_n)\} \) is a coherent sequence too, since we are working over GF(2). Now we have: there exists a GF(2)-linear function \( f : \text{N} \to \text{N} \) such that \( \exists n_1. \forall m \geq n_1, h_m = f|_{\text{GF}(\alpha_m)} \) and there exists a GF(2)-linear function \( g : \text{N} \to \text{N} \) such that \( \exists n_2. \forall m \geq n_2, k_m = g|_{\text{GF}(\alpha_m)} \). Let \( n = \max(n_1, n_2) \). Then \( \forall m \geq n, h_m = f|_{\text{GF}(\alpha_m)} \) and \( k_m = g|_{\text{GF}(\alpha_m)} \), so \( l_m = h_m + k_m = (f + g)|_{\text{GF}(\alpha_m)} \). Since \( f + g : \text{N} \to \text{N} \) is again a linear function, the proposition is proved. \( \Box \)
Definition 3.38 A sequence of $\text{GF}(2)$-linear functions $\{h_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ is said to be small if $\exists n. \forall m \geq n, \text{GF}(\alpha_m)h_m \subseteq \text{GF}(\alpha_{m-1})$. Let $S$ denote the subset of $\prod_{n=0}^{\infty} \text{End} \text{GF}(\alpha_n)$ consisting of small sequences.

Proposition 3.39 The set $S$ of small sequences forms a subspace of $\prod_{n=0}^{\infty} \text{End} \text{GF}(\alpha_n)$.

Proof. First, note that the sequence of zero functions is small. Now let $\{h_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ and $\{k_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ be small sequences. To prove $S$ is a subspace, we need to show that $\{l_n = h_n + k_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ is a small sequence too. Now we have: $\exists n_1. \forall m \geq n_1, \text{GF}(\alpha_m)h_m \subseteq \text{GF}(\alpha_{m-1})$ and $\exists n_2. \forall m \geq n_2, \text{GF}(\alpha_m)k_m \subseteq \text{GF}(\alpha_{m-1})$. Let $n = \max(n_1, n_2)$. Then $\forall m \geq n$, $\text{GF}(\alpha_m)h_m \subseteq \text{GF}(\alpha_{m-1})$ and $\text{GF}(\alpha_m)k_m \subseteq \text{GF}(\alpha_{m-1})$, so $\text{GF}(\alpha_m)(l_m) = \text{GF}(\alpha_m)(h_m + k_m) \subseteq \text{GF}(\alpha_{m-1})$. □

Definition 3.40 A sequence of $\text{GF}(2)$-linear functions $\{h_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ is said to nest if $\exists n. \forall m \geq n, \forall 0 \leq i < 2^{m-1}, \text{Tr}_{\alpha_{m-1}}(h_m(2^i)) = \text{Tr}_{\alpha_{m-1}}(h_m(2^i + 2^{m-1})) = h_{m-1}(2^i)$. Let $N$ denote the subset of $\prod_{n=0}^{\infty} \text{End} \text{GF}(\alpha_n)$ consisting of nesting sequences.

Proposition 3.41 The set $N$ of nesting sequences forms a subspace of $\prod_{n=0}^{\infty} \text{End} \text{GF}(\alpha_n)$.

Proof. First, note that the sequence of zero functions is nested. Now let $\{h_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ and $\{k_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ be nesting sequences. To prove $N$ is a subspace, we need to show that $\{l_n = h_n + k_n : \text{GF}(\alpha_n) \rightarrow \text{GF}(\alpha_n)\}$ is a nesting sequence too. Now we have: $\exists n_1. \forall m \geq n_1, \forall 0 \leq i < 2^{m-1}, \text{Tr}_{\alpha_{m-1}}(h_m(2^i)) =$
\[ \text{Tr}_{\alpha_{m-1}}(\tilde{h}_m(2^{i+2m-1})) = \tilde{h}_{m-1}(2^i), \text{ and } \exists n_2, \forall m \geq n_2, \forall 0 \leq i < 2^{m-1}, \text{Tr}_{\alpha_{m-1}}(\tilde{\hat{k}}_m(2^i)) = \text{Tr}_{\alpha_{m-1}}(\tilde{k}_m(2^{i+2m-1})) = \tilde{h}_{m-1}(2^i). \] Let \( n = \max(n_1, n_2). \) Then \( \forall m \geq n, \forall 0 \leq i < 2^{m-1}, \text{Tr}_{\alpha_{m-1}}(\tilde{h}_m(2^i)) = \text{Tr}_{\alpha_{m-1}}(\tilde{\hat{k}}_m(2^{i+2m-1})) \) and \( \tilde{k}_{m-1}(2^i) \text{ Tr}_{\alpha_{m-1}}(\tilde{k}_m(2^i)) = \text{Tr}_{\alpha_{m-1}}(\tilde{h}_m(2^{i+2m-1})) = \tilde{h}_{m-1}(2^i). \) Now \( l_n = h_n + k_n \) implies \( \tilde{l}_n = \tilde{h}_n + \tilde{k}_n. \) Also the trace is a linear function. So \( \text{Tr}_{\alpha_{m-1}}((\tilde{l}_m)(2^i)) = \text{Tr}_{\alpha_{m-1}}((\tilde{h}_m + \tilde{k}_m)(2^i)) = \text{Tr}_{\alpha_{m-1}}(\tilde{h}_m)(2^i) + \text{Tr}_{\alpha_{m-1}}(\tilde{k}_m)(2^i) = \text{Tr}_{\alpha_{m-1}}(\tilde{h}_m(2^{i+2m-1})) + \text{Tr}_{\alpha_{m-1}}(\tilde{k}_m(2^{i+2m-1})) = \text{Tr}_{\alpha_{m-1}}((\tilde{h}_m + \tilde{k}_m)(2^{i+2m-1})) = \text{Tr}_{\alpha_{m-1}}(\tilde{l}_m(2^{i+2m-1})). \) Also, \( \tilde{h}_{m-1}(2^i) + \tilde{k}_{m-1}(2^i) = (\tilde{h}_m + \tilde{k}_m)(2^i) = \tilde{l}_{m-1}(2^i). \)

**Definition 3.42** A sequence of \( GF(2) \)-linear functions \( \{h_n : GF(\alpha_n) \to GF(\alpha_n)\} \) is said to have the martingale property if \( \exists n, \forall m \geq n, \forall 0 \leq i < 2^{m-1}, \tilde{h}_m(2^i) + \tilde{h}_m(2^{i+2m-1}) = \tilde{h}_{m-1}(2^i). \) Let \( M \) denote the subset of \( \prod_{n=0}^{\infty} \text{End } GF(\alpha_n) \) consisting of sequences having the martingale property.

**Proposition 3.43** The set \( M \) of sequences with the martingale property forms a subspace of \( \prod_{n=0}^{\infty} \text{End } GF(\alpha_n). \)

**Proof.** First, note that the sequence of zero functions has the martingale property.

Now let \( \{h_n : GF(\alpha_n) \to GF(\alpha_n)\} \) and \( \{k_n : GF(\alpha_n) \to GF(\alpha_n)\} \) be sequences with the martingale property. To prove \( M \) is a subspace, we need to show that \( \{l_n = h_n + k_n : GF(\alpha_n) \to GF(\alpha_n)\} \) is a sequence with the martingale property too. Now we have: \( \exists n_1, \forall m \geq n_1, \forall 0 \leq i < 2^{m-1}, \tilde{h}_m(2^i) + \tilde{h}_m(2^{i+2m-1}) = \tilde{h}_{m-1}(2^i) \) and \( \exists n_2, \forall m \geq n_2, \forall 0 \leq i < 2^{m-1}, \tilde{k}_m(2^i) + \tilde{k}_m(2^{i+2m-1}) = \tilde{k}_{m-1}(2^i). \) Let \( n = \max(n_1, n_2). \) Then \( \forall m \geq n, \forall 0 \leq i < 2^{m-1}, \tilde{h}_m(2^i) + \tilde{h}_m(2^{i+2m-1}) = \tilde{h}_{m-1}(2^i) \) and \( \tilde{k}_m(2^i) + \tilde{k}_m(2^{i+2m-1}) = \tilde{k}_{m-1}(2^i), \) so \( (\tilde{l}_m)(2^i) + (\tilde{l}_m)(2^{i+2m-1}) = (\tilde{h}_m + \tilde{k}_m)(2^i) + (\tilde{h}_m + \tilde{k}_m)(2^{i+2m-1}) = (\tilde{h}_m + \tilde{k}_m)(2^i) + (\tilde{h}_m + \tilde{k}_m)(2^{i+2m-1}) = (\tilde{h}_m + \tilde{k}_m)(2^{i+2m-1}) = \tilde{l}_{m-1}(2^i). \)
\( \bar{k}_m(2^{i+2^n-1}) = \bar{h}_m(2^i) + \bar{k}_m(2^i) + \bar{h}_m(2^{i+2^n-1}) + \bar{k}_m(2^{i+2^n-1}) = \bar{h}_{m-1}(2^i) + \bar{k}_{m-1}(2^i) = \bar{f}_{m-1}(2^i). \) □

**Theorem 3.44** Coherent sequences have the martingale property: \( C \subseteq M. \) In other words, if \( \{h_n\} \) is a sequence of linear functions with \( h_n(2^i) = h_{n-1}(2^i) \) for \( 0 \leq i < 2^{n-1} \), then \( \dot{h}_n(2^i) + \ddot{h}_n(2^{i+2^n-1}) = \dot{h}_{n-1}(2^i) \), for \( 0 \leq i < 2^{n-1} \).

