Computational Complexity of Finite Field Multiplication

Examensarbete utfört i Datatransmission
vid Linköpings Tekniska Högskola

Nils-Hassan Quttineh

LiTH-ISY-EX-3402-2003
Linköping 2003

Computational Complexity of Finite Field Multiplication

Examensarbete utfört i Datatransmission
vid Tekniska Högskolan i Linköping

Nils-Hassan Quttineh

LiTH-ISY-EX-3402-2003

Supervisor: **Mikael Olofsson**
Examiner: **Mikael Olofsson**

Linköping 29th August 2003

Computational Complexity of Finite Field Multiplication

© 2003 Nils-Hassan Quttineh

This document was prepared using LaTeX 2_ε. Algorithms were implemented using `MAGMA` (from University of Sydney). All plots included were produced using `MATLAB` (from MathWorks, Inc.).

Abstract

The subject for this thesis is to find a basis which minimizes the number of bit operations involved in a finite field multiplication. The number of bases of a finite field increases quickly with the extension degree, and it is therefore important to find efficient search algorithms. Only fields of characteristic two are considered.

A complexity measure is introduced, in order to compare bases. Different methods and algorithms are tried out, limiting the search in order to explore larger fields. The concept of equivalent bases is introduced.

A comparison is also made between the Polynomial, Normal and Triangular Bases, referred to as known bases, as they are commonly used in implementations. Tables of the best found known bases for all fields up to $\mathbb{F}_{2^{24}}$ is presented.

A list of the best found bases for all fields up to $\mathbb{F}_{2^{25}}$ is also given.

Notations

Symbol	Description	Page
p	a prime number	5
q	a prime power, p^m	5
m	degree or dimension	6
$\mathbb{F}_q$	ground field	6
$\mathbb{F}_q^*$	multiplicative group	5
$\mathbb{F}_{q^m}$	extension field	6
α	primitive element	6
$p(x)$	primitive polynomial	6
Tr( )	trace function	9
θ	a basis	6
θ'	the dual basis	10
θ^q	equivialent basis of θ	17
$\boldsymbol{a}$	coordinate-vector for an element	11
$\boldsymbol{T_k}(\theta)$	the k:th matrix for basis θ	13
$\boldsymbol{w}(T)$	the weight of a matrix	14
$\boldsymbol{C}(\theta)$	complexity of basis θ	14
PB	Polynomial Basis	7
NB	Normal Basis	8
TB	Triangular Basis	8
DP	The dual of a Polynomial Basis	10
DN	The dual of a Normal Basis	10
DT	The dual of a Triangular Basis	10
CL	Coset Leaders	20

Contents

Abstract **i**

Notations **iii**

1 Introduction **1**

1.1 Background 1

1.2 Problem Definition 2

1.3 Outline of the thesis 2

2 Mathematical Background **3**

2.1 Groups, Rings and Fields 3

2.2 Extension Fields 5

2.3 Bases 6

2.4 Trace Function 9

3 Multiplication **11**

3.1 Complexity 11

3.2 An Example 14

3.3 Equivalent Bases 17

4 Different Approaches and Results **23**

4.1 Presentation of Methods 23

4.2 Exhaustive Search 25

4.2.1 Algorithm 25

4.2.2 Results 26

4.3 Multiples of Polynomial Bases 28

4.3.1 Algorithm 28

4.3.2 Results 29

4.4 Limitation on the Multiples 30

4.4.1 Algorithm 30

4.4.2 Results 31

4.5 Structural Design Algorithm 31

4.5.1 Algorithm 32

4.5.2 Results 34

4.6 Conclusions 35

5 Comparison to Known Bases **37**

5.1 Known Bases 37

5.2 Dual relations 38

5.2.1 Polynomial Bases 39

5.2.2 Normal Bases 40

5.2.3 Triangular Bases 41

5.3 Polynomial and Normal Bases 42

5.4 Polynomial and Triangular Bases 43

5.5 Polynomial Bases and their Multiples 44

5.6 Summary 45

6 Conclusions and future research **47**

6.1 Conclusions 47

6.2 Future research 48

A Primitive polynomials **49**

A.1 Table of Primitive Polynomials over $\mathbb{F}_2$ 50

B Statistics **51**

B.1 Tables 51

B.2 Figures 53

C Figures **55**

C.1 Polynomial Bases 56

C.2 Normal Bases 63

C.3 Triangular Bases 70

C.4 Polynomial and Normal Bases 77

C.5 Polynomial and Triangular Bases 84

C.6 Multiples of Polynomial Bases 91

D Tables of Known Bases **99**

D.1 Polynomial Bases 100

D.2 Dual Polynomial Bases 101

D.3 Triangular Bases 102

D.4 Dual Triangular Bases 103

D.5 Normal Bases 104

Bibliography **105**

Chapter 1

Introduction

In this chapter an introduction to the problem is presented, together with some background information and an outline of this thesis.

1.1 Background

It is not unusual that mathematical areas when first discovered get classified as not useful for the daily life. This is the case for subjects like Abstract Algebra, Number Theory and Finite Fields. But since the enormous success of personal computers, a neverending request for safer and more correct transmission of information is seen.

The best examples of a daily life application of error-correcting codes are CD-records and CD-Roms. The information is encoded using Reed-Solomon (RS) codes, the most common type of error-correcting codes.

Another area is security applications, like bank services over the internet, sending important messages, secure phone lines and so on. The need for cryptography is constantly growing.

The Theory of Encryption and Coding Theory are both based on the mathematics of Finite Fields, also called Galois Fields. It is therefore important to find ways of improvement in the implementation of computations performed in Finite Fields.

1.2 Problem Definition

In order to perform arithmetical operations in finite fields, which is neccessary when considering cryptography and error-correcting applications, finite field arithmetics is needed.

The elements in a finite field can be represented in different ways, defined by the basis used. By changing basis representation, the amount of work connected to multiplication of elements could be decreased. A complexity measure is introduced, in order to compare bases.

The subject for this thesis is to find a basis which minimizes the number of bit operations involved in a finite field multiplication. Only fields of characteristic two are considered.

1.3 Outline of the thesis

The mathematical background needed throughout this thesis is presented in Chapter 2. The construction of finite fields and extension fields is explained, together with mathematical concepts used throughout this thesis.

In Chapter 3, we introduce a complexity measure, making it possible to compare bases. A small example is also found, in order for the reader to fully understand the difficulties involved.

Different methods and algorithms are presented in Chapter 4, together with the results. Conclusions and comments are also found here.

Chapter 5 includes a comparison of Polynomial, Normal and Triangular Bases to the results from the previous chapter. The result tells us which standard bases that are good when considering multiplication.

Finally, in Chapter 6, the results are summarized and commented. Also, some proposals and ideas for future research are presented.

Chapter 2

Mathematical Background

In this section we look into the mathematics needed for this thesis. Basic statements and standard material are given without proof. For more details and proofs, we refer to McEliece [1] and Herstein [2].

2.1 Groups, Rings and Fields

Definition 1 (Group) *A nonempty set of elements $\mathcal{G}$ is said to form a group if a binary operation is defined on $\mathcal{G}$, denoted $\circ$, such that*

1. Closure: *$a, b \in \mathcal{G}$ implies that $a \circ b \in \mathcal{G}$.*
2. Associativity: *$a, b, c \in \mathcal{G}$ implies that $a \circ (b \circ c) = (a \circ b) \circ c$.*
3. Identity: *There exists an element $e \in \mathcal{G}$ such that $a \circ e = e \circ a = a$ for all $a \in \mathcal{G}$.*
4. Inverse: *For every $a \in \mathcal{G}$ there exists an element $a^{-1} \in \mathcal{G}$ such that $a^{-1} \circ a = a \circ a^{-1} = e$.*

If $\circ$ is commutative, that is if $a \circ b = b \circ a$ holds for all $a, b \in \mathcal{G}$, then $\mathcal{G}$ is called an Abelian Group.

Both the identity element and the inverse of an element in a group $\mathcal{G}$ can be shown to be uniquely determined. The best example of an Abelian group

is the set of integers under addition. Considering all nonsingular matrices under the operation matrix-multiplication, we get a non-Abelian group.

Definition 2 (Ring) *A Ring $\mathcal{R}$ is a nonempty set under two binary operations, normally called addition, denoted by $+$, and multiplication, denoted by $\star$, with the following properties.*

1. *$\mathcal{R}$ is an Abelian group under addition.*
2. *For every $a, b \in \mathcal{R}$, the product $a \star b$ is in $\mathcal{R}$.*
3. *Multiplication is associative, that is $a \star (b \star c) = (a \star b) \star c$ holds for any $a, b, c \in \mathcal{R}$.*
4. *Multiplication is distributive over addition, that is $a \star (b + c) = a \star b + a \star c$ and $(b + c) \star a = b \star a + c \star a$ holds for any $a, b, c \in \mathcal{R}$.*

If the multiplication in $\mathcal{R}$ is commutative, that is if $a \star b = b \star a$ holds for any $a, b \in \mathcal{R}$, then $\mathcal{R}$ is called a commutative ring.

A ring is called a *ring with identity* if the ring has a multiplicative identity, that is, there exists an element 1 such that $a \star 1 = 1 \star a = a$ for all $a \in \mathcal{R}$.

The most commonly used ring is the integer ring, which is commutative and contains infinetly many elements. But there exists other rings, like the residue class of integers modulo n, denoted $\mathbb{Z}_n$. This is a commutative ring with a finite number of elements under addition and multiplication reduced modulo n. It contains exactly the n integer elements $\{0, 1, \ldots, n-1\}$.

Definition 3 (Field) *A field $\mathcal{F}$ is a commutative ring with the additional property that the set of nonzero elements of $\mathcal{F}$ form an Abelian group under multiplication. A field with finitely many elements is called a finite field.*

A field is simply a commutative ring in which we can divide by any nonzero element. The set $\mathbb{R}$ containing the real numbers and the set $\mathbb{Q}$ containing the rational numbers are examples of fields. A finite field is also called a Galois Field after the French mathematician Evartiste Galois, who lived in the 19th century.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Table 2.1: Addition and Multiplication tables for the Finite Field $\mathbb{F}_7$.

In order to find a finite field, we can remember the finite ring $\mathbb{Z}_n$ containing n elements. If we choose $n = p$, where p is a prime, we get a finite field with p elements. Those are normally referred to as prime fields, and will be denoted $\mathbb{F}_p$.[1] The nonzero elements of a field $\mathbb{F}_q$ will be referred to as the multiplicative group of $\mathbb{F}_q$ and usually denoted $\mathbb{F}_q^*$.

An example is presented in Table 2.1, where addition and multiplication tables for the finite field $\mathbb{F}_7$ is found.

2.2 Extension Fields

So far we have discussed finite fields with size equal to a prime. Is it possible to find a field containing 9 elements? To straighten things out, we present this lemma.

Lemma 1 *There exists a finite field with q elements if and only if q is a prime power, that is $q = p^m$, where p is a prime and m is a positive integer. Any two fields with the same number of elements are isomorphic, which means that there is a one-to-one mapping from one of the fields to the other such that the algebraic structure is preserved.*

Considering Lemma 1, one could say that only one finite field with q elements exists and will be denoted $\mathbb{F}_q$. We now want to construct $\mathbb{F}_{q^m}$, that is an extension of the field $\mathbb{F}_q$. Because of Lemma 1, we are guaranteed that such a field exists.

[1] The smalles field is $\mathbb{F}_2$, where addition and multiplication are performed modulo 2.

Definition 4 (Extension Field) *Let $\mathcal{F}$ and $\mathcal{K}$ be fields such that $\mathcal{F} \subset \mathcal{K}$ holds. Then $\mathcal{K}$ is called an extension of $\mathcal{F}$ and $\mathcal{F}$ is called a subfield of $\mathcal{K}$.*

The set of complex numbers $\mathbb{C}$ is an extension of the real numbers $\mathbb{R}$, constructed by adjoining a root of the irreducible polynomial $x^2 + 1$ over $\mathbb{R}$. The root is well known and is often denoted i. The same works for finite fields. Using a root of an irreducible polynomial over a prime field results in an extension of the prime field. First of all, we need to know what is meant by an irreducible polynomial over a field.

Definition 5 *A polynomial $p(x)$ that is divisible only by $\alpha \cdot p(x)$ or α, where $\alpha \in \mathbb{F}_q$, is called an irreducible polynomial over $\mathbb{F}_q$. If the leading term is equal to 1, the polynomial is called monic. A monic irreducible polynomial of degree ≥ 1 is called a prime polynomial.*

By adjoining a root of an irreducible polynomial of degree m over $\mathbb{F}_q$, an extension field $\mathbb{F}_{q^m}$ is constructed that contains exactly q^m elements. The field $\mathbb{F}_q$ will be refered to as the groundfield. The multiplicative group $\mathbb{F}_{q^m}^*$ of nonzero elements can be shown to be cyclic, meaning that it contains generators (at least one) which are called primitive elements. The order of such elements is equal to the size of $\mathbb{F}_{q^m}^*$, that is $q^m - 1$.

Definition 6 *A primitive polynomial is a prime polynomial having a primitive element as a root.*

To illustrate the construction of an extension field, an example is presented in Table 2.2, where the primitive polynomial $p(x) = x^3 + x + 1$ is used to define $\mathbb{F}_{2^3}$.

2.3 Bases

An extension field $\mathbb{F}_{q^m}$ can be constructed by adjoining a root of an irreducible polynomial of degree m over $\mathbb{F}_q$. Even more convenient, by using a primitive polynomial $p(x)$, the root will become a generator for $\mathbb{F}_{q^m}^*$. This can be seen as the set of polynomials over $\mathbb{F}_q$ reduced modulo $p(x)$. A finite field can also be viewed as a vector space of dimension m over $\mathbb{F}_q$. If we have a vector space, it is meaningful to talk about bases.

Exponential	*Polynomial*	*Basis* $\theta = \begin{pmatrix} \alpha & \alpha^2 & \alpha^6 \end{pmatrix}$
$\alpha^{-\infty}$	0	$\begin{pmatrix} 0 & 0 & 0 \end{pmatrix}$
α^0	1	$\begin{pmatrix} 0 & 1 & 1 \end{pmatrix}$
α^1	α	$\begin{pmatrix} 1 & 0 & 0 \end{pmatrix}$
α^2	α^2	$\begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$
α^3	$\alpha + 1$	$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$
α^4	$\alpha^2 + \alpha$	$\begin{pmatrix} 1 & 1 & 0 \end{pmatrix}$
α^5	$\alpha^2 + \alpha + 1$	$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$
α^6	$\alpha^2 + 1$	$\begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$

Table 2.2: Elements of $\mathbb{F}_{2^3}$ expressed in Exponential and Polynomial Form, and to the right expressed in the basis θ. Element α is a root of the primitive polynomial $x^3 + x + 1$.

There are many distinct bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, some of them have been looked deeper into and are well known. The most common ones are Polynomial Bases, also called standard or canonical. Other examples are Normal Bases and Triangular Bases. These bases are widely known and are already used in implementations. They will therefore be considered and used for comparison in future chapters, and deserve some special attention.

Definition 7 (Polynomial Basis) *Let ϑ be an element of $\mathbb{F}_{q^m}$ such that $\{\vartheta^i\}_{i=0}^{m-1}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $\{\vartheta^i\}_{i=0}^{m-1}$ is called a polynomial basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

It can be shown that there exists at least one polynomial basis of a field over any of it's subfields. The element $\vartheta \in \mathbb{F}_{q^m}$ generates a polynomial basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ if and only if ϑ is a root of an irreducible polynomial $p(x)$ of degree m over $\mathbb{F}_q$.

Example 1 *Let α be a root of the primitive polynomial $p(x) = x^3 + x + 1$ over $\mathbb{F}_2$. If we use $\vartheta = \alpha^2$ from the field $\mathbb{F}_{2^3}$, the result is a polynomial basis looking like*

$$\{ (\alpha^2)^i \}_{i=0}^{3-1} = \{ (\alpha^2)^0, (\alpha^2)^1, (\alpha^2)^2 \} = \{1, \alpha^2, \alpha^4\}$$

Definition 8 (Normal Basis) *Let ϑ be an element of $\mathbb{F}_{q^m}$ such that $\{\vartheta^{q^i}\}_{i=0}^{m-1}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $\{\vartheta^{q^i}\}_{i=0}^{m-1}$ is called a normal basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

There is always at least one normal basis of a field over any of it's subfields. One of the advantages of normal bases are that raising an element to power q is a simple cyclic shift of the vector representing the element.

Furthermore, $\{\vartheta^{q^i}\}_{i=0}^{m-1}$ is the set of all roots of $p(x)$. But it is important to notice that not all irreducible polynomials of degree m generate normal bases.

Example 2 *Once again, consider the field $\mathbb{F}_{2^3}$ where α is a root of the primitive polynomial $p(x) = x^3 + x + 1$ over $\mathbb{F}_2$. If we use $\vartheta = \alpha^2$ the result is a normal basis looking like*

$$\{\ (\alpha^2)^{2^i}\ \}_{i=0}^{3-1} \ = \ \{\ (\alpha^2)^{2^0}, (\alpha^2)^{2^1}, (\alpha^2)^{2^2}\ \} \ = \ \{\alpha^2, \alpha^4, \alpha\}$$

All elements of a normal basis are roots of the same irreducible polynomial over $\mathbb{F}_q$.

Definition 9 (Triangular Bases) *Let $\{\vartheta^i\}_{i=0}^{m-1}$ be a polynomial basis over $\mathbb{F}_q$ with ϑ being a root of the monic irreducible polynomial $p(x) = \sum_{i=0}^{m} p_i x^i$ over $\mathbb{F}_q$. Then $\{\sigma_j\}_{j=0}^{m-1}$ given by $\sigma_j = \sum_{i=0}^{m-1-j} p_{i+j+1}\vartheta^i$ is the triangular basis corresponding to $\{\vartheta^i\}_{i=0}^{m-1}$.*

The triangular bases will only be used in the purpose of comparison. To find information on the special features and applications of this basis, we refer to Olofsson [3, Ch. 4].

Example 3 *We use the same Polynomial Basis as in Example 1, that is* $\theta = \{1, \alpha^2, \alpha^4\}$*, with* $\vartheta = \alpha^2$*. The monic irreducible polynomial having* α^2 *as root is* $p(x) = x^3 + x + 1$*, with coefficients* $[1, 1, 0, 1]$*. The Triangular Basis* σ *corresponding to polynomial basis* θ *is*

$$\begin{aligned}
\boldsymbol{\sigma_0} = \textstyle\sum_{i=0}^{3-1-0} p_{i+0+1} \cdot (\alpha^2)^i &= p_1 \cdot (\alpha^2)^0 \ + \ p_2 \cdot (\alpha^2)^1 \ + \ p_3 \cdot (\alpha^2)^2 \\
&= 1 \cdot 1 + 0 \cdot \alpha^2 + 1 \cdot \alpha^4 \ = \ 1 + \alpha^4 \ = \ \boldsymbol{\alpha^5} \\
\boldsymbol{\sigma_1} = \textstyle\sum_{i=0}^{3-1-1} p_{i+1+1} \cdot (\alpha^2)^i &= p_2 \cdot (\alpha^2)^0 \ + \ p_3 \cdot (\alpha^2)^1 \ = \ 0 \cdot 1 + 1 \cdot \alpha^2 \ = \ \boldsymbol{\alpha^2} \\
\boldsymbol{\sigma_2} = \textstyle\sum_{i=0}^{3-1-2} p_{i+2+1} \cdot (\alpha^2)^i &= p_3 \cdot (\alpha^2)^0 \ = \ 1 \cdot 1 \ = \ \mathbf{1}
\end{aligned}$$

We conclude that the triangular basis corresponding to θ *is* $\sigma = \{\alpha^5, \alpha^2, 1\}$.

2.4 Trace Function

The trace function is a linear mapping over $\mathbb{F}_q$ from $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q$. With the use of this function, we can derive useful relations later.

Definition 10 (Trace) *Let* α *be an element of* $\mathbb{F}_{q^m}$*. The trace of* α *over* $\mathbb{F}_q$ *is defined as* $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) \triangleq \sum_{i=0}^{m-1} \alpha^{q^i}$.

If there is no confusion about which fields that are involved, we write $\mathrm{Tr}(\alpha)$. To learn more about the trace function, look into McEliece [1, Ch. 8].

Example 4 *Consider the field* $\mathbb{F}_{2^3}$ *and define* α *to be a root of the primitive polynomial* $p(x) = x^3 + x + 1$ *over* $\mathbb{F}_2$*. The trace of* α *over* $\mathbb{F}_2$ *is given by*

$$\mathrm{Tr}(\alpha) \ = \ \sum_{i=0}^{3-1} \alpha^{2^i} \ = \ \alpha + \alpha^2 + \alpha^4 \ = \ \alpha + \alpha^2 + (\alpha^2 + \alpha) \ = \ 0$$

A complete list with the trace for all elements in the finite field $\mathbb{F}_{2^3}$ can be found in Table 2.3, on page 10.

With the use of the trace function, a special kind of bases can now be defined.

Definition 11 (Dual Bases) *Let* $\{\theta_i\}_{i=0}^{m-1}$ *and* $\{\theta'_j\}_{j=0}^{m-1}$ *be bases of* $\mathbb{F}_{q^m}$ *over* $\mathbb{F}_q$*. If*

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\theta_i\theta'_j) \;=\; \begin{cases} 0 & , i \neq j \\ 1 & , i = j \end{cases}$$

holds, the bases are said to be dual.

The dual basis is sometimes called complementary basis. It can be shown that given a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, there exists a unique dual of that basis. The dual bases will play an important role later, when we formulate the problem of multiplication in finite fields.

Example 5 *The dual basis of* $\theta = \begin{pmatrix} \alpha^1 & \alpha^2 & \alpha^6 \end{pmatrix}$ *is here shown to be* $\theta' = \begin{pmatrix} \alpha^2 & \alpha^3 & \alpha^0 \end{pmatrix}$*. The values of the trace-function can be found in Table 2.3.*

$\mathrm{Tr}(\theta_i\,\theta'_j)$	α^2	α^3	α^0
α^1	1	0	0
α^2	0	1	0
α^6	0	0	1

The only products with trace-value equal to 1, are those where indices of the basis elements are the same. Therefore, the bases are said to be dual.

Element β	*Tr*(β)
0	0
1	1
α	0
α^2	0
α^3	1
α^4	0
α^5	1
α^6	1

Table 2.3: A table showing the trace for all elements of $\mathbb{F}_{2^3}$.

Chapter 3

Multiplication

A presentation of the problem to be solved, and all mathematical relations that will be needed in this thesis are derived. The complexity measure used throughout this thesis is introduced, followed by an example in order for the reader to fully understand the problem.

3.1 Complexity

The subject for this thesis is to find a basis which minimizes the number of bit operations involved in a finite field multiplication. In order to compare bases and fully understand the difficulties involved, we derive a mathematical formulation. From now on, only finite fields of the form $\mathbb{F}_{2^m}$ will be considered.

Assume that we want to multiply two elements in a field $\mathbb{F}_{2^m}$. We denote the elements α and β, and their product is called γ. The basis used will be denoted θ and it's dual basis θ'. The elements expressed in basis θ can be written as

$$\alpha = \sum_{i=0}^{m-1} a_i\theta_i \qquad \beta = \sum_{i=0}^{m-1} b_i\theta_i \qquad \gamma = \sum_{i=0}^{m-1} c_i\theta_i$$

where $\boldsymbol{a}, \boldsymbol{b}$ and $\boldsymbol{c}$ are the corresponding coordinate vector for the elements respectively.

With the use of this notation, the following equation is quickly noted.

$$\gamma = \alpha \cdot \beta = \sum_{i=0}^{m-1} a_i\theta_i \cdot \sum_{j=0}^{m-1} b_j\theta_j = \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \theta_i\theta_j \tag{3.1}$$

In the end, we want an expression where everything is described with elements exclusively from the ground field $\mathbb{F}_2$. On the following lines, we show how to find an expression for the coordinate vector of an element, using the trace function and the dual basis θ'.

Theorem 1 (Trace Relation) *Let $\gamma = \sum_{i=0}^{m-1} c_i \cdot \theta_i$ be an element in the extension field $\mathbb{F}_{2^m}$. Let θ be the basis used, and θ' it's dual basis. Then the following holds*

$$c_k \quad = \quad \mathrm{Tr}(\theta'_k\gamma) \tag{3.2}$$

For details on the proof, we refer to McEliece [1, page 111]. We are now ready to derive a relation between the coordinate vector $\boldsymbol{c}$ and the coordinate vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ expressed in basis θ, using the trace-function and the dual basis θ'.

Theorem 2 (Matrix Relation) *Let α and β represent two elements in the extension field $\mathbb{F}_{2^m}$, using the basis θ and dual basis θ'. Let γ represent the product of α and β, that is $\gamma = \alpha \cdot \beta$. Then it follows that*

$$c_k \quad = \quad \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \cdot \mathrm{Tr}(\theta'_k\theta_i\theta_j) \tag{3.3}$$

Proof: By using the linearity of the trace function, and with the help of Equations 3.1 and 3.2, we show the following:

$$\begin{aligned} c_k \overset{(3.2)}{=} Tr(\theta'_k\gamma) &\overset{(3.1)}{=} Tr\left(\theta'_k \cdot \left[\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \theta_i\theta_j\right]\right) \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \cdot Tr(\theta'_k\theta_i\theta_j) \end{aligned}$$

■

With the use of equation 3.3 we can now calculate each coordinate of the product, using only the coordinate vectors from the two operators and the basis used together with its corresponding dual basis. In the following page, some final arrangements are done, in order to get the desired expression.

