Normality of Bent Functions
Monomial- and Binomial-Bent Functions

Nils Gregor Leander

Dissertation
zur Erlangung des Grades eines
Doktor der Mathematik
der Ruhr Universität Bochum
am Fachbereich Mathematik

unter der Betreuung von
Prof. Dr. Hans Dobbertin

November 2004
Acknowledgment

First of all many thanks to Prof. Hans Dobbertin for supervising this thesis. His great support and advice helped me a lot in my research over the past three years. He always pointed out the right questions and taught me not to be afraid of huge polynomials.

I would like to thank all the members of the CITS research group and the Lehrsuthl für Informatik. I really enjoyed the fruitful discussions with Magnus Daum, Eike Kiltz, Tanja Lange and specially with Patrick Felke, who always had time to discuss even stupid ideas. Thanks to Elena Prokhnorenko and Rita Schröer for their technical and administrative support.

Thanks also to the European Union for their Marie Curie Fellowship, that allowed me to spent three months in Aarhus, Denmark. Many thanks to all the people at the BRICS research group for their hospitality. Especially to Ronald Cramer for very interesting discussions in the smoking room.

Thanks to the CODES research group at INRIA in Versailles for two great weeks of joint research and their great hospitality. Special thanks to Claude Carlet and Anne Canteaut for many ideas and suggestions of open problems.

I would also like to thank the GRIM research group in Toulon. Thanks to Philippe Langevin and Julien Bringer for their invitation and pointing me to interesting questions and tools and of course for organizing the great YACC conferences.

Thanks to Alexander Kholohosa for nice discussions about more Niho bent functions and reviewing the first version of a proof for these families.

I would also like to thank our students, Thorsten Doliwa and Michael Kallweit, for implementing my algorithms.

Finally, thanks to Milena for her endless love and to my family for supporting me in everything I decided to do.
# Contents

1 Preface and Summary 1

2 Preliminaries 9

3 Normal and Non-Normal Bent Functions 15
   3.1 Introduction ........................................... 15
   3.2 Normality of the known families of bent functions ........ 16
      3.2.1 Direct constructions ............................... 16
      3.2.2 Modified Maiorana-McFarland Bent Functions ....... 17
   3.3 Non Normal Bent Functions ............................... 22
   3.4 An Algorithm for Checking Normality ..................... 25
   3.5 Further Applications of the Algorithm .................... 25
      3.5.1 Maiorana-McFarland Functions ...................... 26
      3.5.2 Other Classes of Bent Functions .................... 27

4 Normal Extensions of Bent Functions 29
   4.1 Introduction ........................................... 29
   4.2 Normal Extensions and Normality of Direct Sums .......... 31
   4.3 Examples of Normal Extensions ........................... 35
   4.4 Duality of Normal Extensions and Plug-in Theorem ....... 38
   4.5 Normality Inherits Downwards ........................... 40
   4.6 Totally Non-Normal Bent Functions ..................... 42
      4.6.1 Testing Totally Non-Normality .................... 43

5 Monomial Bent Functions 45
   5.1 Introduction ........................................... 45
   5.2 Known Cases ............................................ 48
      5.2.1 The Gold Case ...................................... 48
      5.2.2 The Dillon Case .................................... 50
      5.2.3 The Dillon-Dobbertin Case ......................... 53
   5.3 A New Bent Exponent for $n = 4r$ ........................ 56
5.4 Niho Exponents and Stickelberger’s Theorem . . . . . . . . . . 61

6 Binomial Bent Functions 67
6.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . 67
6.2 Main Results . . . . . . . . . . . . . . . . . . . . . . . . . . . 69
6.3 Niho’s Theorem and Dickson Polynomials . . . . . . . . . . . 72
6.4 One-to-one Rational Functions . . . . . . . . . . . . . . . . . 77
6.5 Proof of Theorem 6.1 . . . . . . . . . . . . . . . . . . . . . . . 82
6.6 Proof of Theorem 6.3 . . . . . . . . . . . . . . . . . . . . . . . 84
6.7 Niho Bent Functions with $2^t$ Terms . . . . . . . . . . . . . . 85
Chapter 1
Preface and Summary

Bent functions are maximally nonlinear Boolean functions with an even number of variables and were introduced by Rothaus [38] in 1976. Because of their own sake as interesting combinatorial objects, but also because of their relations to coding theory and applications in cryptography, they have attracted a lot of research, specially in the last ten years.

Despite their simple and natural definition, bent functions have turned out to admit a very complicated structure in general. On the other hand many special explicit constructions are known, primary ones giving bent functions from scratch and secondary ones building a new bent function from one or several given bent functions.

This thesis mainly deals with two important aspects of bent functions.

Normality of Bent Functions
The main complexity characteristics for Boolean functions on $\mathbb{F}_2^n$ which are relevant to cryptography are the algebraic degree and the nonlinearity. But other criteria have also been studied. One of them is the question if there exists a space of dimension $\frac{n}{2}$ such that the restriction of a given function is constant (resp. affine) on this space. This question is also interesting due to a close relationship to the recently developed notion of algebraic immunity of Boolean functions (see [33]) which is related to the algebraic attack on stream ciphers.

We call the functions for which such a space exists normal (resp. weakly-normal). The notion of normality was introduced for the first time in [21]. While for increasing dimension $n$ a counting argument can be used to prove that nearly all Boolean functions are non-normal, the situation for bent functions is different. Most of the well studied families of bent functions are obviously normal and furthermore, unlike for arbitrary Boolean functions, normality has strong consequences for the behavior of bent functions. One of
the consequences is, that if a bent function $f$ is constant on an $\frac{n}{2}$-dimensional affine subspace, then $f$ is balanced on each of the other cosets of this affine subspace. In other words, a normal bent function can be understood as a collection of balanced functions and the question if non-normal bent functions exist, is therefore an important question towards a characterization of bent functions in general. The interpretation of a normal bent function as a collection of balanced functions was used in [21] for a new primary construction of normal bent functions. Furthermore, this fact was used in the same paper to construct balanced functions with high nonlinearity.

The third chapter of this thesis is devoted to the discussion of normality of bent functions. We recall that all the main known families of bent functions are normal and present the first non-normal and even non-weakly normal bent functions, thus answering an important question about the general structure of bent functions. These functions belong to a class of bent functions discovered by Dillon and Dobbertin in [20]. As a consequence of this result we demonstrate for the first time a bent function, that is not affine equivalent to any bent function in the Maiorana-McFarland nor the Partial Spread family of bent functions.

The main results of Chapter 3 will be published in [7].

In the fourth chapter we develop the concept of normal extensions, which turns out to be a very powerful tool to prove results on the normality of bent functions constructed from other bent functions. The notion of a normal extension can be viewed as a generalization of the direct sum of an arbitrary bent function with a normal bent function. In particular this concept enables us to prove, that the direct sum of a normal and a non-normal bent function is always non-normal, confirming an open conjecture by S. Gangopadhyay, S. Maitra [31] and C. Carlet. The main theorem is actually more general and states, that every normal extension of a non-normal bent function is non-normal. We furthermore construct examples of normal extensions not corresponding to a direct sum of bent functions.

The main results of this chapter will be published in [14].

We also present two algorithms that allowed us to check the desired properties. At the end of Chapter 3 we sketch an algorithm that verifies if a given function is (weakly) normal or not, much faster than by exhaustively checking all subspaces and in Chapter 4 we describe a generalization that enables us to test, if a bent function is a normal extension of another bent function.

Monomial and Binomial Bent Functions
A complete classification of bent functions is elusive and looks hopeless today. As a first step towards a characterization of all bent functions, in the second
part of this thesis we focus on traces of power functions, so called *monomial* Boolean functions. This approach is well known in related areas like almost perfect non linear (APN) functions or *m*-sequences, but has not yet been comprehensively studied for bent functions. This approach turns out to be very fruitful for several reasons. The only known non-normal bent functions are monomial bent functions, demonstrating that the study of monomial functions leads to new classes of bent functions. Furthermore, one result of our considerations is, that for each of the well studied families of bent function, there is a monomial bent function belonging to these classes. Moreover, carefully studying the proofs for the monomial bent functions all these families can quite easily be rediscovered. In this sense most of the variety of (at least known) bent functions can already be discovered by the investigation of monomial functions.

In Chapter 5 we first recall all the known cases of monomial bent functions. In the case of the Dillon exponent we give an alternative proof of the known connection to the Kloosterman Sum, avoiding results from coding theory. In the case of the Dillon-Dobbertin monomial bent function we present an algorithmic approach to study the dual of these bent functions. Using this algorithm we conclude, that for dimension 8 the dual of this bent function is linearly equivalent to the function itself, whereas for dimensions 10, 12, 14 the dual is not linearly equivalent to the monomial bent function.

As one of our main results in this Chapter we present a new class of monomial bent functions, not corresponding to one of the known monomial bent functions. This class was found with the help of computer experiments by A. Canteaut, who first conjectured that the concrete examples found belong to the new class.

In contrast to the first part, where we prove the bentness of several monomial functions, in the last part of Chapter 5 we give a strong indication why a large class of monomial Boolean functions does not contain any bent functions. This contrast is also reflected in the different technique we apply in this section.

In Chapter 6 we take the natural step forward and extend our focus to linear combinations of two power functions. In particular we focus on Niho power functions, i.e. power functions where the restriction to the subfield of index 2 is linear. Using classical results for the Walsh-Spectrum of these functions and techniques recently developed by Dobbertin, we present several new primary constructions of bent functions. These results are based on new techniques to study certain properties of rational functions. More precisely we present a general procedure to prove that certain rational functions induce one-to-one mappings.

These techniques and the Multivariate-Method developed by Dobbertin
(see [23]) follow the same line of reasoning. Both approaches are strongly based on properties of mappings, that can be defined in a global way, meaning that these properties are valid for an infinite chain of finite fields. In both situations this results in generic discussion of specific rational functions. These generic discussions are often conceptionally relatively easy, while the actual inherent computations require the help of computer algebra. One key step is often to find the factorization of (parameterized) polynomials, which usually is not feasible by hand calculations. Nevertheless, once the factorization has been found, verifying the result is much easier and can in most cases be done by hand.

The main results from Chapter 6 will be published in [19]

**Related Topics**

Bent functions play a very important role in Cryptography. In the design of Stream-Ciphers or for S-Boxes in Block-Ciphers, there is a strong need for highly non-linear functions, to make these ciphers resistant against linear attacks. Due to the fact that high non-linearity is not the only important criterion in this area, bent functions are usually not directly used, but they serve as a starting point for the construction of highly non-linear functions that also meet other criteria. For example the best known constructions for highly non-linear balanced functions, introduced by Dobbertin (see [21]), are based on normal bent functions.

Bent functions also play an important role in the area of Reed-Muller Codes. The first order Reed-Muller Code consists of all affine functions on $\mathbb{F}_2^n$ and, if $n$ is even, bent functions on $\mathbb{F}_2^n$ can be characterized as the functions having the maximal possible distance to all the code-words in the first order Reed-Muller Code.

Furthermore Kerdock codes are constructed using (quadratic) bent functions. These non-linear codes achieve parameters that linear codes cannot achieve.

Another field that is closely related (at least in special cases) is Difference Sets. Given an abelian (multiplicative) group $G$ of order $v$, a subset $D \subseteq G$ of order $k$ is called a $(v,k,\lambda)$-difference set in $G$, if for each non-identity element $g$ in $G$, the equation

$$g = xy^{-1}$$

has exactly $\lambda$ solutions $(x,y)$ in $D$. It is known that, given a non trivial difference set $D$ in $(\mathbb{F}_2^n, +)$, we always have

1. $n$ is even,
2. $k = 2^{n-1} + 2^{n/2-1}$, $\lambda = 2^{n-2} + 2^{n/2-1}$ or
There is a natural one-to-one correspondence between Boolean functions on $\mathbb{F}_2^n$ and subsets of $\mathbb{F}_2^n$. A Boolean function $f$ on $\mathbb{F}_2^n$ can be characterized by its support, i.e. by the set

$$E_f := \{ x \in \mathbb{F}_2^n \mid f(x) = 1 \}.$$ 

As bent functions are precisely the Boolean functions having ideal autocorrelation, it is easy to see that this set $E_f$ is a non-trivial difference set in $\mathbb{F}_2^n$ if and only if $f$ is a bent function. Thus, the open question of characterizing all non-trivial difference set $D$ in $(\mathbb{F}_2^n,+)$ is equivalent to characterizing all bent functions.

Bent functions can also be characterized in terms of graph theory. Given a boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, we can associate the graph $G_f$, where the vertex set of $G_f$ is equal to $\mathbb{F}_2^n$, while the edge set $E_f$ of $G_f$ is defined as

$$E_f = \{ (u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid f(u+v) = 1 \}$$

It was shown in [1, 2], that $f$ is a bent function if and only if for all vertices $u,v$ the number of vertices adjacent to both $u$ and $v$ is constant. In particular that means that $G_f$ is a strongly regular graph. Note that this characterization is equivalent to the characterization of bent functions as difference sets.

Concerning properties of monomial functions, we would like to mention some other related topics.

The area of binary $m$-sequences, in particular computing the cross-correlation of a sequence and its decimation corresponds to computing the Walsh-spectra of monomial Boolean functions. There are some minor differences, mainly in the notation. A binary $m$-sequences can be represented by first choosing a generator $\alpha$ of $\mathbb{F}_2^n$ and a non-zero element $a \in \mathbb{F}_2^n$. The sequence is then defined as

$$s(t) = \text{tr}(aa^t) \quad 0 \leq t \leq 2^n - 2.$$ 

Given an integer $d$ coprime to $2^n - 1$, the sequence $\{s(td)\}$ is called a decimation of $\{s(t)\}$. One of the main characteristic in this topic is the cross-correlation between two sequences $\{s(t)\}$ and $\{r(t)\}$ defined by

$$\theta_{s,r}(\tau) = \sum_{t=0}^{2^n-2} (-1)^{r(t+\tau)+s(t)}, \quad 0 \leq \tau \leq 2^n - 2.$$ 

With this notation, the cross-correlation of the sequence $\{s(t)\}$ and its decimation by $d$ coincides with the Walsh-Coefficients of the monomial function
$x \rightarrow \text{tr}(ax^d)$, up to a constant of $-1$. A main difference to our considerations is, as explained in Chapter 5, that the exponents we will consider always have a non trivial common divisor with $2^n - 1$.

The Walsh-Coefficients of monomial functions also appear in the theory of binary codes with two zeros $\alpha$ and $\alpha^d$, where $d$ is usually coprime to $2^n - 1$. The dual of such a code can be represented by all words

$$(\text{tr}(ax^d + bx))_{x \in \mathbb{F}_2^n}$$

where $a, b \in \mathbb{F}_2^n$. Thus the weights of these code words corresponds to the Walsh-Coefficients of $x \rightarrow \text{tr}(ax^d)$, again up to a constant of $-1$.

We would also like to point out a connection to almost perfect non-linear (APN) functions. From a cryptographical point of view these function are the optimal choice for S-Boxes in Block-Ciphers due to their resistance against differential attacks. The properties of APN functions are not directly connected to Walsh-Transformations, but the application of monomial functions to this area is well known. Moreover, all APN functions known are equivalent to monomial functions. For many of these monomial functions the Multivariate Method mentioned above is the main tool to prove the APN property.

One important step to classify all APN power mappings was taken at WCC 2003 by Dobbertin [24], where he introduced the notion of a power function for the infinite (but locally finite) field

$$\mathcal{L} = \bigcup_{(n, m) = 1} \mathbb{F}_{2^n}$$

where $m$ is an integer. A mapping $\pi : \mathcal{L} \rightarrow \mathcal{L}$ is called a power mapping if $\pi|_{\mathbb{F}_{2^n}}$ is a power mapping for every $n$ with $\gcd(n, m) = 1$. Thus every power mapping on $\mathcal{L}$ can be represented by a sequence of exponents $(d_n)_{n \in \mathbb{N}}$ where

$$\pi|_{\mathbb{F}_{2^n}} = x^{d_n}.$$ 

This sequence of exponents has the property that, given integers $n_1$ and $n_2$ such that $n_1 | n_2$ and

$$\pi|_{\mathbb{F}_{2^{n_1}}} = x^{d_{n_1}}$$

$$\pi|_{\mathbb{F}_{2^{n_2}}} = x^{d_{n_2}},$$

then

$$d_{n_1} \equiv d_{n_2} \mod 2^{n_1} - 1.$$ 

Vice versa every sequence of exponents fulfilling this property defines a power mapping on $\mathcal{L}$. 
The easiest example of a power function on $L$ is the case where all the exponents $d_n$ are the same. Thus, the problem of characterizing all fixed exponents $d$, such that the mapping $x \rightarrow x^d$ is APN for an infinite number of finite fields of characteristic two, is a special case of the approach described above. It is easy to see, that every fixed exponent of the so called Gold and Kasami case fulfill this condition. A well known and challenging conjecture is, that there are no other exponents with this property. Using methods from algebraic geometry some progress in proving this conjecture was made in [28] where they adopted techniques used in the closely related area of hyperovals (see for example [32]). The main idea was to transfer the APN property into a property of certain algebraic curves and use known bounds on the number of points of these curves to deduce a contradiction to the APN property.

It turns out, that all known APN functions defined on concrete finite fields can be extended to power functions defined on the field $L$. All the known exponents of monomial bent functions can also be defined in a similar global way. As we are considering finite fields with even degree over $F_2$ and traces of non-bijective power mappings, we have to consider a slightly different global field.
Chapter 2
Preliminaries

Throughout let $n = 2k$ be an even number. We recall some definitions and basic properties.

**Walsh-Transform and Bent Functions**

Given a Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, the function

$$a \in \mathbb{F}_2^n \mapsto f^W(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) + \langle a, x \rangle}$$

is called the *Walsh transform* of $f$. Moreover, the values $f^W(a), a \in \mathbb{F}_2^n$ are called the Walsh coefficients of $f$. The set

$$\{f^W(a), a \in \mathbb{F}_2^n\}$$

is called the Walsh-spectrum of $f$. Note that the Walsh-spectrum is not changed if we replace $f$ by $f \circ H$ where $H$ is a bijective affine or linear mapping, moreover adding an affine mapping does not change the absolute values of the Walsh-spectrum. Thus in most of our discussions we do not distinguish between these affine or linear equivalent functions.

By looking at the $\pm 1$ valued function $F = (-1)^f$ the Walsh-transform of $f$ corresponds (up to scaling) to the additive Fourier transform of $F$.

$$\hat{F} = 2^{-k} \sum_{x \in \mathbb{F}_2^n} F(x)(-1)^{\langle y, x \rangle}.$$ 

Due to the fact, that this transform is effected by the Hadamard matrix

$$((-1)^{\langle y, x \rangle})_{x,y \in \mathbb{F}_2^n}$$

it is also sometimes called *Hadamard transform*. There are a few properties of the Hadamard transform, that we like to recall here.
For the operator $F \rightarrow \hat{F}$ we have the involution law
\[ \hat{\hat{F}} = F \]
and with
\[ (F \ast G)(x) = \sum_{u \in \mathbb{F}_2^n} F(u + x)G(x) \]
the convolution law
\[ \hat{F} \ast \hat{G} = 2^k \hat{F} \hat{G}. \]
If we regard $\mathbb{R}^{\mathbb{F}_2^n}$ as an inner-product space where,
\[ \langle F, G \rangle = \sum_{x \in \mathbb{F}_2^n} F(x)G(x) \]
the map $F \rightarrow \hat{F}$ is an orthogonal operator on $\mathbb{R}^{\mathbb{F}_2^n}$, i.e.
\[ \sum_{x \in \mathbb{F}_2^n} F(x)G(x) = \sum_{y \in \mathbb{F}_2^n} \hat{F}(y)\hat{G}(y). \]

A measure of the linearity of a Boolean function $f$ with respect to the Walsh transform is defined by
\[ \text{Lin}(f) = \max_{a \in \mathbb{F}_2^n} |f^W(a)|. \]
Obviously we have the upper bound
\[ 2^n \geq \text{Lin} f, \]
and it is attained if and only if $f$ is affine.

For $n$ even, $f$ is called bent if $\text{Lin}(f) = 2^{n/2}$, which is the minimal value that can occur and we then have $f^W(a) = \pm 2^{n/2}$ for all $a \in \mathbb{F}_2^n$, since
\[ \sum_{a \in \mathbb{F}_2^n} f^W(a)^2 = 2^n \quad (\text{Parseval’s equation}). \]

Note that Parseval’s equation is a direct consequence of the above mentioned fact that the operator $F \rightarrow \hat{F}$ is orthogonal. Another measurement for the linearity of a Boolean function $f$ is the autocorrelation function. It is defined by
\[ AC_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x+a) + f(x)}. \]

Bent functions can also be characterized in terms of their Autocorrelation function, which again follows directly from the orthogonality of the Fourier transform.
Proposition 2.1. A Boolean function $f$ on $\mathbb{F}_2^n$ is bent if and only if $AC_f(a) = 0$ for all non-zero $a \in \mathbb{F}_2^n$.

Bent functions always occur in pairs. In fact, given a bent function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, we define the dual $f^*$ of $f$ by the equation

$$(-1)^{f^*(a)} 2^{n/2} = f_W(a),$$

i.e. we consider the signs of the Walsh-coefficients of $f$. Due to the involution law the Fourier transform is self-inverse. Thus the dual of a bent function is again a bent function, and we have the rule $f^{**} = f$.

Every Boolean function can be uniquely described by its Algebraic Normal Form (ANF)

$$f(x) = \sum_{u \in \mathbb{F}_2^n} \lambda_u \prod_{i=1}^n x_i^{u_i}, \quad \lambda_u \in \mathbb{F}_2.$$

The degree of a Boolean function is the maximal value of $\text{wt}(u)$ such that $\lambda_u \neq 0$. It was already proven by Rothaus, that the degree of a bent function is at most $k$. Furthermore the dual of a bent function of degree 2 (resp. $k$) has also degree 2 (resp. $k$) (see [38]).

Given Boolean functions $f_i : \mathbb{F}_2^{n_i} \rightarrow \mathbb{F}$ ($i = 1, 2$), we define their direct sum $f_1 \oplus f_2 : \mathbb{F}_2^{n_1} \oplus \mathbb{F}_2^{n_2} \rightarrow \mathbb{F}_2$ by setting

$$(f_1 \oplus f_2)(x_1 + x_2) = f_1(x_1) + f_2(x_2), \quad x_i \in \mathbb{F}_2^{n_i}.$$

The Walsh transform of a direct sum is given by

$$(f \oplus g)^W = f^W g^W.$$

Boolean Functions on $\mathbb{F}_2^n$

We will often identify the vector space $\mathbb{F}_2^n$ with the Galois field $L = \mathbb{F}_{2^n}$. As the notion of a Walsh transform refers to a scalar product, it is convenient to choose the isomorphism such that the canonical scalar product $\langle \cdot, \cdot \rangle$ in $\mathbb{F}_2^n$ coincides with the canonical scalar product in $L$, which is the trace of the product:

$$\langle x, y \rangle = \sum_{i=1}^n x_i y_i = \text{tr}_L(xy), \quad x, y \in L.$$

Thus the Walsh transform of $f : L \rightarrow \mathbb{F}_2$ is defined as

$$f^W(c) = \sum_{x \in L} (-1)^{f(x)} \chi_L(cx), \quad c \in L,$$
where
\[ \chi_L(x) := (-1)^{\text{tr}_L(x)} \]
is the canonical additive character on \( L \).

We often make use of the following known properties of the trace function.
\[ \text{tr}_L(x) = \text{tr}_L(x^2) \]
\[ \text{tr}_L(x) = 0 \iff x = y^2 + y \]

Throughout let \( K = \mathbb{F}_{2^k} \) be the subfield of \( L \) with \([L : K] = 2\). When dealing with Boolean functions on \( L \), in particular monomial functions, we will use the following notation. The \emph{conjugate} of \( x \in L \) over \( K \) will be denoted by \( \overline{x} \), i.e.
\[ \overline{x} = x^{2^k}. \]

We denote the \emph{relative trace} from \( L \) onto \( K \) by
\[ \text{tr}_{L/K}(x) = x + \overline{x} \]

Note that according to the transitivity law for the trace function we have
\[ \text{tr}_L = \text{tr}_K \circ \text{tr}_{L/K}. \]

The relative norm with respect to \( L/K \) is defined as
\[ \text{norm}_{L/K}(x) = x \overline{x} \]
and maps \( L \) onto \( K \).