**Proof.** First,

\[
\dot{h}_n(2^i) = \sum_{j=1}^{2^n} [f^{-1}_{n,i-(-1),j} * h_n(2^{j-1}) \quad \text{(by Corollary 3.35)}
\]

\[
= \sum_{j=1}^{2^n} P_{2n-j} \varphi^i * h_n(2^{j-1})
\]

\[
= \sum_{j=1}^{2^n} P_{2n-1+(2n-1-j)} \varphi^i * h_n(2^{j-1})
\]

\[
= \sum_{j=1}^{2^n} (P_{2n-1} * P_{2n-1-j}) \varphi^i * h_n(2^{j-1})
\]

\[
= \sum_{j=1}^{2^n} [(\alpha_{n-1} + 1) * P_{2n-1-j}] \varphi^i * h_n(2^{j-1})
\]

\[
= \sum_{j=1}^{2^n} (\alpha_{n-1} * P_{2n-1-j} + P_{2n-1-j}) \varphi^i * h_n(2^{j-1}).
\]

And,

\[
\ddot{h}_n(x^{2^{i+2^n-1}})
\]

\[
= \sum_{j=1}^{2^n} [f^{-1}_{n,i+2^{n-1}-(-1),j} * h_n(2^{j-1}) \quad \text{(by Corollary 3.35)}
\]

\[
= \sum_{j=1}^{2^n} P_{2n-j} \varphi^{i+2^n-1} * h_n(2^{j-1})
\]

\[
= \sum_{j=1}^{2^n} P_{2n-j} \varphi^{2^n-1+i} * h_n(2^{j-1})
\]
\begin{align*}
&= \sum_{j=1}^{2^n} (P_{2^n-j} \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n-1} (P_{2^n-j} \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) + \sum_{j=2^n-1+1}^{2^n} (P_{2^n-j} \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n-1} (P_{2^n-j} \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) + \sum_{j=2^n-1+1}^{2^n} P_{2^n-j} \varphi^i \ast h_n(2^{j-1}), \\
&\text{since } P_{2^n-j} < \alpha_{n-1} \text{ for } 2^{n-1} + 1 \leq j \leq 2^n \text{ and by Lemma 3.4.} \\
&= \sum_{j=1}^{2^n-1} (P_{2^n-1+(2n-1-j)} \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) + \sum_{j=2^n-1+1}^{2^n} P_{2^n-1+(2n-1-j)} \varphi^i \ast h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n-1} (((\alpha_{n-1} + 1) \ast P_{2n-1-j}) \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) \\
&\quad + \sum_{j=2^n-1+1}^{2^n} (((\alpha_{n-1} + 1) \ast P_{2n-1-j}) \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n-1} (((\alpha_{n-1} + 1) \ast P_{2n-1-j}) \varphi^{2n-1} + \varphi^{2n-1}) \varphi^i \ast h_n(2^{j-1}) \\
&\quad + \sum_{j=2^n-1+1}^{2^n} (((\alpha_{n-1} + 1) \ast P_{2n-1-j}) \varphi^{2n-1} \ast h_n(2^{j-1}) \\
&= \sum_{j=1}^{2^n-1} (((\alpha_{n-1} + 1) \ast P_{2n-1-j}) \varphi^i \ast h_n(2^{j-1}) \\
&\quad + \sum_{j=2^n-1+1}^{2^n} (((\alpha_{n-1} + 1) \ast P_{2n-1-j}) \varphi^i \ast h_n(2^{j-1}) \\
&\text{by Lemma 3.8 and Lemma 3.4 with } P_{2^{n-1-j}} \varphi^i \ast h_n(2^{j-1}), \text{ for } 1 \leq j \leq 2^{n-1}. \\
&= \sum_{j=1}^{2^n-1} (\alpha_{n-1} \ast P_{2n-1-j}) \varphi^i \ast h_n(2^{j-1}) \\
&\quad + \sum_{j=2^n-1+1}^{2^n} (\alpha_{n-1} \ast P_{2n-1-j} + P_{2n-1-j}) \varphi^i \ast h_n(2^{j-1})
\end{align*}
So,

\[ h_n(2^i) + \tilde{h}_n(2^{i+2^{n-1}}) \]

\[
= \sum_{j=1}^{2^n} (\alpha_{n-1} \ast P_{2^{n-1}-j} + P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) + \sum_{j=1}^{2^n-1} (\alpha_{n-1} \ast P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
+ \sum_{j=2^{n-1}+1}^{2^n} (\alpha_{n-1} \ast P_{2^{n-1}-j} + P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
= \sum_{j=1}^{2^n} (\alpha_{n-1} \ast P_{2^{n-1}-j} + P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
+ \sum_{j=2^{n-1}+1}^{2^n} (\alpha_{n-1} \ast P_{2^{n-1}-j} + P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
+ \sum_{j=2^{n-1}+1}^{2^n} (\alpha_{n-1} \ast P_{2^{n-1}-j} + P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
= \sum_{j=1}^{2^n} (\alpha_{n-1} \ast P_{2^{n-1}-j} + P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
+ \sum_{j=1}^{2^n-1} (\alpha_{n-1} \ast P_{2^{n-1}-j}) \varphi^i \ast h_n(2^{j-1}) \\
= \sum_{j=1}^{2^n-1} P_{2^{n-1}-j} \varphi^i \ast h_{n-1}(2^{j-1}) \quad \text{(by hypothesis)} \\
= \sum_{j=1}^{2^n-1} [f_{n-1}]_{i+1,j} \ast h_{n-1}(2^{j-1}) \quad \text{(by Corollary 3.35)} \\
= \tilde{h}_{n-1}(2^i), \text{ as required.} \qed

**Theorem 3.45** The martingale property implies the coherence property: \( M \subseteq C \). In other words, if a sequence \( \{h_n : GF(\alpha_n) \to GF(\alpha_n)\} \) of GF(2)-linear functions satisfies \( h_n(2^i) + \tilde{h}_n(2^{i+2^{n-1}}) = \tilde{h}_{n-1}(2^i) \), for \( 0 \leq i < 2^{n-1} \), then \( h_n(2^i) = h_{n-1}(2^i) \), for \( 0 \leq i < 2^{n-1} \).
PROOF. We want to show \( h_n(2^i) = h_{n-1}(2^i) \), for \( 0 \leq i < 2^{n-1} \). For \( 0 \leq i < 2^{n-1} \), we have

\[
h_n(2^i) = \sum_{j=0}^{2^n-1} \left[ f_n \right]_{i+1,j+1} * h_n(2^j)
\]

\[
= \sum_{j=0}^{2^n-1} 2^i \varphi^j * h_n(2^j) \quad \text{(by Equation 3.11)}
\]

\[
= \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^j * h_n(2^j) + \sum_{j=2^{n-1}}^{2^n-1} 2^i \varphi^j * h_n(2^j)
\]

\[
= \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^j * h_n(2^j) + \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^{2^{n-1}+j} * h_n(2^{2^{n-1}+j}) 
\]

( by change of indices)

\[
= \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^j * h_n(2^j) + \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^{2^{n-1}+j} * h_n(2^{2^{n-1}+j}) 
\]

( since \( 2^i < a_{n-1} \), for \( 0 \leq i < 2^{n-1} \))

\[
= \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^j * (h_n(2^j) + h_n(2^{2^{n-1}+j})) 
\]

\[
= \sum_{j=0}^{2^{n-1}-1} 2^i \varphi^j * h_{n-1}(2^j) \quad \text{(by hypothesis)}
\]

\[
= \sum_{j=0}^{2^{n-1}-1} \left[ f_{n-1} \right]_{i+1,j+1} * h_{n-1}(2^j) \quad \text{(by Equation 3.11)}
\]

\[
= h_{n-1}(2^i). \square
\]

**Corollary 3.46** The martingale property is equivalent to coherence. \( \square \)

We now provide some examples demonstrating the independence of the function spaces introduced in this section.

**Example 3.47** A coherent sequence need not nest, i.e. \( C \not\subseteq N \).
Let
\[ h_n(2^i) = \begin{cases} 
\beta_k, & \text{if } i = 2^k - 1, 1 \leq k \leq n; \\
0, & \text{otherwise.}
\end{cases} \]
for all \( n \). Then \( \{h_n\} \) is a coherent sequence. But
\[
\tilde{h}_n(2^0) = \sum_{k=1}^{n+1} \beta_k P_{2^{n+1}-2^k}
\]

Example 3.48 A small sequence need not nest, i.e. \( S \not\subseteq N \).

Let
\[
h_n(2^i) = \begin{cases} 
1, & \text{if } i = 2^n - 1; \\
0, & \text{otherwise,}
\end{cases}
\]
for all \( n \). Then \( \{ h_n \} \) is small. But \( h_n(2^i) = 1 \), for all \( n \) and all \( i \), so \( \{ h_n \} \) is not nesting.

**Example 3.49** A small sequence need not be coherent, i.e. \( S \not\subseteq C \).

The sequence \( \{ h_n \} \) of Example 3.48 works here.

**Example 3.50** A nesting sequence need not be coherent, i.e. \( N \not\subseteq C \).

Let \( h_1 = \{1, 1\} \) and \( h_n(2^i) = \beta_n \), for all \( i \) and \( n \geq 2 \). We then have that \( \{ h_n \} \) is nesting. But also

\[
h_n(2^i) = \begin{cases} 
\beta_n & \text{if } i = 2^n - 1; \\
0 & \text{otherwise},
\end{cases}
\]

i.e. \( \{ h_n \} \) is not a coherent sequence.

**Example 3.51** A nesting sequence need not be small, i.e. \( N \not\subseteq S \).

The nesting sequence \( \{ h_n \} \) of Example 3.50 works here, since \( h_n(2^{2^n-1}) = \beta_n \not\in \text{GF}(\alpha_{n-1}) \) for all \( n \).