Definition 12 (Matrix T_k) *The matrix used to describe the calculation of the k:th coordinate of* $\mathbf{c}$ *when performing multiplication in a Finite Field, using basis* θ *and it's dual basis* θ'*, will be denoted* $\boldsymbol{T_k}(\theta)$*.*

$$\boldsymbol{T_k}(\theta) \;=\; \begin{pmatrix} \mathrm{Tr}(\theta'_k\theta_0\theta_0) & \mathrm{Tr}(\theta'_k\theta_0\theta_1) & \dots & \mathrm{Tr}(\theta'_k\theta_0\theta_{m-1}) \\ \mathrm{Tr}(\theta'_k\theta_1\theta_0) & \mathrm{Tr}(\theta'_k\theta_1\theta_1) & \dots & \mathrm{Tr}(\theta'_k\theta_1\theta_{m-1}) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\theta'_k\theta_{m-1}\theta_0) & \mathrm{Tr}(\theta'_k\theta_{m-1}\theta_1) & \dots & \mathrm{Tr}(\theta'_k\theta_{m-1}\theta_{m-1}) \end{pmatrix}$$

We want to rearrange Equation 3.3 in order to clearly see what happens.

$$\boldsymbol{c_k} \;=\; \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_i b_j \cdot Tr(\theta'_k\theta_i\theta_j) \;=\; a \cdot \boldsymbol{T_k} \cdot b^T \tag{3.4}$$

where $\boldsymbol{T_k}$ is the matrix defined above.

With the use of Equation 3.4 we define the matrix $\boldsymbol{T_k}$ related to the computation of each coordinate $\boldsymbol{c_k}$, independent of the choise of elements to be multiplied. The contents of those matrices are the result of trace-operations, and therefore belongs to $\mathbb{F}_q$. As the only groundfield considered here is $\mathbb{F}_2$, the matrices contain 1:s and 0:s.

Each position in those matrices containing a 1 corresponds to a bit operation, known as XOR or AND, which is related to a time-cost. Therefore, a basis that generates sparce matrices[1] will be efficient considering finite field multiplication. As we are interested in the number of elements equal to 1 in the matrices $\boldsymbol{T_k}$, we define the weight of a matrix.

[1] A matrix where most elements are 0.

Definition 13 (Matrix Weight) *The weight of a matrix T, that is the number of nonzero elements in it, will be denoted by* $\boldsymbol{w}(T)$.

The weight of a matrix $\boldsymbol{T_k}$ will be equal to the number of inputs to the XOR-tree needed in order to calculate $\boldsymbol{c_k}$. The tree can be built using $\boldsymbol{w(T_k) - 1}$ two-inputs XOR. Using Definitions 12 and 13 we define a complexity related to each basis, that can be used to compare bases to each other.

Definition 14 (Complexity of a Basis) *The sum of all weights for the* $\boldsymbol{T_k}$ *matrices, defined by basis* θ *of dimension* m*, is the complexity of that basis.*

$$\boldsymbol{C}(\theta) \;=\; \sum_{k=0}^{m-1} \boldsymbol{w}(\boldsymbol{T_k}(\theta))$$

We have now defined a complexity that can be used to compare bases. The total number of nonzero elements in the m matrices $\boldsymbol{T_k}$, for $k \in \{0 \ldots m-1\}$, is a good measure of how efficient a basis will be in implementations. With this result in mind, we demonstrate a small example.

3.2 An Example

We want to multiply elements α^3 and α^5 from the field $\mathbb{F}_{2^3}$, where alpha is a root of the primitive polynomial $x^3 + x + 1$. We choose to use the basis $\theta = \begin{pmatrix} \alpha & \alpha^2 & \alpha^6 \end{pmatrix}$ and it's dual basis $\theta' = \begin{pmatrix} \alpha^2 & \alpha^3 & 1 \end{pmatrix}$. It is easy to do this by hand, and the result should of course be $\alpha^3 \cdot \alpha^5 = \alpha^8 = \alpha$. To perform the multiplication on bit-level, we express our elements as vectors with respect to the basis chosen. By using Equation 3.2 we find

$$\begin{array}{rcl} \boldsymbol{a} & = & \begin{pmatrix} Tr(\alpha^3 \cdot \alpha^2) & Tr(\alpha^3 \cdot \alpha^3) & Tr(\alpha^3 \cdot 1) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\ \boldsymbol{b} & = & \begin{pmatrix} Tr(\alpha^5 \cdot \alpha^2) & Tr(\alpha^5 \cdot \alpha^3) & Tr(\alpha^5 \cdot 1) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \end{array}$$

Using the formulas derived in the last section, we should now be able to perform the multiplication using only coordinate vectors $\boldsymbol{a}$ and $\boldsymbol{b}$.

In this example, where dimension $m = 3$, using bases θ and θ' defined as above, the calculations performed in order to find the coordinate c_0 would look like this:

$$
\begin{aligned}
\boldsymbol{c_0} &= \boldsymbol{a} \cdot \boldsymbol{T_0} \cdot \boldsymbol{b^T} \\
&= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\theta'_0\theta_0\theta_0) & Tr(\theta'_0\theta_0\theta_1) & Tr(\theta'_0\theta_0\theta_2) \\ Tr(\theta'_0\theta_1\theta_0) & Tr(\theta'_0\theta_1\theta_1) & Tr(\theta'_0\theta_1\theta_2) \\ Tr(\theta'_0\theta_2\theta_0) & Tr(\theta'_0\theta_2\theta_1) & Tr(\theta'_0\theta_2\theta_2) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\alpha^2\alpha\ \alpha) & Tr(\alpha^2\alpha\ \alpha^2) & Tr(\alpha^2\alpha\ \alpha^6) \\ Tr(\alpha^2\alpha^2\alpha) & Tr(\alpha^2\alpha^2\alpha^2) & Tr(\alpha^2\alpha^2\alpha^6) \\ Tr(\alpha^2\alpha^6\alpha) & Tr(\alpha^2\alpha^6\alpha^2) & Tr(\alpha^2\alpha^6\alpha^6) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\alpha^4) & Tr(\alpha^5) & Tr(\alpha^2) \\ Tr(\alpha^5) & Tr(\alpha^6) & Tr(\alpha^3) \\ Tr(\alpha^2) & Tr(\alpha^3) & Tr(\ 1\ ) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}}_{\boldsymbol{T_0}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \mathbf{1}
\end{aligned}
$$

In the first step we use Equation 3.4, insert the basis elements, and calculate the trace for all positions in matrix $\boldsymbol{T_0}$. Use Table 2.3 on page 10 to follow the calculations. Finally, the coordinate vectors are multiplied into the matrix, resulting in the scalar value 1. This is the value of coordinate $\boldsymbol{c_0}$.

The weight of matrix $\boldsymbol{T_0}$ is equal to 6. This should be noted as it will be used later, when calculating the complexity of basis θ. An important thing to understand is that, no matter which two elements we choose to multiply in $\mathbb{F}_{2^3}$, the matrices $\boldsymbol{T_k}$ calculated in this example will always be the same as long as basis θ is used. The only things changing are the coordinate vectors of the elements to be multiplied.

In the same way we find c_1 and c_2:

$$\begin{aligned}
\boldsymbol{c_1} &= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\theta_1'\theta_0\theta_0) & Tr(\theta_1'\theta_0\theta_1) & Tr(\theta_1'\theta_0\theta_2) \\ Tr(\theta_1'\theta_1\theta_0) & Tr(\theta_1'\theta_1\theta_1) & Tr(\theta_1'\theta_1\theta_2) \\ Tr(\theta_1'\theta_2\theta_0) & Tr(\theta_1'\theta_2\theta_1) & Tr(\theta_1'\theta_2\theta_2) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\alpha^5) & Tr(\alpha^6) & Tr(\alpha^3) \\ Tr(\alpha^6) & Tr(\ 1\ ) & Tr(\alpha^4) \\ Tr(\alpha^3) & Tr(\alpha^4) & Tr(\alpha\ ) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}}_{\boldsymbol{T_1}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \boldsymbol{0}
\end{aligned}$$

The weight of matrix $\boldsymbol{T_1}$ is equal to 6. Also notice that matrix $\boldsymbol{T_k}$ is symmetric.

$$\begin{aligned}
\boldsymbol{c_2} &= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\theta_2'\theta_0\theta_0) & Tr(\theta_2'\theta_0\theta_1) & Tr(\theta_2'\theta_0\theta_2) \\ Tr(\theta_2'\theta_1\theta_0) & Tr(\theta_2'\theta_1\theta_1) & Tr(\theta_2'\theta_1\theta_2) \\ Tr(\theta_2'\theta_2\theta_0) & Tr(\theta_2'\theta_2\theta_1) & Tr(\theta_2'\theta_2\theta_2) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} Tr(\alpha^2) & Tr(\alpha^3) & Tr(\ 1\ ) \\ Tr(\alpha^3) & Tr(\alpha^4) & Tr(\alpha\ ) \\ Tr(\ 1\ ) & Tr(\alpha\ ) & Tr(\alpha^5) \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}}_{\boldsymbol{T_2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \boldsymbol{0}
\end{aligned}$$

We can therefore conclude that $\boldsymbol{c} = \begin{pmatrix} \boldsymbol{1} & \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}$.

In the begining of this example, we expressed elements α^3 and α^5 using basis θ to get the coordinate vectors $\boldsymbol{a}$ and $\boldsymbol{b}$. Let us now go backwards and see what element corresponds to the coordinate vector $\boldsymbol{c}$.

$$\boldsymbol{c} \bullet \theta \;=\; \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \bullet \begin{pmatrix} \alpha & \alpha^2 & \alpha^6 \end{pmatrix} \;=\; 1{\cdot}\alpha + 0{\cdot}\alpha^2 + 0{\cdot}\alpha^6 \;=\; \boldsymbol{\alpha}$$

The calculation seems to be correct! The weight of $\boldsymbol{T_2}$ is 5, giving a total complexity of $\boldsymbol{C} = 6 + 6 + 5 = 17$. On page 18, we find a picture showing an implementation using the same basis as above.

3.3 Equivalent Bases

In the last part of this section, some final definitions and mathematical concepts are presented. They will be used and referred to in chapters to come. First of all, we look at a well known property of the trace function that will be very useful.

Lemma 2 *Consider the elements α and α^q from the field $\mathbb{F}_{q^m}$. The trace of α and α^q over $\mathbb{F}_q$ will always be the same. That is $Tr(\alpha) = Tr(\alpha^q)$.*

For proof, look into McEliece [1, Ch. 8]. This will be used to show that some bases have the same complexity, but first we introduce the terminology equivalent bases.

Definition 15 (Equivalent Bases) *Let $\{\theta_i\}_{i=0}^{m-1}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $\{\theta_i^q\}_{i=0}^{m-1}$ and $\{\theta_i\}_{i=0}^{m-1}$ are called equivalent bases. The notation θ^q will be used.*

Here follows a short proof supporting the statement that if θ is a basis, θ^q is also a basis.

Proof: We know that θ is a basis, meaning that its elements are lineary indepentant. We choose to express the elements of θ using a normal basis. The raising of an element to q is a simple cyclic shift of the vector representing the element in a normal basis, therefore we conclude that the elements are still linearly independent. ■

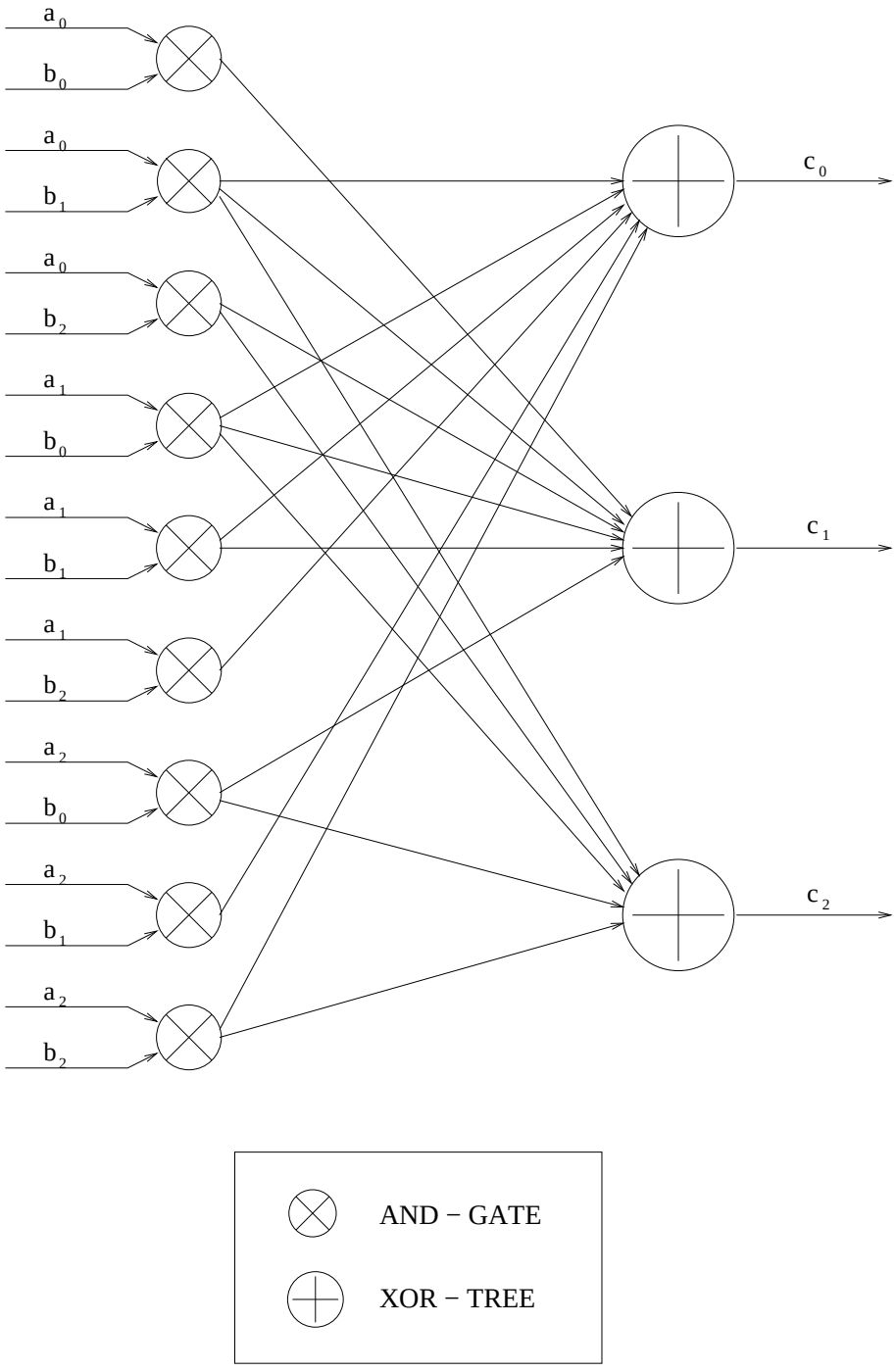

Figure 3.1: A figure showing the implementation of basis θ, taken from the exampel in Section 3.2.

When we refer to equivalent bases, it might sometimes be the set of equivalent bases, found by repeatedly finding the next equivalent basis.

$$\theta \longleftrightarrow \theta^q, \qquad \theta^q \longleftrightarrow (\theta^q)^q, \quad \ldots \quad , \theta^{q^{m-1}} \longleftrightarrow \theta^{q^m}$$

This can be described as the set of equivalent bases $\{ \theta, \theta^q, \ldots, \theta^{q^{m-1}} \}$, and will be referred to as an equivalence class of bases. Each class contains at most m different bases, as $\theta^{q^m} = \theta$. We should now try to motivate the name equivalent bases better. The main result is that if two bases are equivalent, they will have the same complexity. Before we can prove this, we need another theorem.

Theorem 3 *Let θ denote a basis and θ^q the equivalent basis. Furthermore, let θ' denote the dual basis of θ. Then the dual basis of θ^q is θ'^q.*

Proof: In general, for indicies i and j we get

$$Tr({\theta_i}^q \cdot {\theta'_j}^q) = Tr((\theta_i \cdot \theta'_j)^q) = Tr(\theta_i \cdot \theta'_j)$$

In the last step, we use Lemma 2. As θ and θ' are dual, and the trace of their product is equal to the trace for the product of θ^q and θ'^q, they must be dual as well. We also know that each basis has a unique dual basis, which is all we need to finish the proof. ■

We are now ready to prove our main result for this chapter.

Theorem 4 *If two bases are equivalent, then $\boldsymbol{T_k}(\theta)$ is equal to $\boldsymbol{T_k}(\theta^q)$, that is*

$$\boldsymbol{T_k}(\theta) = \boldsymbol{T_k}(\theta^q)$$

Proof: In general, on the i:th row and j:th column in matrix $\boldsymbol{T_k}(\theta^q)$, we have

$$Tr({\theta'_k}^q \cdot \theta_i^q \cdot \theta_j^q) = Tr((\theta'_k \cdot \theta_i \cdot \theta_j)^q) = Tr(\theta'_k \cdot \theta_i \cdot \theta_j)$$

■

We have shown that $\boldsymbol{T_k}(\theta)$ is equal to $\boldsymbol{T_k}(\theta^q)$ and therefore have the same weight. Then it follows directly that $\boldsymbol{C}(\theta) = \boldsymbol{C}(\theta^q)$, as the complexity by definition is equal to the sum of all weights of $\boldsymbol{T_k}$.

Corollary 1 *If two bases are equivalent, the complexity related to them will be the same.*

$$\boldsymbol{C}(\theta) = \boldsymbol{C}(\theta^q)$$

Together with the concept of equivalent bases, two other notations that are effective and helpful will be used. They are conjugacy classes and cyclotomic cosets. More information can be found in Wicker [4, Ch. 3].

Definition 16 (Conjugacy Classes) *Let α be an element in the finite field $\mathbb{F}_{q^m}$. The conjugates of α with respect to the subfield $\mathbb{F}_q$ are the elements $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \ldots$, and they form a set called the conjugacy class of α with respect to $\mathbb{F}_q$.*

All elements within a conjugacy class are equivalent to each other. Before we look at an example, another definition is presented, closely related to the conjugacy classes.

Definition 17 (Cyclotomic Cosets) *The Cyclotomic Cosets modulo n, where $n = q^m - 1$, with respect to the field $\mathbb{F}_q$ are a partitioning of the integers $\{\ 0, 1, \ldots, n-1\ \}$ into sets of the form*

$$\{a, aq, aq^2, aq^3, \ldots, aq^{d-1}\}$$

The cyclotomic cosets *modulo* n with respect to $\mathbb{F}_q$ thus contains the exponents of the elements in each conjugacy class. This is an effective way to describe different conjugacy classes.

In the same way, one could describe a basis as a set containing the exponents of the basis elements, expressed with the help of a primitive element from the field. A notation closely related to the cyclotomic cosets are the coset leaders. The easiest way to understand is to look at an example.

Example 6 *Let's use the field $\mathbb{F}_{2^3}$ defined by $x^3 + x + 1$ once again. In the following table, we can see how the conjugacy classes and cyclotomic cosets*

are related. The Coset Leaders, simply the first element from each coset, will be denoted CL.

CONJUGACY CLASS		*CYCLOTOMIC COSETS*		*COSET LEADERS*
$\{\alpha^0\}$	$\longleftrightarrow$	$\{0\}$		0
$\{\alpha^1, \alpha^2, \alpha^4\}$	$\longleftrightarrow$	$\{1, 2, 4\}$	$\Longrightarrow$	1
$\{\alpha^3, \alpha^6, \alpha^5\}$	$\longleftrightarrow$	$\{3, 6, 5\}$		3

Before we start to look at some algorithms that solves this problem, one last definition is presented.

Definition 18 (Multiple) *Let* $\{\theta_i\}_{i=0}^{m-1}$ *and* $\{\sigma_i\}_{i=0}^{m-1}$ *be two sets of elements from* $\mathbb{F}_{q^m}$*. If there exists a* $\beta \in \mathbb{F}_{q^m}^*$ *such that* $\sigma_i = \beta \cdot \theta_i$ *holds for all* $i \in \{0 \dots m-1\}$*, then* $\{\sigma_i\}_{i=0}^{m-1}$ *is called a multiple of* $\{\theta_i\}_{i=0}^{m-1}$*.*

It should be noticed that once you find a basis, it can be multiplied by any nonzero element from the field and still be a basis. Therefore, all multiples of a basis are also valid bases.

Example 7 *The elements are taken from the field* $\mathbb{F}_{2^3}$*. The set* $\{\alpha^3, \alpha^5, \alpha^6\}$ *is a multiple of* $\{\alpha^1, \alpha^3, \alpha^4\}$*, with* $\beta = \alpha^2$*.*

$$\{\alpha^3, \alpha^5, \alpha^6\} \;=\; \alpha^2 \bullet \{\alpha^1, \alpha^3, \alpha^4\}$$

Chapter 4

Different Approaches and Results

In this chapter, an introduction to the problem of finding valid bases is made, followed by a description of the different methods. Results from each method are also presented.

4.1 Presentation of Methods

To get an overview, we look at the second smallest extension field possible, namely $\mathbb{F}_{2^3}$. By adjoining a root α of the primitive polynomial $x^3 + x + 1$ over $\mathbb{F}_2$, we get the eight elements $\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. To find a basis for the vectorspace $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$, we need to choose three of the elements.

First of all, the 0-element cannot be used. That leaves us with only 7 elements to choose from. By using a well known formula from combinatorics, we calculate in how many ways we can choose three out of seven elements.

$$\binom{7}{3} = \frac{7!}{4! \cdot 3!} = 35$$

There are 35 possible combinations, but not all of them qualify as bases. In order to find out if a combination is a basis, a test is performed to see if the elements are linearly independent. If so, the combination works as a basis. Each element is mapped onto the groundfield $\mathbb{F}_2$ as vectors, using the

defining polynomial. These vectors are then tested for linear independence. If the vectors are linear indepentent, so are the elements.

Only 28 of the 35 combinations in $\mathbb{F}_{2^3}$ qualify as bases. One is the combination of elements α, α^2 and α^6, the basis used in Section 3.2. A complete list of bases for $\mathbb{F}_{2^3}$ can be found in Table 4.8, on page 36.

All elements of a field can be described as exponents of a primitive element. Therefore, the notation $\begin{pmatrix} \alpha^1 & \alpha^2 & \alpha^6 \end{pmatrix}$ for basis θ will be replaced with the set $\{ 1, 2, 6 \}$. During the search in a specific field, the same α is used all the time, and the only information needed is the exponential values.

A possible method is to search through all valid basis-combinations and calculate the complexity related to each one and save the best basis found. The single biggest problem with this method is that the number of combinations needed to search through increase rapidly when looking at bigger fields.

Consider the field $\mathbb{F}_{2^4}$ containing 15 nonzero elements. As the dimension m is 4, we need to choose four elements out of fifteen in order to find a basis. By using the same formula as before, we now get 1365 different combinations. This should be compared to the 35 combinations from the previous field.

$m :=$	Combinations $\binom{2^m-1}{m}$	# Bases
2	3	3
3	35	28
4	1.365	840
5	169.911	83.328
6	67.945.521	27.998.208
7	89.356.415.775	32.509.919.232
8	396.861.704.798.625	132.640.470.466.560

Table 4.1: A table showing the number of possible basis-combinations in each Finite Field $\mathbb{F}_{2^m}$ for dimensions 2 up to 8, along with the actual number of bases.

The number of possible combinations literally explode as we consider larger fields, which can be seen in Table 4.1. For instance, let us say that we can test 1.000.000 combinations each second. Even for the not so big field $\mathbb{F}_{2^8}$, including 256 elements, it would take approximately 12.5 years to search through all possible combinations! This fact makes it clear that such an approach does not hold in the long run.

4.2 Exhaustive Search

To start with, this is unexplored territory. To get an idea of what to look for, the first thing to do was to search through all possible basis combinations for small fields. This is a classical exhaustive search method.

4.2.1 Algorithm

The search algorithm is not hard to understand. One could say that it consists of one loop for each dimension m. All combinations are tested in order to find bases. The complexity for each basis is calculated, and if the value is better than the best found so far, the basis is saved. In pseudocode the algorithm looks like this for $m = 3$.

Algorithm 1 Exhaustive Search

Initialize $best = m^3$, $basis = \{\ \}$

```
 1: for i = 0 ... (q^m − 3) do
 2:   for j = i + 1 ... (q^m − 2) do
 3:     for k = j + 1 ... (q^m − 1) do
 4:       if { i, j, k } is a basis then
 5:         if Complexity of { i, j, k } < best then
 6:           best := Complexity
 7:           basis := { i, j, k }
 8:         end if
 9:       end if
10:     end for
11:   end for
12: end for
```

The variable *best* is initialized with m^3, the worst possible value of the complexity, corresponding to m matrices filled with 1:s on all $m \cdot m$ positions. When the algorithm is finished, variable *basis* contains the best found basis having a complexity equal to *best*.

This algorithm is easily extended to greater dimensions than m equal to 3. The only thing changing is that a new loop is added for each dimension, together with a counter, testing sets with m components.

The extra loop for each dimension is the reason why this algorithm does not work for larger fields. Each loop includes an exponential growth of elements, making it harder and harder to complete the search. It is impossible to search through all combinations even for quite small fields, already noticed in Table 4.1.