The \emph{unit circle} of \( L \) is the set
\[ \mathcal{S} = \{ u \in L : u \overline{u} = 1 \} \]
of all elements having relative norm 1. In other words \( \mathcal{S} \) is the group of \((2^k + 1)\)-st roots of unity, and therefore the order of \( \mathcal{S} \) is \( 2^k + 1 \), since \( L^* \) is cyclic and \( 2^k + 1 \) divides \( 2^n - 1 \).

Note that \( \mathcal{S} \cap K = \{ 1 \} \) and each non-zero element of \( L \) has a unique \emph{polar coordinate representation}, i.e.
\[ x = \lambda u \]
with \( \lambda \in K^* \) and \( u \in \mathcal{S} \). According to the analogy to \( \mathbb{C}/\mathbb{R} \) we write \( \lambda = \|x\| \) for the \emph{length} and \( u = \varphi(x) \) for the \emph{angle} of \( x \). We have
\[ \text{norm} x = \sqrt{x \overline{x}}, \quad (2.1) \]
\[ \varphi(x) = \sqrt{x / \overline{x}}. \quad (2.2) \]

Where the symbol \( \sqrt{X} \) stands for the inverse of the Frobenius mapping \( \varphi(X) = X^2 \), which makes sense, as we deal with finite fields of characteristic 2. Concretely here \( \sqrt{z} = z^{2^{k-1}} \) for \( z \in K = \mathbb{F}_{2^k} \).
Normality of Boolean Functions

Chapter 3 and Chapter 4 are mainly devoted to the discussion of normality of bent functions. We recall the basic definitions here.

Normality is a property of the restriction of Boolean functions to subspaces or affine translations of subspaces. For simplicity we call a $t$-dimensional affine subspace a flat of dimension $t$.

**Definition 2.2.** A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}$ is called normal if there exists a flat of dimension $m$, such that $f$ is constant on this flat.

As bentness is invariant under addition of affine functions, it is natural to consider a generalization of Definition 2.2.

**Definition 2.3.** A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}$ is called weakly-normal if there exists a flat of dimension $m$, such that the restriction of $f$ to this flat is affine.

Unlike for arbitrary Boolean functions, for bent functions being normal has strong consequences. The following well known lemmas state some of the most important properties of normal bent functions.

**Lemma 2.4.** Assume that $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is a normal bent function, which is accordingly constant on an affine subspace $V \subseteq \mathbb{F}_2^n$ with $\dim V = k$. Then $f$ is balanced on each proper coset of $V$.

Normality of a bent function is also reflected in the dual bent function, as stated in the next lemma.

**Lemma 2.5.** Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a bent function and $V \subseteq \mathbb{F}_2^n$ any $n/2$-dimensional subspace. Then $f$ is constant on $a + V$ for $a \in \mathbb{F}_2^n$ if and only if $f^* + \phi_a$ is constant on $V^\perp$. Where

\[
\phi_a(x) = \langle a, x \rangle
\]

□

Another important observation is, that a bent function $f$ on $\mathbb{F}_2^n$ cannot be constant on an affine subspace of dimension greater than $k$. This is a direct consequence of the following lemma.

**Lemma 2.6.** Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}$ be a Boolean function, $U \subseteq \mathbb{F}_2^n$ a subspace and $g = f|_U$, then $\text{Lin}(g) \leq \text{Lin}(f)$
Proof. There exist several ways of proving this known fact. The simplest one is by induction: it suffices to consider the case that $\dim U + 1 = n$. Thus suppose without loss of generality $U = \mathbb{F}_2^{n-1}$ and $f_0 = g = f|_{U \times \{0\}}$, $f_1 = f|_{U \times \{1\}}$. Then
\[
f^W = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} f^W_0 \\ f^W_1 \end{pmatrix} = \begin{pmatrix} f^W_0 + f^W_1 \\ f^W_0 - f^W_1 \end{pmatrix},
\]
i.e. $f^W|_{U \times \{0\}} = f^W_0 + f^W_1$ and $f^W|_{U \times \{1\}} = f^W_0 - f^W_1$. On the other hand,
\[
\max \{|a_0 + a_1|, |a_0 - a_1|\} \geq |a_0|
\]
for all numbers $a_0, a_1$, and therefore $\text{Lin}(f) \geq \text{Lin}(g)$. 
\[\square\]
Chapter 3

Normal and Non-Normal Bent Functions

3.1 Introduction

For arbitrary Boolean functions, an easy counting argument shows that there must exist non normal functions of \( n \) variables for \( n > 10 \). It was even shown in [21] that, for increasing dimension, nearly all functions are non normal. Asymptotically, there exist Boolean functions of \( n \) variables which are not affine on any \( \alpha \log_2(n) \)-dimensional affine subspace for every \( \alpha > 1 \) (see [12]). But the question if there exist non normal bent functions was an open problem.

The question of normality can be generalized to the following combinatorial problem. Given a set of bent functions \( \mathcal{B} \), determine the maximal dimension \( d(\mathcal{B}) \) such that for all functions \( f \in \mathcal{B} \) there exists an affine subspace \( U \) of dimension \( d(\mathcal{B}) \) such that \( f \) is constant on \( U \).

The following section investigates all known families of bent functions and their normality. We prove that most functions in the main classes of bent functions (the Maiorana-McFarland class, the Partial Spread class and the class \( \mathcal{N} \)) are normal. We also prove the normality of some modified Maiorana-McFarland bent functions. In Section 3.3 we present the first non normal bent function and even a non weakly-normal bent function. As normality is defined via the existence of a flat fulfilling certain criteria, it is very hard to check this property, both in theory and with an algorithm. In order to decide normality of Boolean functions, in Section 3.4 we sketch an algorithm which is much faster than a naive approach would be. Finally, Section 3.5 contains some further applications for this algorithm.

The main results of this chapter will be published in a Special issue on
Coding and Cryptography by Discrete Applied Mathematics [7]. See also [6, 16].

3.2 Normality of the known families of bent functions

3.2.1 Direct constructions

Amongst all known constructions for bent functions, there exist three families which can be directly constructed (i.e., which are not derived from other bent functions): the Maiorana-McFarland class, the Partial Spread class and the class $\mathcal{N}$ which was introduced by Dobbertin [21].

Maiorana-McFarland functions

Definition 3.1. Let $\pi: \mathbb{F}_2^k \rightarrow \mathbb{F}_2^k$ be a permutation and $h: \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ an arbitrary Boolean function. Then $f: \mathbb{F}_2^k \times \mathbb{F}_2^k \rightarrow \mathbb{F}_2$ with

$$f(x, y) = \langle x, \pi(y) \rangle + h(y)$$

is called a Maiorana-McFarland function. The set of all Maiorana-McFarland functions is denoted by $\mathcal{M}$.

All Maiorana-McFarland functions are bent. Moreover, they are obviously normal, since they are constant on the $k$-dimensional subspace $\mathbb{F}_2^k \times \{\pi^{-1}(0)\}$.

Partial spreads

The Partial spread family, denoted by $\mathcal{P}S$, was introduced by Dillon [17]. It is defined as follows.

Definition 3.2. Let $\{E_i, i = 1, 2 \ldots N\}$, with $N = 2^{k-1}$ or $N = 2^{k-1} + 1$, be a set of $N$ subspaces of $\mathbb{F}_2^{2k}$ of dimension $k$ such that $E_i \cap E_j = \{0\}$ for all $i \neq j$. The Boolean function $f$ of $2k$ variables defined by

$$\{x \in \mathbb{F}_2^{2k}, f(x) = 1\} = \bigcup_{i=1}^{N} E_i$$

is called a Partial Spread. Moreover, $f$ is said to be in the class $\mathcal{P}S^+$ if $N = 2^{k-1} + 1$ and in the class $\mathcal{P}S^-$ if $N = 2^{k-1}$.

Dillon proved that all partial spreads are bent [17]. By definition, any function in the class $\mathcal{P}S^+$ is normal since it takes the value 1 on all $k$-dimensional subspaces $E_i$. The situation is different for
3.2. NORMALITY OF THE KNOWN FAMILIES OF BENT FUNCTIONS

the functions in $\mathcal{P}S^-$: they are not constant on any $E_i$ since they vanish at 0. Determining whether there exist non normal and non weakly-normal functions in the class $\mathcal{P}S^-$ is still an open problem. However, this problem can be solved for a subclass of $\mathcal{P}S^-$, called $\mathcal{P}S_{ap}$, defined by Dillon [17, p. 97]. This subclass consists of all functions of the form

$$f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \rightarrow \mathbb{F}_2, \quad (x, y) \mapsto g(xy^{2^k-2})$$

where $g$ is any balanced function from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$ such that $g(0) = 0$.

It is clear that all functions in $\mathcal{P}S_{ap}$ are normal since they vanish on the $k$-dimensional subspace $\{0\} \times \mathbb{F}_{2^k}$.

**Class $\mathcal{N}$** A third family, called class $\mathcal{N}$, was exhibited by Dobbertin [21].

**Definition 3.3.** Let $g$ be a balanced function from $\mathbb{F}_{2^k}$ into $\mathbb{F}_2$ and let $T_g$ denote the affine subspace spanned by the support of its Walsh transform. Let $\psi$ be a mapping from $\mathbb{F}_{2^k}$ to itself and $\phi$ be a permutation of $\mathbb{F}_{2^k}$ such that both $\phi$ and $\psi$ are affine on all sets $aT$, $a \in \mathbb{F}_{2^k}^*$. The function $f$ defined by

$$\forall (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}, \quad f(x, \phi(y)) = \begin{cases} g\left(\frac{x + \psi(y)}{y}\right) & \text{if } y \neq 0 \\ 0 & \text{if } y = 0 \end{cases}$$

is said to be in class $\mathcal{N}$.

It is shown in [21] that all functions in $\mathcal{N}$ are bent. Moreover, family $\mathcal{N}$ contains both the Maiorana-McFarland class and the $\mathcal{P}S_{ap}$ class as extremal cases. It is obvious that any function in family $\mathcal{N}$ is normal because it vanishes on the $k$-dimensional space $\mathbb{F}_2^k \times \{\phi(0)\}$.

Since bentness is invariant under addition of an affine function and under right composition by an affine permutation, it is natural to consider the completions of the previous classes under these transformations. We denote by $\mathcal{B}$ the completed version of any class $\mathcal{B}$.

**Proposition 3.4.** All functions in $\mathcal{M} \cup \mathcal{P}S^+ \cup \mathcal{P}S_{ap} \cup \mathcal{N}$ and their duals are weakly-normal.

### 3.2.2 Modified Maiorana-McFarland Bent Functions

Now, we focus on some bent functions derived from the Maiorana-McFarland family by adding an indicator function of a flat $E$ and we prove their normality. In particular we are interested in functions described in [11] and below.
These functions are all of the following form:

\[ f : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2 \]

\[ f(x, y) = \langle x, \pi(y) \rangle + h(x) + \Phi_E(x, y) \]

where \( \pi : \mathbb{F}_2^k \to \mathbb{F}_2^k \) is a permutation, \( h : \mathbb{F}_2^k \to \mathbb{F}_2 \) is an arbitrary function and \( \Phi_E \) is the characteristic function of \( E \):

\[ \Phi_E(x, y) : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2, \]

\[ \Phi_E(x, y) = 1 \quad \text{if and only if} \quad (x, y) \in E. \]

For some of these functions we shall show that they are normal, or at least weakly-normal.

Carlet’s construction  
In [11] Carlet considers only the special situation, where \( E \) is of the form \( \tilde{E} \times \mathbb{F}_2^k \) for a subspace \( \tilde{E} \) of \( \mathbb{F}_2^k \). We denote the characteristic function \( \Phi_{\tilde{E} \times \mathbb{F}_2^k}(x, y) \) just by \( \phi_{\tilde{E}}(x) \) to simplify the notation.

The bent functions constructed in [11] are described in the following theorem.

**Theorem 3.5.** [11] Let \( E \) be any linear subspace of \( \mathbb{F}_2^k \), and \( \pi \) be a permutation on \( \mathbb{F}_2^k \) such that for any element \( \lambda \) of \( \mathbb{F}_2^k \), the set \( \pi^{-1}(\lambda + E^{\perp}) \) is a flat. Then the function

\[ f(x, y) = \langle x, \pi(y) \rangle + \phi_E(x) \]

is bent.

It is obvious that these functions are normal, because \( f \) restricted to \( \{0\} \times \mathbb{F}_2^k \) equals 1. Therefore, in order to find non normal bent functions one might consider a small appropriate generalization which also involves a function \( h \) as the general form of the Maiorana-McFarland-construction requires. It can be proven that this construction leads to bent functions in the same way as Carlet’s original result.

**Lemma 3.6.** Let \( E \) and \( \pi \) be as in Theorem 3.5, and \( h \) be a Boolean function on \( \mathbb{F}_2^k \), such that for any element \( \lambda \) of \( \mathbb{F}_2^k \), the function \( h \) is affine on \( \pi^{-1}(\lambda + E^{\perp}) \). Then

\[ f(x, y) = \langle x, \pi(y) \rangle + h(y) + \phi_E(x) \]

is bent.

The next lemma shows that all these functions are still normal bent functions.
3.2. NORMALITY OF THE KNOWN FAMILIES OF BENT FUNCTIONS

Lemma 3.7. All bent functions $f$ defined in Lemma 3.6 are normal.

Proof. We assume w.l.o.g that $\pi(0) = 0$ and $h(0) = 0$. We first consider the case that $h$ is not constant on $\pi^{-1}(E^\perp)$. Then, we find an element $y_0 \in \pi^{-1}(E^\perp)$, with $h(y_0) = 1$. Define the hyperplane

$$S = \{x \in \mathbb{F}_2^k : \langle x, \pi(y_0) \rangle = 1\},$$

then it is clear that $S \cap E = \emptyset$ since $\pi(y_0) \in E^\perp$. Therefore, the restriction of $f$ to the $k$-dimensional flat $$(S \times \{0\}) \cup (S \times \{y_0\})$$
is constant and equal to 0.

If $h$ is constant on the flat $\pi^{-1}(E^\perp)$ then $f(x, y)$ is constant and equal to $1 + h(y)$ on the $k$-dimensional flat $E \times \pi^{-1}(E^\perp)$.

Note that the first part of the above proof shows that actually every function derived from the Maiorana-McFarland family by adding an indicator function of the form $\Phi_{E \times \mathbb{F}_2^k}$ is weakly-normal.

Canteaut’s construction Another class of bent functions can be derived from the Maiorana-McFarland functions by adding the indicator function of a linear subspace $E$ of $\mathbb{F}_2^k \times \mathbb{F}_2^k$ with codimension 2. This construction is based on some properties of the derivatives of the dual function. Recall that the derivative of a Boolean function on $\mathbb{F}_2^n$, $f$, with respect to any direction $a \in \mathbb{F}_2^n$ is the Boolean function $D_af : x \mapsto f(x + a) + f(x)$.

Proposition 3.8. [8, Th. 8] Let $f$ be a bent function of $2k$ variables, $k \geq 2$. Let $a$ and $b$ be two distinct nonzero elements of $\mathbb{F}_2^{2k}$ and $E = \langle a, b \rangle^\perp$. Then, the function $f + \Phi_E$ is bent if and only if the dual function, $f^*$, satisfies $D_aD_bf^* = 0$.

Note that this result can also be deduced from [11, p. 94]. The previous proposition enables us to derive some new bent functions from the Maiorana-McFarland family. From now on, we use an explicit description of the scalar product via the trace mapping: $\mathbb{F}_2^k$ is identified with the finite field of order $2^k$, $\mathbb{F}_{2^k}$, and the linear functions are the mappings $y \mapsto \text{tr}(by)$ on $\mathbb{F}_{2^k}$, where $b$ describes $\mathbb{F}_{2^k}$ and $\text{tr}$ is the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$. The scalar product of two elements $x$ and $y$ then corresponds to $\text{tr}(xy)$. As an example, the following corollary exhibits a bent function obtained from the Maiorana-McFarland family by the construction described in Proposition 3.8.
Corollary 3.9. Let $k = gr$ where $g$ is odd and $r > 1$. Let

$$s = 1 + \sum_{i=0}^{\frac{g-1}{2}} (2^r - 1)2^{(2i+1)r}.$$ 

Let $\alpha, \beta$ and $\lambda$ be three nonzero elements in $\mathbb{F}_{2^k}$ such that $\alpha$ has order $(2^r - 1)$, $\text{tr}(\beta^2(\alpha^2 + \alpha)) = 0$ and $\text{tr}(\lambda(\alpha^2 + \alpha)) = 0$. Let $x, y \in \mathbb{F}_{2^k}$, then the $2k$-variable function

$$g(x, y) = \text{tr}(xy^s) + \text{tr}(\lambda y^{3s}) + \text{tr}(x + \beta y) \text{tr}(\alpha x + \alpha^{2^r-1} \beta y)$$

is bent and does not belong to the completed version of the Maiorana-McFarland family.

**Proof.** Let $f$ be the $2k$-variable bent function in the Maiorana-McFarland family defined by

$$f(x, y) = \text{tr}(xy^s) + \text{tr}(\lambda y^{3s}).$$

Let $a = (1, \beta)$, $b = (\alpha, 2^r-1 \beta)$ and $V = (a, b)$. From Prop. 3.8, we deduce that $g$ is bent if and only if $D_a D_b f^* = 0$. Let $x \mapsto x^d$ be the inverse of $x \mapsto x^s$ over $\mathbb{F}_{2^k}$, i.e. $d = 2^{k-1} + 2^{r-1}$. The dual $f^*$ of $f$ is given by [17, p. 91]:

$$f^*(x, y) = \text{tr}(x^d y) + \text{tr}(\lambda (x^d)^{3s}) = \text{tr}(x^d y) + T \text{r}(\lambda x^3).$$

We obtain after some calculations that, for this choice of $\alpha, \beta$ and $\lambda$, $D_a D_b f^* = 0$, implying that $g$ is bent.

Now, $g$ belongs to $\overline{M}$ if and only if there exists a $k$-dimensional subspace $U \subset \mathbb{F}_{2^k}^2$ such that $D_u D_v g = 0$ for any $u, v \in U$ [17, page 102]. We can prove that $U = \mathbb{F}_{2^k} \times \{0\}$ does not satisfy this condition. Thus, if $g$ belongs to $\overline{M}$, there exist two nonzero distinct elements $u, v \in \mathbb{F}_{2^k}^2$ with $u \not\in \mathbb{F}_{2^k} \times \{0\}$ such that $D_u D_v g = D_u D_v f + D_u D_v \Phi_V = 0$. This implies that $D_u D_v f$ is constant on $\mathbb{F}_{2^k}^2$. By computing $D_u D_v f$, we deduce that the function $D_u D_v f$ is constant only if there exist $\mu, \nu \in \mathbb{F}_{2^k}^2$, $\mu \neq \nu$, such that

$$(x + \mu + \nu)^s + (x + \mu)^s + (x + \nu)^s + x^s = 0, \text{ } \forall x \in \mathbb{F}_{2^k},$$

or if there exist $\mu, \nu \in \mathbb{F}_{2^k}^2$ such that

$$x \mapsto \text{tr}(\mu((x + \nu)^s + x^s))$$

is constant on $\mathbb{F}_{2^k}$. Using the expression for $s$, we can then prove that none of these conditions is satisfied (see e.g. [8, Corollary 6]).

However, we can prove that any function derived from the Maiorana-McFarland family by adding the indicator function of a linear subspace of codimension 2, as described in Proposition 3.8, is normal.
3.2. NORMALITY OF THE KNOWN FAMILIES OF BENT FUNCTIONS

Lemma 3.10. Let $\pi$ be a permutation on $\mathbb{F}_2^k$ and $\xi_i$ be arbitrary Boolean functions on $\mathbb{F}_2^k$. For any nonzero $\alpha$ and $\beta$ in $\mathbb{F}_2^k$, $\alpha \neq \beta$, the function
\[
g(x, y) = \text{tr}(x\pi(y)) + \text{tr}(\alpha x)\text{tr}(\beta x) + \xi_1(y)\text{tr}(\alpha x) + \xi_2(y)\text{tr}(\beta x) + \xi_3(y)
\]
is normal.

Proof. Let
\[
E = \{ x \in \mathbb{F}_2^k : \text{tr}(x) = \text{tr}(\alpha x) = 0 \} = \langle 1, \alpha \rangle^\perp.
\]
The function $g$ restricted to $y \in \pi^{-1}(E^\perp)$ can be represented as
\[
g(x, y)|_{\mathbb{F}_2^k \times \pi^{-1}(E^\perp)} = \text{tr}(\alpha x)\text{tr}(\beta x) + \xi_1(y)\text{tr}(\alpha x) + \xi_2(y)\text{tr}(\beta x) + \xi_3(y)
\]
by changing the functions $\xi_i$ appropriately.

For a fixed $y \in \pi^{-1}(E^\perp)$ we denote $g_y(x) := g(x, y)$. The support of $g_y$ is either a coset of $E$ or the complement of a coset of $E$. We have
\[
E^\perp = \{ 0, \alpha, \beta, \alpha + \beta \}.
\]
Thus, there are four possibilities to choose $y$. At least for two different values $y_0$ and $y_1$ the supports of $g_{y_0}$ and of $g_{y_1}$ have the same size. W.l.o.g we assume that the size of the support of $g_{y_0}$ and $g_{y_1}$ is $\#E$. Now, it follows that $g_{y_0}(x) = g_{y_1}(x) = 0$ for $x$ in the affine hyperplane $(c_0 + E) \cup (c_1 + E)$, where the $c_i + E$, $i = 0, 1$ are different cosets of $E$. Hence $g$ is constant on the $k$-dimensional flat
\[
\{(c_0 + E) \cup (c_1 + E)\} \times \{ y_0, y_1 \}.
\]

\[\square\]

Theorem 3.11. Let $\pi$ be a permutation of $\mathbb{F}_2^k$ and $h$ be an arbitrary Boolean function on $\mathbb{F}_2^k$. Let $E$ be a linear subspace of $\mathbb{F}_2^k \times \mathbb{F}_2^k$ of codimension 2 such that
\[
f(x, y) = \text{tr}(x\pi(y)) + h(y) + \Phi_E(x, y)
\]
is bent. Then $f$ is normal.

Proof. Let $E = \langle (\alpha_1, \alpha_2), (\beta_1, \beta_2) \rangle^\perp$. If $\dim(\alpha_1, \beta_1) < 2$, then $f$ belongs to the Maiorana-McFarland class, implying that it is normal. Actually, a bent function $f$ of $2k$ variables belongs to $\overline{M}$ if and only if there exists a $k$-dimensional subspace $V \subset \mathbb{F}_2^{2k}$ such that $D_aD_bf = 0$ for any $(a, b) \in V$ [17, page 102]. Here, we obviously have that $D_aD_bf = 0$ for any $a, b \in \mathbb{F}_2^k \times \{0\}$.

Now, if $\alpha_1$ and $\beta_1$ are two nonzero distinct elements of $\mathbb{F}_2^k$, $f$ corresponds to the sum of $\text{tr}(x\pi(y)) + \text{tr}(\alpha_1 x)\text{tr}(\beta_1 x) + \xi_1(y)\text{tr}(\alpha_1 x) + \xi_2(y)\text{tr}(\beta_1 x) + \xi_3(y)$ and a linear mapping. From the previous lemma, we deduce that $f$ is normal. \[\square\]
CHAPTER 3. NORMAL AND NON-NORMAL BENT FUNCTIONS

3.3 Non Normal Bent Functions

Here, we exhibit some examples of non normal and even non weakly-normal bent functions. One set of functions that turns out to include non normal functions is the class of Kasami functions. This class of bent functions was found by Dobbertin and Dillon in [20] and some of the functions in this class seemed to be good candidates for non normal bent functions.

The Dillon-Dobbertin functions are defined as follows (see also Chapter 5):

Definition 3.12. Let $d = 2^r - 2^r + 1$ with $\gcd(r, n) = 1$ and $\alpha \in \mathbb{F}_{2^n}$. Then, we call $f_{\alpha,r} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ with $f_{\alpha,r}(x) = \text{tr}(\alpha x^d)$ a Dillon-Dobbertin function.

Under some conditions these functions are bent.