**Example 3.52** A sequence with the martingale property need not be small, i.e. \( M \not\subseteq S \).

Let \( h_n(2^0) = 1 \) and \( h_n(2^i) = 0 \), for \( 1 \leq i < 2^n \) and for all \( n \). Then \( \{ h_n \} \) satisfies the martingale property, but we have \( \forall n, h_n(2^{2^n-1}) = \beta_n > \alpha_{n-1} \), i.e. \( \{ h_n \} \) is not small.
Small, coherent sequences

This section completes the investigation of the relationship between the function spaces \( C, N \) and \( S \) by showing (Corollary 3.63) that

\[
C \cap N = N \cap S = S \cap C. \tag{3.43}
\]

**Theorem 3.53** For coherent sequences, nesting implies smallness : \( C \cap N \subseteq S \). In other words, if a sequence of \( GF(2) \)-linear functions \( \{h_n : GF(\alpha_n) \to GF(\alpha_n)\} \) has

\[
h_n(2^i) = h_{n-1}(2^i) \text{ for } 0 \leq i < 2^{n-1} \text{ and } Tr_{\alpha_{n-1}}(\tilde{h}_n(2^i)) = Tr_{\alpha_{n-1}}(\tilde{h}_n(2^{i+2^{n-1}})) = \tilde{h}_{n-1}(2^i) \text{ for } 0 \leq i < 2^{n-1},
\]

then \( h_n(x) \in GF(\alpha_{n-1}), \text{ for } x \in GF(\alpha_n) \).

**Proof.** First, since \( \tilde{h}_n(2^i) \in GF(\alpha_n) \) for \( 0 \leq i < 2^n \), we have

\[
h_n(2^i) = \sum_{j=1}^{2^n} [f_n]_{i-(1),j} \tilde{h}_n(2^j) = \sum_{j=1}^{2^n} 2^i \phi^{j-1} \tilde{h}_n(2^{j-1}) \quad \text{(by Equation 3.11)}
\]

\[< \alpha_n. \tag{3.44}\]

Since \( \{h_n\} \) nests, there exists \( m \) such that for all \( n \geq m \):

\[
\tilde{h}_{n+1}(2^i) = \begin{cases} 
\tilde{h}_n(2^i) * \alpha_n + b_i, & 0 \leq i < 2^n; \\
\tilde{h}_n(2^{i-2^n}) * \alpha_n + b_i, & 2^n \leq i < 2^{n+1}, 
\end{cases}
\]

for some \( b_i \in GF(\alpha_n) \). Also since \( \{h_n\} \) is a coherent sequence, we have \( \tilde{h}_{n+1}(2^i) + \tilde{h}_{n+1}(2^{i+2^n}) = \tilde{h}_n(2^i) \), for \( 0 \leq i < 2^n \) by Theorem 3.44. So

\[
b_i + b_{2^n+i} = \tilde{h}_n(2^i). \tag{3.45}\]

For \( 0 \leq i < 2^n \), since \( h_{n+1}(2^i) = h_n(2^i) \), and \( h_n(2^i) < \alpha_n \) by Equation 3.44, \( h_{n+1}(2^i) \in GF(\alpha_n) \), for \( 0 \leq i < 2^n \). For \( 2^n \leq i < 2^{n+1} \), we have \( h_{n+1}(2^i) \)

\[= \sum_{j=1}^{2^{n+1}} [f_{n+1}]_{i-(1),j} \tilde{h}_{n+1}(2^j)\]
\[
\sum_{j=1}^{2^{n+1}} 2^{j} \varphi^{j-1} \ast \tilde{h}_{n+1}(2^j) = \\
\sum_{j=1}^{2^n+(i-2^n)} 2^{2^n+(i-2^n)} \varphi^{j-1} \ast \tilde{h}_{n+1}(2^j) = \\
\sum_{j=1}^{2^{n+1}} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast \tilde{h}_{n+1}(2^j) = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast \tilde{h}_{n+1}(2^j) + \sum_{j=2^n}^{2^{n+1}} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast \tilde{h}_{n+1}(2^j) = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_j) + \\
\sum_{j=2^n}^{2^{n+1}} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast (\tilde{h}_{n}(2^{i-2^n}) \ast \alpha_n + b_j) = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_j) + \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{2^n+(j-1)} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_{2^n+j}) = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_j) + \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{2^n} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_{2^n+j}) = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_j) + \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast (\alpha_n + 1)) \varphi^{j-1} \ast (\tilde{h}_{n}(2^j) \ast \alpha_n + b_{2^n+j}) = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast \tilde{h}_{n}(2^j) \ast \alpha_n + \sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast b_j + \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast \tilde{h}_{n}(2^j) \ast \alpha_n + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{j-1} \ast \tilde{h}_{n}(2^j) \ast \alpha_n = \\
\sum_{j=1}^{2^n} (2^{i-2^n} \ast \alpha_n) \varphi^{j-1} \ast b_{2^n+j} + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{j-1} \ast b_{2^n+j}.
\]
\[
= \sum_{j=1}^{2^n} (2^{i-2^n} \alpha_n) \varphi^{i-1} \ast (b_j + b_{2^n+j}) + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast \hat{h}_n(2^j) \ast \alpha_n \\
+ \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast b_{2^n+j} \\
= \sum_{j=1}^{2^n} (2^{i-2^n} \alpha_n) \varphi^{i-1} \ast \hat{h}_n(2^j) + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast \hat{h}_n(2^j) \ast \alpha_n \\
+ \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast b_{2^n+j} \quad \text{(by (3.45))} \\
= \sum_{j=1}^{2^n} (2^{i-2^n} \varphi^{i-1} \ast \alpha_n \varphi^{i-1}) \ast \hat{h}_n(2^j) + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast \hat{h}_n(2^j) \ast \alpha_n \\
+ \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast b_{2^n+j} \\
= \sum_{j=1}^{2^n} (2^{i-2^n} \varphi^{i-1} \ast \hat{h}_n(2^j)) \ast (\alpha_n \varphi^{i-1} + \alpha_n) + \sum_{j=1}^{2^n} 2^{i-2^n} \varphi^{i-1} \ast b_{2^n+j} \\
< \alpha_n \quad \text{(since } 2^{i-2^n} \varphi^{i-1}, \hat{h}_n(2^j), \alpha_n \varphi^{i-1} + \alpha_n, b_{2^n+j} < \alpha_n).}
\]

Hence we have \( h_{n+1}(2^i) \in GF(\alpha_n), \text{ for } x \in GF(\alpha_{n+1}). \)

**Lemma 3.54** \([f_n^{-1}]_{i+2^n-1,j+2^n-1} = [f_n^{-1}]_{i,j+2^n-1} = [f_n^{-1}]_{i,j}\)

**Proof.** For \(1 \leq i, j < 2^n-1\),

\[
[f_n^{-1}]_{i+2^n-1,j+2^n-1} \\
= P_{2^n-(j+2^n-1)} \varphi^{i+2^n-1} \quad \text{(by Corollary 3.35)} \\
= P_{2^n-i-j} \varphi^{i+2^n-1-1} \\
= P_{2^n-2+(2^n-2-j)} \varphi^{i-2^n-1} \\
= (P_{2^n-2+(2^n-2-j)} \varphi^{2^n-1}) \varphi^{i-1} \\
= P_{2^n-2+(2^n-2-j)} \varphi^{i-1}, \quad \text{since } P_{2^n-2+(2^n-2-j)} < \alpha_{n-1}, \text{ and by Lemma 3.4} \\
= P_{2^n-(j+2^n-1)} \varphi^{i-1}
\]
Also, since \([f_{n-1}]_{i,j+2^n-1} = P_{2n-2(j+2^n-1)} \varphi^{i-1} = P_{2n-1-j} \varphi^{i-1} = [f_{n-1}]_{i,j}\), we then have
\([f_{n-1}]_{i+2^n-1,j+2^n-1} = [f_{n-1}]_{i,j+2^n-1} = [f_{n-1}]_{i,j}\). \(\square\)

Lemma 3.55 \([f_{n-1}]_{i,j} < \alpha_n\), for \(1 \leq i, j \leq 2^n\).

**Proof.** By Corollary 3.35, we have \([f_{n-1}]_{i,j} = P_{2n-j} \varphi^{i-1}\) for \(1 \leq i, j \leq 2^n\). But \(P_{2n-j} < P_{2n} = \alpha_n + 1\) and \(P_{2n-j} \neq \alpha_n\), so we have \(P_{2n-j} < \alpha_n\), and so \([f_{n-1}]_{i,j} = P_{2n-j} \varphi^{i-1} < \alpha_n\), since \(\text{GF}(\alpha_n)\) is closed under \(\varphi\). \(\square\)

Corollary 3.56 \([f_{n-1}]_{i,j+2^n-1} < \alpha_{n-1}\), for \(1 \leq i \leq 2^n\) and \(1 \leq j \leq 2^{n-1}\).

**Proof.** Follows by Lemma 3.54 and Lemma 3.55. \(\square\)

Lemma 3.57 \([f_{n-1}]_{1,j} = [f_{n-1}]_{1,j+2^{n-1}} \ast (\alpha_{n-1} + 1)\) for \(1 \leq j \leq 2^{n-1}\).

**Proof.** We know \([f_{n-1}]_{1,j} = P_{2n-j}\) and \([f_{n-1}]_{1,j+2^{n-1}} = P_{2n-(j+2^{n-1})}\). Now since \(1 \leq j \leq 2^{n-1}\), so \(2^{n-1} \leq 2^n - j \leq 2^n - 1\). Hence the decomposition of \(2^n - j\) as a sum of powers of \(2\) contains \(2^{n-1}\) for every \(1 \leq j \leq 2^{n-1}\). Also, \(2^n - j = (2^n - (j + 2^{n-1})) + 2^{n-1}\). So by Corollary 3.15, \(P_{2n-j} = P_{2n-(j+2^{n-1})} \ast P_{2n-1} = P_{2n-(j+2^{n-1})} \ast (\alpha_{n-1} + 1)\). Hence \([f_{n-1}]_{1,j} = [f_{n-1}]_{1,j+2^{n-1}} \ast (\alpha_{n-1} + 1)\). \(\square\)

Lemma 3.58 For \(1 \leq i \leq 2^n\) and \(1 \leq j \leq 2^{n-1}\), \([f_{n-1}]_{i,j} = [f_{n-1}]_{i,j+2^{n-1}} \ast \alpha_{n-1} + C_{n,i,j}\)

for some \(C_{n,i,j} < \alpha_{n-1}\).