4.2.2 Results

The exhaustive search approach did not hold for long, but it gave us something to start with, an idea of what to look for. All fields up to $\mathbb{F}_{2^6}$ have been totally searched, and the results are positive. A statistical study of the field $\mathbb{F}_{2^6}$ can be found in Table 4.2, where some information is presented.

Tables for all fields between $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^6}$ can be found in Appendix B, together with figures of the distribution.

The standard bases seems to do quite well. Both the Polynomial Bases and their duals along with the Triangular Bases have representatives with complexity close to the best one found. The Normal Bases, on the other hand, does not seem to fit in at all.

Statistics for the Field $\mathbb{F}_{2^6}$ All 27.998.208 bases evaluated				
Basis	# Bases	# Eq.Classes	Complexity	Quota
Polynomial	54	9	48	1.0667
Normal	4	4	66	1.4667
Triangular	54	9	47	1.0444
Dual Polynomial	54	9	47	1.0444
Dual Triangular	54	9	51	1.1333
Best Found	6	1	45	-

Table 4.2: Statistics for $\mathbb{F}_{2^6}$. The column "Complexity" shows the best value found for each class of bases. The "Quota" is relative to the best found.

Considering Figures 4.1 and 4.2 showing the distribution of complexity over the bases for the fields $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^6}$, the trend is that a normal distribution is approached. The average values found in the search indicate this as well. This means that using a random choosen basis, the complexity will probably be bad.

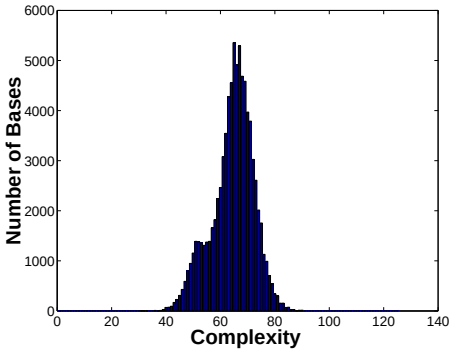

Figure 4.1: To the left, a diagram showing the distribution of 83.328 bases from $\mathbb{F}_{2^5}$. Lowest value found is 31 and the highest is 90. On average, a basis has a complexity of 64.5.

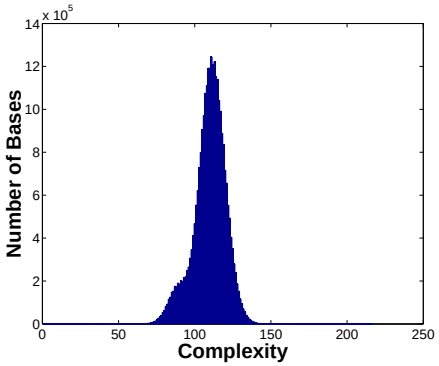

Figure 4.2: To the right, a diagram showing the distribution of 27.998.208 bases from $\mathbb{F}_{2^6}$. Lowest value found is 45 and the highest is 162. On average, a basis has a complexity of 109.7.

With knowledge of the best possible bases for smaller fields, we might find a pattern of some kind. Here follows a table presenting the best found bases for each field, along with the complexity and primitive polynomial used. Only one representative from each equivalence class is presented.

$m :=$	Polynomial	Basis	Complexity
2	$x^2 + x + 1$	{ 0, 1 }	5
3	$x^3 + x + 1$	{ -1, 0, 1 }	11
4	$x^4 + x + 1$	{ -1, 0, 1, 2 }	20
5	$x^5 + x^2 + 1$	{ -2, -1, 0, 1, 2 }	31
6	$x^6 + x + 1$	{-14, -7, 0, 7, 14, 21 }	45

Table 4.3: The best bases found in fields $\mathbb{F}_{2^m}$ for dimensions between 2 and 6.

We can see a clear trend. The features resemble the structure of Polynomial Bases. Exponent 0 is always part of a Polynomial Basis, and the other elements are generated from a given one, with the result of a common stepsize.

The similarities are obvious, and should be used to limit the search in a smart way. The structure of the best found bases are the same as for Polynomial Bases, but the elements are slightly shifted in order to center exponent 0.

4.3 Multiples of Polynomial Bases

The previous results, found with Algorithm 1, indicate that the structure of a basis with low complexity looks much like the Polynomial Bases, but with a shift of some kind. The idea is therefore to test all Polynomial Bases for each field, together with all multiples of them. This limits the search enormously and lets us carry on further up in the fields.

4.3.1 Algorithm

The definition of a polynomial basis follows here, to fresh up our memory.

Definition 7 (Polynomial Basis) *Let ϑ be an element of $\mathbb{F}_{q^m}$ such that $\{\vartheta^i\}_{i=0}^{m-1}$ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Then $\{\vartheta^i\}_{i=0}^{m-1}$ is called a polynomial basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.*

A polynomial basis is generated by one element from the present field, limiting the number of combinations to the size of the field. But the concept of equivalent bases makes it possible to reduce them even more.

Values from the same Cyclotomic Coset will generate equivalent Polynomial Bases. It is therefore enough to try all coset leaders for the field in question. Let CL denote the set of coset leaders, i.e. the first element from each coset.

Algorithm 2 Multiples of Polynomial Bases

Initialize $best = m^3$, $basis = \{\ \}$

```
1: for t ∈ CL do
2:    PB := possible Polynomial Basis generated by (α^t)
3:    if PB is a basis then
4:       for all Multiples of PB do
5:          if Complexity of Multiple < best then
6:             best := Complexity
7:             basis := Multiple
8:          end if
9:       end for
10:   end if
11: end for
```

Like the previous algorithm, variables *best* and *basis* are used to store the best found basis during the search. The first loop runs through all the Coset Leaders for the field in question, to see whether they work as a generator for a Polynomial Basis or not.

If an element does work, all possible multiples of the Polynomial Basis are tested. If the complexity of a certain multiple is better than the best basis found so far, it is saved along with the basis produced. This is repeated until all elements have been tried out together with all possible multiples.

4.3.2 Results

This algorithm clearly limits the search, meaning that we cannot be sure that we find the best basis possible. Although, the results for all fields up to $\mathbb{F}_{2^6}$ coinsided with those previously found, which is a good sign.

From now on, the primitive polynomials used to define each finite field are found in Appendix A. The best found bases from each field still contains exponent 0, and it seems to be centered when possible. Results were found for all fields up to $\mathbb{F}_{2^{13}}$.

$m :=$	Basis	Complexity
7	{-3, -2, -1, 0 ,1 ,2 ,3}	61
8	{-129, -86, -43, 0, 43, 86, 129, 172}	107
9	{-4, -3, -2, -1, 0, 1, 2, 3, 4}	101
10	{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5}	126
11	{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6}	155
12	{-1375,. . . , -550, -275, 0, 275, 550,. . . , 1650}	180
13	{-2058,. . . , -686, -343, 0, 343, 686,. . . , 2058}	298

Table 4.4: The best bases found in fields $\mathbb{F}_{2^m}$ for dimensions 7 up to 13, found using Algorithm 2, based on Multiples of Polynomial Bases. Primitive polynomials used to define each field are found in Appendix A.

The complexity naturally increases for each new dimension, but not strictly. So far, the only exception is the field $\mathbb{F}_{2^8}$. Also notice the drastic increase in complexity for the field $\mathbb{F}_{2^{13}}$, compared with earlier ones. These unexpected results are not fully understood, but some ideas are presented later on.

4.4 Limitation on the Multiples

By using Algorithm 2, results are found for all fields up to $\mathbb{F}_{2^{13}}$, and all bases seem to contain exponent 0. Therefore, we limit our search even more, allowing only multiples of Polynomial Bases where exponent 0 is included.

Example 8 *Consider the Polynomial Basis* $\{\alpha^0, \alpha^2, \alpha^4\}$ *from the field* $\mathbb{F}_{2^3}$*, defined by the primitive polynomial* $p(x) = x^3 + x + 1$*. There are 7 possible multiples, but only three resulting in a new basis including exponent 0, namely factors* α^0*,* α^3 *and* α^5*.*

$$\alpha^3 \cdot \{\alpha^0, \alpha^2, \alpha^4\} = \{\alpha^3, \alpha^5, \alpha^7\} = \{\alpha^3, \alpha^5, \alpha^0\}$$
$$\alpha^5 \cdot \{\alpha^0, \alpha^2, \alpha^4\} = \{\alpha^5, \alpha^7, \alpha^9\} = \{\alpha^5, \alpha^0, \alpha^2\}$$

The factor α^0 *is the Polymonial Basis itself, and will always be considered. The other two factors results in new bases, including exponent 0.*

4.4.1 Algorithm

This approach limits the search even more, testing only m multiples of each Polynomial Basis found in each field $\mathbb{F}_{2^m}$. This is the only difference between Algorithms 2 and 3.

Algorithm 3 PB Multiples with constraints

Initialize $best = m^3$, $basis = \{\ \}$

```
1: for t ∈ CL do
2:    PB := possible Polynomial Basis generated by (α^t)
3:    if PB is a basis then
4:       for Multiples of PB including exponent 0 do
5:          if Complexity of Multiple < best then
6:             best := Complexity
7:             basis := Multiple
8:          end if
9:       end for
10:   end if
11: end for
```

4.4.2 Results

The number of multiples tried out for each Polynomial Basis is decreased from $q^m - 1$ to m, a great improvement letting us go all the way up to $\mathbb{F}_{2^{21}}$. As the search is limited even more, we are not able to guarantee that the result is optimal. But once again, our results merge with those found in earlier searches.

$m :=$	Basis	Complexity
14	{-6 · 57,. . . , -1 · 57 , 0, 1 · 57,. . . , 7 · 57 }	246
15	{-7 · 1389,. . . , -1 · 1389 , 0, 1 · 1389,. . . , 7 · 1389 }	281
16	{-7 · 1019,. . . , -1 · 1019 , 0, 1 · 1019,. . . , 8 · 1019 }	442
17	{-9 · 2743,. . . , -1 · 2743 , 0, 1 · 2743,. . . , 7 · 2743 }	363
18	{-8 · 9709,. . . , -1 · 9709 , 0, 1 · 9709,. . . , 9 · 9709 }	405
19	{-9 · 3113,. . . , -1 · 3113 , 0, 1 · 3113,. . . , 9 · 3113 }	595
20	{-8 · 13981,. . . , -1 · 13981 , 0, 1 · 13981,. . . , 11 · 13981 }	508
21	{-11 · 128397,. . . , -1 · 128397 , 0, 1 · 128397,. . . , 9 · 128397 }	555

Table 4.5: The best bases found in fields $\mathbb{F}_{2^m}$ for all dimensions between 14 and 21, by using Algorithm 3 based on Limited Multiples of Polynomial Bases. Primitive polynomials used to define each field are found in Appendix A.

The structure of a basis with low complexity is now seen quite clearly. Elements sharing a common stepsize, spread out on both sides of exponent 0, are most likely to generate a good basis.

4.5 Structural Design Algorithm

So far, the best found bases for all fields up to $\mathbb{F}_{2^{21}}$ have shared some common features. All bases includes exponent 0 and the rest of the elements are most of the time uniformly spread, surrounding exponent 0.

This specific structure is used when designing the next algorithm, with the adjustment that only bases where exponent 0 is truly centered are considered. The reason for this is to hold down the number of possibilities, otherwise this method would not be an improvement at all.

4.5.1 Algorithm

Let us assume that exponent 0 is always centered and surrounded by elements on a common stepsize t. Denote the basis ϑ.

$$\vartheta = \{\underbrace{\ldots, \alpha^{-2t}, \alpha^{-t}, \alpha^{0}, \alpha^{t}, \alpha^{2t}, \ldots}_{m \text{ elements}}\}$$

The center element, α^0, is fixed. That leaves us with $m-1$ elements needed in order to obtain a basis for $\mathbb{F}_{2^m}$. These should be equally divided between the sides, more specific $\frac{m-1}{2}$ elements on each side.

If the dimension is even, exponent 0 cannot be centered. In this case, two sets of elements are considered, each including m elements. The following example shows the idea.

Example 9 *If we look at the field $\mathbb{F}_{2^4}$, with dimension $m = 4$, the number of elements on each side is $\frac{4-1}{2} = 1.5$. This should of course be rounded upwards to 2, making a small adjustment in the formula. Number of elements on each side, $N = \lceil \frac{m-1}{2} \rceil$.*

Element α^0 cannot be centered as we should have a total of 4 elements, therefore we create two new sets by skipping the outmost element on each side. In this way, the element α^0 is as centered as possible.

$$\{\alpha^{-2t}, \alpha^{-t}, \alpha^{0}, \alpha^{t}, \alpha^{2t}\}$$

$$\swarrow \qquad \searrow$$

$$\{\alpha^{-2t}, \alpha^{-t}, \alpha^{0}, \alpha^{t}\} \qquad \{\alpha^{-t}, \alpha^{0}, \alpha^{t}, \alpha^{2t}\}$$

It is easy to create one of the sets from the other, simply by switching the sign of all exponents. In other words, stepsize t has become $-t$. In a finite field, every negative number is equivalent to a number greater than 0. Therefore, both sets above will be covered, assuming that all t-values are tried out.

How many values of the stepsize t do we need to try, without testing two equal sets. A finite field of the form $\mathbb{F}_{q^m}$ contains $q^m - 1$ nonzero elements. Element α^{q^m-1} is always equal to 1, and can not be used as a generator. This leaves us with $q^m - 2$ elements. Therefore, by testing the stepsize t for all values between 1 and $q^m - 2$, we cover all possible sets.

Once again, the concept of equivalent sets makes it possible to reduce the number of t-values. All numbers from the same cyclotomic coset will generate equivalent sets. It is therefore enough to try out the coset leaders for the field in question. The algorithm looks like this in pseudo code.

Let CL denote the set of coset leaders. The dimension is denoted with m. If the dimension is even, the set with most elements on the right is used.

Algorithm 4 Structural Design Algorithm

Initialize $N = \lceil \frac{m-1}{2} \rceil$, $best = m^3$, $basis = \{\ \}$

```
1: for t ∈ CL do
2:    Set := {α^{-Nt}, ..., α^{-t}, α^0, α^t, ..., α^{Nt}}
3:    if Set is a basis then
4:       if Complexity of Set < best then
5:          best := Complexity
6:          basis := Set
7:       end if
8:    end if
9: end for
10:
11: for Multiples of basis including exponent 0 do
12:    if Complexity of Multiple < best then
13:       best := Complexity
14:       basis := Multiple
15:    end if
16: end for
```

For all values of t, one from each Cyclotomic Coset, a set is created. If this set is a basis, its complexity is calculated. Like earlier algorithms, the best found value is always saved.

The second for-loop tests all multiples of the best found basis, but only those including exponent 0, to see if it might get even better. The reason for this is that earlier results show that exponent 0 is not always exactly centered, but often shifted one step to either side.

This is the most efficient algorithm of them all, but to the cost of great limitations in the search. The idea is to test only sets resembeling what has been found before, skipping combinations that probably would give us an average complexity.

4.5.2 Results

Once again, the results from this algorithm match earlier results, justifying its use for unexplored fields. Results have been found up to $\mathbb{F}_{2^{25}}$, a field of reasonable size even for implementations.

$m :=$	Stepsize	Multiple	Complexity
22	1091	$5 \cdot 1091$	655
23	27007	$-1 \cdot 27007$	663
24	943033	-	963
25	1465043	$-2 \cdot 1465043$	791

Table 4.6: The best bases found in fields $\mathbb{F}_{2^m}$ for dimensions 22 up to 25, by using Algorithm 4 based on Structural Design. The primitive polynomials used to define each field are found in Appendix A.

In Table 4.6, the complexity of the bases are found, and they are described using the notation *Stepsize* and *Multiple*. The following example explains how to interpet this.

Example 10 *Look at the field $\mathbb{F}_{2^{23}}$, where the Stepsize $t = 27007$ and $Multiple = 27007$. The set { -11·t,. . . , -2·t, -1·t, 0, 1·t, 2·t,. . . , 11·t } should be shifted using the multiple 27007, in order to get the basis with lowest complexity.*

Example 11 *For the field $\mathbb{F}_{2^{24}}$, with Stepsize $t = 943033$ and no $Multiple$, the basis looks like this.*

$$\{ \text{ -11·t,. . . , -2·t, -1·t, 0, 1·t, 2·t,. . . , 11·t, 12·t } \}$$

As the dimension is even, exponent 0 cannot be centered, and the set with most elements on the right is used. As there is no multiple, no shift is necessary to get the basis with lowest complexity.

4.6 Conclusions

A table including the best found bases for all fields up to $\mathbb{F}_{2^{25}}$ is presented. The bases are described using the notation *Stepsize* and *Multiple*.

The table is divided into four parts, to show us how long each algorithm could go. The first part is completely searched. Second and third part were found using Multiples of Polynomial Bases, first allowing all multiples but later only those including exponent 0. Last part were found using the Structural Design Algorithm, leading all the way to $\mathbb{F}_{2^{25}}$.

$m :=$	Stepsize	Multiple	Complexity	Method
2	1	-	5	
3	1	-	11	Exhaustive
4	1	-	20	Search
5	1	-	31	
6	7	-	45	
7	1	-	61	
8	43	-	107	
9	1	-	101	Multiples
10	1	-	126	of PB
11	1	$1 \cdot 1$	155	
12	275	-	180	
13	343	-	298	
14	57	-	246	
15	1389	-	281	
16	1019	-	442	
17	2743	$-1 \cdot 2743$	363	Limitations
18	9709	-	405	on Multiples
19	3113	-	595	
20	13981	$1 \cdot 13981$	508	
21	128397	$-1 \cdot 128397$	555	
22	1091	$5 \cdot 1091$	655	
23	27007	$-1 \cdot 27007$	663	Structural
24	943033	-	963	Design
25	1465043	$-2 \cdot 1465043$	791	

Table 4.7: The best bases found in each field $\mathbb{F}_{2^m}$ for dimensions between 2 and 25, using the algorithm based on Structural Design.

It should be noted that the results for each new algorithm agrees with earlier results. Only the first part of the table are facts, as all possibilities have been tried out, assuring us an optimal basis. The following results are from algorithms limiting the search more and more, with the consequence of uncertain results.

It is interesting to notice for which fields the complexity suddenly rises more than usual, often followed by a decreased value for the next field. The fields referred to are those with dimension 8, 13, 16, 19 and 24. Common for those fields are that no Irreducible Polynomials over $\mathbb{F}_2$ of weight 3 exist. Every other field among those listed have Irreducible Polynomials of weight 3.

The weight of a polynomial is the number of nonzero coefficients in it. For example, the weight of $x^5 + x + 1$ is equal to 3, and the weight of the polynomial $x^5 + x^4 + x^2 + x + 1$ is equal to 5. The minimal polynomial of an element is the polynomial of lowest degree having the element as a root.

The weight of a polynomial is interesting in implementations of sequential multiplication, as the polynomial defines the feedback. Interesting result were found during the search using Multiples of Polynomial Bases. The Polynomial Basis shifted to the best found basis, is generated by an element. The minimal polynomial of this element has a weight, and it is also 3 in all fields except for dimensions 8, 13, 16 and 19, where it is 5. The same is probably true for dimension 24 as well, but this has only been investigated for fields up to $\mathbb{F}_{2^{21}}$.

Type	Equivalence Classes			Complexity
PB:	{ 0,1,2 }	{ 0,2,4 }	{ 0,4,1 }	12
	{ 0,6,5 }	{ 0,5,3 }	{ 0,3,6 }	13
DP:	{ 5,2,1 }	{ 3,4,2 }	{ 6,1,4 }	19
TB:	{ 6,1,0 }	{ 5,2,0 }	{ 3,4,0 }	11
DT:	{ 1,2,3 }	{ 2,4,6 }	{ 4,1,5 }	16
NB:	{ 6,5,3 }			15
Other:	{ 0,1,5 }	{ 0,2,3 }	{ 0,4,6 }	14
	{ 1,2,6 }	{ 2,4,5 }	{ 4,1,3 }	17
	{ 1,3,5 }	{ 2,6,3 }	{ 4,5,6 }	17
	{ 1,3,6 }	{ 2,6,5 }	{ 4,5,3 }	20

Table 4.8: A complete list of bases for the Finite Field $\mathbb{F}_{2^3}$.

Chapter 5

Comparison to Known Bases

Well known bases are those called Polynomial, Normal and Triangular Bases. In this chapter, the complexities for those bases and their respective duals are found and calculated. A comparison between the well known bases and those found in the search from last chapter is also made.

5.1 Known Bases

Bases that have been studied earlier, used in implementations or having other nice advantages, are here refered to as known bases. The most common ones are Polynomial and Normal Bases, together with Triangular Bases. All those are used in implementations, therefore it is interesting to know how good they are considering multiplication.

Because these bases have a certain structure, it is easy to generate them. There are no search-methods needed, which of course makes it possible to generate bases in quite large fields. Known bases for all fields from $\mathbb{F}_{2^2}$ to $\mathbb{F}_{2^{24}}$ are found and evaluated. Along with the known bases, their respective dual bases are also tried out.

In this chapter, possible relations between the known bases are tried out. First of all, we try to find a connection between the complexity for bases and their duals. This is tested with the help of graphs, by plotting the complexity of each basis against its dual value. This experiment is performed for all fields from $\mathbb{F}_{2^3}$ up to $\mathbb{F}_{2^{15}}$ for Polynomial, Normal and Triangular Bases.

All elements generating a Normal Basis works as generators for Polynomial Bases as well. In Olofsson [3, Ch.5], bases with this property are considered. Therefore, a comparison of complexity for such bases might be interesting. A figure presenting the relation of complexity for Polynomial Bases and Normal Bases generated by the same element is found in Section 5.3.

Another relation considered is the one between Triangular Bases and the Polynomial Bases. A Triangular Basis is defined by a Polynomial Basis, and therefore we look at the complexity of these bases. A figure presenting this relation is found in Section 5.4.

It would also be interesting to know if there excists any connection between the complexity of Polynomial Bases and the best Multiple of them. In the same way as for the dual relations, this is done by graphs, for all fields between $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^{15}}$. In Section 5.5, a figure showing this relation is found.

In Section 5.6, a summary of the best found complexity values for all known bases in fields up to $\mathbb{F}_{2^{24}}$ is found in Table 5.1 on page 46. This table also contains the overall best value found for each field, making it possible to see how good the known bases are considering multiplication.

The complete set of figures are found in Appendix C.

5.2 Dual relations

Is it possible to say anything about the complexity of a dual basis just by looking at the basis related to it? This is an interesting question, but not easy to answer. To get an idea, some graphs are presented where the complexity of bases together with the respective dual bases can be found.

For example, the complexity of all Polynomial Bases are saved together with its corresponding dual values. These values are then plotted in a graph, with the complexity of the Polynomial Bases on one axis, and the corresponding dual values on the other.

A dotted line is also found in the graph, showing $y = x$, in order to see which basis is the better one. Any point above this line has a greater complexity for the basis represented on the y-axis. If a point lies on the line, it means that the complexity is equal for the basis and its dual.

Also, the overall best found value for the field in question is seen as a dash-dotted line, going in both the x and y direction.

5.2.1 Polynomial Bases

Here follows a graph for Polynomial Bases from the field $\mathbb{F}_{2^9}$.

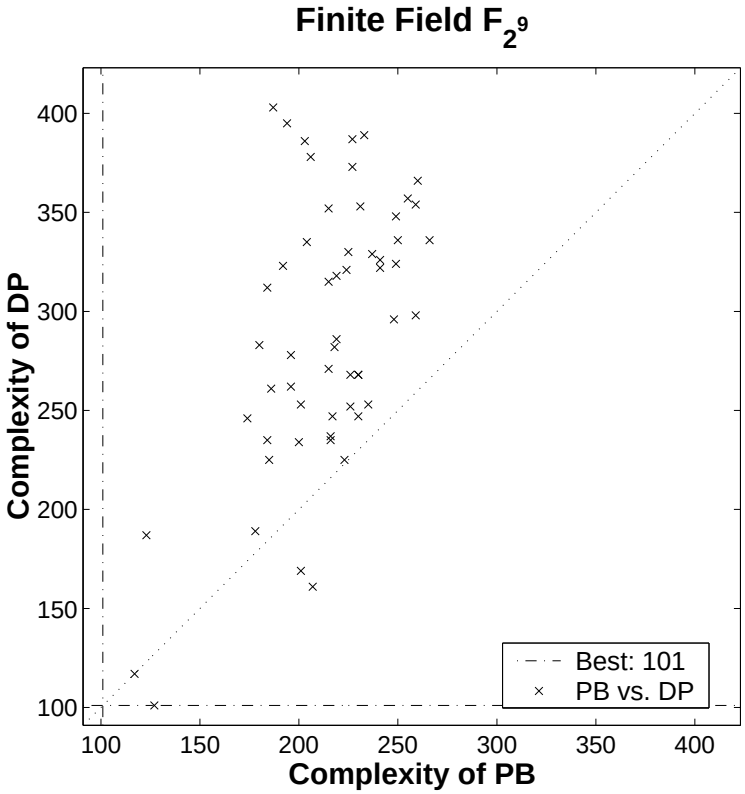

Figure 5.1: A figure showing the complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^9}$.

The complexity of the duals is spread out over a wide range, while the complexity of the Polynomial Bases is more stable. It seems like the complexity of Polynomial Bases is better than its duals most of the time, with only a few exceptions. The basis with lowest complexity is a Dual Basis though. In general, most of the bases have a complexity far away from the best value found. These features are common for all fields searched, and the rest of the figures are found in Appendix C.1.