Theorem 3.13. [20] Let $r$ and $f_{\alpha,r}$ be as in Definition 3.12. If $n$ is not divisible by 3 and $\alpha \notin \{x^3 | x \in \mathbb{F}_{2^n}\}$ then $f_{\alpha,r}$ is bent.

For some values of $n$ it is possible to show that the Dillon-Dobbertin functions are always normal.

Lemma 3.14. Let $n = 2k$ with $k$ even. The Dillon-Dobbertin power functions

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$$

$$x \mapsto \text{tr}(\alpha x^d)$$

are normal.

Proof. First note that $\gcd(d, 2^n - 1) = 3$, i.e.,

$$U = \{x^d | x \in \mathbb{F}_{2^n}^*\} = \{x^3 | x \in \mathbb{F}_{2^n}\}$$

and there exist $\lambda_1, \lambda_2 \notin U$ such that

$$\mathbb{F}_{2^n}^* = U \cup \lambda_1 U \cup \lambda_2 U.$$ 

In the case where $4|n$, we will show that $\lambda_1, \lambda_2$ can be chosen in $\mathbb{F}_{2^k}$. It is sufficient to show that there exists $x \in \mathbb{F}_{2^k}$ such that $x \notin U$. Let $g$ be a generator of $\mathbb{F}_{2^k}$. $g$ is in $U$ if and only if $g^{2^k - 1} = 1$. But

$$g^{2^{n-1}} = g^{(2^k - 1)(2^k + 1)}$$

$$= g^{2^k + 1} 2^{k-1}$$

as $2^k + 1$ is not divisible by 3 if $k$ is even. So we can choose $\lambda_1 = g$ and $\lambda_2 = g^2$. Note that if $\alpha' = \alpha c^d$ for some $c \in \mathbb{F}_{2^n}^*$ then $f_{\alpha,r(cx)} = f_{\alpha',r}(x)$ for
all $x \in \mathbb{F}_{2^n}$. Thus, we can assume that $\alpha$ is in $\{1, g, g^2\} \subset \mathbb{F}_{2^k}$. So for $x \in \mathbb{F}_{2^k}$ we get

$$f_{\alpha,k}(x) = \text{tr}(\alpha x^d)$$

$$= \text{tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(\text{tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(\alpha x^d))$$

$$= \text{tr}_{\mathbb{F}_{2^k}/\mathbb{F}_2}(\alpha x^d \text{tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(1))$$

$$= 0.$$

This proves the lemma.

So we can only hope to get non normal Dillon-Dobbertin functions for $k$ odd. Furthermore, as all quadratic bent functions are normal, only the case $r \neq 1$ is interesting. As it is known that all bent functions on $\mathbb{F}_9^5$ are normal, the first possibility for a Dillon-Dobbertin function to be non normal is $n = 10$.

We found out that for $n = 10$ all the Dillon-Dobbertin functions are normal but by addition of a linear function they can be modified into non normal functions.

**Fact 3.15.** Let $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2 \subset \mathbb{F}_{2^{10}}$. Then there exists $\beta \in \mathbb{F}_{2^{10}}$ such that the function $f : \mathbb{F}_{2^{10}} \rightarrow \mathbb{F}_2$ with

$$f(x) = \text{tr}(\alpha x^{57} + \beta x)$$

is non normal.

**Verification** This can be verified using the algorithm described in Section 3.4.

Furthermore, we found that for $n = 14$ and $r = 3$ the corresponding Dillon-Dobbertin functions are non weakly-normal.

**Fact 3.16.** Let $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2 \subset \mathbb{F}_{2^{14}}$. The function $f : \mathbb{F}_{2^{14}} \rightarrow \mathbb{F}_2$ with

$$f(x) = \text{tr}(\alpha x^{57})$$

is non weakly-normal.

**Verification** By using the algorithm described in Section 3.4.

These results are verified with a computer algorithm, proving these results theoretically is still an open problem. We state the following conjecture.

**Conjecture 3.17.** All non quadratic Dillon-Dobbertin functions on $\mathbb{F}_{2^{2k}}$ with $k$ odd and $k \geq 7$ are non weakly-norkal.
Corollary 3.18. The Dillon-Dobbertin bent function $f : \mathbb{F}_{2^{14}} \rightarrow \mathbb{F}_2$ defined by

$$f(x) = \text{tr}(\alpha x^{57})$$

with $\alpha \in \mathbb{F}_4 \setminus \mathbb{F}_2 \subset \mathbb{F}_{2^{14}}$ and its dual do not belong to $\overline{M} \cup \overline{PSS} \cup \overline{N}$.

**Proof.** We know from Proposition 3.4 that all functions in $\overline{M} \cup \overline{PSS} \cup \overline{N}$ are weakly-normal. Thus, the only remaining case is family $\overline{PSS}$. But, any function in $\overline{PSS}$ of $2k$ variables has degree $k$ since its restrictions to some $k$-dimensional subspaces have an odd weight. It follows that $f$ does not belong to the completed class $\overline{PSS}$ because its algebraic degree is equal to 4. The same argument is valid for the dual function since the dual of a bent function of $2k$ variables of degree $k$ has degree $k$ [17, p. 80].

Next we show how to construct non weakly-normal bent functions of $n$ variables for all even $n \geq 14$. The following lemma is a generalization of Theorem 4.5 of [26]. As a more general result will be presented in the next chapter, we skip the proof of this lemma.

**Lemma 3.19.** Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a Boolean function. The following properties are equivalent:

1. $f$ is (weakly) normal
2. The function $g : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 \rightarrow \mathbb{F}_2$

$$(x, y, z) \mapsto f(x) + yz$$

is (weakly) normal

Thus, given a non normal function $f$ with $n$ variables Lemma 3.19 can be used to construct a non normal function with $n + 2$ variables.

According to this procedure applied recursively, if $f$ is a Boolean function on $\mathbb{F}_2^n$ and if $f'$ is a quadratic bent function on $\mathbb{F}_2^r$, then $f$ is (weakly) normal if and only if $g(x, y) = f(x) + f'(y)$ is (weakly) normal. An important observation from our point of view is that, if the function $f$ in the above lemma is bent, then $g$ is also bent.

With Fact 3.15 and Fact 3.16 we get:

**Fact 3.20.** There exist non normal bent functions of $n$ variables for all even $n \geq 10$ and non weakly-normal bent functions for all even $n \geq 14$.

From Corollary 3.18, we deduce that for any even $n \geq 14$, the bent functions of $n$ variables obtained by recursively applying Lemma 3.19 to the Dillon-Dobbertin function of 14 variables (and their duals) do not belong to $\overline{M} \cup \overline{PSS} \cup \overline{N}$. 


3.4 An Algorithm for Checking Normality

The main idea of the algorithm presented here is to make use of the fact, that a Boolean function which is affine on a flat $A$ is also affine on all flats contained in $A$.

Moreover, the function is either constant on $A$ and hence constant on all flats contained in $A$, or we can find two flats $A_0, A_1 \subset A$ with $\dim(A_0) = \dim(A_1) = \dim(A) - 1$ and $A = A_0 \cup A_1$ such that the function is 0 on $A_0$ and 1 on $A_1$. In the latter case, of course, the function is also constant on all flats of $A_0$ and $A_1$ respectively.

Hence, it suffices for a given Boolean function, first to determine the flats of a "small" dimension $t_0$ on which the function is constant and then to combine these spaces to get those flats of dimension $k$ on which the function is affine.

Therefore, the general structure of the algorithm can be described as follows:

**Algorithm 3.21.**

**Input:** a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, a starting dimension $t_0$

**Output:** a list of all flats of dimension $k$ on which $f$ is affine

For all subspaces $U$ of $\mathbb{F}_2^n$ with $\dim(U) = t_0$ do

- Determine all flats $a + U$ with $f|_{a+U} = 0$ and $f|_{a+U} = 1$ resp.
- Combine pairs $(a_1 + U, a_2 + U)$ with $f|_{a_1+U} = f|_{a_2+U} = 0$ (resp. with $f|_{a_1+U} = f|_{a_2+U} = 1$) to get flats $a_1 + \hat{U} = a_1 + \langle U, a_1 + a_2 \rangle$ of dimension $t_0 + 1$ such that $f|_{a_1+\hat{U}} = 0$ (resp. $f|_{a_1+\hat{U}} = 1$)

Repeat the last step for new flats with equal $\hat{U}$ up to dimension $k - 1$

Combine pairs of flats $(a_1 + \hat{U}, a_2 + \hat{U})$ with $\dim(\hat{U}) = k - 1$

(independent of whether $f|_{a_1+\hat{U}}$ is 0 or 1)

to get those flats of dimension $k$ on which $f$ is affine

Output these flats of dimension $k$

More details and improvements can be found in [16]. A randomized version of this algorithm was presented in [3].

3.5 Further Applications of the Algorithm

Besides the application of checking (weak) normality, which is quite straightforward with the above described algorithm, there are some other applications for this algorithm.
CHAPTER 3. NORMAL AND NON-NORMAL BENT FUNCTIONS

3.5.1 Maiorana-McFarland Functions

The second application of the algorithm we want to describe here is the problem to decide whether a given bent function is a Maiorana-McFarland bent function. Recall that we denote the class of all functions which are equivalent to a Maiorana-McFarland function under affine transformations by $\mathcal{M}$.

Due to the following lemma it is possible to use the above described algorithm to determine whether a function is in $\mathcal{M}$ or not.

Lemma 3.22.
Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function. The following properties are equivalent:

i) $f$ is in $\mathcal{M}$.

ii) There exists a subspace $U$ of dimension $k$ such that the function $f$ is affine on every coset of $U$.

The proof of this Lemma is obvious since the second property is invariant under addition of an affine function and under right composition by an affine permutation. As the algorithm described in this paper outputs every coset of dimension $k$ on which $f$ is affine, this property can be checked easily.

In practice this means that for $n = 8$ we can decide whether a bent function is in $\mathcal{M}$ in less than a second, for $n = 10$ in less than a minute and even for $n = 14$ in a few days.

The possibility to determine if a given function is in $\mathcal{M}$ can be used to compute an experimental bound on the number of bent functions for $n = 8$. Note that $n = 8$ is the first dimension where the number of bent functions is not known. An lower bound on the number of bent functions can be obtained by considering the number of Maiorana-McFarland bent functions, an upper bound can be derived by the number of Boolean functions of degree at most $k$. The following table can be found in [37].

<table>
<thead>
<tr>
<th>Number of Bent Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$n$</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>8</td>
</tr>
</tbody>
</table>
3.5. **FURTHER APPLICATIONS OF THE ALGORITHM**

By generating "random" bent functions and checking whether they are in $\mathcal{M}$ as previously described, the ratio $q$ of the number of bent functions in $\mathcal{M}$ to the number of all bent functions can be estimated. Then, if $\mu_n$ is the number of functions in $\mathcal{M}$ in $n$ variables, the number of all bent functions can be estimated as $\frac{1}{n} \mu_n$.

But we are unable to estimate this number until we have solved the following two problems.

First the number $\mu_8$ of functions in $\mathcal{M}$ for $n = 8$ is not known exactly. The functions in $\mathcal{M}$ are all affine equivalent to $\langle x, \pi(y) \rangle + h(y)$, where $\pi$ is a permutation and $h$ an arbitrary Boolean function. The number of functions of this form is $2^2 (2^k!)$.

The problem is to determine the length of the orbit under the action of the group $AL(n)$ of all affine transformations. This length is equal to $\#AL(n)$ if and only if there are no $A \in AL(n)$ such that $f \circ A = f$. We computed the length of the orbit for randomly chosen functions in $\mathcal{M}$ and all of them had orbit length $\#AL(n)$, but it would be much more satisfying to have a theoretical result, so it remains an open problem to determine $\#\mathcal{M}$ for $n \geq 8$.

The second problem is that the generation of bent functions for $n = 8$ usually uses hill-climbing algorithms and these algorithms might find functions in $\mathcal{M}$ more or less often than they should.

### 3.5.2 Other Classes of Bent Functions

For some other classes of bent function it is also possible to use the algorithm presented in Section 3.4 to decide if a given bent function is in a specific class of bent functions. Examples are the classes $PS^+$ and $PS^-$ introduced in [17]. As the support of bent functions in these classes is defined via the union of subspaces of dimension $n/2$, the algorithm can be used easily to check if a function belongs to one of these classes.
Chapter 4

Normal Extensions of Bent Functions

4.1 Introduction

As we saw in the last chapter, taking any non-normal (resp. not weakly normal) bent function \( f \) we can produce an infinite series of non-normal, resp. not weakly normal, bent functions: for any not (weakly) normal bent functions \( f \), the bent function

\[
f \oplus B_m
\]

is again not (weakly) normal, where \( \oplus \) is the sum of functions with disjoint sets of variables (called direct sum), and where the normal bent functions \( B_m \), \( m \) even, are defined as

\[
B_m(x_1, x_2, \ldots, x_{m-1}, x_m) = x_1x_2 + \ldots + x_{m-1}x_m = \langle (x_1, x_3, \ldots, x_{m-1}), (x_2, x_4, \ldots, x_m) \rangle
\]

and represent the simplest type of bent functions.

S. Gangopadhyay, S. Maitra [31] and C. Carlet conjectured that, much more general, the direct sum of a non-normal bent function with any normal one is non-normal (the same statement for weak normality can easily be reduced to the latter.)

In this chapter, we introduce the notion of a normal extension of bent functions, which allows us to characterize when the direct sum of two bent functions is normal. The notion of a normal extension turns out to be a generalization of the direct sum of a normal and a non-normal bent function. We then demonstrate that, in a normal extension of bent functions,
normality inherits downwards. This includes the confirmation of the above mentioned conjecture as a special case, i.e., we in fact have the rule: “non-normal $\oplus$ normal = non-normal” for bent functions. The main theorem is more general and we present some constructions of normal extensions, that are not equivalent to a direct sum.

Throughout this section, the capital letters $V$, $W$ and $U$, possibly with an index, stand for finite-dimensional vector spaces over $\mathbb{F}_2$, the two-element field, endowed with a scalar product. The dimension of $V$ is always denoted by $n$. Concretely we can assume $V = \mathbb{F}_2^n$ and $\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$.

We say that $V$ is a direct sum of $V_1$ and $V_2$, and we write $V = V_1 \oplus V_2$, if $V_1, V_2 \subseteq V$ are subspaces of $V$ such that each $x \in V$ can be uniquely represented as $x = x_1 + x_2$, where $x_i \in V_i$ ($i = 1, 2$), or equivalently

$$
V_1 + V_2 = V,
$$
$$
V_1 \cap V_2 = \{0\}.
$$

On the other hand, given $\mathbb{F}_2$-vector spaces $V_1$ and $V_2$, which we consider as disjoint, $V_1 \oplus V_2$, their direct sum, is well-defined. In fact, we can construct $V_1 \oplus V_2$ as the cartesian product $V_1 \times V_2$ with coordinate-wise operations if we identify $V_1$ with $V_1 \times \{0\}$ and $V_2$ with $\{0\} \times V_2$:

$$
V_1 \oplus V_2 = V_1 \times V_2
$$

In the sequel we shall apply the notion of isomorphic Boolean functions. Two Boolean functions $f_i : V_i \rightarrow \mathbb{F}_2$ ($i = 1, 2$) are called isomorphic if there is a one-to-one $\mathbb{F}_2$-linear mapping (i.e. a vector space isomorphism) $\phi$ from $V_1$ onto $V_2$ with

$$
f_1(x) = f_2(\phi(x))
$$

for all $x \in V_1$. We say that $f_1$ and $f_2$ are complementary-isomorphic if the complement $f_1 + 1$ of $f_1$ is isomorphic to $f_2$.

Convention For the sake of formal simplicity, we shall in the remainder of this chapter use the notion normal in the sense that a Boolean function $f$ with $n$ variables is constant on a subspace $N$ with $\dim N = n/2$, called a normality subspace of $f$. This is no essential restriction, since we are concerned with bent functions, and the property bent is invariant under composition with translations.

The main results of this chapter will be published in [14].
4.2 Normal Extensions and Normality of Direct Sums

In the following definition we introduce our main concept, the notion of a normal extension for bent functions.

**Definition 4.1.** Suppose $U \subseteq V$, let $\beta : U \to \mathbb{F}_2$ and $f : V \to \mathbb{F}_2$ be bent functions. Then we say that $f$ is a normal extension of $\beta$, in symbols $\beta \preceq f$ if there is a direct decomposition $V = U \oplus W_1 \oplus W_2$ such that

(i) $\beta(u) = f(u + w_1)$ for all $u \in U, w_1 \in W_1$,  
(ii) $\dim W_1 = \dim W_2$.

Note that condition (i) can also be written as $f|_{U \oplus W_1} = \beta \oplus 0$, here 0 denoting the 0-function on $W_1$. Thus the restriction of $f$ on $U \oplus W_1$ is a “blown-up” bent function.

As we shall see later (Theorem 4.11), we can replace $\beta$ by any other bent function $\beta'$ on $U$ and get again a normal extension.

**Proposition 4.2.** Given an arbitrary bent function $f$, the set

$$\mathcal{N}_f = \{ \beta : \beta \preceq f, \beta \text{ bent} \},$$

is partially ordered by the relation $\preceq$, where $f \in \mathcal{N}_f$ is the greatest element.

In fact it is obvious that $\preceq$ is reflexive, transitive, and anti-symmetric:

(1). $f \preceq f$,
(2). if $f \preceq g$ and $g \preceq h$ then $f \preceq h$,
(3). if $f \preceq g$ and $g \preceq f$ then $f = g$,

for all bent functions $f, g, h$.

We mention that a bent function $f$ is normal if and only if $\varepsilon \preceq f$, where $\varepsilon \in \mathbb{F}_2$ (more precisely, $\varepsilon$ is a mapping from $\mathbb{F}_2^0$ to $\mathbb{F}_2$; but in order to simplify the notation, it is common practice to identify the mappings from the one-element set $\mathbb{F}_2^0$ to a set $A$ with the elements of $A$).
It is easy to see that, if $\beta$ is normal and $f$ is a normal extension of $\beta$, then $f$ is also normal (the relation $\preceq$ is transitive, thus $\varepsilon \preceq \beta \preceq f$ implies $\varepsilon \preceq f$). One of our main results is that vice versa, normality also inherits downwards, see Theorem 4.12.

Obviously, we get a normal extension of any $\beta$ by taking any normal bent function $g$ and setting $f = \beta \oplus g$:

$$\beta \preceq \beta \oplus g$$

for normal $g$.

We shall see in the next section that there are much more normal extensions than direct sums.

It is trivial that normality inherits to direct sums.

**Proposition 4.3.** The direct sum of normal bent functions is normal.

Conversely, the normality of the direct sum of bent functions does not imply that these functions are normal, since

$$\beta \oplus (\beta + \varepsilon), \quad \varepsilon \in \mathbb{F}_2,$$

is normal for any bent function $\beta$. More generally

$$(\beta \oplus g_1) \oplus ((\beta + \varepsilon) \oplus g_2)$$

is normal, where $g_1$ and $g_2$ are normal bent functions. If we replace the direct sums $\beta \oplus g_1$ and $(\beta + \varepsilon) \oplus g_2$ by arbitrary normal extensions of $\beta$ and $\beta + \varepsilon$, respectively, then we already come to the general situation, where a direct sum of bent functions is normal:

**Theorem 4.4.** Let $f_i : V_i \rightarrow \mathbb{F}_2, i = 1, 2$, be bent functions. The direct sum $f_1 \oplus f_2$ is normal if and only if isomorphic or complementary-isomorphic bent functions $\beta_1$ and $\beta_2$ exist such that $f_i$ is a normal extension of $\beta_i$ ($i = 1, 2$).

**Proof.** “$\Rightarrow$”:

Set $n_i = \dim V_i$ ($i = 1, 2$). Suppose $V_1 \oplus V_2 = V_1 \times V_2$ and

$$h(x_1, x_2) = (f_1 \oplus f_2)(x_1, x_2) = f_1(x_1) + f_2(x_2).$$

According to the normality of $h$, there is a subspace $N$ of $V_1 \times V_2$ of dimension $n_1 + n_2$ such that $h$ is constant on $N$. Assume without loss of generality

$$h(x_1, x_2) = 0,$$

i.e. $f_1(x_1) = f_2(x_2)$

for all $(x_1, x_2) \in N$. Define subspaces $W_1, N_1 \subseteq V_1$ associated to $N$ as follows

$$N_1 = \{ x \in V_1 \mid (x, x') \in N \text{ for some } x' \in V_2 \}$$

$$W_1 = \{ x \in V_1 \mid (x, 0) \in N \} ,$$

where $f_1(x_1) = f_2(x_2)$, $f_1(x_1) \in V_1$, and $(x_1, x_2) \in N$.
and similarly $W_2, N_2 \subseteq V_2$. Choose direct complements $U_i$ of $W_i$ in $N_i$:

$$N_i = U_i \oplus W_i.$$ 

Now we set

$$\beta_i = f_i|_{U_i}.$$ 

We have to show that these $\beta_i$ are isomorphic bent functions and $\beta_i \leq f_i$.

**Claim 1** $f_i$ is constant on any coset of $W_i$ in $N_i$.

**Proof.** Suppose $x, y \in N_1, x + y \in W_1$, then $(x + y, 0) \in N$ and $(x, x_2) \in N$ for some $x_2 \in V_2$. Thus $(y, x_2) \in N$ and therefore

$$f_1(x) = f_2(x_2) = f_1(y).$$

**Claim 2** $N \cap (U_1 \times U_2) = \varnothing$ is an isomorphism between $U_1$ and $U_2$.

**Proof.** Let $u_1 \in U_1$, then $(u_1, y) \in N$ for some $y \in N_2$. Since $N_2 = U_2 \oplus W_2$ we can decompose $y = u_2 + w$ with $u_2 \in U_2, w \in W_2$. Hence $(0, w) \in N$ and $(u_1, u_2) \in N \cap (U_1 \times U_2)$. Actually $u_2$ is unique. In fact, if $(u_1, u_2), (u_1, u'_2) \in N \cap (U_1 \times U_2)$, then $(0, u_2 + u'_2) \in N$ and $u_2 + u'_2 \in U_2 \cap W_2 = 0$, i.e. $u_2 = u'_2$. This shows that $\varphi$ is a bijective mapping. Moreover $\varphi$ is $F_2$-linear, since, considered as a subset of $U_1 \times U_2$, it is closed under addition.

**Claim 3** $\beta_1(x) = \beta_2(\varphi(x))$ for all $x \in U_1$.

**Proof.** This follows from $(x, \varphi(x)) \in N$, i.e.

$$h(x, \varphi(x)) = f_1(x) + f_2(\varphi(x)) = 0$$

for all $x \in U_1$, because $\beta_i$ is defined as the restriction of $f_i$ to $U_i$.

**Claim 4** $\beta_i$ is a bent function $(i = 1, 2)$.

**Proof.** We shall show that for each non-zero $a \in U_1$:

$$\sum_{x \in U_1} (-1)^{\beta_i(x+a)+\beta_i(x)} = 0.$$ 

This will prove Claim 4 by Proposition 2.1. From Lemma 2.4 we know that

$$\sum_{(x_1, x_2) \in N} (-1)^{h((a,0)+(x_1, x_2))} = 0,$$
since \((a, 0) \notin N\). On the other hand, as easy to see,

\[
N = M \oplus (W_1 \times W_2)
\]

for \(M = \varphi = \{(x, \varphi(x)) \mid x \in U_1\}\). We conclude, using Claims 1 and 3:

\[
\sum_{(x_1, x_2) \in N} (-1)^{h((a, 0) + (x_1, x_2))}
\]

\[
= \sum_{(x_1, x_2) \in N} (-1)^{h(x_1 + a, x_2)}
\]

\[
= \sum_{x_1 \in U_1} \sum_{w_1 \in W_1} \sum_{w_2 \in W_2} (-1)^{h(x_1 + w_1 + a, x_1 + w_2)}
\]

\[
= \#(W_1 \times W_2) \left( \sum_{x \in U_1} (-1)^{f_1(x + a) + f_2(\varphi(x))} \right)
\]

\[
= \#(W_1 \times W_2) \left( \sum_{x \in U_1} (-1)^{\beta_1(x + a) + \beta_1(x)} \right),
\]

thus proving Claim 4. \(\square\)

It remains to show that \(\dim V_i - \dim N_i = \dim W_i\). We abbreviate

\[
n_i = \dim V_i,
\]

\[
r_i = \dim W_i
\]

\[
m = \dim U_i
\]

\[
r_i' = \dim V_i - \dim N_i = n_i - (r_i + m).
\]

From the preceding proof we know that

\[
\dim N = m + r_1 + r_2.
\]

On the other hand

\[
\dim N = \frac{1}{2}(n_1 + n_2).
\]

Thus \(n_1 + n_2 = 2(m + r_1 + r_2)\), i.e.

\[
(r_i' - r_1) + (r_2' - r_2) = 0 \quad (4.1)
\]
4.3. EXAMPLES OF NORMAL EXTENSIONS

We have $f_i|_{N_i} = \beta \oplus 0$, where $0$ denotes the 0-function on $W_i$, and therefore $\text{Lin}(\beta \oplus 0) = 2^{\frac{r_i}{2}} \times 2^{r_i}$, since $\beta$ is bent. By Lemma 2.6,

$$\text{Lin}(f_i) = 2^{(m + r_i + r'_i)/2} \geq 2^{m/2 + r_i},$$

that is $r'_i - r_i \geq 0$. Together with (4.1) this proves $r_i = r'_i$ as desired.