**Proof.** For \(1 \leq i \leq 2^n\) and \(1 \leq j \leq 2^{n-1}\),

\([f_{n-1}]_{i,j} = [f_{n-1}]_{i,j} \varphi^{i-1}\) (by Corollary 3.35)
\[
\begin{align*}
&= ([f^{-1}]_{i,j+2^n-1} \ast (\alpha_{n-1} + 1))\varphi^{i-1} \quad \text{(by Lemma 3.57)} \\
&= ([f^{-1}]_{i,j+2^n-1} \ast \alpha_{n-1}) \varphi^{i-1} + [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \\
&= [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \ast \alpha_{n-1} \varphi^{i-1} + [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \\
&= [f^{-1}]_{i,j+2^n-1} \ast \alpha_{n-1}\varphi^{i-1} + [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \quad \text{(by Corollary 3.35)} \\
&= [f^{-1}]_{i,j+2^n-1} \ast (\alpha_{n-1} + \sum_{j=0}^{i-2} \beta_{n-1} \varphi^j) \\
&\quad + [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \quad \text{(by Lemma 3.7)} \\
&= [f^{-1}]_{i,j+2^n-1} \ast \alpha_{n-1} + [f^{-1}]_{i,j+2^n-1} \ast \sum_{j=0}^{i-2} \beta_{n-1} \varphi^j + [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \\
&= [f^{-1}]_{i,j+2^n-1} \ast \alpha_{n-1} + C_{n,i,j}, \quad \text{for some } C_{n,i,j} < \alpha_{n-1}. \\
&\quad \text{(since } \sum_{j=0}^{i-2} \beta_{n-1} \varphi^j < \alpha_{n-1} \text{ and } [f^{-1}]_{i,j+2^n-1}, \ [f^{-1}]_{i,j+2^n-1} \varphi^{i-1} \\
&\quad < \alpha_{n-1} \text{ by Corollary 3.56 and since } GF(\alpha_n) \text{ is closed under } \varphi).\square
\end{align*}
\]

**Theorem 3.59** Small, coherent sequences nest: \( C \cap S \subseteq N \). In other words, if a sequence of \( GF(2) \)-linear functions \( \{h_n : GF(\alpha_n) \to GF(\alpha_n)\} \) ultimately has \( h_n(x) \in GF(\alpha_{n-1}) \), for \( x \in GF(\alpha_n) \) and \( h_n(2^i) = h_{n-1}(2^i) \), for \( 0 \leq i < 2^{n-1} \), then 
\[
\text{Tr}_{\alpha_{n-1}}(\tilde{h}_n(2^i)) = \text{Tr}_{\alpha_{n-1}}(\tilde{h}_n(2^{i+2^{n-1}}))
\]
\[
= \tilde{h}_{n-1}(2^i) \quad \text{for } 0 \leq i < 2^{n-1}.
\]

**Proof.** For \( 1 \leq i \leq 2^{n-1} \),
\[
\tilde{h}_n(2^i) = \sum_{j=1}^{2^n} [f^{-1}]_{i,j} \ast h_n(2^{j-1})
\]
\[
= \sum_{j=1}^{2^n-1} [f^{-1}]_{i,j} \ast h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} [f^{-1}]_{i,j} \ast h_n(2^{j-1})
\]
\[
= \sum_{j=1}^{2^n-1} ([f^{-1}]_{i,j+2^n-1} \ast \alpha_{n-1} + C_{n,i,j}) \ast h_n(2^{j-1}) + \sum_{j=2^{n-1}+1}^{2^n} [f^{-1}]_{i,j} \ast h_n(2^{j-1})
\]
\[
\quad \text{(for some } C_{n,i,j} < \alpha_{n-1}, \text{ by Lemma 3.58)}
\]

\[
\]
\[
\sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i, 2^n-1, j} * h_n(2^i) + \sum_{j=1}^{2^{n-1}} C_n, i, j * h_n(2^j-1) + \\
\sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i, j} * h_n(2^j-1).
\]

Now since \(C_{n, i, j} < \alpha_{n-1}\), \(h_n(2^j-1) < \alpha_{n-1}\) by smallness, and \([f_n^{-1}]_{i, j} < \alpha_{n-1}\) for \(1 \leq i \leq 2^n, 2^n + 1 \leq j \leq 2^n\) by Corollary 3.56. Thus for some \(C_i < \alpha_{n-1}\), one has

\[
h_n(2^i) = \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i, 2^n-1, j} * h_n(2^i) * \alpha_{n-1} + C_i
\]

\[
= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i, j} * h_n(2^j-1) * \alpha_{n-1} + C_i \quad \text{(by Lemma 3.4)}
\]

\[
= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i, j} * h_n(2^j-1) * \alpha_{n-1} + C_i \quad \text{(by hypothesis)}
\]

So we have \(Tr_{\alpha_{n-1}}(\hat{h}_n(2^i)) = \hat{h}_{n-1}(2^i)\). Also,

\[
\hat{h}_n(2^{i+2^n-1}) = \sum_{j=1}^{2^n} [f_n^{-1}]_{i, 2^n, j} * h_n(2^i)
\]

\[
= \sum_{j=1}^{2^{n-1}} [f_n^{-1}]_{i, 2^n, j} * h_n(2^i) + \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i, 2^n-1, j} * h_n(2^i)
\]

\[
= \sum_{j=1}^{2^{n-1}} [(f_n^{-1})_{i, 2^n, j} * \alpha_{n-1} + C_{n, i, 2^n, j}] * h_n(2^i) + \\
\sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i, 2^n-1, j} * h_n(2^i) \quad \text{(for some } C_{n, i, 2^n-1, j} < \alpha_{n-1}, \text{ by Lemma 3.58)}
\]

\[
= \sum_{j=1}^{2^n} [f_n^{-1}]_{i, 2^n-1, j} * \alpha_{n-1} * h_n(2^j-1) + \sum_{j=1}^{2^{n-1}} C_{n, i, 2^n-1, j} * h_n(2^j-1)
\]

\[
+ \sum_{j=2^{n-1}+1}^{2^n} [f_n^{-1}]_{i, 2^n-1, j} * h_n(2^j-1).
\]

Now since \(C_{n, i, 2^n-1, j} < \alpha_{n-1}\), \(h_n(2^j-1) < \alpha_{n-1}\) by smallness, and \([f_n^{-1}]_{i, 2^n-1, j} < \alpha_{n-1}\) for \(1 \leq i \leq 2^n\), we have \(2^{n-1} + 1 \leq j \leq 2^n\) by Corollary 3.56. Thus for some
\[ C_i < \alpha_{n-1}, \]

\[ \tilde{h}_n(2^i) = \left( \sum_{j=1}^{2^n-1} [f_{n-1}]_{i+j+2^{n-1}, i+2^{n-1}} \ast h_n(2^{j-1}) \right) \ast \alpha_{n-1} + C_i \]

\[ = \left( \sum_{j=1}^{2^n-1} [f_{n-1}]_{i,j} \ast h_n(2^{j-1}) \right) \ast \alpha_{n-1} + C_i \quad \text{(by Lemma 3.4)} \]

\[ = \left( \sum_{j=1}^{2^n-1} [f_{n-1}]_{i,j} \ast h_{n-1}(2^{j-1}) \right) \ast \alpha_{n-1} + C_i \quad \text{(by hypothesis)} \]

\[ = \tilde{h}_{n-1}(2^i) \ast \alpha_{n-1} + C_i. \]

So \( \text{Tr}_{\alpha_{n-1}}(\tilde{h}_n(2^{i+2^{n-1}})) = \tilde{h}_{n-1}(2^i) \), i.e. \( \{h_n\} \) nests. \( \square \)

**Corollary 3.60** For coherent sequences, the concepts of nesting and smallness coincide. Thus \( C \cap N = C \cap S. \square \)

**Lemma 3.61** \( \text{Tr}_{\alpha_{n-1}}(P_{2^n-i} \varphi^j) = P_{2^n-i} \varphi^j \) for \( 1 \leq i \leq 2^{n-1} \).

**Proof.** By Corollary 3.14, we have \( P_{2^n-i} \varphi^j = P_{2^n-1-i} \varphi^j \ast \alpha_{n-1} + P_{2^n-1-i} \ast \sum_{k=0}^{j-1} \beta_{n-1} \varphi^k + P_{2^n-1-i} \varphi^j \) for \( 1 \leq i \leq 2^{n-1} \). So \( \text{Tr}_{\alpha_{n-1}}(P_{2^n-i} \varphi^j) = P_{2^n-i} \varphi^j \), since \( P_{2^n-1-i} \ast \sum_{k=0}^{j-1} \beta_{n-1} \varphi^k + P_{2^n-1-i} \varphi^j < \alpha_{n-1} \). \( \square \)

**Lemma 3.62** For small sequences, nesting implies coherence : \( S \cap N \subset C \). In other words, if a sequence of GF(2)-linear functions \( \{h_n : \text{GF}(\alpha_n) \to \text{GF}(\alpha_n)\} \) ultimately has \( h_n(x) \in \text{GF}(\alpha_{n-1}) \), for \( x \in \text{GF}(\alpha_n) \) and \( \text{Tr}_{\alpha_{n-1}}(h_n(2^i)) = \text{Tr}_{\alpha_{n-1}}(h_{n-1}(2^{i+2^{n-1}})) = \tilde{h}_{n-1}(2^i) \) for \( 0 \leq i < 2^{n-1} \), then \( h_n(2^i) = h_{n-1}(2^i) \), for \( 0 \leq i < 2^{n-1} \).