5.2.2 Normal Bases

It should be noted that the dual of a Normal Basis is also a Normal Basis. As a consequence of that, we get a symmetric figure. Here follows a graph for Normal Bases from the field $\mathbb{F}_{2^9}$.

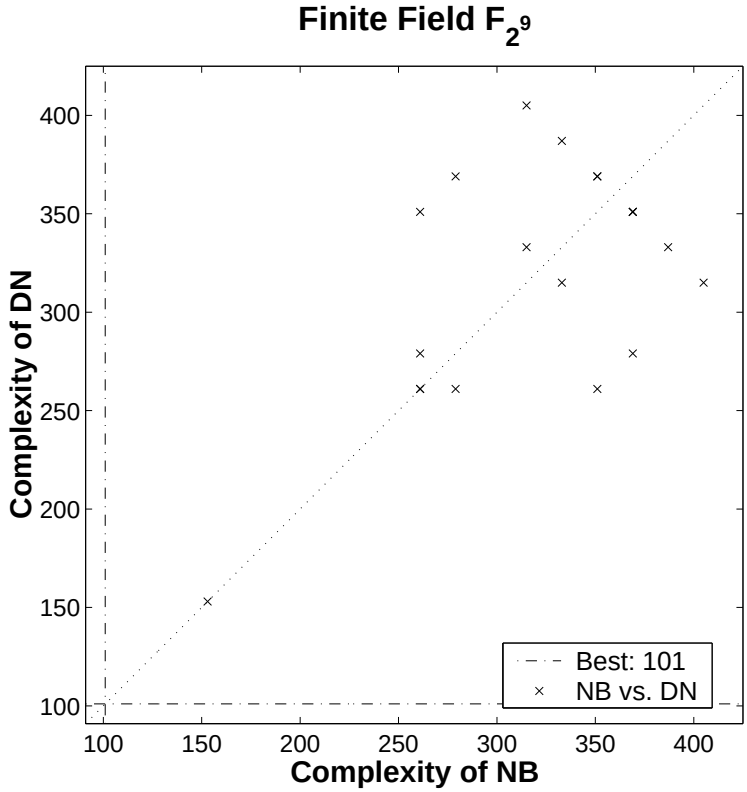

Figure 5.2: A figure showing the complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^9}$.

All matrices $\boldsymbol{T_k}$ have the same weight, as they are only a cyclic shift of each-other. Therefore, the complexity of the Normal Bases is always a multiple of m, creating a grid of discrete values.

In the figure, we can see that one basis got a complexity much better than the rest. This is found in most of the other fields as well, that the main part of the bases are really bad, with a few exceptions. The other figures are found in Appendix C.2.

5.2.3 Triangular Bases

Here follows a graph for Triangular Bases from the field $\mathbb{F}_{2^9}$.

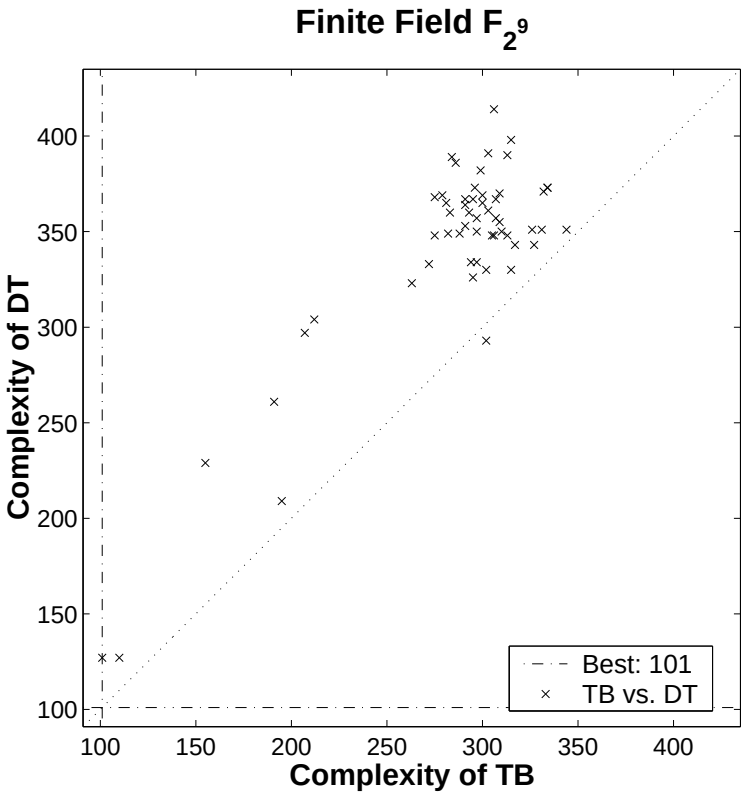

Figure 5.3: A figure showing the complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^9}$.

The complexity of the Triangular bases seems to be better than their duals most of the time. In general, the complexity of a Triangular Basis or its dual is not good, but with a few important exceptions.

In this figure, and for all figures in Appendix C.3, there exists one or two Triangular Bases with complexity close to the best found value.

5.3 Polynomial and Normal Bases

A figure showing the complexity of Polynomial Bases and Normal Bases, generated from the same element, taken from the field $\mathbb{F}_{2^9}$.

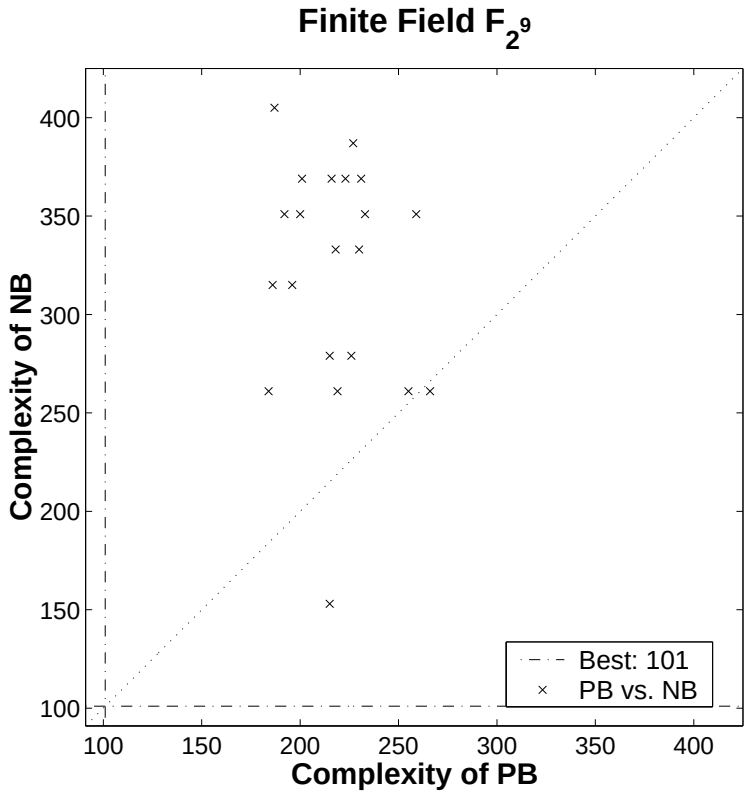

Figure 5.4: A figure showing the complexity of Polynomial Bases and Normal Bases, generated by the same element.

In general, the Normal Bases have a high complexity. The Polynomial Bases related to those seems to have a lower complexity, but still not a good value. One basis deviates from the others, having a complexity much better than the rest. It also seems like there is a relation between the best Normal Basis and the Polynomial Basis with lowest complexity. This is seen for all fields, found in Appendix C.4.

5.4 Polynomial and Triangular Bases

A figure showing the complexity of Polynomial Bases and the Triangular Basis related to it, taken from the field $\mathbb{F}_{2^9}$.

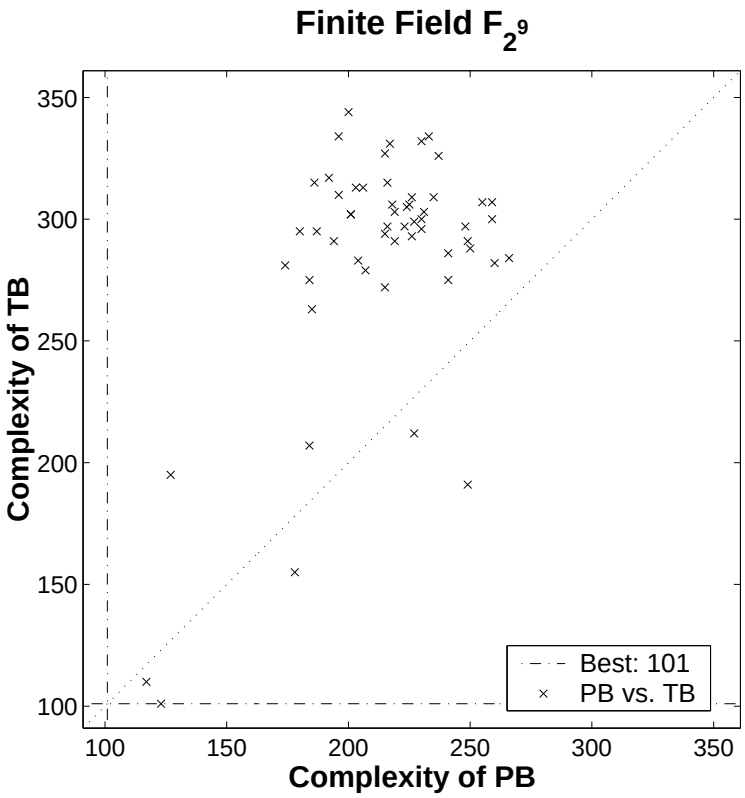

Figure 5.5: A figure showing the complexity of Polynomial Bases and the Triangular Bases related to it.

The complexity is really high for most of the bases, with only a few exceptions. A Polynomial Basis with low complexity seems to generate a Triangular Basis with low complexity. These features are seen in the other fields as well, and the figures are found in Appendix C.5.

5.5 Polynomial Bases and their Multiples

Is there any relation between the complexity of the best Polynomial Basis and the best found Multiple of a Polynomial Basis? If so, one could just search through all Polynomial Bases, skipping the work of testing multiples.

In order to answer this question, the complexity for all Polynomial Bases and the best found Multiple related to them were calculated. Results from the field $\mathbb{F}_{2^9}$ are found in this figure.

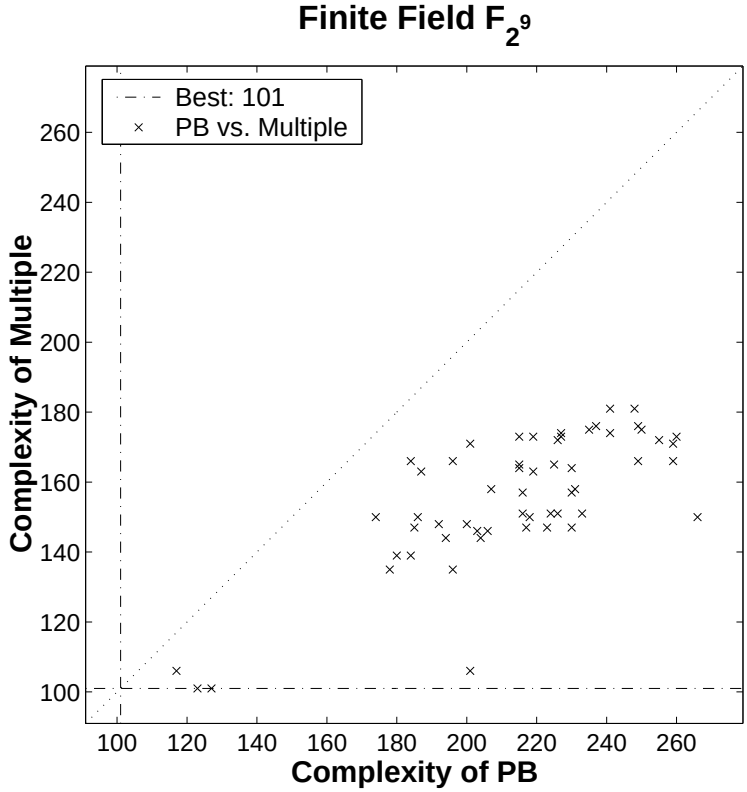

Figure 5.6: A figure showing the Complexity of Polynomial Bases and their respective best Multiples from the field $\mathbb{F}_{2^9}$.

The complexity of a Multiple Basis is always less than, or perhaps equal to, the complexity of the Polynomial Basis related to it. A Polynomial Basis with good complexity seems to generate a Multiple with good complexity.

The overall best Multiple in a field is not always generated by the best Polynomial Basis though, which is seen in Figure 5.6. On the other hand, sometimes a Polynomial Basis with average complexity generates a Multiple with complexity not far from the best. This is seen in the same figure, near the value 200 on the x-axis.

Similair features are found in the other fields. All the figures for fields $\mathbb{F}_{2^3}$ through $\mathbb{F}_{2^{15}}$ are found in Appendix C.6.

5.6 Summary

On page 46 follows a table presenting the best found complexity for each class of known bases, looking at fields between $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^{24}}$. The best found complexity for each field is also presented in the table, in order to compare how good the different bases are considering its complexity of multiplying elements. As the dual of a Normal Basis is a Normal Basis as well, the column DN is not included, as it would be the same as NB.

The class of known bases that seems to work best is the Dual Polynomial Bases, with a complexity near the best found throughout the fields. As mentioned earlier, the Normal Bases are always the worst choise, except for dimensions 11 and 14 where the Dual Triangular Bases have complexities even higher.

In the smaller fields, Triangular Bases are as good as the Polynomial Bases, or perhaps even better. In larger fields, the Triangular Bases are not as stable, sometimes having a complexity far away from the best one. This could be seen in fields $\mathbb{F}_{2^{12}}$ and $\mathbb{F}_{2^{14}}$. But they are in fact the best choise in dimensions 8, 16 and 24, which is interesting.

Common for these dimensions is the fact that no Minimal Polynomials of weight three exists. It means that for some of the dimensions, where the complexity found has been much higher than normal, the Triangular Bases are suddenly a better choise than the Dual Polynomial Bases.

Tables describing how to generate the best found known bases in each field are found in Appendix D.

Field $\mathbb{F}_{2^m}$ m :=	Complexity					
	PB	NB	TB	DP	DT	BEST
2	5	6	5	5	5	5
3	12	15	11	12	12	11
4	22	28	20	20	22	20
5	36	45	31	31	38	31
6	48	66	47	47	51	45
7	70	133	61	62	83	61
8	141	168	114	127	119	107
9	117	153	101	101	127	101
10	148	190	127	128	131	126
11	177	231	160	160	246	155
12	213	276	256	183	261	180
13	385	585	356	315	455	298
14	297	378	357	261	422	246
15	330	675	356	282	347	281
16	571	1360	458	501	452	442
17	428	1377	370	365	448	363
18	441	630	531	420	501	405
19	871	2223	683	642	1288	595
20	593	1260	652	510	614	508
21	652	1995	820	567	1098	555
22	715	1386	790	695	786	655
23	792	1035	697	670	820	663
24	1335	2520	1066	1083	1416	963
25	-	-	-	-	-	791

Table 5.1: The best bases found up to $\mathbb{F}_{2^{24}}$. The best complexity found for each field can be found in the column BEST. The notations used are:

Polynomial Bases (PB), Normal Bases (NB) and Triangular Bases (TB). Also Dual Polynomial Bases (DP) and Dual Triangular Bases (DT).

Chapter 6

Conclusions and future research

Here follows conclusions and ideas on what could be done in the future.

6.1 Conclusions

Different methods have been used throughout this thesis. To start with, an exhaustive search was made for smaller fields, in order to get started. No previous work has been found, aiming at finding a general solution to this problem, so we did not know what to look for.

The other methods limited the search more and more. In this way we gained speed to the algorithms, but to the cost of uncertain results. As there is no general lower bound for the complexity, it is hard to say how good the results are. They could be compared to the complexity of known bases though, as they are easy to generate. For results, look into Appendix D.

The complexity of the best found basis in each extension field between $\mathbb{F}_{2^2}$ and $\mathbb{F}_{2^{24}}$ is in fact lower than for the standard bases. Sometimes the best found complexities coinside, but this is the case only for lower dimensions.

Our main result is the structure found for optimal bases. To find a basis with low complexity, we should look for a shifted Polynomial Basis, where exponent 0 is centered, or slightly moved from the center.

6.2 Future research

During the work on this thesis, many ideas and interesting thoughts popped up. Due to the limitations in time, many of those are left unanswered. Here follows some ideas that would be interesing to continue working with.

- **General formula:** It would naturally be interesting to find a general formula for the optimal basis in each field. It is not certain that such a fomula exists, but constraints and general features could not be impossible to find.

- **Connection between Complexity and the Weight of Minimal Polynomials:** The complexity of bases in a field seems to be connected to the Weight of Minimal Polynomials. For all fields where there does not exist a Minimal Polynomial of weight 3, the complexity is remarkably increased.

- **General bounds:** Is it possible to find a general upper and lower bound for the complexity of bases in a finite field. An obvious upper bound is m^3, corresponding to all m matrices filled with m^2 digits. Is it possible to push this limit?

  The lower bound is not that easy. It seems reasonable to say that each one of the $\boldsymbol{T_k}$ matrices should contain at least one digit on every row, otherwise all information is not considered during the calculations. There are m matrices, one for each dimension, and they all contain m rows, giving a possible lower bound for the complexity of m^2. This is nothing but a loose idea though, which needs to look deeper into.

- **Wider equivalence concept:** Is it possible to define equivalent bases more widely, covering a bigger set? This would decrease the time in calculations, making it possible to search larger fields.

Appendix A

Primitive polynomials

This appendix contains a table of the primitive polynomials over $\mathbb{F}_2$ used when defining extension fields throughout this thesis. All results are based on finite fields constructed by using these primitive polynomials.

For example, the Finite Field $\mathbb{F}_{2^9}$ was constructed by adjoining a root of the primitive polynomial $x^9 + x^4 + 1$. This root, denoted by α, becomes a generator for the multiplicative group $\mathbb{F}_{q^m}^*$.

According to Table 4.4 found on page 29, the basis with lowest complexity for $\mathbb{F}_{2^9}$ is the following set.

$$\{ \text{-4, -3, -2, -1, 0, 1, 2, 3, 4} \}$$

The numbers represent the exponents of α defining the basis.

$$\{ \alpha^{-4}, \alpha^{-3}, \alpha^{-2}, \alpha^{-1}, \alpha^0 , \alpha^1 , \alpha^2 , \alpha^3 , \alpha^4 \ \}$$

If the field is constructed by another primitive polynomial, this basis might not be the best one anymore. Therefore, in order to reconstruct the best found bases for each field, use only the primitive polynomials found in the table on next page.

A.1 Table of Primitive Polynomials over $\mathbb{F}_2$

$m :=$	Primitive Polynomial
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1$
6	$x^6 + x + 1$
7	$x^7 + x^3 + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$
9	$x^9 + x^4 + 1$
10	$x^{10} + x^3 + 1$
11	$x^{11} + x^2 + 1$
12	$x^{12} + x^7 + x^6 + x^5 + x^3 + x + 1$
13	$x^{13} + x^4 + x^3 + x + 1$
14	$x^{14} + x^7 + x^5 + x^3 + 1$
15	$x^{15} + x^5 + x^4 + x^2 + 1$
16	$x^{16} + x^5 + x^3 + x^2 + 1$
17	$x^{17} + x^3 + 1$
18	$x^{18} + x^{12} + x^{10} + x + 1$
19	$x^{19} + x^5 + x^2 + x + 1$
20	$x^{20} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x + 1$
21	$x^{21} + x^6 + x^5 + x^2 + 1$
22	$x^{22} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + 1$
23	$x^{23} + x^5 + 1$
24	$x^{24} + x^{16} + x^{15} + x^{14} + x^{13} + x^{10} + x^9 + x^7 + x^5 + x^3 + 1$
25	$x^{25} + x^8 + x^6 + x^2 + 1$

Table A.1: Primitive Polynomials used to define the Finite Fields $\mathbb{F}_{2^m}$ in this thesis, where m is the degree of extension.

Appendix B

Statistics

The fields $\mathbb{F}_{2^3}$ to $\mathbb{F}_{2^6}$ has been totally searched. Every possible basis combination has been evaluated. The statistical results from this search is presented in the following tables, and graphs showing the distribution of the complexity for bases in each field are found in Section B.2.

B.1 Tables

Statistics for the Field $\mathbb{F}_{2^3}$ All 28 bases evaluated				
Basis	# Bases	# Eq.Classes	Complexity	Quota
Polynomial	6	2	12	1.0909
Normal	1	1	15	1.3636
Triangular	6	2	11	1
Dual Polynomial	6	2	12	1.0909
Dual Triangular	6	2	12	1.0909
Best Found	3	1	11	-

Table B.1: Statistics for $\mathbb{F}_{2^3}$. The column "Complexity" shows the best value found for each class of bases. The "Quota" is relative to the best complexity.

Statistics for the Field $\mathbb{F}_{2^4}$ All 840 bases evaluated				
Basis	# Bases	# Eq.Classes	Complexity	Quota
Polynomial	12	3	22	1.1
Normal	2	2	28	1.4
Triangular	12	3	20	1
Dual Polynomial	12	3	20	1
Dual Triangular	12	3	22	1.1
Best Found	4	1	20	-

Table B.2: Statistics for $\mathbb{F}_{2^4}$. The column "Complexity" shows the best value found for each class of bases. The "Quota" is relative to the best complexity.

Statistics for the Field $\mathbb{F}_{2^5}$ All 83328 bases evaluated				
Basis	# Bases	# Eq.Classes	Complexity	Quota
Polynomial	30	6	36	1.1613
Normal	3	3	45	1.4516
Triangular	30	6	31	1
Dual Polynomial	30	6	31	1
Dual Triangular	30	6	38	1.2258
Best Found	5	1	31	-

Table B.3: Statistics for $\mathbb{F}_{2^5}$. The column "Complexity" shows the best value found for each class of bases. The "Quota" is relative to the best complexity.

Statistics for the Field $\mathbb{F}_{2^6}$ All 27.998.208 bases evaluated				
Basis	# Bases	# Eq.Classes	Complexity	Quota
Polynomial	54	9	48	1.0667
Normal	4	4	66	1.4667
Triangular	54	9	47	1.0444
Dual Polynomial	54	9	47	1.0444
Dual Triangular	54	9	51	1.1333
Best Found	6	1	45	-

Table B.4: Statistics for $\mathbb{F}_{2^6}$. The column "Complexity" shows the best value found for each class of bases. The "Quota" is relative to the best complexity.

B.2 Figures

The distribution of the Complexity for all bases in the fields $\mathbb{F}_{2^3}$ through $\mathbb{F}_{2^6}$ seems to approach a Normal Distribution. It could also be two distributions merging together, one of them shifted a little to the left, and the second one having a higher peak to the right.

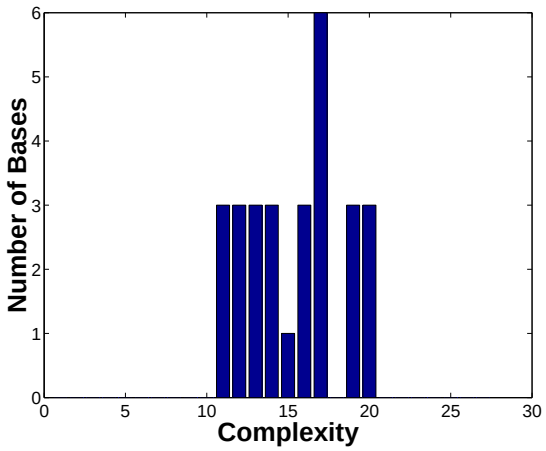

Figure B.1: A diagram showing the distribution of Complexity for all bases in $\mathbb{F}_{2^3}$.

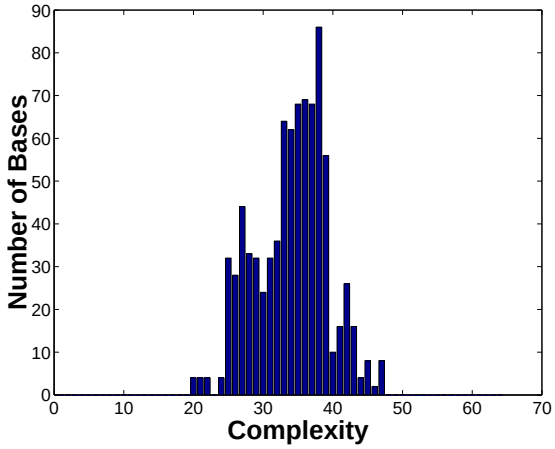

Figure B.2: A diagram showing the distribution of Complexity for all bases in $\mathbb{F}_{2^4}$.

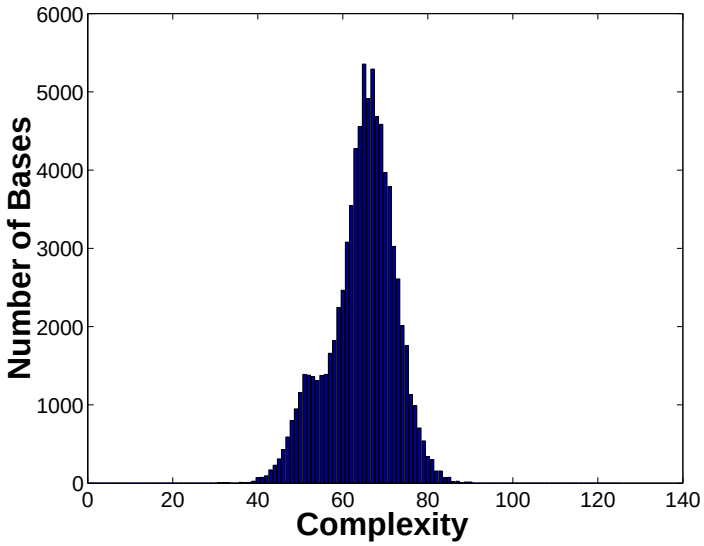

Figure B.3: A diagram showing the distribution of Complexity for all bases in $\mathbb{F}_{2^5}$.