The preceding construction of the $\beta_i$ from $N$ can be inverted, as we shall see in the sequel.

"⇐":

Conversely assume that $\beta_i \preceq f_i$ with isomorphic or complementary-isomorphic $\beta_1$ and $\beta_2$. Without loss of generality, we can assume that $\beta_1$ and $\beta_2$ are defined on $U$ and that $\beta_1 = \beta_2 + \varepsilon$ with $\varepsilon \in F_2$. Accordingly, let $V_i = U \times W_i \times W_i$ such that

$$f_i(u, w, 0) = \beta_i(u) \text{ for all } u \in U, w \in W_i.$$

Hence, $h = f_1 \oplus f_2$ is constant $\varepsilon$ on the subspace $N$ of $V = V_1 \times V_2$ defined as

$$N = \{(u, w_1, 0, u, w_2, 0) \mid w_i \in W_i, u \in U\},$$

since

$$h(u, w_1, 0, u, w_2, 0) = f_1(u, w_1, 0) + f_2(u, w_2, 0) = \beta_1(u) + \beta_2(u) = \varepsilon.$$

Finally note that we have $\dim N = r_1 + r_2 + \dim U = \frac{1}{2} \dim V$. \qed

4.3 Examples of Normal Extensions

In this section we will describe explicit constructions of normal extensions of bent functions. Accordingly, let $\beta : U \rightarrow F_2$ and $f : V = U \times W \times W \rightarrow F_2$ be Boolean functions; let $r = \dim W$ and $m = \dim U$. By Definition 4.1, $\beta \preceq f$ means that

$$f(x, y, 0) = \beta(x)$$

for all $x \in U$, $y \in W$.

**Proposition 4.5.** Assume that $r = 1$, i.e., $W = F_2$. Given bent functions $\beta$ and $g$ on $U$, we have $\beta \preceq f$ for $f$ defined on $U \times W \times W$ by setting for all...
\( x \in U: \)

\[
\begin{align*}
  f(x,0,0) &= \beta(x), \\
  f(x,1,0) &= \beta(x), \\
  f(x,0,1) &= g(x), \\
  f(x,1,1) &= g(x) + 1.
\end{align*}
\]

Moreover, \( f \) is a bent function.

Conversely in case \( r = 1 \), \( \beta \preceq f \) occurs for bent functions if and only if, up to equivalence, \( f \) is of this form.

In the preceding proposition we get a direct sum if and only if \( g = \beta \) or \( g = \beta + 1 \).

Proposition 4.5 is a special case of the following general setting, see [9].

**Theorem 4.6.** Let \( h : \mathbb{F}_2^n \times \mathbb{F}_2^m \rightarrow \mathbb{F}_2 \) be a Boolean function such that, for every \( z \in \mathbb{F}_2^m \), the function on \( \mathbb{F}_2^n \):

\[ h_z : x \rightarrow h(x,z) \]

is bent. Then \( h \) is bent if and only if the function

\[ \varphi_a : z \rightarrow h^*_a(z) \]

is bent for every \( a \in \mathbb{F}_2^n \). And the dual of \( h \) is \( h^*(a,b) = \varphi_a^*(b) \).

If for every \( z \in \mathbb{F}_2^m \), there exists a \( \beta_z \preceq h_z \) with the same decomposition \( \mathbb{F}_2^n = U \times W_1 \times W_2 \), then \( \beta \preceq h \), with the decomposition \( \mathbb{F}_2^{n+m} = (U \times \mathbb{F}_2^n) \times W_1 \times W_2 \) where

\[ \beta : U \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \]

is defined by

\[ \beta(u,z) = \beta_z(u). \]

However this Proposition is not constructive. We shall give two special constructive cases of normal extensions of bent functions. The first one is the following proposition, which can be easily verified (see also [10]):

**Proposition 4.7.** Let \( f_1, f_2 : U \rightarrow \mathbb{F}_2 \) and \( g_1, g_2 : U' \rightarrow \mathbb{F}_2 \) be bent functions, then

\[ h : U \times U' \rightarrow \mathbb{F}_2 \]

with

\[ h(x,z) = f_1(x) + g_1(z) + (f_1(x) + f_2(x))(g_1(z) + g_2(z)) \]

is bent, and the dual of \( h \) is given by

\[ h^*(a,b) = f_1^*(a) + g_1^*(b) + (f_1^*(a) + f_2^*(a))(g_1^*(b) + g_2^*(b)), \]

\( a \in U, \ b \in U' \).
Indeed, for every \( z \in U' \), the function \( h_z : x \mapsto h(x, z) \) is bent (since it equals \( f_1 \) or \( f_1 + 1 \) for some values of \( z \), and \( f_2 \) or \( f_2 + 1 \) for the other values) and the function \( z \mapsto h^*_z(a) \) is bent too, for every \( a \in U \), since it equals \( f_1^*(a) + g_1(z) + (f_1^*(a) + f_2^*(a))(g_1(z) + g_2(z)) \). This implies Proposition 4.7, according to Theorem 4.6. If we assume that \( g_1, g_2 \) in Proposition 4.7 are normal with the same normality subspace, i.e., \( U' = W \times W \) with \( g_1(y, 0) = g_2(y, 0) = 0 \) for all \( y \in W \), then we get
\[
h(x, y, 0) = f_1(x),
\]
which means that \( f_1 \preceq h \).

We state another generalization of Proposition 4.5, in the framework of Theorem 4.6, based on the Maiorana-McFarland bent functions. The MM-construction always gives a bent function on \( V \) with \( \dim V \) even. First represent \( V = W \times W \), where \( W \) is endowed with a scalar product. Ingredients for this construction are any permutation \( \pi : W \rightarrow W \) and any Boolean function \( \tau : W \rightarrow \mathbb{F}_2 \). Define for all \( x, y \in W \)
\[
M(x, y) = \langle x, \pi(y) \rangle + \tau(y).
\]
It is well-known and very easy to see that \( M \) is a bent function on \( V \) and that its dual is \( M^*(a, b) = \langle b, \pi^{-1}(a) \rangle + \tau(\pi^{-1}(a)) \).

Now let
\[
(f_w)_{w \in W}, \quad f_w : U \rightarrow \mathbb{F}_2
\]
be an arbitrary collection of bent functions on \( U \). For the sake of conformity with our previous notation, set \( \beta = f_0 \) and assume \( \pi(0) = 0, \tau(0) = 0 \).

Then, using \( M \), we get the following normal extension \( h \) on \( W \times W \times U \) of \( \beta \) by setting
\[
h(x, y, z) = f_y(z) + M(x, y).
\]
Such an \( h \) will be called an extension of MM-Type of \( \beta \).

Proposition 4.8. If \( \beta \) is a bent function and \( h \) is a normal extension of MM-type of \( \beta \), then \( h \) is also bent.

Indeed, we have \( h^*_z(a, b) = f_1^{\pi^{-1}(a)}(z) + \langle b, \pi^{-1}(a) \rangle + \tau(\pi^{-1}(a)) \). Note that the dual of \( h \) is of the same type as \( h \):
\[
h^*(a, b, c) = f_1^{\pi^{-1}(a)}(c) + \langle b, \pi^{-1}(a) \rangle + \tau(\pi^{-1}(a)).
\]
4.4 Duality of Normal Extensions and Plug-in Theorem

In this section, we will discuss normal extensions in the context of duality (see Section 1), and writing $\beta \preceq f$ (i.e., $f$ is a normal extension of $\beta$) we shall, according to Definition 4.1, assume that $\beta : U \to \mathbb{F}_2$ and $f : V = U \times W \times W \to \mathbb{F}_2$ are bent functions such that $r = \dim W$, $m = \dim U$ and

$$f(x, y, 0) = \beta(x)$$

for all $x \in U$, $y \in W$.

**Lemma 4.9.** Under the hypothesis above, we have $f^W(a, 0, c) = 2^r \beta^W(a)$, that is, $f^*(a, 0, c) = \beta^*(a)$, for all $a \in U$ and $c \in W$.

**Proof.** We compute for all $a \in U$:

$$\sum_{c \in W} (-1)^{f^*(a, 0, c)}$$

$$= 2^{-r-m/2} \sum_{c \in W} \sum_{x \in U} \sum_{y, z \in W} (-1)^{f(x, y, z)} \langle (a, x), (c, z) \rangle$$

$$= 2^{-r-m/2} \sum_{x \in U} \sum_{y, z \in W} (-1)^{f(x, y, z)} \left( \sum_{c \in W} (-1)^{\langle c, z \rangle} \right)$$

$$= 2^{-m/2} \sum_{x \in U} \sum_{y \in W} (-1)^{f(x, y, 0)} \langle (a, x) \rangle$$

$$= (2^{-m/2} \times 2^r) \beta^W(a)$$

$$= 2^r (-1)^{\beta^*(a)}.$$

The left hand sum can take on its extremal values $\pm 2^r$ only if $f^*(a, 0, c) = \beta^*(a)$, for every $c \in W$. \qed

**Proposition 4.10.** $\beta \preceq f$ if and only if $\beta^* \preceq f^*$.

**Proof.** It is enough to prove that $\beta \preceq f$ implies $\beta^* \preceq f^*$. Thus assume that $\beta \preceq f$. For all $a \in U$, $c \in W$, we have $f^*(a, 0, c) = \beta^*(a)$, according to Lemma 4.9, and therefore $\beta^* \preceq f^*$, where the subsets $W_1 = \{0\} \times W \times \{0\}$ and $W_2 = \{0\} \times \{0\} \times W$ of $V$ interchange their roles (cf. Definition 4.1). \qed

We are now in a position to prove the “Plug-in Theorem” for normal extensions:
4.4. DUALITY OF NORMAL EXTENSIONS AND PLUG-IN THEOREM

**Theorem 4.11.** Let $\beta$ be a bent function on $U$ and $f$ a bent function on $V = U \times W \times W$. Assume that $\beta \preceq f$. Let

$$\beta' : U \to \mathbb{F}_2$$

be any bent function. Modify $f$ by setting for all $x \in U$, $y \in W$

$$f'(x, y, 0) = \beta'(x),$$

while $f'(x, y, z) = f(x, y, z)$ for all $x \in U$, $y, z \in W$, $z \neq 0$. Then $f'$ keeps to be bent and we have $\beta' \preceq f'$.

**Proof.** We only prove that $f'$ is a bent function. Everything else is obvious. We derive:

$$f^{W}(a, b, c) = \sum_{x \in U} \sum_{y \in W} \sum_{z \in W} (-1)^{f'(x, y, z) + (a, x) + (b, y) + (c, z)}$$

$$= \sum_{x \in U} \sum_{y \in W} \sum_{z \in W} (-1)^{f(x, y, z) + (a, x) + (b, y) + (c, z)}$$

$$- \sum_{x \in U} \sum_{y \in W} (-1)^{\beta(x) + (a, x) + (b, y)}$$

$$+ \sum_{x \in U} \sum_{y \in W} (-1)^{\beta'(x) + (a, x) + (b, y)}$$

$$= f^{W}(a, b, c) + \left( \sum_{y \in W} (-1)^{(b, y)} \right) \left( \beta^{W}(a) - \beta^{W}(a) \right).$$

For $b \neq 0$ we conclude that $f^{W}(a, b, c) = f^{W}(a, b, c)$. On the other hand for $b = 0$ we get

$$f^{W}(a, 0, c) = f^{W}(a, 0, c) + 2^r \left( \beta^{W}(a) - \beta^{W}(a) \right),$$

and, according to Lemma 4.9, we know that $f^{W}(a, 0, c) = 2^r \beta^{W}(a)$, that is $f^{W}(a, 0, c) = 2^r \beta^{W}(a) = \pm 2^r + m/2$ as desired. 

Recall that $f$ is normal if and only if $\varepsilon \preceq f$ for $\varepsilon \in \mathbb{F}_2$. Note that in this case, the Plug-in Theorem reduces to the well-known fact that we can change the constant value $\varepsilon$ on a normality subspace and get again a bent function.
4.5 Normality Inherits Downwards

**Theorem 4.12.** Suppose that \( \beta \preceq f \) for bent functions \( \beta \) and \( f \). If \( f \) is normal, then also \( \beta \) is normal.

**Proof.** Let \( f : V = U \times W \times W \to \mathbb{F}_2 \) and \( \beta : U \to \mathbb{F}_2 \) be bent functions such that \( f(u, w, 0) = \beta(u) \) for all \( u \in U, w \in W \), and assume that \( N \subseteq V = U \times W \times W \) is a subspace with \( \dim N = r + m/2 \) such that

\[
f|_N = \text{constant 0}.
\]

We have to show that \( \beta \) is normal. Define the following subspaces:

\[
M = U \times W \times \{0\}, \\
\tilde{N} = N \cap M, \\
N_0 = \{u \in U : (u, w, 0) \in N \text{ for some } w \in W\}, \\
W_0 = \{w \in W : (0, w, 0) \in N\}.
\]

Note that \( N_0 \) is the projection of \( \tilde{N} \) to \( U \) and that

\[
\beta|_{N_0} = \text{constant 0}.
\]

For each \( u \in N_0 \), choose an element \( \psi(u) \) in \( W \) such that \( (u, \psi(u), 0) \in \tilde{N} \cap (\{u\} \times W \times \{0\}) \), then

\[
\tilde{N} \cap (\{u\} \times W \times \{0\}) = \{(u, \psi(u) + w, 0) : w \in W_0\}
\]

and therefore

\[
\tilde{N} = \{(u, \psi(u) + w, 0) : u \in N_0, w \in W_0\}.
\]

We claim that \( \dim N_0 = m/2 \), which implies that \( \beta \) is normal as stated. Consider the following set

\[
\Gamma = \{\gamma : \gamma \text{ is a bent function on } U \text{ with } \gamma|_{N_0} = \text{constant 0} \}.
\]

Of course \( \beta \in \Gamma \). For each \( \gamma \in \Gamma \), let \( f_\gamma \) denote the resulting bent function on \( V \) obtained from \( f \) via exchanging \( \beta \) by \( \gamma \) in the sense of Theorem 4.11. Then \( f \) and \( f_\gamma \) coincide on \( N \), i.e.,

\[
f_\gamma|_N = \text{constant 0}.
\]
Applying Lemma 2.4 to $f$ implies that for each proper coset $a + N$ of $N$ in $V$, $a \in V \setminus N$, we have

$$\sum_{b \in a + N} (-1)^{f(b)} = \sum_{b \in M \cap (a + N)} (-1)^{f(b)} + \sum_{b \in (a + N) \setminus M} (-1)^{f(b)} = 0.$$ 

Consequently the sum

$$\sum_{b \in M \cap (a + N)} (-1)^{f(b)}$$

is independent of $\gamma \in \Gamma$. Now choose some fixed $u_0 \in U \setminus N_0$, and take $a = (u_0, 0, 0)$. Then $M \cap (a + N) = a + (M \cap N) = a + \tilde{N}$, since $a \in M$ and consequently in view of (4.2)

$$\sum_{b \in M \cap (a + N)} (-1)^{f(b)} = \sum_{b \in (u_0, 0, 0) + \tilde{N}} (-1)^{f(b)} = \sum_{u \in N_0} \sum_{w \in W_0} (-1)^{f(u_0 + u, \psi(u) + w, 0)} = \sum_{u \in N_0} \sum_{w \in W_0} (-1)^{\gamma(u_0 + u)}$$

$$= 2^s \left( \sum_{x \in u_0 + N_0} (-1)^{\gamma(x)} \right),$$

where $s$ denotes the dimension of $W_0$. We conclude that for each fixed proper coset $N'_0$ of $N_0$ in $U$ the sum

$$\sum_{x \in N'_0} (-1)^{\gamma(x)}$$

is independent of $\gamma$. However, for $\dim N_0 < m/2$ it is a trivial matter to find bent functions $\gamma$ on $U$, which are constant 0 on $N_0$, and the preceding sum attains different values (while Lemma 2.4 states that this sum is 0 in case of $\dim N_0 = m/2$). In fact, if $\dim N_0 < m/2$ then $\tilde{U} = N_0 \cup N'_0$ is a subspace of $U$ with $\dim \tilde{U} \leq m/2$. Let $\gamma_1$ be any bent function on $U$, which is constant on $\tilde{U}$, and take a linear map $\ell : U \to \mathbb{F}_2$ separating $N_0$ and $N'_0$ in the sense that

$$\ell|_{N_0} = \text{constant } 0,$$

$$\ell|_{N'_0} = \text{constant } 1.$$
Now set $\gamma_2 = \gamma_1 + \ell$. Then we have $\gamma_i \in \Gamma$, $(i = 1, 2)$ and
\[
\gamma_1 \mid N'_0 = \text{constant } 0, \\
\gamma_2 \mid N'_0 = \text{constant } 1.
\]
But $\sum_{x \in N'_0} (-1)^{\gamma_1(x)} = \# N'_0$ and $\sum_{x \in N'_0} (-1)^{\gamma_2(x)} = -\# N'_0$, a contradiction. Hence $\dim N_0 = m/2$ and $\beta$ is normal.

In view of the preceding theorem, Section 3 provides many constructions of new non-normal bent functions from a given one.

Since $f = \beta \oplus g$ is a normal extension of $\beta$ if $g$ is normal, we get as a consequence from Theorem 4.12:

**Corollary 4.13.** The direct sum of a normal and a non-normal bent function is always non-normal.

We note that, vice versa, Corollary 4.13 in combination with Theorem 4.4 implies Theorem 4.12: assume that we have a counterexample for Theorem 4.12, i.e., $\beta \preceq f$ for a non-normal bent function $\beta$ and a normal bent function $f$, then $\beta \oplus f$ would be normal by Theorem 4.4, and we would have a counterexample for the statement of the corollary.

### 4.6 Totally Non-Normal Bent Functions

We have seen, that the relation $\beta \preceq f$ for bent functions, in view of the Plug-in Theorem 4.11, describes a property of the restriction of $f$ to $V \setminus (U \times W \times \{0\})$ (see Definition 4.1), which has nothing to do with a particular $\beta$. Under this aspect, only the size, i.e. the number of variables, of $\beta$ is of importance.

Recall the notation
\[
\mathcal{N}_f = \{\beta : \beta \preceq f, \beta \text{ bent}\}
\]
(see Proposition 4.2). It can be considered as a kind of generalized normality of $f$ if $\mathcal{N}_f \setminus \{f\}$ is non-empty. Otherwise we call $f$ **totally non-normal**.

The existence of totally non-normal bent functions is clear, as we know that non-normal bent functions exist at all: simply take a non-normal one of minimal size. Whether this minimal size is 8 or 10, is not known.

Using the algorithm described below, we confirmed that the non-normal functions of Chapter 3 (Fact 3.15 and Fact 3.16) are totally non-normal.
4.6. TOTALLY NON-NORMAL BENT FUNCTIONS

4.6.1 Testing Totally Non-Normality

Let \( f : \mathbb{F}_2^n \to \mathbb{F}_2 \) be a bent function. Based on ideas sketched in 3.4 we describe an algorithm, that tests if a given function is totally non-normal, i.e. if there exists a Boolean function \( \beta \) such that \( \beta \leq f \) or not.

We first reformulate the main idea of the Algorithm 3.4. Given a subspace \( U \subset \mathbb{F}_2^n \), we define the functions \( f_U \) and \( f_U^c \) as:

\[
f_U^c : \mathbb{F}_2^n/U \to \mathbb{F}_2 \\
f_U^c(U + a) = \begin{cases} 1 & \text{if } f|_{U+a} \equiv c \\ 0 & \text{otherwise} \end{cases}
\]

The key observation of Algorithm 3.4 is, that \( f \) is constant \( c \) on a flat of dimension \( n/2 \) if and only if for every \( t \leq n/2 \) there exists a subspace \( U \) of dimension \( t \), such that \( f_U^c \) is constant 1 on a flat of dimension \( m - t \).

This leads to a recursive view of Algorithm 3.4 for checking if a Boolean function \( f \) is normal. We start by computing \( f_U^c \) for all subspaces \( U \) of a starting dimension \( t_0 \) and for all these functions we recursively go on in the same manner. Note that, despite the easier description, implementing the algorithm as described in [16] is most likely more efficient. This is due to the fact, that the excepted support of the functions \( f_U^c \) becomes very small with increasing dimensions of \( U \).

In order to check, if a function is totally non-normal, we first check if it is normal or not. If it is normal, then we are done. If it is non-normal, we have to check, if it is a normal-extension of a non-normal bent function. As it is known that all bent functions in 6 variables are normal, it is enough to check, if the function is a normal-extension of some \( \beta : \mathbb{F}_2^m \to \mathbb{F}_2 \) where \( m > 6 \).

By definition if \( f \) is a normal extension of \( \beta \), then there exist subspace \( V \) of dimension \( (n + m)/2 \), which can be decomposed into a direct sum of an \( m \) dimensional space \( U \) and a \( (n - m)/2 \) dimensional space \( W \), such that for all \( u \in U \) the function \( f \) is constant on every subset \( u + W \).

The algorithm is divided into two parts. At first we are searching for candidates for \( U \), simply by computing all the functions \( f_U^c \) for every \( U \) of dimension \( m \).

In a second step we define new functions \( f_U \) as

\[
f_U : \mathbb{F}_2^n/U \to \mathbb{F}_2 \\
f_U(U + a) = \begin{cases} 1 & \text{if } f_U^c \equiv 1 \text{ or } f_U^t \equiv 1 \\ 0 & \text{otherwise} \end{cases}
\]

With the help of these functions, the question whether \( f \) is a normal extension can be easily characterized.
Lemma 4.14. There exist a function $\beta : \mathbb{F}_2^m \to \mathbb{F}_2$, such that $\beta \preceq f$ if and only if there exist a $m$ dimensional subspace $U$ such that $f^U$ is constant 1 on an $(n - m)/2$ dimensional subspace.

Proof. “$\Rightarrow$”: If $\beta \preceq f$ we can decompose $\mathbb{F}_2^n = U \otimes W_1 \otimes W_2$ such that for all $u \in U$ and $w_1 \in W_1$

$$f(u + w_1) = \beta(u)$$

thus we see that $f^U$ is constant 1 on the $(n - m)/2$ dimensional subspace $W_1$. “$\Leftarrow$”: If for an $m$ dimensional subspace $U$ the function $f^U$ is constant on an $(n - m)/2$ dimensional subspace $W_1$, we find a subspace $W_2$ of dimension $(n - m)/2$, such that $\mathbb{F}_2^n = U \otimes W_1 \otimes W_2$ and a function $\beta : U \to \mathbb{F}_2$, such that for all $u \in U$ and $w_1 \in W_1$

$$f(u + w_1) = \beta(u)$$

consequently due to Lemma 4.9 $\beta$ must be bent and thus $\beta \preceq f$.

The complete algorithm works like follows.

Algorithm 4.15.
Input: a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$

Output: a decomposition $\mathbb{F}_2^n = U \otimes W_1 \otimes W_2$ and a function $\beta : U \to \mathbb{F}_2$

such that for all $u \in U$ and $w_1 \in W_1$ we have

$$f(u + w_1) = \beta(u)$$

or “NULL” if such a function does not exist.

For all $8 \leq m \leq n - 2$

For all subspaces $U$ of $\mathbb{F}_2^n$ with $\dim(U) = m$

Compute $f^U$

If $f^U$ is constant on a $(n - m)/2$ dimensional subspace $W_1$

Output $U, W_1$ and $\beta := f|U$.

