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
3. \( k = 2^{n-1} - 2^{n/2-1}, \lambda = 2^{n-2} - 2^{n/2-1}. \)

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 \textit{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 \textit{m-sequences} can be represented by first choosing a generator \( \alpha \) of \( \mathbb{F}_2^* \) and a non-zero element \( a \in \mathbb{F}_2^n \). The sequence is then defined as

\[
\{ s(t) \} = \{ \text{tr}(aa^t) \mid 0 \leq t \leq 2^n - 2 \}.
\]

Given an integer \( d \) coprime to \( 2^n - 1 \), the sequence \( \{ s(td) \} \) is called a \textit{decimation} of \( \{ s(t) \} \). One of the main characteristic in this topic is the \textit{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

$$\pi|_{\mathbb{F}_{2^{n_1}}} = x^{d_{n_1}} \quad \pi|_{\mathbb{F}_{2^{n_2}}} = x^{d_{n_2}},$$

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 $x \to x^d$ 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.