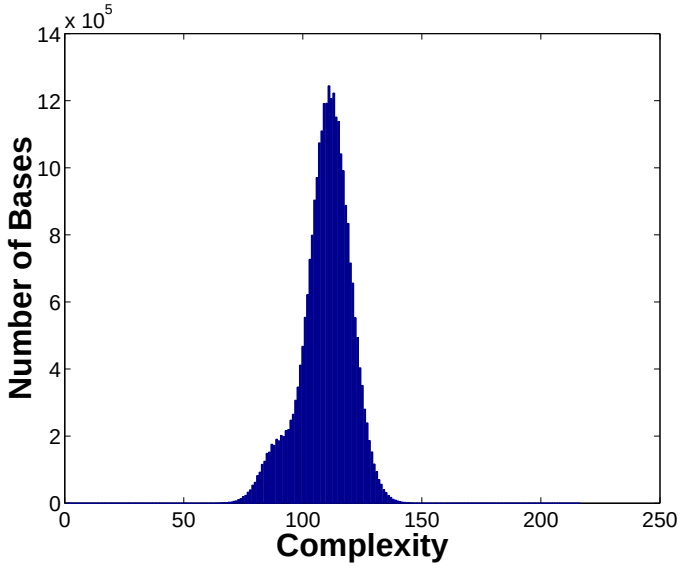

Figure B.4: A diagram showing the distribution of Complexity for all bases in $\mathbb{F}_{2^6}$.

Appendix C

Figures

Here follows the complete set of figures from the different investigations discussed earlier in Chapter 5. Each section contain figures from all the fields between $\mathbb{F}_{2^3}$ and $\mathbb{F}_{2^{15}}$.

All figures presented here have some common features. The axes show the Complexity for the bases represented. A dotted line is also found in the graph, showing $y = x$, in order to see which one is the better. Any point above this line has a greater complexity for the basis represented on the y-axis. If a point lies on the line, it means that the complexity is equal for the two bases represented.

Also, the overall best found value for the field in question is seen as a dash-dotted line, going in both the x and y direction.

C.1 Polynomial Bases

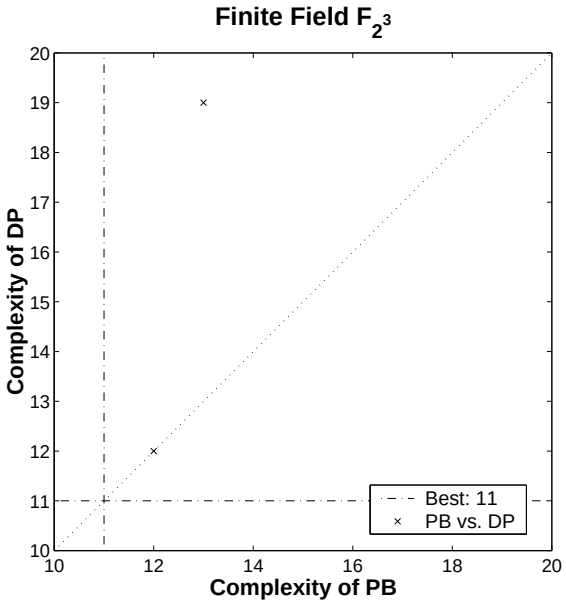

Figure C.1: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^3}$.

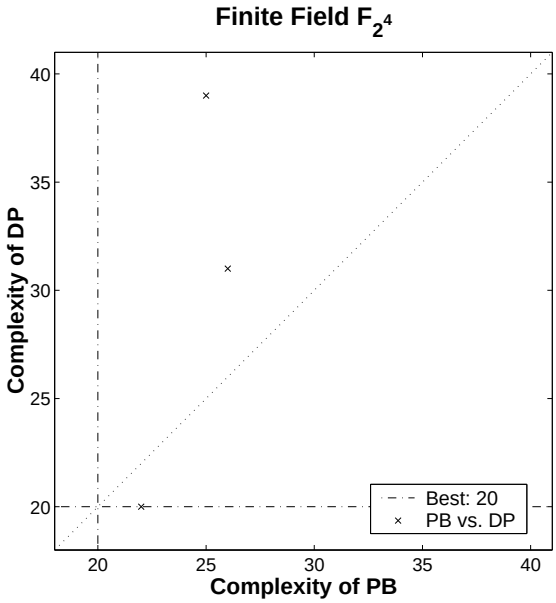

Figure C.2: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^4}$.

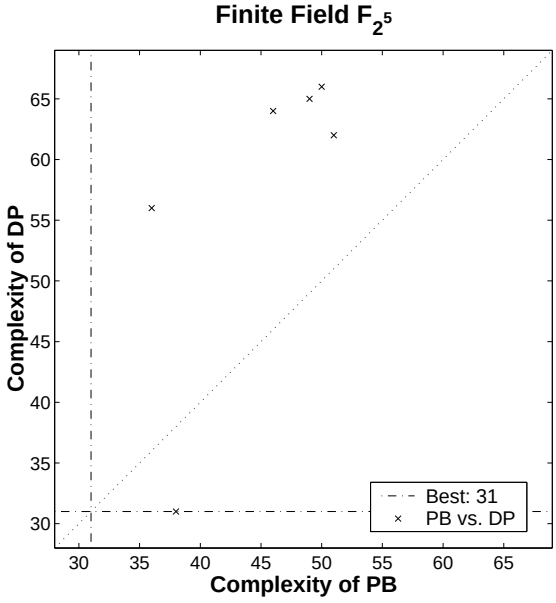

Figure C.3: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^5}$.

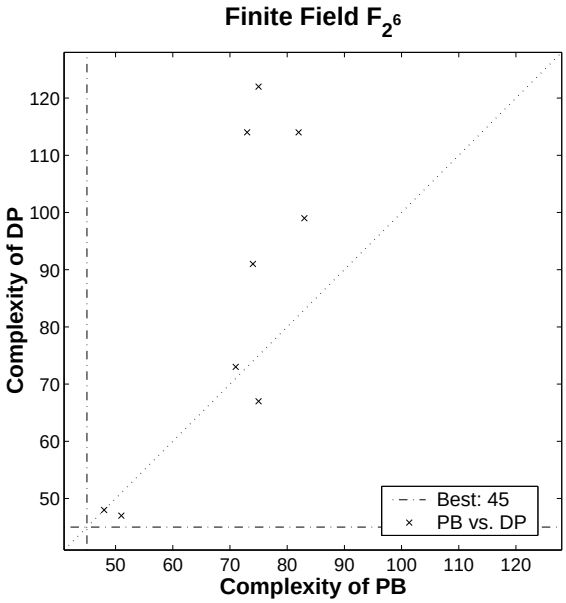

Figure C.4: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^6}$.

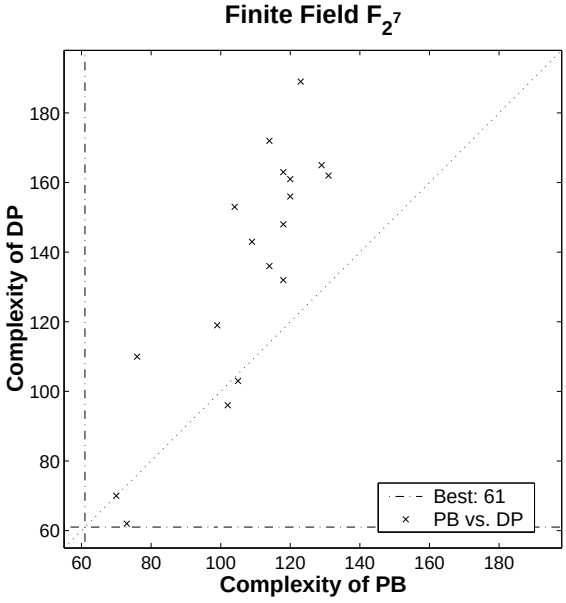

Figure C.5: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^7}$.

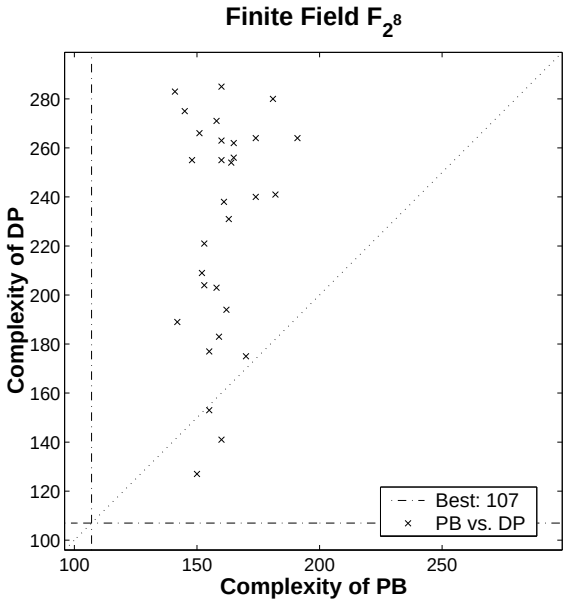

Figure C.6: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^8}$.

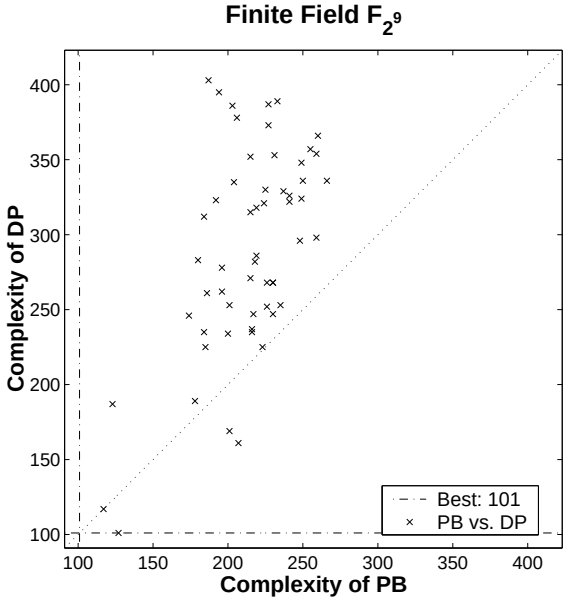

Figure C.7: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^9}$.

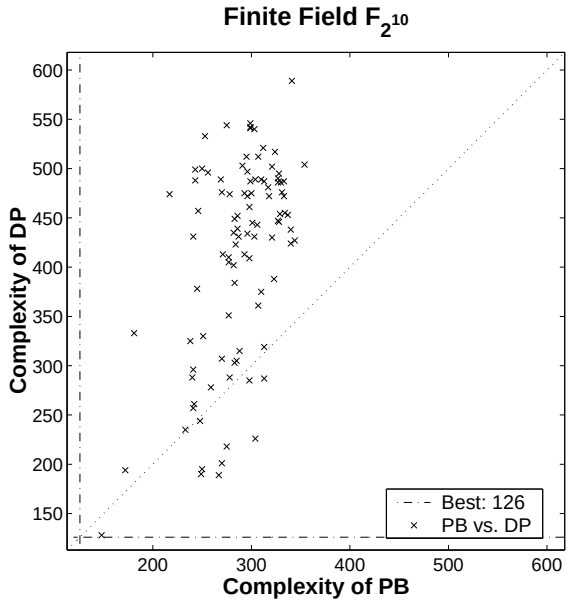

Figure C.8: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^{10}}$.

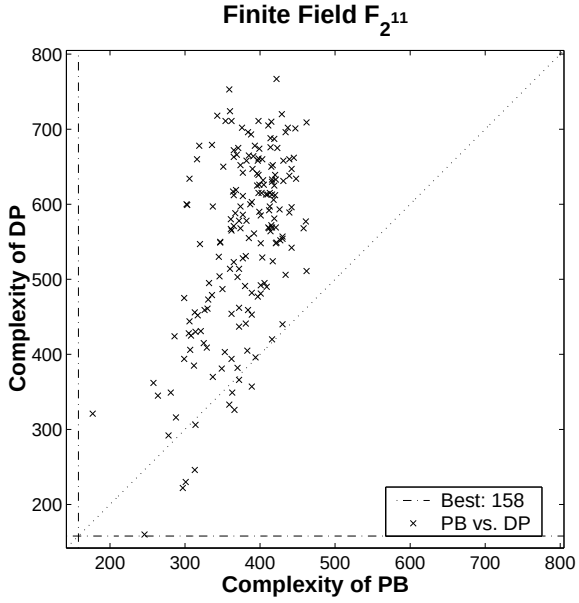

Figure C.9: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^{11}}$.

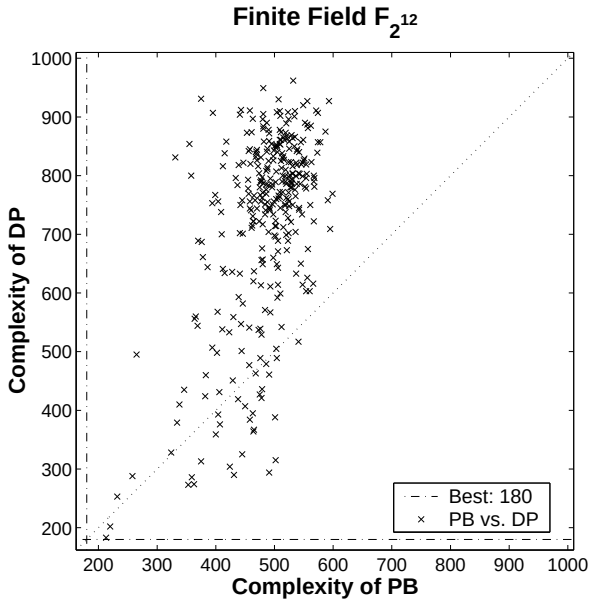

Figure C.10: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^{12}}$.

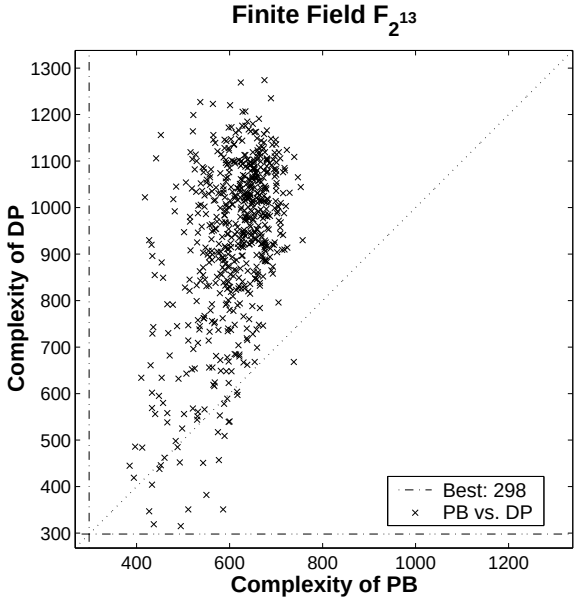

Figure C.11: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^{13}}$.

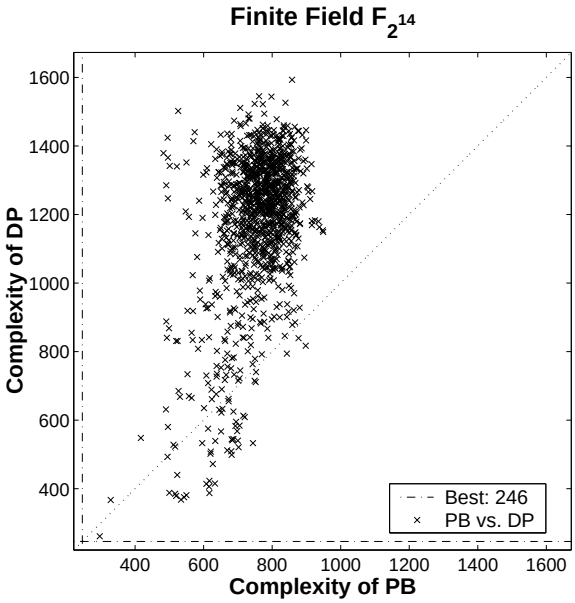

Figure C.12: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^{14}}$.

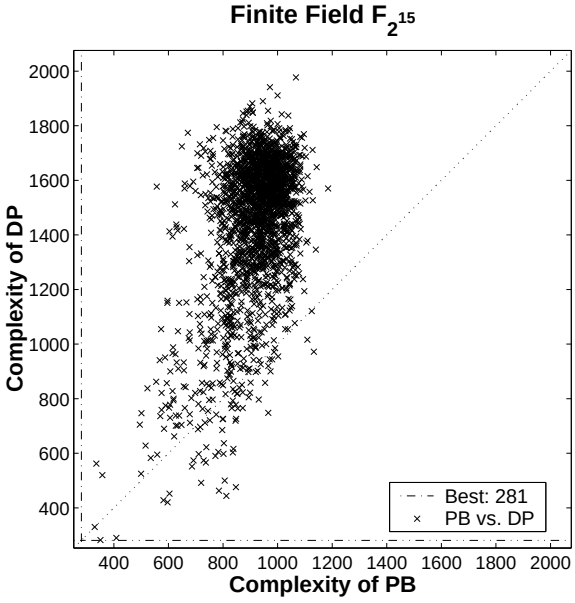

Figure C.13: Complexity of Polynomial Bases and their Duals from the field $\mathbb{F}_{2^{15}}$.

C.2 Normal Bases

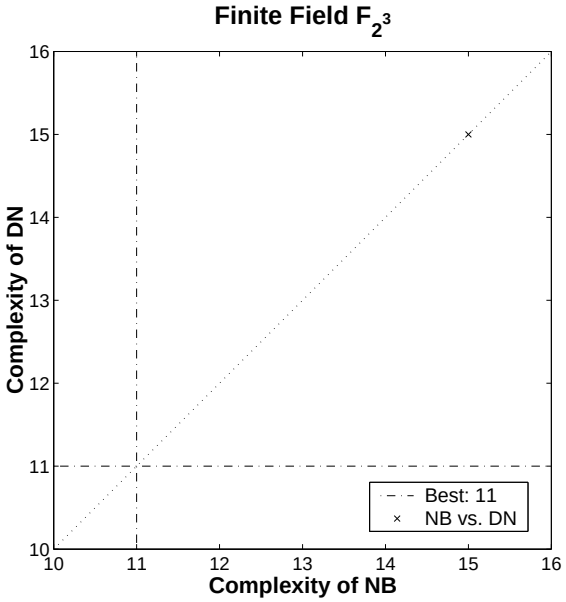

Figure C.14: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^3}$.

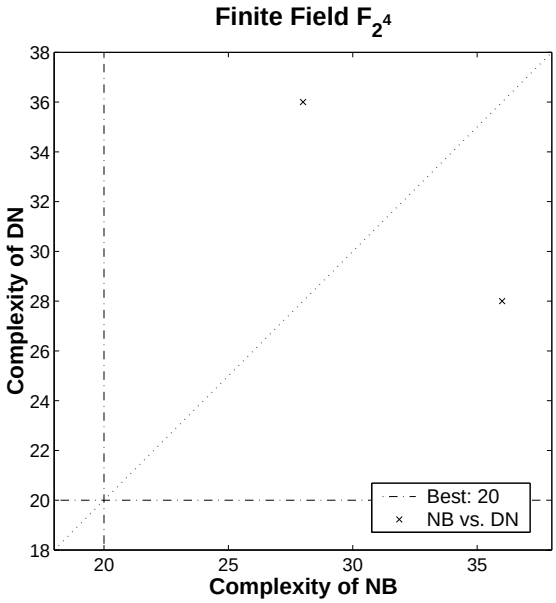

Figure C.15: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^4}$.

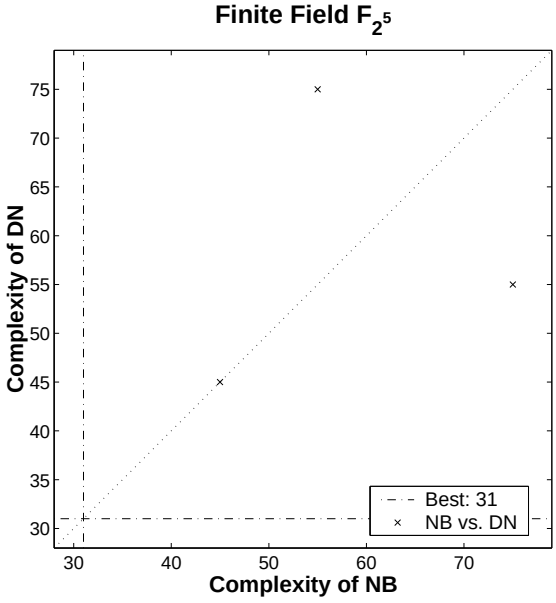

Figure C.16: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^5}$.

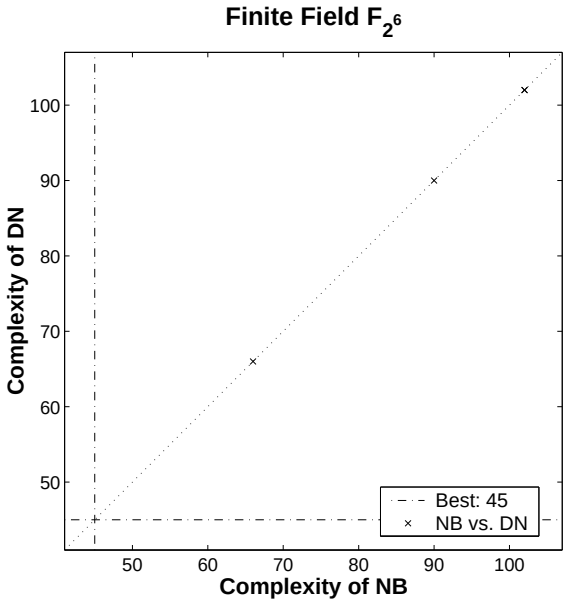

Figure C.17: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^6}$.

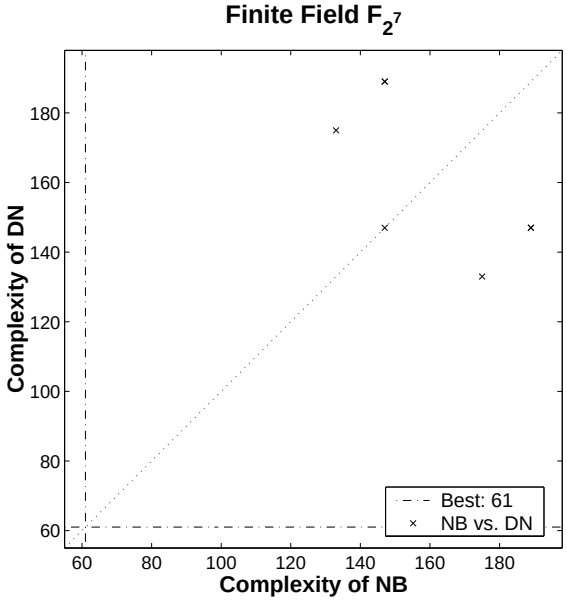

Figure C.18: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^7}$.

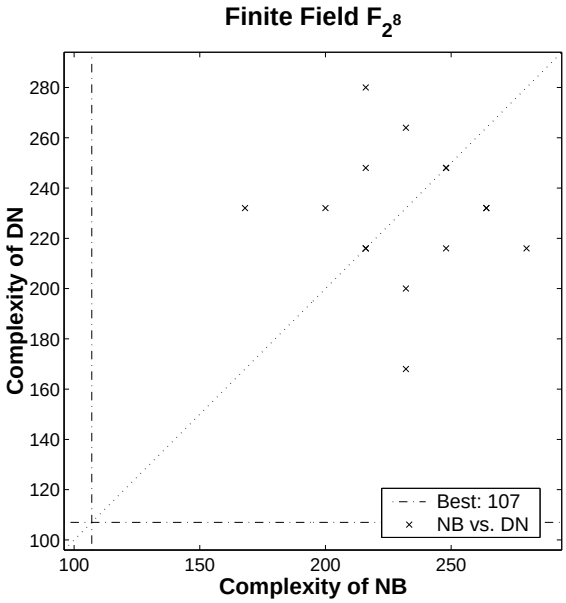

Figure C.19: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^8}$.

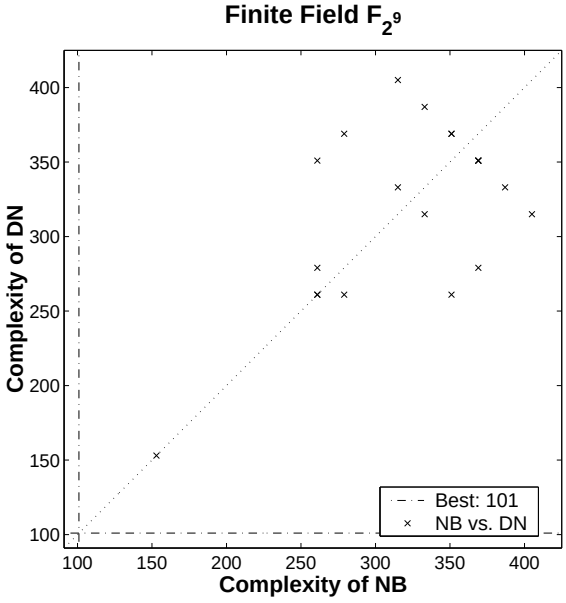

Figure C.20: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^9}$.