End for

End for
Chapter 5

Monomial Bent Functions

5.1 Introduction

In this chapter we consider bent functions constructed by power functions. Recall that $L$ is the finite field with $2^n$ elements and $K$ is the subfield of index 2 in $L$.

More precisely we are interested in Boolean functions of the form

$$f : L \rightarrow \mathbb{F}_2$$

$$f(x) = \text{tr}(\alpha x^d)$$

An exponent $d$ (always understood modulo $2^n - 1$) is called a bent exponent, if there exists an $\alpha$ such that the Boolean function $\text{tr}(\alpha x^d)$ is bent.

Although monomial functions have been widely studied in closely related arrays as APN-functions, $m$-sequences and coding theory, this approach has not yet been consequently undertaken for bent functions.

There are a few known cases of bent exponents, which will be described in the following section. As one of the main results of this chapter we will present a new bent exponent. This exponent actually leads to functions belonging to the Maiorana-McFarland class of bent functions.

A remarkable point is, that for all the well studied families of bent functions, there is at least one monomial bent function belonging to one of these families. Furthermore, carefully considering the proofs in the following section, it is quite easy to rediscover all the known classes of bent functions. In some sense this strengthened the need to fully understand (at least) the monomial bent functions, as they include a wide variety of bent functions. Furthermore as explained in Chapter 3 the Kasami exponent leads to bent functions not included in one of the well known classes.
In the last section of this Chapter we apply Stickelberger’s theorem to deduce some strong indication why a large class of exponents will not lead to bent exponents.

Computer experiments suggest that if $n$ is divisible by 6 then $d = 2^{n/3} + 2^{n/6} + 1$ is a bent exponent. Proving this conjecture is a challenging open problem.

As mentioned in Chapter 1, Dobbertin introduced the notion of power functions on the infinite field $L = \bigcup_{(n,m)=1} F_{2^n}$ where $m$ is an integer. A mapping $\pi : L \rightarrow L$ is called a power mapping if $\pi|_{F_{2^n}}$ is a power mapping for every $n$ with $\gcd(n, m) = 1$. It turns out that all known APN functions can be extended to power mappings on this field. A similar approach works also in all known cases of monomial bent functions. As we always require $n$ to be even and due to the fact that $d$ is not coprime to $2^n - 1$ - we have to take into account the role of $\alpha$ - we have to consider slightly different global fields $\mathcal{L}$. Given even integers $n, m$ where $m | n$ and a monomial Boolean function

$$f(x) = \text{tr}_L(x^d)$$

on $\mathbb{F}_{2^n}$ the restriction to $x \in \mathbb{F}_{2^k}$ becomes

$$f(x) = \text{tr}_K(x^d \text{tr}_{L/K}(1)) \quad x \in \mathbb{F}_{2^k}.$$ 

Thus if $n/m$ is even, this restriction is constant $0$. Given $t \in \mathbb{N}$ let

$$\mathcal{L} = \bigcup_{\gcd(n,2)=1} \mathbb{F}_{2^{t_n}}.$$

This construction ensures that the restriction to subfields is non-zero. Further considerations have to be taken into account, to ensure that every restriction of a global power mapping on $\mathcal{L}$ is bent. This includes a discussion of the appropriate choice of the coefficient $\alpha$.

**Preliminaries**

As $\text{tr}(x^d) = \text{tr}(x^{2d})$ for all $x$, we can always replace $d$ by any exponent in the cyclotomic coset of $d$.

There are some necessary conditions for $d$ to be a bent exponent. Let $\text{wt}(d)$ denote the binary weight of $d$. As mentioned in Chapter 1 bent functions have degree at most $k$ and as the degree of $\text{tr}(\alpha x^d)$ is either 0 or $\text{wt}(d)$ (see [13]), it follows that the binary weight of a bent exponent is at most $k$. 
Furthermore a bent exponent \( d \) cannot be coprime to \( 2^n - 1 \). Otherwise, if \( d \) is coprime to \( 2^n - 1 \) we get 
\[
\sum_{x \in L} \chi_L(\alpha x^d) = \sum_{x \in L} \chi_L(\alpha x) = 0
\]
for every non-zero \( \alpha \in L \) in contradiction to the bentness property.

Note that a function \( f(x) = \text{tr}(\alpha x^d) \) cannot be bent for every non-zero \( \alpha \). If \( f \) would be bent for every \( \alpha \in L^* \), this would allow the construction of a vectorial bent function from \( L \) to \( L \) which is not possible (see Section 6.8 and [36]).

Denote \( \gcd(d, 2^n - 1) \) by \( s \). Moreover let 
\[
W = \{ \gamma \in L \mid \gamma^d = 1 \} = \{ \gamma \in L \mid \gamma^s = 1 \}.
\]
Clearly, \( f \) is constant on all cosets \( \lambda W \). Consequently we get 
\[
f_W(0) = 1 + s \sum_{\lambda \in L^*/W} \chi_L(\alpha x^d) \equiv 1 \mod s.
\]
Assume that \( f_W(0) = 2^k \) then \( s \) divides \( 2^k - 1 \). On the other hand if \( f_W(0) = -2^k \) then \( s \) divides \( 2^k + 1 \). As \( \gcd(2^k - 1, 2^k + 1) = 1 \) we see, that \( d \) is coprime either to \( 2^k - 1 \) or to \( 2^k + 1 \). Summarizing we get

**Lemma 5.1.** Let \( d \) be a bent exponent. Then \( \gcd(d, 2^n - 1) \neq 1 \). Furthermore let \( f(x) = \text{tr}(\alpha x^d) \) be a bent function. Then

1. \( \gcd(d, 2^k - 1) = 1 \) if and only if \( f_W(0) = -2^k \)
2. \( \gcd(d, 2^k + 1) = 1 \) if and only if \( f_W(0) = 2^k \)

Let \( \alpha, \beta \in L^* \). If \( \beta = \alpha \lambda^d \) for some non-zero element \( \lambda \in L \), the functions \( x \to \text{tr}(\alpha x^d) \) and \( x \to \text{tr}(\beta x^d) \) are linear equivalent. It follows that for our considerations we can always replace \( \alpha \) by any element in the same coset of \( U \), where 
\[
U = \{ x^d \mid x \in L^* \} = \{ x^\gcd(d, 2^n - 1) \mid x \in L^* \}.
\]
Note that for any \( \gamma \in L \) with \( \gamma^d = 1 \) the Walsh-coefficients of \( f(a) \) and \( f(\gamma a) \) are equal. Thus we can always replace \( a \) by any element in the same coset of \( W \).
5.2 Known Cases

In this section we discuss the known cases of monomial bent functions. We give an alternative proof of the Gold Case by directly computing the dual. For the Dillon Case we give a new simple and direct proof of the known link to the Kloosterman Sum.

In the case of the Kasami Exponent we discuss an algorithmic approach, to decide if the dual of these bent functions are linear equivalent to the function itself.

5.2.1 The Gold Case

This case belongs to the class of quadratic bent functions, the easiest and best understood class of bent functions. It is well known, that the dual of a quadratic bent function is again a quadratic bent function. Furthermore all quadratic bent functions are linear or affine equivalent, which can easily be proven, using the theory of quadratic forms. It follows that the dual of any quadratic bent function is equivalent to the function itself. Nevertheless finding the explicit linear or affine mapping is not always trivial. We give an alternative proof for the bentness of the monomial functions with the Gold exponent, that allows us to characterize the dual via a linear mapping applied to the function itself.

**Theorem 5.2.** Let \( \alpha \in \mathbb{F}_{2^n} \), \( r \in \mathbb{N} \) and \( d = 2^r + 1 \). The function

\[
f : L \rightarrow \mathbb{F}_2
\]

with

\[
f(x) = \text{tr}(\alpha x^d),
\]

is bent if and only if

\[
\alpha \notin \{x^d \mid x \in \mathbb{F}_{2^n}\}
\]

**Proof.** "\( \Leftarrow \)" Assume that \( \alpha \) is not a \( d \)-th power. We will prove that \( f \) is bent by computing the dual of \( f \).

\[
f^W(a) = \sum_{x \in \mathbb{F}_{2^n}} \chi_L(\alpha x^d + ax)
\]

\[
= \sum_{x \in \mathbb{F}_{2^n}} \chi_L(\alpha(x + \gamma)^d + \alpha \gamma^d + \alpha \gamma^2 x + \alpha \gamma x^{2^r} + ax)
\]
5.2. KNOWN CASES

for any $\gamma \in \mathbb{F}_2^n$. Assume we could choose $\gamma$, such that for every $x \in \mathbb{F}_{2^n}$ we have $\text{tr}(\alpha \gamma^2 x + \alpha \gamma x^2 + ax) = 0$. In this case

$$f^W(a) = \sum_{x \in \mathbb{F}_2^n} \chi_L(\alpha x + \gamma)^d + \alpha \gamma^d$$

$$= (-1)^{\text{tr}(\alpha \gamma^d)} \sum_{x \in \mathbb{F}_2^n} \chi_L(\alpha x + \gamma)^d$$

$$= (-1)^{\text{tr}(\alpha \gamma^d)} f^W(0).$$

So in order to prove that $f$ is bent, we have to consider the linear equation

$$0 = \text{tr}(\alpha \gamma^2 x + \alpha \gamma x^2 + ax)$$

$$= \text{tr}(x^2 (\alpha^2 \gamma^2 r + \alpha \gamma + a^2 r ))$$

This can only be true for all $x \in \mathbb{F}_{2^n}$ if

$$\alpha^2 \gamma^2 r + \alpha \gamma + a^2 r = 0.$$  

In order to be able to choose $\gamma$ appropriately, we have to prove that the linear mapping

$$H(\gamma) = \alpha^2 \gamma^2 r + \alpha \gamma$$

is bijective, i.e. the mapping has a trivial kernel if $\alpha \notin \{x^d \mid x \in \mathbb{F}_{2^n}\}$. For $\gamma \neq 0$ we compute

$$H(\gamma) = 0$$

$$\gamma^{2^r - 1} = \alpha^{1 - 2^r}$$

$$(\gamma^d)^{2^r - 1} = (\alpha^{-1})^{2^r - 1}$$

but as $\gcd(2^r - 1, d) = 1$ the left-hand side is a $d$th power, while the right-hand side is a $d$th power iff $\alpha$ is a $d$th power. Thus whenever $\alpha$ is not a $d$th power the function is bent.

"$\Rightarrow$": On the other hand this immediately implies, that if $\alpha$ is not a $d$th power, than $f$ is not bent. Otherwise the function would be bent for every $\alpha \in L^*$ which is not possible as explained in the last section.

If $f$ is bent $H^{-1}$ exists and with $\gamma = H^{-1}(a^2 r)$ we get

$$f^W(a) = (-1)^{f(H^{-1}(a))} f^W(0).$$

Remark 5.3. Note, that not for every $r$ the coefficient $\alpha$ can be chosen, such that the corresponding monomial function is bent. In the case where $\gcd(d, 2^n - 1) = 1$ every $\alpha \in \mathbb{F}_{2^n}$ is a $d$th power. In other words a Gold Exponent $d$ is a bent exponent if and only if $x \to x^d$ is not a bijection.
5.2.2 The Dillon Case

Let \( d = 2^k - 1 \). We consider the monomial function

\[
f : L \rightarrow \mathbb{F}_2
\]

with

\[
f(x) = \text{tr}(ax^d).
\]

This exponent was first considered by Dillon [17] as an example of bent functions belonging to the PS-class. Dillon proved that this function is bent if and only if \( \alpha \) is a zero of the Kloosterman Sum. This connection was proven using results from coding theory. We give an alternative direct proof of this known fact.

Obviously this function is constant on \( \lambda K^* \) for all \( \lambda \in L \), where \( K \) is the subfield of index 2 in \( L \). So this leads to a bent function if and only if it belongs to the class \( PS_{ap} \). We include a proof for completeness.

We recall the definition of the set

\[
S = \{ u \in L \mid u^{2^k+1} = 1 \}
\]

and the fact that every element \( x \in L^* \) can be uniquely represented as \( x = \lambda u \) with \( \lambda \in K^* \) and \( u \in S \) (see Chapter 1).

We can restrict to the case \( a \in S \), as here

\[
f^W(a) = f^W(\lambda a),
\]

for all \( \lambda \in K^* \).

\[
f^W(a) = \sum_{x \in L} \chi_L(ax^d + ax) = 1 + \sum_{u \in S} \sum_{\lambda \in K^*} \chi_L(\alpha u^d + a\lambda u) = 1 + \sum_{u \in S} \chi_L(\alpha u^d) \sum_{\lambda \in K^*} \chi_L(a\lambda u) = 1 + \sum_{u \in S} \chi_L(\alpha u^d) \sum_{\lambda \in K} \chi_L(a\lambda u) - \sum_{u \in S} \chi_L(\alpha u^d) = 1 + 2^k \sum_{\lambda \in K} \chi_L(\alpha u^d) - \sum_{u \in S} \chi_L(\alpha u^d) = 1 + 2^k \sum_{\lambda \in K} \chi_L(\alpha u^d) - \sum_{u \in S} \chi_L(\alpha u^d) = 1 + 2^k \chi_L(\alpha a^{-d}) - \sum_{u \in S} \chi_L(\alpha u^d)
\]
Thus in order to show $f^W(a) = \pm 2^k$, we have to show that

$$S(\alpha) = \sum_{u \in S} \chi_L(\alpha u) = 1.$$ 

This last condition can be transferred into a condition on Kloosterman Sums $K(\alpha)$ where

$$K(\alpha) := \sum_{x \in K} \chi_K(1/x + \alpha x)$$

with the convention, that $1/0 = 0$.

Note that wlog. we can choose $\alpha \in K$ (see refIntroMonomial). We make use of the fact, that for every $u \in S$ the element $u + \pi$ can be represented by $1/c$ where $c \in K$ and $\text{tr}_K(c) = 1$ and, vice versa, every $1/c \in K$ with
\[ \text{tr}_K(c) = 1 \] uniquely represents the set \( \{u, \overline{u}\} \) as explained in Section 6.3.

\[
S(\alpha) = \sum_{u \in S} \chi_K(\alpha(u + \overline{u}))
\]
\[
= 1 + \sum_{u \in S \setminus \{1\}} \chi_K(\alpha(u + \overline{u}))
\]
\[
= 1 + 2 \left( \sum_{c \in K, \; \text{tr}_K(c) = 1} \chi_K \left( \frac{\alpha}{c} \right) \right)
\]
\[
= 1 + 2 \left( \sum_{c \in K} \chi_K \left( \frac{\alpha}{c} \right) \right) - 2 \left( \sum_{c \in K^* \setminus \{0\}, \; \text{tr}_K(c) = 0} \chi_K \left( \frac{\alpha}{c} \right) \right) - 2
\]
\[
= -1 - \sum_{\beta \in K \setminus \mathbb{F}_2} \chi_K \left( \frac{\alpha}{\beta^2 + \beta} \right)
\]
\[
= -1 - \sum_{\beta \in K \setminus \mathbb{F}_2} \chi_K \left( \alpha \left( \frac{1}{\beta} + \frac{1}{1 + \beta} \right) \right)
\]
\[
= -1 - \sum_{\gamma \in K \setminus \mathbb{F}_2} \chi_K \left( \alpha \left( \gamma + \frac{1}{1 + \gamma} \right) \right)
\]
\[
= -1 - \sum_{\gamma \in K \setminus \mathbb{F}_2} \chi_K \left( \alpha \left( \gamma + 1 + \frac{1}{\gamma} \right) \right)
\]
\[
= -1 - \sum_{\gamma \in \alpha^{-1}K \setminus \alpha^{-1} \mathbb{F}_2} \chi_K \left( \alpha \left( \gamma + \frac{1}{\gamma} \right) \right)
\]
\[
= -1 - \sum_{\gamma \in \alpha^{-1/2}K \setminus \alpha^{-1/2} \mathbb{F}_2} \chi_K \left( \alpha \gamma + \frac{1}{\gamma} \right)
\]
\[
= 1 - K(\alpha).
\]

Summarizing we proved that

\[
f^W(a) = 2^k \chi_L(\alpha a^{-d}) + K(\alpha)
\]

and as \(2^k d = -d \mod 2^n - 1\) and \(\alpha^{2^k} = \alpha\) we get the following theorem.

**Theorem 5.4.** Let \(a \in L\). Then

\[
f^W(a) = 2^k \chi_L(\alpha a^d) + K(\alpha)
\]
5.2. KNOWN CASES

In particular the spectrum of $f$ is uniquely determined by $f^W(0)$. As a corollary we get

**Corollary 5.5.** The exponent $d = 2^k - 1$ is a bent exponent. $f(x) = \text{tr}(\alpha x^d)$ is bent if and only if $K(\alpha) = 0$. In this case the dual of $f$ is identical to the function itself.

In [29] it was shown, that such an $\alpha$ exist for every $k$, i.e. bent functions of this type exist for every $n$. Furthermore as

$$S(\alpha) = \sum_{u \in S} \chi_L(\alpha u) = \sum_{u \in S} \chi_L(\alpha u^s)$$

for every integer $s$ coprime to $2^k + 1$ we get

**Corollary 5.6.** For every integer $s$ coprime to $2^k + 1$ the function

$$f'(x) = \text{tr}(\alpha x^{sd})$$

is bent whenever $K(\alpha) = 0$.

5.2.3 The Dillon-Dobbertin Case

Regarding the question of normality of bent functions, the Kasami exponent $d = 2^{2r} - 2^r + 1$ is the most interesting case of a bent exponent (see also Chapter 3). The following theorem was conjectured by Holman and Xiang in 1998 and was proven by Dillon and Dobbertin in [20].

**Theorem 5.7.** Let $d = 2^{2r} - 2^r + 1$ with $\gcd(r, n) = 1$ and $\alpha \in \mathbb{F}_{2^n}$. The function

$$f : \mathbb{F}_2^n \to \mathbb{F}_2^n$$

with

$$f(x) = \text{tr}(\alpha x^d)$$

is bent if and only if $\alpha \not\in \{x^3 | x \in \mathbb{F}_{2^n}\}$.

Despite the strong similarities of this theorem and the Gold Exponent, the proof of Theorem 5.7 is distinct more complex and requires very sophisticated techniques. Unfortunately it does not give any insight to the structure of the dual function, as it is proven that $f^W(a)^2 = 2^n$ for all $a \in L$.

As a first step to investigate the dual function we propose an algorithm, to check if the dual is linear equivalent to the function itself. Remarkably, using the algorithm described below, it turns out that this is true for $n = 8$ but not for $n = 10, 12$ or 14. A theoretical approach for computing the dual is an interesting open challenge.
An Algorithm for Checking Linear Equivalence of Bent Functions

The algorithm presented here is a generalization of an algorithm presented in [27]. Depending on the functions our algorithm clearly outperforms the original algorithm.

Let us consider two Boolean functions

\[ f, g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \]

The task is, given \( f \) and \( g \), to determine if there exists a bijective linear mapping

\[ H : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n \]

such that

\[ g = f \circ H. \]

and, if such a linear mapping exists, to compute it. It should be remarked that \( H \) may not be uniquely determined given \( f \) and \( g \). If there exists a linear function \( G \) such that \( f = f \circ G \), then obviously \( G \circ H \) is also a linear transformation that maps \( f \) to \( g \). Vice versa, if there are two linear mappings \( H, G \) such that \( f \circ H = f \circ G = g \), then \( f \) is invariant under composition with the linear mappings \( H \circ G^{-1} \) and \( G \circ H^{-1} \).

The idea presented at FSE03 by J. Fuller and W. Millan was to look at the so called “1-local neighborhood” of the functions \( f \) and \( g \) and uses this to compute the linear transformation \( H \). In order to compute candidates for \( H \) the algorithm uses two well known necessary (but not sufficient) conditions, wether two Boolean functions are linearly equivalent. On the one hand, two functions \( f' \) and \( g' \) are linearly equivalent, the Walsh-Coefficients of \( f' \) and \( g' \) have the same distribution. On the other hand the same is true for the Autocorrelation-Coefficients of \( f' \) and \( g' \).

Considering the “1-local neighborhood” can also be formulated as adding to the function \( f \) a Boolean function \( h \) of Hamming weight 1 and find \( h' \), such that \( g + h' = f \circ H + h \). This technique generalizes to an arbitrary Boolean function \( h \), and more generally we get:

**Lemma 5.8.** Let \( f, g \) be linear equivalent functions with \( g = f \circ H \) and \( h, h' : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) be two arbitrary Boolean functions. Then

\[(f + h) \circ H = (g + h')\]

if and only if

\[ h' = h \circ H. \]
5.2. KNOWN CASES

For most purposes it might be a good choice to select \( h \) with hamming-weight 1. In this case only \( 2^n \) linear equivalent functions have to be checked.

In [27] they choose a basis for \( \mathbb{F}_2^n \) and then subsequently choose \( h \) to be the characteristic function of each element in the basis. In the next step they test for all \( h' \) linear equivalent to \( h \) if the functions \( f' \) and \( g' \) are linear equivalent using the Walsh and Autocorrelation-spectra. The set of all functions \( h' \) passing these tests are candidates for \( h \circ H \). This allows them to compute candidates for the image of each element in the base independently and finally derive candidates for the entire linear mapping \( H \).

However for bent functions it turns out that this does not work, as the “1-local neighborhood” of two bent functions, even when they are not linear equivalent, is similar in terms of their Walsh- and Autocorrelation-spectrum.

Generalizing the ideas from [27], we change \( f \) by adding \( h \) and that test for all functions \( h' = h \circ G \) linear equivalent to \( h \) if the Walsh- and Autocorrelation-Coefficients of \( f + h \) and \( g + h' \) are the same. The set of all mappings \( h' \) fulfilling this condition are candidates for \( h \circ H \).

Clearly it is not useful to choose an arbitrary function \( h \) because the number of functions linear equivalent to \( h \) might be to high.

Our algorithm works with quadratic functions of the form \( x_i x_j \) for \( h \). A linear mapping will map \( x_i x_j \) to

\[
x_i x_j \rightarrow \left( \sum_{i=0}^{n} \lambda_i x_i \right) \left( \sum_{j=0}^{n} \mu_j x_j \right).
\]

As we only deal with bijective linear mappings there are \( \frac{(2^n-1)(2^n-2)}{2} \) linear equivalent functions that have to be checked. The advantage is, that using quadratic functions, the Walsh- and Autocorrelation-spectra differ enough to reduce the number of candidates for the correct value of \( h' \) even for bent functions.

Furthermore, if the algorithm outputs more than one possible function \( h' \), which may happen because \( f \) is invariant under some linear transformation or because there exists functions \( h' \) such that \( f + h \) and \( g + h' \) have the same spectra, although they are not linear equivalent, it is much easier to put the right things together. This is done by subsequently using the monomials \( h_i = x_i x_{i+1} \) for \( h \). We get possibilities for \( h_i \circ H \) of the form \( h_i \circ H = H(x)_i H(x)_j \) and possibilities for \( h_{i+1} = H'(x)_{i+1} H'(x)_{i+2} \) and we can easily check if these parts fit together by checking if they have a common factor. This avoids the potentially exponential task of checking all possibilities at the end of the algorithm presented at FSE 2003.
5.3 A New Bent Exponent for \( n = 4r \)

Based on computer experiments, Anne Canteaut ([5]) conjectured that for \( r \) odd and \( n = 4r \) the exponent \( d = (2^r + 1)^2 \) is a bent exponent. As the main result of this section we present a proof for this fact. The proof of this theorem shows, that the corresponding Boolean function belongs to the well known class of Maiorana-McFarland bent functions. A starting point for the proof of this Theorem is a technique used by Dobbertin in a similar situation, see [22] for details.

The following lemma will be an crucial part in the proof of Theorem 5.10

**Lemma 5.9.** Let \( r \) be an odd integer and \( K = \mathbb{F}_{2^r} \). Then the function

\[
\pi : K^2 \rightarrow K^2
\]

with

\[
\pi(x, y) = \left( \frac{\pi_1(x, y)}{\pi_2(x, y)} \right) = \left( \begin{array}{c} x^3 + x + y^3 \\ x^3 + x^2y + xy^2 + y \end{array} \right)
\]

is a bijection.