**Proof.** First we denote \( h_{n-1}(2^i) \) by \( a_i \), and \( h_n(2^i) \) by \( b_i \), for \( 0 \leq i < 2^{n-1} \). Since \( \{h_n\} \) is a small sequence, we have \( a_i, b_i < \alpha_{n-1} \), for \( 0 \leq i < 2^{n-1} \). We want to show \( a_i = b_i \), for \( 0 \leq i < 2^{n-1} \). Since \( \{h_n\} \) is a nesting sequence, we have

\[ \text{Tr}_{\alpha_{n-1}}(h_n(2^i)) = \tilde{h}_{n-1}(2^i), \quad (3.46) \]
for $0 \leq i < 2^n-1$. Now by Corollary 3.35, $\tilde{h}_{n-1}(2^i) = \sum_{j=1}^{2^n-1} [f_{n-1}]_{i-(-1)j} \ast h_{n-1}(2^{j-1}) = \\
\sum_{j=1}^{2^n-1} P_{2n-1-j} \varphi^i \ast h_{n-1}(2^{j-1}) = \sum_{j=1}^{2^n-1} a_{j-1} \ast P_{2n-1-j} \varphi^i$ and $\tilde{h}_{n}(2^i) = \sum_{j=1}^{2^n-1} [f_{n}]_{i-(-1)j} \ast \\
h_{n-1}(2^{j-1}) = \sum_{j=1}^{2^n} P_{2n-j} \varphi^i \ast h_{n}(2^{j-1}) = \sum_{j=1}^{2^n} b_{j-1} \ast P_{2n-j} \varphi^i$. So, $\text{Tr}_{\alpha_{n-1}}(\tilde{h}_{n}(2^i))$ \\
= $\text{Tr}_{\alpha_{n-1}}\left(\sum_{j=1}^{2^n} b_{j-1} \ast P_{2n-j} \varphi^i}\right)$ \\
= $\text{Tr}_{\alpha_{n-1}}\left(\sum_{j=1}^{2^n} b_{j-1} \ast P_{2n-j} \varphi^i\right)$, since $P_{2n-j} \varphi^i < \alpha_{n-1}$, for $2^n-1 < j \leq 2^n$ \\
and $b_{j-1} < \alpha_{n-1}$, so $b_{j-1} \ast P_{2n-j} \varphi^i < \alpha_{n-1}$, for $2^n-1 < j \leq 2^n$. \\
= $\sum_{j=1}^{2^n} b_{j-1} \ast \text{Tr}_{\alpha_{n-1}}(P_{2n-j} \varphi^i)$ \\
= $\sum_{j=1}^{2^n} b_{j-1} \ast (P_{2n-j-1} \varphi^i)$ (by Lemma 3.61) \\
By Equation 3.46, we then have $\sum_{j=1}^{2^n-1} a_{j-1} \ast P_{2n-1-j} \varphi^i = \sum_{j=1}^{2^n-1} b_{j-1} \ast P_{2n-1-j} \varphi^i$, 
for $0 \leq i < 2^n-1$. i.e. $\sum_{j=1}^{2^n-1} (a_{j-1} + b_{j-1}) \ast P_{2n-1-j} \varphi^i = 0$, for $0 \leq i < 2^n-1$. i.e. \\
\[
\begin{bmatrix}
P_{2n-1-1} & P_{2n-1-2} & \ldots & P_0 \\
P_{2n-1-1} \varphi & P_{2n-1-2} \varphi & \ldots & P_0 \varphi \\
\vdots & \vdots & \ldots & \vdots \\
P_{2n-1-1} \varphi^{2n-1-1} & P_{2n-1-2} \varphi^{2n-1-1} & \ldots & P_0 \varphi^{2n-1-1}
\end{bmatrix}
\begin{bmatrix}
a_0 + b_0 \\
a_1 + b_1 \\
\vdots \\
a_{2n-1-1} + b_{2n-1-1}
\end{bmatrix}
= 0.
\]
Notice that the $2^n-1 \times 2^n-1$ matrix on the left hand side of the equality is $f_{n-1}^{-1}$. We know the det($f_{n-1}$) = 1 by Lemma 3.18, so det($f_{n-1}^{-1}$) = 1 too. Since the determine is not equal to 0, the equation above has unique solution which is the 0 vector. i.e. $a_i = b_i$, for $0 \leq i < 2^n-1$. So we proved $\{h_n\}$ is a coherent sequence. □

**Corollary 3.63** $C \cap N = N \cap S = S \cap C.$ □
References


Table 3.1: The $16 \times 16$ transform matrix $f_4$

$$
\begin{bmatrix}
\text{FFFF} & 5555 & 3333 & 1111 & 0F0F & 0505 & 0303 & 0101 & FF & 55 & 33 & 11 & F & 5 & 3 & 1 \\
9CAF & 785A & 2EE48 & 19C4 & 0959 & 07F7 & 02C2 & 0181 & 9C & 78 & 2E & 19 & 9 & 7 & 2 & 1 \\
CD64 & 46B8 & 3C41 & 1482 & 0C13 & 0421 & 03FA & 015F & CD & 46 & 3C & 14 & C & 4 & 3 & 1 \\
B380 & 6240 & 2750 & 1EF0 & 0B8A & 0645 & 025B & 01F6 & B3 & 62 & 27 & 1E & B & 6 & 2 & 1 \\
F0F2 & 5053 & 3034 & 1018 & 0FF0 & 0550 & 0330 & 0110 & F0 & 50 & 30 & 10 & F & 5 & 3 & 1 \\
95F5 & 7FAF & 2C8C & 1848 & 09C5 & 078F & 02EC & 0198 & 95 & 7F & 2C & 18 & 9 & 7 & 2 & 1 \\
C175 & 429A & 3FBE & 15D7 & 0CDE & 0467 & 03C6 & 014B & C1 & 42 & 3F & 15 & C & 4 & 3 & 1 \\
B809 & 6407 & 250C & 1F08 & 0B39 & 0627 & 027C & 01E8 & B8 & 64 & 25 & 1F & B & 6 & 2 & 1 \\
FF00 & 5500 & 3300 & 1100 & 0F00 & 0500 & 0300 & 0100 & FF & 55 & 33 & 11 & F & 5 & 3 & 1 \\
9C33 & 7822 & 2E66 & 19DD & 0550 & 07F0 & 02C0 & 0180 & 9C & 78 & 2E & 19 & 9 & 7 & 2 & 1 \\
CDA9 & 46FE & 3C7D & 1496 & 0C1F & 0425 & 03F9 & 015E & CD & 46 & 3C & 14 & C & 4 & 3 & 1 \\
B333 & 6222 & 2777 & 1EEE & 0B81 & 0643 & 0259 & 01F7 & B3 & 62 & 27 & 1E & B & 6 & 2 & 1 \\
F002 & 5003 & 3004 & 1008 & 0FF0 & 0555 & 0333 & 0111 & F0 & 50 & 30 & 10 & F & 5 & 3 & 1 \\
9560 & 7FD0 & 2CA0 & 1850 & 09CC & 0788 & 02EE & 0199 & 95 & 7F & 2C & 18 & 9 & 7 & 2 & 1 \\
C1B4 & 42D8 & 3F81 & 15C2 & 0CD2 & 0463 & 03C5 & 014A & C1 & 42 & 3F & 15 & C & 4 & 3 & 1 \\
B8B1 & 6463 & 2529 & 1F17 & 0B32 & 0621 & 027E & 01E9 & B8 & 64 & 25 & 1F & B & 6 & 2 & 1 
\end{bmatrix}
$$
Table 3.2: The first row of $f_4$ as Pascal’s Triangle modulo 2

\[
\begin{array}{cccccccccccc}
1 \\
1 & 1 \\
1 & 0 & 1 \\
1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\end{array}
\]
CHAPTER 4. EXPONENTIALIATION IN THE QUADRATIC CLOSURE OF GF(2)

Theorem 4.6 below represents a key result on exponentiation in the quadratic closure of GF(2). It was originally proved by H. W. Lenstra, Jr. in 1980 [Le2]. In this chapter, we give an alternative, more elementary approach to the proof of this result. First, it is convenient to establish some special notation. Set:

\[ S_n = \sum_{0 \leq i < j < 2^n} \beta_n \varphi^i \ast \beta_n \varphi^j \]  \hspace{1cm} (4.1)

\[ = \sum_{i=1}^{2^n-1} (\beta_n \varphi^i \ast \sum_{j=0}^{i-1} \beta_n \varphi^j) \]

\[ = \sum_{i=0}^{2^n-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1} \beta_n \varphi^j); \]

\[ T_n = \sum_{i=0}^{2^n-1-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j); \]  \hspace{1cm} (4.2)

\[ D_n = \sum_{i=0}^{2^n-1} (\beta_n \ast \beta_{n+1}) \varphi^i; \]  \hspace{1cm} (4.3)

\[ E_n = \sum_{i=0}^{2^n-1} (\beta_n \ast \beta_n \varphi) \varphi^i. \]  \hspace{1cm} (4.4)

Lemma 4.1 \( x \varphi^{2^n} = x + a, \) where \( x = a \ast \alpha_n + b, \) \( 0 \leq a, b < \alpha_n.\)
PROOF.

\[ x \varphi^{2^n} = (a * \alpha_n + b)\varphi^{2^n} \]
\[ = a\varphi^{2^n} * \alpha_n\varphi^{2^n} + b\varphi^{2^n} \]
\[ = a * (\alpha_n + 1) + b, \text{ since } 0 \leq a, b < \alpha_n \]
\[ = a * \alpha_n + a + b \]
\[ = a * \alpha_n + b + a \]
\[ = x + a. \square \]

Lemma 4.2 $\beta_n\varphi^{2^{n-1}} = \beta_n^{2^{n-1}} = \beta_n + \beta_{n-1}$.