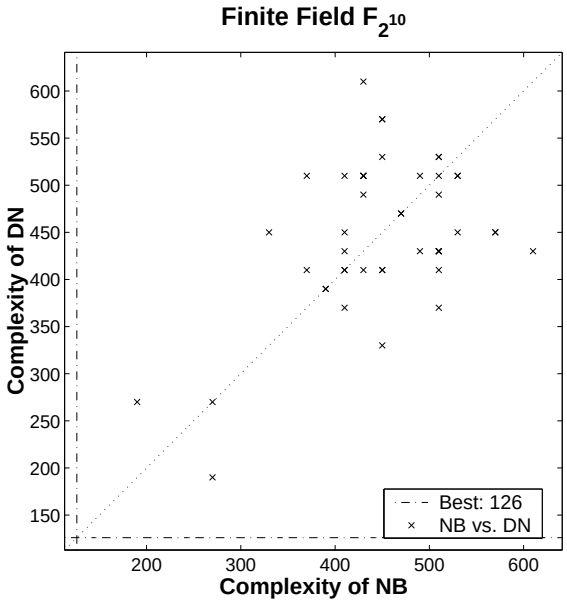

Figure C.21: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^{10}}$.

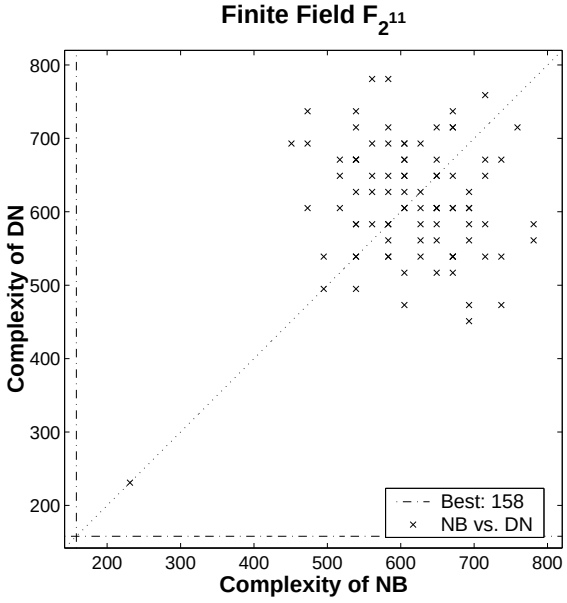

Figure C.22: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^{11}}$.

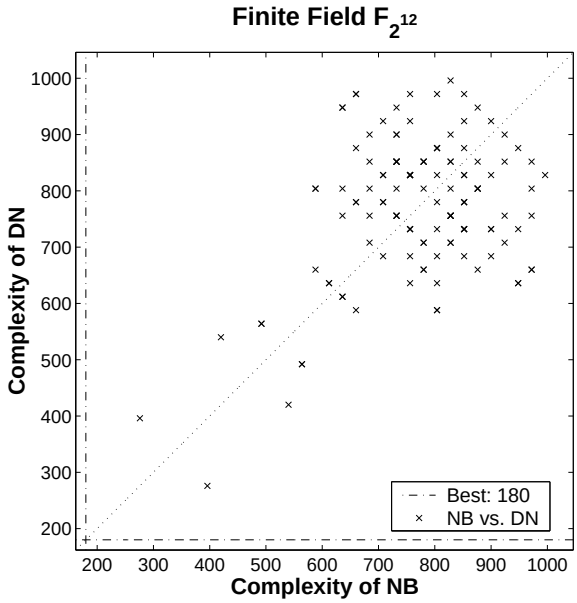

Figure C.23: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^{12}}$.

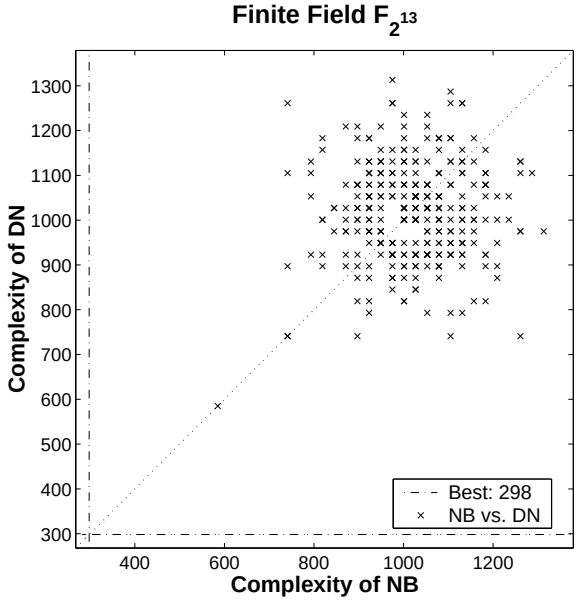

Figure C.24: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^{13}}$.

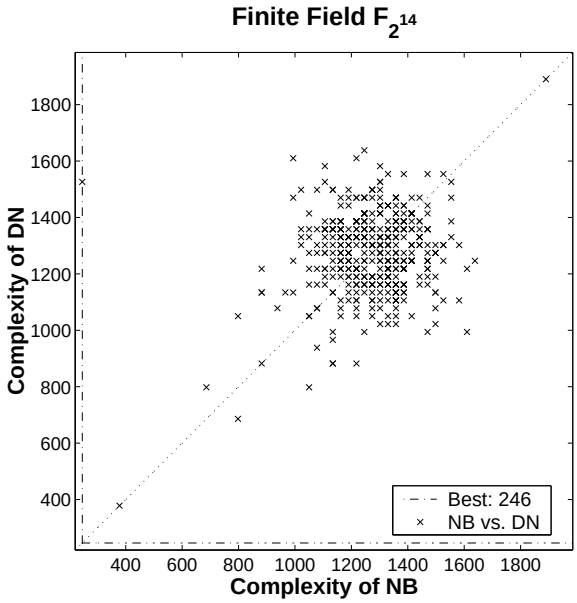

Figure C.25: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^{14}}$.

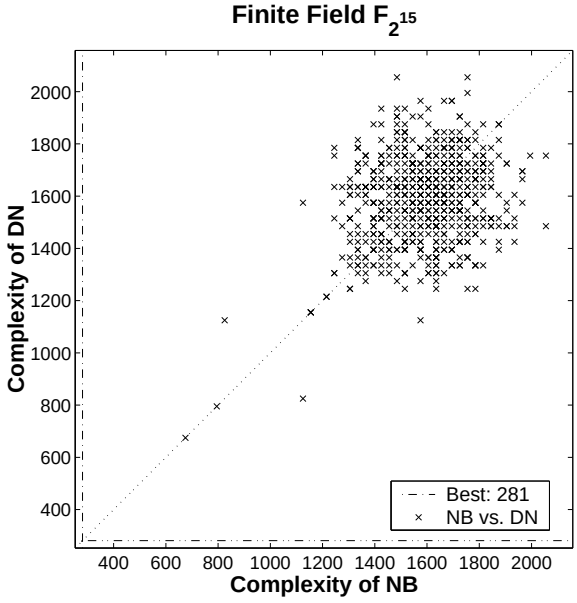

Figure C.26: Complexity of Normal Bases and their Duals from the field $\mathbb{F}_{2^{15}}$.

C.3 Triangular Bases

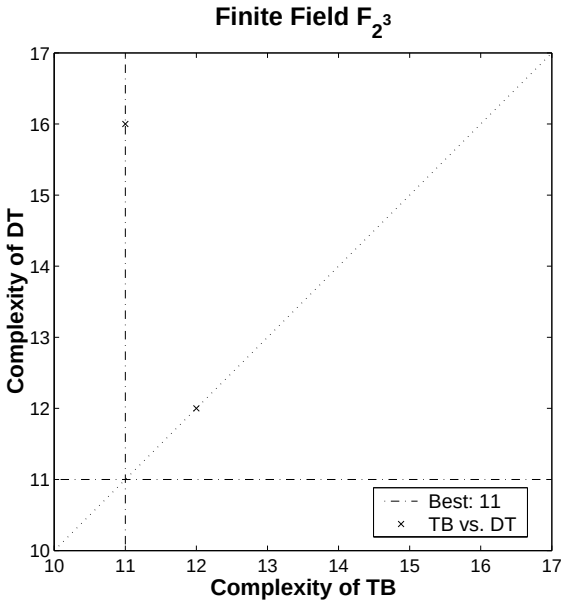

Figure C.27: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^3}$.

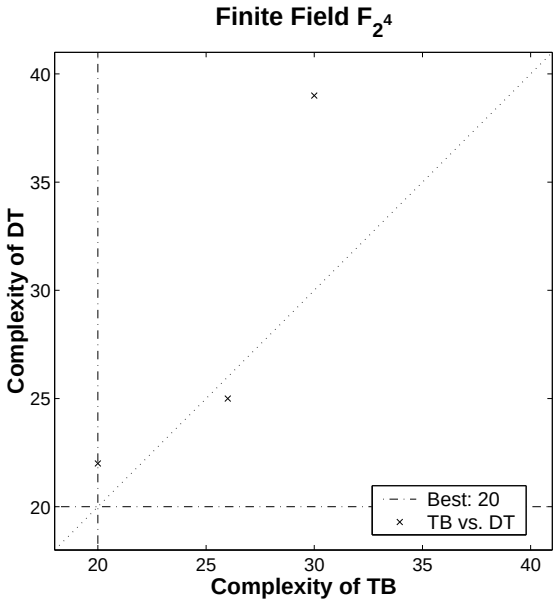

Figure C.28: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^4}$.

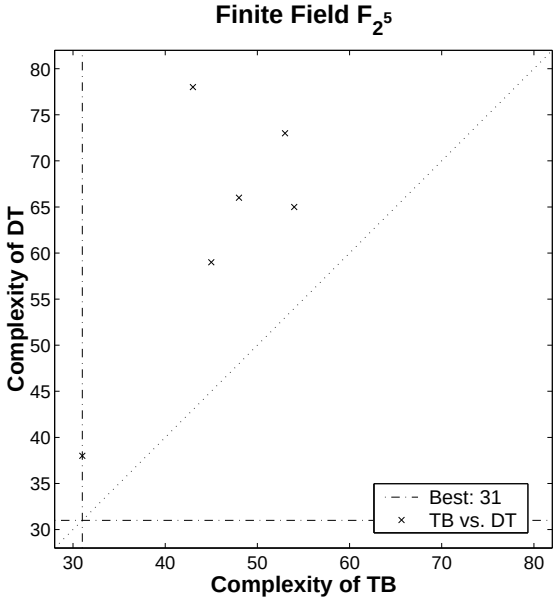

Figure C.29: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^5}$.

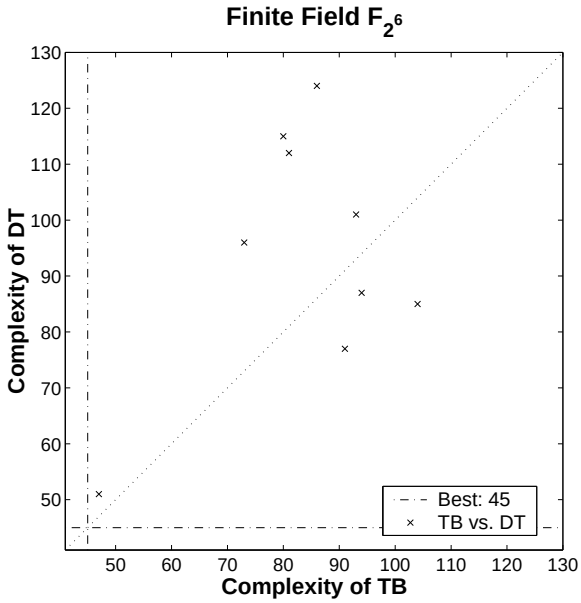

Figure C.30: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^6}$.

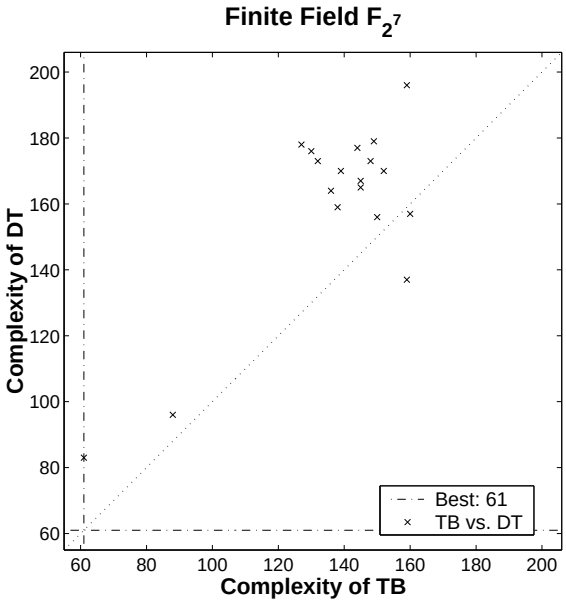

Figure C.31: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^7}$.

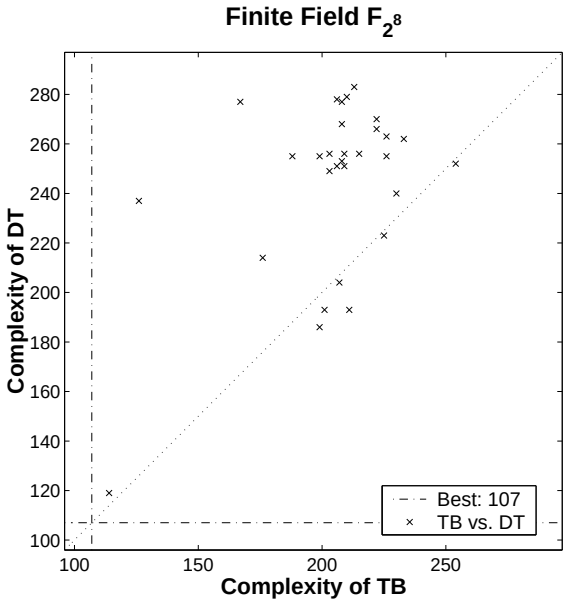

Figure C.32: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^8}$.

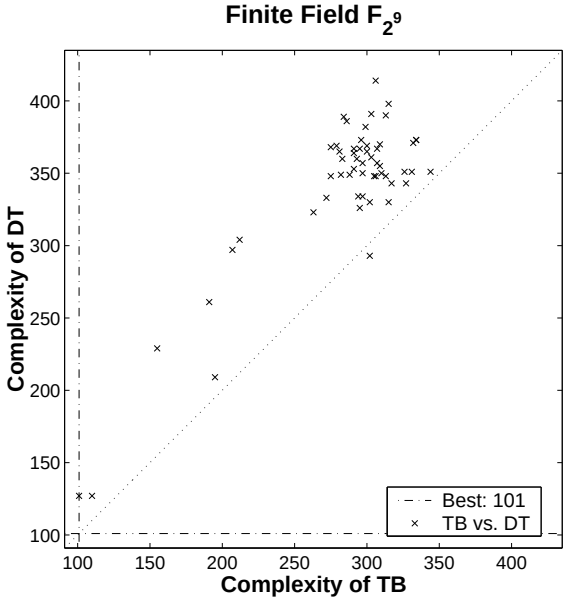

Figure C.33: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^9}$.

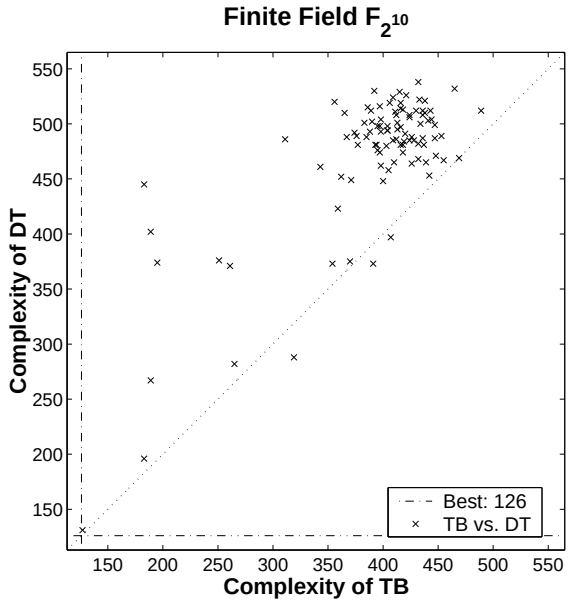

Figure C.34: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^{10}}$.

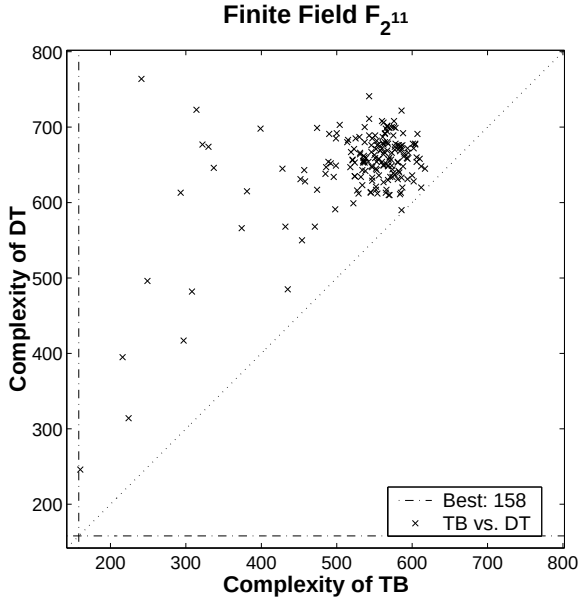

Figure C.35: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^{11}}$.

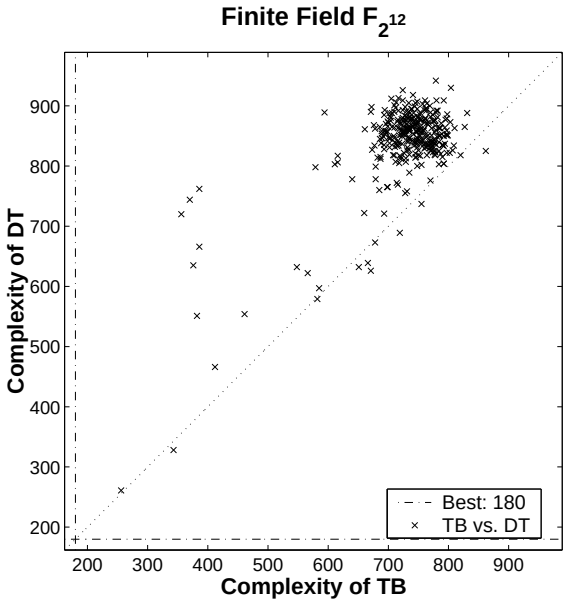

Figure C.36: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^{12}}$.

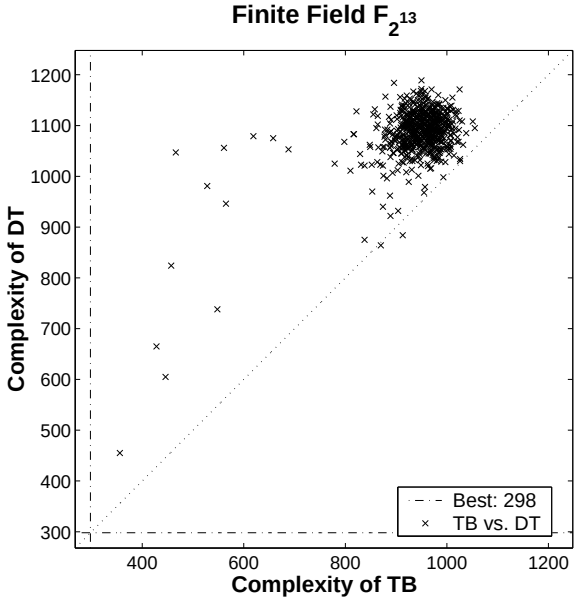

Figure C.37: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^{13}}$.

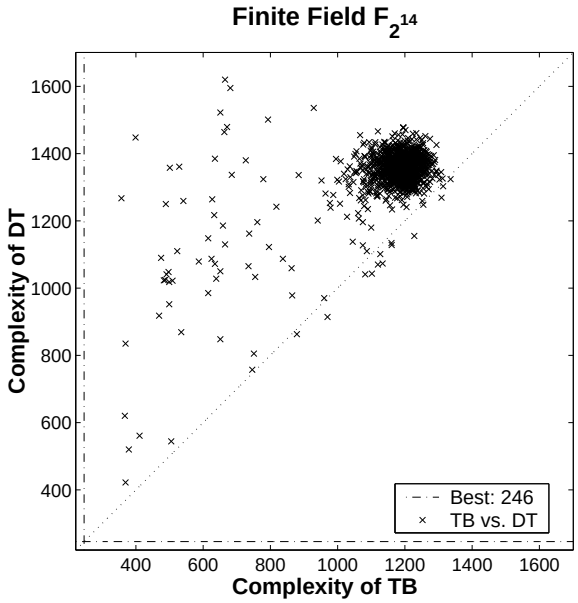

Figure C.38: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^{14}}$.

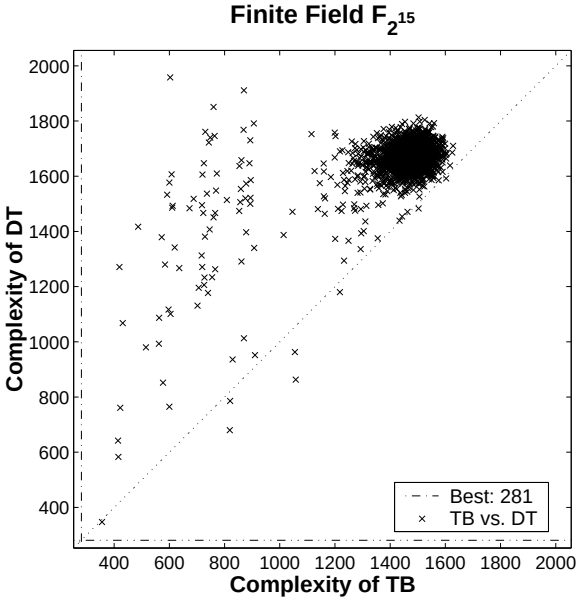

Figure C.39: Complexity of Triangular Bases and their Duals from the field $\mathbb{F}_{2^{15}}$.

C.4 Polynomial and Normal Bases

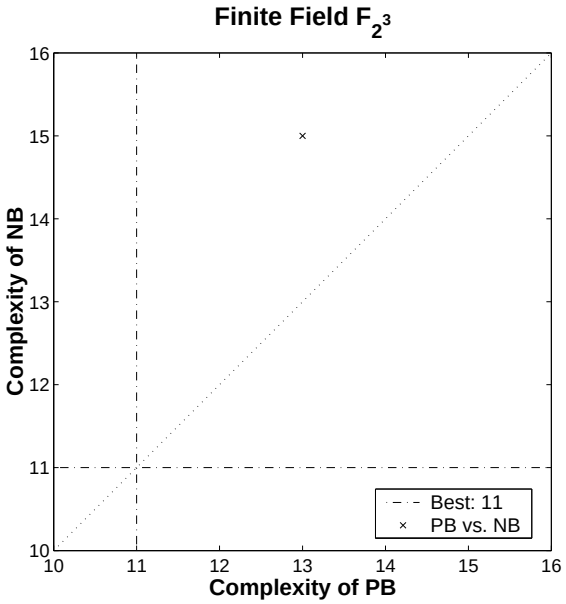

Figure C.40: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^3}$.

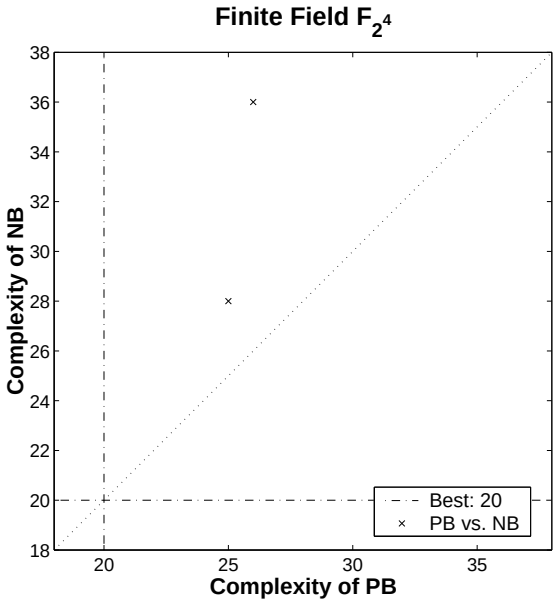

Figure C.41: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^4}$.