**Proof.** We are going to show that for every \( c, d \in K \) there is at most one pair \( (x, y) \in K^2 \) such that

\[
g_1(x, y, d^2) := x^3 + x + y^3 + d^2 = 0 \quad (5.1)
g_2(x, y, c^2) := x^3 + x^2y + xy^2 + y + c^2 = 0 \quad (5.2)
\]

proving that the function \( \pi \) is injective, and thus bijective as a mapping from a finite set onto itself.

We consider zeros of the resultant of these equations with respect to \( y \). We will prove that there is always a unique solution \( x \) such that \( \text{res}(g_1, g_2, y) = 0 \).

As \( \gcd(3, 2^r - 1) = 1 \) for every fixed \( x \), equation (5.1) yields to a unique \( y \), this will prove the lemma.

The resultant is given by the following equation.

\[
\text{res}(g_1, g_2, y) = (c^4 + c^2d^2 + d^4)x^3 + c^2x^2
\]

\[
+ (c^2d^2 + d^4 + 1)x + c^6 + c^4d^2 + c^2d^4 + d^6 + d^2
\]

To simplify the notation we denote \( \gamma = c^2 + cd + d^2 \). I.e.

\[
\text{res}(g_1, g_2, y) = \gamma^2x^3 + c^2x^2
\]

\[
+ (c^2d^2 + d^4 + 1)x + c^6 + (\gamma^2 + 1)d^2 \quad (5.3)
\]
Remark that $\gamma = 0$ if and only if $c = d = 0$ or

$$\left(\frac{c}{d}\right)^2 + \frac{c}{d} + 1 = 0$$

which would imply $\text{tr}_K(1) = 0$, a contradiction as $r$ is odd. The case $c = d = 0$ trivially give a unique $x$ with $\text{res}(g_1, g_2, y) = 0$, so we can assume that $\gamma \neq 0$.

Replacing $x$ by $x + \left(\frac{c}{\gamma}\right)^2$, we can eliminate the quadratic term of (5.3) and get

$$0 = \gamma^2 x^3 + \left(\frac{d(c + d)(\gamma + 1)}{\gamma}\right)^2 x$$

$$+ \left(\frac{(\gamma + 1)(c^3 + c^2 d + cd^2 + c + d^3)}{\gamma}\right)^2 .$$

Assume that $d(c + d)(\gamma + 1) = 0$. We have to distinguish several cases.

1. If $d = 0$, then we conclude that $\gamma = c^2$ and

$$0 = c^4 x^3 + \left(\frac{(c^2 + 1)(c^3 + c)}{c^2}\right)^2 .$$

By assumption $c = \gamma \neq 0$ and, as 3 is coprime to $2^r - 1$, this gives a unique solution $x$.

2. If, on the other hand, $c = d \neq 0$, we see that $\gamma = c^2$ again an

$$0 = c^4 x^3 + \left(\frac{(c^2 + 1)c}{c^2}\right)^2$$

so again there exist a unique solution for $x$.

3. If $\gamma + 1 = 0$ then necessarily $x = 0$.

Thus we can assume that $d(c + d)(\gamma + 1) \neq 0$. Replacing furthermore $x$ by

$$\left(\frac{d(c + d)(\gamma + 1)}{\gamma^2}\right) x$$

and dividing by the leading coefficient, we finally get the following equation

$$x^3 + x + \frac{A^2}{B} = 0,$$

where

$$A = \gamma(c^3 + c^2 d + cd^2 + c + d^3).$$
and

\[ B = d^3(c + d)^3(\gamma + 1). \]

Using a result on Dickson Polynomials presented in [20], we see that this equation has a unique solution \( x \) if and only if \( \text{tr}(B/A^2) = 0 \).

For this we note that

\[ B = d^3(d^3 + A) \]

and so

\[ \frac{B}{A^2} = \frac{d^3}{A} + \left( \frac{d^3}{A} \right)^2, \]

which proofs the uniqueness of the solution \( x \) with \( \text{res}(g_1, g_2, y) = 0 \).

Let \( n = 4r \) be an even integer where \( r \) is odd. \( L = \mathbb{F}_{2^n} \) and \( E = \mathbb{F}_{2^r} \). As \( r \) is odd the polynomial

\[ \beta^4 + \beta + 1 \quad (5.4) \]

is irreducible over \( E \) as it is irreducible over \( \mathbb{F}_2 \). We conclude that \( E[\beta] = L \). Note that \( \beta \) is a primitive element in \( \mathbb{F}_{16} \). In particular every element \( x \in L \) can be represented as

\[ x = x_3\beta^3 + x_2\beta^2 + x_1\beta + x_0 \]

with \( x_i \) in \( E \).

**Theorem 5.10.** With the notation from above let \( d = (2^r+1)^2 = 2^{2r}+2^{r+1}+1 \) and \( \alpha = \beta^5 \). The function

\[ f : L \to \mathbb{F}_2 \]

\[ f(x) = \text{tr}_L(\alpha x^d) \]

is bent. In particular \( d \) is a bent exponent.

**Proof.** The first step to prove the theorem will be to derive a representation of

\[ f(x) = \text{tr}_L(\alpha x^d) = \text{tr}_L(\beta^5(x_3\beta^3 + x_2\beta^2 + x_1\beta + x_0)^d), \]

as a function of the \( x_i \)'s. Here we note that due to (5.4)

\[ \text{tr}_{L/E}(1) = \text{tr}_{L/E}(\beta) = \text{tr}_{L/E}(\beta^2) = 0 \]

and \( \text{tr}_{L/E}(\beta^3) = 1 \) and thus,

\[ \text{tr}_L(x) = \text{tr}_{E/\mathbb{F}_2}(\text{tr}_{L/E}(x)) = \text{tr}_{E/\mathbb{F}_2}(x_3). \]
If we denote
\[ p(\beta) = x_3\beta^3 + x_2\beta^2 + x_1\beta + x_0, \]
we see that
\[ f(x) = \text{tr}_L \left( \beta^5 p(\beta^2) p(\beta^2) p(\beta) \right). \]

As \( r \) is odd, we have either \( r = 1 \mod 4 \) or \( r = 3 \mod 4 \) and \( 2^r = 2 \mod 15 \) resp. \( 2^r = 8 \mod 15 \). Thus as \( \beta \in \mathbb{F}_{16} \) we get either
\[ f(x) = \text{tr}_L \left( \beta^5 p(\beta^4) p(\beta^2) p(\beta) \right) \]
or
\[ f(x) = \text{tr}_L \left( \beta^5 p(\beta^4) p(\beta^8) p(\beta) \right). \]

These two expressions are equivalent under the linear transformation where \( \beta \) is replaced by \( \beta^3 \), and as bentness is a property invariant under linear mappings we choose w.l.o.g.
\[ f(x) = \text{tr}_L \left( \beta^5 p(\beta^4) p(\beta^2) p(\beta) \right). \]

Let \( z \) be an arbitrary element in \( L \) and \( z = z_3\beta^3 + z_2\beta^2 + z_1\beta + z_0 \) its decomposition. In order to prove that \( f \) is a bent function, we are going to prove that all the Walsh-coefficients are \( \pm 2^{n/2} \), so we have to study
\[ f^W(z) = \sum_{x \in L} \chi_L(\beta^5 x^d + zx). \]

Using the properties of the trace mapping with respect to the described decomposition, we derive the following representation (we skip the long but straightforward computation).
\[
\begin{align*}
    f(x) + \text{tr}_L(zx) &= \text{tr}_E \left( x_0^2 x_1^2 + x_0^2 x_2^2 + x_0 x_1^3 + x_0 x_2^3 + x_1 x_2 \right) \\
    &\quad + x_0 x_1 x_2^2 + x_0 x_2 x_3 + x_0 x_3^3 + x_0 z_3 \\
    &\quad + x_1 x_2 x_3^3 + x_1 x_2 x_3 + x_1 x_3^3 + x_1 z_2 \\
    &\quad + x_2 x_3^3 + x_2 z_1 + x_3 z_0 + x_3 z_3 \right).
\end{align*}
\]

Using the fact that \( \text{tr}_E(x^2) = \text{tr}_E(x) \) we can simplify this expression
\[
\begin{align*}
    f(x) + \text{tr}_L(zx) &= \text{tr}_E \left( x_1^3 x_2 + x_1^3 x_3 + x_1^2 + x_1 x_2^3 + x_1 x_2 x_3 \right) \\
    &\quad + x_1 x_2 x_3 + x_1 x_2 + x_1 x_3^3 + x_1 z_2 \\
    &\quad + x_2 x_3^3 + x_2 z_1 + x_3 z_0 + x_3 z_3 \\
    &\quad + g(x_1, x_2, x_3, z_0). \notag
\end{align*}
\]
where 
\[ g(x_1, x_2, x_3, z_3) = x_1^3 + x_1^2 x_2 + x_1 x_2^2 + x_1 + x_2^3 + x_2 + x_3^3 + z_3. \]

Furthermore if we replace \( x_1 \) by \( x_1 + x_2 \) we get
\[
f(x') + \text{tr}_L(zx') = \text{tr}_E \left( x_1^3 x_3 + x_1 x_2^3 + x_1 z_2 + x_1 + x_3 z_0 + x_3 z_3 + g_1(x_1, x_3, z_3) x_0 \\
+ g_2(x_1, x_3, z_1, z_2) x_2 \right),
\]
where 
\[ x' = x_3 \beta^3 + x_2 \beta^2 + (x_1 + x_2) \beta + x_0 \]
and \( g_1 \) and \( g_2 \) are defined like in the proof of Lemma 5.9. Thus, computing the Walsh transform we get
\[
f^W(z) = \sum_{x \in L} \chi_L(\beta^5 x^d + ax) \\
= \sum_{x' \in L} \chi_L(\beta^5 x'^d + ax') \\
= \left( \sum_{x_1, x_3 \in E} \chi_E(x_1^3 x_3 + x_1 x_2^3 + x_1 z_2 + x_1 + x_3 z_0 + x_3 z_3) \right) \\
\left( \sum_{x_0 \in E} \chi_E(g_1(x_1, x_3, z_3) x_0) \right) \\
\left( \sum_{x_2 \in E} \chi_E(g_2(x_1, x_3, z_1, z_2) x_2) \right).
\]

Using the well known fact that
\[
\sum_{y \in E} \chi_E(ay) = \begin{cases} 
0 & \text{if } a \neq 0 \\
2^r & \text{if } a = 0
\end{cases}
\]
we conclude
\[
f^W(z) = 2^{2r} \left( \sum_{(x_1, x_3) \in M} \chi_K(x_1^3 x_3 + x_1 x_2^3 + x_1 z_2 + x_1 + x_3 z_0 + x_3 z_3) \right),
\]
where
\[ M = \{ (x_1, x_3) \in E^2 \mid g_1(x_1, x_3, z_3) = 0 \text{ and } g_2(x_1, x_3, z_1, z_2) = 0 \}. \]
5.4. NIHO EXPONENTS AND STICKELBERGER’S THEOREM

In order to proof that $f$ is bent, i.e. $f^{\nu}(z) = \pm 2^r$, it is sufficient to show, that for every $z_1, z_2, z_3 \in \mathbb{F}_2^r$ the set $M$ contains exactly one element. This is covered by the Lemma 5.9, which concludes the proof.

The proof of Theorem 5.10 shows that the bent function constructed with the new exponent leads to functions in the known class of Maiorana Mc-Farland bent functions as explained below.

If we identify $L$ with $(E^2)^2$ by mapping

$$x = x_3\beta^3 + x_2\beta^2 + x_1\beta + x_0$$

to

$$\left( \begin{array}{c} x_0 \\ x_2 \\ x_3 \\ x_1 \end{array} \right),$$

and choosing the following inner product on $(E^2)$

$$\langle \left( \begin{array}{c} x_0 \\ x_2 \end{array} \right), \left( \begin{array}{c} x_1 \\ x_3 \end{array} \right) \rangle = \text{tr}_E(x_0x_1 + x_2x_3)$$

we see that the function $f(x) = \text{tr}(\alpha x^d)$ is linear equivalent to

$$f'\left( \left( \begin{array}{c} x_0 \\ x_2 \end{array} \right), \left( \begin{array}{c} x_1 \\ x_3 \end{array} \right) \right) = \langle \left( \begin{array}{c} x_0 \\ x_2 \end{array} \right), \left( \begin{array}{c} \pi_1(x_1, x_3) \\ \pi_2(x_1, x_3) \end{array} \right) \rangle + h(x_1, x_3),$$

where

$$h(x_1, x_3) = \text{tr}_E(x_1^3x_3 + x_1x_3^3 + x_1)$$

and

$$\pi(x, y) = \left( \begin{array}{c} \pi_1(x_1, x_3) \\ \pi_2(x_1, x_3) \end{array} \right)$$

as in Lemma 5.9.

5.4 Niho Exponents and Stickelberger’s Theorem

Unlike in the other parts of this chapter, we are not interested in proving that a certain exponent is a bent exponent. Here, on the contrary, we are interested in arguing, that a special class of exponents does not contain any bent exponents. This contrast is also reflected in the different technique we apply in this section.

The special class of exponents we are interested in are the so called Niho Exponents. We say an exponent $d$ is a Niho-Exponent if $d \mod 2^k - 1 = 1$, 

i.e. \( d = (2^k - 1)s + 1 \) for some integer \( s \). In Chapter 6 we will extensively study certain linear combinations of Niho-power functions.

Here we present some indications, that the only Niho-Exponent, that is a bent exponent has weight 2 and therefore corresponds to the Gold case \( 2^k + 1 \) described above.

The main tool to study these functions is Stickelberger’s Theorem on the divisibility of certain Gauss Sums. This theorem has been used by P. Langevin and P. Veron (see [30]) to derive conditions on the nonlinearity of certain bijective power functions. As we are interested in bent exponents, that means in particular that \( \gcd(d, 2^n - 1) \neq 1 \), but the technique from [30] can easily be adapted for non-bijective power mappings.

Following [30], given a power function

\[
f : \mathbb{F}_{2^n} \to \mathbb{F}_2 \\
f(x) = \text{tr}(\alpha x^d)
\]

we use the notation

\[
V_d(j) := \text{wt}(j) + \text{wt}(-jd),
\]

where \(-jd\) has to be interpreted modulo \(2^n - 1\), and

\[
v_d := \min\{V_d(j) \mid 1 \leq j \leq 2^n - 2\}
\]

and

\[
J_d := \{j \mid V_d(j) = v_d\}.
\]

The following polynomial will play an important role in our discussions.

\[
P_d(X) := \sum_{j \in J_d} X^j
\]

Remark that \( P_d(X)^2 = P_d(X) \), as for every \( j \in J_d \) the cyclotomic equivalent value \( 2j \) is in \( J_d \) as well. Consequently, if we consider \( P_d \) as a mapping, we actually get a Boolean function.

We give a straightforward generalization of Proposition 4.1 in [30]. Note that as \( f \) is not a bijection different values of \( \alpha \) may lead to function that not linear equivalent, thus we have to including the dependency on \( \alpha \) whenever \( f \) is not a bijection. This Theorem is proven using Stickelberger’s Theorem.

**Theorem 5.11.** With the notation from above all Walsh-coefficients are divisible by \( 2^{v_d} \). Moreover the Walsh-coefficient \( f^W(a) \) is exactly divisible by \( 2^{v_d} \) if and only if \( P_d(\alpha a^{-d}) \neq 0 \).
5.4. NIHO EXPONENTS AND STICKELBERGER’S THEOREM

Proof. See [30]

As a function is bent if and only if all the Walsh-Coefficients are exactly divisible by $2^k$, we see that, in the case of a bent function, the function

$$P_d : L \to \mathbb{F}_2$$

$$a \to P_d(\alpha a^{-d})$$

must be constant. More precisely

Lemma 5.12. Let $f(x) = \text{tr}(\alpha x^d)$ be a bent function. Then

$$v_d \leq k.$$

Furthermore

1. If $v_d < k$ then $P_d(\alpha a^{-d}) \equiv 0$.
2. If $v_d = k$ then $P_d(\alpha a^{-d}) \equiv 1$.

With respect to Theorem 5.11, Lemma 5.12 and Proposition 5.14 it makes sense to distinguish the case where the mapping $x \to P_d(\alpha x^d)$ is constant for every $\alpha$, from the case where only for some $\alpha$ the mapping $x \to P_d(\alpha x^d)$ is constant. We call an exponent $d$ locally constant if there exist an $\alpha$, such that $P_d(\alpha x^d)$ is constant, while an exponent $d$, where $P_d(\alpha x^d)$ is constant for all $\alpha$, is called globally constant.

With this notation, we see that if $d$ is a bent exponent, then $d$ is (at least) locally constant. Furthermore based on computer experiments we state the following conjecture.

**Conjecture 5.13.** All locally constant exponents are globally constant. In particular if $d$ is a bent exponent, then $d$ is globally constant.

The next Proposition demonstrates the importance of the notation of globally constant exponents in connection with Stickelberger’s Theorem.

**Proposition 5.14.** An exponent $d$ is globally constant if and only if $jd = 0 \mod 2^n - 1$ for all $j \in J_d$.

**Proof.** If $jd = 0 \mod 2^n - 1$ for all $j \in J$ than clearly $P(\alpha x^d)$ is constant for all $\alpha$. So we now assume that $d$ is globally constant. We denote

$$J_d^s = \{ j \in J_d | jd = s \mod 2^n - 1 \}$$
We compute
\[ P_d(\alpha x^d) = \sum_{j \in J_d} \alpha_j x^{jd} = \sum_{0 \leq s < 2^n} \sum_{j \in J_d^s} \alpha_j x^{jd} \]
\[ = \sum_{j \in J_d^0} \alpha_j + \sum_{0 < s < 2^n} \left( \sum_{j \in J_d^s} \alpha_j \right) x^s. \]

It follows that for all \( 0 < s < 2^n \) and for all \( \alpha \)
\[ \sum_{j \in J_d^s} \alpha_j = 0. \]

which can only be true if \( J_d^s = \emptyset \) for all \( s \neq 0 \), which proves the Proposition. \( \square \)

The condition that \( jd = 0 \mod 2^n - 1 \) for all \( j \in J_d \) makes the handling of the values \( \text{wt}(j) + \text{wt}(-jd) \), which in general is very difficult, much easier. This will be the key to our main result.

**Theorem 5.15.** If \( d = (2^k - 1)s + 1 \) is a globally constant exponent then \( \text{wt}(d) = 2 \), i.e. the only globally constant exponent corresponds to the Gold Case.

The two following Lemmas will be used in the proof of our main theorem.

**Lemma 5.16.** For all \( r \neq 0 \mod 2^k + 1 \) we have \( \text{wt}((2^k - 1)r) = 2^k \).

**Proof.** Consider the mapping
\[ g : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2, \quad g(x) = \text{tr}(x^{2^k-1}) \]
which is constant on \( u\mathbb{F}_{2^k}^* \) for all \( u \). If \( r \neq 0 \mod 2^k + 1 \), then there exists an element \( v \neq 0 \) with \( \text{tr}(v^{2^k-1}) \neq 0 \), and so \( g \) restricted to \( v\mathbb{F}_{2^k} \) has degree \( k \), and thus the degree of \( g \) is at least \( k \). On the other hand as \( g \) is the sum of function of degree \( k \), the degree of \( g \) is at most \( k \), which proof the claim. \( \square \)

**Lemma 5.17.** Let \( \text{wt}(d) = t \geq 2 \) then \( V(2^k - 2^{t-1} + 1) = k. \)

**Proof.** As \( \text{wt}(2^k - 2^{t-1} + 1) = k - t + 2 \), we have to prove that \( \text{wt}(d(2^k - 2^{t-1} + 1)) = t - 2 \). We compute
\[ d(2^k - 2^{t-1} + 1) = 2^{t-1}d - (2^k + 1) \]
So it is sufficient to show that \( wt(d - 2^{n-t+1} - 2^{k-t+1}) = wt(d) - 2 \), i.e. that in the binary expansion of \( d \), the \((n-t+1)\)th and the \((k-t+1)\)th bit are 1. If \( wt(d) = wt((2^k - 1)s + 1) = t \), as \( wt((2^k - 1)s) = k \), we see that the \((k-t+1)\)th bit of \( d = 1 \). As the binary expansion of \((2^k - 1)s\) for \( s \neq 0 \mod 2^k + 1 \), is always of the form \( a\overline{a} \), we see that also the \((n-t+1)\)th bit is 1, as the \((k-t+1)\)th bit of \( d + 1 = (2^k - 1)s \) is 0.

**Proof of Theorem 5.15.** We are going to prove that whenever \( wt(d) \neq 2 \) then \( d \) is not globally constant.

We denote
\[
\tilde{v}_d := \min \{ V_d(j) \mid jd = 0 \mod 2^n - 1 \}
\]
and
\[
\tilde{J}_d := \{ j \mid V_d(j) = \tilde{v}_d \text{ and } jd = 0 \mod 2^n - 1 \}
\]
We are going to prove that \( \tilde{v}_d = k \) and that there exists a \( j \) such that \( V(j) = k \), but \( j \not\in \tilde{J}_d \). This will prove the Theorem using Proposition 5.14, as if \( v_d < \tilde{v}_d \), the exponent is clearly not globally constant.

If \( jd = 0 \mod 2^n - 1 \), as \( d = 1 \mod 2^k - 1 \), we see that \( j = 0 \mod 2^k - 1 \) and so \( j = (2^k - 1)r \) for some \( r \). From Lemma 5.16 it follows immediately that \( \tilde{v}_d = k \). Lemma 5.17 shows that for \( j_0 = 2^k - 2^{t-1} + 1 \) we have \( V(j_0) = k \). On the other hand \( j(2^k - 2^{t-1} + 1) = 0 \mod 2^n - 1 \) if and only if \( t = 2 \). We see that the exponent is not globally constant if \( wt(d) > 2 \), which concludes the proof of the Theorem.

A proof of Conjecture 5.13 would confirm that the only Niho-Type Exponent, that yields to a bent function is the well known Gold-Case.
CHAPTER 5. MONOMIAL BENT FUNCTIONS
Chapter 6

Binomial Bent Functions

6.1 Introduction

The natural step forward, after looking at monomial bent functions, is to consider Boolean functions constructed via a linear combination of several power functions. Taking this approach to the limit means looking again at general Boolean functions and, as a general classification of bent functions is elusive today, we concentrate (with the exception of the construction presented in Section 6.7) on linear combinations of two power functions.

Very little is known in this case, so a first step in finding examples of such bent functions is to search for concrete examples, using computer algorithms. In general, due to the complexity of the problem, these computer experiments are strictly limited to small values of $n$. Thus, it makes sense to further constrict our focus.

In the this chapter we study traces of a linear combination of Niho power functions. Recall that power function on $\mathbb{F}_{2^n}$ is called a Niho power function if its restriction to $\mathbb{F}_{2^k}$ is linear. The considered functions are therefore weakly normal. In this way, under certain conditions, we get as our main results (Theorems 6.1, 6.2 and 6.3) three primary constructions of bent functions as linear combinations of two Niho power functions. Theorem 6.2 actually belongs to a more general class of bent functions, discussed in section 6.7. One advantage of focusing on Niho power functions is, that the classical theorem of Niho [35] serves as a starting point for proving our results. Furthermore we make use of new methods to handle Walsh transforms of Niho power functions from [25].

We introduce a new general method to prove that certain rational functions are one-to-one. This technique follows the sprit of the multivariate method introduced by Dobbertin (see [23]), in the sense that the rational
functions considered here introduce one-to-one mappings on an infinite chain of finite fields. This is also reflected in the techniques developed here which, like with the multivariate method, mainly manipulate generic properties of the discussed mappings. Another similarity is, that some of these manipulations can only be treated with the help of computer algebra packages.

**Niho power functions.** Recall that we say $d$ (always understood modulo $2^n - 1$) is a *Niho exponent* and $x^d$ is a *Niho power function*, if the restriction of $x^d$ to $\mathbb{F}_{2^k}$ is linear or in other words

$$d \equiv 2^i \pmod{2^k - 1}$$

for some $i < n$. Without loss of generality we can assume that $d$ is in the *normalized form* with $i = 0$, and then we have a unique representation

$$d = (2^k - 1)s + 1$$

with $2 \leq s \leq 2^k$, because here $s$ and $s'$ give the same power function $d$ on $\mathbb{F}_{2^n}$ iff $s \equiv s' \pmod{2^k + 1}$.