PROOF.

\[ \beta_n\varphi^{2^{n-1}} = (\beta_{n-1} * \alpha_{n-1})\varphi^{2^{n-1}} \]
\[ = \beta_{n-1}\varphi^{2^{n-1}} * \alpha_{n-1}\varphi^{2^{n-1}} \]
\[ = \beta_{n-1} * (1 + \alpha_{n-1}), \text{ by Lemma 3.4 and Lemma 3.8} \]
\[ = \beta_{n-1} + \beta_{n-1} * \alpha_{n-1} \]
\[ = \beta_{n-1} + \beta_n, \text{ by Lemma 3.6}. \square \]

Lemma 4.3 If $a \in GF(\alpha_{n-1})$, then $a\varphi^{2^{n-1}} = a\varphi^{2^{n-1}-i}$.

PROOF. $a\varphi^{2^{n-1}} = a\varphi^{2^{n-1}-(2^{n-1}-i)} = a\varphi^{2^{n-1}+(2^{n-1}-i)} = (a\varphi^{2^{n-1}})\varphi^{(2^{n-1}-i)}$
\[ = a\varphi^{2^{n-1}-i}, \text{ by Lemma 3.4}. \square \]

Lemma 4.4 $\beta_n\varphi^k \geq \beta_n$, for all $n, k \geq 0$
PROOF. We will prove the lemma by induction on n.

(Base) We have $\beta_0 = 1$, and $\beta_0 \varphi^k = 1$ for all $k \geq 0$, so $\beta_0 \varphi^k \geq \beta_0$.

(IH) Assume $\forall k, \beta_n \varphi^k \geq \beta_n$.

(IS)

\[
\beta_{n+1} \varphi^k = (\alpha_n \ast \beta_n) \varphi^k, \text{ by Lemma 3.6}
\]

\[
= \alpha_n \varphi^k \ast \beta_n \varphi^k
\]

\[
= (\alpha_n + \sum_{i=0}^{k-1} \beta_n \varphi^i) \ast \beta_n \varphi^k, \text{ by Lemma 3.7}
\]

\[
= \beta_n \varphi^k \ast \alpha_n + (\sum_{i=0}^{k-1} \beta_n \varphi^i) \ast \beta_n \varphi^k.
\]

\[
\geq \beta_n \ast \alpha_n, \quad \text{since } \beta_n \varphi^k, (\sum_{i=0}^{k-1} \beta_n \varphi^i) \ast \beta_n \varphi^k < \alpha_n, \text{ and by (IH)}.
\]

\[
= \beta_{n+1}, \text{ by Lemma 3.6.}\]

\[\square\]

Lemma 4.5

If $\beta_n \ast \beta_n \varphi > \beta_n$, then $\beta_{n+1} \ast \beta_{n+1} \varphi < \beta_{n+1}$.

If $\beta_n \ast \beta_n \varphi < \beta_n$, then $\beta_{n+1} \ast \beta_{n+1} \varphi > \beta_{n+1}$.

PROOF.

\[
\beta_{n+1} \ast \beta_{n+1} \varphi = (\alpha_n \ast \beta_n) \ast (\alpha_n \ast \beta_n) \varphi
\]

\[
= \alpha_n \ast \beta_n \ast \alpha_n \varphi \ast \beta_n \varphi
\]

\[
= \alpha_n \ast \beta_n \ast (\alpha_n + \beta_n) \ast \beta_n \varphi
\]

\[
= \alpha_n \ast \beta_n \ast \alpha_n \ast \beta_n \varphi + \alpha_n \ast \beta_n \ast \beta_n \ast \beta_n \varphi
\]
\[
\alpha_n^2 \beta_n \beta_n \varphi + \alpha_n \beta_n \beta_n \beta_n \varphi \\
= (\alpha_n + \beta_n) \beta_n \beta_n \varphi + \alpha_n \beta_n \beta_n \beta_n \varphi \\
= \alpha_n (\beta_n \beta_n \varphi + \beta_n \beta_n \beta_n \varphi) + \beta_n \beta_n \beta_n \varphi \\
= \alpha_n (\beta_n \beta_n \varphi + \beta_n \varphi^2) + \beta_n \varphi^2.
\]

By Lemma 4.4, \(\beta_n \varphi^2 \geq \beta_n\). So if \(\beta_n \beta_n \varphi > \beta_n\), then \(\beta_n \beta_n \varphi + \beta_n \varphi^2 < \beta_n\), so \\
\(\beta_{n+1} \beta_{n+1} \varphi < \alpha_n \beta_n = \beta_{n+1}\), while if \(\beta_n \beta_n \varphi < \beta_n\), then \(\beta_n \beta_n \varphi + \beta_n \varphi^2 > \beta_n\), \\
so \(\beta_{n+1} \beta_{n+1} \varphi > \alpha_n \beta_n = \beta_{n+1}\). \(\square\)

**Corollary 4.6**

\[\beta_n \beta_n \varphi > \beta_n, \text{ when } n \text{ is even.}\]

\[\beta_n \beta_n \varphi < \beta_n, \text{ when } n \text{ is odd.}\]

**Proof.** \(\beta_1 \beta_1 \varphi = 2 \times 3 = 1 < 2 = \beta_1\).

The rest follows by induction using Lemma 4.5. \(\square\)

**Lemma 4.7** \(D_n = \alpha_n + E_n + S_n + \beta_n\).

**Proof.** \(D_n = \sum_{i=0}^{2^n-1} (\beta_n \beta_{n+1}) \varphi^i \)

\[= \sum_{i=0}^{2^n-1} (\alpha_n \beta_n \beta_n \varphi^i), \text{ by Lemma 3.6}\]

\[= \sum_{i=0}^{2^n-1} (\alpha_n \beta_n \varphi^i) \]

\[= \sum_{i=0}^{2^n-1} \alpha_n \varphi^i \beta_n \varphi^{i+1} \]

\[= \alpha_n \beta_n \varphi + \sum_{i=1}^{2^n-1} (\alpha_n \varphi^i \beta_n \varphi^{i+1})\]
\[
= \alpha_n \cdot \beta_n \varphi + \sum_{i=1}^{2^n-1} (\alpha_n + \sum_{j=0}^{i-1} \beta_n \varphi^j) \cdot \beta_n \varphi^{i+1} \\
= \alpha_n \cdot \beta_n \varphi + \sum_{i=1}^{2^n-1} \alpha_n \cdot \beta_n \varphi^{i+1} + \sum_{i=1}^{2^n-1} (\sum_{j=0}^{i-1} \beta_n \varphi^j) \cdot \beta_n \varphi^{i+1} \\
= \alpha_n \cdot (\beta_n \varphi + \sum_{i=1}^{2^n-1} \beta_n \varphi^{i+1}) + \sum_{i=1}^{2^n-1} (\sum_{j=0}^{i-1} \beta_n \varphi^j) \cdot \beta_n \varphi^{i+1} \\
= \alpha_n \cdot \sum_{i=0}^{2^n-1} \beta_n \varphi^{i+1} + \sum_{i=1}^{2^n-2} \left( \sum_{j=0}^{i-1} \beta_n \varphi^j \cdot \beta_n \varphi^{i+1} + \left( \sum_{j=0}^{2^n-2} \beta_n \varphi^j \right) \cdot \beta_n \varphi^{2n} \right) \\
= \alpha_n \cdot \left( \sum_{i=0}^{2^n-1} \beta_n \varphi^i \right) \varphi + \sum_{i=1}^{2^n-2} \left[ \left( \sum_{i=1}^{2^n-1} \beta_n \varphi^i \right) \cdot \beta_n \varphi^{i+1} \right] \\
+ (1 + \beta_n \varphi^{2^n-1}) \cdot \beta_n \varphi^{2n}, \text{ by Lemma 3.10} \\
= \alpha_n \cdot \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + \sum_{i=1}^{2^n-2} \left( \sum_{j=0}^{i-1} \beta_n \varphi^j \cdot \beta_n \varphi^{i+1} \right) + \beta_n \varphi^{2n} \\
= \beta_n \varphi^{2n} \cdot \beta_n \varphi^{2n-1}, \text{ by Lemma 3.10} \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + \sum_{i=1}^{2^n-2} \sum_{j=0}^{i-1} \beta_n \varphi^j \cdot \beta_n \varphi^{i+1} + \beta_n + \beta_n \varphi^{2n} \cdot \beta_n \varphi^{2n-1}, \\
\text{by Lemma 3.4 and change of indices} \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + \sum_{i=1}^{2^n-2} \sum_{j=0}^{i-1} \beta_n \varphi^j \cdot \beta_n \varphi^{i+1} + \beta_n + \beta_n \varphi + \beta_n \\
+ \beta_n \varphi^{2n} \cdot \beta_n \varphi^{2n-1} \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + \beta_n \varphi^{2n} \cdot \beta_n \varphi^{2n-1} + \sum_{i=1}^{2^n-1} \left( \sum_{j=0}^{i-1} \beta_n \varphi^j \right) \cdot \beta_n \varphi^i \\
+ \beta_n + \beta_n \varphi + \beta_n \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + (S_n + \beta_n + \beta_n) + \beta_n \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + \beta_n + \beta_n \varphi + \beta_n \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + S_n + \beta_n \\
= \alpha_n + \sum_{i=1}^{2^n-2} \left( \beta_n \varphi^i \cdot \beta_n \varphi^{i+1} \right) + S_n + \beta_n \\
= \alpha_n + \sum_{i=0}^{2^n-1} \left( \beta_n \varphi^i \right) + S_n + \beta_n \\
= \alpha_n + E_n + S_n + \beta_n, \text{ by (4.4).} \]
Corollary 4.8

If $n$ is even and $S_n = 0$, then $D_n = \alpha_n + \beta_n + 1$.