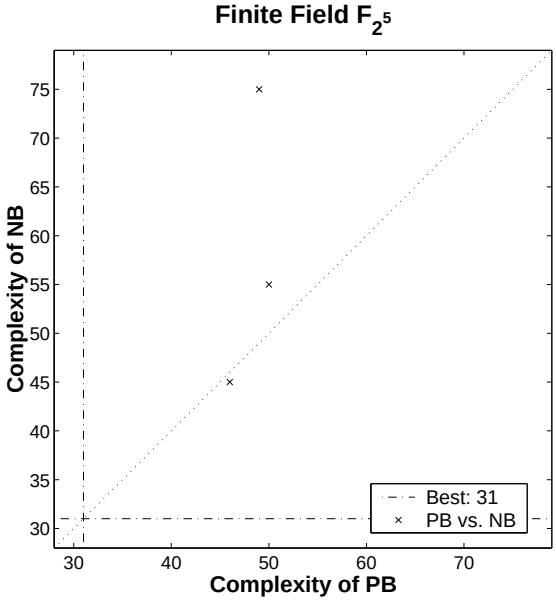

Figure C.42: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^5}$.

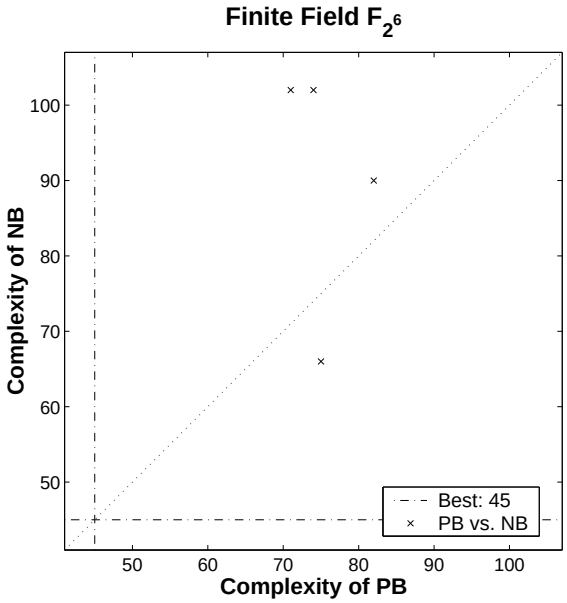

Figure C.43: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^6}$.

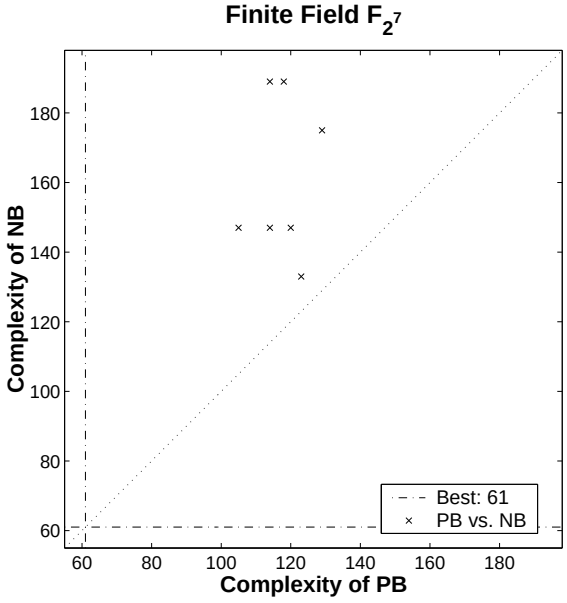

Figure C.44: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^7}$.

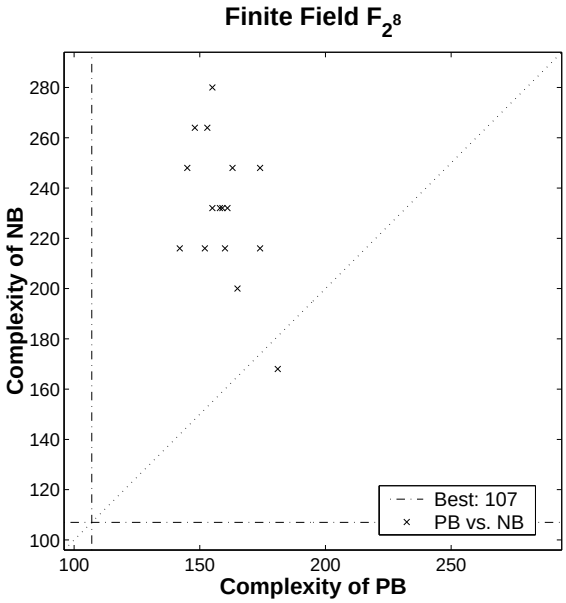

Figure C.45: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^8}$.

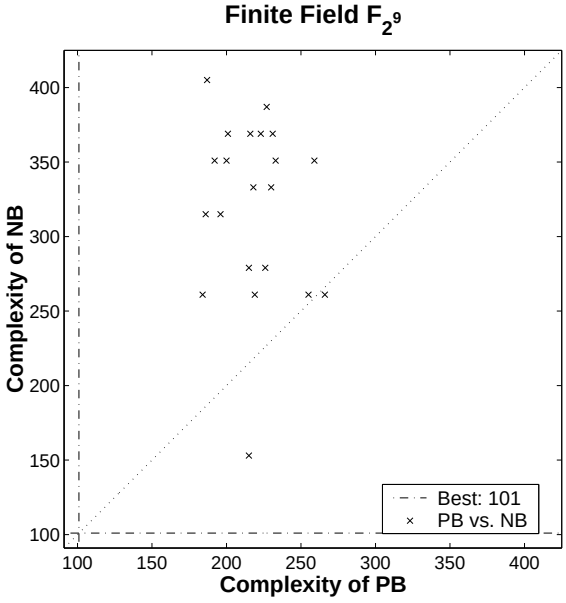

Figure C.46: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^9}$.

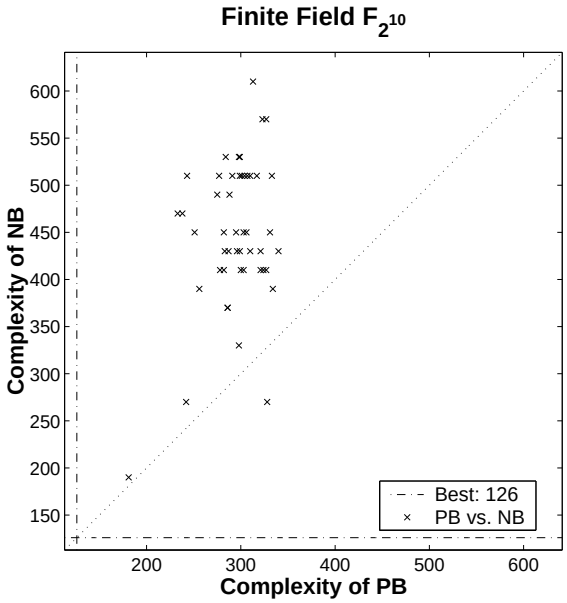

Figure C.47: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^{10}}$.

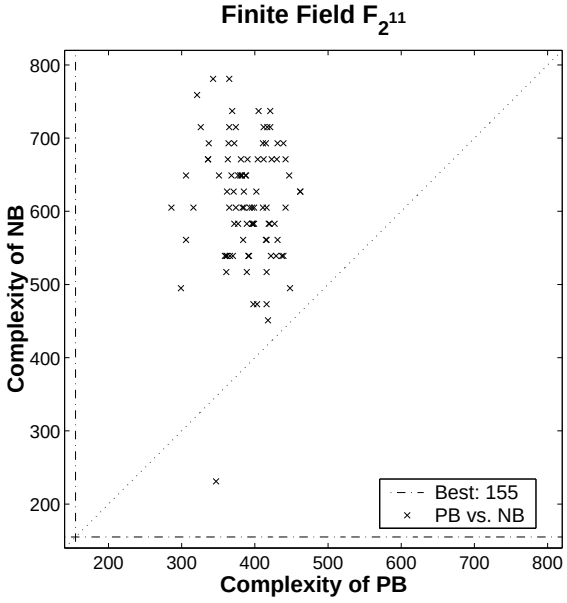

Figure C.48: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^{11}}$.

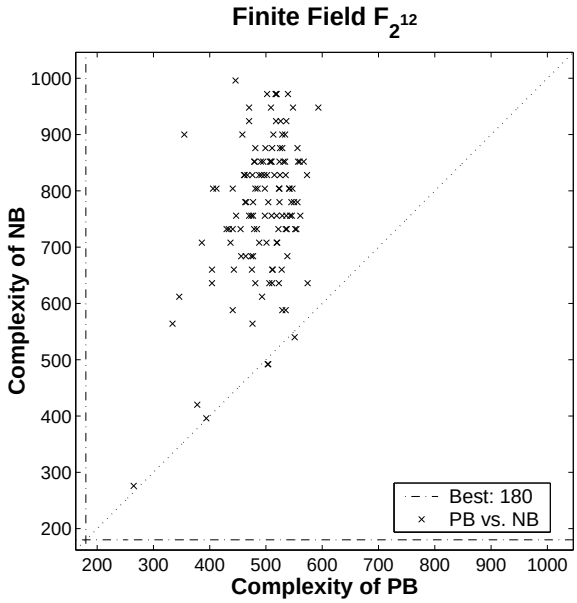

Figure C.49: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^{12}}$.

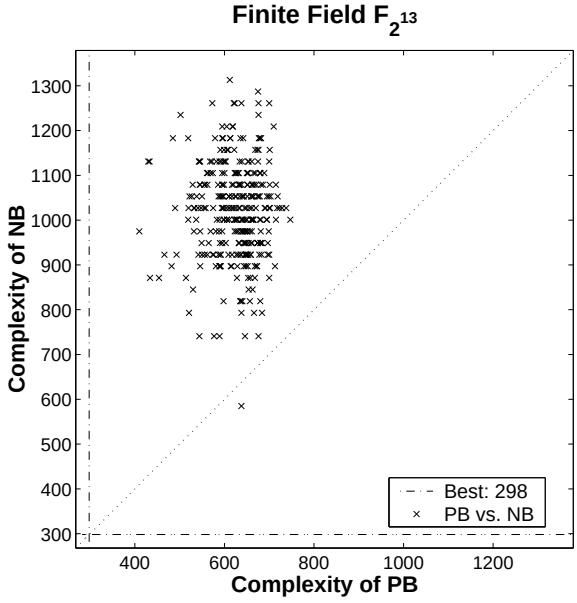

Figure C.50: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^{13}}$.

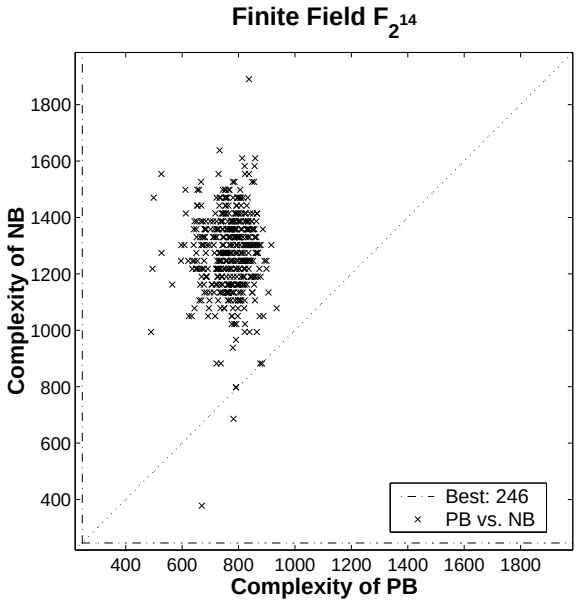

Figure C.51: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^{14}}$.

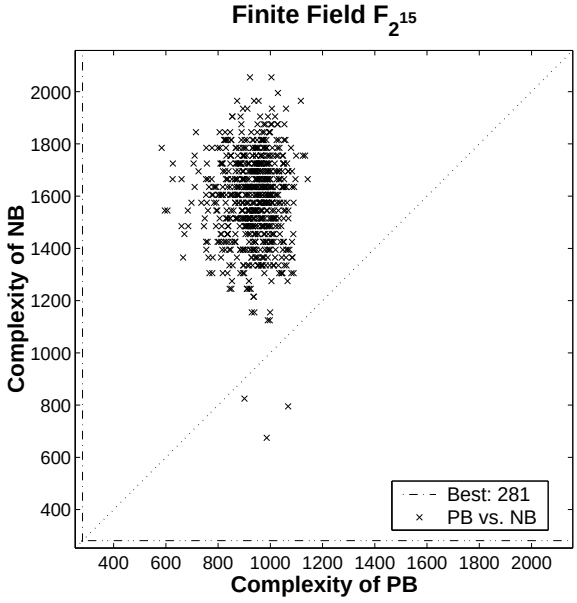

Figure C.52: Complexity of Polynomial and Normal Bases from the field $\mathbb{F}_{2^{15}}$.

C.5 Polynomial and Triangular Bases

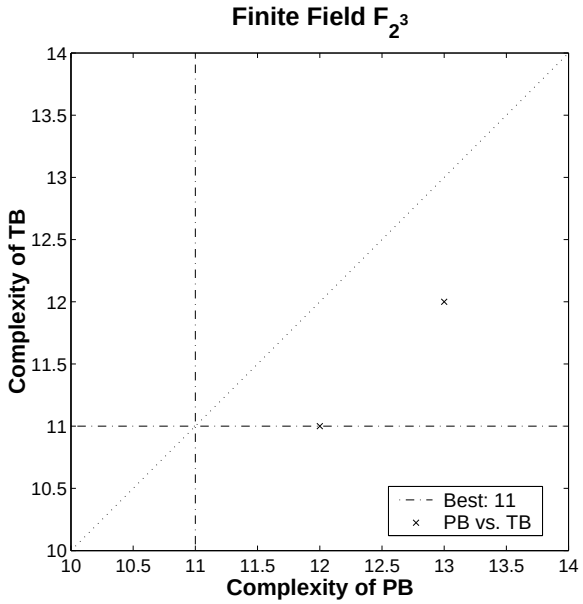

Figure C.53: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^3}$.

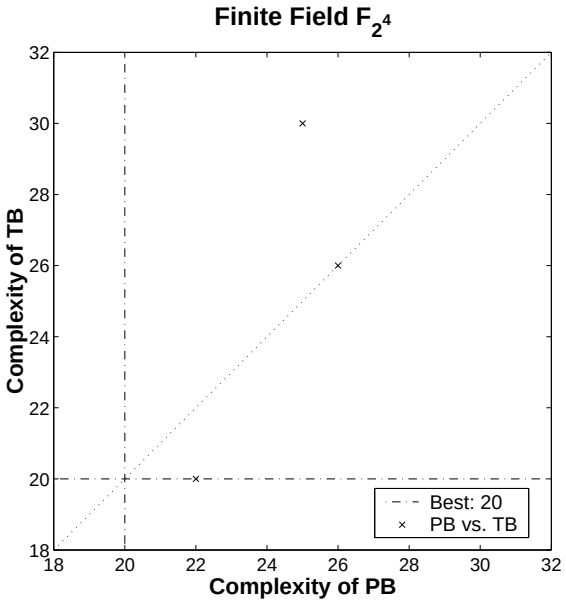

Figure C.54: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^4}$.

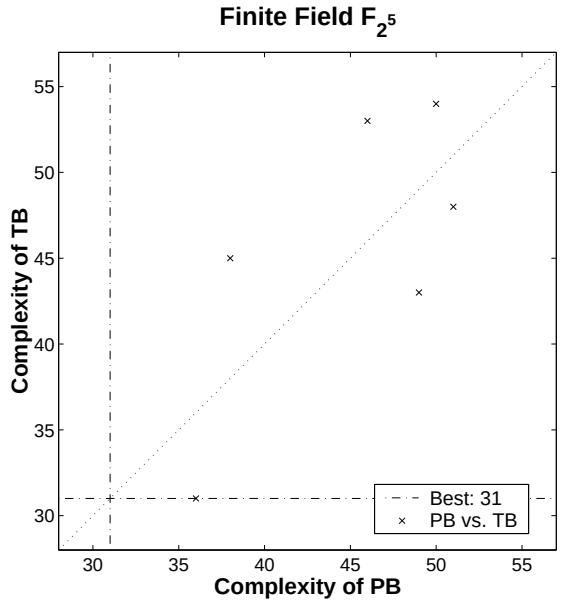

Figure C.55: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^5}$.

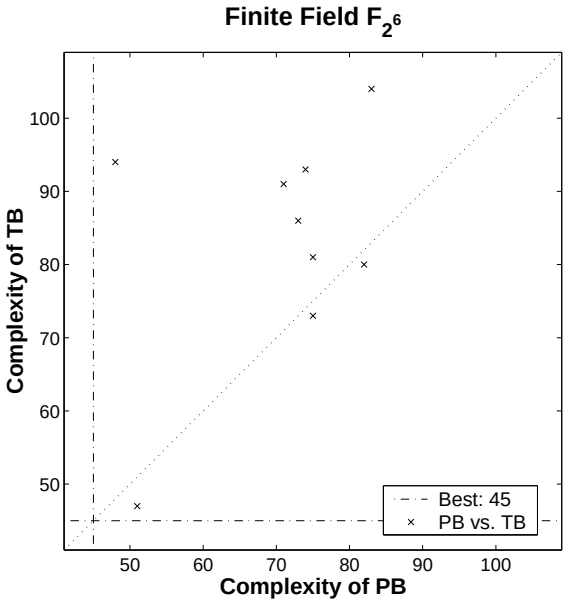

Figure C.56: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^6}$.

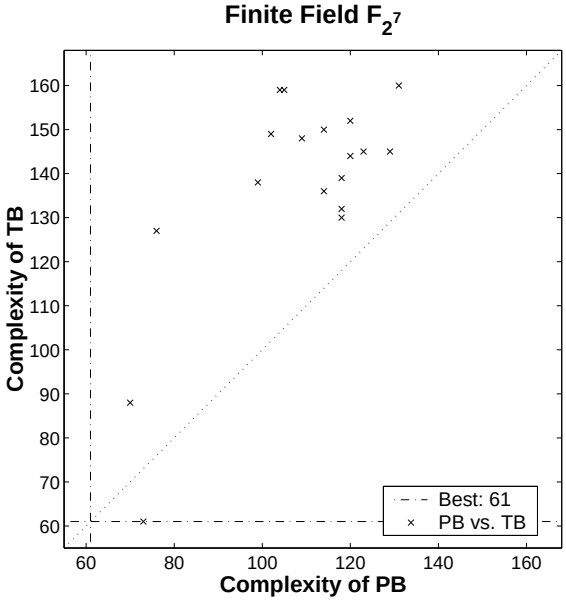

Figure C.57: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^7}$.

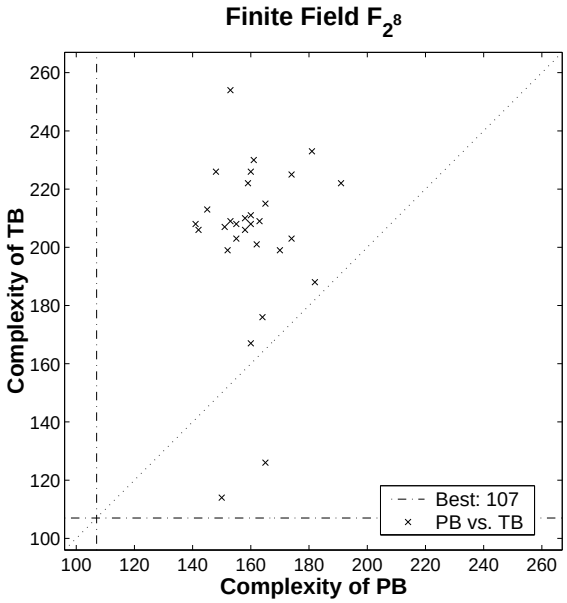

Figure C.58: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^8}$.

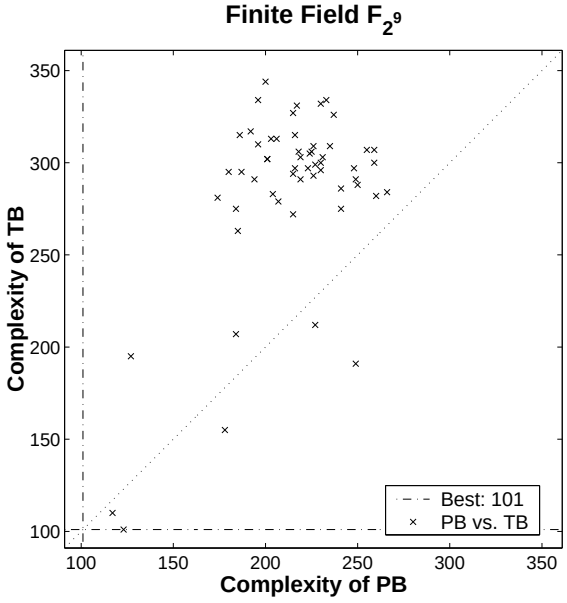

Figure C.59: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^9}$.

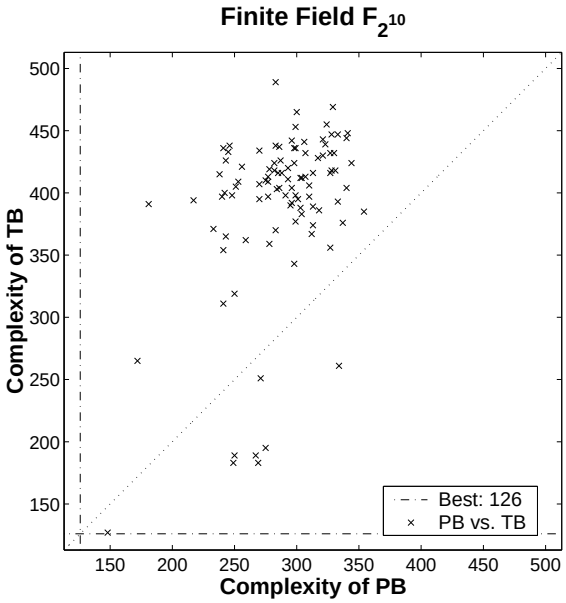

Figure C.60: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^{10}}$.

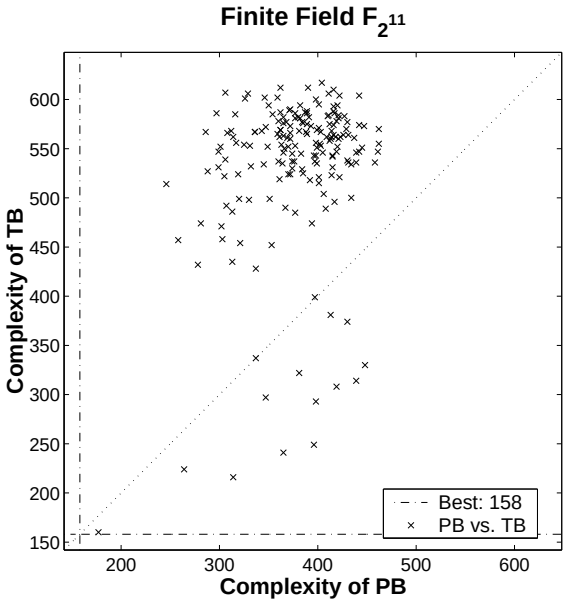

Figure C.61: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^{11}}$.

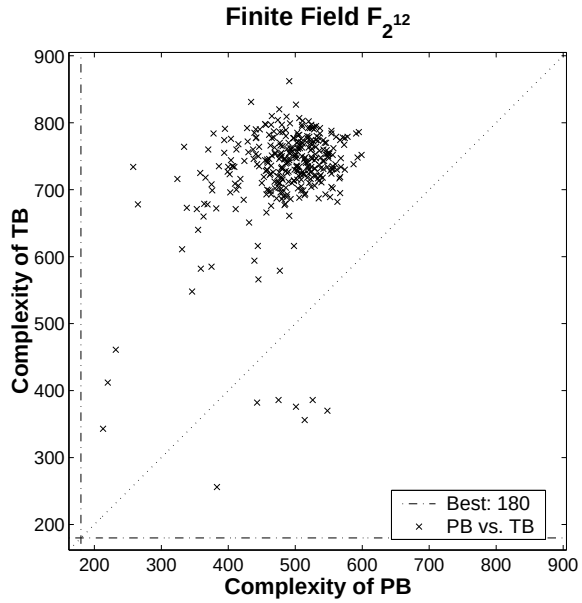

Figure C.62: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^{12}}$.

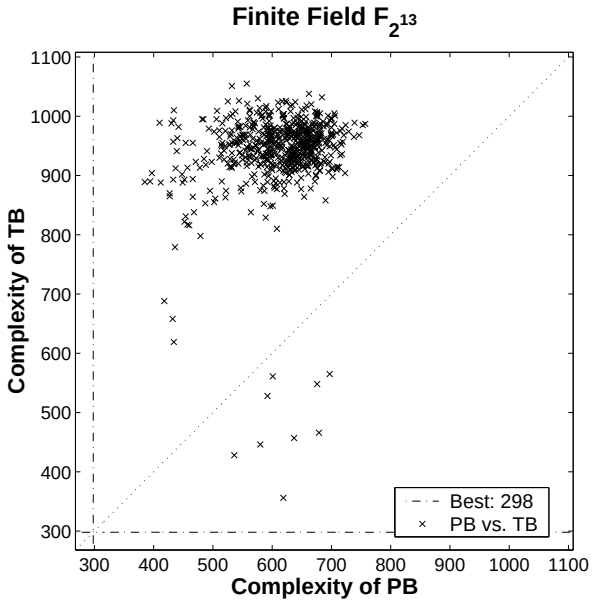

Figure C.63: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^{13}}$.