The conjugated exponent corresponding to a normalized $d = (2^k - 1)s + 1$, i.e. $d' = 2^kd$, is of the same type, where $s$ has to be replaced by $1 - s$ (mod $2^k + 1$):

$$2^kd = (2^k - 1)(1 - s) + 1 \pmod{2^n - 1}.$$ 

From this point of view we see that there are two equivalent ways to normalize a Niho exponent. The sum of the corresponding two values for $s$ equals 1 (modulo $2^k + 1$).

The inverse of a Niho exponent, if it exists, is again of Niho type: in fact for $d = (2^k - 1)s + 1$ we have $\gcd(d, 2^n - 1) = 1$ if and only if $2s - 1$ is invertible modulo $2^k + 1$, i.e. $\gcd(2s - 1, 2^k + 1) = 1$, and in this case

$$d^{-1} = (2^k - 1)s' + 1 \pmod{2^n - 1}, \quad s' = s/(2s - 1) \pmod{2^k + 1}$$

since $d((2^k - 1)s' + 1) = -2(-2ss' + s + s') + 1 = 1 \pmod{2^k + 1}$.

**Convention.** If some $s$, used to define a Niho exponent as above, is written as a fraction, then this has to be interpreted modulo $2^k + 1$. For instance

$$s = \frac{1}{2} = 2^{k-1} + 1.$$
6.2. MAIN RESULTS

6.2 Main Results

Let $L = \mathbb{F}_{2^n}$ and $n = 2k$. We consider Boolean functions

$$f(x) = \text{tr}_L(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$$

on $L$, for $\alpha_1, \alpha_2 \in L$, where the $d_i = (2^k - 1)s_i + 1$, $i = 1, 2$, are Niho exponents. We anticipate that if $f$ is bent, then necessarily w.l.o.g.

$$d_1 = (2^k - 1) \frac{1}{2} + 1.$$

This conjecture is suggested by computer experiments. In the sequel we require this choice of $d_1$. Observe that $d_1$ is cyclotomic equivalent to $2d_1 = 2^k + 1$, we have

$$x^{d_1} = \sqrt{x^2} = \text{norm } x.$$

This special choice of $d_1$ implies that replacing $\alpha_1$ by $\alpha_1'$ does not change $f$ if (and only if) $\alpha_1 + \alpha_1' \in K$.

For $\alpha_2 = 0$, we get bent functions iff $\alpha_1 \not\in K$:

$$f(x) = \text{tr}_L(\alpha_1 x^{d_1}) = \text{tr}_L(\alpha_1 \text{ norm } x) = \text{tr}_K((\alpha_1 + \overline{\alpha_1}) \text{ norm } x),$$

which belong to a trivial class of bent function, the quadratic ones. It seems that there are no more bent functions of the form $f(x) = \text{tr}_L(\alpha x^d)$ with Niho exponent $d$.

For the following theorems we require that

$$\alpha_1 + \overline{\alpha_1} = \text{norm } \alpha_2.$$

However, this general form can easily be reduced to the case $\alpha_2 = 1$, as we shall see.

**Theorem 6.1.** Define

$$d_2 = (2^k - 1) 3 + 1.$$

If $k \equiv 2 \pmod{4}$ assume that $\alpha_2 = \beta^5$ for some $\beta \in L^*$. Otherwise, i.e. if $k \not\equiv 2 \pmod{4}$, $\alpha_2 \in L^*$ is arbitrary. Then $f$ is a bent function with degree$^1$

$k$.

$^1$We identify $L = \mathbb{F}_{2^n}$ with $\mathbb{F}_{2^n}$. The binary degree of the $n$-variate polynomials representing a function of the form $\text{tr}(\alpha x^d)$, which is not identically zero, is precisely the Hamming weight $\omega(d)$ of the binary representation of $d$ (reduced modulo $2^n - 1$).
From $\omega(d_2) = \omega(2^k + (2^{k-1} - 1)) = 1 + (k - 1) = k$ we conclude that $f$, as a multi-variate binary function, has in fact degree $k$, the maximal degree a bent functions can attain.

**Theorem 6.2.** Suppose that $k$ is odd. Define

$$d_2 = (2^k - 1) \frac{1}{4} + 1.$$  

Then $f$ is a bent function of degree 3.

Observe that $d_2$ is cyclotomic equivalent to and can be replaced by

$$4d_2 = 2^k + 3.$$

From $\omega(4d_2) = 3$ we conclude that $f$ has degree 3.

**Theorem 6.3.** Suppose that $k$ is even. Define

$$d_2 = (2^k - 1) \frac{1}{6} + 1.$$  

Then $f$ is a bent function of degree $k$.

Note that

$$2d_2 = (1 + 4 + 16 + \cdots + 2^{k-2}) + 2$$

and therefore $\omega(d_2) = k/2 + 1$ and consequently $f$ has actually degree $k$.

**Remark 6.4.** The preceding theorems were conjectured based on computer experiments worked out by Canteaut, Carlet and Gaborit for $k \leq 6$. Every found example of that exhaustive search is now covered by one of our theorems.

**Remark 6.5.** The value of $s_2$ in Theorems 6.1, 6.2, 6.3 can be replaced by $1 - s_2$, resp., since this does not change the cyclotomic class. Thus the alternative values are

$$s_2 = -2, \frac{3}{4}, \frac{5}{6} \pmod{2^k + 1},$$

respectively.

**Remark 6.6.** The bent functions given by the preceding theorems for the essential case $\alpha_2 = 1$ do not depend on $\alpha_1$ and can be written as

$$f(x) = \text{tr}_K(\text{norm } x) + \text{tr}_L(x^{d_2}),$$  

for the respective $d_2$.  

\begin{equation}
(6.1)
\end{equation}
Remark 6.7. The construction of theorem 6.2 belongs to a more general class of Niho bent functions, see section 6.7 for more details.

Remark 6.8. In general, given a bent function of the form

\[ f(x) = \text{tr}_L \left( \sum_{i=1}^{m} \alpha_i x^{d_i} \right) \]

for Niho exponents \( d_i = (2^k-1)s_i+1 \) \((i = 1, \ldots, m)\), and setting \( f_\lambda(x) = f(\lambda x) \) for \( \lambda \in K \) we get a collection of bent functions, for \( \lambda \neq 0 \), such that

\[ f_\lambda + f_\mu = f_{\lambda+\mu}. \]

for all \( \lambda, \mu \in K \). Thus defining

\[ C = \{ f_\lambda : \lambda \in K \} \]

we get a \( k \)-dimensional subcode \( C \) of the Reed-Muller code \( \text{RM}(r, n) \) of order \( r = \deg f \), which consists of bent functions and the zero function.

We can put the latter observation into other terms, using the notion of a vectorial bent function. Define \( F : L \to K \) as

\[ F(x) = \text{tr}_{L/K} \left( \sum_{i=1}^{m} \alpha_i x^{d_i} \right). \]

If \( f(x) = \text{tr}_L \left( \sum_{i=1}^{m} \alpha_i x^{d_i} \right) \) is bent then all component functions of \( F \), i.e. functions of the form \( \text{tr}_K(\lambda F(x)) \), \( \lambda \in K^* \), are bent. In fact

\[
\begin{align*}
\text{tr}_K(\lambda F(x)) &= \text{tr}_K \left( \lambda \text{tr}_{L/K} \left( \sum_{i=1}^{m} \alpha_i x^{d_i} \right) \right) \\
&= \text{tr}_K \left( \text{tr}_{L/K} \left( \lambda \sum_{i=1}^{m} \alpha_i x^{d_i} \right) \right) \\
&= \text{tr}_L \left( \sum_{i=1}^{m} \alpha_i (\lambda x)^{d_i} \right) \\
&= f(\lambda x).
\end{align*}
\]

Kaisa Nyberg [36] refers to the property that all component functions of a vectorial Boolean function are bent by calling them vectorial bent functions.

Thus for the bent functions \( f \) in (6.1) above one obtains, as another way to state our main results:
CHAPTER 6. BINOMIAL BENT FUNCTIONS

**Theorem 6.9.** Let \( d = (2^k - 1)s + 1 \) be a Niho exponent. Then the vectorial Boolean function

\[
F(x) = \text{norm } x + x^d + \overline{x}^d
\]

from \( L \) onto \( K \) is bent for \( s = 3 \), for \( s = \frac{1}{3} \) if \( k \) is odd and for \( s = \frac{1}{6} \) if \( k \) is even, respectively.

Using Dickson polynomials (see page 76), the angle functions \( \varrho \) (see (2.2)) we can represent \( F \) for Theorem 6.9 also in the form

\[
F(x) = \text{norm } x \left( 1 + D_{2s-1} (\varrho(x)) \right).
\]

A vectorial bent function from \( \mathbb{F}_2^n \) to \( \mathbb{F}_2^m \) exists only if \( m \leq k = n/2 \) as shown by Kaisa Nyberg [36]. Hence the dimension of the image vector space of the \( F \) in Theorem 6.9 is maximal.

We recall the previously known constructions of vectorial bent functions. They are straightforward generalizations of classical constructions of bent functions due to Marioana-McFarland [34] and Dillon [18], respectively. A vectorial bent function \( F : K \times K \to K \) is defined by setting

\[
F(y, z) = y \pi(z) + h(z) \quad \text{(Marioana-McFarland construction)},
\]

where \( \pi \) is a permutation of \( K \) and \( h : K \to K \) is any mapping, and by setting

\[
F(y, z) = \sigma(y/z) \quad \text{(Dillon construction)}
\]

with the convention \( y/0 = 0 \), where \( \sigma \) is a permutation of \( K \) with \( \sigma(0) = 0 \).

**Remark 6.10.** Whenever a new construction of bent functions is found, the question arises, what is the structure of the corresponding dual bent functions. (For instance the constructions of Marioana-McFarland and Dillon are closed under forming duals.) We presently do not have an answer here.

### 6.3 Niho’s Theorem and Dickson Polynomials

Niho’s theorem [35] is presented below. For the reader’s convenience, we include a proof (cf. [22]).

**Theorem 6.11.** Assume that

\[
d = (2^k - 1)s + 1
\]
is a Niho exponent and
\[ f(x) = \text{tr}(x^d). \]

Then \( f^W(c) = (N(c) - 1)2^k \), where \( N(c) \) is the number of \( u \in \mathcal{S} \) such that
\[ u^{2^s-1} + \bar{u}^{2^s-1} + cu + \bar{c}u = 0, \tag{6.2} \]
for each \( c \in L = \mathbb{F}_{2^n} \).

Thus the Walsh spectrum of \( f \) is at most \( 2s \)-valued, and the occurring values are among
\[ -2^k, 0, 2^k, 2 \cdot 2^k, \ldots, (2s - 2)2^k. \]

**Proof.** Recall that every nonzero \( x \in L \) has a polar coordinate representation \( x = \lambda u \), where \( \lambda \in K = \mathbb{F}_{2^k} \) and \( u \in \mathcal{S} \). Using this and \( \text{tr}_L = \text{tr}_K \circ \text{tr}_{L/K} \), we have
\[
 f^W(c) = \sum_{z \in \mathbb{F}_{2^n}} \chi_L(cz + z^d) \\
 = 1 + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathbb{F}_{2^k}^*} \chi_L(c\lambda u + \lambda^d u^d) \\
 = 1 + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathbb{F}_{2^k}^*} \chi_L(\lambda(cu + u^d)) \\
 = 1 - \#\mathcal{S} + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathbb{F}_{2^k}} \chi_K(\lambda(cu + u^d + \bar{c}u^{-1} + u^{-d})) \\
 = -2^k + \sum_{u \in \mathcal{S}} \sum_{\lambda \in \mathbb{F}_{2^k}} \chi_K(\lambda(cu + u^{1-2s} + \bar{c}u^{-1} + u^{2s-1})) \\
 = (N(c) - 1)2^k.
\]

The same proof shows that more generally if
\[ f(x) = \text{tr}_{L} \left( \sum_{i=1}^{m} \alpha_i x^{d_i} \right) \]
for Niho exponents \( d_i = (2^k - 1)s_i + 1 \) (\( i = 1, \ldots, m \)), then \( N(c) \) is the number of solutions \( u \) in \( \mathcal{S} \) of
\[ cu + \bar{c}u + \sum_{i=1}^{m} \alpha_i u^{1-2s_i} + \sum_{i=1}^{m} \bar{\alpha}_i \bar{u}^{1-2s_i} = 0, \]
or equivalently by replacing \( u \) by \( \overline{u} \)
\[
cu + \overline{c}u + \sum_{i=1}^{m} \alpha_i u^{2^{s_1} - 1} + \sum_{i=1}^{m} \overline{\alpha_i} \overline{u}^{2^{s_1} - 1} = 0.
\]
This means for the \( f \) in Theorems 6.1, 6.2 and 6.3, where \( s_1 = \frac{1}{2} \) that the equation
\[
cu + \overline{c}u + \alpha_1 + \overline{\alpha_1} + \alpha_2 u^{2^{s_2} - 1} + \overline{\alpha_2} \overline{u}^{2^{s_2} - 1} = 0
\]
has to be considered. We assume that \( \alpha_2 = 1 \) and thus \( \alpha_1 + \overline{\alpha_1} = 1 \). (The assertion of our theorems can easily be reduced to that case, see section 6.5.) Therefore in order to confirm that \( f \) is bent, setting \( s = s_2 \) we have to show that the number of roots \( u \) in \( S \) of
\[
G_c(u) = u^{2^{s_1} - 1} + \overline{u}^{2^{s_1} - 1} + cu + \overline{c}u + 1 = 0
\]
is either 0 or 2.

**Remark 6.12.** Niho’s Theorem in combination with Parseval’s equation obviously implies that it suffices to prove that (6.4) never has exactly one solutions. Thus in the case where \( c \in K \), i.e. \( c = \overline{c} \) we can argue as follows. \( G_c(1) = 1 \), so in this case \( u = 1 \) is never a solution. Furthermore
\[
G_c(u) = u^{2^{s_1} - 1} + \overline{u}^{2^{s_1} - 1} + c(u + \overline{u}) + 1 = G_c(\overline{u}),
\]
thus whenever \( u \) is a solution of (6.4) the conjugate \( \overline{u} \) is also a solution and exactly one solution is never possible. Nevertheless for the proof of theorems 6.1 and 6.3 we explicitly show that we have either 0 or 2 solutions to demonstrate the power of our general technique.

In [25] the value distribution of the Walsh spectrum of \( \text{tr}(x^{d_2}) \) for \( d_2 = (2^k - 1)3 + 1 \) of Theorem 6.1 has been determined for odd \( k \), which requires to analyze the number of solutions of the closely related equation for \( s = 3 \):
\[
u^5 + \overline{u}^5 + cu + \overline{c}u = 0.
\]
This problem was settled with the development of new approach using Dickson polynomials [25], which will be explained below. It is also the basic tool for proving the results of the present paper.

Given \( c \in L \setminus K \) the idea of [25] is to consider \( c, \overline{c} \) and the associated equations \( G_c(u) = 0 \) and \( G_{\overline{c}}(u) = 0 \) simultaneously:
\[
G_c(u) G_{\overline{c}}(u) = 0.
\]
Then we can change from the parameters $u \in S$ and $c \in L$ to new parameters $\beta$, resp. $\gamma$, $T$ and $N$ in the small field $K$. The advantage of this procedure is that we end up with an equation where we have to count the solutions with a special “trace condition” instead of counting solutions with a “norm condition”, which turns out to be much easier.

The twins $c, \bar{c} \in L \setminus K$ are replaced by the coefficients of their (common) minimal polynomial

$$m_{c, \bar{c}} = X^2 + TX + N$$

over $K$, that is

$$T = \text{tr}_{L/K}(c) = \text{tr}_{L/K}(\bar{c}) = c + \bar{c},$$

$$N = \text{norm}_{L/K}(c) = \text{norm}_{L/K}(\bar{c}) = c\bar{c}.$$ 

Necessary and sufficient conditions for $T, N \in K$ to represent $c, \bar{c} \in L \setminus K$ in this way are $T \neq 0$ and

$$\text{tr}_K(N/T^2) = 1.$$ \hspace{1cm} (6.6)

We recall the following simple, but very important observation:

**Fact.** We have $\text{tr}_K(x) = 0$ for $x \in K$ if and only if there exists some $y \in K$ with $x = y^2 + y$.

Thus (6.6) means that $X^2 + TX + N$ is irreducible over $K$. Fortunately (6.6) can be ignored in this context, as it is included in (6.7) (see below).

Similarly $\beta$ stands for $u, \bar{u} \in S \setminus \{1\}$ in the sense that

$$m_{u, \bar{u}}(X) = X^2 + \frac{1}{\beta}X + 1.$$ 

or equivalently

$$\beta = \frac{1}{u + \bar{u}}.$$ 

A necessary and sufficient condition for $\beta$ to play this role is

$$\text{tr}_K(\beta) = 1.$$ 

Sometimes it is convenient to make also use of the parameter $\gamma$:

$$\gamma = 1/\beta.$$
Changing to the new parameters, \( G_c(u) G_{\tau}(u) \) can be transformed as follows, where \( D_i(X) \) denotes the \( i \)-th Dickson polynomial over \( \mathbb{F}_2 \):

\[
G_c(u) G_{\tau}(u) = \left( u^{2s-1} + \bar{u}^{2s-1} + cu + \bar{c}u + 1 \right) \left( u^{2s-1} + \bar{u}^{2s-1} + c\bar{u} + e\bar{u} + 1 \right) \\
= \left( u^{2s-1} + \bar{u}^{2s-1} + 1 \right)^2 + \left( u^{2s-1} + \bar{u}^{2s-1} + 1 \right) (c + \bar{c})(u + \bar{u}) \\
+ (cu + c\bar{u})(\bar{c}u + e\bar{u}) \\
= (D_{2s-1}(\gamma) + 1)^2 + (D_{2s-1}(\gamma) + 1) \gamma T + T^2 + \gamma^2 N.
\]

Dickson polynomials satisfy the functional equation

\[
D_i(X + X^{-1}) = X^i + X^{-i},
\]

the iteration rule

\[
D_i(D_j(X)) = D_{ij}(X)
\]

and can be obtained by the recursion

\[
D_{i+2}(X) = XD_{i+1}(X) + D_i(X)
\]

with \( D_0(X) = 0 \) and \( D(X) = X \). We give a list of the Dickson polynomials for \( i < 10 \):

\[
\begin{align*}
D_0(X) &= 0, \\
D_1(X) &= X, \\
D_2(X) &= X^2, \\
D_3(X) &= X^3 + X, \\
D_4(X) &= X^4, \\
D_5(X) &= X^5 + X^3 + X, \\
D_6(X) &= X^6 + X^2, \\
D_7(X) &= X^7 + X^5 + X, \\
D_8(X) &= X^8, \\
D_9(X) &= X^9 + X^7 + X^5 + X.
\end{align*}
\]

Summarizing we have seen that \( G_c(u) G_{\tau}(u) = 0 \) with \( u \in \mathcal{S} \) is equivalent to the following equation in \( \mathbb{K} \):

\[
\left( \frac{(D_{2s-1}(1/\beta) + 1)\beta}{T} \right)^2 + \frac{(D_{2s-1}(1/\beta) + 1)\beta}{T} + \beta^2 = \frac{N}{T^2}.
\]  
(6.7)

Given \( T \) and \( N \) we have to count the number of solutions \( \beta \) with trace 1 of (6.7). Now the trick is that we can look at this solution counting problem...
also in another way. Given any non-zero $T$ and $\beta$ with trace 1, we can interpret (6.7) as definition of $N$. This makes sense, because it then follows, as already mentioned above, that $\text{tr}_K(N/T^2) = \text{tr}_K(\beta) = 1$ and therefore $T$, $N$ represent $c, \tau$ via $m_{c,\tau}(X) = X^2 + TX + N$. We then have to look at the number of solutions of (6.7) different from the given $\beta$ (for more details see [25]). The special cases $T = 0$ and $T = 1$ have to be considered separately.

6.4 One-to-one Rational Functions

After these preparations, the verification of our main results will come down to the following two lemmas (to be honest, they have been found for that reason), as we shall see in the next sections.

Remark 6.13. The technique used here to prove the below Lemmas 6.14 and 6.15 is due to Dobbertin and Leander. It is in some sense similar to the multi-variate method (see [23], where the multi-variate method is described in its general form), insofar as a “generic” point of view is taken. As for the multi-variate method, also here algebraic computations are applied, which often need Computer Algebra support. Decomposition of multi-variate polynomials (with variables which are considered to be independent) and formal elimination of variables, i.e. for instance computation of resultants, as basic steps.

We briefly describe the method and roughly explain why it works. Suppose that an irreducible multi-variate polynomial $F(a, x_1, \ldots, x_m)$ is given, and that we have to show that $F(a, x_1, \ldots, x_m) = 0$ implies that $a$ has trace 0, i.e. we can represent $a = b^2 + b$ in each of the considered fields. If this fact has “generic” reasons then we can represent these “local” $b$ in a “global” way as a fixed rational function of $a, x_1, \ldots, x_m$:

$$b = R(a, x_1, \ldots, x_m) = \frac{C(a, x_1, \ldots, x_m)}{D(a, x_1, \ldots, x_m)}$$

Assume that $R$ in fact exists. Then $X = b$ is a zero of the rational function

$$(X + R(X^2 + X, x_1, \ldots, x_m))(X + 1 + R(X^2 + X, x_1, \ldots, x_m)).$$

In the generic case we can expect that this rational function is essentially, up to avoiding denominators, the polynomial

$$F(X^2 + X, x_1, \ldots, x_m),$$

which therefore factorizes in the form

$$Q(X, x_1, \ldots, x_m) Q(X + 1, x_1, \ldots, x_m).$$
Thus we consider $b$ as unknown, substitute $a = b^2 + b$ in $F$ and decompose $F$ in order to compute $Q$. We can assume that $a$ occurs in $Q$ with some odd exponent. Using then $b^2 = b + a$ we reduce $Q$ and get the polynomial $C(a, x_1, ..., x_m) + D(a, x_1, ..., x_m)b$, which gives $R = C/D$. Common zeros of $C$ and $D$ need an extra discussion.

Given a concrete field $K$ of characteristic 2, we find $b \in E$ with $a = b^2 + b$ in some extension field $E$ of $K$. Thus if $F(a, x_1, ..., x_m) = 0$ for $a, x_1, ..., x_m \in K$, then our generic result implies that $b = R(a, x_1, ..., x_m)$ and therefore $b \in K$, i.e., $\text{tr}_K(a) = 0$.

This simple machinery, which works of course for any non-zero characteristic, will turn out to be very powerful and effective.

Define

$$T_\varepsilon = \{x \in K : \text{tr}_K(x) = \varepsilon\}, \quad \varepsilon \in \mathbb{F}_2.$$

**Lemma 6.14.** Let $K$ be any finite field of characteristic 2. Then the rational functions

$$\Phi(x) = \frac{1}{x^4} + \frac{1}{x^2} + x$$

and

$$\Psi(x) = \frac{1}{x^8} + \frac{1}{x^2} + x,$$

respectively, induce a permutation of $T_1$.

**Proof.** The proof is essentially the same for both rational functions. We consider first $\Phi(x) = 1/x^4 + 1/x^2 + x$. Note that

$$\text{tr}(\Phi(x)) = \text{tr}(1/x^4) + \text{tr}(1/x^2) + \text{tr}(x) = \text{tr}(1/x) + \text{tr}(1/x) + \text{tr}(x) = \text{tr}(x).$$

Thus $\Phi$ maps $T_\varepsilon$ into itself. It remains to confirm that for $\Delta \neq 0$

$$\Phi(x + \Delta) = \Phi(x)$$

implies $\text{tr}(x) = 0$. We have $\Phi(x) = U(x)/V(x)$ with polynomials $U(x) = x^5 + x^2 + 1$ and $V(x) = x^4$. Substituting $x^2 = y^2 + y$ the idea is to represent $y$ as a rational function of $x$ and $\Delta$ as described above\(^2\). We see that the polynomial

$$(\Phi(x + \Delta) + \Phi(x))V(x + \Delta)V(x) = U(x + \Delta)V(x) + U(x)V(x + \Delta)$$

\(^2\text{We take } x^2 = y^2 + y \text{ instead of } x = y^2 + y, \text{ since here } U(x + \Delta)V(x) + U(x)V(x + \Delta) \text{ is a polynomial in } x^2.\)
factorizes in the form

\[ \Delta Q(\Delta, y) Q(\Delta, y + 1) \]

with

\[ Q(\Delta, y) = y^4 + y^3 + \Delta^2 y^2 + \Delta y + \Delta^2. \]

On the other hand we can write \( Q \) uniquely as

\[ Q(\Delta, y) = C(\Delta, x^2) + D(\Delta, x^2)y \]

with polynomials \( C \) and \( D \). In fact to compute \( C \) and \( D \), reduce \( Q \) modulo \( y^2 = y + x^2 \). Here we have

\[ C(\Delta, x) = x^2 + \Delta^2(x + 1), \]

\[ D(\Delta, x) = x + \Delta^2 + \Delta. \]

Summarizing we conclude for \( \Delta \neq 0 \) that \( \Phi(x + \Delta) = \Phi(x) \) implies \( Q(\Delta, y) = 0 \) w.l.o.g., thus \( x^2 = y^2 + y \) for \( y = C(\Delta, x^2)/D(\Delta, x^2) \). Hence \( y \in K \) and \( \text{tr}(x) = 0 \). It remains to confirm that \( C(\Delta, x) \) and \( D(\Delta, x) \) have no common zeros \( x \) in \( T_1 \), which is trivial in our case, since already \( D(\Delta, x) = 0 \) implies \( \text{tr}(x) = 0 \).