If $n$ is even and $S_n = 1$, then $D_n = \alpha_n + \beta_n$.

If $n$ is odd and $S_n = 0$, then $D_n = \alpha_n + \beta_n$.

If $n$ is odd and $S_n = 1$, then $D_n = \alpha_n + \beta_n + 1$.

PROOF. If $n$ is even, we have $\beta_n \beta_n \varphi > \beta_n$ by Corollary 4.6. So $E_n = \sum_{i=0}^{2^n-1} (\beta_n \beta_n \varphi)^i = 1$ by Lemma 3.10. If $n$ is odd, we have $\beta_n \beta_n \varphi < \beta_n$ by Corollary 4.6. So $E_n = \sum_{i=0}^{2^n-1} (\beta_n \beta_n \varphi)^i = 0$ by Lemma 3.9. The results follow by Lemma 4.7. □

Lemma 4.9 $\sum_{i=0}^{2^n-1} \beta_{n+1} \varphi^i = \alpha_n + S_n$.

PROOF.

\[
\sum_{i=0}^{2^n-1} \beta_{n+1} \varphi^i = \sum_{i=0}^{2^n-1} (\alpha_n \beta_n) \varphi^i, \text{ by Lemma 3.6}
\]

\[
= \alpha_n \beta_n + \sum_{i=1}^{2^n-1} \alpha_n \varphi^i \beta_n \varphi^i
\]

\[
= \alpha_n \beta_n + \sum_{i=1}^{2^n-1} \beta_n \varphi^i \alpha_n + \sum_{j=0}^{i-1} \beta_n \varphi^j, \text{ by Lemma 3.7}
\]

\[
= \alpha_n \beta_n + \sum_{i=1}^{2^n-1} \beta_n \varphi^i \alpha_n + \sum_{j=0}^{i-1} \beta_n \varphi^j
\]

\[
= \sum_{i=0}^{2^n-1} \beta_n \varphi^i \alpha_n + S_n, \text{ by (4.2)}
\]

\[
= \alpha_n + S_n, \text{ by Lemma 3.10}. \square
\]

Lemma 4.10 $\alpha_n^{\alpha_{n+1}} = \alpha_{n+1} + \alpha_n + S_n$. 
PROOF.
\[ n^+1 = \alpha_{n+1} \varphi^2 = 2 \alpha_n + \sum_{i=0}^{2^n-1} \beta_{n+1} \varphi^i, \text{ by Lemma 3.7} \]
\[ = \alpha^{n+1} + \alpha_n + S_n, \text{ by Lemma 4.9}. \]

Lemma 4.11 \( \alpha_n^\alpha_{n-1} = \alpha_{n} \varphi^{\alpha_{n-1}} = \alpha_n + \alpha_{n-1} + k_n, \text{ where } k_n = 0 \text{ or } 1. \)

PROOF.
\[ \alpha_n^{2n-1} = \alpha_n + \sum_{i=0}^{2n-1-1} \beta_n \varphi^i \]
\[ = \alpha_n + \alpha_{n-1} + (\sum_{i=0}^{2n-1-1} \beta_n \varphi^i), \text{ by Lemma 3.7}. \]

Let \( k_n = \alpha_{n+1} + \beta_{n} \varphi^i \). We have \( \alpha_n^\alpha_{n-1} = \alpha_n + \alpha_{n-1} + k_n, \)
and
\[ k_n \varphi = \alpha_{n-1} \varphi + \sum_{i=0}^{2n-1-1} \beta_n \varphi^{i+1} \]
\[ = \alpha_{n-1} + \beta_{n-1} + \sum_{i=1}^{2n-1} \beta_n \varphi^i, \text{ by Lemma 3.7 and change of indices}. \]

So
\[ k_n + k_n \varphi = \alpha_{n-1} + \beta_{n-1} + \sum_{i=0}^{2n-1-1} \beta_n \varphi^i + \alpha_n + \beta_n + \sum_{i=1}^{2n-1} \beta_n \varphi^i \]
\[ = (\beta_n + \sum_{i=0}^{2n-1-1} \beta_n \varphi^i) + \beta_n + (\sum_{i=1}^{2n-1-1} \beta_n \varphi^i + \beta_n \varphi^{2n-1}) \]
\[ = \beta_n + \beta_n + \beta_n + \beta_n, \text{ by Lemma 4.2} \]
\[ = 0. \]

Since \(0 = k_n + k_n \varphi = k_n + k_n^2 = k_n(1 + k_n), \) we have \( k_n = 0 \text{ or } k_n = 1, \)
i.e. \( \alpha_n^\alpha_{n-1} = \alpha_n + \alpha_{n-1} + k_n, \text{ where } k_n = 0 \text{ or } 1. \)
Lemma 4.12 \( \sum_{i=0}^{2^{n-1}-1} \beta_n \varphi^i \ast (\sum_{i=0}^{2^{n-1}-1} \beta_n \varphi^i) \varphi^{2^{n-1}} = \beta_{n-1}. \)

**Proof.**

From Lemma 4.11 and Lemma 3.7, we have \( \sum_{i=0}^{2^{n-1}-1} \beta_n \varphi^i = \alpha_{n-1} + k_n, \) where \( k_n = 0 \) or 1.

Also, since \( k_n = 0 \) or 1, so \( k_n \varphi^m = k_n, \) for all \( m. \) (*)

So

\[
\sum_{i=0}^{2^{n-1}-1} \beta_n \varphi^i \ast (\sum_{i=0}^{2^{n-1}-1} \beta_n \varphi^i) \varphi^{2^{n-1}} = (\alpha_{n-1} + k_n) \ast (\alpha_{n-1} + k_n) \varphi^{2^{n-1}} \\
= (\alpha_{n-1} + k_n)^2 (\alpha_{n-1} + k_n + k_n \alpha_{n-1} + k_n + k_n \alpha_{n-1} + k_n^2) \\
= \alpha_{n-1}^2 + k_n \alpha_{n-1} + \alpha_{n-1} + k_n + k_n \alpha_{n-1} + k_n^2 \\
= \alpha_{n-1}^2 + \alpha_{n-1} + k_n + k_n, \text{ by (*)} \\
= (\alpha_{n-1} + \beta_{n-1}) + \alpha_{n-1}, \text{ by Lemma 3.7} \\
= \beta_{n-1}. \square
\]

Lemma 4.13 \( T_n + T_n \varphi^{2^{n-1}} = \alpha_{n-1} + D_{n-1}. \)

**Proof.** \( T_n \varphi^{2^{n-1}} \)

\[
= \sum_{i=0}^{2^{n-1}-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^{n-1}-1} \beta_n \varphi^j) \varphi^{2^{n-1}} \\
= \sum_{i=0}^{2^{n-1}-2} (\beta_n \varphi^i \varphi^{2^{n-1}} \ast \sum_{j=i+1}^{2^{n-1}-1} \beta_n \varphi^{i+j}) \\
= \sum_{i=0}^{2^{n-1}-2} [(\beta_n \varphi^{2^{n-1}}) \varphi^i \ast \sum_{j=i+1}^{2^{n-1}-1} (\beta_n \varphi^{2^{n-1}}) \varphi^j]
\]
\begin{align*}
\sum_{i=0}^{2^n-1-2} [(\beta_n + \beta_{n-1})\varphi^i & \times \sum_{j=i+1}^{2^n-1-1} (\beta_n + \beta_{n-1})\varphi^j], \text{ by Lemma 4.2} \\
= \sum_{i=0}^{2^n-1-2} [(\beta_n\varphi^i + \beta_{n-1}\varphi^i) & \times \sum_{j=i+1}^{2^n-1-1} (\beta_n\varphi^j + \beta_{n-1}\varphi^j)] \\
= \sum_{i=0}^{2^n-1-2} (\beta_n\varphi^i & \times \sum_{j=i+1}^{2^n-1-1} \beta_n\varphi^j) + \sum_{i=0}^{2^n-1-2} (\beta_n\varphi^i & \times \sum_{j=i+1}^{2^n-1-1} \beta_{n-1}\varphi^j) \\
+ \sum_{i=0}^{2^n-1-2} (\beta_{n-1}\varphi^i & \times \sum_{j=i+1}^{2^n-1-1} \beta_n\varphi^j) + \sum_{i=0}^{2^n-1-2} (\beta_{n-1}\varphi^i & \times \sum_{j=i+1}^{2^n-1-1} \beta_{n-1}\varphi^j) \\
= T_n & + \sum_{i=0}^{2^n-1-2} (\beta_n\varphi^i \times \sum_{j=i+1}^{2^n-1-1} \beta_n\varphi^j) + \sum_{i=0}^{2^n-1-2} (\beta_n\varphi^i \times \sum_{j=i+1}^{2^n-1-1} \beta_{n-1}\varphi^j) + S_{n-1} \\
= T_n & + [\beta_n \times \sum_{j=i+1}^{2^n-1-1} \beta_n\varphi^j + \sum_{j=i+1}^{2^n-1-1} (\beta_n\varphi^i \times \sum_{j=i+1}^{2^n-1-1} \beta_n\varphi^j)] \\
+ \left[ \sum_{i=1}^{2^n-1-2} (\beta_n\varphi^i \times \sum_{j=0}^{2^n-1-1} \beta_{n-1}\varphi^j) + \beta_n\varphi^{2^n-1-1} \times \sum_{j=0}^{2^n-1-2} \beta_{n-1}\varphi^j \right] + S_{n-1} \\
= T_n + \beta_n & \times \sum_{i=1}^{2^n-1-1} \beta_{n-1}\varphi^j + \sum_{i=1}^{2^n-1-2} \beta_{n-1}\varphi^j + \sum_{i=1}^{2^n-1-2} \beta_{n-1}\varphi^j \times \sum_{j=0}^{2^n-1-1} \beta_{n-1}\varphi^j \\
+ \beta_n\varphi^{2^n-1-1} \times \sum_{j=0}^{2^n-1-2} \beta_{n-1}\varphi^j + S_{n-1} \\
= T_n & + \beta_n \times (\beta_n-1 + \sum_{j=0}^{2^n-1-1} \beta_{n-1}\varphi^j) + \sum_{i=1}^{2^n-1-2} \beta_{n-1}\varphi^j + \sum_{j=0}^{2^n-1-1} \beta_{n-1}\varphi^j \\
+ \beta_n\varphi^{2^n-1-1} \times (\sum_{j=0}^{2^n-1-1} \beta_{n-1}\varphi^j + \beta_{n-1}\varphi^{2^n-1-1}) + S_{n-1} \\
= T_n & + \beta_n \times (\beta_n-1 + 1) + \sum_{i=1}^{2^n-1-2} \left[ \beta_n\varphi^i \times (\beta_n-1\varphi^i + 1) \right] + \beta_n\varphi^{2^n-1-1} \times (1 + \beta_{n-1}\varphi^{2^n-1-1}) + S_{n-1}, \\
\text{by Lemma 3.10} \\
= T_n & + \sum_{i=0}^{2^n-1-1} [\beta_n\varphi^i \times (1 + \beta_{n-1}\varphi^i)] + S_{n-1} \\
= T_n & + \sum_{i=0}^{2^n-1-1} \beta_n\varphi^i + \sum_{i=0}^{2^n-1-1} \beta_{n-1}\varphi^i \times \beta_{n-1}\varphi^i + S_{n-1} \\
= T_n & + (\alpha_{n-1} + S_{n-1}) + D_{n-1} + S_{n-1}, \text{ by Lemma 4.9 and (4.3)} \\
= T_n & + \alpha_{n-1} + D_{n-1}. \\
\text{So } T_n + T_n\varphi^{2^n-1} = \alpha_{n-1} + D_{n-1}. \square
\end{align*}
Lemma 4.14 \( S_n = \beta_{n-1} + \alpha_{n-1} + D_{n-1} \).