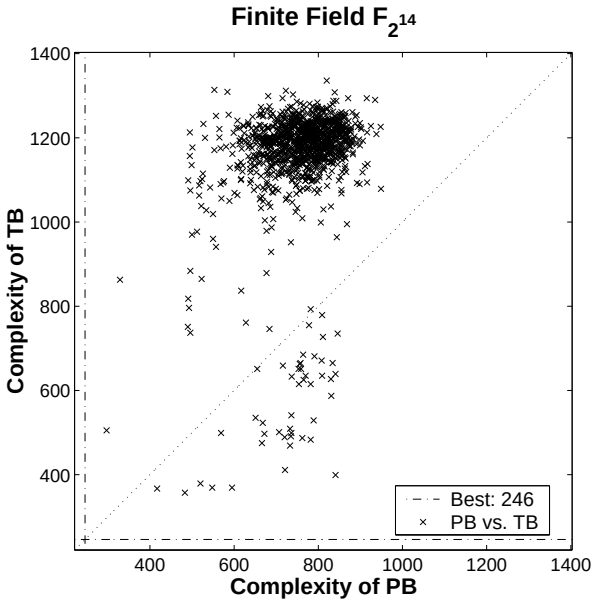

Figure C.64: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^{14}}$.

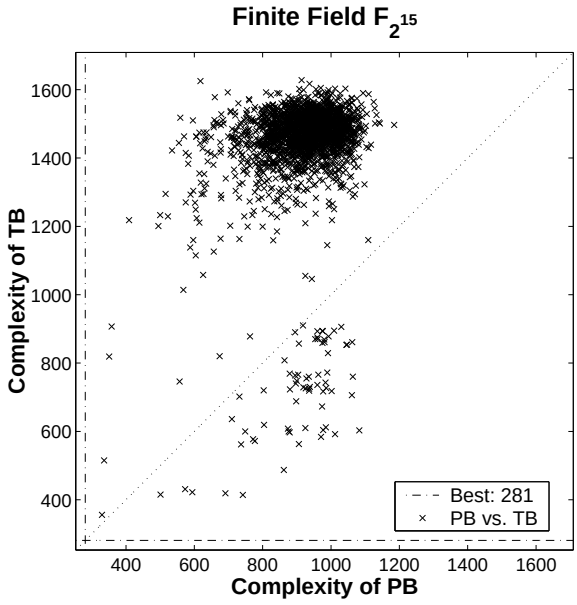

Figure C.65: Complexity of Polynomial and Triangular Bases from the field $\mathbb{F}_{2^{15}}$.

C.6 Multiples of Polynomial Bases

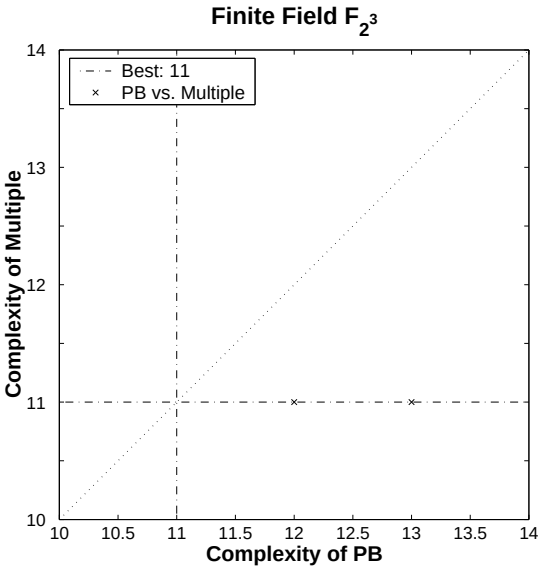

Figure C.66: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^3}$.

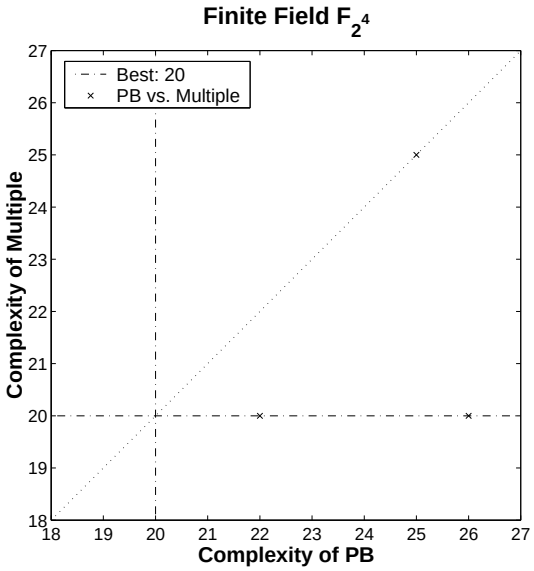

Figure C.67: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^4}$.

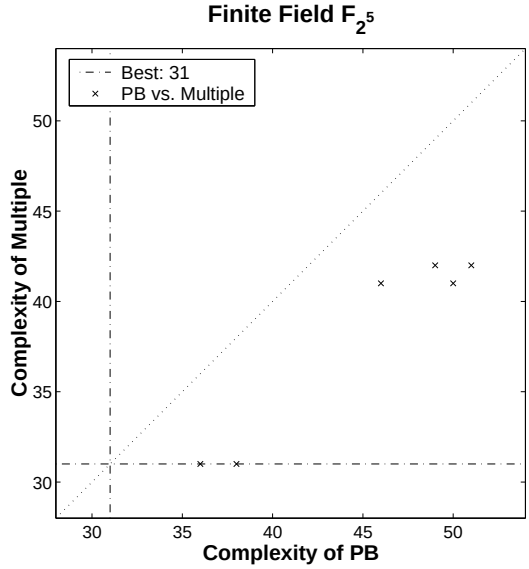

Figure C.68: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^5}$.

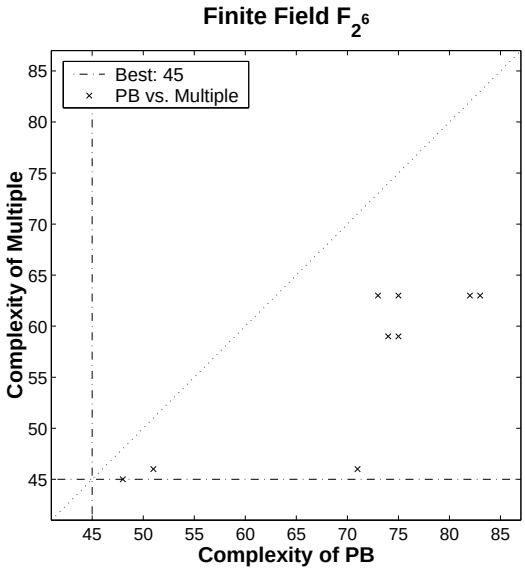

Figure C.69: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^6}$.

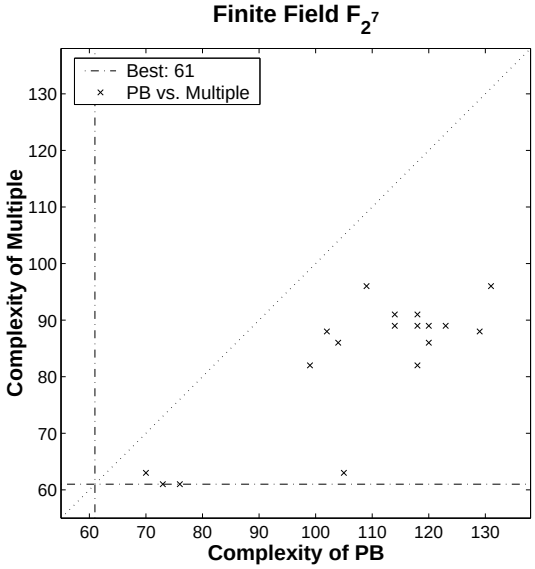

Figure C.70: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^7}$.

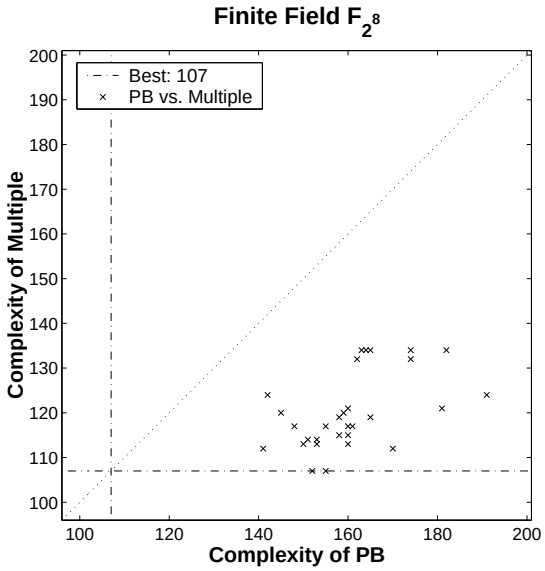

Figure C.71: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^8}$.

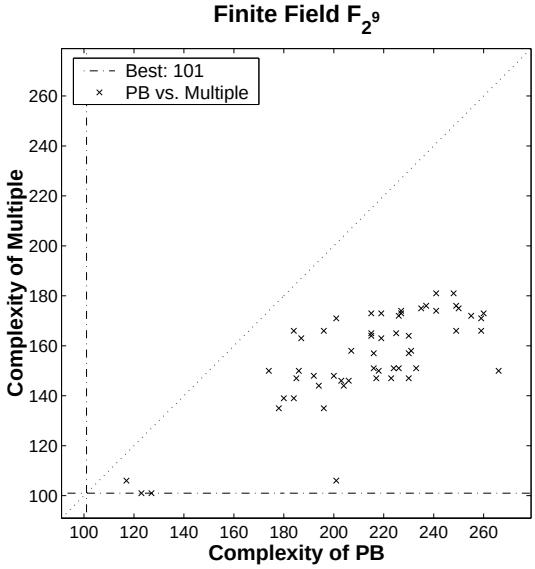

Figure C.72: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^9}$.

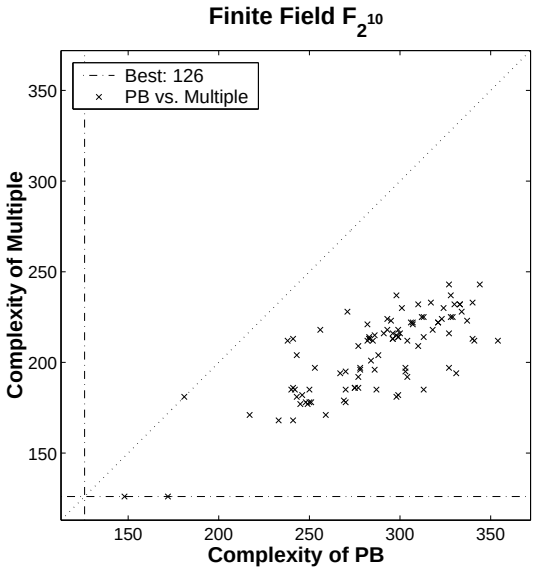

Figure C.73: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^{10}}$.

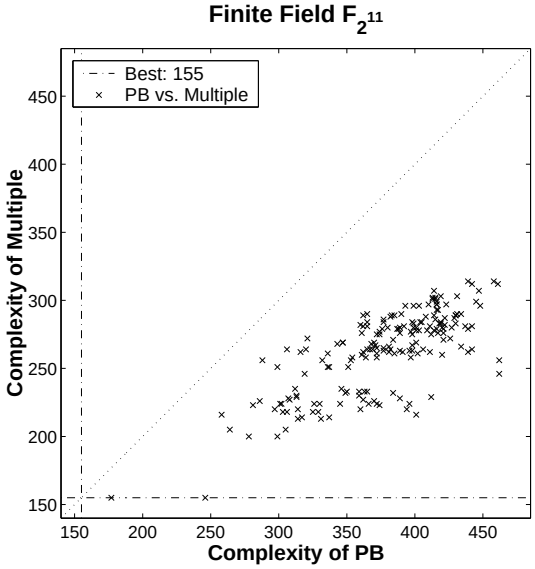

Figure C.74: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^{11}}$.

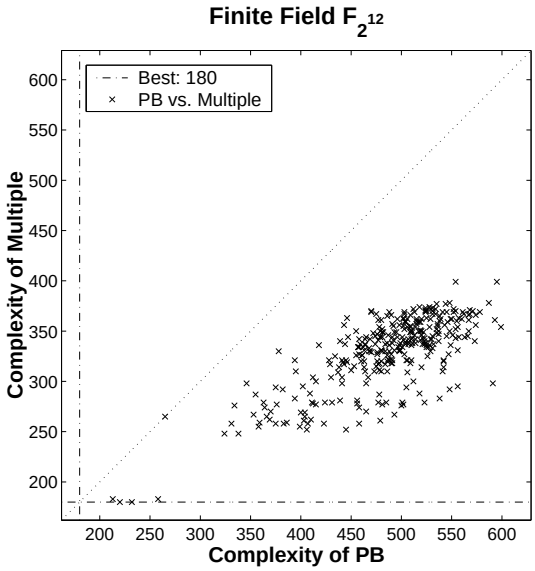

Figure C.75: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^{12}}$.

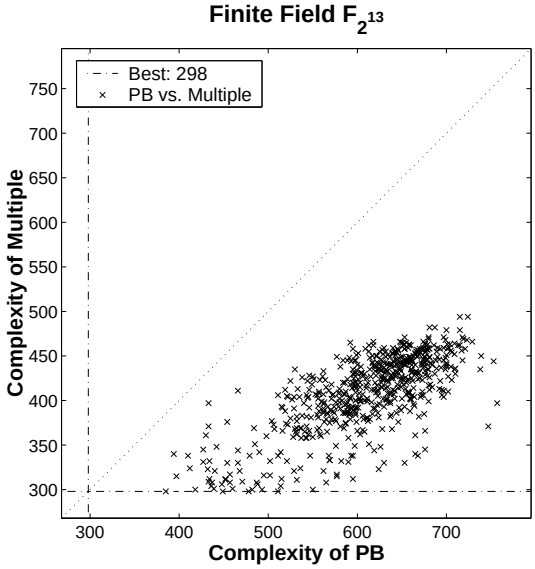

Figure C.76: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^{13}}$.

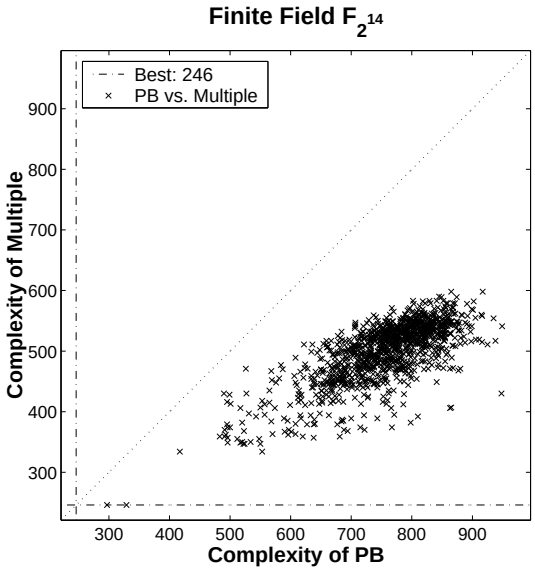

Figure C.77: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^{14}}$.

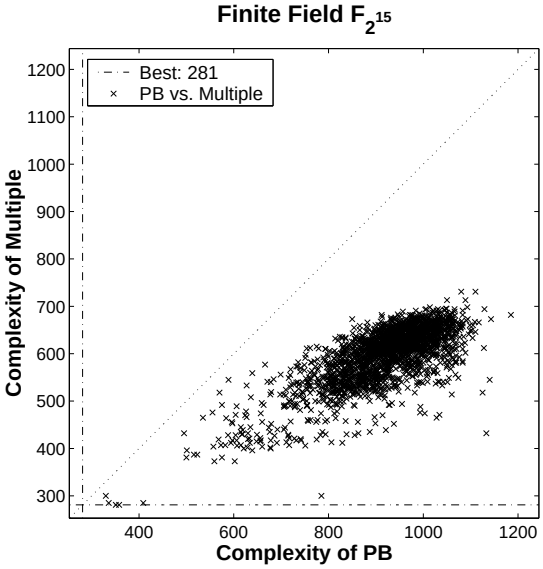

Figure C.78: Complexity of Polynomial Bases and their best Multiples, taken from the field $\mathbb{F}_{2^{15}}$.

Appendix D

Tables of Known Bases

This appendix contains tables of known bases, one for each standard basis, describing the best found bases for all fields from $\mathbb{F}_{2^2}$ up to $\mathbb{F}_{2^{24}}$.

The first table shows Polynomial Bases. Any root of the minimal polynomial will generate the Polynomial Basis with the complexity given in the table.

The second table shows Duals of Polynomial Bases. A root of the minimal polynomial generates a Polynomial Basis, and the dual basis of that PB is the one with best complexity.

The third table presents the best found Triangular Bases. The root of the minimal polynomial, given in the table, generates the Polynomial Basis used to define the best Triangular Basis.

The fourth table presents the best found Dual Triangular Bases. In the same way as for the Triangular Bases, the root of the minimal polynomial generates a Polynomial Basis, which is used to define a Triangular Basis. The dual of this TB is the Dual Triangular Basis with lowest complexity.

In the fifth table, a list of the best Normal Bases is found. The roots of the minimal polynomial found in the table generates the Normal Basis with best complexity.

As the duals of Normal Bases are Normal Bases as well, the table is the same as for the Normal Bases.

D.1 Polynomial Bases

$m :=$	*minimal polynomials*	Complexity
2	$x^2 + x + 1$	5
3	$x^3 + x + 1$	12
4	$x^4 + x + 1$	22
5	$x^5 + x^2 + 1$	36
6	$x^6 + x^3 + 1$	48
7	$x^7 + x + 1$	70
8	$x^8 + x^5 + x^3 + x^2 + 1$	141
9	$x^9 + x + 1$	117
10	$x^{10} + x^3 + 1$	148
11	$x^{11} + x^2 + 1$	177
12	$x^{12} + x^3 + 1$	213
13	$x^{13} + x^8 + x^5 + x^3 + 1$	385
14	$x^{14} + x^5 + 1$	297
15	$x^{15} + x + 1$	330
16	$x^{16} + x^{11} + x^6 + x^5 + 1$	571
17	$x^{17} + x^3 + 1$	428
18	$x^{18} + x^9 + 1$	441
19	$x^{19} + x^{16} + x^{13} + x^3 + 1$	871
20	$x^{20} + x^3 + 1$	593
21	$x^{21} + x^2 + 1$	652
22	$x^{22} + x + 1$	715
23	$x^{23} + x^5 + 1$	792
24	$x^{24} + x^{15} + x^9 + x^6 + 1$	1335

Table D.1: The best Polynomial Bases found in each Finite Field $\mathbb{F}_{2^m}$ for all extension degrees between 2 and 24.

D.2 Dual Polynomial Bases

$m :=$	*minimal polynomials*	Complexity
2	$x^2 + x + 1$	5
3	$x^3 + x + 1$	12
4	$x^4 + x + 1$	20
5	$x^5 + x^3 + 1$	31
6	$x^6 + x + 1$	47
7	$x^7 + x^3 + 1$	62
8	$x^8 + x^4 + x^3 + x^2 + 1$	127
9	$x^9 + x^5 + 1$	101
10	$x^{10} + x^3 + 1$	128
11	$x^{11} + x^9 + 1$	160
12	$x^{12} + x^8 + x^7 + x^6 + x^5 + x + 1$	183
13	$x^{13} + x^9 + x^7 + x^3 + 1$	315
14	$x^{14} + x^5 + 1$	261
15	$x^{15} + x^7 + 1$	282
16	$x^{16} + x^{10} + x^8 + x^3 + 1$	501
17	$x^{17} + x^{11} + 1$	365
18	$x^{18} + x^3 + 1$	420
19	$x^{19} + x^{13} + x^{11} + x^9 + 1$	642
20	$x^{20} + x^5 + 1$	510
21	$x^{21} + x^7 + 1$	567
22	$x^{22} + x + 1$	695
23	$x^{23} + x^9 + 1$	670
24	$x^{24} + x^{10} + x^6 + x^3 + 1$	1083

Table D.2: The best Dual Polynomial Bases found in each Finite Field $\mathbb{F}_{2^m}$ for all extension degrees between 2 and 24.

D.3 Triangular Bases

$m :=$	*minimal polynomials*	Complexity
2	$x^2 + x + 1$	5
3	$x^3 + x + 1$	11
4	$x^4 + x + 1$	20
5	$x^5 + x^2 + 1$	31
6	$x^6 + x + 1$	47
7	$x^7 + x^3 + 1$	61
8	$x^8 + x^4 + x^3 + x^2 + 1$	114
9	$x^9 + x^4 + 1$	101
10	$x^{10} + x^3 + 1$	127
11	$x^{11} + x^2 + 1$	160
12	$x^{12} + x^7 + x^6 + x^4 + 1$	256
13	$x^{13} + x^{12} + x^{10} + x^3 + 1$	356
14	$x^{14} + x^7 + x^5 + x^3 + 1$	357
15	$x^{15} + x + 1$	356
16	$x^{16} + x^{10} + x^9 + x^6 + 1$	458
17	$x^{17} + x^5 + 1$	370
18	$x^{18} + x^3 + 1$	531
19	$x^{19} + x^{15} + x^{13} + x^9 + 1$	683
20	$x^{20} + x^3 + 1$	652
21	$x^{21} + x^{16} + x^8 + x^7 + 1$	820
22	$x^{22} + x + 1$	790
23	$x^{23} + x^5 + 1$	697
24	$x^{24} + x^{19} + x^{13} + x^{11} + 1$	1066

Table D.3: The best Triangular Bases found in each Finite Field $\mathbb{F}_{2^m}$ for all extension degrees between 2 and 24.

D.4 Dual Triangular Bases

$m :=$	*minimal polynomials*	Complexity
2	$x^2 + x + 1$	5
3	$x^3 + x^2 + 1$	12
4	$x^4 + x + 1$	22
5	$x^5 + x^2 + 1$	38
6	$x^6 + x + 1$	51
7	$x^7 + x^3 + 1$	83
8	$x^8 + x^4 + x^3 + x^2 + 1$	119
9	$x^9 + x^4 + 1$	127
10	$x^{10} + x^3 + 1$	131
11	$x^{11} + x^2 + 1$	246
12	$x^{12} + x^7 + x^6 + x^4 + 1$	261
13	$x^{13} + x^{12} + x^{10} + x^3 + 1$	455
14	$x^{14} + x^9 + x^6 + x^2 + 1$	422
15	$x^{15} + x + 1$	347
16	$x^{16} + x^{10} + x^9 + x^6 + 1$	452
17	$x^{17} + x^3 + 1$	448
18	$x^{18} + x^3 + 1$	501
19	$x^{19} + x^{15} + x^{13} + x^9 + 1$	1288
20	$x^{20} + x^3 + 1$	614
21	$x^{21} + x^7 + 1$	1098
22	$x^{22} + x + 1$	786
23	$x^{23} + x^5 + 1$	820
24	$x^{24} + x^{15} + x^{14} + x^{12} + x^{10} + x^8 + 1$	1416

Table D.4: The best Dual Triangular Bases found in each Finite Field $\mathbb{F}_{2^m}$ for all extension degrees between 2 and 24.

D.5 Normal Bases

$m :=$	*minimal polynomial*	Complexity
2	1	6
3	2	15
4	3, 2, 1	28
5	4, 2, 1	45
6	5, 4, 1	66
7	6, 5, 2	133
8	7, 5, 3	168
9	8, 6, 5, 4, 1	153
10	9, 8, 7, 6, 5, 4, 3, 2, 1	190
11	10, 8, 4, 3, 2	231
12	11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1	276
13	12, 10, 7, 4, 3	585
14	13, 12, 9, 8, 1	378
15	14, 12, 9, 7, 5, 4, 2	675
16	15, 13, 12, 11, 10, 8, 7, 5, 3, 2, 1	1360
17	16, 14, 13, 12, 11, 10, 9, 7, 5, 3, 1	1377
18	17, 16, 13, 12, 10, 9, 8, 2, 1	630
19	18, 16, 11, 8, 6, 4, 1	2223
20	19, 18, 15, 14, 12, 11, 6, 3, 1	1260
21	20, 19, 17, 15, 14, 13, 9, 5, 4	1995
22	21, 20, 18, 16, 15, 14, 13, 10, 7, 5, 2	1386
23	22, 20, 16, 8, 7, 6, 4	1035
24	23, 21, 20, 19, 18, 17, 9, 8, 7, 5, 3	2520

Table D.5: The best Normal Bases (and DN) found in each Finite Field $\mathbb{F}_{2^m}$ for all extension degrees between 2 and 24.

To save space, only the degrees of the mid terms are listed, since irreducible polynomials over $\mathbb{F}_2$ always contain the terms 1 and x^m, where m is the degree. The column *minimal polynomial* should be interpeted like this.

For m equal to 3, the minimal polynomial should be $x^3 + x^2 + 1$, as the only mid term found in the table is 2. For m equal to 4, we have mid terms with degree 3, 2 and 1, and the minimal polynomial should be $x^4+x^3+x^2+x^1+1$.

Bibliography

[1] Robert J. McEliece: *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, Boston (1987)

[2] I.N. Herstein: *topics in Algebra*, Second Edition. John Wiley & Sons, New York (1975)

[3] Mikael Olofsson: *VLSI Aspects on Inversion in Finite Fields*. Unitryck, Linköping (2002)

[4] Stephen B. Wicker: *Error Control Systems for Digital Communication and Storage*. Prentince-Hall, Upper Saddle River, New Jersey (1995)