The other rational function \( \Psi(x) = 1/x^8 + 1/x^2 + x \) can be handled in precisely the same way. Here \( U(x) = x^9 + x^6 + 1 \) and \( V(x) = x^8 \). This leads to

\[ Q(\Delta, y) = y^8 + \Delta y^5 + (\Delta^4 + \Delta^2 + 1)y^4 \]
\[ + (\Delta^3 + \Delta^2 + \Delta)y^3 + \Delta^3 y^2 + \Delta^3 y + \Delta^4 \]
\[ C(\Delta, x) = x^4 + (\Delta^4 + \Delta^2)x^2 + \Delta^4 x + \Delta^4, \]

\[ D(\Delta, x) = \Delta(x^2 + (\Delta^2 + \Delta)x + \Delta^3 + \Delta^2). \]

\( C(\Delta, x) \) and \( D(\Delta, x) \) have a common zero \( \Delta \) if and only if the resultant \( \text{res}(C, D, \Delta) \) of \( C \) and \( D \) with respect to \( \Delta \) is zero. In this case we have

\[ \text{res}(C, D, \Delta) = x^{14}, \]

which is non-zero. In general it suffices here to get a contradiction by showing that the zeros of resultant have trace 0.

\[ \square \]

**Lemma 6.15.** Let \( K \) be any finite field of characteristic 2 and suppose that \( a \in K \) has absolute trace 1. Then the rational functions

\[ R_a(x) = \frac{(x + 1)(ax^4 + x^3 + ax^2 + x + a^2)(ax^4 + x^3 + (a + 1)x^2 + a^2)}{x(x^4 + x^2 + a)(x^2 + a^2)} \]
CHAPTER 6. BINOMIAL BENT FUNCTIONS

and

\[ S_a(x) = \frac{1}{x} + \frac{x^2 + x}{a(a + x^4 + x^2)}, \]

respectively, induce a permutation of \( K \setminus \mathbb{F}_2 \).

**Proof.** We first consider \( R_a \). Let \( U_a(x) \) and \( V_a(x) \) denote the nominator and denominator polynomial of \( R_a(x) \), respectively. \( V_a(x) \) is non-zero for non-zero \( x \), since \( \text{tr}(a) = 1 \). We note that \( R_a(x) \) can be written as

\[
R_a(x) = \frac{\Phi(\sqrt{a} + x^2 + x) + \Phi(\sqrt{a})}{x^2}
\]  

with \( \Phi \) (see Lemma 6.14) defined as

\[
\Phi(x) = \frac{1}{x^4} + \frac{1}{x^2} + x.
\]

Thus \( R_a(x) \) is non-zero for \( x \notin \mathbb{F}_2 \), since \( \Phi \) is one-to-one on \( T_1 \) by Lemma 6.14 and \( a, a + x^2 + x \in T_1 \).

To confirm that \( R_a \) is one-to-one, we argue as before. Suppose on the contrary that \( R_a(x) = R_a(y) \) for \( x, y \notin \mathbb{F}_2, x \neq y \). We have to present \( a = b^2 + b \) in \( K \) to get a contradiction to \( \text{tr}(a) = 1 \). Substituting \( a = b^2 + b \), the polynomial

\[
(R_a(x) + R_a(y)) V_a(x)V_a(y) = U_a(x)V_a(y) + U_a(y)V_a(x)
\]

factorizes in the form

\[
a^2 (x + y) Q(b, x, y) Q(b + 1, x, y)
\]

with

\[
Q(b, x, y) = b^6 + (x + y)^3 b^4 + xy(x + y)b^3 + (xy(x + y)^3 + (x + 1)^4(y + 1)^4 + x^2y^2)b^2 + x^2y^2(x + y)(xy + x + y)b + x^2(xy + 1)^2y^2(y + 1)^2.
\]

Reducing \( Q \) modulo \( b^2 = b + a \) we get

\[
Q(b, x, y) = C(a, x, y) + D(a, x, y)b
\]

with

\[
C(a, x, y) = a^3 + (x + y + 1)^4a^2 + xy(xy + x + y)(xy(x + y) + (x + 1)^2(y + 1)^2)a + x^2(x + 1)^2y^2(y + 1)^2,
\]

\[
D(a, x, y) = a^2 + xy(x + y)a + xy(x + 1)^2(y + 1)^2(xy + x + y).
\]
6.4. ONE-TO-ONE RATIONAL FUNCTIONS

Summarizing we conclude for \( x \neq y \) that \( R_a(x) = R_a(y) \) implies \( Q(b, x, y) = 0 \) w.l.o.g., thus \( a = b^2 + b \) for \( b = C(a, x, y)/D(a, x, y) \). It remains to confirm that \( D(a, x, y) \) has no zeros \( a \) in \( \mathbb{T}_1 \). On the contrary, suppose \( D(a, x, y) = 0 \).

Then \( C(a, x, y) = 0 \) and \( \text{res}(C, D, a) = 0 \). Here we have

\[
\text{res}(C, D, a) = x^2(x + 1)^6y^2(y + 1)^6(x + y)^2(x + y + 1)^6.
\]

Consequently \( x + y + 1 = 0 \), because \( x, y \not\in \mathbb{F}_2 \) and \( x \neq y \). On the other hand, from \( C = D = 0 \) we get \( a \) as a rational function in \( x \) and \( y \), in our case

\[
a = \frac{xy(x + 1)^2(y + 1)^2}{x^2 + xy + y^2 + 1}.
\]

A substitution of \( y = x + 1 \) yields \( a = x^4 + x^2 \), which implies that \( \text{tr}(a) = 0 \), a contradiction.

It remains to show that \( R_a \) does not attain the value 1. Conversely assuming \( R_a(x) = 1 \), i.e. \( U_a(x) = V_a(x) \) we have to conclude that \( a \) has trace 0. To this end we apply the same technique as before and substitute \( a = b^2 + b \). Then the polynomial \( U_a(x) + V_a(x) \) factorizes

\[
U_a(x) + V_a(x) = Q(b, x)Q(b + 1, x)
\]

with

\[
Q(b, x) = b^4 + (x^4 + x + 1)b^2 + (x^3 + x^2)b + x^3 + x.
\]

For \( C \) and \( D \) satisfying \( Q = C + Db \) we compute

\[
C(a, x) = a^2 + (x^4 + x)a + x^3 + x,
\]
\[
D(a, x) = x(x + 1)^3.
\]

Now \( C = 0 \) contradicts our assumption \( x \not\in \mathbb{F}_2 \).

To confirm that \( S_a \) is one-to-one we compute in the same way as before for \( R_a \):

\[
Q(b, x, y) = b^3 + (x + y)^2b^2 + (x + 1)(y + 1)^2b + xy(x + y + 1),
\]
\[
C(a, x, y) = (x + y + 1)^2a + xy(x + y + 1),
\]
\[
D(a, x, y) = a + x^2y^2,
\]
\[
\text{res}(C, D, a) = xy(x + y + 1)(x + 1)(y + 1).
\]

Thus \( a = x^4 + x^2 \), a contradiction.

To show that \( S_a(x) \in \mathbb{F}_2 \) is impossible the same method works. We leave the details to the reader. \( \square \)
6.5 Proof of Theorem 6.1

Let \( d_2 = (2^k - 1) 3 + 1 \), then obviously \( \gcd(d_2, 2^n - 1) = \gcd(5, 2^k + 1) \) equals 5 for \( k \equiv 2 \pmod{4} \) and it equals 1 for \( k \not\equiv 2 \pmod{4} \). Thus, in both cases, there is an element \( b \) in \( \mathbb{F}_{2^n} \) with \( \alpha_2 b^{d_2} = 1 \). Therefore

\[
\text{norm} \alpha_2 \text{norm} b^{d_2} = \text{norm} \alpha_2 b^{d_1 d_2} = \text{norm} \alpha_2 \text{norm} b^{d_2} = \text{norm} \alpha_2 \text{norm} b = 1,
\]

and the substitution \( x \leftarrow bx \) in \( f(x) \) gives

\[
f(bx) = \text{tr}_L (\alpha_1 \text{norm} bx + \alpha_2 (bx)^{d_2}) = \text{tr}_L \left( \frac{\alpha_1}{\text{norm} \alpha_2} \text{norm} x + x^{d_2} \right).
\]

Now the general case \( \alpha_1 + \alpha_1 = \text{norm} \alpha_2 \) for Theorem 6.1 follows from \( \alpha_2 = 1 \) and \( \alpha_1 + \overline{\alpha_1} = 1 \).

Using Niho’s theorem (Theorem 6.11) in order to confirm Theorem 6.1 we have to prove that, for all \( c \in L = \mathbb{F}_{2^n}, n = 2k \), the number of \( u \in S \) such that

\[
G_c(u) = u^5 + \overline{u}^5 + cu + \overline{c}u + 1 = 0
\]

is either 0 or 2 (see (6.4)). Recall that

\[
S = \{ u \in L : u\overline{u} = 1 \},
\]

\( K = \mathbb{F}_{2^k} \), and \( x \in K \) iff \( x \in L \) and \( x = \overline{x} = x^{2^k} \). We shall apply the approach described in Section 4. Recall that

\[
\beta = 1/(u + \overline{u}), \quad \text{tr}(\beta) = 1,
\]

\[
T = c + \overline{c},
\]

\[
N = c\overline{c}.
\]

Case 1: \( T = 0 \), i.e. \( c \in K \). Then \( G_c(u) = 0 \) iff

\[
u^5 + \overline{u}^5 + c(u + \overline{u}) = 1
\]

i.e. iff

\[
c = D_5(1/\beta)\beta + \beta = 1/\beta^4 + 1/\beta^2 + 1 + \beta,
\]

where \( D_5(X) = X^5 + X^3 + X \) denotes the 5-th Dickson polynomial. Thus given \( c \) we have no or precisely two solutions \( u \in S \) of \( G_c(u) = 0 \) if and only if

\[
\beta \mapsto \Phi(\beta) = 1/\beta^4 + 1/\beta^2 + \beta
\]

is one-to-one for \( \beta \in T_1 \), the set of elements in \( K \) with trace 1, which is true by Lemma 6.14. (For further details concerning this approach see [25] in Section 4, Case 1 especially.)
Case 2a: \( T = 1 \). Note that this case occurs if and only if \( u = 1 \) is a solution of \( G_c(u) = 0 \). Then on the other hand \( G_c(u) G_{c\bar{u}}(u) = 0 \) with \( u \neq 1 \) iff
\[
c\bar{c} = \Psi(\beta) = 1/\beta^8 + 1/\beta^2 + \beta,
\]
where \( \beta = 1/(u + \overline{u}) \in K \) and therefore \( \text{tr}_K(\beta) = 1 \), see (6.7). Arguing as before in Case 1 we have to show that \( \Psi \) is one-to-one on \( T_1 \), which is true by Lemma 6.14. The two solutions of \( G_c(u) = 0 \) and \( G_{c\bar{u}}(u) = 0 \) are \( u = 1 \) and \( u = u_0 \), respectively \( u = 1 \) and \( u = \overline{u_0} \), where \( \beta_0 = 1/(u_0 + \overline{u_0}) \) is the unique solution of (6.9) with trace 1.

Case 2b: \( T \not\in F_2 \). By (6.7) we have
\[
N = T^2\beta^2 + \Phi_1(\beta) T + \Phi_1(\beta)^2,
\]
with
\[
\Phi_1(\beta) := (D_5(1/\beta) + 1) \beta = \Phi(\beta) + 1.
\]
We have to show that for each \( T \not\in F_2 \)
\[
\beta \mapsto T^2\beta^2 + \Phi_1(\beta) T + \Phi_1(\beta)^2
\]
maps two-to-one for \( \beta \in T_1 \). (For details concerning this approach we refer again to [25], Section 4, Case 2 in particular.) In other words, since \( u = 1 \) is impossible (see Case 2a above), given \( T \not\in F_2 \) and \( \beta \) with \( \text{tr}_K(\beta) = 1 \) we have to show that there is a unique non-zero \( \Delta \) with \( \text{tr}_K(\Delta) = 0 \) and
\[
T^2\beta^2 + \Phi_1(\beta) T + \Phi_1(\beta)^2 = T^2(\beta + \Delta)^2 + \Phi_1(\beta + \Delta) T + \Phi_1(\beta + \Delta)^2
\]
that is
\[
\Delta^2 = (\Phi_1(\beta + \Delta) + \Phi_1(\beta)) / T + (\Phi_1(\beta + \Delta) + \Phi_1(\beta))^2 / T^2.
\]
Setting \( \Delta = x^2 + x \), this means that
\[
x^2 + (\Phi_1(\beta + x^2 + x) + \Phi_1(\beta)) / T + \varepsilon = 0,
\]
or equivalently
\[
T = \frac{\Phi_1(\beta + x^2 + x) + \Phi_1(\beta)}{x^2 + \varepsilon}
\]
for an unique set \( \{x, x + 1\} \) and \( \varepsilon \in F_2 \). The pairs \( (x, \varepsilon) \) and \( (x + 1, \varepsilon + 1) \) give the same \( T \). Hence w.l.o.g. we can choose \( \varepsilon = 0 \). Then the right hand rational function of equation (6.11) coincides with \( R_a(x) \) for \( a = \beta^2 \), since \( \Phi_1(\beta) = \Phi(\beta) + 1 \), see (6.8). Thus the existence of an unique non-zero \( \Delta = x^2 + x \) for given \( T \) and \( \beta \) is guaranteed in view of Lemma 6.15. This completes the proof that the Boolean function \( f \) in Theorem 6.1 is bent.
6.6 Proof of Theorem 6.3

Let $k$ be even. Hence $\frac{1}{3}$ (mod $2^k + 1$) exists. Again w.l.o.g. we can assume that $\alpha_1 + \overline{\alpha_1} = 1$ and $\alpha_2 = 1$, because $d_2$ is invertible. (In fact $s_2 = \frac{1}{6}$ and therefore $2s_2 - 1 = -\frac{2}{3}$, which is invertible modulo $2^k + 1$; see Section 4.)

Since $s_1 = \frac{1}{2}$ and $s_2 = \frac{1}{6}$, by Niho’s theorem, we have $G_c(u) = cu + \overline{cu} + u^2 + \overline{u}^3 + 1$. Taking third powers is one-to-one on $S$. Thus $G_c(u)$ can be replaced by

$$G_c(u) = cu^3 + \overline{cu}^3 + u^2 + \overline{u}^2 + 1.$$ 

In what follows parameters $\gamma$, $\beta$, $T$ and $N$ are used, which are defined as before.

**Case 1:** $c \in K$. Then $G_c(u) = 0$ is equivalent to

$$(c + \beta) (\beta^2 + 1) = 0$$

Note that $\beta \neq 1$, since $\text{tr}_K(\beta) = 1$, but $\text{tr}_K(1) = 0$ ($k$ is even). Hence $c = \beta$, and we have at most one solution as desired.

**Case 2:** $c \not\in K$. We consider $G_c(u) G_{\overline{c}}(u) = 0$, which becomes after substitution the following equation in $K$:

$$\gamma^4 + 1 + (\gamma^2 + 1) D_3(\gamma) T + D_3(\gamma)^2 N + T^2 = 0,$$

where $D_3(X) = X^3 + X$ denotes the 3-rd Dickson polynomial. (This is of course also included in the general formula (6.7).) Using the iteration rule $D_i(D_j(X)) = D_{ij}(X)$ for Dickson polynomials, here with $i = 3$ and $j = 2/3$, it follows if $\beta$ is replaced by $1/D_3(\gamma)$.) In term of $\beta$ we get

$$F_T(\beta) := \beta^2 + T \beta + \frac{\beta^6}{\beta^4 + 1} T^2 = N,$$

where $\gamma = \frac{1}{2}$ and $s_2 = \frac{1}{6}$, by Niho’s theorem, we have $G_c(u) = cu + \overline{cu} + u^2 + \overline{u}^3 + 1$. Taking third powers is one-to-one on $S$. Thus $G_c(u)$ can be replaced by

$$G_c(u) = cu^3 + \overline{cu}^3 + u^2 + \overline{u}^2 + 1.$$ 

In what follows parameters $\gamma$, $\beta$, $T$ and $N$ are used, which are defined as before.

**Case 2a:** $c + \overline{c} = 1$. If $T = 1$ then the preceding equation becomes

$$F_1(\beta) = \beta^2 + \beta + \frac{\beta^6}{\beta^4 + 1} = N.$$ 

We have to show that $F_1$ is one-to-one on $T_1$, the set of all elements in $K$ with trace 1. This is in fact a consequence of Lemma 6.14, since $\text{tr}_K(1) = 0$ and

$$F_1(\beta + 1) = 1/\beta^4 + 1/\beta^2 + \beta + 1 = \Phi(\beta) + 1.$$
Case 2b: $T \not\in \mathbb{F}_2$. We have to show that for each $\beta$ and $T$, there is precisely one non-zero $\Delta$ with trace 0 such that $F_T(\beta) + F_T(\beta + \Delta) = 0$. We argue as in the proof of Theorem 6.1 in Case 2b. In the present case, we can reduce the latter statement to the fact that $S_\alpha$ in Lemma 6.15 induces a permutation of $K \setminus \mathbb{F}_2$. This completes the proof of Theorem 6.3.

6.7 Niho Bent Functions with $2^t$ Terms

In this section we present a construction of bent functions as linear combinations, not only consisting of two, but of $2^r$ many Niho exponents for any $r$ coprime to $k$. This construction covers as a special case Theorem 6.2. A bent function consisting of 4 Niho exponents was conjectured by Alexander Kholosha based on computer experiments. This construction is also included in the general form given here.

**Theorem 6.16.** Given $r \in \mathbb{N}$ with $\gcd(r, k) = 1$ and $\alpha \in L$ with $\alpha + \alpha^{2^r} = 1$.

Furthermore let

$$d_i = (2^k - 1)s_i + 1 \quad 1 \leq i < 2^{r-1}$$

be a set of Niho-Exponents. Then

$$f : L \to \mathbb{F}_2$$

with

$$f(x) = \text{tr} \left( \alpha x^{2^r+1} + \sum_{i=1}^{2^{r-1}-1} x^{d_i} \right)$$

is bent.

**Proof.** We have to study the equation

$$G_c(u) = cu + c\overline{u} + 1 + \sum_i u^{2s_i-1} + \sum \overline{u}^{2s_i-1}$$

where

$$s_i = \frac{i}{2^r} \mod 2^k + 1.$$

We denote $a = 2^{r-1}$. Replacing $u$ by $u^a$ leads to

$$G_c(u^a) = cu^a + c\overline{u}^a + 1 + \sum_{i=1}^{2^{r-1}-1} (u^a)^{2s_i-1} + \sum \overline{u}^{2s_i-1}$$

$$= cu^a + c\overline{u}^a + 1 + \sum_{i=1}^{2^{r-1}-1} \overline{u}^i + \sum_{i=1}^{2^{r-1}-1} u^i$$

$$= cu^a + c\overline{u}^a + 1 + \frac{u^a + u}{u + 1} + \frac{\overline{u}^a + \overline{u}}{\overline{u} + 1}$$
Again have to show that this equation has either 0 or 2 solutions, or due to Parsevals-Equation never 1 solution.

**Case 1:** $c \in K$. We have

$$G_c(u^a) = G_c(\overline{u}^a)$$

so as $G_c(1) \neq 0$ in this case we never have one solution.

**Case 2:** $c \notin K$. We consider as above

$$G_c(u^a)G(\overline{u}^a)$$

Let

$$B = \frac{u^a + u}{u + 1} + \frac{\overline{u}^a + \overline{u}}{\overline{u} + 1}.$$ 

This yields to

$$G_c(u^a)G(\overline{u}^a) = (c + \overline{c})^2 + (u + \overline{u})^2 c\overline{c} + (c + \overline{c})(u + \overline{u})^a(B + 1) + (B + 1)^2$$

where

$$(B + 1) = \frac{u^a + u}{u + 1} + \frac{\overline{u}^a + \overline{u}}{\overline{u} + 1} + 1$$

$$= \frac{u^{a-1} + \overline{u}^{a-1}}{u + \overline{u}} + (u + \overline{u})^{a-1}$$

$$= \frac{D_{a-1}(u + \overline{u})}{u + \overline{u}} + (u + \overline{u})^{a-1}$$

Now we replace again $1/(u + \overline{u})$ by $\beta$, $c + \overline{c}$ by $T$ and $c\overline{c} = N$. We end up with the following linear equation.

$$N = T^2 \beta^{2a} + T(D_{a-1}(1/\beta)\beta^{a+1} + \beta) + (D_{a-1}(1/\beta)\beta^{a+1} + \beta)^2$$

It is easy to show by induction that the Dickson-Polynomials $D_{a-1}$ for $a = 2^{r-1}$ are of a special type

$$D_{a-1}(X) = \sum_{i=1}^{r-1} X^{2^{r-1}+1-2^i}$$

so we get
6.7. NIHO BENT FUNCTIONS WITH $2^T$ TERMS

\[ H(\beta) := N \]
\[ = T^2 \beta^{2a} + T \left( \sum_{i=0}^{r-1} \beta^{2^i} \right) + \left( \sum_{i=0}^{r-1} \beta^{2^i} \right)^2 \]
\[ = (T^2 + 1) \beta^{2a} + (T + 1) \left( \sum_{i=1}^{r-1} \beta^{2^i} \right) + T \beta \]

If $T = 1$ the preceding equation reduces to

\[ N = \beta \]

and we get a unique solution $\beta$ with $H(\beta) = 0$, as desired in the case where $G_{c}(1) = 0$. So in the sequel we can assume that $T \notin F_2$.

We have to show that there is a unique element $\Delta \neq 0$ with $\text{tr}(\Delta) = 0$, such that $H(\Delta) = 0$. We replace $\Delta$ by $y^2 + y$ where $y \notin F_2$ and get

\[ H(y^2 + y) = T^2(y^2 + y)^{2a} + T \left( \sum_{i=0}^{r} (y^2 + y)^{2^i} \right) + \left( \sum_{i=0}^{r} (y^2 + y)^{2^i} \right)^2 \]
\[ = T^2(y^{4a} + y^{2a}) + T(y^{2a} + y) + (y^{2a} + y)^2 \]
\[ = (T + 1)^2 y^{2a} + (T^2 + T)y^{2a} + y^2 + Ty \]
\[ = ((T + 1)y^{2a} + y) ((T + 1)(y + 1)^{2a} + (y + 1)) \]

Wlog. we assume that

\[ (T + 1)y^{2a-1} + 1 = (T + 1)y^{2r-1} + 1 = 0 \]

which yields to a unique $y$ as

\[ \gcd(2^r - 1, 2^k - 1) = \gcd(r, k) = 1 \]

which proves the theorem.

Remark 6.17. This construction demonstrates the restriction of computer experiments in the following sense. For every $k_0 \in \mathbb{N}$ we can choose $r$ such that $\gcd(k, r_0) \neq 1$ for every $1 < k < k_0$ (e.g. $r = (k_0 - 1)!$). Therefore there are always families of bent functions with a fixed number of terms, that can not be found by computer experiments at all.
Bibliography