Proof. \( S_n = \sum_{i=0}^{2^n-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1} \beta_n \varphi^j) \)

\( = \sum_{i=0}^{2^n-1-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1} \beta_n \varphi^j) + \sum_{i=2^n-2}^{2^n-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1} \beta_n \varphi^j) \)

\( = \sum_{i=0}^{2^n-1-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) + \sum_{i=2^n-1-2}^{2^n-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) \)

\( = \sum_{i=0}^{2^n-1-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) + \sum_{i=2^n-1-2}^{2^n-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) \)

\( + \sum_{i=0}^{2^n-1-2} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) + \sum_{i=2^n-1-2}^{2^n-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) \)

\( = \sum_{i=0}^{2^n-1-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) + \sum_{i=2^n-1-1}^{2^n-1} (\beta_n \varphi^i \ast \sum_{j=i+1}^{2^n-1-1} \beta_n \varphi^j) \)

\( = T_n + (\sum_{i=0}^{2^n-1-1} \beta_n \varphi^i) \ast (\sum_{j=0}^{2^n-1-1} \beta_n \varphi^j) \varphi^{2^n-1} + T_n \varphi^{2^n-1}, \text{ by (4.2)} \)

\( = T_n + T_n \varphi^{2^n-1} + (\sum_{i=0}^{2^n-1-1} \beta_n \varphi^i) \ast (\sum_{j=0}^{2^n-1-1} \beta_n \varphi^j) \varphi^{2^n-1} \)

\( = \alpha_{n-1} + D_{n-1} + \beta_{n-1} \), by Lemma 4.13 and Lemma 4.12. \( \square \)

Lemma 4.15 Let \( n = 4r + k \), where \( r \geq 0 \) and \( 0 \leq k < 4 \). Then we have:

\[ S_n = 0, \quad \text{when } k = 0 \text{ or } 3; \]

\[ S_n = 1, \quad \text{when } k = 1 \text{ or } 2. \] (4.5)

Proof. We will prove the lemma by induction on \( r \).

(Base) From Lemma 8, we have \( \alpha_{n+1} = \alpha_{n+1} + \alpha_n + S_n \). Now

\( \alpha_0 = \alpha_1 + \alpha_0 \), so \( S_0 = 0; \)
\( \alpha_2^{21} = \alpha_2 + \alpha_1 + 1, \) so \( S_1 = 1; \)
\( \alpha_3^{22} = \alpha_3 + \alpha_2 + 1, \) so \( S_2 = 1; \)
\( \alpha_4^{23} = \alpha_4 + \alpha_3, \) so \( S_3 = 0. \)

(IH) Assume (4.5) is true for \( r \leq t \) and \( 0 \leq k < 4. \)

(IS) We want to show (3.7) is true for \( r = t + 1 \) and \( 0 < k < 4 \) too.

(1) \( r = t + 1, k = 0: \) then \( n = 4(t + 1) + 0 = 4t + 4, \) and \( n - 1 = 4t + 3. \)
By (IH), we have \( S_{n-1} = S_{4t+3} = 0. \)
Since \( n - 1 = 4t + 3 \) is an odd number, we have \( D_{n-1} = \alpha_{n-1} + \beta_{n-1} \) by Corollary 4.5.
Now by Lemma 4.14, we have
\[
S_n = S_{4t+4} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} = \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1}) = 0.
\]

(2) \( r = t + 1, k = 1: \) then \( n = 4(t + 1) + 1 = 4t + 5, \) and \( n - 1 = 4t + 4. \)
By (1), we have \( S_{n-1} = S_{4t+4} = 0. \)
Since \( n - 1 = 4t + 4 \) is an even number, we have \( D_{n-1} = \alpha_{n-1} + \beta_{n-1} + 1 \) by Corollary 4.5.
Now by Lemma 4.14, we have
\[
S_n = S_{4t+5} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} = \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1} + 1) = 1.
\]

(3) \( r = t + 1, k = 2: \) then \( n = 4(t + 1) + 2 = 4t + 6, \) and \( n - 1 = 4t + 5. \)
By (2), we have \( S_{n-1} = S_{4t+5} = 1. \)
Since $n - 1 = 4t + 5$ is an odd number, we have $D_{n-1} = \alpha_{n-1} + \beta_{n-1} + 1$ by Corollary 4.5.

Now by Lemma 4.14, we have

\[
S_n = S_{4t+6} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} = \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1} + 1) = 1.
\]

(4) $r = t + 1, k = 3$: then $n = 4(t + 1) + 3 = 4t + 7$, and $n - 1 = 4t + 6$.

By (3), we have $S_{n-1} = S_{4t+6} = 1$.

Since $n - 1 = 4t + 6$ is an even number, we have $D_{n-1} = \alpha_{n-1} + \beta_{n-1}$ by Corollary 4.5.

Now by Lemma 4.14, we have

\[
S_n = S_{4t+7} = \beta_{n-1} + \alpha_{n-1} + D_{n-1} = \beta_{n-1} + \alpha_{n-1} + (\alpha_{n-1} + \beta_{n-1}) = 0.
\]

So we showed that (4.5) is true for $r = t + 1$ and $0 \leq k < 4$. □

**Theorem 4.16** Let $n = 4r + k$, where $r \geq 0$, and $0 \leq k < 4$. Then we have:

\[
\alpha_{n+1}^a = \alpha_{n+1} + \alpha_n, \quad \text{when } k = 0 \text{ or } 3;
\]

\[
\alpha_{n+1}^b = \alpha_{n+1} + \alpha_n + 1, \quad \text{when } k = 1 \text{ or } 2.
\]

**Proof.** By Lemma 4.10 and Lemma 4.15. □
CHAPTER 5. CONCLUSION

The loop transversal method is a new approach to the design of linear error-correcting block codes. In the binary case, greedy loop transversal codes coincide with the Conway/Sloane lexicodes. However, in a good channel, the greedy loop transversal method provides a more efficient way of constructing these codes. It has been used to determine the dimensions of the codes for channel lengths up to the sixties (and three hundreds for double errors). In the ternary case, loop transversal codes are not lexicodes. The greedy loop transversal method is being used in an attempt to construct “record breaking” codes.

The graphs of the syndrome functions of the loop transversal codes in the binary case have curious fractal properties. The syndrome functions may be interpreted as polynomials in Conway’s field $\mathbb{O}_2$. Passing from such a polynomial function to its coefficient sequence provides a linear transform, analogous to the discrete Fourier transform. Despite the sizes of the transform matrices, we are able to construct the inverse matrices. Also, some interesting properties inherent in the field $\mathbb{O}_2$ are discussed.

The inverse transformation matrices $F_{2^n}$ obtained in Chapter 3 may be used to derive the transforms, i.e. the coefficient sequences, of the greedy white-noise binary syndromes presented in Chapter 2. Figures 5.1 - 5.4 display the 32-dimensional
transforms of the $t$-error syndromes, for $1 \leq t \leq 4$. Figure 5.5 displays the 256-dimensional transform of the 2-error syndrome. Two features are readily apparent from these transforms. The first is the apparent simplicity of the transforms when compared with the original syndromes. The second is the similarity of the transforms for the various values of $t$. This similarity illustrates the way in which the syndrome functions generalize the logarithm function.

Future topics include the investigation of methods for the construction of linear codes in modules over rings and corresponding non-linear binary codes.
Figure 5.1: Transformed syndrome function (n=32, t=1)
Figure 5.2: Transformed syndrome function (n=32, t=2)
Figure 5.3: Transformed syndrome function (n=32, t=3)
Figure 5.4: Transformed syndrome function (n=32, t=4)
Figure 5.5: Transformed syndrome function (n=256, t=2)
BIBLIOGRAPHY


